LMS J. Comput. Math. 14 (2011) 87–98 © 2011 Author
doi:10.1112/S1461157010000227

Primitivity testing of finite nilpotent linear groups

Tobias Rossmann

Abstract

We describe a practical algorithm for primitivity testing of finite nilpotent linear groups over various fields of characteristic zero, including number fields and rational function fields over number fields. For an imprimitive group, a system of imprimitivity can be constructed. An implementation of the algorithm in Magma is publicly available.

1. *Introduction*

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. In the case where G is found to be imprimitive, we also want to construct a decomposition $V = U_1 \oplus \cdots \oplus U_r$ as above. We refer to these combined tasks as *primitivity testing* of G.

In [15], the author has obtained an algorithm for irreducibility testing of finite nilpotent linear groups over a range of fields of characteristic zero. In the present paper, we continue this research by developing a practical algorithm for primitivity testing in the same class of linear groups. To the author's knowledge, an effective method for primitivity testing in any non-trivial class of linear groups has so far only been obtained over finite fields [8].

The algorithm described in this paper can test primitivity of arbitrary finite nilpotent linear groups defined over a field K of characteristic zero such that the following conditions (see [15, Section 1]) are satisfied.

- (F1) We can algorithmically factorise univariate polynomials over K.
- (F2) For any extension of K of the form $E = K(\zeta_{2^j} + \zeta_{2^j}^{-1}, \zeta_q)$, where ζ_i denotes a primitive ith root of unity, we can decide solvability of the equation $\alpha^2 + \beta^2 = -1$ in E and we can find a solution of such an equation whenever it exists.

As has been explained in [15], both of these conditions are satisfied if K is a number field or a rational function field over a number field. An implementation of the author's algorithm for primitivity testing over these two families of fields is publicly available in the package *finn* [16] for Magma [1]. We note that *finn* also provides an implementation of the algorithm [15] for irreducibility testing of finite nilpotent linear groups.

We may use a simplified version of the algorithm described here to decide primitivity of finite nilpotent linear groups non-constructively (that is, without constructing a decomposition $V = U_1 \oplus \cdots \oplus U_r$ as above). For this purpose, in (F2) we still have to assume that we can decide solvability of $\alpha^2 + \beta^2 = -1$, but we no longer need to be able to find a solution.

Received 23 June 2010; revised 30 September 2010.

2000 Mathematics Subject Classification 20D15, 20H20.

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

2. *Overview*

Unless explicitly stated otherwise, in this paper we always assume that K is a field of characteristic zero such that conditions (F1) and (F2) are satisfied. We always let V be a non-trivial K-vector space of finite dimension $|V : K|$.

Let $G \leqslant \mathrm{GL}(V)$ be an irreducible finite nilpotent linear group. The algorithm for primitivity testing of G described in this paper is based on the following. First, the case that G is abelian can be easily treated (Section 5), so let G be non-abelian. Next, using algorithms from [**15**], we can either exhibit that G is imprimitive, or we can prove that all abelian normal subgroups of G are cyclic (Section 6). Let us therefore assume that we are in the latter case.

The finite nilpotent groups all of whose abelian normal subgroups are cyclic are well understood (see Theorem 6.2 below). We use this to study the enveloping algebras of G (Section 7) and the maximal subgroups of G (Section 8). In this way, we are able to either find a maximal subgroup $H < G$ which fixes a subspace $U < V$ that belongs to a system of imprimitivity for G, or we can prove that G is primitive. For three important families of ground fields K, we obtain simplifications (§§ 8.4–8.5); these fields are (i) number fields, (ii) rational function fields over number fields, and (iii) fields containing $\sqrt{-1}$. A summary of the algorithm is given in Section 9. Finally, in Section 10, we report on the implementation in Magma and provide sample run-times.

As in [**15**], the first major step is to attempt to construct a non-cyclic abelian normal subgroup. This approach is taken from [**4**, Section 3], where an algorithm for irreducibility and primitivity testing of nilpotent linear groups over finite fields was developed. However, subsequent steps of the present method differ considerably from [**4**].

3. *Preliminaries and notation*

We collect basic notions from the theory of linear groups (see [**19**, Section 1] and [**18**, Section 14]) and establish some notation.

Let K be any field. The *enveloping algebra* $K[G]$ of a linear group $G \leqslant \mathrm{GL}(V)$ is the subalgebra of $\mathrm{End}(V)$ generated by G. We say that G is *completely reducible* (respectively *homogeneous*) if $K[G]$ is semisimple (respectively simple). It follows that G is completely reducible if and only if V is a direct sum of irreducible $K[G]$-submodules. Furthermore, G is homogeneous if and only if G is completely reducible and the $K[G]$-composition factors of V are all isomorphic. By Maschke's theorem, finite linear groups in characteristic zero are completely reducible. If G is abelian, then it is homogeneous if and only if $K[G]$ is a field.

Let G be completely reducible and let $(U_i)_{i \in I}$ be representatives of the isomorphism classes of irreducible $K[G]$-submodules of V. Define V_i to be the sum of all $K[G]$-submodules of V that are isomorphic to U_i. Then each V_i is a maximal homogeneous $K[G]$-submodule of V, called a *homogeneous component*, and $V = \bigoplus_{i \in I} V_i$ is the *homogeneous decomposition* for G. If G is completely reducible and $N \triangleleft G$, then G permutes the homogeneous decomposition for N by Clifford's theorem.

If V is irreducible as a $K[G]$-module, then G is called *irreducible*. Suppose that G is irreducible. A *system of imprimitivity* for G is a set $\mathcal{U} = \{U_1, \ldots, U_r\}$ of subspaces $0 < U_i < V$ such that (i) $V = U_1 \oplus \cdots \oplus U_r$ and (ii) G permutes $\mathcal{U}$ in its natural action on subspaces. Note that the permutation action of G on $\mathcal{U}$ is necessarily transitive by irreducibility of G. The elements of $\mathcal{U}$ are *blocks* and the subgroups $\mathrm{Stab}_G(U_i)$ are *block stabilisers* for G. If G admits a system of imprimitivity, then G is *imprimitive*; otherwise, G is *primitive*. Note that we only apply these notions to irreducible groups.

Let K have characteristic zero. We denote by ζ_n a primitive nth root of unity, where we assume that all the ζ_n are contained in some algebraic extension of K. We write $\mathbf{E}_n = \mathbf{Q}(\zeta_n)$. If a group G acts by automorphisms on a field F, we let F^G be the fixed field of this action.

4. *Basic facts regarding imprimitivity*

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

LEMMA 4.1. *Let $G \leqslant \mathrm{GL}(V)$ be irreducible and let $U < V$.*
(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 [18, Theorem 15.1(iii)] and [18, Theorem 15.3]. □

LEMMA 4.2. *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 $U < V$ 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 4.1. Let $U < V$ 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 Ug is $|G : \mathrm{Stab}_G(U)| \leqslant |G : H|$. Hence, $H = \mathrm{Stab}_G(U)$ and U is a block for G. □

LEMMA 4.3. *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. Both U and Ug are distinct irreducible $K[H]$-submodules, whence $U \cap Ug = 0$. This proves (i); part (ii) then follows immediately. □

LEMMA 4.4. *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 $\mathfrak{U}$ be a system of imprimitivity for G, say $|\mathfrak{U}| = r$. A primitive permutation representation of G has prime degree [18, Lemma 5.1]. Since an imprimitive action of G on $\mathfrak{U}$ yields a smaller system of imprimitivity for G, the result follows by induction on r. □

Given a system of imprimitivity for G of composite size, we may use standard permutation group algorithms [7, Chapter 4] to construct one of prime size. This will become relevant for estimating the computational difficulty of constructing a block; see § 8.3.

COROLLARY 4.5. *Let $G \leqslant \mathrm{GL}(V)$ be an irreducible nilpotent group. Then G is imprimitive if and only if some prime index subgroup of G is a block stabiliser for G.*

5. *Primitivity testing of abelian groups*

Primitivity of irreducible finite abelian linear groups in characteristic zero can be easily tested. It is worthwhile to discuss this in detail since, in Section 8, primitivity of a certain type of non-abelian group $G \leqslant \mathrm{GL}(V)$ will be shown to be connected to that of an irreducible abelian normal subgroup of G. For a group G and $n \geqslant 1$, we write $G^n = \langle g^n : g \in G \rangle$.

As is well known, a finite irreducible abelian group $G \leqslant \mathrm{GL}(V)$ is cyclic; indeed, G is a subgroup of the multiplicative group of the field $K[G]$. The maximal subgroups of G are precisely of the form G^p, where p is a prime divisor of $|G|$. The following is now immediate from Lemma 4.2.

PROPOSITION 5.1. *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 one-dimensional $K[G^p]$-subspace of V is a block for G.*

REMARK 5.2. Let G and p be as in Proposition 5.1. 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 $p^2 | n$. 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.

REMARK 5.3. If $K/\mathbf{Q}$ is finitely generated, then a homogeneous finite abelian K-linear group of degree d has order $\mathcal{O}(d^{1+\varepsilon})$ for any $\varepsilon > 0$; see [15, Lemma 5.4]. Hence, $|G|$ is 'small' in Proposition 5.1 and it is feasible to test primitivity of G by looping over all primes p with $p^2 || G|$ 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 relative degree $|K[G] : K[G^p]|$ can then be effectively computed using the degrees of the minimal polynomials of g and g^p.

6. *Non-cyclic abelian normal subgroups*

The following well-known consequence of Clifford's theorem is the basis of the algorithm for primitivity testing developed in this paper.

LEMMA 6.1. *Let $G \leqslant \mathrm{GL}(V)$ be irreducible. If $A \lhd G$ is finite, non-cyclic, and abelian, then A is inhomogeneous. Hence, the homogeneous components of V as a $K[A]$-module constitute a system of imprimitivity for G.*

Proof. Since A is non-cyclic, $K[A]$ cannot be a field. □

As in [15, § 4.1], we define an ANC *group* to be a finite nilpotent group all of whose abelian normal subgroups are cyclic. In [15], practical algorithms for the following tasks have been developed.

- Given a finite nilpotent group G, either construct a non-cyclic abelian normal subgroup of G or prove that G is an ANC group [15, Algorithm 4.3].
- Given a finite abelian $A \leqslant \mathrm{GL}(V)$, construct the homogeneous decomposition of V as a $K[A]$-module [15, Algorithm 5.2].

Primitivity testing of finite nilpotent linear groups over K is thus reduced to the case of non-abelian ANC groups. The structure of these groups is well understood. Denote by D_{2^j}, SD_{2^j}, and Q_{2^j} the dihedral, semidihedral, and generalised quaternion groups of order 2^j, 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 6.2 [14, Lemma 3]. *A finite nilpotent group G is an* ANC *group if and only if:*
(i) *G_2 is cyclic or isomorphic to Q_8 or to D_{2^j}, SD_{2^j}, or Q_{2^j} $(j \geqslant 4)$; and*
(ii) *$G_{2'}$ is cyclic.*

7. ANC *groups and their enveloping algebras*

In this section, K can be arbitrary of characteristic $\neq 2$. We refer to [10, Chapter III] for details of the following. Recall that a *quaternion algebra* over K is a central simple four-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) irreducible $\mathcal{A}$-module has K-dimension two. For $a, b \in K^\times$, define $(a, b|K)$ to be the K-algebra with basis $(1, i, j, k)$ and multiplication $i^2 = a$, $j^2 = b$, $ij = k = -ji$. Then $(a, b|K)$ is a quaternion algebra [10, Proposition III.1.1]; it splits if and only if $ax^2 + by^2 = 1$ for some $x, y \in K$ [10, Theorem III.2.7].

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. As in [15, § 6.1], 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. In addition, define $\delta(G) = 1$ if G_2 is dihedral or generalised quaternion and $\delta(G) = -1$ if G_2 is semidihedral. As shown by Lemmas 7.1 and 7.3 below, these numerical invariants occur naturally in the study of the enveloping algebras of linear ANC groups.

LEMMA 7.1 (Cf. [14, Section 4]). *Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian* ANC *group which contains a homogeneous cyclic subgroup A of index two. Write $Z = \mathrm{Z}(K[G])$. Then $Z = K[A]^G$ and $K[G] \cong (\vartheta(G), -1|Z)$ as Z-algebras. In particular, $|K[G] : K[A]| = 2$.*

Proof. Let $g \in G$ with $G = \langle A, g\rangle$ and $g^2 = \vartheta(G) \cdot 1_V$. Define $F = K[A]$. Then $K[G] = F + gF$ but $F \neq gF$ so that $K[G] = F \oplus gF$. Hence, $K[G]$ is the cyclic algebra $(F/F^G, \sigma, \vartheta(G))$, where $\sigma \in \mathrm{Gal}(F/F^G)$ is conjugation by g; see [12, Chapter 30] for background. In particular, $K[G]$ is simple, $Z = F^G$, and $|K[G] : Z| = 4$. If $\vartheta(G) = 1$, then $K[G] \cong \mathrm{M}_2(Z) \cong (1, -1|Z)$. Let $\vartheta(G) = -1$. If $h \in A$ has order four, then $h \notin Z$. Since $|F : Z| = 2$, we obtain $F = Z[h]$. Thus, $K[G] = Z[G_2] = Z[H]$, where $H = \langle g, h\rangle \cong \mathrm{Q}_8$. Clearly, $Z[H] \cong (-1, -1|Z)$. □

We say that $G \leqslant \mathrm{GL}(V)$ is *split homogeneous* if $K[G]$ is simple and split. Hence, 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.

COROLLARY 7.2. *Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian* ANC *group and let $A \triangleleft G$ be irreducible and cyclic of index two. Then G is split homogeneous.*

Proof. We have $|V : Z| = 2$ and thus $K[G] \cong \mathrm{M}_2(Z)$, where $Z = K[A]^G$, by Lemma 7.1. □

The field Z in Lemma 7.1 can be easily determined explicitly as follows.

LEMMA 7.3. *Let $G \leqslant \mathrm{GL}(V)$ be a non-abelian* ANC *group. Let $A \triangleleft G$ be homogeneous and cyclic of index two, say $A_2 = \langle x\rangle$ and $A_{2'} = \langle y\rangle$. Then $\mathrm{Z}(K[G]) = K[x + \delta(G)x^{-1}, y]$.*

Proof. Write $Z = \mathrm{Z}(K[G])$ and $\delta = \delta(G)$. Since $G/A \cong \mathrm{C}_2$ acts via $x \mapsto \delta x^{-1}$ on A_2, we see that $K[x + \delta x^{-1}, y] \subseteq Z$. As $Z = K[A]^G$, we have $|K[A] : Z| = 2$. Since x is a root of $T^2 - (x + \delta x^{-1})T + \delta$ in $(K[x + \delta x^{-1}, y])[T]$, we obtain $|K[A] : K[x + \delta x^{-1}, y]| \leqslant 2$. □

For $n = 2^j m$ with m odd, define $\mathbf{E}_n^+ = \mathbf{Q}(\zeta_{2^j} + \zeta_{2^j}^{-1}, \zeta_m)$.

COROLLARY 7.4. *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 two.*

(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 $\mathbf{E}_n^+ K$.*

8. *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 4.5, it suffices to test if some maximal subgroup of G is a block stabiliser. The maximal subgroups of G are easily described (§ 8.1). In § 8.2, 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 §§ 8.4–8.5.

Throughout this section, $G \leqslant \mathrm{GL}(V)$ is an irreducible non-abelian ANC group and $A \lhd G$ is cyclic with $|G:A| = 2$. We assume that A is irreducible; otherwise, we obtain a system of imprimitivity for G via Lemma 4.3. In practice, A can be found as in [**15**, § 6.1].

8.1. *Maximal subgroups of G*

We have $G = \langle a, g\rangle$, where $A = \langle a\rangle$ and $g^2 = \vartheta(G) \cdot 1_V$. In practice, such elements can be found as in [**15**, § 6.1]. Write $a = a_2 \cdot a_{2'}$ according to $A = A_2 \times A_{2'}$. The two subgroups of index two 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. We see that if $K/\mathbf{Q}$ is finitely generated, then it is feasible to loop over all maximal subgroups of G; recall from Section 5 that $|A|$, and hence also $|G| = 2|A|$, is 'small' in terms of $|V:K|$. Also note that if $H < G$ is any maximal subgroup of G, then H is itself an ANC group.

LEMMA 8.1. *Let $H < G$ be a maximal subgroup with $A \neq H$, say $|G:H| = p$. Then $|H:A^p| = 2$. Moreover, $A^p = \mathrm{C}_H(A^p)$ unless $G_2 \cong \mathrm{Q}_8$ and $p = 2$; in the latter case, $H \cong A$ is irreducible.*

Proof. If p is odd or $G_2 \ncong \mathrm{Q}_8$, then the claim follows from the above description of the maximal subgroups of G; note that H is then non-abelian. Let $G_2 \cong \mathrm{Q}_8$ and $p = 2$. Since A_2 is irreducible but non-central, $X^2 + 1$ is irreducible over $E = K[G_{2'}]$, so that $|V:E| = 2$. It follows that $H_2 \cong \mathrm{C}_4$ is irreducible over E, whence H is irreducible over K. □

COROLLARY 8.2. *Every maximal subgroup of G is homogeneous.*

Proof. If $A \neq H < G$ is maximal, then $K[H]$ is simple by Lemmas 7.1 and 8.1. □

8.2. *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 8.1, if $G_2 \cong \mathrm{Q}_8$, then we also assume that p is odd.

LEMMA 8.3. *H is a block stabiliser for G if and only $|K[A]:K[A^p]| = p$ 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 8.2, it acts faithfully on U. Lemma 7.1 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 4.2 that H is a block stabiliser for G if and only if $|G:H| = |V:K|/|U:K|$. This is equivalent to $p = 2^{-\lambda}|K[A]:K[A^p]|$; note that $|K[A]:K[A^p]| \leqslant p$. □

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 two in G (see § 8.1), we may ignore H_2 by the following.

LEMMA 8.4. *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 8.3 is the same for H_1 and H_2. The result follows since if H_1 is not split homogeneous, then $\vartheta(H_1) = \vartheta(G) = \vartheta(H_2) = -1$, whence H_2 is not split homogeneous by Corollary 7.4(ii). □

We can therefore test primitivity of G by using Lemma 8.3 and Corollary 7.4 to 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 $\alpha^2+\beta^2=-1$ in Corollary 7.4(ii).

8.3. *Constructing a block*

Setup. Let $G=\langle a,g\rangle$ be as in § 8.1. Suppose that $H<G$ is a maximal subgroup of index p which is a block stabiliser for G. By Lemma 8.4, 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 8.2), this is equivalent to constructing an irreducible $K[H]$-submodule of V (Lemmas 4.1 and 4.2). What follows is essentially an application of the general method for irreducibility testing of ANC groups described in [**15**, Section 6].

Dihedral and semidihedral cases. First, let $\vartheta(G)=1$ (and so $\vartheta(H)=1$). Since g is not scalar but $g^2=1$, there exists $0\neq x\in V$ with $xg=\pm x$. It follows that $x\cdot K[H]=x\cdot K[b]$ 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 $F=K[b]$, $Z=\mathrm{Z}(K[H])$, $F'=\mathbf{E}_{n/p}K$, and $Z'=\mathbf{E}^+_{n/p}K$. Lemma 7.3 gives us an explicit isomorphism between the towers $F/Z/K$ and $F'/Z'/K$. Since H is split homogeneous (Lemma 8.3), -1 is a sum of two squares in Z (Corollary 7.4(ii)). Now $c=b^{n/(4p)}$ is not central in H and $|F:Z|=2$, whence $F=Z[c]$ and $F'=Z'(\sqrt{-1})$. Hence, the pairs $(\alpha,\beta)\in Z\times Z$ with $\alpha^2+\beta^2=-1$ correspond one to one to the elements $f\in F$ with $\mathrm{Norm}_{F/Z}(f)=-1$.

It is easily verified that every $K[H]$-submodule of V of F-dimension two satisfies the assumptions on V in [**15**, Lemma 6.1]; note that H is reducible since it is a block stabiliser. It follows that finding an irreducible $K[H]$-submodule of V is equivalent (up to solving systems of linear equations) to finding $f\in F$ with $\mathrm{Norm}_{F/Z}(f)=-1$ as follows. Given $f\in F$ with $\mathrm{Norm}_{F/Z}(f)=-1$, the map $g-f$ is singular, and non-trivial elements in its kernel generate irreducible $K[H]$-submodules. Conversely, if $x\cdot K[H]$ is an irreducible $K[H]$-submodule of V, then $xg=xf$ for a unique $f\in F$ and then $\mathrm{Norm}_{F/Z}(f)=-1$ holds.

As we remarked in Section 4, given any system of imprimitivity for G, we may construct one of prime size. We conclude that for an irreducible imprimitive ANC group $G\leqslant\mathrm{GL}(V)$ with $G_2\cong \mathrm{Q}_{2^j}$ such that a cyclic subgroup of index two in G is irreducible, finding a system of imprimitivity is equivalent to solving $\alpha^2+\beta^2=-1$ in one of the fields Z corresponding to a maximal subgroup $H<G$ which is a block stabiliser. Note that there may in general be different possible choices for H and hence for Z.

8.4. *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; details will be given in Proposition 8.8 below. For background on number fields and their completions, we refer to [**3**].

PROPOSITION 8.5 [**5**, Theorem 1]. *Let F be a number field. Then -1 is a sum of two squares in F if and only if F is totally imaginary and $|F_{\mathfrak{p}}:\mathbf{Q}_2|$ is even for all primes $\mathfrak{p}$ above 2 in F.*

The following is related to [**5**, Theorem 3]. For $(r,n)=1$, denote the order of $r+n\mathbf{Z}$ in $(\mathbf{Z}/n\mathbf{Z})^\times$ by $\mathrm{ord}(r \bmod n)$; this includes $\mathrm{ord}(r \bmod 1)=1$.

LEMMA 8.6. *Let F be a number field and p be an odd rational prime. Then -1 is a sum of two squares in $\mathbf{E}_{p^a}F$ for some $a \geqslant 1$ if and only if it is a sum of two squares in $\mathbf{E}_pF$.*

Proof. Let $\mathcal{F}$ be a 2-adic completion of F. We may assume that the ζ_{p^i} lie in some common extension of $\mathcal{F}$. By [**13**, Satz II.7.12(i)], we have $|\mathcal{F}(\zeta_{p^i}) : \mathcal{F}| = \mathrm{ord}(2^f \bmod p^i)$, where f is the residue class degree of $\mathcal{F}$. Now $(\mathbf{Z}/p^a\mathbf{Z})^\times = K \times C$, where $K \cong \mathbf{Z}/p^{a-1}\mathbf{Z}$ is the kernel of the natural map $(\mathbf{Z}/p^a\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$ and $C \cong \mathrm{C}_{p-1}$. We see that $\mathrm{ord}(2^f \bmod p^a) \equiv \mathrm{ord}(2^f \bmod p) \bmod 2$. Since $F(\zeta_{p^i})$ is totally imaginary for any $i \geqslant 1$, the claim now follows from Proposition 8.5. □

The following is a simple application of Proposition 8.5.

COROLLARY 8.7 (See [**15**, § 8.1]). *Suppose that K is a number field. Let $m \geqslant 1$ be odd. Then -1 is a sum of two squares in $\mathbf{E}_mK$ if and only if:*

(i) *K is totally imaginary or $m > 1$; and*
(ii) *$\mathrm{ord}(2 \bmod m) \cdot |K_\mathfrak{p} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p}$ above 2 in K.*

PROPOSITION 8.8. *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 8.3, $|K[A] : K[A^p]| = p$ 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 and the result follows. Let $\vartheta(G) = -1$. Since G is split homogeneous by irreducibility of A (Corollary 7.2), we know that -1 is a sum of two squares in $\mathbf{E}_n^+K$. Write $n = p^am$ for $p \nmid m$. As noted in Remark 5.2, $a \geqslant 2$. Let p be odd. By applying Lemma 8.6 with $F = \mathbf{E}_m^+K$, we see that -1 is a sum of two squares in $\mathbf{E}_{n/p}^+K$. Hence, H is split homogeneous and thus a block stabiliser for G. Let $p = 2$. Then $a \geqslant 4$ by assumption. Now $\mathbf{E}_{2^a}^+$ is totally real, while $\mathbf{E}_n^+K$ is totally imaginary. Hence, $\mathbf{E}_mK$ is totally imaginary. As $a \geqslant 4$, we have $\sqrt{2} \in \mathbf{E}_{n/2}^+$ and, since $|\mathbf{Q}_2(\sqrt{2}) : \mathbf{Q}_2| = 2$, we conclude from Proposition 8.5 that -1 is a sum of two squares in $\mathbf{E}_{n/2}^+K$. □

Recall that the case $G_2 \cong \mathrm{Q}_8$ and $p = 2$ is ruled out by Lemma 8.1. Thus, for a maximal subgroup $H < G$ of index p, Proposition 8.8 covers all cases but one: $G_2 \cong \mathrm{Q}_{16}$ and $p = 2$. In this case, $\mathrm{Z}(K[H]) \cong \mathbf{E}_{4m}^+K = \mathbf{E}_mK$ (where $|G| = 16m$), and we may apply Corollary 8.7 to decide if H is split homogeneous.

8.5. *Other fields*

Function fields. Exactly as in [**15**, § 8.3], we may apply the results of § 8.4 to rational function fields over number fields using the following two facts. Let E be a number field and $K = E(\mathbf{X})$, where $\mathbf{X} = (X_1, \ldots, X_t)$ is algebraically independent. Then -1 is a sum of two squares in K if and only if it is a sum of two squares in E. If $F \supseteq E$ is another number field which is contained in some extension of K, then $\mathbf{X}$ is algebraically independent over F. Consequently, Proposition 8.8 and the comments following it remain valid if K is a rational function field over a number field.

Fields containing $\sqrt{-1}$. Suppose that K is a field of characteristic zero with $\sqrt{-1} \in K$ and such that (F1) is satisfied. (Of course, (F2) is then also satisfied.) We now briefly discuss how we may test primitivity of finite nilpotent linear groups over K under these assumptions. We note that polynomial factorisation is used to find the homogeneous decomposition for an abelian group in [**15**, Algorithm 5.2].

Given an irreducible finite nilpotent group $G \leqslant \mathrm{GL}(V)$, we can use NoncyclicAbelian [15, Algorithm 4.3] and either (i) construct a non-cyclic abelian normal subgroup and hence a system of imprimitivity for G, or (ii) prove that G is an ANC group. It is shown in [15, § 8.1] that 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 Section 5.

9. *An algorithm for primitivity testing of finite nilpotent linear groups*

We may now summarise the main algorithm for primitivity testing. For the reduction to ANC groups (see Section 2), we let NoncyclicAbelian denote a function, which, given a finite nilpotent group $G \leqslant \mathrm{GL}(V)$, returns either a non-cyclic abelian normal subgroup of G or fail if G is an ANC group; see [15, Algorithm 4.3] for a description of such a function. We also rely on the function HomogeneousDecompositionAbelian, which, given a finite abelian $A \leqslant \mathrm{GL}(V)$, returns the homogeneous decomposition for A; see [15, Algorithm 5.2]. Finally, NonzeroElement returns a non-zero vector of a non-zero vector space.

The following is an algorithm for primitivity testing of finite nilpotent linear groups over any field K of characteristic zero such that (F1)–(F2) are satisfied. For the important case of number fields, we illustrate how the techniques described in § 8.4 can be applied (see lines 11–13). To simplify the pseudo-code, for an imprimitive group G we return a block for G instead of a system of imprimitivity. Clearly, the system of imprimitivity containing a given block can be obtained using the orbit-stabiliser algorithm [7, § 4.1].

Algorithm 9.1. 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 $p^2 \| |G|$ 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 two 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 § 8.1
9: **if** A is reducible **then return** false, NonzeroElement(V) $\cdot K[A]$
10: $S \leftarrow \{p{:}p \text{ is an odd prime with } p^2 \| |G| \text{ and } |K[A] : K[A^p]| = p\}$
11: **if** K is a number field **then**
12: $q \leftarrow \vartheta(G) = 1$ **or** $|G_2| \geqslant 32$ **or**
$(G_2 \cong \mathrm{Q}_{16}$ **and** $\mathrm{ord}(2 \bmod |G_{2'}|) \cdot |K_{\mathfrak{p}} : \mathbf{Q}_2|$ is even for all primes $\mathfrak{p}|2$ of $K)$
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** $S \leftarrow \{p \in S : -1$ is a sum of two squares in $\mathbf{E}^+_{|A|/p} K\}$
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

Remark 9.2. As explained in § 8.3, solving the norm equation $b \cdot b^g = -1_V$ in line 18 is equivalent to solving $\alpha^2 + \beta^2 = -1$ in $K[A^p]^G \cong_K \mathbf{E}^+_{n/p} K$, where $n = |A|$; we can do this since we assumed that condition (F2) holds for K. In practice, as in the case of irreducibility testing [15, Section 8], we generally use a norm equation solver for this step. We note that norm equations for extensions F/F' of number fields can be solved algorithmically [6, 17]. However,

the known algorithms for this purpose rely on the computation of the class group of F, so that F has to be 'small' for such computations to be feasible.

REMARK 9.3. Algorithm 9.1 can be simplified if we only wish to decide primitivity of G without ever constructing a block. As we have seen in Section 8, in this case, we do not have to actually solve any of the equations $\alpha^2 + \beta^2 = -1$ in line 18. Therefore, condition (F2) on K from Section 1 can be relaxed to the following: for any $n \geqslant 1$, we may decide if -1 is a sum of two squares in $\mathbf{E}_n^+ K$.

REMARK 9.4. Because of randomisations employed in [**15**, Algorithm 4.3], 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. [**18**, Lemma 15.2].

10. *The implementation and examples*

10.1. *Notes on the implementation*

The Magma package *finn* includes an implementation of the above algorithm for primitivity testing of irreducible finite nilpotent linear groups; *finn* can handle linear groups defined over number fields and rational function fields over number fields.

Since Algorithm 9.1 shares common ingredients with the method for irreducibility testing in [**15**], a function which simultaneously tests irreducibility and primitivity of a finite nilpotent linear group is provided in *finn*. This function will thus determine if the input group is (a) reducible, (b) imprimitive but irreducible, or (c) primitive. In the cases (a) and (b), it will then proceed to construct a submodule (case (a)) or a system of imprimitivity (case (b)), unless the user requested to merely decide to which of the three classes (a)–(c) the input group belongs.

10.2. *Run-times over* $\mathbf{Q}$

We will now illustrate the practicality of Algorithm 9.1 by providing sample run-times. These were all obtained using the 64-bit version of Magma V2.16-12 on an Intel Xeon E5440. The examples below are available from the web page of *finn*.

Table 1 shows run-times for primitivity testing over the rationals. For each group, we provide information on the group ('group'), its degree ('deg'), and the number of defining generators

TABLE 1. *Run-times for linear groups over the rationals.*

Group	Deg	Gens	Num	Den	Prim?	Size	Total	Decide
$G_1 \cong 5^{1+2}$	20	4	7	3	No	5	0.01	0.01
$G_2 \cong W(2,7)$	42	7	34,387	6204	No	7	0.29	0.01
G_3 (order $2^5 5^3$, class 3)	80	4	4.94×10^6	1.91×10^5	No	2	0.70	0.24
$G_4 \cong W(5,2) \otimes W(2,3)$	96	11	1	1	No	2	0.36	0.07
$G_5 \cong \mathrm{Q}_8 \times \mathrm{C}_{11}$	20	5	7.1×10^7	3.34×10^6	Yes	–	0.02	0.02
$G_6 \cong \mathrm{Q}_{16} \times \mathrm{C}_7$	24	5	3.2×10^{11}	3.68×10^{10}	Yes	–	0.04	0.04
$G_7 \cong \mathrm{D}_{16} \times \mathrm{C}_{11}$	40	5	1.26×10^{11}	2.21×10^9	No	2	0.12	0.09
$G_8 \cong \mathrm{Q}_{16} \times \mathrm{C}_{25}$	160	5	5.6×10^7	4.76×10^6	No	5	0.82	0.48

('gen'). We also give approximate values for the largest absolute value of any numerator ('num') or denominator ('den') among the entries of the defining generators. We indicate whether the group was found to be primitive ('prim?') and, 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 (see § 10.1) 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; see [**15**, Section 9] for run-times of irreducibility testing.

The group $W(i,p)$ is $\mathrm{C}_p \wr \cdots \wr \mathrm{C}_p$ (i factors) faithfully represented as an irreducible maximal p-subgroup of $\mathrm{GL}_d(\mathbf{Q})$, where $d=(p-1)p^{i-1}$; see [**11**, § 4.5]. Apart from G_4 (which is taken from [**15**]), the generating sets for the groups in Table 1 were obtained from copies of the 'natural' ones using two steps of randomisation. First, the product replacement algorithm [**2**] was used to obtain new generating sets; the main reason for including this step is that the natural generating sets often yield extremal run-times (in either direction) for the construction of a non-cyclic abelian normal subgroup via NoncyclicAbelian. Second, the generators were replaced by conjugates under partially randomised block matrices; this was meant to increase the sizes of matrix entries and to hide any obvious imprimitivity evident from the shapes of the matrices.

The practical limitations of our implementation are the same as for irreducibility testing. As remarked in [**15**], explicit solutions of $\alpha^2+\beta^2=-1$ in cyclotomic fields are known from [**9**, Example 38.13d] whenever they exist; these solutions are used in *finn*. We did not include any examples for which a norm equation solver was used to solve $\alpha^2+\beta^2=-1$; as we already indicated in Remark 9.2, such computations are only feasible in small cases.

10.3. *Run-times over other fields*

In Table 2, we provide run-times for groups over proper extensions of the rationals. All of these groups are generated by matrices with moderately sized entries so that computations are not rendered impractical by coefficient explosions. The evident increase in run-times compared to Table 1 is mostly a consequence of the fact that the underlying linear algebra in Magma is highly optimised over the rationals.

Table 2. *Run-times for linear groups over fields other than* $\mathbf{Q}$.

Group	Field	Degree	Gens	Prim?	Size	Total	Decide
$G_9 \cong \mathrm{D}_{16} \wr \mathrm{C}_4$	$\mathbf{Q}(\sqrt{2})$	8	8	No	2	0.08	0.01
$G_{10} \cong \mathrm{C}_{49} \cdot \mathrm{C}_{49}$	$\mathbf{Q}(\zeta_{49})$	7	5	No	7	1.00	0.16
G_{11} (order 3^{40}, class 27)	$\mathbf{Q}(\sqrt{-3})$	27	9	No	3	1.47	0.12
G_{12} (order $2^3 5^5$, class 4)	$\mathbf{Q}(X)$	40	5	No	5	4.74	0.03
$G_{13} \cong \mathrm{SD}_{16} \times \mathrm{C}_5$	$\mathbf{Q}(\sqrt{-2})$	8	5	Yes	–	0.04	0.04
$G_{14} \cong \mathrm{SD}_{32} \times \mathrm{C}_5$	$\mathbf{Q}(\sqrt[4]{2})$	16	5	No	2	0.43	0.37

Acknowledgement. The author would like to thank Dane Flannery and Alla Detinko for comments and discussions on earlier versions of this paper.

References

1. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) no. 3–4, 235–265.

2. 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 (1995) no. 13, 4931–4948.
3. H. Cohen, *Number theory. Tools and Diophantine equations, vol. 1*, Graduate Texts in Mathematics 239 (Springer, New York, 2007).
4. A. S. Detinko and D. L. Flannery, 'Computing in nilpotent matrix groups', *LMS J. Comput. Math.* 9 (2006) 104–134 (electronic).
5. 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 (1971) 310–315.
6. C. Fieker, 'Über relative Normgleichungen in algebraischen Zahlkörpern'. PhD Thesis, Technische Universität Berlin, 1997.
7. D. F. Holt, B. Eick and E. A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications (Chapman & Hall/CRC, Boca Raton, FL, 2005).
8. D. F. Holt, C. R. Leedham-Green, E. A. O'Brien and S. Rees, 'Testing matrix groups for primitivity', *J. Algebra* 184 (1996) no. 3, 795–817.
9. B. Huppert, *Character theory of finite groups*, De Gruyter Expositions in Mathematics 25 (Walter de Gruyter, Berlin, 1998).
10. T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics 67 (American Mathematical Society, Providence, RI, 2005).
11. C. R. Leedham-Green and S. McKay, *The structure of groups of prime power order*, London Mathematical Society Monographs. New Series 27 (Oxford University Press, Oxford, 2002) Oxford Science Publications.
12. F. Lorenz, *Algebra, vol. II*, Universitext (Springer, New York, 2008); Fields with structure, algebras and advanced topics. Translated from the German by Silvio Levy.
13. J. Neukirch, *Algebraische Zahlentheorie* (Springer, Berlin, 1992).
14. P. Roquette, 'Realisierung von Darstellungen endlicher nilpotenter Gruppen', *Arch. Math. (Basel)* 9 (1958) 241–250.
15. T. Rossmann, 'Irreducibility testing of finite nilpotent linear groups', *J. Algebra* 324 (2010) no. 5, 1114–1124.
16. T. Rossmann, 'finn — computing with finite nilpotent linear groups, 0.5' 2010, see http://www.maths.nuigalway.ie/∼tobias/finn.
17. D. Simon, 'Solving norm equations in relative number fields using S-units', *Math. Comp.* 71 (2002) no. 239, 1287–1305 (electronic).
18. D. A. Suprunenko, *Matrix groups* (American Mathematical Society, Providence, RI, 1976); Translated from the Russian, translation edited by K. A. Hirsch, Translations of Mathematical Monographs 45.
19. B. A. F. Wehrfritz, *Infinite linear groups. An account of the group-theoretic properties of infinite groups of matrices*, Ergebnisse der Matematik und ihrer Grenzgebiete 76 (Springer, New York, 1973).

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

tobias.rossmann@googlemail.com