The nilpotency of finite groups with
an automorphism satisfying an identity\footnote{MSC2010: 20D45 (automorphisms of groups), 20D15 (nilpotent groups), 17B70 (graded Lie algebras).}^†

Wolfgang Alexander Moens

FACULTY OF MATHEMATICS, UNIVERSITY OF VIENNA,
OSKAR-MORGENSTERN-PLATZ 1, 1090 VIENNA, AUSTRIA
E-Mail: Wolfgang.Moens@univie.ac.at
Tel: +43-1-4277-50468

April 2, 2019

Abstract

We generalise the positive solution of the Frobenius conjecture (by J. Thompson) and refinements thereof (by Higman, Kreknin, and Kostrikin). This allows us to also extend the positive solution of the restricted Burnside problem for prime exponents (by Kostrikin) and a generalisation of it (by E. Khukhro).

We do this by studying the structure of groups that admit an automorphism with a prescribed polynomial identity. In fact, to each polynomial \( r(t) = \sum_{\lambda=0}^{d} a_{\lambda} \cdot t^{\lambda} \in \mathbb{Z}[t] \), we assign integer-valued invariants \( \iota_{1} \) and \( \iota_{2} \), and we will prove that they satisfy the following property. Let \( G \) be a finite group with an automorphism \( \alpha : G \to G \) satisfying

\[ \{ x^{a_{0}} \cdot \alpha(x^{a_{1}}) \cdots \alpha^{d}(x^{a_{d}}) \mid x \in G \} = \{ 1_{G} \}. \]

If \( G \) has no \( \iota_{1} \)-torsion, then \( G \) is nilpotent and the subgroup \( \Gamma_{d^{e}+1}(G) \) of the lower central series is a \( \iota_{2} \)-group.

By specialising \( r(t) \) to linear, cyclotomic or Anosov polynomials, we can also recover and extend a number of results in the literature.

\footnote{This work was supported by the Austrian Science Fund (FWF) grants: \( J – 3371 – N^{25} \) ("Representations and gradings of solvable Lie algebras") and \( P30842 – N^{35} \) ("Infinitesimal Lie rings: gradings and obstructions").}
## Contents

1 Introduction  
1.1 Motivation  
1.2 Main results  
1.3 Strategy to prove theorem 1.2.3  
1.4 Overview  

2 Existence of identities  
2.1 Proof of proposition 1.2.1  
2.2 Proof of proposition 1.2.2  
2.3 Examples  
2.4 Constructing regular automorphisms of finite order  

3 Proving the nilpotency of a finite group  
3.1 Special case: solvable groups  
3.2 Proof of theorem 1.3.1  

4 Proving the bounded nilpotency of Lie rings  
4.1 Special case: Lie algebras  
4.2 Proof of theorem 1.3.6  

5 Bounding the class of a nilpotent group  
5.1 Infinitesimal Lie rings of nilpotent groups  
5.2 Proof of theorem 1.3.7  

6 Verifying the technical conditions of our auxiliary theorems  
6.1 Arithmetically-free subsets  
6.2 Proof of proposition 1.3.11  
6.3 The invariant Cong(r(t))  
6.3.1 Reduced resultants  
6.3.2 Examples  
6.4 The invariants Discr∗(r(t)) and Prod( r(t) )  
6.4.1 Integrality and computation  
6.4.2 Examples  

7 Corollaries of the main theorem  
7.1 Periodic groups that are residually-finite  
7.1.1 Special case: p-groups that are residually-finite  
7.1.2 Proof of corollary 1.2.4  
7.2 Regular automorphisms of finite groups  
7.2.1 Special case: finite, solvable groups  
7.2.2 Proof of corollary 1.2.5  

3  

11  

23  

28  

33  

35  

47
1 Introduction

1.1 Motivation

Let us begin by recalling three well-known results in the theory of finite groups and let us see how they have been generalised using identities of automorphisms.

**Theorem 1.1.1** (Rowley [50]). A finite group $G$ is solvable if it admits an automorphism that displaces every element of $G$ other than $1_G$.

Such an automorphism is also called regular or fixed-point-free. Theorem 1.1.1 has a long history, going back to at least Gorenstein—Herstein [18], and it was finally confirmed by means of the classification of the finite, simple groups. We refer to Rowley’s paper for a particularly short proof.

By considering a special case, we can hope to obtain a stronger conclusion.

**Theorem 1.1.2** (J. Thompson [60]). A finite group is nilpotent if it admits a regular automorphism of prime order.

Such automorphisms naturally appear in the study of groups acting simply-transitively on finite sets, and theorem 1.1.2 gives a positive answer to (what is generally known as) the Frobenius conjecture. Thompson’s proof used the celebrated $p$-complement theorem [61] and an earlier result of Witt and Higman, but it did not require the classification of the finite, simple groups.

A follow-up result is:

**Theorem 1.1.3** (Higman [23]; Kreknin—Kostrikin [37, 38]). A nilpotent group $G$ has class at most $(p − 1)^{2(a−1)}$ if $G$ admits a regular automorphism of prime order $p$.

In [23], Higman proved that there exists some (huge) upper bound for $c(G)$ that depends only on $p$. Later, Kreknin and Kostrikin showed in [37, 38] that the bound can be reduced to the much lower value $(p − 1)^{2(a−1)}$. But it is conjectured that the minimal upper bound $h(p)$ on $c(G)$ satisfies $h(p) = [(p^2 − 1)/4]$. This problem has been referred to as the Higman conjecture, and it still open for primes $p \geq 11$. 

3
We next make some elementary, but important, observations that do not use any of the impressive results mentioned above. We suppose that the group $G$ is finite or nilpotent, and we suppose that $\alpha : G \to G$ is a regular automorphism of finite order $n$. Then the transformation $1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1}$ of $G$, defined by $x \mapsto x \cdot \alpha(x) \cdot \alpha^2(x) \cdots \alpha^{n-1}(x)$, vanishes identically. If, moreover, $n$ is a prime, then the group $G$ will have no $n$-torsion.

These observations show that theorem 1.1.1 partially extends to:

**Theorem 1.1.4** (Ersoy [17]). A finite group $G$ is solvable if it admits an automorphism $\alpha : G \to G$ and an odd number $n$ such that the map $1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1}$ vanishes identically.

Such automorphisms naturally appear in the study of automorphisms with finite order and with finite Reidemeister-number [7,30]. Examples show that the oddness of $n$ is necessary, and the proof of theorem 1.1.4 uses the classification of the finite, simple groups.

By specialising to $n$ a prime, we can hope to obtain a stronger result. And, indeed, theorem 1.1.2 extends to:

**Theorem 1.1.5** (Hughes—Thompson [26]; Kegel [33]). A finite group $G$ is nilpotent if it admits an automorphism $\alpha : G \to G$ and a prime $p$ such that the map $1 + \alpha + \cdots + \alpha^{p-1}$ vanishes identically.

Such automorphisms naturally appear in the study of almost-regular automorphisms of prime order by Bettio, Endimioni, Jabara, Wehrfritz, Zappa, and others [7,16]. The solvability of $G$ was proven by Hughes—Thompson using the fundamental results of Hall and Higman about minimal polynomials of operators on finite-dimensional vector spaces [22]. The nilpotency of $G$ is due to Kegel.

We also mention a result that complements theorem 1.1.3. Let $d(G)$ be the minimal cardinality of a generating set for a group $G$. E. Khukhro showed the existence of a map $C : N \times P \to N$ with the following property.

**Theorem 1.1.6** (E. Khukhro [34]). Consider a finite $p$-group $G$ admitting an automorphism $\alpha : G \to G$, for which the map $1 + \alpha + \cdots + \alpha^{p-1}$ vanishes identically. Then the class of $G$ is bounded from above by $C(d(G), p)$.

This theorem applies, in particular, to finite $p$-groups with a partition. By specialising theorem 1.1.6 to finite groups of exponent $p$ (and the automorphism $x \mapsto x$), we also recover Kostrikin’s positive solution of the restricted Burnside problem in exponent $p$. We note that Zel’manov later proved an impressive extension1 of theorem 1.1.6:

**Theorem 1.1.7** (Zel’manov [68]). Consider a $p$-group $G$ that is residually-finite. Suppose that $G$ admits an automorphism $\alpha : G \to G$ such that the map $1 + \alpha + \cdots + \alpha^{p-1}$ vanishes identically. Then $G$ is locally-nilpotent.

---

1We refer to proposition 1 of [68] for a quantitative, but much more technical, version of this result.
Together with J. Wilson’s earlier use of the classification of the finite, simple groups [64], this gave a positive solution of the compact Burnside problem (also known as the Platonov conjecture).

In view of these results, we propose the following family of problems.

**Meta-Problem 1.1.8.** We are given a finite number of polynomials

\[ r_1(t) := \sum_{0 \leq j \leq d_1} a_{1,j} \cdot t^j, \ldots, r_k(t) := \sum_{0 \leq j \leq d_k} a_{k,j} \cdot t^j \]

with integer coefficients, and we are told that some finite group \( G \) admits an endomorphism \( \gamma : G \to G \) such that the map

\[ G \to G : x \mapsto \prod_{1 \leq i \leq k} \prod_{0 \leq j \leq d_i} \gamma^j(x^{a_{i,j}}) \]

vanishes identically. Prove that the group \( G \) is “close to abelian” provided that the torsion of \( G \) is “compatible” with certain invariants of the polynomial \( r(t) := r_1(t) + \cdots + r_k(t) \).

We refer to section 8 for additional, motivating examples with polynomials \( r(t) \) that are linear or Anosov.

### 1.2 Main results

This text aims to give a partial solution to the above Meta-Problem 1.1.8. In order to make our results precise, we first fix some terminology and notation. We consider a group \((G, \cdot)\), together with an endomorphism \( \gamma : G \to G \), and a polynomial \( r(t) := a_0 + a_1 \cdot t + \cdots + a_d \cdot t^d \in \mathbb{Z}[t] \). We say that \( r(t) \) is a **monotone identity** of \( \gamma \) if and only if the map \( r(\gamma) : G \to G \), defined by

\[ x \mapsto x^{r(\gamma)} := x^{a_0} \cdot \gamma(x^{a_1}) \cdots \gamma^d(x^{a_d}) \]

vanishes identically. In this case, we will simply write \( r(\gamma) = 1_G \). More generally, we say that \( r(t) \) is an **identity** of \( \gamma \) if and only if there exists a decomposition \( r(t) = r_1(t) + \cdots + r_k(t) \) of \( r(t) \) into polynomials \( r_1(t), \ldots, r_k(t) \in \mathbb{Z}[t] \), such that the map \( r_1(\gamma) \cdots r_k(\gamma) : G \to G \), defined by

\[ x \mapsto x^{r_1(\gamma) \cdots r_k(\gamma)} \]

vanishes identically. We will abbreviate this to \( r_1(\gamma) \cdots r_k(\gamma) = 1_G \). We will verify in proposition 2.1.3 that the identities of a given endomorphism form an ideal of \( \mathbb{Z}[t] \).

**Existence results.** We begin in section 2 by observing that identities of endomorphisms are easy to obtain — at least in the context of solvable groups.

**Proposition 1.2.1.** Consider a group \( G \) with an endomorphism \( \gamma : G \to G \). If \( G \) admits a subnormal series \( G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} = \{1_G\} \) of \( \gamma \)-invariant subgroups such that each factor \( G_i/G_{i+1} \) is free-abelian of finite rank or elementary-abelian
of finite rank, then the endomorphism $\gamma$ has a monic identity of degree $d(G_1/G_2) + \cdots + d(G_i/G_{i+1})$.

We see, in particular, that automorphisms of virtually-polycyclic groups have an identity of degree equal to the Hirsch-length of the group. We will prove proposition 1.2.1 by generalising the theorem of Cayley—Hamilton. In the other direction, techniques of Higman and the Mal’cev-correspondence give us:

**Proposition 1.2.2.** Consider a monic polynomial $r(t) \in \mathbb{Z}[t]$. Let $\lambda$ and $\mu$ be roots of $r(t)$ in $\mathbb{C}$, and let $k$ be any natural number satisfying $r(\lambda \cdot \mu) = \cdots = r(\lambda \cdot \mu^{k-1}) = 0$. Then there is a finitely-generated, torsion-free, $k$-step nilpotent group $N$ admitting an endomorphism $\beta : N \rightarrow N$ with $r(t)^k$ as an identity.

Such a natural number $k$ always exists and we see that long(er) arithmetic progressions of roots yield groups of high(er) class. We will derive an analogous result for finite groups.

**Structure results.** In definitions 1.3.5 and 1.3.9, we will introduce the integer-valued invariants $\text{Cong}(r(t))$, $\text{Discr}^*(r(t))$, and $\text{Prod}(r(t))$ of a polynomial $r(t) \in \mathbb{Z}[t]$ and we will prove:

**Theorem 1.2.3 (Main).** Consider a finite group $G$, together with an endomorphism $\gamma : G \rightarrow G$, and an identity $r(t)$ of $\gamma$, say of degree $d$. If $G$ has no $(r(1) \cdot \text{Cong}(r(t)))$-torsion, then $G$ is nilpotent and $\Gamma_{d^2+1}(G)$ is a $(\text{Discr}^*(r(t)) \cdot \text{Prod}(r(t)))$-group.

Here, we recall that $G = \Gamma_1(G) \geq \Gamma_2(G) \geq \cdots$ is the lower central series of $G$, defined recursively by $\Gamma_1(G) := G$ and $\Gamma_{k+1}(G) := [\Gamma_k(G), G]$. And, if the order of every element in a group $G$ divides a natural power of a fixed integer $m$, then we say that $G$ is an $m$-group. If $\{1_G\}$ is the only $m$-group contained in $G$, then we say that $G$ has no $m$-torsion.

In section 7.1, we will use standard techniques in order to extend theorem 1.2.3 from finite groups to periodic, residually-finite groups.

**Corollary 1.2.4.** Consider a periodic, residually-finite group $G$, together with an automorphism $\alpha : G \rightarrow G$ and a monic and monotone identity $r(t)$ of degree $d$. If $G$ has no $(r(1) \cdot \text{Cong}(r(t)))$-torsion, then $G$ is locally-nilpotent and $\Gamma_{d^2+1}(G)$ is a $(\text{Discr}^*(r(t)) \cdot \text{Prod}(r(t)))$-group.

In section 7.2, we will (implicitly) use the classification of the finite, simple groups in order to give a more general answer to Meta-Problem 1.1.8:

**Corollary 1.2.5.** Consider a finite group $G$ admitting a regular automorphism $\alpha : G \rightarrow G$ and let $r(t)$ be an identity $r(t)$ of $\alpha$, say of degree $d$. Then $G$ is a split extension of a solvable $(r(1) \cdot \text{Cong}(r(t)) \cdot \text{Discr}^*(r(t)) \cdot \text{Prod}(r(t)))$-group by a nilpotent group of class at most $d^2$. 
Applications. Once we have obtained a partial answer to Meta-Problem 1.1.8, it makes sense to consider applications. In subsection 8.1, we will specialise our main results to linear polynomials. This will allow us to extend a classic result (of Baer [4], Schenkmman—Wade [51], and J. Alperin [2]) about the structure of finite groups admitting a universal power automorphism:

Proposition 1.2.6. Consider a finite group $G$ admitting an endomorphism with a linear identity $a_0 + a_1 \cdot t \in \mathbb{Z}[t]$. If $\gcd(|G|, a_0 \cdot a_1 \cdot (a_0 + a_1)) = 1$, then $G$ is abelian.

In subsection 8.2, we will specialise our theorems to cyclotomic polynomials. Let us say that an automorphism $\alpha : G \to G$ is cyclotomic of natural index $n > 1$ if the cyclotomic polynomial $\Phi_n(t)$ is a monotone identity of $\alpha$, i.e.: $\Phi_n(\alpha) = 1_G$. Let us also say that an automorphism is cyclotomic if it is cyclotomic of some index $n > 1$. Theorem 1.1.2 of Thompson and theorem 1.1.5 of Hughes—Thompson and Kegel then extend to:

Theorem 1.2.7. A residually-finite group is locally-nilpotent if it admits a cyclotomic automorphism.

Theorem 1.1.3 of Higman and Kreknin—Kostrikin, and theorem 1.1.6 of Khukhro further extend to:

Theorem 1.2.8. Consider a locally-nilpotent group $G$ with a cyclotomic automorphism of index $n > 1$ and let $p$ be the largest prime divisor of $n$. Then every finitely-generated subgroup $N$ of $G$ is nilpotent of class $c(N) \leq \max\{\frac{(p - 1)}{2}, C(p \cdot d(N), p)\}$.

In subsection 8.2, we will also recover two recent results of Jabara about automorphisms with finite Reidemeister-number (cf. corollaries 8.2.7 and 8.2.8).

Corollary 1.2.9 (Theorem A of Jabara [30]). Consider a residually-finite group $G$ admitting an automorphism $\alpha : G \to G$ of prime order $p$. If the Reidemeister-number of $\alpha$ is finite, then $G$ has an $\alpha$-invariant subgroup $N$ of finite index that is nilpotent of class $c(N) \leq (p - 1)^2$.

Let $A : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be the map in J. Alperin’s theorem 1 of [1].

Corollary 1.2.10 (Theorem B of Jabara [30]). Consider a finitely-generated, solvable group $G$ with an automorphism $\alpha : G \to G$ of prime order $p$. If the Reidemeister-number $n$ of $\alpha$ is finite, then $G$ has a finite-index subgroup $N$ that is nilpotent of class $c(N) \leq (p - 1)^2 + A(p, n) + (p - 1)^2$.

We note that Jabara’s proofs of these corollaries implicitly used the classification of the finite simple groups, as well as Zel’manov’s positive solution of the restricted Burnside problem in arbitrary exponent, and the theorems of Hartley, Hartley—Meixner, Fong, and Khukhro (cf. corollary 5.4.1 of [35]). Our proofs, on the other hand, avoid all of these rather difficult results.

In subsection 8.3, we will specialise our results to Anosov polynomials. This will allow us to make a minor contribution related to S. Smale’s problem about the existence of
Anosov diffeomorphisms on compact manifolds (see proposition 8.3.3). In subsection 8.4, we will show (by means of explicit examples) why our methods must fail for polynomials of the form $\Psi_n(t) := (t^n - 1)/(t - 1) = 1 + t + \cdots + t^{n-1}$, with $n \in \mathbb{N} \setminus \mathbb{P}$.

1.3 Strategy to prove theorem 1.2.3

Proving the nilpotency of a finite group. For a polynomial $r(t) := a_0 + a_1 \cdot t + \cdots + a_d \cdot t^d \in \mathbb{Z}[t]$ and integers $u > j \geq 0$, we define the partial sum

$$r_{u,j}(t) := \sum_{i \equiv j \mod u} a_i \cdot t^i,$$

so that we obtain the periodic decomposition $r(t) = r_{u,0}(t) + \cdots + r_{u,u-1}(t)$ of $r(t)$. In section 3, we will extend techniques of Higman [23, 24] and J. Thompson [60] in the context of the Frobenius conjecture in order to prove the technical result:

**Theorem 1.3.1.** Consider a finite group $G$ admitting a regular automorphism $\alpha : G \rightarrow G$, and an identity $r(t)$ of $\alpha$. Suppose that, for every prime $q$ dividing $|G|$, and for every natural $2 \leq u \leq \deg(r(t)) + 1$, we have

$$\gcd_{0 \leq j \leq u-1} (r_{u,j}(t) \mod q) = 1_{\mathbb{F}_q}. $$

Then $G$ is nilpotent.

Condition (1) can be verified efficiently by means of the Euclidean algorithm in $\mathbb{F}_q[t]$.

The nilpotency and bounded nilpotency of Lie rings. Let us briefly recall a definition and a recent result about the nilpotency of graded Lie rings. A finite subset $X$ of an abelian group $(A, \cdot)$ is arithmetically-free if and only if, for each $x$ and $y$ in $X$, there exists a natural number $n$ such that the element $x \cdot y^n$ is not in $X$.

**Example 1.3.2.** The roots of a polynomial $r(t) := a_d \cdot t^d + \cdots + a_1 \cdot t + a_0 \in \mathbb{Z}[t]$ form an arithmetically-free subset $X$ of $(\mathbb{Q}^\times, \cdot)$ in each of the following cases: $X$ is product-free and $r(0) \neq 0$; $r(t)$ is irreducible and $r(0) \cdot r(1) \neq 0$; $r(t)$ is an Anosov polynomial, or more generally:

$$r(0) \cdot \prod_{1 \leq u \leq d} \det(\text{circ}_{0 \leq j \leq u-1}(r_{u,j}(1))) \neq 0.$$

This property is particularly relevant when trying to prove the nilpotency of graded Lie rings.

**Theorem 1.3.3** (Moens [44, 45]). For every finite, arithmetically-free subset $X$ of the multiplicative group $(\mathbb{F}^\times, \cdot)$ of a field $\mathbb{F}$, there exists a minimal natural number $H(X, \mathbb{F}^\times)$ with the following property. Consider a decomposition

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

8
of a Lie ring \( L \) into additive subgroups \( L_\lambda \) that are labeled by the elements \( \lambda \) of \( \mathbb{F}^\times \), and suppose that for all labels \( \lambda, \lambda' \in \mathbb{F}^\times \), we have the inclusion

\[
[L_\lambda, L_{\lambda'}] \subseteq L_{\lambda \lambda'}.
\]

Suppose further that the support \( \{ \lambda \in \mathbb{F}^\times | \lambda \neq \{0_L\} \} \) of this grading is contained in \( X \). Then \( L \) is nilpotent and

\[
c(L) \leq H(X, \mathbb{F}^\times) \leq |X|^{2|X|}.
\]

**Example 1.3.4.** For a prime \( p \), let \( X_p \) be the set of primitive \( p' \)th roots of unity in \( \mathbb{Q}^\times \). Higman showed in [23] that \( H(X_p, \mathbb{Q}^\times) \) is well-defined and at least \( [(p^2 - 1)/4] \). Kreknin and Kostrikin later showed in [37, 38] that \( H(X_p, \mathbb{Q}^\times) \leq (p-1)^{2^{(p-1)}} \).

In order to apply this theorem to Lie rings with an endomorphism satisfying an identity, we introduce two invariants.

**Definition 1.3.5** \((\text{Discr}_s(r(t)))\) and \((\text{Prod}(r(t)))\). Consider a polynomial \( r(t) \in \mathbb{Z}[t] \). If \( r(t) \) is constant, we define \( \text{Discr}_s(r(t)) := r(t) \) and \( \text{Prod}(r(t)) := 1 \). Else, we let \( a \) be the leading coefficient of \( r(t) \), we let \( \lambda_1, \ldots, \lambda_l \) be the distinct roots of \( r(t) \) with corresponding multiplicities \( m_1, \ldots, m_l \), and we set \( m := \max\{m_1, \ldots, m_l\} \). We then define

\[
\text{Discr}_s(r(t)) := a^{1+2d^2} \cdot (m-1)! \cdot \prod_{1 \leq i,j \leq l, i \neq j} (\lambda_i - \lambda_j)^m
\]

and

\[
\text{Prod}(r(t)) := a^{2d^3} \cdot \prod_{1 \leq i,j \leq l, r(\lambda_i \lambda_j) \neq 0} r(\lambda_i \cdot \lambda_j) = a^{2d^3} \cdot \prod_{1 \leq i,j,k \leq l, r(\lambda_i \lambda_j \lambda_k) \neq 0} a \cdot (\lambda_i \cdot \lambda_j - \lambda_k)^m.
\]

We will show in lemmas 6.4.1 and 6.4.3 that \( \text{Discr}_s(r(t)) \) and \( \text{Prod}(r(t)) \) are integer-valued and non-zero invariants of \( r(t) \) unless \( r(t) \) is itself the zero polynomial. In section 4, we will use these invariants to prove:

**Theorem 1.3.6.** Consider a Lie ring \( L \), together with an endomorphism \( \gamma : L \rightarrow L \) of the Lie ring, and a non-zero polynomial \( r(t) \in \mathbb{Z}[t] \) satisfying \( r(\gamma) = 0_L \). Suppose that the roots of \( r(t) \) form an arithmetically-free subset \( X \) of \( (\mathbb{Q}^\times, \cdot) \). Then the additive group of the lower central ideal \( \Gamma_{H(X, \mathbb{Q}^\times)+1}(L) \) of \( L \) is a \((\text{Discr}_s(r(t)) \cdot \text{Prod}(r(t)))\)-group.

We will prove the theorem by combining theorem 1.3.3 with classic techniques of Higman [23, 24], Kreknin [37], Kostrikin [38], and E. Khukhro [35].

**A bound on the class of a nilpotent group.** These results about the structure of Lie rings can easily be lifted to the analogous results about the structure of nilpotent groups (cf. section 5):

**Theorem 1.3.7.** Consider a nilpotent group \( G \), together with an automorphism \( \alpha : G \rightarrow G \), and a non-zero identity \( r(t) \) of \( \alpha \). Suppose that the roots of \( r(t) \) form an arithmetically-free subset \( X \) of \( (\mathbb{Q}^\times, \cdot) \). Then \( \Gamma_{H(X, \mathbb{Q}^\times)+1}(G) \) is a \((\text{Discr}_s(r(t)) \cdot \text{Prod}(r(t)))\)-group.
This infinitesimal approach should not really come as a surprise. Indeed, infinitesimal Lie rings were used with great efficiency in the proof of theorem 1.1.3 by Higman and Kreknin—Kostrikin and in the proof of 1.1.6 by (Kostrikin and) E. Khukhro. They were also crucial in Zel’manov’s solution of the restricted Burnside problem [66,67] and in the vast generalisation of that result to pro-$p$ groups with an identity [70] (using the commutator collection process of Wilson—Zel’manov [65] and Lazard’s well-known linearity-criterion of [39]). Infinitesimal Lie rings and their gradings also appeared in solutions of the co-class conjectures (of Leedham-Green and Newman) by Shalev—Zel’manov [52] and Shalev [54].

We refer to the literature for more examples of how certain problems about residually-finite groups can be solved by studying the correct Lie ring corresponding with that group and problem (e.g.: the book [35] and the surveys [24,56,57,69]).

**Corollary 1.3.8.** If the group $G$ of theorem 1.3.7 has no $(\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t)))$-torsion, then $c(G) \leq H(X, \mathbb{Q}^\times)$. In contrast: if the roots of $r(t)$ do not form an arithmetically-free subset of $\mathbb{Q}^\times$, then proposition 1.2.2 gives us finitely-generated, torsion-free, nilpotent groups $N$ of arbitrarily large class $k$ such that $r(t)^k$ is an identity of some automorphism of $N$.

**Proof of our main theorem 1.2.3.** In order to combine our two auxiliary results, we introduce some more terminology.

**Definition 1.3.9 (Cong$(r(t))$).** We define the periodic congruence number $\text{Cong}(r(t))$ of a polynomial $r(t) \in \mathbb{Z}[t]$ to be the (unique) non-negative generator of the (principal) $\mathbb{Z}$-ideal

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

One can easily check, by evaluating in $t = 0$, that $r(0) \mid \text{Cong}(r(t))$.

**Example 1.3.10.** If an irreducible polynomial $r(t) \in \mathbb{Z}[t]$ does not coincide with any of its partial sums $r_{u,j}(t)$ (where $u \geq 2$), then $\text{Cong}(r(t)) \neq 0$.

In subsection 6.2, we will use this invariant to verify the technical conditions of our auxiliary theorems 1.3.1 and 1.3.7:

**Proposition 1.3.11.** Consider a polynomial $r(t) \in \mathbb{Z}[t]$ and a field $\mathbb{F}$ of characteristic $q \geq 0$. If $q$ does not divide $r(1) \cdot \text{Cong}(r(t))$, then property (1) holds and the roots of $r(t) \mod q$ in $\mathbb{F}$ form an arithmetically-free subset of the multiplicative group $(\mathbb{F}^\times, \cdot)$.

We can finally prove our main theorem 1.2.3:

**Proof.** Suppose that $\gamma$ maps an element $x$ of $G$ to $x$ or $1_G$. Then $x^{r(1) \cdot r(0)} = 1_G$, so that also $x^{\gamma(\text{Cong}(r(t)))} = 1_G$. Since $\gcd(|G|, r(1) \cdot \text{Cong}(r(t))) = 1$, we conclude that $x = 1_G$.

This observation proves that $\gamma$ is injective and therefore an automorphism of the finite
group \( G \). It also proves that \( \gamma \) is regular.

According to proposition 1.3.11, we may apply theorem 1.3.1 in order to conclude that \( G \) is nilpotent. Proposition 1.3.11 also implies that the of roots \( r(t) \) form an arithmetically-free subset \( X \) of \((\mathbb{Q}^\times, \cdot)\) of cardinality at most \( d \). So we may apply theorem 1.3.7 in order to conclude that \( \Gamma_{d^{d^2+1}}(G) \) is a \((\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t)))\)-group.

1.4 Overview

In section 2, we will prove propositions 1.2.1 and 1.2.2 about the existence of identities. In sections 3, 4, and 5, we prove the three steps in our proof of our main theorem 1.2.3: theorem 1.3.1, theorem 1.3.6, and theorem 1.3.7. In section 6, we briefly discuss the invariants \( \text{Cong}(r(t)), \text{Discr}_*(r(t)), \) and \( \text{Prod}(r(t)) \) of a polynomial \( r(t) \in \mathbb{Z}[t] \). We will show how to compute them in general and in special cases. In section 7, we prove corollaries 1.2.4 and 1.2.5. Finally, in section 8, we specialise our results to linear identities, cyclotomic identities, Anosov identities, and split identities.

2 Existence of identities

2.1 Proof of proposition 1.2.1

In view of our main results, it makes sense to inquire about the general existence of identities.

**Problem 2.1.1.** We are given a group \( G \) and an endomorphism \( \alpha : G \rightarrow G \). Construct a (non-trivial) identity \( r(t) \) of the endomorphism.

Elementary examples show that we cannot expect a positive solution to problem 2.1.1 for arbitrary groups \( G \). But we claim that the automorphisms of a finitely-generated, torsion-free, nilpotent group come with a non-trivial identity. In order to make this precise, we first make a basic observation.

**Lemma 2.1.2 (Composition of polynomial maps).** Let \( m, k_1, \ldots, k_m \in \mathbb{N} \) and let

\[
u(1,1)(t), \ldots, \nu(1,k_1)(t), \ldots, \nu(m,1)(t), \ldots, \nu(m,k_m)(t)\]

be polynomials with integer coefficients. Then there exists an \( n \in \mathbb{N} \) and polynomials \( s_1(t), \ldots, s_n(t) \in \mathbb{Z}[t] \) such that

\[
\prod_{1 \leq j \leq m} \sum_{1 \leq i \leq k_j} \nu_{(j,i)}(t) = s_1(t) + \cdots + s_n(t)
\]

and such that for all group endomorphisms \( \gamma : G \rightarrow G \), we have the equality of maps

\[
(\nu_{(m,1)}(\gamma) \cdots \nu_{(m,k_m)}(\gamma)) \circ \cdots \circ (\nu_{(1,1)}(\gamma) \cdots \nu_{(1,k_1)}(\gamma)) = s_1(\gamma) \cdots s_n(\gamma).
\]

(2)

In particular: if (2) vanishes identically, then \( \prod_i \sum_i \nu_{(j,i)}(t) \) is an identity of \( \gamma \).
The proof is a simple induction on \( m \in \mathbb{N} \), and we leave it to the reader. As an immediate consequence, we obtain:

**Proposition 2.1.3.** Let \( G \) be a group and let \( \gamma : G \to G \) be an endomorphism of \( G \). Then the identities of \( \gamma \) form an ideal of \( \mathbb{Z}[t] \).

**Proof.** Let \( r(t) \) and \( s(t) \) be identities of \( \gamma \) and let us show that \( r(t) + s(t) \) is again an identity of \( \gamma \). By assumption, there exist decompositions \( r(t) = r_1(t) + \cdots + r_n(t) \) and \( s(t) = s_1(t) + \cdots + s_m(t) \) such that \( r_1(\gamma) \cdots r_n(\gamma) = 1_G = s_1(\gamma) \cdots s_m(\gamma) \). Then, obviously, we also have \( r_1(\gamma) \cdots r_n(\gamma) \cdot s_1(\gamma) \cdots s_m(\gamma) = 1_G \), so that \( \sum_i r_i(t) + \sum_j s_j(t) = r(t) + s(t) \) is an identity of \( \gamma \).

Now let \( r(t) \) be an identity of \( \gamma \) and let \( s(t) \in \mathbb{Z}[t] \) be a polynomial. In order to show that \( r(t) \cdot s(t) \) is again an identity of \( \gamma \), we first consider a decomposition \( r(t) = r_1(t) + \cdots + r_n(t) \) of \( r(t) \) such that \( r_1(\gamma) \cdots r_n(\gamma) = 1_G \). Next, we use lemma 2.1.2 to find, for each \( 1 \leq j \leq n \), a natural number \( k_j \in \mathbb{N} \) and polynomials \( u_{(j,1)}(t), \ldots, u_{(j,k_j)}(t) \in \mathbb{Z}[t] \) such that \( s(t) \cdot r_j(t) = u_{(j,1)}(t) + \cdots + u_{(j,k_j)}(t) \) and such that \( r_j(\gamma) \cdot s(\gamma) = u_{(j,1)}(\gamma) \cdots u_{(j,k_j)}(\gamma) \). We then need only verify that \( s(t) \cdot r(t) = \sum_j s(t) \cdot r_j(t) = \sum_j \sum_i u_{(j,i)}(t) \) and that, for an arbitrary \( x \in G \), we have:

\[
1_G = \prod_{1 \leq j \leq n} \left( x^{s(\gamma)} \right)^{r_j(\gamma)} = \prod_{1 \leq j \leq n} \prod_{1 \leq i \leq k_j} x^{u_{(j,i)}(\gamma)} = x^{u_{(1,1)}(\gamma)} \cdots x^{u_{(n,k_n)}(\gamma)}. \]

\( \square \)

**Lemma 2.1.4.** Consider a group \( G \) with an endomorphism \( \gamma : G \to G \). Suppose that \( G \) admits a subnormal series \( G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_l \supseteq G_{l+1} = \{1_G\} \) of \( \gamma \)-invariant subgroups and identities \( r_1(t), \ldots, r_l(t) \in \mathbb{Z}[t] \) of the induced endomorphisms \( \gamma_{G_l/G_{l+1}} : G_l/G_{l+1} \to G_l/G_{l+1} \) on the factors \( G_l/G_{l+1} \). Then \( r_1(t) \cdots r_l(t) \) is an identity of \( \gamma \).

**Proof.** For each \( r_j(t) \), there exists a \( k_j \in \mathbb{N} \) and polynomials \( u_{(j,1)}(t), \ldots, u_{(j,k_j)}(t) \in \mathbb{Z}[t] \) such that \( \sum_i u_{(j,i)}(t) = r_j(t) \) and such that \( u_{(j,1)}(\gamma_{G_l/G_{l+1}}) \cdots u_{(j,k_j)}(\gamma_{G_l/G_{l+1}}) = 1_{G_l/G_{l+1}} \). So the map \( u_{(j,1)}(\gamma) \cdots u_{(j,k_j)}(\gamma) \) sends \( G_j \) into \( G_{j+1} \). The composition of these maps therefore vanishes on all of \( G \). Lemma 2.1.2 now implies that \( \prod_j \sum_i u_{(j,i)}(t) = r_1(t) \cdots r_l(t) \) is an identity of \( \gamma \).

\( \square \)

**Proposition 2.1.5** (Cayley–Hamilton). Consider a group \( G \) with an endomorphism \( \gamma : G \to G \). If \( G \) admits a subnormal series \( G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_l \supseteq G_{l+1} = \{1_G\} \) of \( \gamma \)-invariant subgroups such that every factor \( G_l/G_{l+1} \) is free-abelian of finite rank or elementary-abelian of finite rank, then the endomorphism \( \gamma \) has a monic identity \( \chi(t) \) of degree \( d(G_1/G_2) + \cdots + d(G_l/G_{l+1}) \).

**Proof.** If \( G_l/G_{l+1} \) is free-abelian, then we may compute the characteristic polynomial \( \chi_l(t) = \det(t \cdot I_{G_l/G_{l+1}} - \gamma_{G_l/G_{l+1}}) \in \mathbb{Z}[t] \) of the induced endomorphism \( \gamma_{G_l/G_{l+1}} \). Else, the factor \( G_l/G_{l+1} \) is elementary-abelian, say isomorphic to \( (\mathbb{Z}_p^k, +) \), so that we may
compute the characteristic polynomial \( \chi_i(t) \in \mathbb{F}_p[t] \) of \( \gamma_{G_i/G_{i+1}} \) over the field \( \mathbb{F}_p \). There then exists a monic polynomial \( \chi_i(t) \in \mathbb{Z}[t] \) of the same degree \( k \) as \( \chi_i(t) \) such that \( \chi_i(t) \equiv \chi_i(t) \mod p = \chi_i(t) \). According to the (classic) theorem of Cayley—Hamilton and lemma 2.1.4, the product

\[
\chi(t) := \chi_1(t) \cdot \chi_2(t) \cdots \chi_l(t) \in \mathbb{Z}[t],
\]

is an identity of \( \gamma \), and \( \chi(t) \) clearly has degree \( d(G_1/G_2) + \cdots + d(G_i/G_{i+1}) \). Since each \( \chi_i(t) \) is monic, so is \( \chi(t) \).

If all the factors \( G_i/G_{i+1} \) in theorem 2.1.5 are free-abelian of finite rank, then the polynomial \( \chi(t) \) is uniquely determined by this construction, so that we may refer to \( \chi(t) \) as the characteristic polynomial of the endomorphism with respect to the series \( (G_i)_i \). One can verify that if \( G \) is a finitely-generated, torsion-free, nilpotent group, then the factors \( \Gamma_i^*(G)/\Gamma_{i+1}^*(G) \) will all be free-abelian of finite rank.

**Corollary 2.1.6.** Consider a virtually-poly cyclic group \( N \). Then every automorphism \( \alpha : N \rightarrow N \) of \( N \) admits an identity \( r(t) \) of degree equal to the Hirsch-length of \( N \).

**Proof.** Let us consider a characteristic series \( N \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_l \trianglerighteq G_{l+1} = \{1_N\} \), such that \( N/G_1 \) is finite and such that all the factors \( G_i/G_{i+1} \) are free-abelian of finite rank. Then the constant polynomial \( |N/G_1| \) is an identity of the induced automorphism on \( N/G_1 \). Now let \( \chi(t) \) be the characteristic polynomial of the induced automorphism \( \alpha_{G_i} : G_i \rightarrow G_i \) with respect to the series \( G_1 \trianglerighteq \cdots \trianglerighteq G_l \trianglerighteq G_{l+1} = \{1_G\} \), as in proposition 2.1.5. Then lemma 2.1.4 shows that \( r(t) := |N/G_1| \cdot \chi(t) \in \mathbb{Z}[t] \) is an identity of \( \alpha \) and it has the correct degree.

We conclude with some remarks that will be useful later on.

**Remark 2.1.7.** Assume that the \( \gamma \) of theorem 2.1.5 is an automorphism. If \( \gamma(0) = \pm 1 \), then every \( \gamma \)-invariant subgroup \( M \) of \( G \) is also \( \langle \gamma \rangle \)-invariant, so that the induced map \( \gamma_M : M \rightarrow M \) is an automorphism of \( G \).

**Proof.** It suffices to show that \( \gamma^{-1}(M) \subseteq M \). One can use induction on \( l \in \mathbb{N} \) to show that for every \( x \in M \), we have \( (\chi_1(\gamma) \cdots \chi_l(\gamma))(x) \in x^{(0)} \cdot \gamma(M) \). Then theorem 2.1.5 gives \( I_G \in x^{(0)} \cdot \gamma(M) \). So, if \( \chi(0) = \pm 1 \), then \( \gamma^{-1}(x) \in M \).

**Remark 2.1.8.** Assume that the \( \gamma \) of theorem 2.1.5 is an automorphism. If \( \chi(0) \cdot \chi(1) = \pm 1 \), then \( \gamma \) is regular and uniform in the sense that the map \( -1 + \gamma : G \rightarrow G : x \mapsto x^{-1} \cdot \gamma(x) \) is injective and surjective.

**Proof.** Suppose that \( \chi(0) \cdot \chi(1) = \pm 1 \). The automorphism is regular since any fixed point \( x \) of \( \gamma \) satisfies \( x^{\pm 1} = x(1) = 1_G \). In order to prove the uniformity of \( \gamma \), it suffices to prove that each of the induced automorphisms \( \gamma_{G_i/G_{i+1}} \) is uniform (cf. lemma 1.6 of [29]). The condition \( \chi(1) = \pm 1 \) implies that \( \chi_1(1), \ldots, \chi_l(1) \in \{\pm 1\} \). The latter is equivalent to \( \det(\gamma_{G_i/G_{i+1}} - I_{G_i/G_{i+1}}), \ldots, \det(\gamma_{G_i/G_{i+1}} - I_{G_i/G_{i+1}}) \in \{\pm 1\} \) (since the factors
$G_i / G_{i+1}$ are abelian, we use the additive notation for them.). The latter implies that the maps $\gamma G_i / G_2 = \mathbb{I} G_i / G_2, \ldots, \gamma G_i / G_{i+1} = \mathbb{I} G_i / G_{i+1}$ are isomorphisms. This means that the automorphisms $\gamma G_i / G_2, \ldots, \gamma G_i / G_{i+1}$ are (regular and) uniform.

**Remark 2.1.9** (Lemma 2.4 of Endimioni [16]). Consider a virtually-polycyclic group $G$ of Hirsch-length $l$, together with an automorphism $\alpha : G \longrightarrow G$ of finite order $m$. Suppose that $\alpha$ fixes only finitely-many elements. Then $G$ has a characteristic subgroup $N$ of finite index such that $(1 + t + \cdots + t^{m-1})^l$ and $m^l - 1 = (1 + t + \cdots + t^{m-1})$ are identities of the induced automorphism $\alpha_N : N \longrightarrow N$.

**Proof.** Let us abbreviate $\Psi_m(t) := 1 + t + \cdots + t^{m-1}$ and let us consider the map $\Psi_m(\alpha) : G \longrightarrow G$. Endimioni’s lemma shows that the $l$-fold composition $\Psi_m(\alpha)^l$ vanishes on a characteristic, polycyclic subgroup $N$ of finite index in $G$. Lemma 2.1.2 then implies that $\Psi_m(t)^l$ is an identity of the induced automorphism $\alpha_N$. Since the identities of $\alpha_N$ form an ideal of $\mathbb{Z}[t]$, and since $t^m - 1 = (t - 1) \cdot \Psi_m(t)$ is an identity of $\alpha_N$, we see that also $\text{Res}(t - 1, \Psi_m(t)^l) \cdot \Psi_m(t) = \pm m^{l-1} \cdot \Psi_m(t)$ is an identity of $\alpha_N$. 

### 2.2 Proof of proposition 1.2.2

We have just seen that every endomorphism of a finitely-generated, torsion-free, nilpotent group comes with a family of monic identities (the characteristic polynomials). It is natural to also consider the converse problem:

**Problem 2.2.1.** We are given a monic polynomial $r(t) \in \mathbb{Z}[t]$. Construct a finitely-generated, torsion-free, nilpotent group $G$ and an endomorphism $\gamma : G \longrightarrow G$ such that $r(t)$ is an identity of the endomorphism $\gamma$.

We will show, in several steps, that this problem has a positive answer. We begin by proving the corresponding statement for Lie algebras.

**Proposition 2.2.2.** Consider a monic polynomial $r(t) \in \mathbb{Z}[t]$ with $r(0) \neq 0$. Let $\lambda$ and $\mu$ be roots of $r(t)$ in $\mathbb{Q}$, and let $k$ be any natural number satisfying $r(\lambda \cdot \mu) = \cdots = r(\lambda \cdot \mu^{k-1}) = 0$. Then there is a finitely-generated, $k$-step nilpotent Lie algebra $L$ over the rational numbers with an automorphism $\overline{\gamma} : L \longrightarrow L$ such that $r(\overline{\gamma}) = 0_L$.

**Proof.** According to proposition 2.1.3, the identities of an endomorphism form an ideal of $\mathbb{Z}[t]$. So we may assume that $r(t)$ is square-free and that $\text{Discr} r(t) \neq 0$. If $k = 1$, then we simply consider the companion operator $\gamma : \mathbb{Q}^{\deg(r(t))} \longrightarrow \mathbb{Q}^{\deg(r(t))}$ of $r(t)$ on the abelian group $(\mathbb{Q}^{\deg(r(t))}, +)$. It is well-known that this endomorphism $\gamma$ satisfies $r(\gamma) = 0_{\mathbb{Q}^{\deg(r(t))}}$.

So we may further assume that $k \geq 2$. We let $F$ be the free $k$-step nilpotent Lie algebra (over the rational numbers) on the generators $x_{1,1}, \ldots, x_{1,d}, x_{2,1}, \ldots, x_{2,d}$. Let $C \in \text{GL}_d(\mathbb{Q})$ be the companion operator of $r(t)$ and let $A$ be the direct sum $C \oplus C \in \text{GL}_{2d}(\mathbb{Q}) \cap \text{Mat}_{2d,2d}(\mathbb{Z})$. This $A$ defines a linear transformation of the $\mathbb{Q}$-span of the generators of $F$ (in the obvious way) and $A$ extends (in a unique way) to an automorphism
α : F → F of the Lie algebra F. We now consider the ideal I of F that is generated by the subset \{r(α)(F)\} of F. This ideal is \langle α \rangle-invariant, so that we may consider the quotient Lie algebra \( L := F/I \) with the induced automorphism \( \overline{α} : L \rightarrow L \). By construction, we have \( r(\overline{α}) = 0_L \).

In order to prove that \( c(L) ≥ k \), we may assume that L has coefficients in the complex numbers. Indeed, the larger Lie algebra \( L^C := L \otimes_\mathbb{R} \mathbb{C} \) over the complex numbers satisfies \( c(L) = c(L^C) \) and it naturally admits the automorphism \( \overline{α}^C := \overline{α} \otimes 1 \) satisfying \( r(\overline{α}^C) = 0_{L^C} \).

Let \( V \) be the (complex) span of the generators \( x_{1,1, \ldots, x_{2,d}} \). Since \( r(t) \) has no repeated roots, the operator \( C \in GL_d(\mathbb{Q}) \) can be diagonalised over \( \mathbb{C} \). So we may choose an ordered eigenbasis \( \{(y_{1,1}, \ldots, y_{1,d}, \ldots, y_{2,d})\} \) of \( V \) and scalars \( λ_1, \ldots, λ_d, μ_1, \ldots, μ_d \in \mathbb{C} \) such that, for each \( i \in \{1, 2\} \) and \( j \in \{1, \ldots, d\} \), we have

\[
\alpha(y_{i,j}) = \lambda_j \cdot y_{i,j} \quad \text{and} \quad \alpha(y_{2,j}) = μ_j \cdot y_{2,j}.
\]

It is clear that \( \{λ_1, \ldots, λ_d\} = \{μ_1, \ldots, μ_d\} \) is the set of roots of \( r(t) \). After permuting these basis vectors, may further assume that

\[
r(μ_2) = r(λ_1) = r(\lambda_1 \cdot μ_2) = \cdots = r(\lambda_1 \cdot μ_2^{k-1}) = 0.
\]

Let us define a partial order on the elements of \( \text{Mat}_{2,d}(\mathbb{Z}) \). For \( a = (a_{i,j})_{i,j}, b = (b_{i,j})_{i,j} \in \text{Mat}_{2,d}(\mathbb{Z}) \) we write \( a ≤ b \) if and only if \( a_{1,1} ≤ b_{1,1}, \ldots, a_{2,d} ≤ b_{2,d} \). For each element \( a \in \text{Mat}_{2,d}(\mathbb{Z}) \) satisfying \( 0 ≤ a \), we define the family \( \mathcal{B}(a) \) of all left-normed Lie monomials in the eigenvectors \( y_{1,1}, \ldots, y_{2,d} \) such that each \( y_{i,j} \) appears with multiplicity exactly \( a_{i,j} \). For the remaining \( a \), we define \( \mathcal{B}(a) := \emptyset \). If \( F(a) = \langle \mathcal{B}(a) \rangle \) denotes the (complex) span of \( \mathcal{B}(a) \), then we naturally obtain the grading

\[
F = \bigoplus_{a \in \text{Mat}_{2,d}(\mathbb{Z})} F(a)
\]

of the Lie algebra F by the grading group \( \langle \text{Mat}_{2,d}(\mathbb{Z}), + \rangle \).

In order to understand the structure of the ideal I, we introduce some notation. For left-normed monomials \([v_1, \ldots, v_i]\) and \([w_1, \ldots, w_j]\), we define the expression

\[
[[v_1, \ldots, v_i]; [w_1, \ldots, w_j]] := [v_1, \ldots, v_i, w_1, \ldots, w_j].
\]

For each \( a \in \text{Mat}_{2,d}(\mathbb{Z}) \), we define the \( \mathbb{C} \)-span

\[
I(a) = \sum_{0 ≤ b, c ∈ \text{Mat}_{2,d}(\mathbb{Z}) \atop c ≤ b + c = a} r(A_b) \cdot [[v; w] | v ∈ \mathcal{B}(b), w ∈ \mathcal{B}(c)],
\]

where

\[
A_b := \left( \prod_{1 ≤ j ≤ d} λ_j^{b_{1,j}} \right) \cdot \left( \prod_{1 ≤ j ≤ d} μ_j^{b_{2,j}} \right) ∈ \mathbb{C}.
\]
By construction, we have $I = \sum_{a \in \text{Mat}_{2,d}(\mathbb{Z})} I(a)$. Since we also have the inclusions $I(a) \subseteq F(a)$, we derive from (i) the direct sum decomposition

$$I = \bigoplus_{a \in \text{Mat}_{2,d}(\mathbb{Z})} I(a).$$

Since $I(a) \subseteq F(a)$, we conclude that the Lie algebra $L$ is also graded:

$$L = \bigoplus_{a \in \text{Mat}_{2,d}(\mathbb{Z})} L(a),$$

with homogeneous components $L(a) := F(a)/I(a)$. Since

$$\Gamma_k(L) = \bigoplus_{0 \leq a \in \text{Mat}_{2,d}(\mathbb{Z})} \sum_{i,j} a_{i,j} = k L(a),$$

we need only show that there exists an $a \in \text{Mat}_{2,d}(\mathbb{Z})$ with $\sum_{i,j} a_{i,j} = k$ and $I(a) \subseteq F(a)$. We claim that

$$a := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & k - 1 & 0 & \cdots & 0 \end{pmatrix} \in \text{Mat}_{2,d}(\mathbb{Z})$$

is such an element. If we define the monomials

$$v_1 := [y_{1,1}, y_{2,2}, \ldots, y_{2,2}]$$
$$v_2 := [y_{2,2}, y_{1,1}, y_{2,2}, \ldots, y_{2,2}]$$
$$\vdots$$
$$v_k := [y_{2,2}, \ldots, y_{2,2}, y_{1,1}],$$

of length $k$, then $B(a) = \{v_1, v_2, \ldots, v_k\}$. Now (5) implies that

$$I(a) = \langle r(\lambda_1) \cdot v_1, r(\lambda_1 \cdot \mu_2) \cdot v_1, \ldots, r(\lambda_1 \cdot \mu_2^{k-1}) \cdot v_1,$$
$$r(\mu_2) \cdot v_2, r(\lambda_1 \cdot \mu_2) \cdot v_2, \ldots, r(\lambda_1 \cdot \mu_2^{k-1}) \cdot v_2,$$
$$r(\mu_2) \cdot v_3, r(\mu_2^2) \cdot v_3, \ldots, r(\lambda_1 \cdot \mu_2^{k-1}) \cdot v_3,$$
$$\vdots,$$
$$r(\mu_2) \cdot v_k, r(\mu_2^k) \cdot v_k, \ldots, r(\lambda_1 \cdot \mu_2^{k-1}) \cdot v_k \rangle.$$

Since the anti-symmetry of the Lie bracket implies $v_3 = v_4 = \cdots = v_k = 0$, we may use (3) in order to conclude that $I(a) = \{0\} \subseteq \langle v_1, v_2, \ldots, v_k \rangle = F(a)$. This finishes the proof.

**Remark 2.2.3.** If $\lambda \neq \mu$, then the above proof can be simplified by replacing the free $k$-step nilpotent Lie algebra on $2d$ generators with the free $k$-step nilpotent Lie algebra on $d$ generators, and by replacing the operator $C := A \oplus A$ with the operator $C := A$. In this case, the resulting Lie algebra will have all the correct properties, but it will have a strictly smaller dimension. The details are straightforward and we omit them. Cf. examples 2.3.2 and 2.4.3.
Remark 2.2.4. This proof was inspired, in part, by Higman’s construction in [23] of regular automorphisms of prime order on groups of prescribed class. But it is also closely related to the so-called Auslander—Scheuneman relations for the construction of semi-simple Anosov automorphisms (cf. Payne’s construction in [47]).

We now consider the Mal’cev-correspondence:

Proposition 2.2.5. Consider a finite-dimensional, nilpotent Lie algebra \( L \) over the rational numbers, together with an automorphism \( \gamma : L \rightarrow L \). Suppose that for every lower central factor \( \Gamma_i(L)/\Gamma_{i+1}(L) \), we are given a monic polynomial \( r_i(t) \in \mathbb{Z}[t] \) such that the induced automorphism \( \gamma_i : \Gamma_i(L)/\Gamma_{i+1}(L) \rightarrow \Gamma_i(L)/\Gamma_{i+1}(L) \) satisfies \( r_i(\gamma_i) = 0_{\Gamma_i(L)/\Gamma_{i+1}(L)} \).

(i). Then \( s(t) := r_1(t) \cdots r_c(L)(t) \) is a monic identity of the automorphism \( \exp(\gamma) : \exp(L) \rightarrow \exp(L) \).

(ii). Then the characteristic polynomial \( \chi(t) \) of \( \gamma \) divides a natural power of \( s(t) \) and \( \chi(t) \) has integer coefficients.

Proof. (i.). Let us abbreviate \( G := \exp(L) \) and \( \beta := \exp(\gamma) \). We recall that the Baker—Campbell—Hausdorff formula defines the group operation on \( G \). This formula implies, in particular, that the induced automorphisms \( \gamma_i : \Gamma_i(L)/\Gamma_{i+1}(L) \rightarrow \Gamma_i(L)/\Gamma_{i+1}(L) \) and \( \beta_i : \Gamma_i(G)/\Gamma_{i+1}(G) \rightarrow \Gamma_i(G)/\Gamma_{i+1}(G) \) on the lower central factors coincide. So \( r_i(t) \) is an identity of \( \beta_{\Gamma_i(G)/\Gamma_{i+1}(G)} \). We may now apply lemma 2.1.4. (ii.). Since \( r_i(\gamma_i) = 0_{\Gamma_i(L)/\Gamma_{i+1}(L)} \), the characteristic polynomial \( \chi_i(t) = \det(t \cdot 1_{\Gamma_i(G)/\Gamma_{i+1}(G)} - \gamma_i) \in \mathbb{Q}[t] \) of \( \gamma_i \) divides a natural power of \( r_i(t) \). Since \( r_i(t) \) is monic with integer coefficients, Gauss’ lemma tells us that \( \chi_i(t) \) has integer coefficients as well. Since each term \( \Gamma_i(L) \) of the lower central series of \( L \) is invariant under \( \gamma \), the characteristic polynomial \( \chi(t) \) of \( \gamma \) is just the product \( \chi_1(t) \cdots \chi_c(L)(t) \). This suffices to prove the second claim.

Proposition 2.2.6. Consider a monic polynomial \( r(t) \in \mathbb{Z}[t] \). Let \( \lambda \) and \( \mu \) be roots of \( r(t) \) in \( \overline{\mathbb{Q}} \), and let \( k \) be any natural number satisfying \( r(\lambda \cdot \mu) = \cdots = r(\lambda \cdot \mu^{k-1}) = 0 \). Then \( r(t)^k \) is an identity of an endomorphism \( \beta : N \rightarrow N \) of a finitely-generated, torsion-free, \( k \)-step nilpotent group \( N \).

Proof. We may assume that \( r(0) \neq 0 \), since otherwise we may simply consider a finitely-generated, free nilpotent group \( F \) of class \( k \) and the endomorphism \( \gamma : F \rightarrow F : x \mapsto 1_F \). So we may apply proposition 2.2.2 in order to find a finitely-generated, \( k \)-step nilpotent Lie algebra \( L \) over the rationals and automorphism \( \overline{\mathbb{Q}} : L \rightarrow L \) satisfying \( r(\overline{\mathbb{Q}}) = 0_L \). Let us consider the torsion-free, \( k \)-step nilpotent, divisible group \( G := \exp(L) \) corresponding with \( L \), together with the automorphism \( \beta := \exp(\overline{\mathbb{Q}}) \) of \( G \) corresponding with \( \overline{\mathbb{Q}} \). According to proposition 2.2.5, the polynomial \( r(t)^k \) is a monic identity of \( \beta \). We see, in particular, that if \( N \) is any \( \beta \)-invariant, full subgroup of \( G \), then \( r(t)^k \) is an identity of the restriction \( \beta_N : N \rightarrow N \). Now, since the characteristic polynomial \( \chi(t) \) of \( \overline{\mathbb{Q}} \) has integer coefficients
Let us illustrate the construction of 2.1 with a concrete example.

Example 2.3.1. We consider the discrete Heisenberg group $H$, defined as the subgroup:

$$H := \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{Z} \right\} \subseteq \text{GL}_3(\mathbb{Z}).$$

Let $\gamma : H \to H$ be the automorphism that is given by

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & y & x \cdot y + \frac{y \cdot (y-1)}{2} - z \\ 0 & 1 & x + y \\ 0 & 0 & 1 \end{pmatrix},$$

and let us use the series $H \geq [H, H] \geq \{ 1 \}$ with factors $H/[H, H] \cong \mathbb{Z}^2$ and $[H, H]/\{ 1 \} \cong \mathbb{Z}$. A straight-forward computation gives us the characteristic polynomials $\chi_1(t) = -1 - t + t^2$ and $\chi_2(t) = 1 + t$, so that the characteristic polynomial of $\gamma$ with respect to the series is given by $\chi(t) := (-1 - t + t^2) \cdot (1 + t)$. By substitution, as in the proof of Proposition 2.1.5, we obtain

$$\forall v \in H : \quad \gamma^3(v) \cdot \gamma^2(v^{-1}) \cdot \gamma(v) \cdot \gamma(v^{-1}) = 1,$$

so that the inverse automorphism $\gamma^{-1} : H \to H$ is given by the formula $\gamma^{-1}(v) = \gamma^2(v) \cdot \gamma^3(v^{-1}) \cdot (v^{-1}) \cdot \gamma(v) \cdot v^{-1}$, and therefore by

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -x + y & x \cdot y - \frac{x \cdot (1 + x)}{2} - z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}.$$
We may use (a minor variation on) the construction of 2.2 to go in the other direction:

**Example 2.3.2.** Let \( r(t) := (t^2 - t - 1) \cdot (t + 1) \) be the polynomial of example 2.3.1. Let us construct a regular automorphism \( \beta : N \to N \) on a finitely-generated, torsion-free, two-step nilpotent group \( N \) such that \( r(t) \) is the characteristic polynomial of \( \beta \).

The roots of \( r(t) \) are \(-1, \frac{1 + \sqrt{5}}{2}, \) and \( \frac{1 - \sqrt{5}}{2} \), and the product of the latter two roots is the first root (cf. remark 2.2.3). So we consider the free two-step nilpotent Lie algebra \( F = \mathbb{Q} \cdot x_1 + \mathbb{Q} \cdot x_2 + \mathbb{Q} \cdot [x_1, x_2] \) on the generators \( x_1 \) and \( x_2 \). Then the companion matrix

\[
A := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \text{GL}_4(\mathbb{Z})
\]

of \((t^2 - t - 1)\) defines a linear transformation of the \( \mathbb{Q} \)-span of the generators: \( \alpha(x_1) := x_2 \) and \( \alpha(x_2) := x_1 + x_2 \). This map extends (in a unique way) to an automorphism \( \alpha : F \to F \) of the Lie algebra \( F \): \( \alpha([x_1, x_2]) = [\alpha(x_1), \alpha(x_2)] = -[x_1, x_2] \). We let \( I \) be the ideal of \( F \) that is generated by the subset \((\alpha^2 - \alpha - \mathbb{1}_F)(\mathbb{Q} \cdot x_1 + \mathbb{Q} \cdot x_2) + (\alpha + \mathbb{1}_F)(\mathbb{Q} \cdot [x_1, x_2])\) of \( F \). Then the induced automorphism \( \overline{\alpha} : L \to L \) on the quotient Lie algebra \( L := F/I \) satisfies \( r(\overline{\alpha}) = 0_L \). In fact: \( I = \{0_F\} \) and, with respect to the ordered basis \((\overline{x}_1, \overline{x}_2, \frac{[x_1, x_2]}{2})\), the automorphism of \( L \) is given by the matrix

\[
\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.
\]

We may now use the Baker—Campbell—Hausdorff formula to define the group operation \(*\) on \( L \). For rational numbers \( c_1, c_2, c_{12} \) and \( C_1, C_2, C_{12} \), we define \((c_1 \cdot \overline{x}_1 + c_2 \cdot \overline{x}_2 + c_{12} \cdot \frac{[x_1, x_2]}{2}) * (C_1 \cdot \overline{x}_1 + C_2 \cdot \overline{x}_2 + C_{12} \cdot \frac{[x_1, x_2]}{2})\) to be

\[
(c_1 + C_1) \cdot \overline{x}_1 + (c_2 + C_2) \cdot \overline{x}_2 + (c_{12} + C_{12} + (c_1 \cdot C_2 - c_2 \cdot C_1)) \cdot \frac{[x_1, x_2]}{2}.
\]

One can then verify that

\[
N := \mathbb{Z} \cdot \overline{x}_1 + \mathbb{Z} \cdot \overline{x}_2 + \mathbb{Z} \cdot \frac{[x_1, x_2]}{2}
\]

is an \( \overline{\alpha}\)-invariant subgroup of \((L, \ast)\) of class two and Hirsch-length 3. The restriction \( \beta : N \to N \) of \( \overline{\alpha} \) to \( N \) is an endomorphism of \( N \) and \( r(t) \) is the characteristic polynomial of \( \beta \) (with respect to the series of the isolators of the lower central series of \( N \)). Since also \( r(0) = -1 \), we may use remark 2.1.7 in order to conclude that \( \beta \) is, in fact, an automorphism of \( N \). Since \( r(1) = -2 \) and since \( N \) is torsion-free, we know that all fix-points of \( \beta \) are trivial, so that \( \beta \) is regular. In fact, the group \( N \) is a twisted Heisenberg group:

\[
N \cong \left\{ \begin{pmatrix} 1 & x & \frac{x}{2} \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{Z} \right\} \subseteq \text{GL}_3(\mathbb{Q}).
\]
And, under this identification, the automorphism \( \beta : N \to N \) is given by:

\[
\begin{pmatrix}
1 & x & z \\
0 & 1 & y \\
0 & 0 & 1
\end{pmatrix}
\mapsto
\begin{pmatrix}
1 & y & 2xu + u^2z \\
0 & 1 & x + y \\
0 & 0 & 1
\end{pmatrix}.
\]

This group \( N \) is not the discrete Heisenberg group \( H \) of example 2.3.1. But \( H \) is a normal subgroup of index 2 in \( N \).

2.4 Constructing regular automorphisms of finite order

Let us explain how the construction of subsection 2.2 can be used to obtain regular automorphisms of finite order on finitely-generated, torsion-free, nilpotent groups of class 2.

Example 2.4.1 \((A \text{ regular automorphism of order } 2 \text{ on an abelian group})\). We consider the cyclotomic polynomial \( r(t) := \Phi_2(t) = 1 + t \) and the case \( k = 1 \). The companion operator of \( r(t) \) is given by \( \gamma : \mathbb{Z} \to \mathbb{Z} : x \mapsto -x \). This endomorphism is clearly an automorphism of order 2. Since \( \mathbb{Z} \) has no \( \Phi_2(1) \)-torsion, this automorphism is regular.

Example 2.4.2 \((A \text{ regular automorphism of order } 3 \text{ on a nilpotent group of class } 2)\). Let \( r(t) := \Phi_3(t) = 1 + t + t^2 \) be the minimal polynomial of the primitive third roots of unity. Define the semi-simple operator

\[
A := \begin{pmatrix}
0 & 1 & 0 & 0 \\
-1 & -1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & -1 & -1
\end{pmatrix} \in \text{GL}_4(\mathbb{Z}).
\]

Then \( A \) naturally extends to a semi-simple automorphism \( \alpha : F \to F \) of the free 2-step nilpotent Lie algebra on the generators \( x_1, x_2, x_3, x_4 \). The commutator ideal \([F, F]\) is \( \alpha \)-invariant and the matrix of \( \alpha \) with respect to the (ordered) basis

\[
(\{x_1, x_2, x_3, x_4, [x_1, x_2], [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4], [x_3, x_4]\})
\]

is given by:

\[
M := \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}.
\]
One can easily verify that

\[
    r(M) = \begin{pmatrix}
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 2 & 1 & 1 & 2 & 0 & 0 \\
    0 & 0 & 0 & 0 & -1 & 1 & -2 & -1 & 0 & 0 \\
    0 & 0 & 0 & 0 & -1 & -2 & 1 & -1 & 0 & 0 \\
    0 & 0 & 0 & 0 & 2 & 1 & 1 & 2 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3
    \end{pmatrix}
\]

has rank 4. Define the vectors

\[
    v_1 := r(\alpha)([x_1, x_2]) = 3[x_1, x_2],
\]
\[
    v_2 := r(\alpha)([x_1, x_4]) = [x_1, x_3] + [x_1, x_4] - 2[x_2, x_3] + [x_2, x_4],
\]
\[
    v_3 := r(\alpha)([x_2, x_3]) = [x_1, x_3] - 2[x_1, x_4] + [x_2, x_3] + [x_2, x_4],
\]
\[
    v_4 := r(\alpha)([x_3, x_4]) = 3[x_3, x_4],
\]
\[
    v_5 := [x_1, x_3],
\]
\[
    v_6 := [x_2, x_4].
\]  

Then \((x_1, x_2, x_3, x_4, v_1, v_2, v_3, v_4, v_5, v_6)\) is an ordered basis of \(F\) that restricts to the ordered basis \((v_1, v_2, v_3, v_4)\) of \(I\) (the ideal of \(F\) that is generated by the subset \(r(\alpha)(F)\)). So we obtain an ordered basis \((\bar{\tau}_1, \bar{\tau}_2, \bar{\tau}_3, \bar{\tau}_4, \bar{\tau}_5, \bar{\tau}_6)\) for \(L := F/I\). The Lie bracket of \(L\) is determined by the relations:

\[
    [\bar{\tau}_1, \bar{\tau}_2] = 0_L,
\]
\[
    [\bar{\tau}_1, \bar{\tau}_4] = \bar{\tau}_5 + \bar{\tau}_6,
\]
\[
    [\bar{\tau}_1, \bar{\tau}_3] = \bar{\tau}_5,
\]
\[
    [\bar{\tau}_2, \bar{\tau}_3] = \bar{\tau}_5 + \bar{\tau}_6,
\]
\[
    [\bar{\tau}_2, \bar{\tau}_4] = \bar{\tau}_6,
\]
\[
    [\bar{\tau}_5, L] = \{0_L\},
\]
\[
    [\bar{\tau}_6, L] = \{0_L\}.
\]

The product \(w*u'\) of two elements \(w = \sum_{i\leq 4} a_i \bar{\tau}_i + a_5 \bar{\tau}_5 + a_6 \bar{\tau}_6\) and \(w' = \sum_{i\leq 4} b_i \bar{\tau}_i + b_5 \bar{\tau}_5 + b_6 \bar{\tau}_6\) of \(L\) is then (explicitly) defined by the Baker—Campbell—Hausdorff formula:

\[
    w*u' := w + w' + \frac{1}{2} \cdot [w, w']
\]
\[
    = \sum_{i\leq 4} (a_i + b_i) \bar{\tau}_i
\]
\[
    + \left( a_5 + b_5 + \begin{pmatrix} a_1 & b_1 \\ a_3 & b_3 \end{pmatrix} + \begin{pmatrix} a_4 & b_4 \\ a_3 & b_3 \end{pmatrix} \right) \frac{\bar{\tau}_5}{2}
\]
\[
    + \left( a_6 + b_6 + \begin{pmatrix} a_1 & b_1 \\ a_4 & b_4 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ a_3 & b_3 \end{pmatrix} \right) \frac{\bar{\tau}_6}{2}.
\]

We see, in particular, that

\[
    N := Z \cdot \tau_1 + Z \cdot \tau_2 + Z \cdot \tau_3 + Z \cdot \tau_4 + Z \cdot \frac{\tau_5}{2} + Z \cdot \frac{\tau_6}{2}
\]

21
is a (2-step nilpotent) subgroup of \((L, \ast)\).

With respect to the ordered basis \((\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6)\) of \(L\), the induced automorphism \(\pi : L \longrightarrow L\) is given by the matrix

\[
\pi = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
-1 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & -1 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 1 \\
0 & 0 & 0 & 0 & 1 & -1
\end{pmatrix}.
\]

We see, in particular, that \(N\) is mapped into itself by \(\pi\), so that the restriction \(\beta : N \longrightarrow N\) of \(\pi\) to \(N\) is an endomorphism of the group \((N, \ast)\). By construction, \((\pi(0))^2 = (1)^2\), we may use remark 2.1.7 to conclude that \(\beta\) is an automorphism. Since \(\pi(1))^2\) is an identity of \(\beta\) and it is even the characteristic polynomial of \(\beta\) w.r.t. the isolators of the lower central series of \(N\). Since \((\pi(0))^2 = (1)^2\), we may use remark 2.1.7 to conclude that \(\beta\) is an automorphism. Since \(N\) has no \((\pi(1))^2\)-torsion, we see that \(\beta\) is regular. So the order of \(\beta\) is exactly 3.

Example 2.4.3 (A regular automorphism of odd order \(n > 1\) on a nilpotent group of class 2). Since example 2.4.2 treats the case \(n = 3\), we may assume that \(n \geq 5\). Then every primitive \(n\)'th root \(\lambda\) factorises as the product of two distinct primitive \(n\)'th roots: \(\lambda = \lambda^{-1} \cdot \lambda\), so that remark 2.2.3 is relevant. Our construction (applied to the free 2-step nilpotent Lie algebra on \(\varphi(n)\) generators and to the companion matrix of \(\Phi_n(t)\)) then produces a regular automorphism \(\beta : N \longrightarrow N\) of a finitely-generated, torsion-free, 2-step nilpotent group \(N\) of Hirsch-length \(1 + (\varphi(n) + f(n))\), where \(f(n) := \{\{(i, j) \in \mathbb{Z}^n \times \mathbb{Z}^n \mid i + j \in \mathbb{Z}^n\}\}. We omit the computations.

Example 2.4.4 (A regular automorphism of order \(2^{a+1} > 2\) on a nilpotent group of class 2). We let \(C\) be the companion operator of \(\Phi_{2a+1}(t)\), and we define \(A := C \oplus C\). We then consider the free, 2-step nilpotent Lie algebra \(F\) on \(\varphi(2^{a+1}) + \varphi(2^{a+1})\) generators, which span a subspace \(V\) of \(F\). We extend \(A\) to an automorphism \(\alpha : F \longrightarrow F\) of \(F\). We define the ideal \(I := \Phi_{2^{a+1}}(\alpha)V + \Phi_{2a}(\alpha)[F, F]\) = \(\Phi_{2a}(\alpha)[F, F]\) of \(F\). Then \(L := F/I\) will have class 2, and we obtain a regular automorphism of order \(2^{a+1}\) on a finitely-generated, torsion-free group of class 2. The computations are straight-forward and we omit them.

Corollary 2.4.5. For every natural number \(n > 2\), there exists a finitely-generated, torsion-free, 2-step nilpotent group \(G\) with a regular automorphism of order \(n\).

Proof. If \(n\) is odd, then we may use example 2.4.3. If \(n\) is a natural power of 2, then we may use example 2.4.4. If \(n\) is 2 times an odd number, then we may take the direct product of the group in example 2.4.1 and the group in example 2.4.3. Else, we may take the direct product of the group in example 2.4.4 and the group in example 2.4.3. This covers all natural \(n > 2\). In each case, the group has class 2 and the automorphism is regular of order \(n\).
Remark 2.4.6. The condition $n > 2$ is also necessary.

Proof. If $n = 1$, then it is clear that the automorphism cannot be regular. If $n = 2$, then the group cannot have class two. For, suppose that $n = 2$ and $c(G) = 2$. Then, according to the Bass—Guivarch formula [6, 21], the growth of $G$ is at least of degree $l + 1$ (where $l$ is the Hirsch-length of $G$). Since $G$ is polycyclic, we may use remark 2.1.9 to find a characteristic subgroup $K$ of finite index in $G$ such that $(1 + t)^l$ is a monotone identity of the induced automorphism $\alpha_K : K \rightarrow K$. According to theorem 1.3.7, $[K, K]$ is then a torsion subgroup of $G$, and therefore the trivial group. So $G$ is virtually-abelian. By using the Bass—Guivarch formula once more, we conclude that $G$ grows with degree at most $l$. But, since the growth of $G$ is an invariant of $G$, we have obtained a contradiction. \qed

Remark 2.4.7. If $n$ is not a natural power of a prime, then the automorphism $\beta$ of example 2.4.3 will even be uniform (by Remark 2.1.8, cf. Lemma 6.3.8). So, in particular: by specialising $n := 15$, we obtain a uniform automorphism of order 15 on a nilpotent group $N$ of class 2 and Hirsch-length $\frac{1}{2} \cdot (\varphi(15) + f(15)) = 16$. This may be compared with a result of Jabara (example 5 of [29]). We do note that there appears to be a minor (and fixable) error in the construction of Jabara’s example.

3 Proving the nilpotency of a finite group

Preliminaries. We recall some basic terminology. Let $G$ be a group and let $\alpha$ be one of its automorphisms. We say that $\alpha$ is regular if it displaces all elements other than $1_G$. A subgroup $A$ of $G$ is $\alpha$-invariant if $\alpha(A) \subseteq A$. An $\alpha$-invariant section of $G$ is a quotient $A/B$ of an $\alpha$-invariant subgroup $A$ of $G$ by an $\alpha$-invariant, normal subgroup $B$ of $A$.

The following result is well-known, but we include its proof for completeness.

Lemma 3.0.1. Let $G$ be a finite group and let $\alpha$ be a regular automorphism. (i.) The map $\tau : G \rightarrow G : x \mapsto x^{-1} \cdot \alpha(x)$ is a bijection. (ii.) If $A/B$ is an $\alpha$-invariant section then the corresponding automorphism $\tau : A/B \rightarrow A/B : a \cdot B \mapsto \alpha(a) \cdot B$ is also regular. (iii.) If $p$ is a prime, then $G$ has a $p$-Sylow subgroup that is $\alpha$-invariant.

Proof. (i.) Since $\alpha$ is injective, so is $\tau$. Since $G$ is finite, $\tau$ is also surjective. (ii.) Since $\alpha$ is a bijection and since $B$ is $\alpha$-invariant, we also have $\tau^{-1}(B) = B$. Now suppose that $\alpha(a) \cdot B = a \cdot B$. Then $\tau(a) \in B$, so that also $a \in B$. (iii.) If $P$ is a $p$-Sylow subgroup, then so is $\alpha(P)$. By Sylow’s theorem, there exists $a \in G$ such that $\alpha(P) = P^a$. Choose $b \in G$ such that $\tau(b^{-1}) = a$. Then $P^b$ is a $p$-Sylow subgroup of $G$ that is $\alpha$-invariant:

$$\alpha(P^b) = \alpha(b^{-1}) \cdot \alpha(P) \cdot \alpha(b) = (b^{-1} \cdot a) \cdot (a^{-1} \cdot P \cdot a) \cdot (a^{-1} \cdot b) = P^b. \qed$$
Proposition 3.1.1. Consider a finite, solvable group $G$ with a regular automorphism $\alpha : G \rightarrow G$ and an identity $r(t)$ of $\alpha$. Suppose that, for every prime $q$ dividing $|G|$, we have
\[ \prod_{\text{gcd} 0 \leq j \leq u-1} (r_{u,j}(t) \text{ mod } q) = 1_{q^*}. \]
Then $G$ is nilpotent.

We suppose that the statement is not true and we will eventually derive a contradiction. We may suppose that $G$ is a counter-example of minimal order. Then every characteristic section of smaller order satisfies the conditions of the theorem and is therefore nilpotent.

**Claim 1:** There exist distinct primes $p$ and $q$, together with an elementary-abelian $p$-group $P$ and an elementary-abelian $q$-group $Q$ such that
1. $G = Q \rtimes P$,
2. $\alpha(Q) = Q \neq 1_Q$ and $\alpha(P) = P \neq 1_P$,
3. $C_G(Q) = Q$, and
4. For every $u \in \{2, \ldots, \deg(r(t)) + 1\}$, we have $\gcd_{0 \leq j \leq u-1} (r_{u,j}(t) \text{ mod } q) = 1_{q^*}$.

**Proof.** Let $Q$ be the Fitting subgroup of $G$, which is known to satisfy $C_G(Q) = Q$. Since $G$ is solvable and not nilpotent, we have
\[ 1_G < Q < G. \]
Suppose for a moment that the group $Q$ has at least two minimal characteristic subgroups, say $A$ and $B$. Then these subgroups are also characteristic in $G$, so that the proper sections $G/A$ and $G/B$ are nilpotent by the minimality of $G$ as a counter-example. But then also $G/(A \cap B) = G/1_G \cong G$ is nilpotent, which contradicts our assumption on $G$. So we may assume that the group $Q$ has exactly one minimal characteristic subgroup. Since the Fitting subgroup is nilpotent, this $Q$ is necessarily a $q$-group (for some prime $q$).

Suppose for a moment that $\text{Frat}(Q) \neq 1_G$. Then the characteristic section $G/\text{Frat}(Q)$ is proper, so that (by the minimality of $G$ as a counter-example) the section $G/\text{Frat}(Q)$ is nilpotent. Since $Q$ is normal in $G$, we have the inclusion $\text{Frat}(Q) \subseteq \text{Frat}(G)$. Then also $G/\text{Frat}(G) \cong (G/\text{Frat}(Q))/(\text{Frat}(G)/\text{Frat}(Q))$ is nilpotent, so that $G$ is nilpotent. But this contradicts our choice of $G$. This contradiction allows us to conclude that $Q$ is an elementary-abelian $q$-group.

Suppose next that $K/Q$ is a proper, characteristic subgroup of $G/Q$. Then $K$ is a proper, characteristic subgroup of $G$. The minimality of $G$ as a counter-example then
implies that the characteristic subgroup $K$ of $G$ is nilpotent. So $K$ is contained in the Fitting subgroup $Q$ of $G$ and $K/Q$ is the trivial subgroup of $G/Q$. This shows that the solvable group $G/K$ is characteristically-simple, and therefore an elementary-abelian $p$-group (for some prime $p$).

Since $G$ is not nilpotent, we necessarily have $p \neq q$. Now let $\tilde{P}$ be a $p$-Sylow subgroup of $G$. Since $\alpha$ is regular, we can use lemma 3.0.1 in order to find a conjugate $P := \tilde{P}^g = g^{-1} \cdot \tilde{P} \cdot g$ of $\tilde{P}$ in $G$ that is $\alpha$-invariant: $\alpha(P) = P$. Since $\gcd(|Q|, |P|) = 1$, we have $G = Q \rtimes P$. The characteristic subgroup $Q$ of $G$ is, of course, also $\alpha$-invariant.

**Claim 2:** There is a (non-trivial) finite-dimensional vector space $V$ over $\mathbb{F}_q$, a (non-trivial) elementary-abelian $p$-group $R \leq \text{GL}(V)$, and a $\beta \in \text{GL}(V)$ such that:

1. $r(\beta)(V) = \{0_V\}$, and
2. $\beta \in N_{\text{GL}(V)}(R) \setminus C_{\text{GL}(V)}(R)$.

**Proof.** Since $\alpha(P) = P$, we have the decomposition $(Q \rtimes P) \times \langle \alpha \rangle = Q \times (P \rtimes \langle \alpha \rangle)$. Let $\theta : P \rtimes \langle \alpha \rangle \rightarrow \text{Aut}(Q)$ be the action of $P \rtimes \langle \alpha \rangle$ on $Q$ via conjugation within $G$. Define the elementary-abelian $p$-group $R := \theta(P)$ and the linear automorphism $\beta := \theta(\alpha)$. Then we clearly have $\beta \in N_{\text{Aut}(Q)}(R)$.

Suppose for a moment that $\beta$ centralizes $R$. For every $x \in P$, we then have

$$\theta([\alpha, x]) = [\theta(\alpha), \theta(x)] = 1_{\text{Aut}(Q)}.$$ 

So the element $[\alpha, x]$ of $P$ acts trivially on $Q$ via conjugation within $G$. So $[\alpha, x] \subset P \cap C_G(Q) = P \cap Q = 1_G$. In other words: $\alpha$ fixes every element of $P$. Since $\alpha$ is assumed to be regular on $G$, we conclude that $P = 1_G$, so that $G = Q \rtimes P \cong Q$ is nilpotent. This contradicts our choice of $G$ as a minimal counter-example. So we may conclude that $\beta \in N_{\text{Aut}(Q)}(R) \setminus C_{\text{Aut}(Q)}(R)$.

The elementary-abelian $q$-group $Q$ naturally admits the structure of a finite-dimensional vector space $V$ over $\mathbb{F}_q$. Its group of automorphism $\text{Aut}(Q)$ can then be identified with $\text{GL}(V)$. Under this identification, we naturally have $R \leq \text{GL}(V)$, $\beta \in \text{GL}(V)$, and $\beta \in N_{\text{GL}(V)}(R) \setminus C_{\text{GL}(V)}(R)$. Since $r(t)$ is an identity of $\alpha : G \rightarrow G$, and since $\beta : Q \rightarrow Q$ is obtained by restricting $\alpha$ to the characteristic subgroup $Q$ of $G$, we see that $r(t)$ annihilates the corresponding vector space endomorphism $\beta : V \rightarrow V$. We may finish the proof by extending the scalars of $V$ in the obvious way.

Since $p \neq q$, the elements of the abelian group $R$ are semi-simple operators of $V$. So we may consider the decomposition of $V$ into its $R$-character spaces $V_\chi := \{v \in V | \forall A \in R : A(v) = \chi(A) \cdot v\}$. Since $V$ is finite-dimensional, there are necessarily only finitely-many of these (non-zero) character spaces, say:

$$V = V_{\chi_1} \oplus \cdots \oplus V_{\chi_k}.$$ (6)
Since $\beta \in N_{GL(V)}(R)$, we also have $\langle \beta \rangle \subseteq N_{GL(V)}(R)$. So, for each $\chi \in \hat{R}$ and for each $n \in \mathbb{Z}$, we may define the (possibly new) character

$$(\beta^n \ast \chi) : R \rightarrow \mathbb{F}_q^\mathbb{Z} : A \mapsto \chi(\beta^{-n} \circ A \circ \beta^n).$$

**Claim 3:** The group $\langle \beta \rangle$ naturally acts on the set $C := \{V_{\chi_1}, \ldots, V_{\chi_k}\}$ of (non-zero) character spaces via the rule $: (\beta) \times C \rightarrow C : (\beta^n, V_{\chi_i}) \mapsto \beta^n(V_{\chi_i}).$

**Proof.** Consider an arbitrary $\chi \in \hat{R}$ and $n \in \mathbb{Z}$. Let us first show that $\beta^n(V_{\chi_i}) \subseteq V_{\beta^n \ast \chi_i}$. To do this, we select an arbitrary $v \in V_{\chi_i}$ and $A \in R$. Then

$$A(\beta^n(v)) = \beta^n((\beta^{-1} \circ A \circ \beta^n)(v)) = \beta^n(\chi(\beta^{-n} \circ A \circ \beta^n) \cdot v) = ((\beta^n \ast \chi)(A) \cdot \beta^n(v)).$$

So $V = \beta^n(V) = \beta^n(V_{\chi_1}) + \cdots + \beta^n(V_{\chi_k}) \subseteq V_{\beta^n \ast \chi_1} + \cdots + V_{\beta^n \ast \chi_k} \subseteq V$. Since $V$ is finite-dimensional and since the sum (6) is direct, we may in fact conclude that $(\beta^n \ast \chi_1, \ldots, \beta^n \ast \chi_k)$ is a permutation of $(\chi_1, \ldots, \chi_k)$. We see, in particular, that $\beta^n(V_{\chi_i}) = V_{\beta^n \ast \chi_i}$. So, for all $n,m \in \mathbb{Z}$, we have $\beta^n(\beta^m(V_{\chi_i})) = (\beta^n \circ \beta^m)(V_{\chi_i})$. \hfill $\square$

**Claim 4:** There exists a character $\zeta \in \hat{R}$ such that $\beta(V_{\zeta}) \neq V_{\zeta}$.

**Proof.** By assumption, $\beta$ acts non-trivially on $R$ by conjugation within $GL(V)$. So there exists an element $A \in R$ such that $\beta^{-1} \circ A \circ \beta$ and $A$ are distinct operators of $V$. This difference can be detected in some vector $v$ of some character space, say $V_{\zeta}$:

$$(\beta^{-1} \circ A \circ \beta)(v) \neq A(v).$$

Suppose for a moment that $\beta(V_{\zeta}) = V_{\zeta}$. Then $\beta(v) \in V_{\zeta}$ and we obtain the contradiction

$$A(v) \neq (\beta^{-1} \circ A \circ \beta)(v)$$
$$= \beta^{-1}(A(\beta(v)))$$
$$= \beta^{-1}(\zeta(A) \cdot \beta(v))$$
$$= \zeta(A) \cdot v$$
$$= A(v).$$

So we may indeed conclude that $\beta(V_{\zeta}) \neq V_{\zeta}$. \hfill $\square$

**Claim 5:** We have $V_{\zeta} = \{0_V\}$.

**Proof.** Let $u$ be the minimal natural number such that $V_{\zeta} = \beta^u(V_{\zeta})$. Then this $u$ is at least 2 according to claim 4. It is clear from the definition of the partial sums $r_{u,0}(t), \ldots, r_{u,u-1}(t)$ that we have $r_{u,0}(t) + \cdots + r_{u,u-1}(t) = r(t)$. By evaluation in $\beta$, we obtain the equality $r_{u,0}(\beta) + \cdots + r_{u,u-1}(\beta) = r(\beta)$ of linear maps. Since $(r(\beta))(V) = \{0_V\}$, we have the equality of vector spaces

$$(r_{u,0}(\beta))(V_{\zeta}) + (r_{u,1}(\beta))(V_{\zeta}) + \cdots + (r_{u,u-1}(\beta))(V_{\zeta}) = (r(\beta))(V_{\zeta}) = \{0_V\}. \quad (7)$$

26
Let $\alpha$ be a regular automorphism of $G$ and $\beta$ be an identity element of $G$. We suppose that, for every prime $q$ dividing $|G|$, we have
\[
\prod_{2 \leq u \leq \deg(r(t)) + 1} \gcd_{0 \leq j \leq u-1} (r_{u,j}(t) \mod q) = 1_{F_q}.
\]

Claim: $G$ is nilpotent.

Proof. According to proposition 3.1.1, we need only show that $G$ is solvable. We suppose that the statement is not true and we will deduce a contradiction. Let $G$ be a counterexample of minimal order. Then every proper, $\alpha$-invariant section of $G$ is nilpotent.

If $|G|$ is the power of a single prime, then the class equation tells us that $G$ is nilpotent, and therefore solvable. So we may assume that some odd prime $p$ divides $|G|$. By lemma 3.0.1, we obtain a $p$-Sylow subgroup $P$ of $G$ that is $\alpha$-invariant. We now distinguish between two cases.

(i.) If $P$ has a non-trivial, normal, $\alpha$-invariant subgroup $H$ with $N_G(H) = G$, then $G$ is the extension of a $p$-group $H$ by a (proper, $\alpha$-invariant section, and therefore) nilpotent group $N_G(H)/H$. (ii.) Else, every non-trivial, normal, $\alpha$-invariant subgroup $H$ of $P$ has a normaliser $N_G(H)$ that is properly contained in $G$. This subgroup $N_G(H)$ is also $\alpha$-invariant, and therefore nilpotent. So every $p'$-element normalising $H$ must also centralise $H$. We may therefore apply Thompson’s norm $p$-complement theorem of [61] to obtain a normal $p$-complement $K$ to $P$. Since this group $K$ is proper and $\alpha$-invariant, it is also nilpotent. So we see, in particular, that $G$ is the extension of a nilpotent group $K$ by a

---

2This is essentially Thompson’s proof of the Frobenius conjecture [60], and we include it here for completeness.
$p$-group $P$.

In either case, $G$ is nilpotent-by-nilpotent, and therefore solvable. \hfill \Box

4 Proving the bounded nilpotency of Lie rings

4.1 Special case: Lie algebras

Before proving theorem 1.3.6, we consider an easier case that will be useful for applications.

**Lemma 4.1.1** (Binomial commutator formula). Consider a Lie ring $L$ with coefficients in a ring $R$. Let $\gamma : L \to L$ be a Lie endomorphism of $L$, let $\lambda, \mu \in R$ be coefficients, and let $v, w \in L$. For all $m \in \mathbb{N}$, we then have

$$(\gamma - (\lambda \cdot \mu) \cdot \mathbb{I}_L)^m([v, w]) = \sum_{0 \leq i \leq m} \binom{m}{i} \cdot [\lambda^{m-i} \cdot (\gamma - \lambda \cdot \mathbb{I}_L)^i(v), \gamma^i \circ (\gamma - \mu \cdot \mathbb{I}_L)^{m-i}(w)].$$

If, for some $m_\lambda, m_\mu \in \mathbb{N}$, we have $(\gamma - \lambda \cdot \mathbb{I}_L)^{m_\lambda}(v) = 0_L = (\gamma - \mu \cdot \mathbb{I}_L)^{m_\mu}(w)$, then we also have

$$(\gamma - \lambda \cdot \mu \cdot \mathbb{I}_L)^{m_\lambda + m_\mu}([v, w]) = 0_L.$$

**Proof.** One can prove the first formula by a simple induction on $m$ and Pascal’s binomial identity $\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$. By specializing to $m = m_\lambda + m_\mu$, we also obtain the second formula. \hfill \Box

**Proposition 4.1.2.** Consider a Lie algebra $L$ over a field $\mathbb{F}$, together with an automorphism $\alpha : L \to L$, and an identity $r(t)$ of $\alpha$. Suppose that $L$ is the direct sum $L = \bigoplus_{n \in \mathbb{N}} L_n$ of finite-dimensional, $\alpha$-invariant subspaces $L_n$. If $X := \{ \lambda \in \mathbb{F} \mid r(\lambda) = 0 \}$ is an arithmetically-free subset of $\mathbb{F}^\times$, then $L$ is nilpotent and $c(L) \leq H(X, \mathbb{F}^\times)$.

**Proof.** We define the Lie algebra $\tilde{L} := \mathbb{F} \otimes_{\mathbb{F}} L$ with coefficients in $\mathbb{F}$ and the automorphism $\mathbb{I} \otimes \tilde{\alpha}$ of $\tilde{L}$. Then $L$ naturally embeds into $\tilde{L}$ via the map $v \mapsto 1 \otimes v$ and we still have the property $r(\tilde{\alpha}) = 0_{\tilde{L}}$. We also note that $\tilde{L}$ is the direct sum of the finite-dimensional, $\alpha$-invariant subspaces $\tilde{L}_n := \mathbb{F} \otimes L_n$.

So we may consider the generalised eigenspace decomposition $\tilde{L}_n = \bigoplus_{\lambda \in \mathbb{F}} E(n, \lambda)$ of $\tilde{L}_n$ with respect to $\tilde{\alpha}_{\tilde{L}_n} : \tilde{L}_n \to \tilde{L}_n$, where

$$E(n, \lambda) := \{ v \in \tilde{L}_n \mid \exists m \in \mathbb{N} : (\tilde{\alpha}_{\tilde{L}_n} - \lambda \cdot \mathbb{I}_{\tilde{L}_n})^m v = 0 \}.$$ 

Since $r(\tilde{\alpha}_{\tilde{L}_n}) = 0_{\tilde{L}_n}$, all the generalised eigenvalues of $\tilde{\alpha}_{\tilde{L}_n} : \tilde{L}_n \to \tilde{L}_n$ are contained in $X$. By defining $E(\lambda) := \bigoplus_{n \in \mathbb{N}} E(n, \lambda)$, we obtain the generalised eigenspace decomposition of $\tilde{L}$:

$$\tilde{L} = \bigoplus_{\lambda \in \mathbb{F}} E(\lambda),$$

28
and we see that all the generalised eigenvalues of $\hat{\alpha}$ are contained in $X \subseteq \mathbb{F}^*$. According to the commutator-formula of lemma 4.1.1, this decomposition is, in fact, a grading of $\hat{L}$ by $\mathbb{F}^*$. Since $X$ is an arithmetically-free subset of $\mathbb{F}^*$, we may apply theorem 1.3.3 in order to conclude that $c(L) \leq c(\hat{L}) \leq H(X, \mathbb{F}^*)$. \hfill $\square$

### 4.2 Proof of theorem 1.3.6

For an integer $h$ and a Lie ring $M$ with coefficients in a ring $R$, we define the $h$-torsion ideal $T_h(M)$ of $M$ by

$$T_h(M) := \{ v \in M | \exists n \in \mathbb{N} : h^n \cdot v = 0_M \}.$$  

It is clear that such a set $T_h(M)$ is a Lie ideal of $M$ that is invariant under $R$-multiplications and $M$-endomorphisms.

**Theorem 4.2.1** (Embedding modulo bad torsion). **Consider a Lie ring $L$ with an endomorphism $\gamma : L \to L$ and identity $\tau(t)$ of $\gamma$. Then the Lie ring $\text{Discr}_*(\tau(t)) \cdot L$ embeds into a Lie ring $K$ such that the quotient $K$ of $K$ by its $(\text{Discr}_*(\tau(t)) \cdot \text{Prod}(\tau(t)))$-torsion ideal is the direct sum $K = \bigoplus_{\lambda \in \mathbb{Q}} K_{\lambda}$ of additive subgroups $K_{\lambda}$, and such that, for all $\lambda, \mu \in \mathbb{Q}$, we have $[K_{\lambda}, K_{\mu}] \subseteq K_{\lambda \cdot \mu}$, and $\{ \lambda \in \mathbb{Q} | K_{\lambda} \neq \{0_K\} \} \subseteq \{ \lambda \in \mathbb{Q} | r(\lambda) = 0 \}$.

Let us use the abbreviations $\delta := \text{Discr}_*(\tau(t))$ and $\pi := \text{Prod}(\tau(t))$. We may assume that $r(t)$ is not a constant polynomial, since otherwise we trivially have $\delta \cdot L = 0_L$, and there is nothing to prove. Let $\lambda_1, \ldots, \lambda_l$ be the distinct roots with respective multiplicities $m_1, \ldots, m_l$ and let $a$ be the leading coefficient, so that

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

Let $R := \mathbb{Z}[\lambda_1, \ldots, \lambda_l]$ be the ring generated by the roots and let $\mathbb{F}$ be the field of fractions of $R$. We next introduce a new Lie ring $\tilde{L} := R \otimes \mathbb{Z} L$ with coefficients in $R$. This new Lie ring $\tilde{L}$ naturally admits the Lie ring endomorphism $\tilde{\gamma} : \tilde{L} \to \tilde{L} : \sum_j a_j \otimes v_j \mapsto \sum_j a_j \otimes (\gamma(v_j))$ and this map inherits the property $r(\tilde{\gamma}) = 0_{\tilde{L}}$. We further define the ideal $T := T_{a \cdot \delta \cdot \pi}(\tilde{L}) = T_{a \cdot \pi}(\tilde{L})$ of $\tilde{L}$. And for each $\lambda \in R$, we define the $R$-submodule

$$E_\lambda := \{ v \in \tilde{L} | \exists n \in \mathbb{N} : (\tilde{\gamma} - \lambda \cdot 1_{\tilde{L}})^n v \in T \}$$  

of $\tilde{L}$.

**Claim 1:** For all $\lambda, \mu \in R$, we have
4.1.1

By combining (10), we obtain:

\[ (a \cdot \delta \cdot \pi)^k \cdot (\tilde{\gamma} - \lambda \cdot \mathbb{I})^m v = 0 \]

where each \( \lambda \in \mathbb{F} \) is contained in some \( K_{\mu} \). So it suffices to show that for such a word \( w \), we have \( w \in K \). Let us do this. We may suppose that \( r(\mu_1) = \cdots = r(\mu_n) = 0 \), since

\[ \text{Claim 3: This } K \text{ is a Lie subring of } \tilde{L}. \]

\[ K := \sum_{\lambda \in \mathbb{F}} K_{\lambda}. \]

\[ \text{Proof. According to the Jacobi-identity and the bi-linearity of the Lie bracket, the Lie } R \text{-subalgebra of } \tilde{L} \text{ generated by the } R \text{-submodule } K \text{ of } \tilde{L} \text{ is the } R \text{-span of left-normed words } w \text{ of the form } w := [v_1, \ldots, v_n], \]

where each \( v_i \) is contained in some \( K_{\mu_i} \). So it suffices to show that for such a word \( w \), we have \( w \in K \). Let us do this. We may suppose that \( r(\mu_1) = \cdots = r(\mu_n) = 0 \), since
otherwise $w$ is contained in the ideal $T$ and therefore in $K$. If $\mu_1, \mu_2, \ldots, \mu_1 \cdots \mu_n := \lambda$ are all roots of $r(t)$, then we need only apply claim 1.b $(n - 1)$-times in order to conclude that $w \in K_\lambda$ and therefore $w \in K$. Else, there exists an index $n_0 \in \{1, \ldots, n - 1\}$, such that $\mu_1 \cdots \mu_{n_0} := \mu$ is a root, but $\mu \cdot \mu_{n_0+1}$ is not. Define $u := [v_1, \ldots, v_{n_0}]$. By applying claim 1.b $(n_0 - 1)$-times, we see that $u \in K_\mu$. By applying claim 1.c, we see that $[u, v_{n_0+1}] \in T$. So also $w = [[u, v_{n_0+1}], v_{n_0+2}, \ldots, v_n] \in T \subseteq K$. 

We now note that $T := T_{\delta \cdot \pi}(L) = T_{\delta \cdot \pi}(K)$ is also the $(\delta \cdot \pi)$-torsion ideal of $K$ and we consider the quotient $\overline{K} := K/T$. For each $\lambda \in \mathbb{F}$, we define the $R$-submodule $\overline{K}_\lambda$ of $\overline{K}$ by:

$$\overline{K}_\lambda := K_\lambda/T.$$  

Claim 4: $\overline{K} = \bigoplus_{\lambda \in \mathbb{F}} \overline{K}_\lambda$ is a grading of the Lie ring $\overline{K}$ by $(\mathbb{F}, \cdot)$ and the support of this grading is contained in $X$.

**Proof.** In view of claims 2 and 3, we need only show that the above decomposition is direct. We select arbitrary $v_{\lambda_1} \in K_{\lambda_1}, \ldots, v_{\lambda_i} \in K_{\lambda_i}$ such that $v_{\lambda_1} + \cdots + v_{\lambda_i} \in T$ and we then need to show that $v_{\lambda_1}, \ldots, v_{\lambda_i} \in T$. So we select an arbitrary $i \in \{1, \ldots, l\}$ and will show that $v_{\lambda_i} \in T$.

By definition, there exist $m, k \in \mathbb{N}$ such that for all $j \in \{1, \ldots, l\}$, we have:

$$(a \cdot \delta \cdot \pi^k \cdot (\gamma - \lambda_j \cdot \mathbb{I}_K)^m v_{\lambda_j} = 0_K$$  \hspace{1cm} (12)

Define the auxiliary polynomial $s(t) = \prod_{j \neq i} (t - \lambda_j)^m \in R[t]$. Then the theory of resultants tells us that there exist polynomials $g(t), h(t) \in R[t]$ such that

$$g(t) \cdot s(t) + h(t) \cdot (t - \lambda_i)^m = \text{Res}(s(t), (t - \lambda_i)^m) = s(\lambda_i)^m.$$  \hspace{1cm} (13)

Since $T$ is invariant under $\gamma$ and multiplication by elements of $R$, we see that $(a \cdot \delta \cdot \pi^k \cdot s(\gamma))(v_{\lambda_i}) = (a \cdot \delta \cdot \pi^k \cdot s(\gamma))(v_{\lambda_1} + \cdots + v_{\lambda_i}) \in T$. So, by definition, there exists a $k' \in \mathbb{N}$ such that

$$(a \cdot \delta \cdot \pi^k \cdot s(\gamma))(v_{\lambda_i}) = 0_K.$$  \hspace{1cm} (14)

By first evaluating (13) in $\gamma$ and then in $v_{\lambda_i}$, and by substituting (12) and (14), we obtain:

$$(a \cdot \delta \cdot \pi)\cdot s(\lambda_i)^m v_{\lambda_i} = (a \cdot \delta \cdot \pi)\cdot g(\gamma)(s(\gamma)v_{\lambda_i})$$

$$+ (a \cdot \delta \cdot \pi)\cdot h(\gamma)((\gamma - \lambda_i \cdot \mathbb{I}_K)^m v_{\lambda_i})$$

$$= 0_K.$$  \hspace{1cm} (15)

Since the factor $s(\lambda_i)$ divides $\delta$ in the ring $R$, there exists some $k'' \in \mathbb{N}$ such that also $(a \cdot \delta \cdot \pi)^{k+k''} \cdot v_{\lambda_i} = 0_K$. We may therefore conclude that $v_{\lambda_i} \in T$. 

**Claim 5:** We have the inclusion $1 \otimes (\delta \cdot L) \subseteq K$. 

31
Proof. For each \( i \in \{1, \ldots, l\} \) and each \( j \in \{0, \ldots, m_i - 1\} \), we define the polynomial \( P_{i,j}(t) := r(t)/(t - \lambda_i)^{m_i - 1} \) with coefficients in the ring \( R := \mathbb{Z}[\lambda_1, \ldots, \lambda_l] \). Let us first show that, for each polynomial \( P_{i,j}(t) \), there exists a coefficient \( \theta_{i,j} \in R \) such that

\[
\text{Discr}_e(r(t)) = \sum_{1 \leq i \leq l} \sum_{0 \leq j \leq m_i - 1} \theta_{i,j} \cdot P_{i,j}(t).
\]  

(15)

The partial fraction decomposition of \( a/r(t) \) is given by

\[
a/t(t) = \sum_{1 \leq i \leq l} \sum_{0 \leq j \leq m_i - 1} \frac{1}{j!} \cdot \left( \left( \frac{a}{P_{i,0}(t)} \right)^{(j)} (\lambda_i) \right) \cdot (t - \lambda_i)^{j - m_i}.
\]

For each \( i \in \{1, \ldots, l\} \), we define the auxiliary polynomial \( s_i(t) := \prod_{1 \leq j \leq l} (t - \lambda_j) \in R[t] \).

Then the \( j \)'th derivative of \( a/(P_{i,0}(t)) \) is clearly of the form \( b_{i,j}(t)/(s_i(t))^{2m} \), for some explicitly computable \( b_{i,j}(t) \in R[t] \). We see, in particular, that

\[
a = \sum_{1 \leq i \leq l} \sum_{0 \leq j \leq m_i - 1} \frac{b_{i,j}(\lambda_i)}{(s_i(\lambda_i))^{2m}} \cdot P_{i,j}(t).
\]

After multiplying both sides of this equality by \( \text{Discr}_e(r(t))/a \), we see that

\[
\theta_{i,j} := \frac{(m - 1)!}{j!} \cdot \left( -1 \right)^{j(l-1)} \cdot a^{2d^2} \cdot \prod_{1 \leq k, n \leq l} (\lambda_k - \lambda_n)^m \cdot b_{i,j}(\lambda_i)
\]

is a solution to (15) in the ring of coefficients \( R \), where \( m := \max\{m_1, \ldots, m_l\} \).

We now select an arbitrary \( v \in L \). Corresponding with the \((i,j)\)'th term of 15, we define \( v_{i,j} := P_{i,j}(\tilde{\gamma})(1 \otimes v) \in \tilde{L} \). Then we observe that \((\tilde{\gamma} - \lambda_i \cdot 1_K)^{m_i - 1} \cdot v_{i,j} = r(\tilde{\gamma})(1 \otimes v) = 0_K \), so that \( v_{i,j} \in K_{\lambda_i} \). By evaluating the expression (15) in \( \tilde{\gamma} \) and then in \( 1 \otimes v \), we see that

\[1 \otimes (\delta \cdot v) = \sum_{1 \leq i \leq l} \sum_{0 \leq j \leq m_i - 1} \theta_{i,j} \cdot v_{i,j} \in \sum_{1 \leq i \leq l} \sum_{0 \leq j \leq m_i - 1} R \cdot K_{\lambda_i} \subseteq K.\]

So we may indeed conclude that \( 1 \otimes (\delta \cdot L) \subseteq K \).

By restricting the map \( \iota : L \to \tilde{L} : v \mapsto 1 \otimes v \), we obtain an embedding \( \iota' : \delta \cdot L \to K \) of Lie rings with integer coefficients. This finishes the proof of theorem 4.2.1.

We recall that the derived series of a Lie ring \( L \) is defined recursively by \( \Delta_0(L) := L \) and \( \Delta_{i+1}(L) := [\Delta_i(L), \Delta_i(L)] \).

**Corollary 4.2.2.** Consider a Lie ring \( L \) with an endomorphism \( \gamma : L \to L \) and a polynomial \( r(t) \in \mathbb{Z}[t] \) of degree \( d \) such that \( r(\gamma) = 0_L \). If \( r(0) \cdot r(1) \neq 0 \), then the additive group of the derived ideal \( \Delta_{2d}(L) \) of \( L \) is a \( (\text{Discr}_e(r(t)) \cdot \text{Prod}(r(t))) \)-group.

**Proof.** Let \( K \) be the graded Lie ring of theorem 4.2.1 and let \( T \) be the corresponding ideal. According to Shalev’s proposition 2.4 in [53], we have \( \Delta_{2d}(K/T) = \{0_{K/T}\} \), so that \( \Delta_{2d}(\text{Discr}_e(r(t)) \cdot L) \subseteq \Delta_{2d}(K) \subseteq T \). So every element of \( \Delta_{2d}(L) \) is annihilated by a natural power of \( (\text{Discr}_e(r(t)) \cdot \text{Prod}(r(t))) \).

\[\square\]
Corollary 4.2.3. Consider a Lie ring $L$ with an endomorphism $\gamma : L \to L$ and a polynomial $r(t) \in \mathbb{Z}[t]$ such that $r(\gamma) = 0_L$. If the roots of $r(t)$ form an arithmetically-free subset $X$ of $(\mathbb{Q}^\times, \cdot)$, then the additive group of the lower central ideal $\Gamma_{H(X, \mathbb{Q}^\times)+1}(L)$ of $L$ is a $(\text{Discr}^* \cdot \text{Prod}(r(t)))$-group.

Proof. Let $K$ be the graded Lie ring of theorem 4.2.1 and let $T$ be the corresponding ideal. According to theorem 1.3.3, we have $\Gamma_{H(X, \mathbb{Q}^\times)+1}(K/T) = \{0_{K/T}\}$, so that $\Gamma_{H(X, \mathbb{Q}^\times)+1}(\text{Discr}(r(t)) \cdot L) \subseteq \Gamma_{H(X, \mathbb{Q}^\times)+1}(K) \subseteq T$. So every element of $\Gamma_{H(X, \mathbb{Q}^\times)+1}(L)$ is annihilated by a natural power of $(\text{Discr}(r(t)) \cdot \text{Prod}(r(t)))$.

This finishes the proof of theorem 1.3.6.

5 Bounding the class of a nilpotent group

5.1 Infinitesimal Lie rings of nilpotent groups

We will prove theorem 1.3.7 by reducing it to an analogous problem about the (corresponding) Lie ring. So let us briefly recall some elementary constructions and properties of infinitesimal Lie rings. We fix a group $G$, an automorphism $\alpha : G \to G$, and an identity $r(t)$ of the automorphism. Let us suppose that $G$ admits a characteristic Lie-series, that is: a series

$$G = G_1 \geq G_2 \geq \cdots \geq G_i \geq G_{i+1} \geq \cdots$$

of characteristic subgroups with trivial intersection $\bigcap_{i \in \mathbb{N}} G_i = \{1_G\}$, satisfying the grading-like property

$$[G_i, G_j] \subseteq G_{i+j}$$

for all $i, j \in \mathbb{N}$. Then each term $G_{i+1}$ is normal in its predecessor $G_i$ and we can define the structure of an abelian group on the corresponding factor group $L_i := G_i/G_{i+1}$:

$$x \cdot G_{i+1} + y \cdot G_{i+1} := (x \cdot y) \cdot G_{i+1},$$

for all $x, y \in G_i$. We obtain, in particular, an abelian group

$$L := \bigoplus_{i \in \mathbb{N}} L_i.$$

Let us also use the additive notation for this group: $(L, +)$.

For each $x \cdot G_{i+1}$ (with $x \in G_i$) and $y \cdot G_{j+1}$ (with $y \in G_j$), we may further define the bracket

$$[x \cdot G_{i+1}, y \cdot G_{j+1}] := [x, y] \cdot G_{i+j+1}$$

and extend it $\mathbb{Z}$-linearly to all of $L$. One can then verify, using the Hall—Witt identities on $G$, that this operation is a Lie bracket on the additive group $L$. So we have obtained

---

Also sometimes referred to as a “strongly-central series,” or a “central series in the strong sense.”
the infinitesimal Lie ring \((L, +, [\cdot, \cdot])\) of \(G\) corresponding with the characteristic Lie-series \((G_i)\).

Since the subgroups \(G_i\) are all characteristic in \(G\), the automorphism \(\alpha : G \rightarrow G\) of \(G\) naturally descends to an automorphism \(\overline{\alpha}_i : G_i/G_{i+1} \rightarrow G_i/G_{i+1}\) of each of the factors \(G_i/G_{i+1}:\)

\[
\overline{\alpha}_i(x \cdot G_{i+1}) := \alpha(x) \cdot G_{i+1}.
\]

By extending these automorphisms \(\overline{\alpha}_1, \ldots, \overline{\alpha}_k\) in a \(\mathbb{Z}\)-linear fashion to all of \(L\), we obtain an automorphism \(\overline{\alpha} : L \rightarrow L\) of the Lie ring \(L\).

Since \(r(t)\) is an identity of \(\alpha\), it is also an identity of each \(\overline{\alpha}_i\), and therefore an identity of \(\overline{\alpha}\): \(r(\overline{\alpha}) = 0_L\).

All of this can be summarised in:

**Proposition 5.1.1.** Consider a group \(G\) with a characteristic Lie-series and let \(L\) be the corresponding Lie ring. If \(\alpha : G \rightarrow G\) is an automorphism of \(G\) with identity \(r(t)\), then the induced automorphism \(\overline{\alpha} : L \rightarrow L\) of the Lie ring satisfies \(r(\overline{\alpha}) = 0_L\)

Two characteristic Lie-series will be used in this text in order to say something about the nilpotency of a group: the lower central series (in subsection 5.2) and the Zassenhaus series (in subsection 7.1.1).

### 5.2 Proof of theorem 1.3.7

We consider a nilpotent group \(G\), together with an automorphism \(\alpha : G \rightarrow G\), and a monic identity \(r(t)\) of \(\alpha\) of degree \(d\). We suppose that the roots of \(r(t)\) form an arithmetically-free subset \(X\) of \((\mathbb{Q}^\times, \cdot)\). Let us abbreviate \(\delta := \text{Discr}_*(r(t))\) and \(\pi := \text{Prod}(r(t))\). Let us show that \(\Gamma_{d^2\delta+1}(G)\) is a \((\delta \cdot \pi)\)-group.

Since \(G\) is nilpotent, we need only show that, for all natural \(i \geq d^2\delta + 1\), the factor \(\Gamma_i(G)/\Gamma_{i+1}(G)\) is a \((\delta \cdot \pi)\)-group.

Since the lower central series \((\Gamma_k(G))_k\) of \(G\) is a characteristic Lie-series of \(G\), it makes sense to consider the corresponding Lie ring \(L\) and the induced automorphism \(\overline{\alpha} : L \rightarrow L\) (as in proposition 5.1.1). Since \(r(\overline{\alpha}) = 0_L\), we may apply theorem 1.3.6 in order to conclude that the additive group of the ideal \(\Gamma_{d^2\delta+1}(L)\) is a \((\delta \cdot \pi)\)-group. In particular: for all natural \(i \geq d^2\delta + 1\), the additive group of \(\Gamma_i(L)/\Gamma_{i+1}(L)\) is a \((\delta \cdot \pi)\)-group. And, by construction, the latter is isomorphic to the factor group \(\Gamma_i(G)/\Gamma_{i+1}(G)\).
6 Verifying the technical conditions of our auxiliary theorems

Our main result relies on two auxiliary theorems and each of these results makes some rather technical assumptions on a polynomial \( r(t) \). We had already mentioned that condition (1) of theorem 1.3.1 can be decided easily by means of the Euclidian algorithm over a field of finite characteristic. We will show in subsection 6.1 that also the technical condition of theorem 1.3.7 can be decided via a straight-forward computation. Moreover, in subsection 6.2, we will prove that both technical conditions are satisfied if \( \gcd(r(1) \cdot \text{Cong}(r(t)), q) = 1 \). This then finishes the last step in our proof of theorem 1.2.3.

We also verify that \( \text{Discr}_*(r(t)) \) and \( \text{Prod}(r(t)) \) are non-zero integers (provided that \( r(t) \neq 0 \)). And we will illustrate all of this with examples.

6.1 Arithmetically-free subsets

**Proposition 6.1.1.** We consider a monic polynomial \( r(t) \in \mathbb{Z}[t] \) of degree \( d \) and we let \( C \) be its companion operator. We next define the homogeneous polynomial

\[
\hat{r}(t_1, \ldots, t_d) := \det \left( t_1 \cdot r(C \otimes C^1) + \cdots + t_d \cdot r(C \otimes C^d) \right)
\]

of degree \( d^2 \) in the variables \( t_1, \ldots, t_d \) with integer coefficients. Let \( F \) be an algebraically-closed field of characteristic \( q \geq 0 \). Then the following statements are equivalent:

1. The roots of \( r(t) \) in \( F \) form an arithmetically-free subset of \( (F^\times, \cdot) \).
2. \( \hat{r}(t_1, \ldots, t_d) \not \equiv 0 \mod q \).

**Proof.** Let \( \lambda_1, \ldots, \lambda_d \) be the roots of \( r(t) \) in \( F \), listed with the correct multiplicities. Then \( X := \{ \lambda_1, \ldots, \lambda_d \} \) is an arithmetically-free subset of \( (F^\times, \cdot) \) if and only if the auxiliary polynomial

\[
s(t_1, \ldots, t_d) := \prod_{1 \leq i,j \leq d} \left( t_1 \cdot r(\lambda_i \cdot \lambda_j^1) + \cdots + t_d \cdot r(\lambda_i \cdot \lambda_j^d) \right)
\]

in the variables \( t_1, \ldots, t_d \) with coefficients in \( F \) does not vanish identically. So it suffices to show that \( \hat{r}(t_1, \ldots, t_d) \equiv s(t_1, \ldots, t_d) \mod q \).

To do this, we consider the companion matrix \( \overline{C} \) of \( r(t) \mod q \). Its generalised eigenvalues are precisely \( \lambda_1, \ldots, \lambda_d \). So the generalised eigenvalues of the \( (d^2 \times d^2) \)-matrix \( \overline{M} := t_1 \cdot r(\overline{C} \otimes \overline{C}^1) + \cdots + t_d \cdot r(\overline{C} \otimes \overline{C}^d) \) with coefficients in \( F[t_1, \ldots, t_d] \) are exactly

\[
t_1 \cdot r(\lambda_i \cdot \lambda_j^1) + \cdots + t_d \cdot r(\lambda_i \cdot \lambda_j^d),
\]

where \( i \) and \( j \) run over \( \{1, \ldots, d\} \). Since \( r(t) \) is monic, we have \( \overline{C} \equiv C \mod q \), so that we may indeed conclude that

\[
s(t_1, \ldots, t_d) = \det(\overline{M}) \equiv \det \left( t_1 \cdot r(C \otimes C^1) + \cdots + t_d \cdot r(C \otimes C^d) \right) \mod q \equiv \hat{r}(t_1, \ldots, t_d) \mod q. \quad \square
\]
6.2 Proof of proposition 1.3.11

We consider a polynomial \( r(t) \in \mathbb{Z}[t] \) of degree \( d \) and an algebraically-closed field \( \mathbb{F} \) of characteristic \( q \geq 0 \). We suppose that \( r(1) \cdot \text{Cong}(r(t)) \equiv 0 \) mod \( q \).

Claim 1: For every natural number \( u \geq 2 \), we have

\[
\gcd(r_{0,0}(t) \mod q, \ldots, r_{u,u-1}(t) \mod q) = 1_{\mathbb{F}}.
\]

Proof. Since \( q \) does not divide \( \text{Cong}(r(t)) \), there exists an integer \( n \) such that \( n \cdot \text{Cong}(r(t)) \equiv 1 \) mod \( q \). By definition, there exist polynomials \( s_0(t), \ldots, s_{u-1}(t) \in \mathbb{Z}[t] \) such that \( \text{Cong}(r(t)) = \sum_j s_j(t) \cdot r_{u,j}(t) \). Then \( \sum_j (n \cdot s_j(t) \mod q) \cdot (r_{u,j}(t) \mod q) \equiv 1 \) mod \( q \). So, the greatest common divisor of the \( r_{u,j}(t) \) mod \( q \) in \( \mathbb{F}[t] \) divides \( 1_{\mathbb{F}} \).

Claim 2: The roots of \( r(t) \) mod \( q \) in \( \mathbb{F} \) form an arithmetically-free subset \( X \) of the multiplicative group \( (\mathbb{F}^\times, \cdot) \).

Proof. First, we note that \( \text{Cong}(r(t)) \equiv 0 \) mod \( q \), so that \( r(0) \equiv 0 \) mod \( q \). We may suppose that \( r(t) \) is not a constant polynomial, since otherwise \( X = \emptyset \) and there is nothing to prove. Since \( r(1) \not\equiv 0 \) mod \( q \), we see that \( X \subseteq \mathbb{F} \setminus \{0_{\mathbb{F}}, 1_{\mathbb{F}}\} \subseteq \mathbb{F}^\times \).

We suppose that \( X \) is not arithmetically-free, and we will derive a contradiction. By assumption, there exist \( a, b \in X \) such that the internal arithmetic progression \( a, a \cdot b, a \cdot b^2, \ldots \) is contained in \( X \). Let \( u \) be the (multiplicative) order of \( b \), which is at least \( 2 \) (since \( 1 \not\in X \)). Consider the partial sum decomposition of \( r(t) \):

\[
r(t) = \sum_{0 \leq j < u} r_{u,j}(t) = \sum_{0 \leq j < u} R_{u,j}(t^u) \cdot t^j,
\]

where \( R_0(t), \ldots, R_{u-1}(t) \in \mathbb{Z}[t] \). For every \( k \geq 0 \), we may evaluate this expression in \( t = a \cdot b^k \) to obtain:

\[
0_{\mathbb{F}} = r(a \cdot b^k) = \sum_{0 \leq j < u} R_{u,j} \left((a \cdot b^k)^u \right) \cdot (a \cdot b^k)^j = \sum_{0 \leq j < u} (R_{u,j}(a^u) \cdot a^j) \cdot (b^k)^j = \sum_{0 \leq j < u} r_{u,j}(a) \cdot (b^k)^j.
\]

So \( (r_{u,0}(a), \ldots, r_{u,u-1}(a)) \) is a solution to the linear Vandermonde system

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & b & \cdots & b^{u-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & b^{u-1} & \cdots & (b^{u-1})^{u-1}
\end{pmatrix}
\begin{pmatrix}
\theta_0 \\
\theta_1 \\
\vdots \\
\theta_{u-1}
\end{pmatrix}
= 
\begin{pmatrix}
0 \\
0 \\
\vdots \\
0
\end{pmatrix}.
\]

36
The determinant of this system is given by the well-known formula \( \prod_{0 \leq i < j \leq u-1} (b^i - b^j) \).

None of the factors \((b^i - b^j)\) vanishes, since otherwise \(b^{j-i} = 1\), which would imply that \(b\) has order less than \(u\) (a contradiction). So the partial sums \(r_{u,0}(a), \ldots, r_{u,u-1}(a)\) all vanish.

In the proof of claim 1, we saw that there exist polynomials \(s_0(t), \ldots, s_{u-1}(t) \in \mathbb{Z}[t]\) such that \(1_F = \sum_{0 \leq j < u} (s_j(t) \cdot r_{u,j}(t) \bmod q)\). By evaluating in \(t = a\), we obtain:

\[
1_F = \sum_{0 \leq j < u} s_j(a) \cdot r_{u,j}(a) = \sum_{0 \leq j < u} s_j(a) \cdot 0_F = 0_F.
\]

This contradiction finishes the proof of claim 2. \(\square\)

### 6.3 The invariant \(\text{Cong}(r(t))\)

#### 6.3.1 Reduced resultants

In order to compute the periodic congruence number of the linear, cyclotomic, and split polynomials, we introduce some terminology. We recall that the resultant \(\text{Res}(r(t), s(t))\) of two polynomials \(r(t), s(t) \in \mathbb{Z}[t]\) can be defined as the determinant of the corresponding Sylvester matrix \(\text{Syl}(r(t), s(t))\). By applying Cramer’s rule, we see that there exist polynomials \(R(t), S(t) \in \mathbb{Z}[t]\) such that

\[
\text{Res}(r(t), s(t)) = r(t) \cdot R(t) + s(t) \cdot S(t).
\]

The set of all integers that can be obtained as such a polynomial combination of \(r(t)\) and \(s(t)\) forms an ideal \(I = \mathbb{Z} \cap (r(t) \cdot \mathbb{Z}[t] + s(t) \cdot \mathbb{Z}[t])\) of \(\mathbb{Z}\). And, since \(\mathbb{Z}\) is a principal ideal domain, \(I\) is generated by a single element (unique up to a unit): the reduced resultant \(\text{RRRes}(r(t), s(t))\) of \(r(t)\) and \(s(t)\). This \(\text{RRRes}(r(t), s(t))\) clearly divides the resultant \(\text{Res}(r(t), s(t))\), and it appears in the work of Myerson [46] and Pohst [49] (cf. subsection 2.3 of [59], as well as the threads MathOverflow17501 and MathOverflow248574).

It is possible to extend this definition to more than two polynomials.

**Definition 6.3.1.** We define the reduced resultant \(\text{RRRes}(r_1(t), \ldots, r_n(t))\) of polynomials \(r_1(t), \ldots, r_n(t) \in \mathbb{Z}[t]\) to be the (unique) non-negative generator of the principal ideal

\[
\mathbb{Z} \cap (r_1(t) \cdot \mathbb{Z}[t] + \cdots + r_n(t) \cdot \mathbb{Z}[t]).
\]

We will be interested in the reduced resultants corresponding with periodic decompositions of a polynomial \(r(t) := a_0 + a_1 \cdot t + \cdots + a_d \cdot t^d \in \mathbb{Z}[t]\). Recall from the introduction that, for integers \(u > j \geq 0\), we define the partial sum

\[
r_{u,j}(t) := \sum_{i \equiv j \mod u} a_i \cdot t^i \in \mathbb{Z}[t].
\]
Definition 6.3.2. Let \( u \in \mathbb{N} \). We define the \( u \)'th reduced resultant \( \text{RRes}_u(r(t)) \) of a polynomial \( r(t) \in \mathbb{Z}[t] \) to be the reduced resultant \( \text{RRes}(r_{u,0}(t), \ldots, r_{u,u-1}(t)) \in \mathbb{Z} \), corresponding with the \( u \)'th periodic decomposition \( r(t) = r_{u,0}(t) + \cdots + r_{u,u-1}(t) \) of \( r(t) \).

We immediately obtain:

**Proposition 6.3.3.** The periodic congruence number \( \text{Cong}(r(t)) \) of a non-constant polynomial \( r(t) \in \mathbb{Z}[t] \) of degree \( d \in \mathbb{N} \) is the least common multiple of the reduced resultants

\[
\text{RRes}_2(r(t)), \ldots, \text{RRes}_{d+1}(r(t)).
\]

We will need two elementary properties of reduced resultants.

**Lemma 6.3.4 (Division).** Consider integer polynomials \( a(t), b(t), c(t) \in \mathbb{Z}[t] \) with \( a(t) \cdot b(t) = c(t) \). For every integer \( u \geq 2 \), we have

\[
\text{RRes}_u(a(t)) | \text{RRes}_u(c(t)).
\]

**Proof.** We first note that for every natural \( i \geq 0 \), we have

\[
c_{u,i}(t) = \sum_{j+k \equiv i \mod u} a_{u,j}(t) \cdot b_{u,k}(t).
\]  

(16)

By definition, there exist polynomials \( C_0(t), \ldots, C_{u-1}(t) \in \mathbb{Z}[t] \) that give us the equality \( \text{RRes}_u(c(t)) = \sum_{0 \leq i < u} C_i(t) \cdot c_{u,i}(t) \). Using (16), we obtain:

\[
\text{RRes}_u(c(t)) = \sum_{0 \leq i < u} C_i(t) \cdot \left( \sum_{j+k \equiv i \mod u} a_{u,j}(t) \cdot b_{u,k}(t) \right).
\]

So \( \text{RRes}_u(c(t)) \in (a_{u,0}(t) \cdot \mathbb{Z}[t] + \cdots + a_{u,u-1}(t) \cdot \mathbb{Z}[t]) \cap \mathbb{Z} \). This proves the lemma. \( \square \)

**Lemma 6.3.5 (Composition).** Consider \( r(t) \in \mathbb{Z}[t] \). Consider natural numbers \( u \geq 2 \), and \( n, m \). If \( m \cdot n \equiv 1 \mod u \), then

\[
\text{RRes}_u(r(t^m))) | \text{RRes}_u(r(t)).
\]

**Proof.** Let the polynomial be given by \( r(t) = \sum_{0 \leq j \leq d} a_j \cdot t^j \) and define \( s(t) := r(t^m) \). Then for all \( 0 \leq i < u \), we have

\[
s_{u,i}(t) = \sum_{0 \leq j \leq d \atop m \cdot j \equiv i \mod u} a_j \cdot (t^m)^j = \sum_{0 \leq j \leq d \atop j \equiv n \cdot i \mod u} a_j \cdot (t^m)^j = r_{u,n \cdot i \mod u}(t^m).
\]

By definition, there exist \( c_{u,0}(t), \ldots, c_{u,u-1}(t) \in \mathbb{Z}[t] \) such that \( \text{RRes}_u(r(t)) = \sum_j c_{u,j}(t) \cdot r_{u,j}(t) \). By substituting \( t \mapsto t^m \), we obtain

\[
\text{RRes}_u(r(t)) = \sum_j c_{u,j}(t^m) \cdot r_{u,j}(t^m) \in s_{u,0}(t) \cdot \mathbb{Z}[t] + \cdots + s_{u,u-1}(t) \cdot \mathbb{Z}[t].
\]

We conclude that \( \text{RRes}_u(r(t)) \in (s_{u,0}(t) \cdot \mathbb{Z}[t] + \cdots + s_{u,u-1}(t) \cdot \mathbb{Z}[t]) \cap \mathbb{Z} \). \( \square \)
6.3.2 Examples

Example 6.3.6 (Cf. Examples 2.3.2 and 2.3.1). Let us consider the polynomial \( r(t) = t^3 - 2t - 1 \) again. Then
\[
\begin{align*}
(1) \quad r(1) \cdot \text{Cong}(r(t)) &= (-2) \cdot (2).
\end{align*}
\]
Moreover, the roots of \( r(t) \) in an algebraically-closed field \( \overline{F} \) form an arithmetically-free subset \( X \) of the multiplicative group \( (\overline{F}^\times, \cdot) \) if and only if \( \text{char} (\overline{F}) \neq 2 \). Finally, we have
\[
H(X, \overline{Q}^\times) = 2.
\]

Proof. (i) We first use the Euclidian algorithm in \( \mathbb{Q}[t] \) to find that \( 2 = -2 \cdot r_{2,0}(t) + 0 \cdot r_{2,1}(t) \) and \( 2 = -2 \cdot r_{3,0}(t) - 1 \cdot r_{3,1}(t) + 0 \cdot r_{3,2}(t) \), so that \( \text{Cong}(r(t)) \neq 2 \). On the other hand, we note that \( \text{Cong}(r(t)) \neq 1 \), since otherwise there exist \( s_0(t), s_1(t), s_2(t) \in \mathbb{Z}[t] \) such that
\[
1 \equiv s_0(t) \cdot r_{3,0}(t) + s_1(t) \cdot r_{3,1}(t) + s_2(t) \cdot r_{3,2}(t) \equiv s_0(t) \cdot (t^3 - 1) \mod 2.
\]
So we may conclude that \( \text{Cong}(r(t)) = 2 \).

(ii) We next note that \( r(t) \equiv (t^3 - 1) \mod 2 \), so that the roots of \( r(t) \) in \( \overline{F}_2 \) do not form an arithmetically-free subset of \( (\overline{F}_2^\times, \cdot) \). Now suppose that \( \text{char}(\overline{F}) \neq 2 \). Since \( r(1) \cdot \text{Cong}(r(t)) = -2^2 \), we may use proposition 1.3.11 in order to conclude that the roots of \( r(t) \) in \( \overline{F} \) form an arithmetically-free subset of \( (\overline{F}^\times, \cdot) \). But we may also use proposition 6.1.1 to come to the same conclusion. Let
\[
C := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}
\]
be the companion operator of \( r(t) \). A straight-forward computation in the ring \( \mathbb{Z}[t_1, t_2, t_3] \) then shows that the homogeneous polynomial
\[
\hat{r}(t_1, t_2, t_3) := \det (t_1 \cdot r(C \otimes C) + t_2 \cdot r(C \otimes C^2) + t_3 \cdot r(C \otimes C^3))
\]
\[
= 2^3 \cdot (t_1 + t_3)^3 \cdot (t_2^2 + 7 \cdot t_2 \cdot t_3 + t_3^2)
\]
\[
\cdot (t_1^2 + 7 \cdot t_1 \cdot t_2 + 35 \cdot t_1 \cdot t_3 + t_2^2 + 25 \cdot t_2 \cdot t_3)
\]
\[
\cdot (5 \cdot t_1^2 + 30 \cdot t_1 \cdot t_2 + 135 \cdot t_1 \cdot t_3 + 9 \cdot t_2^2 + 99 \cdot t_2 \cdot t_3 + 63 \cdot t_2 \cdot t_3)
\]
in the variables \( t_1, t_2 \) and \( t_3 \) vanishes precisely if the characteristic of the field is 2.

(iii) Finally, we consider a grading \( \bigoplus \lambda K_{\lambda} \) of a Lie ring \( K \) by the group \( (\overline{Q}^\times, \cdot) \) such that the support is contained in \( X \). Then
\[
[K, K] \subseteq [K_{-1}, K_{-1}] + [K_{-1}, K_{1-\sigma}] + [K_{-1}, K_{1+\sigma}]
\]
\[
+ [K_{1+\sigma}, K_{1+\sigma}] + [K_{1+\sigma}, K_{1-\sigma}] + [K_{1-\sigma}, K_{1-\sigma}] \subset K_{-1},
\]
and therefore \([K, K], K \] \subseteq [K_{-1}, K_{-1}] + [K_{-1}, K_{1-\sigma}] + [K_{-1}, K_{1+\sigma}] \subseteq \{0_K\} \). This proves the inequality \( H(X, \overline{Q}^\times) \leq 2 \). Example 2.3.2 shows that also \( H(X, \overline{Q}^\times) \geq 2 \).
Example 6.3.7 (Constant and linear polynomials). For \( r(t) := a_0 + a_1 \cdot t \in \mathbb{Z}[t] \), we have

\[
r(1) \cdot \text{Cong}(r(t)) = (a_0 + a_1) \cdot |a_0|.
\]

Proof. We had already observed in the introduction that \( a_0 = r(0) \mid \text{Cong}(r(t)) \). But we also have \( a_0 = 1 \cdot r_{2,0}(t) + 0 \cdot r_{2,1}(t) \). So \( \text{Cong}(r(t)) = |a_0| \).

Before computing \( \text{Cong}(\Phi_n(t)) \), we record some elementary properties of the cyclotomic polynomials.

Lemma 6.3.8. Let \( n > 1 \) be a natural number and let \( m \) be its radical. Then \( \text{deg}(\Phi_n(t)) = \phi(n) \), where \( \phi \) is the Euler totient-function. Then

\[
\Phi_n(t) = \Phi_m(t^{n/m}). \quad (17)
\]

Let \( p \) be an odd prime that does not divide \( m \). Then

\[
\Phi_{p \cdot m}(t) \cdot \Phi_m(t) = \Phi_m(t^p). \quad (18)
\]

If \( m \) is odd, then

\[
\Phi_{2 \cdot m}(t) = \Phi_m(-t). \quad (19)
\]

If \( n = m \), then \( \Phi_n(1) = m \). If \( n \neq m \), then \( \Phi_n(1) = 1 \).

Proposition 6.3.9. For every square-free natural number \( n \) and natural number \( u \geq 2 \), we have \( \text{RRes}_u(\Phi_n(t)) = 1 \).

Proof. Define \( r(t) := \Phi_n(t) \). Since \( \text{RRes}_2(-1 + t) = 1 \), we may assume that \( n > 1 \).

Case: \( n \) is a prime. Suppose first that \( u \geq \phi(n) + 1 = (n - 1) + 1 = n \). Then \( r_{u,0}(t) = 1 \), so that \( 1 = 1 \cdot r_{u,0}(t) + 0 \cdot r_{u,1}(t) + \cdots + 0 \cdot r_{u,u-1}(t) \), and therefore \( \text{RRes}_u(r(t)) = 1 \). Next, we suppose that \( 2 \leq u < n \). Then \( n - 1 \not\equiv u - 1 \mod u \), so that \( 1 = r_{u,0}(t) + 0 \cdot r_{u,1}(t) + \cdots + 0 \cdot r_{u,u-2}(t) - t \cdot r_{u,u-1}(t) \). This also implies that \( \text{RRes}_u(r(t)) = 1 \).

Case: \( n \) is square-free and odd. Let us proceed by induction on the number \( l \) of distinct prime factors of \( n \). The base of the induction, \( l = 1 \), is given by the previous paragraph. So we suppose that \( l > 1 \). Let \( n = p_1 \cdots p_l \) be the decomposition of \( n \) into (distinct, odd) primes. We may, as before, suppose that \( u \) is an integer satisfying \( 2 \leq u \leq \phi(n) + 1 = (p_1 - 1) \cdots (p_l - 1) + 1 \). Then we note that there is at least one \( i \in \{1, \ldots, l\} \) such that \( p_i \) does not divide \( u \). Formula (18) tells us that \( \Phi_n(t) | \Phi_{n/p_i}(t^{p_i}) \).

Lemma 6.3.4, lemma 6.3.5, and the induction hypothesis then imply that

\[
\text{RRes}_u(\Phi_n(t)) | \text{RRes}_u(\Phi_{n/p_i}(t^{p_i})) | \text{RRes}_u(\Phi_{n/p_i}(t)) = 1.
\]

Case: \( n \) is square-free and even. Formula (19) gives us the equality \( \Phi_n(t) = \Phi_n/2(-t) \).

The odd case then tells us that

\[
\text{RRes}_u(\Phi_n(t)) = \text{RRes}_u(\Phi_n/2(-t)) = \text{RRes}_u(\Phi_n/2(t)) = 1.
\]
This finishes the proof.

Proposition 6.3.10. For every natural number \( n \), we have:

\[
\text{Cong}(\Phi_n(t)) = \begin{cases} 
1 & \text{if } n \text{ is square-free,} \\
0 & \text{if } n \text{ is not square-free.}
\end{cases}
\]

Proof. Let \( m \) be the radical of \( n \). If \( n \) is not square-free, then the \( n/m \)-partial decomposition of \( \Phi_n(t) \) is \( \Phi_n(t) + 0 + \cdots + 0 \), so that \( \text{RRes}_{n/m}(\Phi_n(t)) = 0 \), and therefore \( \text{Cong}(\Phi_n(t)) = \text{lcm}_{u>1} \text{RRes}_u(\Phi_n(t)) = 0 \). Else, \( n \) is square-free, and we may apply proposition 6.3.9 to conclude that \( \text{Cong}(\Phi_n(t)) = \text{lcm}_{u>1} \text{RRes}_u(\Phi_n(t)) = 1 \).

We immediately obtain:

Example 6.3.11 (Cyclotomic polynomials). Consider a natural number \( n > 1 \) and the corresponding cyclotomic polynomial \( \Phi_n(t) \). Then

\[
\Phi_n(1) \cdot \text{Cong}(\Phi_n(t)) = \begin{cases} 
n & \text{if } n \text{ is a prime,} \\
1 & \text{if } n \text{ is square-free but not a prime,} \\
0 & \text{if } n \text{ is not square-free.}
\end{cases}
\]

Example 6.3.12 (Split polynomials). Let \( n > 1 \) be a natural number, and let us consider the corresponding split polynomial \( \Psi_n(t) := (t^n - 1)/(t - 1) = 1 + t + \cdots + t^{n-1} \in \mathbb{Z}[t] \).

\[
\Psi_n(1) \cdot \text{Cong}(\Psi_n(t)) = \begin{cases} 
n & \text{if } n \text{ is a prime,} \\
0 & \text{if } n \text{ is not a prime.}
\end{cases}
\]

Proof. If \( n \) is a prime, then \( \Psi_n(t) = \Phi_n(t) \), and we may apply 6.3.11. So suppose that \( n \) is composite, and let \( 1 < u < n \) be a divisor of \( n \). Then the \( u \)'th partial decomposition is \( \Psi_n(t) = t^0 \cdot \Psi_{n/u}(t^u) + \cdots + t^{u-1} \cdot \Psi_{n/u}(t^u) \). These terms generate the principal ideal \( \Psi_{n/u}(t^u) \cdot \mathbb{Z}[t] \) in \( \mathbb{Z}[t] \). Since \( \deg(\Psi_{n/u}(t^u)) = (n/u - 1) \cdot u \geq 1 \), we have \( \text{RRes}_u(\Psi_n(t)) = 0 \). So also \( \text{Cong}(\Psi_n(t)) = \text{lcm}_{2 \leq u \leq n} \text{RRes}_u(\Psi_n(t)) = 0 \).

6.4 The invariants \( \text{Discr}_s(r(t)) \) and \( \text{Prod}(r(t)) \)

Let us fix a non-zero polynomial \( r(t) \in \mathbb{Z}[t] \), say of degree \( d \). In the introduction, we had claimed that the invariants \( \text{Discr}_s(r(t)) \) and \( \text{Prod}(r(t)) \) are non-zero integers. Let us briefly verify this and let us also give an effective way of computing these invariants.

6.4.1 Integrality and computation

\( \text{Discr}_s(r(t)) \). When considering \( \text{Discr}_s(r(t)) \), we may assume that \( r(t) \) has degree at least 2, since otherwise the computation is quite straight-forward. As before, we let \( a \) be the leading coefficient of \( r(t) \), we let \( \lambda_1, \ldots, \lambda_l \) be the distinct roots of \( r(t) \) with corresponding
multiplicities $m_1, \ldots, m_l$, and we set $m := \max\{m_1, \ldots, m_l\}$. In other words: we have the factorisation

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

of $r(t)$. We may then use the standard algorithms to compute the square-free factorisation

$$r(t) = u_1(t)^1 \cdot u_2(t)^2 \cdots u_n(t)^n$$

of $r(t)$ in $\mathbb{Z}[t]$, with the convention that $n$ be minimal. Then $u(t) := u_1(t) \cdots u_n(t)$ is a greatest square-free factor $u(t) := u_1(t) \cdots u_n(t)$ of $r(t)$ in $\mathbb{Z}[t]$, and it is unique up to its sign. Then $m = n, \ l = \deg(u(t))$, and the leading coefficient $\bar{a}$ of $u(t)$ divides $a$ in $\mathbb{Z}$. So the polynomial

$$v(t) := (a/\bar{a}) \cdot u(t) = a \cdot (t - \lambda_1) \cdots (t - \lambda_l)$$

has integer coefficients. Let $\text{Syl}(v(t), v'(t))$ be the Sylvester matrix of $v(t)$ and its formal derivative $v'(t)$.

**Lemma 6.4.1.** We have

$$\text{Discr}_*(r(t)) = a^{1+2d^2-2m(l-1)-m} \cdot (m-1)! \cdot (\det (\text{Syl}(v(t), v'(t))))^m$$

and $\text{Discr}_*(r(t)) \in \mathbb{Z} \setminus \{0\}$.

**Proof.** By using the formula $\text{Discr}_*(v(t)) = (-1)^l (l-1)! \cdot a^{2d^2-2} \cdot \prod_{1 \leq i \neq j \leq l} (\lambda_i - \lambda_j)$ we obtain

$$\text{Discr}_*(r(t))/(\{(m-1)! \cdot (\det (\text{Syl}(v(t))))^m\}) = (-1)^{m(l-1)/2} \cdot a^{1+2d^2-2m(l-1)}$$

Since $m, l \leq d$, we have $0 \leq 1 + 2d^2 - 2m(l - 1)$ and therefore $a^{1+2d^2-2m(l-1)} \in \mathbb{Z} \setminus \{0\}$. Since $v(t) \in \mathbb{Z}[t]$, we also have $\text{Discr}(v(t)) \in \mathbb{Z} \setminus \{0\}$. So we may indeed conclude that $\text{Discr}_*(r(t)) \in \mathbb{Z} \setminus \{0\}$. Finally, by using the formula

$$\text{Discr}(v(t)) = (-1)^{(l-1)/2} \cdot a^{-1} \cdot \det (\text{Syl}(v(t), v'(t)))$$

we obtain (20!).

**Remark 6.4.2.** Formula (20) allows us to compute $\text{Discr}_*(r(t))$ *without having to extract roots*. Indeed: the invariants $m, v(t)$, and $l$ are given by the algorithm for the square-free factorisation of $r(t)$.

$\text{Prod}(r(t))$. Let us now find a similar formula for $\text{Prod}(r(t))$. Let $C$ be the companion matrix of $(1/a) \cdot v(t)$ and let us consider its Kronecker square $C \otimes C$. The corresponding characteristic polynomial is given by

$$\chi_{C \otimes C}(t) = \prod_{1 \leq i, j \leq l} (t - \lambda_i \cdot \lambda_j).$$

We may next use the Euclidean algorithm in order to compute a greatest factor $w(t)$ of $\chi_{C \otimes C}(t)$ (in the ring $\mathbb{Q}[t]$) that is co-prime to $r(t)$. Since such a factor $w(t)$ is determined
only up to a (non-zero) rational number, we may choose the unique \( w(t) \) with leading coefficient \( a^{2 \deg(w(t))} \). We then have the factorisation

\[
w(t) = \prod_{1 \leq i, j \leq l, r(\lambda_i, \lambda_j) \neq 0} a^2 \cdot (t - \lambda_i \cdot \lambda_j).
\]

**Lemma 6.4.3.** We have

\[
\Prod(r(t)) = a^{2(d^2 - \deg(w(t)))} \cdot \det(Syl(r(t), w(t)))
\]

and \( \Prod(r(t)) \in \mathbb{Z} \setminus \{0\} \).

**Proof.** We define the auxiliary, monic polynomials

\[
\bar{r}(t) := \prod_{1 \leq i, j \leq l, r(\lambda_i, \lambda_j) \neq 0} (t - a^2 \cdot \lambda_i \cdot \lambda_j) \quad \text{and} \quad \tilde{r}(t) := \prod_{1 \leq i, j \leq l, r(\lambda_i, \lambda_j) = 0} (t - a^2 \cdot \lambda_i \cdot \lambda_j).
\]

These polynomials have rational coefficients since their roots are permuted by every automorphism \( \sigma \in \text{Gal}(\mathbb{Q}(\lambda_1, \ldots, \lambda_l) : \mathbb{Q}) \). In order to prove that \( \bar{r}(t) \in \mathbb{Z}[t] \), we next consider the auxiliary polynomial

\[
s(t; t_1, \ldots, t_l) := \prod_{1 \leq i, j \leq l} (t - t_i \cdot t_j)
\]

in the variable \( t \) with coefficients in the domain \( \mathbb{Z}[t_1, \ldots, t_l] \). According to Vieta’s formula, we have

\[
s(t; t_1, \ldots, t_l) = \sum_{0 \leq k \leq l^2} (-1)^k \cdot e_k^{[t]}(t_1 \cdot t_1, t_1 \cdot t_2, \ldots, t_l \cdot t_l) \cdot t^{l^2 - k},
\]

where each \( e_k^{[t]}(t_1, \ldots, t_l) := \sum_{1 \leq n_1 < \cdots < n_k \leq l} t_{n_1} t_{n_2} \cdots t_{n_k} \) is the elementary symmetric polynomial in the variables \( t_1, \ldots, t_l \). We note that each coefficient \( e_k^{[t]}(t_1^2, \ldots, t_l^2) \) in this expression is a also symmetric polynomial in the variables \( t_1, \ldots, t_l \). So, according to the fundamental theorem for symmetric functions, there exist polynomials \( P_1(t_1, \ldots, t_l), \ldots, P_{l^2}(t_1, \ldots, t_l) \in \mathbb{Z}[t_1, \ldots, t_l] \) such that

\[
s(t; t_1, \ldots, t_l) = \sum_{0 \leq k \leq l^2} P_k(e_1^{[t]}(t_1, \ldots, t_l), \ldots, e_l^{[t]}(t_1, \ldots, t_l)) \cdot t^{l^2 - k}.
\]

By evaluating \( t_i \mapsto a \cdot \lambda_i \), we obtain

\[
s(t; a \cdot \lambda_1, \ldots, a \cdot \lambda_l) = \sum_{0 \leq k \leq l^2} P_k(a \cdot e_1^{[t]}(\lambda_1, \ldots, \lambda_l), \ldots, a^l \cdot e_l^{[t]}(\lambda_1, \ldots, \lambda_l)) \cdot t^{l^2 - k}.
\]

Since \( u(t) = \sum (-1)^k \cdot a \cdot e_k^{[t]}(\lambda_1, \ldots, \lambda_l) \cdot t^{l^2 - k} \) and \( P_1(t_1, \ldots, t_l), \ldots, P_{l^2}(t_1, \ldots, t_l) \) all have integer coefficients, we see that the monic polynomial \( s(t; a \cdot \lambda_1, \ldots, a \cdot \lambda_l) \) also has integer coefficients. Since \( s(t; a \cdot \lambda_1, \ldots, a \cdot \lambda_l) \) is a product

\[
s(t; a \cdot \lambda_1, \ldots, a \cdot \lambda_l) = \tilde{r}(t) \cdot \bar{r}(t)
\]
of two monic polynomials with rational coefficients, we may use Gauss’ lemma to conclude that also \( \overline{r}(t), \overline{w}(t) \in \mathbb{Z}[t] \). We see, in particular, that \( w(t) = \overline{r}(a^2 \cdot t) \in \mathbb{Z}[t] \), so that \( \text{Res}(r(t), w(t)) \in \mathbb{Z} \). We now observe that

\[
\text{Prod}(r(t)) := a^{2d^3} \cdot \prod_{1 \leq i, j \leq l} r(\lambda_i \cdot \lambda_j)
\]

is a non-zero integer. By using the formula \( \text{Res}(r(t), w(t)) = \det(Syl(r(t), w(t))) \), we finally obtain formula (22).

**Remark 6.4.4.** Formula (22) allows us to compute \( \text{Prod}(r(t)) \) without having to extract roots. Indeed: we only need the algorithm for the square-free factorisation of \( r(t) \) in \( \mathbb{Z}[t] \) and the Euclidean algorithm in the ring \( \mathbb{Q}[t] \).

### 6.4.2 Examples

**Example 6.4.5** (Cf. Examples 2.3.2, 2.3.1, and 6.3.6). Once more we consider the monic polynomial \( r(t) := t^3 - 2t - 1 \) with integer coefficients. We then have

\[
\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t)) = (-5) \cdot (-2^7 \cdot 5).
\]

**Proof.** The roots of this polynomial are simple and given by \( \lambda_1 := -1, \lambda_2 := \frac{1 - \sqrt{5}}{2} \) and \( \lambda_3 := \frac{1 + \sqrt{5}}{2} \). By definition, we therefore have

\[
\text{Discr}_*(r(t)) = -(\lambda_1 - \lambda_2)^2 \cdot (\lambda_2 - \lambda_3)^2 \cdot (\lambda_3 - \lambda_1)^2 = -5.
\]

We next note that \( r(\lambda_i \cdot \lambda_j) = 0 \) if and only if \( \{i, j\} = \{2, 3\} \). So definition 1.3.5 gives us

\[
\text{Prod}(r(t)) := \prod_{1 \leq i, j \leq 3} r(\lambda_i \cdot \lambda_j) = -2^7 \cdot 5.
\]

Let us now come to the same conclusions without using the polynomial’s roots.

**Proof.** Since \( r(t) \) is monic, we do not have to keep track of leading coefficients. The square-free factorisation of the monic polynomial \( r(t) \) is given by \( r(t) = u_1(t)^1 \), so that \( r(t) = u(t) = v(t) \) and \( m = 1 \). By using formula (20), we obtain

\[
\text{Discr}_*(r(t)) = (1 - 1)! \cdot \det \begin{pmatrix}
1 & 0 & -2 & -1 & 0 \\
0 & 1 & 0 & -2 & -1 \\
3 & 0 & -2 & 0 & 0 \\
0 & 3 & 0 & -2 & 0 \\
0 & 0 & 3 & 0 & -2
\end{pmatrix} = -5.
\]

The companion matrix of \( r(t) \) is

\[
C := \begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 2 & 0
\end{pmatrix},
\]

44
so that its Kronecker-square is given by

\[
C \otimes C := \begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 2 \\
0 & 1 & 0 & 0 & 2 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 2 & 0 \\
1 & 2 & 0 & 2 & 4 & 0 & 0 \\
\end{pmatrix}
\]

We therefore have \( \chi_{C \otimes C}(t) = -(-1 + t)(1 + t)^2(1 - 3t + t^2)(-1 + t + t^2)^2 \) and \( w(t) = (t^2 + t - 1)^2(t^2 - 3t + 1)(-1). \) Formula (21) allows us to conclude once more that

\[
\text{Prod}(r(t)) = \det \begin{pmatrix}
1 & 0 & -2 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -2 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & -2 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & -2 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & -2 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -2 & -1 \\
1 & -2 & -5 & 9 & 3 & -11 & 6 & -1 & 0 \\
0 & 1 & -2 & -5 & 9 & 3 & -11 & 6 & -1 \\
0 & 0 & 1 & -2 & -5 & 9 & 3 & -11 & 6 \\
\end{pmatrix} = -2^7 \cdot 5.
\]

**Example 6.4.6** (Linear polynomials). For every polynomial \( r(t) := a_0 + a_1 \cdot t \in \mathbb{Z}[t] \) of degree 1, we have

\[
\text{Discr}_n(r(t)) \cdot \text{Prod}(r(t)) = \begin{cases}
(a_1^2) \cdot (a_0 \cdot a_1 \cdot (a_0 + a_1)) & \text{if } a_0 \cdot (a_0 + a_1) \neq 0, \\
(a_1^2) \cdot (a_2^2) & \text{if } a_0 \cdot (a_0 + a_1) = 0.
\end{cases}
\]

**Proof.** By definition, we have \( \text{Discr}_n(r(t)) := a_1^{1+2+1} \cdot (1-1)! \cdot 1 = a_1^2. \) The root of \( r(t) \) is \( \lambda_1 := -a_0/a_1. \) If \( \lambda_1^2 \neq \lambda_1, \) then \( a_0(a_0 + a_1) \neq 0 \) and \( \text{Prod}(r(t)) := a_1^2 \cdot (a_1(\lambda_1 \cdot \lambda_1) + a_0) = a_0 a_1(a_0 + a_1). \) Else, we have \( a_0(a_0 + a_1) = 0, \) so that \( \text{Prod}(r(t)) := a_2^2 \cdot 1. \)

**Example 6.4.7** (Cyclotomic polynomials). Consider a natural number \( n > 1 \) and the corresponding cyclotomic polynomial \( \Phi_n(t). \) Then \( \text{Discr}_n(\Phi_n(t)) \cdot \text{Prod}(\Phi_n(t)) \) divides a natural power of \( n. \)

**Proof.** If \( n = 2, \) then \( \Phi_2(t) = 1 + t, \) so that we need only apply example 6.4.6. So we assume that \( n > 2. \) Since the cyclotomic field \( K_n \) corresponding with \( \Phi_n(t) \) is monogenic,
we know that $\text{Discr}(\Phi_n(t))$ coincides with the field discriminant

$$\Delta_{K_n} = (-1)^{\varphi(n)/2} \cdot n^{\varphi(n)/2} \prod_{p \mid n} p^{\varphi(n)/\varphi(p)}$$

of $K_n$. We see, in particular, that $\text{Discr}_*(\Phi_n(t))$ divides $n^n$.

By construction, for each root $\lambda$ of the monic polynomial $\Phi_n(t)$, there exists a natural $m$ (properly) dividing $n$, such that $\lambda$ is an $m$'th root of unity. Since also $\overline{\Phi_n(t)} \in \mathbb{Z}[[t]]$, there exist non-negative integers $a_m$ such that

$$\overline{\Phi_n(t)} = \prod_{m \mid n, m \neq n} \Phi_m(t)^{a_m}.$$ 

So

$$\text{Prod}(\Phi_n(t)) = \text{Res}(\Phi_n(t), \overline{\Phi_n(t)}) = \prod_{m \mid n, m \neq n} \text{Res}(\Phi_n(t), \Phi_m(t))^{a_m}.$$ 

The factors in this expression were computed explicitly by E. Lehmer [40], Apostol [3], Dresden [15], and several others [8]. We see, in particular, that also $\text{Prod}(\Phi_n(t))$ divides a natural power of $n$. This finishes the proof. \hfill \Box

Example 6.4.8 (Split polynomials). Consider a natural number $n > 1$ and the corresponding split polynomial $\Psi_n(t) = 1 + t + \cdots + t^{n-1}$. Then

$$\text{Discr}_*(\Psi_n(t)) \cdot \text{Prod}(\Psi_n(t)) = (n^{n-2}) \cdot (n^{n-1}).$$

Proof. According to formula (20), we have:

$$\text{Discr}_*(\Psi_n(t)) = \det (\text{Syl}(\Psi_n(t), \Psi_n'(t))) = \text{Res}(\Psi_n(t), \Psi_n'(t)) = \text{Res}(t-1, \Psi_n'(t))^{-1} \cdot \text{Res}(t^n - 1, \Psi_n'(t)) = (-1)^n \cdot \binom{n}{2}^{-1} \cdot \det (\text{Syl}(t^n - 1, \Psi_n'(t))).$$

By performing row and column operations on the matrix $\text{Syl}(t^n - 1, \Psi_n'(t))$, we obtain

$$\det (\text{Syl}(t^n - 1, \Psi_n'(t))) = -\det \begin{pmatrix}
0 & 1 & 2 & \cdots & n - 1 \\
1 & 0 & 1 & \cdots & n - 2 \\
2 & 1 & 0 & \cdots & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 2 & 3 & \cdots & 0
\end{pmatrix} = (-1)^n \cdot \binom{n}{2} \cdot n^{n-2}. \quad 46$$
So $\text{Discr}_n(\Psi_n(t)) = n^{n-2}$. Now let $\omega_n$ be a primitive $n$'th root of unity. We then have

$$\nabla_n(t) = \prod_{0 < i, j < n \mod n} (t - \omega_n^{i+j}) = (t - 1)^{n-1},$$

and therefore \(\text{Prod}(\Psi_n(t)) = \text{Res}(\Psi_n(t), \nabla_n(t)) = \Psi_n(1)^{n-1} = n^{n-1}. \) \hfill \Box

### 7 Corollaries of the main theorem

#### 7.1 Periodic groups that are residually-finite

##### 7.1.1 Special case: \(p\)-groups that are residually-finite

**The Zassenhaus series.** We fix a prime \(p\) and we recall some definitions from the literature. The Zassenhaus series \((\Delta_n(G, p))_{n \in \mathbb{N}}\) of a group \(G\) with respect to \(p\) is defined by the formula

$$\Delta_n(G, p) := \prod_{i, j \leq n} \Gamma_{i,p}(G)^{p^j}. $$

Alternatively, it can be defined by \(\Delta_n(G, p) := \{g \in G \mid g - 1 \in \Delta^n\}\), where \(\Delta\) is the augmentation ideal of the group algebra \(\mathbb{F}_p G\) of \(G\) over the prime field \(\mathbb{F}_p\). It is easy to verify that a finitely-generated group \(G\) is residually-(a finite \(p\)-group) if and only if \(\bigcap_{n \in \mathbb{N}} \Delta_n(G, p) = \{1_G\}\).

**The (restricted) Lazard Lie algebra.** This series \((\Delta_n(G, p))_n\) is known to be a characteristic Lie-series of \(G\). So we can define a Lie ring

$$L(G, p) := \bigoplus_{n \in \mathbb{N}} \Delta_n(G, p)/\Delta_{n+1}(G, p),$$

as in proposition 5.1.1. And, since the additive group \((L(G, p), +)\) has exponent \(p\), the Lie ring \(L(G, p)\) also admits coefficients in \(\mathbb{F}_p\). This Lie algebra over \(\mathbb{F}_p\) is the Lazard Lie algebra of \(G\) with respect to the prime \(p\). But \(L(G, p)\) admits even more structure. For each homogeneous subspace \(L_n := \Delta_n(G, p)/\Delta_{n+1}(G, p)\) of \(L(G, p)\), we can define a map

$$[p] : L_n \rightarrow L_{p^n} : g \cdot \Delta_{n+1}(G, p) \mapsto g^p \cdot \Delta_{p^n+1}(G, p).$$

One can then verify that these maps extend to a map \([p] : L(G, p) \rightarrow L(G, p)\) on all of \(L(G, p)\) such that \((L(G, p), [p])\) is a \(p\)-restricted Lie algebra over \(\mathbb{F}_p\) (in the sense of Jacobson [32]). We note that \(L(G, p)\) is generated, as a restricted Lie algebra, by the homogeneous component \(L_1 = \Delta_1(G, p)/\Delta_2(G, p)\).

**The nilpotency of \(L(G, p)\).** Just like the Lie ring corresponding with the lower central series, this restricted Lie algebra \(L(G, p)\) captures important properties of a group \(G\). Let us prove one property (proposition 7.1.3) that will be used in the proof of corollary 1.2.4.

---

4 This series is also known as the Jennings, Lazard, Brauer, or \(p\)-lower central series.
Lemma 7.1.1. Consider a finitely-generated group $G$ that is residually-(a finite $p$-group). Suppose that $G$ admits an automorphism $\alpha : G \to G$ with a monic identity $r(t)$ satisfying $r(1) \cdot \text{Cong}(r(t)) \not\equiv 0 \mod p$. Then $L(G, p)$ is nilpotent.

Proof. We recall that the induced automorphism $\overline{\alpha} : L(G, p) \to L(G, p)$ of the Lie algebra $L$ satisfies $\overline{\alpha}(\overline{L}) = 0_{L(G, p)}$. Since $G$ is finitely-generated and since the Zassenhaus-series is characteristic, each of the homogeneous components $L_n := \Delta_n(G, p)/\Delta_{n+1}(G, p)$ of $L(G, p)$ will be a finite-dimensional, $\alpha$-invariant subspace of $L(G, p)$. So we may combine propositions 1.3.11 and 4.1.2 in order to conclude that $L(G, p)$ is nilpotent.

Lemma 7.1.2. Consider a finitely-generated group $G$ that is residually-(a finite $p$-group) and suppose that $L(G, p)$ is nilpotent. If $G$ is periodic, then $G$ is finite.

Proof. Define $M$ to be the ordinary subalgebra of $L(G, p)$ that is generated by the (finite-dimensional) homogeneous component $L_1 = \Delta_1(G, p)/\Delta_2(G, p)$ of $L(G, p)$. As a subalgebra of $L(G, p)$, this $M$ is nilpotent. Since $M$ is also finitely-generated, this $M$ is finite-dimensional over $\mathbb{F}_p$. Let $\{v_1, \ldots, v_l\}$ be a basis for $M$. Bahturin’s lemma for restricted Lie algebras (proposition 2, p. 17, of [5]) now implies that $L(G, p)$ is spanned by the elements of

$$B := \bigcup_{j \in \mathbb{Z}_{\geq 0}} \{v_1^{[pj]}, \ldots, v_l^{[pj]}\}.$$  

By assumption, each element of $G$ is annihilated by a natural power of $p$, so that this set $B$ is finite. As a result, we may conclude that $L(G, p)$ is finite-dimensional over $\mathbb{F}_p$, and therefore finite. Since $G$ is residually-finite, we have $|G| = |L(G, p)| \cdot |\bigcap_n \Delta_n(G, p)| = |L(G, p)|$. So also $G$ is finite.

Proposition 7.1.3. Consider a finitely-generated $p$-group $G$ that is residually-finite. Suppose that $G$ admits an automorphism $\alpha : G \to G$ with a monic identity $r(t)$ satisfying $r(1) \cdot \text{Cong}(r(t)) \not\equiv 0 \mod p$. Then $G$ is finite.

Proof. We need only combine lemmas 7.1.1 and 7.1.2.

7.1.2 Proof of corollary 1.2.4

We consider a periodic, residually-finite group $G$, together with an automorphism $\alpha : G \to G$ and a monic and monotone identity $r(t) = a_0 + a_1 \cdot t + \cdots + a_d \cdot t^d \in \mathbb{Z}[t]$ of $\alpha$. We assume that $G$ has no $(r(1) \cdot \text{Cong}(r(t)))$-torsion. We may assume that $a_d = 1$.

Claim 1: Every finitely-generated subgroup $S$ of $G$ is contained in a finitely-generated, $(\alpha)$-invariant subgroup $\tilde{S}$ of $G$.

Proof. The subgroup $S$ is contained in the finitely-generated subgroup

$$\tilde{S} := \langle \alpha^{-(d-1)}(S), \ldots, \alpha^{-1}(S), S, \alpha(S), \ldots, \alpha^{d-1}(S) \rangle$$
of $G$. We need only show that $\tilde{S}$ is invariant under $\alpha$ and $\alpha^{-1}$. Since $a_d = 1$, we have $\alpha(S) \subseteq \langle \tilde{S}, \alpha^d(S) \rangle = \langle \tilde{S}, \alpha^d(S^a) \rangle \subseteq \langle \tilde{S}, S, \alpha(S), \ldots, \alpha^{d-1}(S) \rangle = \tilde{S}$. Since $a_0 | \text{Cong}(r(t))$ and since $G$ has no $\text{Cong}(r(t))$-torsion, we see that $\alpha^{-1}(S) \subseteq \langle \alpha^{-d}(S), \tilde{S} \rangle = \langle \alpha^{-d}(S^a), \tilde{S} \rangle \subseteq \langle S, \alpha^{-1}(S), \ldots, \alpha^{-(d-1)}(S) \rangle, \tilde{S} = \tilde{S}$.

Claim 2: $G$ is locally-finite and nilpotent.

Proof. Let $S$ be an arbitrary finitely-generated subgroup of $G$, and let us show that $S$ is finite and nilpotent. According to the previous claim, we may assume that $S$ is $\langle \alpha \rangle$-invariant. As a subgroup of the residually-finite group $G$, this $S$ admits a family of finite-index, characteristic subgroups $(S_i)_i$ with trivial intersection. Since none of the finite quotients $S/S_i$ has any $(r(1) \cdot \text{Cong}(r(t)))$-torsion, we may apply our main theorem 1.2.3 in order to conclude that each finite quotient $S/S_i$ is nilpotent.

Since $S$ is finitely-generated, periodic, and residually-nilpotent, we may use a well-known result of Baer (as in [55]) in order to conclude that $S$ decomposes as the direct product $\prod_p T_p$ of finitely-many maximal $p$-subgroups, $T_p$ (where each $p$ is a prime). Since every such subgroup $T_p$ is finitely-generated and $\langle \alpha \rangle$-invariant, we may further suppose that $S$ is a finitely-generated, residually-finite, $p$-group. So we may apply proposition 7.1.3 to $S$ in order to conclude that $S$ is a finite (and therefore nilpotent) $p$-group.

Claim 3: $\Gamma_{d^2+1}(G)$ is a $(\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t)))$-group.

Proof. We need only show that the order of each element in $\Gamma_{d^2+1}(G)$ divides a natural power of $(\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t)))$. The group $G$ is the union of its finitely-generated subgroups. According to claims 1 and 2, each of these subgroups $S$ is contained in a finite, $\langle \alpha \rangle$-invariant subgroup $\tilde{S}$. So $G = \bigcup F$ and $\Gamma_{d^2+1}(G) = \bigcup F \Gamma_{d^2+1}(F)$, where $F$ runs over the finite, $\langle \alpha \rangle$-invariant subgroups of $G$. We now apply theorem 1.2.3 to these subgroups $F$, the induced automorphism $\alpha F : F \rightarrow F$, and the polynomial $r(t)$ in order to conclude that every element of $\Gamma_{d^2+1}(F)$ is a $(\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t)))$-torsion element.

This finishes the proof of corollary 1.2.4.

7.2 Regular automorphisms of finite groups

7.2.1 Special case: finite, solvable groups

Theorem 7.2.1. Consider a finite, solvable group $G$, together with a regular automorphism $\alpha : G \rightarrow G$ and an identity $r(t)$ of $\alpha$. Then $G$ has a characteristic subgroup $K$ such that

1. $C$ is a $\text{Cong}(r(t))$-group, and
2. $G/K$ is nilpotent and it has no $\text{Cong}(r(t))$-torsion.
Let us use the abbreviation $\kappa := \text{Cong}(r(t))$. We first observe that the conclusions of the theorem are satisfied in three special cases:

(O.a.) Every nilpotent group satisfies the conclusions, since its $\kappa$-torsion subgroup is characteristic and the corresponding quotient is a nilpotent $\kappa'$-group.

(O.b.) Every $\kappa$-group also satisfies the conclusions in a trivial way.

(O.c.) Every finite $\kappa'$-group satisfies the conclusions according to proposition 3.1.1.

We assume that the theorem is false and we will eventually derive a contradiction. Let $G$ be a counter-example of minimal order. We then observe that,

(O.d.) Every proper characteristic section of $G$ satisfies the conclusion of the theorem.

We will repeatedly use observations (O.a.), (O.b.), (O.c.), and (O.d.) in the proof.

Claim 1: If a characteristic subgroup $D$ of $G$ is a $\kappa$-group, then $D = \{1_G\}$.

Proof. Suppose otherwise. Then $G/D$ is a proper quotient of $G$. By the minimality of $G$ as a counter-example, there exists some characteristic subgroup $E/D$ of $G/D$ that is a $\kappa$-group with nilpotent, $\kappa'$ quotient $(G/D)/(E/D)$. As an extension of two $\kappa$-groups ($D$ and $E/D$), the characteristic subgroup $E$ of $G$ is also a $\kappa$-group. Moreover, $G/E \cong (G/D)/(E/D)$ is nilpotent and it has no $\kappa$-torsion. This contradicts our choice of $G$. □

Claim 2: If a characteristic subgroup $D$ of $G$ has $\kappa$-torsion, then $D = G$.

Proof. Suppose otherwise. Then $D$ is proper, so that it has a non-trivial, characteristic $\kappa$-subgroup $E$. The subgroup $E$ is then also characteristic in $G$. This contradicts the previous claim. □

Let $F$ be the Fitting subgroup of $G$. Since $G$ is assumed to be a finite, solvable group, we have

$$1_G < F < G.$$  

Claim 3: Then $F$ has no $\kappa$-torsion.

Proof. Since $F$ is a proper, characteristic subgroup of $G$, we need only apply the previous claim. □

Claim 4: Then $F$ is elementary-abelian.

Proof. Let $P$ be an arbitrary, non-trivial, characteristic subgroup of $F$. Then $G/P$ has a characteristic, $\kappa$-subgroup $E/P$ with $\kappa$-torsion-free, nilpotent quotient $(G/P)/(E/P) \cong G/E$. This $E$ is naturally also characteristic in $G$.

Suppose for a moment that $E \neq G$. Then the second claim implies that $E$ has no $\kappa$-torsion. Since $E/P$ is a $\kappa$-group, we conclude that $E = P$. But, in this case, $G$ is the
extension of two groups (\(P\) and \(G/P\)) that are both \(\kappa\)-torsion-free. So \(G\) has no \(\kappa\)-torsion. Observation (O.c.) implies that \(G\) is nilpotent, which contradicts our choice of \(G\).

So we may conclude that for every non-trivial, characteristic subgroup \(P\) of \(F\), the quotient \(G/P\) is a \(\kappa\)-group. Now note that \(|G/P| = |G/F| \cdot |F/P|\). Since \(F\) has no \(\kappa\)-torsion, neither has \(F/P\). So \(|F/P| = 1\) and \(F = P\). This implies that the Fitting subgroup \(F\) coincides with each of its non-trivial characteristic subgroups. This proves that \(F\) is characteristically-simple. Since \(F\) is also nilpotent, we conclude that \(F\) is indeed elementary-abelian.

\[\text{Claim 5: Then } G/F \text{ is elementary-abelian.}\]

\[\text{Proof.} \quad \text{Since } G \text{ is solvable, so is } G/F, \text{ so that we need only prove that } G/F \text{ is a characteristically-simple group. Let } E/F \text{ be a proper characteristic subgroup of } G/F \text{ and let us show that it is the trivial group. This } E \text{ is proper and characteristic in } G. \text{ According to the second claim, this } E \text{ has no } \kappa\text{-torsion. According to observation (O.c.), this } E \text{ is nilpotent. As a normal, nilpotent subgroup of } G, \text{ this } E \text{ is contained in the Fitting subgroup } F \text{ of } G. \text{ So } E/F \text{ is indeed the trivial subgroup of } G/F.\]

\[\text{Claim 6: There exist distinct primes } p \text{ and } q, \text{ together with an elementary-abelian } p\text{-group } P, \text{ and an elementary-abelian } q\text{-group } Q \text{ such that:}\]

\[\text{i. } G = Q \rtimes P,\]

\[\text{ii. } \alpha(Q) = Q \neq 1_Q \text{ and } \alpha(P) = P \neq 1_P,\]

\[\text{iii. } C_G(Q) = Q, \text{ and}\]

\[\text{iv. For every } u \in \{2, \ldots, \deg(r(t)) + 1\}, \text{ we have } \gcd_{0 \leq j \leq u-1}(r_{u,j}(t) \mod q) = 1_{F_q}.\]

\[\text{Proof.} \quad \text{According to claim 4, the (non-trivial, characteristic, self-centralising) subgroup } F \text{ of } G \text{ is isomorphic to an elementary-abelian } q\text{-group } Q, \text{ for some prime } q. \text{ According to claim 5, the (non-trivial) quotient } G/F \text{ is isomorphic to an elementary-abelian } p\text{-group, for some prime } p. \text{ If } p = q, \text{ then } G \text{ is obviously nilpotent (contradicting our choice of } G). \text{ So } p \neq q \text{ and we may use lemma 3.0.1 to find an } \alpha\text{-invariant subgroup } P \text{ of } G \text{ (necessarily isomorphic to } G/F \text{) that complements } Q:\]

\[G = Q \rtimes P.\]

By definition, for each \(2 \leq u \leq \deg(r(t)) + 1\), there exist polynomials \(s_0(t), \ldots, s_{u-1}(t) \in \mathbb{Z}[t]\) such that \(s_0(t) \cdot r_{u,0}(t) + \cdots + s_{u-1}(t) \cdot r_{u,u-1}(t) = \kappa.\) According to claim 3, we have \(\kappa \neq 0 \mod q.\) So we may indeed conclude that \(\gcd_{0 \leq j \leq u-1}(r_{u,j}(t) \mod q) = 1_{F_q}.\)

We have now shown that our group \(G\) satisfies claim 1 in the proof of proposition 3.1.1. We may now re-cycle steps 2, 3, 4, 5 and 6 of that proof (verbatim) in order to obtain our contradiction. This finishes the proof of theorem 7.2.1.

51
7.2.2 Proof of corollary 1.2.5

We consider a finite group $G$ admitting a regular automorphism $\alpha : G \rightarrow G$. Let $r(t)$ be any non-zero identity $r(t)$ of $\alpha$, say of degree $d$, and let $X$ be its set of roots in $\overline{\mathbb{Q}}$.

**Claim:** Then $G$ is a split extension of the form $G = S \rtimes N$, where $S$ is a solvable $(r(1) \cdot \text{Cong}(r(t)) \cdot \text{Discr}(r(t)) \cdot \text{Prod}(r(t)))$-subgroup and where $N$ is a nilpotent subgroup of class at most $d^2$.

**Proof.** Let us abbreviate $\kappa := \text{Cong}(r(t))$, $\delta := \text{Discr}(r(t))$, and $\pi := \text{Prod}(r(t))$. According to Rowley’s theorem 1.1.1, the group $G$ is solvable. So we may apply theorem 7.2.1 in order to find a characteristic $\kappa$-subgroup $K$ of $G$ such that $G/K$ is a nilpotent $\kappa'$-group. Let $S/K$ be the $(r(1) \cdot \delta \cdot \pi)$-torsion subgroup of $G/K$. Then $S$ is a characteristic $(r(1) \cdot \kappa \cdot \delta \cdot \pi)$-subgroup of $G$ and the nilpotent quotient $G/S \cong (G/K)/(S/K)$ has no $(r(1) \cdot \kappa \cdot \delta \cdot \pi)$-torsion.

We may assume that $r(1) \cdot \kappa \neq 0$, since otherwise $G/S$ is the trivial group, and there is nothing further to prove. We then consider the induced automorphism $\overline{\alpha} : G/S \rightarrow G/S$. Since $r(t)$ is an identity of $\overline{\alpha}$, we may use our main theorem 1.2.3 in order to conclude that the quotient $G/S$ is nilpotent of class at most $H(X, \overline{\mathbb{Q}}^\times) \leq d^2$. Since $\gcd(|S|, |G/S|) = 1$, we may use the theorem of Schur—Zassenhaus in order to conclude that $G$ is a split extension of $S$ by $G/S$. \qed

Let us illustrate this proof with an example.

**Example 7.2.2.** Consider a finite group $G$ with a regular automorphism $\alpha : G \rightarrow G$ and suppose that $r(t) := t^3 - 2t - 1$ is an identity of $\alpha$. Then $\Gamma_3(G)$ is a solvable 10-group and the Fitting-height of $G$ is at most 2.

**Proof.** Let $X$ be the set of roots of $r(t)$ in $\overline{\mathbb{Q}}$. According to example 6.3.6 and example 6.4.5, we have:

| $r(t)$ | $-2$ | $2$ | $-5$ | $-2^7 \cdot 5$ | $2$ |
|-------|------|-----|------|----------------|----|
| $r(1)$ | $\text{Cong}(r(t))$ | $\text{Discr}(r(t))$ | $\text{Prod}(r(t))$ | $H(X, \overline{\mathbb{Q}}^\times)$ |

So $K$ is a 2-group and $G/K$ is a nilpotent group of odd order. This already shows that the Fitting-height of $G$ is at most 2. Finally, the lower central term $[[G, G], G] = \Gamma_{H(X, \overline{\mathbb{Q}}^\times) + 1}(G)$ of the group $G$ is contained in the solvable $(2 \cdot 5)$-group $S$. \qed

**Remark 7.2.3.** The groups of example 7.2.2 exist. For (non-trivial) examples, we refer to the discrete Heisenberg group of example 2.3.1, to the twisted Heisenberg group of example 2.3.2, and to corollary 2.2.7.
8 Applications

8.1 Linear polynomials

We recall that an endomorphism $\gamma : G \to G$ of a group $G$ is a (universal) power endomorphism if there exists an integer $m$ such that for all $x \in G$ we have $\gamma(x) = x^m$.\footnote{A group admitting such an endomorphism is also said to be $m$-commutative (or $m$-abelian).}

It is immediately clear that such an endomorphism has $r(t) = -m + t$ as a monotone identity. Moreover, we see that $\gamma$ is a regular automorphism if and only if $\gcd(|G|, r(0) \cdot r(1)) = \gcd(|G|, m \cdot (m - 1)) = 1$.

Power endomorphisms naturally appear in the study of autoproperties \cite{9} and of Schur-multipliers \cite{42}. More generally, we may consider endomorphisms admitting a linear identity that is not necessarily monic or monotone.

**Proposition 8.1.1.** Consider a finite group $G$ admitting an endomorphism with a linear identity $a_0 + a_1 \cdot t \in \mathbb{Z}[t]$. If $\gcd(|G|, a_0 \cdot a_1 \cdot (a_0 + a_1)) = 1$, then $G$ is abelian.

**Proof.** Set $r(t) := a_0 + a_1 \cdot t$. According to Example 6.3.7, we have $r(1) \cdot \text{Cong}(r(t)) = (a_0 + a_1)\cdot |a_0|$. Since $G$ has no $a_0 \cdot (a_0 + a_1)$-torsion, we may apply our main theorem 1.2.3 in order to conclude that $[G, G]$ is a $(\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t)))$-group. But, according to Example 6.4.6, we have $\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t))|a_0 \cdot a_1 \cdot (a_0 + a_1)$. And, since we have assumed that $G$ has no $a_0 \cdot a_1 \cdot (a_0 + a_1)$-torsion, we may conclude that $[G, G] = \{1_G\}$. \qed

We recover, in particular, a classic result of Baer \cite{4}, Schenkman—Wade \cite{51}, and Alperin \cite{2}: a finite group is abelian if it admits a regular power automorphism.

8.2 Cyclotomic polynomials

8.2.1 Proof of theorems 1.2.7 and 1.2.8

Let us do this in a few steps. For a natural number $n$, we let $\pi$ be the radical of $n$: the product of the distinct primes that divide $n$.

**Lemma 8.2.1.** Let $G$ be a group with a cyclotomic automorphism $\alpha : G \to G$ of index $n > 1$. Then $\alpha^{n/\pi} : G \to G$ is a cyclotomic automorphism of square-free index $\pi$.

**Proof.** According to formula (17) of lemma 6.3.8, we have $\Phi_n(t) = \Phi_{n/\pi}(t^{n/\pi})$. So, if $\Phi_n(t)$ is a monotone identity of $\alpha$, then $\Phi_{n/\pi}(t)$ is a monotone identity of $\alpha^{n/\pi}$. \qed

**Proposition 8.2.2.** A finite group is nilpotent if it admits a cyclotomic automorphism.

**Proof.** According to lemma 8.2.1, we may assume that the index $n$ is square-free. If $n$ is a prime, then we apply Kegel’s theorem 1.1.5. Else, we may combine example 6.3.11 with theorem 1.2.3. \qed

53
We can also give an upper bound on the class of the group.

**Proposition 8.2.3.** Consider a finite group $G$ with a cyclotomic automorphism of index $n > 1$. Let $p$ be the largest prime dividing $n$ and let $\overline{\pi}$ be the radical of $n$.

1. If $\overline{\pi} = p$ and $G$ has no $p$-torsion, then $c(G) \leq (p - 1)^{2(p-1)}$.
2. If $\overline{\pi} = p$ and if $G$ is a $p$-group, then $c(G) \leq C(d(G), p)$.
3. If $\overline{\pi} \neq p$, then $c(G) \leq (p - 1)^{2(p-1)}$.

More generally: if $P$ is the $p$-Sylow subgroup of $G$, then we have

$$c(G) \leq \max\{(p - 1)^{2(p-1)}, C(d(P), p)\} \leq \max\{(p - 1)^{2(p-1)}, C(d(G), p)\}.$$

**Proof.** Proposition 8.2.2 tells us that $G$ is nilpotent. Let $\alpha : G \to G$ be the cyclotomic automorphism of index $n > 1$. According to lemma 8.2.1, we may assume that $n$ is square-free. (i.) We combine our main theorem 1.2.3 with examples 6.3.11 and 6.4.7. (ii.) We need only apply theorem 1.1.6. (iii.) We need only show that an arbitrary $p$-Sylow subgroup $Q$ of $G$ satisfies $c(Q) \leq (p - 1)^{2(p-1)}$. We let $L$ be the Lie ring of $Q$ corresponding with the lower central series of $Q$, as in proposition 5.1.1. Then the Lie automorphism $\overline{\pi} : L \to L$ satisfies $\Phi_n(\overline{\pi}) = 0_L$. Since $n$ is composite, there exists a prime $l$, distinct from $q$, that divides $n$. We may then apply (17) of lemma 6.3.8 in order to obtain a natural number $\mu$ such that $\Phi_n(l)$ divides $\Phi_l(\mu)$ in the ring $\mathbb{Z}[l]$. Then the Lie automorphism $\overline{\pi}$ satisfies $\Phi_l(\overline{\mu}) = 0_L$. The first claim now gives us $c(Q) = c(L) \leq (l - 1)^{2(l-1)} \leq (p - 1)^{2(p-1)}$. \[\square\]

This already proves theorems 1.2.7 and 1.2.8 in the finite case. In order to extend these results from finite groups to locally-(residually-finite) groups, we make some elementary observations.

**Lemma 8.2.4.** Consider a group $G$ with an automorphism $\alpha : G \to G$ and a monotone identity $r(t) := a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{Z}[t]$ of degree $n \geq 1$. Suppose that $a_0, a_n \in \{1, -1\}$. Let $H$ be a finitely-generated subgroup of $G$ and define the subgroup

$$\tilde{H} := \langle \alpha^{-n+1}(H), \ldots, \alpha^{-1}(H), H, \alpha(H), \ldots, \alpha^n(H) \rangle$$

of $G$. Then $\tilde{H}$ is $(\alpha)$-invariant and $d(\tilde{H}) \leq (2n - 1) \cdot d(H)$. Suppose, moreover, that $G$ is residually-finite. Then $\tilde{H}$ admits a family $(\tilde{H}_i)_i$ of $\tilde{H}$-characteristic, finite-index subgroups with trivial intersection, so that $r(t)$ is a monotone identity of all the induced automorphisms $\alpha_{\tilde{H}/\tilde{H}_i} : \tilde{H}/\tilde{H}_i \to \tilde{H}/\tilde{H}_i$.

**Proof.** Let us show that $\tilde{H}$ is invariant under $\alpha$ and $\alpha^{-1}$. Since $a_n \in \{1, -1\}$, we observe that $\alpha(\tilde{H}) \subseteq \langle \alpha^{-n+2}(H), \ldots, \alpha^{-1}(H), \alpha^n(H) \rangle \subseteq \langle \tilde{H}, \alpha^{n-1}(H), \ldots, \alpha(H), H \rangle \subseteq \tilde{H}$. Since $a_0 \in \{1, -1\}$, we similarly observe that $\alpha^{-1}(\tilde{H}) \subseteq \tilde{H}$. So $\tilde{H}$ is $(\alpha)$-invariant. By construction, we also have $d(\tilde{H}) \leq (2n - 1) \cdot d(H)$. Finally, we suppose that $G$, and therefore the subgroup $\tilde{H}$, is residually-finite. Let $\tilde{H} = N_1 \supseteq N_2 \supseteq \cdots$ be a normal series of finite-index subgroups with finite intersection. Since $\tilde{H}$ is finitely-generated, every subgroup $N_i$ contains the $\tilde{H}$-characteristic subgroup $\tilde{H}_i := \bigcap_{\beta \in \text{Aut}(\tilde{H})} \beta(N_i)$ of finite index in
\( \tilde{H} \) (the characteristic core). Since \( \bigcap_i \tilde{H}_i \subseteq \bigcap_i N_i = \{1\} \), we see that \( (\tilde{H}_i)_i \) is the desired series.

**Theorem 8.2.5.** Consider a residually-finite group \( G \) with a cyclotomic automorphism of index \( n > 1 \). Then every finitely-generated subgroup \( H \) of \( G \) is locally-nilpotent and

\[
c(H) \leq \max\{ (p - 1)^{(p-1)}, C(p \cdot d(H), p) \},
\]

where \( p \) is the largest prime dividing \( n \). If, moreover, \( n \) is not a natural power of \( p \), then \( H \) is nilpotent of class \( c(H) \leq (p - 1)^{(p-1)} \).

**Proof.** We need only combine proposition 8.2.3 with lemma 8.2.4.

This proves theorem 1.2.7. Since finitely-generated, nilpotent groups are known to be residually-finite, we have also obtained theorem 1.2.8. By requiring that our automorphism be almost-regular (in the sense that it fixes only finitely-many elements of the group), we obtain the related result:

**Proposition 8.2.6.** Consider a residually-finite group \( G \) with a cyclotomic automorphism of index \( n > 1 \) and let \( p \) be the largest prime dividing \( n \). Suppose that the automorphism is almost-regular. Then \( G \) is nilpotent and it has an \( \alpha \)-invariant subgroup \( N \) of finite index and of class \( c(N) \leq (p - 1)^{(p-1)} \).

**Proof.** Let \( \alpha : G \to G \) be the automorphism of the locally-nilpotent group \( G \). In view of lemma 8.2.1 and theorem 8.2.5, we may assume that \( n = p \). Since \( G \) is locally-nilpotent, we may consider the \( p \)-Sylow subgroup \( P \) of the torsion subgroup \( T \) of \( G \). This \( P \) is a characteristic subgroup of \( G \) such that the locally-nilpotent factor \( G/P \) has no \( p \)-torsion.

Let us first show that this \( P \) is finite. Since \( G \) is residually-finite, so is its subgroup \( P \). Since \( \alpha \) fixes only finitely-many elements of \( G \), we may select a finite-index subgroup \( M \) of \( P \) such that \( M \cap C_G(\alpha) = \{1_G\} \). After replacing \( M \) with the finite-index subgroup \( \bigcap_{0 \leq i \leq p - 1} \alpha^i(M) \) of \( P \), we may further assume that \( M \) is \( \alpha \)-invariant. So the restriction of \( \alpha \) to the locally-nilpotent \( p \)-group \( M \) is a regular, cyclotomic automorphism of index \( p \). But it is well-known that such a group \( M \) is trivial (cf. [23] and [35]). We conclude that \( P \) is indeed a finite group.

Since \( P \) is a finite \( p \)-group, \( P \) is nilpotent. Theorem 1.3.7 implies that also the quotient \( G/P \) is nilpotent. We see, in particular, that \( G \) is solvable, and therefore nilpotent (by Khukhro’s theorem of [28]).

Since \( P \) is a finite subset of the residually-finite group \( G \), we may select a subgroup \( N \) of finite index in \( G \) such that \( N \cap P = \{1_G\} \). After replacing \( N \) with \( \bigcap_{0 \leq i \leq p - 1} \alpha^i(N) \), may further suppose that it is \( \alpha \)-invariant. Since the nilpotent group \( N \) has no \( p \)-torsion, we may apply theorem 1.3.7 and conclude that \( c(N) \leq (p - 1)^{(p-1)} \).
8.2.2 Proof of corollaries 1.2.9 and 1.2.10

We had already mentioned in the introduction that cyclotomic automorphisms appear in the study of automorphisms with a finite Reidemeister-number. And, indeed:

Corollary 8.2.7 (Theorem A of Jabara [30]). Consider a residually-finite group $G$ admitting an automorphism $\alpha : G \rightarrow G$ of prime order $p$. If the Reidemeister-number of $\alpha$ is finite, then $G$ has an $\alpha$-invariant subgroup $N$ of finite index that is nilpotent of class $c(N) \leq (p-1)^2(p-1)$.

Proof. It is easy to show that $G$ has an $\langle \alpha \rangle$-invariant, finite-index subgroup $M$ such that the induced automorphism $\alpha_M : M \rightarrow M$ is cyclotomic of index $p$ (cf. lemma 5 of [30]).

It is also easy to see that $\alpha_M$ is almost-regular (cf. lemma 1 and 4 of [30]). We then apply theorem 8.2.6 to this $M$ and the induced automorphism $\alpha_M$ in order to obtain the $\alpha$-invariant subgroup $N$ of finite index in $G$. □

Let $A : \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{N}$ be the map in J. Alperin’s theorem 1 of [1].

Corollary 8.2.8 (Theorem B of Jabara [30]). Consider a finitely-generated, solvable group $G$ with an automorphism $\alpha : G \rightarrow G$ of prime order $p$. If the Reidemeister-number $n$ of $\alpha$ is finite, then $G$ has a finite-index subgroup $N$ that is nilpotent of class $c(N) \leq (p-1)^2(p-1)$ and $dl(G) \leq 2^n + A(p,n) + (p-1)^2(p-1)$.

Proof. We re-consider Jabara’s proof of theorem $B$ in [30] and we replace theorem $A$ of [30] with corollary 8.2.7. This way, we obtain the subgroup $N$ without relying on the classification. By assumption, $G$ is finitely-generated. So, after replacing $N$ with $\bigcap_{\beta \in \text{Aut}(G)} \beta(N)$, we may further assume that $N$ is characteristic in $G$. Then the induced automorphism $\alpha_{G/N} : G/N \rightarrow G/N$ on the finite, solvable group $G/N$ fixes at most $2^n$ elements (cf. lemma 1 and 4 of [30]) and its order divides $p$. If $\alpha_{G/N}$ has order 1, then $|G/N| \leq 2^n$. Else, we may apply Alperin’s theorem 1 of [1] to $G/N$ and $\alpha_{G/N}$ in order to conclude that $dl(G/N) \leq A(p,n,m)$. Since $dl(G) \leq dl(G/N) + dl(N)$, we are done. □

8.3 Anosov polynomials

We recall that a monic polynomial $r(t) \in \mathbb{Z}[t]$ is said to be Anosov if and only if $r(0) = \pm 1$ and $r(t)$ has no roots of modulus one. Such polynomials naturally appear in the study of Anosov-diffeomorphisms on compact manifolds (e.g. [10, 13, 47]) and we recall one such situation in particular:

Theorem 8.3.1 (Manning – [43]). A nil-manifold $M$ admits an Anosov diffeomorphism if and only if the fundamental group $\pi_1(M)$ of $M$ admits an automorphism $\alpha : \pi_1(M) \rightarrow \pi_1(M)$ with an Anosov identity.

In fact: every known example of an Anosov-diffeomorphism on a compact manifold is topologically-conjugated to an infra-nil-manifold endomorphism (cf. [11]) and it is conjectured that there are no other examples (cf. Smale’s problem 3.5 in [58]). So it makes sense
to ask which (fundamental) groups admit an automorphism with an Anosov identity and one might be tempted to conjecture:

**Problem 8.3.2.** A finitely-generated, residually-finite group is virtually-nilpotent if it admits an automorphism with an Anosov identity.

We have not been able to give a positive answer in the most general case, but we can prove it for a large family of examples.

**Proposition 8.3.3.** Consider a finitely-generated group $G$, together with an automorphism admitting an Anosov identity $r(t)$. If $G$ has a $p$-congruence system such that $\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t)) \not\equiv 0 \mod p$, then $G$ is virtually-nilpotent.

Here we do not assume that the $p$-congruence system comes with a bound. So we use the terminology of definition B.1 in [14], rather than the original terminology of Lubotzky in [41].

**Proof.** After replacing $G$ with an appropriate characteristic subgroup of finite index, we may assume that $G$ is finitely-generated and residually-(a finite $p$-group). Let us consider the Zassenhaus series $(\Delta_i(G,p))_{i \in \mathbb{N}}$ of $G$ with respect to the prime $p$. Since $\bigcap_i \Delta_i(G,p) = \{1_G\}$, we need only show that each factor $G/\Delta_i(G,p)$ is nilpotent of class at most $d^2$, where $d$ is the degree of $r(t)$. Let $\alpha : G \longrightarrow G$ be the automorphism. Since the series is characteristic, we obtain the induced automorphism $\alpha_{G/\Delta_i(G,p)} : G/\Delta_i(G,p) \longrightarrow G/\Delta_i(G,p)$ with identity $r(t)$. Since $G/\Delta_i(G,p)$ is a finite $p$-group and since the roots of an Anosov-polynomial form an arithmetically-free subset of $(\mathbb{Q}^\times, \cdot)$, we may apply theorem 1.3.7 in order to conclude that $c(G/\Delta_i(G,p)) \leq d^2$. This finishes the proof. 

We recall that the invariants $\text{Discr}_*(r(t))$ and $\text{Prod}(r(t))$ of a polynomial $r(t)$ are easy to compute with the methods of section 6. We refer to Table 1 for some examples that have been studied in the literature.

**Corollary 8.3.4.** Consider a finitely-generated group $G$ with an automorphism $\alpha : G \longrightarrow G$ admitting an Anosov identity $r(t)$. If $G$ is linear in characteristic zero, then $G$ is virtually-nilpotent.

**Proof.** Platonov’s theorem [48] tells us that, for almost-all primes $p$, the group $G$ has a $p$-congruence system. On the other hand, we saw in lemma 6.4.1 and lemma 6.4.3 that only finitely-many primes divide $\text{Discr}_*(r(t)) \cdot \text{Prod}(r(t))$. So almost-all primes $p$ satisfy the conditions of proposition 8.3.3.

**8.4 Split polynomials (fail)**

In this final subsection, we show how our methods must fail for an important family of polynomials. According to theorem 1.1.2, a finite group is nilpotent if it admits a regular automorphism of prime order. Theorem 1.1.3 even provides an upper bound on the class
Table 1: Invariants of Anosov polynomials in Table 1 of [47].

| $r(t)$                              | $\text{Discr}_s(r(t))$ | $\text{Prod}(r(t))$ |
|--------------------------------------|-------------------------|---------------------|
| $t^2 - t - 1$                        | $-5$                    | $-2^2$              |
| $t^3 - 3t - 1$                       | $-3^4$                  | $2^3 \cdot 3^9$    |
| $t^3 - t - 1$                        | $23$                    | $-2^3$              |
| $t^4 + t^3 - 4t^2 - 4t + 1$          | $3^2 \cdot 5^3$        | $-2^4 \cdot 5^{19}$|
| $t^4 + 3t^2 + 1$                     | $2^4 \cdot 5^2$        | $2^8 \cdot 5^{16}$ |
| $t^4 - t^3 - t^2 + t + 1$            | $3^2 \cdot 13$         | $2^{12} \cdot 7$   |
| $t^4 + 2t^3 + 3t^2 - 3t + 1$        | $5^2 \cdot 13^2$       | $2^{20} \cdot 5^8 \cdot 239^2$ |
| $t^4 - t - 1$                        | $-283$                  | $-2^4$              |
| $t^5 + t^4 - 4t^3 - 3t^2 + 3t + 1$  | $11^4$                  | $-2^5 \cdot 43^2 \cdot 67$ |
| $t^5 - t^3 - 2t^2 - 2t - 1$         | $47^2$                  | $-2^5 \cdot 5^9 \cdot 191^2$ |
| $t^5 + t^4 + 2t^3 + 4t^2 + t + 1$  | $2^4 \cdot 13^3$       | $-2^{25} \cdot 5^9 \cdot 13^3 \cdot 191$ |
| $t^5 - t - 1$                        | $19 \cdot 151$         | $-2^5$              |

of such a group. More generally, we have theorem 1.1.1, which states that a finite group $G$ is solvable if it admits a regular automorphism, say of order $n$.

**Open Problem 8.4.1.** Given a finite group $G$ with a regular automorphism of order $n$, find an upper bound on the derived length of $G$.

If $n$ is a prime, then theorem 1.1.3 provides the obvious bound $\text{dl}(G) \leq \log_2(c(G)) + 1 \leq \log_2((n - 1)2^{n-1}) + 1$ for the derived length $\text{dl}(G)$ of $G$. The combined work of Gorenstein—Herstein [18] and Kovac [36] further shows that $\text{dl}(G) \leq 3$ if $n = 4$. All other cases are still unresolved (cf. Example 8.4.6 below). But, by replacing the derived length of $G$ with a coarser invariant, we can obtain a meaningful answer.

**Theorem 8.4.2** (Hoffman [25], Gross [19], Khukhro [27]; Jabara [31]). Consider a finite group $G$ admitting a regular automorphism of order $n$, and let $l_n$ be the number of primes dividing $n$ (counted with multiplicity).

(i.) Then the Fitting-height of $G$ is at most $7 \cdot l_n^2$.

(ii.) More specifically: if $\gcd(|G|, n) = 1$, then the Fitting-height of $G$ is at most $l_n$.

Since the Fitting-height gives us a measure of how close a group is to being nilpotent, we see that theorem 8.4.2 refines theorem 1.1.1 and 1.1.4 in the spirit of Meta-Problem 1.1.8. We refer to [62] and [63] for more general results and to Shalev’s interesting note [55] for applications thereof. Moreover, it is known that the latter bound on the Fitting-height is best possible:
Example 8.4.3 (Gross [20]). Let \( n \) be a natural number and let \( p, q \) be two primes not dividing \( n \). Then there is a finite \( \{p, q\}\)-group \( G \) of Fitting-height \( l_n \) admitting a regular automorphism \( \alpha : G \rightarrow G \) of order \( n \).

Before using this example, we introduce some terminology.

Definition 8.4.4 (Split automorphisms). Let \( n \) be a natural number. Let us say that an automorphism \( \alpha : G \rightarrow G \) of a group \( G \) is split of index \( n \) if the split polynomial \( \Psi_n(t) := (t^n - 1)/(t - 1) = 1 + t + \cdots + t^{n-1} \) is a monotone identity of \( \alpha \): \( \Psi_n(\alpha) = 1_G \). Let us further say that an automorphism is split if it is split of some natural index \( n > 1 \).

Remark 8.4.5 (Cf. remarks 1 and 2 of [30]). (i) One can verify that, for every split automorphism of index \( n \) and for every \( x \in G \), we have the additional properties

\[
\alpha^n(x) = x \quad \text{and} \quad (x \cdot \alpha)^n = \mathbb{I}_{G \times \text{Aut}(G)}.
\]

For this reason, some authors also speak of “split automorphisms of order \( n \)” But this terminology is (slightly) misleading because the order of \( \alpha \) need only divide \( n \). For example: in every group of exponent \( n \), the automorphism \( x \mapsto x \) is split of index \( n \) but it has order 1. These examples are particularly relevant in the context of the (general, ordinary, restricted, and compact) Burnside problem. (ii) One can similarly verify that if a regular automorphism \( \alpha : G \rightarrow G \) of a finite group \( G \) satisfies \( \alpha^n = \mathbb{1}_G \), then that automorphism is also split of index \( n \). (iii) We conclude that, for a regular automorphism \( \alpha : G \rightarrow G \) of a finite group \( G \), the properties \( \alpha^n = \mathbb{1}_G \) and \( \Psi_n(\alpha) = 1_G \) are equivalent.

Let us now consider the non-nilpotent group \( G \) and the regular automorphism \( \alpha \) of Example 8.4.3. Since \( \alpha \) is regular of order \( n \), it is also a split automorphism of index \( n \). So theorem 1.2.3 must fail to prove the nilpotency of finite groups admitting a split automorphism of composite (and co-prime) index. The invariants of \( \Psi_n(t) \) further show how the theorem fails. On the one hand, we have \( \gcd(|G|, \Psi_n(1) \cdot \text{Discr}(\Psi_n(t)) \cdot \text{Prod}(\Psi_n(t))) = \gcd(|G|, (n) \cdot (n^{n-2}) \cdot (n^{n-1})) = 1 \). But, on the other hand, we (fortunately) have

\[
\text{Cong}(\Psi_n(t)) = \begin{cases} 0 & \text{if } n \text{ is composite}, \\ 1 & \text{else}. \end{cases}
\]

We conclude with a more positive observation related to problem 8.4.1. We had already mentioned that is not known whether the derived length of a finite group \( G \) can be bounded if it is known to admit a regular automorphism \( \alpha : G \rightarrow G \) satisfying \( \Psi_6(\alpha) = 1_G \). — even with the additional assumption \( \gcd(|G|, 6) = 1 \). Our methods have not been able to decide this either. But we do have the partial result:

Example 8.4.6. Let \( r(t) \) be a proper divisor of \( \Psi_6(t) = 1 + t + t^2 + t^3 + t^4 + t^5 \) in \( \mathbb{Z}[t] \) and suppose that a finite group \( G \) admits an automorphism \( \alpha : G \rightarrow G \) satisfying \( r(\alpha) = 1_G \). Then \( G \) has 6-torsion or \( [[G, G], G] = \{1_G\} \).

Proof. We suppose that \( \gcd(|G|, 6) = 1 \) and we will show that \( c(G) \leq 2 \). We first observe that \( \Psi_6(t) \) factors into irreducibles as \( \Psi_6(t) = \Phi_2(t) \cdot \Phi_3(t) \cdot \Phi_5(t) \). We may suppose that
\(r(t) \neq 1\), since otherwise \(G = \{x^1 | x \in G\} = \{1_G\}\), so that there is nothing to prove. If \(r(t) = \Phi_2(t) \cdot \Phi_6(t)\), then also \(\Phi_2(\alpha^3) = 1_G\). Similarly, if \(r(t) = \Phi_3(t) \cdot \Phi_6(t)\), then also \(\Phi_3(\alpha^2) = 1_G\). So, after replacing \(\alpha\) with a suitable power of \(\alpha\), we need only consider the cases in which \(r(t)\) is \(\Phi_2(t)\), \(\Phi_3(t)\), \(\Phi_6(t)\), or \(\Phi_2(t) \cdot \Phi_3(t)\). A simple computation (as explained in subsection 6.4) shows that, for such a polynomial \(r(t)\), we have \(\gcd(|G|, r(1) \cdot \cong(r(t)) \cdot \discr_*(r(t)) \cdot \prod(r(t))) = 1\):

| \(r(t)\) | \(r(1)\) | \(\cong(r(t))\) | \(\discr_*(r(t))\) | \(\prod(r(t))\) |
|-------|-------|-------------|----------------|----------------|
| \(\Phi_2(t)\) | 2     | 1           | 1              | 2              |
| \(\Phi_3(t)\) | 3     | 1           | 3              | \(3^2\)        |
| \(\Phi_6(t)\) | 1     | 1           | 3              | \(2^2\)        |
| \(\Phi_2(t) \cdot \Phi_3(t)\) | 2 \cdot 3 | 2 \cdot 3 | 3 | \(-2^1 \cdot 3^3\) |

So our main theorem 1.2.3 implies that \(G\) is nilpotent of class at most \(3^2 = 6561\). But, with a little more work, we can obtain a sharper bound. Let \(X\) be the set of roots of \(r(t)\) in \(\overline{\mathbb{Q}}^x\). Another simple computation (as explained in subsection 6.3) then shows that \(X\) is an arithmetically-free subset of \((\overline{\mathbb{Q}}^x, \cdot)\) with \(H(X, \overline{\mathbb{Q}}^x) \leq 2\):

| \(r(t)\) | \(\hat{r}(t_1, \ldots, t_d)\) | \(H(X, \overline{\mathbb{Q}}^x)\) |
|-------|-------------------|----------------|
| \(\Phi_2(t)\) | \(2 \cdot t_1\) | 1 |
| \(\Phi_3(t)\) | \(3^4 \cdot t_1^2 \cdot t_2^2\) | 2 |
| \(\Phi_6(t)\) | \(2^2 \cdot t_1^4 + 2 \cdot 3 \cdot t_1^3 \cdot t_2 + 3^2 \cdot t_1^2 \cdot t_2^2\) | 1 |
| \(\Phi_2(t) \cdot \Phi_3(t)\) | \(2^9 \cdot 3^7 \cdot t_1^2 \cdot (t_1 - t_2)^2 \cdot t_2^2 \cdot (t_1 + t_3)^3\) | 2 |

So we may use corollary 1.3.8 to conclude that \([[G, [G, G]]] = \{1_G\}\).

Acknowledgements. The author would like to thank Efim Zel’manov and Lance Small for their hosting (2013 – 2015) and their support during the first phase of the project at the University of California, San Diego. The author also thanks Jonas Deré (for helpful discussions about the construction of automorphisms in subsection 2.2 and Anosov-diffeomorphisms in subsection 8.3), Evgeny Khukhro (for his very valuable feedback on an earlier draft of this paper), Gerry Myerson (for providing references to the relevant results about reduced resultants that informed subsection 6.4), John Thompson (for allowing the re-use of his proof in subsection 3.2), and Bertram Wehrfritz (for his generous comments about the structure of linear groups in section 8). The author also thanks Harald Schwab (for his generous help with the project) and the “Geometry and Analysis on Groups” seminar at the University of Vienna.

References

[1] J. L. Alperin. Automorphisms of solvable groups. *Proc. Amer. Math. Soc.*, 13:175–180, 1962.
[2] J. L. Alperin. A classification of $n$-abelian groups. *Canad. J. Math.*, 21:1238–1244, 1969.

[3] Tom M. Apostol. Resultants of cyclotomic polynomials. *Proc. Amer. Math. Soc.*, 24:457–462, 1970.

[4] Reinhold Baer. Factorization of $n$-soluble and $n$-nilpotent groups. *Proc. Amer. Math. Soc.*, 4:15–26, 1953.

[5] J. A. Bahturin. *Lectures on Lie algebras*, volume 4 of *Studien zur Algebra und ihre Anwendungen [Studies in Algebra and its Applications]*. Akademie-Verlag, Berlin, 1978. Lectures given at Humboldt University, Berlin and Lomonosov University, Moscow.

[6] H. Bass. The degree of polynomial growth of finitely generated nilpotent groups. *Proc. London Math. Soc. (3)*, 25:603–614, 1972.

[7] Egle Bettio, Enrico Jabara, and Bertram A. F. Wehrfritz. Groups admitting an automorphism of prime order with finite centralizer. *Mediterr. J. Math.*, 11(1):1–12, 2014.

[8] Charles Ching-an Cheng, James H. McKay, and Stuart Sui Sheng Wang. Resultants of cyclotomic polynomials. *Proc. Amer. Math. Soc.*, 123(4):1053–1059, 1995.

[9] Christopher D. H. Cooper. Power automorphisms of a group. *Math. Z.*, 107:335–356, 1968.

[10] Karel Dekimpe. Hyperbolic automorphisms and Anosov diffeomorphisms on nilmanifolds. *Trans. Amer. Math. Soc.*, 353(7):2859–2877, 2001.

[11] Karel Dekimpe. What an infra-nilmanifold endomorphism really should be. . . . *Topol. Methods Nonlinear Anal.*, 40(1):111–136, 2012.

[12] Jonas Deré. Which infra-nilmanifolds admit an expanding map or an Anosov diffeomorphism? A study of the dynamical properties of self-maps on infra-nilmanifolds. *PhD. thesis: Katholieke Universiteit Leuven*, 2015.

[13] Jonas Deré. A new method for constructing Anosov Lie algebras. *Trans. Amer. Math. Soc.*, 368(2):1497–1516, 2016.

[14] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Second edition.

[15] Gregory Dresden. Resultants of cyclotomic polynomials. *Rocky Mountain J. Math.*, 42(5):1461–1469, 2012.

[16] Gérard Endimioni. Polycyclic group admitting an almost regular automorphism of prime order. *J. Algebra*, 323(11):3142–3146, 2010.

[17] Kıvanç Ersoy. Finite groups with a splitting automorphism of odd order. *Arch. Math. (Basel)*, 106(5):401–407, 2016.

[18] Daniel Gorenstein and I. N. Herstein. Finite groups admitting a fixed-point-free automorphism of order 4. *Amer. J. Math.*, 83:71–78, 1961.
[19] Fletcher Gross. Solvable groups admitting a fixed-point-free automorphism of prime power order. *Proc. Amer. Math. Soc.*, 17:1440–1446, 1966.

[20] Fletcher Gross. A note on fixed-point-free solvable operator groups. *Proc. Amer. Math. Soc.*, 19:1363–1365, 1968.

[21] Yves Guivarc’h. Croissance polynomiale et périodes des fonctions harmoniques. *Bull. Soc. Math. France*, 101:333–379, 1973.

[22] P. Hall and Graham Higman. On the $p$-length of $p$-soluble groups and reduction theorems for Burnside’s problem. *Proc. London Math. Soc. (3)*, 6:1–42, 1956.

[23] Graham Higman. Groups and rings having automorphisms without non-trivial fixed elements. *J. London Math. Soc.*, 32:321–334, 1957.

[24] Graham Higman. Lie ring methods in the theory of finite nilpotent groups. In *Proc. Internat. Congress Math. 1958*, pages 307–312. 1960.

[25] Frederick Hoffman. Nilpotent height of finite groups admitting fixed-point-free automorphisms. *Math. Z.*, 85:260–267, 1964.

[26] D. R. Hughes and J. G. Thompson. The $H$-problem and the structure of $H$-groups. *Pacific J. Math.*, 9:1097–1101, 1959.

[27] E. I. Huho. Finite groups that admit a 2-automorphism without fixed points. *Mat. Zametki*, 23(5):651–657, 1978.

[28] E. I. Huho. Nilpotency of solvable groups that admit a splitting automorphism of prime order. *Algebra i Logika*, 19(1):118–129, 133, 1980.

[29] Enrico Jabara. Polycyclic groups equipped with a uniform automorphism of order $pq$. *Rend. Circ. Mat. Palermo (2)*, 54(3):367–380, 2005.

[30] Enrico Jabara. Automorphisms with finite Reidemeister number in residually finite groups. *J. Algebra*, 320(10):3671–3679, 2008.

[31] Enrico Jabara. The Fitting length of finite soluble groups II: Fixed-point-free automorphisms. *J. Algebra*, 487:161–172, 2017.

[32] N. Jacobson. Restricted Lie algebras of characteristic $p$. *Trans. Amer. Math. Soc.*, 50:15–25, 1941.

[33] Otto H. Kegel. Die Nilpotenz der $H_p$-Gruppen. *Math. Z.*, 75:373–376, 1960/1961.

[34] E. I. Khukhro. Locally nilpotent groups that admit a splitting automorphism of prime order. *Mat. Sb. (N.S.)*, 130(172)(1):120–127, 128, 1986.

[35] Evgenii I. Khukhro. Nilpotent groups and their automorphisms, volume 8 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1993.

[36] L. G. Kovács. Groups with regular automorphisms of order four. *Math. Z.*, 75:277–294, 1960/1961.

[37] V. A. Kreknin. Solvability of Lie algebras with a regular automorphism of finite period. *Dokl. Akad. Nauk SSSR*, 150:467–469, 1963.
[38] V. A. Kreknin and A. I. Kostrikin. Lie algebras with regular automorphisms. Dokl. Akad. Nauk SSSR, 149:249–251, 1963.

[39] Michel Lazard. Groupes analytiques $p$-adiques. Inst. Hautes Études Sci. Publ. Math., (26):389–603, 1965.

[40] Emma T. Lehmer. A numerical function applied to cyclotomy. Bull. Amer. Math. Soc., 36(4):291–298, 1930.

[41] Alexander Lubotzky. A group theoretic characterization of linear groups. J. Algebra, 113(1):207–214, 1988.

[42] Avinoam Mann. The exponents of central factor and commutator groups. J. Group Theory, 10(4):435–436, 2007.

[43] Anthony Manning. Anosov diffeomorphisms on nilmanifolds. Proc. Amer. Math. Soc., 38:423–426, 1973.

[44] Wolfgang A. Moens. Arithmetically-free group-gradings of Lie algebras: I. 2016.

[45] Wolfgang Alexander Moens. Arithmetically-free group-gradings of Lie algebras: II. J. Algebra, 492:457–474, 2017.

[46] Gerald Myerson. On resultants. Proc. Amer. Math. Soc., 89(3):419–420, 1983.

[47] Tracy L. Payne. Anosov automorphisms of nilpotent Lie algebras. J. Mod. Dyn., 3(1):121–158, 2009.

[48] V. P. Platonov. A certain problem for finitely generated groups. Dokl. Akad. Nauk BSSR, 12:492–494, 1968.

[49] M. Pohst. A note on index divisors. In Computational number theory (Debrecen, 1989), pages 173–182. de Gruyter, Berlin, 1991.

[50] Peter Rowley. Finite groups admitting a fixed-point-free automorphism group. J. Algebra, 174(2):724–727, 1995.

[51] Eugene Schenkman and L. I. Wade. The mapping which takes each element of a group onto its n-th power. Amer. Math. Monthly, 65:33–34, 1958.

[52] A. Shalev and E. I. Zelmanov. Pro-p groups of finite coclass. Math. Proc. Cambridge Philos. Soc., 111(3):417–421, 1992.

[53] Aner Shalev. Automorphisms of finite groups of bounded rank. Israel J. Math., 82(1-3):395–404, 1993.

[54] Aner Shalev. The structure of finite $p$-groups: effective proof of the coclass conjectures. Invent. Math., 115(2):315–345, 1994.

[55] Aner Shalev. Centralizers in residually finite torsion groups. Proc. Amer. Math. Soc., 126(12):3495–3499, 1998.

[56] Aner Shalev. Lie methods in the theory of pro-p groups. In New horizons in pro-p groups, volume 184 of Progr. Math., pages 1–54. Birkhäuser Boston, Boston, MA, 2000.
[57] Pavel Shumyatsky. Applications of Lie ring methods to group theory. In Nonassociative algebra and its applications (São Paulo, 1998), volume 211 of Lecture Notes in Pure and Appl. Math., pages 373–395. Dekker, New York, 2000.
[58] S. Smale. Differentiable dynamical systems. Bull. Amer. Math. Soc., 73:747–817, 1967.
[59] Xavier Taixés i Ventosa and Gabor Wiese. Computing congruences of modular forms and Galois representations modulo prime powers. In Arithmetic, geometry, cryptography and coding theory 2009, volume 521 of Contemp. Math., pages 145–166. Amer. Math. Soc., Providence, RI, 2010.
[60] John Thompson. Finite groups with fixed-point-free automorphisms of prime order. Proc. Nat. Acad. Sci. U.S.A., 45:578–581, 1959.
[61] John G. Thompson. Normal $p$-complements for finite groups. Math. Z, 72:332–354, 1959/1960.
[62] John G. Thompson. Automorphisms of solvable groups. J. Algebra, 1:259–267, 1964.
[63] Alexandre Turull. Fitting height of groups and of fixed points. J. Algebra, 86(2):555–566, 1984.
[64] John S. Wilson. On the structure of compact torsion groups. Monatsh. Math., 96(1):57–66, 1983.
[65] John S. Wilson and Efim I. Zel’manov. Identities for Lie algebras of pro-$p$ groups. J. Pure Appl. Algebra, 81(1):103–109, 1992.
[66] E. I. Zel’manov. Solution of the restricted Burnside problem for groups of odd exponent. Izv. Akad. Nauk SSSR Ser. Mat., 54(1):42–59, 221, 1990.
[67] E. I. Zel’manov. Solution of the restricted Burnside problem for 2-groups. Mat. Sb., 182(4):568–592, 1991.
[68] E. I. Zel’manov. On periodic compact groups. Israel J. Math., 77(1-2):83–95, 1992.
[69] E. I. Zel’manov. Lie ring methods in the theory of nilpotent groups. In Groups ’93 Galway/St. Andrews, Vol. 2, volume 212 of London Math. Soc. Lecture Note Ser., pages 567–585. Cambridge Univ. Press, Cambridge, 1995.
[70] Efim Zel’manov. Lie algebras and torsion groups with identity. J. Comb. Algebra, 1(3):289–340, 2017.