Diplomarbeit

Polycyclic presentations for matrix groups

Björn Assmann

Betreuerin
Professor Dr. Bettina Eick
Institut für Geometrie
Technische Universität Braunschweig
Pockelstr.14
38106 Braunschweig

Braunschweig, den 9. September 2003

Eidesstattliche Erklärung

Hiermit bestätige ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Hilfsmittel verfasst habe.

Braunschweig, den 9. September 2003 Unterschrift

Contents

Chapter 1

Introduction

A group G is called *polycyclic* if there exists a subnormal series of the form

$$G = G_1 \rhd G_2 \rhd \cdots G_n \rhd G_{n+1} = 1 \qquad (*)$$

with cyclic factors G_i/G_{i+1}. By a well-known result of Hirsch every polycyclic group is finitely presented (see also Theorem 2.2.2). Among the finite presentations of a polycyclic group G, there are some that reflect the structure of the subnormal series $(*)$. Such presentations are called polycyclic presentations (pc-presentations) and will be defined in Section 2.2.

If a polycyclic group G is given by a pc-presentation, then many problems of group theory can be solved in practice. For example, one can determine if G is torsion-free and calculate the torsion subgroup T, if T exists. Further, one can compute the derived series and the Hirsch length of the group G. Also various methods for computations with subgroups, factor groups and extensions are available. All these methods are available in the package 'Polycyclic' [8] of the computer algebra system GAP [24].

Groups often arise in a natural way as matrix groups over $\mathbb{Q}$ (for instance in the study of symmetries of crystals). But for such matrix groups certain problems are difficult to solve. For example, it is not easy to decide, if the torsion subgroup exists, and to calculate it if it does. On the other hand, these problems are easy to solve once a pc-presentation for a polycyclic group is known. Therefore a method is needed to determine a pc-presentation for a given polycyclic matrix group.

The aim of this thesis is the description and implementation of algorithms for the following tasks: Let G be a finitely generated subgroup of $GL(d, R)$ where the ring R is either $\mathbb{Q}, \mathbb{Z}$ or a finite field $\mathbb{F}_q$. Then

- we can test whether G is solvable;
- if G is polycyclic, then we can determine a pc-presentation for G.

If $R = \mathbb{Z}$ or $\mathbb{F}_q$ the group G is polycyclic if and only if G is solvable (see Chapter 2, Section 2.3). Therefore, we can test if such a G is polycyclic.

The implemented algorithms are available in the GAP-package 'Polenta' [1], which can be downloaded from

http://cayley.math.nat.tu-bs.de/software/content.html

The implementation is based on the computer algebra systems GAP [24] and KANT [10]. Our aim was the development and the implementation of practical algorithms, that is, algorithms which can be applied to a collection of significant examples.

The overall algorithm involves ideas from different areas of computational mathematics. It utilizes classical methods like the orbit-stabilizer algorithm optimized to the given structure. In addition it also uses techniques from algebraic number theory, for example, the factorization of fractional ideals. Finally also representation theory is used, for example, the calculation of certain submodule series plays an important role.

1.1 History and related research

In 1985 John D. Dixon [5] investigated the orbit-stabilizer problem for linear groups. He found a structure theorem for polycyclic subgroups of $GL(d, \mathbb{Q})$ (see Corollary 2.4.5), which is important in this context also.

Based on this, Gretchen Ostheimer [14] proved in 1996, that the calculation of a pc-presentation for a polycyclic subgroup of $GL(d, \mathbb{Q})$ can be reduced to three simpler problems: the calculation of a pc-presentation for

- solvable groups in $GL(d, \mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field;
- multiplicative subgroups of an algebraic extension field of $\mathbb{Q}$;
- unipotent subgroups of $GL(d, \mathbb{Q})$.

Ostheimer described algorithms for all three steps, but a full implementation was not available.

In 2001 Bettina Eick [6] refined the approach of Ostheimer and described practical approaches for the first two parts of Ostheimer's method.

Part one is based on an algorithm of Charles C. Sims [22] for the computation of the order of solvable permutation groups. This algorithm together with an efficient implementation is given in this thesis.

Part two is based on computations in algebraic number fields and representation theory, and has been developed with the help of Jürgen Klüners and Florian Hess.

Part three has been known for some time, and can be solved following the ideas of Chapter 9 in the book of Sims [21].

Finally, we note that there exists an alternative approach to compute a polycyclic presentation of a rational polycyclic matrix group by Robert Beals (see for example [2] and [3]). We are not aware of an implementation of this method, which uses randomized methods.

1.2 Overview and structure of the thesis

In Chapter 2 we give a brief introduction to polycyclic groups. It covers polycyclic presentations, polycyclic generating sequences and the connections between solvable and polycyclic groups.

As outlined in Section 1.1, it is possible to reduce the problem of the calculation of a pc-presentation for a polycyclic matrix group $G \leq GL(d, \mathbb{Q})$ to three simpler groups, which are interesting in their own right. These are finite matrix groups, multiplicative subgroups of an algebraic extension of $\mathbb{Q}$ and unipotent matrix groups:

Chapter 3 describes algorithms to compute a pc-presentation for finite matrix groups over a given ring.

Chapter 4 provides methods to calculate a pc-presentation for multiplicative subgroups of an algebraic extension of $\mathbb{Q}$.

In Chapter 5 we outline how to compute pc-presentations of unipotent rational matrix groups.

For the splitting of $G \leq GL(d, \mathbb{Q})$ into the three mentioned kind of groups, some representation theory is needed. Regard $\mathbb{Q}^d$ as the natural $\mathbb{Q}G$-module. Chapter 6 contains an algorithm for the determination of the radical series of $\mathbb{Q}^d$. Further, we show that for the *p-congruence subgroup* $K \lhd G$ (see Definition 2.4.2) it is possible to compute a composition series of the $\mathbb{Q}K$-module $\mathbb{Q}^d$.

Finally, in Chapter 7 we present the overall algorithm to compute a pc-presentation for a rational polycyclic matrix group and propose some refinements. Further we show that a similar approach can be used to test if a matrix group over $\mathbb{Q}, \mathbb{Z}$ or a finite field $\mathbb{F}_q$ is solvable or not. For a matrix group over $\mathbb{Z}$ or $\mathbb{F}_q$, we can also test, if the given group is polycyclic.

In Chapter 8 we give runtimes of the implemented algorithms and describe the bottle necks.

1.3 Acknowledgments

I am grateful for Bettina Eick for her supervision. She was always available when help was needed and I always obtained reliable advice from her. Further, I would like to thank Csaba Schneider for lots of helpful comments on writing this text and Gretchen Ostheimer for giving me a very nice introduction to the topic of this thesis. Finally I want to thank Jürgen Klüners for his help in algebraic number theory and Christian Sievers for his hint for Lemma 5.1.5.

Chapter 2

Polycyclic groups

This chapter provides some basic facts about polycyclic groups and a structure theorem for polycyclic matrix groups. For further background on polycyclic groups we refer to [21] chapter 9, [19] page 147ff and [20].

2.1 Polycyclic sequences

2.1.1 Definition: Let G be a polycyclic group with a subnormal series

$$G = G_1 \rhd G_2 \rhd \cdots G_n \rhd G_{n+1} = 1 \qquad (*)$$

with cyclic factors G_i/G_{i+1}. A list $\mathcal{G} = (g_1, \ldots, g_n)$ is called a *polycyclic sequence* (or sometimes a *polycyclic generating sequence*) for G if

$$G_i/G_{i+1} = \langle g_i G_{i+1} \rangle$$

for $i = 1, \ldots, n$. For every factor G_i/G_{i+1} we denote by $r_i \in \mathbb{N} \cup \{\infty\}$ the index of G_{i+1} in G_i. We call $(r_1, \ldots, r_n)$ the *relative orders* of $\mathcal{G}$.

2.1.2 Lemma: *Let g be an element of a polycyclic group G with polycyclic sequence $\mathcal{G} = (g_1, \ldots, g_n)$. Then we can write g uniquely as*

$$g = g_1^{e_1} \cdot \cdots \cdot g_n^{e_n}$$

where $(e_1, \ldots, e_n) \in \mathbb{Z}^n$ and $0 \leq e_i < r_i$ if $r_i < \infty$.

Proof: We proof the lemma by induction. Let $g \in G_n$. Then g can be uniquely written as $g = g_n^{e_n}$ where $e_n \in \mathbb{Z}$ and $0 \leq e_n < r_n$ if $r_n < \infty$.

Now we assume that $g \in G_i$ with $i < n$. Since $G_i/G_{i+1} = \langle g_i G_{i+1} \rangle$ there exists an $\hat{e}_i \in \mathbb{Z}$ such that $gG_{i+1} = g_i^{\hat{e}_i} G_{i+1}$. The number $\hat{e}_i$ is unique if $r_i = \infty$. Then we set $e_i := \hat{e}_i$. If $r_i < \infty$, then the exponent can be uniquely chosen by setting $e_i := \hat{e}_i \mod r_i$. It follows that $g_i^{-e_i} g \in G_{i+1}$. By induction we can suppose that we can write uniquely $g_i^{-e_i} g = g_{i+1}^{e_{i+1}} \cdots g_n^{e_n}$ where $(e_{i+1}, \ldots, e_n) \in \mathbb{Z}^{n-i}$ and $0 \leq e_j < r_j$ if $r_j < \infty$ for $j = i+1, \ldots, n$. We deduce that

$$g = g_i^{e_i} \cdots g_n^{e_n}.$$

For $i = 1$ this gives the wanted result. •

2.1.3 Definition: The unique list $(e_1, \ldots, e_n) \in \mathbb{Z}^n$ from the last Lemma 2.1.2 is called the *exponent vector* of g with respect to $\mathcal{G}$. It will be denoted by $\exp_{\mathcal{G}}(g)$.

2.1.4 Example: Regard the group G generated by the matrices

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

We verify that $g_2^{g_1} = g_2^{-1} \in \langle g_2 \rangle$. Thus

$$G \rhd \langle g_2 \rangle \rhd 1$$

is a subnormal series of G with cyclic factors and so G is polycyclic. The list $\mathcal{G} = (g_1, g_2)$ is a polycyclic sequence for G with relative orders $(2, \infty)$. Consider the element

$$g := \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \in G.$$

It is easy to see that $g = g_1 g_2^{-2}$ and so $\exp_{\mathcal{G}}(g) = (1, -2)$.

2.1.5 Definition: Let G be a polycyclic group. A polycyclic sequence $\mathcal{G}$ for G is called a *constructive polycyclic sequence (constructive pc-sequence)*, if the relative orders of $\mathcal{G}$ are known and if there exists a practical algorithm, which computes for any element $g \in G$ the exponent vector $\exp_{\mathcal{G}}(g)$.

Note that in general, it is a non-trivial task to find a constructive polycyclic sequence for a polycyclic matrix group.

2.2 Polycyclic presentations

Let G be a polycyclic group with a polycyclic sequence $\mathcal{G} = (g_1, \ldots, g_n)$ and relative orders $(r_1, \ldots, r_n)$. Denote by I the finite index set of $\mathcal{G}$, that is

$$I := \{\, i \,|\, 1 \leq i \leq n, r_i \neq \infty \,\}.$$

By the properties of a polycyclic group it follows that $g_i^{g_j^{\pm 1}} \in G_{j+1}$ for $1 \leq j < i \leq n$ and $g_i^{r_i} \in G_{i+1}$ for $1 \leq i \leq n$ and $r_i \neq \infty$. Thus we can write these expressions as words in the generators $g_{j+1}, \ldots, g_n$ respectively $g_{i+1}, \ldots, g_n$.

2.2.1 Definition: The equations

$$\begin{aligned} g_i^{g_j} &= g_{j+1}^{a(i,j,j+1)} \cdots g_n^{a(i,j,n)} \text{ for } 1 \leq j < i \leq n, \\ g_i^{g_j^{-1}} &= g_{j+1}^{b(i,j,j+1)} \cdots g_n^{b(i,j,n)} \text{ for } 1 \leq j < i \leq n \text{ and } j \notin I \end{aligned}$$

are called the conjugate relations and

$$g_i^{r_i} = g_{i+1}^{c(i,i+1)} \cdots g_n^{c(i,n)} \text{ for } i \in I$$

are said to be the power relations of the polycyclic sequence $\mathcal{G}$.

The next theorem shows that the power-conjugate relations of a polycyclic sequence give rise to a finite presentation for the group G.

2.2.2 Theorem: *Let $\mathcal{G}$ be a polycyclic sequence of a polycyclic group G with power-conjugate relations as in Definition 2.2.1. Let F be a free group on the abstract generators in $\mathcal{F} = \{ f_1, \ldots, f_n \}$. Define R to be the set of relations*

$$\begin{aligned} f_i^{f_j} &= f_{j+1}^{a(i,j,j+1)} \cdots f_n^{a(i,j,n)} \text{ for } 1 \leq j < i \leq n, \\ f_i^{f_j^{-1}} &= f_{j+1}^{b(i,j,j+1)} \cdots f_n^{b(i,j,n)} \text{ for } 1 \leq j < i \leq n \text{ and } j \notin I \\ f_i^{r_i} &= f_{i+1}^{c(i,i+1)} \cdots f_n^{c(i,n)} \text{ for } i \in I. \end{aligned}$$

Then $\langle \mathcal{F} \,|\, R \rangle$ is a presentation for G.

Proof: See [21] Section 9.4. or [6] Chapter 2, Lemma 2.2. •

2.2.3 Definition: The finite presentation $\langle \mathcal{F} \,|\, R \rangle$ of a polycyclic group G of Theorem 2.2.2 is called a *polycyclic presentation (pc-presentation)* of G.

2.2.4 Example: Consider the group G defined in Example 2.1.4 with the polycyclic sequence $\mathcal{G} = (g_1, g_2)$. We obtain the power-conjugate relations

$$\begin{aligned} g_2^{g_1} &= g_1^0 g_2^{-1} \\ g_1^2 &= g_1^0 g_2^0 \end{aligned}$$

of $\mathcal{G}$. By Theorem 2.2.2

$$\left\langle f_1, f_2 \mid f_2^{f_1} = f_2^{-1},\ f_1^2 = 1 \right\rangle$$

is a polycyclic presentation for G. Note that G is the infinite dihedral group.

2.2.5 Corollary: *Let $\mathcal{G}$ be a constructive pc-sequence of a polycyclic group G. Then by calculating the power-conjugate relations we can calculate a polycyclic presentation for G.*

2.3 Solvable versus polycyclic

The class of polycyclic groups is closed with respect to forming subgroups, factor groups and extensions (see [21] Section 9.3). Further, every polycyclic group is solvable but the converse is not true. In the following we recall some connections between solvable and polycyclic groups.

2.3.1 Theorem: *A group G is polycyclic if and only if it is solvable and every subgroup of G is finitely generated. In particular a finite group is polycyclic if and only if it is solvable.*

Proof: See [20] Chapter 1, Proposition 4. •

2.3.2 Theorem: *Every solvable group of automorphisms of a polycyclic group is polycyclic.*

Proof: See [20] Chapter 2, Theorem 1. •

2.3.3 Corollary: *Let G be subgroup of $GL(d, \mathbb{Z})$. Then G is polycyclic if and only if G is solvable.*

Proof: Let G be a solvable subgroup of $GL(d, \mathbb{Z})$. The additive group $\mathbb{Z}^d$ is polycyclic. Therefore, by Theorem 2.3.2, $G \leq GL(d, \mathbb{Z}) = Aut(\mathbb{Z}^d)$ is polycyclic. Conversely, we assume that G is a polycyclic group. Then G is solvable by Theorem 2.3.1. •

2.4 Matrix groups

Let G be a subgroup of $GL(d,\mathbb{Q})$ which is generated by a finite number of elements $g_1,\ldots,g_k$. Define π to be the set of primes which divide a denominator of a matrix entry of $g_1,\ldots,g_k,g_1^{-1},\ldots,g_k^{-1}$. Denote by $\mathbb{Q}_\pi$ the set of rational numbers whose denominator is divisible by primes in π only. Then it can be observed readily, that the group G is contained in $GL(d,\mathbb{Q}_\pi)$.

2.4.1 Definition: Let $G \leq GL(d,\mathbb{Q}_\pi)$ and let p be an odd prime which is not contained in π. Then p is called an *admissible prime* for the matrix group G.

If $p \notin \pi$, then there is an homomorphism

$$\begin{array}{rccl} \chi_p: & \mathbb{Q}_\pi & \to & \mathbb{Z}/p\mathbb{Z} \\ & \frac{a}{b} & \to & (a+p\mathbb{Z})\cdot(b+p\mathbb{Z})^{-1}. \end{array}$$

2.4.2 Definition: Let be G be a subgroup of $GL(d,\mathbb{Q}_\pi)$ and let p be an admissible prime for G. The map

$$\psi_p : G \to GL(d,p)$$

which applies χ_p to every entry of a matrix $g \in G$, is said to be the *p-congruence homomorphism* from G to $GL(d,p)$. The kernel of ψ_p is denoted by $K_p(G)$ and is said to be the *p-congruence subgroup* of G. The image of ψ_p is called the *p-modular image* and we denote it by $I_p(G)$.

2.4.3 Definition: Let U be a subgroup of $GL(d,\mathbb{Q})$. An element $u \in U$ is called *unipotent* if there exists a natural number $m \in \mathbb{N}$ such that

$$(u-1)^m = 0.$$

The group U is called *unipotent*, if every element in U is unipotent.

We can now formulate the important structure theorem of Dixon on which the algorithms in this book are based.

2.4.4 Theorem: *Let G be a finitely generated subgroup of $GL(d,\mathbb{Q}_\pi)$ and p an admissible prime for G. If the kernel $K_p(G)$ of the p-congruence homomorphism has a solvable subgroup of finite index, then the commutator subgroup $K_p(G)'$ is unipotent. Further, the group $K_p(G)$ is torsion-free.*

Proof: See [5] Lemma 9 and Section 7. •

2.4.5 Corollary: *Let G be a polycyclic subgroup of $GL(d,\mathbb{Q})$. Then the kernel $K_p(G)$ of the p-congruence homomorphism is torsion-free and $K_p(G)'$ is unipotent.*

Proof: If G is polycyclic, then $K_p(G)$ is polycyclic as well. Thus $K_p(G)$ is solvable and we can apply Theorem 2.4.4. •

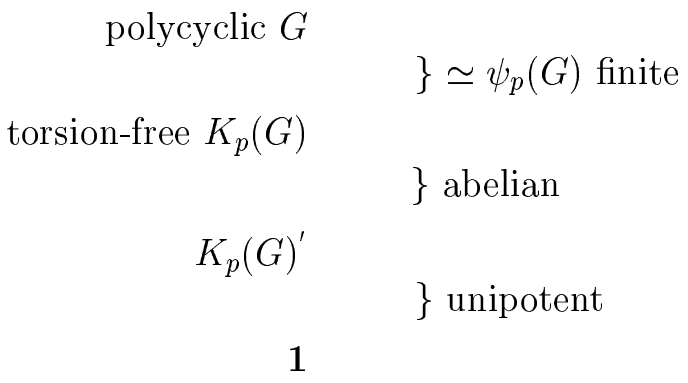


Figure 2.1: Corollary 2.4.5 to Dixon's Theorem

Chapter 3

Finite solvable matrix groups

Let $G \leq GL(d, R)$ be a finite matrix group where R is a ring. By Theorem 2.3.1 the group G is solvable if and only if G is polycyclic. In this chapter we want to describe a method to compute a polycyclic presentation (see Definition 2.2.3) for G, if G is solvable. Further, our algorithm can be used to test if G is solvable.

Recall that a constructive polycyclic sequence of a group G is a polycyclic sequence, for which the relative orders are known, and a practical algorithm is given to compute the exponent vector for any element g in G. By Corollary 2.2.5, it is sufficient to calculate a constructive polycyclic sequence for G, to obtain a polycyclic presentation for G.

We use an inductive approach for this purpose. For the trivial subgroup $N := \{1\} \lhd G$ a constructive polycyclic sequence is given. For the induction step we assume, that a constructive polycyclic sequence for a normal subgroup N of G is available. In the following Section 3.1 we show how to extend such a constructive polycyclic sequence to a group $H := \langle g, N \rangle$ where g is in $G \backslash N$. Then in Section 3.2 we present methods to compute suitable elements g for such an extension. Finally in Section 3.3 the algorithm for the calculation of a constructive polycyclic sequence of a finite solvable matrix group is presented.

3.1 Cyclic extensions of constructive pc-sequences

Let N be a normal subgroup of a finite solvable matrix group G acting faithfully on set W. Suppose that a constructive pc-sequence for N is given, consisting of the elements

$$\mathcal{N} = (n_1, \ldots, n_k)$$

with relative orders $(r_1, \ldots, r_k)$. Further let g be an element of $G \backslash N$ and define $H := \langle g, N \rangle$. The group H is called a *cyclic extension* of N. We want to extend the constructive pc-sequence of N to a constructive pc-sequence

$$\mathcal{H} = (g, n_1, \ldots, n_k)$$

of H. The following lemma follows directly from the definition of the relative orders and the exponent vector.

3.1.1 Lemma:

1. *Let r be the smallest natural number such that $g^r \in N$ and hence $r = [H : N]$. Then the relative orders of $\mathcal{H}$ are given by $(r, r_1, \ldots, r_k)$.*
2. *Let $h = g^e n$ be an arbitrary element of H where $e \in \mathbb{Z}$ and $n \in N$. This implies that*

$$exp_{\mathcal{H}}(h) = (e \bmod r, exp_{\mathcal{N}}(n)).$$

In our way to the extension of a constructive pc-sequence, stabilizers and orbits will play an important role. They allow us to divide the calculation of the relative order r in smaller pieces. For this reason we recall some basic definitions:

3.1.2 Definition: Let G be a group acting on a set $W := \{1, \ldots, n\}$ and let $B := (w_1, \ldots, w_k)$ be a sequence of different points in W. Define $G_0 := G$ and $G_i := Stab_{G_{i-1}}(w_i)$ for $1 \leq i \leq k$. Then the series

$$G = G_0 \geq G_1 \geq \cdots \geq G_k$$

is called the *stabilizer-chain* corresponding to B. The sequence B is called a *base* for G, if the group G_k is trivial.

Since N is a normal subgroup of the matrix group G, we note that

$$(wN)g = (wg)N$$

for all g in G. Therefore G acts on the set of N-orbits in W. The following lemma shows, that the stabilizers H_i have the same relationship to the stabilizers N_i as H to N. This is the reason, why the concept of a base and its corresponding stabilizers is very useful for the determination of the structure of a cyclic extension.

3.1.3 Lemma: *Let N be a normal subgroup of G acting faithfully on a set W. Define the group H to be a cyclic extension of N generated by N and an element $g \in G\backslash N$. Then there exists a natural number $l = l(H,N) \in \mathbb{N}$ and an element $n \in N$ such that*

$$Stab_H(w) = \left\langle g^l n^{-1}, Stab_N(w) \right\rangle$$

for any $w \in W$. Therefore $Stab_H(w)$ is a cyclic extension of $Stab_N(w)$.

Proof: Let w be an element of W. The group H acts on the set of N-orbits in W and so there exists a $l = l(H,N) \in \mathbb{N}$ such that we can write wH as the disjoint union

$$wH = wN \cup wNg \cup \cdots \cup wNg^{l-1}.$$

We deduce that $wNg^l = wN$ and hence there exists an $n \in N$ such that $wg^l = wn$. So the group $\langle g^l n^{-1}, Stab_N(w)\rangle$ is contained in the stabilizer of w in H.

Conversely suppose that h is an element of $Stab_H(w)$ and write $h = g^e\hat{n}$ for a natural number $e \in \mathbb{N}$ and $\hat{n} \in N$. Now it follows that

$$wN = (wh)N = (wg^e\hat{n})N = wNg^e$$

and so $e = k \cdot l$ by the choice of l. This implies that

$$g^e\hat{n} = g^{kl}\hat{n} = \left(g^l n^{-1} n\right)^k \hat{n} = \left(g^l n^{-1}\right)^k \bar{n}\hat{n}$$

for some $\bar{n} \in N$. We deduce that $\bar{n}\hat{n}$ must be an element of $Stab_N(w)$, because $g^e\hat{n}$ and $\left(g^l n^{-1}\right)^k$ stabilize w. Thus h is contained in $\langle g^l n^{-1}, Stab_N(w)\rangle$.
•

The following picture resumes the result of Lemma 3.1.3.

$H := \langle g, N \rangle$

N

$Stab_H(w) = \langle g^l n^{-1}, Stab_N(w) \rangle$

$Stab_N(w)$

The last lemma leads us to a method for the calculation of the index $[H : N]$.

3.1.4 Proposition: *Let $N = N_0$ be a normal subgroup of G which acts faithfully on a set W and let $B := \{w_1, \ldots, w_k\}$ be base for N. Denote by $H = H_0$ the cyclic extension $\langle g, N \rangle$, where g is an element of $G \backslash N$. Let $\hat{B} = \{w_1, \ldots, w_k, w_{k+1}, \ldots, w_{\hat{k}}\}$ be a base for H and define $H_i := Stab_{H_{i-1}}(w_i)$ and $N_i := Stab_{N_{i-1}}(w_i)$ for $1 \leq i \leq \hat{k}$. Then the iterated application of Lemma 3.1.3 to the stabilizer-chain H_i can be used to calculate the index*

$$[H : N] = \prod_{i=1}^{\hat{k}} l(H_{i-1}, N_{i-1}).$$

Proof: By repeated application of Lemma 3.1.3 there exists an $l_i = l(H_{i-1}, N_{i-1}) \in \mathbb{N}$, $n_i \in N_{i-1}$ such that

$$H_i := \left\langle g_i^{l_i} n_i^{-1}, N_i \right\rangle$$

for $1 \leq i \leq k$ where $g_1 := g$ and $g_i := g_{i-1}^{l_{i-1}} n_{i-1}^{-1}$ for $2 \leq i \leq k+1$. Therefore $H_k = \left\langle g_k^{l_k} n_k^{-1} \right\rangle$ and so this group is cyclic. If H_k is non-trivial we extend the set $B = \{w_1, \ldots, w_k\}$ to a set $\hat{B} = \{w_1, \ldots, w_k, w_{k+1}, \ldots, w_{\hat{k}}\}$ such that $H_{\hat{k}}$ is trivial. Then $\hat{B}$ is a base for H. Recall that the number $l_i := l(H_{i-1}, N_{i-1})$ is defined to be the smallest natural number such that $w_i g_i^{l_i} = w_i$ for $k+1 \leq i \leq \hat{k}$ where $g_i = g_{i-1}^{l_{i-1}}$ for $k+2 \leq i \leq \hat{k}$. Now we claim that

$$[H : N] = \prod_{i=1}^{\hat{k}} l_i = \prod_{i=1}^{\hat{k}} l(H_{i-1}, N_{i-1}).$$

Since $g_{\hat{k}}^{l_{\hat{k}}} \in H_{\hat{k}} = \{1\}$ we deduce that

$$1 = g_{\hat{k}}^{l_{\hat{k}}} = g_{k+1}^{\prod_{i=k+1}^{\hat{k}} l_i} = g^{\prod_{i=1}^{\hat{k}} l_i} \tilde{n}$$

for some $\tilde{n} \in N$. This implies that $[H : N]$ divides $\prod_{i=1}^{\hat{k}} l_i$.

Conversely, since l_1 is the smallest number such that $w_1 N_0 g_1^{l_1} = w_1 N_0$, we deduce that l_1 divides $[H : N]$, which is the order gN in G/N. The element $g_2 N = (g_1^{l_1} n_1^{-1})N = g_1^{l_1} N$ is of order $[H : N]/l_1$ in G/N. Thus the number l_2 must divide $[H : N]/l_1$, because l_2 is the smallest number such that $w_2 N_1 = w_2 N_1 g_2^{l_2}$ and $g_2^{[H:N]/l_1} \in N_1$. By induction we follow that $\prod_{i=1}^{\hat{k}} l_i$ divides the index $[H : N]$, which shows that the equality holds. •

Lemma 3.1.1 demanded first to calculate the index $[H : N]$ for completing the list of relative orders of the pc-sequence of the group $H = \langle g, N \rangle$. Second for a given element $h \in H$ we should be able to determine a natural number e such that $h = g^e n$ for an $n \in N$, for the calculation of the exponent vector of h. This can be realized by shifting through the orbits, which arise in the calculation of the index $[H : N]$.

3.1.5 Lemma: *Denote by N and $H := \langle g, N \rangle$ groups like in the Proposition 3.1.4. Suppose that the index $[H : N]$ were calculated by the methods in Proposition 3.1.4 and that the arising orbits of the points $w_i \in \hat{B}$ were stored including the corresponding transversals. Let h be an element of H. Then by shifting through the orbits $w_i N_{i-1}$ a natural number e can be determined such that $h = g^e n$.*

Proof: By induction we want to proof that for $h_i \in H_{i-1} = \langle g_i, N_{i-1} \rangle$ we can determine a natural number e_i such that $h_i = g_i^{e_i} \tilde{n}_i$ where $\tilde{n}_i \in N_{i-1}$. For $i = 1$ this gives the wanted result. First let $i = \hat{k} + 1$. Then $e_i = 0$ because $H_{\hat{k}}$ is trivial. Now we assume that $i \in \{1, \ldots, \hat{k}\}$. By construction we know that

$$w_i H_{i-1} = w_i N_{i-1} \cup w_i N_{i-1} g_i \cup \cdots \cup w_i N_{i-1} g_i^{l_i - 1}.$$

Using the membership test for the orbits, we can determine a natural number $s \in \{0, \ldots, l_i - 1\}$ such that $w_i N_{i-1} h_i = w_i N_{i-1} g_i^s$ and an $\bar{n}_i \in N_{i-1}$ such that $h_{i+1} := h_i g_i^{-s} \bar{n}_i$ is an element of $H_i = Stab_{H_{i-1}}(w_i)$. By induction we suppose that we can calculate a natural number e_{i+1} such that $h_{i+1} = g_{i+1}^{e_{i+1}} \tilde{n}_{i+1}$. It follows that

$$h_{i+1} = g_{i+1}^{e_{i+1}} \tilde{n}_{i+1} = (g_i^{l_i} n_i^{-1})^{e_{i+1}} \tilde{n}_{i+1} = g_i^{l_i e_{i+1}} \hat{n}_{i+1}$$

for some $\hat{n}_{i+1} \in N$. We deduce that

$$h_i = h_{i+1}(\bar{n}_i^{-1} g_i^s) = g_i^{l_i e_{i+1}} \hat{n}_{i+1}(\bar{n}_i^{-1} g_i^s) = g_i^{l_i e_{i+1} + s} \hat{n}$$

for some $\hat{\hat{n}} \in N$. The element $\hat{\hat{n}}$ must be in N_{i-1} because h_i and g_i stabilize w_{i-1}. Therefore we can set $e_i := l_i e_{i+1} + s$. •

Now all the necessary elements for the extension of a constructive polycyclic pc-sequence of N are given. For the implementation we store the arising orbits $w_i N_{i-1}$ under H and the corresponding transversals. Together with the relative orders this data structure includes all the necessary data for the determination of exponents vectors and a membership test.

3.2 Abelian Upwards Extensions

Let N be a normal subgroup of G and suppose that N is given by a constructive polycyclic sequence

$$\mathcal{N} = (n_1, \ldots, n_k).$$

Our aim is to compute an abelian upwards extension of N. This is a group H such that $N \lhd H \trianglelefteq G$ and H/N is abelian. Assume that H is generated by $\{h_1, \ldots, h_l\}$ and N. Since H/N is abelian, all groups $\hat{H}$ with $N \leq \hat{H} \leq H$ are normal subgroups of H by the correspondence principle. Therefore

$$\mathcal{H} = (h_1, \ldots, h_l, n_1, \ldots, n_k)$$

is a polycyclic sequence for H. So the elements $h_1, \ldots, h_l$ can be used to extend the constructive polycyclic sequence of N step by step to a constructive pc-sequence of H.

Let g be an arbitrary element of $G \backslash N$. We describe a method which tests if $\langle g, N \rangle^G$ is an abelian upwards extension of N. If the result is positive, then it returns a generator list for H. If $\langle g, N \rangle^G / N$ is not abelian, then it returns an element whose use we will discuss later.

The concept is the following: We regard $\bar{\mathcal{E}} := \{gN\}$ as an incomplete generator list for $\langle g, N \rangle^G / N$. Now, we add conjugates under the action of the generators of G to $\bar{\mathcal{E}}$. We iterate this procedure. During the extension of the generator list, we test if all elements in $\bar{\mathcal{E}}$ commute, i.e. $[\varepsilon_i N, \varepsilon_j N] = N$ holds for all $\varepsilon_i N, \varepsilon_j N \in \bar{\mathcal{E}}$, which is equivalent to $[\varepsilon_i, \varepsilon_j] \in N$ (ε_i and ε_j commute modulo N).

```
AbelianUpwardsExtension( G, N, g )
(01)    set 𝓔 := {g}
(02)    # close 𝓔 under the conjugation action of G
(03)    for every element ε in 𝓔 do
(04)        Ê := { ε^g | g generator of G }
(05)        if all elements in 𝓔 ∪ Ê commute modulo N then
(06)            set 𝓔 := 𝓔 ∪ Ê
(07)        else
(08)            return [ε_i, ε_j] such that [ε_i, ε_j] ∉ N
(09)        end if
(10)    end for
(11)    return 𝓔
```

The algorithm terminates because G is a finite group, and so we can add only a finite number of elements to $\mathcal{E}$.
If this method returns a list $\mathcal{E}$, then $H := \langle \mathcal{E}, N \rangle$ is an abelian upwards extension of N. Namely H/N is non empty (because $g \notin N$), H/N is abelian and $H \trianglelefteq G$ (because $N \trianglelefteq G$ and $(H/N)^G = H/N$).
If the algorithm returns an element $\hat{g}$, then $\hat{g} = [g^x, g^y] \notin N$ where x, y are words in the generators of G. Under the assumption that g is contained in the i-th term $G^{(i)}$ of the derived series, we deduce that $\hat{g} \in G^{(i+1)}$ because $g^x, g^y \in G^{(i)}$.

The element $\hat{g}$ can be used for a recursive call with the input $(G, N, \hat{g})$. Since the length of the derived series of $G \leq GL(d, R)$ is bounded by $d + 2$ (see Theorem 3.3.1), a repetitive application of this algorithm can be made only a finite number of times.

We note that `AbelianUpwardsExtension` blows up the generator list $\mathcal{E}$ in a wasteful manner. In the sixth line we extend the generators list $\mathcal{E}$ by elements of $\hat{\mathcal{E}}$. But we do not check, if an element $\hat{e} \in \hat{\mathcal{E}}$ is already contained in the group $\langle \mathcal{E}, N \rangle$. We can respond to this problem, by using extensions of the constructive polycyclic sequence of N described in Section 3.1.

```
AbelianUpwardsExtensionFaster( G, N, g )
  set 𝓔 := {g}
  set H := ⟨ g, N ⟩
  for every element ε in 𝓔 do
     Ê := { e^g | g generator of G }
     for every element ê ∈ Ê do
```

```
      if ε̂ commutes with all elements in ε_i ∈ E modulo N then
        if not ε̂ ∈ H
          set H := ⟨ ε̂, H ⟩
          (extension of a constructive pc-sequence, see 3.1)
          add ε̂ to E
        end if
      else
        return [ε̂, ε_i] such that [ε̂, ε_i] ∉ N
      end if
    end for
  end for
  return H
```

3.3 Constructive polycyclic sequences

Let $G \leq GL(d, R)$ be a finite matrix group where R is a ring. We present an algorithm which computes a constructive polycyclic sequence for G.

In the last section we remarked, that the function `AbelianUpwardsExtensionFaster` can be used for a recursive call. We specify this now. Let N be a normal subgroup of G for which a constructive pc-sequence is already known. Let g be an element of $G \backslash N$ and let $i \in \mathbb{N} \cup \{0\}$ such that g is in the i-th term $G^{(i)}$ of the derived series. Then the following method can be used to extend the constructive pc-sequence of N to the group $\langle g, N \rangle$.

```
Extension( G, N, g, i )
  if i > bound for the derived length of G then
      return fail (G is not polycyclic)
  end if
  h := AbelianUpwardsExtensionFaster( G, N, g )
  if h is a group element then
      N_new := Extension( G, N, h, i+1 )
      return Extension( G, N_new, g, i )
  else
      return h
  end if
```

In the second line of the last algorithm we need to know the derived length of G (or a least un upper bound for it). This is given by the following theorem.

3.3.1 Theorem: *Let G be a polycyclic subgroup of $GL(d, R)$. Then the length of the derived series of G is bounded by $d + 2$.*

Proof: See [16]. •

Now a constructive pc-sequence for the matrix group G can be computed via the following method.

```
ConstructivePcSequenceFinite( G )
  set N := ⟨1⟩
  for every generator g of G do
      N := Extension( G, N, g, 0)
      if N = fail then
          return "G is not polycyclic"
      end if
  end for
  return N
```

Chapter 4

Algebraic number fields

Denote by $\mathbb{F}$ an algebraic extension of the field $\mathbb{Q}$ and let $\mathcal{A} := \{a_1, \ldots, a_n\}$ be a finite subset of $\mathbb{F} \setminus \{0\}$, where $a_i \neq 0$ for $i = 1, \ldots, n$. The aim of this chapter is to describe an algorithm to calculate a presentation for the abelian multiplicative group $A := \langle a_1, \ldots, a_n \rangle$. Certainly A is polycyclic (for example, $\mathcal{A}$ is a polycyclic sequence). Therefore by Corollary 2.2.5 it is sufficient to determine a constructive polycyclic sequence for A. This is a polycyclic sequence, for which the relative orders are known and a efficient method is given to calculate exponent vectors (see Definition 2.1.5).

It will turn out, that the following set plays an important role.

4.0.2 Definition: Let $\mathcal{E} = \{h_1, \ldots, h_l\}$ be a subset of an abelian group A. The relation lattice for $\mathcal{E}$ is

$$rl(\mathcal{E}) := \left\{ (e_1, \ldots, e_l) \in \mathbb{Z}^l \mid h_1^{e_1} \cdots h_l^{e_l} = 1 \right\}.$$

Since A is an abelian group, the sum of two in elements in $rl(\mathcal{E})$ is still in $rl(\mathcal{E})$. Thus, the name lattice is justified.

An algorithm to determine $rl(\mathcal{A})$ is presented in Section 4.1. Afterwards, in Section 4.2, we describe a method that uses the relation lattices to compute a constructive polycyclic sequence for the group A. In Section 4.3 we give an example application.

Before we start the description of the algorithms, we state three basic definitions of algebraic number theory. For further background see [23].

4.0.3 Definition: Let $\mathbb{F}$ be a subfield of $\mathbb{C}$ such that $[\mathbb{F} : \mathbb{Q}]$ is finite. Then $\mathbb{F}$ is called a *number field* or an *algebraic extension* of $\mathbb{Q}$.

4.0.4 Definition: A complex number θ is said to be an *algebraic integer*, if the minimal polynomial f_θ of θ is in $\mathbb{Z}[X]$.

4.0.5 Definition: Let $\mathbb{F}$ be a number field. The set of algebraic integers in $\mathbb{F}$ is called the *maximal order* $\mathcal{O}$ of $\mathbb{F}$. An element $u \in \mathcal{O}$ is called a *unit*, if u^{-1} is also contained in $\mathcal{O}$. The set of all units in $\mathcal{O}$ is called the *unit group* of $\mathcal{O}$ and is denoted by $U(\mathcal{O})$.

4.1 Computing relation lattices in number fields

Let $\mathcal{A} := \{a_1, \ldots, a_n\}$ be a finite subset of a number field $\mathbb{F}$ with $a_i \neq 0$ for $i = 1, \ldots, n$. Our aim is to determine the relation lattice $rl(\mathcal{A})$. Recall that this is defined as

$$rl(a_1, \ldots, a_n) := \left\{ (e_1, \ldots, e_n) \in \mathbb{Z}^n | \prod a_i^{e_i} = 1 \right\}.$$

We proceed in three steps: First we calculate the unit relation lattice, defined as

$$url(a_1, \ldots, a_n) := \left\{ (e_1, \ldots, e_n) \in \mathbb{Z}^n | \prod a_i^{e_i} \in U(\mathcal{O}) \right\}$$

where $U(\mathcal{O})$ is the group of units of the maximal order $\mathcal{O}$ of $\mathbb{F}$. Every vector $r = (r_1, \ldots, r_n)$ in a basis $\mathcal{B}$ of $url(A)$ gives rise to a unit

$$u(r) = a_1^{r_1} \cdot a_2^{r_2} \cdots a_n^{r_n} \in U(\mathcal{O}).$$

Second, we will calculate the relation lattice of the elements

$$\{ u(r) \mid r \in \mathcal{B} \}.$$

Third, using the achieved informations we will be able to calculate the relation lattice of the set $\mathcal{A}$.

4.1.1 Calculating the unit relation lattice

Before we start to describe a method for the calculation of the unit relation lattice $url(a_1, \ldots, a_n)$, we want to show with the following example, how unique factorization can be used for the calculation of a relation lattice of elements in an abelian group.

4.1.1 Example: Suppose that three numbers $49, 21$ and 9 are given and our task is to find the relation lattice $rl(49, 21, 9)$, i.e. the set of all relation vectors (r_1, r_2, r_3) in $\mathbb{Z}^3$ such that

$$49^{r_1} \cdot 21^{r_2} \cdot 9^{r_3} = 1.$$

If we want to do this in a systematic way, we could do the following: Factorize these numbers and get

$$49 = 7^2 \ , \ \ 21 = 7 \cdot 3 \ , \ \ 9 = 3^2.$$

Now we can solve the problem for each of the arising factors. For example, a relation vector (r_1, r_2, r_3) of 49,21 and 9 must eliminate all the occurring powers of 7 and thus

$$7^{2r_1} \cdot 7^{r_2} \cdot 7^{0 \cdot r_3} = 1.$$

This gives rise to two conditions:

	49	**21**	**9**		
7	$2 \cdot r_1$	$+ 1 \cdot r_2$	$+ 0 \cdot r_3$	$=$	0
3	$0 \cdot r_1$	$+ 1 \cdot r_2$	$+ 2 \cdot r_3$	$=$	0

Solving these equations we find that $rl(49, 21, 9)$ must be a subset of $\mathbb{Z}(1, -2, 1)$. Conversely every element of $\mathbb{Z}(1, -2, 1)$ lies in $rl(49, 21, 9)$ and so we have

$$rl(49, 21, 9) = \{\ z(1, -2, 1) \mid z \in \mathbb{Z}\ \}.$$

Unfortunately we are not always able to determine a unique factorization of the elements $a_i \in \mathbb{F}$ into irreducible factors. For example in the ring of integers of $\mathbb{Q}(\sqrt{-5})$ we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

where 2, 3, $(1 + \sqrt{-5})$ are $(1 - \sqrt{-5})$ are irreducible. So in the following we use fractional ideals and describe a method to factorize expressions like $(a_i) = a_i\mathcal{O}$. First we remind the reader of some results of their arithmetic structure. A more detailed description of fractional ideals can be found in [23] Chapter 5.

4.1.2 Definition: Let $\mathbb{F}$ be a extension field of $\mathbb{Q}$ and $\mathcal{O}$ its maximal order. An $\mathcal{O}$-submodule $\mathfrak{a}$ of $\mathbb{F}$ is called a fractional ideal of $\mathcal{O}$, if there exists some non-zero $c \in \mathcal{O}$ such that $c\mathfrak{a} \subset \mathcal{O}$.

4.1.3 Lemma: *The fractional ideals of $\mathcal{O}$ are subsets of $\mathbb{F}$ of the form $c^{-1}\mathfrak{b}$, where $\mathfrak{b}$ is an ideal of $\mathcal{O}$ and c is a non-zero element of $\mathcal{O}$.*

Proof: Suppose that $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$ and let $c \in \mathcal{O}, c \neq 0$ such that $c\mathfrak{a} \subset \mathcal{O}$. Then the set $\mathfrak{b} := c\mathfrak{a}$ must be an ideal of $\mathcal{O}$ and we deduce that $\mathfrak{a} = c^{-1}\mathfrak{b}$. •

As it turns out, in an algebraic number field, such fractional ideals can be uniquely factorized into the product of prime ideals.

4.1.4 Theorem: *The non-zero fractional ideals of $\mathcal{O}$ form an abelian group under multiplication, where the product of two fractional ideals $\mathfrak{a}_1, \mathfrak{a}_2$ is*

$$\mathfrak{a}_1\mathfrak{a}_2 = (c_1^{-1}\mathfrak{b}_1)(c_2^{-1}\mathfrak{b}_2) = (c_1c_2)^{-1}\mathfrak{b}_1\mathfrak{b}_2$$

and the inverse of a fractional ideal $\mathfrak{a}$ is defined as $\mathfrak{a}^{-1} := \{\, x \in \mathbb{F} \mid x\mathfrak{a} \subset \mathcal{O} \,\}$. The identity of this group is $\mathcal{O}$.

Proof: [23] Theorem 5.5. •

Further we need to know what are the prime elements in this arithmetical structure.

4.1.5 Definition: Let R be a ring. An ideal $\mathfrak{p}$ of R is called prime if for any two ideals $\mathfrak{a}, \mathfrak{b}$

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{p} \text{ implies } \mathfrak{a} \subset \mathfrak{p} \text{ or } \mathfrak{b} \subset \mathfrak{p}.$$

4.1.6 Remark: For the motivation of the last definition regard the ring $R = \mathbb{Z}$. Here an element p is called prime if from $p|ab$ we can always deduce that $p|a$ or $p|b$ for all $a, b \in \mathbb{Z}$. Then the element p is prime if and only if $p\mathbb{Z}$ is a prime ideal. The condition $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ corresponds to $p \mid ab$.)

4.1.7 Theorem: *Every non-zero fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ can be written uniquely up to the order of the factors as a finite product of prime ideals of $\mathcal{O}$:*

$$\mathfrak{a} = \prod \mathfrak{p}_i^{e_i} \quad e_i \in \mathbb{Z}$$

Proof: See [23] Theorem 5.6. and page 110. •

There are algorithms available for determining such a factorization (see [4] Section 4.8. and [18] Chapter 7). So we are able to factorize a given fractional ideal into a unique product of prime ideals.

4.1.8 Lemma: *Let $\mathbb{F}$ be a number field and denote by $\mathcal{O}$ its maximal order. If a is a non-zero element in $\mathbb{F}$, then $a\mathcal{O}$ is a fractional ideal.*

Proof: For a given number field $\mathbb{F}$, there always exists a complex number θ such that $\mathbb{F} = \mathbb{Q}(\theta)$. Every element a in $\mathbb{F}$ can be written as a $\mathbb{Q}$-linear combinations of powers of θ. So there exists an $m \in \mathbb{Z} \subset \mathcal{O}$ such that $m \cdot a \in \mathbb{Z}[\theta] \subset \mathcal{O}$. Therefore the $\mathcal{O}$-module $a\mathcal{O}$ is a fractional ideal. •

In the example 4.1.1 we found relations among the numbers 49, 21 and 9 via the factorization in prime powers. Now we can solve the problem of finding the relations among the fractional ideals $a_i\mathcal{O}$ via the factorization into prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$.

4.1.9 Definition: Let I be a non-zero fractional ideal of $\mathcal{O}$ and write

$$I = \prod_{j=1}^{l} \mathfrak{p}_j^{e_j}$$

The quantity $\nu_{\mathfrak{p}_j}(I) := e_j$ is called the $\mathfrak{p}_j$-adic valuation of I.

The $\mathfrak{p}$-adic valuation satisfies the property $\nu_{\mathfrak{p}}(IJ) = \nu_{\mathfrak{p}}(I) + \nu_{\mathfrak{p}}(J)$.

Recall that $\mathcal{A} := \{a_1, \ldots, a_n\}$ is a finite subset of a number field $\mathbb{F}$ with $a_i \neq 0$ for $i = 1, \ldots, n$. Let

$$(a_i) = a_i\mathcal{O} = \prod_{j=1}^{l} \mathfrak{p}_j^{e_{ij}}.$$

We construct the matrix $(\nu_{\mathfrak{p}_j}(a_i\mathcal{O}))_{ji}$

$$\begin{array}{c} \\ \mathfrak{p}_1 \\ \mathfrak{p}_2 \\ \vdots \\ \mathfrak{p}_l \end{array} \begin{array}{c} \begin{array}{cccc} (a_1) & (a_2) & \ldots & (a_n) \end{array} \\ \begin{pmatrix} e_{11} & e_{12} & \ldots & e_{1n} \\ e_{21} & e_{22} & \ldots & e_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ e_{l1} & e_{l2} & \ldots & e_{ln} \end{pmatrix} \end{array}$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ are the prime ideals appearing in the factorization of all the fractional ideals $a_i\mathcal{O}$ and $\nu_{\mathfrak{p}_j}(a_i\mathcal{O})$ is the $\mathfrak{p}_j$-adic valuation of $a_i\mathcal{O}$.

4.1.10 Proposition:

Let $\mathbb{F}$ be an extension field of $\mathbb{Q}$ and $a_1, \ldots, a_n$ be elements in $\mathbb{F}\backslash\{0\}$.

1. *Denote by $N \leq \mathbb{Z}^n$ the integral nullspace N of the matrix $(\nu_{\mathfrak{p}_j}(a_i))_{ji}$. Then $N = rl(a_1\mathcal{O}, \ldots, a_n\mathcal{O})$.*
2. *The relation lattice $rl(a_1\mathcal{O}, \ldots, a_n\mathcal{O})$ is equal to the unit relation lattice $url(a_1, \ldots, a_n) := \{(e_1, \ldots, e_n) \in \mathbb{Z}^n | \prod a_i^{e_i} \in U(\mathcal{O})\}$.*

Proof:

1. Let $r = (r_1, \ldots, r_n)$ be a vector in $\mathbb{Z}^n$. Then

$$\begin{aligned}
& (r_1, \ldots, r_n) \in rl(a_1\mathcal{O}, \ldots, a_n\mathcal{O}) \\
\Leftrightarrow \quad & (a_1)^{r_1} \cdots (a_n)^{r_n} = \mathcal{O} \\
\Leftrightarrow \quad & (\prod_{j=1}^{l} \mathfrak{p}_j^{\nu_{\mathfrak{p}_j}(a_1\mathcal{O})})^{r_1} \cdots (\prod_{j=1}^{l} \mathfrak{p}_j^{\nu_{\mathfrak{p}_j}(a_n\mathcal{O})})^{r_n} = \mathcal{O} \\
\Leftrightarrow \quad & \mathfrak{p}_1^{\sum_{i=1}^n r_i \nu_{\mathfrak{p}_1}(a_i\mathcal{O})} \cdots \mathfrak{p}_l^{\sum_{i=1}^n r_i \nu_{\mathfrak{p}_l}(a_i\mathcal{O})} = \mathcal{O} \\
\Leftrightarrow \quad & \sum_{i=1}^{n} r_i \nu_{\mathfrak{p}_j}(a_i\mathcal{O}) = 0 \quad \text{for } j = 1, \ldots, l \qquad \text{by Theorem 4.1.7} \\
\Leftrightarrow \quad & (\nu_{\mathfrak{p}_j}(a_i\mathcal{O}))_{ji} \cdot (r_1, \ldots, r_n)^t = 0
\end{aligned}$$

2. Let $r = (r_1, \ldots, r_n)$ be a vector in $\mathbb{Z}^n$. Then

$$\begin{aligned}
& (r_1, \ldots, r_n) \in rl(a_1\mathcal{O}, \ldots, a_n\mathcal{O}) \\
\Leftrightarrow \quad & (a_1)^{r_1} \cdots (a_n)^{r_n} = \mathcal{O} \\
\Leftrightarrow \quad & \prod_{i=1}^{n} a_i^{r_i}\mathcal{O} = \mathcal{O} \\
\Leftrightarrow \quad & \prod_{i=1}^{n} a_i^{r_i} \in U(\mathcal{O}) \\
\Leftrightarrow \quad & (r_1, \ldots, r_n) \in rul(a_1, \ldots, a_n)
\end{aligned}$$

•

4.1.2 Calculating the relation lattice in $U(\mathcal{O})$

Let $u_1, \ldots, u_m$ be units of the maximal order $\mathcal{O}$. Our task is to find the relations between these units. Again it is necessary to work in an unique factorization domain whose existence is guaranteed by the following theorem of Dirichlet.

4.1.11 Theorem: *Every unit u of an order over $\mathbb{Z}$ can be written uniquely as*

$$u = \zeta^{f_0} \cdot \varepsilon_1^{f_1} \cdot \varepsilon_2^{f_2} \cdots \varepsilon_r^{f_r}$$

where ζ is the generator of the torsion subgroup of $\mathcal{O}$ and $\varepsilon_1, \ldots, \varepsilon_r$ are the fundamental units of the maximal order.

Proof: [23] Appendix B. •

There are algorithms available for computing the torsion unit and the fundamental units (see [18] Chapter 6). Now we proceed as in Section 4.1.1.

4.1.12 Lemma: *Let $u_1, \ldots, u_m \in U(\mathcal{O})$. For $i = 1, \ldots, m$ write*

$$u_i = \zeta^{f_{0i}} \prod_{j=1}^{r} \varepsilon_j^{f_{ji}}$$

and define o_ζ to be the order of ζ. Denote by $R_1 \leq \mathbb{Z}^m$ the integral nullspace of the matrix

$$\begin{array}{c} \\ \varepsilon_1 \\ \vdots \\ \varepsilon_r \end{array} \begin{array}{c} \begin{array}{cccc} u_1 & u_2 & \ldots & u_m \end{array} \\ \begin{pmatrix} f_{11} & f_{12} & \ldots & f_{1m} \\ \ldots & \ldots & \ldots & \ldots \\ f_{r1} & f_{r2} & \ldots & f_{lm} \end{pmatrix} \end{array}$$

and let $R_2 \leq \mathbb{Z}^m$ such that $R_2/(o_\zeta \mathbb{Z})^m$ is the nullspace of the matrix

$$\begin{array}{c} \\ \zeta \end{array} \begin{array}{c} \begin{array}{cccc} u_1 & u_2 & \ldots & u_m \end{array} \\ \begin{pmatrix} f_{01} & f_{02} & \ldots & f_{0m} \end{pmatrix} \end{array}$$

in $\mathbb{Z}^m/(o_\zeta \mathbb{Z})^m$. Then $rl(u_1, \ldots, u_m) = R_1 \cap R_2$.

Proof: Let $r = (r_1, \ldots, r_m)$ be a vector in $\mathbb{Z}^m$. Then

$$\begin{aligned}
& (r_1, \ldots, r_m) \in rl(u_1, \ldots, u_m) \\
\Leftrightarrow \quad & u_1^{r_1} \cdots u_m^{r_m} = 1 \\
\Leftrightarrow \quad & (\zeta^{f_{01}} \prod_{j=1}^{r} \varepsilon_j^{f_{j1}})^{r_1} \cdots (\zeta^{f_{0m}} \prod_{j=1}^{r} \varepsilon_j^{f_{jm}})^{r_m} = 1 \\
\Leftrightarrow \quad & \zeta^{\sum_{i=1}^{m} f_{0i} r_i} \prod_{j=1}^{r} \varepsilon_j{}^{\sum_{i=1}^{m} f_{ji} r_i} = 1 \\
\Leftrightarrow \quad & \sum_{i=1}^{m} f_{0i} r_i = 0 \bmod o_\zeta \quad \text{and} \\
& \sum_{i=1}^{m} f_{ji} r_i = 0 \quad \text{for } j = 1, \ldots, r \qquad \text{by Theorem 4.1.11} \\
\Leftrightarrow \quad & (r_1, \ldots, r_m) \in R_1 \cap R_2
\end{aligned}$$

•

4.1.13 Lemma: *Let $u_1, \ldots, u_m \in U(\mathcal{O})$. If the multiplicative group*

$$\langle u_1, \ldots, u_m \rangle$$

is torsion-free then $R_1 \subset R_2$, where R_1, R_2 are defined as in Lemma 4.1.12.

Proof: Suppose that $R_1 \not\subset R_2$. Then there is an element $(r_1, \ldots, r_m) \in R_1 \setminus R_2$. We deduce that

$$\prod_{i=1}^{m} u_i^{r_i} = \prod_{i=1}^{m} (\zeta^{f_{0i}} \prod_{j=1}^{r} \varepsilon_j^{f_{ji}})^{r_i} = \underbrace{\zeta^{\sum_{i=1}^{m} f_{0i} r_i}}_{\neq 1 \text{ since } r \notin R_2} \underbrace{\prod_{j=1}^{r} \varepsilon_j^{\sum_{i=1}^{m} f_{ji} r_i}}_{=1 \text{ since } r \in R_1} \neq 1.$$

This implies that $\prod_{i=1}^{m} u_i^{r_i}$ would have finite non-trivial order, which is impossible. •

4.1.3 Summary

Let $a_i, \ldots, a_n$ be arbitrary elements of an extension field of $\mathbb{Q}$. Now we are in the position to describe a method to calculate the relation lattice

$$rl(a_1, \ldots, a_n) := \{(e_1, \ldots, e_n) \in \mathbb{Z}^n | \prod a_i^{e_i} = 1\}.$$

Suppose that $url(a_1, \ldots, a_n) \leq \mathbb{Z}^n$ has dimension m in $\mathbb{Z}^n$. Then compute a basis $r_1, \ldots, r_m \in \mathbb{Z}^n$ for $url(a_1, \ldots, a_n) \leq \mathbb{Z}^n$ and consider the matrix

$$R := \begin{pmatrix} r_1 \\ \ldots \\ r_m \end{pmatrix}.$$

Recall that for $r \in url(a_1, \ldots, a_n)$ we defined the unit $u(r)$ as $\prod_{j=1}^{n} a_i^{r_j}$. Let $s_1, \ldots, s_o$ be a basis for $rl\,(u(r_1), \ldots, u(r_m)) \leq \mathbb{Z}^m$ and define the matrix

$$S := \begin{pmatrix} s_1 \\ \ldots \\ s_o \end{pmatrix}.$$

4.1.14 Lemma: *A generating set for the relation lattice $rl(a_1, \ldots, a_n)$ is given by the rows of the matrix*

$$T := S \cdot R$$

Proof: Let t be a row of the matrix T. Then we can write $t = s \cdot R$ where s is a row of the matrix S. This implies

$$\begin{aligned} & {a_1}^{t_1} \cdot {a_2}^{t_2} \cdots {a_n}^{t_n} \\ = \;& a_1^{\sum_{j=1}^{m} s_j r_{j1}} \cdot a_2^{\sum_{j=1}^{m} s_j r_{j2}} \cdots a_n^{\sum_{j=1}^{m} s_j r_{jn}} \\ = \;& (\prod_{i=1}^{n} a_i^{r_{1i}})^{s_1} \cdot (\prod_{i=1}^{n} a_i^{r_{2i}})^{s_2} \cdots (\prod_{i=1}^{n} a_i^{r_{mi}})^{s_m} \\ = \;& u(r_1)^{s_1} \cdot u(r_2)^{s_2} \cdots u(r_m)^{s_m} \\ = \;& 1 \end{aligned}$$

and so t is an element of $rl(a_1, \ldots, a_n)$.

Vice versa assume, that t is an element of $rl(a_1, \ldots, a_n)$. Then t must be in $url(a_1, \ldots, a_n)$ and is therefore a $\mathbb{Z}$-linear combination of the rows of R, and so $t = \alpha \cdot R$ with $\alpha \in \mathbb{Z}^m$. We deduce, that α must be in the subspace generated by the rows of S, because $u(r_1)^{\alpha_1} \cdots u(r_m)^{\alpha_m} = 1$. This implies, that t is a $\mathbb{Z}$-linear combination of the rows of T. •

4.2 Constructive polycyclic sequences

Let A be a finitely generated abelian group and suppose that a method is given to calculate the relation lattice $rl(\mathcal{E})$ for an arbitrary finite subset $\mathcal{E}$ of A. We want to determine a constructive polycyclic sequence for A.

4.2.1 Lemma: *Let $\mathcal{A} := \{a_1, \ldots, a_n\}$ be an arbitrary generating set for the abelian group A with relation lattice $rl(\mathcal{A})$. Write the vectors of a generating set of $rl(\mathcal{A})$ row by row into a matrix RL. Applying the Smith normal form algorithm to RL we can determine a minimal generating set $\mathcal{G}$ for A and calculate the relative orders of $\mathcal{G}$ viewed as a polycyclic sequence.*

Proof: Suppose that $RL \in \mathbb{Z}^{m\times n}$. We can determine row and column transformations R and C such that $R \cdot RL \cdot C$ is equal to a matrix $S \in \mathbb{Z}^{m\times n}$ in Smith normal form. That is, there is some $k > 0$ such that the entry $s_i := S_{ii}$ is positive for $i = 1, \ldots, k$, S has no other nonzero entries and s_i divides s_{i+1} for $i = 1, \ldots, k-1$.

Denote by j the smallest natural number such that $s_j \neq 1$. The matrix C can be interpreted as base change matrix of $\mathbb{Z}^n$ and the multiplication from the left with the matrix R just changes the generating set of the subspace generated by the rows of $RL \cdot C$. We deduce, that the rows of S are a generating set of $rl(\mathcal{A})$ in coordinate vectors corresponding to the new basis. Then the rows $\bar{c}_j, \ldots, \bar{c}_n \in \mathbb{Z}^n$ between the j-th and the n-th row of C^{-1} give rise to a minimal generating set $\bar{c}_j + rl(\mathcal{A}), \ldots, \bar{c}_n + rl(\mathcal{A})$ for $\mathbb{Z}^n/rl(\mathcal{A})$ (as the preimage of the j-th until the n-th unit vector in the new basis). The elements $\bar{c}_j + rl(\mathcal{A}), \ldots, \bar{c}_n + rl(\mathcal{A})$ have the orders $(s_j, \ldots, s_k, 0, \ldots, 0)$. They give rise to a minimal generating set

$$\mathcal{G} := \{ \prod_{i=1}^{n} a_i^{\bar{c}_{ki}} \mid k = j, \ldots, n \}$$

for A with relative orders $(s_j, \ldots, s_k, 0, \ldots, 0)$.

For further background on finitely generated abelian groups and the Smith normal form see [21] Section 8.3. •

It rests to describe a method to compute exponent vectors corresponding to a given polycyclic sequence.

4.2.2 Lemma: *Let $\mathcal{A} := \{a_1, \ldots, a_n\}$ be a minimal generating set for an abelian group A and let a be a non-trivial element of A. Then the exponent*

vector of the element a corresponding to $\mathcal{A}$ can be calculated in determining the relation lattice $rl(\{a\} \cup \mathcal{A})$.

Proof: Let $\mathcal{B}$ be a basis of $rl(\{a\} \cup \mathcal{A})$ written row by row in a matrix. Bring $\mathcal{B}$ in triangular form (via integer operation) and let r be the first row of the transformed matrix. We deduce that r_1 is equal to 1 because $\mathcal{A}$ is a generating set for A. Then the exponent vector can be read off as

$$exp_{\mathcal{A}}(a) = -(r_2, \ldots, r_{n+1}).$$

•

4.3 Example

The methods described in this chapter were implemented in GAP [24] and are part of the GAP-package 'Alnuth' [7]. For the fundamental algorithms as the determination of the maximal order, the unit group and the ideal valuation we used the computer algebra system KANT [10]. The GAP-package 'Alnuth' provides an interface from GAP to KANT.

Let $\theta \in \mathbb{C}$ be a root of the irreducible polynomial

$$f := x^4 - 4x^3 - 28x^2 + 64x + 16.$$

Denote by $\mathbb{F}$ the number field $\mathbb{Q}(\theta)$ and consider the following elements in $\mathbb{F}$

$$\begin{aligned}
a_1 &: = 4/3 - 2/3\theta - 1\theta^2 - 1/3\theta^3 \\
a_2 &: = -1/3 - 1\theta + 2\theta^2 + 2\theta^3 \\
a_3 &: = 5/3 - 1\theta - 1/2\theta^2 - 1/2\theta^3 \\
a_4 &: = -1/4 - 3\theta^2 - 1/2\theta^3 \\
a_5 &: = -1/2\theta^3 \\
a_6 &: = 129140/3 + 178538\theta - 146945/3\theta^2 - 53893/3\theta^3 \\
a_7 &: = 7843/9 + 10748/3\theta - 2243/2\theta^2 - 320\theta^3.
\end{aligned}$$

We want to calculate a presentation for the multiplicative group

$$A := \langle a_1, \ldots, a_7 \rangle .$$

The calculation of the relation lattice

$$rl(a_1, \ldots, a_7) := \{(e_1, \ldots, e_7) \in \mathbb{Z}^7 | \prod_{i=1}^{7} a_i^{e_i} = 1\}.$$

costed about 10 milliseconds with a Pentium III processor with 850 mhz under the system Linux. The relation lattice is equal to

$$\langle\, (1,0,0,1,1,-1,0), (0,1,1,0,0,0,-1)\,\rangle \leq \mathbb{Z}^7.$$

The minimal generating set for A calculated by the algorithm in Lemma 4.2.1 is

$$(a_2, a_4, a_5, a_6, a_7)$$

with the relative orders $(0, \ldots, 0)$. This is a constructive polycyclic sequence for A. By Theorem 2.2.2, the group A is isomorphic to the polycyclic presented group

$$\begin{aligned} X &:= \left\langle x_1, \ldots, x_5 \,\middle|\, x_i^{x_j} = x_i,\ x_i^{x_j^{-1}} = x_i \ \text{for}\, 1 \leq i < j \leq 5 \right\rangle \\ &= \left\langle x_1, \ldots, x_5 \,\middle|\, [x_i, x_j] = 1 \ \text{for}\, 1 \leq i < j \leq 5 \right\rangle. \end{aligned}$$

In total the computation of this polycyclic presented group costed about 20 milliseconds.

Chapter 5

Unipotent groups

Let U be a subgroup of $GL(d, \mathbb{Q})$. Recall that an element $u \in U$ is called *unipotent* if there exists a natural number $m \in \mathbb{N}$ such that

$$(u - 1)^m = 0,$$

and that the group U is called *unipotent*, if every element in U is unipotent.

We will see, that every finitely generated unipotent matrix group $U \leq GL(d, \mathbb{Q})$ is polycyclic. It is our goal to determine a polycyclic presentation of U. According to Corollary 2.2.5, it is sufficient to calculate a constructive polycyclic sequence for U to get a polycyclic presentation.
Denote by $UT(d, \mathbb{Z})$ the group of all upper unitriangular matrices in $GL(d, \mathbb{Z})$, i.e. every element in $UT(d, \mathbb{Z})$ has the form

$$\begin{pmatrix} 1 & * & \dots & & * \\ & 1 & * & \dots & * \\ & & & & \vdots \\ & & & \ddots & * \\ & & & & 1 \end{pmatrix}.$$

In the next section we describe a method to determine a matrix g such that $U^g \leq UT(d, \mathbb{Z})$, if U is finitely generated. Then in section 5.2 we show how to compute a constructive polycyclic sequence for any subgroup of $UT(d, \mathbb{Z})$.

5.1 Conjugation

Let $U := \langle u_1, \ldots, u_n \rangle$ be an unipotent rational matrix group. In this section we determine a matrix $g \in GL(d, \mathbb{Q})$ such that U^g is a subgroup of $UT(d, \mathbb{Z})$.

5.1.1 Definition: Let V be a vector space over a field $\mathbb{F}$. Regard a chain of subspaces in V

$$\ldots V_{i-1} \subset V_i \subset V_{i+1} \ldots$$

Then the chain (V_i) is called a *flag*, if for all i we have $V_i \neq V_{i+1}$.

Denote by u an unipotent element of $GL(d, \mathbb{Q})$. Let

$$\langle b_d \rangle \subset \langle b_{d-1}, b_d \rangle \subset \ldots \langle b_1, \ldots, b_d \rangle$$

be a flag of $\mathbb{Q}^d$. It is said to be a flag for u if it has the property that

$$b_i u = b_i + \sum_{j=i+1}^{d} \beta_{ij} b_j \qquad (*)$$

for $i = 1, \ldots, d$ and an unitriangular matrix $\beta \in UT(d, \mathbb{Q})$. This is equivalent with the property that $b_i + \langle b_{i+1}, \ldots, b_d \rangle$ is a eigenvector to the eigenvalue 1 for u in $\mathbb{Q}^d / \langle b_{i+1}, \ldots, b_d \rangle$.

5.1.2 Lemma: *Let u be a matrix in $GL(d, \mathbb{Q})$. Then u is unipotent if and only if all eigenvalues of u are equal to 1.*

Proof: If all the eigenvalues of u are equal to 1, we deduce by conjugation to the Jordan-Normal form that u is unipotent. Conversely denote by λ an arbitrary eigenvalue of u with eigenvector x. It follows that

$$x(u-1)^n = (\lambda - 1)^n x$$

for every number $n \in \mathbb{N}$. Since u is unipotent, there is an $m \in \mathbb{N}$ such that $(u-1)^m = 0$. We deduce that $(\lambda - 1)^m x = 0$ and thus $\lambda = 1$. •

5.1.3 Lemma: *Denote by u an unipotent element of $GL(d, \mathbb{Q})$. Then there exists a flag for u with the property $(*)$. If $\{b_1, \ldots, b_d\}$ is the corresponding basis of this flag, then we define the matrix*

$$b := \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}.$$

Then $u^{b^{-1}}$ is an element of $UT(d, \mathbb{Q})$.

Proof: Let m be the smallest natural number such that $(u-1)^m = 0$. Then there exists a non-trivial vector $x \in \mathbb{Q}^d$ such that

$$x(u-1)^{m-1} \neq 0.$$

Therefore, $b_d := x(u-1)^{m-1}$ is an eigenvector of u with eigenvalue 1. Now induce the action of u to $\mathbb{Q}^d / \langle b_d \rangle$. Since the induced action is still unipotent we find by induction a flag for u with the property $(*)$. Let $\{b_1, \ldots, b_d\}$ be a basis for this flag. We deduce that there exists an $\beta \in UT(d, \mathbb{Q})$ such that $bu = \beta b$. It follows that $u^{b^{-1}} \in UT(d, \mathbb{Q})$. •

So we are able to bring every unipotent matrix in $GL(d, \mathbb{Q})$ in unitriangulized form. The next theorem shows, that this is also possible for an unipotent group.

5.1.4 Theorem: *Let U be an unipotent subgroup of $GL(d, \mathbb{Q})$. Then there exists an element $g \in GL(d, \mathbb{Q})$ such that $U^g \leq UT(d, \mathbb{Q})$.*

Proof: See [25] Corollary 1.21 or [19] 8.1.10. •

Let $U := \langle u_1, \ldots, u_n \rangle$ be an unipotent subgroup of $GL(d, \mathbb{Q})$. Now we construct an element $b \in GL(d, \mathbb{Q})$ with the property that $U^{b^{-1}} \leq UT(d, \mathbb{Q})$. This is, we calculate a flag with the property $(*)$ for all generators of U. Define the matrix

$$\hat{u} := \begin{pmatrix} u_1 - 1 & u_2 - 1 & \cdots & u_n - 1 \end{pmatrix}.$$

Since U is conjugated to a subgroup of $UT(d, \mathbb{Q})$, there exists a non-trivial vector $x \in \mathbb{Q}^d$ such that $x\hat{u} = 0$. We calculate such a vector x and set $b_d := x$. Now we induce the action of U to $\mathbb{Q}^d / \langle b_d \rangle$ and get a group $\tilde{U}$. The group $\tilde{U}$ is still unipotent and so we can proceed by induction. In this way we find the vectors b_i for $i = 1, \ldots, d$ with the property $(*)$ for all generators of U. As in Lemma 5.1.3, we deduce that the matrix

$$b := \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}$$

has the property that $U^{b^{-1}} \leq UT(d, \mathbb{Q})$.

Finally we have to find a matrix which conjugates a subgroup of $UT(d, \mathbb{Q})$ to a subgroup of $UT(d, \mathbb{Z})$.

For a number $x = \frac{a}{b} \in \mathbb{Q}$ we denote by $\mathfrak{d}(x) = b$ the denominator of x and for the numbers $x_1, \ldots, x_k \in \mathbb{Z}$ we define $lcm(x_1, \ldots, x_k)$ to be the least common multiple of $x_1, \ldots, x_k$.

5.1.5 Lemma: *Let u be an element of $UT(d, \mathbb{Q})$. Define*

$$c := \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_d \end{pmatrix} \in GL(d, \mathbb{Z})$$

to be the diagonal matrix with the entries

$$\begin{aligned} c_1 &:= 1 \\ c_i &:= lcm(\mathfrak{d}(c_1^{-1} u_{1i}), \ldots, \mathfrak{d}(c_{i-1}^{-1} u_{(i-1)i})). \end{aligned}$$

Then $u^c \in UT(d, \mathbb{Z})$.

Proof: Obviously we have that $(u^c)_{ij} = c_i^{-1} u_{ij} c_j$. We deduce that $(u^c)_{ij} = 0$ for $i > j$ and that $(u^c)_{ii} = 1$ for $i = 1, \ldots, d$. For $j > i$ we see that

$$c_i^{-1} u_{ij} c_j = (c_i^{-1} u_{ij}) c_j = (c_i^{-1} u_{ij}) lcm(\mathfrak{d}(c_1^{-1} u_{1j}), \ldots, \mathfrak{d}(c_{j-1}^{-1} u_{(j-1)j})) \in \mathbb{Z}$$

and thus $u^c \in UT(d, \mathbb{Z})$. •

5.1.6 Remark: There are easier ways to find a matrix c such that $u^c \in UT(d, \mathbb{Z})$. For example we could choose $c := diag(l^0, l^1, \ldots, l^{d-1})$, where l is the least common multiple of the denominators of all entries in u. The approach of Lemma 5.1.5 has the advantage, that it produces a matrix with smaller integer entries.

5.1.7 Corollary: *Let $U := \langle u_1, \ldots, u_n \rangle$ be a subgroup of $UT(d, \mathbb{Q})$. Define*

$$c := \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_d \end{pmatrix} \in GL(d, \mathbb{Z})$$

to be the diagonal matrix with the entries

$$\begin{aligned} c_1 &:= 1 \\ c_i &:= lcm(\left\{ \mathfrak{d}(c_j^{-1} (u_k)_{ji}) \mid 1 \leq j \leq i-1, 1 \leq k \leq n \right\}). \end{aligned}$$

Then $U^c \leq UT(d, \mathbb{Z})$.

5.1.8 Example: Let U be the unipotent group generated by the matrices

$$u_1 := \begin{pmatrix} 7/3 & 7/3 & 0 & 8/3 \\ -11/9 & -10/9 & -2/9 & -14/9 \\ 1/12 & -1/6 & 1/2 & -5/6 \\ 37/36 & 37/18 & 17/18 & 41/18 \end{pmatrix}, u_2 := \begin{pmatrix} 1/3 & -2/3 & 1 & -1/3 \\ 7/9 & 7/3 & -1/9 & 5/3 \\ -2/3 & -5/3 & 1/4 & -37/12 \\ -2/9 & -1/3 & -1/36 & 13/12 \end{pmatrix}.$$

First we conjugate U to a subgroup of $UT(d, \mathbb{Q})$. The matrix

$$b := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -3 \\ 0 & 1 & 1 & 5 \\ 1 & 2 & 1 & 1 \end{pmatrix}$$

contains row vectors which are a basis of a flag for u_1, u_2 with the property $(*)$. By conjugation with b^{-1} we get

$$u_1^{b^{-1}} = \begin{pmatrix} 1 & -1/12 & 0 & 37/36 \\ 0 & 1 & -1/3 & -3 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 1 \end{pmatrix}, u_2^{b^{-1}} = \begin{pmatrix} 1 & 1/12 & 1/9 & -2/9 \\ 0 & 1 & -2/3 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

According to Corollary 5.1.7 we calculate

$c_1 := 1$

$c_2 := lcm(\ \mathfrak{d}(-1/12), \mathfrak{d}(1/12)\ ) = 12$

$c_3 := lcm(\ \mathfrak{d}(0), \mathfrak{d}(1/9), \mathfrak{d}(c_2^{-1}(-1/3)), \mathfrak{d}(c_2^{-1}(-2/3))\ ) = 36$

$c_4 := lcm(\ \mathfrak{d}(37/36), \mathfrak{d}(-2/9), \mathfrak{d}(c_2^{-1}(-3)), \mathfrak{d}(c_2^{-1}0), \mathfrak{d}(c_3^{-1}4), \mathfrak{d}(c_3^{-1}(-1))\ ) = 36.$

Therefore we define

$$c := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 \\ 0 & 0 & 36 & 0 \\ 0 & 0 & 0 & 36 \end{pmatrix},$$

set $g := b^{-1}c$ and get

$$u_1^g = \begin{pmatrix} 1 & -1 & 0 & 37 \\ 0 & 1 & -1 & 9 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 1 \end{pmatrix}, u_2^g = \begin{pmatrix} 1 & 1 & 4 & -8 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

5.2 Constructive pc-sequences

Let U be a subgroup of $UT(d,\mathbb{Z})$. In this section we determine a constructive pc-sequence for U. First we show, that the group of all unitriangular matrices over the integers $UT(d,\mathbb{Z})$ is polycyclic and give a constructive pc-sequence for $UT(d,\mathbb{Z})$. Second we induce the constructive pc-sequence of $UT(d,\mathbb{Z})$ to a constructive pc-sequence of U.
The following example gives a good intuition for the structure of $UT(d,\mathbb{Z})$.

5.2.1 Example: Denote by a, b two elements in $UT(4,\mathbb{Z})$. We verify that

$$\begin{aligned} ab &= \begin{pmatrix} 1 & a_{12} & * & * \\ & 1 & a_{23} & * \\ & & 1 & a_{34} \\ & & & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b_{12} & * & * \\ & 1 & b_{23} & * \\ & & 1 & b_{34} \\ & & & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a_{12}+b_{12} & * & * \\ & 1 & a_{23}+b_{23} & * \\ & & 1 & a_{34}+b_{34} \\ & & & 1 \end{pmatrix} \end{aligned}$$

So by matrix calculation, we see that the projection on the first subdiagonal

$$\begin{aligned} \phi \;:\; UT(d,\mathbb{Z}) &\to \mathbb{Z}^{d-1} \\ a &\mapsto (\; a_{12},\; a_{23},\; \ldots,\; a_{d-1,d} \;) \end{aligned}$$

is a homomorphism.

5.2.2 Lemma: *The group of all unitriangular matrices over the integers $UT(d,\mathbb{Z})$ is polycyclic. Therefore all subgroups of $UT(d,\mathbb{Z})$ are polycyclic.*

Proof: For $k \in \{1,\ldots,k\}$ we define

$$U_k := \{u \in UT(d,\mathbb{Z}) \mid u_{ij} = 0 \text{ if } i \neq j \text{ and } j - i < k \;\}.$$

It is easy to see that U_k is a subgroup of $UT(d,\mathbb{Z})$ for $k = 1,\ldots,d$.

We proof by induction that $U_k \leq UT(d,\mathbb{Z})$ is polycyclic. For $k = 1$ this gives the wanted result. Certainly $U_d = \{1\}$ is polycyclic. Now we assume that $k < d$ and that U_{k+1} is polycyclic. Define

$$\begin{aligned} \phi_k \;:\; U_k &\to \mathbb{Z}^{d-k} \\ u &\mapsto (\; u_{1,1+k},\; u_{2,2+k},\; \ldots,\; u_{d-k,k} \;) \end{aligned}$$

to be the projection on the k-th subdiagonal. The kernel of ϕ_k is equal to U_{k+1} and thus polycyclic by hypothesis. Further $Im\,\phi_k = \mathbb{Z}^{d-k}$ is polycyclic. Therefore U_k is polycyclic.

We deduce that $UT(d,\mathbb{Z})$ is polycyclic. Subgroups of polycyclic groups are polycyclic (see [21] Section 9.3). •

5.2.3 Corollary: *Let $U := \langle u_1, \ldots, u_n \rangle$ be an unipotent subgroup of $GL(d,\mathbb{Q})$. Then the group U is polycyclic.*

Proof: In Section 5.1 we showed, that there exists a $g \in GL(d,\mathbb{Q})$ such that $U^g \leq UT(d,\mathbb{Z})$. Thus U is polycyclic. •

In the following example we outline a constructive polycyclic sequence for $UT(4,\mathbb{Z})$.

5.2.4 Example: It is easy to verify that the matrices

$$a_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix},\ a_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ & 1 & 1 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix},\ a_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ & 1 & 0 & 0 \\ & & 1 & 1 \\ & & & 1 \end{pmatrix},$$

$$a_4 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix},\ a_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ & 1 & 0 & 1 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix},\ a_6 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}$$

are a generating set for $UT(4,\mathbb{Z})$. Further they form a polycyclic sequence for $UT(4,\mathbb{Z})$. We determine the exponent vector of an element $x \in UT(4,\mathbb{Z})$ corresponding to the pc-sequence $\mathcal{A} := (a_1, \ldots, a_6)$. For example, we regard the matrix

$$x := \begin{pmatrix} 1 & 3 & -1 & 1 \\ & 1 & 5 & 4 \\ & & 1 & -2 \\ & & & 1 \end{pmatrix}.$$

The entries on the first subdiagonal are $\alpha_1 = 3, \alpha_2 = 5$ and $\alpha_3 = -2$. Therefore $(a_1^3 a_2^5 a_3^{-2})^{-1} x$ has only zeros on the first subdiagonal and is equal to

$$\begin{pmatrix} 1 & 0 & -16 & -11 \\ 0 & 1 & 0 & 14 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now on the second subdiagonal we find the entries $\alpha_4 = -16$ and $\alpha_5 = 14$. So by multiplication from the left with $(a_4^{-16}a_5^{14})^{-1}$ we get

$$\begin{pmatrix} 1 & 0 & 0 & -11 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

A further multiplication from the left with $(a_6^{-11})^{-1}$ yields the identity matrix. We deduce that

$$x = a_1^3 a_2^5 a_3^{-2} a_4^{-16} a_5^{14} a_6^{-11}.$$

Therefore the exponent vector of x corresponding to $\mathcal{A}$ is

$$exp_{\mathcal{A}}(x) = (3, 5, -2, -16, 14, -11).$$

We see that in this way we can determine $exp_{\mathcal{A}}(x)$ for every $x \in UT(4, \mathbb{Z})$ in a practical way. Thus $\mathcal{A}$ is a constructive polycyclic pc-sequence for $UT(4, \mathbb{Z})$.

5.2.5 Corollary: *The method presented in Example 5.2.4 can be used to determine a constructive polycyclic sequence for the group $UT(d, \mathbb{Z})$.*

5.2.6 Lemma: *Let U be a subgroup of $UT(d, \mathbb{Z})$. A constructive pc-sequence for $UT(d, \mathbb{Z})$ can be used to determine a constructive pc-sequence for U.*

Proof: This is a well-known fact. See for example [6, Chapter 3]. The methods POLY_SUBGROUP and POLY_MEMBER described in [21, Chapter 9] can also be applied for this purposes. •

Algorithms in the domain of the last Lemma have been implemented already and are part of the 'Polycyclic'-package [8] which is a part of the GAP-system.

Chapter 6

Rational Module Series

Let G be a finitely generated solvable subgroup of $GL(d, \mathbb{Q})$. Recall that we defined $K_p(G)$ as the kernel of the *p-congruence homomorphism*

$$\psi_p : G \to GL(n, p)$$

where p is an admissible prime for G (see Definition 2.4.2). The aim of this chapter is to compute a so-called module composition series of the natural $\mathbb{Q}K_p(G)$-module $V = \mathbb{Q}^d$. This is a sequence of $\mathbb{Q}K_p(G)$-submodules

$$V = V_1 > V_2 > \cdots > V_m = 0$$

such that V_i/V_{i+1} is irreducible as a $\mathbb{Q}K_p(G)$-module. For the case that G is abelian, we describe a method to determine a composition series for $\mathbb{Q}^d$ seen as a $\mathbb{Q}G$-module.

This chapter is organized as follows: Section 6.1 cites basic definitions and results from module theory. Section 6.2 determines the image and the kernel of the induced action of G to the factors of a modules series. In Section 6.3 and 6.4 we compute a certain submodule series called radical series. Finally we outline in Section 6.5 and Section 6.6 methods to refine a radicals series to a composition series.
In our description we follow the presentation in [6, chapter 5].

6.1 Module Theory and *p-congruence* subgroups

In this section we want to cite some basic results from module theory which will be used throughout this chapter.

6.1.1 Definition: Let G be a group.

1. An abelian group $(M, +)$ is called a *G-module*, if G operates via automorphisms on M. Thus there is a homomorphism $\varphi : G \to Aut(M)$.
2. Let $\mathbb{F}$ be a field and M a $\mathbb{F}$-vectorspace. Then M is called a *$\mathbb{F}G$-module*, if G operates via $\mathbb{F}$-linear automorphisms on M. In this case there exists a homomorphism $\varphi : G \to GL(M)$.

Naturally a subset $N \subset M$ (subspace $N \leq M$) is called a G-submodule ($\mathbb{F}G$-submodule) of M, if N is a G-module ($\mathbb{F}G$-module).

6.1.2 Definition: Let G be a group and V be a $\mathbb{Q}G$-module.

1. V is said to be *irreducible* if it does not contain any $\mathbb{Q}G$-submodule other than 0 and V, and if $V \neq 0$.
2. V is said to be *semisimple* if it is the direct product of irreducible $\mathbb{Q}G$-modules.
3. We say that V is *Artinian* if V satisfies the descending chain condition on submodules, that is a sequence

$$V_1 \supset V_2 \supset V_3 \ldots$$

of submodules must stabilize.

6.1.3 Definition: Let G be a subgroup $GL(d, \mathbb{Q})$. We define as its *algebra*

$$\mathbb{Q}[G] = \left\{ \sum_{i=1}^{k} \alpha_i g_i \mid \alpha_i \in \mathbb{Q}, g_i \in G \right\}.$$

The dimension of $\mathbb{Q}[G]$ is the dimension of this set as a $\mathbb{Q}$-vectorspace. $\mathbb{Q}[G]$ is a subspace of the matrix algebra $M^{d\times d}(\mathbb{Q})$ and thus an upper bound of the dimension of $\mathbb{Q}[G]$ is d^2. We can consider $\mathbb{Q}[G]$ as a $\mathbb{Q}G$-module where G operates from the right. A basis of a finite dimensional module which is given by module generators can be computed by the well-known and very efficient *spinning algorithm* (see [12]).
The following lemma is essential for our investigations and will be used at various places throughout this chapter.

6.1.4 Lemma: *(***Schur, modified version***) Let G be a group and V an irreducible $\mathbb{Q}G$-module with $\varphi : G \to GL(V)$. Then every non-zero element of $\mathbb{Q}[G^\varphi]$ is invertible.*

Proof: See [9] Lemma 1.5. •

6.1.5 Corollary: *Let A be an abelian group and V an irreducible $\mathbb{Q}A$-module with $\varphi : A \to GL(V)$. Then $\mathbb{Q}[A^\varphi]$ is a field.*

6.1.6 Lemma: *Let $G \leq GL(d, \mathbb{Q}_\pi)$ (see Section 2.4) and $V = \mathbb{Q}^d$ the natural G-module. Then*

1. *$K_p(G) = G \cap K_p(GL(d, \mathbb{Q}_\pi))$.*
2. *$K_p(G^g) = (K_p(G))^g$ for $g \in GL(d, \mathbb{Q}_\pi)$ and thus $K_p(G)$ is invariant under base changes.*
3. *Let W be a $\mathbb{Q}G$-submodule of V. For the induced action on V and V/W we obtain that $K_p(G)_W \leq K_p(G_W)$ and $K_p(G)_{V/W} \leq K_p(G_{V/W})$.*

Proof: Elementary. •

6.2 Induced Action

The aim of this section is to investigate the induced action of rational matrix groups to the factors of a submodule series.

6.2.1 Integral Basis of rational spaces

In this section we want to examine when a rational space $W \leq \mathbb{Q}^d$ has an integral basis, which can be extended to a basis of $\mathbb{Z}^d$.

6.2.1 Definition: Let X be any subset of $\mathbb{Q}^d$. The *dual lattice* X^* and the *orthogonal space* $X^\perp$ are defined as

$$X^* := \{\, y \in \mathbb{Z}^d \mid y \cdot x = 0 \text{ for all } x \in X \,\}$$

$$X^\perp := \{\, y \in \mathbb{Q}^d \mid y \cdot x = 0 \text{ for all } x \in X \,\}.$$

6.2.2 Definition: Let L be a sublattice of $\mathbb{Z}^d$. Then L is called *pure* if and only if the group $\mathbb{Z}^d/L$ is torsion-free. Further we define the *pure hull* $\bar{L}$ of L as the unique sublattice of $\mathbb{Z}^d$ such that $\bar{L}/L = T(\mathbb{Z}^d/L)$, where $T(\mathbb{Z}^d/L)$ is the torsion group of $\mathbb{Z}^d/L$. Note that $T(\mathbb{Z}^d/L)$ exists because $\mathbb{Z}^d/L$ is abelian.

6.2.3 Lemma: *There exists an integral basis of $\mathbb{Z}^d$ through a sublattice L if and only if L is pure. Further the pure hull of L, denoted by $\bar{L}$, is pure.*

Proof: Assume that L is a pure sublattice of dimension k. Then $\mathbb{Z}^d/L$ is isomorphic to $\mathbb{Z}^{d-k}$. Denote by $\{e_1, \ldots, e_{d-k}\}$ representatives of a basis of $\mathbb{Z}^d/L$. Merging this set with a basis of L we get a integral basis of $\mathbb{Z}^d$ through L.

Conversely assume that there exists an integral basis of $\mathbb{Z}^d$ through L. Then $\mathbb{Z}^d/L$ is isomorphic to $\mathbb{Z}^{d-k}$ and thus L is pure.

Let $\bar{L}$ be the pure hull of L. We have to show that $\mathbb{Z}^d/\bar{L}$ is torsion-free. Let $z \in \mathbb{Z}^d$ such that there exists a natural number $n \in \mathbb{N}$ such that $nz \in \bar{L}$. It follows that there is an $m \in \mathbb{N}$ such that $mnz \in L$. We deduce that $z \in \bar{L}$ and $z + \bar{L}$ is the trivial element of $\mathbb{Z}^d/\bar{L}$. •

The following lemma gives us a method to compute the pure hull $\bar{L}$.

6.2.4 Lemma:

1. *Let X be an arbitrary subset of $\mathbb{Q}^d$. Then it follows that*

$$X^{**} = X^{\perp\perp} \cap \mathbb{Z}^d$$

   and thus $dim_{\mathbb{Q}}(X^{**}) = dim_{\mathbb{Q}}(X^{\perp\perp})$.

2. *Let $L \leq \mathbb{Z}^d$. Then L^{**} is equal to the pure hull $\bar{L}$ of L.*

Proof:

1. $X^{**} = X^{*\perp} \cap \mathbb{Z}^d = (X^{\perp} \cap \mathbb{Z}^d)^{\perp} \cap \mathbb{Z}^d = X^{\perp\perp} \cap \mathbb{Z}^d$.

2. Let $\bar{l}$ be an element of $\bar{L}$. Then there exists a natural number n such that $n\bar{l} = l \in L$. For all $x \in L^*$ we have $0 = x \cdot l = x \cdot (n\bar{l}) = n(x \cdot \bar{l})$ and thus $x \cdot \bar{l} = 0$. This implies that $\bar{l} \in L^{**}$ and so $\bar{L} \subset L^{**}$.

   Conversely we know by 1. that the $\mathbb{Q}$-dimension of L and L^{**} are the same and that

$$L^{**} = L^{\perp\perp} \cap \mathbb{Z}^d = \langle L \rangle_{\mathbb{Q}} \cap \mathbb{Z}^d.$$

   Therefore we can write every $l \in L^{**}$ as $l = \sum_{i=1}^{k} \frac{a_i}{b_i} l_i$ where $\frac{a_i}{b_i} \in \mathbb{Q}$ and $l_i \in L$. Now we get that $(\prod b_i)l \in L$ and so $l + \bar{L}$ is in the torsion group of $\mathbb{Z}^d/L$. Therefore $L^{**} \subset \bar{L}$.

•

6.2.5 Corollary: *Let W be a subspace of $\mathbb{Q}^d$. Then there exists an integral basis $\mathcal{B}$ of $\mathbb{Z}^d$ through W.*

Proof: We know that $(W^{**})^{**} = (W \cap \mathbb{Z}^d)^{**} = ((W \cap \mathbb{Z}^d)^{\perp} \cap \mathbb{Z}^d)^* = (W^{\perp} \cap \mathbb{Z}^d)^* = W^{**}$ and so W^{**} is a pure sublattice of $\mathbb{Z}^d$. Further we know that the $\mathbb{Q}$-dimensions of W^{**} and W are the same, which implies that an integral basis $\mathcal{B}$ through W^{**} is also an integral basis through W. •

6.2.2 Factor modules

Let π be a set of primes. Recall that the ring $\mathbb{Q}_\pi$ was defined as the set of rational numbers whose denominator is divisible by primes in π only. Let K be a subgroup of $GL(d, \mathbb{Q}_\pi)$ and denote by V the natural K-module $\mathbb{Q}^d$. Let

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

be a series of $\mathbb{Q}K$-modules. We induce the action of K to the factors of this series via the action homomorphism

$$\nu : K \to K_{V_0/V_1} \times K_{V_1/V_2} \times \cdots \times K_{V_{n-1}/V_n}.$$

The following Lemma examines the structure of the image and the kernel under this homomorphism.

6.2.6 Lemma: *Suppose that $K \leq GL(d, \mathbb{Q}_\pi)$ for a set of primes π. Then $ker(\nu)$ is a unipotent subgroup of $GL(d, \mathbb{Q}_\pi)$ and $K_{V_i/V_{i+1}} \leq GL(d_i, \mathbb{Q}_\pi)$ for $1 \leq i \leq n$, where $\sum_{i=1}^{n} d_i = d$.*

Proof: By Corollary 6.2.5 there exists an integral basis $\mathcal{B} = \{b_1, \ldots, b_d\}$ of $\mathbb{Z}^d$ through the module series. Denote by $g := (b_1, \ldots, b_d)^{t-1} \in GL(d, \mathbb{Z})$ the corresponding base change matrix from the canonical basis of $\mathbb{Q}^d$ to $\mathcal{B}$. It follows that K^g is a subgroup of $GL(d, \mathbb{Q}_\pi)$ in block-upper-triangular form. That is every element k of K^g is of the form

$$\begin{pmatrix} k_0 & * & * & * \\ & k_1 & * & * \\ & & \ddots & * \\ & & & k_{n-1} \end{pmatrix}$$

where k_i is a matrix in $GL(d_i, \mathbb{Q}_\pi)$ with $\sum_{i=0}^{n-1} d_i = d$. The induced action of K on the factor V_i/V_{i+1} of the module series is conjugated in $GL(d_i, \mathbb{Z})$

to the matrix group generated by the blocks k_i of the matrices $k \in K^g$. We deduce that $K_{V_i/V_{i+1}}$ is a subgroup of $GL(d_i, \mathbb{Q}_\pi)$. Further $ker(\nu)$ is a unipotent subgroup of $GL(d, \mathbb{Q}_\pi)$, since $ker(\nu)^g$ is in upper-triangular form. •

6.3 Computing radicals

Let $G \leq GL(d, \mathbb{Q})$ be a finitely generated solvable group and denote by $V := \mathbb{Q}^d$ the natural $\mathbb{Q}G$-module. We want to determine a basis for the so-called radical $Rad_G(V)$.

6.3.1 Definition: Let G be a group and V be a $\mathbb{Q}G$-module. The *radical* $Rad_G(V)$ is defined as the intersection of all maximal $\mathbb{Q}G$-submodules of V.

6.3.2 Definition: Let G be a group and V be a $\mathbb{Q}G$-module. Then G is called *semisimple* if $Rad_G(V) = 0$.

For our purposes we will need the following lemma which is a part of basic module theory.

6.3.3 Lemma: *Let G be a subgroup $GL(d, \mathbb{Q})$ and $V = \mathbb{Q}^d$ the natural $\mathbb{Q}G$-module.*

1. *$\mathbb{Q}[G]$ is an Artinian algebra and V is an Artinian module.*
2. *$Rad_G(V) < V$, and $Rad_G(V) = 0$ if and only if V is semisimple. So $V/Rad_G(V)$ is always semisimple.*
3. *$Rad_G(V) = V\, Rad_G(\mathbb{Q}[G])$*
4. *If W is a $\mathbb{Q}G$-submodule of $Rad_G(V)$, then $Rad_G(V/W) = Rad_G(V)/W$.*

Proof: See [13] Chapter 7, Lemma 7.11., Satz 7.14 and Satz 7.18. •

First we describe a method for computing the radical for an abelian group. Then we extend the method to non-abelian groups.

6.3.1 Abelian rational matrix groups

Let $A \leq GL(d, \mathbb{Q})$ be a finitely generated abelian group. We want to determine the radical $Rad_A(V)$. First we have to cite some results from module

theory. For more details we refer to [13, Section 7.3.]. Note that the $\mathbb{Q}A$-module $\mathbb{Q}[A]$, with A acting from the right, can be seen as a ring. Under this point of view the $\mathbb{Q}A$-submodules of $\mathbb{Q}[A]$ correspond to the right ideals of $\mathbb{Q}[A]$.

6.3.4 Definition: Let $\mathfrak{R}$ be ring. An element $\mathfrak{r} \in \mathfrak{R}$ is called *nilpotent* if there is a natural number n such that $\mathfrak{r}^n = 0$.

6.3.5 Proposition: *Let $\mathfrak{R}$ be an abelian artinian ring. The radical $Rad(\mathfrak{R})$, which is defined as the intersection of the maximal ideals of $\mathfrak{R}$, is composed of the nilpotent elements of $\mathfrak{R}$, i.e.*

$$Rad(\mathfrak{R}) \;=\; \{\, \mathfrak{r} \in \mathfrak{R} \mid \mathfrak{r} \textit{ nilpotent} \,\}$$

Proof: See [13] Folgerung 7.22. •

We denote a matrix or a matrix group diagonalizable if it is conjugated in $GL(d, \mathbb{C})$ to a diagonal matrix or a diagonal matrix group.

6.3.6 Lemma: *Let $A \leq GL(d, \mathbb{Q})$ be a finitely generated abelian group and $\mathcal{B}$ be a basis for $\mathbb{Q}[A]$. Then $Rad_A(\mathbb{Q}[A]) = 0$ if and only if each element in $\mathcal{B}$ is diagonalizable.*

Proof: Assume that $Rad_A(\mathbb{Q}[A]) = 0$. Then

$$Rad_A(V) = V\,Rad_A(\mathbb{Q}[A]) = V0 = 0.$$

Therefore V is semisimple. So we can write $V = \mathbb{Q}^d$ as the direct product of irreducible $\mathbb{Q}[A]$-modules

$$V = V_1 \oplus \cdots \oplus V_r.$$

By Schur's Lemma $\mathbb{Q}[A_{V_i}]$ is a field and thus it is generated by a primitive element a_i, which possesses an irreducible minimal polynomial p_i. Since $\mathbb{Q}$ is separable, the polynom p_i has no multiple zeros. This implies that a_i is diagonalizable. So $\mathbb{Q}[A]$ is diagonalizable on each V_i and therefore $\mathbb{Q}[A]$ on V too.

Conversely we assume that every element in $\mathcal{B}$ is diagonalizable. First we show that all elements in $\mathcal{B}$ are simultaneously diagonalizable. It suffices to show by induction that two elements $b, c \in \mathcal{B}$ are simultaneously diagonalizable. Denote by $b_1, \ldots, b_s$ the eigenvalues of b and by $Eig(b, b_i)$ the space of all eigenvectors of the matrix b of the eigenvalue b_i. If $e \in Eig(b, b_i)$, then

it follows that $(ec)b = (eb)c = (b_i e)c = b_i(ec)$ and so $ec \in Eig(b, b_i)$. Thus, the vector space $Eig(b, b_i)$ is a c-invariant submodule of V for $i = 1, \ldots, s$. Certainly the matrix c is diagonalizable on $Eig(b, b_i)$ and so b and c are simultaneously diagonalizable. This implies that all elements in $\mathcal{B}$ are simultaneously diagonalizable.

We deduce, that the algebra $\mathbb{Q}[A]$ is diagonalizable. So there exists an element $c \in GL(d, \mathbb{C})$ such that $\mathbb{Q}[A]^c$ is in diagonal form. Let $r \in Rad_A(\mathbb{Q}[A])$. By Proposition 6.3.5, there exists an $n \in \mathbb{N}$ such that $r^n = 0$. This implies, that $(r^c)^n = 0$ and hence $r^c = 0$. We deduce that $Rad_A(\mathbb{Q}[A]) = 0$. •

6.3.7 Corollary: *Let A be an abelian finitely generated rational matrix group. Then A is diagonalizable if and only if $Rad_A(V) = 0$.*

Proof: This follows directly by Lemma 6.3.6 and Lemma 6.3.3. •

6.3.8 Lemma: *Let $A \leq GL(d, \mathbb{Q})$ be a finitely generated abelian group and $\mathcal{B}$ be a basis for $\mathbb{Q}[A]$. Let $a \in \mathbb{Q}[A]$ with minimal polynomial $f_a(x) \in \mathbb{Q}[x]$ and let $f_a(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r}$ be its factorization into irreducible factors. Then a is diagonalizable if and only if $e_1 = \cdots = e_r = 1$. If a is not diagonalizable, then $f_1(a) \cdots f_r(a)$ is a non-trivial nilpotent element of $Rad_A(\mathbb{Q}[A])$.*

Proof: The matrix a is is diagonalizable in $GL(d, \mathbb{C})$ if and only if f_a has no multiples zeros in $\mathbb{C}$. This is equivalent with $e_1 = \cdots = e_r = 1$.

Certainly the element $\alpha := f_1(a) \cdots f_r(a)$ is nilpotent since $\alpha^{max\{e_i\}} = 0$. By Proposition 6.3.5 we know that $\alpha \in Rad_A(\mathbb{Q}[A])$. So if a is not diagonalizable, then there is at least one $e_i \neq 1$, which implies that α is a non-trivial nilpotent element of $Rad_A(\mathbb{Q}[A])$. •

Let $A \leq GL(d, \mathbb{Q})$ be a finitely generated abelian group and $V = \mathbb{Q}^d$ the natural $\mathbb{Q}A$-module. We outline an algorithm to determine the radical $Rad_A(V)$. Using the *spinning algorithm* we calculate a basis for the $\mathbb{Q}A$-module $\mathbb{Q}[A]$. For every new element which we add to the basis, we can check with the help of lemma 6.3.8 if it is diagonalizable. If not we can determine, again with the aid of Lemma 6.3.8, a nilpotent element $\alpha \in Rad_A(\mathbb{Q}[A])$. The $\mathbb{Q}A$-module W generated by $V\alpha$ is a submodule of $Rad_A(V)$ by Lemma 6.3.3. Now proceed by inducing the action of A to the module V/W. The algorithm terminates because the number of diagonalizable elements which we can add to to the basis of $\mathbb{Q}[A]$ is bounded by d.

```
RadicalOfAbelianGroup(A)
  set V := Q^d and W := 0 ≤ V
  set B := { }
  repeat
      find a new basis element b in Q[A]\⟨B⟩ (via the spinnig algorithm)
      compute the minimal polynomial f_b of b
      determine a factorization of f_b = f_1^e1 ··· f_r^er
      if there exists an e_i ≠ 1 then
          calculate the nilpotent element α:=f_1(b)···f_r(b)
          spin up the QA-module U/W generated by (V/W)α
          set W:=U
          induce the action of A to V/W
          set B := { }
      else
          set B := B ∪ {b}
      end if
  until B is a basis of Q[A]
  return W
```

6.3.2 Rational matrix groups

Let G be a finitely generated solvable subgroup of $GL(d,\mathbb{Q})$. This section gives a method to calculate the radical $Rad_G(V)$, where V is the natural $\mathbb{Q}G$-module $\mathbb{Q}^d$. The kernel of the *p-congruence homomorphism* $K_p(G)$ is unipotent-by-abelian by Theorem 2.4.4 because $K_p(G) \leq G$ is solvable. This is of vital importance for this algorithm. The following theorem shows, that it is sufficient to compute $Rad_{K_p(G)}(V)$.

6.3.9 Theorem: *Let $G \leq GL(d,\mathbb{Q})$ and N a normal subgroup of G such that $[G:N] < \infty$. Denote by V the natural $\mathbb{Q}G$-module $\mathbb{Q}^d$. Then it follows that $Rad_G(V) = Rad_N(V)$.*

Proof: See [25] 1.5. and 1.8. •

So we need to outline a method to compute the radical of a rational matrix group which is unipotent-by-abelian.

6.3.10 Proposition: *Let $K \leq GL(d,\mathbb{Q})$ be an unipotent-by-abelian group. Then K is triangularizable.*

Proof: See [15] Corollary 2.8. •

6.3.11 Lemma: *Let K be an unipotent-by-abelian subgroup of $GL(d,\mathbb{Q})$. Let V be the natural $\mathbb{Q}K$-module $\mathbb{Q}^d$. Then for all $k \in K'$ the set $V(k-1)$ is a subset of $Rad_K(V)$.*

Proof: By Proposition 6.3.10, there exists an $c \in GL(d,\mathbb{C})$ such that K^c is in triangular form. The commutator subgroup K' is unipotent and so $(x(k-1))^c = x^c(k^c-1)$ is nilpotent for all $x \in K$ and $k \in K'$. It follows that $x(k-1)$ is nilpotent. Therefore the ideal in $\mathbb{Q}[K]$ generated by $(k-1)$ is nilpotent as well. By [13, Lemma 7.20] this implies that $(k-1)$ is an element of $Rad_K(\mathbb{Q}[K])$. Now by Lemma 6.3.3 we conclude that $V(k-1) \subset Rad_K(V)$. •

Now we are ready to describe a method to compute $Rad_{K_p(G)}(V) = Rad_G(V)$. Regard the submodule $W \leq V$ which is spanned up by the set

$$\{\, [k,l]-1 \mid k,l \text{ generators of } K_p(G) \,\}.$$

By Lemma 6.3.11 we conclude that $W \subset Rad_{K_p(G)}(V)$, because $K_p(G)$ is unipotent-by-abelian. Further $K_p(G)$ acts as an abelian group on V/W and so we can compute $Rad_{K_p(G)}(V/W)$ with the algorithm of the section 6.3.1. By Lemma 6.3.3 it follows that $Rad_{K_p(G)}(V/W) = Rad_{K_p(G)}(V)/W$ and we are done.

In case we have just normal subgroup generators of $K_p(G)$, we have to modify this approach.
First we have to close the basis of $\mathbb{Q}[K_p(G)]$ under the conjugation action of G.
Second it is possible, that we calculate a module W which is "too small", i.e. a module W such that $K_p(G)$ does not act in an abelian way on V/W. In computing $Rad_{K_p(G)}(V/W)$, where W is spanned up by normal subgroup generators only, we have to make sure that $\mathbb{Q}[K_p(G)]$ acting on V/W is abelian. In spinning up a basis of $\mathbb{Q}[K_p(G)]$ we check if each element g which we add to the partial basis $\{g_1,\ldots,g_j\}$ commutes with all g_i for $i = 1,\ldots,j$. If there is an i such that $gg_i \neq g_ig$ we reset $W := \langle W([g,g_i]-1)\rangle$.

Let G be a finitely generated solvable subgroup of $GL(d,\mathbb{Q})$ and let $K_p(G)$ be the kernel of the *p-congruence homomorphism* given by a list of normal subgroup generators. The following method determines the radical $Rad_G(V)$.

```
Radical(G, K_p(G))
   let 𝒦 be a list containing normal subgroup generators of K_p(G)
   set V := ℚ^d
   compute the G-submodule W of V generated by {V([k,l]-1) | k,l ∈ 𝒦}
   induce the matrix action of G and K_p(G) to V/W
   set ℬ := { }
   repeat
        find a new basis element b in ℚ[⟨𝒦⟩^G] \ ⟨ℬ⟩ (via the spinnig algorithm)
        if b commutes with all elements in the partial basis ℬ then
            compute the minimal polynomial f_b of b
            determine a factorization of f_b = f_1^{e_1} ··· f_r^{e_r}
            if there exists an e_i ≠ 1 then
                calculate the nilpotent element α := f_1(b) ··· f_r(b)
                spin up the G-module U/W generated by (V/W)α
                reset W := U
                set ℬ := { }
            else
                set ℬ := ℬ ∪ {b}
            end if
        else
            determine b̂ ∈ ℬ such that [b, b̂] ≠ 1
            spin up the G-module W' generated by W([b, b̂] - 1)
            reset W := W'
            set ℬ := { }
        end if
        induce the action of G and K_p(G) to V/W
   until ℬ is a basis for ℚ[⟨𝒦⟩^G] = ℚ[K_p(G)]
   return W
```

6.3.12 Remark: In the last algorithm `Radical(`G`,`$K_p(G)$`)`, we can replace $K_p(G)$ by any unipotent-by-abelian group $K \trianglelefteq G$ which is of finite index in G.

6.4 Radical series

Let G be a finitely generated solvable subgroup of $GL(d, \mathbb{Q})$ and $V = \mathbb{Q}^d$ its natural $\mathbb{Q}G$-module. Now it is straightforward to formulate an algorithm to calculate the so-called radical series.

6.4.1 Definition: Let G be a finitely generated solvable subgroup of $GL(d,\mathbb{Q})$ and $V=\mathbb{Q}^d$ its natural $\mathbb{Q}G$-module. The radical series

$$\mathbb{Q}^d = R_0 > R_1 > \cdots > R_n = 0$$

is defined by $R_{i+1} := Rad_G(R_i)$.

The algorithm presented in section 6.3.2 can be used in an iterated way as follows

```
RadicalSeries(G)
  set Rad:=Q^d
  set Series:=[Rad]
  determine K_p(G) and set K := K_p(G)
      while Rad≠ 0 do
          let G_R and K_R be the induced action of G and K to Rad
          Rad:=Radical(G_R,K_R) (Section 6.3.2)
          add Rad to Series
          set G := G_R and K := K_R
      end while
  return Series
```

6.4.2 Lemma: *The algorithm* `RadicalSeries` *ist correct.*

Proof: By Remark 6.3.12 it remains to show that in every loop K_R is unipotent-by-abelian and of finite index in G_R. By Lemma 6.1.6 we have $K_R = K_p(G)_R \leq K_p(G_R) \trianglelefteq G_R$ and so K_R is unipotent-by-abelian. From $[G : K_p(G)] < \infty$ we deduce that $[G_R : K_R] < \infty$ by the homomorphism theorem. •

In a similar way we construct the faster algorithm `RadicalSeriesOfAbelianGroup`. It works as `RadicalSeries` with the only difference that it uses the algorithm `RadicalOfAbelianGroup` instead of `Radical`. Note, that for this approach it is not necessary to calculate $K_p(G)$.

6.4.3 Remark: By Lemma 6.3.3 $Rad_G(R_i/R_{i+1}) = 0$ and thus R_i/R_{i+1} is a semisimple $\mathbb{Q}G$-module.

6.5 Semisimple groups

Let S be a finitely generated semisimple solvable subgroup of $GL(d,\mathbb{Q})$. Recall that the group S is called semisimple if $Rad_S(V) = 0$, where $V = \mathbb{Q}^d$.

6.5.1 Remark: If $Rad_S(V) = 0$ then $Rad_{K_p(S)}(V) = 0$ by Theorem 6.3.9. This implies that V is the direct product of irreducible $K_p(S)$-modules.

We want to determine a splitting of the natural $\mathbb{Q}K_p(S)$-module $\mathbb{Q}^d$ into irreducible modules.

6.5.2 Corollary: *Let $S \leq GL(d,\mathbb{Q})$ be a finitely generated semisimple solvable group and denote p as an admissible prime for S. Then $K_p(S)$ is abelian and torsion-free.*

Proof: By Lemma 6.3.11 every element of the commutator of $K_p(S)$ must be trivial. Further $K_p(S)$ is torsion-free by Theorem 2.4.4. •

Thus it is sufficient to describe a splitting method for abelian semisimple groups.

6.5.1 Abelian semisimple groups

Let A be a finitely generated abelian semisimple matrix subgroup of $GL(d,\mathbb{Q})$. Our aim is to calculate a splitting of the natural $\mathbb{Q}A$-module $V = \mathbb{Q}^d$ into irreducible modules.
The first step will be to determine a primitive element c of the matrix algebra $\mathbb{Q}[A]$, i.e. an element c such that $\mathbb{Q}[c] = \mathbb{Q}[A]$. Recall that by Lemma 6.3.3 $\mathbb{Q}[A]$ is semisimple as a $\mathbb{Q}A$-module if and only if V is semisimple as $\mathbb{Q}A$-module.

6.5.3 Lemma: *Let $A := \langle a_1,\ldots,a_k\rangle$ be an abelian semisimple matrix subgroup of $GL(d,\mathbb{Q})$. Let $\mathcal{B} = \{b_1,\ldots,b_l\}$ be a basis for the semisimple algebra $\mathbb{Q}[A]$. Then almost all linear combinations of $b_1,\ldots,b_l$ yield an primitive element for $\mathbb{Q}[A]$.*

Proof: By induction it suffices to show that the statement is true for the case $l = 2$. So let x, y be the elements of the basis $\mathcal{B}$. We want to show that for almost all $a \in \mathbb{Q}$ we have $\mathbb{Q}[x + ay] = \mathbb{Q}[x, y]$. Thus we have to find two polynomials $f, g \in \mathbb{Q}[X]$ such that $f(x + ay) = x$ and $g(x + ay) = y$ for almost all $a \in \mathbb{Q}$. By Corollary 6.3.7 we can assume that there exists an element $c \in GL(d,\mathbb{C})$ such that $\mathbb{Q}[A^c]$ is in diagonal form. Define $\hat{x} := x^c$

and $\hat{y} := y^c$. If $\hat{x}_i$ and $\hat{y}_i$ are the entries on the diagonals of $\hat{x}$ and $\hat{y}$ we have to find polynomials $f, g \in \mathbb{Q}[X]$ with $f(\hat{x}_i + a\hat{y}_i) = \hat{x}_i$ and $g(\hat{x}_i + a\hat{y}_i) = y_i$ for $i = 1, \ldots, d$. Complex polynomials $f, g \in \mathbb{C}[X]$ verifying these conditions can be found by interpolation. We only have to make sure that $\hat{x}_i + a\hat{y}_i = \hat{x}_j + a\hat{y}_j$ implies $\hat{x}_i = \hat{x}_j$ and $\hat{y}_i = \hat{y}_j$. This is easy to achieve in choosing an a such that $a \neq \frac{\hat{x}_i - \hat{x}_j}{\hat{y}_i - \hat{y}_j}$ for all $i, j \in \{1, \ldots, d\}$. We deduce that $f(x + ay) = x$ and $g(x + ay) = y$. Since x, y and $x + ay$ are rational f, g can be chosen in $\mathbb{Q}[X]$. •

It is well-known, that an element c such that $\mathbb{Q}[A] = \mathbb{Q}[c]$ has a minimal polynomial whose degree is equal to $dim(\mathbb{Q}[A])$. Now we can outline the following algorithm to determine a primitive element of $\mathbb{Q}[A]$.

```
PrimitiveElement(A)
  determine via the spinning algorithm a basis B of Q[A].
  repeat
      set c :=RandomLinearCombination(B)
      set m :=MinimalPolynomial(c)
  until (degree of m) = Length(B)
  return c
```

Note that the length of the basis $\mathcal{B}$ is bounded by d because $\mathbb{Q}[A]$ is diagonalizable.

6.5.4 Definition: A module W is called *homogeneous* if it it is the direct product of irreducible and isomorphic modules.

Once we are able to calculate a primitive element of $\mathbb{Q}[A]$ where A is an abelian semisimple group, we can use the following Lemma to split the natural $\mathbb{Q}A$-module V into the direct product of homogeneous submodules $W \leq V$.

6.5.5 Lemma: *Let c be a diagonalizable element of $GL(d, \mathbb{Q})$. Write the minimal polynomial f of c as the product of irreducible polynomials*

$$f = f_1 \cdot f_2 \cdots f_r$$

(Note that $f_i \neq f_j$ for $i \neq j$ because c is diagonalizable.) Further we define the submodule W_i of $V = \mathbb{Q}^d$ as the kernel of the linear mapping defined by $f_i(c)$ for $i = 1, \ldots, r$. Then it follows that

1. *V can be written as the direct product of the W_i, i.e.*

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_r.$$

Further W_i is $\mathbb{Q}[c]$-invariant for $i = 1, \ldots, r$.

2. *W_i is a homogeneous $\mathbb{Q}[c]$-module for $i = 1, \ldots, r$.*

Proof:

1. The matrix algebra $\mathbb{Q}[c]$ is abelian and so W_i is a $\mathbb{Q}[c]$-invariant submodule of V. Via induction over i we want to prove that

$$ker(f_1(c) \cdots f_i(c)) = W_1 \oplus W_2 \oplus \cdots \oplus W_i.$$

For $i = r$ this gives the wanted result.

If $i = 1$ then we have $ker(f_1(c)) = W_1$ and so the statement is true. Now assume that $ker(f_1(c) \cdots f_{i-1}(c)) = W_1 \oplus W_2 \oplus \cdots \oplus W_{i-1}$ and let $w \in ker(f_1(c) \cdots f_i(c))$. Because f_i and $f_1 \cdots f_{i-1}$ are coprime, there exist $\alpha, \beta \in \mathbb{Q}$ such that $1 = \alpha f_i + \beta f_1 \cdots f_{i-1}$. Thus we can write

$$w = \underbrace{\alpha f_i(c)w}_{\in ker(f_1(c)\cdots f_{i-1}(c))} + \underbrace{\beta f_1(c) \cdots f_{i-1}(c)w}_{\in W_i}.$$

If $w \in W_i$ and $w \in ker(f_1(c) \cdots f_{i-1}(c))$, then we can deduce that $w = 0$. It follows that $(W_1 \oplus \cdots \oplus W_{i-1}) \cap W_i = 0$ and that $ker(f_1(c) \cdots f_i(c)) = (W_1 \oplus \cdots \oplus W_{i-1}) + W_i$.

2. First we induce the action of $\mathbb{Q}[c]$ to W_i. Now we have $f_i(c) = 0$ and so f_i is the minimal polynomial of c. Assume that $I \neq \mathbb{Q}[c]$ is an ideal of $\mathbb{Q}[c]$. Certainly $c + I$ is a primitive element of $\mathbb{Q}[c]/I$. The minimal polynomial f_{c+I} of $c + I$ must be a divisor of f_i. Therefore $f_{c+I} = f_i$, because $I \neq \mathbb{Q}[c]$, and hence $I = 0$. We deduce that the algebra $\mathbb{Q}[c]$ is simple. This implies that W_i is homogeneous for $i = 1, \ldots, r$ (see [11] Chapter 17 Corollary 4.5. and Proposition 4.7.).

•

The following Lemma gives a method to split a homogeneous $\mathbb{Q}A$-module W, where A is an abelian subgroup of $GL(d, \mathbb{Q})$.

6.5.6 Lemma: *Let $A \leq GL(d,\mathbb{Q})$ be an abelian group and W be a homogeneous $\mathbb{Q}A$-submodule of $\mathbb{Q}^d$. Then every non-trivial vector $w \in W$ is contained in an irreducible $\mathbb{Q}A$-submodule of W.*

Proof: Let w be a non-trivial vector in W. Denote by U the $\mathbb{Q}A$-module which is generated by w. It is possible to write $W = \oplus_{i=1}^{s} W_i$, where the W_i are irreducible $\mathbb{Q}A$-modules and hence $w = \sum_{i=1}^{s} w_i$ where $w_i \in W_i$. Because w is non-trivial there is at least one $i \in \{1,\ldots,n\}$ with $w_i \neq 0$. We want to show that the projection $\phi : U \to W_i$ is a bijective $\mathbb{Q}A$-homomorphism. The map ϕ is clearly a surjective $\mathbb{Q}A$-homomorphism and so it suffices to show that ϕ is injective. Let u be an element of U such that $\phi(u) = 0$. It is possible to write $u = w^a$ with $a \in \mathbb{Q}[A]$. It follows that $0 = \phi(u) = \phi(w^a) = \phi(w)^a = w_i^a$. By Schur's lemma (6.1.4) we deduce that $a = 0$ and so $u = 0$. We conclude that ϕ is bijective and thus $U = W_i$. Therefore the module U is irreducible. •

Finally we carried all the necessary elements together to achieve the aim of this section: Under the assumption that A is a finitely generated abelian semisimple subgroup of $GL(d,\mathbb{Q})$ we want to calculate a direct splitting of the natural $\mathbb{Q}A$-module $V = \mathbb{Q}^d$ into irreducible modules.

```
IrreducibleSplitting(A)
  set c :=PrimitiveElement(ℚ[A]) (see 6.5.3)
  let f be the minimal polynomial of c
  factorize f = f_1 ··· f_r where f_i irreducible
  set W_i := ker(f_i(c)) for i = 1,...,r
  # splitting into homogeneous submodules (see 6.5.5)
  split V = W_1 ⊕ ··· ⊕ W_r
  # splitting into irreducible submodules (see 6.5.6)
  for i = 1 to r do
    split W_i by spinning up vectors
  end for
  return the irreducible splitting of V
```

6.6 Composition series

Now we are ready to outline the main result of this section: Let G be a finitely generated solvable subgroup of $GL(d,\mathbb{Q})$. Denote by $K_p(G)$ the

kernel of the *p-congruence homomorphism* defined in Section 2.4 and by V the natural $\mathbb{Q}K_p(G)$-module $\mathbb{Q}^d$. We present an algorithm which calculates a composition series of V, i.e. a sequence of $\mathbb{Q}K_p(G)$-submodules

$$V = V_1 > V_2 > \cdots > V_m = 0$$

such that V_i/V_{i+1} is irreducible. Further we desribe an algorithm which calculates a composition series of V seen as a $\mathbb{Q}G$-module, under the assumption that G is abelian.

Let $\mathbb{Q}^d = R_0 > R_1 > \cdots > R_n = 0$ be the radical series defined in the section 6.4. By Theorem 6.3.9 $Rad_{K_p(G)}(V) = Rad_G(V)$ because $K_p(G)$ is of finite index in G. Therefore $K_p(G)_{R_i/R_{i+1}}$ is a semisimple group by Lemma 6.3.3. Further by Lemma 6.1.6 we get that $K_p(G)_{R_i/R_{i+1}}$ is a subgroup of $K_p(G_{R_i/R_{i+1}})$, which is by Corollary 6.5.2 abelian and torsion-free. Thus $K_p(G)_{R_i/R_{i+1}}$ is a free abelian semisimple group and we can apply the methods of section 6.5.1 to split R_i/R_{i+1} into irreducible $\mathbb{Q}K_p(G)$-modules.

```
CompositionSeries(K_p(G))
    # compute the radical series (section 6.4)
    compute V = R_0 > R_1 > ··· > R_n = 0
    for all factors of this series do
      induce the action of K_p(G) to R_i/R_{i+1}
      # irreducible splitting (section 6.5.1)
      split R_i/R_{i+1} into irreducible QK_p(G)-modules
    end for
    return the refined radical series
```

For abelian groups we can formulate a similar and faster approach.

```
CompositionSeriesAbelianGroup(G)
    # compute the radical series of an abelian group (section 6.4)
    compute V = R_0 > R_1 > ··· > R_n = 0
    for all factors of this series do
      induce the action of G to R_i/R_{i+1}
      # irreducible splitting (section 6.5.1)
      split R_i/R_{i+1} into irreducible QG-modules
    end for
    return the refined radical series
```

Chapter 7

Main algorithms

Let G be a finitely generated subgroup of $GL(d, \mathbb{Q})$. As the main result of this thesis, we outline in this chapter an algorithm which computes a polycyclic presentation of the group G, if G is polycyclic. Further we show that a similar approach can be used to test if a finitely generated subgroup $H \leq GL(d, R)$ is solvable, where $R = \mathbb{Q}$, $\mathbb{Z}$ or a finite field $\mathbb{F}_q$. If $R = \mathbb{Z}$ or $\mathbb{F}_q$ the group H is solvable if and only if it is polycyclic (see Section 2.3). Therefore, in this case we can also test if H is polycyclic.
We begin this chapter with some remarks about the calculation of normal subgroup generators.

7.1 Normal subgroup generators

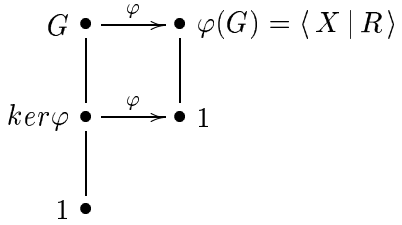
We suppose that $G := \langle g_1, \ldots, g_k \rangle$ is a finitely generated group and that

$$\varphi : G \to \varphi(G)$$

is a group homomorphism. Further we assume, that we know how to calculate a finite presentation of the group

$$\varphi(G) = \langle\, X \mid R \,\rangle$$

where $X = \{\varphi(g_1), \ldots, \varphi(g_k)\}$ and R are relations in X.

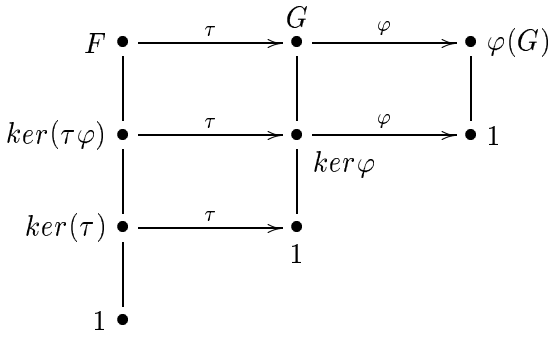


7.1.1 Lemma: *Define the set*

$$R(G) := \{\, r(g_1, \ldots, g_k) \mid r \in R \,\}.$$

Then $R(G)^G = ker\varphi$.

Proof: Let F be a free group on k generators $f_1, \ldots, f_k$. Define τ to be the map $\tau : F \to G$, $f_i \mapsto g_i$. Then by the definition of a finite presentation we know that $R(F)^F = ker(\tau\varphi)$, where $R(F)$ are the relations in R expressed in the elements $f_1, \ldots, f_k$. The elements in $R(F)$ are normal subgroup generators of $ker(\tau\varphi)$. Thus $\tau(R(F)) = R(G)$ are normal subgroup generators for $ker\varphi$.



•

The calculation of normal subgroup generators of φ gets a little more complicated if we are only able to calculate a finite presentation $\varphi(G) = \langle Y|S\rangle$ with $Y \neq X = \{\varphi(g_1), \ldots, \varphi(g_k)\}$. In this case we have to convert the presentation $\varphi(G) = \langle Y|S\rangle$ to a presentation $\varphi(G) = \langle X|R\rangle$.

7.1.2 Proposition: *Let $H = \langle Y|S\rangle$ be a finitely presented group and let X be an arbitrary generating set for H. Then there exists a finite presentation of the form $H = \langle X|R\rangle$.*

Proof: Every element $x \in X$ can be written as a word $w_x(Y)$ over the set $Y \cup Y^{-1}$. Vice versa we can write $y = w_y(X)$ for every $y \in Y$. Then we

have the following relations in H:

$$s(w_y(X)|y \in Y) = 1 \text{ for } s = s(Y) \in S,$$

$$x = w_x(w_y(X)|y \in Y) \text{ for } x \in X.$$

We call these relations R. Define $\hat{X} := \{\hat{x_1}, \ldots, \hat{x_k}\}$ to be a set of abstract symbols and define the group $\hat{H} := \left\langle \hat{X} | R(\hat{X}) \right\rangle$. Then there is an epimorphism $\pi : \hat{H} \to H$, $\hat{x_i} \mapsto x_i$, because the elements $x_i \in X$ fulfill the relations in R. On the other hand the map $\sigma : Y \to \hat{H}$, $y_i \mapsto w_{y_i}(\hat{X})$ can also be extended to an homomorphism $H \to \hat{H}$, since every relation in S is fulfilled by the the elements $w_{y_i}(\hat{X})$ in $\hat{H}$. Further every element x can be expressed as a word in Y and so σ is surjective. Since π and σ are inverse to each other we get that $H \cong \hat{H}$. •

Assume that a finite presentation of $\varphi(G) = \langle Y|S\rangle$ is given, where Y is not equal to $X = \{\varphi(g_1), \ldots, \varphi(g_k)\}$. Then we can compute normal subgroup generators of $ker\varphi$ in the following way: Convert the presentation $\varphi(G) = \langle Y|S\rangle$ to a presentation $\varphi(G) = \langle X|R\rangle$ using Proposition 7.1.2. Then calculate normal subgroup generators of $ker\varphi$ using Lemma 7.1.1.

7.2 Solvability

7.2.1 Finite matrix groups

Let G be a finite matrix group. Then G is solvable if and only if G is polycyclic by Theorem 2.3.1. Therefore we can use the algorithm `ConstructivePcSequenceFinite`, explained in Section 3.3, to test if G is solvable.

7.2.2 Rational matrix groups

Let G be a finitely generated subgroup of $GL(d, \mathbb{Q})$. In Section 6.4 we described the algorithm `RadicalSeries` to compute the radical series of the natural $\mathbb{Q}G$-module $\mathbb{Q}^d$, if G is solvable. The next Lemma and Proposition show that this algorithm can be used to test if G is solvable.

7.2.1 Lemma: *Let K be a finitely generated subgroup of $GL(d,\mathbb{Q})$ and let*

$$\mathbb{Q}^d = V_0 > V_1 > \cdots > V_n = 0$$

be a series of $\mathbb{Q}K$-modules such that K acts in an abelian way on the factors of this series. Then the group K is solvable.

Proof: By Lemma 6.2.6, we can find a matrix $g \in GL(d,\mathbb{Q})$ such that K^g is in block-upper-triangular form. That is, every element $k \in K^g$ is of the form

$$\begin{pmatrix} k_0 & * & * & * \\ & k_1 & * & * \\ & & \ddots & * \\ & & & k_{n-1} \end{pmatrix}$$

where the k_i are matrices in $GL(d_i,\mathbb{Q})$ with $\sum_{i=0}^{n-1} d_i = d$. The matrices $\{\, k_i \mid k \in K \,\}$ correspond to the induced action of K to the factor V_i/V_{i+1} (see again Lemma 6.2.6). By hypothesis $K_{V_i/V_{i+1}}$ is an abelian group for $i = 0,\ldots,n-1$. Therefore the matrices $\{\, k_i \mid k \in K^g \,\}$ generate an abelian group for $i = 0,\ldots,n-1$. Thus, the commutator of two matrices in K^g is in upper-triangular form. It follows that the commutator subgroup K' is unipotent and thus K is unipotent-by-abelian. Therefore the group K is solvable. •

7.2.2 Proposition: *Let G be a finitely generated subgroup of $GL(d,\mathbb{Q})$. Then the group G is solvable if and only if the image under the p-congruence homomorphism $I_p(G)$ is solvable and if the algorithm* `RadicalSeries` *(see Section 6.4) returns a submodule series $\mathbb{Q}^d = V_0 > V_1 > \cdots > V_n = 0$.*

Proof: Assume that G is solvable. Then $I_p(G) \cong G/K_p(G)$ is solvable. Further the algorithm `RadicalSeries` terminates by Section 6.4.

Now we assume that $I_p(G)$ is solvable and that the algorithm `RadicalSeries(`G`,` $K_p(G)$`)` terminates (Note that the finite group $I_p(G)$ is polycyclic. Therefore normal subgroup generators for $K_p(G)$ can be obtained by calculating a polycyclic presentation of $I_p(G)$.) Let $\mathbb{Q}^d = V_0 > V_1 > \cdots > V_n = 0$ be the submodule series which is returned by the algorithm. By the construction of the algorithm $K_p(G)_{V_i/V_{i+1}}$ is abelian for $i = 0,\ldots,n-1$. Therefore, $K_p(G)$ is solvable by Lemma 7.2.1. This implies that the group G is solvable. •

Therefore we can specify the following algorithm for a finitely generated group $G \leq GL(d,\mathbb{Q})$:

```
IsSolvable(G)
  let ψ_p : G → GL(d,p) be the p-congruence homomorphism
  # (see Definition 2.4.2 )
  try to determine a constructive pc-sequence for I_p(G) = ψ_p(G)
  # (see Chapter 3 on finite groups)
  if this fails then
    return 'fail'
    # (I_p(G) is not solvable, see Section 7.2.1)
  fi
  calculate normal subgroups generators for K_p(G) = ker(ψ_p)
  # (see Section 7.1)
  try to compute the radical series V = V_1 > V_2 > ··· > V_m = 0
  # (see Section 6.4)
  if this fails then
    return 'false'
  else
    return 'true'
  fi
```

7.3 Calculating presentations

7.3.1 Finite matrix groups

Let G be a finite matrix group. By Corollary 2.2.5 it is sufficient to calculate a constructive polycyclic sequence to get a polycyclic presentation of G. This can be done by the algorithm `ConstructivePcSequenceFinite`, explained in Section 3.3.

7.3.2 Rational matrix groups

Let the group $G := \langle g_1, \ldots, g_k \rangle$ be a polycyclic subgroup of $GL(d, \mathbb{Q})$. By Corollary 2.2.5 it is sufficient to calculate a constructive polycyclic sequence to get a polycyclic presentation of G. This can be done by the following algorithm:

```
ConstructivePcSequence(G)
  let ψ_p : G → GL(d,p) be the p-congruence homomorphism
  # (see Definition 2.4.2)
  determine a constructive pc-sequence for I_p(G) = ψ_p(G)
  # (see Chapter 3 on finite groups)
  calculate normal subgroups generators for K_p(G) = ker(ψ_p)
  # (see Section 7.1)
  let V := Q^d be the natural QK_p(G)−module
  compute a composition series V = V_1 > V_2 > ··· > V_m = 0
  # (see Section 6.6)
  let ν : K_p(G) → K_p(G)_{V_0/V_1} × K_p(G)_{V_1/V_2} × ··· × K_p(G)_{V_{n-1}/V_n}
  # (see Section 6.2.2)
  for i in [0...(n-1)] do
    determine a constructive pc-sequence C_i of K_p(G)_{V_i/V_{i+1}}
    # K_p(G)_{V_i/V_{i+1}} ≤ K_p(G_{V_i/V_{i+1}}) is abelian by Corollary 6.5.2
    # (Q[K_p(G)_{V_i/V_{i+1}}] is a field by Schur's Lemma, apply Chapter 4)
  od
  merge C_1,...,C_{n-1} to a constructive pc-sequence of K_p(G)^ν.
  let U_p(G) be the kernel of ν
  combine I_p(G) and K_p(G)^ν to a constructive pc-sequence of G/U_p(G)
  calculate normal subgroup generators of U_p(G)
  determine a constructive pc-sequence for the unipotent group U_p(G)
  # (see Chapter 5)
  combine G/U_p(G) and U_p(G) to a constructive pc-sequence of G
  return the constructive pc-sequence of G
```

7.3.1 Remark: We have to pay attention to the fact that we can only compute normal subgroup generators for $K_p(G)$ and $U_p(G)$. Therefore we have to close the constructive pc-sequences for $K_p(G)^\nu$ and $U_p(G)$ under the conjugation action of G.

For a finitely generated abelian group $A \leq GL(d, \mathbb{Q})$ we can proceed by a similar but faster approach. The only modification to the last algorithm is, that we can skip the calculations in the finite part $I_p(G)$:

```
ConstructivePcSequenceAbelianGroup(A)
  let V := Q^d be the natural QA−module
  compute a composition series V = V_1 > V_2 > ··· > V_n = 0
  # (see Section 6.6)
  let ν : A → A_{V_0/V_1} × A_{V_1/V_2} × ··· × A_{V_{n−1}/V_n}
  # (see Section 6.2.2)
  for i in [0...(n-1)] do
    determine a constructive pc-sequence C_i of A_{V_i/V_{i+1}}
    # (Q[A_{V_i/V_{i+1}}] is a field by Schur's Lemma, apply Chapter 4)
  od;
  merge C_1, ..., C_{n−1} to a constructive pc-sequence of A^ν.
  let U_p(A) be the kernel of ν
  calculate normal subgroup generators of U_p(A)
  determine a constructive pc-sequence for the unipotent group U_p(A)
  # (see Chapter 5)
  combine A^ν and U_p(A) to a constructive pc-sequence of A
  return the constructive pc-sequence of A
```

The big advantage of this approach for abelian groups is not that we economize a lot of time in skipping the calculations in the finite part $I_p(G)$. In practice this is the fewest time consuming step. Rather, the benefit of this method is, that we use the generators $a_1, \ldots, a_k$ of the abelian group A instead of the normal subgroup generators of $K_p(A)$ for the further computations. In general the matrices $a_1, \ldots, a_k$ have much smaller entries. Also it is not necessary to close the set A^ν under the conjugation action of A.

7.3.2 Remark: The algorithm `ConstructivePcSequence` works correctly if the input G is a polycyclic group. But what does happen if the finitely generated group G is not polycyclic ?

- Case 1: G is not solvable. Then either the computation of a constructive pc-sequence for the finite image $I_p(G)$ or the computation of the radical series with the help of $K_p(G)$ must fail (See Section 7.2). The described algorithms detect this.

- Case 2: G is solvable but not polycyclic. In this case the algorithm does not terminate.

  The algorithm is able to calculate a constructive pc-sequence for $I_p(G)$ and for $K_p(G)^\nu$. Since $K_p(G)$ is of finite index in G, $K_p(G)^\nu$ is a finitely generated abelian group and thus polycyclic. When we close the constructive pc-sequence of $K_p(G)^\nu$, which is maybe uncomplete

because we used only normal subgroup generators of $K_p(G)$, under the conjugation action of G, we must finish after a finite number of steps. This is because every strictly ascending chain of subgroups of $K_p(G)^\nu$ is finite (see [20] Chapter 1 Section A.).

The calculation of a constructive pc-sequence for $U_p(G)$ does not terminate. This is because we receive an infinite number of generators for $U_p(G)$ when we try to close the set of normal subgroup generators for $U_p(G)$ under the conjugation action of G.

7.4 A further possible refinement

Let G be a polycyclic subgroup of $GL(d, R)$. Our aim is to describe a further method for the determination of a constructive polycyclic sequence of G. It has not been implemented so far.

Let

$$R^d = V_0 > V_1 \cdots > V_m = 0$$

be a submodule series of the natural G-module R^d. We induce the action of G to this series

$$\nu : G \to G_{V_0/V_1} \times \cdots \times G_{V_{m-1}/V_m}.$$

The image under this action G^ν is the direct product of polycyclic matrix groups of smaller dimension than d. The kernel under this action $ker(\nu)$ is an unipotent matrix group. With the algorithms described in Section 7.3 we can calculate a constructive pc-sequence for $G_{V_i/V_{i+1}}$ for $i = 0, \ldots, m-1$ and thus for G^ν. Then we calculate normal subgroup generators for $ker(\nu)$. Using these we calculate a constructive pc-sequence for the unipotent group $ker(\nu)$ (and close this pc-sequence under the conjugation action of G). Finally we combine the constructive pc-sequences of G^ν and $ker(\nu)$ to a constructive pc-sequence of G.

If $R = \mathbb{Q}$ we can use for example the radical series as the required submodule series $\mathbb{Q}^d = V_0 > \cdots > V_m = 0$. It can be computed by the the algorithm of Section 6.4.
If $R = \mathbb{F}_q$ we can use the Meataxe (see for example [17]) to calculate a submodule series with irreducible factors.

Chapter 8

Performance

In this chapter we present the runtimes of the main algorithms of this thesis for some example groups. Further we give a short desription of the bottle necks of the algorithm for the determination of a constructive polycyclic sequence.

8.1 Runtimes

We outline the runtimes for the following algorithms.

- **ConPcsFinite**: Determination of a constructive polycyclic sequence for $\psi_p(G)$, where $G \leq GL(d, \mathbb{Q})$ is the given group (see Section 3.3).
- **IsSolvable**: Test if the given group is solvable (see Section 7.2).
- **ConPcs**: Determination of a constructive polycyclic sequence for the given group (see Section 7.3.2).
- **PcPresent**: Calculation of a polycyclic presented group isomorphic to the given one (see Section 7.3.2 and Corollary 2.2.5).

Note that every algorithm in this list includes the preceding algorithms.

The following matrix groups are used as examples:

- G_1 is the group generated by the matrices

$$\begin{pmatrix} 73/10 & -35/2 & 42/5 & 63/2 \\ 27/20 & -11/4 & 9/5 & 27/4 \\ -3/5 & 1 & -4/5 & -9 \\ -11/20 & 7/4 & -2/5 & 1/4 \end{pmatrix}, \begin{pmatrix} -42/5 & 423/10 & 27/5 & 479/10 \\ -23/10 & 227/20 & 13/10 & 231/20 \\ 14/5 & -63/5 & -4/5 & -79/5 \\ -1/10 & 9/20 & 1/10 & 37/20 \end{pmatrix}.$$

- G_2 is the group generated by the matrices

$$\begin{pmatrix} 5 & 2 & -8 & 17 & -1 \\ -69/4 & -15/4 & 449/20 & -163/5 & 53/20 \\ -2 & 4 & 9/5 & 63/5 & 3/5 \\ 13/4 & 3/4 & -121/20 & 57/5 & -17/20 \\ 241/4 & 7/4 & -1477/20 & 319/5 & -189/20 \end{pmatrix}, \begin{pmatrix} 19/2 & 0 & -3 & -19/2 & -1/2 \\ -74/5 & 129/20 & 7/4 & 159/4 & 9/10 \\ 53/10 & 4/5 & -4 & 9/2 & -9/10 \\ 37/10 & -41/20 & -7/4 & -29/4 & -3/5 \\ 137/5 & -457/20 & 37/4 & -559/4 & 3/10 \end{pmatrix}.$$

- G_3 is the group generated by the matrices

$$\begin{pmatrix} -492568055 & -715902540 & -559233360 & 913773168 \\ 853152732 & 1239979321 & 968620464 & -1582701120 \\ 796991748 & 1158354480 & 904858501 & -1478515764 \\ 543797628 & 790360020 & 617396520 & -1008810083 \end{pmatrix},$$

$$\begin{pmatrix} -348686135 & -530151780 & -271469520 & 913773168 \\ -603941868 & -918249479 & -470198736 & 1582701120 \\ -215499732 & -327651600 & -167777219 & 564742596 \\ -793008492 & -1205711460 & -617396520 & 2078172517 \end{pmatrix}.$$

- G_4 is a subgroup of $GL(4,\mathbb{Q})$ with 5 generators. In GAP this group can be found under `AlmostCrystallographicGroup(4,2,[0,-3,-2,1,-1,-2,4])` as a part of the 'AcLib'-Package.
- G_5 is a subgroup of $GL(4,\mathbb{Q})$ with 5 generators. In GAP this group can be found under `AlmostCrystallographicGroup(4,86,[0,-2,-1,-2,-1])` as a part of the 'AcLib'-package.
- G_6 is a subgroup of $GL(16,\mathbb{Z})$ with 9 generators. In GAP this group can be found under `PolExamples(5)` as a part of the 'Polenta'-package.
- G_7 is a subgroup of $GL(16,\mathbb{Q})$ with 5 generators. In GAP this group can be found under `PolExamples(24)` as a part of the 'Polenta'-package.

The calculations were made on a Pentium 4 with 2 gigahertz under the system Linux. The runtimes are outlined in milliseconds.

Group G	ConPcsFinite	IsSolvable	ConPcs	PcPresent
G_1	10	50	300	490
G_2	10	150	26300	35890
G_3	10	20	190	240
G_4	10	170	2770	2950
G_5	20	170	1720	2060
G_6	830	9440	41530	57270
G_7	50	600	458330	479040

Note that the runtimes of two computations of a polycyclic presentation for the same group can differ. This is because during the algorithm some random choices are made, which can have a great influence on further computations. For example the orbits points, which are used in ConPcsFinite (see Section 3.1), are randomly choosen. Also the algorithm `PrimitiveElement` (see Section 6.5) uses randomized methods.

8.2 Bottle necks

The calculation of normal subgroup generators (see Section 7.1) of $K_p(G)$ and $U_p(G)$ produces matrices with much more complex entries in comparison with these of the input group. This slows down further computations. Further, we have to conjugate the group $U_p(G) \leq GL(d, \mathbb{Q})$ to a subgroup of $UT(d, \mathbb{Z})$ (see Section 5.1). This operation increases the bit length of the matrix entries to a large extend. That is the reason why the computation of a constructive polycyclic sequence of $U_p(G)$ is in the general the most time consuming step. For example the determination of a constructive polycyclic seqeuence of the group G_7 costed in total 458 seconds. Just for the unipotent part $U_p(G_7)$ the algoritm needed 450 seconds.

A further problem is, that the storage of the orbits used in the computations in the finite group $\psi_p(G)$ (see Section 3.1) can cost too much memory. This happens for example for the wreath product $G_6 \; wr \; P \leq GL(128, \mathbb{Z})$, where P is a polycyclic permutation group of order 8.

Bibliography

[1] Björn Assmann, *Polenta - Polycyclic presentations for matrix groups - A GAP 4 package*, http://cayley.math.nat.tu-bs.de/software/content.html, 2003.

[2] Robert Beals, *Improved algorithms for the Tits alternative*, Groups and Computation III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ. 8, pages 63-77, de Gruyter Berlin 2001.

[3] Robert Beals, *Towards polynomial time algorithms for matrix groups*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 28, 1997.

[4] Henri Cohen: *A course in computational algbraic number theory*, Springer Verlag 1993.

[5] John D. Dixon: *The orbit-stabilizer problem for linear groups*, Can. J. Math., Vol. 17, No. 2, pages 238-259, 1985.

[6] Bettina Eick, *Algorithms for Polycyclic Groups*, Habilitationsschrift, Kassel 2001.

[7] Bettina Eick and Björn Assmann, *Alnuth - A GAP package containing methods for number fields and an interface to KANT*, http://cayley.math.nat.tu-bs.de/software/content.html, 2003.

[8] Bettina Eick and Werner Nickel, *Polycyclic - Computation with polycyclic groups. A GAP 4 package*, http://cayley.math.nat.tu-bs.de/software/content.html, 2003.

[9] Martin Isaacs, *Character Theory of finite groups*, Dover Publications Inc. New York, 1994.

[10] The KANT Group, *KANT - Computational Algebraic Number Theory*, http://www.math.tu-berlin.de/~kant/kash.html, 2003.

[11] Serge Lang, *Algebra*, Addison-Wesley, 1993.

[12] E.M. Luks: *Computing in solvable matrix groups*, In Proc. 33rd IEEE Sympos. Foundations Comp. Sci., pages 111-120, 1992.

[13] W. Müller: *Darstellungtheorie von endlichen Gruppen*, Teubner Stuttgart 1980.

[14] Gretchen Ostheimer: *Algorithms for polycyclic-by-Finte Groups*, Phd Thesis, Rutgers University, Math. Dept., 1996.

[15] Gretchen Ostheimer: *Practical Algorithms for Polycyclic Matrix Groups*, J. Symbolic Computation 11, 1-000, 2001.

[16] M. F. Newman: *The soluble length of soluble linear groups*, Math. Z., 126, pages 59-70, 1972

[17] R. Parker: *The computer calculation of modular characters. (The Meataxe)*, in M. Atkinson (ed.), Computational Group Theory, Academic Press, London, pages 267-74, 1984.

[18] Micheal E. Pohst:*Computational Algebraic Number Theory*, DMV Seminar Band 21, Birkhäuser 1993.

[19] D.J.S. Robinson: *A course in the Theory of Groups*, volume 80 of *Graduate Texts in Math.*, Springer Verlag, New York, Heidelberg, Berlin 1982.

[20] Daniel Segal: *Polycyclic groups*, Cambridge University Press, 1983.

[21] Charles C. Sims: *Computation with finitely presented groups*, Cambrigde University Press, 1994.

[22] Charles C. Sims: *Computing the Order of a Solvable Permutation Group*, J. Symbolic Computation 9, 699-705, 1990.

[23] Ian Stewart and David Tall: *Algebraic number theory and Fermat's last theorem*, A K Peters 2002.

[24] The GAP Group, *GAP - Groups, Algorithms and Programming*, http://www.gap-system.org, 2003.

[25] B. A. F. Wehrfritz: *Infinite linear groups*, Springer-Verlag, New York, Heidelberg, Berlin 1973.