# Irreducibility testing of finite nilpotent linear groups

Tobias Rossmann[a]

[a]*School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway, Ireland*

**Abstract**

We describe an algorithm for irreducibility testing of finite nilpotent linear groups over various fields of characteristic zero, including number fields and rational function fields over number fields. For a reducible group, our algorithm constructs a proper submodule. An implementation in Magma is publicly available.

*Keywords:* irreducibility testing, linear groups, nilpotent groups

The definitive version of this article has been published:
J. Alg. 324: 1114–1124, 2010.
DOI: 10.1016/j.jalgebra.2010.04.031

## 1. Introduction

Let $G \leqslant \mathrm{GL}(V)$ be a linear group over a field $K$. One of the most fundamental computational tasks involving $G$ is to decide whether $G$ is irreducible. In addition, we want to construct a proper $G$-invariant subspace of $V$ whenever $G$ is found to be reducible. We refer to these combined tasks as *irreducibility testing* of $G$.

If the underlying field $K$ is finite, then irreducibility of $G$ can be tested effectively using the Meat-Axe Las Vegas algorithm [14, §7.4]. If $K$ is infinite, then the techniques underpinning the Meat-Axe may still be applied but they will in general not suffice to decide irreducibility of $G$ [13]. Research on irreducibility testing in the case that $K$ is infinite has so far mostly focused on providing practical tools that may or may not succeed for specific examples; see e.g. [11, 13, 23, 24]. Recently, progress has been made in the case that $G$ is finite and $K$ is of characteristic zero. In particular, irreducibility testing of $G$ in the case $K = \mathbf{Q}$ has then been considered in [22, 29] using computations in algebras; this is partially available in Magma V2.16 [2].

In this paper, we describe a new algorithm for irreducibility testing of arbitrary finite nilpotent linear groups $G$ defined over a field $K$ of characteristic zero such that the following conditions are satisfied.

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

(F1) We may algorithmically factorise polynomials over $K$.

(F2) For any extension of the form $E = K(\zeta_{2^k} + \zeta_{2^k}^{-1}, \zeta_q)$ of $K$, where $\zeta_i$ denotes a primitive $i$th root of unity, we may decide solvability of $\alpha^2 + \beta^2 = -1$ in $E$ and we may find a solution of such an equation whenever it exists.

Our approach for irreducibility testing of $G$ is not based on computations in algebras but uses elementary group theory. As a result, we not only test irreducibility but we also obtain structural information about $G$. In a forthcoming paper [27], we will show how this can be exploited to also test primitivity of $G$ if $K$ is a cyclotomic field or if (F1) holds and $\sqrt{-1} \in K$.

Conditions (F1)–(F2) are satisfied for number fields and rational function fields over these; see [31] for (F1) and §8 for (F2). The MAGMA package *finn* [28] contains an implementation of our method for irreducibility testing for these two families of fields $K$. The practicality of our method is indicated by run-times given in §9 below.

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 [6, 7]. Moreover, in [6] a method to simultaneously test irreducibility and primitivity of nilpotent linear groups over finite fields is described. This has been the starting point of the results described in this paper.

Throughout, $K$ is always a field of characteristic zero and $V$ is a non-trivial $K$-vector space of finite dimension $|V : K|$. We assume that condition (F1) holds for $K$. As above, for $i \geqslant 1$, $\zeta_i \in \overline{K}$ denotes a primitive $i$th root of unity, where $\overline{K}$ is a fixed algebraic closure of $K$.

## 2. Overview

Let $G \leqslant \mathrm{GL}(V)$ be a finite nilpotent group. If $G$ is abelian, then it is well-known how irreducibility of $G$ can be tested; cf. [1, §5.2] and see §5.2 below. We may thus assume that $G$ is non-abelian. Our algorithm for irreducibility testing of $G$ is based on the following two steps. First, we can find a non-cyclic abelian normal subgroup of $G$ or prove that no such subgroup exists (Section 4). In the second step, two cases can occur: if we found a non-cyclic abelian $A \lhd G$, then we can either prove reducibility of $G$ or we can construct $H < G$ and $U < V$ such that $G$ acts irreducibly on $V$ if and only if $H$ acts irreducibly on $U$ (Section 5); we then replace $G$ by the image of $H$ in $\mathrm{GL}(U)$ and $V$ by $U$ and start again. On the other hand, if $G$ does not have non-cyclic abelian normal subgroups, then we can test irreducibility of $G$ directly (Section 6). Only in this final case do we have to assume that condition (F2) from §1 is satisfied; (F1), in contrast, is used throughout.

A similar strategy for irreducibility testing is used in [6, §3] for nilpotent linear groups over finite fields. However, we use different methods to perform the tasks involved. In particular, our method for locating non-cyclic abelian normal subgroups is considerably simpler, and it will succeed whenever such a subgroup exists.

## 3. Preliminaries and notation

The following is a collection of basic facts on completely reducible modules; see [5, §4.3]. Let $R$ be a ring and $M$ be an $R$-module. If $M$ does not have any proper submodules and $M \neq 0$, then $M$ is *irreducible* (or simple). If $M$ is a direct sum of irreducible $R$-modules, then $M$ is *completely reducible* (or semisimple). 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 $M$.

Suppose that $F$ is a field, $W$ is a finite-dimensional $F$-vector space, and $R$ is an (associative) $F$-algebra of endomorphisms of $W$ containing the identity $1_W$. Then (i) $W$ is a completely reducible $R$-module if and only if $R$ is semisimple and (ii) $W$ is a homogeneous $R$-module if and only if $R$ is simple; see [30, §14]. Let $G \leqslant \mathrm{GL}(W)$. Denote by $F[G]$ the subalgebra of $\mathrm{Hom}_F(W, W)$ generated by $G$. We say that $G$ is *completely reducible*, *homogeneous*, or *irreducible* if $W$ is a completely reducible, homogeneous, or irreducible $F[G]$-module, respectively. By Maschke's theorem [25, 8.1.2], finite linear groups in characteristic zero are completely reducible.

## 4. Finding non-cyclic abelian normal subgroups

We give an algorithm which constructs a non-cyclic abelian normal subgroup of a non-abelian finite nilpotent group or proves that no such subgroup exists.

### *4.1. ANC groups*

We call a finite nilpotent group all of whose abelian normal subgroups are cyclic an *ANC group*. Denote by $\mathrm{D}_{2^k}$, $\mathrm{SD}_{2^k}$, and $\mathrm{Q}_{2^k}$ 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.

**Theorem 4.1** ([26, 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 $\mathrm{Q}_8$ or to $\mathrm{D}_{2^k}$, $\mathrm{SD}_{2^k}$, or $\mathrm{Q}_{2^k}$ ($k \geqslant 4$), and*
(ii) *$G_{2'}$ is cyclic.*

The following is essentially [6, Lem. 3.6]. The new proof we give for the "only if" part will lead to a very simple algorithm below.

**Proposition 4.2.** *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.* By [6, 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. Clearly, $H_2 \cong \mathrm{Q}_8$ implies that $G_2 = H_2$. 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 $p$. By [25, 5.3.6], $H_p$ would then be cyclic or generalised quaternion. These cases are ruled out by our assumption and the fact that $H$ has class 2. Hence, $A(h)$ is non-cyclic for some $h \in H_p$. ♦

### *4.2. The function* NoncyclicAbelian

We introduce NoncyclicAbelian which constructs a non-cyclic abelian normal subgroup of a non-abelian finite nilpotent group $G$ or proves that $G$ is an ANC group. For a finite abelian group $A$, we let ExponentElement($A$) denote an element $a \in A$ whose order $\mathrm{ord}\,(a)$ coincides with the exponent $\exp(A)$.

**Algorithm 4.3.** NoncyclicAbelian(G)
**Input:** a non-abelian 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

```
 1: let A ◁ G be abelian
 2: loop
 3:     if A is non-cyclic then return A
 4:     a ← ExponentElement(A), C ← C_G(a)
 5:     if C ⩽̸ A, say c ∈ C \ A then
 6:         while [c, g] ∉ A for some g ∈ G do c ← [c, g]
 7:         A ← ⟨a, c⟩
 8:     else
 9:         H ← C_G(ExponentElement([G, G]))
10:         if H_p is non-cyclic abelian for some p then return H_p
11:         if H_p ≇ Q_8 is non-abelian for some p then
12:             if Z(H_p) is non-cyclic then return Z(H_p)
13:             repeat choose h ∈ H_p, let A ← ⟨h, Z(H_p)⟩ until A is non-cyclic
14:             return A
15:         return fail
```

While choosing $A = 1$ would be valid in line 1, in our implementation [28], we use [6, Alg. 1] to construct a non-central abelian normal subgroup of $G$. Note that in lines 5–6, we perform membership tests in cyclic subgroups. In line 8, $A = \mathrm{C}_G(A)$ 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 4.2; termination is guaranteed provided that in line 13, we do not choose the same element $h$ twice.

## 5. Reduction using non-cyclic abelian normal subgroups

We now describe how our algorithm for irreducibility testing of a finite nilpotent linear group makes use of non-cyclic abelian normal subgroups. Recall that $K$ is a field of characteristic zero such that condition (F1) from §1 holds.

*5.1. Irreducibility testing and normal subgroups*

**Lemma 5.1** ([6, Thm. 3.1]). *Let $G \leqslant \mathrm{GL}(V)$ be completely reducible, $N \lhd G$, and $V = U_1 \oplus \cdots \oplus U_r$ be the homogeneous decomposition of $V$ as a $K[N]$-module. Then $G$ is irreducible if and only if $G$ acts transitively on $\{U_1, \ldots, U_r\}$ and $\mathrm{Stab}_G(U_1)$ acts irreducibly on $U_1$.*

Given $U_1, \ldots, U_r$, the orbit of $U_1$ under $G$ and $\mathrm{Stab}_G(U_1)$ can be computed at the same time using the orbit-stabiliser algorithm [14, §4.1]. As in [6], we will only apply Lemma 5.1 for abelian $N$; in §5.2, we describe methods for decomposing $V = U_1 \oplus \cdots \oplus U_r$ in this case. Note that if $N \lhd G$ is non-cyclic abelian, then $K[N]$ is not a field, whence $N$ acts inhomogeneously on $V$.

*5.2. The homogeneous decomposition for abelian groups*

We describe two methods for constructing the homogeneous decomposition of the natural module of a finite abelian linear group over $K$. The first one is an already known Las Vegas algorithm. The second approach has a potentially smaller memory footprint and it also often performed better during our experiments. We begin with a well-known ingredient used in both methods.

*The homogeneous decomposition for a single endomorphism.* Let $\phi$ be an endomorphism of $V$. It is well-known that $V$ is a completely reducible $K[\phi]$-module if and only if the minimal polynomial $f$ of $\phi$ is square-free; see [30, §17]. Supposing that this is the case, let $f = f_1 \cdots f_r$ be the factorisation of $f$ into irreducibles. Then it is easy to see that the homogeneous components of $V$ as a $K[\phi]$-module are the kernels $\mathrm{Ker}(f_1(\phi)), \ldots, \mathrm{Ker}(f_r(\phi))$.

*First method.* The following has already been used in [1, §5.2]. Let $G \leqslant \mathrm{GL}(V)$ be completely reducible and abelian and let $(v_1, \ldots, v_s)$ be a $K$-basis of $K[G]$. It is proved in [9, §§2–3] that for sufficiently large finite $E \subset K$, a random element $v = e_1 v_1 + \cdots + e_s v_s$ with high probability satisfies $K[G] = K[v]$, where the $e_i$ are chosen independently and uniformly from $E$. If $K[G] = K[v]$, then we may find the homogeneous decomposition of $V$ as a $K[G]$-module as above. Since for any $v \in K[G]$, we have $K[v] = K[G]$ if and only if $\mathrm{degree}(f) = s$, where $f$ is the minimal polynomial of $v$, we obtain a Las Vegas algorithm for computing the homogeneous decomposition of $V$ as a $K[G]$-module.

*Second method.* In the last paragraph, to compute a basis of $K[G]$ using a "spinning-type" algorithm (cf. [8, §3.1]), $\mathcal{O}(|V : K|^3)$ 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 needs to store $\mathcal{O}(n \cdot |V : K|^2)$ field elements, where $n$ is the number of defining generators of $G$.

**Algorithm 5.2.** HomogeneousDecompositionAbelian($G$)
**Input:** a 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*

In line 13, a suitable $i$ exists for the following reason: let $e = \exp(H) = \mathrm{ord}\,(a)$. We have $r = 1$ so that $K[a]$ is a field. The element $a$ is a primitive $e$th 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 $i$. Note that $K[c]$ is semisimple since $G$ is abelian [16, IV, §9].

**Proposition 5.3.** *Algorithm 5.2 terminates and returns the homogeneous decomposition of $V$ as a $K[G]$-module.*

*Proof.* Each iteration of the while loop either decreases $|\bigoplus \mathit{quasi} : K|$ or it increases $|\mathit{quasi}|$. The estimate $|\mathit{quasi}| \leqslant |\bigoplus \mathit{quasi} : K|$ implies that after $\mathcal{O}(|V : K|^2)$ iterations, *quasi* will be empty whence Algorithm 5.2 terminates. The following statements, which clearly remain true after every execution of the body of the while loop imply the correctness of Algorithm 5.2: (i) $V = \bigoplus (\mathit{quasi} \cup \mathit{homg})$ (the union being disjoint), (ii) $G$ acts homogeneously on all elements of *homg*, and (iii) for distinct elements $U_1, U_2 \in \mathit{quasi} \cup \mathit{homg}$, there exists $g \in K[G]$ such that $U_1$ and $U_2$ are homogeneous non-trivial $K[g]$-modules, but the simple $K[g]$-submodules of $U_1$ and $U_2$ are not isomorphic. ♦

*Irreducibility testing of abelian groups.* Let $G \leqslant \mathrm{GL}(V)$ be homogeneous and abelian and $0 \neq x \in V$. Then $K[G]$ is a field and $G$ is reducible if and only if $x \cdot K[G] < V$. We can thus test irreducibility of completely reducible abelian linear groups over $K$.

*5.3. Bounding the order of a homogeneous abelian subgroup*

We only need an inhomogeneous abelian normal subgroup of the finite nilpotent group $G \leqslant \mathrm{GL}(V)$ in order to use Lemma 5.1. Instead of attempting to construct a non-cyclic abelian $A \lhd G$ as in §4, we may thus consider the task of either finding an *inhomogeneous* abelian $A \lhd G$ or proving that $G$ is an ANC group. This can be done by modifying Algorithm 4.3: whenever we have found a cyclic $A \lhd G$, 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. Define $\xi_K\colon \mathbf{N} \to \mathbf{N} \cup \{\infty\}$ by $\xi_K(d) = \sup\Big(|A| : A \leqslant \mathrm{GL}_d(K) \text{ is homogeneous finite abelian}\Big)$.

**Lemma 5.4.** *If $K/\mathbf{Q}$ is finitely generated, then $\xi_K(d) = \mathcal{O}(d^{1+\varepsilon})$ for all $\varepsilon > 0$.*

*Proof.* For $m \geqslant 1$, define $\psi(m) = |K(\zeta_m) : K|$. Let $E$ be the algebraic closure of $\mathbf{Q}$ in $K$. Then $E/\mathbf{Q}$ is finitely generated by [20, Thm. 1.6.1(ii)] so that $|E : \mathbf{Q}| < \infty$. [18, Thm. VI.1.12] yields $\psi(m) = |\mathbf{Q}(\zeta_m) : \mathbf{Q}(\zeta_m) \cap K|$ whence $1 \leqslant \frac{\varphi(m)}{\psi(m)} = |\mathbf{Q}(\zeta_m) \cap K : \mathbf{Q}| \leqslant |E : \mathbf{Q}|$, where $\varphi$ is Euler's function. It follows from [12, Thm. 327] that there exists $C > 0$ such that $m \leqslant C \cdot \psi(m)^{1+\varepsilon}$ for all $m \geqslant 1$. If $G \leqslant \mathrm{GL}_d(K)$ is finite, abelian, and homogeneous, then $\psi(|G|) = |K[G] : K| \leqslant d$ whence $|G| \leqslant C \cdot d^{1+\varepsilon}$. ♦

Thus, if $K/\mathbf{Q}$ is finitely generated then the membership tests and centraliser computations in InhomogeneousAbelian can be performed efficiently. However, in our implementation [28] we nonetheless use NoncyclicAbelian since it performed better during our experiments.

## 6. Irreducibility testing of ANC groups

Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian ANC group. We now describe how irreducibility testing of $G$ is related to condition (F2) from §1.

### *6.1. Nice generators*

Define $\vartheta(G) = 1$ if $G_2$ is dihedral or semidihedral and $\vartheta(G) = -1$ if $G_2$ is generalised quaternion. There exists a cyclic $A \lhd G$ with $|G : A| = 2$ and we may assume that $A$ is homogeneous. We essentially get $A$ from Algorithm 4.3 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 $A = \langle h \rangle \times G_{2'}$ for any non-central $h \in G_2$. Let $A = \langle a \rangle$ and pick $g \in G_2 \setminus A$. Write $a = a_2 \cdot a_{2'}$ 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 $g^2 = \vartheta(G) \cdot 1_V$.

### *6.2. Characterisation of submodules*

We keep the notation from §6.1. Since $A$ is homogeneous, $F = K[A]$ is a field. Let $U$ be any 1-dimensional $F$-subspace of $V$. Then $U + Ug$ is a $K[G]$-submodule of $V$ and we may hence assume that $V = U + Ug$. If $U = Ug$, then $A$ and hence $G$ is irreducible. Thus, suppose that $V = U \oplus Ug$. The quotient $G/A$ naturally acts as a subgroup of $\mathrm{Gal}(F/K)$ on $F$. Let $Z$ be the fixed field and $\mathrm{Norm}_{F/Z}\colon F \to Z, b \mapsto b \cdot b^g$ be the norm map.

**Lemma 6.1.**

(i) *Let* $0 \neq x \in V$. *Then* $x \cdot K[G] < V$ *if and only if there exists* $b \in F$ *with* $\mathrm{Norm}_{F/Z}(b) = \vartheta(G)$ *such that* $x \in \mathrm{Ker}(g - b)$.

(ii) *Let* $b \in F$ *satisfy* $\mathrm{Norm}_{F/Z}(b) = \vartheta(G)$. *Then* $\mathrm{Ker}(g - b) \neq 0$.

*Proof.* Since $|V : F| = 2$, a proper $K[G]$-submodule of $V$ has $F$-dimension 1. If $0 \neq x \in V$, then $x \cdot F$ is $K[G]$-invariant if and only if $xg = xb$ for some $b \in F$. Now $xg = xb$ implies $x \cdot \vartheta(G) = xg^2 = xbg = xgb^g = xbb^g = x \cdot \mathrm{Norm}_{F/Z}(b)$ whence (i) follows. By choosing a $K$-basis according to $V = U \oplus Ug \cong_F F^2$, we may assume that $A$ is generated by $a = \mathrm{diag}(\tilde{a}, \tilde{a})$ where $a \mapsto \tilde{a}$ induces a $K$-isomorphism $F \xrightarrow{\lambda} \tilde{F} = K[\tilde{a}]$, and $g = \left[\begin{smallmatrix} \cdot & s \\ s' & \cdot \end{smallmatrix}\right]$. As in the proof of [6, Lem. 3.14], using $g^2 = \vartheta(G) \cdot 1_V$, we find $s' = \vartheta(G) \cdot s^{-1}$ and hence $a^g = \mathrm{diag}(s\tilde{a}s^{-1}, s^{-1}\tilde{a}s) \in A$. Let $\sigma \in \mathrm{Gal}(F/Z)$ be conjugation by $g$. We have seen that conjugation by $s$ induces $\tilde{\sigma} \in \mathrm{Gal}(\tilde{F}/K)$ such that $\sigma\lambda = \lambda\tilde{\sigma}$. If $b = \mathrm{diag}(\tilde{b}, \tilde{b})$, then $\tilde{b} \cdot \tilde{b}^{\tilde{\sigma}} = (b \cdot b^{\sigma})^{\lambda} = \vartheta(G)$, whence $\left[\begin{smallmatrix} -\tilde{b}^{-1} & \cdot \\ \vartheta(G)s^{-1} & s^{-1}\tilde{b}s \end{smallmatrix}\right](g - b) = \left[\begin{smallmatrix} 1 & -\tilde{b}^{-1}s \\ \cdot & \cdot \end{smallmatrix}\right]$ is singular. This proves (ii). ♦

Thus, $G$ is reducible if and only if $\mathrm{Norm}_{F/Z}(b) = \vartheta(G)$ for some $b \in F$. If $\vartheta(G) = 1$, then $G$ is reducible and the non-zero vectors of $\mathrm{Ker}(g \pm 1)$ generate proper $K[G]$-submodules of $V$. Let $\vartheta(G) = -1$ and write $|G| = 2^k \cdot q$, where $q$ is odd. Define $F' = K(\zeta_{2^{k-1}}, \zeta_q)$ and $Z' = K(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1}, \zeta_q)$. The towers $F/Z/K$ and $F'/Z'/K$ of $K$-extensions are isomorphic. Since $F' = Z'(\sqrt{-1})$, we see that the $b \in F$ with $\mathrm{Norm}_{F/Z}(b) = -1$ are in one-to-one correspondence with pairs $(\alpha, \beta) \in Z \times Z$ satisfying $\alpha^2 + \beta^2 = -1$. Hence, if $\vartheta(G) = -1$, then $G$ is reducible if and only if $\alpha^2 + \beta^2 = -1$ can be solved in $Z$. Moreover, constructing a proper submodule is then equivalent (up to solving systems of linear equations) to finding a solution of this equation.

*6.3. An algorithm for irreducibility testing of ANC groups*

Assuming condition (F2) from §1, the following is an algorithm for irreducibility testing of ANC groups.

The function NonzeroElement returns a non-zero vector of a non-trivial vector space. To simplify our pseudo-code, we only return generators of submodules for reducible groups. Bases of the submodules can then be found using the "spinning algorithm" [14, §7.4.1].

**Algorithm 6.2.** IsIrreducibleANC$(G, A)$

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

1: find $\vartheta(G)$, $g$, and $a = a_2 \cdot a_{2'}$ as in §6.1
2: $x \leftarrow$ NonzeroElement$(V)$, $U \leftarrow x \cdot K[A]$
3: **if** $U = V$ **then return** `true`
4: **if** $U + Ug < V$ **then return** `false`, $x$
5: **if** $\vartheta(G) = 1$ **then return** `false`, NonzeroElement$(\mathrm{Ker}(g - 1))$
6: **if** $\alpha^2 + \beta^2 \neq -1_V$ for all $\alpha, \beta \in Z = K\left[a_2 + a_2^{-1}, a_{2'}\right]$ **then return** `true`
7: find $\alpha, \beta \in Z$ such that $\alpha^2 + \beta^2 = -1_V$
8: **return** `false`, NonzeroElement$\left(\mathrm{Ker}\left(g - \alpha - \beta \cdot a_2^{\mathrm{ord}\,(a_2)/4}\right)\right)$

## 7. An algorithm for irreducibility testing of finite nilpotent groups

Assuming that conditions (F1)–(F2) from §1 hold, we are now in a position to summarise our main algorithm.

**Algorithm 7.1.** IsIrreducible($G$)
**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

We note that if we apply the above pseudo-code in the case that $G$ is not nilpotent or finite, then the output (if any) will in general not be meaningful.

## 8. Aspects of the field: solving $\alpha^2 + \beta^2 = -1$

Algorithm 7.1 can test irreducibility of any finite nilpotent linear group over $K$ provided that conditions (F1)–(F2) from §1 are satisfied. We will now consider condition (F2) and its implications for various fields.

### *8.1. Fields containing $\sqrt{-1}$*

A special case occurs if $\sqrt{-1} \in K$; we may detect this since we assumed that (F1) holds. 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 $K[h] \subseteq K[A]$ is not a field. Thus, $A$ acts inhomogeneously on $V$ and IsIrreducibleANC will never be called in line 10 of Algorithm 7.1. Hence, if $\sqrt{-1} \in K$, then we can test irreducibility of arbitrary finite nilpotent linear groups over $K$ and, moreover, our algorithm for this is also considerably simpler than in general.

### *8.2. Number fields*

Let $K$ be a number field; we refer to [4] for background.

**Proposition 8.1** ([10, Thm. 1])**.** *Let $E$ be a number field. Then $\alpha^2 + \beta^2 = -1$ has a solution in $E$ if and only if*

(i) *$E$ is totally imaginary, and*

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

Given $E$, the conditions in Proposition 8.1 can be tested algorithmically and this already implies that (F2) holds for number fields. However, recall that we need to investigate the solvability of $\alpha^2 + \beta^2 = -1$ in an extension $E = K(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1}, \zeta_q)$ (denoted $Z'$ in §6) of $K$, where $q \geqslant 1$ is odd and $k \geqslant 3$. The field $E$ will in general have larger degree than $K$ and, in practice, we may be unable to apply Proposition 8.1 to $E$ even if we can apply it to $K$.

We now discuss how we may directly read off from $K$, $k$, and $q$ whether conditions (i)–(ii) in Proposition 8.1 hold in $E$. Since $\mathbf{Q}(\zeta_{2^{k-1}} + \zeta_{2^{k-1}}^{-1})$ is totally real, $E$ is totally imaginary if and only if $K$ is totally imaginary or $q > 1$. Regarding (ii), if $k \geqslant 4$, then $\sqrt{2} \in E$ and all degrees $|E_{\mathfrak{p}} : \mathbf{Q}_2|$ in Proposition 8.1 are even, independently of $K$ or $q$. If $(k, q) = (3, 1)$, then $E = K$ and we may apply Proposition 8.1. In the remaining case, $E = K(\zeta_q)$ for odd $q > 1$. It follows from [4, Prop. 3.5.18] and basic facts on factorisation in number fields [4, §4.4.9] that (ii) holds if and only if $\operatorname{ord}(2 \bmod q) \cdot |K_{\mathfrak{q}} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{q}$ of $K$ above 2, where $\operatorname{ord}(2 \bmod q)$ is the order of $2 + q\mathbf{Z}$ in $(\mathbf{Z}/q\mathbf{Z})^\times$.

Hence, we can decide irreducibility of arbitrary finite nilpotent linear groups over number fields. Moreover, our algorithm for this is also practical for moderately sized input; see §9. In [28], we generally use a norm equation solver to find solutions of $\alpha^2 + \beta^2 = -1$ in $E$. Using the norm equation solvers available in MAGMA this is, however, only practical for $|E : \mathbf{Q}| \leqslant 20$ (approximately). We note that an explicit solution of $\alpha^2 + \beta^2 = -1$ in $\mathbf{Q}(\zeta_q)$ is known from [15, Ex. 38.13d] whenever it exists.

*8.3. Function fields*

Let $E$ be a number field and $K = E(X_1, \ldots, X_t)$, where $X_1, \ldots, X_t$ are algebraically independent over $E$. The following known results and §8.2 imply that condition (F2) is satisfied for $K$.

**Lemma 8.2.**

(i) *Let* $\gamma$ *be an algebraic element over* $E$ *which is contained in some field extension of* $K$. *Then* $X_1, \ldots, X_t$ *are algebraically independent over* $E(\gamma)$.

(ii) $-1$ *is a sum of* $\ell$ *squares in* $K$ *if and only if it is a sum of* $\ell$ *squares in* $E$.

*Proof.* Part (i) follows from [18, Prop. VIII.3.2], [18, Lem. VIII.4.10], and [5, Prop. 11.3.1]. Repeated application of [17, Cor. IX.1.2(ii)] gives (ii). ♦

## 9. The implementation and examples

*9.1. Notes on the implementation*

The MAGMA-package *finn* [28] contains an implementation of our algorithm for irreducibility 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. In order to illustrate the practicality of our method, no Meat-Axe techniques are used in [28]. These methods would not suffice to decide irreducibility

for all input groups but whenever they work, they usually outperform our more involved method.

An important property shared by all of the above-mentioned input fields $K$ is that we may use [7, §3] to obtain an effectively computable isomorphism from the input group $G$ onto a linear group $\tilde{G}$ defined over a finite field. We then perform many of the group-theoretic computations in Algorithm 7.1 in $\tilde{G}$ instead of $G$. This significantly improves the practicality of our method since arithmetic over finite fields is considerably faster in practice.

*9.2. Run-times 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 [21]):

> 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 unless the module is irreducible, this solves a more general problem than our algorithm.

Table 1 shows run-times of irreducibility testing for linear groups over the rationals. All run-times below were obtained on an Intel Xeon E5440 with 16GB RAM running MAGMA V2.16-4 under 64-bit Linux. The examples given cover many of the cases that can occur within Algorithm 7.1. 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 entries in the defining generators. Finally, we give the time in seconds (unless otherwise indicated) irreducibility testing took using our algorithm ("time-$f$") as well as the time ("time-M") it took for the MAGMA function INDECOMPOSABLESUMMANDS to decompose the natural $\mathbf{Q}G_i$-module into a direct sum of irreducibles.

The group $W(i,p)$ is $\mathrm{C}_p \wr \cdots \wr \mathrm{C}_p$ ($i$ factors) realised as an irreducible maximal $p$-subgroup of $\mathrm{GL}_d(\mathbf{Q})$, where $d = (p-1)p^{i-1}$; see [19, §4.5]. We did not use the "natural" generating sets for any of the groups in Table 1. Instead, we applied the product replacement algorithm [3] 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 $\alpha^2 + \beta^2 = -1$ in $\mathbf{Q}(\zeta_{16} + \zeta_{16}^{-1}, \zeta_{11})$; cf. §6. In fact, $\alpha^2 + \beta^2 = -1$ can be solved in $\mathbf{Q}(\zeta_{11})$. As we remarked in §8, explicit solutions of these equations are known over cyclotomic

| group | deg | gens | num | den | irr? | dim | time-$f$ | time-M |
|---|---|---|---|---|---|---|---|---|
| $G_1 \cong \mathrm{Q}_8 \curlyvee \mathrm{Q}_8$ | 16 | 5 | 1 | 1 | no | 4 | 0.01 | 0.06 |
| $G_2 \cong W(5,2) \times W(2,3)$ | 22 | 11 | 1 | 1 | no | 16 | 0.01 | 30min |
| $G_3 \cong \mathrm{C}_2^4 \rtimes \mathrm{C}_2^2$ | 8 | 8 | 5251 | 46 | no | 4 | 0.01 | 0.01 |
| $G_4$ (order 576, class 3) | 14 | 8 | $8.18 \cdot 10^8$ | $2.09 \cdot 10^7$ | no | 4 | 0.01 | 0.01 |
| $G_5$ (order 16,384, class 4) | 16 | 14 | $1.7 \cdot 10^{12}$ | $4.33 \cdot 10^{11}$ | no | 8 | 0.11 | 0.04 |
| $G_6 \cong (\mathrm{Q}_8 \times \mathrm{C}_5) \otimes W(2,3)$ | 48 | 8 | 2 | 1 | yes | – | 0.06 | 29.43min |
| $G_7 \cong \mathrm{C}_3 \rtimes \mathrm{C}_3^2$ | 18 | 3 | $9.30 \cdot 10^5$ | $2.99 \cdot 10^5$ | no | 6 | 0.03 | 0.26 |
| $G_8 \cong (\mathrm{Q}_{16} \times \mathrm{C}_3) \otimes W(2,3)$ | 96 | 10 | 66 | 18 | yes | – | 0.52 | 1.29 |
| $G_9 \cong \mathrm{D}_{32} \times \mathrm{C}_{11}$ | 80 | 5 | $8.78 \cdot 10^7$ | $4.16 \cdot 10^6$ | yes | – | 0.17 | 3.61 |
| $G_{10} \cong W(5,2) \otimes W(2,3)$ | 96 | 11 | 1 | 1 | yes | – | 0.41 | 3h 43min |
| $G_{11} \cong 5^{1+2}$ | 100 | 5 | 1 | 1 | no | 20 | 0.17 | 86.13 |
| $G_{12} \cong \mathrm{Q}_{32} \times \mathrm{C}_{11}$ | 160 | 5 | 1 | 1 | no | 80 | 0.33 | 2h 43min |
| $G_{13} = G_2$ | 22 | 100 | 1 | 1 | no | 16 | 0.12 | 31min |
| $G_{14} = G_3^x$ | 8 | 8 | $2.72 \cdot 10^{32}$ | $1.38 \cdot 10^{30}$ | no | 4 | 0.08 | 0.04 |

Table 1: Run-times for linear groups over the rationals

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, such computations are infeasible. The smallest (degree-wise) rational example of this type is $\mathrm{Q}_{16} \times \mathrm{C}_{23}$ acting in degree 176; it takes less than a second to (non-constructively) prove reducibility of this group. Apart from this exceptional behaviour involving $\alpha^2 + \beta^2 = -1$, in our experiments over the rationals, constructing submodules took little extra time in addition to deciding irreducibility.

### *9.3. Run-times for $K \neq \mathbf{Q}$*

To illustrate the performance of our algorithm over proper extensions of $\mathbf{Q}$, we now consider groups over the fields $\mathbf{Q}(\gamma)$ and $\mathbf{Q}(X)$, where $\gamma$ 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 1). The conjugating matrices were chosen such that no additional coefficient explosion occurred in the transition from $G_i$ to $G_{i,\gamma}$ or $G_{i,X}$.

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 2–3, 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, in practice, $K$ is restricted to being a "small" extension of $\mathbf{Q}$; [28] provides further irrational conjugates of the $G_i$ that illustrate this.

**Acknowledgements**

The author wishes to express his gratitude to Dane Flannery and Alla Detinko for many helpful discussions during the preparation of this paper. Fur-

| group | time-$f$ | vector-mode |
|---|---|---|
| $G_{1,\gamma}$ | 0.07 | 0.07 |
| $G_{2,\gamma}$ | 0.16 | 0.15 |
| $G_{3,\gamma}$ | 0.08 | 0.08 |
| $G_{4,\gamma}$ | 0.23 | 0.21 |
| $G_{5,\gamma}$ | 1.57 | 1.47 |
| $G_{6,\gamma}$ | 0.86 | – |
| $G_{7,\gamma}$ | 0.52 | 0.50 |
| $G_{8,\gamma}$ | 40.38 | – |
| $G_{9,\gamma}$ | 8.44 | – |
| $G_{10,\gamma}$ | 3.54 | – |
| $G_{11,\gamma}$ | 4.14 | 3.79 |
| $G_{12,\gamma}$ | 25.01 | 4.70 |
| $G_{13,\gamma}$ | 0.87 | 0.83 |
| $G_{14,\gamma}$ | 0.16 | 0.15 |

Table 2: Run-times over $\mathbf{Q}(\gamma)$

| group | time-$f$ | vector-mode |
|---|---|---|
| $G_{1,X}$ | 0.06 | 0.06 |
| $G_{2,X}$ | 0.46 | 0.42 |
| $G_{3,X}$ | 0.39 | 0.25 |
| $G_{4,X}$ | 1.12 | 0.91 |
| $G_{5,X}$ | 26.33 | 24.42 |
| $G_{6,X}$ | 1.40 | – |
| $G_{7,X}$ | 4.12 | 2.69 |
| $G_{8,X}$ | 16.5min | – |
| $G_{9,X}$ | 14.57 | – |
| $G_{10,X}$ | 3.76 | – |
| $G_{11,X}$ | 26.32 | 12.21 |
| $G_{12,X}$ | 17h 27min | 8.67 |
| $G_{13,X}$ | 1.14 | 0.79 |
| $G_{14,X}$ | 1.51 | 1.15 |

Table 3: Run-times over $\mathbf{Q}(X)$

thermore, the author is indebted to Bettina Eick for valuable comments on earlier drafts.

## References

[1] B. Assmann and B. Eick. Computing polycyclic presentations for polycyclic rational matrix groups. *J. Symbolic Comput.*, 40(6):1269–1284, 2005.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] 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.

[4] H. Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[5] P. M. Cohn. *Basic algebra*. Springer-Verlag London Ltd., London, 2003. Groups, rings and fields.

[6] A. S. Detinko and D. L. Flannery. Computing in nilpotent matrix groups. *LMS J. Comput. Math.*, 9:104–134 (electronic), 2006.

[7] 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.

[8] A. S. Detinko and D. L. Flannery. On deciding finiteness of matrix groups. *J. Symbolic Comput.*, 44(8):1037–1043, 2009.

[9] W. Eberly. Decomposition of algebras over finite fields and number fields. *Comput. Complexity*, 1(2):183–210, 1991.

[10] 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.

[11] S. P. Glasby. The Meat-Axe and $f$-cyclic matrices. *J. Algebra*, 300(1):77–90, 2006.

[12] 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.

[13] 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.

[14] 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.

[15] B. Huppert. *Character theory of finite groups*, volume 25 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1998.

[16] N. Jacobson. *Basic algebra. II*. W. H. Freeman and Co., San Francisco, Calif., 1980.

[17] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[18] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[19] 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.

[20] A. Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.

[21] MAGMA computational algebra system. `http://magma.maths.usyd.edu.au`.

[22] G. Nebe and A. Steel. Recognition of division algebras. *J. Algebra*, 322(3):903–909, 2009.

[23] 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.

[24] W. Plesken and B. Souvignier. Constructing rational representations of finite groups. *Experiment. Math.*, 5(1):39–47, 1996.

[25] 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.

[26] P. Roquette. Realisierung von Darstellungen endlicher nilpotenter Gruppen. *Arch. Math. (Basel)*, 9:241–250, 1958.

[27] T. Rossmann. Primitivity testing of finite nilpotent linear groups (in preparation).

[28] T. Rossmann. *finn – computing with finite nilpotent linear groups, 0.4*, 2010. Available from `http://www.maths.nuigalway.ie/~tobias/finn`.

[29] B. Souvignier. Decomposing homogeneous modules of finite groups in characteristic zero. *J. Algebra*, 322(3):948–956, 2009.

[30] D. A. Suprunenko. *Matrix groups*. American Mathematical Society, Providence, R.I., 1976. Translated from the Russian, Translation edited by K. A. Hirsch, Translations of Mathematical Monographs, Vol. 45.

[31] 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.