School of Mathematics, Statistics and Applied Mathematics
National University of Ireland, Galway

PhD thesis

Algorithms for Nilpotent Linear Groups

Tobias Rossmann

March 2011

Supervisors
Dane Flannery and Alla Detinko

Contents

Introduction

Irreducibility testing. By a **linear group** over a field K, we mean a subgroup G of the general linear group $\mathrm{GL}(V)$ of a finite-dimensional vector space V over K. Given G, one of the most fundamental computational tasks is to decide if G fixes a proper subspace U of V. We then say that G is **reducible**. If no such subspace exists and if $V \neq 0$, then G is **irreducible**. In addition to deciding irreducibility, if G is found to be reducible, then we want to construct an invariant subspace U as above. We refer to these combined tasks as **irreducibility testing** of G. We sometimes also use the term "constructive irreducibility testing" to emphasise the difference from the decision problem, which merely asks if G is irreducible or not.

The Meataxe. If the underlying field K is finite, then irreducibility of G can be tested effectively using the MEATAXE Las Vegas algorithm [39, §7.4]. Nowadays, the term "MEATAXE" usually refers to variations of the Holt-Rees extension [41] of Parker's original method [62]. The MEATAXE was originally developed as a tool for the construction of representations of finite (simple) groups. For example, it featured prominently in Norton's construction of the sporadic simple group J_4 [60]; see [64] for similar applications. Beyond the successes of the MEATAXE in the construction of representations, it became a starting point and major ingredient of the "Matrix Group Recognition Project" which is concerned with the development of algorithms for linear groups over finite fields; see [61] for a survey of achievements.

Related work: irreducibility testing over infinite fields. For an infinite ground field K, the basic techniques underpinning the MEATAXE may still be applied but they will in general not succeed to decide irreducibility of G [37]. Possible applications of MEATAXE techniques in characteristic zero have been investigated by Parker [63], Holt [37, §3], and Glasby [35]. Using a different approach, Plesken and Souvignier [67] developed tools for irreducibility testing over the rationals that can be applied in some special cases. In short, so far, most of the work on irreducibility testing over infinite fields has been aimed at providing practical tools that may or may not be applicable in specific situations.

Regarding more systematic approaches, progress has recently been made on irreducibility testing of finite linear groups over fields of characteristic zero. Nebe and Steel [58] obtained a practical algorithm for deciding irreducibility of a finite linear group over the rationals. Their method is based on computations in algebras. An

This work is supported by the Research Frontiers Programme of Science Foundation Ireland, grant 08/RFP/MTH1331.

algorithm for irreducibility testing of finite linear groups over the rationals based on their approach has been included in MAGMA V2.16 [7]. We finally note that Souvignier [83] developed heuristics for finding invariant subspaces for reducible finite linear groups over the rationals based on techniques surrounding the Nebe-Steel-algorithm.

Related work: computing with nilpotent linear groups. Nilpotent linear groups have already been shown to be well-suited for computations [21, 22]. We note that nilpotency and finiteness of linear groups can be tested effectively over many fields, including number fields and rational function fields over these [21, 22]. For a recent survey of algorithms for linear groups over infinite domains, see [18]. In [21], Detinko and Flannery developed an algorithm which simultaneously tests irreducibility and primitivity (see below for a definition) of nilpotent linear groups over finite fields. Their work has been the starting point of the results described in this thesis.

Results: irreducibility testing. One of the main contributions of this thesis is an algorithm for constructive irreducibility testing of arbitrary finite nilpotent linear groups defined over a range of fields of characteristic zero, including number fields and rational function fields over number fields. A description of this algorithm has been previously published in [74]. An implementation is publicly available in the MAGMA package *finn* [76]. Since MAGMA V2.17, most of the functionality provided by *finn* has been included in MAGMA itself.

In addition to the above, in this thesis, we also develop an algorithm for deciding (non-constructively, in general) irreducibility of infinite finitely generated nilpotent linear groups over number fields.

Primitivity testing. Let $G \leqslant \mathrm{GL}(V)$ be an irreducible linear group over a field K. If there exists a non-trivial decomposition $V = U_1 \oplus \cdots \oplus U_r$ of vector spaces such that G permutes the U_i, then G is **imprimitive**; otherwise, G is **primitive**. A common strategy in the theory of linear groups is to first reduce problems to irreducible and then to primitive groups. Given an irreducible group G, consider the task of algorithmically deciding whether G is primitive. Similar to the case of irreducibility testing above, if G is found to be imprimitive, then we also want to construct a decomposition $V = U_1 \oplus \cdots \oplus U_r$ which is permuted by G. We refer to these combined tasks as (constructive) **primitivity testing** of G.

Results: primitivity testing. Our algorithm for irreducibility testing of a finite nilpotent linear group G is largely based on elementary group theory. As a consequence, it also provides us with insight into the structure of G. By exploiting this, we obtain an algorithm for constructive primitivity testing of irreducible finite nilpotent linear groups over the same family of fields as above. This research has been described in [75]; an implementation is again available in *finn* and included in recent versions of MAGMA. We note that while primitivity of linear groups over

finite fields can be tested using a method of Holt et al. [40], the author is not aware of any other work on primitivity testing over infinite fields.

Other results. In addition to the development of the algorithms outlined above, this thesis also contains purely theoretical structural results. Most importantly, as a by-product of our computational work, we investigate the structure of primitive finite nilpotent linear groups over number fields. In particular, in the case of a cyclotomic ground field K, we determine an explicit class $\mathfrak{G}$ of pairwise non-isomorphic abstract finite nilpotent groups such that:

(i) For each $G \in \mathfrak{G}$, there is a primitive linear group $G(K)$ over K with $G \cong G(K)$.

(ii) If H is a primitive finite nilpotent linear group over K, then there exists a unique $G \in \mathfrak{G}$ such that H and $G(K)$ are similar, i.e. represented by conjugate matrix groups over K.

Strategies for irreducibility and primitivity testing

We now sketch the strategies that underly our algorithms for irreducibility and primitivity testing; details will be provided in Parts I–II. To avoid technical issues, in this overview, we assume that K is a number field. As we indicated above, for irreducibility and primitivity testing of finite nilpotent linear groups, we can actually handle a considerably larger class of ground fields.

Let $G \leqslant \mathrm{GL}(V)$ be a finite nilpotent group, where $V \neq 0$ is a finite-dimensional vector space over K. We want to test irreducibility and (if G is found to be irreducible) primitivity of G. The case of abelian groups is easily treated, so we may assume that G is non-abelian. We then proceed using the following two steps. First, we can either construct a non-cyclic abelian normal subgroup of G or we can prove that no such subgroup exists. In the second step, we distinguish two cases:

(i) If we found a non-cyclic abelian normal subgroup of G, then G cannot be primitive (but it might be reducible). In this situation, we can either prove reducibility of G or we can construct a subgroup $H < G$ and a subspace $U < V$ such that G acts irreducibly on V if and only if H acts irreducibly on U. We then replace G by the image of H in $\mathrm{GL}(U)$ and V by U and start again.

(ii) If all the abelian normal subgroups of G are cyclic, then we can test irreducibility and primitivity of G directly. This step heavily depends on the known classification of abstract finite nilpotent groups all of whose abelian normal subgroups are cyclic.

The above strategy is due to Detinko and Flannery [21, §3] who employed a variation to test irreducibility and primitivity of nilpotent linear groups over finite fields [21, Alg. 7]. However, we use different methods to perform the tasks involved. For

instance, our method for locating non-cyclic abelian normal subgroups is considerably simpler, and it will succeed whenever such a subgroup exists. We also note that the case of characteristic zero often differs drastically from the corresponding situation over finite fields.

Now let $G \leqslant \mathrm{GL}(V)$ be a possibly infinite but finitely generated nilpotent group. Disregarding some easy special cases, we can use the following variation of the above strategy to decide irreducibility of G. We can either (a) construct an inhomogeneous abelian normal subgroup of G or (b) we can construct a maximal abelian normal subgroup of G which is homogeneous. (An abelian group $A \leqslant \mathrm{GL}(V)$ is called homogeneous if the K-algebra it generates is a field.) In case (a), we can proceed similar to case (i) from above, thus either proving reducibility of G or reducing to smaller dimension. In case (b), the K-algebra generated by G is in an explicit way a "crossed product" an we can use algorithms from computational number theory [31] and group cohomology [38] to decide irreducibility of G non-constructively.

Overview of the thesis

Part I: Computing with nilpotent linear groups

The first two chapters collect background material on linear groups (nilpotent and otherwise) and algebras. In Chapter 3, we consider congruence homomorphisms; the results given there are largely known from [22] but our approach is different. Our techniques for computing with abelian normal subgroups of nilpotent linear groups are described in Chapter 4. In Chapter 5, the first main result of this thesis is obtained, namely an algorithm for deciding irreducibility of nilpotent linear groups over number fields. The final Chapter 6 of Part I contains a structural analysis of a class of "exceptional groups" that we encountered in Chapter 5.

Part II: Irreducibility and primitivity testing of finite nilpotent linear groups

In Part II, we develop our algorithms for irreducibility and primitivity testing of finite nilpotent linear groups. This part is essentially a combined version of the papers [74, 75]. We first consider finite nilpotent groups all of whose abelian normal subgroups are cyclic (Chapter 7). Then we develop methods for irreducibility (Chapter 8) and primitivity testing (Chapter 10) for linear groups of this form. Between these two chapters, in Chapter 9, we study the equation $x^2 + y^2 = -1$ which arises naturally. Finally, in Chapter 11, we state our main algorithms and comment on our implementation in the MAGMA-package *finn*.

Part III: The structure of primitive finite nilpotent linear groups

In Chapter 12, we show that if G is a finite nilpotent group all of whose abelian normal subgroups are cyclic and if K is a number field, then there is an essentially

unique irreducible linear group $G(K)$ over K with $G \cong G(K)$. In particular, it follows that isomorphic primitive finite nilpotent linear groups over K are similar. After introducing some technical tools in Chapter 13, in the final Chapter 14, we investigate primitivity of $G(K)$ for fixed K and varying G.

Acknowledgements

First and foremost, I would like to express my gratitude to my supervisors Dane Flannery and Alla Detinko. Their helpful advice and constructive suggestions over the course of this project have been instrumental in making the thesis itself and the previously published parts possible. Furthermore, I am indebted to Bettina Eick for valuable comments and for various helpful discussions. I would also like to thank Eamonn O'Brien for MAGMA-related advice and for arranging the inclusion of my package *finn* into MAGMA. Many thanks are due to Heiko Dietrich for proofreading the thesis. I am grateful to Claus Fieker who kindly provided explanations of the algorithmic solution of norm equations and of his methods for computing with relative Brauer groups. Finally, I would like to thank Stephen Glasby for discussions on irreducibility testing.

Part I.

Computing with nilpotent linear groups

1. Basic facts on irreducibility and primitivity of linear groups

We recall some largely well-known facts on linear groups and algebras and establish notation. Unless otherwise indicated, throughout this thesis, let K be an arbitrary field and $V \neq 0$ be a finite-dimensional K-vector space. In computational settings, we tacitly assume that we are given algorithms for the basic field operations in K and for testing equality of elements of K.

1.1. Basics on rings, modules, and algebras

The results mentioned in this section are folklore; see [14, Ch. 4–5] or [53, §§28–29].

For us, rings are unital and ring homomorphisms preserve identities. In particular, if S is a subring of the ring R, then S contains the identity of R so that the inclusion $S \hookrightarrow R$ is a ring homomorphism.

Unless otherwise specified, when we speak of vector spaces we mean left vector spaces while modules refer to right modules. We denote the ring of endomorphisms of a module M by $\mathrm{End}(M)$. If $\mathcal{D}$ is a division ring, and W is a $\mathcal{D}$-vector space, then we regard W as a $(\mathcal{D}, \mathrm{End}(W))$-bimodule. Note that if $W \cong \mathcal{D}^e$ (the left $\mathcal{D}$-space of row vectors of length e over $\mathcal{D}$), then $\mathrm{End}(W) \cong \mathrm{M}_e(\mathcal{D})$ (the ring of $e \times e$ matrices over $\mathcal{D}$). Here, $\mathrm{M}_e(\mathcal{D})$ acts by right-multiplication on $\mathcal{D}^e$. We write $|W : \mathcal{D}|$ for the dimension of W over $\mathcal{D}$.

Let R be a ring and let M be an R-module. If $S \subset M$ is a not necessarily proper subset of M, then we write SR for the R-submodule of M generated by S. If M does not have any proper submodules and $M \neq 0$, then M is **irreducible**. If M is a direct sum of irreducible submodules, then M is **completely reducible**. By Schur's lemma, if M is irreducible, then $\mathrm{End}(M)$ is a division ring. Conversely, if M is completely reducible and $\mathrm{End}(M)$ is a division ring, then M is irreducible.

If $M = \sum_{i \in I} M_i$ for irreducible submodules $M_i \leqslant M$, then there exists $J \subset I$ such that $M = \bigoplus_{j \in J} M_j$; in particular, M is then completely reducible. If M is a direct sum of isomorphic irreducible R-modules, then M is **homogeneous**. Let M be completely reducible and let $(W_i)_{i \in I}$ be representatives of the isomorphism classes of irreducible submodules of M. Define U_i to be the sum of all submodules of M that are isomorphic to W_i. Then each U_i is a maximal homogeneous submodule called a **homogeneous component** of M and $M = \bigoplus_{i \in I} U_i$ is the **homogeneous decomposition** of M.

Let R be a ring. If R is completely reducible when regarded as a right R-module, then R is **semisimple**; this is equivalent to R being completely reducible as a left

R-module. Furthermore, R is semisimple if and only if every right R-module is completely reducible; again the same is true for left modules. If $R \neq 0$ and R does not have any non-trivial 2-sided ideals, then R is **simple**.

Let R be a ring and let K be a subring of R which is a field. Let $x \in R$ commute with all elements of K. We obtain a natural homomorphism $K[X] \to R, \sum_i a_i X^i \mapsto \sum_i a_i x^i$ ($a_i \in K$, almost all $a_i = 0$). If the kernel of this homomorphism is non-trivial, then it is generated by a unique monic polynomial $\mathrm{mpol}_K(x)$ called the **minimal polynomial** of x over K. Note that $\mathrm{mpol}_K(x)$ is defined if and only if the subring $K[x]$ of R generated by K and x is finite-dimensional over K.

By an **algebra** over a field K we mean a K-vector space $\mathcal{A}$ endowed with a K-bilinear multiplication which turns $\mathcal{A}$ into a ring. Unless explicitly stated otherwise, we write "algebra" for "finite-dimensional algebra". As rings, simple algebras are semisimple. If $\mathcal{A} \neq 0$, then we identify K with the central subalgebra $K \cdot 1_{\mathcal{A}}$ of $\mathcal{A}$, where $1_{\mathcal{A}}$ is the identity of $\mathcal{A}$. If $a_1, \ldots, a_r$ are commuting elements of $\mathcal{A}$, then we write $K[a_1, \ldots, a_r]$ for the subalgebra generated by these elements.

Let $\mathcal{A}$ be a K-algebra. The **radical** $\mathrm{rad}(\mathcal{A})$ of $\mathcal{A}$ is the intersection of all maximal right ideals of $\mathcal{A}$; again, "right" can be replaced by "left" here. The algebra $\mathcal{A}$ is semisimple if and only if $\mathrm{rad}(\mathcal{A}) = 0$. An alternative characterisation of $\mathrm{rad}(\mathcal{A})$ is as follows: $\mathrm{rad}(\mathcal{A})$ is the sum of all nilpotent ideals of $\mathcal{A}$ and $\mathrm{rad}(\mathcal{A})$ is itself a nilpotent ideal. If $\mathcal{A}$ is commutative, then $\mathrm{rad}(\mathcal{A})$ is the set of nilpotent elements in $\mathcal{A}$. In particular, subalgebras of semisimple commutative K-algebras are again semisimple.

1.2. Wedderburn theory

1.1 Proposition ([53, 29.F2])**.** *Let $\mathcal{A} \neq 0$ be a semisimple algebra. Then $\mathcal{A}$ is simple if and only if all irreducible $\mathcal{A}$-modules are isomorphic.*

While the following is well-known, the author has not been able to locate a reference for the exact version given here.

1.2 Proposition. *Let $\mathcal{A}$ be a subalgebra of* $\mathrm{End}(V)$.

(i) $\mathcal{A}$ is semisimple if and only if V is a completely reducible $\mathcal{A}$-module.

(ii) $\mathcal{A}$ is simple if and only if V is a homogeneous $\mathcal{A}$-module.

Proof. By [85, Thm 14.3], if V is a completely reducible (resp. irreducible) $\mathcal{A}$-module, then $\mathcal{A}$ is semisimple (resp. simple). If V is a homogeneous $\mathcal{A}$-module, then $\mathcal{A}$ acts faithfully on any irreducible $\mathcal{A}$-submodule U of V. We may then regard $\mathcal{A}$ as a subalgebra of $\mathrm{End}(U)$ so that $\mathcal{A}$ is simple. This concludes the proof of the "if" parts. The "only if" parts follow from the preceding proposition and the fact that modules of semisimple algebras are completely reducible. ♦

1.3 Theorem ([53, Thm 29.1])**.**

(i) Let $\mathcal{A}$ be a semisimple algebra. Then $\mathcal{A}$ has only finitely many minimal 2-sided ideals, say $\mathcal{A}_1, \ldots, \mathcal{A}_r$. Moreover, each $\mathcal{A}_i$ is a simple algebra, and $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$.

(ii) If $\mathcal{B}_1, \ldots, \mathcal{B}_s$ are simple K-algebras, then $\mathcal{B} = \mathcal{B}_1 \oplus \cdots \oplus \mathcal{B}_s$ is semisimple and the $\mathcal{B}_i$ are precisely the minimal 2-sided ideals of $\mathcal{B}$.

The ideals $\mathcal{A}_i$ in (i) are the **Wedderburn components** of $\mathcal{A}$ and $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$ is the **Wedderburn decomposition** of $\mathcal{A}$.

1.4 Proposition ([48, Thm XVII.4.3])**.** *Let $\mathcal{A} \neq 0$ be a semisimple algebra. Then the Wedderburn components of $\mathcal{A}$ are precisely the homogeneous components of $\mathcal{A}$ as a right $\mathcal{A}$-module.*

1.5 Proposition ([48, Thm XVII.4.4])**.** *Let $\mathcal{A}$ be a semisimple algebra and $V \neq 0$ be an $\mathcal{A}$-module. Let $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_r$ be the Wedderburn decomposition of $\mathcal{A}$. Then $V = V\mathcal{A}_1 \oplus \cdots \oplus V\mathcal{A}_r$ and each $V\mathcal{A}_i$ is the sum of all irreducible submodules of V that are isomorphic to an irreducible $\mathcal{A}$-submodule of $\mathcal{A}_i$. Hence, the homogeneous components of V are precisely those submodules $V\mathcal{A}_i$ which are non-zero.*

1.6 Corollary. *Let $\mathcal{A}$ be a semisimple subalgebra of $\mathrm{End}(V)$. Then the homogeneous components of V as an $\mathcal{A}$-module are $\mathrm{End}_{\mathcal{A}}(V)$-submodules of V.* ♦

1.7 Theorem (Wedderburn; [53, Thm 29.5])**.** *A K-algebra $\mathcal{A}$ is simple if and only if it is isomorphic to $\mathrm{M}_e(\mathcal{D})$ for some $e \geqslant 1$ and a K-division algebra $\mathcal{D}$. In this case, e is unique and $\mathcal{D}$ is unique up to isomorphism.*

The essentially unique irreducible module of a simple algebra $\mathrm{M}_e(\mathcal{D})$ as in Wedderburn's theorem is easily described.

1.8 Proposition. *Let $\mathcal{D}$ be a K-division algebra and $e \geqslant 1$. Then $\mathcal{D}^e$ is an irreducible $\mathrm{M}_e(\mathcal{D})$-module.*

Proof. We may naturally regard $\mathrm{M}_e(\mathcal{D})$ as the endomorphism ring of the left $\mathcal{D}$-vector space $\mathcal{D}^e$. Now apply [53, 28.F8]. ♦

Let $\mathcal{D}$ be a K-division algebra and $\mathcal{A} \cong \mathrm{M}_e(\mathcal{D})$. Then $|\mathcal{D} : \mathrm{Z}(\mathcal{D})| = m^2$ for an integer $m \geqslant 1$ (see [53, 29.F7]) called the **index** of $\mathcal{A}$; we write $\mathrm{index}(\mathcal{A}) = m$.

1.9 Corollary. *If $\mathcal{A}$ is a simple K-algebra, then the K-dimension of the irreducible $\mathcal{A}$-module is $\mathrm{index}(\mathcal{A}) \cdot \sqrt{|\mathcal{A} : K| \cdot |\mathrm{Z}(\mathcal{A}) : K|}$.* ♦

1.3. Irreducibility and primitivity of linear groups

Recall that by a **linear group** over K, we mean a subgroup G of the automorphism group $\mathrm{GL}(V)$ of a finite-dimensional vector space over K. The **degree** of G is the dimension $|V : K|$. The group G generates a subalgebra $K[G]$ of $\mathrm{End}(V)$ which we call the **enveloping algebra** of G. Note that $K[G]$ consists precisely of the K-linear

combinations of elements of G. We say that G is **completely reducible**, **homogeneous**, or **irreducible** according to whether V has the property in question as a $K[G]$-module. If G is completely reducible, then the **homogeneous decomposition** and the **homogeneous components** of G are understood accordingly. By Maschke's theorem (cf. [87, Cor. 1.6]), finite linear groups in characteristic zero are completely reducible.

If L/K is a finite field extension and $H \leqslant \mathrm{GL}(W)$ for a finite-dimensional L-space W, then by **restricting scalars**, we may naturally regard H as a K-linear group of degree $|W : K| = |W : L||L : K|$ (see [14, Prop. 7.1.2]). Since $K[H] \subset L[H]$, we see that if H is irreducible over K, then it is also irreducible over L.

A **system of imprimitivity** for $G \leqslant \mathrm{GL}(V)$ is a set $\mathcal{U} = \{U_1, \ldots, U_r\}$ of non-zero subspaces $U_i \leqslant V$ such that

(i) $V = U_1 \oplus \cdots \oplus U_r$, and

(ii) G permutes $\mathcal{U}$ in its natural action on subspaces.

We will usually exclude the trivial system of imprimitivity $\{V\}$. A non-trivial subspace $0 < U < V$ which belongs to some system of imprimitivity for G is called a **block** for G. A **block stabiliser** for G is a subgroup of the form $\mathrm{Stab}_G(U)$ for some block U for G. Suppose that G is irreducible. If G admits a non-trivial system of imprimitivity, then G is **imprimitive**; otherwise, G is **primitive**. Note that we only apply these notions to irreducible groups.

Two linear groups $G \leqslant \mathrm{GL}(V)$ and $H \leqslant \mathrm{GL}(W)$ over the same field K are **similar** if there exists a vector space isomorphism $V \xrightarrow{\theta} W$ such that $g \mapsto \theta^{-1} g \theta$ maps G onto H.

By identifying $\mathrm{GL}_d(K) = \mathrm{GL}(K^d)$ with respect to the standard basis of K^d, all of the preceding notions can be naturally rephrased in terms of a **matrix group** over K, i.e. a subgroup of some $\mathrm{GL}_d(K)$. In particular, $G \leqslant \mathrm{GL}_d(K)$ and $H \leqslant \mathrm{GL}_e(K)$ are similar if and only if $d = e$ and $H = x^{-1}Gx$ for some $x \in \mathrm{GL}_d(K)$.

1.4. Clifford's theorem

For our purposes, Clifford's theorem provides us with both completely reducible linear groups and systems of imprimitivity.

1.10 Theorem (Clifford)**.** *Let $G \leqslant \mathrm{GL}(V)$ be completely reducible and $N \lhd G$. Then N is completely reducible and the homogeneous components for N constitute a system of imprimitivity for G.*

Proof. See [68, 8.1.3] for a proof in the case that G is irreducible; the completely reducible case then follows immediately. ♦

The following can essentially be found in [73, p. 243].

1.11 Lemma. *Let $G \leqslant \mathrm{GL}(V)$ and let $\mathcal{U}$ be a system of imprimitivity for G. Suppose that each element of $\mathcal{U}$ is an $\mathrm{End}_{K[G]}(V)$-submodule of V. Let $U \in \mathcal{U}$ and $H = \mathrm{Stab}_G(U)$. If G acts transitively on $\mathcal{U}$, then the restriction map $\mathrm{End}_{K[G]}(V) \to \mathrm{End}_{K[H]}(U)$ is an isomorphism.*

Proof. Let T be a right transversal for H in G with $1 \in T$. Clearly, if $\phi \in \mathrm{End}_{K[G]}(V)$ vanishes on U, then it vanishes on each Ut $(t \in T)$ and hence on V. This proves injectivity. Conversely, given $\psi \in \mathrm{End}_{K[H]}(U)$ it is easily verified that the K-endomorphism ϕ of V defined by $(\sum_{t\in T} u_t t)\phi = \sum_{t\in T}(u_t\psi)t$ $(u_t \in U)$ centralises G; clearly ϕ restricts to ψ on U. ⧫

By Corollary 1.6, a system of imprimitivity for G obtained using Clifford's theorem satisfies the conditions in Lemma 1.11. The following result from [21] is one of the core ingredients of our methods for irreducibility testing; we include a proof since parts of it will appear in our algorithms.

1.12 Corollary ([21, Thm 3.1])**.** *Let $G \leqslant \mathrm{GL}(V)$ be completely reducible and $N \lhd G$. Let $V = U_1 \oplus \cdots \oplus U_r$ be the homogeneous decomposition of V as a $K[N]$-module. Then G is irreducible if and only if*

(i) G acts transitively on $\mathcal{U} = \{U_1, \ldots, U_r\}$, and

(ii) $\mathrm{Stab}_G(U_1)$ acts irreducibly on U_1.

Proof. If G acts intransitively on $\mathcal{U}$, then the direct sum over any orbit of G on $\mathcal{U}$ is a proper $K[G]$-submodule of V. Also, if $W < U_1$ is H-invariant, where $H = \mathrm{Stab}_G(U_1)$, then W generates a proper $K[G]$-submodule of V. Hence, conditions (i) and (ii) are necessary for G to be irreducible. Conversely, let (i) and (ii) be satisfied. By (ii) and Schur's lemma, $\mathrm{End}_{K[H]}(U_1)$ is a division ring. According to the last lemma, $\mathrm{End}_{K[G]}(V) \cong \mathrm{End}_{K[H]}(U_1)$, whence G is irreducible. ⧫

2. Completely reducible nilpotent linear groups

We collect fundamental facts regarding nilpotent linear groups; the results stated here can mostly be found in [85, 87, 25]. As before, unless otherwise noted, K is an arbitrary field and V is a non-trivial finite-dimensional vector space over K.

2.1. Semisimple, diagonalisable, and unipotent elements

For the following, see [87, §7] and [77, §7.A].

Let $\phi \in \mathrm{End}(V)$. We say that ϕ is **semisimple** if $K[\phi]$ is a semisimple algebra. By Proposition 1.2(i), ϕ is semisimple if and only if V is a completely reducible $K[\phi]$-module. By basic linear algebra, this is the case if and only if the minimal polynomial f of ϕ is square-free. Recall that ϕ is **diagonalisable**, i. e. represented by a diagonal matrix over some field extension of K, if and only if $\gcd(f, f') = 1$ (where f' is the formal derivative of f). In other words, ϕ is diagonalisable if and only if f remains square-free over every extension of K. Hence, if ϕ is diagonalisable, then it is semisimple. If K is perfect, then, conversely, a semisimple ϕ is diagonalisable.

If $\phi - 1$ is nilpotent, i. e. $(\phi - 1)^n = 0$ for some n, then ϕ is **unipotent**. A group $G \leqslant \mathrm{GL}(V)$ is **unipotent** if it consists entirely of unipotent elements. This is equivalent to the existence of a chain $0 = V_0 < \cdots < V_e = V$ of subspaces such that $[V_i, G] \leqslant V_{i-1}$ $(1 \leqslant i \leqslant e)$; here, for a subspace $U \leqslant V$, we write $[U, G]$ for the K-span of $\{u(g - 1) : u \in U, g \in G\}$. In other words, G is unipotent if and only if it acts nilpotently on V. It follows [42, Satz III.2.9] that G is then itself nilpotent. More concretely, let

$$\mathrm{UT}_d(K) = \begin{bmatrix} 1 & & & \\ K & 1 & & \\ \vdots & \ddots & \ddots & \\ K & \dots & K & 1 \end{bmatrix} \leqslant \mathrm{GL}_d(K)$$

be the group of **unitriangular** $d \times d$ matrices over K. This group is nilpotent of class $d - 1$ (see [68, p. 127]). A group $G \leqslant \mathrm{GL}(V)$ is unipotent if and only if, for a suitable basis of V, it can be represented by a subgroup of $\mathrm{UT}_d(K)$, where $d = |V : K|$; cf. [87, Cor. 1.21].

2.2. The Jordan decomposition

In this section, we have to assume that K is perfect.

2.1 Theorem ([87, p. 91])**.** *For any $g \in \mathrm{GL}(V)$, there exist unique elements $g_\mathrm{u}, g_\mathrm{s} \in \mathrm{GL}(V)$ such that*

(i) g_u *is unipotent,*

(ii) g_s *is semisimple, and*

(iii) $g = g_\mathrm{u}g_\mathrm{s} = g_\mathrm{s}g_\mathrm{u}$.

We note that g_u and g_s are polynomials in g; cf. [6, Lem. A.1]. The decomposition $g = g_\mathrm{u}g_\mathrm{s}$ is known as the (multiplicative) **Jordan decomposition** of g. It can be effectively computed provided that an algorithm for polynomial factorisation over K is available; an implementation is e.g. available in Magma. For $G \leqslant \mathrm{GL}(V)$, define subsets $G_\mathrm{u} = \{g_\mathrm{u} : g \in G\}$ and $G_\mathrm{s} = \{g_\mathrm{s} : g \in G\}$ of $\mathrm{GL}(V)$. The following is a special case of [81, 3.1.7].

2.2 Proposition. *Let $G \leqslant \mathrm{GL}(V)$ be locally nilpotent.*

(i) G_u *and* G_s *are subgroups of* $\mathrm{GL}(V)$.

(ii) $g \mapsto g_\mathrm{u}$ *(resp.* $g \mapsto g_\mathrm{s}$*) is an epimorphism of* G *onto* G_u *(resp.* G_s*).*

(iii) $[G_\mathrm{u}, G_\mathrm{s}] = 1$.

2.3. Reduction of irreducibility testing to completely reducible groups

Let K be perfect. We describe how, given a nilpotent group $G \leqslant \mathrm{GL}(V)$, we can either prove that G is completely reducible or we can construct a proper $K[G]$-submodule of G. The method described here is known from [22, §4.1]. The following is stated in [22, Lem. 4.5] for nilpotent linear groups.

2.3 Lemma. *Let $G \leqslant \mathrm{GL}(V)$ be locally nilpotent. Then G is completely reducible if and only if $G_\mathrm{u} = 1$.*

Proof. The "only if" part is [85, Cor. 29.1]. For the converse, by a theorem of Zassenhaus, a locally soluble linear group is soluble [85, Thm 19.9]. The "if" part then follows from [85, Thm 22.5]. ♦

Suppose that a nilpotent group $G = \langle g_1, \ldots, g_n \rangle \leqslant \mathrm{GL}(V)$ is given. Assuming that we can compute Jordan decompositions over K, in view of Proposition 2.2, we

may construct $G_{\mathrm{u}} = \langle (g_1)_{\mathrm{u}}, \ldots, (g_n)_{\mathrm{u}} \rangle$ and hence decide if G is completely reducible. If $G_{\mathrm{u}} \neq 1$, then

$$V^{G_{\mathrm{u}}} = \{x \in V : xg_{\mathrm{u}} = x \text{ for all } g \in G\} = \bigcap_{i=1}^{n} \mathrm{Ker}\,((g_i)_{\mathrm{u}} - 1)$$

is a proper $K[G]$-submodule of V (use Proposition 2.2(iii)).

2.4. Torsion in nilpotent linear groups

The following is fundamental for our work on infinite nilpotent linear groups.

2.4 Theorem ([25, Cor. 6.5])**.** *Let G be a completely reducible nilpotent linear group. Then $G/\mathrm{Z}(G)$ and $[G, G]$ are finite. More precisely, if c is the nilpotency class and d the degree of G, then $|G : \mathrm{Z}(G)| \leqslant C$ and $|G'| \leqslant C$, where $C = d^{(c+1)(d-1)}$.*

2.5 Lemma. *Let G be a completely reducible nilpotent linear group, $G \xrightarrow{\pi} H$ be a homomorphism with torsion-free kernel, and $A \leqslant G$. If A^{π} is abelian, then so is A.*

Proof. $[A, A] \leqslant \mathrm{Ker}(\pi) \cap [G, G] = 1$, since $[G, G]$ is finite by Theorem 2.4. ♦

2.6 Corollary. *Let G be a completely reducible nilpotent linear group.*

(i) ([22, Lem. 4.8].) *If $N \lhd G$ is torsion-free, then $N \leqslant \mathrm{Z}(G)$.*

(ii) If G is torsion-free, then it is abelian.

Proof. For (i), let $g \in G$ be arbitrary, π be the projection $G \to G/N$, and $A = \langle N, g \rangle$. Lemma 2.5 shows that g centralises N. Clearly, (ii) follows from (i). ♦

The following is well-known.

2.7 Proposition ([77, Cor. 1.10])**.** *Let G be a nilpotent group. Then the elements of finite order in G form a locally finite subgroup $\mathrm{T}(G)$ of G. If G is finitely generated, then $\mathrm{T}(G)$ is finite.*

We call $\mathrm{T}(G)$ the **torsion subgroup** of G.

2.8 Lemma. *Let G be a group, $1 = Z_0 \leqslant Z_1 = \mathrm{Z}(G) \leqslant \cdots$ be the upper central series of G, and $i \geqslant 1$.*

(i) ([68, 5.2.19]) *If $\mathrm{Z}(G)$ is torsion-free, then so is Z_i/Z_{i-1}.*

(ii) ([42, Satz III.2.13]) *If $\mathrm{Z}(G)$ has exponent dividing e, then so does Z_i/Z_{i-1}.*

2.9 Corollary. *A nilpotent group is torsion-free if and only if its centre is.* ♦

Recall that K is **formally real** if it admits an ordering compatible with the field operations. Equivalently, K is formally real if and only if -1 is not a sum of squares in K; we refer to [14, §8.8] for details on formally real fields.

2.10 Proposition. *Let K be formally real and let $G \leqslant \mathrm{GL}(V)$ be an irreducible nilpotent linear group of odd degree. Then G is abelian and $\mathrm{T}(G) \leqslant \langle -1 \rangle$.*

Proof. Let $T = \mathrm{T}(\mathrm{Z}(G))$. Since G is irreducible, $K[G]$ is simple. Hence, $F = K[T] \subset \mathrm{Z}(K[G])$ is a field. Since $|F : K|$ is finite, there exists a finitely generated (hence cyclic) subgroup $T_0 \leqslant T$ with $F = K[T_0]$. We may naturally regard V as an F-vector space. As $|V : K| = |V : F||F : K|$, we see that $|F : K|$ is odd. By [14, Lem. 8.8.6], F is then formally real. On the other hand, $F = K[T_0]$ is a cyclotomic extension of K. Since $\mathbf{Q}$ is the only formally real cyclotomic field, $F = K$ and $T \leqslant \langle -1 \rangle$.

Choose any ordering of K. By replacing G with $\langle G, -1 \rangle$, we may assume that $-1 \in G$. Since $|V : K|$ is odd, we then have $G = G^+ \times \langle -1 \rangle$, where $G^+ = \{g \in G \mid \det(g) > 0\}$. Note that $K[G] = K[G^+]$, so G^+ is irreducible. By applying what we have just proved to G^+ instead of G, we see that $\mathrm{Z}(G^+)$ is torsion-free. Hence, G^+ itself is torsion-free (Corollary 2.9) and therefore abelian (Corollary 2.6(ii)). It follows that G is abelian and $\mathrm{T}(G) = \mathrm{T}(G^+) \times \langle -1 \rangle = \langle -1 \rangle$. ♦

2.5. Sylow subgroups of the general linear group over Q

We recall known results on the Sylow p-subgroups of $\mathrm{GL}_d(\mathbf{Q})$. In later chapters, we will use these groups as a source of examples for testing our algorithms.

Let G be any group and p be a prime. Then a **Sylow p-subgroup** of G is a maximal p-subgroup of G. By Zorn's lemma, every p-subgroup of G is contained in a Sylow p-subgroup.

Let $\mathrm{W}_{p,1} = \mathrm{C}_p \leqslant \mathrm{GL}_{p-1}(\mathbf{Q})$ be generated by the companion matrix

$$\begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ -1 & \cdots & -1 & -1 \end{bmatrix}$$

of the pth cyclotomic polynomial. Let $\mathrm{W}_{p,k+1} = \mathrm{W}_{p,k} \wr \mathrm{C}_p \leqslant \mathrm{GL}_{(p-1)p^k}(\mathbf{Q})$.

2.11 Proposition.

(i) $\mathrm{W}_{p,k} \leqslant \mathrm{GL}_{(p-1)p^{k-1}}(\mathbf{Q})$ *is irreducible for all p.*

(ii) $\mathrm{W}_{2,k} \leqslant \mathrm{GL}_{2^{k-1}}(\mathbf{Q})$ *is absolutely irreducible.*

Proof. We have $\mathrm{W}_{p,k} = \mathrm{C}_p \wr P$ where P is the (transitive) Sylow p-subgroup of he symmetric group on p^{k-1} letters (cf. [68, 1.6.19]). Now apply [85, Lem. 15.4]. ♦

2.12 Theorem ([49, §4.5])**.**

(i) The Sylow p-subgroups of $\mathrm{GL}_d(\mathbf{Q})$ are finite and pairwise conjugate.

(ii) Let $d = a_0 + (p-1)(a_1 + a_2 p + \cdots + a_k p^{k-1})$ where $0 \leqslant a_0 < p-1$ and $0 \leqslant a_i < p$ for $1 \leqslant i \leqslant k$. Then the image of the natural embedding of $\prod_{i=1}^{k} \mathrm{W}_{p,i}^{\times a_i}$ into $\mathrm{GL}_d(\mathbf{Q})$ is a Sylow p-subgroup of $\mathrm{GL}_d(\mathbf{Q})$.

2.6. Bounds for the nilpotency class I: number fields

We write class(G) for the nilpotency class of a nilpotent group G.

2.13 Theorem ([88])**.**

(i) Let $G \leqslant \mathrm{GL}_d(\mathbf{Z})$ be nilpotent. If d is not a power of 2, then $\mathrm{class}(G) \leqslant d-1$*; otherwise,* $\mathrm{class}(G) \leqslant d$*. Moreover, the respective bound is attained for each d.*

(ii) Let $G \leqslant \mathrm{GL}_d(\mathbf{Q})$ be nilpotent. Then $\mathrm{class}(G) \leqslant 3d/2$*.*

A precise bound for the class of a nilpotent subgroup of $\mathrm{GL}_d(\mathbf{Q})$ can also be found in [88]. For our purposes, it suffices to notice that the nilpotency class of a nilpotent linear group over $\mathbf{Q}$ is bounded by a linear function of the degree. By restriction of scalars, this extends to number fields as follows.

2.14 Corollary. *Let K be a number field. Then a nilpotent subgroup of $\mathrm{GL}_d(K)$ has nilpotency class at most $3d|K:\mathbf{Q}|/2$.* ♦

3. Congruence homomorphisms

In this chapter, we introduce the classical notion of a congruence homomorphism. We describe how for finitely generated matrix groups over number fields and rational function fields in characteristic zero, congruence homomorphisms with torsion-free kernels can be obtained; cf. [22, §3]. We then study the effects of the previously constructed congruence homomorphisms on reducibility of a matrix group. Finally, we describe how congruence homomorphisms can be used to simplify the computation of minimal polynomials over rational function fields; we make use of this technique in our MAGMA package *finn*, to be described in §11.4.

Throughout this chapter, we assume that K is a field of characteristic zero.

3.1. Fundamentals on congruence homomorphisms

Basic definitions. Let $R \xrightarrow{\pi} S$ be a homomorphism of commutative rings. We obtain an induced group homomorphism $\mathrm{GL}_d(R) \xrightarrow{\pi_d} \mathrm{GL}_d(S)$. Let $\mathrm{CL}_d(\pi)$ be the kernel of π_d. For $G \leqslant \mathrm{GL}_d(R)$, we call $G_\pi = G \cap \mathrm{CL}_d(\pi)$ the **π-congruence subgroup** of G. By abuse of notation, we denote the restriction of π_d to G, which we call the **π-congruence homomorphism** of G, simply by π. The **π-congruence image** of G is G^π.

For the purposes of this thesis, the most important instance of a congruence homomorphism is the case that π is the projection $R \to R/\mathfrak{a}$ for some ideal $\mathfrak{a}$ of R. In this case, we also speak of $\mathfrak{a}$-congruence homomorphisms, $\mathfrak{a}$-congruence subgroups, etc. and write $\mathrm{CL}_d(R, \mathfrak{a})$ for the $\mathfrak{a}$-congruence subgroup of $\mathrm{GL}_d(R)$.

Torsion-free congruence subgroups. We are only interested in congruence homomorphisms with torsion-free kernels. Hence, for finite groups, these will be isomorphisms. Even for infinite nilpotent matrix groups, such congruence homomorphisms are related to group-theoretic properties, as has already been indicated in §2.4.

We will obtain torsion-free congruence subgroups using the following fundamental result. The special case $R = \mathbf{Z}$ was originally proved by Minkowski [57, §1].

3.1 Lemma (Suprunenko; [85, Thm 12.3])**.** *Let R be a* UFD *of characteristic zero. Let $p \in R$ be a prime element such that $p^2 \nmid q$ for all rational primes q and $p \nmid 2$. Then $\mathrm{CL}_d(R, pR)$ is torsion-free.*

Computing with congruence homomorphisms. Let the matrix group $G \leqslant \mathrm{GL}_d(K)$ be given by a finite generating set S as a *monoid*. Note that if the finite set T generates G as a group, then we may always take $S = T \cup T^{-1}$. Let E be the set

of all non-zero matrix entries in S. Then $\mathbf{Z}[E]$, the subring of K generated by E, is the smallest subring S of K such that $G \leqslant \mathrm{GL}_d(S)$.

Our main goal in this chapter is as follows: find a ring R with $\mathbf{Z}[E] \subset R \subset K$ and an epimorphism $R \xrightarrow{\pi} F$ onto a field F such that

(i) F is "nicer" (i.e. more amenable to computations) than K,

(ii) $\mathrm{CL}_d(\pi)$ is torsion-free, and

(iii) we may easily compute the restriction of π to $\mathbf{Z}[E]$.

An important example of a "nicer" ring in (i) would be a finite field; in practice, arithmetic over finite fields is considerably faster than over infinite fields.

Instead of working directly with $\mathbf{Z}[E]$, we introduce the larger ring $R \supset \mathbf{Z}[E]$ for theoretical reasons. For instance, $\mathbf{Z}[E]$ might not be a UFD, so that we cannot directly apply Lemma 3.1. Note that the group G, or more precisely, the given generating set of G, is only used to obtain the set E.

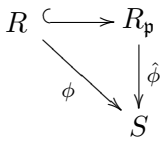
We will achieve the goals in (i)–(iii) for two major cases of K, namely number fields and rational function fields. Solutions for these two cases have already been obtained in [22, §3]. In the case of rational function fields (Section 3.4), the method we describe here coincides with that given in [22, Ex. 3.6]. However, we systematically use a different theoretical justification (namely, localisation at prime ideals).

3.2. Localisation

We now quickly describe the special case of localisation which we will require; see e.g. [56, §4] for background.

Let R be an integral domain with field of fractions F. For a prime ideal $\mathfrak{p}$ of R, define the **localisation** $R_\mathfrak{p}$ of R at $\mathfrak{p}$ by $R_\mathfrak{p} = \{a/b : a \in R, b \in R \setminus \mathfrak{p}\} \subset F$. Then $R_\mathfrak{p}$ is a subring of F and elements of R outside of $\mathfrak{p}$ are units of $R_\mathfrak{p}$.

The ring $R_\mathfrak{p}$ can be characterised by the following universal property: for any ring homomorphism $R \xrightarrow{\phi} S$ such that $a\phi$ is a unit of S for all $a \in R \setminus \mathfrak{p}$, there exists a unique ring homomorphism $R_\mathfrak{p} \xrightarrow{\hat{\phi}} S$ such that



commutes. Explicitly, $\hat{\phi}$ is given by $(a/b)\hat{\phi} = (a\phi)/(b\phi)$ for $a \in R$ and $b \in R \setminus \mathfrak{p}$.

The localisation $R_\mathfrak{p}$ is a **local ring**, meaning that it contains a unique maximal ideal, namely $\mathfrak{p}\,R_\mathfrak{p}$ (the ideal of $R_\mathfrak{p}$ generated by $\mathfrak{p}$). Hence, $R_\mathfrak{p}^\times = R_\mathfrak{p} \setminus \mathfrak{p}\,R_\mathfrak{p}$. The natural map $R/\mathfrak{p} \xrightarrow{\iota} R_\mathfrak{p}/\mathfrak{p}\,R_\mathfrak{p}$ is injective. We may thus naturally regard $R_\mathfrak{p}/\mathfrak{p}\,R_\mathfrak{p}$ as the field of fraction of $R/\mathfrak{p}$.

Suppose that $\mathfrak{p}$ is a maximal ideal of R. Then ι is an isomorphism and we thus obtain a natural epimorphism $R_\mathfrak{p} \xrightarrow{\psi} R/\mathfrak{p}$ with kernel $\mathfrak{p}\,R_\mathfrak{p}$. This map is the extension of the projection $R \xrightarrow{\pi} R/\mathfrak{p}$ to $R_\mathfrak{p}$ as constructed above. More generally, by a **reduction modulo** $\mathfrak{p}$ on $R_\mathfrak{p}$ we mean a ring epimorphism $R_\mathfrak{p} \to F$ with kernel $\mathfrak{p}\,R_\mathfrak{p}$. Such a map always restricts to an epimorphism $R \to F$ with kernel $\mathfrak{p}$.

3.3. Congruence homomorphisms for number fields

Throughout this section, let K be a number field and R be its ring of integers. We refer to [13, Ch. 3–4] and [59, Ch. I–II] for background.

Torsion-free congruence subgroups

3.2 Proposition. *Let p be an odd rational prime which is unramified in K. Let $\mathfrak{p} \lhd R$ be a prime ideal with $\mathfrak{p} \mid p$ and let $R_\mathfrak{p} \xrightarrow{\pi} R/\mathfrak{p}$ be the natural map. Then $\mathrm{CL}_d(\pi)$ is torsion-free.*

Proof. It is known that $R_\mathfrak{p}$ is the valuation ring of K with respect to the $\mathfrak{p}$-adic valuation; see [14, p. 369]. In particular, $R_\mathfrak{p}$ is a UFD. As p is unramified in K, we have $\mathfrak{p}\,R_\mathfrak{p} = pR_\mathfrak{p}$. Using the natural isomorphism $R/\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}\,R_\mathfrak{p}$, the claim now follows from Lemma 3.1; note that rational primes other than p are units in $R_\mathfrak{p}$. ♦

3.3 Remarks.

(i) It is well-known that the finitely many rational primes which ramify in K are precisely those dividing the discriminant $\mathrm{disc}(K/\mathbf{Q})$; see [13, Prop. 3.3.23].

(ii) Using a very different approach, Proposition 3.2 can also be obtained as a corollary to [26, Lem. 9].

(iii) Proposition 3.2 is not generally true for arbitrary rational primes p:

  (a) $-1 \in \mathrm{CL}_1(\mathbf{Z}, 2)$ is a torsion element; here $p = 2$.

  (b) Let $K = \mathbf{Q}(\zeta_3)$, where ζ_3 is a primitive third root of unity. Let R be the ring of integers of K. Then $3R = \mathfrak{p}^2$ for a prime ideal $\mathfrak{p}$ and $\zeta_3 \in \mathrm{CL}_1(R, \mathfrak{p})$; here $p = 3$ ramifies.

Computing with congruence homomorphisms

Setup. Throughout, we assume that $E \subset K^\times$ is a fixed finite set, as e.g. obtained from a matrix group as in §3.1. For almost all prime ideals $\mathfrak{p}$ of R, we then have $E \subset R_\mathfrak{p}$. We assume that K is given as a simple extension of $\mathbf{Q}$, say $K = \mathbf{Q}(\theta)$, where θ is integral. Let $f \in \mathbf{Z}[X]$ be the minimal polynomial of θ and $N = \mathrm{degree}(f)$.

We will now describe how, for suitably chosen $\mathfrak{p}$, we obtain a reduction $R_\mathfrak{p} \xrightarrow{\pi} F$ modulo $\mathfrak{p}$ that allows us to easily compute $a\pi$ for $a \in E$ and such that the induced congruence homomorphism has torsion-free kernel. The following is well-known.

3.4 Proposition (Cf. [59, Satz I.8.3])**.** *Let p be a rational prime which does not divide $|R : \mathbf{Z}[\theta]|$. Denote by $\bar{\cdot}$ the natural map $\mathbf{Z}[X] \to \mathbf{F}_p[X]$. Let $f_1, \dots, f_r \in \mathbf{Z}[X]$ be monic polynomials such that $\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r}$ is the factorisation of $\bar{f}$ into irreducibles. Define $\mathfrak{p}_i = pR + f_i(\theta)R$ $(1 \leqslant i \leqslant r)$.*

(i) $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct prime ideals of R and $pR = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

(ii) $X \mapsto \theta$ induces an isomorphism $\mathbf{F}_p[X]/(\bar{f}_i) \to R/\mathfrak{p}_i$.

(iii) The embedding $\mathbf{Z}[\theta] \hookrightarrow R$ induces an isomorphism $\mathbf{Z}[\theta]/(\mathbf{Z}[\theta] \cap \mathfrak{p}_i) \to R/\mathfrak{p}_i$.

Proof. See the proof of [59, Satz I.8.3] for (i) and (ii). Clearly, the inclusion $\mathbf{Z}[\theta] \hookrightarrow R$ induces an isomorphism $\mathbf{Z}[\theta]/(\mathbf{Z}[\theta] \cap \mathfrak{p}_i) \to (\mathbf{Z}[\theta] + \mathfrak{p}_i)/\mathfrak{p}_i$. Now $|R : \mathfrak{p}_i|$ is a power of p, while p does not divide $|R : \mathbf{Z}[\theta]|$. Hence, $\mathbf{Z}[\theta] + \mathfrak{p}_i = R$ and (iii) follows. ♦

Rationalities. Each non-zero $a \in K$ has a unique representation

$$a = \big(a_0 + a_1\theta + \cdots + a_{N-1}\theta^{N-1}\big) \,/\, \mathrm{den}(a),$$

where $a_0, \dots, a_{N-1}, \mathrm{den}(a) \in \mathbf{Z}$, the **denominator** $\mathrm{den}(a)$ of a is positive, and $\gcd\big(a_0, \dots, a_{N-1}, \mathrm{den}(a)\big) = 1$. Write $\mathrm{num}(a) = a\,\mathrm{den}(a)$ for the **numerator** of a. Note that, in general, all of these numbers depend on the choice of θ and that these definitions remain valid if θ is non-integral.

Choosing a good prime. Let p be an odd rational prime and suppose that p does not divide

(i) the discriminant $\mathrm{disc}(K/\mathbf{Q})$,

(ii) the index $|R : \mathbf{Z}[\theta]|$, or

(iii) any denominator $\mathrm{den}(a)$ for $a \in E$.

We note that by [12, Prop. 4.4.4(2)], the discriminant of f satisfies

$$\mathrm{disc}(f) = \mathrm{disc}(K/\mathbf{Q}) \cdot |R : \mathbf{Z}[\theta]|^2$$

so (i)–(ii) can be equivalently stated by requiring that p does not divide $\mathrm{disc}(f)$.

Computing reduction modulo $\mathfrak{p}$. Having chosen p as just explained, we now use the notation from Proposition 3.4. Since p is unramified in K, we have $pR = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Let $\mathfrak{p} = \mathfrak{p}_i$ for some i. Let F be a field of size p^k, where $k = \mathrm{degree}(\bar{f}_i)$, and let $x \in F$ be a root of $\bar{f}_i$; of course, $F \cong \mathbf{F}_p[X]/(\bar{f}_i)$.

From Proposition 3.4, we obtain an epimorphism $R \xrightarrow{\pi} F$ with kernel $\mathfrak{p}$ such that the restriction of π to $\mathbf{Z}[\theta]$ acts via

$$\left(\sum_{i=0}^{N-1} c_i\theta^i\right)\pi = \sum_{i=0}^{N-1} (c_i \bmod p)x^i$$

where $c_0, \ldots, c_{N-1} \in \mathbf{Z}$.

Let $R_\mathfrak{p} \xrightarrow{\hat{\pi}} F$ be the extension of π to $R_\mathfrak{p}$ as in §3.2. It follows from Proposition 3.2 that $\mathrm{CL}_d(\hat{\pi})$ is torsion-free. Let $a \in E$. Then $a\hat{\pi} = (\mathrm{num}(a)\pi)/(\mathrm{den}(a) \bmod p)$, where $\mathrm{num}(a)\pi$ can be computed as just explained since $\mathrm{num}(a) \in \mathbf{Z}[\theta]$.

3.4. Congruence homomorphisms for rational function fields

In this section, K is an arbitrary field of characteristic zero. A **rational function field** over K is a finitely generated purely transcendental extension of K with an explicitly given transcendence basis. Throughout, let $\mathbf{X}_r = (X_1, \ldots, X_r)$, where the X_i are algebraically independent over K.

Torsion-free congruence subgroups

Let $\alpha \in K^r$. The kernel $\mathfrak{m}(\alpha)$ of $K[\mathbf{X}_r] \to K, f \mapsto f(\alpha)$ is the ideal generated by $\{X_1 - \alpha_1, \ldots, X_r - \alpha_r\}$; cf. [65, p. 12]. Let

$$K_{[\alpha]} = K[\mathbf{X}_r]_{\mathfrak{m}(\alpha)} = \{f/g : f, g \in K[\mathbf{X}_r], g(\alpha) \neq 0\}.$$

By extension, we obtain an epimorphism $K_{[\alpha]} \xrightarrow{\mathrm{ev}_\alpha} K$ called **evaluation** (at α). Note that we may recover α from $K_{[\alpha]} \subset K(\mathbf{X}_r)$. We will use the notation $b(\alpha)$ for the image of $b \in K_{[\alpha]}$ under ev_α.

3.5 Proposition (Cf. [23, §2])**.** *Let K be any field of characteristic zero and $\alpha \in K^r$ be arbitrary. Then $\mathrm{CL}_d(\mathrm{ev}_\alpha)$ is torsion-free.*

Our proof of Proposition 3.5 below relies on the following technical lemma which we will use again in §3.5.

3.6 Lemma. *Let $\mathcal{E}$ be a class of homomorphisms of commutative rings which satisfies the following conditions.*

(E1) $(K_{[\alpha]} \xrightarrow{\mathrm{ev}_\alpha} K) \in \mathcal{E}$ *for all fields K of characteristic zero and all scalars $\alpha \in K$.*

(E2) Let $(R_1 \xrightarrow{\lambda} R_2) \in \mathcal{E}$, where R_i is an integral domain with field of fractions F_i. Suppose that R_i' is a subring of R_i which generates F_i as a field and that

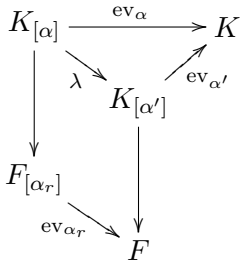
$$\begin{array}{ccc} R_1' & \hookrightarrow & R_1 \\ {\scriptstyle\lambda'}\downarrow & & \downarrow{\scriptstyle\lambda} \\ R_2' & \hookrightarrow & R_2 \end{array}$$

commutes. Then $\lambda' \in \mathcal{E}$.

(E3) If $(R_1 \xrightarrow{\lambda} R_2) \in \mathcal{E}$ and $(R_2 \xrightarrow{\mu} R_3) \in \mathcal{E}$, then $\lambda\mu \in \mathcal{E}$.

Then $(K_{[\alpha]} \xrightarrow{\mathrm{ev}_\alpha} K) \in \mathcal{E}$ for all fields K of characteristic zero, $r \geqslant 1$, and $\alpha \in K^r$.

Proof. We proceed by induction on r, the case $r = 1$ being covered by (E1). Let K and $\alpha \in K^r$ for $r > 1$ be given. Define $\alpha' = (\alpha_1, \ldots, \alpha_{r-1})$ and $F = K(\mathbf{X}_{r-1})$. We obtain a commutative diagram



where λ is induced by $K[\mathbf{X}_r] \to K[\mathbf{X}_{r-1}], f \mapsto f(X_1, \ldots, X_{r-1}, \alpha_r)$ and the vertical maps are inclusions. By induction, $\mathrm{ev}_{\alpha'}, \mathrm{ev}_{\alpha_r} \in \mathcal{E}$. Property (E2) yields $\lambda \in \mathcal{E}$, whence (E3) shows that $\mathrm{ev}_\alpha \in \mathcal{E}$. ⧫

Proof of Proposition 3.5. Let $\mathcal{E}$ be the class of homomorphisms $R \xrightarrow{\lambda} S$ of commutative rings such that $\mathrm{CL}_d(\lambda)$ is torsion-free. Clearly, conditions (E2)–(E3) in Lemma 3.6 are satisfied. It thus only remains to consider (E1). Let K be arbitrary of characteristic zero and $\alpha \in K$. Since $K[X]$ is a UFD, so is $K_{[\alpha]}$ [14, Thm 10.3.7]. The maximal ideal of $K_{[\alpha]}$ is generated by $X - \alpha$. As every rational prime is a unit of $K_{[\alpha]}$, we conclude from Lemma 3.1 that $\mathrm{CL}_d(K_{[\alpha]} \xrightarrow{\mathrm{ev}_\alpha} K)$ is torsion-free. ⧫

Computing with congruence homomorphisms

We now consider how computations with congruence homomorphisms for rational function fields can be performed in practice. Let $F = K(\mathbf{X}_r)$ and let $E \subset F^\times$ be finite. Suppose that we have found $\alpha \in K^r$ such that $E \subset K_{[\alpha]}$. We then say that α is **admissible** for E; cf. [23, §2]. Clearly, $e(\alpha)$ can then be readily computed for any $e \in E$. We may thus effectively compute the restriction of ev_α to $\mathbf{Z}[E]$ and hence the induced congruence homomorphism $\mathrm{GL}_d(\mathbf{Z}[E]) \to \mathrm{GL}_d(K)$ whose kernel is torsion-free by Proposition 3.5.

It remains to find an admissible α. We first argue why such a point exists. Let $E = \{e_1, \ldots, e_n\}$. Write $e_i = g_i/h_i$ for non-zero $g_i, h_i \in K[\mathbf{X}_r]$ with $\gcd(g_i, h_i) = 1$. Define f to be the product of the distinct irreducible factors of the h_i. Clearly, α is admissible for E if and only if $f(\alpha) \neq 0$. If f is scalar, then each $\alpha \in K^r$ is admissible for E, so let f be non-scalar. Elementary considerations (cf. [28, p. 32]) show that infinitely many $\alpha \in K^r$ are admissible for E. On the other hand, if $r > 1$, then there will in general also be infinitely many non-admissible points in K^r.

Geometrically speaking, the algebraic set $\mathrm{V}(f) = \{\omega \in K^r : f(\omega) = 0\}$ is a **thin subset** of K^r in the sense of Serre [80, §3]. In practice, points of $\mathrm{V}(f)$ are rarely encountered and we thus quickly obtain an admissible α by random choice.

3.5. Preservation of reducibility under congruence homomorphisms

In this section, we prove the following; the case $K = \mathbf{Q}$ in (i) is well-known [37, §3].

3.7 Proposition.

(i) Let K be a number field, R be its ring of integers, $\mathfrak{p} \neq 0$ be a prime ideal of R, and $R_\mathfrak{p} \xrightarrow{\pi} R/\mathfrak{p}$ be the natural map. If $G \leqslant \mathrm{GL}_d(R_\mathfrak{p})$ is reducible over K, then G^π is reducible over $R/\mathfrak{p}$.

(ii) Let K be any field of characteristic zero and let $\alpha \in K^r$. If $G \leqslant \mathrm{GL}_d(K_{[\alpha]})$ is reducible over $K(\mathbf{X}_r)$, then $G(\alpha)$ is reducible over K.

3.8 Remark. The converse statements of Proposition 3.7 are false, i.e. reducibility of a congruence image does *not* imply reducibility of the original group:

(i) The companion matrix of the 12th cyclotomic polynomial ϕ_{12} generates an irreducible subgroup of $\mathrm{GL}_4(\mathbf{Q})$ but ϕ_{12} splits over all finite fields [84, p. 219].

(ii) Let $G = \left\langle \left[\begin{smallmatrix} 0 & 1 \\ 1 & X \end{smallmatrix}\right] \right\rangle \leqslant \mathrm{GL}_2(\mathbf{Q}(X))$. Then G is irreducible and $G \leqslant \mathrm{GL}_2(\mathbf{Q}_{[0]})$. However, $G(0) = \left\langle \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \right\rangle \leqslant \mathrm{GL}_2(\mathbf{Q})$ is reducible.

We will prove Proposition 3.7 by reducing to the case of PIDs.

The Smith normal form. We refer to [10, §15] for details of the following. Let R be a PID and a be an $m \times n$ matrix over R. Let $r \leqslant \min(m, n)$ be the rank of a. Then there exist $s \in \mathrm{GL}_m(R)$, $t \in \mathrm{GL}_n(R)$ and a sequence $a_1, \ldots, a_r$ of non-zero elements of R such that

(i) $a_i \mid a_{i+1}$ for $1 \leqslant i < r$, and

(ii) we have

$$sat = \begin{bmatrix} \mathrm{diag}(a_1, \ldots, a_r) & . \\ . & . \end{bmatrix},$$

where the zero blocks have the appropriate sizes.

Furthermore, up to multiplication by units of R, the elements $a_1, \ldots, a_r$ are unique. The matrix sat is the **Smith normal form** of a.

Preservation of reducibility for PIDs. If $G \leqslant \mathrm{GL}(M)$, where M is a left module over a commutative ring R, then we may define $R[G]$ to be the R-subalgebra of $\mathrm{End}(M)$ generated by G; this extends the definition of the enveloping algebra of a linear group from §1.3. The following is a trivial generalisation of [85, Lem. 22.3] using the same proof.

3.9 Lemma. *Let R be a* PID*, V be a free left R-module of finite rank, and $G \leqslant \mathrm{GL}(V)$. Suppose that $M \leqslant V$ is an $R[G]$-submodule. Then there exists an $R[G]$-submodule $M \leqslant M' \leqslant V$ of the same rank as M such that M' is a direct summand of V as an R-module.*

Proof. By taking the Smith normal form of a matrix for the inclusion $M \hookrightarrow V$, we obtain a basis $(x_1, \ldots, x_d)$ of V and non-zero $a_1, \ldots, a_e \in R$ ($e \leqslant d$) such that $(a_1x_1, \ldots, a_ex_e)$ is a basis of M. Define $M' = \langle x_1, \ldots, x_e \rangle_R$. It only remains to show that M' is G-invariant. If $g \in G$, then $x_ig = \sum_{j=1}^{d} r_jx_j$ and $(a_ix_i)g = \sum_{j=1}^{e} s_jx_j$ ($r_j, s_j \in R$). Since $(a_ix_i)g = a_i(x_ig)$, we obtain $a_ir_j = 0$ (hence $r_j = 0$) for $j > e$. Therefore, $x_ig \in M'$. ♦

3.10 Proposition. *Let R be a* PID*, $\mathfrak{p}$ be a prime ideal of R, and $R \xrightarrow{\pi} R/\mathfrak{p}$ be the natural map. If $G \leqslant \mathrm{GL}_d(R)$ is reducible over the field of fractions of R, then G^π is reducible over the field of fractions of $R/\mathfrak{p}$.*

Proof. Let K be the field of fractions of R and $0 < U < K^d$ be a $K[G]$-submodule. By scaling the elements of a K-basis of U accordingly, we see that $M = U \cap R^d$ is an $R[G]$-submodule of R^d of rank $|U : K|$. Lemma 3.9 gives us an R-module decomposition $R^d = M' \oplus N$ where $M' \geqslant M$ is an $R[G]$-submodule of R^d of rank $|U : K|$. We may thus find $x \in \mathrm{GL}_d(R)$ such that $G^x = \left[\begin{smallmatrix} * & \vdots \\ * & * \end{smallmatrix}\right]$ where both diagonal blocks have degree > 0. Evidently, $(G^x)^\pi = (G^\pi)^{x\pi}$ is reducible. ♦

Proof of Proposition 3.7.

(i) This follows from Proposition 3.10 since $R_\mathfrak{p}$ is a PID.

(ii) For $r = 1$, the claim follows from Proposition 3.10, since $K_{[\alpha]}$, being a localisation of the PID $K[X]$, is itself a PID; cf. [56, Thm 4.1]. Now define a class $\mathcal{E}$ of ring homomorphisms as follows. Let $R_1 \xrightarrow{\lambda} R_2$ be any homomorphism between integral domains. Let F_i be the field of fractions of R_i. Then $\lambda \in \mathcal{E}$ if and only if G^λ is reducible over F_2 for every group $G \leqslant \mathrm{GL}_d(R_1)$ which is reducible over F_1. Clearly, conditions (E2)–(E3) in Lemma 3.6 are satisfied and we have just proved that (E1) holds too. ♦

3.6. Some facts on rational function fields

We collect some known results on rational function fields. Let K be an arbitrary field and let $\mathbf{X} = (X_1, \ldots, X_r)$ be algebraically independent over K. Everything in this section is to be understood to take place within some fixed algebraically closed extension Ω/K.

3.11 Proposition. *Let F/K be algebraic.*

(i) $\mathbf{X}$ is algebraically independent over F.

(ii) F and $K(\mathbf{X})$ are linearly disjoint.

(iii) $|F : K| = |F(\mathbf{X}) : K(\mathbf{X})|$.

Proof.

(i) See [71, Thm 3.3.4].

(ii) This follows from (i) and [48, Prop. VIII.3.3].

(iii) Write $L = K(\mathbf{X})$. Clearly, $FL = F(\mathbf{X})$. Let $(f_i)_{i\in I}$ be a K-basis of F. By (ii), $(f_i)_{i\in I}$ remains linearly independent over L. Since F/K is algebraic, FL is the L-span of F (see [71, p. 118]). Hence, FL is the L-span of $(f_i)_{i\in I}$ which is therefore an L-basis of FL. ⧫

3.12 Corollary. *Let f be an irreducible polynomial over K. Then f remains irreducible over $K(\mathbf{X})$.*

Proof. Let $\alpha \in \Omega$ be a root of f and define $F = K(\alpha)$. Then $F(\mathbf{X}) = K(\mathbf{X})(\alpha)$ and $|F(\mathbf{X}) : K(\mathbf{X})| = \text{degree}(f)$ shows that f remains irreducible over $K(\mathbf{X})$. ⧫

3.7. Minimal polynomials and evaluation

Let K have characteristic zero, $\mathbf{X} = (X_1, \ldots, X_r)$ be algebraically independent over K, and $\alpha \in K^r$.

3.13 Lemma. *Let $x \in \mathrm{M}_d(K(\mathbf{X}))$ and suppose that $f(x) = 0$ for some non-zero $f \in K[T]$. Then* $\mathrm{mpol}_{K(\mathbf{X})}(x) = \mathrm{mpol}_K(x)$.

Proof. We may assume that f is monic. Let $f = f_1 \cdots f_n$ be the factorisation into monic irreducibles over K. By Corollary 3.12, the f_i remain irreducible over $K(\mathbf{X})$. Since $g = \mathrm{mpol}_{K(\mathbf{X})}(x)$ divides f (in $K(\mathbf{X})[T]$) and since we have unique factorisation, we see that g is a product of some of the f_i. Hence, g has coefficients in K whence $g = \mathrm{mpol}_K(x)$. ⧫

It is known that a finite subgroup of $\mathrm{GL}_d(K(\mathbf{X}))$ is isomorphic to a subgroup of $\mathrm{GL}_d(K)$ [85, Cor. 12.4]. We can make the following stronger statement.

3.14 Proposition (Cf. [69, Lem. 2.2], [70])**.** *Let $G \leqslant \mathrm{GL}_d(K_{[\alpha]})$ be finite. Then there exists $t \in \mathrm{GL}_d(K(\mathbf{X}))$ such that $g(\alpha) = t^{-1}gt$ for all $g \in G$.*

Proof. Let $g \in G$ and $f = \mathrm{mpol}_{K(\mathbf{X})}(g) \in K(\mathbf{X})[T]$. Since g has finite order, n say, f divides $T^n - 1$. Lemma 3.13 shows that f has coefficients in K. Let $f = f_1 \cdots f_r$ be the factorisation into monic irreducibles over K (hence over $K(\mathbf{X})$, by Corollary 3.12). Then the characteristic polynomial h of g over $K(\mathbf{X})$ is of the form $h = \pm f_1^{e_1} \cdots f_r^{e_r}$ (see [48, Cor. XIV.3.6]). Hence, h has coefficients in K and therefore $\mathrm{trace}(g) \in K$.

Now for any $x \in \mathrm{M}_d(K_{[\alpha]})$, we have $\mathrm{trace}(x(\alpha)) = (\mathrm{trace}\, x)(\alpha)$. Thus, $\mathrm{trace}(g) = (\mathrm{trace}(g))(\alpha) = \mathrm{trace}(g(\alpha))$. By a well-known result from representation theory [68, 8.3.7], it follows that $G \to \mathrm{GL}_d(K(\mathbf{X})), g \mapsto g(\alpha)$ is equivalent to the natural representation $G \hookrightarrow \mathrm{GL}_d(K(\mathbf{X}))$ which proves the claim. ⧫

3.15 Remark. This gives another (and very quick) proof of Proposition 3.5.

3.16 Corollary. *Let $G \leqslant \mathrm{GL}_d(K_{[\alpha]})$ be a finite group and let $x \in K[G]$. Then we have $\mathrm{mpol}_{K(\mathbf{X})}(x) = \mathrm{mpol}_K(x(\alpha))$.*

Proof. Let t be as in Proposition 3.14. Then $x(\alpha) = t^{-1}xt$ is similar to x over $K(\mathbf{X})$. The result now follows from Lemma 3.13. ♦

In the next chapter, we will describe a method for computing the homogeneous decomposition for a finite abelian linear group (Algorithm 4.3). Our method will rely on the computation and factorisation of the minimal polynomial of group elements and their differences (as linear maps). For a base field of the form $K(\mathbf{X})$, we may thus perform these computations over K instead of $K(\mathbf{X})$; this contributes noticeably to the practical performance of our algorithm.

3.8. Bounds for the nilpotency class II: rational function fields

The following illustrates the use of results from Chapters 2–3; it can be regarded as a slight generalisation of [22, Lem. 4.13] in characteristic zero. As above, we write $\mathbf{X} = (X_1, \ldots, X_r)$.

3.17 Proposition. *Let K be a field of characteristic zero. Suppose that nilpotent subgroups of $\mathrm{GL}_d(K)$ have nilpotency class at most $C(d)$. Then nilpotent subgroups of $\mathrm{GL}_d(K(\mathbf{X}))$ have nilpotency class at most $C(d)+1$.*

Proof. Let $G \leqslant \mathrm{GL}_d(K(\mathbf{X}))$ be nilpotent. By Proposition 2.2, $G \leqslant G_\mathrm{u} \times G_\mathrm{s}$, where both factors are nilpotent of class at most $\mathrm{class}(G)$. It thus suffices to establish the given bound for the nilpotency class of G_u and G_s, respectively.

Now G_u is conjugate to a subgroup of $\mathrm{UT}_d(K(\mathbf{X}))$. Since $\mathrm{UT}_d(F)$ has class $d-1$ for any field F (cf. [68, p. 127]), we obtain $\mathrm{class}(G_\mathrm{u}) \leqslant d-1 \leqslant C(d)$.

Let $c = \mathrm{class}(G_\mathrm{s})$. Choose a finitely generated subgroup $H \leqslant G_\mathrm{s}$ with $\mathrm{class}(H) = c$; we may e.g. take $H = \langle x_1, \ldots, x_c \rangle$, where $x_i \in G_\mathrm{s}$ with $[x_1, \ldots, x_c] \neq 1$. As explained in §3.4, since H is finitely generated, there exists $\alpha \in K^r$ with $H \leqslant \mathrm{GL}_d(K_{[\alpha]})$. We then have $\mathrm{class}(H(\alpha)) \leqslant C(d)$. By Proposition 3.5, the congruence subgroup $\mathrm{CL}_d(\mathrm{ev}_\alpha)$ is torsion-free. Since H consists entirely of semisimple elements, it is completely reducible by Lemma 2.3. Corollary 2.6(i) now yields $H \cap \mathrm{CL}_d(\mathrm{ev}_\alpha) \leqslant \mathrm{Z}(H)$ and thus $c \leqslant C(d)+1$. ♦

By combining this with Corollary 2.14, we see that the nilpotency class of a nilpotent linear group over a rational function field over a number field is bounded by a linear function of the degree; cf. [22, Ex. 4.14].

4. Computing with abelian normal subgroups

In this chapter, let K be a field of characteristic zero such that we can algorithmically factorise polynomials over K into irreducibles. This assumption is satisfied for algebraic number fields and for rational function fields over these [86].

In §4.1, we consider the problem of constructing the homogeneous decomposition of a completely reducible abelian linear group over K. We recall a known Las Vegas algorithm[1] for this purpose and describe a second algorithm which is specific to *finite* abelian linear groups.

The rest of this chapter is then devoted to the following computational problem. Suppose that a completely reducible, non-abelian, nilpotent group $G \leqslant \mathrm{GL}(V)$ is given by finitely many generators. In the case that K is a number field or a rational function field over a number field, we describe how we may perform one of the following tasks:

(A1) Construct an inhomogeneous abelian normal subgroup of G.

(A2) Construct a homogeneous maximal abelian normal subgroup of G.

In the case of number fields, we will see in the next chapter that either outcome allows us to proceed further with deciding irreducibility of G. For *finite* nilpotent linear groups, we will later improve and extend the methods developed here in Part II.

4.1. Computing the homogeneous decomposition

Recall from §2.3 that we can test complete reducibility of abelian linear groups over K. In this section, we consider the problem of constructing the homogeneous decomposition of the natural module of a completely reducible abelian linear group over K. The first method we present is an already known Las Vegas algorithm. The second approach we describe is specifically designed for finite abelian linear groups (and cannot be successfully applied to infinite groups). It has the advantage of a potentially smaller memory footprint and it also often performed better during our experiments. This section is an expanded version of [74, §5.2].

[1] Recall [5, §2.3] that a **Las Vegas algorithm** either returns a correct answer or it fails — the probability of failure being bounded by a constant.

4.1.1. A single endomorphism

We begin with a well-known ingredient used in both methods. Let ϕ be an endomorphism of V. As we remarked in §2.1, V is a completely reducible $K[\phi]$-module if and only if the minimal polynomial f of ϕ is square-free. Supposing that this is the case, let $f = f_1 \cdots f_r$ be the factorisation into irreducibles. The following description of the homogeneous components of V as a $K[\phi]$-module is well-known; cf. [4, §5.2]. By basic linear algebra, we have $V = U_1 \oplus \cdots \oplus U_r$, where $U_i = \mathrm{Ker}(f_i(\phi)) \neq 0$ for $1 \leqslant i \leqslant r$. The algebra $K[\phi]$ naturally acts as the field $K[X]/(f_i)$ on U_i, whence U_i is a homogeneous $K[\phi]$-module. If $0 \neq x \in U_i$, then the minimal polynomial of ϕ acting on $x \cdot K[\phi]$ is f_i. Hence, if U_i and U_j have isomorphic irreducible $K[\phi]$-submodules, then $i = j$. We conclude that $U_1, \ldots, U_r$ are the homogeneous components of V as a $K[\phi]$-module.

4.1.2. The general case

The following is a refined version of a result which is due to Dixon [26, Lem. 5]; Dixon's original result has already been used in [4, §5.2].

4.1 Lemma. *Let $\mathcal{A}$ be a commutative semisimple subalgebra of* $\mathrm{End}(V)$ *with basis $(a_1, \ldots, a_s)$. Let $c \geqslant 2$ be an integer and let E be a finite subset of K with $|E| \geqslant cs(s-1)$. Then with probability at least $1-1/c$, a random element $a = e_1a_1 + \cdots + e_sa_s$ satisfies $\mathcal{A} = K[a]$, where the e_i are chosen independently and uniformly from E.*

Proof. This follows from [27, Lem. 2.1 & 3.1]. ♦

If $K[G] = K[x]$, then we may find the homogeneous decomposition of V as a $K[G]$-module using §4.1.1. Clearly, for any $x \in K[G]$, we have $K[G] = K[x]$ if and only if $\mathrm{degree}(f) = |K[G] : K|$, where f is the minimal polynomial of x. A basis of $K[G]$ can be computed using a standard "spinning-type" algorithm (cf. [4, §5.1]). This yields a Las Vegas algorithm for computing the homogeneous decomposition of V as a $K[G]$-module as in [2, §6.5.1].

4.2 Remark. In our pseudo-code, lists are designated using square brackets.

Algorithm 4.1 HomogeneousDecompositionAbelian(G) (general case)

Input: a completely reducible abelian group $G = \langle g_1, \ldots, g_n \rangle \leqslant \mathrm{GL}(V)$, K perfect and infinite
Output: the homogeneous components of V as a $K[G]$-module

```
repeat
    let x ∈ K[G] be a "random" element as in Lemma 4.1
    let f ∈ K[X] be the minimal polynomial of x
until degree(f) = |K[G] : K|
let f = f_1 ··· f_r be the factorisation into irreducibles
return [Ker(f_1(x)), ..., Ker(f_r(x))]
```

We note that a deterministic algorithm for computing the Wedderburn decomposition of a semisimple commutative algebra is given in [32, §7]. This yields yet

another method for computing the homogeneous decomposition of a completely reducible abelian linear group (see Proposition 1.5).

4.1.3. Finite abelian groups

In §4.1.2, to compute a basis of $K[G]$ using a "spinning-type" algorithm, $\mathcal{O}(|V:K|^3)$ field elements have to be stored. Since this can become infeasible in large dimensions, we now propose a different method for finding the homogeneous decomposition if G is *finite* abelian. This method, given in Algorithm 4.3, needs to store $\mathcal{O}(n \cdot |V:K|^2)$ field elements, where n is the number of defining generators of G.

We will often use the following simple function for constructing an element of order $\exp(G)$ in a finite abelian group G.

Algorithm 4.2 ExponentElement(G)

Input: a finite abelian group $G = \langle g_1, \ldots, g_n \rangle$
Output: an element $g \in G$ with $\operatorname{ord}(g) = \exp(G)$
1: $M \leftarrow \operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_n))$, say $M = \prod_{p \in S} p^{\alpha(p)}$ for a set of primes S and $\alpha(p) > 0$
2: **for** $p \in S$ **do** find $i(p) \in \{1, \ldots, n\}$ with $p^{\alpha(p)} \mid \operatorname{ord}(g_{i(p)})$
3: **return** $\prod_{p \in S} g_{i(p)}^{\operatorname{ord}(g_{i(p)})/p^{\alpha(p)}}$

Algorithm 4.3 HomogeneousDecompositionAbelian(G) (finite case)

Input: a completely reducible finite abelian $G = \langle g_1, \ldots, g_n \rangle \leqslant \mathrm{GL}(V)$
Output: the homogeneous components of V as a $K[G]$-module
1: *quasi* $\leftarrow [V]$, *homg* $\leftarrow [\,]$
2: **while** *quasi* is non-empty **do**
3: pick and remove U from *quasi*
4: let $G \xrightarrow{\varrho} \mathrm{GL}(U)$ be the action on U and write $H = G^{\varrho}$
5: $a \leftarrow$ ExponentElement(H)
6: let $U_1, \ldots, U_r$ be the homogeneous components of U as a $K[a]$-module
7: **if** $H = \langle a \rangle$ **then**
8: append $U_1, \ldots, U_r$ to *homg*
9: **else if** $r > 1$ **then**
10: append $U_1, \ldots, U_r$ to *quasi*
11: **else**
12: find $b = g_j^{\varrho} \in H$ such that $b \notin \langle a \rangle$
13: find i such that U is an inhomogeneous R-module, where $R = K[b - a^i]$
14: append the homogeneous components of U as an R-module to *quasi*
15: **return** *homg*

4.3 Proposition. *Given a completely reducible finite abelian input group G, Algorithm 4.3 terminates and returns the homogeneous decomposition of V as a $K[G]$-module.*

Proof. We first argue that the steps performed are even valid. Let $U \leqslant V$ be a $K[G]$-submodule and $x \in K[G]$. Then $K[x]$ is semisimple and hence all $K[x]$-modules are completely reducible. By commutativity of $K[G]$ and Corollary 1.6,

the homogeneous components of U as a $K[x]$-module are $K[G]$-submodules. Hence, at all times during the execution of Algorithm 4.3, each element of $quasi \cup homg$ is a $K[G]$-submodule of V and it makes sense to speak of the homogeneous components of U as a module over $K[a]$ or $K[b - a^i]$ in lines 6 and 14, respectively.

In line 13, a suitable i exists for the following reason: let $e = \exp(H) = \operatorname{ord}(a)$. We have $r = 1$ so that $K[a]$ is a field. The element a is a primitive eth root of unity whence $X^e - 1 = \prod_{i=0}^{e-1}(X - a^i)$ in $(K[a])[X]$. Since a and b commute, the evaluation map $\eta\colon (K[a])[X] \to K[a, b]$, $f \mapsto f(b)$ is a homomorphism. As $0 = b^e - 1 = (X^e - 1)\eta = \prod_{i=0}^{e-1}(X - a^i)\eta = \prod_{i=0}^{e-1}(b - a^i)$, we conclude that $c = b - a^i \neq 0$ is singular for some i. Hence, $K[c]$ is not a field so that U is an inhomogeneous $K[c]$-module.

Consider the following statements.

(i) $V = \bigoplus (quasi \cup homg)$ (the union being disjoint) as $K[G]$-modules.

(ii) G acts homogeneously on all elements of $homg$.

(iii) For distinct elements $U_1, U_2 \in quasi \cup homg$, there exists $g \in K[G]$ such that U_1 and U_2 are homogeneous non-trivial $K[g]$-modules, but the irreducible $K[g]$-submodules of U_1 and U_2 are not isomorphic.

All of these statements are initially true and they also remain true after every execution of the body of the while loop. Note that each iteration of the while loop either decreases $|\bigoplus quasi : K|$ or it increases $|quasi|$. Since every element of $quasi$ is non-zero, $|quasi| \leqslant |\bigoplus quasi : K|$. It follows that after $\mathcal{O}(|V : K|^2)$ iterations, $quasi$ will be empty so that Algorithm 4.3 terminates.

At termination, $quasi$ is empty so that (i) gives $V = \bigoplus quasi$. By (ii), each element $U \in homg$ is contained in a homogeneous component, $\tilde{U}$ say, of V as a $K[G]$-module. Now $V/U \cong_{K[G]} \bigoplus (homg \setminus \{U\})$. If $\tilde{U}$ were distinct from U, then $\tilde{U}/U$ would contain an irreducible submodule M. By the Jordan-Hölder theorem, M would then be isomorphic to a $K[G]$-composition factor of some $W \in homg \setminus \{U\}$, contradicting (iii). Hence, $U = \tilde{U}$. ♦

4.1.4. Irreducibility testing of abelian linear groups

Let $G \leqslant \mathrm{GL}(V)$ be an abelian group, given by finitely many generators. We now summarise how irreducibility of G can be tested. Using §2.3, we may assume that G is completely reducible. We then construct the homogeneous decomposition of $V = U_1 \oplus \cdots \oplus U_r$ as a $K[G]$-module. If $r > 1$, then G is evidently reducible, so let $r = 1$. Then $K[G]$ is a field and hence V is a right $K[G]$-vector space. We see that G is reducible if and only if $x \cdot K[G] < V$ for an arbitrary non-zero $x \in V$.

4.1.5. Polynomial factorisation vs irreducibility testing

We have just described an algorithm for irreducibility testing of finitely generated abelian linear groups over any field K of characteristic zero which admits algorithmic polynomial factorisation. Conversely, an algorithm for irreducibility testing of

finitely generated abelian linear groups over an arbitrary field K can be used to factorise polynomials as follows. Let $f \in K[X]$ be a non-constant monic polynomial. We may assume that $f(0) \neq 0$. Let g be the companion matrix of f. Then the polynomial f is irreducible if and only $\langle g \rangle$ is an irreducible subgroup of $\mathrm{GL}_d(K)$, where $d = \mathrm{degree}(f)$. Furthermore, if $0 < U < K^d$ is g-invariant, then the minimal polynomial of g acting on U is a proper divisor of f.

4.2. Abelian normal subgroups with a given property

Let G be a finite nilpotent group (not necessarily linear) and suppose that $\mathcal{E}$ is a set of subgroups of G. Under suitable computational assumptions, we wish to either construct an abelian normal subgroup of G in $\mathcal{E}$ or we wish to construct a maximal abelian normal subgroup of G which fails to be in $\mathcal{E}$. Later on, this problem, which is solved by the simple Algorithm 4.4, will play a vital part in irreducibility testing of nilpotent linear groups.

Apart from being able to decide whether $A \in \mathcal{E}$ holds for a given abelian $A \lhd G$, in order to use Algorithm 4.4, we need to be able to (i) compute centralisers of abelian normal subgroups of G and (ii) decide membership in abelian normal subgroups of G; in both cases, the abelian normal subgroups are given by generators. Assuming this, the correctness of Algorithm 4.4 is immediate from the following basic facts.

4.4 Proposition. *Let G be a group and let $A \lhd G$ be abelian.*

(i) ([51, 1.3.2(ii)]) *If G is supersoluble, then A is a maximal abelian normal subgroup of G if and only if $A = \mathrm{C}_G(A)$.*

(ii) ([68, 5.2.3]) *If $cA \in \mathrm{C}_G(A)/A \cap \mathrm{Z}(G/A)$, then $\langle A, c \rangle$ is an abelian normal subgroup of G.*

4.5 Proposition ([68, 5.2.1])**.** *If G is nilpotent and $1 \neq N \lhd G$, then $N \cap \mathrm{Z}(G) \neq 1$.*

Algorithm 4.4 FindAbelianWithProperty$(G, \mathcal{E})$

Input: a finite nilpotent group G, a set $\mathcal{E}$ of subgroups of H
Output: either `true` and an abelian normal subgroup of G in $\mathcal{E}$, or `false` and a maximal abelian normal subgroup of G which does not belong to $\mathcal{E}$

1: **if** G is abelian **then return** $G \in \mathcal{E}$, G
2: let $A \lhd G$ be abelian
3: **loop**
4: **if** $A \in \mathcal{E}$ **then return** `true`, A
5: $C \leftarrow \mathrm{C}_G(A)$
6: **if** $C = A$ **then return** `false`, A
7: let $c \in C \setminus A$
8: **while** $[c, g] \notin A$ for some $g \in G$ **do** $c \leftarrow [c, g]$
9: $A \leftarrow \langle A, c \rangle$

4.6 Remark. One of the major cases that we are interested in is when $\mathcal{E}$ is the set of non-cyclic subgroups of G. In Part II, we will extend Algorithm 4.4 and obtain an algorithm which, given a finite nilpotent group G, either constructs a non-cyclic abelian normal subgroup of G or proves that no such subgroup exists (Algorithm 7.1).

The initial abelian normal subgroup. The choice of an initial abelian normal subgroup A of G in line 2 of Algorithm 4.4 is arbitrary; in particular, we may simply take $A = 1$. In practice, however, we use the following algorithm from [21, §2.2].

Algorithm 4.5 NoncentralAbelian(G)

Input: a non-abelian finite nilpotent group $G = \langle g_1, \dots, g_n \rangle$
Output: a non-central abelian normal subgroup of G
1: let $a \in G$ be a non-central element among $g_1, \dots, g_n$
2: **while** $[a, g_i] \notin \mathrm{Z}(G)$ for some i **do** $a \leftarrow [a, g_i]$
3: **return** $\langle a, [a, g_1], \dots, [a, g_n] \rangle$

4.3. Constructing abelian normal subgroups using congruence homomorphisms

Let $G = \langle g_1, \dots, g_n \rangle \leqslant \mathrm{GL}_d(K)$ be a finitely generated non-abelian completely reducible nilpotent group. We assume that $R \subset K$ is a subring with $G \leqslant \mathrm{GL}_d(R)$ and that $R \xrightarrow{\pi} F$ is an effectively computable epimorphism onto a finite field F such that the congruence subgroup $G_\pi = G \cap \mathrm{CL}_d(\pi)$ is torsion-free. It follows from Chapter 3 that we may always find such R and π if K is a number field or a rational function field over a number field.

We now describe how we may perform one of the tasks (A1)–(A2) from the beginning of this chapter.

A polycyclic presentation of G^π. We describe how we may obtain an epimorphism $G \xrightarrow{\psi} H$ onto a finite polycyclically presented group H such that

(i) $\mathrm{Ker}(\psi) = G_\pi$,

(ii) we can compute g_i^ψ for $1 \leqslant i \leqslant n$, and

(iii) for any $h \in H$ we can construct a specific $g \in G$ with $g^\psi = h$.

If the reference to ψ is clear, then in (iii) we also say that we can **lift** elements of H to G. Recall that a **section** of a homomorphism $G_1 \xrightarrow{\theta} G_2$ is a set map $G_2 \xrightarrow{\sigma} G_1$ with $\sigma\theta = 1$. In more sophisticated language, (iii) then asserts that we have an explicitly computable section $H \to G$ of $G \xrightarrow{\phi} H$.

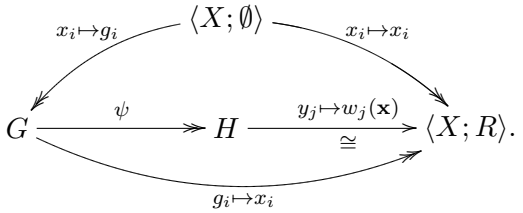
A group H as above and an epimorphism ψ can be obtained as follows. First, G^π is a finite nilpotent (hence polycyclic) matrix group over a finite field with defining generators $g_1^\pi, \ldots, g_n^\pi$. Using various methods (e. g. [54, §4], [2, §3]), we may construct a polycyclically presented group $H = \langle Y; S\rangle$ together with an effectively computable isomorphism $G^\pi \xrightarrow{\lambda} H$.

Write $Y = \{y_1, \ldots, y_m\}$, $\mathbf{y} = (y_1, \ldots, y_m)$, and $S = \{s_1(\mathbf{y}), \ldots, s_t(\mathbf{y})\}$. During the construction of the above polycyclic presentation of G^π, we keep track of the group operations performed in G^π leading from the given generators $g_1^\pi, \ldots, g_n^\pi$ to the polycyclic generating sequence used to construct the above presentation of G^π; the implementation of [2, §3] in the package Polenta [3] for GAP [34] uses this approach. We thus obtain explicit words w_j such that $y_j = w_j(g_1^\pi, \ldots, g_n^\pi)^\lambda$ for $1 \leqslant j \leqslant m$. It follows that if we define ψ to be the composite $G \xrightarrow{\pi} G^\pi \xrightarrow{\lambda} H$, then conditions (i)—(iii) above are satisfied.

Generators of G_π. Using a collection algorithm [39, §8.1.3] in H, we may write $g_i^\psi = v_i(\mathbf{y})$ for $1 \leqslant i \leqslant n$. Let $X = \{x_1, \ldots, x_n\}$ (n distinct symbols) and $\mathbf{x} = (x_1, \ldots, x_n)$. Define

$$R = \left\{x_i^{-1} \cdot v_i\left(w_1(\mathbf{x}), \ldots, w_m(\mathbf{x})\right) : 1 \leqslant i \leqslant n\right\} \cup \left\{s_k(w_1\left(\mathbf{x}\right), \ldots, w_m(\mathbf{x})) : 1 \leqslant k \leqslant t\right\}.$$

By [68, 2.2.3], the map $x_i \mapsto g_i^\psi$ induces an isomorphism $\langle X; R\rangle \to H$; the inverse is given by $y_j \mapsto w_j(\mathbf{x})$. We obtain a commutative diagram



Hence, G_π is generated by $E = \{r(g_1, \ldots, g_n) : r(\mathbf{x}) \in R\}$ as a normal subgroup of G. Since $G_\pi \leqslant \mathrm{Z}(G)$ by Corollary 2.6(i), we therefore have $G_\pi = \langle E\rangle$.

Lifting subgroups of H. Let $U = \langle u_1, \ldots, u_r\rangle \leqslant H$. As explained above, we may construct preimages $c_1, \ldots, c_r \in G$ with $u_i = c_i^\psi$. We then have $U\psi^{-1} = \langle c_1, \ldots, c_r, E\rangle$, where E is the previously constructed generating set of G_π.

Final step. Let $\mathcal{E} = \{U \leqslant H : U\psi^{-1}$ is inhomogeneous$\}$. We just described how generators of $U\psi^{-1}$ can be computed for given generators of $U \leqslant H$. If U is abelian, then so is $U\psi^{-1}$ by Lemma 2.5. We may then use the techniques from §4.1 to determine if $U\psi^{-1}$ is homogeneous and hence decide if $U \in \mathcal{E}$. It follows that by using FindAbelianWithProperty$(H, \mathcal{E})$ (see §4.2), we may construct an abelian $A \triangleleft G$ such that A is either inhomogeneous or A is maximal abelian (i.e. $A = \mathrm{C}_G(A)$) and homogeneous.

5. Deciding irreducibility of nilpotent linear groups over number fields

We describe an algorithm for deciding irreducibility of nilpotent linear groups over number fields. We first recall some facts on Brauer groups (Section 5.1) and then relate these to abelian normal subgroups of linear groups (Section 5.2). We then summarise some computational problems for Brauer groups for which solutions have recently become available (Section 5.4). Finally, we give our algorithm (Section 5.5).

5.1. Background on Brauer groups and crossed products

We collect well-known facts on Brauer groups and crossed products; see e. g. [53, §§29–30], [15, Ch. 5], and [24, Ch. 5]. Throughout, let K be arbitrary.

Central simple algebras. The K-algebra $\mathcal{A}$ is **central simple** if $\mathcal{A}$ is simple and $\mathrm{Z}(\mathcal{A}) = K$. If $\mathcal{A}$ is a central simple K-algebra, then $|\mathcal{A} : K| = d^2$ for an integer $d \geqslant 1$ called the **degree** of $\mathcal{A}$.

Similarity. Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be central simple K-algebras. By Wedderburn's theorem, $\mathcal{A}_i \cong \mathrm{M}_{e_i}(\mathcal{D}_i)$ for a central K-division algebra $\mathcal{D}_i$. We say that $\mathcal{A}_1$ and $\mathcal{A}_2$ are **similar** if $\mathcal{D}_1$ and $\mathcal{D}_2$ are K-isomorphic. We let $\mathcal{A}_1 \sim \mathcal{A}_2$ denote similarity of $\mathcal{A}_1$ and $\mathcal{A}_2$ and we write $[\mathcal{A}_1]$ for the class of all central simple K-algebras similar to $\mathcal{A}_1$. The similarity class of a central K-division algebra $\mathcal{D}$ consists of all K-algebras isomorphic to $\mathrm{M}_e(\mathcal{D})$ for some $e \geqslant 1$.

The Brauer group. The class of central simple K-algebras is closed under tensor products. Moreover, taking tensor products of central simple K-algebras is compatible with similarity. Ignoring set-theoretic difficulties surrounding "classes of classes" (these obstacles can be easily overcome; see [15, p. 188]), we may define

$$\mathrm{Br}(K) = \{[\mathcal{A}] : \mathcal{A} \text{ is a central simple } K\text{-algebra}\}$$

endowed with the multiplication $[\mathcal{A}_1][\mathcal{A}_2] = [\mathcal{A}_1 \otimes \mathcal{A}_2]$. Then $\mathrm{Br}(K)$ is an abelian group, called the **Brauer group** of K. The identity element of $\mathrm{Br}(K)$ is $[K]$, the class of all simple K-algebras that are **split**, i. e. isomorphic to $\mathrm{M}_e(K)$ for some $e \geqslant 1$. The inverse of $[\mathcal{A}] \in \mathrm{Br}(K)$ is $[\mathcal{A}^\circ]$, where $\mathcal{A}^\circ$ is the **opposite algebra** of $\mathcal{A}$ (obtained by reversing the multiplication in $\mathcal{A}$).

Relative Brauer groups. Let L/K be a field extension. If $\mathcal{A}$ is any K-algebra, then we obtain an L-algebra $\mathcal{A}_L = \mathcal{A} \otimes_K L$. The rule $\mathcal{A} \mapsto \mathcal{A}_L$ induces a homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(L)$, the kernel $\mathrm{Br}(L/K)$ of which is called the **relative Brauer group** of L over K. We say that L is a **splitting field** of the central simple K-algebra $\mathcal{A}$ if $[\mathcal{A}] \in \mathrm{Br}(L/K)$; this is equivalent to $\mathcal{A}_L \cong \mathrm{M}_d(L)$, where d is the degree of $\mathcal{A}$. If $L_2/L_1/K$ is a tower of fields, then $\mathrm{Br}(L_1/K)$ is a subgroup of $\mathrm{Br}(L_2/K)$. We have $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$, the directed union being taken over all finite Galois extensions L/K within some fixed algebraic closure of K.

Exponent and index. The group $\mathrm{Br}(K)$ is periodic. Let $\mathcal{A}$ be a central simple K-algebra. The order of $[\mathcal{A}] \in \mathrm{Br}(K)$ is called the **exponent** $\exp(\mathcal{A})$ of $\mathcal{A}$. Clearly, the index $\mathcal{A}$ (see §1.2) only depends on the similarity class of $\mathcal{A}$. It is always the case that the $\exp(\mathcal{A})$ divides $\mathrm{index}(\mathcal{A})$. Conversely, every prime divisor of $\mathrm{index}(\mathcal{A})$ divides $\exp(\mathcal{A})$. While $\mathrm{index}(\mathcal{A}) \neq \exp(\mathcal{A})$ is possible in general, it is a consequence of the Brauer-Hasse-Noether theorem that if K is a number field (or more generally a global or local field), then always $\mathrm{index}(\mathcal{A}) = \exp(\mathcal{A})$.

Crossed products. Let L/K be a finite Galois extension with Galois group Γ. Let $\phi \in \mathrm{Z}^2(\Gamma, L^\times)$ be a normalised 2-cocycle. Define $L \star_\phi \Gamma$ to be the right L-vector space with basis $(u_\sigma)_{\sigma\in\Gamma}$ endowed with the multiplication $au_\sigma = u_\sigma a^\sigma$ $(a \in L, \sigma \in \Gamma)$ and $u_\sigma u_\tau = u_{\sigma\tau} \cdot (\sigma, \tau)\phi$ $(\sigma, \tau \in \Gamma)$, extended K-linearly. Then $L \star_\phi \Gamma$ is a central simple K-algebra and L (identified with $u_1 \cdot L$) is a maximal subfield and a splitting field of $L \star_\phi \Gamma$. The algebra $L \star_\phi \Gamma$ is called the **crossed product** of L by Γ determined by ϕ. The crossed product $L \star_\phi \Gamma$ splits if and only if ϕ is a coboundary. More generally, the rule $\phi \mapsto L \star_\phi \Gamma$ induces an isomorphism $\mathrm{H}^2(\Gamma, L^\times) \to \mathrm{Br}(L/K)$. In particular, the exponent of $L \star_\phi \Gamma$ coincides with the order of the cohomology class $[\phi]$ in $\mathrm{H}^2(\Gamma, L^\times)$. Using Corollary 1.9, we see that the index of $L \star_\phi \Gamma$ is exactly the dimension of the (unique) irreducible module of $L \star_\phi \Gamma$ as a right L-space.

5.2. Crossed products and abelian normal subgroups

Let $G \leqslant \mathrm{GL}(V)$, where K is arbitrary. Let $A \lhd G$ with $A = \mathrm{C}_G(A)$ and suppose that A is homogeneous. Let $1 \to A \hookrightarrow G \xrightarrow{-} \Gamma \to 1$ be an exact sequence of groups and regard A as a Γ-module in the usual way. We now examine the structure of $K[G]$; our reasoning is similar to the proof of [53, 34.F8].

The quotient Γ as a Galois group. Clearly, the action of Γ on A extends to an action of Γ on $L = K[A]$ by K-algebra automorphisms: for $\sigma \in \Gamma$, say $\sigma = \overline{g}$ with $g \in G$, and $x \in L$, we let $x^\sigma = g^{-1}xg$. Since A is homogeneous, L and $Z = L^\Gamma$ are field extensions of K. Now $A = \mathrm{C}_G(A)$ whence Γ acts faithfully on L. We may naturally regard V as a right L-vector space. Of course, the induced right K-action is related to the given left K-action on V via $v\lambda = \lambda v$ $(\lambda \in K, v \in V)$. Hence, $|V : K| = |V : L||L : K|$ and thus $|\Gamma| \leqslant |\mathrm{Gal}(L/K)| \leqslant |L : K| < \infty$ by [14, Cor.

7.5.2]. By Artin's theorem [48, Thm VI.1.8], L/Z is therefore Galois and the above action of Γ on L allows us to identify Γ with $\mathrm{Gal}(L/Z)$. Note that Z is contained in the centre of $K[G]$ so that we may regard $K[G]$ as a Z-algebra.

Extension structure. Choose a normalised section $\Gamma \xrightarrow{s} G$ of $G \xrightarrow{\bar{\cdot}} \Gamma$, i. e. $\overline{\sigma^s} = \sigma$ for all $\sigma \in \Gamma$ and $1_\Gamma^s = 1_G$. Let $\phi \in \mathrm{Z}^2(\Gamma, A)$ be the corresponding cocycle defined by $\sigma^s\tau^s = (\sigma\tau)^s \cdot (\sigma, \tau)\phi$ for $\sigma, \tau \in \Gamma$. Let $\tilde{\phi} \in \mathrm{Z}^2(\Gamma, L^\times)$ be obtained from ϕ via the inclusion $A \hookrightarrow L^\times$.

5.1 Proposition. *The rule $u_\sigma a \mapsto \sigma^s a$ ($\sigma \in \Gamma, a \in L$) induces a Z-algebra isomorphism $L \star_{\tilde{\phi}} \Gamma \to K[G]$.*

Proof. There is a unique linear map $L \star_{\tilde{\phi}} \Gamma \xrightarrow{T} K[G]$ of right L-spaces satisfying $u_\sigma T = \sigma^s$. By construction, this is a Z-algebra epimorphism. Since crossed products are simple, it is an isomorphism. ⧫

We therefore say that $K[G]$ is a crossed product of L by Γ.

5.2 Remark. Proposition 5.1 can also be obtained using the more general ring-theoretic definition of a crossed product in [81, p. 23]. Namely, it follows from [81, 5.3.2] that $K[G]$ is a crossed product $(K[G], L, G, G/A)$. Using the above interpretation of $G/A \cong \Gamma$ as $\mathrm{Gal}(L/Z)$, this leads us back to the classical crossed product.

5.3 Corollary.

(i) $K[G]$ is simple with centre Z. In particular, G is homogeneous.

(ii) L is a maximal subfield of $K[G]$.

(iii) $|K[G] : Z| = |G : A|^2$ and thus $|K[G] : K| = |G : A||L : K|$. ⧫

Together with Proposition 4.4(i), we obtain the following.

5.4 Corollary. *Let G be a supersoluble linear group. If G has a homogeneous maximal abelian normal subgroup, then G itself is homogeneous.* ⧫

5.3. Example: cyclic algebras and nilpotent linear groups

In the special case of a cyclic Galois group, a crossed product is called a **cyclic algebra**. We describe a family of nilpotent linear groups whose enveloping algebras admit explicit descriptions as cyclic algebras. In this section, K is an arbitrary field of characteristic zero.

Facts on cyclic algebras. We refer to [53, §30.4] for details on the following. Let L/K be a cyclic Galois extension of degree m. Write $\Gamma = \mathrm{Gal}(L/K)$. Choose a generator $\sigma \in \Gamma$. For $\lambda \in K^\times$, define $\mathrm{cyc}(L/K, \lambda, \sigma)$ to be the right L-space with basis $(1, g, \ldots, g^{m-1})$ with multiplication $ag = ga^\sigma$ $(a \in L)$ and $g^m = \lambda$, extended in the natural way. Then $\mathrm{cyc}(L/K, \lambda, \sigma)$ is a crossed product of L by Γ (and hence a cyclic algebra). Conversely, all crossed products of L by Γ can be brought into this form in an explicit way [52, p. 197]. Denote by $\mathrm{N}_{L/K}\colon L \to K$ the norm map. The exponent of a cyclic algebra $\mathrm{cyc}(L/K, \lambda, \sigma)$ is given by $\min\bigl(e \geqslant 1 : \mathrm{N}_{L/K}(\alpha) = \lambda^e \text{ for some } \alpha \in L^\times\bigr)$. Recall that for a central simple algebra over a number field, the exponent and the index coincide.

A family of nilpotent linear groups. Suppose that K contains a primitive mth root of unity ζ_m. Let $\lambda, \nu \in K^\times$ and suppose that $X^m - \nu$ is irreducible over K. Let $\beta = \sqrt[m]{\nu}$ and define

$$H = \left\langle \underbrace{\begin{bmatrix} \beta & & & \\ & \beta\cdot\zeta_m^{-1} & & \\ & & \ddots & \\ & & & \beta\cdot\zeta_m^{-m+1} \end{bmatrix}}_{u}, \underbrace{\begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ \lambda & & & \end{bmatrix}}_{g} \right\rangle.$$

By Kummer theory [14, §11.10], the assumption $\zeta_m \in K$ ensures that $K(\beta)/K$ is cyclic. Now regard H as a K-linear group of degree m^2 instead of as a $K(\beta)$-linear group of degree m. Then $A = \langle g^m, u, [u, g]\rangle = \langle \lambda, u, \zeta_m\rangle$ is a homogeneous maximal abelian normal subgroup of H with $H/A \cong \mathrm{C}_m$. Clearly, H is a quotient of the class-2 group

$$H(m) = \Bigl\langle u, g \;\Bigm|\; [u, g]^m = [u, g, g] = [u, g, u] = 1 \Bigr\rangle.$$

It is known (cf. [46, 14.12]) that $K[H]$ is isomorphic to $\mathrm{cyc}(K(\beta)/K, \lambda, \sigma)$ in the natural way, where σ is the generator $\beta \mapsto \beta\cdot\zeta_m$ of $\mathrm{Gal}(K(\beta)/K)$. We will give another interpretation of H in Example 6.19 below.

5.4. Computing in relative Brauer groups over number fields

In this thesis, we use the standard notation C^*, Z^*, B^*, H^*, and ∂ for cochains, cocycles, coboundaries, cohomology, and differentials, respectively.

Let L/Z be a Galois extension of number fields and $\Gamma = \mathrm{Gal}(L/Z)$. Fieker [31, §4] describes an algorithm which for a given $\phi \in \mathrm{Z}^2(\Gamma, L^\times)$ decides if $[\phi] \in \mathrm{H}^2(\Gamma, L^\times)$ is trivial. More specifically, for $\phi \in \mathrm{Z}^2(\Gamma, L^\times)$, he constructs

(i) a Γ-invariant finitely generated subgroup $U \leqslant L^\times$ such that (a) $\phi \in \mathrm{Z}^2(\Gamma, U)$ and (b) $[\phi]$ is trivial in $\mathrm{H}^2(\Gamma, L^\times)$ if and only if $[\phi]$ is trivial in $\mathrm{H}^2(\Gamma, U)$ and

(ii) an isomorphism $\mathbf{Z}/m \oplus \mathbf{Z}^r \xrightarrow{\lambda} U$ such that λ and λ^{-1} are effectively computable.

It is then possible to compute the (unique) Γ-module structure on $A = \mathbf{Z}/m \oplus \mathbf{Z}^r$ which turns λ into a Γ-equivariant map. Next, we compute an explicit preimage $\psi \in \mathrm{Z}^2(\Gamma, A)$ of ϕ. It follows that $[\phi]$ is trivial in $\mathrm{H}^2(\Gamma, L^\times)$ if and only if $[\psi]$ is trivial in $\mathrm{H}^2(\Gamma, A)$. Computations in $\mathrm{H}^2(\Gamma, A)$ are possible using Holt's algorithm [38]. Thus, we can test if ψ (hence ϕ) is a coboundary. Furthermore, if this is the case, then we can find $a \in \mathrm{C}^1(\Gamma, A)$ with $\psi = a\partial$. Using λ, we therefore find $b \in \mathrm{C}^1(\Gamma, L^\times)$ with $\phi = b\partial$.

Since $\mathrm{H}^2(\Gamma, L^\times)$ has exponent dividing $|\Gamma|$, we can compute the order of any cohomology class in $\mathrm{H}^2(\Gamma, L^\times)$ defined by a cocycle. We note that Fieker's method for obtaining U (hence A) above relies on the computation of the class group of L which can be prohibitively expensive when $|L : \mathbf{Q}| > 30$, say. At the time of this writing, an implementation of the above method is available in Magma only in the case that $L/\mathbf{Q}$ (instead of merely L/Z) is Galois. Finally, we remark that Fieker also describes a non-constructive method for deciding if $\phi \in \mathrm{Z}^2(\Gamma, L^\times)$ is a coboundary using local computations. Note that by §5.3, in the special case that Γ is cyclic, we can avoid cohomological computations altogether by testing solubility of norm equations.

5.5. An algorithm for deciding irreducibility of nilpotent linear groups over number fields

We may decide irreducibility of a given finitely generated nilpotent group $G \leqslant \mathrm{GL}(V)$, where K is a number field, using Algorithm 5.1 below. This algorithm is "partially constructive": if G is found to be reducible, then we often (but not always) obtain a proper $K[G]$-submodule of V; see Remark 5.5(ii). We then return a generator of such a submodule; see Remark 5.5(i). The function NonzeroElement which we will use throughout this thesis returns a non-zero vector of a non-zero vector space.

We now explain how Algorithm 5.1 works.

1. Initial steps. First, we use §2.3 to ensure that the input group G is completely reducible. We then catch the easy case of an abelian group using §4.1.4. Next, we find a congruence homomorphism with torsion-free kernel and finite image defined on G and construct a polycyclic presentation of the congruence image. We thus obtain a homomorphism $G \xrightarrow{\psi} H$ with properties as in §4.3.

2. Constructing an abelian normal subgroup. We can lift abelian normal subgroups of H to those of G as described in §4.3. We can then use §4.1 to decide if such lifted subgroups are homogeneous. Using §4.2, we may therefore either (A1) construct an inhomogeneous abelian normal subgroup A of G, or (A2) a maximal abelian normal subgroup A of G which is homogeneous.

Algorithm 5.1 IsIrreducible(G) (general case, partially constructive)

Input: a nilpotent group $G = \langle g_1, \ldots, g_n \rangle \leqslant \mathrm{GL}(V)$, where K is a number field
Output: `true` or `false` according to whether G is irreducible or not;
if a second value is returned, then it is a generator of a proper $K[G]$-submodule of V

loop
  if $G_{\mathrm{u}} = \langle (g_1)_{\mathrm{u}}, \ldots, (g_n)_{\mathrm{u}} \rangle \neq 1$ **then return** `false`, NonzeroElement($V^{G_{\mathrm{u}}}$)
  if G is abelian **then**
    $x \leftarrow$ NonzeroElement (HomogeneousDecompositionAbelian(G)[1])
    if $x \cdot K[G] < V$ **then return** `false`, x **else return** `true`
  construct an epimorphism $G \xrightarrow{\psi} H$ onto a finite group as in §4.3
  $r, B \leftarrow$ FindAbelianWithProperty($H, \mathcal{E}$) for $\mathcal{E} = \{B \leqslant H : B\psi^{-1}$ is inhomogeneous$\}$
  $A \leftarrow B\psi^{-1}$
  if $r =$ `false` **then**
    let $\Gamma = H/B$ act on A via the ψ-induced isomorphism $G/A \to \Gamma$
    construct a normalised section $\Gamma \to G$ and the corresponding cocycle $\phi \in \mathrm{Z}^2(\Gamma, A)$
    compute the order m of $[\phi]$ in $\mathrm{H}^2(\Gamma, L^\times)$, where $L = K[A]$
    if $|V : K| = m|L : K|$ **then return** `true` **else return** `false`
  homg $\leftarrow$ HomogeneousDecompositionAbelian(A), $U \leftarrow$ *homg*[1]
  if G acts intransitively on *homg* **then return** `false`, NonzeroElement(U)
  $G \leftarrow \mathrm{Im}(\theta)$, $V \leftarrow U$ where $\mathrm{Stab}_G(U) \xrightarrow{\theta} \mathrm{GL}(U)$ is the induced action

3. The crossed product case. Suppose we are in the "crossed product case" (A2). Since the known epimorphism $G \xrightarrow{\psi} H$ induces an isomorphism $G/A \to \Gamma$, where $\Gamma = H/B$, we may regard G as an extension of A by Γ. By lifting the images of a section $\Gamma \to H$ for the projection $H \to \Gamma$, we obtain a section $\Gamma \to G$ for the composite $G \xrightarrow{\psi} H \to \Gamma$ ("the product of sections is a section"). By Proposition 5.1, $K[G]$ is then in an explicit way a crossed product of $L = K[A]$ by Γ, with Γ acting faithfully by K-automorphisms on L. Using §5.4, we compute the order m of the cohomology class defined by ϕ in $\mathrm{H}^2(\Gamma, L^\times)$. This gives us the index of $K[G]$. Since we already computed the degree $|L : K|$ when we proved that A was homogeneous (Section 4.1.2), we may now read off the dimension $m|L : K|$ of the (unique) irreducible $K[G]$-module. We may therefore decide irreducibility of G by testing if $|V : K| = m|L : K|$.

4. Reduction. In case (A1), we found an inhomogeneous abelian normal subgroup A of G. We detect this and we compute the list *homg* of homogeneous components of V as a $K[A]$-module using Algorithm 4.1. We then compute the orbit of $U =$ *homg*[1] under G and (a finite generating set of) $\mathrm{Stab}_G(U)$ at the same time using the orbit-stabiliser algorithm [39, §4.1]. We then use Corollary 1.12 to reduce the problem of deciding irreducibility of G to that of deciding irreducibility of a linear group of smaller degree. We thus replace G and start again.

5.5 Remarks.

(i) Given a generator of a $K[G]$-submodule U of V, a basis of U can be found using the "spinning algorithm" [39, §7.4.1]. A minor technical difficulty however

occurs: in the pseudo-code of Algorithm 5.1, it would *not* suffice to generate $K[G]$-submodules, since line 16 might have been previously executed, changing G and V. In practice, we would store the original input group and we would also keep track of the inclusion of the current V into the original ambient space. This purely technical complication is the main reason why we only return generators of submodules in our pseudo-code.

(ii) If our algorithm reports reducibility of G, then, unless we encountered the crossed product case (lines 9–13), we also obtain a proper $K[G]$-submodule.

(iii) The method for irreducibility testing of finite linear groups over the rationals in MAGMA V2.16 also relies on index computations; these are performed using an algorithm of Nebe and Steel [58]. Their approach is however very different from ours: for a given finite $G \leqslant \mathrm{GL}_d(\mathbf{Q})$, they compute the centraliser $\mathcal{C}$ of G in $\mathrm{M}_d(\mathbf{Q})$. After reducing to the case that $\mathcal{C}$ is simple, they determine the index of $\mathcal{C}$ using the theory of orders. If $\mathcal{C}$ is a division algebra or, equivalently, if G is irreducible, then this can be detected at this point.

(iv) The explicit crossed product descriptions in our approach do not seem to be readily available in general. On the one hand, it is well-known that every central simple algebra over a number field is isomorphic to a cyclic algebra, i. e. a crossed product with cyclic Galois group. (This is the original "fundamental theorem in the theory of algebras" of Brauer-Hasse-Noether [8].) On the other hand, to the author's knowledge, no constructive proof of this result is known, nor is any practical method for representing a given central simple algebra over a number field as a crossed product available.

(v) We note that if we apply Algorithm 5.1 in the case that G is not nilpotent, then the output (if any) will in general not be meaningful.

We have thus obtained a partially constructive algorithm for irreducibility testing of nilpotent linear groups over number fields. As we will show in Part II of this thesis, if we restrict attention to *finite* nilpotent linear groups, we can do considerably more. First, in that case, we can handle a larger class of ground fields, including rational function fields over number fields. Second, we obtain a method for irreducibility testing of finite nilpotent groups which is fully constructive in all cases. Third, we can also test primitivity of finite nilpotent linear groups. Lastly, our algorithms for irreducibility and primitivity testing of finite nilpotent linear groups are practical, performing well on a range of explicit examples; an implementation is publicly available as a MAGMA-package [76]. (In contrast, Algorithm 5.1 has not been implemented.)

6. Groups with homogeneous maximal abelian normal subgroups

The most interesting case that we encountered in our algorithm for deciding irreducibility of (possibly) infinite nilpotent linear groups (Algorithm 5.1) was the following. We are given a finitely generated nilpotent group $G \leqslant \mathrm{GL}(V)$ and a homogeneous maximal abelian normal subgroup $A \lhd G$. The enveloping algebra $K[G]$ of G is then a crossed product of $L = K[A]$ by $G/A \cong \mathrm{Gal}(L/Z)$, where $Z = \mathrm{Z}(K[G])$ (Proposition 5.1). We are led to a series of theoretical questions which we will answer in this chapter.

Question 1: What is the structure of G as an abstract group?

We will see in §§6.2–6.3 that G is an extension of $\mathrm{A}(m,r) = \mathbf{Z}/m \oplus \mathbf{Z}^r$ by a subgroup of $\mathrm{R}(m,r) = \mathrm{U}(m) \ltimes (\mathbf{Z}/m)^r$, where $\mathrm{U}(m)$ is the group of unipotent elements in $(\mathbf{Z}/m)^\times$ and all the actions have natural descriptions. Conversely, all such extensions are nilpotent and have $\mathrm{A}(m,r)$ as a maximal abelian normal subgroup.

Question 2: Given an abstract extension G of $\mathrm{A}(m,r)$ by a subgroup Γ of $\mathrm{R}(m,r)$, is there a faithful representation ϱ of G over some field K such that $\mathrm{A}(m,r)$ acts homogeneously via ϱ?

The answer is yes — we may even require K to be a number field (Corollary 6.17).

Question 3: To what extent is the representation ϱ from the previous question uniquely determined?

First note that if ϱ is as in the last question, then G acts homogeneously via ϱ. Now fix a field K of characteristic zero and a cocycle $\phi \in \mathrm{Z}^2(\Gamma, \mathrm{A}(m,r))$ which defines G as an extension of $\mathrm{A}(m,r)$ by $\Gamma \leqslant \mathrm{R}(m,r)$. We then consider a certain class $\mathfrak{D}_0$ of *irreducible* K-representations ϱ of G such that (i) $\mathrm{A}(m,r)$ acts homogeneously via ϱ and (ii) $\mathrm{Z}(K[G^\varrho]) = K$. While we will not give a precise definition of $\mathfrak{D}_0$ at this point, we note that it contains all faithful irreducible representations of G over K that satisfy (i)–(ii). In Proposition 6.23, we will see that the equivalence classes of representations in $\mathfrak{D}_0$ are in natural 1–1 correspondence with the equivalence classes of certain field-theoretic objects which we call "(m,r)-structures over K". Informally, an (m,r)-structure over K amounts to (1) a choice η of a primitive mth root of unity over K, (2) elements $\theta_1, \ldots, \theta_r$ (all within some field extension of K) such that $\theta_i^m \in K^\times$ for $1 \leqslant i \leqslant r$, and (3) a technical condition allowing us to identify Γ with $\mathrm{Gal}(L/K)$, where $L = K(\eta, \theta_1, \ldots, \theta_r)$.

Throughout this chapter, K is a field of characteristic zero and ζ_m is a primitive mth root of unity over K. All field extensions of K will be contained in some fixed algebraic closure of K. We note that the results of this chapter will not be used elsewhere in this thesis.

6.1. Cocycles and compatibility

The content of this section is folklore; cf. e.g. [9, §III.8], [79, §VII.5], [68, §11.1].

Compatible pairs. Let G_1 and G_2 be groups and let A_i be a G_i-module. A pair $(G_2 \xrightarrow{\lambda} G_1, A_1 \xrightarrow{\alpha} A_2)$ of group homomorphisms is **compatible** if α is a G_2-module homomorphism when G_2 acts on A_1 via γ. Such a compatible pair (λ, α) induces a homomorphism $\mathrm{Z}^2(G_1, A_1) \xrightarrow{\mathrm{Z}^2(\lambda,\alpha)} \mathrm{Z}^2(G_2, A_2)$ via $(g,h)(\phi.\,\mathrm{Z}^2(\lambda,\alpha)) = (g^\lambda, h^\lambda)\phi\alpha$ for $g, h \in G_2$.

Comparing group extensions. Let G be a group, A be a G-module, and let $0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be an extension of A by G. Let H be another group and let B be a H-module. Suppose that $G \xrightarrow{\lambda} H$ and $A \xrightarrow{\alpha} B$ are group isomorphisms such that α is a G-module isomorphism when G acts on B via λ. (In other words, λ^{-1} and α are compatible.) Given α and λ, we may regard E as an extension of the underlying abelian group of B by H by requiring the following diagram to be commutative

$$\begin{array}{ccccc} A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G \\ {\scriptstyle\alpha}\downarrow & & \| & & \downarrow{\scriptstyle\lambda} \\ B & \longrightarrow & E & \longrightarrow & H. \end{array}$$

The compatibility condition on α and λ implies that the induced H-action on B is the original one. That is, E is an extension of the H-module B by H.

The canonical extension

$$E(\phi)$$

associated with $\phi \in \mathrm{Z}^2(G, A)$ has $G \times A$ as its underlying set with multiplication $(g,a)(h,b) = (gh, a + b + (g,h)\phi)$ for $a, b \in A$ and $g, h \in G$. We will always assume that ϕ is **normalised**, i. e. $(g,1)\phi = (1,g)\phi = 0$ for all $g \in G$. Under this assumption, we may identify A with its image in $E(\phi)$ via $a \mapsto (1,a)$.

Comparing crossed products. Let L/K be a finite Galois extension. Write $\Gamma = \mathrm{Gal}(L/K)$ and let $\phi \in \mathrm{Z}^2(\Gamma, L^\times)$. Suppose that $L \xrightarrow{\theta} \tilde{L}$ is a K-isomorphism onto another field extension $\tilde{L}$ of K. Let $\tilde{\Gamma} = \mathrm{Gal}(\tilde{L}/K)$. We obtain induced isomorphisms $\tilde{\Gamma} \xrightarrow{\lambda} \Gamma$ and $L^\times \xrightarrow{\alpha} \tilde{L}^\times$, where $\gamma^\lambda = \theta\gamma\theta^{-1}$ for $\gamma \in \tilde{\Gamma}$ and α is the restriction of θ. Clearly, λ and α are compatible. Let $\tilde{\phi} = \phi.\,\mathrm{Z}^2(\lambda,\alpha)$. Then we obtain a canonical K-isomorphism $L \star_\phi \Gamma \to \tilde{L} \star_{\tilde{\phi}} \tilde{\Gamma}$ given by $u_{\gamma^\lambda} \cdot a \mapsto \tilde{u}_\gamma \cdot (a\theta)$ for $\gamma \in \tilde{\Gamma}$ and $a \in L$,

where $(u_\sigma)_{\sigma\in\Gamma}$ (resp. $(\tilde{u}_\gamma)_{\gamma\in\tilde{\Gamma}}$) denotes the canonical right L-basis (resp. $\tilde{L}$-basis) of the corresponding crossed product as in §5.2.

6.2. $\mathfrak{R}(m,r)$ and $\mathrm{A}(m,r)$

For the purposes of this chapter, the main abstract properties of homogeneous maximal abelian normal subgroups of finitely generated nilpotent linear groups are captured by the following.

6.1 Notation. Let G a group. We write $A \blacktriangleleft G$ if $A \triangleleft G$, $A = \mathrm{C}_G(A)$, A is finitely generated, $\mathrm{T}(A)$ is cyclic, and $[A,G] \leqslant \mathrm{T}(A)$.

6.2 Lemma. *Let G be a finitely generated nilpotent linear group over an arbitrary field. If $A \triangleleft G$ is maximal abelian and homogeneous, then $A \blacktriangleleft G$.*

Proof. Since G is polycyclic, A is finitely generated; see [51, §1.3]. As A is homogeneous, $\mathrm{T}(A)$ is cyclic. By Proposition 4.4(i), $A = \mathrm{C}_G(A)$. Corollary 5.4 shows that G is homogeneous and therefore completely reducible. Hence $[G,G]$ is finite by Theorem 2.4. Therefore, $[A,G] \leqslant A \cap \mathrm{T}(G) = \mathrm{T}(A)$. ♦

We will now investigate the structure of groups G with a given $A \blacktriangleleft G$. For $m \geqslant 1$ and $r \geqslant 0$, define $\mathrm{A}(m,r) = \mathbf{Z}/m \oplus \mathbf{Z}^r$. Further let

$$\mathfrak{R}(m,r) = \begin{bmatrix} (\mathbf{Z}/m)^\times & & & \\ \mathbf{Z}/m & 1 & & \\ \vdots & & \ddots & \\ \mathbf{Z}/m & & & 1 \end{bmatrix} \leqslant \mathrm{GL}_{r+1}(\mathbf{Z}/m).$$

Note that $\mathfrak{R}(m,r) = (\mathbf{Z}/m)^\times \ltimes (\mathbf{Z}/m)^r$ (natural action). The group $\mathfrak{R}(m,r)$ has a natural faithful action on $\mathrm{A}(m,r)$ by formal matrix multiplication:

$$(x_0,\ldots,x_r)\begin{bmatrix} a_0 & & & \\ a_1 & 1 & & \\ \vdots & & \ddots & \\ a_r & & & 1 \end{bmatrix} = (x_0a_0 + \cdots + x_ra_r, x_1, \ldots, x_r).$$

Clearly, if G is any group and $A \blacktriangleleft G$, then $A \cong \mathrm{A}(m,r)$, where $r = \mathrm{rank}(A)$ and $m = |\mathrm{T}(A)|$. By the following, the abstract groups G with $A \blacktriangleleft G$ are precisely the extensions of $\mathrm{A}(m,r)$ by subgroups of $\mathfrak{R}(m,r)$.

6.3 Proposition.

(i) Let G be a group and $A \blacktriangleleft G$. Let $A \xrightarrow{\alpha} \mathrm{A}(m,r)$ be an isomorphism. Then there exists an embedding $G/A \xrightarrow{\lambda} \mathfrak{R}(m,r)$ such that α is a G/A-module isomorphism when G/A acts on $\mathrm{A}(m,r)$ via λ. Therefore, G is as an extension of $\mathrm{A}(m,r)$ by a subgroup of $\mathfrak{R}(m,r)$.

(ii) Let $0 \to \mathrm{A}(m,r) \xrightarrow{\iota} G \to \Gamma \to 1$ *be an extension of* $\mathrm{A}(m,r)$ *by* $\Gamma \leqslant \mathfrak{R}(m,r)$. *Then* $\mathrm{Im}(\iota) \blacktriangleleft G$.

Proof.

(i) Let $e_0 = 1 + (m) \in \mathbf{Z}/m = \mathrm{T}(\mathrm{A}(m,r))$ and let $(e_1, \dots, e_r)$ be the standard basis of $\mathbf{Z}^r \leqslant \mathrm{A}(m,r)$ (embedded in the natural way). Denote by $f_0, \dots, f_r$ the preimages of $e_0, \dots, e_r$ under α. Write $\Gamma = G/A$ and let $\sigma \in \Gamma$. Then $f_0^\sigma = f_0^{x_0}$ and $f_i^\sigma = f_0^{x_i} \cdot f_i$ $(1 \leqslant i \leqslant r)$, where $x_i \in \mathbf{Z}/m$. Define

$$\sigma^\lambda = \begin{bmatrix} x_0 & & & \\ x_1 & 1 & & \\ \vdots & & \ddots & \\ x_r & & & 1 \end{bmatrix} \in \mathrm{M}_{r+1}(\mathbf{Z}/m).$$

A routine calculation shows that $(\sigma_1\sigma_2)^\lambda = \sigma_1^\lambda \sigma_2^\lambda$ for all $\sigma_1, \sigma_2 \in \Gamma$. Since Γ acts faithfully on $A = \langle f_0, \dots, f_r \rangle$, the map λ is injective. It follows that λ embeds Γ into $\mathfrak{R}(m,r)$. By construction, $(a^\sigma)\alpha = (a\alpha)\sigma^\lambda$ for all $a \in A$ and $\sigma \in \Gamma$. The final remark follows from compatibility as in §6.1.

(ii) Obvious. ♦

6.4 Corollary. *Let* G *be a group and* $A \blacktriangleleft G$.

(i) $A^{|\mathrm{T}(A)|} \leqslant \mathrm{Z}(G) = A^G$. *Hence,* $|G : A| \leqslant |G : \mathrm{Z}(G)| < \infty$ *and* $|G'| < \infty$.

(ii) G/A *is metabelian.*

Proof. We may assume that G is an extension of $\mathrm{A}(m,r)$ by $\Gamma \leqslant \mathfrak{R}(m,r)$. Clearly, Γ is metabelian. Since $m\,\mathrm{A}(m,r) = m\mathbf{Z}^r$ is a trivial $\mathfrak{R}(m,r)$-module, $m\,\mathrm{A}(m,r) \leqslant \mathrm{Z}(G)$. If $g \in G \setminus A$, then g has non-trivial action on $\mathrm{A}(m,r)$ whence $\mathrm{Z}(G) \leqslant \mathrm{A}(m,r)$. We therefore have $\mathrm{Z}(G) = \mathrm{A}(m,r)^\Gamma$. By a well-known result of Schur [68, 10.1.4], the finiteness of $G/\mathrm{Z}(G)$ implies that of $[G,G]$. ♦

6.3. Nilpotency and $\mathrm{R}(m,r)$

Given an extension G of $\mathrm{A}(m,r)$ by $\Gamma \leqslant \mathfrak{R}(m,r)$, we characterise nilpotency of G in terms of Γ. Together with the last section, this gives an answer to Question 1 from the beginning of the chapter. The following is well-known.

6.5 Lemma. *Let* R *be a commutative Artinian ring with Jacobson radical* $\mathrm{rad}(R)$. *Then the set* U *of unipotent elements in* R *is* $1 + \mathrm{rad}(R)$. *Moreover,* $U \leqslant R^\times$.

Proof. By [53, 28.F39], $\mathrm{rad}(R)$ is the set of nilpotent elements of R whence $U = 1 + \mathrm{rad}(R)$. It is well-known that U is a subgroup of $R^\times$ [85, p. 35]. ♦

We write $\mathrm{U}(m)$ for the group of unipotent elements in $\mathbf{Z}/m$.

6.6 Corollary. $\mathrm{U}(m) = \{x + (m) \in \mathbf{Z}/m : x \equiv 1 \bmod p \text{ for all primes } p \mid m\}$.

Proof. This follows since $\mathrm{rad}(\mathbf{Z}/m)$ is clearly generated by $\underline{m} + (m)$, where $\underline{m}$ is the product of the distinct prime divisors of m. ⧫

Let

$$\mathrm{R}(r,m) = \begin{bmatrix} \mathrm{U}(m) & & & \\ \mathbf{Z}/m & 1 & & \\ \vdots & & \ddots & \\ \mathbf{Z}/m & & & 1 \end{bmatrix} \leqslant \mathfrak{R}(r,m),$$

so $\mathrm{R}(r,m) = \mathrm{U}(m) \ltimes (\mathbf{Z}/m)^r$.

6.7 Lemma. *Let G be an extension of $\mathrm{A}(m,r)$ by $\Gamma \leqslant \mathfrak{R}(m,r)$. The following are equivalent:*

(i) G is nilpotent.

(ii) $\Gamma \leqslant \mathrm{R}(m,r)$.

(iii) Γ acts nilpotently on $\mathrm{A}(m,r)$.

Proof. Let $A = \mathrm{A}(m,r)$. By construction, $[A,\Gamma] \leqslant \mathrm{T}(A)$. We conclude that G is nilpotent if and only if (a) Γ is nilpotent and (b) Γ acts nilpotently on $\mathrm{T}(A) = \mathbf{Z}/m$. Note that (b) is equivalent to (iii).

For a matrix $\sigma \in \Gamma$, let $\sigma_0 \in (\mathbf{Z}/m)^\times$ be the image of σ under the homomorphism $\mathfrak{R}(m,r) \to (\mathbf{Z}/m)^\times$ which sends σ to its entry in position $(1,1)$. Let $\mathbf{Z}/m = \langle a \rangle$. Then $[a,\sigma] = -a + a\sigma = (\sigma_0 - 1)\cdot a$. Hence for $\sigma, \tau, \ldots \in \Gamma$, we have $[\ldots[[a,\sigma],\tau],\ldots] = (\sigma_0 - 1)(\tau_0 - 1)\cdots\cdot a$. By taking $\sigma = \tau = \ldots$, we see that if Γ acts nilpotently on $\mathrm{T}(A)$, then $\Gamma_0 = \{\sigma_0 : \sigma \in \Gamma\} \leqslant \mathrm{U}(m)$; this is clearly equivalent to $\Gamma \leqslant \mathrm{R}(m,r)$. We have proved (i)→(iii)↔(b)→(ii). Now Corollary 6.6 shows that $\mathrm{U}(m)$ indeed acts nilpotently on $\mathbf{Z}/m$. It follows that $\mathrm{R}(m,r)$ acts nilpotently on $\mathbf{Z}/m$ and on $(\mathbf{Z}/m)^r \lhd \mathrm{R}(m,r)$. Hence, $\mathrm{R}(m,r)$ is nilpotent and it acts nilpotently on A. This proves (ii)→(i). ⧫

In Lemma 6.10, we will obtain a field-theoretic interpretation of this result. In summary, the class of finitely generated nilpotent groups G with $\mathrm{A}(m,r) \cong A \blacktriangleleft G$ coincides with the class of extensions of $\mathrm{A}(m,r)$ by subgroups of $\mathrm{R}(m,r)$.

6.4. Field extensions: (m,r)-structures

Let $L = K(\zeta_m, \theta_1, \ldots, \theta_r)$ be an algebraic extension such that $\theta_i^m \in K^\times$ for $1 \leqslant i \leqslant r$. The different roots of $X^m - \theta_i^m$ are precisely given by $\theta_i \zeta_m^k$ $(0 \leqslant k < m)$. Hence, L is the (minimal) splitting field of $\{X^m - 1, X^m - \theta_1^m, \ldots, X^m - \theta_r^m\}$ over K whence L/K is Galois.

Let $\sigma \in \mathrm{Gal}(L/K)$. Then $\zeta_m^\sigma = \zeta_m^{x_0}$ for a unique $x_0 \in (\mathbf{Z}/m)^\times$. Moreover, for $1 \leqslant i \leqslant r$, we have $(\theta_i^\sigma/\theta_i)^m = (\theta_i^m)^\sigma/\theta_i^m = 1$ and thus $\theta_i^\sigma = \theta_i \zeta_m^{x_i}$ for a unique

$x_i \in \mathbf{Z}/m$. A routine computation shows that the map $\mathrm{Gal}(L/K) \xrightarrow{\lambda} \mathfrak{R}(m,r)$ defined by

$$\sigma^\lambda = \begin{bmatrix} x_0 & & & \\ x_1 & 1 & & \\ \vdots & & \ddots & \\ x_r & & & 1 \end{bmatrix}$$

is an embedding. Moreover, if $\mathrm{A}(m,r) \xrightarrow{\alpha} \!\!\!\rightarrow \langle \zeta_m, \theta_1, \ldots, \theta_r \rangle \leqslant L^\times$ denotes the evident epimorphism, then λ and α are compatible, i. e. α is $\mathrm{Gal}(L/K)$-equivariant when $\mathrm{Gal}(L/K)$ acts on $\mathrm{A}(m,r)$ via λ. Note that α restricts to an injection on the torsion subgroup of $\mathrm{A}(m,r)$, i.e. $\mathrm{Ker}(\alpha)$ is torsion-free.

6.8 Definition. An (m,r)**-structure** over K is a triple $(L/K, \lambda, \alpha)$, where

(i) L/K is a Galois extension,

(ii) $\mathrm{Gal}(L/K) \xrightarrow{\lambda} \Gamma$ is an isomorphism onto a subgroup $\Gamma \leqslant \mathfrak{R}(m,r)$, and

(iii) $\mathrm{A}(m,r) \xrightarrow{\alpha} L^\times$ is a homomorphism such that (a) λ and α are compatible, (b) $\mathrm{Ker}(\alpha)$ is torsion-free, and (c) $L = K[\mathrm{Im}(\alpha)]$.

Below, (m,r)-structures will naturally arise from certain linear representations of extensions of $\mathrm{A}(m,r)$ by subgroups of $\mathfrak{R}(m,r)$.

6.9 Lemma. *Let* $\left(L/K, \mathrm{Gal}(L/K) \xrightarrow{\lambda} \Gamma, \mathrm{A}(m,r) \xrightarrow{\alpha} L^\times\right)$ *be an* (m,r)*-structure over* K*. Let* $(e_1, \ldots, e_r)$ *be a* $\mathbf{Z}$*-basis of the right summand in* $\mathrm{A}(m,r) = \mathbf{Z}/m \oplus \mathbf{Z}^r$*. Define* $\theta_i = e_i\alpha \in L^\times$ *for* $1 \leqslant i \leqslant r$*. Then* $\theta_i^m \in K^\times$ *and* $L = K(\zeta_m, \theta_1, \ldots, \theta_r)$*.*

Proof. We have $m \cdot e_i \in \mathrm{A}(m,r)^\Gamma$ whence $\theta_i^m \in L^{\mathrm{Gal}(L/K)} = K$. ♦

Hence, an (m,r)-structure over K essentially amounts to a sequence $\theta_1, \ldots, \theta_r$ as above together with a choice of a primitive mth root of unity over K. The field-theoretic role of the subgroup $\mathrm{R}(m,r)$ of $\mathfrak{R}(m,r)$ is explained by the following.

6.10 Lemma. *Let* $(L/K, \lambda, \alpha)$ *be an* (m,r)*-structure over* K*. Then the following are equivalent.*

(i) $\mathrm{Im}(\lambda) \leqslant \mathrm{R}(m,r)$*.*

(ii) $\zeta_p \in K$ *for all primes* $p \mid m$*.*

(iii) $\mathrm{Gal}(\mathbf{E}_m K/K) \leqslant (\mathbf{Z}/m)^\times$ *is unipotent (i.e. it is a subgroup of* $\mathrm{U}(m)$*).*

Proof.

(i)↔(ii) We identify $\Gamma = \mathrm{Im}(\lambda)$ and $\mathrm{Gal}(L/K)$ via λ. Let $A = \mathrm{Im}(\alpha)$ so that α induces a Γ-equivariant epimorphism from $\mathrm{A}(m,r)$ onto A. Since $\mathrm{Ker}(\alpha)$ is torsion-free, α maps the torsion-subgroup $\mathbf{Z}/m$ of $\mathrm{A}(m,r)$ isomorphically onto $\langle\zeta_m\rangle \leqslant L^\times$.

We again denote the product of the distinct prime divisors of m by $\underline{m}$. Let $\sigma \in \Gamma$ and let $\sigma_0 \in (\mathbf{Z}/m)^\times$ be the entry in position $(1,1)$ of σ. Then $\zeta_m^\sigma = \zeta_m^{\sigma_0}$. Now $\sigma \in \mathrm{R}(m,r)$ if and only if $\sigma_0 \in \mathrm{U}(m)$ which by Corollary 6.6 is equivalent to $\sigma_0 \equiv 1 \bmod \underline{m}$. Writing $k = m/\underline{m}$, the last condition is obviously equivalent to $\sigma_0 k \equiv k \bmod m$ and thus to $(\zeta_m^k)^\sigma = \zeta_m^k$. It follows that $\Gamma \leqslant \mathrm{R}(m,r)$ is equivalent to $\zeta_m^k \in K$ and thus to $\zeta_{\underline{m}} \in K$.

(ii)↔(iii) Immediate, since the map $\sigma \mapsto \sigma_0$ from the last step of the proof is exactly the surjective restriction homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\mathbf{E}_m K/K)$. ♦

6.11 Remark. Let $(L/K,\lambda,\alpha)$ be an (m,r)-structure over K which satisfies one of the conditions in the last lemma. Using the expression of L in terms of radicals in Lemma 6.9, it follows that L/K is a special case of a so-called "quasi-Kummer extension"; see [1, §§1D.5–6] for results on such extensions.

A proper field-theoretic study of (m,r)-structures is beyond the scope of this thesis. We contend ourselves with the following elementary existence result.

6.12 Proposition. *Let $\Gamma \leqslant \mathfrak{R}(m,r)$, Then there exists a number field K and an (m,r)-structure $(L/K,\lambda,\alpha)$ over K with $\mathrm{Im}(\lambda) = \Gamma$. Moreover, we may assume that α is injective.*

Proof. Suppose that $(L/K,\lambda,\alpha)$ is an (m,r)-structure over K with $\mathrm{Im}(\lambda) = \mathfrak{R}(m,r)$ and such that α is injective. Define K' to be the fixed field of $\Gamma\lambda^{-1}$ and λ' to be the restriction of λ to $\Gamma\lambda^{-1} = \mathrm{Gal}(L/K')$. Then $(L/K',\lambda',\alpha)$ is an (m,r)-structure of the desired form. It thus suffices to consider the case $\Gamma = \mathfrak{R}(m,r)$. We inductively define number fields L_i as follows. Let $L_0 = \mathbf{Q}(\zeta_m)$. For $i \geqslant 1$, let p_i be a rational prime which does not divide the discriminant of $L_{i-1}/\mathbf{Q}$ and define $L_i = L_{i-1}(\theta_i)$, where $\theta_i = \sqrt[m]{p_i}$. Since p_i is unramified in L_{i-1}, we see that $X^m - p_i$ is an Eisenstein polynomial over any p_i-adic completion of L_{i-1}. Hence, $|L_i : L_{i-1}| = m$. Let $L = L_r = \mathbf{Q}(\zeta_m,\theta_1,\ldots,\theta_r)$. Using the introductory remarks from this section, we obtain an (m,r)-structure $(L/\mathbf{Q},\lambda,\alpha)$. By construction, $|L : \mathbf{Q}| = \varphi(m)m^r = |\mathfrak{R}(m,r)|$ whence λ maps $\mathrm{Gal}(L/K)$ isomorphically onto $\mathfrak{R}(m,r)$.

It remains to show that α is injective. Let $x_0,\ldots,x_r \in \mathbf{Z}$ satisfy $\zeta_m^{x_0}\theta_1^{x_1}\cdots\theta_r^{x_r} = 1$. By taking mth powers, we obtain $p_1^{x_1}\cdots p_r^{x_r} = 1$. Now by construction, the p_i are all distinct. Since we have unique factorisation in $\mathbf{Z}$, we conclude that $x_1 = \ldots = x_r = 0$. Hence, $m \mid x_0$ and α is injective. ♦

6.5. Representations, (m,r)-structures, and algebras

In this rather technical section, we study the relationship between representations of groups and (m,r)-structures over a given field. This will allow us to give answers to Questions 2–3 from p. 47.

For the remainder of this section, we fix a field K of characteristic zero, a subgroup $\Gamma \leqslant \mathfrak{R}(m,r)$, and a normalised cocycle $\phi \in \mathrm{Z}^2(\Gamma, A)$, where $A = \mathrm{A}(m,r)$. Further, let $G = E(\phi)$. We identify A with the subgroup $\{(1_\Gamma, a) : a \in A\}$ of G. Let $(t_\sigma)_{\sigma\in\Gamma}$ be the canonical transversal of A in G, i. e. $t_\sigma = (\sigma, 0)$. If ϱ is a K-representation of a group, then we write $K[\varrho]$ for the enveloping algebra of the image of ϱ.

Classes of representations, (m,r)-structures, and algebras

Our investigations in this section are based on the interplay between the following three classes.

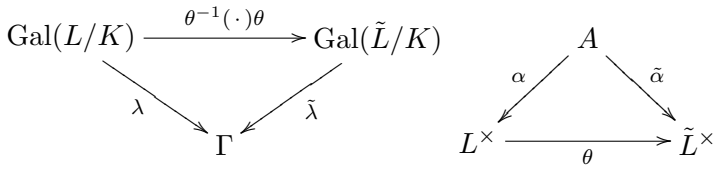
6.13 Notation.

(i) Define $\mathfrak{D}$ to be the class of K-representations ϱ of G such that A^ϱ is homogeneous, $\mathrm{Ker}(\varrho)$ is torsion-free, $\mathrm{Ker}(\varrho) \leqslant A$, and $\mathrm{Z}(K[\varrho]) = K$.

(ii) Define $\mathfrak{E}$ to be the class of (m,r)-structures $\left(L/K, \mathrm{Gal}(L/K) \xrightarrow{\lambda} \Gamma, A \xrightarrow{\alpha} L^\times\right)$; note that we require $\mathrm{Im}(\lambda) = \Gamma$.

(iii) Define $\mathfrak{A}$ to be the class of central simple finite-dimensional K-algebras.

There are natural equivalence relations (which we all denote by $\approx$) on these classes: For $\mathfrak{D}$, we let $\approx$ be equivalence of K-representations, while for $\mathfrak{A}$ we take isomorphism of K-algebras. Let $E = (L/K, \lambda, \alpha) \in \mathfrak{E}$ and $\tilde{E} = (\tilde{L}/K, \tilde{\lambda}, \tilde{\alpha}) \in \mathfrak{E}$. Then $E \approx \tilde{E}$ if and only if there exists a K-isomorphism $L \xrightarrow{\theta} \tilde{L}$ such that the diagrams



commute.

Ignoring set-theoretic difficulties which can be overcome ("classes of classes"), we write $\mathfrak{X}/\approx$ for the "quotient class" of $\mathfrak{X} = \mathfrak{D}, \mathfrak{E}, \mathfrak{A}$ with respect to the equivalence relation just defined.

From representations to field extensions

We describe a canonical way of extracting an (m,r)-structure in $\mathfrak{E}$ from a representation in $\mathfrak{D}$.

6.14 Proposition. *Let $\varrho \in \mathfrak{D}$.*

(i) Let $L = K[A^\varrho]$. Define $\Gamma \xrightarrow{\mu} \mathrm{Gal}(L/K)$ as follows: σ^μ ($\sigma \in \Gamma$) is conjugation by t_σ^ϱ. Then μ is an isomorphism.

(ii) Let $A \xrightarrow{\alpha} L^\times$ be the restriction of ϱ. Then $(L/K, \mu^{-1}, \alpha) \in \mathfrak{E}$.

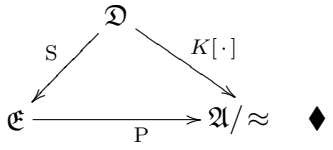
(iii) *Let* $\tilde{\phi} = \phi.\,\mathrm{Z}^2(\mu^{-1},\alpha) \in \mathrm{Z}^2(\mathrm{Gal}(L/K), L^\times)$. *Then there is a* K*-algebra isomorphism* $K[\varrho] \xrightarrow{\xi} L\star_{\tilde{\phi}}\mathrm{Gal}(L/K)$ *such that the composite* $G \xrightarrow{\varrho\xi} L\star_{\tilde{\phi}}\mathrm{Gal}(L/K)$ *is given by* $(\sigma,a)\mapsto u_{\sigma\mu}\cdot(a\alpha)$.

Proof. By Corollary 6.4, $[G,G]$ is finite. Let $N = \mathrm{Ker}(\varrho)$. Suppose that $x \in G$ centralises A modulo N. Then $[A,x] \subset N \cap [G,G] = 1$ whence $x \in \mathrm{C}_G(A) = A$. It follows that A^ϱ is self-centralising in G^ϱ. Since $N \leqslant A$, we obtain a ϱ-induced isomorphism $G/A \cong G^\varrho/A^\varrho$. Hence, we may regard G^ϱ as an extension of A^ϱ by Γ; we see that $\sigma \mapsto t^\varrho_\sigma$ is a normalised section for this extension. Parts (i) and (iii) now follow from §5.2 (note that $\mathrm{Z}(K[\varrho]) = K$),. while (ii) holds by construction. ♦

Maps, part I

Let $\mathfrak{D} \xrightarrow{\mathrm{S}} \mathfrak{E}$ be the map which sends $\varrho \in \mathfrak{D}$ to the (m,r)-structure in part (ii) of Proposition 6.14. Part (iii) shows that we may regard $K[\,\cdot\,]\colon \varrho \mapsto K[\varrho]$ as a map $\mathfrak{D} \to \mathfrak{A}$. Finally, let $\mathfrak{E} \xrightarrow{\mathrm{P}} \mathfrak{A}$ take an (m,r)-structure $(L/K,\lambda,\alpha) \in \mathfrak{E}$ to the crossed product $L\star_{\tilde{\phi}}\mathrm{Gal}(L/K)$, where $\tilde{\phi} = \phi.\,\mathrm{Z}^2(\lambda,\alpha)$. The following is immediate from Proposition 6.14(iii).

6.15 Corollary. *The following diagram commutes.*



♦

From field extensions to representations

For a given (m,r)-structure $E \in \mathfrak{E}$, we construct a representation $\varrho \in \mathfrak{D}$ such that, among other things, the (m,r)-structure $\varrho.\,\mathrm{S}$ extracted from ϱ (as defined above) is equivalent to E.

6.16 Proposition. *Let* $(L/K,\lambda,\alpha) \in \mathfrak{E}$.

(i) *Regard* α *as a linear* L*-representation of* A *and let* $\varrho = \alpha\uparrow_A^G$ *be the induced representation. If we regard* ϱ *as a* K*-representation, then* $\varrho \in \mathfrak{D}$.

(ii) *Let* $\tilde{\phi} = \phi.\,\mathrm{Z}^2(\lambda,\alpha) \in \mathrm{Z}^2(\mathrm{Gal}(L/K), L^\times)$. *Then there is a* K*-algebra isomorphism* $K[\varrho] \xrightarrow{\xi} L\star_{\tilde{\phi}}\mathrm{Gal}(L/K)$ *such that the composite* $G \xrightarrow{\varrho\xi} L\star_{\tilde{\phi}}\mathrm{Gal}(L/K)$ *is given by* $(\sigma,a)\mapsto u_{\sigma\lambda^{-1}}\cdot(a\alpha)$.

(iii) $\varrho.\,\mathrm{S}$ *is equivalent to* $(L/K,\lambda,\alpha)$.

(iv) *The natural* $K[\varrho]$*-module is the regular one.*

Proof.

- As is well-known [43, p. 215], $\mathrm{Ker}(\varrho) = \bigcap_{g\in G} \mathrm{Ker}(\alpha)^g = \bigcap_{\sigma\in\Gamma} \mathrm{Ker}(\alpha)\sigma$. Since λ and α are compatible, $\mathrm{Ker}(\alpha)$ is Γ-invariant so that $\mathrm{Ker}(\alpha) = \mathrm{Ker}(\varrho)$.

- We first consider ϱ as an L-representation of G; see [68, p. 238] for background on induced representations. The natural LG-module associated with ϱ is given by $V = \bigoplus_{\sigma\in\Gamma} L\otimes t_\sigma$, the action being the evident one. We regard ϱ as a matrix representation with respect to the L-basis $(1_L \otimes t_\sigma)_{\sigma\in\Gamma}$ of V. We see that if $a \in A$, then $a^\varrho = \mathrm{diag}\left((a\sigma^{-1})\alpha\right)_{\sigma\in\Gamma}$; that is, a^ϱ is the diagonal matrix with entry $(a\sigma^{-1})\alpha$ in position (σ,σ). It follows from compatibility of λ and α that $(a\sigma^{-1})\alpha = (a\alpha)^{\sigma^{-1}\lambda^{-1}}$.

- Let $\tilde{L} = K[A^\varrho]$. As $\mathrm{Ker}(\alpha) = \mathrm{Ker}(\varrho)$, the rule $x \mapsto \mathrm{diag}\left(x^{\sigma^{-1}\lambda^{-1}}\right)_{\sigma\in\Gamma}$ yields an isomorphism $A\alpha \to A^\varrho$. Since $L = K[A\alpha]$, we may extend this map to a K-epimorphism $L \xrightarrow{\theta} \tilde{L}$ (given by the same rule). Now L is a field so that θ is an isomorphism. Note that by construction, $a\alpha\theta = a^\varrho$ for $a \in A$.

- As in the proof of Proposition 6.14, we see that (a) A^ϱ coincides with its own centraliser in G^ϱ and (b) we obtain a ϱ-induced isomorphism $G^\varrho/A^\varrho \cong \Gamma$. The map $\Gamma \to G^\varrho, \sigma \mapsto t_\sigma^\varrho$ is a normalised section of the composite $G^\varrho \xrightarrow{\text{proj.}} G^\varrho/A^\varrho \xrightarrow{\cong} \Gamma$. We may thus regard G^ϱ as an extension of A^ϱ by Γ. Clearly, the corresponding cocycle is simply $\phi.\,\mathrm{Z}^2(\Gamma, A \xrightarrow{\varrho} A^\varrho)$.

  The induced action of Γ on A^ϱ is as follows: for $a \in A$ and $\sigma \in \Gamma$, we have $(a\alpha\theta)^\sigma = (a^\varrho)^\sigma = (t_\sigma^\varrho)^{-1} a^\varrho t_\sigma^\varrho = (t_\sigma^{-1} a t_\sigma)^\varrho = (a\sigma)^\varrho = (a\sigma)\alpha\theta = (a\alpha)^{\sigma\lambda^{-1}}\theta$. Hence, the action of Γ on A^ϱ is the restriction of the unique Γ-action on $\tilde{L}$ such that θ is Γ-equivariant when Γ acts on L via λ^{-1}.

- Since θ is a K-isomorphism, the above action of Γ on $\tilde{L}$ gives an isomorphism $\Gamma \xrightarrow{\mu} \mathrm{Gal}(\tilde{L}/K)$; also, using §5.2, we obtain an explicit K-isomorphism between $K[\varrho]$ and $\tilde{L} \star_\psi \mathrm{Gal}(\tilde{L}/K)$, where $\psi = \phi.\,\mathrm{Z}^2(\mu^{-1}, A \xrightarrow{\varrho} \tilde{L}^\times)$. Using the last step, we obtain commutative diagrams

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & L^\times \\ & {\scriptstyle\varrho}\searrow & \downarrow{\scriptstyle\theta} \\ & & \tilde{L}^\times \end{array} \qquad \begin{array}{ccc} \mathrm{Gal}(\tilde{L}/K) & \xrightarrow{\mu^{-1}} & \Gamma \\ {\scriptstyle\theta(\,\cdot\,)\theta^{-1}}\downarrow & \nearrow{\scriptstyle\lambda} & \\ \mathrm{Gal}(L/K) & & \end{array}$$

  Together with §6.1, we obtain an explicit K-isomorphism $\tilde{L} \star_\psi \mathrm{Gal}(\tilde{L}/K) \cong L \star_{\tilde{\phi}} \mathrm{Gal}(L/K)$, where $\tilde{\phi} = \phi.\,\mathrm{Z}^2(\lambda, \alpha)$. This proves (ii).

- Part (i) now follows immediately: A^ϱ is homogeneous since $\tilde{L} \cong_K L$ is a field, $\mathrm{Ker}(\varrho) = \mathrm{Ker}(\alpha)$ is torsion-free, and $\mathrm{Z}(K[\varrho]) = K$ follows from the preceding crossed product description. We also see that θ furnishes an equivalence between $(L/K, \lambda, \alpha)$ and $\varrho.\,\mathrm{S} = (\tilde{L}/K, \mu^{-1}, A \xrightarrow{\varrho} \tilde{L}^\times)$, which proves (iii).

- For the final statement, we once again regard ϱ as an L-representation. We see that t_σ^ϱ ($\sigma \in \Gamma$) is a monomial matrix whose non-zero entry in row $\tau \in \Gamma$ is in column $\tau\sigma$. Let e be a unit vector in V (the natural LG-module for ϱ). We conclude that $V = e \cdot LG$. By the above description of A^ϱ and $\tilde{L}$, we see that the diagonal entries of elements in $\tilde{L}$ exhaust all of L. Thus, $e \cdot L1_G = e \cdot \tilde{L}$. Hence, $e \cdot LG = e \cdot KG = e \cdot K[\varrho]$. Since $|V : K| = |\Gamma||L : K| = |K[\varrho] : K|$, part (iv) follows. ♦

Question 2: existence of representations

We are now in a position to give an affirmative answer to Question 2 from p. 47.

6.17 Corollary. *Let G be a group and $A \blacktriangleleft G$. Then there exists a faithful representation ϱ of G over some number field K such that A^ϱ is homogeneous.*

Proof. We may assume that $G = E(\phi)$, where $\phi \in \mathrm{Z}^2(\Gamma, A)$, $A = \mathrm{A}(m,r)$ and $\Gamma \leqslant \mathfrak{R}(m,r)$. Using Proposition 6.12, we find an (m,r)-structure $E = (L/K, \lambda, \alpha)$ over a number field K such that $\mathrm{Im}(\lambda) = \Gamma$ and α is injective. Now take $\varrho = \alpha \uparrow_A^G$, regarded as a K-representation, and apply Proposition 6.16(i). ♦

6.18 Remark. Since G is polycyclic by Corollary 6.4, there exists a faithful $\mathbf{Z}$-linear representation of G by the Auslander-Swan theorem [51, 3.3.1]. The point of Corollary 6.17 is that A acts homogeneously.

6.19 Example. We may use Proposition 6.16 to reinterpret the ad hoc construction of a nilpotent linear group whose enveloping algebra is a cyclic algebra from §5.3.

Consider the extension of $\mathrm{A}(m,2)$ by $\Gamma = \left\langle \begin{bmatrix} 1 & & \\ 1 & 1 & \\ \cdot & \cdot & 1 \end{bmatrix} \right\rangle \leqslant \mathrm{R}(m,2)$ given by

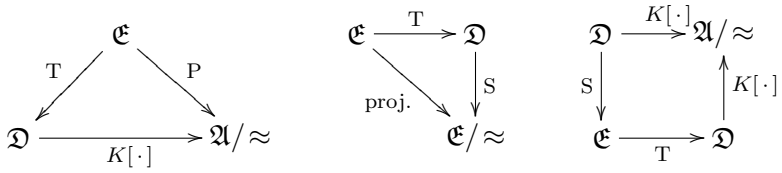
$$G = \Big\langle e_0, e_1, e_2, g \;\Big|\; e_0^m = 1,\ [e_1, g] = e_0,\ g^m = e_2,\ [e_0, e_1] = [e_0, e_2] = [e_1, e_2] = [e_0, g] = [e_2, g] = 1 \Big\rangle;$$

here $\mathrm{A}(m,2)$ is embedded into G via $(x_0, x_1, x_2) \mapsto e_0^{x_0} e_1^{x_1} e_2^{x_2}$. By setting $u = e_1$ and rewriting relations using $e_0 = [u, g]$ and $e_2 = g^m$, we see that G is the group $H(m)$ from §5.3. Suppose that $\zeta_m \in K$ and let $\lambda, \nu \in K^\times$, where $X^m - \nu$ is irreducible over K. Let $\beta = \sqrt[m]{\nu}$ and $L = K(\beta)$. Define $\alpha\colon \mathrm{A}(m,2) \to L^\times$, $(x_0, x_1, x_2) \mapsto \zeta_m^{x_0} \beta^{x_1} \lambda^{x_2}$. Let $\sigma \in \mathrm{Gal}(L/K)$ be the generator $\beta \mapsto \beta \cdot \zeta_m$. Define an isomorphism $\mathrm{Gal}(L/K) \to \Gamma$ via $\sigma \mapsto \begin{bmatrix} 1 & & \\ 1 & 1 & \\ \cdot & \cdot & 1 \end{bmatrix}$. Then $E = (L/K, \lambda, \alpha)$ is an (m,r)-structure over K. We see that if ϱ is the representation of G associated with E as in Proposition 6.16(i), then G^ϱ is the group H from §5.3.

Maps, part II

Let $\mathfrak{E} \xrightarrow{\mathrm{T}} \mathfrak{D}$ be the map which sends $(L/K, \lambda, \alpha) \in \mathfrak{E}$ to the K-restriction of the L-induced representation $\alpha \uparrow_A^G$.

6.20 Corollary. *The following diagrams commute.*



Proof. Commutativity of the first two diagrams follows from Proposition 6.16(ii)–(iii). For the third diagram, use Corollary 6.15 and the first diagram here. ⧫

6.21 Lemma. *The maps* S, T, P, *and* $K[\,\cdot\,]$ *preserve the equivalence relations defined above.*

Proof. We only define the (canonical) maps establishing the respective equivalences and omit the easy but tedious verifications that these maps do indeed yield equivalences. For P, the claim follows from §6.1. Let $\varrho_1, \varrho_2 \in \mathfrak{D}$ be equivalent. Denote the KG-module corresponding to ϱ_i by V_i. Then there exists a KG-module isomorphism $V_1 \xrightarrow{\gamma} V_2$. We obtain a K-algebra isomorphism $K[\varrho_1] \xrightarrow{\theta} K[\varrho_2]$ given by $x\theta = \gamma^{-1}x\gamma$. This proves $K[\varrho_1] \cong K[\varrho_2]$. Furthermore, θ restricts to an isomorphism $K[A^{\varrho_1}] \to K[A^{\varrho_2}]$ and this map is readily seen to establish the equivalence of $\varrho_1.\mathrm{S}$ and $\varrho_2.\mathrm{S}$. Let $E = (L/K, \lambda, \alpha) \in \mathfrak{E}$ and $\tilde{E} = (\tilde{L}/K, \tilde{\lambda}, \tilde{\alpha}) \in \mathfrak{E}$ and suppose that $L \xrightarrow{\theta} \tilde{L}$ furnishes an equivalence between these (m, r)-structures. Using the explicit matrix constructions in the proof of Proposition 6.16, we may identify the natural modules V and $\tilde{V}$ for $E.\mathrm{T}$ and $\tilde{E}.\mathrm{T}$ with $L^{|\Gamma|}$ and $\tilde{L}^{|\Gamma|}$, respectively. It is readily checked that θ induces a KG-isomorphism $V \to \tilde{V}$ in its natural action on entries. This proves that $E.\mathrm{T}$ and $\tilde{E}.\mathrm{T}$ are equivalent. ⧫

Question 3: the 1–1 correspondence

We have seen that, up to equivalence, every (m, r)-structure in $\mathfrak{E}$ arises from a representation in $\mathfrak{D}$. However, an (m, r)-structure $E \in \mathfrak{E}$ does not uniquely determine a representation ϱ in $\mathfrak{D}$. We will now see that if we restrict attention to *irreducible* representations in $\mathfrak{D}$, then we do indeed obtain bijections on equivalence classes. This will provide an answer to Question 3 from p. 47.

6.22 Lemma.

(i) Let $\varrho \in \mathfrak{D}$ and $n \geqslant 1$. Then $n \cdot \varrho = \varrho \oplus \cdots \oplus \varrho \in \mathfrak{D}$ (n times) and $\varrho.\mathrm{S} \approx (n \cdot \varrho).\mathrm{S}$.

(ii) Let $\varrho \in \mathfrak{D}$ and let π be an irreducible subrepresentation of ϱ. Then $\pi \in \mathfrak{D}$ and $\varrho.\mathrm{S} \approx \pi.\mathrm{S}$. ⧫

Let $\mathfrak{D}_0 \subset \mathfrak{D}$ be the class of irreducible representations in $\mathfrak{D}$. Then T induces a map $\mathrm{T}_0\colon \mathfrak{E} \to \mathfrak{D}_0$ which sends an (m, r)-structure $E \in \mathfrak{E}$ to an irreducible constituent of $E.\mathrm{T}$; note that the irreducible constituents of $E.\mathrm{T}$ are all equivalent.

6.23 Proposition. *The maps* S *and* T_0 *induce mutually inverse bijections between* $\mathfrak{D}_0/\approx$ *and* $\mathfrak{E}/\approx$.

Our proof of Proposition 6.23 below relies on the following simple observation.

6.24 Lemma. *Let* $H \xrightarrow{\varrho} \mathrm{GL}(V)$ *and* $H \xrightarrow{\pi} \mathrm{GL}(W)$ *be* K*-representations of a group* H. *Let* $K[\varrho] \xrightarrow{\theta} K[\pi]$ *be an isomorphism of* K*-algebras such that* $\varrho\theta = \pi$. *Suppose that* ϱ *is irreducible. Then* π *is equivalent to a multiple of* ϱ.

Proof. We have $(xh^\varrho)\theta = (x\theta)h^\pi$ $(x \in K[\varrho], h \in H)$ whence θ is a KH-module isomorphism. Also, $K[\varrho]$ (and hence also $K[\pi]$) is simple by irreducibility of ϱ.

It is well-known (cf. [66, §3.3]) that V is $K[\varrho]$-isomorphic (hence KH-isomorphic) to a minimal right ideal, $\mathfrak{a}$ say, of $K[\varrho]$. Hence, $V \cong_{KH} \mathfrak{a} \cong_{KH} \mathfrak{a}\theta \leqslant_{KH} K[\pi]$. It follows that the essentially unique irreducible $K[\pi]$-module is KH-isomorphic to V. The claim follows since W is a homogeneous KH-module by simplicity of $K[\pi]$. ♦

Proof of Proposition 6.23. We freely use Lemma 6.21. If $E \in \mathfrak{E}$, then Lemma 6.22 and Corollary 6.20 (middle diagram) give $E.\,\mathrm{T}_0\,\mathrm{S} \approx E.\,\mathrm{T}\,\mathrm{S} \approx E$. Now let $\varrho \in \mathfrak{D}_0$. Write $(L/K, \lambda, \alpha) = \varrho.\,\mathrm{S}$ and let $\tilde{\phi} = \phi.\,\mathrm{Z}^2(\lambda, \alpha)$. Define $\pi = \varrho.\,\mathrm{S}\,\mathrm{T}$. Using Propositions 6.14 and 6.16, we obtain K-isomorphisms $K[\varrho] \cong L \star_{\tilde{\phi}} \mathrm{Gal}(L/K) \cong K[\pi]$ such that the two triangles in the diagram

$$\begin{array}{ccc} G & \xrightarrow{\quad\pi\quad} & K[\pi] \\ {\scriptstyle\varrho}\downarrow & \searrow & \downarrow{\scriptstyle\cong} \\ K[\varrho] & \xrightarrow[\cong]{} & L \star_{\tilde{\phi}} \mathrm{Gal}(L/K) \end{array}$$

commute, where the diagonal map is $(\sigma, a) \mapsto u_{\sigma\lambda^{-1}} \cdot (a\alpha)$. Lemma 6.24 now shows that ϱ is equivalent to an irreducible constituent of $\pi = \varrho.\,\mathrm{S}\,\mathrm{T}$. Thus, $\varrho \approx \varrho.\,\mathrm{S}\,\mathrm{T}_0$. ♦

Returning to Question 3 from p. 47, let G be an extension of $A = \mathrm{A}(m,r)$ by a subgroup Γ of $\mathrm{R}(m,r)$. We have obtained a natural bijection between (i) equivalence classes of faithful irreducible K-representations ϱ of G such that A^ϱ is homogeneous and $\mathrm{Z}(K[\varrho]) = K$ and (ii) equivalence classes of (m,r)-structures $(L/K, \lambda, \alpha)$ over K such that α is injective and $\mathrm{Im}(\lambda) = \Gamma$. Moreover, if π is a faithful K-representation of G such that A^π is homogeneous and $\mathrm{Z}(K[\varrho]) = K$, then π is a multiple of an irreducible faithful representation arising from an (m,r)-structure over K.

Part II.

Irreducibility and primitivity testing of finite nilpotent linear groups

7. Abstract ANC groups

Let K have characteristic zero and let $A \leqslant \mathrm{GL}(V)$ be a homogeneous finite abelian group. It is easy to see that A is then cyclic. Indeed, A is a subgroup of the multiplicative group of the field $K[A]$. As a known consequence, if $G \leqslant \mathrm{GL}(V)$ is a finite group and $A \triangleleft G$ is non-cyclic abelian, then A is inhomogeneous and G admits a non-trivial system of imprimitivity by Clifford's theorem (Theorem 1.10). Moreover, Corollary 1.12 applies in this situation. We can therefore either conclude that G is reducible or irreducibility of G is equivalent to that of another group, acting in smaller dimension. For the purpose of irreducibility testing of G we may thus proceed as in the "reduction step" of Algorithm 5.1 (see p. 44).

In this chapter, we show that we may always either (i) construct a non-cyclic abelian normal subgroup of a finite nilpotent group $G \leqslant \mathrm{GL}(V)$ or (ii) we can prove that no such subgroup exists. The latter situation then serves as a base case for irreducibility and primitivity testing of G, in the same way that the "crossed product case" (see p. 44) was a base case for deciding irreducibility of possibly infinite nilpotent linear groups. Using the well-understood structure of finite nilpotent groups without non-cyclic abelian normal subgroups, in the following chapters, we will then proceed further with constructive irreducibility and primitivity testing.

This chapter is based on [74, §§4,5.3].

7.1. Fundamental properties

We call a finite nilpotent group all of whose abelian normal subgroups are cyclic an **ANC group**. Denote by D_{2^k}, SD_{2^k}, and Q_{2^k} the dihedral, semidihedral, and generalised quaternion group of order 2^k, respectively. For a finite nilpotent group H, denote by H_p and $H_{p'}$ the Sylow p-subgroup and p-complement of H, respectively. The following is a classification of ANC groups.

7.1 Theorem ([73, Lem. 3])**.** *Let G be a finite nilpotent group. Then G is an ANC group if and only if*

(i) G_2 is cyclic or isomorphic to Q_8 or to D_{2^k}, SD_{2^k}, or Q_{2^k} ($k \geqslant 4$), and

(ii) $G_{2'}$ is cyclic.

We will now consider the problem of recognising if a finite nilpotent group is an ANC group. The following is essentially [21, Lem. 3.6]. The new proof we give for the "only if" part will lead to a very simple algorithm below.

7.2 Proposition. *Let G be a finite nilpotent group such that $[G,G]$ is cyclic. Write $H = \mathrm{C}_G([G,G])$. Then G is an ANC group if and only if*

(i) H_2 is cyclic or $H_2 \cong \mathrm{Q}_8$, and

(ii) $H_{2'}$ is cyclic.

Proof. Observe that $[G,G] \leqslant \mathrm{Z}(H)$; in particular, H has nilpotency class at most 2.

We first show that conditions (i) and (ii) are sufficient for G to be an ANC group. By [21, Lem. 3.6(ii)], if H_p is cyclic for some p, then G_p is either cyclic or $p = 2$, $|G_2| > 8$, and G_2 is dihedral, semidihedral, or generalised quaternion. If $H_2 \cong \mathrm{Q}_8$, then $[G_2,G_2] \leqslant \mathrm{Z}(H_2) \cong \mathrm{C}_2$. As G_2 is non-abelian, $[G_2,G_2] \cong \mathrm{C}_2$. Hence, $[G_2,G_2]$ is a minimal normal subgroup group of G_2 and therefore central. Thus, $G_2 = H_2$.

Conversely, let (i) or (ii) be violated. We construct a non-cyclic abelian normal subgroup of G. We may assume that H_q is cyclic or non-abelian for all primes q, and that $H_p \ncong \mathrm{Q}_8$ is non-abelian but $\mathrm{Z}(H_p)$ is cyclic for some p. If $A(h) = \langle h, \mathrm{Z}(H_p)\rangle$ were cyclic for all $h \in H_p$, then H_p would contain a unique subgroup of order p, namely the one contained in $\mathrm{Z}(H_p)$. By [68, 5.3.6], H_p would then be cyclic or generalised quaternion. These cases are ruled out since H_p has class precisely 2 and $H_p \ncong \mathrm{Q}_8$. Hence, $A(h)$ has to be non-cyclic for some $h \in H_p$. Note that $A(h)$ is normal in G since $[G_p,G_p] \leqslant \mathrm{Z}(H_p)$. ♦

7.2. Finding non-cyclic abelian normal subgroups

We introduce NoncyclicAbelian which constructs a non-cyclic abelian normal subgroup of a finite nilpotent group G or proves that G is an ANC group.

Algorithm 7.1 NoncyclicAbelian(G)

Input: a finite nilpotent group $G = \langle g_1, \ldots, g_n\rangle$
Output: a non-cyclic abelian normal subgroup of G or `fail` if G is an ANC group

if G is cyclic **then return** `fail`
if G is abelian **then return** G
let $A \triangleleft G$ be abelian
loop
  if A is non-cyclic **then return** A
  $a \leftarrow$ ExponentElement(A), $C \leftarrow \mathrm{C}_G(a)$
  if $C \not\leqslant A$, say $c \in C \setminus A$ **then**
    while $[c,g] \notin A$ for some $g \in G$ **do** $c \leftarrow [c,g]$
    $A \leftarrow \langle a, c\rangle$
  else
    $H \leftarrow \mathrm{C}_G$ (ExponentElement$([G,G])$)
    if H_p is non-cyclic abelian for some p **then return** H_p
    if $H_p \ncong \mathrm{Q}_8$ is non-abelian for some p **then**
      if $\mathrm{Z}(H_p)$ is non-cyclic **then return** $\mathrm{Z}(H_p)$
      repeat choose $h \in H_p$, let $A \leftarrow \langle h, \mathrm{Z}(H_p)\rangle$ **until** A is non-cyclic
      return A
    return `fail`

7.3 Remarks.

(i) Regarding the choice of an initial abelian normal subgroup in line 3, the same comments as in §4.2 apply.

(ii) Note that in lines 7–8, we perform membership tests in cyclic subgroups. In line 10, $A = \mathrm{C}_G(A)$ so that G/A embeds into the abelian group $\mathrm{Aut}(A)$ whence $[G, G] \leqslant A$ is cyclic. The remainder of the algorithm then follows the steps in the proof of Proposition 7.2; termination is guaranteed provided that in line 15, we do not choose the same element h twice.

7.3. The order of a finite homogeneous abelian group

In practice, the fields K which we encounter will be finitely generated over $\mathbf{Q}$; in fact, much stronger restrictions usually apply because of limitations of current computer algebra systems. In this section, we show that finite homogeneous abelian linear groups over such fields are (asymptotically) "small". We will later use this to justify why certain computations in abelian linear groups can be done efficiently.

Define $\xi_K\colon \mathbf{N} \to \mathbf{N} \cup \{\infty\}$ by

$$\xi_K(d) = \sup\Big(|A| : A \leqslant \mathrm{GL}_d(K) \text{ is homogeneous finite abelian}\Big).$$

7.4 Proposition. *Let $K/\mathbf{Q}$ be finitely generated,*

(i) $\xi_K(d)$ is finite for all $d \geqslant 1$.

(ii) $\xi_K(d) = \mathcal{O}(d^{1+\varepsilon})$ for all $\varepsilon > 0$.

Proof. For $m \geqslant 1$, define $\psi(m) = |K(\zeta_m) : K|$, where ζ_m denotes a primitive mth root of unity within some algebraic closure of K. Let E be the algebraic closure of $\mathbf{Q}$ in K, i.e. the subfield of K consisting of those elements algebraic over $\mathbf{Q}$. Since $K/\mathbf{Q}$ is finitely generated, so is the subextension $E/\mathbf{Q}$ by [71, Thm 3.3.5]. As a finitely generated algebraic extension, $E/\mathbf{Q}$ is finite. By basic Galois theory [71, Cor. 5.5.2], we have $\psi(m) = |\mathbf{Q}(\zeta_m) : \mathbf{Q}(\zeta_m) \cap K|$. Since $\mathbf{Q}(\zeta_m) \cap K \subset E$, we obtain

$$1 \leqslant \frac{\varphi(m)}{\psi(m)} = |\mathbf{Q}(\zeta_m) \cap K : \mathbf{Q}| \leqslant |E : \mathbf{Q}|,$$

where φ is Euler's function. It follows from asymptotic properties of φ [36, Thm 327] that there exists $C > 0$ such that $m \leqslant C \cdot \psi(m)^{1+\varepsilon}$ for all $m \geqslant 1$.

Now let $d \geqslant 1$ and $G \leqslant \mathrm{GL}_d(K)$ be finite, abelian, and homogeneous of order m, say. Then $K[G] \cong_K K(\zeta_m)$ and therefore $d = |K^d : K[G]| \cdot |K[G] : K| \geqslant |K[G] : K| = \psi(m)$. Thus, $m \leqslant C \cdot \psi(m)^{1+\varepsilon} \leqslant C \cdot d^{1+\varepsilon}$. ♦

7.4. Finding inhomogeneous abelian normal subgroups

In order to use Corollary 1.12, we only need an inhomogeneous abelian normal subgroup of the finite nilpotent group $G \leqslant \mathrm{GL}(V)$. Instead of attempting to construct a non-cyclic abelian $A \triangleleft G$ as in NoncyclicAbelian (Algorithm 7.1), we may thus consider the task of either finding an *inhomogeneous* abelian $A \triangleleft G$ or proving that G is an ANC group. This can be done by modifying Algorithm 7.1 as follows: whenever we have found a cyclic $A \triangleleft G$, then we test whether it is homogeneous. If this is not the case, then we return A. Denote the function thus obtained by InhomogeneousAbelian.

We discuss an advantage of InhomogeneousAbelian over NoncyclicAbelian. Recall that the latter heavily relies on membership tests and centraliser computations. These are performed for cyclic subgroups, and in InhomogeneousAbelian, the cyclic subgroups will be homogeneous. By Proposition 7.4, if $K/\mathbf{Q}$ is finitely generated, then the membership tests and centraliser computations performed by InhomogeneousAbelian can be done efficiently. However, in our implementation [76] we nonetheless use NoncyclicAbelian since it performed better during our experiments.

8. Irreducibility testing of ANC groups

In the last chapter, we reduced the problem of irreducibility testing of finite nilpotent linear groups to the case of ANC groups. We now develop an algorithm for irreducibility testing of ANC groups over a range of fields of characteristic zero. Unless otherwise indicated, let K have characteristic zero.

8.1. Conditions (F1)–(F2) on the ground field

For $i \geqslant 1$, let ζ_i be a primitive ith root of unity over K; we assume that all the ζ_i are contained in some fixed algebraic closure of K. Write $\mathbf{E}_n = \mathbf{Q}(\zeta_n)$. For $n = 2^j m$ with m odd and $j \geqslant 3$, define

$$\mathbf{E}_n^{\pm} = \mathbf{Q}(\zeta_{2^j} \pm \zeta_{2^j}^{-1}, \zeta_m).$$

For $0 \leqslant j \leqslant 2$, we let $\mathbf{E}_n^{\pm} = \mathbf{E}_m$. In addition to the fundamental computational assumptions on K from Chapter 1, our algorithms for irreducibility and primitivity testing of finite nilpotent linear groups over K only require the following computational assumptions (introduced in [74]).

(F1) We can algorithmically factorise univariate polynomials over K.

(F2) For any $n \geqslant 1$, we can decide if $x^2 + y^2 = -1$ has a solution in the composite $\mathbf{E}_n^+ K$ and we can find one such solution whenever it exists.

8.1 Remarks.

(i) As explained in [86], if (F1) is satisfied for K, then it is in fact satisfied for all finite algebraic extensions of K.

(ii) As we have already mentioned in Chapter 4, (F1) is satisfied for number fields and for rational function fields over number fields. We will see in the next chapter that (F2) is also satisfied for these two families of fields.

8.2. Quaternion algebras

In this section, K can be arbitrary of characteristic $\neq 2$.

Basic properties. Recall that a **quaternion algebra** over K is a central simple 4-dimensional algebra over K. A quaternion algebra $\mathcal{A}$ over K **splits** if $\mathcal{A} \cong \mathrm{M}_2(K)$; otherwise $\mathcal{A}$ is a division algebra. Equivalently, $\mathcal{A}$ splits if and only if the unique (up to isomorphism) irreducible $\mathcal{A}$-module has K-dimension 2.

For $a, b \in K^\times$ define $\left(\frac{a,b}{K}\right)$ to be the K-algebra with basis $(1, \mathrm{i}, \mathrm{j}, \mathrm{k})$ and multiplication $\mathrm{i}^2 = a$, $\mathrm{j}^2 = b$, $\mathrm{ij} = \mathrm{k} = -\mathrm{ji}$. Then $\left(\frac{a,b}{K}\right)$ is a quaternion algebra [47, Prop. III.1.1]. For example, $\left(\frac{-1,-1}{\mathbf{R}}\right)$ is the classical algebra of Hamilton's quaternions. Every quaternion algebra over K is isomorphic to $\left(\frac{a,b}{K}\right)$ for some $a, b \in K^\times$; see [47, Thm III.5.1]. The algebra $\left(\frac{a,b}{K}\right)$ splits if and only if $ax^2 + by^2 = 1$ for some $x, y \in K$ ("Hilbert's criterion") [47, Thm III.2.7].

Zero divisors and irreducible modules. Fix a quaternion algebra $\mathcal{A} = \left(\frac{a,b}{K}\right)$. The **conjugate** of an element $x = \alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k}$ $(\alpha, \beta, \gamma, \delta \in K)$ is $\overline{x} = \alpha - \beta\mathrm{i} - \gamma\mathrm{j} - \delta\mathrm{k}$; the **norm** of x

$$\mathrm{N}(x) = x\overline{x} = \overline{x}x = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2 \in K.$$

An element $x \in \mathcal{A}$ is a unit if and only if $\mathrm{N}(x) \neq 0$ [47, Prop. III.2.4]. Note that, as in every finite-dimensional algebra, an element of $\mathcal{A}$ is a zero divisor if and only if it is not a unit; cf. [72, Thm 18.6].

Suppose that $\mathcal{A}$ splits. We wish to find a zero divisor in $\mathcal{A}$ or, equivalently, a non-zero $x \in \mathcal{A}$ with $\mathrm{N}(x) = 0$. If b is a square in K, say $b = q^2$, then $\mathrm{N}(1 + q^{-1}\mathrm{j}) = 0$, so let $\sqrt{b} \notin K$. Since $\mathcal{A}$ splits, by [47, Thm III.2.7], there exists $z \in K(\sqrt{b})$ with $\mathrm{N}_{K(\sqrt{b})/K}(z) = a$; here $\mathrm{N}_{K(\sqrt{b})/K}$ denotes the usual field norm. Note that $(x, y) \mapsto x^{-1} + x^{-1}y\sqrt{b}$ maps pairs $(x, y) \in K^2$ satisfying $ax^2 + by^2 = 1$ to solutions $z \in K(\sqrt{b})$ of the norm equation $\mathrm{N}_{K(\sqrt{b})/K}(z) = a$. Given such a solution z, say $z = r + s\sqrt{b}$ $(r, s \in K)$, we have $a = r^2 - bs^2$ and therefore $\mathrm{N}(r + \mathrm{i} + s\mathrm{j}) = 0$.

Let $0 \neq z \in \mathcal{A}$ be a zero divisor. Then the right $\mathcal{A}$-module endomorphism $\mathcal{A} \to \mathcal{A}, x \mapsto zx$ is not injective and hence not surjective. Therefore, its kernel and image are proper right ideals of $\mathcal{A}$. Conversely, a generator of a proper right ideal of $\mathcal{A}$ is a zero divisor. By comparing dimensions, we see that any proper right ideal of $\mathcal{A}$ is necessarily minimal and therefore an irreducible $\mathcal{A}$-submodule of $\mathcal{A}$.

8.3. ANC groups and their enveloping algebras

This section is based on [75, §7]. For certain ANC groups $G \leqslant \mathrm{GL}(V)$, including all the primitive ones, we can give a precise description of $K[G]$ as a quaternion algebra. This refines the crossed product structure given by §5.2.

For an ANC group G, define $\vartheta(G) = 1$ if G_2 is dihedral or semidihedral, and $\vartheta(G) = -1$ if G_2 is generalised quaternion. Further define $\delta(G) = 1$ if G_2 is dihedral

or generalised quaternion and $\delta(G) = -1$ if G_2 is semidihedral. If G_2 is cyclic, we let $\vartheta(G) = \delta(G) = 0$.

8.2 Proposition (Cf. [73, §4].)**.** *Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian ANC group which contains a homogeneous cyclic subgroup A of index 2. Let $Z = \mathrm{Z}(K[G])$. Then $Z = K[A]^{G/A}$ and $K[G] \cong \left(\frac{\vartheta(G),-1}{Z}\right)$ as Z-algebras. In particular, $|K[G] : K[A]| = 2$.*

Proof. Let $g \in G$ be with $G = \langle A, g\rangle$ and $g^2 = \vartheta(G) \cdot 1_V$. Define $L = K[A]$. By Proposition 5.1, $Z = L^{G/A}$ and $K[G]$ is naturally a crossed product of L by $G/A \cong \mathrm{Gal}(L/Z)$. In particular, $K[G]$ is simple and $|K[G] : Z| = |G : A|^2 = 4$. Hence, $K[G]$ is a quaternion algebra over Z.

Let $h \in A$ have order 4. Then $h \notin Z$ and since $|L : Z| = 2$, we obtain $L = Z[h]$. Thus, $K[G] = Z[G_2] = Z[H]$, where $H = \langle g, h\rangle$. Note that since A is homogeneous, the unique involution in A is $h^2 = -1_V$. Clearly, if $\vartheta(G) = 1$, then $H \cong \mathrm{D}_8$, otherwise $H \cong \mathrm{Q}_8$. In any case, we have $H = \{\pm 1_V, \pm g, \pm h, \pm gh\}$ and since $|K[G] : Z| = 4$, we see that $(1_V, g, h, gh)$ is a Z-basis of $K[G]$. Evidently, $K[G] \cong_Z \left(\frac{\vartheta(G),-1}{Z}\right)$ via $g \mapsto \mathrm{i}$ and $h \mapsto \mathrm{j}$. ♦

We say that $G \leqslant \mathrm{GL}(V)$ is **split homogeneous** if $K[G]$ is simple and split. In other words, G is split homogeneous if and only if the centre Z of $K[G]$ is a field and $K[G]$ is a full matrix algebra over Z.

8.3 Corollary. *Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian ANC group and let $A \lhd G$ be irreducible and cyclic of index 2. Then G is split homogeneous.*

Proof. Let $Z = K[A]^{G/A}$ as in Proposition 8.2. We have $|V : K[A]| = 1$ by irreducibility of A and therefore $|V : Z| = 2$. If $K[G]$ were non-split, then its unique irreducible module would have Z-dimension 4. Thus, $K[G] \cong \mathrm{M}_2(Z)$. ♦

The field Z in Proposition 8.2 can be easily determined explicitly as follows.

8.4 Lemma. *Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian ANC group and let $A \lhd G$ be homogeneous and cyclic of index 2. Choose generators $A_2 = \langle x\rangle$ and $A_{2'} = \langle y\rangle$. Then $\mathrm{Z}(K[G]) = K[x + \delta(G)x^{-1}, y]$.*

Proof. Write $Z = \mathrm{Z}(K[G])$. Since $G/A \cong \mathrm{C}_2$ acts via $x \mapsto \delta(G)x^{-1}$ on A_2 and trivially on $A_{2'}$, we see that $F = K[x + \delta(G)x^{-1}, y] \subset Z$ and $K[A] = F[x]$. Now x is a root of $T^2 - (x + \delta(G)x^{-1})T + \delta(G) \in F[T]$. It follows that that $|K[A] : F| \leqslant 2$. As $|K[A] : Z| = 2$, this completes the proof. ♦

This can be made more explicit in terms of cyclotomic extensions of K.

8.5 Lemma. *Let $n = 2^j m$, where m is odd and $j \geqslant 3$.*

(i) $\mathbf{E}_n^{\pm} = \mathbf{Q}(\zeta_{2^j}^k \pm \zeta_{2^j}^{-k}, \zeta_m^\ell)$ for any odd k and $\ell \geqslant 1$ with $(\ell, m) = 1$.

(ii) Let F/K be some field extension and let $\alpha, \beta \in F$ be primitive 2^jth and mth roots of unity over K, respectively. Then $K(\alpha \pm \alpha^{-1}, \beta) \cong_K \mathbf{E}_n^{\pm} K$.

More precisely:

(a) Let $f = \mathrm{mpol}_K(\alpha)$. Then there is an odd k such that $f(\zeta_{2^j}^k) = 0$. The rule $\alpha \mapsto \zeta_{2^j}^k$ defines a K-isomorphism $K(\alpha) \xrightarrow{\lambda} \mathbf{E}_{2^j} K$.

(b) Let $g = \mathrm{mpol}_{K(\alpha)}(\beta)$. Then there is an ℓ with $(\ell, m) = 1$ such that $g^\lambda(\zeta_m^\ell) = 0$. The rules $\alpha \mapsto \zeta_{2^j}^k$ and $\beta \mapsto \zeta_m^\ell$ define a K-isomorphism $K(\alpha, \beta) \to \mathbf{E}_n K$ which restricts to a K-isomorphism $K(\alpha \pm \alpha^{-1}, \beta) \to \mathbf{E}_n^{\pm} K$.

Proof. By elementary properties of cyclotomic fields [48, VI, §3] and [48, Thm VI.1.14], there exists $\sigma \in \mathrm{Gal}(\mathbf{E}_n/\mathbf{Q})$ with $\zeta_{2^j}^\sigma = \zeta_{2^j}^k$ and $\zeta_m^\sigma = \zeta_m^\ell$. Since $\mathbf{E}_n/\mathbf{Q}$ is abelian, $\mathbf{E}_n^{\pm}/\mathbf{Q}$ is Galois whence $(\mathbf{E}_n^{\pm})^\sigma = \mathbf{E}_n^{\pm}$ and (i) follows. Let Ω be an algebraically closed extension of K containing all of the ζ_i. Part (ii) follows from basic properties of field embeddings [71, Thm 2.8.4], part (i), and the fact that f and g^λ divide the respective cyclotomic polynomials. ⧫

8.6 Corollary. *Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian ANC group of order $2n$. Suppose that G contains a homogeneous cyclic subgroup of index 2.*

(i) If $\vartheta(G) = 1$, then G is split homogeneous.

(ii) If $\vartheta(G) = -1$, then G is split homogeneous if and only if -1 is a sum of two squares in $\mathbf{E}_n^{+} K$.

Proof. The first part is immediate from Proposition 8.2. For (ii), we additionally use Lemmas 8.4–8.5 and the fact that the quaternion algebra $\left(\frac{-1,-1}{Z}\right)$ splits if and only if -1 is a sum of two squares in Z. ⧫

8.4. Irreducibility testing of ANC groups

Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian ANC group and suppose that $A \triangleleft G$ is cyclic and homogeneous of index 2. We now describe how irreducibility of G can be tested and how this is related to condition (F2) from §8.1. We mostly follow [74, §6]; some differences arise since in [74], we did not argue using quaternion algebras.

8.4.1. Nice generators

First note that we essentially get A from Algorithm 7.1 because, unless $G_2 \cong \mathrm{Q}_8$, we necessarily have $A = \mathrm{C}_G([G, G])$; if, on the other hand, $G_2 \cong \mathrm{Q}_8$, then we may take $A = \langle w \rangle \times G_{2'}$ for any non-central $w \in G_2$.

Let $A = \langle a \rangle$ and pick $g \in G_2 \setminus A$. Write $a = a_2 a_{2'}$ according to $A = A_2 \times A_{2'}$. Then G_2 is dihedral or generalised quaternion if and only if $a_2 a_2^g = 1_V$. In these cases, we have $g^2 = \vartheta(G) \cdot 1_V$. If G_2 is semidihedral (equivalently, $a_2 a_2^g = -1_V$),

then either $g^2 = 1_V$ or $(a_2 g)^2 = 1_V$. In the latter case, we replace g by $a_2 g$. We can therefore assume that $G = \langle A, g\rangle$ and $g^2 = \vartheta(G) \cdot 1_V$.

Define $L = K[A]$ and $Z = L^{G/A}$. Let $h \in A$ have order 4. Then $L = Z[h] \cong_Z Z(\sqrt{-1}) \neq Z$ and we have a Z-algebra isomorphism $\left(\frac{\vartheta(G),-1}{Z}\right) \to K[G]$ given by $\mathrm{i} \mapsto g$ and $\mathrm{j} \mapsto h$; see Proposition 8.2 and its proof.

8.4.2. Finding submodules

Choose an arbitrary non-zero $v \in V$. If $v \cdot K[G] \neq V$, then we found a proper $K[G]$-submodule of V so suppose that $V = v \cdot K[G]$. If $|V : L| = 1$, then A and hence G is irreducible. We may thus assume that $|V : L| = 2$; then $K[G] \to V, s \mapsto vs$ is a $K[G]$-module isomorphism. If $K[G]$ is non-split, then G is irreducible so let us assume that $K[G]$ splits; the non-split case happens precisely when $\vartheta(G) = -1$ and -1 is not a sum of two squares in Z.

Since $K[G]$ splits, as explained in §8.2, there is an element $z \in L$ with $\mathrm{N}_{L/Z}(z) = \vartheta(G)$ and $g + z \in K[G]$ is then a zero-divisor. It follows that $v(g + z)$ generates a proper (in fact irreducible) $K[G]$-submodule of V. If $\vartheta(G) = 1$, we may take $z = \pm 1$.

Let $\vartheta(G) = -1$. Then $(x, y) \mapsto x + yh$ defines a bijection between pairs $(x, y) \in Z^2$ with $x^2 + y^2 = -1$ and solutions $z \in L$ of $\mathrm{N}_{L/Z}(z) = -1$. By the following, finding a proper $K[G]$-submodule of V is equivalent (up to basic linear algebra) to finding a solution $(x, y) \in Z^2$ of $x^2 + y^2 = -1$.

8.7 Proposition. *Let $\vartheta(G) = -1$. Suppose that $V = v \cdot K[G] \neq v \cdot L$.*

(i) If $z \in L$ satisfies $\mathrm{N}_{L/Z}(z) = -1$, then $v(g + z)$ generates a proper $K[G]$-submodule of V. Moreover, $\mathrm{Ker}(g + z) \neq 0$.

(ii) If $w \in V$ generates a proper $K[G]$-submodule of V, then there exists a (unique) $z \in L$ with $wg = wz$ and then $\mathrm{N}_{L/Z}(z) = -1$.

Proof.

(i) We already proved the first assertion. Since the quaternion algebra norm satisfies $\mathrm{N}(s) = \mathrm{N}(\bar{s})$ for $s \in K[G]$, we have $0 = \mathrm{N}(g + z) = \mathrm{N}(\overline{g + z}) = (\overline{g + z})(g + z)$. Thus, $v(\overline{g + z})$ is a non-trivial element of $\mathrm{Ker}(g + z)$.

(ii) Let $w \in V$ generate a proper $K[G]$-submodule of V. Then $w \cdot K[G]$ has L-dimension 1 and therefore $w \cdot K[G] = w \cdot L$ holds. Hence, $wg = wz$ for some $z \in L$. We obtain $w \cdot \vartheta(G) = wg^2 = wzg = wgz^g = wzz^g = w \cdot \mathrm{N}_{L/Z}(z)$. Therefore, $\mathrm{N}_{L/Z}(z) = \vartheta(G)$. ♦

By Lemma 8.4, Z is K-isomorphic to $\mathbf{E}_n^+ K$, where $n = |G|/2$. We can therefore test irreducibility of G provided that condition (F2) from §8.1 is satisfied; note that we can use Lemma 8.5 to make the isomorphism $Z \cong_K \mathbf{E}_n^+ K$ explicit.

8.4.3. An algorithm for irreducibility testing of ANC groups

Assuming conditions (F1)–(F2) from §8.1, the following is an algorithm for irreducibility testing of ANC groups with homogeneous cyclic subgroups of index 2. As before, we only return generators of submodules for reducible groups.

Algorithm 8.1 IsIrreducibleANC(G, A)

Input: a non-abelian ANC group $G \leqslant \mathrm{GL}(V)$; a homogeneous cyclic $A \lhd G$, $|G : A| = 2$
Output: `true` if G is irreducible; `false` and a generator of a submodule otherwise

1: find $\vartheta(G)$, g, and $a = a_2 a_{2'}$ as described in §8.4.1
2: $v \leftarrow$ NonzeroElement(V), $U \leftarrow v \cdot K[A]$
3: **if** $U = V$ **then return** `true`
4: **if** $U + Ug < V$ **then return** `false`, x
5: **if** $\vartheta(G) = 1$ **then return** `false`, $x(g + 1)$
6: **if** -1 is not a sum of two squares in Z, where $Z = K\left[a_2 + a_2^{-1}, a_{2'}\right]$, **then return** `true`
7: find $x, y \in Z$ such that $x^2 + y^2 = -1$
8: **return** `false`, $v\left(g + x + y \cdot a_2^{\mathrm{ord}\,(a_2)/4}\right)$

8.4.4. A remark on fields containing $\sqrt{-1}$

A special case occurs if $\sqrt{-1} \in K$; we may detect this if we assume that (F1) holds. Condition (F2) is then trivially satisfied. Recall that polynomial factorisation is used to find the homogeneous decomposition for an abelian group in §4.1.

Suppose that $\sqrt{-1} \in K$ and let $G \leqslant \mathrm{GL}(V)$ be a non-abelian ANC group and $A \lhd G$ be cyclic with $|G : A| = 2$. Let $h \in A$ have order 4. Then $h \notin \mathrm{Z}(G_2) \cong \mathrm{C}_2$ so h is not scalar. Since h has an eigenvalue in K, it follows that $K[h] \subset K[A]$ is not a field. Thus, A acts inhomogeneously on V. It follows that the assumptions of Algorithm 8.1 cannot be satisfied if $\sqrt{-1} \in K$. For the purposes of irreducibility or primitivity testing we may then use Corollary 1.12.

9. On $x^2 + y^2 = -1$

We consider the solubility of the equation $x^2 + y^2 = -1$ from §8.4 in the fields of greatest interest to us: number fields and rational function fields over number fields. We will see that condition (F2) from §8.1 is satisfied for these fields. We also recall a known criterion for solubility of $x^2 + y^2 = -1$ in a number field and we extend this to obtain results about solubility in certain field extensions; this will be used in Chapter 10. This chapter expands [74, §8].

9.1. The case of number fields

In this section, let K be a number field.

Condition (F2). Since we can factorise polynomials over K, we can detect if $\sqrt{-1} \in K$. Assuming that this is not the case, the map $(x, y) \mapsto x + y\sqrt{-1}$ is a bijection between the set of solutions $(x, y) \in K^2$ of $x^2 + y^2 = -1$ and elements $z \in K(\sqrt{-1})$ with $\mathrm{N}_{K(\sqrt{-1})/K}(z) = -1$. As algorithms for solving relative norm equations for number fields are available [30, 82], it follows that condition (F2) is satisfied for number fields. In fact, we use this interpretation as a norm equation to actually solve $x^2 + y^2 = -1$ in practice.

Solubility of $x^2+y^2 = -1$. Both for our theoretical investigations and for practical applications in algorithms, it will often be important to know (without invoking a norm equation solver) if $x^2+y^2 = -1$ has a solution in a given number field K. The fundamental result here is the following.

9.1 Proposition ([29, 16, 33])**.** *-1 is a sum of two squares in K if and only if*

(i) K is totally imaginary, and

(ii) $|K_{\mathfrak{p}} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p}$ above 2 in K.

9.2 Remark. It is known that unless the number field K has a real embedding, -1 is always a sum of at most 4 squares [16].

Extensions of the ground field. Given K, the conditions in Proposition 9.1 can be tested algorithmically; see [12, Alg. 4.1.11 & 6.2.9] and [13, Cor. 4.1.27]. However, recall that in condition (F2), we need to investigate the solubility of $x^2 + y^2 = -1$ in an extension $E = \mathbf{E}_n^+ K$ of K. In general, we will have $|E : \mathbf{Q}| > |K : \mathbf{Q}|$ and, in practice, it might be infeasible to apply Proposition 9.1 to E even if it can be

applied to K. The following lemma shows how we may directly read off from K and n whether conditions (i)–(ii) in Proposition 9.1 hold for E in place of K; part (iii) in the lemma generalises [29, Cor. 2]. For $(r, n) = 1$, we denote the order of $r + n\mathbf{Z}$ in $(\mathbf{Z}/n)^\times$ by $\operatorname{ord}(r \bmod n)$; this includes $\operatorname{ord}(r \bmod 1) = 1$.

9.3 Lemma. *Let $n = 2^j m$ (m odd) and $E = \mathbf{E}_n^+ K$.*

(i) E is totally imaginary if and only if K is totally imaginary or $m > 1$.

(ii) If $j \geqslant 3$, then condition (ii) in Proposition 9.1 is satisfied.

(iii) Let $j \leqslant 2$. Then condition (ii) in Proposition 9.1 is satisfied for E if and only if $\operatorname{ord}(2 \bmod m) \cdot |K_\mathfrak{p} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p}$ above 2 in K.

Proof.

(i) If E has a real embedding, then so do the subfields K and $\mathbf{E}_m$; in particular, this implies that $m = 1$. Conversely, let K have a real embedding and let $m = 1$. Since $\mathbf{E}_n^+ = \mathbf{E}_{2^j} \cap \mathbf{R}$ is totally real, it follows that E has a real embedding.

(ii) We have $\mathbf{Q}(\sqrt{2}) = \mathbf{E}_8^+ \subset E$. Since $|\mathbf{Q}_2(\sqrt{2}) : \mathbf{Q}_2| = 2$ as $X^2 - 2$ is an Eisenstein polynomial, the local degrees in condition (ii) of Proposition 9.1 are even.

(iii) Let $\overline{\mathbf{Q}}_2$ be an algebraic closure of $\mathbf{Q}_2$. We may assume that ζ_m and the completions considered below are all contained in $\overline{\mathbf{Q}}_2$.

Let $t = \operatorname{ord}(2 \bmod m)$. By [13, Prop. 3.5.18], we have $|\mathbf{Q}_2(\zeta_m) : \mathbf{Q}_2| = t$. Using basic facts on factorisation in number fields [59, II, §8], we see that the 2-adic completions of $E = \mathbf{E}_m K$ are precisely the (not necessarily distinct) fields $\mathcal{K}(\zeta_m)$, where $\mathcal{K}$ is a 2-adic completion of K. By basic Galois theory [71, Cor. 5.5.2], $|\mathcal{K}(\zeta_m) : \mathcal{K}|$ divides $|\mathbf{Q}_2(\zeta_m) : \mathbf{Q}_2|$. Hence, $a \mid b \mid c$, where $a = \operatorname{lcm}(t, |\mathcal{K} : \mathbf{Q}_2|)$, $b = |\mathcal{K}(\zeta_m) : \mathbf{Q}_2|$, and $c = t|\mathcal{K} : \mathbf{Q}_2|$. Clearly, if b is even, then so is c. If c is even, then so is a and hence also b. Thus, $b \equiv c \bmod 2$. ♦

Prime powers. The remainder of this section is devoted to proving the following lemma; it will become important for primitivity testing in §10.3.4. The lemma is essentially [75, Lem. 8.6] (which is in turn related to [29, Thm 3]). Let $\underline{n}$ be the product of the prime divisors of an integer n.

9.4 Lemma. *Let $n \geqslant 1$ be odd and let $m \mid n$ such that $\underline{n} = \underline{m}$. Then $x^2 + y^2 = -1$ has a solution in $\mathbf{E}_n K$ if and only if it has a solution in $\mathbf{E}_m K$.*

In order to prove Lemma 9.4, we need some auxiliary results. While the following proposition is certainly known, the author has not been able to locate a reference.

9.5 Proposition. *Let $n \geqslant 1$ and $m \mid n$.*

(i) The natural map $\mathbf{Z}/n \twoheadrightarrow \mathbf{Z}/m$ *induces an epimorphism* $(\mathbf{Z}/n)^\times \xrightarrow{\lambda} (\mathbf{Z}/m)^\times$ *of groups.*

(ii) If $\underline{n} = \underline{m}$*, then* $\mathrm{Ker}(\lambda) = \{x + n\mathbf{Z} : x \in \mathbf{Z}, x \equiv 1 \bmod m\}$.

Proof.

(i) If $(x, n) = 1$ for $x \in \mathbf{Z}$, then clearly $(x, m) = 1$. Hence, we obtain an induced group homomorphism $(\mathbf{Z}/n)^\times \to (\mathbf{Z}/m)^\times$ and it remains to prove that it is surjective. By the Chinese remainder theorem, we may assume that n and m are powers of the same rational prime p, say $m = p^\beta$. If $\beta = 0$, then there is nothing to prove so let $\beta \geqslant 1$. The result then follows since $x \in \mathbf{Z}$ is a unit modulo p^α for $\alpha \geqslant 1$ if and only if it is a unit modulo p; cf. [13, Prop. 4.3.1].

(ii) Let $S = \{x + n\mathbf{Z} : x \in \mathbf{Z}, x \equiv 1 \bmod m\}$. Then $|S| = n/m$ and $\mathrm{Ker}(\lambda) \subset S$. Since $\underline{n} = \underline{m}$, we have $\varphi(n)/\varphi(m) = n/m$. Using (i), we obtain $|\mathrm{Ker}(\lambda)| = n/m$ whence the result follows. ⧫

9.6 Lemma. *Let* G *be a periodic group and let* $N \triangleleft G$ *have odd finite order. Then* $\mathrm{ord}\,(g) \equiv \mathrm{ord}\,(gN) \bmod 2$ *for any* $g \in G$.

Proof. Let $e = \mathrm{ord}\,(gN)$ and $f = \mathrm{ord}\,(g)$ so that $e \mid f$. If e is even, then so is f. Conversely, there exists an odd $r \geqslant 1$ with $g^{er} = 1$ and therefore $f \mid er$. Hence, if f is even, then so is er and hence e. ⧫

Proof of Lemma 9.4. The last two results show that $\mathrm{ord}\,(2 \bmod n) \equiv \mathrm{ord}\,(2 \bmod m) \bmod 2$. Clearly, $n = 1$ if and only if $m = 1$. Now apply Lemma 9.3. ⧫

9.2. The case of cyclotomic fields

In the special case that K is a cyclotomic field, Proposition 9.1 takes the following form.

9.7 Corollary ([29, Cor. 2 & Thm 3])**.** *Let* $n \geqslant 1$ *be odd. Then the following are equivalent:*

(i) -1 *is a sum of two squares in* $\mathbf{E}_n$.

(ii) $\mathrm{ord}\,(2 \bmod n)$ *is even.*

(iii) -1 *is a sum of two squares in* $\mathbf{E}_p$ *for some prime divisor* p *of* n.

Proof. The equivalence (i)↔(ii) follows from Lemma 9.3. Let $n = \prod_{p \in S} p^{\alpha(p)}$ be the prime factorisation of n. By the Chinese remainder theorem, $\mathrm{ord}\,(2 \bmod n) = \mathrm{lcm}\big(\mathrm{ord}\,(2 \bmod p^{\alpha(p)}) : p \in S\big)$. The implication (ii)↔(iii) follows since by Proposition 9.5 and Lemma 9.6, $\mathrm{ord}\,(2 \bmod p^{\alpha(p)}) \equiv \mathrm{ord}\,(2 \bmod p) \bmod 2$. ⧫

9.8 Example. Let p be an odd rational prime such that $\operatorname{ord}(2 \bmod p)$ is even, say $\operatorname{ord}(2 \bmod p) = 2r$. Then $2^r \equiv -1 \bmod p$ and so $\delta^2 = \zeta_p$, where $\delta = \zeta_p^{-2^{r-1}}$. Define $\theta = \delta \prod_{i=0}^{r-1}(\delta^{2^i} + \sqrt{-1}) \in \mathbf{E}_p(\sqrt{-1}) = \mathbf{E}_{4p}$. Then by [43, Ex. 38.13d], we have $\mathrm{N}_{\mathbf{E}_p(\sqrt{-1})/\mathbf{E}_p}(\theta) = \zeta_p \prod_{i=0}^{r-1}(1 + \zeta_p^{2^i}) = -1$. We thus obtain an explicit solution of $x^2 + y^2 = -1$ in $\mathbf{E}_p$ and hence (by Corollary 9.7) in any cyclotomic field that admits a solution. As explained in §8.4, there is an effective bijection between solutions of $x^2 + y^2 = -1$ in $\mathbf{E}_p$ and solutions $z \in \mathbf{E}_p(\sqrt{-1}) = \mathbf{E}_{4p}$ of the norm equation $\mathrm{N}_{\mathbf{E}_{4p}/\mathbf{E}_p}(z) = -1$.

9.3. The case of rational function fields

9.9 Proposition. *Let K be any field and let $\mathbf{X} = (X_1, \ldots, X_r)$ be algebraically independent over K. Then -1 is a sum of ℓ squares in $K(\mathbf{X})$ if and only if it is a sum of ℓ squares in K.*

Proof. The case $r = 1$ is [47, Cor. IX.1.2(ii)]; repeated application then gives the desired result. ⧫

By Proposition 3.11, if E/K is finite, then $\mathbf{X}$ remains algebraically independent over E. Hence, we may apply the above results on solubility of $x^2 + y^2 = -1$ in a number field to the case of a rational function field over a number field. In particular, rational function fields over number fields satisfy condition (F2).

10. Primitivity testing of ANC groups

We develop an algorithm for primitivity testing of ANC groups over fields satisfying conditions (F1)–(F2). In the important special case of number fields, we obtain simplifications. Unless otherwise indicated, let K have characteristic zero. This chapter is based on [75, §8].

10.1. Basic facts regarding imprimitivity

We collect some known and elementary facts; K can be arbitrary in this section.

10.1 Lemma. *Let $G \leqslant \mathrm{GL}(V)$ be irreducible and $U < V$.*

(i) U is a block for G if and only if $|V : K|/|U : K| = |G : \mathrm{Stab}_G(U)|$.

(ii) If U is a block for G, then $\mathrm{Stab}_G(U)$ acts irreducibly on U.

Proof. See [85, Thm 15.1(iii)] and [85, Thm 15.3]. ♦

10.2 Lemma. *Let $G \leqslant \mathrm{GL}(V)$ be irreducible and let $H < G$. Then H is a block stabiliser for G if and only if there exists an irreducible $K[H]$-submodule $U \leqslant V$ with $|V : K|/|U : K| = |G : H|$. In this case, $H = \mathrm{Stab}_G(U)$ and U is a block for G.*

Proof. The "only if" part follows from Lemma 10.1. Let $U \leqslant V$ be a $K[H]$-submodule with $|V : K|/|U : K| = |G : H|$. Then $\sum_{g \in G} Ug = V$ by irreducibility of G. The number of distinct subspaces Ug is $|G : \mathrm{Stab}_G(U)| \leqslant |G : H|$. Let T be a right transversal of $\mathrm{Stab}_G(U)$ in G. Then $V = \sum_{t \in T} Ut$ and therefore $|V : K| \leqslant |T| \cdot |U : K| \leqslant |G : H| \cdot |U : K| = |V : K|$. Hence, $H = \mathrm{Stab}_G(U)$ and $V = \bigoplus_{t \in T} Ut$ whence U is a block for G. ♦

10.3 Lemma. *Let $G \leqslant \mathrm{GL}(V)$ be irreducible and let $H < G$ with $|G : H| = 2$.*

(i) If $U < V$ is an irreducible $K[H]$-submodule, then U is a block for G.

(ii) H is a block stabiliser for G if and only if H is reducible.

Proof. Let $g \in G \setminus H$. Given an irreducible $K[H]$-submodule $U < V$, we have $U \neq U + Ug = V$ by irreducibility of G. As U and Ug are distinct irreducible $K[H]$-submodules, $U \cap Ug = 0$. This proves (i); part (ii) then follows immediately. ♦

10.4 Lemma. *Let $G \leqslant \mathrm{GL}(V)$ be an irreducible nilpotent group. If G is imprimitive, then G admits a system of imprimitivity of prime size.*

Proof. Let $\mathcal{U}$ be a non-trivial system of imprimitivity for G, say $|\mathcal{U}| = r$. A primitive permutation representation of G has prime degree [85, Lem. 5.1]. Since an imprimitive action of G on $\mathcal{U}$ yields a smaller system of imprimitivity for G, the result follows by induction on r. ♦

10.5 Corollary. *Let $G \leqslant \mathrm{GL}(V)$ be an irreducible nilpotent group. Then G is imprimitive if and only if a prime index subgroup of G is a block stabiliser.* ♦

Given a system of imprimitivity for G of composite size, we may use standard permutation group algorithms [39, Ch. 4] to construct one of prime size. This will become relevant for estimating the computational difficulty of constructing a block; see §10.3.3.

10.2. Primitivity testing of abelian groups

Primitivity of irreducible finite abelian linear groups in characteristic zero can be easily tested. In §10.3, primitivity of a non-abelian ANC group $G \leqslant \mathrm{GL}(V)$ will be shown to be connected to that of an irreducible abelian normal subgroup of G. It is therefore worthwhile to discuss the finite abelian case in detail. For a group G and $n \geqslant 1$, we write $G^n = \langle g^n : g \in G \rangle$.

As explained in Chapter 7, a finite irreducible (or merely homogeneous) abelian group $G \leqslant \mathrm{GL}(V)$ is cyclic. The maximal subgroups of G are then precisely of the form G^p, where p is a prime divisor of $|G|$.

10.6 Proposition. *Let $G \leqslant \mathrm{GL}(V)$ be a finite irreducible cyclic group and let p be a prime divisor of $|G|$. Then G^p is a block stabiliser for G if and only if $|K[G] : K[G^p]| = p$. If this is the case, then any 1-dimensional $K[G^p]$-subspace of V is a block for G.*

Proof. The subgroup G^p is itself homogeneous. An irreducible $K[G^p]$-submodule of V is the same thing as a 1-dimensional $K[G^p]$-subspace of V. Let $U \leqslant V$ be one of these. Then $|U : K| = |K[G^p] : K|$ and therefore $|V : K|/|U : K| = |K[G] : K[G^p]|$. Now apply Lemma 10.2. ♦

10.7 Remark. Let G and p be as in Proposition 10.6. Then $|K[G] : K[G^p]| = |\mathbf{E}_n K : \mathbf{E}_{n/p} K| \leqslant |\mathbf{E}_n : \mathbf{E}_{n/p}| = \varphi(n)/\varphi(n/p)$, where φ is Euler's function and $n = |G|$. Thus, if $p^2 \nmid n$, then $|K[G] : K[G^p]| \leqslant p - 1$. Consequently, if G^p is a block stabiliser for G, then $p^2 \mid n$. The converse holds for $K = \mathbf{Q}$ but not in general. For example, $\langle \zeta_{p^2} \rangle \leqslant \mathrm{GL}_1(\mathbf{E}_{p^2})$ is primitive; note that linear groups of degree 1 are vacuously primitive, since there are no proper subspaces at all and hence neither proper submodules nor blocks.

10.8 Remark. Suppose that $K/\mathbf{Q}$ is finitely generated. By Proposition 7.4, the order $|G|$ in Proposition 10.6 is then "small". Thus, it is feasible to test primitivity of G by looping over all primes p with $p^2 \mid |G|$ and testing if $|K[G] : K[G^p]| = p$ for any of them. In practice, we will know a generator, g say, of G. The degree

$|K[G] : K[G^p]|$ can then be effectively computed using the degrees of the minimal polynomials of g and g^p.

10.3. Primitivity testing of ANC groups

In this section, we describe how primitivity of an irreducible non-abelian ANC group $G \leqslant \mathrm{GL}(V)$ can be tested. By Corollary 10.5, it suffices to test if some maximal subgroup of G is a block stabiliser. The maximal subgroups of G can easily be described (Section 10.3.1). In §10.3.2, we will see that in order to test if some maximal subgroup $H < G$ is a block stabiliser, it is not necessary to construct an irreducible $K[H]$-submodule of V. We also describe the construction of a block for G in the case that H is found to be a block stabiliser. In the important cases that K is a number field, a rational function field over a number field, or $\sqrt{-1} \in K$, we describe simplifications in §§10.3.4–10.3.5.

Throughout this section, $G \leqslant \mathrm{GL}(V)$ is an irreducible non-abelian ANC group and $A \triangleleft G$ is cyclic with $|G : A| = 2$. We assume that A is irreducible; otherwise, we obtain a (non-trivial) system of imprimitivity for G via Lemma 10.3.

10.3.1. Maximal subgroups of G

Recall that $G = \langle a, g\rangle$, where $A = \langle a\rangle$ and $g^2 = \vartheta(G) \cdot 1_V$. In practice, such elements can be found as explained in §8.4.1. Write $a = a_2 a_{2'}$ according to $A = A_2 \times A_{2'}$. The two subgroups of index 2 in G (distinct from A) are $H_1 = \langle a^2, g\rangle$ and $H_2 = \langle a^2, a_2 g\rangle$. If p is an odd prime divisor of $|G|$, then $G^p = \langle a^p, g\rangle$ is the unique subgroup of index p in G. Recall from §10.2 that if $K/\mathbf{Q}$ is finitely generated, then $|A|$, and hence also $|G| = 2|A|$, is "small" in terms of $|V : K|$. Hence, if $K/\mathbf{Q}$ is finitely generated, then it is feasible to loop over all maximal subgroups of G. Also note that if $H < G$ is any maximal subgroup of G, then H is itself an ANC group.

10.9 Lemma. *Let $H < G$ be a maximal subgroup with $A \neq H$, say $|G : H| = p$.*

(i) $|H : A^p| = 2$.

(ii) $A^p = \mathrm{C}_H(A^p)$ *unless* $G_2 \cong \mathrm{Q}_8$ *and* $p = 2$.

(iii) If $G_2 \cong \mathrm{Q}_8$ *and* $p = 2$, *then* $H \cong A$ *is irreducible.*

Proof. Parts (i) and (ii) follow from the above description of the maximal subgroups of G; for (ii), note that unless $G_2 \cong \mathrm{Q}_8$ and $p = 2$, the group H is non-abelian whence A^p is maximal abelian and therefore self-centralising in H.

Let $G_2 \cong \mathrm{Q}_8$ and $p = 2$. Let $Z = \mathrm{Z}(K[G])$. By Lemma 8.4, we have $Z = K[G_{2'}]$. Since $A_2 \cong \mathrm{C}_4$ is irreducible over Z but non-central, $X^2 + 1$ is irreducible over Z so that $|V : Z| = 2$. We see that irreducibility H over K is equivalent to that of $H_2 \cong \mathrm{C}_4$ over Z. Let $H_2 = \langle h\rangle$. The minimal polynomial f of h over Z has degree at most 2 and it divides $X^4 - 1 = (X + 1)(X - 1)(X^2 + 1)$, where all factors are irreducible. Hence, $f = X^2 + 1$ and H_2 is indeed irreducible over Z. ♦

10.10 Corollary. *Every maximal subgroup of G is homogeneous.*

Proof. If $A \neq H < G$ is maximal, then $K[H]$ is simple by Proposition 8.2 and Lemma 10.9. ♦

10.3.2. A characterisation of block stabilisers

Let $A \neq H < G$ be a maximal subgroup of index p. We derive conditions for H to be a block stabiliser for G. In view of Lemma 10.9, if $G_2 \cong \mathrm{Q}_8$, then we also assume that p is odd.

10.11 Lemma. *H is a block stabiliser for G if and only if $|K[A] : K[A^p]| = p$ and H is split homogeneous.*

Proof. By irreducibility of A, we have $|V : K[A]| = 1$. Let $U \leqslant V$ be an irreducible $K[H]$-submodule. Since H is homogeneous by Corollary 10.10, it acts faithfully on U. Proposition 8.2 shows that $|U : K[A^p]| = 2^\lambda$, where $\lambda = 0$ or $\lambda = 1$, depending on whether H is split homogeneous or not. Thus, it follows from Lemma 10.2 that H is a block stabiliser for G if and only if $|G : H| = |V : K|/|U : K|$. This is equivalent to $p = 2^{-\lambda}|K[A] : K[A^p]|$. Since $|K[A] : K[A^p]| \leqslant p$, the latter condition is satisfied precisely when $\lambda = 0$ and $|K[A] : K[A^p]| = p$. ♦

It remains to decide if the various maximal subgroups $H < G$ are split homogeneous. Among the two subgroups H_1 and H_2 of index 2 in G (see §10.3.1), we may ignore H_2 by the following.

10.12 Lemma. *If H_2 is a block stabiliser for G, then so is H_1.*

Proof. Note that the condition $|K[A] : K[A^2]| = 2$ in Lemma 10.11 is the same for H_1 and H_2. The result follows since if H_1 is not split homogeneous, then $\vartheta(H_1) = -1$. However, this only happens for $\vartheta(G) = \vartheta(H_2) = -1$, whence H_2 is not split homogeneous by Corollary 8.6(ii). ♦

We can therefore test primitivity of G by using Lemma 10.11 and Corollary 8.6 as follows: we simply test if H_1 or any of the subgroups G^p (where p is an odd prime divisor of $|G|$) is a block stabiliser. Note that in order to merely decide primitivity of G without constructing a block, we do not need to actually solve any of the equations $x^2 + y^2 = -1$ in Corollary 8.6(ii).

10.3.3. Constructing a block

Setup. Let $G = \langle a, g\rangle$ be as in §10.3.1. Suppose that $H < G$ is a maximal subgroup of index p which is a block stabiliser for G. By Lemma 10.12, we may assume that $\vartheta(G) = \vartheta(H)$ and that $H = \langle b, g\rangle$, where $b = a^p$.

We now consider the construction of a block for G which is stabilised by H. Since H is homogeneous (Corollary 10.10), this is equivalent to constructing an irreducible $K[H]$-submodule of V (Lemmas 10.1–10.2). What follows is a slight variation of the general method for irreducibility testing of ANC groups described in §8.4.

Dihedral and semidihedral case. First, let $\vartheta(G) = 1$ (and so $\vartheta(H) = 1$). Since g is not scalar but $g^2 = 1$, there exists $0 \neq v \in V$ with $vg = \pm v$. It follows that $v \cdot K[H] = v \cdot K[b]$ is irreducible as a $K[b]$-module and hence also as a $K[H]$-module.

Generalised quaternion case. Now let $\vartheta(G) = -1$. Let $|G| = 2n$. Define $L = K[b]$ and $Z = \mathrm{Z}(K[H])$; note that Lemmas 8.4–8.5 give us an explicit isomorphism between the towers $L/Z/K$ and $\mathbf{E}_{n/p}K/\mathbf{E}^+_{n/p}K/K$. Since H is split homogeneous (Lemma 10.11), -1 is a sum of two squares in Z (Corollary 8.6(ii)). Equivalently, there exists $z \in L$ with $\mathrm{N}_{L/Z}(z) = -1$. Since H is reducible by assumption, the regular $K[H]$-module is a direct summand of V as a $K[H]$-module. It thus follows from Proposition 8.7 that $\mathrm{Ker}(g + z) \neq 0$. Choose a non-zero $v \in \mathrm{Ker}(g + z)$. Then $v \cdot K[H] = v \cdot K[A^p]$ is an irreducible $K[H]$-submodule. Conversely, we recover a solution $z \in L$ of $\mathrm{N}_{L/Z}(z)$ from any generator of an irreducible $K[H]$-submodule of V as in Proposition 8.7(ii).

As we remarked in §10.1, given any non-trivial system of imprimitivity for G, we may construct one of prime size. Let $G \leqslant \mathrm{GL}(V)$ be an irreducible imprimitive ANC group. Suppose that $G_2 \cong \mathrm{Q}_{2^j}$ $(j \geqslant 3)$ and that the cyclic subgroup of index 2 in G is irreducible, Then finding a non-trivial system of imprimitivity is equivalent to solving $x^2 + y^2 = -1$ in one of the fields Z corresponding to a maximal subgroup $H < G$ (of odd index if $j = 3$; see Lemma 10.9) which is a block stabiliser. Note that there may in general be different possible choices for H and hence for Z.

10.3.4. Block stabilisers over number fields

We show that if K is a number field, then in the majority of cases, the simple condition $|K[A] : K[A^p]| = p$ already determines if $H < G$ with $|G : H| = p$ prime is a block stabiliser for G.

10.13 Proposition. *Suppose that K is a number field. Let $H < G$ be a maximal subgroup of index p with $\vartheta(G) = \vartheta(H)$. Suppose that one of the following conditions is satisfied: p is odd, $\vartheta(G) = 1$, or $|G_2| \geqslant 32$. Then H is a block stabiliser for G if and only if $|K[A] : K[A^p]| = p$.*

Proof. By Lemma 10.11, $|K[A] : K[A^p]| = p$ is necessary for H to be a block stabiliser. It remains to determine if H is split homogeneous. Let $n = |A|$ and suppose that $|K[A] : K[A^p]| = p$. If $\vartheta(G) = 1$, then H is split homogeneous by Corollary 8.6(i) and the result follows.

Let $\vartheta(G) = -1$. Define the logical value $s(F)$ for a field F to be true precisely when -1 is a sum of two squares in F. Since G is split homogeneous by irreducibility of A (Corollary 8.3), we know that $s(\mathbf{E}^+_n K)$ is true. Write $n = p^a m$ for $p \nmid m$. As we noted in Remark 10.7, $a \geqslant 2$. Let p be odd. By Lemma 9.4, we have $s(\mathbf{E}^+_n K) = s(\mathbf{E}_{p^a}(\mathbf{E}^+_m K)) = s(\mathbf{E}_{p^{a-1}}(\mathbf{E}^+_m K)) = s(\mathbf{E}^+_{n/p} K)$. Hence, H is split homogeneous and thus a block stabiliser for G. Finally, let $p = 2$. Then $a \geqslant 4$ by assumption. Since $s(\mathbf{E}^+_n K)$ is true, so is $s(\mathbf{E}^+_{n/2} K)$ by Lemma 9.3. ♦

Recall that the case $G_2 \cong \mathrm{Q}_8$ and $p = 2$ is ruled out by Lemma 10.9, i. e. none of the subgroups of index 2 of G can be a block stabiliser in this situation. Thus, for a maximal subgroup $H < G$ of index p, Proposition 10.13 covers all cases but one: $G_2 \cong \mathrm{Q}_{16}$ and $p = 2$. In this case, $\mathrm{Z}(K[H]) \cong_K \mathbf{E}^+_{4m}K = \mathbf{E}_m K$ (where $|G| = 16m$), and we may apply Lemma 9.3(iii) to decide if H is split homogeneous; note that $\mathbf{E}_m K$ is totally imaginary since this is the case for $\mathrm{Z}(K[G]) \cong_K \mathbf{E}^+_{8m}K = (\mathbf{E}_m K)(\sqrt{2})$.

10.3.5. Other fields

Function fields. Let E be a number field and $K = E(\mathbf{X})$, where $\mathbf{X} = (X_1, \ldots, X_r)$ is algebraically independent over E. Then Proposition 10.13 remains valid for such a field K. Indeed, using the facts from §3.6 and Proposition 9.9, we see that $x^2 + y^2 = -1$ has a solution in $\mathbf{E}^+_n K$ if and only if it has a solution in $\mathbf{E}^+_n E$ (any $n \geqslant 1$). The proof of Proposition 10.13 now immediately carries over to this case, as do the comments following it.

Fields containing $\sqrt{-1}$. Suppose that K is a field of characteristic zero with $\sqrt{-1} \in K$ and such that (F1) is satisfied. We now briefly discuss how we may test primitivity of finite nilpotent linear groups over K under these assumptions.

Given an irreducible finite nilpotent group $G \leqslant \mathrm{GL}(V)$, we can use the function NoncyclicAbelian (Algorithm 7.1) and either (i) construct a non-cyclic abelian normal subgroup and hence a system of imprimitivity for G, or (ii) we can prove that G is an ANC group. As shown in §8.4.4, if G is a non-abelian ANC group and $A \lhd G$ is cyclic with $|G : A| = 2$, then A is necessarily inhomogeneous if $\sqrt{-1} \in K$. It therefore only remains to test primitivity of cyclic groups, which can be done as in §10.2.

11. Algorithms for irreducibility and primitivity testing

In this chapter, we describe our main algorithms for irreducibility and primitivity testing of finite nilpotent linear groups. We also comment on our implementation in the MAGMA-package *finn* and provide sample run-times. Throughout this chapter, we assume that K is a field of characteristic zero such that conditions (F1)–(F2) from §8.1 are satisfied. This chapter is based on [74, §§7,9] and [75, §§9–10].

11.1. An algorithm for irreducibility testing of finite nilpotent groups

We are now in a position to describe our main algorithm for irreducibility testing of finite nilpotent linear groups over K. In contrast to Algorithm 5.1, Algorithm 11.1 is fully constructive: a proper submodule is constructed whenever it exists. Note that, as in Chapter 5, we only return generators of such submodules.

Algorithm 11.1 IsIrreducible(G) (finite case, fully constructive)

Input: a finite nilpotent $G \leqslant \mathrm{GL}(V)$
Output: `true` if G is irreducible or `false` and a generator of a proper submodule

1: **loop**
2: **if** G is abelian **then**
3: $homg \leftarrow$ HomogeneousDecompositionAbelian(G)
4: **if** $|homg| > 1$ **then return** `false`, NonzeroElement($homg[1]$)
5: $x \leftarrow$ NonzeroElement(V)
6: **if** $x \cdot K[G] < V$ **then return** `false`, x **else return** `true`
7: $A \leftarrow$ NoncyclicAbelian(G)
8: **if** $A =$ `fail` **then** let A be a cyclic subgroup of index 2 in G
9: $homg \leftarrow$ HomogeneousDecompositionAbelian(A), $U \leftarrow homg[1]$
10: **if** $|homg| = 1$ **then return** IsIrreducibleANC(G, A)
11: **if** G acts intransitively on $homg$ **then return** `false`, NonzeroElement(U)
12: $G \leftarrow \mathrm{Im}(\theta)$, $V \leftarrow U$ where $\mathrm{Stab}_G(U) \xrightarrow{\theta} \mathrm{GL}(U)$ is the induced action

11.1 Remark. If we only wish to decide irreducibility without ever constructing a submodule, then Algorithm 11.1 can be naturally simplified. In this case we do not need to actually solve any of the equations $x^2 + y^2 = -1$ arising in IsIrreducibleANC (Algorithm 8.1). In this situation, condition (F2) can therefore be relaxed to

(F2$^\flat$) For any $n \geqslant 1$, we may decide if $x^2 + y^2 = -1$ has a solution in $\mathbf{E}_n^+ K$.

11.2. An algorithm for primitivity testing of finite nilpotent groups

What follows is an algorithm for primitivity testing of irreducible finite nilpotent linear groups over K. For the important case of number fields, we illustrate how the specialised techniques described in §10.3.4 can be applied (see lines 11–13).

To simplify our pseudo-code, for an imprimitive group G we return a block for G instead of a full system of imprimitivity. The system of imprimitivity containing a given block can be obtained using an orbit-stabiliser computation [39, §4.1].

Algorithm 11.2 IsPrimitive(G)

Input: an irreducible finite nilpotent $G \leqslant \mathrm{GL}(V)$
Output: `true` if G is primitive, or `false` and a block for G

1: **if** G is abelian **then**
2: **if** there exists a prime p with $p^2 \mid |G|$ and $|K[G] : K[G^p]| = p$ **then**
3: **return** `false`, NonzeroElement(V) $\cdot\, K[G^p]$
4: **return** `true`
5: $A \leftarrow$ NoncyclicAbelian(G)
6: **if** $A =$ `fail` **then** let A be a cyclic subgroup of index 2 in G
7: **if** A is inhomogeneous **then return** `false`, HomogeneousDecompositionAbelian(A)[1]
8: find $\vartheta(G)$ and $g \notin A$ with $g^2 = \vartheta(G) \cdot 1_V$ as in §10.3.1
9: **if** A is reducible **then return** `false`, NonzeroElement(V) $\cdot\, K[A]$
10: $S \leftarrow \{p : \ p \text{ is an odd prime with } p^2 \mid |G| \text{ and } |K[A] : K[A^p]| = p\}$
11: **if** K is a number field **then**
12: $q \leftarrow \vartheta(G) = 1$ **or** $|G_2| \geqslant 32$ **or**
$\big(G_2 \cong \mathrm{Q}_{16}$ **and** ord $(2 \bmod |G_{2'}|) \cdot |K_\mathfrak{p} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p} \mid 2$ of $K\big)$
13: **if** $|K[A] : K[A^2]| = 2$ **and** $q =$ `true` **then** $S \leftarrow S \cup \{2\}$
14: **else**
15: **if** $G_2 \ncong \mathrm{Q}_8$ **and** $|K[A] : K[A^2]| = 2$ **then** $S \leftarrow S \cup \{2\}$
16: **if** $\vartheta(G) = -1$ **then** $S \leftarrow \{p \in S : \exists x, y \in \mathbf{E}_{n/p}^+ K.\ x^2 + y^2 = -1\}$, where $n = |A|$
17: **if** $\exists p \in S$ **then**
18: **if** $\vartheta(G) = 1$ **then** $b \leftarrow 1_V$ **else** find $b \in K[A^p]$ with $b \cdot b^g = -1_V$
19: **return** `false`, NonzeroElement(Ker$(g - b)) \cdot K[A^p]$
20: **return** `true`

11.2 Remarks.

(i) As explained in §10.3.3, solving the norm equation $b \cdot b^g = -1_V$ in line 18 is equivalent to solving $x^2 + y^2 = -1$ in $K[A^p]^G \cong \mathbf{E}_{n/p}^+ K$, where $n = |A|$; we can do this since we assumed that condition (F2) holds for K.

(ii) Similar to the case of irreducibility testing above, Algorithm 11.2 can be simplified if we only wish to decide primitivity of G without ever constructing a block. Again, condition (F2) can then be weakened to (F2$^\flat$).

(iii) Because of randomisations employed in NoncyclicAbelian (Algorithm 7.1), different applications of IsPrimitive to a given group G may produce different subgroups A in line 5. As a consequence, repeated calls of IsPrimitive can return different systems of imprimitivity for the same input group. Further note that a system of imprimitivity obtained using IsPrimitive will in general be refinable. Repeated application can be used to obtain a non-refinable system of imprimitivity; cf. [85, Lem. 15.2].

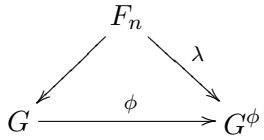
11.3. The use of congruence homomorphisms

Intrinsic computations. In contrast to Algorithm 5.1, the above two algorithms do not depend on a congruence homomorphism mapping the input group to a linear group over a finite field. In practice, however, congruence homomorphisms are valuable here too.

Note that for a finite $G \leqslant \mathrm{GL}_d(K)$, a congruence homomorphism $G \to G^\phi$ with torsion-free congruence subgroup is an isomorphism. Many of the computation in Algorithms 11.1–11.2 only rely on intrinsic group-theoretic properties of G. In practice, such computations for matrix groups over finite fields are usually considerably faster than their counterparts in characteristic zero. In our implementation, we therefore perform such intrinsic computations in the congruence image G^ϕ. For example, we compute a non-cyclic abelian normal subgroup of G^ϕ (or prove that none exists) and then lift it to a subgroup of G.

Lifting. We now briefly describe the details of the aforementioned lifting step. Define a signature Σ (in the sense of universal algebra; cf. [15, Ch. 1]) consisting of the following operations: multiplication $\cdot$, commutation $[-,-]$, conjugation $\hat{}$ (all binary), and a unary exponentiation $(-)^n$ for each $n \in \mathbf{Z}$. Of course, groups are naturally Σ-algebras.

We assume that G above is given by a finite generating sequence, $(g_1, \ldots, g_n)$ say. Let F_n be the free Σ-algebra on n symbols $x_1, \ldots, x_n$. We then have natural Σ-homomorphisms from F_n onto G and G^ϕ rendering



commutative. All our computations in G^ϕ produce elements which are Σ-words in $g_1^\phi, \ldots, g_n^\phi$. For each element $h \in G^\phi$ constructed as part of our algorithms, we store a pair $(h, f) \in G^\phi \times F_n$ with $h = f\lambda$. In this way, we can effectively compute $h^{\phi^{-1}}$ by evaluating f in G.

The main reason why we use Σ-words instead of words in the free group on n generators is that several of our algorithms construct commutators $c = [c_1, \ldots, c_r]$. The length of such an element c as a group word is exponential in r but it is linear as a

Σ-word. In practice, working with group words can thus be prohibitively expensive. Recall from §2.6 and §3.8 that over number fields and rational function fields over number fields, nilpotent linear groups have small nilpotency class in terms of the degree.

Finally, we chose Σ-words over straight-line programs since evaluating the latter involves matrix inversion which can be expensive in practice. Our method only involves inverses of the defining generators of G and these are computed by the matrix group constructor of Magma.

11.4. The Magma package *finn*

The Magma-package *finn* [76] contains an implementation of our algorithms for irreducibility and primitivity testing of finite nilpotent linear groups $G \leqslant \mathrm{GL}(V)$, where the underlying field K is a number field or a rational function field over a number field. We note that the core functions provided by *finn* have been included in Magma V2.17.

Since our algorithms for irreducibility and primitivity testing share common ingredients, we provide a function which simultaneously tests irreducibility and primitivity of a finite nilpotent linear group. This function will thus determine if the input group is (a) reducible, (b) imprimitive but irreducible, or (c) primitive. In the cases (a)–(b), it will then proceed to construct a submodule (resp. a system of imprimitivity), unless the user requested to merely decide to which of the three classes (a)–(c) the input group belongs.

11.5. Example run-times

All run-times below were obtained on an Intel Xeon E5440 with 16GB RAM running the 64-bit version of Magma V2.17-3 under Linux. Up to differences arising from randomisations (see below), the examples below are available in *finn*.

11.5.1. Irreducibility testing for $K = \mathbf{Q}$

The main focus of our implementation has been on the case of linear groups over the rationals. In this situation, our implementation competes with functionality built into Magma V2.16. The following is from the "Summary of New Features in Magma V2.16" (available from the Magma website [55]):

> A new Meataxe algorithm has been developed for splitting general A-modules, where A is a finite dimensional matrix algebra defined over the rational field. This yields an effective algorithm for decomposing a module into indecomposable summands.

Note that this solves a more general problem than our algorithm.

Table 11.1 shows run-times of irreducibility testing for linear groups over the rationals. The examples given cover many of the cases that can occur within Algorithm 11.1. For each group, we give data on the group ("group"), its degree ("deg"), the number of defining generators ("gens"), an entry ("irr?") indicating whether the group is irreducible, and the dimension of the submodule constructed by our algorithm in the reducible case ("dim"). We also give approximations of the largest absolute values of the numerators ("num") and denominators ("den") of the matrix entries in the defining generators. Next, the time in seconds (unless otherwise indicated) irreducibility testing took using our algorithm is given under "time-f". Finally, we also give the time ("time-M") it took for the MAGMA function INDECOMPOSABLESUMMANDS to decompose the natural $\mathbf{Q}G_i$-module (obtained using the MAGMA function GMODULE) into a direct sum of irreducibles.

group	deg	gens	num	den	irr?	dim	time-f	time-M
$G_1 \cong \mathrm{Q}_8 \curlyvee \mathrm{Q}_8$ (central prod.)	16	5	1	1	no	4	0.01	0.15
$G_2 \cong W_{2,5} \times W_{3,2}$	22	11	1	1	no	16	0.02	19.37min
$G_3 \cong \mathrm{C}_2^4 \rtimes \mathrm{C}_2^2$	8	8	25391	2156	no	4	0.02	0.01
G_4 (order 576, class 3)	14	8	$1.55 \cdot 10^{10}$	$1.99 \cdot 10^{8}$	no	4	0.02	0.02
G_5 (order 16,384, class 4)	16	14	$2.50 \cdot 10^{10}$	$3.14 \cdot 10^{9}$	no	8	0.10	0.02
$G_6 \cong (\mathrm{Q}_8 \times \mathrm{C}_5) \otimes W_{3,2}$	48	8	2	1	yes	–	0.08	30.06min
$G_7 \cong \mathrm{C}_3 \ltimes \mathrm{C}_3^2$	18	3	$7.60 \cdot 10^{6}$	$3.13 \cdot 10^{5}$	no	6	0.03	0.27
$G_8 \cong (\mathrm{Q}_{16} \times \mathrm{C}_3) \otimes W_{3,2}$	96	10	137	24	yes	–	0.52	0.97
$G_9 \cong \mathrm{D}_{32} \times \mathrm{C}_{11}$	80	5	$3.00 \cdot 10^{8}$	$2.08 \cdot 10^{6}$	yes	–	0.10	2.67
$G_{10} \cong W_{2,5} \otimes W_{3,2}$	96	11	1	1	yes	–	0.38	3h 29min
$G_{11} \cong 5^{1+2}$	100	5	1	1	no	20	0.17	122.78
$G_{12} \cong \mathrm{Q}_{32} \times \mathrm{C}_{11}$	160	5	1	1	no	80	0.26	2h 40min
$G_{13} = G_2$	22	100	1	1	no	16	0.12	27min
$G_{14} = G_3^x$	8	8	$3.20 \cdot 10^{32}$	$5.22 \cdot 10^{29}$	no	4	0.08	0.05

Table 11.1. Irreducibility testing over the rationals

The group $W_{p,i}$ is $\mathrm{C}_p \wr \cdots \wr \mathrm{C}_p$ (i factors) realised as an irreducible Sylow p-subgroup of $\mathrm{GL}_d(\mathbf{Q})$, where $d = (p-1)p^{i-1}$; see §2.5. We did not use the "natural" generating sets for any of the groups in Table 11.1. Instead, we added a randomisation step by applying the product replacement algorithm [11] to copies of the original generating sets. The groups G_2 and G_{13} only differ in their defining generating sets; G_{14} is a conjugate of G_3. These two examples are meant to illustrate the impact the number of generators (resp. the size of the entries in the matrices) has on the performance of our algorithm.

For G_{12}, constructing a submodule amounts to solving $x^2 + y^2 = -1$ in $\mathbf{E}_{16 \cdot 11}^+$; cf. §8.4. In fact, $x^2 + y^2 = -1$ can be solved in $\mathbf{E}_{11}$. As remarked in Example 9.8, explicit solutions of these equations are known over cyclotomic fields whenever they exist; *finn* then uses these. We do not provide run-times for cases where a norm equation solver is actually used since, apart from small examples and special cases, such computations are infeasible. Apart from this exceptional behaviour involving $x^2 + y^2 = -1$, in our experiments over the rationals, constructing submodules took little extra time in addition to deciding irreducibility.

11.5.2. Irreducibility testing over other fields

To illustrate the performance of our algorithm over extensions of $\mathbf{Q}$, we now consider groups over the fields $\mathbf{Q}(\gamma)$ and $\mathbf{Q}(X)$, where γ satisfies $\gamma^3 - \gamma^2 + 1 = 0$ and X is transcendental over $\mathbf{Q}$. As input groups, we use (irrational) conjugates $G_{i,\gamma}$ and $G_{i,X}$ of G_i in $\mathrm{GL}_{d_i}(\mathbf{Q}(\gamma))$ and $\mathrm{GL}_{d_i}(\mathbf{Q}(X))$, respectively, where d_i is the degree of G_i (see Table 11.1). The conjugating matrices were chosen such that no additional coefficient explosion occurred in the transition from G_i to $G_{i,\gamma}$ or $G_{i,X}$; here the "coefficients" are those of the rational polynomials used to represent field elements.

It turns out that each of the groups $G_{i,\gamma}$ (resp. $G_{i,X}$) is irreducible over $\mathbf{Q}(\gamma)$ (resp. $\mathbf{Q}(X)$) if and only if G_i is irreducible over $\mathbf{Q}$. In Tables 11.2–11.3, we list the resulting run-times obtained using our algorithm ("time-f", as above). For reducible groups, the columns labelled "vector-mode" show how long it took to construct a vector which generates a proper submodule. The discrepancies between the full times and those in "vector-mode" for the groups $G_{12,\gamma}$ and $G_{12,X}$ arose from coefficient explosions occurring in the construction of a submodule.

Since run-times of basic linear algebra quickly increase as the underlying field K becomes "larger" and, furthermore, the underlying linear algebra in Magma is heavily optimised over the rationals, in practice, K is restricted to being a "small" extension of $\mathbf{Q}$; [76] provides further irrational conjugates of the G_i that illustrate this.

group	time-f	vector-mode
$G_{1,\gamma}$	0.04	0.04
$G_{2,\gamma}$	0.09	0.08
$G_{3,\gamma}$	0.04	0.03
$G_{4,\gamma}$	0.21	0.19
$G_{5,\gamma}$	1.49	1.38
$G_{6,\gamma}$	0.70	–
$G_{7,\gamma}$	0.61	0.55
$G_{8,\gamma}$	30.18	–
$G_{9,\gamma}$	8.71	–
$G_{10,\gamma}$	1.75	–
$G_{11,\gamma}$	4.12	3.79
$G_{12,\gamma}$	22.73	2.42
$G_{13,\gamma}$	0.43	0.38
$G_{14,\gamma}$	0.14	0.12

Table 11.2. Irred. testing over $\mathbf{Q}(\gamma)$

group	time-f	vector-mode
$G_{1,X}$	0.09	0.07
$G_{2,X}$	0.32	0.27
$G_{3,X}$	0.21	0.15
$G_{4,X}$	1.07	0.92
$G_{5,X}$	26.15	20.81
$G_{6,X}$	2.18	–
$G_{7,X}$	4.00	3.12
$G_{8,X}$	5.37min	–
$G_{9,X}$	28.40	–
$G_{10,X}$	4.22	–
$G_{11,X}$	32.96	25.24
$G_{12,X}$	12h 34min	5.05
$G_{13,X}$	1.17	0.83
$G_{14,X}$	1.60	1.12

Table 11.3. Irred. testing over $\mathbf{Q}(X)$

11.5.3. Primitivity testing over Q

Table 11.4 shows run-times for primitivity testing over the rationals. In addition to information as in Table 11.1, we indicate whether the group was found to be primitive ("prim?"). For an imprimitive group, we also give the size of the system of imprimitivity constructed ("size"). Two different run-times (all in seconds) of primitivity testing are given for each group. The first ("total") includes irreducibility testing and the construction of a system of imprimitivity in the imprimitive

case. We then repeated the computation without testing irreducibility and without ever constructing a system of imprimitivity; the resulting run-time is also shown ("decide"). All the groups considered here are irreducible.

group	deg	gens	num	den	prim?	size	total	decide
$H_1 \cong 5^{1+2}$	20	4	7	3	no	5	0.02	0.01
$H_2 \cong W_{7,2}$	42	7	34,387	6204	no	7	0.28	0.02
H_3 (order $2^5 5^3$, class 3)	80	4	$4.94 \cdot 10^6$	$1.91 \cdot 10^5$	no	2	0.74	0.25
$H_4 \cong W_{2,5} \otimes W_{3,2}$	96	11	1	1	no	2	0.37	0.08
$H_5 \cong \mathrm{Q}_8 \times \mathrm{C}_{11}$	20	5	$7.1 \cdot 10^7$	$3.34 \cdot 10^6$	yes	–	0.02	0.02
$H_6 \cong \mathrm{Q}_{16} \times \mathrm{C}_7$	24	5	$3.2 \cdot 10^{11}$	$3.68 \cdot 10^{10}$	yes	–	0.04	0.04
$H_7 \cong \mathrm{D}_{16} \times \mathrm{C}_{11}$	40	5	$1.26 \cdot 10^{11}$	$2.21 \cdot 10^9$	no	2	0.12	0.09
$H_8 \cong \mathrm{Q}_{16} \times \mathrm{C}_{25}$	160	5	$5.6 \cdot 10^7$	$4.76 \cdot 10^6$	no	5	0.84	0.48

Table 11.4. Primitivity testing over the rationals

As before, we again made use of the product replacement algorithm to obtain generating sets. The groups H_1 has been obtained from G_{11} in Table 11.1. The practical limitations of primitivity testing are the same as for irreducibility testing.

11.5.4. Primitivity testing over other fields

In Table 11.5, we provide run-times for groups over proper extensions of the rationals. All of these groups are generated by matrices with moderately sized entries.

group	field	degree	gens	prim?	size	total	decide
$H_9 \cong \mathrm{D}_{16} \wr \mathrm{C}_4$	$\mathbf{Q}(\sqrt{2})$	8	8	no	2	0.07	0.01
$H_{10} \cong \mathrm{C}_{49} . \mathrm{C}_{49}$ (non-split ext.)	$\mathbf{Q}(\zeta_{49})$	7	5	no	7	1.08	0.17
H_{11} (order 3^{40}, class 27)	$\mathbf{Q}(\sqrt{-3})$	27	9	no	3	1.39	0.05
H_{12} (order $2^3 5^5$, class 4)	$\mathbf{Q}(X)$	40	5	no	5	4.69	0.02
$H_{13} \cong \mathrm{SD}_{16} \times \mathrm{C}_5$	$\mathbf{Q}(\sqrt{-2})$	8	5	yes	–	0.04	0.04
$H_{14} \cong \mathrm{SD}_{32} \times \mathrm{C}_5$	$\mathbf{Q}(\sqrt[4]{2})$	16	5	no	2	0.42	0.36

Table 11.5. Primitivity testing over fields other than $\mathbf{Q}$

Part III.

The structure of primitive finite nilpotent linear groups

12. Irreducible ANC groups

Throughout this chapter, let K be an arbitrary subfield of the complex field $\mathbf{C}$.

Recall from Chapter 7 that an ANC group is a finite nilpotent group all of whose abelian normal subgroups are cyclic. These groups have been completely classified up to isomorphism (Theorem 7.1). We have seen that every primitive finite nilpotent linear group is an ANC group. In this chapter, we investigate irreducible ANC groups over K. This is a first major step towards a classification of primitive (or, more generally, irreducible) finite nilpotent linear groups over K; we note that primitive nilpotent linear groups over finite fields have been classified up to similarity [19, 20]. The goal of this chapter (to be achieved in §12.4) is to prove the following.

12.1 Proposition.

(i) Every ANC group has a faithful irreducible K-representation.

(ii) Isomorphic irreducible linear ANC groups over K are similar.

We note the following immediate consequence; the corresponding statement for primitive nilpotent linear groups over finite fields has been known [19, Prop. 4.5].

12.2 Corollary. *Two primitive finite nilpotent linear groups over K which are isomorphic as abstract groups are similar (over K).* ♦

Apart from the ubiquitous issue of solving $x^2 + y^2 = -1$ in extensions of K, the proof we give for the existence part (i) in Proposition 12.1 is constructive.

12.1. Cyclic groups

First, we consider the easy case of cyclic groups in Proposition 12.1. We write $g \approx h$ (resp. $G \approx H$) to signify similarity of linear maps and linear groups, respectively.

Regarding the existence part, $H = \langle \zeta_m \rangle \leqslant \mathrm{GL}_1(\mathbf{E}_m K)$ is irreducible when considered as a K-linear group. Uniqueness up to similarity is a consequence of the following simple fact.

12.3 Lemma. *Let $G = \langle g \rangle$ and H be homogeneous finite cyclic linear groups over K. If $G \cong H$, then there exists a generator $h \in H$ such that $g \mapsto h$ induces a K-isomorphism $K[G] \to K[H]$.*

Proof. Write $m = |G| = |H|$. The mth cyclotomic polynomial ϕ_m splits completely both over $K[G]$ and over $K[H]$. Let $f = \mathrm{mpol}_K(g)$. Then $f \mid \phi_m$ so there exists $h \in K[H]$ with $f(h) = 0$. As $K[H]$ is a field, the roots of $X^m - 1$ in $K[H]$ are

precisely the elements of H. Since h is a primitive mth root of unity, we conclude that $H = \langle h \rangle$. Clearly, $g \mapsto h$ is an isomorphism with the properties stated. ♦

In particular, g and h have the same minimal polynomials over K. Hence, if G and H are both irreducible, then $g \approx h$ and thus $G \approx H$. This completes the proof of Proposition 12.1 for cyclic groups.

12.2. Schur indices and the structure of K-representations of a finite group

We briefly recall some well-known facts from representation theory. Throughout, let G be a finite group. If $\chi \in \mathrm{Irr}(G)$ is an ordinary irreducible character of G, then there exists a finite extension L of the character field $K(\chi)$ such that χ is afforded by an LG-module. The **Schur index** $\mathrm{m}_K(\chi)$ of χ over K is the smallest possible degree $|L : K(\chi)|$ of such an extension; see [17, §70], [44, §10], [43, §38] for details.

Let ψ be the character of an irreducible KG-module. By [17, Thm 70.15], there exists $\chi \in \mathrm{Irr}(G)$ such that $\psi = \mathrm{m}_K(\chi)\left(\sum_{\sigma\in\Gamma} \chi^\sigma\right)$, where $\Gamma = \mathrm{Gal}(K(\chi)/K)$. The conjugates $\chi^\sigma \in \mathrm{Irr}(G)$ are distinct. If the KG-module V affords ψ, then the above decomposition of ψ can be found by splitting the EG-module $V_E = V \otimes_K E$, where $E \supseteq K$ is a splitting field for G which is finite and normal over K.

Conversely, let $\chi \in \mathrm{Irr}(G)$. Choose $L \supseteq K(\chi)$ with $|L : K(\chi)| = \mathrm{m}_K(\chi)$ such that χ is afforded by an LG-module V. By [43, Ex. 1.6(e)], the character of V as a KG-module is $\mathrm{m}_K(\chi)\left(\sum_{\sigma\in\Gamma} \chi^\sigma\right)$, where again $\Gamma = \mathrm{Gal}(K(\chi)/K)$. The characters χ^σ are distinct and form a Galois conjugacy class over K [44, Lem. 9.17(c)]. Hence, $\mathrm{m}_K(\chi)\left(\sum_{\sigma\in\Gamma} \chi^\sigma\right)$ is the character of an irreducible KG-module [44, Cor. 10.2(b)] and we conclude from [68, 8.3.7] that V is irreducible when regarded as a KG-module.

12.3. Representations of ANC 2-groups

In this section, we recall descriptions of the irreducible $\mathbf{C}$-representations of an ANC 2-group G. We then compute the Schur indices of their characters and construct the faithful irreducible K-representations of G. Recall from §8.3 that for a non-abelian ANC group G, we defined $\vartheta(G) = 1$ if G_2 is (semi)dihedral, and $\vartheta(G) = -1$ if G_2 is generalised quaternion; also, $\delta(G) = 1$ is G_2 is dihedral or generalised quaternion, and $\delta(G) = -1$ if G_2 is semidihdral.

12.4 Proposition (Cf. [49, Prop. 10.1.16])**.** *Let $G = \langle a, g \rangle$ be a non-abelian ANC 2-group, where $\langle a \rangle$ is cyclic of order 2^j and index 2 in G and $g^2 = 1$ if $\vartheta(G) = 1$ and $g^4 = 1$ if $\vartheta(G) = -1$. Then, up to equivalence, the irreducible $\mathbf{C}$-representations of G of degree > 1 (written over the splitting field $\mathbf{E}_{2^j}K$ of G) are precisely given by*

$$\varrho_k^G \colon G \to \mathrm{GL}_2(\mathbf{E}_{2^j}K),\ \ a \mapsto \begin{bmatrix} \zeta_{2^j}^k & . \\ . & \delta(G)^k\zeta_{2^j}^{-k} \end{bmatrix},\ g \mapsto \begin{bmatrix} . & 1 \\ \vartheta(G) & . \end{bmatrix},$$

where $0 < k < 2^{j-1}$; faithful representations correspond precisely to odd values of k.

We henceforth assume that k is odd. Let χ_k^G be the character of ϱ_k^G. Then $K(\chi_k^G) = K(\zeta_{2^j}^k + \delta(G)\cdot\zeta_{2^j}^{-k})$; in particular, all the fields $K(\chi_k^G)$ with k odd are equal (Lemma 8.5).

12.5 Lemma ([49, Prop. 10.1.17(i)])**.** *If $\vartheta(G) = 1$, then $\mathrm{m}_K(\chi_k^G) = 1$.*

For generalised quaternion groups, we use a variation of [49, Prop. 10.1.17(ii)–(iii)]. The case $G \cong \mathrm{Q}_8$ of the following is well-known; cf. [17, p. 470]. Part (i) can also be deduced from [44, Prb. 10.5].

12.6 Lemma. *Let $G \cong \mathrm{Q}_{2^{j+1}}$ and write $\chi = \chi_k^G$, where k is odd.*

(i) $\mathrm{m}_K(\chi) = 1$ if $x^2 + y^2 = -1$ is soluble in $K(\chi)$.

(ii) If -1 is not a sum of two squares in $K(\chi)$, then $\mathrm{m}_K(\chi) = 2$.

Proof. Since ζ_{2^j} is chosen arbitrarily among the primitive 2^jth roots of unity, we may assume that $k = 1$. Write $\theta_i = \zeta_{2^i} + \zeta_{2^i}^{-1}$. The corresponding statements for the equation $x^2 + \theta_j xy + y^2 = -1$ over $K(\chi) = K(\theta_j)$ are given in [49, Prop. 10.1.17(ii)–(iii)]. We will complete the proof by showing that $a_i = \left[\begin{smallmatrix} 1 & \theta_i/2 \\ \theta_i/2 & 1 \end{smallmatrix}\right]$ is congruent to the 2×2 identity matrix over $\mathbf{Q}(\theta_i)$ for any $i \geqslant 2$; in other words, we will show that the quadratic forms $X^2 + \theta_i XY + Y^2$ and $X^2 + Y^2$ are equivalent over $\mathbf{Q}(\theta_i)$.

We may assume that $\zeta_{2^{i+1}}^2 = \zeta_{2^i}$ for any $i \geqslant 1$. It follows that $\theta_i^2 = 2 + \theta_{i-1}$ for $i \geqslant 3$. We therefore have $(2+\theta_i)(2-\theta_i) = 4 - \theta_i^2 = 2 - \theta_{i-1}$. Define $\lambda_3 = \theta_3$ and $\lambda_i = \lambda_{i-1}/\theta_i \in \mathbf{Q}(\theta_i)$ $(i \geqslant 4)$. By induction, $\lambda_i^2 = 2 - \theta_{i-1}$ for $i \geqslant 3$; indeed, for $i \geqslant 4$, we have $\lambda_i^2 = \lambda_{i-1}^2/\theta_i^2 = (2-\theta_{i-2})/(2+\theta_{i-1}) = 2 - \theta_{i-1}$. We obtain $x_i a_i x_i^T = 1$, where $x_2 = 1$ and $x_i = \left[\begin{smallmatrix} 1 & \\ \theta_i/\lambda_i & -2/\lambda_i \end{smallmatrix}\right]$ $(i \geqslant 3)$. ♦

Let $G = \langle a, g\rangle$ be as in Proposition 12.4. We now construct the faithful irreducible K-representations of G. In some cases, these can be obtained by restricting $\varrho_k = \varrho_k^G$ to K. In the more interesting cases, the images of a and g which we give below are taken from [45, Lem. 5]. Throughout, we make free use of §12.2.

Let χ_k be the character of ϱ_k and $Z = K(\chi_k)$. Recall that $K(\chi_k)$ does not depend on k, where we still assume that k is odd. Define $L = \mathbf{E}_{2^j} K$ and $\Delta = \mathrm{Gal}(L/Z)$. If $\zeta_4 \in Z$, then $L = Z$ (hence $\mathrm{m}_K(\chi_k) = 1$) and ϱ_k can be regarded as an irreducible Z-representation; note that $\mathbf{E}_{2^j}^{\pm}(\zeta_4) = \mathbf{E}_{2^j}$. The restriction of ϱ_k to K is then irreducible. We henceforth assume that $\zeta_4 \notin Z$ so that $L = Z(\zeta_4)$ is a quadratic extension of Z. It follows that

$$\psi\colon L \to \mathrm{M}_2(Z),\ \ \alpha + \zeta_4\cdot\beta \mapsto \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \qquad (\alpha, \beta \in Z)$$

is equivalent to the regular representation of L as a Z-algebra. Hence, $\mathrm{trace}(u\psi) = \mathrm{trace}_{L/Z}(u)$ for $u \in L$. Note that the space of matrices of the form $\left[\begin{smallmatrix} \alpha & \beta \\ \beta & -\alpha \end{smallmatrix}\right]$ $(\alpha, \beta \in Z)$ is the orthogonal complement of $L\psi$ with respect to the trace bilinear form

$(s,t) \mapsto \mathrm{trace}(st)$ on $\mathrm{M}_2(Z)$. We conclude that if $\vartheta(G) = 1$, then the representation $G \to \mathrm{GL}_2(Z)$ given by $a \mapsto \zeta_{2^j}^k \psi$ and $g \mapsto \mathrm{diag}(1,-1)$ affords χ_k. The restriction to K is then irreducible.

Let $\vartheta(G) = -1$ and suppose that there exist $x, y \in Z$ such that $x^2 + y^2 = -1$; by Lemma 12.6 the latter condition is equivalent to $\mathrm{m}_K(\chi_k) = 1$. Since the existence of such a pair (x,y) does not depend on k, we assume that the same choice of (x,y) has been made for all odd k. Let $t = \left[\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right]$ and let $\gamma \in \Delta$ be the non-trivial automorphism given by $(\alpha + \zeta_4 \cdot \beta)^\gamma = \alpha - \zeta_4 \cdot \beta$ for $\alpha, \beta \in Z$. It is readily checked that $(a^\gamma)\psi = t^{-1}(a\psi)t$ for all $a \in L$ and that $t^2 = -1$. We conclude that $G \to \mathrm{GL}_2(Z)$ defined by $a \mapsto (\zeta_{2^j}^k)\psi$ and $g \mapsto t$ affords χ_k and remains irreducible after restriction to K. Finally, if $\zeta_4 \notin Z$ and $\vartheta(G) = -1$ but $\mathrm{m}_K(\chi_k) = 2$, then the restriction of ϱ_k to K affords $2\sum_{\sigma\in\Gamma} \chi_k^\sigma$ (where $\Gamma = \mathrm{Gal}(K(\chi_k)/K)$) and is thus irreducible.

By §12.2, we have thus exhausted all the faithful irreducible K-representations of the non-abelian ANC 2-group G; note that equivalence classes of K-representations correspond to Galois conjugacy classes of ordinary characters.

12.4. Proof of Proposition 12.1

We are now in a position to prove Proposition 12.1. In §12.1, we have seen that it is true for the special case of cyclic groups. Next, we will argue that it is true for any non-abelian ANC 2-group G. Let σ_k be the irreducible K-representation of G which we have obtained from χ_k in §12.3. Of course, the existence statement in Proposition 12.1(i) is obvious at this point. By construction, the image of σ_k is the same for all odd k. Since any faithful irreducible K-representation of G is equivalent to σ_k for some odd k, (ii) follows for ANC 2-groups.

In order to deduce the general case, we proceed as follows. For part (i), let G be a non-abelian ANC group. Write $m = |G_{2'}|$ and suppose that $G_2 \cong H \leqslant \mathrm{GL}(W)$, where W is an $\mathbf{E}_m K$-space and H is irreducible. Then $G \cong \tilde{G} = \langle H, \zeta_m \cdot 1_W \rangle$ and the restriction of $\tilde{G}$ to K is irreducible.

Regarding (ii), let $G \leqslant \mathrm{GL}(V)$ and $H \leqslant \mathrm{GL}(W)$ be irreducible ANC groups over K such that $G \cong H$ (as abstract groups). Using Lemma 12.3, we find $a \in G_{2'} \leqslant \mathrm{Z}(G)$ and $b \in H_{2'} \leqslant \mathrm{Z}(H)$ of order $m = |G_{2'}| = |H_{2'}|$ such that $a \mapsto b$ induces a K-isomorphism $K[a] \xrightarrow{\phi} K[b]$. We may then regard both G and H as Z-linear groups, where $Z = K[a]$ acts on W via ϕ. We see that G_2 and H_2 are isomorphic irreducible Z-linear ANC 2-groups. By using what we have proved above with Z in place of K, we see that there exists a Z-isomorphism $V \to W$ with $t^{-1}G_2 t = H_2$. In particular, $|V : K[a]| = |W : K[b]|$. Since a and b have the same (irreducible) minimal polynomial over K, we obtain $s^{-1}as = b$ for some K-isomorphism $V \xrightarrow{s} W$. Now replace G by $s^{-1}Gs$. Repeating the above steps with $V = W$, $G_{2'} = H_{2'}$, $a = b$, and $\phi = 1$, we obtain $t^{-1}G_2 t = H_2$. Since $t^{-1}at = a$ by Z-linearity of t, we conclude that $t^{-1}Gt = H$. ♦

12.5. Construction of irreducible ANC groups over cyclotomic fields

We illustrate the construction used in our proof of Proposition 12.1 in the special case that K is a cyclotomic field. More precisely, let G be a non-abelian ANC group of order $2n$, where $n = 2^j m$ (m odd). For a given cyclotomic field K, we now describe the (essentially unique) irreducible linear group $G(K)$ over K with $G \cong G(K)$.

First, let $K \subset \mathbf{C}$ be any subfield. Define $Z = \mathbf{E}_n^+ K$ if $\delta(G) = 1$ and $Z = \mathbf{E}_n^- K$ if $\delta(G) = -1$. Further define $L = \mathbf{E}_n K$ so that $L = Z(\sqrt{-1})$.

The case $\sqrt{-1} \in K$. Suppose that $\sqrt{-1} \in K$. Then $\zeta_{2^j} \in Z = L$ and we have

$$G(K) \approx_K \left\langle \begin{bmatrix} \zeta_{2^j}\zeta_m & . \\ . & \zeta_{2^j}^{-1}\zeta_m \end{bmatrix}, \begin{bmatrix} . & 1 \\ \vartheta(G) & . \end{bmatrix} \right\rangle \leqslant \mathrm{GL}_2(Z);$$

here we denote similarity using the symbol $\approx_K$ to indicate that we regard the group on the right-hand side as a linear group over K. Hence, $G(K)$ has degree $2|Z : K|$. Recall the well-known identity $\mathbf{E}_k\mathbf{E}_l = \mathbf{E}_{\mathrm{lcm}(k,l)}$ for all $k, l \geqslant 1$; see [84, Satz 11.14]. Thus, if $K = \mathbf{E}_r$ with $4 \mid r$, then $|Z : K| = |L : \mathbf{Q}|/|K : \mathbf{Q}| = \varphi(\mathrm{lcm}(r, n))/\varphi(r)$.

Odd order cyclotomic field. Henceforth, we assume that $K = \mathbf{E}_r$ is a cyclotomic field, where r is odd. Then $|L : Z| = 2$ and we may write $\zeta_{2^j} = \alpha + \zeta_4\beta$ for $\alpha, \beta \in Z$.

If G_2 is dihedral or semidihedral, then

$$G(K) \approx_K \left\langle \begin{bmatrix} \alpha\zeta_m & \beta\zeta_m \\ -\beta\zeta_m & \alpha\zeta_m \end{bmatrix}, \begin{bmatrix} 1 & . \\ . & -1 \end{bmatrix} \right\rangle \leqslant \mathrm{GL}_2(Z).$$

Therefore, $G(K)$ has degree $2|Z : K| = |L : K| = \varphi(\mathrm{lcm}(r, n))/\varphi(r)$.

Let G_2 be generalised quaternion. Using Lemma 9.3, we see that -1 is a sum of two squares in Z if and only if (i) $rm > 1$ and (ii) $j \geqslant 3$ or $\mathrm{ord}\,(2 \bmod \mathrm{lcm}(r, m))$ is even; note that $\mathrm{ord}\,(2 \bmod \mathrm{lcm}(r, m)) \equiv \mathrm{ord}\,(2 \bmod rm) \equiv \mathrm{ord}\,(2 \bmod r)\,\mathrm{ord}\,(2 \bmod m) \bmod 2$ (consider prime divisors as in the proof of Corollary 9.7).

If $x^2 + y^2 = -1$ for $x, y \in Z$, then

$$G(K) \approx_K \left\langle \begin{bmatrix} \alpha\zeta_m & \beta\zeta_m \\ -\beta\zeta_m & \alpha\zeta_m \end{bmatrix}, \begin{bmatrix} x & y \\ y & -x \end{bmatrix} \right\rangle \leqslant \mathrm{GL}_2(Z)$$

and $G(K)$ again has degree $2|Z : K| = |L : K|$ as in the last case. However, if -1 is not a sum of two squares in Z, then

$$G(K) \approx_K \left\langle \begin{bmatrix} \zeta_{2^j}\zeta_m & . \\ . & \zeta_{2^j}^{-1}\zeta_m \end{bmatrix}, \begin{bmatrix} . & 1 \\ -1 & . \end{bmatrix} \right\rangle \leqslant \mathrm{GL}_2(L)$$

whence $G(K)$ has degree $2|L : K|$.

12.6. Counting irreducible ANC groups

12.7 Proposition. *Let $K/\mathbf{Q}$ be finitely generated and let $\varepsilon > 0$. The number of conjugacy classes of irreducible* ANC *subgroups of $\mathrm{GL}_d(K)$ is $\mathcal{O}(d^{1+\varepsilon})$.*

Proof. By Proposition 7.4, the number of irreducible (or merely homogeneous) finite cyclic subgroups of $\mathrm{GL}_d(K)$ is $\mathcal{O}(d^{1+\varepsilon})$. Define $\psi(n) = |\mathbf{E}_n K : K|$. As explained in the proof of Proposition 7.4, there exists $C > 0$ such that $\psi(n) \leqslant n \leqslant C \cdot \psi(n)^{1+\varepsilon}$ for all $n \geqslant 1$. Let $G \leqslant \mathrm{GL}_d(K)$ be a non-abelian irreducible ANC group, say $|G| = 2n$. For a given n, there are at most 3 different isomorphism classes of such groups and therefore at most that many conjugacy classes in $\mathrm{GL}_d(K)$. Given G and n, the above constructions of irreducible ANC groups show that we either have $d = \psi(n)$ or $d = 2\psi(n)$. By the above estimate, the number of solutions $m \geqslant 1$ of either $d = \psi(m)$ or $d = 2\psi(m)$ is $\mathcal{O}(d^{1+\varepsilon})$, which proves the claim. ♦

Given a finitely generated field extension $K/\mathbf{Q}$, it is natural to ask for the precise number of irreducible or primitive ANC subgroups of $\mathrm{GL}_d(K)$. However, this problem seems to be intractable even for $K = \mathbf{Q}$. For instance, from Theorem 14.13 below, we will obtain a natural bijection between the square-free integers $n \geqslant 1$ with $\varphi(n) = d$ and the conjugacy classes of primitive finite cyclic subgroups of $\mathrm{GL}_d(\mathbf{Q})$. It seems that determining (or merely counting) all such numbers n is a difficult number theoretic problem.

13. Cyclotomic families

In the last chapter, we saw that for an abstract ANC group G and a subfield K of $\mathbf{C}$, there exists an irreducible linear group, $G(K)$ say, over K with $G(K) \cong G$. Moreover, up to similarity, $G(K)$ is uniquely determined by G and K. In the next chapter, we will characterise primitivity of $G(K)$ when K is a number field. Here, we provide the technical foundations for these investigations. Specifically, in this chapter, we investigate the conditions $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| = p$ and $\sqrt{-1} \in \mathbf{E}_n^{\pm} K$ which arose in primitivity testing of ANC groups (Chapter 10). All fields in this chapter are understood to be subfields of the algebraic closure Ω of $\mathbf{Q}$ in $\mathbf{C}$.

13.1. Supernatural numbers

Recall (e. g. from the theory of profinite groups [89, §2.1]) that a **supernatural number** is a formal product $a = \prod_p p^{\alpha(p)}$ taken over all primes, where $\alpha(p) \in \{0, 1, \ldots, \infty\}$. Of course, every natural number is supernatural. Divisibility, greatest common divisors, products, etc. of supernatural numbers are defined in the natural way, extending the corresponding notions for natural numbers. We extend the definition of $\underline{a}$ in §9.1 by setting $\underline{a} = \prod\{p : \alpha(p) > 0\}$. We also extend the p-adic valuation ν_p to supernatural numbers via $\nu_p(a) = \alpha(p)$. The set $\mathbf{S}$ of supernatural numbers forms a complete lattice w.r.t. divisibility; the infimum of a set of supernatural numbers is their greatest common divisor. We write $\top = \prod_p p^{\infty}$ and thus $\gcd(\emptyset) = \top$. If π is a set of primes and $a = \prod_p a^{\alpha(p)}$ is a supernatural number, then we define the **π-part** of a to be $a_\pi = \prod_{p \in \pi} p^{\alpha(p)}$. As usual, π' denotes the complement of π in the set of prime numbers.

13.2. Cyclotomic families

Recall that $\mathbf{E}_n = \mathbf{Q}(\zeta_n)$ is the nth cyclotomic field. Let us call a collection $\mathbf{I} = (\mathbf{I}_n)_{n \geqslant 1}$ of subfields $\mathbf{I}_n \subset \mathbf{E}_n$ a **cyclotomic family**. For a field $K \subset \Omega$, let $\mathbf{I}^*(K) = \{d \geqslant 1 : K \subset \mathbf{I}_d\}$. We define the **I-cyclometer** of K to be the function $\varkappa_K^{\mathbf{I}} : \mathbf{N} \to \mathbf{S}$ defined by $\varkappa_K^{\mathbf{I}}(n) = \gcd(\mathbf{I}^*(K \cap \mathbf{E}_n))$. Note that if $\varkappa_K^{\mathbf{I}}(n) \neq \top$, then $\mathbf{I}^*(K \cap \mathbf{E}_n) \subset \varkappa_K^{\mathbf{I}}(n) \cdot \mathbf{N}$.

13.1 Lemma. *Let $\mathbf{I}$ be a cyclotomic family. Let $n \geqslant 1$ and let $d \mid n$. Then the restriction map $\mathrm{Gal}(\mathbf{E}_n K / \mathbf{I}_d K) \xrightarrow{\varrho} \mathrm{Gal}(\mathbf{E}_n / \mathbf{I}_d)$ is injective. It is surjective if and only if $d \in \mathbf{I}^*(K \cap \mathbf{E}_n)$.*

Proof. First note that $\mathbf{E}_nK/\mathbf{I}_dK$ and $\mathbf{E}_n/\mathbf{I}_d$ are Galois. Let $G = \mathrm{Gal}(\Omega/\mathbf{Q})$, $U = \mathrm{Gal}(\Omega/K) \leqslant G$, $N = \mathrm{Gal}(\Omega/\mathbf{E}_n) \triangleleft G$, and $M = \mathrm{Gal}(\Omega/\mathbf{I}_d) \triangleleft G$. Note that $\mathbf{I}_d \subset \mathbf{E}_d \subset \mathbf{E}_n$. By Galois theory, we obtain a commutative diagram

$$\begin{array}{ccc} (U \cap M)/(U \cap N) & \longrightarrow & M/N \\ \downarrow\cong & & \downarrow\cong \\ \mathrm{Gal}(\mathbf{E}_nK/\mathbf{I}_dK) & \xrightarrow{\varrho} & \mathrm{Gal}(\mathbf{E}_n/\mathbf{I}_d) \end{array}$$

where the unlabelled maps are induced by inclusions and restrictions. The map in the top row naturally factors as

$$\frac{U \cap M}{U \cap N} \xrightarrow{\cong} \frac{(U \cap M)N}{N} \hookrightarrow \frac{M}{N}.$$

This proves that ϱ is injective. By Dedekind's modular law [68, 1.3.14], we have $(U \cap M)N = UN \cap M$. Hence, ϱ is surjective if and only if $UN \cap M = M$ or, equivalently, $M \leqslant UN$. This is in turn equivalent to $K \cap \mathbf{E}_n \subset \mathbf{I}_d$ and thus to $d \in \mathbf{I}^*(K \cap \mathbf{E}_n)$. ♦

We say that a cyclotomic family $\mathbf{I}$ is **ideal** if $\mathbf{I}_n \cap \mathbf{E}_m \subset \mathbf{I}_{(n,m)}$ for all $n, m \geqslant 1$.

13.2 Lemma. *Let* $\mathbf{I}$ *be an ideal cyclotomic family. Then*

$$\varkappa_K^{\mathbf{I}}(n) = \gcd\left(d \mid n : d \in \mathbf{I}^*(K \cap \mathbf{E}_n)\right)$$

for all $n \geqslant 1$.

Proof. By assumption, if $d \in \mathbf{I}^*(K \cap \mathbf{E}_n)$, then $K \cap \mathbf{E}_n \subset \mathbf{I}_d \cap \mathbf{E}_n \subset \mathbf{I}_{(d,n)}$ whence $(d, n) \in \mathbf{I}^*(K \cap \mathbf{E}_n)$. ♦

That is, if $\mathbf{I}$ is ideal, then in order to determine $\varkappa_K^{\mathbf{I}}(n)$, we only need to consider the finitely many divisors of n.

13.3. Regular cyclotomic families

We say that a cyclotomic family $\mathbf{I}$ is **regular** if $\mathbf{I}_n \cap \mathbf{I}_m \subset \mathbf{I}_{(n,m)}$ for any $n, m \geqslant 1$; if the stronger condition $\mathbf{I}_n \cap \mathbf{I}_m = \mathbf{I}_{(n,m)}$ always holds, then $\mathbf{I}$ is **strongly regular**. If $\mathbf{I}_d \subset \mathbf{I}_n$ whenever $d \mid n$, then $\mathbf{I}$ is **isotonic**.

13.3 Lemma. *Let* $\mathbf{I}$ *be a cyclotomic family. Then* $\mathbf{I}$ *is strongly regular if and only if it is regular and isotonic.*

Proof. Let $\mathbf{I}$ be strongly regular and $d \mid n$. Then $\mathbf{I}_d \cap \mathbf{I}_n = \mathbf{I}_{(d,n)} = \mathbf{I}_d$ whence $\mathbf{I}$ is isotonic. Conversely, let $\mathbf{I}$ be regular and isotonic and let $n, m \geqslant 1$. By regularity, we have $\mathbf{I}_n \cap \mathbf{I}_m \subset \mathbf{I}_{(n,m)}$. On the other hand, since (n, m) divides n and m, we also have $\mathbf{I}_{(n,m)} \subset \mathbf{I}_n \cap \mathbf{I}_m$. ♦

13.4 Examples.

(i) It is well-known that $\mathbf{E} = (\mathbf{E}_n)_{n\geqslant 1}$ is strongly regular; see [84, Satz 11.14].

(ii) We will see in §13.5 that $\mathbf{E}^{\pm} = (\mathbf{E}_n^{\pm})_{n\geqslant 1}$ (see §8.1 for a definition) is regular. Also, $\mathbf{E}^{+}$ is strongly regular but $\mathbf{E}^{-}$ is not.

(iii) If $L \subset \Omega$ is any subfield and $\mathbf{I}$ is a (strongly) regular cyclotomic family, then $L \cap \mathbf{I} = (L \cap \mathbf{I}_n)_{n\geqslant 1}$ is a (strongly) regular cyclotomic family too.

13.5 Lemma. *Let $\mathbf{I}$ be a regular cyclotomic family. Let $n \geqslant 1$ with $\varkappa_K^{\mathbf{I}}(n) \neq \top$. Then $\varkappa_K^{\mathbf{I}}(n) = \min(\mathbf{I}^*(K \cap \mathbf{E}_n))$, the minimum being taken with respect to the usual ordering of $\mathbf{N}$.*

Proof. Write $D = \mathbf{I}^*(K \cap \mathbf{E}_n)$. Let $d, e \in D$. Then $K \cap \mathbf{E}_n \subset \mathbf{I}_d \cap \mathbf{I}_e \subset \mathbf{I}_{(d,e)}$ and therefore $(d, e) \in D$. Since $\varkappa_K^{\mathbf{I}}(n) = \gcd(F)$ for some finite $F \subset D$, we conclude that $\varkappa_K^{\mathbf{I}}(n) \in D$ whence minimality follows immediately. ⧫

13.6 Lemma. *Let $\mathbf{I}$ be a strongly regular cyclotomic family. Suppose that $\varkappa_K^{\mathbf{I}}(n) \neq \top$. Then $\mathbf{I}^*(K \cap \mathbf{E}_n) = \varkappa_K^{\mathbf{I}}(n) \cdot \mathbf{N}$.*

Proof. Let $n \geqslant 1$ be divisible by $d = \varkappa_K^{\mathbf{I}}(n)$. Since $\mathbf{I}$ is regular, $d \in \mathbf{I}^*(K \cap \mathbf{E}_n)$ (Lemma 13.5). As $\mathbf{I}$ is isotonic, $K \cap \mathbf{E}_n \subset \mathbf{I}_d \subset \mathbf{I}_n$ and thus $n \in \mathbf{I}^*(K \cap \mathbf{E}_n)$. We mentioned the other inclusion in §13.2. ⧫

13.4. Multiplicative cyclotomic families

Let $\mathbf{I}$ be a cyclotomic family. We say that $\mathbf{I}$ is **multiplicative** if $\mathbf{I}_{nm} = \mathbf{I}_n\mathbf{I}_m$, whenever $(n, m) = 1$. In this case, $\mathbf{I}$ is completely determined by all $\mathbf{I}_{p^\alpha}$, where p is a prime and $\alpha > 0$. Conversely, given $\mathbf{I}_{p^\alpha} \subset \mathbf{E}_{p^\alpha}$ for all primes p and $\alpha > 0$, there exists a unique extension to a multiplicative cyclotomic family.

In this section, we will prove the following.

13.7 Lemma. *Let $\mathbf{I}$ be a multiplicative cyclotomic family, π be a set of primes, and $n, m \geqslant 1$. Then $\mathbf{I}_n \cap \mathbf{I}_m = (\mathbf{I}_{n_\pi} \cap \mathbf{I}_{m_\pi})(\mathbf{I}_{n_{\pi'}} \cap \mathbf{I}_{m_{\pi'}})$.*

We will give a proof below after recalling some elementary facts from Galois theory. The following is well-known, although part (ii) is not usually spelled out explicitly in the literature.

13.8 Proposition. *Let $K \subset E \subset \Omega$ and $K \subset F \subset \Omega$ be subfields such that E/K and F/K are finite Galois and such that $E \cap F = K$. Let $\Gamma = \mathrm{Gal}(EF/K)$, $G = \mathrm{Gal}(E/K)$, and $H = \mathrm{Gal}(F/K)$.*

(i) ([48, Thm VI.1.14]) *The extension EF/K is Galois and the map $\Gamma \to G \times H$ induced by restrictions is an isomorphism.*

(ii) Identify Γ *with* $G \times H$ *via (i). Then the diagram*

$$\begin{array}{ccc} \text{subgroups of } G & \xrightarrow{U \mapsto E^U} & \text{intermediate fields of } E/K \\ \Big\downarrow{\scriptstyle U \mapsto U \times H} & & \Big\uparrow \\ \text{subgroups of } \Gamma & \xrightarrow[\Lambda \mapsto (EF)^\Lambda]{} & \text{intermediate fields of } EF/K \end{array}$$

commutes. Of course, the roles of E *and* F *can be interchanged.*

Proof.

(ii) The identification $\Gamma = G \times H$ takes the following explicit form: each $\sigma \in G$ admits a unique extension $\tilde{\sigma} \in \Gamma$ which acts trivially on F. We then have $\tilde{\sigma} = (\sigma, 1)$. In the same way, H is embedded into Γ. Note that, by construction, the restriction of $(\sigma, \tau) \in \Gamma$ to E is σ.

Write $L = EF$. Clearly, $E \subset L^{1\times H}$. By Galois theory, we have $|L : L^{1\times H}| = |H|$. Using (i), we see that $|H| = |L : E|$ and therefore $E = L^{1\times H}$.

Now let $U \leqslant G$. Then $L^{U\times H} = \left(L^{1\times H}\right)^{U\times 1} = E^U$. ♦

13.9 Corollary. *Let* $K \subset \mathcal{E} \subset \Omega$ *and* $K \subset \mathcal{F} \subset \Omega$ *be subfields such that* $\mathcal{E}/K$ *and* $\mathcal{F}/K$ *are finite Galois and* $\mathcal{E} \cap \mathcal{F} = K$*. Let* $K \subset E_i \subset \mathcal{E}$ *and* $K \subset F_i \subset \mathcal{F}$ *be further subfields for* $i = 1, 2$*. Then* $E_1F_1 \cap E_2F_2 = (E_1 \cap E_2)(F_1 \cap F_2)$*.*

Proof. Let $\Gamma = \mathrm{Gal}(\mathcal{E}\mathcal{F}/K)$, $G = \mathrm{Gal}(\mathcal{E}/K)$, and $H = \mathrm{Gal}(\mathcal{F}/K)$. Identify $\Gamma = G \times H$ as in Proposition 13.8. Let $U_i \leqslant G$ belong to E_i and let $V_i \leqslant H$ belong to F_i. By Proposition 13.8(ii), the subgroups of Γ belonging to E_i and F_i (regarded as intermediate fields of $\mathcal{E}\mathcal{F}/K$) are $U_i \times H$ and $G \times V_i$, respectively. The subgroup of Γ belonging to $E_1F_1 \cap E_2F_2$ is therefore $\langle U_1 \times V_1, U_2 \times V_2\rangle = \langle U_1, U_2\rangle \times \langle V_1, V_2\rangle = (\langle U_1, U_2\rangle \times H) \cap (G \times \langle V_1, V_2\rangle)$, which belongs to $(E_1 \cap E_2)(F_1 \cap F_2)$. ♦

Proof of Lemma 13.7. Set $K = \mathbf{Q}$, $E_1 = \mathbf{I}_{n_\pi}$, $E_2 = \mathbf{I}_{m_\pi}$, $\mathcal{E} = \mathbf{E}_{(nm)_\pi}$, $F_1 = \mathbf{I}_{n_{\pi'}}$, $F_2 = \mathbf{I}_{m_{\pi'}}$, and $\mathcal{F} = \mathbf{E}_{(nm)_{\pi'}}$. Now apply Corollary 13.9. ♦

13.10 Corollary. *Let* $\mathbf{I}$ *be a multiplicative cyclotomic family. Then* $\mathbf{I}$ *is regular.*

Proof. If p is a prime and $\alpha, \beta \geqslant 0$, then clearly $\mathbf{I}_{p^\alpha} \cap \mathbf{I}_{p^\beta} \subset \mathbf{I}_{p^{\min(\alpha,\beta)}}$. The claim now follows from Lemma 13.7. ♦

13.5. Facts on $\mathbf{E}^{\pm}$

By construction, the cyclotomic families $\mathbf{E}^+$ and $\mathbf{E}^-$ are multiplicative; indeed, $\mathbf{E}^{\pm}_{2^j m} = \mathbf{E}^{\pm}_{2^j} \cdot \mathbf{E}_m$ for odd $m \geqslant 1$.

Let $j \geqslant 3$. The three involutions in $\mathrm{Gal}(\mathbf{E}_{2^j}/\mathbf{Q}) \cong (\mathbf{Z}/2^j)^\times$ are $\zeta_{2^j} \mapsto -\zeta_{2^j}$, $\zeta_{2^j} \mapsto \zeta_{2^j}^{-1}$, and $\zeta_{2^j} \mapsto -\zeta_{2^j}^{-1}$. The corresponding fixed fields are $\mathbf{E}_{2^{j-1}}$, $\mathbf{E}^+_{2^j} = \mathbf{E}_{2^j} \cap \mathbf{R}$, and $\mathbf{E}^-_{2^j}$, respectively, and these are precisely the maximal subfields of $\mathbf{E}_{2^j}$. By going through the subgroup lattice of $(\mathbf{Z}/2^j)^\times$, we see that the subfield lattice of $\mathbf{E}_{2^j}$ is as shown in Figure 13.1. We can thus read off the following.

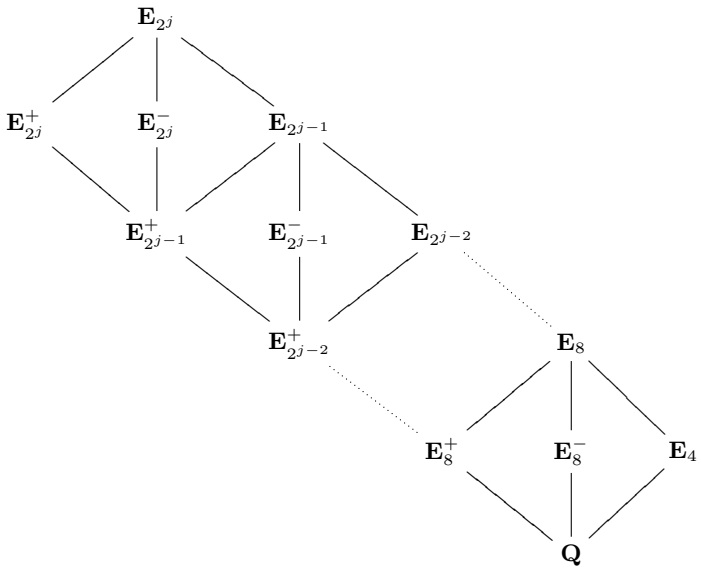


Figure 13.1. The subfield lattice of $\mathbf{E}_{2^j}$ for $j \geqslant 3$

13.11 Lemma. *Let* $1 \leqslant i < j$.

(i) $\mathbf{E}^+_{2^i} \cap \mathbf{E}^+_{2^j} = \mathbf{E}^+_{2^i} \cap \mathbf{E}^-_{2^j} = \mathbf{E}^+_{2^i}$.

(ii) $\mathbf{E}^-_{2^i} \cap \mathbf{E}^-_{2^j} = \mathbf{E}^-_{2^i} \cap \mathbf{E}^+_{2^j} = \mathbf{E}^+_{2^{i-1}}$.

(iii) $\mathbf{E}^+_{2^i} \cap \mathbf{E}^-_{2^i} = \mathbf{E}^+_{2^{i-1}}$.

(iv) $\mathbf{E}_{2^i} \cap \mathbf{E}^+_{2^j} = \mathbf{E}_{2^i} \cap \mathbf{E}^-_{2^j} = \mathbf{E}^+_{2^i}$. ♦

Together with Lemma 13.7, we thus obtain the following.

13.12 Corollary. *Let* $n, m \geqslant 1$.

(i) $\mathbf{E}^+_n \cap \mathbf{E}^+_m = \mathbf{E}^+_n \cap \mathbf{E}_m = \mathbf{E}^+_{(n,m)}$.

(ii) $\mathbf{E}^+_n \cap \mathbf{E}^-_m = \begin{cases} \mathbf{E}^+_{(n,m)/2}, & 0 < \nu_2(m) \leqslant \nu_2(n) \\ \mathbf{E}^+_{(n,m)}, & \text{otherwise.} \end{cases}$

(iii) $\mathbf{E}^-_n \cap \mathbf{E}^-_m = \begin{cases} \mathbf{E}^+_{(n,m)/2}, & 0 \neq \nu_2(n) \neq \nu_2(m) \neq 0 \\ \mathbf{E}^-_{(n,m)}, & \text{otherwise.} \end{cases}$

(iv) $\mathbf{E}_n \cap \mathbf{E}^-_m = \begin{cases} \mathbf{E}^-_{(n,m)}, & \nu_2(n) \geqslant \nu_2(m) \\ \mathbf{E}^+_{(n,m)}, & \text{otherwise.} \end{cases}$ ♦

In particular, we see that $\mathbf{E}^+$ is strongly regular and ideal while $\mathbf{E}^-$ has neither of these properties (but it is regular).

13.6. Cyclometers for $\mathbf{E}$ and $\mathbf{E}^{\pm}$

Let $K \subset \Omega$ be a subfield. We write $\varkappa_K^\circ = \varkappa_K^{\mathbf{E}^\circ}$, $\mathfrak{D}_K^\circ(n) = (\mathbf{E}^\circ)^*(K \cap \mathbf{E}_n) = \{d \geqslant 1 : K \cap \mathbf{E}_n \subset \mathbf{E}_d^\circ\}$, and $\mathfrak{D}_K^\circ(n;i) = \{d \in \mathfrak{D}_K^\circ(n) : d \equiv i \bmod 2\}$, where $\circ \in \{+,-,\ \}$. We now give arithmetical descriptions of these sets.

13.13 Proposition. *Let $n \geqslant 1$.*

(i) If $\mathfrak{D}_K^\circ(n) \neq \emptyset$, then $\mathfrak{D}_K^\circ(n) = \varkappa_K^\circ(n) \cdot \mathbf{N}$, where $\circ \in \{+,\ \}$.

(ii) If $d \in \mathfrak{D}_K^-(n)$, then $(d,n) \in \mathfrak{D}_K^-(n)$ or $2(d,n) \in \mathfrak{D}_K^-(n)$.

(iii) $\mathfrak{D}_K(n;1) = \mathfrak{D}_K^\pm(n;1)$.

(iv) Suppose that $\mathfrak{D}_K^+(n) = \emptyset$ but $\mathfrak{D}_K^-(n) \neq \emptyset$. Then $8 \mid \varkappa_K^-(n)$ and $\mathfrak{D}_K^-(n) = \varkappa_K^-(n) \cdot (2\mathbf{N}-1)$. Furthermore, $\varkappa_K^-(n) = \gcd\big(d \in \mathfrak{D}_K^-(n) : d \mid n\big)$.

(v) Suppose that $\mathfrak{D}_K^+(n) \neq \emptyset$. Then $\mathfrak{D}_K^-(n;0) = 2 \cdot \mathfrak{D}_K^+(n) \subset \mathfrak{D}_K^+(n;0)$. If $\varkappa_K^+(n)$ is even, then $\varkappa_K^-(n) = 2\,\varkappa_K^+(n)$, otherwise $\mathfrak{D}_K^-(n) = \mathfrak{D}_K^+(n)$ and therefore $\varkappa_K^-(n) = \varkappa_K^+(n)$.

Proof. We freely use Corollary 13.12.

(i) This follows from the strong regularity of $\mathbf{E}$ and $\mathbf{E}^+$ via Lemma 13.6.

(ii) $K \cap \mathbf{E}_n \subset \mathbf{E}_d^- \cap \mathbf{E}_n$ which is either equal to $\mathbf{E}_{(d,n)}^-$ or to $\mathbf{E}_{(d,n)}^+ \subset \mathbf{E}_{2(d,n)}^-$.

(iii) This is obvious since $\mathbf{E}_d = \mathbf{E}_d^\pm$ for odd $d \geqslant 1$.

(iv) Let $d,e \in \mathfrak{D}_K^-(n)$, i. e. $K \cap \mathbf{E}_n \subset \mathbf{E}_d^- \cap \mathbf{E}_e^-$. Then $\mathbf{E}_d^- \cap \mathbf{E}_e^-$ is not of the form $\mathbf{E}_f^+$ for any $f \geqslant 1$ whence $\nu_2(d) = \nu_2(e) \geqslant 3$. It follows that $(d,e) \in \mathfrak{D}_K^-(n)$. We conclude that $\varkappa_K^-(n) \in \mathfrak{D}_K^-(n)$ is divisible by 8 and that $\mathfrak{D}_K^-(n) \subset \varkappa_K^-(n) \cdot (2\mathbf{N}-1)$. If $r \geqslant 1$ is odd, then $\mathbf{E}_{\varkappa_K^-(n)}^- \subset \mathbf{E}_{\varkappa_K^-(n)r}^-$ which gives the other inclusion. Finally, if $d \in \mathfrak{D}_K^-(n)$, then

$$K \cap \mathbf{E}_n \subset \mathbf{E}_n \cap \mathbf{E}_d^- = \begin{cases} \mathbf{E}_{(d,n)}^-, & \nu_2(n) \geqslant \nu_2(d) \\ \mathbf{E}_{(d,n)}^+, & \text{otherwise.} \end{cases}$$

Since $\mathfrak{D}_K^+(n) = \emptyset$, we are in the first case. Therefore, $(d,n) \in \mathfrak{D}_K^-(n)$.

(v) Write $e = \varkappa_K^+(n)$ and let $d \in \mathfrak{D}_K^-(n;0)$. Then $K \cap \mathbf{E}_n \subset \mathbf{E}_d^- \cap \mathbf{E}_e^+ = \mathbf{E}_f^+$, where $f = (d,e)/2$ if $\nu_2(e) \geqslant \nu_2(d)$ and $f = (d,e)$ otherwise. By minimality of e (Lemma 13.5) and since d is even, we conclude that $f = e \mid d$ and $\nu_2(d) > \nu_2(e)$. Therefore, $2e \mid d$ and thus $\mathfrak{D}_K^-(n;0) \subset 2\,\varkappa_K^+(n) \cdot \mathbf{N} = 2\,\mathfrak{D}_K^+(n)$ by (i). Conversely, let $d \geqslant 1$ with $2e \mid d$. Then $K \cap \mathbf{E}_n \subset \mathbf{E}_e^+ \subset \mathbf{E}_{d/2}^+ \subset \mathbf{E}_d^-$ whence $2\,\mathfrak{D}_K^+(n) \subset \mathfrak{D}_K^-(n;0)$. The final claim follows from (i), (iii), and what has just been proved. ♦

Extending the notion of supernatural numbers, we may consider formal products $a = \prod_p p^{\alpha(p)}$, where p is a prime and $\alpha(p) \in \mathbf{Z} \cup \{\infty\}$. Such objects (we might call them "superrational numbers") arise as formal quotients of supernatural numbers by natural numbers (whenever the division makes sense). We let $\|a\| = \prod_p p^{\max(\alpha(p),0)}$.

13.14 Corollary. *Let $d \mid n$, $\circ \in \{+, -, \ \}$, and let $\mathrm{Gal}(\mathbf{E}_n K/\mathbf{E}_d^\circ K) \xrightarrow{\varrho} \mathrm{Gal}(\mathbf{E}_n/\mathbf{E}_d^\circ)$ be the restriction map.*

(i) If $\circ \in \{+, \ \}$, then ϱ is surjective if and only if $\varkappa_K^\circ(n) \mid d$.

(ii) If $\circ \in \{-\}$, then ϱ is surjective if and only if

(a) $\varkappa_K^+(n) \mid \|d/2\|$, or

(b) $\varkappa_K^-(n) \mid d$, $\varkappa_K^-(n) \nmid d/2$, and $\varkappa_K^+(n) = \top$.

Proof. We use Lemma 13.1. The first part is immediate from Proposition 13.13(i).

Note that (a) and (b) in (ii) are mutually exclusive. Suppose that $\varkappa_K^+(n) \neq \top$. By Proposition 13.13(v), $\mathfrak{D}_K^-(n)$ consists precisely of those multiples of $\varkappa_K^+(n)$ which are odd (if any) and arbitrary multiples of $2\,\varkappa_K^+(n)$. Hence, if $d \geqslant 1$, then $d \in \mathfrak{D}_K^-(n)$ if and only if $2\,\varkappa_K^+(n) \mid d$ (for d even) or $\varkappa_K^+(n) \mid d$ (for d odd). This is equivalent to $\varkappa_K^+(n) \mid \|d/2\|$.

If $\varkappa_K^+(n) = \varkappa_K^-(n) = \top$, then neither (a) nor (b) can be satisfied and ϱ is not surjective. Suppose that $\varkappa_K^+(n) = \top \neq \varkappa_K^-(n)$ so that Proposition 13.13(iv) applies. In particular, $\varkappa_K^-(n)$ is necessarily even. If $d \geqslant 1$, then $d \in \mathfrak{D}_K^-(n)$ if and only if $\varkappa_K^-(n) \mid d$ and $d/\varkappa_K^-(n)$ is odd. Clearly, the latter condition can be replaced by $\varkappa_K^-(n) \nmid d/2$. ♦

13.7. Cyclometers over number fields

In this section, let K be a number field.

Periodicity. For any $n \geqslant 1$, the intersection $K \cap \mathbf{E}_n$ is a subfield of the maximal abelian subfield K^{ab} of K. By the Kronecker-Weber theorem [59, Thm V.1.10], there exists $c \geqslant 1$ such that $K^{\mathrm{ab}} \subset \mathbf{E}_c$. Recall that the smallest possible value of such a c is known as the **conductor** of K^{ab}. By the following, $\varkappa_K^{\mathbf{I}}$ is "periodic" for every cyclotomic family $\mathbf{I}$.

13.15 Proposition. *Let $\mathbf{I}$ be a cyclotomic family. Then $\varkappa_K^{\mathbf{I}}(n) = \varkappa_K^{\mathbf{I}}(\gcd(n, c))$ for all $n \geqslant 1$.*

Proof. $K \cap \mathbf{E}_n = K \cap \mathbf{E}_n \cap \mathbf{E}_c = K \cap \mathbf{E}_{(n,c)}$. ♦

Computing with $\mathbf{E}$ and $\mathbf{E}^{\pm}$. Let $\circ \in \{+, -, \ \}$. Using Lemma 13.2 and Proposition 13.13(ii), we see that in order to test if $\mathfrak{D}_K^{\circ}(n)$ is empty, it suffices to test if any of the finitely many divisors of $2n$ belongs to it. If $\mathfrak{D}_K^{\circ}(n)$ is found to be non-empty, then the precise value of $\varkappa_K^{\circ}(n)$ can be computed using Lemma 13.2 and Proposition 13.13(iii)–(v). By Proposition 13.15, it suffices to compute $\varkappa_K^{\circ}(n)$ for the divisors of the conductor of K^{ab}. It follows that $\varkappa_K^{\circ}$ is a finite object.

13.8. Applications

Let K be a number field. The main results of this chapter are the following two corollaries; they provide equivalent characterisations of the conditions $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| = p$ and $\sqrt{-1} \in \mathbf{E}_n^{\pm} K$ in terms of cyclometers. As mentioned above, these two conditions are related to primitivity of linear ANC groups.

13.16 Corollary. *Let p be a prime and let $p \mid n$. Then $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| = p$ if and only if $p^2 \mid n$ and $p \mid \frac{n}{\varkappa_K(n)}$.*

Proof. If $p^2 \nmid n$, then $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \leqslant p - 1$. Now apply Corollary 13.14(i) with $d = n/p$; recall that $\varkappa_K(n) \mid n$. ♦

13.17 Corollary. *Let $4 \mid n$.*

(i) The following are equivalent: $\sqrt{-1} \notin \mathbf{E}_n^{+} K$, $\varkappa_K^{+}(n) \mid n$, and $\varkappa_K^{+}(n) \neq \top$.

(ii) $\sqrt{-1} \notin \mathbf{E}_n^{-} K$ if and only if

(a) $\varkappa_K^{+}(n) \mid n/2$, or

(b) $\varkappa_K^{-}(n) \mid n$, and $\varkappa_K^{-}(n) \nmid n/2$.

Proof. Since $4 \mid n$, we have $\mathbf{E}_n = \mathbf{E}_n^{\pm}(\sqrt{-1}) \neq \mathbf{E}_n^{\pm}$. Thus, $|\mathbf{E}_n K : \mathbf{E}_n^{\pm} K| = 2$ is equivalent to $\sqrt{-1} \notin \mathbf{E}_n^{\pm} K$. But it is also equivalent to the restriction map $\mathrm{Gal}(\mathbf{E}_n K / \mathbf{E}_n^{\pm} K) \to \mathrm{Gal}(\mathbf{E}_n / \mathbf{E}_n^{\pm})$ being surjective. Note that since $\mathbf{E}^{+}$ is ideal, if $\varkappa_K^{+}(n) \neq \top$, then $\varkappa_K^{+}(n) \mid n$ by Lemma 13.2. Now apply Corollary 13.14 with $d = n$. This proves (i) and also (ii) provided that we add the extra condition $\varkappa_K^{+}(n) = \top$ to (b). To complete the proof, we show that if (b) is satisfied and $\varkappa_K^{+}(n) \neq \top$, then (a) is satisfied too. Recall from Proposition 13.13(v) that $\varkappa_K^{-}(n) = 2\,\varkappa_K^{+}(n)$ if $\varkappa_K^{+}(n)$ is even and $\varkappa_K^{-}(n) = \varkappa_K^{+}(n)$ otherwise. Suppose that $\varkappa_K^{+}(n)$ is odd. Then $\varkappa_K^{-}(n) = \varkappa_K^{+}(n)$ is odd and $\varkappa_K^{-}(n) \mid n$ implies that $\varkappa_K^{-}(n) \mid n/2$, contradicting our assumption that (b) holds. Therefore, $\varkappa_K^{+}(n)$ is even and $2\,\varkappa_K^{+}(n) \mid n$ which gives $\varkappa_K^{+}(n) \mid n/2$. ♦

14. Primitive ANC groups over number fields

Let G be an ANC group and let K be a number field. By Proposition 12.1, there exists an irreducible linear group $G(K)$ over K with $G \cong G(K)$; furthermore, $G(K)$ is uniquely determined up to similarity. A natural question to ask is the following: given K, for which G is $G(K)$ primitive? In this chapter, we combine results from Chapters 8–10 and 12–13 to obtain number-theoretic conditions (involving cyclometers) which characterise precisely when $G(K)$ is primitive for given G and K. In the special case that K is a cyclotomic field, these conditions simplify drastically, leading to a complete list of those ANC groups G such that $G(K)$ is primitive (Theorem 14.13).

Unless otherwise indicated, fields in this chapter are subfields of the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, and K is a number field.

14.1. The cyclic case

For a supernatural number a, define $\widehat{a} = a \cdot \prod\{p \text{ prime} : \nu_p(a) = 0\}$; in other words, $\widehat{a}$ is the smallest supernatural number (w.r.t. divisibility) which is divisible by a and all primes. The following is elementary.

14.1 Lemma. *Let $r \geqslant 1$ and $d \mid r$. The following are equivalent.*

(i) For each prime p with $p^2 \mid r$, we have $p \nmid \frac{r}{d}$.

(ii) r/d is square-free and $(r/d, d) = 1$.

(iii) $r \mid \widehat{d}$.

Proof.

(i)→(ii): Let (ii) be false. Then, for some prime p, either p^2 divides r/d or p divides $(r/d, d)$. In either case, (i) is not satisfied for the given prime p.

(ii)→(i): Let (ii) be satisfied but (i) be violated for some p. Then p divides $\frac{r}{p} = \frac{r}{dp} \cdot d$ but not the left factor. Hence, p divides d and thus also $(r/d, d)$, a contradiction to (ii).

(i)↔(iii): Statement (i) is equivalent to the following: for each prime p with $\nu_p(r) \geqslant 2$, we have $\nu_p(r) = \nu_p(d)$. Since $\nu_p(d) \leqslant \nu_p(r)$, the last condition can be relaxed to $\nu_p(r) \leqslant \nu_p(d)$. We see that (i) is equivalent to $\nu_p(r) \leqslant \max(\nu_p(d), 1)$ for all p; clearly, this simply means $r \mid \widehat{d}$. ♦

The formalism of supernatural numbers allows us to give the following compact characterisation of primitivity for cyclic groups.

14.2 Proposition. $\mathrm{C}_n(K)$ *is primitive if and only if* $n \mid \widehat{\varkappa_K(n)}$.

Proof. By Corollary 10.5 Proposition 10.6, and Lemma 12.3, $\mathrm{C}_n(K)$ is primitive if and only if for each prime divisor $p \mid n$, we have $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| \neq p$. The claim now follows from Corollary 13.16 and Lemma 14.1. ⧫

14.2. Odd order cyclotomic extensions

The following is well-known.

14.3 Proposition ([71, Thm 5.5.1])**.** *Let E/L and F/L be algebraic extensions. If E/L is Galois, then so is EF/F and* $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/E \cap F)$ *via restriction.*

14.4 Corollary. *Let the notation be as in Proposition 14.3. Then* $\mathrm{Gal}(EF/F)$ *embeds into* $\mathrm{Gal}(E/L)$ *via restriction.* ⧫

Below, we will make use of the following.

14.5 Lemma. *Let $n \geqslant 1$. Write $n = 2^j m$ (m odd) and let p be an odd prime divisor of n. Then $|\mathbf{E}_n K : \mathbf{E}_{n/p} K| = p$ if and only if $|\mathbf{E}_m K : \mathbf{E}_{m/p} K| = p$.*

Proof. By Corollary 14.4, $r = |\mathbf{E}_n K : \mathbf{E}_{n/p} K|$ divides $s = |\mathbf{E}_m K : \mathbf{E}_{m/p} K|$ which in turn divides $|\mathbf{E}_{p^a} : \mathbf{E}_{p^{a-1}}| \leqslant p$, where $a = \nu_p(m)$. Hence, if $r = p$, then $s = p$. Conversely, let $s = p$. Then $a \geqslant 2$ (for otherwise $s \leqslant p - 1$) and r can only be 1 or p. Suppose, for the sake of contradiction, that $r = 1$. Then $\mathbf{E}_m K \subset \mathbf{E}_n K = \mathbf{E}_{n/p} K = (\mathbf{E}_{m/p} K)\mathbf{E}_{2^j}$, whence s divides $t = |(\mathbf{E}_{m/p} K)\mathbf{E}_{2^j} : \mathbf{E}_{m/p} K|$. However, by Corollary 14.4, t divides $|\mathbf{E}_{2^j} : \mathbf{Q}|$, which is a power of 2. This contradicts $s = p$. ⧫

14.3. Some arithmetical conditions

Let $n = 2^j m$, where m is odd and $j \geqslant 2$. Consider the following conditions.

(a) $\varkappa_K^+(n) \neq \top$.

(b) $m \mid \widehat{\varkappa_K(m)}$.

(c) $n/\varkappa_K(n)$ is odd.

(d) K is totally imaginary or $m > 1$.

(e) $\mathrm{ord}\,(2 \bmod m) \cdot |K_\mathfrak{p} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p} \mid 2$ of K.

Using results from preceding chapters, we may summarise major properties of these conditions as follows.

14.6 Lemma.

(i) Condition (a) is equivalent to $\sqrt{-1} \notin \mathbf{E}_n^+K$.

(ii) Condition (b) is equivalent to the following: for each odd prime divisor p *of* n, $|\mathbf{E}_nK : \mathbf{E}_{n/p}K| \neq p$.

(iii) Condition (c) is equivalent to $|\mathbf{E}_nK : \mathbf{E}_{n/2}K| \neq 2$.

(iv) Conditions (b) and (c) are both satisfied if and only if $n \mid \widehat{\varkappa_K(n)}$.

(v) If $j \geqslant 3$, *then (d) is equivalent to* $x^2 + y^2 = -1$ *being soluble in* $\mathbf{E}_n^+K$.

(vi) $x^2 + y^2 = -1$ *is soluble in* $\mathbf{E}_mK$ *if and only if (d) and (e) are satisfied.*

(vii) If $x^2 + y^2 = -1$ *is soluble in* $\mathbf{E}_n^+K$ *and* p *is an odd prime with* $p^2 \mid n$, *then* $x^2 + y^2 = -1$ *is soluble in* $\mathbf{E}_{n/p}^+K$.

Proof.

(i) Corollary 13.17(i).

(ii)–(iv) Lemma 14.1, Lemma 14.5, and Corollary 13.16.

(v)–(vi) Lemma 9.3.

(vii) Lemma 9.4. ♦

14.4. Characterisations of primitivity in the non-abelian case

Let G be a non-abelian ANC group of order $2n$, where $n = 2^jm$ and m is odd.

14.7 Lemma. *Let* $A \triangleleft G(K)$ *be cyclic of index 2. Let* $\circ = +$ *if* G_2 *is dihedral or generalised quaternion and let* $\circ = -$ *if* G_2 *is semidihedral.*

(i) A *is homogeneous if and only if* $\sqrt{-1} \notin \mathbf{E}_n^\circ K$.

(ii) Let A *be homogeneous. Then* A *is irreducible if and only if* $\vartheta(G) = 1$ *or* $x^2 + y^2 = -1$ *is soluble in* $\mathbf{E}_n^+K$.

Proof. In view of the uniqueness statement in Proposition 12.1, we may assume that $G(K)$ is given by the explicit construction from Chapter 12. Thus, $K[A] \cong_K K[a, b]$, where $a = \operatorname{diag}(\zeta_{2^j}, \delta(G)\zeta_{2^j}^{-1}) \in \mathrm{GL}_2(\mathbf{E}_nK)$ and $b = \operatorname{diag}(\zeta_m, \zeta_m) \in \mathrm{GL}_2(\mathbf{E}_nK)$; note that the isomorphism type of $K[a, b]$ does not change if $G(K)$ is rewritten over $\mathbf{E}_n^\circ K$ (if possible) since this amounts to replacing $G(K)$ by $x^{-1}G(K)x$ for a suitable $x \in \mathrm{GL}_2(\mathbf{E}_nK)$. We see that $K[A] \cong_K (\mathbf{E}_n^\circ K)[a]$. The minimal polynomial of a over $\mathbf{E}_n^\circ K$ is $X^2 - (\zeta_{2^j} + \delta(G)\zeta_{2^j}^{-1})X + \delta(G)$ (cf. Lemma 8.4). Thus, $K[A]$ is a field if and only if $\zeta_{2^j} \notin \mathbf{E}_n^\circ K$ or, equivalently, $\mathbf{E}_nK \neq \mathbf{E}_n^\circ K$. Since $\mathbf{E}_n = \mathbf{E}_n^\circ(\sqrt{-1})$, this is equivalent to $\sqrt{-1} \notin \mathbf{E}_n^\circ K$ which proves (i). Now let A be homogeneous.

From the description in Chapter 12, we further obtain that the degree of $G(K)$ is $2^{\ell-1}|\mathbf{E}_nK : K|$, where ℓ is the Schur index of the representation of G_2 over $\mathbf{E}_mK$ used in the construction of $G(K)$. Thus, A is irreducible if and only if $\ell = 1$ which happens precisely under the conditions stated; cf. Lemmas 12.5–12.6. ⧫

Having characterised irreducibility of A in the last lemma, we may now continue to decide primitivity of $G(K)$. The next four propositions constitute the main result of this chapter.

14.8 Proposition.

(i) If G_2 is dihedral, then $G(K)$ is primitive if and only if (a)–(c) hold.

(ii) If G_2 is generalised quaternion with $|G_2| > 16$, then $G(K)$ is primitive if and only if (a)–(d) hold.

Proof. Apply Proposition 10.13, Lemma 14.7, and Lemma 14.6(i)–(v). ⧫

14.9 Proposition. *If $G_2 \cong \mathrm{Q}_8$, then $G(K)$ is primitive if and only if (a),(b),(d), and (e) are satisfied.*

Proof. We have $n = 4m$ and therefore $\mathbf{E}_n^+ = \mathbf{E}_m$. Hence, $x^2 + y^2 = -1$ is soluble in $\mathbf{E}_n^+K$ if and only if (d) and (e) are both satisfied (Lemma 14.6(vi)). By Lemma 10.9, the subgroups of index 2 in G are all irreducible and they can therefore not be block stabilisers, regardless of whether $|\mathbf{E}_nK : \mathbf{E}_{n/2}K| = 2$ or not. The odd prime divisors of n are covered by Proposition 10.13 and Lemma 14.6(ii). ⧫

14.10 Proposition. *Let $G_2 \cong \mathrm{Q}_{16}$. Then $G(K)$ is primitive if and only if (a),(b),(d) hold and (c) is satisfied if (e) is.*

Proof. Since $8 \mid n$, by Lemma 14.6(v), $x^2 + y^2 = -1$ is soluble in $\mathbf{E}_n^+K$ if and only if (d) is satisfied. As before, none of the maximal subgroups of G of odd prime index is a block stabiliser if and only if (b) is satisfied. It remains to consider a non-abelian subgroup, H say, of index 2 in G. By Lemma 10.11 and Corollary 8.6, H is a block stabiliser for G if and only if $|\mathbf{E}_nK : \mathbf{E}_{n/2}K| = 2$ and $x^2 + y^2 = -1$ is soluble in $\mathbf{E}_{n/2}^+K$. The former condition is equivalent to (c) being false. Since $n/2 = 4m$ so that $\mathbf{E}_{n/2}^+ = \mathbf{E}_m$, the latter condition is equivalent to (d) and (e) being true. Hence, primitivity of G is equivalent to (a), (b), (d), and "(c) or not (e)" being true. This gives the condition stated. ⧫

14.11 Proposition. *Let G_2 be semidihedral. Then $G(K)$ is primitive if and only if (b)–(c) hold and $\varkappa_K^-(n) \mid n$.*

Proof. This is a consequence of Proposition 10.13, Corollary 13.17, Lemma 14.7, Lemma 14.6(ii)–(iv), and the following two observations. First, if $n \mid \widehat{\varkappa_K(n)}$, then $\varkappa_K^+(n) \nmid n/2$. Indeed, suppose that $\varkappa_K^+(n) \mid n/2$. Then $\varkappa_K(n) \mid n/2$ and thus $\nu_2(\varkappa_K(n)) \leqslant \nu_2(n/2)$. As $8 \mid n$, we obtain $\nu_2(\widehat{\varkappa_K(n)}) \leqslant \nu_2(n/2) < \nu_2(n)$ and so

$n \nmid \widehat{\varkappa_K(n)}$. Second, if $n \mid \widehat{\varkappa_K(n)}$ and $\varkappa_K^-(n) \mid n$, then $n/\varkappa_K^-(n)$ is odd. For $8 \mid n$ implies that $\nu_2(n) \leqslant \nu_2(\widehat{\varkappa_K(n)}) = \nu_2(\varkappa_K(n)) \leqslant \nu_2(n)$ whence $n/\varkappa_K(n)$ is odd. As $\varkappa_K(n) \mid \varkappa_K^-(n) \mid n$, we conclude that $n/\varkappa_K^-(n)$ is odd. ♦

14.12 Remark. Primitivity of the Sylow p-subgroups of the general linear groups over arbitrary fields has been investigated in [50, 45]. In the case of 2-groups above, there is an unavoidable overlap between the techniques used here and those used in the sources just cited. For instance, the field invariants used in [50] are concerned with the inclusions of the fields $\mathbf{E}_{2^i}$ and $\mathbf{E}_{2^i}^{\pm}$ in the ground field. In our approach, these fields enter (in a different way) via the cyclometers $\varkappa_K$ and $\varkappa_K^{\pm}$.

14.5. Primitive finite nilpotent groups over cyclotomic fields

In this section, we apply the above results to give a precise description of the ANC groups G such that $G(\mathbf{E}_r)$ is primitive. Since $\mathbf{E}_r = \mathbf{E}_{2r}$ for odd r, we may assume that $r \not\equiv 2 \bmod 4$.

14.13 Theorem. *Let $r \not\equiv 2 \bmod 4$. A complete list (up to isomorphism) of those ANC groups G such that $G(\mathbf{E}_r)$ is primitive is given by the following.*

(i) C_n, *where* $n \mid \widehat{r}$.

(ii) $\mathrm{Q}_8 \times \mathrm{C}_m$, *where m and r are odd, $m \mid \widehat{r}$, $rm > 1$, and* $\operatorname{ord}(2 \bmod rm)$ *is even.*

(iii) $\mathrm{Q}_{16} \times \mathrm{C}_m$, *where m and r are odd, $m \mid \widehat{r}$, $rm > 1$, and* $\operatorname{ord}(2 \bmod rm)$ *is odd.*

Proof. Using the properties of the cyclotomic families $\mathbf{E}$ and $\mathbf{E}^{\pm}$ described in Chapter 13, we see that

$$\varkappa_{\mathbf{E}_r}(n) = \begin{cases} (r,n), & (r,n) \equiv 0,1,3 \bmod 4, \\ (r,n)/2, & (r,n) \equiv 2 \bmod 4 \end{cases}$$

and

$$\varkappa_{\mathbf{E}_r}^{\pm}(n) = \begin{cases} (r,n), & (r,n) \equiv 1,3 \bmod 4, \\ (r,n)/2, & (r,n) \equiv 2 \bmod 4, \\ \top, & (r,n) \equiv 0 \bmod 4 \end{cases}$$

for any $n \geqslant 1$. In particular, $\widehat{\varkappa_{\mathbf{E}_r}(n)} = \widehat{(r,n)}$ and

$$\widehat{\varkappa_{\mathbf{E}_r}^{\pm}(n)} = \begin{cases} \widehat{(r,n)}, & (r,n) \equiv 1,2,3 \bmod 4, \\ \top, & (r,n) \equiv 0 \bmod 4 \end{cases}$$

for any $n \geqslant 1$.

Given any $r, n \geqslant 1$, we have $n \mid \widehat{(r,n)}$ if and only if $n \mid \widehat{r}$. Indeed, since $(r,n) \mid r$, we have $\widehat{(r,n)} \mid \widehat{r}$. Thus, if $n \mid \widehat{(r,n)}$, then $n \mid \widehat{r}$. Conversely, let $n \mid \widehat{r}$. Then

$n = (\widehat{r}, n)$ which divides $\widehat{(r, n)}$. We now consider primitivity of $\mathrm{C}_n(\mathbf{E}_r)$. Using the above description of $\varkappa_{\mathbf{E}_r}$ and §14.1, we see that $\mathrm{C}_n(\mathbf{E}_r)$ is primitive if and only if $n \mid \widehat{(r, n)}$. We have just seen that this is equivalent to $n \mid \widehat{r}$.

Let G be a non-abelian ANC group of order $2n$, where $n = 2^j m$ (m odd, $j \geqslant 2$). We now investigate the conditions determining primitivity of $G(\mathbf{E}_r)$ from §14.3 (with $K = \mathbf{E}_r$). The above description of $\varkappa^{\pm}_{\mathbf{E}_r}$ and the introductory comment of the preceding paragraph show the following: condition (a) is equivalent to $4 \nmid r$, condition (b) is equivalent to $m \mid \widehat{r}$, and conditions (b) and (c) are both satisfied if and only if $n \mid \widehat{r}$. Hence, if (b)–(c) are satisfied, then (a) is false. This rules out primitivity of $G(\mathbf{E}_r)$ if G_2 is dihedral or quaternion with $|G_2| > 16$ by Proposition 14.8. Similarly, the case that G_2 is semidihedral is ruled out by Proposition 14.11 since $\varkappa^{+}_{\mathbf{E}_r}(n) = \varkappa^{-}_{\mathbf{E}_r}(n) = \top$ whenever (b)–(c) are satisfied.

The case $G_2 \cong \mathrm{Q}_8$ is now easily treated. Recall that for any odd $s \geqslant 1$, the degree of the sth 2-adic cyclotomic field over $\mathbf{Q}_2$ is precisely $\mathrm{ord}(2 \bmod s)$ [13, Prop. 3.5.18]. By Corollary 9.7, we have $\mathrm{ord}\,(2 \bmod rm) \equiv \mathrm{ord}\,(2 \bmod r)\,\mathrm{ord}\,(2 \bmod m) \bmod 2$. Note that by (a) and since $r \not\equiv 2 \bmod 4$, r has to be odd in order for $G(\mathbf{E}_r)$ to be primitive. It remains to consider the case $G_2 \cong \mathrm{Q}_{16}$. Again, r has to be odd by (a). We therefore have $\varkappa_{\mathbf{E}_r}(n) = (n, r)$ whence $n/\varkappa_{\mathbf{E}_r}(n)$ is necessarily even. Therefore, condition (c) is never satisfied. Thus, primitivity of $G(\mathbf{E}_r)$ is equivalent to (a), (b), (d) being true and (e) being false. This leads to the conditions given. ⧫

14.14 Remark. It is shown in [29, Thm 5] that the set of odd primes p such that $\mathrm{ord}\,(2 \bmod p)$ is even has Dirichlet density 17/24 (see [78, VI, §4] for a definition). In view of Corollary 9.7 (c.f. the remark at the end of [29]), it follows that even if $\mathrm{ord}\,(2 \bmod r)$ is odd, the case (iii) in Theorem 14.13 is still "asymptotically rare".

Notation

Maps usually act on the right. Throughout this thesis, K is a field and V is a non-trivial finite-dimensional K-vector space.

The default parent structures of objects are the natural numbers and the integers, the choice being clear from the context. For example, "let $x \geqslant 0$" means "let $x \in \mathbf{Z}$ with $x \geqslant 0$". As an exception to this rule, in "let $\varepsilon > 0$", the quantity ε is real.

General

$1, 1_M$	identity map (on M), multiplicative identity element (of M)
$A \subset B$, $B \supset A$	A is a (not necessarily proper) subset of B
$\cong$, $\cong_R$	(R-)isomorphism

Linear algebra

$\lvert V : K \rvert$	dimension of V over K
$\mathrm{End}(M)$, $\mathrm{End}_R(M)$	endomorphism ring of an R-module
$\mathrm{GL}(M)$	unit group of $\mathrm{End}(M)$
$\mathrm{M}_d(R)$	ring of $d \times d$ matrices over the ring R
$\mathrm{GL}_d(R)$	unit group of $\mathrm{M}_d(R)$
$\mathrm{mpol}_K(x)$	minimal polynomial of x over K
$\approx$	similarity
$g_\mathrm{u}, g_\mathrm{s}$	multiplicative Jordan decomposition of g

Group theory

$N \triangleleft G$	N is a (not necessarily proper) normal subgroup of G
$\mathrm{Z}(G)$	centre
G', $[G, G]$	derived subgroup
G_p, $G_{p'}$	Sylow p-subgroup, p-complement
G^n	$\langle g^n : g \in G \rangle$
$\mathrm{T}(G)$	torsion subgroup
$\mathrm{class}(G)$	nilpotency class
$\exp(G)$	exponent of G
$\mathrm{ord}\,(g)$	order of g
$A \blacktriangleleft G$	see Notation 6.1
C_n	cyclic group of order n
D_{2^k}, SD_{2^k}, Q_{2^k}	dihedral, semidihedral, generalised quaternion group

Group actions and representations

$\mathrm{Stab}_G(x)$	stabiliser of x in G
A^G	$\{a \in A : ag = a \text{ for all } g \in G\}$
$[a, g]$	$ag - a$ or $a^{-1}a^g$
$E(\phi)$	extension corresponding to $\phi \in \mathrm{Z}^2(G, A)$
$\mathrm{Irr}(G)$	(ordinary) irreducible characters of G
$K(\chi)$	character field
$K[\varrho]$	$K[\mathrm{Im}(\varrho)]$ where ϱ is a representation

Rings

$\mathfrak{a} \lhd R$	$\mathfrak{a}$ is a (not necessarily proper ideal) of R
$R^\times$	unit group of R
$(a, b, \dots)$	ideal generated by $a, b, \dots$; $\gcd(a, b, \dots)$
R/a	$R/(a)$
$R_\mathfrak{p}$	localisation of R at the prime ideal $\mathfrak{p} \lhd R$
$R[G]$	R-algebra generated by G
RG	group ring of G over R
UFD	unique factorisation domain
PID	principal ideal domain

Algebras

$\mathrm{Z}(\mathcal{A})$	centre of $\mathcal{A}$
$L \star_\phi \Gamma$	crossed product
$\mathrm{Br}(K)$, $\mathrm{Br}(L/K)$	(relative) Brauer group
$[\mathcal{A}]$	Brauer class of $\mathcal{A}$
$\exp(\mathcal{A})$	exponent
$\left(\frac{a,b}{K}\right)$	quaternion algebra

Special domains

$\mathbf{Q}_p$	p-adic numbers
$\mathbf{F}_q$	finite field of size q
$\mathbf{E}_n$	$\mathbf{Q}(\zeta_n)$
$\mathbf{E}_n^\pm$	$\mathbf{E}_n^\pm = \mathbf{Q}(\zeta_{2^j} \pm \zeta_{2^j}^{-1}, \zeta_m)$, where $n = 2^j m$, m odd

Field theory

$\mathrm{Gal}(L/K)$	Galois group of L/K
$\mathrm{N}_{L/K}$	norm map
$X, T, X_1, \dots$	indeterminates
$\mathbf{X}_r$, $\mathbf{X}$	the sequence $(X_1, \dots, X_r)$
$K_{[\alpha]}$	the ring of all f/g, where $f, g \in K[\mathbf{X}]$ and $g(\alpha) \neq 0$
ζ_n	primitive nth root of unity over $\mathbf{Q}$

Arithmetic

$\mathrm{ord}(r \bmod n)$	order of $r + n\mathbf{Z}$ in $(\mathbf{Z}/n)^\times$
$\underline{n}$	product of the prime divisors of n
$\nu_p(a)$	p-adic valuation of a
a_π	π-part of a, where π is a set of primes
$\widehat{a}$	$\mathrm{lcm}(a, 2, 3, 5, 7, \dots)$

Miscellaneous

$\vartheta(G)$, $\delta(G)$	see §8.3
$G(K)$	the irreducible ANC group over K which is isomorphic to G
$\varkappa_K$	cyclometer

List of Algorithms

Bibliography

[1] T. Albu. From field theoretic to abstract co-Galois theory. In *Handbook of algebra. Vol. 5*, volume 5 of *Handb. Algebr.*, pages 3–84. Elsevier/North-Holland, Amsterdam, 2008.

[2] B. Assmann. Polycyclic presentations for matrix groups. Diplomarbeit, Technische Universität Braunschweig, 2003.

[3] B. Assmann. Polenta, 2007. A refereed GAP 4-package. Available from `http://www.gap-system.org/Packages/polenta.html`.

[4] B. Assmann and B. Eick. Computing polycyclic presentations for polycyclic rational matrix groups. *J. Symbolic Comput.*, 40(6):1269–1284, 2005.

[5] L. Babai. Randomization in group algorithms: conceptual questions. In *Groups and computation, II (New Brunswick, NJ, 1995)*, volume 28 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 1–17. Amer. Math. Soc., Providence, RI, 1997.

[6] L. Babai, R. Beals, J.-y. Cai, G. Ivanyos, and E. M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (Atlanta, GA, 1996)*, pages 498–507, New York, 1996. ACM.

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[8] R. Brauer, H. Hasse, and E. Noether. Beweis eines Hauptsatzes in der Theorie der Algebren. *J. reine angew. Math.*, 167:399–404, 1932.

[9] K. S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original.

[10] W. C. Brown. *Matrices over commutative rings*, volume 169 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1993.

[11] F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O'Brien. Generating random elements of a finite group. *Comm. Algebra*, 23(13):4931–4948, 1995.

[12] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[13] H. Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[14] P. M. Cohn. *Basic algebra*. Springer-Verlag London Ltd., London, 2003.

[15] P. M. Cohn. *Further algebra and applications*. Springer-Verlag London Ltd., London, 2003.

[16] I. G. Connell. The stufe of number fields. *Math. Z.*, 124:20–22, 1972.

[17] C. W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[18] A. S. Detinko, B. Eick, and D. L. Flannery. Computing with matrix groups over infinite fields (preprint). See `http://larmor.nuigalway.ie/~detinko/DEF_survey.pdf`.

[19] A. S. Detinko and D. L. Flannery. Classification of nilpotent primitive linear groups over finite fields. *Glasg. Math. J.*, 46(3):585–594, 2004.

[20] A. S. Detinko and D. L. Flannery. Nilpotent primitive linear groups over finite fields. *Comm. Algebra*, 33(2):497–505, 2005.

[21] A. S. Detinko and D. L. Flannery. Computing in nilpotent matrix groups. *LMS J. Comput. Math.*, 9:104–134 (electronic), 2006.

[22] A. S. Detinko and D. L. Flannery. Algorithms for computing with nilpotent matrix groups over infinite domains. *J. Symbolic Comput.*, 43(1):8–26, 2008.

[23] A. S. Detinko and D. L. Flannery. On deciding finiteness of matrix groups. *J. Symbolic Comput.*, 44(8):1037–1043, 2009.

[24] M. Deuring. *Algebren*. Zweite, korrigierte Auflage. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 41. Springer-Verlag, Berlin, 1968.

[25] J. D. Dixon. *The structure of linear groups*. Van Nostrand Reinhold, London, 1971.

[26] J. D. Dixon. The orbit-stabilizer problem for linear groups. *Canad. J. Math.*, 37(2):238–259, 1985.

[27] W. Eberly. Decomposition of algebras over finite fields and number fields. *Comput. Complexity*, 1(2):183–210, 1991.

[28] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[29] B. Fein, B. Gordon, and J. H. Smith. On the representation of -1 as a sum of two squares in an algebraic number field. *J. Number Theory*, 3:310–315, 1971.

[30] C. Fieker. *Über relative Normgleichungen in algebraischen Zahlkörpern*. PhD thesis, Technische Universität Berlin, 1997.

[31] C. Fieker. Minimizing representations over number fields. II. Computations in the Brauer group. *J. Algebra*, 322(3):752–765, 2009.

[32] K. Friedl and L. Rónyai. Polynomial time solutions of some problems of computational algebra. In *STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 153–162, New York, NY, USA, 1985. ACM.

[33] G. Fujisaki. Remarks on the Stufe of fields. *Sci. Papers College Gen. Ed. Univ. Tokyo*, 23:1–3, 1973.

[34] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008. Available from `http://www.gap-system.org`.

[35] S. P. Glasby. The Meat-Axe and f-cyclic matrices. *J. Algebra*, 300(1):77–90, 2006.

[36] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman.

[37] D. F. Holt. The Meataxe as a tool in computational group theory. In *The atlas of finite groups: ten years on (Birmingham, 1995)*, volume 249 of *London Math. Soc. Lecture Note Ser.*, pages 74–81. Cambridge Univ. Press, Cambridge, 1998.

[38] D. F. Holt. Cohomology and group extensions in Magma. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 221–241. Springer, Berlin, 2006.

[39] D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of computational group theory.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[40] D. F. Holt, C. R. Leedham-Green, E. A. O'Brien, and S. Rees. Testing matrix groups for primitivity. *J. Algebra*, 184(3):795–817, 1996.

[41] D. F. Holt and S. Rees. Testing modules for irreducibility. *J. Austral. Math. Soc. Ser. A*, 57(1):1–16, 1994.

[42] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[43] B. Huppert. *Character theory of finite groups*, volume 25 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1998.

[44] I. M. Isaacs. *Character theory of finite groups.* Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. Pure and Applied Mathematics, No. 69.

[45] V. S. Konyukh. On linear p-groups (Russian). *Vestsī Akad. Navuk BSSR Ser. Fīz.-Mat. Navuk*, (1):3–8, 124, 1987.

[46] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[47] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[48] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[49] C. R. Leedham-Green and S. McKay. *The structure of groups of prime power order*, volume 27 of *London Mathematical Society Monographs. New Series*. Oxford University Press, Oxford, 2002. Oxford Science Publications.

[50] C. R. Leedham-Green and W. Plesken. Some remarks on Sylow subgroups of general linear groups. *Math. Z.*, 191(4):529–535, 1986.

[51] J. C. Lennox and D. J. S. Robinson. *The theory of infinite soluble groups.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, Oxford, 2004.

[52] F. Lorenz. *Algebra. Vol. 1.* Universitext. Springer, New York, 2006. Fields and Galois theory.

[53] F. Lorenz. *Algebra. Vol. II.* Universitext. Springer, New York, 2008. Fields with structure, algebras and advanced topics.

[54] E. M. Luks. Computing in solvable matrix groups. 33rd annual symposium on Foundations of computer science (FOCS). Proceedings, Pittsburgh, PA, USA, October 24–27, 1992. Washington, DC: IEEE Computer Society Press, 111-120 (1992)., 1992.

[55] MAGMA computational algebra system. `http://magma.maths.usyd.edu.au`.

[56] H. Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[57] H. Minkowski. Zur Theorie der positiven quadratischen Formen. *J. reine angew. Math.*, 101:196–202, 1887.

[58] G. Nebe and A. Steel. Recognition of division algebras. *J. Algebra*, 322(3):903–909, 2009.

[59] J. Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992.

[60] S. Norton. The construction of J_4. In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 of *Proc. Sympos. Pure Math.*, pages 271–277. Amer. Math. Soc., Providence, R.I., 1980.

[61] E. A. O'Brien. Algorithms for matrix groups (preprint). See `http://www.math.auckland.ac.nz/~obrien/research/andrew.pdf`.

[62] R. A. Parker. The computer calculation of modular characters (the meat-axe). In *Computational group theory (Durham, 1982)*, pages 267–274. Academic Press, London, 1984.

[63] R. A. Parker. An integral meataxe. In *The atlas of finite groups: ten years on (Birmingham, 1995)*, volume 249 of *London Math. Soc. Lecture Note Ser.*, pages 215–228. Cambridge Univ. Press, Cambridge, 1998.

[64] R. A. Parker and R. A. Wilson. The computer construction of matrix representations of finite groups over finite fields. *J. Symbolic Comput.*, 9(5-6):583–590, 1990. Computational group theory, Part 1.

[65] D. Perrin. *Algebraic geometry*. Universitext. Springer-Verlag London Ltd., London, 2008.

[66] R. S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982. Studies in the History of Modern Science, 9.

[67] W. Plesken and B. Souvignier. Constructing rational representations of finite groups. *Experiment. Math.*, 5(1):39–47, 1996.

[68] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[69] D. N. Rockmore, K.-S. Tan, and R. Beals. Deciding finiteness for matrix groups over function fields. Technical report, Dartmouth College, 1995. PCS-TR94-227.

[70] D. N. Rockmore, K.-S. Tan, and R. Beals. Deciding finiteness for matrix groups over function fields. *Israel J. Math.*, 109:93–116, 1999.

[71] S. Roman. *Field theory*, volume 158 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[72] S. Roman. *Advanced linear algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2008.

[73] P. Roquette. Realisierung von Darstellungen endlicher nilpotenter Gruppen. *Arch. Math. (Basel)*, 9:241–250, 1958.

[74] T. Rossmann. Irreducibility testing of finite nilpotent linear groups. *J. Algebra*, 324(5):1114–1124, 2010.

[75] T. Rossmann. Primitivity testing of finite nilpotent linear groups. *LMS J. Comput. Math.*, 14:87–98, 2011.

[76] T. Rossmann. *finn – computing with finite nilpotent linear groups, 0.57*, 2011. See `http://www.maths.nuigalway.ie/~tobias/finn`.

[77] D. Segal. *Polycyclic groups*, volume 82 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1983.

[78] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, No. 7.

[79] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

[80] J.-P. Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, second edition, 2008.

[81] M. Shirvani and B. A. F. Wehrfritz. *Skew linear groups*, volume 118 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1986.

[82] D. Simon. Solving norm equations in relative number fields using S-units. *Math. Comp.*, 71(239):1287–1305 (electronic), 2002.

[83] B. Souvignier. Decomposing homogeneous modules of finite groups in characteristic zero. *J. Algebra*, 322(3):948–956, 2009.

[84] G. Stroth. *Algebra. Einführung in die Galoistheorie.* Walter de Gruyter & Co., Berlin, 1998.

[85] D. A. Suprunenko. *Matrix groups*. American Mathematical Society, Providence, R.I., 1976. Translations of Mathematical Monographs, Vol. 45.

[86] B. M. Trager. Algebraic factoring and rational function integration. Symbolic and algebraic computation, Proc. 1976 ACM Symp., Yorktown Heights/N.Y., 219-226 (1976), 1976.

[87] B. A. F. Wehrfritz. *Infinite linear groups. An account of the group-theoretic properties of infinite groups of matrices*. Springer-Verlag, New York, 1973. Ergebnisse der Matematik und ihrer Grenzgebiete, Band 76.

[88] B. A. F. Wehrfritz. Nilpotent subgroups of $\mathrm{GL}(n, \mathbb{Q})$. *Glasg. Math. J.*, 43(3):477–485, 2001.

[89] J. S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1998.

Index