École Polytechnique

M1 internship report

On the complexity of computing the algebraic closure of a finitely generated matrix semigroup

Klara Nosan
M1 Informatique - Voie Jacques Herbrand
klara.nosan@polytechnique.edu

Supervised by:
Amaury Pouly, IRIF, Université de Paris

Co-supervised by:
Sylvain Schmitz, IRIF, Université de Paris,
Mahsa Shirmohammadi, IRIF, Université de Paris,
James Worrell, Oxford University

August 2020

Abstract

Invariants are an important methodology in the area of program verification. Given a linear program, finding the invariants that hold throughout the entire execution of the program can help us prove various temporal safety properties of the program. An algebraic invariant, in particular, assigns to each program location a set of polynomial equations over the program variables that hold in the given location. The strongest algebraic invariant is determined by giving, for each program location, the set of all equations holding at that location. It has been shown that the problem of computing the strongest algebraic invariant of a program can be reduced to that of computing the Zariski closure of a finitely generated semigroup of rational matrices. The algorithm to do so, in turn, generalises (and uses as a subroutine) an algorithm to compute the Zariski closure of a finitely generated group of invertible matrices. Both of the aforementioned algorithms are important technical contributions in computational algebraic geometry, yet the complexity of neither algorithm has been analysed. The motivation behind this internship was to study the two algorithms and attempt to analyse their complexity starting with the group closure algorithm first.

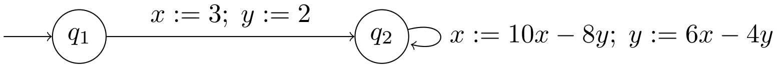
In this report, we first present the mathematical background behind the algorithm to compute the Zariski closure of a finitely generated group of invertible matrices. We give intuition on the complexity of the algorithm and provide algebraic group theoretic facts we can use to reason about the complexity. In particular, we give a proof of a bound on the dimension of a quotient group of two algebraic groups. We propose an adjusted version of the algorithm, which in combination with the aforementioned group theoretic bound reduced the problem to the problem of finding an element of infinite order in a matrix group. We review several approaches to solving the latter problem and propose an appropriate one for our reasoning. Finally, we list all the components of the complexity bound we have found and discuss what is missing in order to establish one.

1 Introduction

Computing program invariants is a classical approach in the verification of temporal safety properties of programs. Given a linear program, finding the invariants that hold throughout the entire execution of the program can help us prove various properties of the program, such as non-termination. To better understand what precisely invariants are and how we can use them for program verification, consider the following example of a linear loop

```
$x := 3$
$y := 2$
while $2y - x \geq -2$ do
    $\begin{bmatrix} x \\ y \end{bmatrix} := \begin{bmatrix} 10 & -8 \\ 6 & -4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$
end
```

The above loop never halts. Although just by observing the program the non-termination is perhaps not immediately obvious, we can easily prove it by computing the invariants of the program. First, observe that we can represent it in the following way



The representation above is an example of an affine program with two locations (q_1 and q_2). *Affine programs* are a simple kind of nondeterministic imperative programs in which the only instructions are assignments whose right-hand sides are affine expressions, such as $x := 10x - 8y$ above. Given such a program, computing the exact reachable states (*i.e.* all the values that the program variables can take in a given location of the program) is often difficult, which is why one turns to computing invariants instead. An *algebraic invariant* of an affine program assigns to each program location a set of polynomial equations over the program variables that hold in the given location. For each given location the set of common zeroes of the polynomials (which we call an *algebraic set*) holding at that location is thus essentially just an overappoximation of the reachable states for that location. In the example above, such a set for the location q_1 could be $\{(x, y) \in \mathbb{R}^2 : x + y - 5 = 0\}$. Note that both $\{(x, y) \in \mathbb{R}^2 : xy - 6 = 0\}$ and $\{(x, y) \in \mathbb{R}^2 : x^2y + xy^2 + 5xy - 6x - 6y - 30 = 0\}$ are also invariants of the program for the location q_1, whereas the latter admits the least solutions and thus represents the best (most precise) approximation of the reachable states out of the three. In general, we say the best overapproximation of the reachable states we can find to be *the strongest algebraic invariant*. In particular, we determine the strongest algebraic invariant by giving, for each program location, the set of *all* equations holding at that location.

Now let us turn our attention to the location q_2 and note that the following polynomial invariant holds $x - 9x^2 - y + 24xy - 16y^2 = 0$. In particular, we can easily verify that all the pairs $(x, y) \in \mathbb{R}^2$ in the set of solutions of the polynomial equation satisfy the guard $2y - x \geq -2$ from the original loop. Having found an algebraic invariant, we can thus conclude that the program we have been analysing will never terminate.

Because of the importance of invariants in program verification, automated invariant synthesis has been a topic of active research in the past two decades and an algorithm to compute the strongest algebraic invariants that hold at each location of a given affine program was first presented in an article published by Hrushovski, Ouakanine, Pouly and Worrell in 2018 [HOPW18]. In particular, the problem of computing the strongest algebraic invariant was reduced to that of computing the Zariski closure of a finitely generated semigroup of rational matrices and an algorithm to do so described. Actually, the algorithm generalises (and uses as a subroutine) an algorithm of Derksen, Jeandel, and Koiran [DJK05] to compute the Zariski closure of a finitely generated group of invertible matrices, which was initially designed to answer several problems in the field of quantum automata.

Both of the aforementioned algorithms are important technical contributions in computational algebraic geometry, yet to the best of our knowledge the complexity of neither algorithm has been analysed. The motivation behind this internship was to study the two algorithms and attempt to analyse their complexity. In particular, our goal was to find a bound on the degree of the polynomial equations defining the Zariski closure of a semigroup of matrices, *i.e.*, the strongest algebraic invariant. Once such a bound is obtained, there is a very straightforward algorithm to compute the Zariski closure due to Seidl and Muller-Olm [MS, MS04], which computes all polynomial invariants of a fixed degree d. Note that the computational aspects of finitely generated matrix semigroups have been an active area of research in recent years. An article published by Kiefer, Haase, et al. just this year [BHK$^+$19], for example, gives a new upper bound on the size of a finitely generated matrix semigroup, in case it is finite. Our aim of giving a bound on the degree of the polynomials defining a finitely generated matrix group is in a similar spirit, but much more general than that.

As the semigroup closure algorithm (and thus its complexity) fundamentally depends on that of the group closure algorithm, the internship was focused on studying the group algorithm first. The work initially required learning about algebraic geometry, group theory, algebraic group theory and algebraic number theory in order to understand how the algorithm works. We then proceeded by analysing the algorithm's complexity on simple instances, in order to gain intuition as to how we could tackle the problem in the general case. We considered several approaches and chose one in which we slightly adjusted the original group closure algorithm, in order to be able to reason on the complexity using group theoretic facts. The fact that the quotient of an algebraic matrix group by a normal subgroup is again a matrix group plays an important role in the algorithm of [DJK05]. A large part of the internship was then dedicated to understanding and adjusting the proof of a bound on the dimension of a quotient group of two algebraic groups, which we could use to reason on the complexity of the algorithm. The adjusted algorithm in combination with the aforementioned group theoretic bound reduced the problem to finding an element of infinite order in a matrix group. We thus also studied several approaches to solving that problem and familiarised ourselves with various aspects of computational group theory and computational algebraic number theory. While our results do not yield a concrete bound on the degree of polynomial equations group closure algorithm just yet, there is only one remaining component of the bound missing. In particular, what remains to be done before the final bound could be obtained, is to compute the size of the coefficients defining the embedding of a quotient group into a linear algebraic group.

In this report, we start by giving a concise overview of the challenges and contributions of the work done during the internship in Section 2. We then provide a brief overview of the mathematical background necessary to understand the algorithm for computing the Zariski closure of a group of matrices in Section 3 and review the algorithm in Section 4. We give the intuition as to why determining its complexity has proven to be a difficult task in Section 5 and state the group theoretical bound on the dimension of a quotient of an algebraic group with a normal subgroup that we have proven in Section 6. We provide some intuition on the proof, as well as an illustrative example, whereas the full proof is given in Appendix B. In Section 7 we present the adjusted algorithm, which reduces the problem of determining the complexity to that of finding an element of infinite order in a matrix group and review the algorithms to do so in Section 8. Finally, we summarise by reviewing all the components of the complexity bound we have found thus far in Section 9 and conclude by discussing the future work to be done on the topic.

2 Challenges and contributions

The aim of this section is to explicitly state the main challenges that arose in the process of determining the complexity of the algorithm to compute the Zariski closure of a finitely generated group of matrices and the contributions we have made towards solving the problem.

First let us note that the complexity depends on three purely mathematical questions:

1. Given a linear algebraic group G and a normal subgroup H, following Theorem 3 we have that G/H can be embedded as a subgroup of a matrix group via a regular mapping. We need to compute a bound on the dimension of the matrix group, the degree of the polynomial defining the regular embedding, and the height and degree of the (algebraic-number) coefficients of this polynomial.
2. Given a finitely generated matrix group that contains an element of infinite order (equivalently which is not finite), find a bound on the shortest product of generators that yields such an infinite-order element.
3. Give an upper bound on the size of a finitely generated matrix group that is finite. In particular, we require a bound on the size of the group in terms of the dimension of the matrices, number of generators, and height and degree of elements of generators.

While the third of the three questions is a well-researched problem in computational algebraic group theory (such bounds are presented in *e.g.* [BBR93, BHK$^+$19]), finding the solutions to the first and the second problem were two of our main challenges. Our third and final challenge was finding a way to put the three bounds together in order to obtain a final complexity bound, since when applied to the objects we are computing with in the algorithm, the three bounds above depend recursively on each other (as further explained Section 5).

Our contributions are as follows:

1. Given a linear algebraic group G and a normal subgroup H, we have found a bound on the dimension of the matrix group and the degree of the polynomial defining the regular embedding of G/H as a subgroup of a matrix group. Note that what is still missing is a bound height and degree of the (algebraic-number) coefficients of this polynomial.

2. Given a finitely generated matrix group that contains an element of infinite order (equivalently which is not finite), we propose an algorithm to find such an element, which in turn, induces a bound on the shortest product of generators that yields an infinite-order element.

3. Given the solutions to the above three mathematical problems, we have provided an alternative version of the algorithm, the complexity of which we know to analyse using the bounds.

3 Mathematical background

3.1 Algebraic number theory

A complex number α is *algebraic* if it is a root of a univariate polynomial with integer coefficients. The defining polynomial of α, denoted p_α, is the unique integer polynomial of least degree, whose coefficients have no common factor, that has α as a root. The *degree* of α is the degree of p_α, and the *height* of α (denoted $h(\alpha)$) is the greatest absolute value of the coefficients of p_α. If p_α is monic then we say that α is an *algebraic integer.* The sum, the difference, the product and the quotient of two algebraic numbers (except for division by zero) are algebraic numbers; this means that the set of all algebraic numbers is a *field*, commonly denoted by $\mathbb{A}$. Given an algebraic field $\mathbb{F}$, the algebraic integers of $\mathbb{F}$, form a ring denoted $O_{\mathbb{F}}$, called the ring of integers. The real and complex numbers that are not algebraic, such as π and e, are called *transcendental numbers.*

A field $\mathbb{K}$ is said to be a *field extension*, denoted $\mathbb{K}/\mathbb{F}$, of a field $\mathbb{F}$, if $\mathbb{F}$ is a subfield of $\mathbb{K}$. Given a field extension $\mathbb{K}/\mathbb{F}$, the larger field $\mathbb{K}$ is an $\mathbb{F}$-vector space. The dimension of this vector space is called the *degree* of the extension and is denoted by $[\mathbb{K} : \mathbb{F}]$.

An *algebraic number field* (or simply number field) $\mathbb{K}$ is a finite degree (and hence algebraic) field extension of the field of rational numbers $\mathbb{Q}$. Thus $\mathbb{K}$ is a field that contains $\mathbb{Q}$ and has finite dimension when considered as a vector space over $\mathbb{Q}$. Each number field $\mathbb{K}$ is a simple extension of $\mathbb{Q}$, *i.e.*, $\mathbb{K}$ can be represented as $\mathbb{K} = \mathbb{Q}(\alpha)$, which is generated by the adjunction of a single element $\alpha \in \mathbb{K}$. Simple extensions are well understood and can be completely classified.

A field $\mathbb{K}$ is said to be *algebraically closed* if every non-constant polynomial $p(x) \in \mathbb{K}[x]$ has a root in $\mathbb{K}$. An example of an algebraically closed field is the field of complex numbers $\mathbb{C}$. The *algebraic closure* of a field $\mathbb{K}$ is the smallest algebraic extension of $\mathbb{K}$ (up to isomorphisms) that is algebraically closed.

Let $p(x) \in \mathbb{K}[x]$ be a polynomial. The *splitting field* of $p(x)$ is the smallest field over which $p(x)$ can be decomposed into linear factors.

A *root of unity*, is any complex number that yields 1 when raised to some positive integer power n, *i.e.*, ζ such that $\zeta^n = 1$. If ζ_n is an nth root of unity and for each $k < n$, $\zeta^k \neq 1$, then we call it a *primitive root of unity.* We can always choose a primitive root of unity by setting $\zeta_n = e^{2i\pi\frac{k}{n}}$. The nth *cyclotomic polynomial*, for any positive integer n, is the unique irreducible polynomial $\Phi(x) \in \mathbb{Q}[x]$ with integer coefficients that is a divisor of $x^n - 1$ and is not a divisor of $x^k - 1$ for any $k < n$. Its roots are all nth primitive roots of unity.

3.2 Linear algebra

Let $\mathbb{K}$ be a field. We denote with M_n the set of all square matrices of dimension n with entries from $\mathbb{K}$. The set of all *invertible* matrices of dimension n with entries from $\mathbb{K}$ form a group together with the operation of ordinary matrix multiplication. We call the group the *general linear group* over $\mathbb{K}$ and denote it by $\mathrm{GL}_n(\mathbb{K})$.

If V is a vector space over $\mathbb{K}$, the general linear group of V, written $\mathrm{GL}(V)$, is the group of all automorphisms of V, *i.e.*, the set of all bijective linear transformations $V \to V$, together with functional composition as group operation. If V has finite dimension n, then $\mathrm{GL}(V)$ and $\mathrm{GL}_n(\mathbb{K})$ are isomorphic.

A square matrix X is said to be *diagonalizable* or nondefective if it is similar to a diagonal matrix, *i.e.*, if there exists an invertible matrix P and a diagonal matrix D such that $P^{-1}XP = D$. A matrix X is called *nilpotent* if there exists some positive integer n such that $X^n = 0$. X is said to be *unipotent* if the matrix $X - I$ is nilpotent. Equivalently, X is unipotent if all eigenvalues of X are equal to 1.

For an algebraically closed field $\mathbb{K}$, a matrix $X \in \mathrm{GL}_n(\mathbb{K})$ is called *semisimple* if it is diagonalizable. Given a matrix X, the *Jordan-Chevalley decomposition* writes X as $X = X_s + X_n$, where X_s is semisimple, X_n is nilpotent, and X_s and X_n commute. It follows that $X = X_s X_u$, where $X_u = I + X_n$ is unipotent, and X_s and X_u commute. For an arbitrary field $\mathbb{K}$, an element X of $\mathrm{GL}_n(\mathbb{K})$ is said to be semisimple if it becomes diagonalizable over the algebraic closure of $\mathbb{K}$.

3.3 Algebraic geometry

Algebraic geometry is a branch of mathematics that studies systems of multivariate polynomial equations.

Let $\mathbb{K}$ be a field (not necessarily algebraically closed). We denote with $\mathbb{K}[x_1, \dots, x_n]$ the ring of polynomials in n variables with coefficients in $\mathbb{K}$. A *polynomial ideal* is a set of polynomials $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ that is stable under addition and absorbs multiplication. In particular

$$\forall f, g \in I : f + g \in I \text{ and } \forall f \in I, g \in \mathbb{K}[x_1, \dots, x_n] : fg \in I.$$

An ideal I of a ring R is said to be a *proper ideal* if I is not the whole of R. A proper ideal I is called a *prime ideal* if for any a and b in R, if ab is in I, then at least one of a and b is in I. A proper ideal I of a ring R is called a *maximal ideal* if there exists no other proper ideal J of R with I a proper subset of J.

An *(affine) algebraic set* or *affine (algebraic) variety* is the set of common zeroes of a finite collection of polynomials S, *i.e.*, a set of the form

$$V(S) = \{x \in \mathbb{K}^n : \forall p \in S.p(x) = 0\}$$

where $S \subseteq \mathbb{K}[x_1, \dots, x_n]$. For an arbitrary S, $V(S) = V(I)$, where I is the ideal generated by S.

Algebraic sets are equipped with a topology called the *Zariski topology*, which is defined by specifying its closed sets. Given an algebraic set $X \subseteq \mathbb{K}^n$, the Zariski topology on X has as closed sets all the algebraic subsets of X, *i.e.*, those sets $A \in X$ that are themselves algebraic sets in $\mathbb{K}^n$. The *Zariski closure* of a subset Y of an algebraic set $X \subseteq \mathbb{K}^n$, denoted $\overline{Y}$, is the smallest algebraic subset of X, such that $Y \subseteq \overline{Y}$.

An algebraic set X is said to be *irreducible* if it is not the union of two proper closed subsets. In other words, $X \in \mathbb{K}^n$ is irreducible if for all algebraic subsets $A, B \subseteq X$ such that $X \subseteq A \cup B$, we have either $X \subseteq A$ or $X \subseteq B$. Note that in some literature, irreducible algebraic sets are called affine varieties, while we have chosen to follow the alternative convention and defined affine (algebraic) varieties to be algebraic sets.

The Zariski topology on a variety is *Noetherian.* This means that the closed subsets of the topology, *i.e.*, affine varieties, satisfy the descending chain condition. Given an affine variety X, for any sequence $Y_1 \supseteq Y_2 \supseteq \dots$ of subvarieties Y_i of X there is an integer n such that $Y_n = Y_{n+1} = \dots$. In particular, any closed subset A of X can be written as a finite union of *irreducible components*, where an irreducible component of Y is a maximal irreducible closed subset of A.

The *dimension* of a topological space is the supremum of all integers n such that there is a chain $\varnothing = Y_0 \subset Y_1 \subset \dots \subset Y_n$ of distinct irreducible closed subsets of a set X. In particular, given a finite topological space, there is no infinite chain of strictly increasing irreducible sets.

Let $X \subseteq \mathbb{K}^m$ and $Y \subseteq \mathbb{K}^n$ be affine varieties. A function $\phi : X \to Y$ is called a *regular map* if it arises as the restriction of a polynomial map $\mathbb{K}^m \to \mathbb{K}^n$. Regular maps are *continuous* with respect to the Zariski topology and the closure of the image of an irreducible set under a regular map is again irreducible. An important fact that we will use later is that given two irreducible affine varieties X and Y, the closure of their product, $\overline{X \cdot Y}$ is also irreducible.

In topology, a set X is said to be *disconnected* if there exist disjoint open sets A, B with $X \subseteq A \cup B$ such that $A \cap X \neq \varnothing$ and $B \cap X \neq \varnothing$, and *connected* otherwise. A set is *Zariski-connected* if it is connected for the Zariski topology on $\mathbb{C}^n$. All irreducible varieties are Zariski-connected.

Note also that the Zariski topology is coarser than the Euclidian topology, in particular, every Zariski-closed set is Euclidean-closed and every Zariski-open set is Euclidean-open. A variety over $\mathbb{C}$ is Zariski-connected if and only if it is Euclidean-connected, thus irreducible varieties over $\mathbb{C}$ are also Euclidean-connected. This is not true over $\mathbb{R}$.

3.4 Group theory

Let G be a group under a binary operation $*$. A subset H of G is called a *subgroup* of G if it also forms a group under the operation $*$, we denote that by $H \leq G$. H is a *normal* subgroup of G, which we denote by $H \lhd G$, if it is invariant under conjugation, *i.e.*, if for every $h \in H$ and every $g \in G$, we have $ghg^{-1} \in H$.

Let G be a group and H a subgroup. The *(left) cosets* of H (in G) are the sets $gH = \{gh : h \in H\}$ for each g in G. We define the *index* of H in G to be the number of cosets of H that fill up G. If the number of cosets of H is finite, we say that H has *finite index* in G. If H is a normal subgroup of G, *i.e.*, $H \lhd G$, the cosets of H in G form a group called the *quotient group* or *factor group*, denoted G/H. Note that a normal subgroup H of a group G has finite index in G if and only if G/H is finite.

The *order* of an element a of a group is the smallest positive integer n such that $a^n = e$, where e is the identity element of the group. If no such n exists, a is said to have *infinite order.* A *torsion* (or *periodic*) group is a group in which every element has finite order. All finite groups are periodic.

A group G is said to be *finitely generated* is it has some finite generating set S so that every element of G can be written as the combination (under the group operation) of finitely many elements of S and of inverses of such elements. One of the most important problems in group theory, known as the *Burnside problem*, asks whether all finitely generated periodic groups are finite. While that is not true in general, the following important result of Schur, which we will need later, is true for subgroups of $\mathrm{GL}_n(\mathbb{K})$

Theorem 1 (Schur)**.** *Every finitely generated periodic subgroup of the general linear group* $\mathrm{GL}_n(\mathbb{K})$ *is finite.*

3.5 Algebraic group theory

An *algebraic group* (sometimes called affine algebraic group) is a group that is an algebraic variety and such that multiplication and inversion are regular maps (*i.e.* restrictions of polynomial maps). An example of an algebraic group is $\mathrm{GL}_n(\mathbb{K})$. Note that $\mathrm{GL}_n(\mathbb{K})$ is an affine variety as we can identify it with a closed subset of $\mathbb{K}^{n^2+1}$ via $A \mapsto (A, \det A^{-1})$, since det is given by a polynomial in the matrix entries. Multiplication $(A, B) \mapsto AB$ is then clearly given by polynomials, and by Cramer's rule, so is inversion $A \mapsto A^{-1}$, *i.e.*, they are both regular maps, so $\mathrm{GL}_n(\mathbb{K})$ is in fact an algebraic group. Note that since matrix multiplication and inversion (and hence also conjugation) are regular maps, they are continuous in the Zariski topology.

A *linear algebraic group* is a Zariski-closed subgroup of $\mathrm{GL}_n(\mathbb{K})$. In the case of linear algebraic groups, regular functions are functions that are polynomial in the entries of an $n \times n$ matrix A and in $\det^{-1}(A)$. Every algebraic group is isomorphic to a linear algebraic group.

Given the fact that an algebraic group G is also an affine variety, we can write it as a finite union of irreducible (resp. connected) components. We denote with G_0 the *identity component* of G, *i.e.*, the connected component of G containing the identity. G_0 is a normal subgroup of G and the irreducible (resp. connected) components of G are the cosets of G_0 in G. In particular, G_0 is of finite index in G.

Given a linear algebraic group G and its connected component of the identity G_0, for each $y \in G$, there exists an integer k, such that $y^k \in G_0$. Actually, for any normal subgroup H of finite index in G, we have that for each $y \in G$, $y^k \in H$ for some integer k.

Let G be a linear group. The Zariski closure of G as a variety, denoted $\overline{G}$, is also a linear algebraic group.

4 The algorithm to compute the Zariski closure of a finitely generated group of matrices

In this section we present the algorithm to compute the Zariski closure of a finitely generated matrix group. Given our interest in complexity, we concentrate on the case of matrices with entries in a number field $\mathbb{K}$, although the algorithm can be extended to more general settings. We start by first giving intuition on how to compute the closure of a cyclic matrix group, *i.e.*, a group generated by a single invertible matrix $X \in \mathrm{GL}_n(\mathbb{K})$. The algorithm to do so, which is a subroutine in the general algorithm, in turn relies on finding the multiplicative relations of a set of numbers $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$. After elaborating on those preliminaries, we proceed by giving the intuition behind the algorithm for the finitely generated case.

4.1 Finding multiplicative relations

Recall that $\mathbb{K}$ is an algebraic number field, let $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$ be a tuple of algebraic numbers. We define the group of multiplicative relations holding among the λ_i to be the subgroup $L(\boldsymbol{\lambda})$ of $\mathbb{Z}^n$ defined by

$$L(\boldsymbol{\lambda}) = \{(a_1, ..., a_n) \in \mathbb{Z}^n : \lambda_1^{a_1} \cdots \lambda_n^{a_n} = 1\}$$

If we consider a group homomorphism $\phi : \mathbb{Z}^n \to \mathbb{K}$ defined by

$$\phi(a_1, \ldots, a_n) = \lambda_1^{a_1} \cdots \lambda_n^{a_n}$$

finding the multiplicative relations amongst the $\lambda_1, \ldots, \lambda_n$ is precisely computing $\ker \phi$. Following [DJK05], the generators of the kernel of ϕ can be found constructively. Moreover, there is a bound on the size of the generators, which is as follows. Recall we denote with $h(\alpha)$ the height of the algebraic number $\alpha \in \mathbb{K}$. Let η be the infimum of $h(\lambda')$ over all $\lambda' \in \mathbb{K}$ that are not roots of unity, $h = \max\{h(\lambda_1), \dots h(\lambda_n), \eta\}$ and ω the largest integer m such that $\mathbb{K}$ contains an m-th root of unity. Then

Theorem 2 (Masser)**.** *The kernel of ϕ is generated by elements $a \in \mathbb{Z}^n$ with*

$$|a| \leq n^{n-1}\omega(h/\eta^{n-1})$$

In other words, Masser's theorem gives us a bound on the size of a basis of the finitely generated abelian group of multiplicative relations $L(\boldsymbol{\lambda})$. Furthermore, the bound depends on the maximum height of the numbers in $\boldsymbol{\lambda}$ and on the values of ω and η, which both depend on the number field $\mathbb{K}$ and can be bound using the degree of the extension $[\mathbb{K} : \mathbb{Q}]$.

A corollary of Masser's result is that a basis for $L(\boldsymbol{\lambda})$ can be found by a brute-force search in space and time polynomial in the length of the binary representation of $L(\boldsymbol{\lambda})$ [OW13]. We can thus see that we will need to keep track of both the maximum height and degree of elements of the matrices we will be using this subroutine on in order to be able to reason using Masser's theorem.

4.2 Computing the Zariski closure of a cyclic group

Let $X \in \mathrm{GL}_n(\mathbb{K})$. To compute the Zariski closure of the group generated by X, $\overline{\langle X\rangle}$, we start by writing X in Jordan normal form, using the Jordan-Chevalley decomposition, to get $X = P(D+N)P^{-1}$, where $D = \mathrm{diag}(\lambda_1, ..., \lambda_n)$ is diagonal, N is nilpotent and $ND = DN$.

Since conjugation is a homeomorphism, $\overline{\langle X\rangle} = \overline{P\,\langle D+N\rangle\, P^{-1}} = P\overline{\langle D+N\rangle}P^{-1}$. Furthermore, $\langle D+N\rangle$ is the image of the set $S := \{(n, \lambda_1^n, .., , \lambda_2^n) \in \mathbb{C}^{n+1} : n \in \mathbb{N}\}$ under a certain polynomial map ϕ. In particular

$$(D+N)^p = \sum_{k=0}^{n-1} \binom{p}{k} N^k D^{p-k} = \sum_{k=0}^{n-1} \binom{p}{k} N^k D^{-k}\,\mathrm{diag}(\lambda_1^p, \dots, \lambda_n^p) = \phi(\lambda_1^p, \dots, \lambda_n^p)$$

where ϕ only depends on D, N and n. Hence $\overline{\langle D+N\rangle} = \overline{\phi(S)} = \overline{\phi(\overline{S})}$. To compute $\overline{\langle D+N\rangle}$ it thus suffices to compute $\overline{S}$ or rather the ideal that generates it.

Let I be the ideal in $\mathbb{C}[x, z_1, \dots, z_n]$, generated by the set of polynomials f such that $f(k, \lambda_1^k, \dots, \lambda_n^k) = 0$ for all $k \in \mathbb{N}$, *i.e.*, the ideal that generates S. Let J be the ideal in $\mathbb{C}[x, z_1, \dots, z_n]$ generated by the set of polynomials

$$z_1^{a_1} \cdots z_n^{a_n} - z_1^{b_1} \cdots z_n^{b_n}$$

where $a_q, b_1, \dots, a_n, b_n \in \mathbb{Z}$ are such that $\lambda_1^{a_1} \cdots \lambda_n^{b_n} = \lambda_1^{b_1} \cdots \lambda_n^{b_n}$. As shown in Appendix A, we have that $I = J$ and hence $\overline{S} = V(I) = V(J)$. We observe that J is precisely the ideal encoding the multiplicative relations among the λ_i, the basis of which we know how to compute using Masser's theorem as indicated in Section 4.1. We thus know how to compute $\overline{S}$ and correspondingly $\overline{\langle X\rangle}$ and have a complexity bound on how to do so.

4.3 Computing the Zariski closure of a finitely generated group

Knowing how to compute the closure of a cyclic group, we can finally turn attention to the finitely generated case. The intuition behind the algorithm can be understood by looking at the properties of the object that we are looking to compute, *i.e.*, the algebraic closure of a finitely generated matrix group. Let $G = \overline{\langle X_1, \dots, X_k\rangle}$ for some $X_i \in \mathrm{GL}_n(\mathbb{K})$. It is well known that G is a closed group. In particular, the irreducible component of the identity G_0 is a normal subgroup of finite index, that is G/G_0, is finite. A way to compute G is to find G_0 and G/G_0, which is precisely the approach of the algorithm. It does not actually compute the two sets, but rather two sets of matrices that have the same properties as G_0 and G/G_0. In particular, the algorithm computes an irreducible group H, and a finite set of matrices S such that $S \cdot H$ is a closed group containing $X_1, \dots, X_k$, that H is a normal subgroup of $S \cdot H$ and that some power of every element of $S \cdot H$ is contained in H.

Let us now recall the original algorithm and then sketch the proof as to how it works and why it terminates.

If we observe the algorithm `OriginalAlgorithm`, we can see that the termination criterion is that both H and S stabilise at some point. In order to prove its correctness we thus first need to show that the sets H and S stop growing. Secondly, we need to convince ourselves that the output $G = S \cdot H$ really is the Zariski closure of $\langle X_1, \dots, X_k\rangle$.

Let us now turn our attention to the algorithm and see how the properties of G_0 and G/G_0 are ensured for H and S. In particular, we can observe that throughout the execution, the following properties hold:

```
Procedure OriginalAlgorithm($X_1, \dots, X_k$)
   input : matrices $X_1, \dots X_k \in \mathrm{GL}_n(\mathbb{K})$
1  $H := \{I_n\}$
2  $S := \{I_n, X_1, \dots, X_k\}$
3  repeat
4      $H_{old} := H$
5      $S_{old} := S$
6      for $y \in S_{old}$ do
7          $H := \overline{H \cdot \overline{\langle y \rangle}_0}$
8          $H := \overline{H \cdot yHy^{-1}}$
9          $G := S \cdot H$
10         for $z \in S_{old}$ do
11             if $yz \notin G$ then $S := S \cup \{yz\}$
12 until $H_{old} = H$ and $S_{old} = S$
   output: $G$
```

- H is an irreducible variety containing the identity I_n,
- $S \cdot H$ contains $X_1, \dots, X_n$ and H,
- $S \cdot H$ is contained in $\overline{\langle X_1, \dots, X_k, H \rangle}$.

The first property follows from the fact that the closure of the image of an irreducible variety remains irreducible under a morphism (Zariski-continuous map). In particular, multiplication under closure and conjugation are both Zariski-continuous. H is irreducible at initialisation, $\overline{\langle y \rangle}_0$ and yHy^{-1} are also irreducible, hence H stays irreducible in the algorithm. The second property is clear since $I_n \in S$ (line 1) and throughout the algorithm S and H never get smaller. The third property follows from the observation that $S \subseteq \langle I_n, X_1, \dots, X_k \rangle$ since we only ever add products of elements of S to S.

Note that $H \subseteq \overline{\langle X_1, \dots, X_k \rangle}$ is closed, irreducible and only increasing during the algorithm. Recall also that since GL_n has finite dimension, there is no infinite chain of increasing strictly increasing irreducible varieties. Hence H eventually stabilises to some value $\widetilde{H}$. Starting from the step where $H = \widetilde{H}$, let $S_1 \subset S_2 \subset \cdots$ be the successive values of S and $\widetilde{S}$ the union of all the S_i. Moreover, note that the inclusions $S_i \subset S_{i+1}$ are strict since the algorithm stops whenever two consecutive values are the same. Then the following properties hold:

- for all $y, z \in \widetilde{H}$, $yz \in \widetilde{H}$,
- for all $y, z \in \widetilde{S}$, $yz \in S \cdot \widetilde{H}$,
- for all $y \in \widetilde{S}$, $y\widetilde{H}y^{-1} \subseteq \widetilde{H}$,
- for all $y \in \widetilde{S}$, some positive power of y belongs to $\widetilde{H}$.

The first property follows from line 8: for $I_n \in S_{old}$ the affectation becomes $H := \overline{H \cdot H}$. The second property follows from the test at line 10 and the assignment at line 11, since $\widetilde{H}$ contains I_n. The third property also follows from line 8 and the fact that H contains the identity. Finally the fourth property follows from line 7 because some positive power of y belongs to $\overline{\langle y \rangle}_0$.

It follows from the observations above and the fact that a closed subsemigroup of $\mathrm{GL}_n(\mathbb{K})$ is a subgroup that $\widetilde{H}$ is a group and $y\widetilde{H}y^{-1} = \widetilde{H}$ for every $y \in \widetilde{S}$. Let $\widetilde{G} = \widetilde{S} \cdot \widetilde{H}$, looking at the properties again, we can see that $\widetilde{G}$ is also a group and $\widetilde{H}$ its normal subgroup, $\widetilde{H} \triangleleft \widetilde{G}$. We can thus consider the quotient $\widetilde{G}/\widetilde{H}$ which is also a linear group as proven in Appendix B. Following the fourth observation above, any element in this quotient has finite order. Furthermore, the quotient is finitely generated, since $\widetilde{G} = \langle I_n, X_1, \dots, X_k \rangle \widetilde{H}$. Putting this together, we have that $\widetilde{G}/\widetilde{H}$ is a finitely generated torsion linear subgroup of $\mathrm{GL}_n(\mathbb{K})$ and following Schur's theorem (Theorem 1) finite. Hence $S_i = \widetilde{S}$ for some i and the algorithm will terminate.

The final thing we have to show is that $\widetilde{G}$ is the closure we are looking for. Looking at the above properties again, we have that $\widetilde{G} \subseteq \overline{\langle X_1, \dots, X_k, H \rangle}$. Since $\widetilde{S}$ is finite and $\widetilde{H}$ is an irreducible variety, $\widetilde{G}$ is closed. Furthermore, $H \subseteq \widetilde{H} \subseteq \widetilde{G}$, $X_1, \dots, X_k \in \widetilde{G}$ and $\widetilde{G}$ is a group, thus $\langle X_1, \dots, X_k, H \rangle \subseteq \widetilde{G}$. Putting these two observations together, we have $\langle X_1, \dots, X_k, H \rangle \subseteq \widetilde{G} \subseteq \overline{\langle X_1, \dots, X_k, H \rangle}$. By virtue $\widetilde{G}$ being closed, we conclude that $\widetilde{G} \subseteq \overline{\langle X_1, \dots, X_k, H \rangle}$.

5 Intuition on the complexity of the algorithm to compute the algorithm to compute the Zariski closure of a finitely generated group of matrices

Understanding how the algorithm constructs the closure, we can now see why it is difficult to bound its complexity. While we have a proof that the algorithm terminates and that the two sets that determine the duration of the execution of the algorithm, H and S, admit certain properties, we have no grip on how precisely (in which order) and how much they grow. In particular, H and S do not necessarily both change in each iteration. Sometimes, the irreducible part (H) will not change, but the finite part (S) will. When the irreducible part reaches its maximum value, we continue adding to the finite part. The question we are aiming to answer is thus: when does the algorithm stop? In this section, we will give some intuition on how we aim to tackle this problem, in particular, how the problem decomposes into the three mathematical problems we discussed in Section 2. In order to do so, we will look at two simplified cases, a run of the algorithm in which H does not increase at all and the case in which H only increases once.

Before focusing on the examples, let us recall again what kind of complexity bound we are looking for. Our goal is analyse the algorithm symbolically and obtain a bound on the degree and coefficients of the polynomials defining the Zariski closure of a finitely generated group of matrices. Note that since we are working with algebraic groups, the field which we are working in will be something we must pay attention to. More specifically, if we start with a group of matrices with entries in a given number field, say $\mathbb{K}$ of given degree d, the group closure might be defined over a field of higher degree. Moreover, if we recall the subroutine for computing the group closure of a cyclic group, we know that it essentially boils down to finding multiplicative relations, the complexity of which is given by Masser's theorem. This in turn relies on both the degree and the height of the input. We hence assume that we will have to keep track of both during the execution.

5.1 Case when H doesn't increase

Let us look at the simplest case of a run of the algorithm, the one when H does not grow and contains only the identity: $H = \{I_n\}$. Note that the group G is finite if and only if H does not increase. We can make a first observation regarding the number field of the entries of the matrices during computation. Let us denote with $\mathbb{K}$ the number field of the input. Clearly H is in $\mathrm{GL}_n(\mathbb{K})$. As S is always obtained by multiplying elements of S, it also stays a subset of $\mathrm{GL}_n(\mathbb{K})$. We compute the closure $G = S \cdot H$ and thus also have $G \leq \mathrm{GL}_n(\mathbb{K})$.

In this case we essentially only need a bound on how much S grows, which we aim to obtain by bounding the quotient G/H. We can do so using group theoretic facts that we will introduce in Section 6, in particular, by embedding the quotient into a subgroup of $\mathrm{GL}_p(\mathbb{K})$ for some p that depends on the degree of the polynomial equations defining H (which we know, since $H = \{I_n\}$). Note that this is precisely Problem 1 in Section 2.

To then get a bound on S (and correspondingly G), we thus need a bound on the size of a finitely generated matrix group that is finite. Let us note here again that finding such a bound given the dimension of the matrices, number of generators, and height and degree of elements of generators, corresponds to the Problem 3 in Section 2.

5.2 Case when H increases only once

Let us now look at the case when H only grows once. This case has the following phases: S increases for a while, H increases once and S continues increasing. In both of the phases where S grows, we have the property that H is a normal subgroup of $\widetilde{G} = \overline{\langle X_1, \dots, X_k \rangle}$, the Zariski closure that we are computing. Similarly to above, we can use that property to give the quotient $\widetilde{G}/H$ the structure of a subgroup of GL_p for some p that will depend on the degree of the polynomial equations defining H. Note here that as long as H does not reach its final value (*i.e.* in this case as long as $H = \{I_n\}$) $\widetilde{G}/H$ will not be finite.

As in the case in the previous section, finding that degree of polynomial equations defining H that induces a bound on p is trivial as long as $H = \{I_n\}$. However, once H increases, things get more complicated. To illustrate why, let us first recall the two assignments that make H grow:

- $H := \overline{H \cdot \overline{\langle y \rangle}_0}$
- $H := \overline{H \cdot yHy^{-1}}$

Looking at both assignments, we can note that the degree of polynomial equations defining H increases when we add the identity component of $\overline{\langle y \rangle}$ to it. In particular, the degree and coefficients of the equations defining H will depend on those of $\overline{\langle y\rangle}_0$. The latter, in turn, relies on Masser's theorem, where the bounds on the degree and height come from an element the last instance of S before H increases. This brings us to yet another question we need to answer: how much does S have to increase before H has to increase too?

Recall that we add $\overline{\langle y\rangle}_0$ to H in order to ensure that some positive power of y is in H. It follows that H will surely increase when executing the first assignment above for an element of $y \in S$ that is of infinite order with respect to H. In other words, to give a bound on when H increases, it suffices to find the shortest product of generators of S that yields such an element. Since we can give the quotient $\widetilde{G}/H$ the structure of a linear algebraic group, finding a bound on the shortest product of generators of $\widetilde{G}/H$ that yields an infinite-order element in $\widetilde{G}/H$, solves our problem. Note that this is precisely Problem 2 in Section 2.

Once we have a bound on the length of the element $y \in S$ that makes S increase, we can finally use Masser's theorem to get the bound on the degree of equations defining H and the dimension p of the embedding. We then again turn to the bound of the size of finitely generated matrix group that is finite (*i.e.* use the results of Problems 1 and 3 in Section 2).

Note that even in this simplified example of an execution of the algorithm, the three mathematical bounds we need for the complexity reasoning depend recursively on each other. The *first bound* on the dimension of the embedding depends on the degree of the polynomials defining H; this depends, in turn, on the size of the basis in Masser's theorem that, in turn, depends on the coefficients of the matrix to which Masser's theorem is applied. This depends on the length of each phase of the algorithm during which H is constant, which depends on the *second bound*, *i.e.*, the bound on the time we need to find an element of infinite order in an infinite matrix group. Finally, the *third bound*, *i.e.*, the bound on the size of a finite matrix group, gives the time to finish after H finally stabilizes.

5.3 The general case

The general case is an execution of the algorithm, within which both H and S increase several times in a certain order. While the setting is very similar to the case where H only increases once, we cannot reuse the same argument to see how much S increases every time before H has to increase. Recall that in the above case, we were able to reduce the problem to the problem of finding an infinite order element in an algebraic group, as in both instances of the execution H was a normal subgroup of $\widetilde{G}$ and hence $\widetilde{G}/H$ was well-defined. However, if we observe the algorithm closely, we see that the property $H \lhd \widetilde{G}$ does not hold in every iteration, *i.e.*, $\widetilde{G}/H$ cannot be given the structure of an algebraic group at every step. In fact, H is a normal subgroup of $S \cdot H$ only straight after initialization when $H = \{I_n\}$ and once H reaches its final value ($H = \widetilde{H}$).

This makes finding a bound on the dimension far more difficult, as we do not know of enough properties of H and S that we could use in our reasoning. Two ways of proceeding arise at this point: we could limit ourselves to analysing the complexity of the algorithm when used to compute the closure of special matrix groups with additional properties, in particular commutativity. Such groups could be *e.g.* solvable or polycyclic groups, which both have non-trivial normal abelian subgroups that could give us the property of H being abelian and make finding a bound for its growth easier. Or, alternatively, try to adjust the algorithm in order to ensure the sets H and S to have more properties we can use in our advantage when determining the complexity. After exploring both options, we choose to pursue the latter, the idea behind which we present in Section 7.

6 Group theoretic bounds

In this section, we introduce the group theoretic bounds we have on the quotient of a group G with a closed normal subgroup $H \lhd G$ and give the reasoning behind them. In particular, we claim the following:

Theorem 3. *Let $H \lhd G$ be a closed normal subgroup of an algebraic group, then G/H is an algebraic group. Furthermore, if $G \leqslant \mathrm{GL}_n(\mathbb{C})$ and H can be defined by polynomial equations of total degree at most d, then G/H is isomorphic to a subgroup of $\mathrm{GL}_p(\mathbb{C})$ with $p \leqslant \binom{m}{d}^2$ where $m = \binom{n^2+d}{d}$. Additionally, if $H \leq GL_n(\mathbb{K})$ is defined over $\mathbb{Q}$, then G/H isomorphic to a subgroup of $GL_p(\mathbb{K})$.*

The full proof of the theorem, which is very technical, can be found in Appendix B. Let us just briefly elaborate on the intuition behind it. Actually, the proof that G/H is an algebraic group is a classical result of algebraic group theory (see *e.g.* [Bor91, Chapter II], [Hum98, Chapter IV] or [Dup, Section 4.1]), whilst the proof of the bound on the dimension of the quotient and the field of the embedding is self-contained. The proof of the former relies on the following group theoretic facts. Given a group G and a normal subgroup $H \lhd G$, the set of cosets of H, denoted by G/H forms a group, which we call the quotient group. In particular, if G and H are algebraic groups, G/H is one too. Secondly, every affine algebraic group can be embedded into a linear algebraic group, *i.e.*, a subgroup of

GL_d for some d. The idea behind the proof that G/H is also a linear algebraic group is thus to give the quotient the structure of one by constructing a homomorphism $\phi : G \to GL(U)$ for some finite vector space U of dimension d, such that $\ker \phi = H$ and $G/H \cong \phi(G)$. (Recall that given a field F and a finite dimensional F-vector space G of dimension p, the general linear group over U, denoted $\mathrm{GL}(U)$ is isomorphic to $\mathrm{GL}_p(F)$, which gives us precisely what we claim). In the case where G is a matrix group, we can further analyse the construction of ϕ and thus obtain the bound on the dimension of the embedding that we claim.

Let us look now at an example that illustrates such an embedding.

Example 4. Let $G = \{\begin{bmatrix}\alpha & \gamma \\ 0 & \beta\end{bmatrix} : \alpha\beta \neq 0\}$ and $H = \{\lambda I_n : \lambda^2 = 1\}$. Then G and H are linear algebraic groups and H is a closed group that is normal in G, so we can consider the quotient G/H. We want to show that this quotient is isomorphic to an algebraic group and hence a linear algebraic group. The idea is to find a homomorphism $\phi : G \to \mathrm{GL}_m$ in such a way that $H = \ker \phi$. If we do so, we will have "cancelled" H and $\operatorname{im} \phi$ will be closed and isomorphic to G/H.

To make things easier, let us first construct a homomorphism $\phi' : G \to \mathbb{C}^p$ such that $H = \ker \phi'$ and equip $\mathbb{C}^p$ with multiplication and inverse that are regular maps, so that it will be isomorphic to GL_m for some m.

An idea to do so is to raise the diagonal elements to the power 2, so that when we plug λ, we get 1. Define

$$\phi' : G \to \mathbb{C}^3 \qquad \begin{bmatrix}\alpha & \gamma \\ 0 & \beta\end{bmatrix} \mapsto (\alpha^2, \beta^2, \gamma).$$

Now by definition, $\phi(H) = \{(1,1,0)\}$ which is what we wanted. However, for ϕ' to be a homomorphism, we would need to be able to express $\phi'(xy)$ simply using $\phi'(x)$ and $\phi'(y)$. If we write

$$\phi'\left(\begin{bmatrix}\alpha & \gamma \\ 0 & \beta\end{bmatrix}\begin{bmatrix}\bar\alpha & \bar\gamma \\ 0 & \bar\beta\end{bmatrix}\right) = \phi'\left(\begin{bmatrix}\alpha\bar\alpha & \alpha\bar\gamma + \gamma\bar\beta \\ 0 & \beta\bar\beta\end{bmatrix}\right) = \left(\alpha^2\bar\alpha^2, \beta^2\bar\beta^2, \alpha\bar\gamma + \gamma\bar\beta\right)$$

we can see that we cannot express $\alpha\bar\gamma + \gamma\bar\beta$ as a polynomial function of $\alpha^2, \bar\alpha^2, \beta^2, \bar\beta^2, \gamma, \bar\gamma$, *i.e.*, ϕ' is not a homomorphism. In order to make it one, we add all products of degree 2:

$$\phi' : G \to \mathbb{C}^6, \begin{bmatrix}\alpha & \gamma \\ 0 & \beta\end{bmatrix} \mapsto (\alpha^2, \beta^2, \gamma^2, \alpha\beta, \alpha\gamma, \beta\gamma).$$

Now we have that

$$\phi'\left(\begin{bmatrix}\alpha\bar\alpha & \alpha\bar\gamma + \gamma\bar\beta \\ 0 & \beta\bar\beta\end{bmatrix}\right) = \left(\alpha^2\bar\alpha^2, \beta^2\bar\beta^2, (\alpha\bar\gamma + \gamma\bar\beta)^2, \alpha\beta\bar\alpha\bar\beta, \alpha\bar\alpha(\alpha\bar\gamma + \gamma\bar\beta), \beta\bar\beta(\alpha\bar\gamma + \gamma\bar\beta)\right).$$

Let us can now check every term: most are clearly products of $\alpha^2, \beta^2, \bar\alpha^2, \bar\beta^2$ so it's easy. The three nontrivial terms are:

- $(\alpha\bar\gamma + \gamma\bar\beta)^2 = \alpha^2\bar\gamma^2 + \gamma^2\bar\beta^2 + 2\alpha\bar\gamma\gamma\bar\beta$: which we can express because we have the cross-product terms $\alpha\gamma$ and $\bar\beta\bar\gamma$.
- $\alpha\bar\alpha(\alpha\bar\gamma + \gamma\bar\beta) = \alpha^2\bar\alpha\bar\gamma + \alpha\bar\alpha\gamma\bar\beta$: we can express using the terms $\bar\alpha\bar\beta$, $\bar\alpha\bar\gamma$ and $\alpha\gamma$ in our representation.
- $\beta\bar\beta(\alpha\bar\gamma + \gamma\bar\beta) = \alpha\beta\bar\beta\bar\gamma + \beta\gamma\bar\beta^2$ similarly to above works because of $\alpha\beta$, $\bar\beta\bar\gamma$ and $\bar\beta^2$) in our representation.

We can now define the multiplication map μ to be

$$\mu((\alpha^2, \beta^2, \gamma^2, \alpha\beta, \alpha\gamma, \beta\gamma), (\bar\alpha^2, \bar\beta^2, \bar\gamma^2, \bar\alpha\bar\beta, \bar\alpha\bar\gamma, \bar\beta\bar\gamma)) = \left(\alpha^2\bar\alpha^2, \beta^2\bar\beta^2, (\alpha\bar\gamma + \gamma\bar\beta)^2, \alpha\beta\bar\alpha\bar\beta, \alpha\bar\alpha(\alpha\bar\gamma + \gamma\bar\beta), \beta\bar\beta(\alpha\bar\gamma + \gamma\bar\beta)\right).$$

Which rewritten in terms of our 6-tuples would be

$$\mu((\alpha^2, \beta^2, \gamma^2, \alpha\beta, \alpha\gamma, \beta\gamma), (\bar\alpha^2, \bar\beta^2, \bar\gamma^2, \bar\alpha\bar\beta, \bar\alpha\bar\gamma, \bar\beta\bar\gamma)) = \left(\alpha^2\bar\alpha^2, \beta^2\bar\beta^2, \alpha^2\bar\gamma^2 + \gamma^2\bar\beta^2 + 2\alpha\gamma\bar\beta\bar\gamma, \alpha\beta\bar\alpha\bar\beta, \alpha^2\bar\alpha\bar\gamma + \alpha\gamma\bar\alpha\bar\beta, \alpha\beta\bar\beta\bar\gamma + \beta\gamma\bar\beta^2\right).$$

We can write

$$\begin{bmatrix}\alpha^2\bar\alpha^2 \\ \beta^2\bar\beta^2 \\ (\alpha\bar\gamma + \gamma\bar\beta)^2 \\ \alpha\beta\bar\alpha\bar\beta \\ \alpha\bar\alpha(\alpha\bar\gamma + \gamma\bar\beta) \\ \beta\bar\beta(\alpha\bar\gamma + \gamma\bar\beta)\end{bmatrix} = \begin{bmatrix}\alpha^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \beta^2 & 0 & 0 & 0 & 0 \\ 0 & \gamma^2 & \alpha^2 & 0 & 0 & 2\alpha\gamma \\ 0 & 0 & 0 & \alpha\beta & 0 & 0 \\ 0 & 0 & 0 & \alpha\gamma & \alpha^2 & 0 \\ 0 & \beta\gamma & 0 & 0 & 0 & \alpha\beta\end{bmatrix}\begin{bmatrix}\bar\alpha^2 \\ \bar\beta^2 \\ \bar\gamma^2 \\ \bar\alpha\bar\beta \\ \bar\alpha\bar\gamma \\ \bar\beta\bar\gamma\end{bmatrix}.$$

And thus get a matrix representation of $(\mathbb{C}^6, \mu)$ and our desired morphism $\phi : G \to \mathrm{GL}_m(\mathbb{C})$, where $m = 6$:

$$\phi\left(\begin{bmatrix} \alpha & \gamma \\ 0 & \beta \end{bmatrix}\right) = A(\alpha^2, \beta^2, \gamma^2, \alpha\beta, \alpha\gamma, \beta\gamma) = \begin{bmatrix} \alpha^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \beta^2 & 0 & 0 & 0 & 0 \\ 0 & \gamma^2 & \alpha^2 & 0 & 0 & 2\alpha\gamma \\ 0 & 0 & 0 & \alpha\beta & 0 & 0 \\ 0 & 0 & 0 & \alpha\gamma & \alpha^2 & 0 \\ 0 & \beta\gamma & 0 & 0 & 0 & \alpha\beta \end{bmatrix}$$

Finally, one can check that the matrix multiplication satisfies our requirements:

$$\phi\left(\begin{bmatrix} \alpha & \gamma \\ 0 & \beta \end{bmatrix}\right)\phi\left(\begin{bmatrix} \bar{\alpha} & \bar{\gamma} \\ 0 & \bar{\beta} \end{bmatrix}\right)$$

$$= \begin{bmatrix} \alpha^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \beta^2 & 0 & 0 & 0 & 0 \\ 0 & \gamma^2 & \alpha^2 & 0 & 0 & 2\alpha\gamma \\ 0 & 0 & 0 & \alpha\beta & 0 & 0 \\ 0 & 0 & 0 & \alpha\gamma & \alpha^2 & 0 \\ 0 & \beta\gamma & 0 & 0 & 0 & \alpha\beta \end{bmatrix} \begin{bmatrix} \bar{\alpha}^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \bar{\beta}^2 & 0 & 0 & 0 & 0 \\ 0 & \bar{\gamma}^2 & \bar{\alpha}^2 & 0 & 0 & 2\bar{\alpha}\bar{\gamma} \\ 0 & 0 & 0 & \bar{\alpha}\bar{\beta} & 0 & 0 \\ 0 & 0 & 0 & \bar{\alpha}\bar{\gamma} & \bar{\alpha}^2 & 0 \\ 0 & \bar{\beta}\bar{\gamma} & 0 & 0 & 0 & \bar{\alpha}\bar{\beta} \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^2\bar{\alpha}2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \beta^2\bar{\beta}^2 & 0 & 0 & 0 & 0 \\ 0 & \alpha^2\bar{\gamma}^2 + \gamma^2\bar{\beta}^2 + 2\alpha\gamma\bar{\beta}\bar{\gamma} & \alpha^2\bar{\alpha}^2 & 0 & 0 & 2(\alpha\gamma\bar{\alpha}\bar{\beta} + \alpha^2\bar{\alpha}\bar{\gamma}) \\ 0 & 0 & 0 & \alpha\beta\bar{\alpha}\bar{\beta} & 0 & 0 \\ 0 & 0 & 0 & \alpha\gamma\bar{\alpha}\bar{\beta} + \alpha^2\bar{\alpha}\bar{\gamma} & \alpha^2\bar{\alpha}^2 & 0 \\ 0 & \beta\gamma\bar{\beta}^2 + \alpha\beta\bar{\beta}\bar{\gamma} & 0 & 0 & 0 & \alpha\beta\bar{\alpha}\bar{\beta} \end{bmatrix}$$

$$= A\big(\alpha^2\bar{\alpha}^2, \beta^2\bar{\beta}^2, (\alpha\bar{\gamma} + \gamma\bar{\beta})^2, \alpha\bar{\alpha}\beta\bar{\beta}, \alpha\bar{\alpha}(\alpha\bar{\gamma} + \gamma\bar{\beta}), \beta\bar{\beta}(\alpha\bar{\gamma} + \gamma\bar{\beta})\big) = \phi\left(\begin{bmatrix} \alpha\bar{\alpha} & \alpha\bar{\gamma} + \gamma\bar{\beta} \\ 0 & \beta\bar{\beta} \end{bmatrix}\right)$$

In the above example, we can observe that we start with a matrix group, the embedding really does require an increase in dimension. Furthermore, if we observe the degree the polynomial equations defining our groups, we can note that H is defined with polynomial equations of degree 2, while the embedding we are working with equations of degree 4, which means we are also facing an increase in the degree. In the general case, we make the following observation, which we show in Appendix C

Proposition 5. *Let $H \leq \mathrm{GL}_n(\mathbb{K})$ defined over $\mathbb{Q}$ as a variety, be a closed normal subgroup of an algebraic group G. If H is defined with polynomial equations of degree at most d, then the morphism $\phi : G \to \mathrm{GL}_p(\mathbb{K})$ that embeds G/H into a linear algebraic group $\mathrm{im}(G)$ has rational coefficients and is of degree at most $2n(d+1)+1$.*

We thus have a bound on both the dimension increase of the embedding of the quotient, as well as the degree of the embedding map, which both depend on the dimension n of the original matrices and the degree of polynomial equations defining H. The latter, in turn, depends on the degree of number field over which H is defined, as shown in Appendix D.

7 Adjusting the algorithm and reducing the problem to finding elements of infinite order

As discussed above, we have seen that having H be a normal subgroup of $\widetilde{G} = \overline{\langle X_1, \ldots, X_k \rangle}$ at every iteration of the algorithm would enable us to give a bound on the dimension of the quotient $\widetilde{G}/H$ and correspondingly on the growth of S. We slightly adjust the original algorithm in order to obtain that property.

The way we change the algorithm is to first go through all the elements in S and grow S and H accordingly, ensuring that some positive power of every element of S is contained in H. We then iterate on H, ensuring that it is closed under product and normal in $S \cdot H$. In particular, we also slightly modify that part of the code and ensure normality only by checking against the generators $X_1, \ldots, X_k$. We can do so since we have that $S \subseteq \langle X_1, \ldots, X_k \rangle$

Procedure AdjustedAlgorithm($X_1, \ldots, X_k$)

```
   input  : $X_1, \ldots, X_k \in \mathrm{GL}_n(\mathbb{K})$
 1 $S := \{I_n, X_1, \ldots, X_k\}$
 2 $H := \{I_n\}$
 3 repeat
 4     $S_{old} := S$
 5     for $y \in S_{old}$ do
 6         $H := \overline{H \cdot \overline{\langle y \rangle}_0}$
 7         $G := S \cdot H$
 8         for $z \in S_{old}$ do
 9             if $yz \notin G$ then  $S := S \cup \{yz\}$
10     repeat
11         $H_{old} := H$
12         $H := \overline{H \cdot H}$
13         for $i$ from 1 to $k$ do
14             $H := \overline{H \cdot X_i H X_i^{-1}}$
15     until $H_{old} = H$
16     ▷ at this point $H \triangleleft \overline{\langle X_1, \ldots, X_k \rangle}$
17 until $S_{old} = S$
   output: $G$
```

at every step of the algorithm, hence H is normal in $S \cdot H$ if and only if $X_i H X_i^{-1} = H$ for all i. Now we have that $H \triangleleft \overline{\langle X_1, \ldots, X_k \rangle}$ *at the end of each iteration (line 15)*, which is what we were aiming for.

Let

$$H_0 = \{I_n\} \subseteq H_1 \subseteq \cdots \subseteq H_l$$

be the sequence of values of H at line 15, then $H_i \triangleleft \widetilde{G} := \overline{\langle X_1, \ldots, X_k \rangle}$ for all i. In particular, the quotient $\widetilde{G}/H_i$ will be isomorphic to a linear algebraic group (not necessarily finite except for the final value of H).

We can now reduce our problem in the following way. For H_i to increase to H_{i+1}, it is sufficient (but not necessary) to find an element y in $\langle X_1, \ldots, X_k \rangle$ such that $\langle y \rangle \cap H_i = \varnothing$, in other words, y has infinite order *with respect to* H_i. As we have seen when proving the termination criterion of the original algorithm, if every $y \in \langle X_1, \ldots, X_k \rangle$ has some finite power that lies in H_i then $\widetilde{G}/H_i$ is finite by Schur's theorem (Theorem 1). As discussed in the previous section, since $H_i \triangleleft \widetilde{G}$, there is a homomorphism $\phi : \mathrm{GL}_n(\mathbb{K}) \to \mathrm{GL}_d(\mathbb{K})$ for some $d \in \mathbb{N}$ such that $H_i = \ker \phi$ and $\widetilde{G}/H_i \cong \phi(G)$. Let $y \in \langle X_1, \ldots, X_k \rangle$, then

$$\exists k \in \mathbb{N}.\, y^k \in H_i \;\Leftrightarrow\; \exists k \in \mathbb{N}.\, \phi(y^k) = I_d \;\Leftrightarrow\; \exists k \in \mathbb{N}.\, \phi(y)^k = I_d.$$

What this means is that finding $y \in \langle X_1, \ldots, X_k \rangle$ of *infinite order with respect to* H_i is the same as finding $z \in \phi_i(\langle X_1, \ldots, X_k \rangle)$ such that z has infinite order (in $\mathrm{GL}_d(\mathbb{K})$). In terms of complexity, this gives us that as long as we can find an element of infinite order in $\phi_i(\widetilde{G})$, the algorithm will have another iteration and H will increase again. Hence we have reduced our problem to the problem of finding an element of infinite order in a linear algebraic group, which we discuss how to do in the following section.

8 Finding elements of infinite order in matrix groups

The problem of finding elements of infinite order in matrix groups is closely related to the problem of deciding finiteness of groups. In particular, finding an element of infinite order in a group demonstrates that the group in question is infinite. A standard reference for deciding finiteness is [BBR93], where several randomised and deterministic polynomial time algorithms that demonstrate finiteness and infiniteness of matrix groups are presented. The algorithm that is of interest to us is the algorithm that demonstrates infiniteness of a group by finding an element of infinite order. While it is an efficient way of finding elements of infinite order, it is, unfortunately, not universal.

The algorithm uses the fact that matrices of finite order satisfy a bound on their norm and works by first constructing a set X of elements of the group G that satisfy that norm bound. If G is finite, then $G = X$, while generating an element of $G \setminus X$, *i.e.*, one that exceeds the bound on the norm, thus presents a certificate that G is infinite. However, the algorithm also crucially relies on the following two facts. Firstly, matrix groups over algebraic number fields can be represented by matrix groups over $\mathbb{Q}$. This is a standard way of representing algebraic number fields, called the *regular representation* ([Coh93, Section 4.2.3]) that requires an increase in the dimension of the matrices that corresponds to the degree of the number field. This reduces the problem to the problem of deciding finiteness of rational matrix groups. Secondly, a finite rational matrix group is conjugate to an integral matrix group, which is a classical result in the theory of groups of finite order (a proof of which can be found in the appendix of [BHK$^+$19]). It is shown that given a group $G \leq \mathrm{GL}_n(\mathbb{Q})$, one can decide in polynomial time whether or not G is equivalent to a group of integral matrices (*i.e.* conjugate to an integral matrix group), and if so, construct an appropriate transforming matrix. What the algorithm does is first try find the equivalent integral group and only then find an element of infinite order in the conjugate group. In particular, the bound on the norm of elements of finite order is only proven for integral matrices. This means that we could only use it if we knew that the groups we have were conjugate to integral matrix groups. The groups that admit such a conjugate pair are groups the elements of which have integral traces and that are either finitely generated or have a semisimple enveloping algebra. This is a condition that arbitrary matrix groups, the Zariski closure of which we will be computing, do not meet, hence, a different approach must be taken.

In the second approach we consider, we again choose to use the regular representation for matrix groups over algebraic number fields using rational matrices of a higher dimension, and describe the algorithm for subgroups of $GL_n(\mathbb{Q})$ only. In this approach, we use a standard construction in commutative algebra and algebraic geometry, called *localization*. Simply put, localization is a formal way to introduce a new ring/module out of an existing one by considering fractions of the elements of the ring with denominators of a given subset of the ring. More concretely, given a ring R and a multiplicatively closed subset S of R, the localization of R at S, denoted $S^{-1}R$,is the set of fractions $\frac{r}{s}$, where $r \in R$ and $s \in S$.

In our particular case, we choose the ring to be the ring of integers $\mathbb{Z}$. Recall that given a prime $p \in \mathbb{Z}$, the ideal generated by p, denoted (p), is a prime ideal. Furthermore, given a ring R and a prime ideal P, recall that the complement of P in R, denoted $S = R - P$, is multiplicatively closed. We can thus use the *localization of* $\mathbb{Z}$ *at the complement of the prime ideal* (p), which is the following

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}.$$

Now consider the ideal $p\mathbb{Z}_{(p)} = \{\frac{ap}{b} : a, b \in \mathbb{Z}, p \nmid b\}$ of $\mathbb{Z}_{(p)}$. Note that it is a proper ideal (*i.e.* it does not equal the whole ring $\mathbb{Z}_{(p)}$), since $1 \notin p\mathbb{Z}_{(p)}$ (if that were the case we would have $ap = b$, but since $p \nmid b$ by assumption, that would be a contradiction). In fact, $\mathbb{Z}_{(p)}$ is a local ring with maximal ideal $p\mathbb{Z}_{(p)}$. We can hence take the quotient by the ideal, which turns out to be $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$.

We now use the fact that we can identify rational matrix groups with groups over $\mathbb{Z}_{(p)}$. In particular, given a finitely generated rational matrix group $G \leq \mathrm{GL}_n(\mathbb{Q})$, there exists a prime $p \in \mathbb{Z}$ such that $G \subseteq \mathrm{GL}(\mathbb{Z}_{(p)})$. In fact, all but finitely many primes will work, as it suffices to take a prime that does not appear in the denominator of any of the coefficients of the generating set of G. Since $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$, we consider the reduction map $\mathrm{GL}_n(\mathbb{Z}_{(p)}) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. The following holds:

Lemma 6 (Minkowski)**.** *For any prime $p \geqslant 3$, the kernel of the reduction map $\mathrm{GL}_n(\mathbb{Z}_{(p)}) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ is torsion-free.*

Using the above lemma, we can now give the algorithm for finding an element of infinite order, which goes as follows. Given a finitely generated infinite rational group $G \leq \mathrm{GL}_n(\mathbb{Q})$, choose the smallest prime p that does not appear in the denominator of any of the coefficients of the generating set of G. Let $\phi : G \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ be the restriction of the reduction map $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Now observe that if we find $x, y \in G$ distinct such that $\phi(x) = \phi(y)$, then $x^{-1}y \in G$ and $\phi(x^{-1}y) = 1$, hence $x^{-1}y \in G \cap \ker \phi$ has infinite order. Since $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ is finite and G is finitely generated, we can enumerate the elements of $\phi(G)$ until we find a duplicate: this happens in time at most p^{n^2}.

Note that to use the algorithm in our complexity reasoning, we will again need to keep track of both the degree of the number field our matrices will live in to determine the dimension of the matrices in the regular representation, as well as their coefficients (in particular their height) to choose the smallest p possible. While the algorithm that we described is not particularly efficient, it does work for all rational matrix groups regardless or not they admit a conjugate integral matrix group pair. Moreover, to the best of our knowledge, the reduction of matrix groups over infinite fields to matrix groups over finite fields (or in our case rather from the infinite ring $\mathbb{Z}_{(p)}$ to the finite quotient $\mathbb{Z}/p\mathbb{Z}$) is the only known way to find an element of infinite order. In fact, the same approach is used in the current state of the art computational group theory algorithms (see [DFO13, DF18]).

9 Putting everything together

Let us now recollect all of the components of the complexity bound we have gathered thus far. Adjusting the algorithm, we propose a new version, in which all properties that H and S have in the original algorithm, still hold. Moreover, we gain the additional property of H always being normal in $\widetilde{G} = \overline{\langle X_1, \ldots, X_k, n\rangle}$, which means that the quotient $\widetilde{G}/H$ is well-defined. In particular, given the sequence of the values of $H_0 = \{I_n\} \subseteq H_1, \subseteq \ldots \subseteq H_l$ throughout the algorithm, at each iteration, we can construct a morphism $\phi_i : \widetilde{G} \to \mathrm{GL}_m(\mathbb{K})$ such that the image of ϕ_i on G is precisely the quotient, *i.e.*, $\phi_i(\widetilde{G}) = \widetilde{G}/H_i$. Furthermore, we have a bound on the dimension increase, m, as well as on the degree of the coefficients of ϕ_i. They both depend on the dimension of the matrices in the original group, n, and the maximum degree of polynomial equations defining H, which in turn relies on the degree number field of H.

We observe that the execution time of the new algorithm will depend fundamentally on when the sequence H_i stops increasing. Note that similarly to the reasoning behind the original algorithm, we can be sure that will be the case, since irreducible varieties satisfy the descending chain condition. This, in turn, means that we can pinpoint the complexity of the algorithm by reasoning on H. In particular, given an irreducible variety H_i at iteration i, the execution of the algorithm will continue precisely when we can find an element $y \in S$ that is of infinite order with respect to H_i. Furthermore, finding such an element is equal to finding $y \in S$ that is of infinite order in $\widetilde{G}/H_i \leq \mathrm{GL}_m(\mathbb{K})$. We know how to do so in time at most $p^{m'^2}$, where p is the smallest prime such that it does not divide any of the denominators of the coefficients of $\widetilde{G}/H_i$ and $m' = m + d$, where d is the degree of the number field of $\widetilde{G}/H$. Note that the latter comes from the regular representation, which we use when dealing with matrix groups over number fields, while in the case of matrix groups over $\mathbb{Q}$, we have $m' = m$.

Recalling all these facts, we see that what we need to compute the bound is both the maximum height and degree of elements in each respective $\widetilde{G}/H_i$. Using the bound we have on the degree of ϕ_i, we note that the degree of the quotient will depend on the degree of the number field of H_i. If we recall our initial discussion on the intuition behind the complexity, we know that it will depend precisely on the degree change we get when computing Zariski closure of a cyclic group, which is related to Masser's theorem. The main problem that remains is keeping track of the height of elements in $\widetilde{G}/H_i$, which again will rely on the height of elements in H_i and the height coefficients of ϕ. As discussed in Appendix C, that is something we do not have a firm grip on (yet) and thus remains the last missing component of the bound to be found, in order to establish one.

10 Summary and future work

Throughout the internship, we studied the algorithm to compute the Zariski closure of a finitely generated group of matrices and got an insight into its areas of application. Our main goal was to analyse its complexity; in the process of which we gained insight into several branches of mathematics, notably group theory, algebraic geometry, algebraic number theory, algebraic group theory and representation theory, as well as their computational aspects. In particular, we studied and slightly adjusted the proof that given an algebraic group G and a closed normal subgroup H the quotient is also an algebraic group. We focused particularly on the embedding of the quotient into a linear algebraic group in the case where G and H are matrix groups, looking at the degree and the coefficients of the embedding. We showed how to use the proven property in the complexity analysis of the group closure algorithm by working with a slightly adjusted algorithm, which reduced the problem of determining the complexity to finding an element of infinite order in a matrix group. We thus considered several approaches to solving the reduced problem, settling on an algorithm based on a reduction of a group over an infinite field to one over a finite field. Finally, we established all the components of the complexity bound we have found and discussed how to put them together to get the full bound.

There is a lot of future work to be done on the subject. The work done as part of the internship only covered studying the complexity of the algorithm to compute the Zariski closure of a finitely generated group of matrices, while the semigroup closure algorithm has not been considered yet. Once a bound on the complexity of the algorithm that computes the Zariski closure of a finitely generated group of matrices is established, it should be generalised to the semigroup closure algorithm. In particular, similarly to the course of action in this internship, the algorithm, which is based on constructing a graph representation of the finitely generated semigroup matrices, needs to be studied and well-understood in order to get the intuition on its complexity first. Then, using the results of the analysis of the group closure algorithm, a complexity bound can be determined. Furthermore, note that throughout the internship, we only focused on finding an upper bound on the degree of polynomial equations defining the Zariski closure of a finitely generated group. To the best of our knowledge, no lower bound on the degree is known either, thus finding one remains another research problem to be addressed in the future.

References

[BBR93] László Babai, Robert Beals, and Daniel N. Rockmore. Deciding finiteness of matrix groups in deterministic polynomial time. In Manuel Bronstein, editor, *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation, ISSAC '93, Kiev, Ukraine, July 6-8, 1993*, pages 117–126. ACM, 1993. doi:10.1145/164081.164104.

[BHK$^+$19] Georgina Bumpus, Christoph Haase, Stefan Kiefer, Paul-Ioan Stoienescu, and Jonathan Tanner. On the size of finite rational matrix semigroups. *CoRR*, abs/1909.04756, 2019. URL: http://arxiv.org/abs/1909.04756, arXiv:1909.04756.

[Bor91] Armand Borel. *Linear algebraic groups.* Graduate texts in mathematics 126. Springer, 2nd edition, 1991.

[Cam] Peter J. Cameron. Matrix groups. URL: http://www.maths.qmul.ac.uk/~pjc/preprints/mgo.pdf.

[Coh93] Henri Cohen. *A course in computational algebraic number theory.* Graduate Texts in Mathematics. Springer, 3rd, corr. print edition, 1993.

[Con] Keith Conrad. Galois descent. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisdescent.pdf.

[DF18] Alla Detinko and Dane Flannery. Linear groups and computation. *Expositiones Mathematicae*, 06 2018. doi:10.1016/j.exmath.2018.07.002.

[DFO13] Alla Detinko, Dane Flannery, and E.A. O?Brien. Recognizing finite matrix groups over infinite fields. *Journal of Symbolic Computation*, 50:100?109, 03 2013. doi:10.1016/j.jsc.2012.04.002.

[Dix71] John D. Dixon. *The structure of linear groups.* Van Nostrand Reinhold mathematical studies, 37. Van Nostrand-Reinhold, 1st edition, 1971.

[DJK05] Harm Derksen, Emmanuel Jeandel, and Pascal Koiran. Quantum automata and algebraic groups. *Journal of Symbolic Computation*, 39:357–371, 03 2005. doi:10.1016/j.jsc.2004.11.008.

[Dup] Nicolas Dupré. Subgroups of linear algebraic groups. URL: https://www.dpmms.cam.ac.uk/~nd332/alg_gps.pdf.

[GL05] Robert M. Guralnick and Martin Dipl Ing Lorenz. Orders of finite groups of matrices. 2005.

[HHHK05] Vesa Halava, Tero Harju, Mika Hirvensalo, and Juhani Karhum´aki. Skolem's problem – on the border between decidability and undecidability, 2005.

[HOPW18] Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. Polynomial invariants for affine programs. 02 2018.

[Hum98] James E. Humphreys. *Linear algebraic groups.* Graduate texts in mathematics 021. Springer, 4 edition, 1998.

[Mil17] James S. Milne. Algebraic geometry (v6.02), 2017. Available at www.jmilne.org/math/.

[MS] Markus Müller-Olm and title = Computing polynomial program invariants journal = Inf. Process. Lett. volume = 91 number = 5 pages = 233–244 year = 2004 Seidl, Helmut.

[MS04] Markus Müller-Olm and Helmut Seidl. A note on karr's algorithm. In *Automata, Languages and Programming: 31st International Colloquium, ICALP 2004, Turku, Finland, July 12-16, 2004. Proceedings*, volume 3142 of *Lecture Notes in Computer Science*, pages 1016–1028. Springer, 2004.

[OW13] Joël Ouaknine and James Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. *CoRR*, abs/1309.1914, 2013. URL: http://arxiv.org/abs/1309.1914, arXiv:1309.1914.

[Sup76] D. A. Suprunenko. *Matrix Groups*, volume 45 of *Translations of mathematical monographs.* American Mathematical Society, 1976.

[Tao] Terrence Tao. The jordan-schur theorem. URL: https://terrytao.wordpress.com/2011/10/05/the-jordan-schur-theorem/.

A Proof of the equality of ideals in the computation of the Zariski closure of a cyclic matrix group

In this appendix, we show that the ideals I and J we define in Section 4.2 are indeed equal. Let us first recall the setting we have. Given $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$, let I be the ideal in $\mathbb{C}[x, z_1, \ldots, z_n]$, generated by the set of polynomials f such that $f(k, \lambda_1^k, \ldots, \lambda_n^k) = 0$ for all $k \in \mathbb{N}$. Let J be the ideal in $\mathbb{C}[x, z_1, \ldots, z_n]$ generated by the set of polynomials

$$z_1^{a_1} \cdots z_n^{a_n} - z_1^{b_1} \cdots z_n^{b_n}$$

where $a_q, b_1, \ldots, a_n, b_n \in \mathbb{Z}$ are such that $\lambda_1^{a_1} \cdots \lambda_n^{b_n} = \lambda_1^{b_1} \cdots \lambda_n^{b_n}$. We claim the following

Lemma 7. *We have $I = J$.*

Proof. Clearly $J \subseteq I$. If $I \neq J$, one can choose a non-zero polynomial $f \in I \setminus J$ such that

$$f = \sum_{i=1}^{r} g_i m_i$$

with m_i a monomial in $\mathbb{C}[z_1, \ldots, z_n]$ and $b_i \in \mathbb{C}[x]$. Choose f such that r is minimal. Writing $\mu_i := m_i(\lambda_1, \ldots, \lambda_n$ for $i = 1, \ldots, r$, we claim that $\mu_1, \ldots, \mu_r$ are pairwise distinct. Indeed, suppose that $\mu_i = \mu_j$ for some $i \neq j$. Then $m_i - m_j \in J$ and thus $f - b_i(m_i - m_j) \in I \setminus J$ would have fewer terms than f.

Now define an LRS (linear recurrence sequence) $\langle u_k : k \in \mathbb{N} \rangle$ by

$$u_k := f(k, \lambda_1^k, \ldots, \lambda_n^k) = \sum_{i=1}^{r} b_i(k) \mu_i^k.$$

Then $u_k = 0$ for all $k \in \mathbb{N}$, since $f \in I$. Recall we have noted that the μ_i are pairwise distinct, hence by the uniqueness of the representation of an LRS by an exponential polynomial (see [HHHK05, Proposition 2.11]), we have that f is identically 0, which is a contradiction and our claim follows. □

Remark 8. Note that this is a variant of [DJK05, Lemma 6], where the ideal J is generated by Laurent polynomials, *i.e.*, polynomials that allow terms of negative degree. In the above solution, however, we only allow polynomials consisting of terms of positive degree.

B Proof of the bound of the dimension of the quotient of an algebraic group with a closed normal subgroup

The aim of this appendix is to prove Theorem 3, which gives a bound on the dimension of the quotient of a linear algebraic group G with a closed normal subgroup $H \triangleleft G$. In what follows, several notions of algebraic geometry, algebraic group theory, representation theory and descent theory are needed for understanding the proof. We do not require the reader to have any pre-existing knowledge of those fields and try to introduce all necessary notions as well as provide references for them as we go along.

Let K be an algebraically closed field, and let K^n denote the affine space of dimension n over K. Given a subset $X \subseteq K^n$, let $I(X) \subseteq K[x_1, \ldots, x_n]$ denote the vanishing ideal of X (*i.e.* the ideal of polynomials that vanish on all points of X). An *affine algebraic variety* is the set of common zeroes of a set of polynomials. All varieties in this section will be affine unless specified. Let $X \subseteq K^n$ be a variety, the *coordinate ring* $K[X]$ is the ring of polynomial functions on X, defined by $K[X] := K[x_1, \ldots, x_n]/I(X)$. Given $f \in K[x_1, \ldots, x_n]$, we denote by $[f] = f + I(X)$ the *equivalence class* of f in $K[X]$. If $X \subseteq K^n$ and $Y \subseteq K^m$ are varieties, a polynomial map from X to Y is the restriction to X of a polynomial map from K^n to K^m. Such a polynomial map $f : X \to Y$ induces an *algebra homomorphism (or comorphism)* $f^* : K[Y] \to K[X]$ defined by $f^*(\phi) = \phi \circ f$. Clearly, a comorphism F uniquely defines a homomorphism f such that $f^* = F$.

Let K be an algebraically closed field and X be an affine variety over K with coordinate ring $K[X] = K[x_1, \ldots, x_n]/I$. If k is a subfield of K, we say that X is *defined over k* if the ideal I is generated by polynomials in $k[x_1, \ldots, x_n]$, that is I is generated by $I_k := I \cap k[x_1, \ldots, x_n]$. In this case, the k-subalgebra $k[X] := k[x_1, \ldots, x_n]/I_k$ of $K[X]$ is called a *k-structure* on X. If X and X' are algebraic varieties defined over k, a morphism $\varphi : X \to X'$ is *defined over k* (or is a k-morphism) if the coordinate functions of φ have coefficients in k. An equivalent, and more abstract, point of view is to say that when $I(X)$ is defined over k then $K[X] = k[X] \otimes_k K$ and then φ is defined over k if its corresponding comorphism is $\varphi_k \times \mathrm{id}_K$. The set $X(k) := X \cap k^n$ is called the *k-rational* points of X.

An *affine algebraic group* (also simply called *algebraic group*) G is an affine variety that is also a group, *i.e.* it has an identity element $e \in G$, and is equipped with multiplication $\mu : G \times G \to G$ and inversion map $\iota : G \to G$ that are both morphisms of algebraic varieties (*i.e.* regular maps). We say that a linear algebraic group G is *defined over k* (or is a k-group) if it is defined over k as a variety and the homomorphism μ (multiplication) and ι (inverse) are defined over k. Note that if $\varphi : G \to G$ is a k-homomorphism of k-group, then the image of φ is defined over k but the kernel might not be.

Lemma 9. *If X, Y are varieties, then $k[X \times Y] = k[X] \otimes k[Y]$. Furthermore, if $f \in k[X \times Y]$ has rational coefficients, then there exists k and $h_1, \ldots, h_k \in k[X]$ and $g_1, \ldots, g_k \in k[Y]$ with rational coefficients such that $f = h_1 \otimes g_1 + \cdots + h_k \otimes g_k$.*

Proof Sketch. To ease notation, write $k[X] = k[x_1, \ldots, x_n]/I(X)$, $k[Y] = k[y_1, \ldots, y_m]/I(Y)$ and

$$k[X \times Y] = k[x_1, \ldots, x_n, y_1, \ldots, y_m]/I(X \times Y).$$

By a slight abuse of notation, $k[x_1, \ldots, x_n] \subseteq k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ with the obvious embedding. Let $\phi : k[X] \otimes k[Y] \to k[X \times Y]$ defined by $\phi([f] \otimes [g]) = [fg]$. This is indeed well-defined since if $[f] = [f'] \in k[X]$ and $[g] = [g'] \in k[Y]$ then $[f'g' - fg] = [(f - f')g + (g - g')f'] = [f - f'][g] + [g - g'][f] = 0$. We now write $\phi(f \otimes g) = fg$, *i.e.*, we do not write the equivalence classes anymore. To see that ϕ is injective, assume that $\sum_{i=1}^{\ell} f_i \otimes g_i \in \ker \phi$ with $\ell > 0$ minimal. Then $f_\ell \neq 0$ so we can choose $x \in X$ such that $f_\ell(x) \neq 0$. Then for every $y \in Y$, $\sum_{i=1}^{\ell} f_i(x) g_i(y) = 0$, thus $g_\ell(y) = f_\ell(x)^{-1} \sum_{i=1}^{\ell-1} f_i(x) g_i(y)$, *i.e.* $g_\ell = f_\ell(x)^{-1} \sum_{i=1}^{\ell-1} f_i(x) \otimes g_i$. Therefore we can write $\sum_{i=1}^{\ell} f_i \otimes g_i$ with $\ell - 1$ elements only which is a contradiction. For surjectivity, note that the coordinate functions $x \mapsto x_i$ of X and $y \mapsto y_i$ of Y are mapped to the coordinate functions of $X \times Y$. Since they generate the ring $k[X \times Y]$, the map ϕ is surjective. Therefore ϕ is an isomorphism. □

A subset Y of a variety X is *locally closed* if it is the intersection of an open and a closed set. Equivalently, a locally closed set is a set that is open in its closure, *i.e.*, Y is locally closed if it is open in $\overline{Y}$. A *constructible set* in is a finite union of locally closed sets. Constructible sets form a Boolean algebra, *i.e.*, one can obtain the class of constructible subsets of a variety X by taking all Boolean combinations (including complementation) of closed subsets.

Theorem 10 (Chevalley)**.** *Let $\phi : X \to Y$ be a morphism of algebraic varieties, then $\phi(X)$ is constructible. In particular, $\phi(X)$ contains a nonempty subset U that is open in $\overline{\phi(X)}$.*

A locally closed subgroup H of G is a locally closed subvariety that is also a subgroup.

Lemma 11. *If H is a locally closed subgroup of G, then H is closed.*

Proof. H is open in $\overline{H}$ which is a closed subgroup of G, thus we can assume that H is open in G (by taking $G = \overline{H}$). But then the complement of H in G is a union of cosets of H which are open (since H is open in G) thus the complement of H is open and H must be closed. □

Lemma 12. *Let $\phi : G \to H$ be a homomorphism of algebraic groups, then $\ker \phi$ and $\phi(G)$ are closed subgroups.*

Proof. This is clear for $\ker \phi$ since ϕ is continuous. By Chevalley's theorem, $\phi(G)$ contains a subset U that is open in $\overline{\phi(G)}$, thus $\phi(G) = \cup_{g \in G} gU$ is open in $\overline{\phi(G)}$, thus locally closed in H. Following the previous lemma, $\phi(G)$, is closed. □

Let G be an algebraic group and X a variety. A *group action* of G on X is a morphism of varieties $\phi : G \times X \to X$, $(g, x) \mapsto g.x = \alpha(g, x)$ satisfying

$$e.x = x \text{ and } g(hx) = (gh)x$$

for all $x \in X$ and $g, h \in G$. If G and X are given with k-structures (*i.e.* G and X are both defined over k as varieties) and α is defined over k, we say that G acts k-morphically on X.

In what follows, we will exclusively consider the case where X is a finite dimensional vector space, which we identify with $k^{\dim X}$ to give it the structure of a variety. When the group action is clear, we denote by $f^g = \phi(f, g)$ the action of $g \in G$ on $f \in V$. A subspace $V \subseteq X$ is called *g-invariant* if $f^g \in V$ for all $f \in V$, and *G-invariant* if it is g-invariant for all $g \in G$.

An important case is when $X = k[G]$ because of the group structure: given $f \in k[G]$ and $g \in G$, define $f^g(x) = f(gx)$ for all $x \in G$, then $f^g : G \to G$ defines a morphism of algebraic groups. Recall that the multiplication map μ of G is a morphism of varieties, so $f^g(x) = f(\mu(g,x))$ is indeed a morphism of varieties. Note that each $g \in G$ induces a ring homomorphism $k[G] \to k[G], f \mapsto f^g$.

Lemma 13. *Let G be an affine algebraic group and V be a finite dimensional subspace of $k[G]$. Then $V^G := \operatorname{span}\{f^g : f \in V, g \in G\}$ is finite dimensional, contains V and is G-invariant. Moreover, there is a morphism of algebraic groups $\psi : G \to \mathrm{GL}(V^G)$ that satisfies $\psi(g)(f) = f^g$ for all $f \in V^G$. Furthermore, if $G \leqslant \mathrm{GL}_n(\mathbb{C})$ and V has a basis with polynomials of total degree at most d then V^G has dimension at most $\binom{d+n^2}{d}$. Additionally, if the basis of V and the multiplication map μ of G has rational coefficients, then V^G has a basis with rational coefficients and ψ has rational coefficients.*

Proof. Note that V^G trivially contains V and is G-invariant by definition. Let $\mu : G \times G \to G, (g,x) \mapsto gx$ denote the multiplication in G. Recall that it is morphism of varieties and thus induces a ring homomorphism $\mu^* : k[G] \to k[G \times G]$. Furthermore note that $k[G \times G]$ is isomorphic to $k[G] \otimes k[G]$ (Lemma 9. Therefore for any $f \in k[G]$, there is a finite decomposition $\mu^*(f) = \sum_i h_i \otimes f_i$ and hence for any $g \in G$, $f^g(x) = \mu^*(f)(g,x) = \sum_i h_i(g) f_i(x)$, *i.e.*, $f^g = \sum_i h_i(g) f_i \in \operatorname{span}\{f_i\}$. When $V = \operatorname{span}\{f\}$ is one-dimensional, this gives that $V^G \subseteq \operatorname{span}\{f_i\}$ and is thus finite dimensional. In the general case, we apply the above decomposition to a finite basis of V.

Let $f_1, \dots, f_r$ be a basis of V^G, then the above decomposition gives us

$$f_i^g = \sum_j m_{ij}(g) \otimes f_j$$

where $m_{ij} : G \to G$ is in fact a morphism of varieties since $f_i^g(x) = f_i(gx)$ is a polynomial in g and x. We can thus define $\psi : G \to GL(V^G)$ by $\psi(g) = (m_{ij}(g))$, which is a morphism of algebraic groups by construction since $\psi(g)(f) = f^g$.

When $G \leqslant \mathrm{GL}_n(\mathbb{C})$, observe that $k[G] = k[y_{ij}]/I$ for some ideal I. Therefore $k[G]$ is generated by the n^2 coordinate functions $F_{ij} = [y_{ij}]$. Then by the usual matrix multiplication, we have for any $d \in \mathbb{N}$ that

$$(F_{ij}(gx))^d = \left(\sum_{k=1}^{n} F_{ik}(g) F_{kj}(x)\right)^d = \sum_{k_1+\cdots+k_n=d} \binom{d}{k_1, \dots, k_n} F_{i1}(g)^{k_1} \cdots F_{in}(g)^{k_n} F_{1j}(x)^{k_1} \cdots F_{nj}(x)^{k_n}$$

thus $\left(F_{ij}^g\right)^d$ is the span of the F^β for $|\beta| = d$ where $F^\beta = \prod_{ij} F_{ij}^{\beta_{ij}}$ and $|\beta| = \sum_{ij} \beta_{ij}$. Let $f = F^\alpha$ be a monomial of total degree $|\alpha| \leqslant d$, then

$$f^g = (F^\alpha)^g = (F^g)^\alpha = \prod_{ij} \left(F_{ij}^g\right)^{\alpha_{ij}} = \prod_{ij} \sum_{|\beta|=\alpha_{ij}} h_\beta(g) F^\beta = \sum_{|\beta|=|\alpha|} h'_\beta(g) F^\beta$$

thus f^g is the span of the F^β for $|\beta| \leqslant d$. Hence, by linearity, for any polynomial $f \in k[G]$ of total degree at most d, f^g is the span of the F^β for $|\beta| \leqslant d$. It follows that if V has a basis with polynomials of total degree at most d then $V^G \subseteq \operatorname{span}\{F^\beta : |\beta| \leqslant d\}$ and thus has dimension at most $\binom{n^2+d}{d}$.

When μ and the basis of V have rational coefficients, we first need to check that V^G has a basis with rational coefficients. If $v_1, \dots, v_k$ is a rational basis of V then we decompose each v_i as $\mu^*(v_i) = \sum_\ell h_{i\ell} \otimes f_{i\ell}$ for some finitely many $h_\ell, f_{i\ell}$. But since μ and v_i have rational coefficients, $\mu^*(v_i) = v_i \circ \mu$ has rational coefficients, hence $h_{i\ell}$ and $f_{i\ell}$ have rational coefficients by Lemma 9. The $f_{i,\ell}$ span V^G as shown above, hence V^G has a rational basis. We now need to check that $\psi(g) = (m_{ij}(g))$ has rational coefficients. Let $f_1, \dots, f_r$ be a rational basis of V^G, then m_{ij} was defined such that $f_i^g = \sum_j m_{ij}(g) \otimes f_j$ and m_{ij} was obtained by writing $\mu^*(f_i) = \sum_j m_{ij} \otimes f_j$. Again, since μ and f_i have rational coefficients, $\mu^*(f_i) = f_i \circ \mu$ is a polynomial with rational coefficients. Therefore the decomposition yields polynomials m_{ij} with rational coefficients, again because the f_j have rational coefficients. □

Corollary 14. *Any affine algebraic group is linear,* i.e.*, is isomorphic to a closed subgroup of* GL_n *for some* n.

Proof. Let G be an affine algebraic group and $f_1, \dots, f_k$ be a set of generators for $k[G]$. Apply Lemma 13 to $V := \operatorname{span}\{f_1, \dots, f_k\}$ to get a morphism $\psi : G \to \mathrm{GL}(V^G)$. Let $H = \operatorname{im} \psi$, which is a closed group by Lemma 12, we claim that the map $\psi : G \to H$ is an isomorphism. To prove that ψ is injective, it suffices to prove that $\psi^* : k[H] \to k[G]$ is surjective. Let e be the identity element of G, then $f_i(x) = f_i^x(e) = \sum_j m_{ij}(x) f_j(e)$, *i.e.*, $f_i = \sum_j f_j(e) m_{ij} \in \operatorname{im} \psi^*$ since $f_j(e) \in k$ is just a coefficient. The claim follows because $k[G]$ is generated by the f_i.

□

Lemma 15. *Let $H \leqslant G$ where H and G are algebraic groups. Then there is a finite dimensional vector space V, a group action $G \times V \to V$, a subspace W of V and a morphism of algebraic group $\psi : G \to \mathrm{GL}(V)$ such that $\psi(g)(f) = f^g$ for all $f \in V$ and $H = \{g \in G : W \text{ is } g\text{-invariant}\}$. Furthermore, if $G \leqslant \mathrm{GL}_n(\mathbb{C})$ and H can be defined by polynomial equations of total degree at most d then V can be taken of dimension at most than $m := \binom{n^2+d}{d}$. We can further take W to be of dimension 1, in which case the bound on the dimension of V above becomes $\binom{m}{d}$. Additionally, if the multiplication map of G has rational coefficients and H is defined over $\mathbb{Q}$, then V is defined over $\mathbb{Q}$ and ψ has rational coefficients.*

Proof. Let G act on $k[G]$ as usual. Let $I := I_G(H)$ be the ideal of $k[G]$ of functions vanishing on H. Since $k[G]$ is Noetherian, I is finitely generated by some $f_1, \dots, f_r$. We apply Lemma 13 to $V := \operatorname{span}\{f_1, \dots, f_r\}$ to get a morphism $\psi : G \to \mathrm{GL}(V^G)$. By construction, $\psi(g)(f) = f^g$ for all $f \in V^G$, thus we can naturally extend it to a ring homomorphism $\psi(g) : k[G] \to k[G], f \mapsto f^g$.

Let $W = I \cap V^G$, note that it is H-invariant as $f^h(x) = f(hx) = 0$ for all $h, x \in H$ since $f \in I$. Conversely, let $g \in G$ and assume that W is g-invariant. Since I is generated by W and $\psi(g)$ is a ring homomorphism, we have

$$\psi(g)(I) = \psi(g)(Wk[G]) = \psi(g)(W)\psi(g)(k[G]) = Wk[G] = I.$$

It follows that all functions in I vanish at g, since $f(g) = f^g(e) = 0$ (since $e \in H$), thus $g \in H$. Therefore we have that $H = \{g \in G : W \text{ is } g - \text{invariant}\}$.

When $G \leqslant \mathrm{GL}_n(\mathbb{C})$ and H can be defined by polynomials equations of degree at most d, it follows that the f_i above are of degree at most d and thus by Lemma 13, the dimension of V^G is bounded by $\binom{n^2+d}{d}$.

Let $m = \dim V$ and define $V' = \bigwedge^m V$ and $W' = \bigwedge^m W$, then W' is a subspace of V' and $\dim W' = 1$. Then G acts on V' by $(f_1 \wedge \cdots \wedge f_m)^g = f_1^g \wedge \cdots \wedge f_m^g$ which is still an element of V' since V is G-invariant. There is a natural morphism of algebraic groups $\phi : \mathrm{GL}(V) \to \mathrm{GL}(V')$ defined by $\phi(M)(f_1 \wedge \cdots \wedge f_m) = (Mf_1) \wedge \cdots \wedge (Mf_m)$, it is clear that it is a morphism of groups and it is a morphism of algebraic varieties.

Then $\psi' = \phi \circ \psi : G \to \mathrm{GL}(V')$ is a morphism of algebraic groups and

$$\psi'(g)(f_1 \wedge \cdots \wedge f_m) = (\psi(g)f_1) \wedge \cdots \wedge (\psi(g)f_m) = f_1^g \wedge \cdots \wedge f_m^g = (f_1 \wedge \cdots \wedge f_m)^g.$$

Let $g \in G$, we claim that W is g-invariant if and only if W' is g-invariant (we postpone the proof to the next paragraph), which shows that $H = \{g \in G : W' \text{ is } g\text{-invariant}\}$. Finally, it is well-known that $\dim V' = \binom{\dim V}{d} = \binom{m}{d}$.

$(f_1 \wedge \cdots \wedge f_m)^g = f_1^g \wedge \cdots \wedge f_m^g \in W'$ if $f_1 \wedge \cdots \wedge f_m \in W'$, *i.e.* W' is g-invariant. Conversely, if W' is g-invariant, let $f_1, \dots, f_m$ be a basis of W, then (since W' has dimension 1), $(f_1 \wedge \cdots \wedge f_m)^g \in W'$ is a multiple of $f_1 \wedge \cdots \wedge f_m$. Therefore $f_i^g \in W$ for all i and thus $f^g \in W$ for all $f \in W$, *i.e.* W is g-invariant, since the f_i form a basis.

If H is defined over $\mathbb{Q}$, then the ideal I has rational coefficients and the space $V := \operatorname{span}\{f_1, \dots, f_r\}$ has a rational basis. Following Lemma 13 again, $\psi : G \to \mathrm{GL}_p(V)$ has rational coefficients and the subspace V, the linear group over which we embed G into, is also defined over $\mathbb{Q}$. □

A *character* of an algebraic group G is a rational representation of degree 1, *i.e.*, a morphism of algebraic groups $\chi : G \to k^*$. The set of characters of G, which we denote by $X^*(G)$, form a group that is abelian and finitely generated.

Let V be a finite dimensional vector space and assume G acts on V. Given $\chi \in X^*(G)$, define

$$V_\chi^G = \{v \in V : v^g = \chi(g)v \text{ for all } g \in G\}.$$

Evidently, V_χ^G is an G-invariant subspace of V (possibly 0). Any nonzero element of V_χ^G is called a *semi-invariant* of G, of *weight* χ. Conversely, if v is any nonzero vector which spans an G-stable line in V, then $v^g = \chi(g)v$ defines a character χ of G. More generally, if $\psi : G \to \mathrm{GL}(V)$ is a *rational representation*, then the semi-invariants of G in V are by definition those of $\psi(G)$. Notice that composition with ψ induces an injective group homomorphism $X^*(\psi(G)) \to X^*(G)$, so that V_χ may be defined in the obvious way for any $\chi \in X^*(G)$ for any character coming from a character of $\psi(G)$.

Lemma 16. *The subset $X^*(G)$ is linearly independent in $k[G]$, in particular the sum $\sum_{\chi \in X^*(G)} V_\chi^G$ is direct.*

Proof. Assume there is a nontrivial relation $\sum_{i=1}^n a_i \chi_i = 0$ with $a_i \neq 0$ and $\chi_i \in X^*(G)$ all distincts, and choose one such that n is minimum. Then for every $g, h \in G$, we have

$$\sum_{i=1}^n a_i(\chi_i(g) - \chi_1(g))\chi_i(h) = \sum_{i=1}^n a_i\chi_i(g)\chi_i(h) - \chi_1(g)\sum_{i=1}^n a_i\chi_i(h) = \sum_{i=1}^n a_i\chi_i(gh) = 0.$$

But since $\chi_1 \neq \chi_2$, there exists $g \in G$ such that $\chi_1(g) - \chi_2(g) \neq 0$, but then

$$0 = \sum_{i=1}^{n} a_i(\chi_i(g) - \chi_1(g))\chi_i = \sum_{i=2}^{n} a_i(\chi_i(g) - \chi_1(g))\chi_i$$

is a nontrivial relation that is strictly smaller, a contradiction. Assume there is a relation $\sum_{i=1}^{n} v_{\chi_i} = 0$ where $v_{\chi_i} \in V_{\chi_i}^G \setminus \{0\}$ and all the $\chi_i \in X^*(G)$ are distincts. Choose such a relation such that n is minimal. Then for all $g \in G$ we have

$$\sum_{i=1}^{n}(\chi_i(g) - \chi_1(g))v_{\chi_i} = \sum_{i=1}^{n} \chi_i(g)v_{\chi_i} - \chi_1(g)\sum_{i=1}^{n} v_{\chi_i} = \sum_{i=1}^{n} v_{\chi_i}^g = \left(\sum_{i=1}^{n} v_{\chi_i}\right)^g = 0.$$

But since $\chi_1 \neq \chi_2$, there exists $g \in G$ such that $\chi_1(g) - \chi_2(g) \neq 0$, but then

$$0 = \sum_{i=1}^{n}(\chi_i(g) - \chi_1(g))v_{\chi_i} = \sum_{i=2}^{n}(\chi_i(g) - \chi_1(g))v_{\chi_i}$$

is a nontrivial relation that is strictly smaller, a contradiction. □

Given an extension field E/F, an automorphism α of E/F is (by definition) an automorphism of E that fixes F pointwise, *i.e.*, $\alpha : E \to E$ satisfies $\alpha(x) = x$ for all $x \in F$. The set of automorphisms of E/F forms a group for composition and is denoted by $\mathrm{Aut}(E/F)$. Given a point $x \in E^n$, an automorphism $\sigma \in \mathrm{Aut}(E/F)$ naturally acts on the coefficients of x. We denote this action by x^σ and extend it to any set X by $X^\sigma = \{x^\sigma : x \in X\}$ Given a polynomial $f \in F[x_1, \dots, x_n]$, an automorphism $\sigma \in \mathrm{Aut}(E/F)$ naturally acts on the coefficients of f, which we denote by f^σ. We extend this action to any set $X \subseteq k[x_1, \dots, x_n]$ by $X^\sigma = \{f^\sigma : f \in X\}$. Note that since σ is an automorphism of E, it induces a ring homomorphism $f \mapsto f^\sigma$ on $E[x_1, \dots, x_n]$.

Let H be a closed normal subgroup of an algebraic group G. We claim the following

Proposition 17. *If H is defined over $\mathbb{Q}$, then $H^\sigma = H$ for every $\sigma \in Aut(\mathbb{C}/\mathbb{Q})$.*

Proof. Let σ be an automorphism of $\mathbb{C}$ fixing $\mathbb{Q}$. If H is an algebraic group defined over $\mathbb{Q}$, it is an algebraic variety defined over $\mathbb{Q}$, hence a set of common zeroes of a set of polynomials in $\mathbb{Q}[x_1, \dots, x_n]$. Let $h \in H$, by definition it is the root of some nonconstant polynomial $f(x_1, \dots, x_n) \in \mathbb{Q}[x_1, \dots, x_n]$. Then $f(\sigma(h)) = \sigma(f(h))$, since σ fixes $\mathbb{Q}$, so $\sigma(h)$ is also a root of $f(x_1, \dots, x_n)$, hence $\sigma(h) = h^\sigma \in H$ and $H^\sigma = H$. □

Proposition 18. *For every character $\chi \in X^*(H)$ and automorphism $\sigma \in Aut(\mathbb{C}/\mathbb{K})$, we have $(V_\chi^H)^\sigma \subseteq V_{\chi'}^{H^\sigma} = V_{\chi'}^H$, where $\chi' \in X^*(H)$.*

Proof. Let $v \in V_\chi^H$, then $v^h = \chi(h)v$ for all $h \in H$, where recall that $v^h = \psi(h)v$. Let $\sigma \in Aut(\mathbb{C}/\mathbb{Q})$ and $h \in H$, then

$$\sigma(\chi(h))\sigma(v) = \sigma(v^h) = \sigma(\psi(h)v) = \sigma(\psi(h))\sigma(v) = \psi(\sigma(h))\sigma(v)$$

since ψ has rational coefficients. Hence $\sigma(v)^{\sigma(h)} = \sigma(\chi(h))\sigma(v)$. Following Proposition 17 $H^\sigma = H$, therefore $\sigma(v)^{h'} = \sigma(\chi(\sigma^{-1}(h')))\sigma(v) = \chi'(h')\sigma(v)$ for any $h' \in H$ where $\chi'(h) = \sigma(\chi(\sigma^{-1}(h)))$ is also a character. □

What the above two propositions give us is that $V = \bigoplus_{\chi \in X^*(H)} V_\chi^H$ is stable under the group action of $Aut(\mathbb{C}/\mathbb{Q})$. Now let U be set of all endomorphisms that stabilize each of the V_χ^H:

$$U = \{f \in \mathrm{End}(V) : \forall \chi \in X^*(H), f(V_\chi^H) \subseteq V_\chi^H\}.$$

We further claim

Proposition 19. *If H is defined over $\mathbb{Q}$, then U is also defined over $\mathbb{Q}$.*

Proof. Let us define a different group action of $Aut(\mathbb{C}/\mathbb{Q})$ on U via conjugation, so that for $f \in U$ and $\sigma \in Aut(\mathbb{C}/\mathbb{Q})$, the action of σ on f is $f^\sigma = \sigma f \sigma^{-1}$. Then

$$f^\sigma V_\chi^H = (\sigma f \sigma^{-1})V_\chi^H = \sigma f V_{\sigma^{-1}\chi}^H = \sigma V_{\sigma^{-1}\chi}^H = V_\chi^H$$

since $f(V_{\sigma-1\chi}^H) \subseteq V_{\sigma-1\chi}^H$ and $\sigma^{-1}(V_\chi^H) = V_{\sigma^{-1}\chi}^H$ for some character $\sigma^{-1}\chi \in X^*(H)$ following Proposition 18.

Hence U is stable under $Aut(\mathbb{C}/\mathbb{Q})$ and thus also defined over $\mathbb{Q}$. □

Remark 20. The problem of showing that a subspace stable under $Aut(K/k)$, where k is a subfield of an algebraically closed field K, is defined over k is problem in *descent theory.* Let K/k be a field extension. A k-vector space W can be extended to a K-vector space $K \otimes_k W$, and W embeds into $K \otimes_k W$ by $w \mapsto 1 \otimes w$. Under this embedding, when $W \neq 0$, a k-basis $\{e_i\}$ of W turns into a K-basis $\{1 \otimes e_i\}$ of $K \otimes_k W$. Passing from W to $K \otimes_k W$ is called *ascent.* In the other direction, if we are given a K-vector space $V \neq 0$, we may ask how to describe the k-subspaces $W \subset V$ such that a k-basis of W is a K-basis of V. For a K-vector space V, we call a k-subspace W such that a k-basis of W is a K-basis of V a *k-form* of V. The passage from a K-vector space V to a k-form of V is called *descent.* (See [Con] and [Mil17, Chapter 16] for more insight.)

We can now finally prove the Theorem 3 using the above lemmas and propositions.

Proof of Theorem 3. Define $I := I_G(H)$ to be the ideal of $k[G]$ of functions vanishing on H. Since $k[G]$ is Noetherian, I is finitely generated by some $f_1, \dots, f_r$. Let V to be the vector space spanned by those f_i, $V := \operatorname{span}\{f_1, \dots, f_r\}$ to get the morphism $\psi : G \to \mathrm{GL}(V^G)$, defined by $\psi(g)(f) = f^g$, where $V^G := \operatorname{span}\{f^g : f \in V, g \in G\}$ is a finite dimensional vector space that contains V and is G-invariant. Furthermore, we have proven that if the basis of V and the multiplication map μ of G has rational coefficients, then V^G has a basis with rational coefficients and ψ has rational coefficients. Finally, let $W = I \cap V^G$ (I is generated by W) and take W such that $\dim W = 1$. All this comes from Lemma 15.

Let $W^G := \operatorname{span}\{w^g : w \in W, g \in G\}$. By construction it is the smallest subspace that contains W and G-invariant. Because of the latter property, we can replace V with W^G. Since W is H-invariant and has dimension 1, H acts on W by scalar multiplication and has an associated character $\chi_0 \in X(H)$ such that $w^h = \chi_0(h)w$ for all $w \in W$ and $h \in H$. Therefore, $W \subseteq V^H_{\chi_0}$. Recall here that $V^H_{\chi_0}$ is the following subset of the vector space V:

$$V^H_{\chi_0} = \{v \in V : v^h = \chi_0(h)v \text{ for all } h \in H\}.$$

Let $V' = \bigoplus_{\chi \in X^*(H)} V^H_\chi$. We further claim that we can replace V (now W^G) with V'. Since $V' \subseteq V$ is finite dimensional and the sum $V' = \bigoplus_{\chi \in X^*(H)} V^H_\chi$ is direct by Lemma 16, only finitely many V^H_χ are nonzero. Observe that for any $g \in G$, $h \in H$, $\chi \in X^*(H)$ and $v \in V^H_\chi$ (*i.e.* $v \in V$ such that $v^h = \chi(h)v$ and hence $v = \chi(h)^{-1}v^h$)

$$v^g = (\chi(h)^{-1}v^h)^g = \chi(h)^{-1}v^{hg} = \chi(h)^{-1}v^{gh'} = \chi(h)^{-1}(v^g)^{h'}$$

where $h' = g^{-1}hg \in H$, since H is normal. But if we define

$$\chi'(h') := \chi(h)^{-1} = \chi(gh'g^{-1})^{-1} = \chi(g^{-1})\chi(h')\chi(g)$$

χ' is also a character. Therefore $v^g \in V^H_{\chi'}$. In fact, since $gH = Hg$, we have $(V^H_\chi)^g = V^g_{\chi'}$ so G just permutes the V^H_χ. In particular, V' is G-invariant. Finally, since $W \subset V'$, we can assume that $V = V' = \bigoplus_{\chi \in V^*(H)} V^H_\chi$ in the rest of the proof.

Let us denote with U the subspace of endomorphisms that stabilize all V^H_χ:

$$U = \{f \in \mathrm{End}(V) : \forall \chi \in X^*(H), f(V^H_\chi) \subseteq V^H_\chi\}.$$

There is a natural isomorphism $U \cong \mathrm{End}(V^H_\chi)$. (Think of U as consisting of all block diagonal matrices with blocks of sizes $\dim V^H_\chi$). Furthermore, if $g \in G$ and if $f \in U$, then for each $\chi \in X^*(H)$

$$\psi(g)f\psi(g)^{-1}V_\chi = \psi(g)fV_{g^{-1}\chi} \subset \psi(g)V_{g^{-1}\chi} = V_\chi.$$

Thus $\psi(G)$ normalizes U and we can define

$$\phi : G \to \mathrm{GL}(U) \qquad \phi(g)(f) = \psi(g)f\psi(g)^{-1}$$

Since ϕ is just a restriction of ψ to U, it is a morphism. We claim that $H = \ker\phi$. We first prove that for every $g \in \ker\phi \implies g \in H$. Let $g \in \ker\phi$ and $f \in \mathrm{GL}(V_{\chi_0})$ and define $p : V \to V_{\chi_0}$ to be the projection on V_{χ_0} (remember that V is the direct sum of the V_χ). Then $f' = f \circ p \in \mathrm{End}(V)$ so $\psi(g)f' = f'\psi(g)$. But $f'(V^H_{\chi_0}) = f(p(V^H_{\chi_0})) = f(V^H_{\chi_0}) = V^H_{\chi_0}$ and

$$\psi(g)V_{\chi_0} = \psi(g)f'(V^H_{\chi_0}) = f'\psi(g)^{-1}V^H_{\chi_0} = f'(V^H_\chi)$$

for some χ since $\psi(g)^{-1}V^H_{\chi_0} = (V^H_{\chi_0})^{g^{-1}}$ and G permutes the V_χ. But if $\chi \neq \chi_0$ then $f'(V^H_\chi) = 0$ because f projects on V_{χ_0} and the V_χ are in direct sum, which is a contradiction since $\psi(g)$ is invertible. Therefore $\psi(g)V^H_{\chi_0} = p(V^H_{\chi_0})$

for all $p \in \mathrm{GL}(V_{\chi_0}^H)$ and $\psi(g)$ thus must be the identity over $V_{\chi_0}^H$. Since $W \subseteq V_{\chi_0}^H$, then $W^g = \psi(g)W = W$ and therefore $g \in H$.

We now prove the converse, *i.e.*, $g \in H \implies g \in \ker \phi$. If $h \in H$ then for all $\chi \in X^*(H)$ and $v \in V_\chi^H$, we have $v^h = \chi(h)v$. Since V is the direct sum of the V_χ^H, $v^h = \chi(h)v$ for all $v \in V$ and similarly for h^{-1}, we have $v^{h^{-1}} = \chi(h^{-1})v$ for all $v \in V$. Therefore

$$\phi(h)(f)v = \psi(h)f\psi(h)^{-1}v = \psi(h)f\chi(h^{-1})v = \chi(h^{-1})\psi(h)f(v)$$

But f stabilizes the V_χ^H therefore $\psi(h)f(v) = (f(v))^h = \chi(h)f(v)$ and thus $\psi(h)(f)v = f(v)$, *i.e.*, $\psi(h)$ is the identity and $h \in \ker \phi$.

Since H is normal in G, we can define a morphism of groups:

$$\pi : G \to G/H \qquad \pi(g) = gH$$

Since $H = \ker \phi$, we can also define the following morphism of groups:

$$\psi^* : G/H \to \phi(G) \qquad \psi^*(gH) = \phi(g)$$

We can show that ψ^* is well-defined: if $gH = g'H$ then $g' = gh$ for some $h \in H$, thus $\psi^*(g'H) = \phi(g') = \phi(h)\phi(g) = \phi(g)$ because $h \in \ker \phi$. Now ψ^* is an isomorphism that is both surjective ($\psi^*(gH) = \phi(g)$ for all $g \in G$) and injective ($gH \in \ker \psi^*$ implies that $g \in \ker \phi$, *i.e.*, $g \in H$).

By Lemma 12, $\phi(G)$ is a closed algebraic group, thus G/H is isomorphic to a closed subgroup of $\mathrm{GL}(U)$. Furthermore, if $G \leqslant \mathrm{GL}_n(\mathbb{C})$ and H can be defined by polynomial equations of total degree at most d, then $\dim V \leqslant \binom{m}{d}$ where $m = \binom{n^2+d}{d}$ by Lemma 15. Recall that $\dim(End(V)) = (\dim V)^2$ and $U \subseteq End(V)$, therefore $\dim U \leqslant (\dim V)^2$ which gives the result.

If H is defined over $\mathbb{Q}$, then following Lemma 15 ψ has rational coefficients. Following Proposition 19 U is then also defined over $\mathbb{Q}$. Given $f \in U$ and ψ, $phi(g)(f) = \psi(g)f\psi(g)^{-1}$, has rational coefficients and given a field $\mathbb{K}$, maps a subgroup of $\mathrm{GL}_n(\mathbb{K})$ to a subgroup of $\mathrm{GL}_p(\mathbb{K})$. □

Remark 21. Note that by replacing V with W^G, we obtain an *irreducible representation* of G, as W^G is the smallest G-invariant vector space (in other words, it does not have a nontrivial G-invariant subspace). What this gives us is the fact that W^G is a direct sum of some minimal H-invariant vector subspaces W_i that are isomorphic to each other (see [Dix71, Chapters 3 and 4], [Cam, Theorem 2.4]), which we prove independently using Lemma 16.

C Degree of the embedding of the quotient into a linear algebraic group

The aim of this appendix is to prove how Proposition 5, which gives a bound on the degree of the embedding of the quotient of two algebraic groups into a linear algebraic group.

Proof of Proposition 5. Construct the embedding as in Theorem 3. Recall $\phi : G \to GL(U)$ is defined by $\phi(g)(f) = \psi(g)f\psi(g)^{-1})$. Let us thus recall the definition of $\psi : G \to \mathrm{GL}(V^G)$. Is constructed to be such that $\psi(g)(f) = f^g$, where $f \in V$ and the action of $g \in G$ on f is such that $f^g(x) = f(\mu(gx))$, where μ is the multiplication map of G. Observe that the definition of ψ, relies on the decomposition of elements of V^G. Given a basis $f_1, \ldots, f_r$ of V^G, write

$$f_i^g = \sum_j m_{ij}(g) \otimes f_j$$

where $m_{ij} : G \to G$ is a morphism of varieties, since $f_i^g(x) = f_i(gx)$ is a polynomial in g and x. We then define ψ via m_{ij} in the following way: $\psi(g) = m_{ij}(g)$.

Recall now the reasoning behind the proof of Lemma 13. When $G \leq \mathrm{GL}_n(\mathbb{C})$, the coordinate ring of G is $k[G] = k[y_{ij}]/I$ for some ideal I. Therefore $k[G]$ is generated by the n^2 coordinate functions $F_{ij} = [y_{ij}]$ (in the example, it was observed that $k[G]$ was generated by $f_u, f_w, f_\alpha, f_\beta$). We have shown that $(F_{ij})^\alpha$ is the span of monomials F^β where $|\beta| = \alpha$ and that for any polynomial $f \in k[G]$ of total degree at most d, f^g is the span of the F^β for $|\beta| \leqslant d$. Now let us rewrite the reasoning behind those two claims slightly differently. By the usual matrix multiplication again, we have for any $\alpha_{ij} \in \mathbb{N}$ that

$$\left(F_{ij}^g\right)^{\alpha_{ij}} = \sum_{k_1+\cdots+k_n=\alpha_{ij}} \binom{\alpha_{ij}}{k_1, \ldots, k_n} F_{i1}(g)^{k_1} \cdots F_{in}(g)^{k_n} F^{\beta_{k_{ij}}} = \sum_{k_{ij}} h_{\beta_{k_{ij}}}(g) F^{\beta_{k_{ij}}}$$

where $h_{\beta_{k_{ij}}}(g) = c_{k_{ij}} F_{i1}(g)^{k_1} \cdots F_{in}(g)^{k_n}$ is a monomial of degree $k_1 + \ldots k_n = \alpha_{ij}$ with $c_{k_{ij}} \in \mathbb{Q}$ a constant and $F^{\beta_{k_{ij}}}$ a monomial of degree α_{ij}. Let us now again look at $f = F^\alpha \in k[G]$ (a monomial of total degree $|\alpha|$), then the calculation from above can be expanded to

$$f^g = (F^\alpha)^g = (F^g)^\alpha = \prod_{ij} \left(F_{ij}^g\right)^{\alpha_{ij}} = \prod_{ij} \left(\sum_{k_{ij}} h_{\beta_{k_{ij}}}(g) F^{\beta_{k_{ij}}} \right)_{|\beta_{k_{ij}}| = \alpha_{ij}} = \prod_{ij} \sum_{|\beta| = \alpha_{ij}} h_\beta(g) F^\beta = \sum_{|\beta| = |\alpha|} h'_\beta(g) F^\beta$$

where h_β has degree α_{ij}. Moreover, h'_β, which is exactly m_{ij} in the decomposition of $f_i^g = \sum_j m_{ij} \otimes f_j$, will be of degree $\sum_{ij} \alpha_{ij} = |\alpha|$. Hence the degree of ψ, defined by $\psi(g) = H'_\beta(g)$, will be at most d, if V can be defined by polynomial equations of degree at most d. More specifically, if we recall the way we construct V in the final proof of the theorem, d will actually be the degree of the polynomial equations we use to define H (or in other words, the ideal I_H vanishing on H).

Let us now draw our attention to ϕ. Recall first the reasoning why ψ^{-1} is a polynomial map. Note that ψ is a morphism of varieties, hence by definition polynomial (in particular a polynomial map in $n^2 + 1$ variables where we must not forget about $\det^{-1}$, which we omitted in the above discussion). Moreover, it is a morphism of algebraic groups and thus ψ^{-1} is also one. Using the observations made above, we take the bound on the degree of ψ to be $d + 1$, where the additional 1 comes from the $\det^{-1}$. To get the degree of ψ^{-1}, use Cramer's rule for computing the inverse of a matrix $A^{-1} = \frac{1}{\det(A)} adj(A)$, where $adj(A)$ is the adjugate matrix, *i.e.*, the transpose of the cofactor matrix of A. In particular its elements are determinants of the minors of A. Following the Leibniz formula for computing a determinant of a matrix $\det(A) = \sum_{\sigma \in S_n} \left(sgn(\sigma) \prod_{i=1}^n a_{i,\sigma_i}\right)$, we can see that for a matrix of dimension $n \times n$, we have to compute products of n entries of the matrix. Recall that ψ is a matrix whose entries are monomials of degree at most $d+1$, hence the degree of the determinant will be at most $n(d+1)$. The elements of the adjugate matrix will be determinants of matrices of dimension $(n-1) \times (n-1)$ and hence their degree at most $(n-1)(d+1)$. The total degree of ψ^{-1} will thus be at most $n(d+1) + (n-1)(d+1) = (2n-1)(d+1)$. Finally, given an element $f \in U$, observe that is an endomorphism of V and hence can be viewed as a matrix. This gives two additional matrix multiplications in $\phi(g)(f) = \psi(g) f \psi(f)^{-1}$ adding degree 2. Hence the degree of ϕ is at most $2n(d+1) + 2$. □

Remark 22. Note that while we can give a bound on the degree of the coefficients of ϕ, we do not have a grip on their height as they depend directly on G. In particular, observing the decomposition functions from the above proof, the h'_β, we can see that they will be of the form

$$h'_\beta(g) = \prod_{ij} h_{\beta_{k_ij}} = \prod_{ij} (c_{k_{ij}} F_{i1}(g)^{k_1} \ldots F_{in}(g)^{k_n})$$

$$= \left(c_{k_{11}} F_{11}(g)^{k_{1_{11}}} \ldots F_{1n}(g)^{k_{n_{11}}}\right) \ldots \left(c_{k_{nn}} F_{n1}(g)^{k_{1_{nn}}} \ldots F_{nn}(g)^{k_{n_{nn}}}\right)$$

$$= c_{k_{11}} \ldots c_{k_{nn}} F_{11}(g)^{k_{1_{11}}} \ldots F_{1n}(g)^{k_{n_{11}}} \ldots F_{n1}(g)^{k_{1_{nn}}} \ldots F_{nn}(g)^{k_{n_{nn}}}$$

where the sum $k_{1_{ij}} + \ldots + k_{n_{ij}}$ equals the degree of $h_{\beta_{k_{ij}}}$ for each ij and the $c_{k_{i}j} \in \mathbb{Q}$. Thus the coefficients (more specifically their height) will directly depend on the coordinate functions F_{ij} that generate $k[G]$.

D Bound on the order of elements in finite matrix groups

In this appendix, we provide a bound on the order of elements in finite matrix groups, which is as follows

Proposition 23. *Let $\mathbb{K}$ be a finite field extension of $\mathbb{Q}$. Then for every $d \in \mathbb{N}$, there exists a uniform bound $A_{d,\mathbb{K}}$ such that every periodic element of $\mathrm{GL}_d(\mathbb{K})$ has order at most $A_{d,\mathbb{K}} := d![\mathbb{K} : \mathbb{Q}]$.*

Proof. If $a \in \mathrm{GL}_d(\mathbb{K})$ has order n then the field k generated by the eigenvalues of a must contain a primitive n^{th} root of unity (since $a^n = I_d$), and hence contains the cyclotomic field of that order. On the other hand, k is a subfield of the splitting field of the characteristic polynomial of a, which has degree d. It follows that the degree of k over $\mathbb{K}$ is at most $d!$, hence $n \leqslant A_{d,\mathbb{K}} := [k : \mathbb{Q}] = [k : \mathbb{K}][\mathbb{K} : \mathbb{Q}] \leqslant d![\mathbb{K} : \mathbb{Q}]$. Actually, note that $A_{d,\mathbb{K}}$ only depends on the degree of $\mathbb{K}$ and not on $\mathbb{K}$ itself. □

Remark 24. Actually, a more general result is true. Such a bound also exists for the more general case where $\mathbb{K}$ is a finitely generated extension of $\mathbb{Q}$, see [Tao, Proposition 5].

E Proof of Minkowski's lemma

In this appendix, we give a proof of Lemma 6, which is adapted from [GL05, Lemma 9] and [Sup76, Theorem 4, p 68]. Recall that the lemma states that for any prime $p \geqslant 3$, the kernel of the reduction map $\mathrm{GL}_n(\mathbb{Z}_{(p)}) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ is torsion-free.

Proof of Lemma 6. Note first that if the kernel contains a torsion element, then it contains one of prime order. Indeed, if $g^r = I_n$ with $g \neq I_n$ and r minimal, write $r = qr'$ with q prime, then $g^{r'} \neq I_n$ by minimality and $(g^{r'})^q = I_n$, hence $q^{r'}$ has prime order q.

Assume now that the kernel contains a torsion element g of prime order q. By definition of the kernel, we have $p \mid g - I_n$ so we can write $g = I_n + ph$ for some $h \neq 0$. Then

$$0 = g^q - I_n = (I_n + ph)^q - I_n = p\left(qh + t + p^{q-1}h^q\right) \qquad \text{where} \qquad t = \sum_{i=2}^{q-1} \binom{q}{i} p^{i-1} h^i. \tag{1}$$

In particular, note that $q \mid t$ because it divides the binomial coefficients. There are two cases: either $q \nmid p$ or $q \mid p$. n the first case, (1) becomes $qh + t = -p^{q-1}h^q$, which implies that $q \mid p^{q-1}h^q \mid h^q \mid h$ because q is prime. Let $a \geqslant 1$ be such that $q^a \mid h$ but $q^{a+1} \nmid h$. Then $-qh = t + p^{q-1}h^q$ by (1), which is impossible since $q^{2a+1} \mid t + p^{q-1}h^q$ whereas $q^{2a+1} \nmid qh$. In the second case, we must have $q = p$ because p is prime. Now, since $p > 2$, we can rewrite (1) as $qh = q^2h^2s$ where $s \in M_n(\mathbb{Z}_{(p)})$ and thus $q \mid h$. Let $a \geqslant 1$ again be such that $q^a \mid h$ but $q^{a+1} \nmid h$. Then $q^{2a+2} \mid q^2h^2s$ but $q^{2a+2} \nmid qh$, which is a contradiction. Hence the kernel of the reduction map cannot contain an element of prime order and is by our initial observation thus torsion-free. □