

Irreducibility testing of finite nilpotent matrix groups over number fields

Tobias Rossmann



Edinburgh, 30 July 2009



This work is supported by the Research Frontiers Programme of Science Foundation Ireland

Goals

Project (supervised by D. Flannery and A. Detinko)

Investigate the structure of nilpotent matrix groups over fields of characteristic zero and develop algorithms for these groups.

This talk

I describe a method for constructive irreducibility testing of finite nilpotent matrix groups over number fields.

A summary of my method (1/2)

Input

A finite nilpotent matrix group G over a number field K or a function field $K(X_1, \dots, X_r)$ where K is a number field.

For simplicity, I only treat the case of a number field in this talk: Henceforth, let K be a fixed number field.

Output

true or false depending on whether G is irreducible or not.

Additionally, in the reducible case, a proper submodule can be returned “in principle”.

A summary of my method (2/2)

Features

- Detailed structural information about the group is obtained.
- The method heavily relies on group-theoretic computations.
- Over the rationals, primitivity can be tested at the same time. (Over number fields, this is work in progress.)
- Variations can be used to test absolute irreducibility or to decompose into direct sums.

Implementation

An implementation in Magma is under development. The core functionality discussed in this talk is already operational.

Previous work (1/2)

Irreducibility testing

- Parker (1998): “An integral meataxe”.
- Plesken, Souvignier (1996): Compute centraliser algebra and homogeneous decomposition of a finite rational matrix group.
- Nebe, Steel (2009): Compute the Schur indices of certain simple \mathbf{Q} -algebras.
- Souvignier (2009): Find zero-divisors.

Previous work (2/2)

Algorithms for nilpotent matrix groups

- Detinko, Flannery (2007): Nilpotency and finiteness testing of finitely generated matrix groups over a range of infinite fields.
- Detinko, Flannery (2006): As a by-product of nilpotency testing, irreducibility and primitivity of nilpotent matrix groups over finite fields can be tested simultaneously.

The strategy (1/3)

The basic approach, taken from (Detinko & Flannery, 2006), is to use the following consequence of Clifford's theorem.

Lemma

Let $G \leq \text{GL}(V)$ be completely reducible and $N \triangleleft G$. Let

$$V = U_1 \oplus \cdots \oplus U_r$$

be the decomposition into N -homogeneous components. Then G is irreducible if and only if

- *G acts transitively on $\{U_1, \dots, U_r\}$, and*
- *$\text{Stab}_G(U_1)$ acts irreducibly on U_1 .*

The strategy (2/3)

Abelian normal subgroups

- We will only apply this lemma to **abelian** normal subgroups.
- This is feasible since (finite) nilpotent groups have plenty of these.
- If $A \triangleleft G$ is abelian but non-cyclic, then A is inhomogeneous.

Reduction

Suppose that $A \triangleleft G$ is abelian but non-cyclic. Then we can either construct a proper submodule for G or we continue irreducibility testing in strictly smaller dimension.

We call this method **reduction**. It can be applied whenever A is inhomogeneous.

The strategy (3/3)

The method (sketch)

Let $G \leq \text{GL}(V)$ be finite and nilpotent.

- Either ① find a non-cyclic abelian normal subgroup or ② prove that no such subgroup exists.
- In case ①, reduce.
- In case ②, decide irreducibility directly.

Problems

- 1 Perform the homogeneous splitting for abelian groups.
- 2 Understand the finite nilpotent groups all of whose abelian normal subgroups are cyclic.
- 3 Construct abelian normal subgroups.

Problem 1: Homogeneous splitting

Lemma (Dixon 1985, Eberly 1991)

If G is completely reducible, finitely generated, and abelian, then $K[G] = K[x]$ for “almost all” $x \in K[G]$.

Remarks

- If we know $|K[G] : K|$, then we can find x with $K[G] = K[x]$.
- We then construct the primary decomposition for x .
- We can then further decompose into irreducible submodules.
- For large degrees, we use an “intrinsic method”.
- Homogeneous finite abelian groups are “small”.

Problem 2.1: ANC groups

Problem 2: Understand the finite nilpotent groups all of whose abelian normal subgroups are cyclic.

Definition

An **ANC group** is a finite nilpotent group all of whose **a**belian **n**ormal subgroups are **c**yclic.

Theorem (Roquette 1958; earlier sources?)

Let G be a finite nilpotent group. Then G is an ANC group iff

- G_2 is cyclic or isomorphic to Q_8 or to one of D_{2^n} , SD_{2^n} or Q_{2^n} ($n \geq 4$), and
- G_{2^i} is cyclic.

Problem 3: Finding abelian normal subgroups (1/2)

Given $G \leq \text{GL}(V)$, we construct abelian normal subgroups as follows.

- 1 Find some initial $A \triangleleft G$, e.g. $A = \langle z \rangle^G$ for $z \in Z_2(G) \setminus Z(G)$.
- 2 If A is non-cyclic, then reduce.
- 3 If A is cyclic but not maximal, then enlarge A and go to 2
To enlarge A , we may e.g. set $A \leftarrow \langle A, g \rangle$ where $1 \neq gA \in Z(G/A) \cap C_G(A)/A$.

After execution of this loop, we have either reduced or we have obtained a maximal abelian $A \triangleleft G$ which is cyclic.

Problem 3: Finding abelian normal subgroups (2/2)

Suppose that $A \triangleleft G$ is cyclic and maximal abelian. Then $G/A \leq \text{Aut}(A)$ is abelian. Hence, $[G, G] \leq A$ is cyclic. Let $H = C_G([G, G])$.

Lemma (corollary to Berger, Kovács, Newman (1980))

The following are equivalent:

- G is an ANC group.
- H_2' is cyclic and H_2 is either cyclic or $H_2 \cong Q_8$.

Lemma

If $H_q \not\cong Q_8$ is non-abelian, then there exists a non-cyclic abelian $B \triangleleft G$ such that $Z(H_q) \leq B < H_q$ and $B/Z(H_q)$ is cyclic.

Problem 2.2: Irreducibility testing of ANC groups (1/2)

Let $G \leq \text{GL}(V)$ be a non-abelian ANC group.

- G contains a cyclic subgroup of index 2, and we may assume that it is homogeneous.
- This already forces G to be homogeneous as well.
- Let $Z = Z(K[G])$.

Lemma

- Let G_2 be (semi)dihedral. Then G is irreducible iff $|V : Z| = 2$.
- Let G_2 be generalised quaternion. If $-1 = a^2 + b^2$ has a solution in Z , then G is irreducible iff $|V : Z| = 2$.
Otherwise, G is irreducible iff $|V : Z| = 4$.

Problem 2.2: Irreducibility testing of ANC groups (2/2)

Theorem (Hasse; Fein, Gordon, Smith; Connell; Fujisaki; Peters)

Let F be a number field with $\sqrt{-1} \notin F$. Then $-1 = a^2 + b^2$ has a solution in F if and only if

- *F is totally imaginary, and*
- *$|F_\nu : \mathbf{Q}_2|$ is even for all places ν above 2.*

Remarks

- The conditions in the lemma can be checked using algorithms implemented in Magma.
- We may therefore decide irreducibility of ANC groups.
- For special fields, e.g. the field Z when $K = \mathbf{Q}$, more explicit descriptions are possible.

Problem 2.3: Submodules for ANC groups (1/2)

Remark

For reducible ANC groups of (semi)dihedral type, submodules can be readily found. We therefore only need to consider the generalised quaternion type.

ANC groups of generalised quaternion type

- Deciding irreducibility amounts to **deciding** whether $-1 = a^2 + b^2$ has a solution in Z . (Easy!)
- Finding submodules amounts to **solving** $-1 = a^2 + b^2$ in Z .

Question: How difficult is this?

Problem 2.3: Submodules for ANC groups (2/2)

- In the current implementation, if possible, theoretically known solutions for $K = \mathbf{Q}$ are used; otherwise, a norm equation solver is used unless $|Z : \mathbf{Q}|$ exceeds a given threshold.
- For $K = \mathbf{Q}$, the open case (to me) of smallest degree occurs for $Z = \mathbf{Q}(\sqrt{2}, \zeta_{23})$ which arises from $Q_{16} \times C_{23}$ acting reducibly in dimension 176 over \mathbf{Q} .

The implementation (1/2)

Facts

- Implemented for base fields $K(X_1, \dots, X_r)$ ($r \geq 0$)
- Focus has been mostly on the rational case.

Sample runtimes (on a 2.4Ghz dual core PC with 3GB RAM)

- $(Q_{16} \times C_3) \otimes \text{Syl}_3(\text{GL}_6) \leq \text{GL}_{48}$ (8 gens): reducible $\approx 0.58\text{s}$
- $\text{Syl}_2(\text{GL}_{16}) \otimes \text{Syl}_3(\text{GL}_6) \leq \text{GL}_{96}$ (11 gens): irreducible $\approx 2.38\text{s}$
- $\text{Syl}_2(\text{GL}_{16}) \otimes \text{Syl}_3(S_9) \leq \text{GL}_{144}$ (11 gens): reducible $\approx 4.37\text{s}$
- $D_{32} \times C_{11} \leq \text{GL}_{80}$ (5 gens): irreducible $\approx 2.59\text{s}$
- $Q_{32} \times C_{11} \leq \text{GL}_{160}$ (5 gens): reducible $\approx 6.45\text{s}$

The implementation (2/2)

More sample runtimes

- $\text{Syl}_2(\text{GL}_{128})$ (8 gens, absolutely irreducible):
 - over \mathbf{Q} : $\approx 2.63\text{s}$
 - over several quadratic fields: $\approx 40\text{s}$
 - over $\mathbf{Q}(X)$: $\approx 17.25\text{s}$
- $\text{Syl}_3(\text{GL}_{54})$ (4 gens):
 - irreducible over \mathbf{Q} : $\approx 0.29\text{s}$
 - reducible over $\mathbf{Q}(\zeta_9)$: $\approx 3.45\text{s}$
 - irreducible over $\mathbf{Q}(X)$: $\approx 1.73\text{s}$
- $\text{Syl}_{13}(\text{GL}_{2028})$ (3 gens): irreducible $\approx 30\text{min}$

Primitivity testing (1/2)

Remarks

- The reduction technique always produces a system of imprimitivity.
- Hence, we only need to decide primitivity for irreducible ANC groups.

Definition

Define $\varkappa_K : \mathbf{N} \rightarrow \mathbf{N}$ by

$$\begin{aligned}\varkappa_K(n) &= \text{conductor of } K \cap \mathbf{Q}(\zeta_n) \\ &= \text{least } m \text{ such that } K \cap \mathbf{Q}(\zeta_n) \subseteq \mathbf{Q}(\zeta_m).\end{aligned}$$

Primitivity testing (2/2)

Theorem

Let $G \leq \text{GL}(V)$ be an irreducible ANC group over K . Let n be the order of a cyclic subgroup of minimal index of G , and let $m = |\text{Z}(G)|$. Then G is primitive if and only if the following two conditions are satisfied:

- G_2 is primitive as a linear group over $K[\text{Z}(G)]$.
- For all primes p , if $p \cdot \kappa_K(n) \mid n$, then $p^2 \nmid m$.

Remarks

- The primitive Sylow subgroups of $\text{GL}_d(F)$ have been classified (Volvacev 1963, Leedham-Green & Plesken 1986, Konyukh 1987).
- Primitivity over the rationals can then be readily tested.