London Mathematical Society ISSN 1461–1570

FINDING INTEGRAL LINEAR DEPENDENCIES OF ALGEBRAIC NUMBERS AND ALGEBRAIC LIE ALGEBRAS

CLAUS FIEKER AND WILLEM A. DE GRAAF

Abstract

We give an algorithm for finding the module of linear dependencies of the roots of a monic integral polynomial. Using this, we describe an algorithm for constructing the algebraic hull of a given matrix Lie algebra in characteristic zero.

1. *Introduction*

One of the major tools in the theory of algebraic groups is their correspondence with Lie algebras. Many problems regarding algebraic groups can be reformulated in terms of the corresponding Lie algebras, for which they are generally easier to solve. There is considerable interest in studying algebraic groups computationally (cf., for example, [**6**, **8**, **11**]). Also, for this it would be of great interest to exploit the connection with Lie algebras. In this paper we treat a question that arises in this context, namely the problem of deciding whether a given Lie algebra corresponds to an algebraic group. In particular, a positive solution to this problem enables us to decide which subalgebras of a Lie algebra of an algebraic group correspond to algebraic subgroups. To tackle this problem we restrict to base fields of characteristic 0, because for that case there is a well-developed theory of the connection between algebraic groups and Lie algebras (see [**5**]). In particular, a connected algebraic (matrix-)group is completely determined by its Lie algebra.

Results of Chevalley yield a construction of the smallest algebraic Lie algebra containing a given Lie algebra (this is called the *algebraic hull*). However, the computationally hardest step is to find all the integral linear dependencies of the roots of a polynomial. This can be done by constructing the splitting field of the given polynomial. But that approach is limited to polynomials which have splitting fields of only moderate sizes. Instead we describe a method that works with approximations to the roots. Combining complex and p-adic approximations to the roots, and the technique of lattice reduction (LLL), we obtain an algorithm for computing the $\mathbb{Z}$-module of integral relations among a given set of algebraic integers. In the literature, several somewhat similar methods for solving this problem are known (cf., for example, [**7**, §2.7.2] and [**13**]). These methods focus on finding one linear dependency, while our algorithms find (a basis of) the whole module of linear dependencies.

This paper is arranged as follows. In Section 2 we describe methods for obtaining a basis of the module of linear dependencies of a set of algebraic numbers. Then in Section 3 algorithms are given for constructing the algebraic hull of a given Lie algebra. These make use of the algorithms of the previous section. The next

Received 14 November 2006, revised 26 April 2007; *published* 16 July 2007.
2000 Mathematics Subject Classification 11Y50,17B45,20G30

section is devoted to showing how the knowledge of the Galois group can in some instances be of help with constructing the algebraic hull. This is used in Section 5, where we give the algebraic hull of the Lie algebra spanned by a semisimple 4×4-matrix. Finally, in Section 6 we report on some practical experiences with an implementation of the algorithms in the computer algebra system MAGMA [**3**, **4**].

2. *Finding integral dependencies among roots*

Let $f \in \mathbb{Q}[x]$ be a square-free polynomial with roots $\alpha_1, \ldots, \alpha_n$ in some field $\Gamma \supset \mathbb{Q}$. The field Γ does not need to be finite or even algebraic over $\mathbb{Q}$. In what follows, Γ will be the field $\mathbb{C}$ of complex numbers or a suitably chosen unramified p-adic field. The roots α_i $(1 \leqslant i \leqslant n)$ are given as rational numbers $\tilde{\alpha}_i$ that approximate the roots good enough so that $\tilde{\alpha}_i$ can be lifted to arbitrary precision using classical Newton-iteration. Elements of $\Gamma \supset K := \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ can be represented as polynomials $g \in \mathbb{Q}[X_1, \ldots, X_n]$ coming from a representation $K \cong \mathbb{Q}[X_1, \ldots, X_n]/I$ for some zero-dimensional ideal $I \subset \mathbb{Q}[X_1, \ldots, X_n]$. Although constructive methods for the construction of I or K are known (see, for example, [**18**]), in general they are limited to small examples: the splitting field can have degree as large as $n!$ over $\mathbb{Q}$ and generically, it has. In what follows we assume f to be monic and integral, so that α_i are algebraic integers. We will give algorithms for the following tasks.

1. Given some $g \in \mathbb{Z}[X_1, \ldots, X_n]$, decide if $g(\alpha_1, \ldots, \alpha_n) = 0$.
2. Given $g_j \in \mathbb{Z}[X_1, \ldots, X_n]$ $(1 \leqslant j \leqslant s)$, find a $\mathbb{Z}$-module basis for

$$\Lambda := \left\{ \underline{e} \in \mathbb{Z}^s \mid \sum_{j=1}^{s} e_j g_j(\alpha_1, \ldots, \alpha_n) = 0 \right\}.$$

Obviously, both tasks are trivial if exact representations for K or I are known, so we essentially assume that $(K : \mathbb{Q})$ is too large to allow direct algebraic constructions to succeed. Our method will be based on approximate representations of the α_i; that is, we are going to use the field $\mathbb{C}$ of complex numbers and certain unramified p-adic extensions of $\mathbb{Q}_p$ for our work. For basic properties of p-adic numbers, we refer to [**21**, **15**].

Let $p \in \mathbb{Z}$ be a prime number. For any $r \in \mathbb{Z}$, we can write $r = p^l r'$ for some r' not divisible by p. The function

$$v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{Z} : r = p^l r' \mapsto l$$

is called the p-adic valuation on $\mathbb{Z}$. We extend v_p to all of $\mathbb{Z}$ by defining $v_p(0) := \infty$ and extend further to $\mathbb{Q}$ by setting $v_p(a/b) = v_p(a) - v_p(b)$. Via

$$|.|_p : \mathbb{Q} \to \mathbb{Q} : x \mapsto p^{-v_p(x)},\ 0 \mapsto 0,$$

this gives rise to the (normalised) p-adic absolute value and thus the p-adic topology on $\mathbb{Q}$. The completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to to $|.|_p$ is called the field of p-adic numbers; it contains the p-adic integers, the completion $\mathbb{Z}_p$ of $\mathbb{Z}$.

Suppose now that over $\mathbb{F}_p$, the field with p elements, f factors as

$$f = \prod_{i=1}^{l} f_i \mod p$$

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

with irreducible, pairwise coprime $f_i \in \mathbb{F}_p[t]$. Then there is an (unramified) extension $\Gamma/\mathbb{Q}_p$ of degree $f_p := \operatorname{lcm}_{i=1}^{l} \deg f_i$ where f splits into linear factors. Furthermore, there is a unique extension of $|.|_p$ to Γ which is again denoted by $|.|_p$. Similarly to $\mathbb{R}$ or $\mathbb{C}$, elements in Γ cannot, in general, be represented exactly; instead, approximations with a given fixed precision have to be used. The advantage of using Γ as a splitting field, rather than $\mathbb{C}$ or K directly, lies in the fact that arithmetic operations in Γ incur less numerical loss of precision than operations with real numbers, while the algebraic degree of $\Gamma/\mathbb{Q}_p$ is still much smaller than the degree of $K/\mathbb{Q}$. The main disadvantage of using Γ or $\mathbb{C}$ is that, since there is no exact representation of elements, in general we cannot decide if an element is zero without additional information.

Lastly, we note that up to Galois conjugation, there is exactly one prime ideal P of $\mathbb{Z}_K$ (the ring of integers of K) such that $\Gamma = K_P$ the P-adic completion at P. For elements $x \in \mathbb{Z}_K$, we have $x \in P^k$ if and only if $|x|_p \leqslant p^{-k}$.

In addition to the p-adic information mainly encoded in Γ, we are also going to need complex information about elements in K. As a number field $K/\mathbb{Q}$, K admits $(K : \mathbb{Q})$ many distinct embeddings $(.)^{(j)}$ $(1 \leqslant j \leqslant (K : \mathbb{Q}))$ into the complex numbers. For any $x \in K$ we define a length:

$$T_2 : K \to \mathbb{R} : x \mapsto \sum_{j=1}^{(K:\mathbb{Q})} |x^{(j)}|^2.$$

Note that $\sqrt{T_2}$ is an Euclidean norm on the $\mathbb{Q}$-vectorspace K. Elementary Galois theory and the inequality between arithmetic and geometric means can be used to derive non-trivial lower bounds on $T_2(x)$:

$$\sqrt[(K:\mathbb{Q})]{N_{K/\mathbb{Q}}(x^2)} \leqslant \frac{1}{K : \mathbb{Q}} T_2(x) \tag{1}$$

which implies for non-zero algebraic integers $x \in \mathbb{Z}_K \setminus \{0\}$ that

$$T_2(x) \geqslant (K : \mathbb{Q}). \tag{2}$$

REMARK. Let $\beta_1, \ldots, \beta_n \in \mathbb{C}$ be the complex roots of f. In general it is extremely difficult to sort the complex roots in such a way that α_i corresponds to β_i, which means that, for example, from $\sum_{i=1}^{n} e_i \alpha_i = 0$ we cannot, in general, conclude that $\sum_{i=1}^{n} e_i \beta_i = 0$.

After these preliminaries we can now state our algorithm for the first problem.

ALGORITHM 1. *Let $\alpha_1, \ldots, \alpha_n \in \Gamma/\mathbb{Q}_p$ be the roots of some monic polynomial $f \in \mathbb{Z}[t]$, and assume that Γ is unramified over $\mathbb{Q}_p$. The α_i are given as sufficiently good approximations $\tilde{\alpha}_i$, such that $|\alpha_i - \tilde{\alpha}_i|_p < |\alpha_j - \tilde{\alpha}_i|_p$ $(1 \leqslant i, j \leqslant n,\ i \neq j)$ and $|f(\tilde{\alpha}_i)|_p < f'(\tilde{\alpha}_i)|_p^2$ in order to apply Newton-lifting. Set $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ and let $g \in \mathbb{Z}[x_1, \ldots, x_n]$ be arbitrary. This algorithm decides whether*

$$g(\alpha_1, \ldots, \alpha_n) = 0.$$

1. *Compute a bound $M > 0$ such that $|g(\alpha_1, \ldots, \alpha_n)^{(j)}| \leqslant M$ for all complex embeddings $(.)^{(j)} : K \to \mathbb{C}$. Such a bound can be obtained by first computing a bound M' on the complex roots $\beta_i \in \mathbb{C}$ of f, and then estimating $|g(\gamma_1, \ldots, \gamma_n)|$ for all choices of $|\gamma_i| \leqslant M'$.*

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

2. *Compute a bound* $r \geqslant (K : \mathbb{Q})$.
3. *Set*
$$k := \left\lceil \frac{r}{(\Gamma : \mathbb{Q}_p)} \frac{\log M}{\log p} \right\rceil.$$
4. *Compute* $\tilde{\alpha}_j$ *such that* $|\tilde{\alpha}_j - \alpha_j|_p \leqslant p^{-k}$ *for* $1 \leqslant j \leqslant n$.
5. *Evaluate* $\tilde{G} := g(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$.
6. *If* $|\tilde{G}|_p > p^{-k}$ *return* **NotZero**; *otherwise return* **IsZero**.

Proof. Throughout this proof, we write $\tilde{\alpha}_i$ for finite precision approximations to the exact root $\alpha_i \in \Gamma$ that we cannot exactly represent. Similarly, $G := g(\alpha_1, \ldots, \alpha_n)$ is the exact element that we cannot compute but need to decide if $G = 0$ and $\tilde{G} := g(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$ is a finite precision approximation.

We first note that since $f \in \mathbb{Z}[t]$ is monic, we have $\alpha_i \in \mathbb{Z}_\Gamma$, the integral closure of $\mathbb{Z}_p$ in Γ. Now $g \in \mathbb{Z}[x_1, \ldots, x_n]$ implies $G \in \mathbb{Z}_\Gamma$ as well. Writing $\tilde{\alpha}_i = \alpha_i + p^k \gamma_i$ with some $\gamma_i \in \mathbb{Z}_\Gamma$ we obtain from the ultrametric property of $|.|_p$:
$$|g(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)|_p \leqslant \max(|g(\alpha_1, \ldots, \alpha_n)|_p, p^{-k});$$
that is, there is no loss of precision in the evaluation.

Let $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, as above, and let P be some prime ideal $\mathbb{Z}_K \supset P|p$ such that $\Gamma = K_P$. Then for $x \in \mathbb{Z}_K$ such that $|x|_p \leqslant p^{-k}$ we obtain $x \in P^k$; thus $N_{K/\mathbb{Q}}(x) \in N_{K/\mathbb{Q}}(P)^k$ and, since $N_{K/\mathbb{Q}}(P)$ is an ideal in $\mathbb{Z}$ generated by $p^{\Gamma:\mathbb{Q}_p}$:
$$p^{k(\Gamma:\mathbb{Q}_p)} \leqslant N_{K/\mathbb{Q}}(x).$$

Now, let us assume that we have k and M as in the algorithm, $|\tilde{G}|_p \leqslant p^{-k}$ and assume $G \neq 0$. From
$$\sqrt[(K:\mathbb{Q})]{N_{K/\mathbb{Q}}(G^2)} \leqslant \frac{T_2(G)}{K : \mathbb{Q}} \leqslant \frac{M^2(K : \mathbb{Q})}{K : \mathbb{Q}} = M^2$$
we get $N_{K/\mathbb{Q}}(G) \geqslant p^{k(\Gamma:\mathbb{Q}_p)}$. And thus
$$\frac{k(\Gamma : \mathbb{Q}_p)}{K : \mathbb{Q}} \leqslant \frac{\log M}{\log p},$$
which contradicts our choices. Thus we conclude that $G = 0$, as claimed. □

While the above algorithm can verify a relation, it does not tell us how to find one. Also, the precision necessary to verify relations can be extremely large; it is essentially linear in $(K : \mathbb{Q}) = \#\operatorname{Gal}(f)$. In order to use similar ideas to find relations, we first need a result allowing us to get a bound on a basis of the relation lattice.

THEOREM 1. *Let* $\alpha_1, \ldots, \alpha_n$ *be algebraic integers,* $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, $r := (K : \mathbb{Q})$, *and define*
$$\Lambda := \left\{ \underline{e} \in \mathbb{Z}^n \mid \sum_{i=1}^{n} e_i \alpha_i = 0 \right\}.$$
Suppose that $|\alpha_i^{(j)}| \leqslant M$ *for all complex embeddings* $(.)^{(j)} : K \to \mathbb{C}$ $(1 \leqslant j \leqslant r)$ *and all* $1 \leqslant i \leqslant n$; *then* Λ *has a* $\mathbb{Z}$*-basis* $\underline{b}_i \in \mathbb{Z}^n$, $1 \leqslant i \leqslant l$, *with*
$$\|\underline{b}_i\|_\infty \leqslant n^{n-1} M^{n-1}.$$

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

Proof. The function

$$f : \mathbb{Z}^n \to \mathbb{R} : \underline{e} \mapsto \sqrt{T_2\left(\sum_{i=1}^{n} e_i \alpha_i\right)}$$

is a convex distance function in the sense of [**16**, p. 250]. Let m be a standard basis element of $\mathbb{Z}^n$; that is, $m = (m_i)_{1 \leqslant i \leqslant n}$ and $m_i = 0$ for all $i \neq i_0$ while $m_{i_0} = 1$. Then $f(m) = \sqrt{T_2(\alpha_{i_0})} \leqslant \sqrt{r}M$. From (2) we get for non-zero algebraic integers $x \in K$ that $T_2(x) \geqslant r$; thus $f(m) \geqslant \sqrt{r}$, for all $m \in \mathbb{Z}^n$ with $f(m) \neq 0$. The rest now follows directly from the proposition of [**16**, p. 250]. □

The next essential ingredient is the LLL algorithm for lattice reduction. We need the following property of a reduced basis [**7**, Theorem 2.6.2.(5)].

LEMMA 1. *Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice. Suppose that Λ contains linearly independent elements $x_1, \ldots, x_l$, of norm $\|x_i\|_2 \leqslant M$. Then for an* LLL*-reduced basis $b_1, \ldots, b_n$ of Λ, we have $\|b_i\|_2^2 \leqslant 2^{n-1}M^2$ for $1 \leqslant i \leqslant l$.*

Combining the previous results we can now give a first algorithm for linear dependencies.

ALGORITHM 2. *Let $f \in \mathbb{Z}[t]$ be monic, and let $\alpha_1, \ldots, \alpha_n \in \Gamma/\mathbb{Q}_p$ be the roots of f in some unramified extension of $\mathbb{Q}_p$ of degree f_p. We assume that elements in Γ are represented as vectors in $\mathbb{Q}_p^{f_p}$ with respect to some fixed basis $\omega_1, \ldots, \omega_{f_p}$. Furthermore, let $g_i \in \mathbb{Z}[x_1, \ldots, x_n]$ be arbitrary $(1 \leqslant i \leqslant s)$ and define*

$$\Lambda := \left\{ \underline{e} \in \mathbb{Z}^s \mid \sum_{i=1}^{s} e_i g_i(\alpha_1, \ldots, \alpha_n) = 0 \right\}.$$

This algorithm computes a $\mathbb{Z}$-basis for Λ.

1. *Compute a bound $M > 0$ such that for each $1 \leqslant i \leqslant s$, $|g_i(\alpha_1, \ldots, \alpha_n)^{(j)}| \leqslant M$ for all complex embeddings $(.)^{(j)} : K \to \mathbb{C}$.*
2. *Set $N := s^{s-1}M^{s-1}$.*
3. *Set*
$$k := \left\lceil \frac{(\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q})}{f_p} \frac{\log NMs}{\log p} \right\rceil.$$
4. *Set $\lambda := N^2 2^{s-1}$.*
5. *Compute $\tilde{\alpha}_j$ such that $|\tilde{\alpha}_j - \alpha_j|_p \leqslant p^{-k}$.*
6. *Compute $\tilde{\beta}_i := g(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n)$ for $1 \leqslant i \leqslant s$, and form a matrix B where the ith row contains the lift of coefficients of $\tilde{\beta}_i$ as elements to $\mathbb{Z}$.*
7. *Form a big matrix $\tilde{B} \in \mathbb{Z}^{(s+f_p)\times(s+f_p)}$ by first concatenating I_s and λB to get $(I_s|\lambda B)$ and then appending a matrix $(0 I_s|\lambda p^k I_{f_p})$ to the bottom.*
8. *Apply the* LLL *algorithm to the rows of $\tilde{B}$, obtaining a new matrix $L = (L_{i,j})_{1 \leqslant i,j \leqslant f_p+s}$.*
9. *The lattice Λ is generated by $(L_{i,j})_{1 \leqslant i \leqslant l, 1 \leqslant j \leqslant s}$, where l is the index of the last row L_i of L with norm $\|L_i\|_2 < \lambda$.*

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

Proof. Using Theorem 1, we see that N is a bound for the maximum norm of a length of a basis-relation, so that NMs is a bound for the complex embedding $|(.)^{(j)}|$ of a possible relation. The precision is now chosen in the same way as in Algorithm 1 so that a possible relation $\underline{e} \in \mathbb{Z}^s$ with $\|e\|_2 < N$ and $|\sum_{i=1}^{s} e_i g_i(\alpha_1, \ldots, \alpha_n)|_p < p^{-k}$ has to be zero.

In the matrix L, the s leftmost columns encode the transformations applied to B, while the rightmost columns give the evaluated relation:

$$\lambda \sum_{i=1}^{s} L_{j,i} g_i(\tilde{\alpha}_1, \ldots, \tilde{\alpha}_n) = \sum_{i=1}^{f_p} L_{j,i+s} \tilde{\omega}_i + p^k x$$

(for some $x \in \mathbb{Z}_\Gamma$). So we see that if there is a relation $\sum_{i=1}^{s} e_i g_i(\alpha_1, \ldots, \alpha_n) = 0$, then the $\mathbb{Z}$-span of the first s rows of $\tilde{B}$ contains a vector $(e_1, \ldots, e_n, u_1, \ldots, u_{f_p})$, with $u_i \in \lambda p^k \mathbb{Z}$. So by adding suitable multiples of the last f_p rows of $\tilde{B}$, we find that $(e_1, \ldots, e_n, 0, \ldots, 0)$ lies in the $\mathbb{Z}$-span of the rows of $\tilde{B}$.

Our choice of k and λ now ensures the following facts.

1. If and only if $(L_{j,i})_{1 \leqslant j \leqslant s}$ is a true relation, is $(L_{j,i+s})_{1 \leqslant j \leqslant f}$ zero.
2. If $(L_{j,i+s})_{1 \leqslant j \leqslant f}$ is not zero, then $\|(L_{i,j})_{1 \leqslant j \leqslant s+f}\|_2 \geqslant \lambda > N$.
3. If there are relations within the bounds of Theorem 1, then the LLL will find them since by Lemma 1, there must be rows in L with norm bounded by $2^{s-1} N < \lambda$, which implies that they are relations. □

In applying the above algorithm, the main problem is the huge precision k needed to guarantee correctness. Since the precision directly determines the bit-length of the entries of B, it is the crucial parameter for the runtime of the LLL algorithm. By [**17**] we know that the runtime depends quadratically on the bit-length on the input; thus we need to try to reduce the precision. Since verification of a relation (using Algorithm 1) is computationally much easier than finding a relation, one method is to just use the above Algorithm 2 with a smaller precision, say $\lceil 1.5(\log N / \log p) \rceil$, apply the LLL algorithm, and test the relations obtained. In cases where Algorithm 1 fails to verify a relation obtained this way, we increase the precision and try again. The proof of the correctness shows that this method must terminate with the correct answer.

If the Galois-action on the p-adic roots $\alpha_1, \ldots, \alpha_n$ is known, then we can substantially improve the runtime, by using the fact that if $\sum_{i=1}^{s} g_i(\alpha_1, \ldots, \alpha_n) = 0$ then we also have $\sum_{i=1}^{s} g_i(\alpha_{\sigma 1}, \ldots, \alpha_{\sigma n}) = 0$ for all $\sigma \in G = \mathrm{Gal}(f)$. This allows us to replace LLL by much faster echelon algorithms over $\mathbb{Z}/p^k\mathbb{Z}$, followed by rational reconstruction.

ALGORITHM 3. *Let $f \in \mathbb{Z}[t]$ be monic, and let $\alpha_1, \ldots, \alpha_n \in \Gamma/\mathbb{Q}_p$ be the roots of f in some unramified extension of $\mathbb{Q}_p$ of degree f_p. Furthermore, let $G = \mathrm{Gal}(f) < S_n$ be given explicitly; that is, $\sigma\alpha_i = \alpha_{\sigma i}$. Now, let $g_i \in \mathbb{Z}[x_1, \ldots, x_n]$ be arbitrary $(1 \leqslant i \leqslant s \leqslant \#G)$ and define*

$$\Lambda := \left\{ \underline{e} \in \mathbb{Z}^s \mid \sum_{i=1}^{s} e_i g_i(\alpha_1, \ldots, \alpha_n) = 0 \right\}.$$

This algorithm computes a $\mathbb{Z}$-basis for Λ.

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

1. *Compute a bound* $M > 0$ *such that for each* i *we have* $|g_i(\beta_1, \ldots, \beta_n)^{(j)}| < M'$.
2. *Set* $N := s^{s-1}M^{s-1}$.
3. *Set* $k := \lceil 2 \log NM / \log p \rceil$.
4. *Select a set* $S \subseteq G$ *of size* s, *containing the identity of* G.
5. *Repeat:*
   6. *compute* $\tilde{\alpha}_j$ *such that* $|\tilde{\alpha}_j - \alpha_j|_p \leqslant p^{-k}$;
   7. *set* $B := ()$ *a matrix with* s *rows and* 0 *columns*;
   8. *for* $\sigma \in S$ *do*
      9. *compute* $\tilde{\beta}_i := g_i(\tilde{\alpha}_{\sigma 1} \ldots, \tilde{\alpha}_{\sigma n})$ *for* $1 \leqslant i \leqslant s$, *and form a matrix* $\tilde{B}$ *where the* i*th row contains the lift of coefficients of* $\tilde{\beta}_i$ *as elements to* $\mathbb{Z}$;
      10. *set* $B := (B|\lambda\tilde{B})$; *that is, append* $\lambda\tilde{B}$ *to the right of* B.
   11. *Apply HNF techniques to compute the nullspace* N *of* $B \in (\mathbb{Z}/p^k\mathbb{Z})^{f_p \times s}$ *in echelon form.*
   12. *Use rational reconstruction to find (if possible) the unique* $\tilde{N} \in \mathbb{Q}^{l \times s}$ *such that* $\tilde{N} \equiv N \mod p^k$. *If this fails, increase the set* S *by randomly selecting at most* $0.2\#S$ *elements in* $G \setminus S$ *and* $k := \lceil 1.2k \rceil$ *and go back to step* 5.
   13. *Compute a matrix* $S \in \mathbb{Z}^{l \times n}$ *such that* S *is a* $\mathbb{Z}$*-basis for the intersection of the* $\mathbb{Q}$*-vectorspace with basis* $\tilde{N}$ *and* $\mathbb{Z}^s$ *(using some saturation method).*
   14. *Apply the* LLL *algorithm to* S *to obtain a* LLL *reduced basis* L.
   15. *Set* $k := \lceil 1.2k \rceil$ *and increase the set* S *by randomly selecting at most* $0.2\#S$ *elements in* $G \setminus S$,
16. *until all rows* L_i *of* L *are norm bounded:* $\|L_i\|_2 < N$ *and are true relations by Algorithm* 1.

Proof. Let $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$; then, since Γ is a splitting field for f, we have $K \otimes_{\mathbb{Q}} \Gamma \cong \Gamma^G = \Gamma^{(K:\mathbb{Q})}$ and the embedding is given via $\alpha_i \mapsto (\sigma(\alpha_i))_{\sigma \in G}$. Furthermore, as $\mathbb{Q}_p$-vectorspace we have

$$\Gamma \cong \mathbb{Q}_p^{f_p} \qquad \text{and} \qquad K \otimes_{\mathbb{Q}} \Gamma \cong \mathbb{Q}_p^{f_p(K:\mathbb{Q})}$$

and the embedding extends via composition with

$$\Gamma \ni \gamma = \sum_{i=1}^{f_p} \gamma_i \omega_i \mapsto (\gamma_i)_{1 \leqslant i \leqslant f_p} \in \mathbb{Q}_p^{f_p}.$$

If we apply this embedding to $V := [g_1(\underline{\alpha}), \ldots, g_s(\underline{\alpha})]_{\mathbb{Q}}$ we get

$$V \otimes \Gamma = [(g_1(\sigma\underline{\alpha}))_{\sigma \in G}, \ldots (g_s(\sigma\underline{\alpha}))_{\sigma \in G}]_{\Gamma}.$$

The fact that extensions of scalars preserve dimension,

$$\dim_{\mathbb{Q}}(V) = \dim_{\Gamma}(V \otimes \Gamma) = \dim_{\mathbb{Q}_p}(V \otimes \Gamma)$$

implies that eventually $\mathrm{rk}_{\mathbb{Q}_p} B = \dim_{\mathbb{Q}}(V)$. Similarly, the increasing precision ensures that the rational reconstruction will be successful, eventually. To be more precise: assume that S is large enough so that $\dim_{\mathbb{Q}}(V) = \mathrm{rk}_{\mathbb{Q}_p} B$ and let $M \in \mathbb{Q}^{l \times s}$ be a $\mathbb{Q}$-basis matrix for the $\mathbb{Q}$-nullspace of B. Without loss of generality, we can furthermore assume that $M = (M_{i,j})$ is in echelon form, and thus M is uniquely

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

defined by V. If the precision k is chosen so that $p^k > \max h(M_{i,j})^2$ for the naive height $h : \mathbb{Q} \to \mathbb{Z} : p/q \mapsto \max(p, q)$, then N in step 11 will allow us to compute M by reconstruction.

If, however, S is too small, it may happen that $\mathrm{rk}_{\mathbb{Q}_p} B < \dim_{\mathbb{Q}}(V)$, which means that the matrix N computed in step 11 does not represent an approximation to M. In this case, either the reconstruction fails or the reconstructed relations cannot be verified in step 16. □

In steps 4, 12 and 15 we increase the size of the matrix by exploiting the Galois action. This is done hoping that generically the new columns are independent from the previous ones so as to increase the rank of B. It is clear that if $S = G$, then the $\mathbb{Z}$-nullspace of B would be precisely Λ; however, if $S = \{I_G\}$ then there will always be spurious relations, some of which may be small in size.

Also, using well-known techniques that generalize rational reconstruction to number fields [**9, 1, 10**] and omitting steps 13 and 14, the algorithms can easily be extended to find R-relations instead of $\mathbb{Z}$-relations for R being any order in some number field.

Remark. The complexity of our algorithms is easily seen to be polynomial in the input data and in $(K : \mathbb{Q})$ as the precision necessary to ensure correctness in Algorithm 1 (and in 2 and 3 as well) is essentially linear in $(K : \mathbb{Q})$. In general we expect $(K : \mathbb{Q})$ to be close to $n! = O(n^n)$, and thus the overall complexity will be exponential. This agrees well with all other published algorithms, as they are always polynomial in the size of the input data — which is mainly the degree of the number field containing $\alpha_1, \ldots, \alpha_n$. In the general situation, this field will have degree exponential in n.

3. *An algorithm for the algebraic hull*

Let V be a finite-dimensional vector space over a field of characteristic 0. A subgroup $G \subset \mathrm{GL}(V)$ is said to be algebraic if there is a set of polynomial functions P on $\mathrm{End}(V)$ such that G consists of all $g \in \mathrm{GL}(V)$ with $f(g) = 0$ for all $f \in P$. To such a group corresponds a Lie algebra, $\mathrm{Lie}(G) \subset \mathfrak{gl}(V)$ (see [**5**, Chapter II, §8]), where by $\mathfrak{gl}(V)$ we denote the Lie algebra of all endomorphisms of V. Now a given Lie subalgebra $\mathfrak{g} \subset \mathfrak{gl}(V)$ is called algebraic if there is an algebraic subgroup $G \subset \mathrm{GL}(V)$ such that $\mathfrak{g} = \mathrm{Lie}(G)$. In [**5**], Chevalley studied this concept in characteristic 0, and gave several criteria for a $\mathfrak{g} \subset \mathfrak{gl}(V)$ to be algebraic.

Let $\mathfrak{g} \subset \mathfrak{gl}(V)$ be any Lie algebra. Then by [**5**, Chapter II, Theorem 13], there is a unique smallest algebraic Lie algebra containing $\mathfrak{g}$. This algebraic Lie algebra is called the algebraic hull of $\mathfrak{g}$. In this section we consider the problem of constructing the algebraic hull for a given $\mathfrak{g} \subset \mathfrak{gl}(V)$.

Here F will be a field of characteristic 0. We will use the language of matrices, rather than that of endomorphisms, as this is more convenient for calculations. In particular, $\mathfrak{gl}(n, F)$ is the Lie algebra of all $n \times n$-matrices over F. By [**5**, Chapter II, Theorem 14], a Lie algebra $\mathfrak{g} \subset \mathfrak{gl}(n, F)$ is algebraic if it is generated by algebraic Lie algebras. It follows that $\mathfrak{g}$ is algebraic if and only if the algebraic hull of the subalgebra spanned by each basis element of $\mathfrak{g}$ is contained in $\mathfrak{g}$. Hence we can compute the algebraic hull of $\mathfrak{g}$ if we can compute it in the case where $\mathfrak{g}$ is spanned by one matrix X.

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

Let $X \in \mathfrak{gl}(n, F)$. Then by $\mathfrak{g}_F(X)$ we denote the algebraic hull of the Lie algebra spanned by X. Let $X = S + N$ be the Jordan decomposition of X. Then from [5, Chapter II, Theorem 10] (see also [2, §7]), it follows that $\mathfrak{g}_F(X) = \mathfrak{g}_F(S) \oplus \mathfrak{g}_F(N)$. Moreover, $\mathfrak{g}_F(N)$ is spanned by N, by [5, Chapter II, §13, Proposition 1]. So the problem is reduced to finding $\mathfrak{g}_F(X)$ when X is semisimple.

The following theorem is proved in [5].

THEOREM 2 (CHEVALLEY). *Let $X \in \mathfrak{gl}(n, F)$ be semisimple, and let $K \supset F$ be an algebraic extension containing the eigenvalues $\alpha_1, \ldots, \alpha_n$ of X. Let $U \in \mathrm{GL}(n, K)$ be such that $Y = UXU^{-1}$ is in diagonal form, with the α_i on the diagonal. Set $\Lambda = \{(e_1, \ldots, e_n) \in \mathbb{Z}^n \mid \sum_i e_i\alpha_i = 0\}$. Then*

1. $\mathfrak{g}_K(X) = U^{-1}\mathfrak{g}_K(Y)U$ *and*
$$\mathfrak{g}_K(Y) = \left\{ \mathrm{diag}(a_1, \ldots, a_n) \mid a_i \in K \text{ and } \sum_i e_i a_i = 0 \text{ for all } (e_1, \ldots, e_n) \in \Lambda \right\};$$
2. $\mathfrak{g}_F(X) \otimes K \cong \mathfrak{g}_K(X)$;
3. $\mathfrak{g}_F(X) \subset A_F(X)$ *where $A_F(X)$ is the associative F-algebra with* 1 *generated by X.*

The first part of statement 1 is straightforward. Let $G_K(X)$ denote the smallest algebraic subgroup of $\mathrm{GL}(n, K)$ such that its Lie algebra contains X. Then $G_K(X) = U^{-1}G_K(Y)U$ and $\mathfrak{g}_K(X) = \mathrm{Lie}(G_K(X)) = U^{-1}\,\mathrm{Lie}(G_K(Y))U = U^{-1}\mathfrak{g}_K(Y)U$. The second part of statement 1 is [5, §13, Proposition 2]. Statement 2 follows from the proof of [5, §13, Theorem 10]. Furthermore, statement 3 is [5, §14, Proposition 14]. (There, it is shown that $\mathfrak{g}_F(X)$ is contained in the associative algebra (not necessarily with 1) generated by X. However, for us it will be more convenient to add the identity.)

In the remainder of this section we use the same notation as in Theorem 2. In particular, we let X be a semisimple $n \times n$-matrix with coefficients in the field F of characteristic 0. We let K be a finite extension of F containing the eigenvalues $\alpha_1, \ldots, \alpha_n$ of X. Furthermore, $\Lambda = \{(e_1, \ldots, e_n) \in \mathbb{Z}^n \mid \sum_i e_i\alpha_i = 0\}$, and $\Lambda_{\mathbb{Q}} = \{(e_1, \ldots, e_n) \in \mathbb{Q}^n \mid \sum_i e_i\alpha_i = 0\}$. By $A_F(X)$ we denote the associative algebra with 1 generated by X. The algorithm for constructing $\mathfrak{g}_F(X)$ is based on the following lemma.

LEMMA 2. *For $\underline{e} = (e_1, \ldots, e_n) \in \mathbb{Q}^n$ and $i \geqslant 0$, set $\Delta_i(\underline{e}) = \sum_{k=1}^n e_k\alpha_k^i$. Let $I = X^0, X, \ldots, X^t$ be a basis of $A_F(X)$. Set*

$$\Upsilon = \left\{ (\gamma_0, \ldots, \gamma_t) \in F^{t+1} \mid \sum_{i=0}^{t} \Delta_i(\underline{e})\gamma_i = 0 \text{ for all } \underline{e} \in \Lambda_{\mathbb{Q}} \right\}.$$

Then $\mathfrak{g}_F(X) = \{\sum_{i=0}^t \gamma_i X^i \mid (\gamma_0, \ldots, \gamma_t) \in \Upsilon\}$.

Proof. Let $Y = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$. Then there is a $U \in \mathrm{GL}(n, K)$ with $UXU^{-1} = Y$. Here $t + 1$ is the degree of the minimal polynomial of X. Then since the minimal polynomial of a semisimple matrix is the square-free part of its characteristic polynomial, the minimal polynomial of Y (over K) is the same as the minimal polynomial of X (over F). Hence $A_K(Y)$ is spanned by $I, Y, Y^2, \ldots, Y^t$.

Set $y = \sum_{i=0}^t \gamma_i Y^i$. Write $y(k, k)$ for the entry in y on position (k, k). Then by Theorem 2, $y \in \mathfrak{g}_K(Y)$ if and only if for all $\underline{e} \in \Lambda$ we have $\sum_k e_k y(k, k) = 0$. It

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

is clear that in this statement we may replace Λ by $\Lambda_{\mathbb{Q}}$. Indeed, Λ is a subgroup of $\mathbb{Z}^n$ and hence it is finitely generated (see, for example, [**20**, Corollary II.3.k]). Furthermore, a $\mathbb{Z}$-basis of Λ will also be a $\mathbb{Q}$-basis of $\Lambda_{\mathbb{Q}}$.

Now $y(k,k) = \sum_{i=0}^{t} \gamma_i \alpha_k^i$, and hence $\sum_{k=1}^{n} e_k y(k,k) = \sum_{i=0}^{t} \Delta_i(\underline{e})\gamma_i$. Now set

$$\Upsilon' = \left\{ (\gamma_0, \ldots, \gamma_t) \in K^{t+1} \mid \sum_{i=0}^{t} \Delta_i(\underline{e})\gamma_i = 0 \text{ for all } \underline{e} \in \Lambda_{\mathbb{Q}} \right\}.$$

Then by Theorem 2 we see that $\mathfrak{g}_K(Y) = \{\sum_{i=0}^{t} \gamma_i Y^i \mid (\gamma_0, \ldots, \gamma_t) \in \Upsilon'\}$. By the same theorem, $\mathfrak{g}_K(X) = U^{-1}\mathfrak{g}_K(Y)U$, and hence $\mathfrak{g}_K(X) = \{\sum_{i=0}^{t} \gamma_i X^i \mid (\gamma_0, \ldots, \gamma_t) \in \Upsilon'\}$.

Now let $X_1, \ldots, X_s$ be any basis of $\mathfrak{g}_F(X)$. Then according to Theorem 2(2) they are also a basis of $\mathfrak{g}_K(X)$. So $\mathfrak{g}_K(X)$ consists of $\sum_i \beta_i X_i$ with $\beta_i \in K$. By Theorem 2(3), $X_i \in A_F(X)$. Hence $\mathfrak{g}_K(X) \cap A_F(X)$ consists of $\sum_i \delta_i X_i$ with $\delta_i \in F$. We conclude that $\mathfrak{g}_K(X) \cap A_F(X) = \mathfrak{g}_F(X)$. From this we get the desired conclusion. □

In order to use this result for a practical algorithm, we restrict to the case where F is an algebraic number field. Then we have the following the algorithm for computing $\mathfrak{g}_F(X)$.

ALGORITHM 4. *Let the notation be as above. We suppose that F is a number field. This algorithm computes an F-basis for $\mathfrak{g}_F(X)$.*

1. *Compute an algebraic extension $K \supset F$ containing the eigenvalues $\alpha_1, \ldots, \alpha_n$ of X.*
2. *Compute (a $\mathbb{Q}$-basis for) $\Lambda_{\mathbb{Q}}$.*
3. *Compute (an F-basis for) Υ (where Υ is as in Lemma 2).*
4. *Return the set consisting of $\sum_{i=0}^{t} \gamma_i X^i$ where $(\gamma_0, \ldots, \gamma_t)$ runs through the basis of the previous step.*

Proof. First we show that all steps are computable. First of all, by iteratively factoring polynomials over number fields we can compute a number field $K \supset F$ containing the eigenvalues $\alpha_1, \ldots, \alpha_n$ of X. Furthermore, K has a finite $\mathbb{Q}$-basis, and a finite F-basis. Then by writing the α_i on a $\mathbb{Q}$-basis of K we can derive a set of linear equations for $\Lambda_{\mathbb{Q}}$, and hence we can compute a basis of this space. Note that $\Delta_i(\underline{e})$ depends linearly on $\underline{e}$. Hence, in order to compute Υ, it is enough to consider $\underline{e}$ in a $\mathbb{Q}$-basis of $\Lambda_{\mathbb{Q}}$. So by writing the $\Delta_i(\underline{e})$ on an F-basis of K, we can derive a set of linear equations for Υ. Therefore, we can compute a basis of this space. The last step is trivially computable.

The correctness of the algorithm follows from Lemma 2. □

EXAMPLE 1. Let $X \in \mathfrak{gl}(4, \mathbb{Q})$ have minimum polynomial $T^4 + bT^2 + c$ with $D = b^2 - 4c$ not a square in $\mathbb{Q}$. Then the eigenvalues of X are $\alpha_1 = \alpha$, $\alpha_2 = -\alpha$, $\alpha_3 = \beta$, $\alpha_4 = -\beta$, where $\alpha^2 = \frac{1}{2}(-b + \sqrt{D})$ and $\beta^2 = \frac{1}{2}(-b - \sqrt{D})$. Then α and β cannot be proportional over $\mathbb{Q}$ (otherwise α^2 and β^2 would be as well). Hence the α_i span a two-dimensional subspace of K. So $\dim \Lambda = 2$, and is spanned by $\underline{e}^1 = (1,1,0,0)$, $\underline{e}^2 = (0,0,1,1)$. Then $\Delta_0(\underline{e}^1) = 2$, $\Delta_1(\underline{e}^1) = \Delta_3(\underline{e}^1) = 0$, $\Delta_2(\underline{e}^1) = 2\alpha^2$. For $\underline{e}^2$ we get the same, except that $\Delta_2(\underline{e}^2) = 2\beta^2$. So

$$\Upsilon = \left\{ (\gamma_0, \ldots, \gamma_3) \in \mathbb{Q}^3 \mid 2\gamma_0 + 2\alpha^2\gamma_2 = 2\gamma_0 + 2\beta^2\gamma_2 = 0 \right\}.$$

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

Hence Υ consists of $(0, \gamma_1, 0, \gamma_3)$. We conclude that $\mathfrak{g}(X)$ is spanned by X, X^3.

As remarked in the introduction, Algorithm 4 works only in cases where the splitting field is of moderate size. Now we show how the algorithms of Section 2 can be used to avoid constructing this field. For simplicity we assume that the characteristic polynomial of X is square-free. The generalisation to the general case is straightforward. Let f be the characteristic polynomial of X, and let α_i $(1 \leqslant i \leqslant n)$ be the roots of f with fixed ordering in some field $\Gamma \supseteq \mathbb{Q}$.

First we find $\Lambda := \{\underline{e} \in \mathbb{Z}^n \mid \sum_{i=1}^n e_i\alpha_i = 0\}$ using $g_i := x_i$ and either Algorithm 2 or Algorithm 3. Let $\underline{e} = (e_1, \ldots, e_n)$ be a basis element of Λ. The second step consists of solving the equations that define Υ (cf. Lemma 2). For $i \geqslant 0$, set $g_i(\underline{e}) = \sum_{k=1}^n e_k x_k^i$, and $\Delta_i(\underline{e}) := g_i(e)(\alpha_1, \ldots, \alpha_n)$. Let $t+1$ be the degree of the minimal polynomial of X. Then, again with Algorithm 2 or 3, we find all integral (or, equivalently, rational) linear dependencies of the $\Delta_i(\underline{e})$, that is, all vectors $u = (u_1, \ldots, u_t) \in \mathbb{Q}^t$ with $\sum_i u_i\Delta_i(\underline{e}) = 0$. Let $M(\underline{e})$ denote the $\mathbb{Q}$-vector space spanned by all those vectors u. Then Υ is equal to the intersection of all $M(\underline{e})$, where $\underline{e}$ runs through a basis of Λ. So in this way we find a basis of Υ, and hence a basis of $\mathfrak{g}_{\mathbb{Q}}(X)$ (cf. Algorithm 4).

4. *The permutation module*

Here we use the same notation as in the previous section. In this section we make some observations that on some occasions directly give a basis of $\mathfrak{g}_F(X)$.

Let f be the characteristic polynomial of X. Let K be the splitting field of f, and $G = \mathrm{Gal}(K/F)$. We represent G as a permutation group on the roots $\alpha_1, \ldots, \alpha_n$ of f. Let M be the permutation module of G over $\mathbb{Q}$; that is, M has basis $w_1, \ldots, w_n$ and $\sigma \cdot w_i = w_{\sigma(i)}$. On many occasions we will write the elements of M as row vectors. Then $\sigma(a_1, \ldots, a_n) = (a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)})$. There is a direct sum decomposition of G-modules $M = M_0 \oplus M_1$, where $M_0 = \{\sum_i a_i w_i \mid \sum_i a_i = 0\}$ and M_1 is spanned by $w_1 + \ldots + w_n$.

Let $(e_1, \ldots, e_n) \in \Lambda_{\mathbb{Q}}$ and $\sigma \in G$; then

$$0 = \sigma\left(\sum_i e_i\alpha_i\right) = \sum_i e_i\alpha_{\sigma(i)} = \sum_i e_{\sigma^{-1}(i)}\alpha_i.$$

It follows that $\Lambda_{\mathbb{Q}}$ is a G-submodule of M. So by Maschke's theorem, $\Lambda_{\mathbb{Q}} = V_1 \oplus \ldots \oplus V_s$, where the V_r are irreducible G-submodules.

From Lemma 2 we recall that $\Delta_i(\underline{e}) = \sum_{k=1}^n e_k\alpha_k^i$, where $\underline{e} \in \mathbb{Q}^n$.

LEMMA 3. *Write $f = x^n + a_1x^{n-1} + \ldots + a_n$. Then the G-submodule $M_1 \subset M$ occurs in $\Lambda_{\mathbb{Q}}$ if and only if $a_1 = 0$. Furthermore, $\Delta_i(\underline{e}) = \mathrm{Tr}(X^i)$, where $\underline{e} = (1, 1, \ldots, 1)$ spans M_1.*

Proof. We have $a_1 = 0$ if and only if $\sum_i \alpha_i = 0$; hence the first statement holds. Set $e = (1, 1, \ldots, 1)$. Let Y be as in the proof of Lemma 2. Then $\Delta_i(\underline{e}) = \sum_k \alpha_k^i = \mathrm{Tr}(Y^i) = \mathrm{Tr}(X^i)$. □

LEMMA 4. *Suppose that f is square-free, and that M_0 is irreducible. Then $a_1 = 0$ implies that $\Lambda_{\mathbb{Q}} = M_1$ and $a_1 \neq 0$ implies that $\Lambda_{\mathbb{Q}} = 0$.*

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

Proof. Note that $\Lambda_{\mathbb{Q}}$ cannot contain M_0 since in that case a vector like $(1,-1,0,\ldots,0)$ would be contained in $\Lambda_{\mathbb{Q}}$, implying that $\alpha_1 = \alpha_2$ (which is impossible because f is square-free). Hence the lemma follows by Lemma 3. □

COROLLARY 1. *Suppose that f is irreducible. Let $A_F(X)$ denote the associative algebra generated by X. Suppose that G is 2-transitive, or that $F = \mathbb{Q}$ and n is prime. If $\mathrm{Tr}(X) = 0$, then $\mathfrak{g}_F(X)$ consists of all $X' \in A_F(X)$ with $\mathrm{Tr}(X') = 0$; otherwise, $\mathfrak{g}_F(X) = A_F(X)$.*

Proof. If G is 2-transitive, then M_0 is irreducible, by [**12**, Corollary 29.10]. If $n = p$ is prime, then M_0 is irreducible over $\mathbb{Q}$. This can be proved as follows. First of all, since G is transitive it contains a p-cycle. Now we let H be the subgroup generated by this p-cycle. Then M is also an H-module. Moreover, as H-module it is isomorphic to the regular module, that is, to the module afforded by the left action of H on the group algebra $\mathbb{Q}H$. The H-submodules of $\mathbb{Q}H$ are exactly the ideals of $\mathbb{Q}H$. But $\mathbb{Q}H$ is isomorphic to $\mathbb{Q}[x]/(x^p - 1)$, which by the Chinese remainder theorem is isomorphic to $\mathbb{Q} \oplus \mathbb{Q}[x]/(x^{p-1} + x^{p-2} + \ldots + 1)$. We conclude that $\mathbb{Q}H$ splits as the direct sum of two simple ideals. Hence the H-module M is a direct sum of two simple submodules. So the same holds for M when viewed as G-module.

Now the result follows by Lemmas 3 and 4. □

In particular, if $G = S_n$ or $G = A_n$ $(n \geqslant 4)$ then we can easily compute $\mathfrak{g}(X)$.

REMARK. If the Galois action is known, then on some occasions we can use Algorithm 1 to give a more efficient algorithm for finding a basis of

$$\Lambda = \left\{ (e_1, \ldots, e_n) \mid \sum_i e_i \alpha_i = 0 \right\}.$$

As above, we denote the permutation module of G by M. We assume that M has a unique decomposition as direct sum of irreducible G-modules, $M = V_1 \oplus \ldots \oplus V_r$. The uniqueness of this decomposition is equivalent to all of the V_i being non-isomorphic. In that case we can compute the direct sum decomposition of M by computing a maximal set of orthogonal primitive idempotents in the centre of the algebra $\mathrm{End}_G(M)$ (which consists of all linear maps $T : M \to M$ with $T(\sigma(v)) = \sigma(T(v))$ for $v \in M$ and $\sigma \in G$). It also follows that $\Lambda_{\mathbb{Q}} = V_{i_1} \oplus \ldots \oplus V_{i_k}$. Now for each V_i we do the following. For each element $(e_1, \ldots, e_n)$ in a basis of V_i, we check whether $\sum_i e_i \alpha_i = 0$, using Algorithm 1. Then Λ is equal to the direct sum of the V_i that pass this test.

5. *Degree* 4

Here we use the observations of the previous section to give a complete description of $\mathfrak{g}_F(X)$, where X is a semisimple 4×4-matrix, with irreducible characteristic polynomial.

Let $f = x^4 + ax^3 + bx^2 + cx + d$ be the characteristic polynomial of X, and suppose that it is irreducible. Let G denote the Galois group $\mathrm{Gal}(K/F)$, where K is the splitting field of f. We remark that if $F = \mathbb{Q}$ then it is straightforward to determine G — for example, by the procedure outlined in [**19**, Theorem 106] . Note that the case where $G = S_4, A_4$ is settled by Corollary 1.

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

PROPOSITION 1. *Suppose that G is not isomorphic to S_4 or A_4. Then*

1. *if $a = 0$ and $a^3 - 4ab + 8c \neq 0$, then $\mathfrak{g}_F(X) = \{X' \in A_F(X) \mid \mathrm{Tr}(X') = 0\}$;*
2. *if $a = 0$ and $a^3 - 4ab + 8c = 0$, then $\mathfrak{g}_F(X)$ is spanned by X, X^3;*
3. *if $a \neq 0$ and $a^3 - 4ab + 8c \neq 0$, then $\mathfrak{g}_F(X)$ is spanned by I, X, X^2, X^3;*
4. *if $a \neq 0$ and $a^3 - 4ab + 8c = 0$, then $\mathfrak{g}_F(X)$ is spanned by $I, X, X^2 + \frac{4}{3a}X^3$.*

Proof. Since G is a transitive permutation group on four points, not isomorphic to S_4, A_4, there remain the possibilities: $G \cong \mathbb{Z}/4\mathbb{Z}$, $G \cong D_8$ and $G \cong V_4$. These groups have respective generating sets $\{(1,2,3,4)\}$, $\{(1,2,3,4),(1,3)\}$, and $\{(1,2)(3,4),(1,4)(2,3)\}$. In the first two cases the module M_0 decomposes as a direct sum of two submodules with bases $\{(1,-1,1,-1)\}$, $\{(1,0,-1,0),(0,1,0,-1)\}$ (this holds for both cases). Now $\Lambda_{\mathbb{Q}}$ cannot contain the second module (as in that case some roots would be equal). If $G = V_4$, then M_0 decomposes as a direct sum of three submodules, respectively spanned by $(1,1,-1,-1)$, $(1,-1,1,-1)$ and $(1,-1,-1,1)$. The G-module $\Lambda_{\mathbb{Q}}$ cannot contain two of these vectors, as otherwise after adding it would follow that two roots were equal.

So in all cases, after maybe renumbering the roots, there are the following possibilities for $\Lambda_{\mathbb{Q}}$: $\Lambda_{\mathbb{Q}} = 0$, $\Lambda_{\mathbb{Q}}$ is spanned by $(1,1,1,1)$, or by $(1,1,1,1)$, $(1,1,-1,-1)$, or by $(1,1,-1,-1)$.

Let $\alpha_1, \ldots, \alpha_4$ be the roots of f. Set $a_1 = \alpha_1+\alpha_2-\alpha_3-\alpha_4$, $a_2 = \alpha_1-\alpha_2-\alpha_3+\alpha_4$ and $a_3 = \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4$. Then the product $a_1a_2a_3$ is a symmetric polynomial in the α_i; hence can be expressed in terms of the coefficients of f. It turns out that $-a_1a_2a_3 = a^3 - 4ab + 8c$. So this number is zero if and only if Λ contains $(1,1,-1,-1)$. This proves statements 1 and 3 (cf. Lemma 3).

Suppose that $a^3 - 4ab + 8c = 0$. Then we can assume that Λ contains $\underline{e} = (1,1,-1,-1)$. In order to obtain a basis of Υ (cf. Algorithm 4) we have to solve the equation $\sum_{i=0}^{3} \Delta_i(\underline{e})\gamma_i = 0$. Note that $\Delta_0(\underline{e}) = \Delta_1(\underline{e}) = 0$. We know that $\alpha_1+\alpha_2-\alpha_3-\alpha_4 = 0$, and also that $\alpha_1+\alpha_2+\alpha_3+\alpha_4 = -a$. These two relations are equivalent to $\alpha_1 + \alpha_2 + \frac{1}{2}a = 0$ and $\alpha_3 + \alpha_4 + \frac{1}{2}a = 0$. Now $\Delta_2(\underline{e}) = 2\alpha_2^2 + a\alpha_2 - 2\alpha_4^2 - a\alpha_4$ as the difference is equal to

$$\left(\alpha_1 - \alpha_2 - \tfrac{1}{2}a\right)\left(\alpha_1 + \alpha_2 + \tfrac{1}{2}a\right) + \left(-\alpha_3 + \alpha_4 + \tfrac{1}{2}a\right)\left(\alpha_3 + \alpha_4 + \tfrac{1}{2}a\right) = 0.$$

Similarly, $\Delta_3(\underline{e}) = -\frac{3}{4}a(2\alpha_2^2 + a\alpha_2 - 2\alpha_4^2 - a\alpha_4)$ as the difference is equal to

$$\begin{aligned}\left(\alpha_1^2 - \alpha_1\alpha_2 - \tfrac{1}{2}a\alpha_1 + \alpha_2^2 + a\alpha_2 + \tfrac{1}{4}a^2\right)\left(\alpha_1 + \alpha_2 + \tfrac{1}{2}a\right)\\ + \left(-\alpha_3^2 + \alpha_3\alpha_4 + \tfrac{1}{2}a\alpha_3 - \alpha_4^2 - a\alpha_4 - \tfrac{1}{4}a^2\right)\left(\alpha_3 + \alpha_4 + \tfrac{1}{2}a\right) = 0.\end{aligned}$$

From this it follows that $3a\Delta_2(\underline{e}) + 4\Delta_3(\underline{e}) = 0$. Furthermore,

$$\Delta_2(\underline{e}) = 2\alpha_2^2 + a\alpha_2 - 2\alpha_4^2 - a\alpha_4 = 2(\alpha_2 - \alpha_4)\left(\alpha_2 + \alpha_4 + \tfrac{1}{2}a\right).$$

From this we conclude that $\Delta_2(\underline{e}) \neq 0$. Indeed, $\alpha_2 - \alpha_4 \neq 0$ as f is irreducible. Secondly, $\alpha_2 + \alpha_4 = -\frac{1}{2}a$ would entail that $\alpha_1 - \alpha_4 = 0$ as $\alpha_1 + \alpha_2 = -\frac{1}{2}a$.

Suppose that $a \neq 0$. Then the equation

$$\sum_{i=0}^{3} \Delta_i(\underline{e})\gamma_i = 0$$

is equivalent to $(-\frac{4}{3a}\gamma_3 + \gamma_3)\Delta_3(\underline{e}) = 0$, and we have just seen that $\Delta_3(\underline{e}) \neq 0$. So $\gamma_3 = \frac{4}{3a}\gamma_2$, and statement 4 is proved.

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

If $a = 0$, then $\Delta_3(\underline{e}) = 0$ and the equation $\sum_i \Delta_i(\underline{e})\gamma_i = 0$ reduces to $\gamma_2 = 0$. Also, $\underline{e}' = (1, 1, 1, 1) \in \Lambda$. Then by adding $\underline{e}$ and $\underline{e}'$ we see that $\alpha_2 = -\alpha_1$ and $\alpha_4 = -\alpha_3$. So $\Delta_1(\underline{e}') = \Delta_3(\underline{e}') = 0$, and $\Delta_0(\underline{e}') = 4$. So we get the equation $4\gamma_0 = 0$. This proves statement 2. □

The calculations in the final part of the proof have been done with the help of MAGMA. Using similar calculations, more results of the same flavour can be derived. Without proof, we state the following result.

PROPOSITION 2. *Let X be a 6×6-matrix with irreducible characteristic polynomial $p = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$. Suppose that the Galois group has number 4, 6, 7, 8, or 11 in the classification of transitive groups in* MAGMA. *Set*

$$r_1 = c + \tfrac{5}{27}\left(a^3 - \tfrac{18}{5}ab\right) \qquad \text{and} \qquad r_2 = e - \tfrac{1}{81}a^5 + \tfrac{1}{27}a^3b - \tfrac{1}{3}ad.$$

Then

1. *if $r_1 = r_2 = 0$ and $a \neq 0$, then $\mathfrak{g}_F(X)$ is spanned by*
$$I, X, \frac{a}{2}X^2 + X^3, \frac{-5a^3}{54}X^2 + \frac{5a}{6}X^4 + X^5;$$
2. *if $r_1 = r_2 = a = 0$, then $\mathfrak{g}_F(X)$ is spanned by X, X^3, X^5;*
3. *if one of r_1, r_2 is nonzero, then $\mathfrak{g}_F(X)$ is equal to $A_F(X)$ if $a \neq 0$, and equal to $\{X' \in A(X_F) \mid \mathrm{Tr}(X') = 0\}$ if $a = 0$.*

6. *Examples*

To generate a set of input examples we used the database of polynomials over the rationals with given Galois groups by Klüners and Malle [14]. In this database the nth transitive permutation group on d points is denoted ${}_dT_n$. For each polynomial of degree d ($6 \leqslant d \leqslant 12$) with Galois group isomorphic to ${}_dT_n$, we computed the companion matrix X of f and used this as input to our algorithms. In Figure 1 we plot the running times for the computation of $\mathfrak{g}_{\mathbb{Q}}(X)$ using the algorithm in Section 3, both using an exact, algebraic representation of the splitting field of f as well as the algorithms of Section 2, against the logarithm of the group size. From the data presented, it is clear that the runtime of all three algorithms depends mainly on the size of the Galois group of f, that is, the degree of the splitting field. Also, clearly, the algebraic representation of the splitting field has the worst runtime behaviour. In Figure 2, we use a variation of the algorithms in Section 3, where instead of using the bounds from Algorithm 1, we compute the relations with a much smaller bound, and the 'verify' them using twice the p-adic precision. While this does not of course give guaranteed results, nevertheless, in all cases where the bounds were small enough to use them, the output obtained in this way was correct. Since this approach does not depend directly on the size of the splitting field, we can use this for larger degrees.

From both the figures we notice that for the purpose of computing algebraic hulls, it does not matter whether Algorithm 2 or 3 is used. For proven results, the time is always dominated by the proof step, while the actual computation takes only negligible time — even in large degrees and large Galois groups.

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

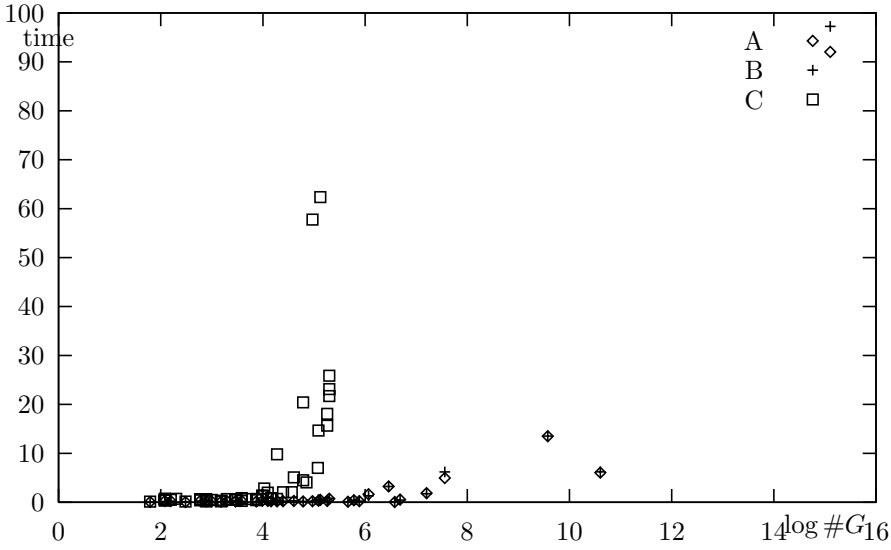

Figure 1: Time vs. $\log \#\,\mathrm{Gal}(f)$ for f of degree 6, 8, 9 and 10 and all transitive groups with proven bounds. **C** is used for data coming from the algebraic, exact representation of the splitting field, **B** is time using Algorithm 3, and **A** is that using Algorithm 2.

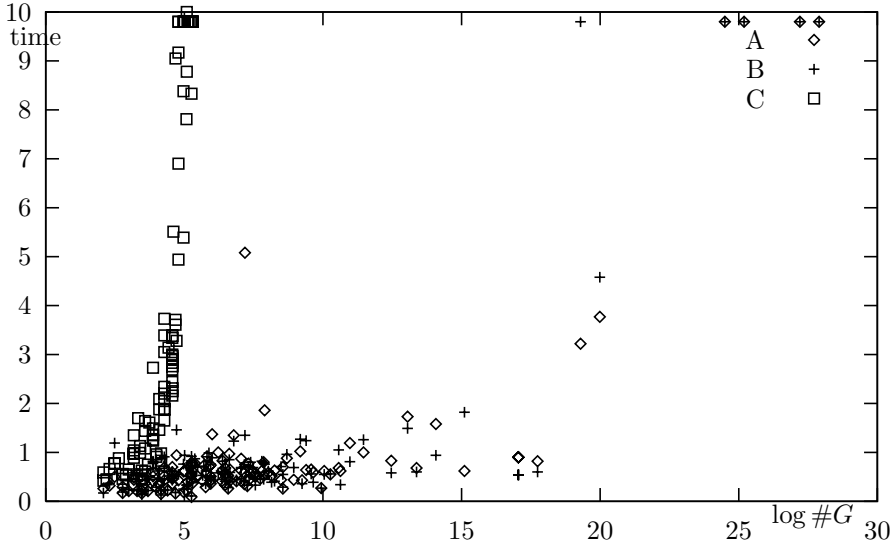

Figure 2: Time vs. $\log \#\,\mathrm{Gal}(f)$ for f of degree 6, 8, 9, 10, 12, 14 and 15 and all transitive groups, using heuristic bounds. **C** is used for data coming from the algebraic, exact representation of the splitting field, **B** is time using Algorithm 3, and **A** is that using Algorithm 2.

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

References

1. K. Belabas, 'A relative van Hoeij algorithm over number fields', *J. Symbolic Comput.* 37 (2004) 641–668. 278
2. A. Borel, *Linear algebraic groups*, 2nd edn (Springer, Berlin/Heidelberg/New York, 1991). 279
3. Wieb Bosma, John J. Cannon and Catherine Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) 235–266. 272
4. John J. Cannon, 'Magma', http://magma.maths.usyd.edu.au. 272
5. Claude Chevalley, *Théorie des groupes de Lie. Tome II. Groupes algébriques*. Actualités Sci. Ind. 1152 (Hermann & Cie., Paris, 1951). 271, 278, 279
6. Arjeh M. Cohen, Scott H. Murray and D. E. Taylor, 'Computing in groups of Lie type', *Math. Comp.* 73 (2004) 1477–1498 (electronic). 271
7. Henri Cohen, *A course in computational algebraic number theory*, 1st edn, Graduate Texts in Mathematics 138 (Springer, Berlin, 1993). 271, 275
8. Harm Derksen, Emmanuel Jeandel and Pascal Koiran, 'Quantum automata and algebraic groups', *J. Symbolic Comput.* 39 (2005) 357–371. 271
9. C. Fieker and C. Friedrichs, 'On reconstruction of algebraic numbers', *Proceedings of the 4th International Symposium* (*ANTS-IV*), Leiden, Netherlands, 2–7 July, 2000, ed. W. Bosma, Lecture Notes in Comput. Sci. 1838 (Springer, Berlin, 2000) 285–296. 278
10. K. Geissler, 'Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern', PhD Thesis, TU-Berlin, 2003. 278
11. Fritz Grunewald and Daniel Segal, 'Some general algorithms. I. Arithmetic groups', *Ann. of Math.* (2) 112 (1980) 531–583. 271
12. Gordon James and Martin Liebeck, *Representations and characters of groups*, 2nd edn (Cambridge University Press, New York, 2001). 282
13. Bettina Just, 'Integer relations among algebraic numbers', *Math. Comp.* 54 (1990) 467–477. 271
14. J. Klüners and G. Malle, 'A database for field extensions of the rationals', *LMS J. Comput. Math* 4 (2001) 182–196, http://www.lms.ac.uk/jcm/4/lms2001-004. 284
15. Serge Lang, *Algebraic number theory*, 2nd edn, Graduate Texts in Mathematics 110 (Springer, Berlin, 1994). 272
16. D. W. Masser, 'Linear relations in algebraic groups', *New advances in transencendence theory* (ed. Alan Baker, Cambridge University Press, New York, 1988) 248–262. 275
17. P. Nguyen and D. Stehlé, 'Floating-point LLL revisited', *Proceedings of Eurocrypt 2005*, Lecture Notes in Comput. Sci. 3494 (Springer, Berlin, 2005) 215–233. 276

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press

18. Guéna el Renault and Kazuhiro Yokoyama, 'A modular method for computing the splitting field of a polynomial', *Algorithmic Number Theory Symposium* (*ANTS VII*), ed. Florian Hess, Sebastian Pauli and Michael Pohst, Lecture Notes in Comput. Sci. 4076 (Springer, Berlin, 2006) 124–140. 272

19. Joseph Rotman, *Galois theory*, 2nd edn, Universitext (Springer, New York, 1998). 282

20. Eugene Schenkman, *Group theory* (D. Van Nostrand Co., Inc., Princeton, N.J./Toronto, Ont./London, 1965). 280

21. Jean-Pierre Serre, *Local fields* (Springer, Berlin, 1979). 272

Claus Fieker claus@maths.usyd.edu.au
http://magma.maths.usyd.edu.au/users/claus

School of Mathematics and Statistics
University of Sydney
Australia

Willem A. de Graaf degraaf@science.unitn.it
http://www.science.unitn.it/~degraaf/

Dipartimento di Matematica
Università di Trento
Italy

https://doi.org/10.1112/S1461157000001406 Published online by Cambridge University Press