Journal of Algebra 322 (2009) 3950–3970

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Constructing arithmetic subgroups of unipotent groups

Willem A. de Graaf [a,*], Andrea Pavan [b,1]

[a] Dipartimento di Matematica, University of Trento, Via Sommarive 14, 38050 Povo (Trento), Italy
[b] Dipartimento di Matematica Pura ed Applicata, University of Padova, Via Trieste 63, 35121 Padova, Italy

ARTICLE INFO

Article history:
Received 3 July 2008
Available online 8 April 2009
Communicated by Gunter Malle

Keywords:
Algebraic groups
Arithmetic groups
Lie algebras
Algorithms

ABSTRACT

Let G be a unipotent algebraic subgroup of some $\mathrm{GL}_m(\mathbb{C})$ defined over $\mathbb{Q}$. We describe an algorithm for finding a finite set of generators of the subgroup $G(\mathbb{Z}) = G \cap \mathrm{GL}_m(\mathbb{Z})$. This is based on a new proof of the result (in more general form due to Borel and Harish-Chandra) that such a finite generating set exists.

1. Introduction

Let G be an algebraic subgroup of $\mathrm{GL}_m(\mathbb{C})$ defined over $\mathbb{Q}$, where $m \geqslant 1$. Then for a subring R of $\mathbb{C}$ we set

$$G(R) = G \cap \mathrm{GL}_m(R).$$

The group $G(\mathbb{Z})$ and any other subgroup Γ of $G(\mathbb{Q})$ commensurable with it are called arithmetic subgroups of G.

Arithmetic groups occur in many contexts. Examples are: the automorphism group of a finitely generated nilpotent group (see [10], Chapter 6), the group of units of the ring of integers of a number field, and the group of units of the group algebra $\mathbb{Z}\mathcal{G}$, where $\mathcal{G}$ is a finite group. A celebrated theorem of Borel and Harish-Chandra [3] says that arithmetic groups are finitely generated. In this paper we consider the problem of computing a finite set of generators of an arithmetic subgroup of a unipotent group.

This problem was also treated in the paper [9] by Grunewald and Segal, where a general algorithm for all arithmetic groups was outlined. However, their declared aim was to show that such a computa-

* Corresponding author.
E-mail addresses: degraaf@science.unitn.it (W.A. de Graaf), pan@math.unipd.it (A. Pavan).

[1] The author would like to thank the University of Trento for its hospitality during 2008, when the work on the paper was carried out.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.03.027

tion is, at least in principle, feasible, and no attempt was made to make the algorithms efficient. And unfortunately their algorithm appears to be unsuited for practical computation. Indeed, one step (i.e., Algorithm 4.2.2) of the algorithm for the unipotent case requires the enumeration of a set of size at least $(2(m!(1+\Delta)^m+1))^{m^2}$, where Δ is a non-negative integer. This is impractical, even for small m.

In this paper we describe a practical algorithm for finding a finite set of generators of $G(\mathbb{Z})$, in case G is unipotent, that is to say, all its elements are unipotent matrices. As a byproduct this yields an independent proof of the Borel–Harish-Chandra theorem in this case. Also, we can show that the groups $G(\mathbb{Z})$ are $\mathfrak{T}$-groups of Hirsch length equal to $\dim G$. In order to show that the algorithm can be used to compute practical examples, we have implemented it in the language of the computer algebra system GAP4 (cf. [8]). However, we do remark that our algorithm, in the worst case, has a time complexity that is exponential in m.

We now sketch the main idea of the algorithm. Let V be the vector space on which G acts naturally. Let

$$0 = V_0 < V_1 < \cdots < V_n = V$$

be a flag of V with respect to the action of G (this means that for $v \in V_i$ and $g \in G$ we have $gv \equiv v \bmod V_{i-1}$). Then we can form the G-module $V^\star = V_{n-1} \oplus \frac{V}{V_1}$. In informal terms the matrix of a $g \in G$ acting on $V^\star$ is formed from the matrix of its action on V by taking the block in the upper left part of the matrix, and the block in the bottom right part of the matrix, and constructing the block matrix consisting of these two blocks. Now let Q be the image of G in $\mathrm{GL}(V^\star)$; then we can recursively compute generators of $Q(\mathbb{Z})$. The recursion works because the Q-flag in $V^\star$ has smaller length. Let $\pi : G \to Q$ be the projection. In Section 2 we describe $\pi(G(\mathbb{Z}))$ (Proposition 2.7). We show how to find generators of $\pi(G(\mathbb{Z}))$, and their preimages in $G(\mathbb{Z})$. Let $N(\mathbb{Z}) \subset G(\mathbb{Z})$ denote the kernel of π. We find a finite set of generators of $N(\mathbb{Z})$, and joined to the elements of $G(\mathbb{Z})$ found earlier this solves the problem.

These ideas are detailed in Section 2. In Section 3 we illustrate them with a simple example. The constructions of Section 2 do not immediately yield an implementable algorithm. In order to obtain that we need some technical preparation. In Section 4 we describe some results that allow us to work with the Lie algebra of G rather than with G itself. Section 5 contains some material on $\mathfrak{T}$-groups. In Section 6 we describe some algorithms for lattices that we need. Then in Section 7 we give a detailed description of the main algorithm, and prove its correctness. The last section describes some practical experiences with our implementation of this algorithm in GAP4.

2. The derived representation

The goal of this section is to introduce some notation, and to prove the results that underpin the main algorithm.

Let V be a finite-dimensional vector space over $\mathbb{Q}$, and L a full-dimensional lattice of V. We do not prove the next lemma here; it will follow from Lemma 6.3.

Lemma 2.1. *Let U and W be two subspaces of V with $U \subseteq W$. Then there exist subspaces U' and W' of V such that*

$$W' \subseteq U'$$

and equalities

$$U \oplus U' = V = W \oplus W'$$

and

$$(L \cap U) + (L \cap U') = L = (L \cap W) + (L \cap W')$$

hold.

In the notations of the lemma above, we say that $W' \subseteq U'$ is a system of L-complements for $U \subseteq W$.

Now let

$$0 = V_0 < V_1 < \cdots < V_n = V$$

be a chain of subspaces of V with $n \geqslant 1$. Then we consider the vector space

$$V^\star = V_{n-1} \oplus \frac{V}{V_1}.$$

We call it the derived vector space. Also, we have the full-dimensional lattice

$$L^\star = (L \cap V_{n-1}) + \frac{L + V_1}{V_1}$$

of $V^\star$, which we call the derived lattice, and the chain of subspaces

$$0 = V_0^\star < V_1^\star < \cdots < V_{n-1}^\star = V^\star$$

of $V^\star$ where

$$V_i^\star = V_i \oplus \frac{V_{i+1}}{V_1}$$

which we call the derived chain. Note that its length is $n-1$, which is strictly less than the length of the chain of V.

Now let $W_{n-1} \subseteq W_1$ be a system of L-complements to $V_1 \subseteq V_{n-1}$, and let us denote by $V \xrightarrow{\xi} V_1$ the projection of V onto V_1 along W_1. By $\mathrm{Hom}(W_{n-1}, V_1)$ we denote the space of all linear maps $W_{n-1} \to V_1$. Then we consider the map

$$\epsilon : \mathrm{End}(V) \longrightarrow \mathrm{Hom}(W_{n-1}, V_1), \qquad \varphi \mapsto \xi \circ \varphi_{|W_{n-1}}. \tag{1}$$

We refer to it as the error map induced by the system $W_{n-1} \subseteq W_1$. Further we define

$$\Gamma = \bigl\{\gamma \in \mathrm{Hom}(W_{n-1}, V_1) \bigm| \gamma(L \cap W_{n-1}) \subseteq L \cap V_1\bigr\}. \tag{2}$$

Since $L \cap W_{n-1}$ is full-dimensional in W_{n-1}, Γ is a lattice of $\mathrm{Hom}(W_{n-1}, V_1)$, and it is full-dimensional since $L \cap V_1$ is full-dimensional in V_1. We refer to it as the lattice induced by the system $W_{n-1} \subseteq W_1$.

Now let G be a unipotent algebraic group defined over $\mathbb{Q}$ acting faithfully on V, and suppose that

$$0 = V_0 < V_1 < \cdots < V_n = V$$

is a flag of V with respect to G, i.e., for all $v \in V_i$ we have $gv \equiv v \bmod V_{i-1}$ for all $g \in G$. We consider the subgroup

$$G_L = \bigl\{g \in G(\mathbb{Q}) \bigm| gL = L\bigr\}$$

of $G(\mathbb{Q})$. We want to find a finite set of generators of this group.

Since V_1 and V_{n-1} are G-stable subspaces of V, G acts on both V_{n-1} and $\frac{V}{V_1}$, hence on their direct sum, that is to say, on the derived vector space. We refer to the action of G on $V^\star$ as the derived action. Further, we denote by N its kernel, which is of course a unipotent algebraic group over $\mathbb{Q}$ acting faithfully on V, by Q its image, which is a unipotent algebraic group over $\mathbb{Q}$ acting faithfully on $V^\star$, and by π the projection of G onto Q. The following lemma is well known; it follows directly from the commutativity of diagram (3) in Section 4.

Lemma 2.2. *The projection π maps $G(\mathbb{Q})$ surjectively onto $Q(\mathbb{Q})$.*

Also we set

$$N_L = \{g \in N(\mathbb{Q}) \mid gL = L\}$$

and

$$Q_{L^\star} = \{q \in Q(\mathbb{Q}) \mid qL^\star = L^\star\}.$$

Of course the derived chain is a flag for $V^\star$ with respect to the action of Q. Since G acts faithfully on V we can regard elements in $G(\mathbb{Q})$ as automorphisms of V. The same consideration applies to elements of $N(\mathbb{Q})$. So we can apply the map ϵ to the elements of these groups.

Proposition 2.3. *For every $g \in G(\mathbb{Q})$ and $h \in N(\mathbb{Q})$ we have*

$$\epsilon(g \cdot h) = \epsilon(g) + \epsilon(h),$$

where ϵ is as in (1)*.*

Proof. Let $v \in W_{n-1}$. Since h is an automorphism of V acting as the identity on $\frac{V}{V_1}$,

$$h(v) - v \in V_1.$$

Further, g is an automorphism of V acting as the identity on V_1, hence

$$g\big(h(v) - v\big) = h(v) - v.$$

Since $W_{n-1} \subseteq W_1$, we have $\xi(v) = 0$. Hence applying ξ to both sides of the previous identity and using linearity we obtain

$$\xi \circ g \circ h(v) = \xi \circ g(v) + \xi \circ h(v)$$

hence the thesis. $\square$

Of course, $N(\mathbb{Q})$ acts on $G(\mathbb{Q})$ by multiplication on the right. Once we endow $\mathrm{Hom}(W_{n-1}, V_1)$ with the obvious group structure given by addition, the previous proposition implies that the restriction of ϵ to $N(\mathbb{Q})$ is a group morphism. Hence $N(\mathbb{Q})$ acts on $\mathrm{Hom}(W_{n-1}, V_1)$ by

$$\mathrm{Hom}(W_{n-1}, V_1) \times N(\mathbb{Q}) \to \mathrm{Hom}(W_{n-1}, V_1), \qquad (x, h) \mapsto x + \epsilon(h).$$

With these observations, we can restate the previous proposition saying that the restriction of ϵ to $G(\mathbb{Q})$ is a morphism of $N(\mathbb{Q})$-sets.

Now let us denote by W the image of $N(\mathbb{Q})$ under ϵ. Then Proposition 2.3 gives us:

Corollary 2.4. *There exists a unique map $\hat{\epsilon} : Q(\mathbb{Q}) \longrightarrow \frac{\mathrm{Hom}(W_{n-1}, V_1)}{W}$ such that the diagram*

$$\begin{tikzcd} G(\mathbb{Q}) \arrow[r, "\epsilon"] \arrow[d, "\pi"] & \mathrm{Hom}(W_{n-1}, V_1) \arrow[d] \\ Q(\mathbb{Q}) \arrow[r, "\hat{\epsilon}"] & \frac{\mathrm{Hom}(W_{n-1}, V_1)}{W} \end{tikzcd}$$

is commutative.

Proof. By Lemma 2.2, the map $\pi : G(\mathbb{Q}) \to Q(\mathbb{Q})$ is surjective. Also, if $g, g' \in G(\mathbb{Q})$ are such that $\pi(g) = \pi(g')$ then $g^{-1}g' \in N(\mathbb{Q})$, hence due to Proposition 2.3 we obtain

$$\epsilon(g') = \epsilon\big(gg^{-1}g'\big) = \epsilon(g) + \epsilon\big(g^{-1}g'\big)$$

thus

$$\epsilon(g) + W = \epsilon(g') + W.$$

These two facts show that the function

$$\hat{\epsilon} : Q(\mathbb{Q}) \longrightarrow \frac{\mathrm{Hom}(W_{n-1}, V_1)}{W}, \qquad q \mapsto \epsilon(g) + W$$

where g is any element of $G(\mathbb{Q})$ such that $\pi(g) = q$, is well defined and, of course, it makes the diagram above commutative. If $\hat{\epsilon}'$ is another such a function, then

$$\hat{\epsilon} \circ \pi = \hat{\epsilon}' \circ \pi$$

hence, by surjectivity of π it follows that $\hat{\epsilon}' = \hat{\epsilon}$. $\square$

Also we set

$$G_{L^\star} = \big\{g \in G(\mathbb{Q}) \bigm| gL^\star = L^\star\big\}.$$

In other words, an element $g \in G(\mathbb{Q})$ lies in $G_{L^\star}$ if and only if $\pi(g)$ lies in $Q_{L^\star}$. Of course, $G_{L^\star}$ contains both G_L and $N(\mathbb{Q})$.

Lemma 2.5. *Let $g \in G_{L^\star}$. Then $g \in G_L$ if and only if $\epsilon(g) \in \Gamma$.*

Proof. If $g \in G_L$ then $g(L \cap W_{n-1}) \subseteq L$, hence

$$\xi \circ g(L \cap W_{n-1}) \subseteq \xi(L) = \xi\big((L \cap V_1) \oplus (L \cap W_1)\big) = L \cap V_1$$

hence $\epsilon(g) \in \Gamma$.

Now let $g \in G_{L^\star}$ such that $\epsilon(g) \in \Gamma$. Then g is an automorphism of V fixing both $L + V_1$ and $L \cap V_{n-1}$, and such that $\xi \circ g$ sends $L \cap W_{n-1}$ in $L \cap V_1$. In particular, since the preimage of $L \cap V_1$ under ξ is $W_1 + (L \cap V_1)$, we have that $g(L \cap W_{n-1}) \subseteq W_1 + (L \cap V_1)$. Further, since $L \cap W_{n-1} \subseteq L + V_1$ and g fixes $L + V_1$, we have that $g(L \cap W_{n-1}) \subseteq L + V_1$. Hence

$$g(L \cap W_{n-1}) \subseteq (L + V_1) \cap \big(W_1 + (L \cap V_1)\big).$$

Since $L=(L\cap V_1)+(L\cap W_1)$, applying Dedekind's modular law we obtain equality

$$L=(L+V_1)\cap\big(W_1+(L\cap V_1)\big)$$

hence $g(L\cap W_{n-1})\subseteq L$. Since $L=(L\cap V_{n-1})+(L\cap W_{n-1})$ and g fixes $L\cap V_{n-1}$, this shows that $g(L)\subseteq L$. Now let $l\in L$. Since g fixes V_1+L, there exist $l_1\in V_1$ and $l_2\in L$ such that $g(l_1)+g(l_2)=l$. Since $g(L)\subseteq L$, we have that $g(l_2)\in L$, hence in particular that $g(l_1)=l-g(l_2)\in L$. Since g fixes V_1, we also have that $g(l_1)\in V_1$, hence $g(l_1)\in L\cap V_1$. Since $V_1\subseteq V_{n-1}$, also $g(l_1)\in L\cap V_{n-1}$ holds. Since g fixes $L\cap V_{n-1}$, we obtain that $l_1\in L\cap V_{n-1}$, hence $l_1+l_2\in L$, hence $L\subseteq g(L)$. So $g\in G_L$. □

Proposition 2.6. *The map given by the chain*

$$G_{L^\star}\xrightarrow{\epsilon}\mathrm{Hom}(W_{n-1},V_1)\longrightarrow\frac{\mathrm{Hom}(W_{n-1},V_1)}{\Gamma}$$

is a group morphism with kernel G_L.

Proof. Let $f,g\in G_{L^\star}$. Then they are automorphisms of V acting as the identity on V_1, fixing V_{n-1} and acting as the identity on $\frac{V}{V_{n-1}}$. Further, they fix $L\cap V_{n-1}$ and $L+V_1$. Now let $l\in L$. Of course, $g(l)-l\in V_{n-1}\cap(L+V_1)$. Since $V_1\subseteq V_{n-1}$, applying Dedekind's modular law we obtain $V_{n-1}\cap(L+V_1)=V_1+(L\cap V_{n-1})$, which shows that

$$f\big(g(l)-l\big)-\big(g(l)-l\big)\in L\cap V_{n-1}$$

hence

$$f\circ g(l)-f(l)-g(l)\in L.$$

Since $\xi(L)=L\cap V_1$, we finally obtain

$$\xi\circ f\circ g(l)-\xi\circ f(l)-\xi\circ g(l)\in L\cap V_1$$

which shows that the map is a group morphism. By Lemma 2.5, its kernel is G_L. □

Proposition 2.7. *Let $\hat\epsilon$ be as in Corollary 2.4. The map Ψ given by the chain*

$$Q_{L^\star}\xrightarrow{\hat\epsilon}\frac{\mathrm{Hom}(W_{n-1},V_1)}{W}\longrightarrow\frac{\mathrm{Hom}(W_{n-1},V_1)}{W+\Gamma}$$

is a group morphism. Its kernel is equal to the image of G_L under π.

Proof. Since $\pi:G(\mathbb{Q})\to Q(\mathbb{Q})$ is surjective and $g\in G(\mathbb{Q})$ is in $G_{L^\star}$ if and only if $\pi(g)\in Q_{L^\star}$, we obtain a surjective map $\pi:G_{L^\star}\to Q_{L^\star}$. By commutativity of the diagram in Corollary 2.4, we also obtain the commutative diagram

$$\begin{tikzcd}
G_{L^\star} \arrow[r, "\epsilon"] \arrow[d, "\pi"] & \mathrm{Hom}(W_{n-1},V_1) \arrow[r] & \frac{\mathrm{Hom}(W_{n-1},V_1)}{\Gamma} \arrow[d] \\
Q_{L^\star} \arrow[rr, "\Psi"] & & \frac{\mathrm{Hom}(W_{n-1},V_1)}{\Gamma+W}
\end{tikzcd}$$

By Proposition 2.6, the top row is a group morphism, hence also the bottom row is. Again by Proposition 2.6, G_L is the kernel of the top row. Hence, since the diagram above is commutative, the image of G_L under π lies in the kernel of Ψ. Now let q be in the kernel of Ψ, and let $g \in G_{L^\star}$ be a preimage of q under π. By commutativity of the diagram above, we have

$$\epsilon(g) \in \Gamma + W.$$

Now let $w \in W$ such that $\epsilon(g) + w \in \Gamma$. Since W is the image of $N(\mathbb{Q})$ under ϵ, there exists $h \in N(\mathbb{Q})$ such that $\epsilon(h) = w$. Hence by Proposition 2.3 we have

$$\epsilon(g \cdot h) = \epsilon(g) + \epsilon(h) \in \Gamma$$

thus by Lemma 2.5 we obtain that $g \cdot h \in G_L$. Of course, $\pi(g \cdot h) = q$. $\square$

3. An example

Let us consider

$$G = \left\{ \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & \frac{1}{2}c^2 \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{C}) \text{ such that } a, b, c \in \mathbb{C} \right\}.$$

It is easy to check that G is an algebraic subgroup of $\mathrm{GL}_4(\mathbb{C})$ defined over $\mathbb{Q}$. Since it is contained in the set of upper-unitriangular matrices of $\mathrm{GL}_4(\mathbb{C})$, it is unipotent. In this example it is rather straightforward to find a set of generators of $G(\mathbb{Z})$ directly. However, in this section we illustrate the results of the previous section by showing how they help us finding a finite set of generators for $G(\mathbb{Z})$.

G acts faithfully on $\mathbb{Q}^4$ by matrix–vector multiplication; also, $\mathbb{Z}^4$ is a full-dimensional lattice of $\mathbb{Q}^4$. Thus we can consider the subgroup $G_{\mathbb{Z}^4}$ of G, and it is easily seen that

$$G(\mathbb{Z}) = G_{\mathbb{Z}^4}.$$

The chain of subspaces

$$0 = V_0 < \langle e_1, e_2 \rangle = V_1 < \langle e_1, e_2, e_3 \rangle = V_2 < V_3 = \mathbb{Q}^4$$

where e_1, e_2, e_3 and e_4 are the standard basis of $\mathbb{Q}^4$, is a flag of V with respect to the action of G. The derived vector space has basis given by $(e_1, 0)$, $(e_2, 0)$, $(e_3, 0)$, $(0, e_3 + V_1)$ and $(0, e_4 + V_1)$; through this basis we can identify it with $\mathbb{Q}^5$, and under this identification the derived lattice corresponds to $\mathbb{Z}^5$. The kernel of the derived action is

$$N = \left\{ \begin{pmatrix} 1 & 0 & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{C}) \text{ such that } b \in \mathbb{C} \right\}.$$

In particular,

$$N_{\mathbb{Z}^4} = \left\{ \begin{pmatrix} 1 & 0 & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{C}) \text{ such that } b \in \mathbb{Z} \right\}$$

and it is straightforward to check that it is an infinite cyclic group with generator

$$n=\begin{pmatrix}1&0&0&1\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

The subgroup

$$Q=\left\{\left(\begin{array}{ccc|cc}1&0&a&0&0\\0&1&c&0&0\\0&0&1&0&0\\\hline 0&0&0&1&c\\0&0&0&0&1\end{array}\right)\in \mathrm{GL}_5(\mathbb{C}) \text{ such that } a,c\in\mathbb{C}\right\}$$

of $\mathrm{GL}_5(\mathbb{C})$ is the image of the derived action, the projection of G onto Q being

$$\pi: G\to Q,\qquad \begin{pmatrix}1&0&a&b\\0&1&c&\frac{1}{2}c^2\\0&0&1&c\\0&0&0&1\end{pmatrix}\mapsto \left(\begin{array}{ccc|cc}1&0&a&0&0\\0&1&c&0&0\\0&0&1&0&0\\\hline 0&0&0&1&c\\0&0&0&0&1\end{array}\right).$$

Now $Q_{\mathbb{Z}^5}$ is a torsion free abelian group of rank 2 with basis given by

$$q_1=\left(\begin{array}{ccc|cc}1&0&1&0&0\\0&1&0&0&0\\0&0&1&0&0\\\hline 0&0&0&1&0\\0&0&0&0&1\end{array}\right),\qquad q_2=\left(\begin{array}{ccc|cc}1&0&0&0&0\\0&1&1&0&0\\0&0&1&0&0\\\hline 0&0&0&1&1\\0&0&0&0&1\end{array}\right).$$

A system of $\mathbb{Z}^4$-complements for $V_1\subseteq V_2$ is given by $W_2\subseteq W_1$ where

$$W_2=\langle e_4\rangle,\qquad W_1=\langle e_3,e_4\rangle.$$

Using the basis e_4 for W_2 and the basis e_1, e_2 for V_1 we can identify $\mathrm{Hom}(W_2,V_1)$ with $\mathrm{M}_{2\times 1}(\mathbb{Q})$; under this identification, the induced lattice Γ corresponds to $\mathrm{M}_{2\times 1}(\mathbb{Z})$. Further, using the standard basis of $\mathbb{Q}^4$ we can identify $\mathrm{End}(\mathbb{Q}^4)$ with $\mathrm{M}_{4\times 4}(\mathbb{Q})$. In this way, the error map is

$$\epsilon: \mathrm{M}_{4\times 4}(\mathbb{Q})\to \mathrm{M}_{2\times 1}(\mathbb{Q}),\qquad \begin{pmatrix}a_{1,1}&a_{1,2}&a_{1,3}&a_{1,4}\\a_{2,1}&a_{2,2}&a_{2,3}&a_{2,4}\\a_{3,1}&a_{3,2}&a_{3,3}&a_{3,4}\\a_{4,1}&a_{4,2}&a_{4,3}&a_{4,4}\end{pmatrix}\mapsto\begin{pmatrix}a_{1,4}\\a_{2,4}\end{pmatrix}.$$

The image of the rational points of N under ϵ is the subspace of $\mathrm{M}_{2\times 1}(\mathbb{Q})$ generated by $\binom{1}{0}$. So in the notation of Section 2 we have $W=\langle\binom{1}{0}\rangle$ and $\Gamma=\mathrm{M}_{2\times 1}(\mathbb{Z})$. Furthermore, the map Ψ from Proposition 2.7 goes from the rational points of Q to $\frac{\mathrm{M}_{2\times 1}(\mathbb{Q})}{W+\Gamma}$.

Now we need two matrices g_1 and g_2 in $G(\mathbb{Q})$ whose images under π are q_1 and q_2, respectively. Their existence is guaranteed by the surjectivity of π. For example, we can take

$$g_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & \frac{1}{2} \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

This shows in particular that g_1 and g_2 are in $G_{\mathbb{Z}^5}$. Also, using commutativity of the diagram in Corollary 2.4, we have that

$$\Psi(q_1) = 0 + W + \Gamma, \qquad \Psi(q_2) = \begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix} + W + \Gamma.$$

Now the kernel of Ψ is generated by q_1 and q_2^2. Therefore, by Proposition 2.7, $\pi(G_{\mathbb{Z}^4})$ is generated by q_1 and q_2^2. Their preimages, g_1 and g_2^2 are only guaranteed to lie in $G_{\mathbb{Z}^5}$; however, here we see that they are already in $G_{\mathbb{Z}^4}$. Now the kernel of π restricted to $G_{\mathbb{Z}^4}$ is $N_{\mathbb{Z}^4}$. So $g_1 N_{\mathbb{Z}^4}$ and $g_2^2 N_{\mathbb{Z}^4}$ generate $\frac{G_{\mathbb{Z}^4}}{N_{\mathbb{Z}^4}}$. We conclude that n, g_1, g_2^2 generate $G_{\mathbb{Z}^4}$.

Of course we could have made a different choice for the preimages of q_1 and q_2. For example, we could have taken

$$g_1' = \begin{pmatrix} 1 & 0 & 1 & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

instead of g_1. Then g_1' is in $G_{\mathbb{Z}^5}$ but it is not in $G_{\mathbb{Z}^4}$. However, since q_1 is in the kernel of Ψ, we get $\hat{\epsilon}(q_1) \in W + \Gamma$ and by the commutativity of the diagram in Corollary 2.4, $\epsilon(g_1') \in W + \Gamma$. This can of course also be checked directly as

$$\epsilon(g_1') = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}.$$

Now we note that

$$n' = \begin{pmatrix} 1 & 0 & 0 & \frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in N(\mathbb{Q}) \quad \text{with} \quad \epsilon(n') = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}.$$

The existence of such an n' is guaranteed by the fact that W is the image of the rational points of N under ϵ. Since N is in the kernel of π we have $\pi(g_1' \cdot (n')^{-1}) = \pi(g_1') = q_1$. So we can work with $g_1'(n')^{-1}$ as preimage of q_1. This choice of preimage works for us since by Proposition 2.3 we have that

$$\epsilon\big(g_1' \cdot (n')^{-1}\big) = \epsilon\big(g_1'\big) - \epsilon(n') = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix} - \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \in \Gamma.$$

Hence $g_1'(n')^{-1} \in G_{\mathbb{Z}^4}$ and we can apply the same considerations as above to prove that n, $g_1'(n')^{-1}$ and g_2^2 are a generating set for $G_{\mathbb{Z}^4}$. As a matter of coincidence, we note that

$$g_1' \cdot (n')^{-1} = g_1.$$

Finally we note that n commutes with both g_1 and g_2^2, hence the chain of subgroups

$$1 < \langle n \rangle < \langle n, g_1 \rangle < \langle n, g_1, g_2^2 \rangle = G_{\mathbb{Z}^4}$$

is a central series for $G_{\mathbb{Z}^4}$ with infinite cyclic factors.

4. The Lie algebra connection

Let $G \subset \mathrm{GL}_m(\mathbb{C})$ be a unipotent algebraic group. As illustrated in Section 3, the results in Section 2 in principle yield an algorithm for finding a finite set of generators of $G(\mathbb{Z})$. However, to make it work efficiently in practice we rather work with the Lie algebra of G than with G itself. In this section we describe the main results that we need for that.

First we review some standard facts on the Lie algebra of an algebraic group; for more details we refer to [2,5,12,13].

As customary we denote the Lie algebras of the algebraic groups $G, H, \ldots$ by $\mathfrak{g}, \mathfrak{h}, \ldots$. Let G be a unipotent algebraic group defined over $\mathbb{Q}$, acting on a vector space V. Then $\mathfrak{g}$ also acts on V. Furthermore, G is connected, and hence a subspace $U \subset V$ is G-stable if and only if it is $\mathfrak{g}$-stable. If this is the case then we get a G-action and a $\mathfrak{g}$-action on U, and those are compatible, in the sense that the corresponding $\mathfrak{g}$-representation is the differential of the G-representation. Similarly we get compatible G- and $\mathfrak{g}$-actions on quotients and direct sums of modules.

An important role in our algorithm is played by the exponential mapping. For a nilpotent $x \in \mathfrak{gl}_m(\mathbb{C})$ we set

$$\exp(x) = \sum_{i=0}^{n-1} \frac{x^i}{i!},$$

and for a unipotent $u \in \mathrm{GL}_m(\mathbb{C})$,

$$\log(u) = \sum_{i=1}^{n-1} (-1)^{i-1} \frac{(u-1)^i}{i}.$$

Since G is defined over $\mathbb{Q}$ we have that $\mathfrak{g} \subset \mathfrak{gl}_m(\mathbb{C})$ has a basis such that all elements have coefficients in $\mathbb{Q}$. The $\mathbb{Q}$-span of such a basis is denoted $\mathfrak{g}_{\mathbb{Q}}$. Then it is well known that the maps $\exp : \mathfrak{g}_{\mathbb{Q}} \to G(\mathbb{Q})$ and $\log : G(\mathbb{Q}) \to \mathfrak{g}_{\mathbb{Q}}$ are mutually inverse. In particular, when we work with the Lie algebra $\mathfrak{g}_{\mathbb{Q}}$ we keep control over the elements of $G(\mathbb{Q})$ by these mappings.

Now let W be another finite-dimensional vector space over $\mathbb{Q}$, H a unipotent algebraic subgroup of $\mathrm{GL}(W)$, and $\varphi : G \to H$ a morphism of algebraic groups. Then we have the diagram

$$\begin{tikzcd} G(\mathbb{Q}) \arrow[r, bend left, "\log"] \arrow[d, "\varphi"] & \mathfrak{g} \arrow[l, bend left, "\exp"] \arrow[d, "\mathrm{d}\varphi"] \\ H(\mathbb{Q}) \arrow[r, bend left, "\log"] & \mathfrak{h} \arrow[l, bend left, "\exp"] \end{tikzcd} \tag{3}$$

and it turns out that it is commutative, i.e., $\exp(\mathrm{d}\varphi(x)) = \varphi(\exp(x))$ for all $x \in \mathfrak{g}$ (cf. [5], Chapter V, §4, Proposition 15).

Now we return to the setting of Section 2. A sequence of subspaces

$$0 = V_0 < V_1 < \cdots < V_n = V$$

is a flag for the action of G if and only if it is a flag for the action of $\mathfrak{g}$. (The latter means that $\mathfrak{g} \cdot V_i \subset V_{i-1}$ for $i > 0$.) In particular, $\mathfrak{g}$ acts on the derived vector space $V^\star$, and the corresponding representation of $\mathfrak{g}$ is the differential of the representation of G on $V^\star$. In particular this means that $\mathfrak{n}$, which is the Lie algebra of N, is the kernel of $\mathrm{d}\pi$ and $\mathfrak{q} = \mathrm{d}\pi(\mathfrak{g})$, where $\mathfrak{q}$ is the Lie algebra of Q.

Proposition 4.1. $\mathfrak{n}$ *is central in* $\mathfrak{g}$.

Proof. Let $x \in \mathfrak{g}$ and $y \in \mathfrak{n}$. Then x is an endomorphism of V such that $x.V \subseteq V_{n-1}$ and $x.V_1 = 0$, and y is an endomorphism of V such that $y.V \subseteq V_1$ and $y.V_{n-1} = 0$. Now let $v \in V$. Then $y.v \in V_1$, hence $x.y.v = 0$. Also, $y.v \in V_1$, hence $x.y.v = 0$. Thus $[x, y].v = 0$. Since $\mathfrak{g}$ acts faithfully on V, $[x, y] = 0$. □

Now let L be a full-dimensional lattice of V, $W_{n-1} \subseteq W_1$ a system of L-complements to $V_1 \subseteq V_{n-1}$, and let us denote by ϵ and by Γ the induced error map and the induced lattice, respectively. Since $\mathfrak{g}$ acts faithfully on V, we can regard its elements as endomorphisms of V. The same consideration applies to $\mathfrak{n}$. So we can consider the restriction of the map ϵ to $\mathfrak{g}$ and $\mathfrak{n}$.

Proposition 4.2. *The restriction of the induced map ϵ to $\mathfrak{n}$ is injective.*

Proof. Let $x \in \mathfrak{n}$ such that $\epsilon(x) = 0$. Since $x(V) \subseteq V_1$, for every $v \in V$ we have

$$x(v) = \xi \circ x(v).$$

Since $\epsilon(x) = 0$, $\xi \circ x(W_{n-1}) = 0$. Hence $x(W_{n-1}) = 0$. Since $x(V_{n-1}) = 0$, we finally have $x(V) = 0$. □

Further, we define

$$\mathfrak{n}_L = \bigl\{ x \in \mathfrak{n} \bigm| \epsilon(x) \in \Gamma \bigr\}.$$

By the previous proposition, it is a full-dimensional lattice of $\mathfrak{n}$. Since $\mathfrak{n}$ acts faithfully on V and V admits a flag with respect to this action, then $\mathfrak{n}$, regarded as a Lie subalgebra of $\mathfrak{gl}(V)$, consists of nilpotent endomorphisms. Hence we can consider the diagram

$$\begin{tikzcd} \mathfrak{n} \arrow[r, "\exp"] \arrow[dr, "\epsilon"'] & \mathrm{GL}(V) \arrow[d, "\epsilon"] \\ & \mathrm{Hom}(W_{n-1}, V_1) \end{tikzcd}$$

Proposition 4.3. *The diagram above is commutative.*

Proof. Let us denote by id_V the identity endomorphism of V. Since $W_{n-1} \subseteq W_1$, $\epsilon(\mathrm{id}_V) = 0$. Now let $x \in \mathfrak{n}$. Then $x(V) \subseteq V_1$ and $x(V_{n-1}) = 0$, hence $x^2(V) = 0$, and

$$\exp x = \mathrm{id}_V + x.$$

Thus

$$\epsilon(\exp x) = \epsilon(\mathrm{id}_V + x) = \epsilon(\mathrm{id}_V) + \epsilon(x) = \epsilon(x). \qquad \square$$

5. $\mathfrak{T}$-groups

The groups $G(\mathbb{Z})$ that we are after are finitely-generated nilpotent and torsion free. Such groups are called $\mathfrak{T}$-groups in the literature (cf. [10]). In this section we review some facts that we need on $\mathfrak{T}$-groups.

It is known that any $\mathfrak{T}$-group admits a (proper normal) central series with infinite cyclic factors; the other way round, every group admitting such a series is clearly a $\mathfrak{T}$-group. Now let G be a group, and let $g_1, \dots, g_n$ be an (ordered) set of elements of G. Then we can consider the chain of subgroups

$$G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n \geqslant G_{n+1} = 1$$

of G where for every $i = 1, \dots, n$,

$$G_i = \langle g_i, \dots, g_n \rangle.$$

We call it the chain associated to $g_1, \dots, g_n$. Further, we say that $g_1, \dots, g_n$ is a $\mathfrak{T}$-sequence for G if the associated chain is a proper central series for G with infinite cyclic factors. It will be convenient to extend this terminology saying that the empty set is a $\mathfrak{T}$-sequence for the trivial group. Every $\mathfrak{T}$-group G has a $\mathfrak{T}$-sequence, and the length of a $\mathfrak{T}$-sequence is an invariant of the group, called the Hirsch-length of G. Furthermore, if $g_1, \dots, g_n$ is a $\mathfrak{T}$-sequence for G then every element $g \in G$ can be written $g = g_1^{e_1} \cdots g_n^{e_n}$, where $e_i \in \mathbb{Z}$.

Now let A be an abelian group, and let $a_1, \dots, a_n \in A$. Then we consider

$$L = \left\{ (e_1, \dots, e_n) \in \mathbb{Z}^n \;\middle|\; a_1^{e_1} \cdots a_n^{e_n} = 1 \right\}$$

which is of course a subgroup of $\mathbb{Z}^n$. We call it the relation lattice of $a_1, \dots, a_n$ in A. For every $e = (e_1, \dots, e_n) \in L$, $e \neq 0$, we can define its height as the minimum $j = 1, \dots, n$ such that $e_j \neq 0$, and its leading coefficient as the integer e_j. Now let $e^{(1)}, \dots, e^{(m)}$ be a basis of L, where for $j = 1, \dots, m$,

$$e^{(j)} = \left(e_1^{(j)}, \dots, e_n^{(j)} \right).$$

We say that the basis is in Hermite normal form if the matrix

$$\begin{pmatrix} e_1^{(1)} & \cdots & e_n^{(1)} \\ \vdots & & \vdots \\ e_1^{(m)} & \cdots & e_n^{(m)} \end{pmatrix} \in M_{m \times n}(\mathbb{Z})$$

is. This means that there exists a sequence of integers

$$1 \leqslant i_1 < \cdots < i_m \leqslant n$$

such that

$$e_i^{(j)} = 0$$

for all $j = 1, \dots, m$ and all $1 \leqslant i < i_j$, and that

$$0 \leqslant e_{i_j}^{(k)} < e_{i_j}^{(j)}$$

for every $1 \leqslant k < j \leqslant m$. It is known that L admits a unique basis in Hermite normal form. We note that the height of any non-zero element of L is one of the integers $i_1, \dots, i_m$. Further, if its height is i_j for some $j = 1, \dots, m$, then its leading coefficient is a (non-zero) multiple of $e_{i_j}^{(j)}$.

The next lemma is a somewhat stronger version of a result of Eick (cf. [6], Lemma 3.19).

Lemma 5.1. *Let G be a $\mathfrak{T}$-group, A an abelian group, and let $\varphi : G \to A$ be a morphism of groups. Further, let $g_1, \dots, g_n$ be a $\mathfrak{T}$-sequence for G, and let $e^{(1)}, \dots, e^{(m)}$ be the basis in Hermite normal form of the relation lattice of $\varphi(g_1), \dots, \varphi(g_n)$ in A. For $j = 1, \dots, m$ set*

$$k_j = g_1^{e_1^{(j)}} \cdots g_n^{e_n^{(j)}}.$$

Then $k_1, \dots, k_m$ is a $\mathfrak{T}$-sequence for the kernel of φ.

Proof. Let us denote by

$$K_1 \geqslant K_2 \geqslant \cdots \geqslant K_m \geqslant K_{m+1} = 1$$

the chain of subgroups of G associated to $k_1, \dots, k_m$. We want to show that it is a (proper normal) central series for $\ker\varphi$ with infinite cyclic factors. Since the basis $e^{(1)}, \dots, e^{(m)}$ is in Hermite normal form, we have the sequence

$$1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n$$

defined as above. It is convenient to set $i_0 = 0$ and $i_{m+1} = n + 1$. Also, let us denote by

$$G = G_1 > G_2 > \cdots > G_n > G_{n+1} = 1$$

the proper central sequence with infinite cyclic factors for G associated to $g_1, \dots, g_n$. Then it is enough to prove that for every $j = 1, \dots, m + 1$ we have

$$\ker\varphi \cap G_{i_{j-1}+1} = \cdots = \ker\varphi \cap G_{i_j-1} = \ker\varphi \cap G_{i_j} = K_j.$$

Indeed, suppose that the previous equalities hold. Then $K_1 = \ker\varphi \cap G_{i_0+1} = \ker\varphi \cap G_1 = \ker\varphi \cap G = \ker\varphi$. Also, for every $j = 1, \dots, m+1$, $G_{i_j} \trianglelefteq G$, hence $K_j = \ker\varphi \cap G_{i_j} \trianglelefteq \ker\varphi \cap G = \ker\varphi$. This shows that the chain is a normal series for $\ker\varphi$. Further, for every $j = 1, \dots, m$, the map $\ker\varphi \to \frac{G}{G_{i_j+1}}$ has kernel $\ker\varphi \cap G_{i_j+1} = K_{j+1}$. Hence it factors through a group monomorphism $\frac{\ker\varphi}{K_{j+1}} \to \frac{G}{G_{i_j+1}}$. The image of $\frac{K_j}{K_{j+1}}$ under it is $\frac{K_j G_{i_j+1}}{G_{i_j+1}} = \frac{(\ker\varphi \cap G_{i_j})G_{i_j+1}}{G_{i_j+1}} = \frac{(\ker\varphi G_{i_j+1}) \cap G_{i_j}}{G_{i_j+1}} \leqslant \frac{G_{i_j}}{G_{i_j+1}}$, and the image of $k_j K_{j+1}$ is $g_{i_j}^{e_{i_j}^{(j)}} G_{i_j+1}$. This shows that the series is central and with infinite cyclic factors.

So we have to prove the previous equalities. It is clear that for every $j = 1, \dots, m + 1$,

$$\ker\varphi \cap G_{i_{j-1}+1} \supseteq \cdots \supseteq \ker\varphi \cap G_{i_j-1} \supseteq \ker\varphi \cap G_{i_j} \supseteq K_j$$

and it remains to prove the reverse inclusions. We proceed by induction on j. Let us consider the base case $j = m + 1$. Then K_j is trivial, and all we have to show is that for every $l = i_m + 1, \dots, n + 1$, $\ker\varphi \cap G_l$ is trivial, too. Again, we proceed by induction on l. In the base case $l = n + 1$, it is obviously true. Now let $l = i_m + 1, \dots, n$ and suppose that $\ker\varphi \cap G_{l+1}$ is trivial. Let $g \in \ker\varphi \cap G_l$. Then $g = g_l^e h$ for some $e \in \mathbb{Z}$ and $h \in G_{l+1}$, and

$$\varphi(g_l)^e + \varphi(h) = 0.$$

Since $h \in \langle g_{l+1}, \dots, g_n \rangle$, then $\varphi(h) \in \langle \varphi(g_{l+1}), \dots, \varphi(g_n) \rangle$. Thus if $e \neq 0$, then there would exist an element in the relation lattice with height l, which is impossible. Hence $e = 0$, hence $g = h \in \ker\varphi \cap G_{l+1}$, hence $g = 1$ by the inductive hypothesis. This concludes the case $j = m+1$. Now let $j = 1, \dots, m$, and suppose that

$$\ker\varphi \cap G_{i_j+1} = \dots = \ker\varphi \cap G_{i_{j+1}-1} = \ker\varphi \cap G_{i_{j+1}} = K_{j+1}.$$

In this case we have to show that for every $l = i_{j-1} + 1, \dots, i_j$,

$$\ker\varphi \cap G_l = K_j$$

and again we proceed by induction on l. Let us just consider the base case $l = i_j$, the inductive step being similar to the one in the case $j = m + 1$. Let $g \in \ker\varphi \cap G_{i_j}$. Then $g = g_{i_j}^e h$ for some $e \in \mathbb{Z}$ and some $h \in G_{i_j+1}$. If $e = 0$ then $g \in G_{i_j+1}$ and we conclude by inductive hypothesis that $g \in K_{j+1}$. Now let us suppose $e \neq 0$. Arguing as before, the relation lattice contains an element of height i_j and leading coefficient e. Thus $e_{i_j}^{(j)}$ divides e. Let us denote by f the quotient. Then $gG_{i_j+1} = k_i^f G_{i_j+1}$, hence by inductive hypothesis $gk_j^{-f} \in \ker\varphi \cap G_{i_j+1} = K_{j+1}$, hence finally $g \in K_j$. $\square$

6. Some algorithms for lattices

In this section we describe some algorithms that solve several problems related to lattices. We mainly work with matrices whose rows span lattices or subspaces in $\mathbb{Q}^n$. We say that a matrix is integral if it has integer entries.

A basic algorithm that we use is the Smith normal form: given an $m \times n$ integral matrix A this algorithm finds an $m \times n$ integral matrix S, and integral unimodular square matrices P and Q with:

1. S is in Smith normal form (this means that there is an r such that $d_i = S(i,i)$ is positive for $1 \leqslant i \leqslant r$, S has no other non-zero entries, and d_i divides d_{i+1} for $1 \leqslant i < r$),
2. $S = PAQ$.

For details on this algorithm we refer to [11], §8.3. One property that we note is the following (cf. [11], Chapter 8, Corollary 3.4).

Lemma 6.1. *Let $q_1, \dots, q_n$ denote the rows of Q^{-1}. They form a basis of $\mathbb{Z}^n$, and d_i is the smallest non-negative integer such that $d_i q_i$ lies in the span of the rows of A for $1 \leqslant i \leqslant r$.*

We also need an algorithm that appears to be well known: in the computer algebra system Magma [4] it is implemented under the name of "saturation." However, we have not been able to find a reference for it in the literature. For this reason we sketch a solution here. Let A be an $m \times n$-matrix with integer entries. Let $V \subset \mathbb{Q}^n$ be the $\mathbb{Q}$-space spanned by the rows of A. The problem is to find a $\mathbb{Z}$-basis for the lattice $\mathbb{Z}^n \cap V$. Without loss of generality we assume that the rows of A are linearly independent. The key observation is the following. Let B be an $m \times n$ integral matrix whose rows span V. Then its rows span $\mathbb{Z}^n \cap V$ if and only if the Smith normal form of B has diagonal entries that are all equal to 1. This follows from Lemma 6.1. This implies the correctness of the following algorithm.

Algorithm 1 *(Saturation).*
Input: an $m \times n$ integral matrix A with linearly independent rows.
Output: an $m \times n$ integral matrix B whose rows span $\mathbb{Z}^n \cap V$, where $V \subset \mathbb{Q}^n$ is the $\mathbb{Q}$-space spanned by the rows of A.

(1) Let S, P, Q be the output of the Smith normal form algorithm with input A.
(2) Let S' be the matrix obtained from S by setting the diagonal entries equal to 1.
(3) Return $B = P^{-1}S'Q^{-1}$.

Algorithm 2 *(Intersection of lattice and subspace).*
Input: an $n \times n$ integral matrix A whose rows span the full-dimensional lattice L in $\mathbb{Q}^n$, and an $m \times n$ matrix B whose rows span an m-dimensional $\mathbb{Q}$-subspace W of $\mathbb{Q}^n$.
Output: an $n \times n$ integral matrix whose rows span L, and whose first m rows span the lattice $W \cap L$.

(1) Let $e_1, \dots, e_n$ and $b_1, \dots, b_m$ denote the rows of A and B, respectively. Write $b_i = \sum_{j=1}^n \beta_{ij} e_j$, and let $B' = (\beta_{ij})$; if necessary multiply the rows of B' by integers in order to get integral entries.
(2) Let C be the output of Algorithm 1 with input B'.
(3) Let S, P, Q be the output of the Smith normal form algorithm with input C.
(4) Return $Q^{-1}A$.

Lemma 6.2. *Algorithm* 2 *is correct.*

Proof. The idea is to use the given basis of L as a basis of $\mathbb{Q}^n$. Let $\psi : \mathbb{Q}^n \to \mathbb{Q}^n$ be the corresponding isomorphism. So if $v \in \mathbb{Q}^n$ then $\psi(v)$ is the vector that contains the coefficients of v with respect to the basis of L. So after the first step the rows of B' form a basis of $\psi(W)$. Of course $\psi(L) = \mathbb{Z}^n \subset \mathbb{Q}^n$.

So the rows of C form a basis of $\psi(W) \cap \psi(L) = \psi(W \cap L)$. Furthermore, the Smith normal form S of C has diagonal entries equal to 1. Therefore the rows of Q^{-1} form a basis of $\mathbb{Z}^n$ and the first m rows form a $\mathbb{Z}$-basis of $\psi(W \cap L)$. Note that for $v \in \mathbb{Q}^n$ we have $\psi^{-1}(v) = \psi(v)A$. Therefore the rows of $Q^{-1}A$ form a basis of L, and the first m are a $\mathbb{Z}$-basis of $W \cap L$. $\square$

Algorithm 3 *(L-complements).*
Input: an $n \times n$ integral matrix A whose rows span a full-dimensional lattice L in $V = \mathbb{Q}^n$; and bases of subspaces $V_1 \subseteq V_{n-1} \subset V$.
Output: an $n \times n$ integral matrix C with the following properties:

- The rows of C span L.
- The first s rows of C span $L \cap V_1$ ($s = \dim V_1$).
- The first t rows of C span $L \cap V_{n-1}$ ($t = \dim V_{n-1}$).

(1) Execute Algorithm 2 with input A and a matrix whose rows span V_{n-1}. Let $w_1, \dots, w_n$ denote the rows of the output.
(2) Let $v_1, \dots, v_s$ be the given basis of V_1, and write $v_i = \sum_{j=1}^t \alpha_{ij} w_j$. Let $A' = (\alpha_{ij})$.
(3) Execute Algorithm 2 with input the $t \times t$-identity matrix, and A'. Let B denote the output.
(4) Let C' be the product of B and the $t \times n$ matrix whose rows are $w_1, \dots, w_t$. Let C be the matrix obtained from C' by appending $w_{t+1}, \dots, w_n$.

Lemma 6.3. *Algorithm* 3 *is correct. Let $u_1, \dots, u_n$ denote the rows of its output matrix B. Let $W_1, W_{n-1} \subset \mathbb{Q}^n$ be the subspaces spanned by $u_{s+1}, \dots, u_n$ and $u_{t+1}, \dots, u_n$, respectively. Then $W_1 \subset W_{n-1}$ are a system of L-complements to $V_1 \subset V_{n-1}$.*

Proof. After the first step $w_1, \dots, w_n$ span L and $w_1, \dots, w_t$ span $L \cap V_{n-1}$. Next we work in V_{n-1} using the basis $w_1, \dots, w_t$. We rewrite the basis elements of V_1 with respect to this basis. We note that multiplying a $v \in \mathbb{Q}^t$ with the matrix with rows $w_1, \dots, w_t$ is the reverse transformation. So the rows of C' span $L \cap V_{n-1}$ and the first s rows of C' span $L \cap V_1$. Therefore the output is correct.

The last statement follows directly from the definition of L-complements. $\square$

Remark 6.4. The output of Algorithm 3 has one more useful property. Let W_1, W_{n-1} be as in Lemma 6.3. The bases of the spaces W_1 and W_{n-1} that are produced by this algorithm are bases of $L \cap W_1$ and $L \cap W_{n-1}$, respectively.

Algorithm 4 *(Integral relations).*
Input: An $m \times n$-matrix A with rational coefficients.
Output: an $m \times n$ integral matrix whose rows are a basis of the lattice

$$\Lambda = \left\{ (e_1, \dots, e_m) \in \mathbb{Z}^m \;\middle|\; \sum_{i=1}^{m} e_i a_i \in \mathbb{Z}^n \right\},$$

where $a_1, \dots, a_m$ are the rows of A.

(1) Let M be the matrix obtained by appending the $n \times n$-identity matrix at the bottom of A.
(2) Let $v_1, \dots, v_m$ be a basis of the space $\{v \in \mathbb{Q}^{m+n} \mid vM = 0\}$. If necessary multiply each v_i by an integer to ensure that it has integral coefficients.
(3) Let B be the output of the saturation algorithm (Algorithm 1) applied to the matrix with the v_i as rows.
(4) Output the rows of B with the last n coefficients deleted.

Lemma 6.5. *Algorithm* 4 *is correct.*

Proof. Note that the matrix M has rank n; therefore in step (2) we find m linearly independent basis vectors. Now set

$$\Lambda' = \left\{ e = (e_1, \dots, e_{m+n}) \in \mathbb{Z}^{m+n} \;\middle|\; eM = 0 \right\}.$$

Then $(e_1, \dots, e_{m+n}) \mapsto (e_1, \dots, e_m)$ is a bijection $\Lambda \to \Lambda'$. Now after step (3) B is a basis of Λ'. We conclude that the output is a basis of Λ. $\square$

7. The main algorithm

Now we return to our initial problem. Let $G \subset \mathrm{GL}_m(\mathbb{C})$ be a unipotent algebraic group defined over $\mathbb{Q}$. Set $V = \mathbb{Q}^m$ and let L be a full-dimensional lattice in V. The problem is to compute a finite set of generators of the group $G_L = \{g \in G(\mathbb{Q}) \mid g(L) = L\}$.

We assume that G is defined as subset of $\mathrm{GL}_m(\mathbb{C})$ by polynomial equations that have coefficients in $\mathbb{Q}$. Then as a first step we find the Lie algebra $\mathfrak{g}$ of G as follows. First we compute a set $\mathcal{S}$ of generators for the radical of the ideal generated by the polynomials that define G (cf. [1]). Then we obtain the Lie algebra by differentiating the elements of $\mathcal{S}$.

The second step will be to compute a flag $0 = V_0 < V_1 < \cdots < V_n = V$ of V for the action of $\mathfrak{g}$. This is done by straightforward linear algebra: V_1 is the space killed by all elements of $\mathfrak{g}$; V_2/V_1 is the subspace of V/V_1 that is killed by all elements of $\mathfrak{g}$, and so on.

Now we have the input for our main algorithm which we now state. We use the notation of Sections 2, 4.

Algorithm 5 *(Main algorithm).*
Input: a non-zero finite-dimensional vector space V over $\mathbb{Q}$, a full-dimensional lattice L of V, a Lie subalgebra $\mathfrak{g} \subset \mathfrak{gl}(V)$ that is the Lie algebra of a unipotent algebraic group G, and a flag

$$0 = V_0 < V_1 < \cdots < V_n = V$$

of V with respect to the action of $\mathfrak{g}$.
Output: a $\mathfrak{T}$-sequence for G_L.

(1) If $n = 1$ then return the empty set, else go to step (2).
(2) Compute the derived vector space $V^\star$, the derived lattice $L^\star$, the derived flag $0 = V_0^\star < V_1^\star < \cdots < V_{n-1}^\star = V^\star$.
(3) Compute the kernel $\mathfrak{n}$ and the image $\mathfrak{q}$ of the derived action of $\mathfrak{g}$ on $V^\star$, together with the projection $\mathrm{d}\pi : \mathfrak{g} \to \mathfrak{q}$.
(4) Apply the algorithm recursively to the vector space $V^\star$, the lattice $L^\star$, the Lie algebra $\mathfrak{q}$ and the derived flag. Denote by $q_1, \ldots, q_k$ the result.
(5) Compute a system $W_{n-1} \subseteq W_1$ of L-complements to $V_1 \subseteq V_{n-1}$ (Algorithm 3), the induced lattice Γ and the induced error map $\epsilon : \mathrm{End}(V) \to \mathrm{Hom}(W_{n-1}, V_1)$.
(6) Compute a basis $x_1, \ldots, x_l$ of $\mathfrak{n}_L$ and set $n_i = \exp(x_i)$ for $1 \leqslant i \leqslant l$.
(7) For $1 \leqslant i \leqslant k$ compute a preimage x of $\log(q_i)$ under $\mathrm{d}\pi$ and set $g_{q_i} = \exp(x)$.
(8) Compute the image W' of $\mathfrak{n}$ under ϵ.
(9) Compute a basis $\mathcal{W} = \{w_1, \ldots, w_k\}$ in Hermite normal form of the relation lattice of the elements $\epsilon(g_{q_i}) + \Gamma + W'$ in $\frac{\mathrm{Hom}(W_{n-1}, V_1)}{\Gamma + W'}$ for $i = 1, \ldots, k$.
(10) For each w_i in $\mathcal{W}$ do the following
   (a) Write $w_i = (e_1^{(i)}, \ldots, e_k^{(i)})$ and set

$$g_{w_i} = g_{q_1}^{e_1^{(i)}} \cdots g_{q_k}^{e_k^{(i)}}.$$

   (b) Compute $v_{w_i} \in W'$ and $\gamma_{w_i} \in \Gamma$ such that $v_{w_i} + \gamma_{w_i} = \epsilon(g_{w_i})$.
   (c) Compute the preimage n_{w_i} of $-v_{w_i}$ under $\epsilon : \mathfrak{n} \to \mathrm{Hom}(W_{n-1}, V_1)$.
   (d) Compute $g_i = g_{w_i} \cdot \exp(n_{w_i})$.
(11) Return $g_1, \ldots, g_k, n_1, \ldots, n_l$.

We start by commenting on the computability of various steps.

5. We note that Algorithm 3 produces bases of $L \cap W_{n-1}$ and $L \cap V_1$. We use these bases to represent an element of $\mathrm{Hom}(W_{n-1}, V_1)$ as an $s \times t$-matrix (where $s = \dim(V_1)$, $t = \dim(W_{n-1})$). Then a $\mathbb{Z}$-basis of Γ is the set of elementary $s \times t$-matrices, which have one coefficient equal to 1, and all other coefficients equal to 0. Computing $\epsilon(a)$ for an $a \in \mathrm{End}(V)$ is standard linear algebra. Indeed, for $a \in \mathrm{End}(V)$ and $w \in W_{n-1}$ write $aw = v_1 + w_1$, where $v_1 \in V_1$ and $w_1 \in W_1$. Then $\epsilon(a)w = v_1$.
6. Here we first compute a basis of the space $\epsilon(\mathfrak{n}) \subset \mathrm{Hom}(W_{n-1}, V_1)$. Using Algorithm 2 we find a $\mathbb{Z}$-basis of $\Gamma \cap \epsilon(\mathfrak{n})$. The inverse images of the basis elements under ϵ are then a basis of $\mathfrak{n}_L$ (Proposition 4.2).
8. In step (6) we already obtained a basis of W', and a basis $\gamma_1, \ldots, \gamma_{st}$ of Γ such that $\gamma_1, \ldots, \gamma_m$ are a basis of $W' \cap \Gamma$. Let $N = st - m$ and for $\gamma \in \mathrm{Hom}(W_{n-1}, V_1)$ set $\psi(\gamma) = (c_{m+1}, \ldots, c_{st})$, where the c_i are defined by $\gamma = \sum_i c_i \gamma_i$. Then $\psi : \mathrm{Hom}(W_{n-1}, V_1) \to \mathbb{Q}^N$ is a linear map and $\gamma \in \Gamma + W'$ if and only if $\psi(\gamma) \in \mathbb{Z}^N$. Set $u_i = \epsilon(g_{q_i})$ for $1 \leqslant i \leqslant k$. We want to compute a $\mathbb{Z}$-basis of the lattice

$$\Lambda = \left\{ (e_1, \ldots, e_k) \in \mathbb{Z}^k \;\middle|\; \sum_{i=1}^{k} e_i u_i \in W' + \Gamma \right\}.$$

Now $(e_1, \ldots, e_k)$ lies in Λ if and only if $\sum_i e_i \psi(u_i) \in \mathbb{Z}^N$. So we get a basis of Λ by applying Algorithm 4 with input the matrix with rows $\psi(u_i)$. Then we compute the Hermite normal form (cf. [11], §8.1) of the basis of Λ obtained.

The other steps are straightforward. We now prove the correctness of the algorithm.

Theorem 7.1 *(Correctness of the main algorithm). Let V be a non-zero finite-dimensional vector space over $\mathbb{Q}$, L a full-dimensional lattice of V, and G a unipotent algebraic subgroup of* $\mathrm{GL}(V)$. *Further, let $\mathfrak{g} \subset \mathfrak{gl}(V)$ be the Lie algebra of G. Then Algorithm* 5, *with input V, L and $\mathfrak{g}$ and a flag*

$$0 = V_0 < V_1 < \cdots < V_n = V$$

of V with respect to the action of $\mathfrak{g}$, returns a $\mathfrak{T}$-sequence for the subgroup G_L of $\mathrm{GL}(V)$.

Proof. As a first thing we notice that, since $\mathfrak{g}$ is the Lie algebra of G, as seen in Section 4 the given flag is also a flag of V with respect to the action of G. Hence the hypothesis of Section 2 is satisfied, and we can consider all the constructions described there. As seen in Section 4, $\mathfrak{n} \subset \mathfrak{gl}(V)$ is the Lie algebra of N and $\mathfrak{q} \subset \mathfrak{gl}(V^\star)$ is the Lie algebra of Q. Now we proceed by induction on the length n of the flag.

If $n = 1$, then every vector of V is G-fixed, hence G is the trivial subgroup of $\mathrm{GL}(V)$ and G_L is the trivial subgroup of $\mathrm{GL}(V)$, hence the empty set is a $\mathfrak{T}$-sequence for G_L.

Now suppose that $n \geqslant 2$. By the inductive hypothesis, $q_1, \ldots, q_k$ is a $\mathfrak{T}$-sequence for the subgroup $Q_{L^\star}$ of $\mathrm{GL}(V^\star)$. By results in Section 4, the exponential map gives a bijection from $\mathfrak{n}$ to $N(\mathbb{Q})$ and, since by Proposition 4.1 the Lie algebra $\mathfrak{n}$ is abelian, it is also a group morphism. Further, using Proposition 4.3 and Lemma 2.5, it is easily seen that the image of $\mathfrak{n}_L$ under the exponential map is N_L. Hence $n_1, \ldots, n_s$ is a $\mathfrak{T}$-sequence for N_L, regardless of their order. As seen in Section 4, we have $\exp(\mathrm{d}\pi(x)) = \pi(\exp(x))$ for all $x \in \mathfrak{g}$. So for $i = 1, \ldots, k$ we get

$$\pi(g_{q_i}) = q_i. \tag{4}$$

In particular, $g_{q_i} \in G_{L^\star}$. By commutativity of the diagram in Corollary 2.4,

$$\Psi(q_i) = \epsilon(g_{q_i}) + \Gamma + W$$

and, due to Proposition 4.3, W' is equal to the image W of $N(\mathbb{Q})$ under ϵ. Hence $\mathcal{W}$ is a basis in Hermite normal form for the relation lattice of $\Psi(q_i)$, $i = 1, \ldots, k$, in $\frac{\mathrm{Hom}(W_{n-1}, V_1)}{\Gamma + W}$. For $1 \leqslant i \leqslant k$ set

$$h_i = q_1^{e_1^{(i)}} \cdots q_k^{e_k^{(i)}},$$

where $w_i = (e_1^{(i)}, \ldots, e_k^{(i)})$ is as in the algorithm. By Lemma 5.1, the ordered set $h_1, \ldots, h_k$ is a $\mathfrak{T}$-sequence for the kernel of Ψ. Owing to (4) we have that g_{w_i} is an element of $G_{L^\star}$ satisfying

$$\pi(g_{w_i}) = h_i$$

for $1 \leqslant i \leqslant k$. Again by commutativity of the diagram in Corollary 2.4, we have that $\epsilon(g_{w_i}) \in \Gamma + W = \Gamma + W'$ (hence step (b) makes sense). Since $\exp(n_{w_i}) \in N(\mathbb{Q})$, we have $g_i \in G_{L^\star}$ and

$$\pi(g_i) = h_i.$$

Further, using Propositions 2.3 and 4.3, we obtain that

$$\epsilon(g_i) = \epsilon(g_{w_i}) + \epsilon(n_{w_i}) = v_{w_i} - v_{w_i} + \gamma_{w_i} \in \Gamma.$$

Hence by Lemma 2.5 we have that $g_i \in G_L$. Thus by Proposition 2.7 the ordered set $g_1 N_L, \ldots, g_k N_L$ is a $\mathfrak{T}$-sequence for $\frac{G_L}{N_L}$. Using Proposition 4.1 we get that N is central in G, hence N_L is central in G_L. Therefore we finally obtain that $g_1, \ldots, g_k, n_1, \ldots, n_l$ is a $\mathfrak{T}$-sequence for G_L. $\square$

Corollary 7.2. *Let the notation be as in Theorem* 7.1. *Let $\mathcal{H}$ denote the $\mathfrak{T}$-group generated by the output of Algorithm* 5. *Then the Hirsch length of $\mathcal{H}$ is equal to the dimension of G. Moreover, the Lie algebra of the radicable hull of $\mathcal{H}$ is isomorphic over $\mathbb{Q}$ to $\mathfrak{g}$.*

Proof. We use the notation of the proof of Theorem 7.1. By induction, $q_1, \dots, q_k$ is a $\mathfrak{T}$-sequence for $Q_{L^\star}$. This group has dimension equal to $\dim G - \dim N = \dim G - l$. Therefore the $\mathfrak{T}$-sequence output by the algorithm is of length equal to $\dim G$.

Let $h_1, \dots, h_r$ denote the $\mathfrak{T}$-sequence output by the algorithm. From [10], Chapter 6, we get that the Lie algebra of the radicable hull of $\mathcal{H}$ is isomorphic to the Lie algebra spanned by $\log(h_i)$. But the latter one is $\mathfrak{g}$. $\square$

Remark 7.3. The algorithm can be slightly modified in order to compute even a finite presentation of G_L. To show how this can be done, we need to introduce some further notation.

Let $\mathcal{G}$ be a $\mathfrak{T}$-group and $g_1, \dots, g_n$ a $\mathfrak{T}$-sequence for $\mathcal{G}$. We say that a word w in $g_1, \dots, g_n$ is normal if it is of the form $g_1^{e_1} \cdots g_n^{e_n}$ for some $e_i \in \mathbb{Z}$. If this is the case, the depth of w is the minimum i such that e_i is non-zero. It is an easy induction to prove that every element g of $\mathcal{G}$ can be written in a unique way as a normal word w in $g_1, \dots, g_n$. Also, $g \in \mathcal{G}_i = \langle g_i, \dots, g_n \rangle$ if and only if w has depth at least i. Since $g_1, \dots, g_n$ is a $\mathfrak{T}$-sequence, for every $1 \leqslant i < j \leqslant n$ we have that $[g_i, g_j] \in \mathcal{G}_{j+1}$. Hence there exist a unique normal word $w_{[g_i,g_j]}$ (of depth at least $j+1$) such that

$$[g_i, g_j] = w_{[g_i,g_j]}.$$

It is well known that

$$\left\langle g_1, \dots, g_n \;\middle|\; [g_i, g_j] = w_{[g_i,g_j]} \text{ for } 1 \leqslant i < j \leqslant n \right\rangle$$

is a finite presentation for G. We call it the standard presentation for $\mathcal{G}$ with respect to $g_1, \dots, g_n$.

Recall that the algorithm as it stands computes a $\mathfrak{T}$-sequence $g_1, \dots, g_k, n_1, \dots, n_l$ for G_L. Now we want to sketch how it can be modified in order to compute the standard presentation for G_L with respect to such a $\mathfrak{T}$-sequence. Of course it will be enough to show how to compute the normal words of the forms $w_{[g_i,g_j]}$, $w_{[g_i,n_j]}$ and $w_{[n_i,n_j]}$ (for any suitable choice of the indexes i and j). The proof of Theorem 7.1 shows that N_L is central in G_L. Hence it follows at once that

$$w_{[g_i,n_j]} = w_{[n_i,n_j]} = 1.$$

So the only hard part is to compute the words of the form $w_{[g_i,g_j]}$. To this end we can suppose by inductive hypothesis that step (4) of the algorithm, along with a $\mathfrak{T}$-sequence $q_1, \dots, q_k$ for $Q_{L^\star}$, produces also the standard presentation

$$\left\langle q_1, \dots, q_k \;\middle|\; [q_i, q_j] = w_{[q_i,q_j]} \text{ for } 1 \leqslant i < j \leqslant k \right\rangle$$

of $Q_{L^\star}$ with respect to $q_1, \dots, q_k$. Recall that, using the notations of the proof of Theorem 7.1, $h_1, \dots, h_k$ is a $\mathfrak{T}$-sequence for the kernel of Ψ. Furthermore, the proof even shows that we can effectively write its elements as normal words in $q_1, \dots, q_k$ (of increasing depth). There are algorithms known for computing a standard presentation of a subgroup of a $\mathfrak{T}$-group (cf. [11]; an implementation of the algorithms for this purpose is available in the GAP4 package "polycyclic," [7]). So we can compute the standard presentation

$$\left\langle h_1, \dots, h_k \;\middle|\; [h_i, h_j] = w_{[h_i,h_j]} \text{ for } 1 \leqslant i < j \leqslant k \right\rangle$$

for the kernel of Ψ with respect to $h_1, \dots, h_k$. Since every $w_{[h_i,h_j]}$ is a normal word in $h_1, \dots, h_k$, we can evaluate it in $g_1, \dots, g_k$ (that it to say, substituting every h_i with g_i). In this way we obtain a normal word $u_{[g_i,g_j]}$ in $g_1, \dots, g_n$. Since $\pi : G_L \to K$ sends g_i in h_i and has kernel N_L, we obtain that

$$n = [g_i, g_j]u_{[g_i,g_j]}^{-1} \in N_L.$$

Since $n_1, \dots, n_s$ is a $\mathfrak{T}$-sequence for N_L, we can write n as a normal word v in $n_1, \dots, n_s$. This can be done effectively, being equivalent to write an element of a lattice in terms of a (ordered) basis. Since $u_{[g_i,g_j]}v$ is a normal word in $g_1, \dots, g_k, n_1, \dots, n_l$, it now follows easily that

$$w_{[g_i,g_j]} = u_{[g_i,g_j]}v.$$

8. Practical performance

It is rather straightforward to see that the complexity of Algorithm 5 is exponential in the length of the flag of V. Indeed, if the flag has maximal length, or in other words, $\dim V_i = i$, then $\dim V^\star = 2n - 2$. So in the worst case the dimension of the ambient vector space is roughly doubled in each step of the recursion.

It turns out that the dimension of the spaces $\mathrm{Hom}(W_{n-1}, V_1)$ increases even faster (in the worst case by about a factor of 4 each step of the recursion). For this reason we avoid working with the entire space $\mathrm{Hom}(W_{n-1}, V_1)$. Instead we consider the associative algebra with one $A \subset \mathrm{End}(V)$ generated by the elements of the Lie algebra $\mathfrak{g}$. Let $U = \epsilon(A) \subset \mathrm{Hom}(W_{n-1}, V_1)$. Then $\epsilon(G) \subset U$, so we can work with the space U instead of $\mathrm{Hom}(W_{n-1}, V_1)$. In fact we choose to work with a potentially somewhat bigger space, namely the subspace of $\mathrm{Hom}(W_{n-1}, V_1)$ consisting of the matrices that have non-zero entries only in those positions for which there are elements in U that have non-zero entries in those positions. This space has the advantage that its intersection with the lattice Γ is easily computed. Furthermore, in practice it is only slightly bigger than U.

We have implemented the algorithm in the language of GAP4 [8]. We use three series of Lie algebras in $\mathfrak{gl}_n(\mathbb{Q})$ to generate test inputs to the algorithm. The terms of the first series are denoted $\mathfrak{g}_n$, which is spanned by

$$x_i = e_{1,i+1} \quad \text{for } 1 \leqslant i \leqslant n-1,$$
$$x_n = \sum_{j=2}^{n-1} e_{j,j+1}$$

(here $e_{i,j}$ is the $n \times n$-matrix with a 1 on position (i, j) and zeros elsewhere). The only non-zero commutators are $[x_i, x_n] = x_{i+1}$ for $1 \leqslant i \leqslant n-2$. So $\mathfrak{g}_n$ is of dimension n and of nilpotency class $n-1$.

The second series of Lie algebras is denoted $\mathfrak{h}_n$, which is spanned by

$$y_1 = \sum_{i=1}^{n-1} i e_{i,i+1},$$
$$y_k = \sum_{i=1}^{n-k} e_{i,i+k} \quad \text{for } 2 \leqslant k \leqslant n-1.$$

Here the only non-zero commutators are $[y_1, y_k] = -k y_{k+1}$ for $2 \leqslant k \leqslant n-2$. So $\mathfrak{h}_n$ is of dimension $n-1$ and of nilpotency class $n-2$. In fact, as abstract Lie algebras, $\mathfrak{h}_n \cong \mathfrak{g}_{n-1}$. We note that both Lie algebras have a flag of maximal length.

Table 1
Time (in seconds) for the main algorithm with input $\mathfrak{g}_n$, $\mathfrak{h}_n$ and $\mathfrak{u}_n$.

n	time $\mathfrak{g}_n$	time $\mathfrak{h}_n$	time $\mathfrak{u}_n$
6	0.7	0.4	1.8
7	3	3	11
8	24	16	95
9	204	133	963

The terms of the third series, denoted $\mathfrak{u}_n$, are spanned by all matrices $e_{i,j}$ for $1 \leqslant i < j \leqslant n$. In other words, $\mathfrak{u}_n$ is the full upper triangular Lie algebra. Also this Lie algebra has a flag of maximal length.

In Table 1 we list the running times[2] of the algorithm with input the Lie algebras $\mathfrak{g}_n$, $\mathfrak{h}_n$ and $\mathfrak{u}_n$, for $n = 6, 7, 8, 9$. In all cases for the lattice L we have taken $\mathbb{Z}^n \subset \mathbb{Q}^n$.

On Table 1 we make the following comments:

- We see that the algorithm is efficient enough to tackle nontrivial examples.
- However, the running times do confirm the analysis above that the complexity of the algorithm is exponential in the length of the flag.
- Also we see that the length of the flag has a great bearing on the running time, as $\mathfrak{h}_n \cong \mathfrak{g}_{n-1}$, but the algorithm needs markedly longer for $\mathfrak{h}_n$ than for $\mathfrak{g}_{n-1}$.
- Of course, for groups of higher dimension, but equal flag length, the algorithm also has to work harder, as is shown by comparing $\mathfrak{g}_n$ and $\mathfrak{h}_n$ on the one hand, and $\mathfrak{u}_n$ on the other hand.
- Finally we remark that it turned out that for $n \geqslant 10$ our program was not able to complete the computation within 1 GB of memory. So for higher flag lengths a more memory efficient implementation would be needed, for example using sparse matrices (that are not currently available in GAP).

References

[1] Thomas Becker, Volker Weispfenning, Gröbner Bases, A Computational Approach to Commutative Algebra, Grad. Texts in Math., vol. 141, Springer-Verlag, New York, 1993 (in cooperation with Heinz Kredel).
[2] Armand Borel, Linear Algebraic Groups, second ed., Grad. Texts in Math., vol. 126, Springer-Verlag, New York, 1991.
[3] Armand Borel, Harish-Chandra, Arithmetic subgroups of algebraic groups, Ann. of Math. (2) 75 (1962) 485–535.
[4] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system, I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symbolic Comput. 24 (3–4) (1997) 235–265.
[5] Claude Chevalley, Théorie des groupes de Lie. Tome III. Théorèmes généraux sur les algèbres de Lie, Actualités Sci. Ind., vol. 1226, Hermann & Cie, Paris, 1955.
[6] Bettina Eick, Algorithms for polycyclic groups, Habilitation Thesis, Technische Universität Braunschweig, 2001.
[7] Bettina Eick, Werner Nickel, Polycyclic, a GAP package, http://www.gap-system.org/Packages/polycyclic.html, 2004 (accepted).
[8] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.10, http://www.gap-system.org, 2007.
[9] Fritz Grunewald, Daniel Segal, Some general algorithms, I. Arithmetic groups, Ann. of Math. (2) 112 (3) (1980) 531–583.
[10] Daniel Segal, Polycyclic Groups, Cambridge Tracts in Math., vol. 82, Cambridge University Press, Cambridge, 1983.
[11] Charles C. Sims, Computation with Finitely Presented Groups, Encyclopedia Math. Appl., vol. 48, Cambridge University Press, Cambridge, 1994.
[12] Patrice Tauvel, Rupert W.T. Yu, Lie Algebras and Algebraic Groups, Springer Monogr. Math., Springer-Verlag, Berlin, 2005.
[13] William C. Waterhouse, Introduction to Affine Group Schemes, Grad. Texts in Math., vol. 66, Springer-Verlag, New York, 1979.

[2] The computations were done on a 2 GHz processor with 1 GB of memory for GAP.