

Parametrizing algebraic varieties
using Lie algebras

Jana Pílníková

A dissertation
submitted in partial fulfillment of the requirements
for the degree of
Doctor of Natural Sciences

at

Research Institute for Symbolic Computations
Johannes Kepler University
Linz, Austria

Committee in charge:

Prof. Dr. Josef Schicho, advisor
Dr. Willem A. de Graaf

Autumn 2006

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Jana Pílníková

Linz, September 2006

Zusammenfassung

In dieser Arbeit wird eine neue Methode für die Parametrisierung von algebraischen Varietäten über einen Körper der Charakteristik Null vorgestellt. Das Parametrisierungsproblem wird auf ein Problem von Finden eines Isomorphismus von Algebren reduziert.

Wir führen die Lie-Algebra einer Varietät als eine Lie-Algebra, die mit die Gruppe der Automorphismen der Varietät zusammenhängt, ein. Wenn wir einen Isomorphismus von dieser Algebra und irgendeiner klassischen Lie-Algebra gestalten (zum Beispiel die Algebra von Matrizen mit die Spur Null), dann können wir den Isomorphismus für die Parametrisierung der Varietät verwenden. Das Problem des Findens eines Isomorphismus der Lie-Algebren wird weiter auf die Trivialisierung einer assoziativen Algebra reduziert, d.h. auf das Finden eines Isomorphismus der gegebenen Algebra und einer Algebra von Matrizen. Wenn der Grundkörper nicht algebraisch abgeschlossen ist, ist das letztere ein klassisches Problem aus der Zahlentheorie. Wir präsentieren Algorithmen zur Trivialisierung von Algebren von Grad bis zu 4 über den rationalen Zahlen und über Zahlkörpern.

In der vorliegenden Arbeit wird diese Parametrisierungsmethode auf Del-Pezzo-Flächen von Grad 8 und 9 angewandt. Der Algorithmus ist für den Grundkörper der rationalen Zahlen implementiert.

Abstract

In the thesis we present a new method for parametrizing algebraic varieties over the field of characteristic zero. The problem of parametrizing is reduced to a problem of finding an isomorphism of algebras.

We introduce the Lie algebra of a variety as a Lie algebra related to its group of automorphisms. Constructing an isomorphism of this one and some classical Lie algebra (for example the algebra of matrices of the zero trace) then leads to parametrizing the variety. The problem of finding an isomorphism of Lie algebras is further reduced to trivializing an associative algebra, which means finding an isomorphism of the algebra and a full matrix algebra. The last is a classical problem in number theory, when regarded over algebraically non-closed fields. We give algorithms for trivializing algebras of degrees up to 4 over number fields.

In our work we used the method to parametrize Del Pezzo surfaces of degrees 8 and 9 over number fields. The algorithms are implemented for the case of the field of the rationals.

To the memory of my grandmother.

Contents

Chapter 1. Introduction	1
Chapter 2. Preliminaries	6
1. Some notions from algebraic geometry	6
2. Associative and Lie algebras	9
3. Algebraic groups and their Lie algebras	15
Chapter 3. Automorphisms of a variety	18
1. The Lie algebra of the variety	18
2. Computing $\mathfrak{g}_0(X, k)$	20
3. Varieties and modules	22
4. Illustrating example: \mathbb{P}^1 and \mathfrak{sl}_2	24
5. Conics and their Lie algebras	27
6. Variety as an orbit of an algebraic group	29
Chapter 4. Del Pezzo surfaces of degree 8	33
1. Embeddings of $\mathbb{P}^1 \times \mathbb{P}^1$	33
2. Blow-up of the projective plane	40
Chapter 5. Del Pezzo surfaces of degree 9	44
1. Severi-Brauer varieties	44
2. Parametrizing Del Pezzo surfaces of degree 9	45
3. More on the algebra of a Severi-Brauer variety	48
Chapter 6. Trivializing central simple algebras	52
1. Cyclic algebras and left ideals	52
2. Algebras of degree 2	54
3. Algebras of degree 3	55
4. Algebras of degree 4	59
Bibliography	65

Acknowledgements

I want to thank the people who contributed significantly to the results presented in this thesis: Josef Schicho for explaining the problem of parametrization and giving a lot of geometrical background and Willem de Graaf for his work and help with Lie algebras. I thank also Mike Harrison for his incredible insights and hints during the work.

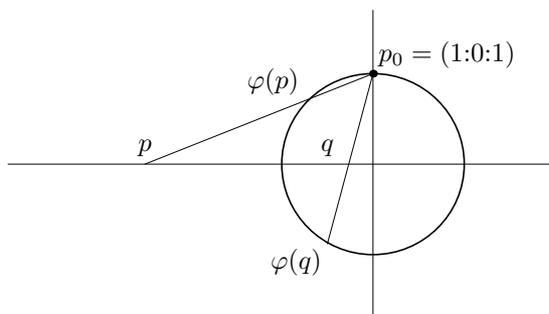
A part of the research was carried out at University of Sydney where I was visiting the Magma group in September 2004. I am grateful to John Cannon for making the visit possible.

Most of all I would like to express my gratitude to my advisor Josef Schicho for introducing me to several areas of mathematics, sharing interesting research problems with me and for all his interest, encouragements and patience.

CHAPTER 1

Introduction

Finding a parametrization of algebraic varieties is a classical problem in algebraic geometry. Informally speaking, the task is to find for a variety $X \subset \mathbb{P}^n$ given as a zero set of a finite collection of polynomials an invertible map $\mathbb{P}^d \rightarrow X$ for some d . The map is in coordinates described by homogeneous polynomials of the same degree. As an example we take the unit circle in \mathbb{P}^2 given implicitly as a zero set of the polynomial $x_1^2 + x_2^2 - x_0^2$. If we find one point p_0 on the circle, we can use the *stereographic projection* and find a parametrization by considering the points of intersection of X with the lines through p_0 .



A point p on the horizontal axis has coordinates $(s : t : 0)$ and the line through p and p_0 is then given by $tx_0 - sx_1 - tx_2$. The line and the circle meet in points p_0 and $\varphi(p)$. The coordinates of the second point give a parametrization $\mathbb{P}^1 \rightarrow X \subset \mathbb{P}^2$ of the circle:

$$(s : t) \mapsto (s^2 + t^2 : 2st : t^2 - s^2).$$

If a variety given over the field of the rationals \mathbb{Q} can be parametrized over the algebraic closure $\overline{\mathbb{Q}}$, one may pose the question whether it is possible to find a parametrization also over the rationals. By “parametrization over k ” we mean that the polynomials describing the map $\mathbb{P}^d \rightarrow X$ have their coefficients in k . In our example we were able to parametrize the circle over \mathbb{Q} because the first point p_0 had its coordinates in \mathbb{Q} . If we know the method of stereographic projection, then for a nonsingular conic these two problems become equivalent: we can find a \mathbb{Q} -parametrization of the conic X if and only if we can find a single \mathbb{Q} -rational point on X . A similar pattern emerges for many other varieties, including those of higher dimensions. The stereographic projection is replaced

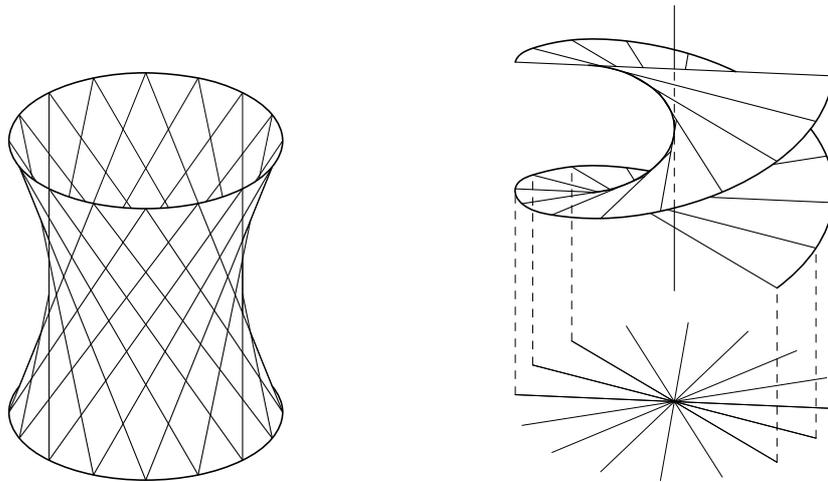
by different methods (e.g. using divisor arithmetics) and then the knowledge of a single \mathbb{Q} -rational point again leads to a \mathbb{Q} -parametrization. But finding such a point turns out to be a very hard problem. Some recent achievements in this research area can be found for example in [Lan97, PT04].

Let us mention that the *Hasse principle* holds for conics. It means that a conic defined over \mathbb{Q} has a rational point (a so-called *global solution*) if and only if it has a point over every completion of \mathbb{Q} (i.e. with respect to any valuation which is possible to define on \mathbb{Q} , a so-called *local solution*). The latter condition basically means that there exists a real solution to the defining equation of the conic, and also that for every prime number $p \in \mathbb{N}$ there is a solution modulo p (or modulo some small power of p in exceptional cases). In case of conics, the Hasse principle has also a constructive form. Namely, for a given curve one finds a finite set \mathcal{S} of “critical primes”. It means that if for each prime $p \in \mathcal{S}$ one gets a solution modulo p , then it is possible to combine these local solutions into a global one, so a rational point is constructed (cf. e.g. [Cas78]). Apart from the constructive version of the Hasse principle, there are also other efficient methods for finding a rational point on a conic (see e.g. [Sim05]).

For all varieties considered in our work, the Hasse principle holds too. Nevertheless in these cases it gives only a statement on the existence of a rational point. Though there are methods for finding a finite set of “critical primes”, still the problem of combining the local solutions into a global one remains. We do not pursue this direction in our work.

Here we will deal with some of *Del Pezzo surfaces*. By definition they are rational (i.e. parametrizable over an algebraically closed field) smooth surfaces having their anticanonical divisor ample. A basic tool for constructing Del Pezzo surfaces is *blowing up* the projective plane in one or more points. To blowup the plane in a point, one removes the point and replaces it with the projective line. A surface obtained by blowing up the projective plane in at most 8 points in a general position (no three points lie on a line, no six points are on a conic) turns out to be Del Pezzo. After blowing up the projective plane in more than 8 points, the anticanonical divisor of the resulting surface is not ample, hence the surface is not Del Pezzo. On the other hand we have that Del Pezzo surfaces come in degrees 1 till 9. Those of degree 9 are isomorphic to the projective plane after passing to an algebraically closed field. A Del Pezzo surface of degree 8 is either $\mathbb{P}^1 \times \mathbb{P}^1$ or a blowup of the projective plane in one point. Finally, Del Pezzo surface of degree d , where $1 \leq d \leq 7$, is a blowup of the projective plane in $9 - d$ points in a general position, see [Man86]. In particular, every nonsingular cubic surface in \mathbb{P}^3 is a blowup of the projective plane in 6 points.

The parametrization algorithm which we introduce is demonstrated on Del Pezzo surfaces of degrees 9 and 8. It follows that all these surfaces are parametrizable over an algebraically closed field. Here we give a method which decides whether a given surface has a parametrization over \mathbb{Q} , and finds one in the affirmative case. For blowups in one point, the decision part of the algorithm is not relevant since blowups are always parametrizable over the field where they are implicitly defined. But the constructive part of the method gives an efficient algorithm for parametrizing these surfaces, which is also preferable to known methods, see e.g. [Man86].



On the left: The surface $\mathbb{P}^1 \times \mathbb{P}^1$ embedded into \mathbb{P}^3 .

On the right: The blowup of \mathbb{P}^2 can be imagined as one turn of the helix.

Parametrizing Del Pezzo surfaces of degree 9 and those of degree 8 which are embeddings of $\mathbb{P}^1 \times \mathbb{P}^1$, is a part of the more general problem of parametrizing surfaces over the rationals. In 1998, Schicho [Sch98] gave an algorithm for parametrizing surfaces over algebraically closed fields. In the algorithm one reduces to several base cases which, except some trivial cases (e.g. \mathbb{P}^2), are Del Pezzo surfaces of degrees 5 till 9 and conic fibrations (see also [Isk80]). Note that rational Del Pezzo surfaces of degrees smaller than 5 are mapped in this step to surfaces of larger degree. When parametrizing over the rationals, these particular cases have to be treated again so that the properties of the field of the rationals are considered. The case of conic fibrations was solved in [Sch00]. Rational parametrization of Del Pezzo surfaces of degree 5 is discussed in [SB92], degree 6 is dealt with in [HS06] and degree 7 can be found in e.g. [Man86]. So this work gives a \mathbb{Q} -rational parametrization of the remaining cases. The contained material is also presented in [dGHPS06, dGPS]. Thereby the whole problem of parametrizing surfaces over \mathbb{Q} is solved.

Now we give a brief sketch of our method. We reduce the problem of parametrization to a problem of trivializing a central simple algebra, i.e. finding an isomorphism of an associative algebra and a full matrix algebra.

Let X' denote the variety defined over k which we want to parametrize. We assume that by some previous analysis we know the isomorphism class of X' . More precisely, we know that X' is over the algebraic closure \bar{k} isomorphic to a “standard variety” Y and we know a k -parametrization of Y . If we find a k -isomorphism between X' and Y , we have also constructed a desired parametrization of X' .

Assume that $Y \subset \mathbb{P}^n$ is anticanonically embedded. The first step in finding a parametrization of X' is to embed it anticanonically, $\iota: X' \hookrightarrow \mathbb{P}^n$. Let X denote the image $\iota(X')$. Then X' and Y are k -isomorphic exactly if X and Y are projectively equivalent over k .

Next we introduce the Lie algebra of a variety as the Lie algebra of the algebraic group of the projective transformations fixing the variety. In all examples considered here it is the group of all automorphisms of X . The algebraic group considered in this construction is linear and so is the Lie algebra as well. Hence we have its $(n + 1)$ -dimensional representation (provided that $X \subseteq \mathbb{P}^n$). If X and Y are projectively equivalent over k , then their Lie algebras are two k -representations of the same Lie algebra and the corresponding $(n + 1)$ -dimensional modules are isomorphic. We show that under some assumptions also the other implication is true: if the modules of Lie algebra representations corresponding to the varieties X and Y are k -isomorphic, then so are X and Y . Furthermore, we prove that a module isomorphism coincides with the projective equivalence of the varieties X and Y and hence yields the required parametrization of X' .

To find an isomorphism of modules, we first have to construct an isomorphism of Lie algebras of X and Y . If the field k is not algebraically closed, this is a very difficult task. We transform this problem to finding an isomorphism of associative algebras. More precisely, we always reduce to an isomorphism of a given algebra and a full matrix algebra. Here we give algorithms for algebras up to degree 4.

The algorithms for parametrizing Del Pezzo surfaces described in the thesis are implemented for $k = \mathbb{Q}$ and included into Magma V2.13, [BCP97].

Notation and terminology

Throughout the whole work, by k we denote a field of characteristic 0. The main focus is to develop algorithms for $k = \mathbb{Q}$. But except the characteristic being 0 we do

not use any special properties of the field of the rationals, therefore we stick to the more general notation “ k ” instead of “ \mathbb{Q} ”. The algebraic closure of k is denoted by \bar{k} .

The dimension of a vector space V over the field k is denoted $[V : k]$. The linear span of vectors v_1, \dots, v_n (i.e. the set $\{\sum_{i=1}^n c_i v_i \mid c_i \in k\}$) is denoted by $\text{span}\{v_1, \dots, v_n\}$ or $\text{span}_k\{v_1, \dots, v_n\}$.

If G, H, G_i, \dots denote algebraic groups, then, as is usually done, $\mathfrak{g}, \mathfrak{h}, \mathfrak{g}_i, \dots$ denote their Lie algebras.

If A is an algebra (associative or Lie) over a field k and $k' \supset k$ a field extension, then the algebra $A \otimes_k k'$ obtained from A by enlarging the field of coefficients is also denoted by $A_{k'}$.

By a *twist* of a k -algebra A we mean a k -algebra A' such that there is a field extension $k' \supset k$ with the property $A_{k'} \cong A'_{k'}$. For algebraic varieties X and X' defined over k we say analogously that X' is a *twist* of X if there is an isomorphism $X \mapsto X'$ defined over an extension k' of k .

Sometimes we are slightly sloppy in the language of representation theory in the following way. Though an isomorphism of modules of algebraic groups is defined for a single group (“two G -modules are isomorphic”), we say sometimes for isomorphic groups G_1 and G_2 that “ G_1 - and G_2 -module are isomorphic”. By this we mean that there is a fixed isomorphism $\varphi: G_1 \rightarrow G_2$ of groups (and from the context it is always clear which φ is taken) and an invertible map $\mu: V_1 \rightarrow V_2$ of the modules of G_1 and G_2 respectively, such that $\mu(gv) = \varphi(g)\mu(v)$. This situation occurs only if G_1 and G_2 are subgroups of some $\mathbf{GL}_n(k)$ and V_1 and V_2 respectively are their natural modules. Analogously we use this language for modules of linear Lie algebras.

CHAPTER 2

Preliminaries

This chapter consists mainly of known definitions and facts. An exception is the analysis of the algorithm `EnvelopingAlgebra` in the second section.

1. Some notions from algebraic geometry

By an (*algebraic*) k -variety X we mean a quasiprojective variety which is defined by polynomials over k . By $\mathcal{V}(I)$ we mean the variety defined by ideal I and $\mathcal{I}(X)$ denotes the vanishing ideal of X .

If X is a k -variety (i.e. defined over k) and $k' \supset k$ is a field extension of k , then $X(k')$ denotes the set of all k' -rational points on X .

We say that a variety X is k' -rational, if there is a k' -rational map $\mathbb{P}^d \rightarrow X(k')$ (called a *parametrization*) with a k' -rational inverse. In the thesis the input variety is always a \bar{k} -rational projective variety, almost always a surface. For a given \bar{k} -rational surface we decide whether it is also k -rational, and construct a parametrization over k in the affirmative case.

1.1. Tangent spaces. Since the notion of the tangent space is local in its nature, here we assume that $X \subseteq \mathbb{A}^n$ is an affine variety. Let $x \in X$. The line $L \subset \mathbb{A}^n$ is *tangent* to X at x , if its intersection multiplicity with X at x is at least 2. The *tangent space* of X at x is the geometric locus of all points on lines tangent to X at x . We will denote this space by $\mathcal{T}_x(X)$.

For a point $x \in X$, by \mathfrak{m}_x we denote the maximal ideal of the local ring \mathcal{O}_x of all functions on X which are regular at x . Let $f \in k[X]$ be the restriction of $F \in k[\mathbb{A}^n]$, $f = F|_X$. Then $d_x: k[X] \rightarrow \mathcal{T}_x(X)^*$, such that $f \mapsto (F - F(x) \pmod{\mathfrak{m}_x^2})|_{\mathcal{T}_x(X)}$, is well defined i.e. does not depend on the choice of F . Further we have

$$d_x(f + g) = d_x f + d_x g, \quad d_x(fg) = f(x)d_x g + d_x f g(x).$$

The kernel of $d_x|_{\mathfrak{m}_x}$ is exactly \mathfrak{m}_x^2 , therefore d_x is an isomorphism of $\mathfrak{m}_x/\mathfrak{m}_x^2$ and $\mathcal{T}_x(X)^*$. (cf. [Sha94], §. II.1). We have an alternative

DEFINITION 2.1. The *tangent space* of X at x is defined by $\mathcal{T}_x(X) = (\mathfrak{m}_x/\mathfrak{m}_x^2)^*$.

For more insight let us again consider the map $d_x: \mathcal{O}_x \rightarrow (\mathcal{T}_x(X))^*$, which is the unique extension of d_x on $k[X]$ as defined before. Its pullback d_x^* maps $(\mathcal{T}_x(X))^{**} = \mathcal{T}_x(X) \rightarrow \mathcal{O}_x^*$. If $(a_1, \dots, a_n) \in \mathcal{T}_x(X)$, then by d_x^* this point is identified with the map $(a_1, \dots, a_n)^* \circ d_x = \sum_i a_i \frac{\partial}{\partial t_i}|_x$ (differentiation followed by evaluation at x). Therefore elements of the tangent space of X at x can be viewed as *point derivations*, i.e. linear maps $\delta: \mathcal{O}_x \rightarrow k$ such that $\delta(fg) = \delta(f)g(x) + f(x)\delta(g)$.

Let now $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties and let $\varphi: X \rightarrow Y$ be a morphism. Let $x \in X$ and $y = \varphi(x)$. The pullback $\varphi^*: k[Y] \rightarrow k[X]$ then gives a well defined map $\mathfrak{m}_y/\mathfrak{m}_y^2 \rightarrow \mathfrak{m}_x/\mathfrak{m}_x^2$. Its dual maps $\mathcal{T}_x(X) \rightarrow \mathcal{T}_y(Y)$ and is called the *differential of φ* and denoted by $d_x\varphi$. Here we give an explicit differentiation formula (see [Hum75], §.5.4.)

Let φ be given by m coordinate functions $\varphi_i(t_1, \dots, t_n)$, $i = 1, \dots, m$. Let us identify the tangent spaces at x and $y = \varphi(x)$ with linear subspaces of k^n and k^m . The point $(a_1, \dots, a_n) \in k^n$ represents the point derivation $\mathcal{O}_x \rightarrow k$ given by $\sum_i a_i \frac{\partial}{\partial t_i}|_x$. Then its image is

$$d\varphi(a) = (b_1, \dots, b_m) \quad \text{where} \quad b_k = \sum_i a_i \frac{\partial \varphi_k}{\partial t_i}(x).$$

1.2. Divisors and rational maps. For an irreducible variety X , a collection of irreducible closed subvarieties C_1, \dots, C_r of codimension 1 in X together with assigned multiplicities $k_1, \dots, k_r \in \mathbb{Z}$ is called a *Weil divisor* on X and denoted

$$D = k_1 C_1 + \dots + k_r C_r.$$

If all $k_i = 0$, we write $D = 0$. If all $k_i \geq 0$ and some $k_i > 0$, we write $D > 0$ and say that D is *effective*. All Weil divisors form a free abelian group generated by subvarieties of codimension 1. We denote this group by $\text{Div } X$.

A *Cartier divisor* (or a *locally principal divisor*) is a maximal family of pairs $\{(U_i, f_i)\}$ consisting of Zariski open subsets U_i of X and rational functions f_i such that

- (i) $\bigcup_i U_i = X$,
- (ii) for each i, j the rational functions $f_i^{-1}f_j$ and $f_i f_j^{-1}$ are regular on $U_i \cap U_j$.

For a pair (U, f) in the Cartier divisor D we also say that it represents the divisor D locally (on the open set U). Cartier divisors also form a group: if a divisor D is represented by (U, f) and D' by (U, f') , then $D + D'$ is represented by (U, ff') .

If the variety X is nonsingular, then the groups of Weil and Cartier divisors are isomorphic. In the whole work we deal only with nonsingular varieties therefore from now on we don't distinguish Weil and Cartier divisor.

Let $f \in k(X)$ be nonzero. Then f defines a divisor represented by (U, f) for all open $U \subseteq X$ and denoted by (f) . Such divisors are called *principal divisors*. For divisors D

and D' we write $D \sim D'$ if $D - D'$ is principal. All principal divisors form a subgroup of $\text{Div } X$. The factor group of all divisors modulo principal divisors is called the *Picard group* of X and denoted by $\text{Pic } X$.

Let $\varphi: X \rightarrow Y$ be a dominant map (i.e. the image $\varphi(X)$ is dense in Y). Since any divisor is principal in some affine subset of X , the pullback φ^* defines a map $\text{Div } Y \rightarrow \text{Div } X$. The pullback of a principal divisor is principal, therefore we have also a map $\varphi^*: \text{Pic } Y \rightarrow \text{Pic } X$.

If C is a subvariety of X of codimension 1 with the vanishing ideal $\mathcal{I}(C) \subset k[X]$, we can define the valuation v_C on $k[X] \setminus \{0\}$ by taking for $v_C(f)$ the largest $n \in \mathbb{N}$ such that $(\mathcal{I}(C))^n$ is in the ideal generated by f . The valuation extends to $k(X) \setminus \{0\}$ by $v_C(f/g) = v_C(f) - v_C(g)$ for $f, g \in k[X] \setminus \{0\}$.

Let D be a divisor on X . The subset of $k(X)$

$$\mathcal{L}(D) = \{f \in k(X) \mid D + (f) \geq 0\}$$

together with $\{0\}$ is a linear space, since for each irreducible codimension 1 subvariety $C \subset X$ and all $f, g \in k(X)$ it holds $v_C(f + g) \geq \min\{v_C(f), v_C(g)\}$. We call $\mathcal{L}(D)$ the *Riemann-Roch space* of D . One can prove (see e.g. [Sha94]) that if X is a projective variety, then $\mathcal{L}(D)$ is finite-dimensional for all D . In following we will always assume that $[\mathcal{L}(D) : k] < \infty$.

If f_0, \dots, f_n is a basis of $\mathcal{L}(D)$, then we associate with D a rational map

$$\iota_D = (f_0 : \dots : f_n) : X \rightarrow \mathbb{P}^n.$$

Choosing another basis of $\mathcal{L}(D)$ leads to an image of X in \mathbb{P}^n which is projectively equivalent to the former one.

LEMMA 2.2. *If $D \sim D'$ are divisors on a variety X , then $\iota_D(X)$ and $\iota_{D'}(X)$ are projectively equivalent.*

PROOF. Let $g \in k(X)$ be such that $D = D' + (g)$. If f_0, \dots, f_n is a basis of $\mathcal{L}(D)$, then $f_0g, \dots, f_n g$ is a basis of $\mathcal{L}(D')$. In projective space $(f_0 : \dots : f_n)$ is the same map as $(f_0g : \dots : f_n g)$, hence the assertion of the lemma follows. \square

LEMMA 2.3. *Let $\varphi: X \rightarrow Y$ be an isomorphism of varieties. For a divisor $D' \in \text{Div } Y$ and its pullback $D = \varphi^*(D') \in \text{Div } X$ then holds that $\iota_D(X)$ and $\iota_{D'}(Y)$ are projectively equivalent.*

PROOF. If $D' + (g) \geq 0$, then also $\varphi^*(D' + (g)) = D + (\varphi^*g) \geq 0$. From φ being an isomorphism then follows that if g_0, \dots, g_n is a basis of $\mathcal{L}(D')$, then $\varphi^*(g_0), \dots, \varphi^*(g_n)$

is a basis of $\mathcal{L}(D)$. Then $\iota_D(X) = (\varphi^*(g_0) : \cdots : \varphi^*(g_n))(X) = (g_0 : \cdots : g_n)(\varphi(X)) = \iota_{D'}(Y)$. \square

We will describe now the very rough idea of our parametrization algorithm. Let X be a variety that we want to parametrize. Suppose that we know (by some preceding analysis) not only that X is \bar{k} -rational but also that it is isomorphic over \bar{k} to a variety X_0 having a k -rational parametrization. Deciding the existence and finding an isomorphism of X_0 and X over k would solve the problem of finding a k -parametrization of X .

We say that the divisor D on the variety X is *very ample*, if ι_D is an embedding. Let D be a very ample divisor such that the class of D in $\text{Pic } X$ is fixed under any automorphism of X . If $\varphi_1, \varphi_2: X_0 \rightarrow X$ are two isomorphisms, then $\varphi_1^*(D) \sim \varphi_2^*(D)$. By the two lemmata above it follows that $\iota_{D_0}(X_0)$ and $\iota_D(X)$ are projectively equivalent, where D_0 is the pullback of D by any isomorphism $X_0 \rightarrow X$.

If X_0 and X are k -varieties and the embeddings ι_{D_0} and ι_D are defined over k , then the problem of deciding existence and finding a k -isomorphism $X_0 \rightarrow X$ is therefore reduced to finding a projective equivalence over k .

In almost all examples considered, we take an anticanonical divisor as the very ample divisor. This divisor class is invariant under automorphisms of the variety. Further, for a k -variety there is always an anticanonical divisor over k , therefore the associated embedding is defined over k . The only exception is Example 4.6, where for the sake of simplicity, another very ample divisor is taken.

2. Associative and Lie algebras

2.1. Structure of semisimple associative algebras. Let A be a finite-dimensional k -algebra and V an A -module. We say that the module V is *semisimple*, if for each submodule $V_1 \subset V$ there is a submodule $V_2 \subset V$ such that $V = V_1 \oplus V_2$. An algebra is called *semisimple*, if it is semisimple as a module over itself. If there are no nontrivial (two-sided) ideals in A , then A is said to be *simple*.

THEOREM 2.4 (Wedderburn's structure theorem). *Every semisimple k -algebra is a direct sum of finitely many simple algebras and each summand is isomorphic to a matrix algebra over a unique division algebra.*

PROOF. [Jac89, Pie82]. \square

By Wedderburn's theorem the study of semisimple algebras can be reduced to study of simple ones. Further, since the center of a simple algebra is a field, every simple

algebra can be regarded as a *central simple algebra* A , which by definition is a finite-dimensional simple k -algebra such that the center $\mathbf{C}(A)$ is isomorphic to k . For any such algebra A there is $n \in \mathbb{N}$ and a unique central division algebra Δ over k such that A is isomorphic to $M_n(\Delta)$, the algebra of all matrices over Δ .

LEMMA 2.5. *If the field k is algebraically closed, then the only division algebra over k is the field k itself.*

PROOF. If Δ is a division algebra over k , then the minimal polynomial of any element in Δ is irreducible over k . Only linear polynomials over an algebraically closed field are irreducible, therefore each element in Δ is of the form $\gamma \cdot 1$ for $\gamma \in k$. \square

If the algebra A is central simple over k , then the algebra $A_{k'} = A \otimes_k k'$ obtained from A by extending the coefficient field, is central simple over k' and its dimension $[A_{k'} : k'] = [A : k]$. Moreover by the previous lemma, if k' is algebraically closed, $A_{k'} \cong M_n(k')$ for some $n \in \mathbb{N}$. Consequently, the dimension of any central simple algebra is always a square, therefore we can talk about the *degree* of the algebra, which is the integer $\sqrt{[A : k]}$. The field k' such that $A_{k'} \cong M_n(k')$ is called a *splitting field* of A .

2.2. Lie algebras. A *Lie algebra* \mathfrak{g} is a vector space over k together with a (non-associative) bilinear operation $[\cdot, \cdot]: \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$ satisfying

- (i) $[x, y] + [y, x] = 0$ (anticommutativity), *
- (ii) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ (Jacobi identity).

If A is an associative algebra over k , then it can be turned into a Lie algebra if we replace the associative multiplication by the *Lie bracket* $[x, y] = xy - yx$. We denote this Lie algebra by A_{Lie} .

The Lie algebra is called *simple*, if it contains no nontrivial ideal.

Important examples are the Lie algebras $\mathfrak{gl}_n(k)$ and $\mathfrak{sl}_n(k)$, where $\mathfrak{gl}_n(k) = M_n(k)_{\text{Lie}}$ and $\mathfrak{sl}_n(k)$ is the subalgebra of $\mathfrak{gl}_n(k)$ containing all $n \times n$ matrices of zero trace, so $[\mathfrak{sl}_n(k) : k] = n^2 - 1$. The algebra $\mathfrak{gl}_n(k)$ has the ideal consisting of scalar matrices, the algebra $\mathfrak{sl}_n(k)$ is simple.

The following theorem about the structure of automorphisms of the Lie algebra $\mathfrak{sl}_n(k)$ will be important.

THEOREM 2.6. *The group of automorphisms of the Lie algebra of 2×2 matrices of trace 0 is the set of mappings $x \mapsto a^{-1}xa$ for $a \in \mathbf{GL}_2(k)$.*

*In case the characteristic of the field equals 2, the property (i) is replaced by $[x, x] = 0$ (in other characteristics these two are equivalent).

The group of automorphisms of the Lie algebra of $n \times n$ matrices, $n > 2$ of trace 0 is the set of mappings $x \mapsto a^{-1}xa$ and $x \mapsto -a^{-1}x^t a$ for $a \in \mathbf{GL}_n(k)$.

PROOF. For algebraically closed fields this is Theorem 5 in [Jac79], Chapter IX. If k is not algebraically closed, let $\alpha: x \mapsto a^{-1}xa$ for $a \in \mathbf{GL}_n(\bar{k})$ be an automorphism of $\mathfrak{sl}_n(k)$. Then $xa = a\alpha(x)$ for each $x \in \mathfrak{sl}_n(k)$ gives a system of linear conditions for entries of the matrix a , where all these conditions are over k . Therefore a can be taken to be from $\mathbf{GL}_n(k)$. The case $x \mapsto -a^{-1}x^t a$ is analogous. \square

A Lie algebra homomorphism (i.e. a vector space homomorphism preserving the multiplication) $\mathfrak{g} \rightarrow \mathfrak{gl}_n(k)$ is called a *representation of \mathfrak{g}* . The representation $\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_d(k)$ where $d = [\mathfrak{g} : k]$ such that $(\text{ad } x)y = [x, y]$ is called the *adjoint representation of \mathfrak{g}* .

Not for every Lie algebra \mathfrak{g} there exists an associative algebra A such that $\mathfrak{g} \cong A_{\text{Lie}}$. But to any Lie algebra we can assign an associative algebra as follows. Let $\mathfrak{g} \subset A_{\text{Lie}}$ for an associative algebra A . Then the (associative) subalgebra of A generated by \mathfrak{g} is called an *enveloping algebra of \mathfrak{g} (in A)*. The *universal enveloping algebra $\mathfrak{U}(\mathfrak{g})$ of \mathfrak{g}* is the largest enveloping algebra of \mathfrak{g} in a sense that any enveloping algebra of \mathfrak{g} is the universal enveloping algebra modulo an ideal in $\mathfrak{U}(\mathfrak{g})$.

Here we describe and analyze the algorithm which for twists of $\mathfrak{sl}_n(k)$, (i.e. such \mathfrak{g} that $\mathfrak{g} \otimes \bar{k} \cong \mathfrak{sl}_n(\bar{k})$) constructs an enveloping algebra. This is the case needed in our parametrization problem.

LEMMA 2.7. *Let \mathfrak{g} be a twist of $\mathfrak{sl}_n(k)$ such that there is an n^2 -dimensional enveloping algebra A of \mathfrak{g} . Then A is central simple.*

PROOF. Let us fix an embedding $\rho: \mathfrak{g} \hookrightarrow A_{\text{Lie}}$. Then $\rho(\mathfrak{g})$ has no center and hence does not contain the identity. Therefore $A_{\text{Lie}} = \mathfrak{g} \oplus \text{span}\{I\}$. Any two-sided ideal in A is an ideal in A_{Lie} . The only ideals of A_{Lie} are 0 , k (the center of A), $\rho(\mathfrak{g})$ and A_{Lie} . But k is not an ideal in A and 0 and A_{Lie} are trivial ideals. Since \mathfrak{g} is simple, the only nontrivial ideal in A has to coincide with $\rho(\mathfrak{g})$. This ideal cannot be nilpotent since otherwise (by Engel's theorem, cf. [Hum72]) also \mathfrak{g} would be nilpotent. Hence the radical of A is zero. So A is the direct sum of simple ideals. But the center of A , which is a direct sum of centers of direct summands, has dimension 1, therefore A is central simple. \square

DEFINITION 2.8. A *Cartan subalgebra* of a Lie algebra \mathfrak{g} is a nilpotent subalgebra $\mathfrak{h} \subseteq \mathfrak{g}$ which is equal to its normalizer, i.e. if $[x, y] \in \mathfrak{h}$ for all $x \in \mathfrak{h}$, then $y \in \mathfrak{h}$.

ALGORITHM: **EnvelopingAlgebra**

INPUT: \mathfrak{g} – a Lie algebra which is a twist of $\mathfrak{sl}_n(k)$.

OUTPUT: A – an associative algebra and an embedding $\mathfrak{g} \hookrightarrow A_{\text{Lie}}$.

- (1) $\mathfrak{h} :=$ a Cartan subalgebra of \mathfrak{g} ;
- (2) $k' :=$ a splitting field of \mathfrak{h} , i.e. a number field containing the eigenvalues of $\text{ad } h$ for $h \in \mathfrak{h}$;
- (3) **if** $k' = k$ **then**
 construct an isomorphism $\mathfrak{g} \rightarrow \mathfrak{sl}_n(k)$ (e.g. according to [dG00], §5.11);
 return $M_n(k)$ and $\mathfrak{g} \rightarrow (M_n(k))_{\text{Lie}}$
 end if;
- (4) construct an isomorphism $\rho': \mathfrak{g} \otimes k' \rightarrow \mathfrak{sl}_n(k') \subset \mathfrak{gl}(V')$ using the split Cartan subalgebra $\mathfrak{h} \otimes k'$;
- (5) viewing the k' -space V' of dimension n as a vector space V over k gives a representation $\rho: \mathfrak{g} \rightarrow \mathfrak{sl}_{dn}(k) \subset \mathfrak{gl}(V)$ with $[V : k] = dn$, d being the degree of k' over k ;
- (6) $\rho(\mathfrak{g})^* :=$ the algebra generated by $\rho(\mathfrak{g})$;
- (7) **return** $\rho(\mathfrak{g})^*$ and $\mathfrak{g} \rightarrow (\rho(\mathfrak{g})^*)_{\text{Lie}}$.

The following assertions show that in case of “good” twists of \mathfrak{sl}_n our algorithm indeed constructs the smallest possible enveloping algebra, and discuss its uniqueness.

LEMMA 2.9. *The representation $\rho: \mathfrak{g} \rightarrow (\rho(\mathfrak{g})^*)_{\text{Lie}}$ constructed by the algorithm **EnvelopingAlgebra** is an injective homomorphism of the Lie algebras.*

PROOF. Follows from the fact that \mathfrak{g} as a twist of $\mathfrak{sl}_n(k)$ is a simple algebra. \square

LEMMA 2.10. *Let A be a twist of $M_n(k)$. Suppose \mathfrak{g} is a Lie algebra over k such that $\mathfrak{g} \oplus k \cong A_{\text{Lie}}$. Let $\rho(\mathfrak{g})^*$ be the enveloping algebra constructed by the algorithm. Then $\rho(\mathfrak{g})^*$ is a twist of $M_n(k)$. In particular, $[\rho(\mathfrak{g})^* : k] = n^2$.*

PROOF. Let a_0, \dots, a_{n^2-1} be a k -basis of A . It can be chosen so that after viewing a_i 's as $n \times n$ matrices over some extension k' of k we have that $a_0 = I_n$ is the identity matrix and a_i for $i \geq 1$ are matrices of zero trace. The structure constants in A with respect to this basis are in k :

$$a_i a_j = \sum_k c_{ij}^k a_k, \quad c_{ij}^k \in k.$$

From the assumption there is an isomorphism of Lie algebras $\mathfrak{g} \oplus k \rightarrow A_{\text{Lie}}$. Let φ denote the restriction of this map to \mathfrak{g} . After extending the field of coefficients to k' we have

$\varphi(\mathfrak{g} \otimes k') = \mathfrak{sl}_n(k')$, the linear span of a_1, \dots, a_{n^2-1} . Let b_1, \dots, b_{n^2-1} be the basis of \mathfrak{g} such that $a_i = \varphi(b_i)$.

Let $\rho': (\mathfrak{g} \otimes k') \rightarrow \mathfrak{sl}_n(k')$ be the representation (over k') constructed in the step (4) of the algorithm. We have to show that the (associative) structure constants in A with respect to the basis $a_0, \rho'(b_1), \dots, \rho'(b_{n^2-1})$ are also in k .

Denote $\alpha = \rho' \circ \varphi^{-1}$, so α is an automorphism of $\mathfrak{sl}_n(k')$. By Theorem 2.6 then α either maps $x \mapsto a^{-1}xa$ or $x \mapsto -a^{-1}x^t a$. In the first case we have

$$\rho'(b_i)\rho'(b_j) = (\alpha \circ \varphi(b_i))(\alpha \circ \varphi(b_j)) = \alpha(a_i)\alpha(a_j) = \dots = c_{ij}^0 a_0 + \sum_{k=1}^{n^2-1} c_{ij}^k \rho'(b_k).$$

Similarly in the second case we get

$$\rho'(b_i)\rho'(b_j) = -c_{ji}^0 a_0 - \sum_{k=1}^{n^2-1} (-c_{ji}^k) \rho'(b_k).$$

Finally, the k -dimension of $\rho(\mathfrak{g})^*$ is equal to the k -dimension of $\rho'(\mathfrak{g})^*$. \square

Note that the assumption $\mathfrak{g} \oplus k \cong A_{\text{Lie}}$ is stronger than \mathfrak{g} being a twist of $\mathfrak{sl}_n(k)$. Indeed, if \mathfrak{g} is the Lie algebra over \mathbb{Q} of zero-trace skew Hermitian matrices of degree 3 (i.e. all matrices $x \in M_3(\mathbb{Q}(i))$ such that $x^t + \bar{x} = 0$), then \mathfrak{g} splits over $\mathbb{Q}(i)$, i.e. $\mathfrak{g} \otimes \mathbb{Q}(i) \cong \mathfrak{sl}_3(\mathbb{Q}(i))$. On the other hand there is no twist of $M_3(\mathbb{Q})$ having splitting field of degree 2. In this case one finds out that $[\rho(\mathfrak{g})^* : k] = 18$, though $n = 3$.

PROPOSITION 2.11. *Let \mathfrak{g} be a twist of \mathfrak{sl}_n such that there is an embedding $\mathfrak{g} \hookrightarrow A$, where A is a twist of $M_n(k)$. Let A_1, A_2 be two enveloping algebras of \mathfrak{g} , both of dimension n^2 . Then A_1 and A_2 are isomorphic or antiisomorphic, where the second possibility can occur only if $n > 2$.*

PROOF. Firstly, by Lemma 2.7, any n^2 -dimensional enveloping algebra of \mathfrak{g} is central simple. Therefore both A_1 and A_2 are twists of $M_n(k)$.

Let now ρ_i be a fixed embedding $\mathfrak{g} \hookrightarrow (A_i)_{\text{Lie}}$, $i = 1, 2$. Since A_i is a twist of $M_n(k)$, for each $x \in \mathfrak{g}$ the image $\rho_i(x)$ can be understood as a matrix in $M_n(\bar{k})$, the associative multiplication in A_i being then just a multiplication of matrices.

Let further $\varphi: A_1 \rightarrow A_2$ be a linear map such that $\varphi([a, b]) = [\varphi(a), \varphi(b)]$. Such a map exists because the Lie algebra isomorphism $\rho_2 \circ \rho_1^{-1}$ easily extends to $\rho_1(\mathfrak{g}) \oplus I_n$. Clearly $\varphi(\rho_1(\mathfrak{g})) = \rho_2(\mathfrak{g})$, so φ restricts to a Lie algebra isomorphism $\rho_1(\mathfrak{g}) \rightarrow \rho_2(\mathfrak{g})$. Then φ as a map from A_1 uniquely extends to a linear map $A_1 \otimes \bar{k} = M_n(\bar{k}) \rightarrow M_n(\bar{k})$. Restriction to the matrices of trace 0 leads to a Lie algebra automorphism of $\mathfrak{sl}_n(\bar{k})$. By Theorem 2.6 there are two possibilities: (1) φ maps x to $a^{-1}xa$ for some regular a . Then

φ is an automorphism of $M_n(\bar{k})$, i.e. an isomorphism $A_1 \rightarrow A_2$. (2) $\varphi(ab) = -\varphi(b)\varphi(a)$, therefore $\psi: A_1 \rightarrow A_2, x \mapsto -\varphi(x)$ is an antiisomorphism of algebras. \square

COROLLARY 2.12. *The Lie algebra \mathfrak{g} is isomorphic to $\mathfrak{sl}_n(k)$ if and only if $\rho(\mathfrak{g})^*$ is isomorphic to $M_n(k)$.*

PROOF. There exists an embedding $\rho: \mathfrak{sl}_n(k) \rightarrow M_n(k)_{\text{Lie}}$. Since there is an antiisomorphism $M_n(k) \rightarrow M_n(k)$ (e.g. $x \mapsto x^t$), the claim follows. \square

2.3. Representations of semisimple Lie algebras. For a Lie algebra \mathfrak{g} we define the sequence of ideals $\mathfrak{g}^{(i)}$ (called the *derived series*) by $\mathfrak{g}^{(0)} = \mathfrak{g}, \mathfrak{g}^{(i)} = [\mathfrak{g}^{(i-1)}, \mathfrak{g}^{(i-1)}]$. The algebra \mathfrak{g} is called *solvable*, if $\mathfrak{g}^{(n)} = 0$ for some n . The unique maximal solvable ideal in \mathfrak{g} is called the *radical of \mathfrak{g}* and denoted by $\text{Rad } \mathfrak{g}$. If $\text{Rad } \mathfrak{g} = 0$, then \mathfrak{g} is called *semisimple*. Clearly, a simple algebra is also semisimple.

In following we assume that \mathfrak{g} is a semisimple Lie algebra with a fixed split Cartan subalgebra \mathfrak{h} (so all eigenvalues of $\text{ad } h$ for all $h \in \mathfrak{h}$ are in the field k). It follows that $\text{ad } \mathfrak{h}$ is diagonalizable over k . Therefore \mathfrak{g} is a direct sum of the subspaces $\mathfrak{g}_\alpha = \{x \in \mathfrak{g} \mid [h, x] = \alpha(h)x \text{ for all } h \in \mathfrak{h}\}$, where α ranges over \mathfrak{h}^* . The space \mathfrak{g}_0 is the centralizer of \mathfrak{h} in \mathfrak{g} and it is equal to \mathfrak{h} . The set of all nonzero $\alpha \in \mathfrak{h}^*$ such that $\mathfrak{g}_\alpha \neq 0$ is denoted by Φ . The elements of Φ are called *roots of \mathfrak{g} relative to \mathfrak{h}* . By Φ^+ resp. Φ^- we denote the set of positive resp. negative roots.

If V is any \mathfrak{g} -module, then \mathfrak{h} acts diagonally on $V: V = \coprod V_\lambda$, where λ ranges over \mathfrak{h}^* and $V_\lambda = \{v \in V \mid h \cdot v = \lambda(h)v\}$. If $V_\lambda \neq 0$, we call it *weight space* and λ is called *weight of V_λ* .

For a \mathfrak{g} -module V , each \mathfrak{g}_α for $\alpha \in \Phi$ maps weight spaces to the weight spaces, more precisely \mathfrak{g}_α maps V_λ to $V_{\lambda+\alpha}$. A nonzero vector $v \in V_\lambda$ for some λ killed by all $\mathfrak{g}_\alpha, \alpha \in \Phi^+$ is called a *highest weight vector* and denoted by v^+ . Then λ is called a *highest weight*.

LEMMA 2.13. *Let V be an irreducible finite dimensional \mathfrak{g} -module, with a highest weight vector v^+ . Then v^+ is unique up to (nonzero) scalar multiples.*

PROOF. See [Hum72], Corollary to Theorem 20.2. \square

THEOREM 2.14. *Let V, W be finite dimensional \mathfrak{g} -modules of the same highest weight λ . If V and W are irreducible, then they are isomorphic.*

PROOF. See [Hum72], Theorem A in §20.3. \square

If v^+ is the highest weight vector of an irreducible finite dimensional module V , then $V = \mathfrak{U}(\mathfrak{g}) \cdot v^+$. Actually, V is spanned by vectors $x_{\alpha_1} \dots x_{\alpha_m} v^+$, where $\alpha_1, \dots, \alpha_m \in \Phi^-$. This gives a very fast algorithm for constructing an isomorphism of modules:

- (1) Fix a split Cartan subalgebra \mathfrak{h} in \mathfrak{g} .
- (2) Check whether the two \mathfrak{g} -modules V and V' have the same dimension and the same highest weight.
- (3) Set v^+ be the highest weight vector in V and v'^+ the highest weight vector in V' .
- (4) Take v_1, \dots, v_n to be a basis of V such that the action of \mathfrak{h} is diagonal with respect to this basis.
- (5) For each v_i take a chain $x_{\alpha_1} \dots x_{\alpha_m} \in \mathfrak{U}(\mathfrak{g})$ such that $v_i = x_{\alpha_1} \dots x_{\alpha_m} v^+$. Then v_i is by the module isomorphism mapped to $x_{\alpha_1} \dots x_{\alpha_m} v'^+$.

The last notion to be defined is a *Chevalley basis* of a semisimple algebra \mathfrak{g} . It is a basis $\{x_\alpha, \alpha \in \Phi; h_i, i = 1 \dots m\}$ such that $\{h_i, i = 1 \dots m\}$ is a basis of a split Cartan subalgebra of \mathfrak{g} and x_α are root vectors satisfying

- (i) $[x_\alpha, x_{-\alpha}]$ is a \mathbb{Z} -linear combination of h_1, \dots, h_l ,
- (ii) if $\alpha, \beta, \alpha + \beta \in \Phi$, $[x_\alpha, x_\beta] = c_{\alpha, \beta} x_{\alpha + \beta}$, then $c_{-\alpha, -\beta} = -c_{\alpha, \beta}$.

It holds that the structure constants of any algebra \mathfrak{g} with respect to its Chevalley basis are integral (cf. e.g. [Hum72]).

3. Algebraic groups and their Lie algebras

DEFINITION 2.15. An *algebraic group* is an algebraic variety G together with

- (i) an element $e \in G$,
- (ii) a morphism $\mu: G \times G \rightarrow G$, $(g, h) \mapsto gh$,
- (iii) a morphism $\iota: G \rightarrow G$, $g \mapsto g^{-1}$.

with respect to which G is a group. We call G a *k-group*, if G is a k -variety and morphisms μ and ι are defined over k .

A *morphism* of algebraic groups is a morphism of algebraic varieties which is also a homomorphism of groups.

Since an algebraic group has a transitive group of automorphisms (namely $g \mapsto gh$) and the singular locus is a proper closed subset of the variety, an algebraic group is a non-singular variety.

For a finite-dimensional space V over k , the group $\mathbf{GL}(V)$ of all automorphisms of V is an algebraic k -group since it is a principal open subset of $M_d(k)$ (given by the

k -polynomial equation $\det g \neq 0$) and both multiplication and inverse of a matrix are polynomial maps with integer coefficients. A closed subgroup of $\mathbf{GL}(V)$ is called a *linear algebraic group*. A morphism $G \rightarrow \mathbf{GL}(V)$ of algebraic groups is called a *rational (linear) representation* of G .

With an algebraic group G we can associate a *Lie algebra* $L(G)$ which is the tangent space $\mathcal{T}_e(G)$ of G at e endowed with the multiplication as follows.

Let A be a commutative k -algebra and M be an A -module. A *k -derivation* from A to M is a k -linear map $\delta: A \rightarrow M$ such that $\delta(ab) = \delta(a)b + a\delta(b)$ for all $a, b \in A$. The set of all k -derivations from A to M is denoted $\text{Der}_k(A, M)$.

Then the *Lie algebra of G* is the space of all left invariant derivations in $\text{Der}_k(k[G], k[G])$, i.e.

$$L(G) = \{\delta \in \text{Der}_k(k[G], k[G]) \mid \delta\lambda_g = \lambda_g\delta \ \forall g \in G\}$$

where $\lambda_g f(h) = f(g^{-1}h)$ for all $f \in k[G]$, $g, h \in G$ is a *left translation*.

We can relate the Lie algebra of an algebraic group G with the tangent space of the group at the identity e (we recall that $\mathcal{T}_e(G) = (\mathfrak{m}_e/\mathfrak{m}_e^2)^*$):

THEOREM 2.16. *Let $\Theta: L(G) \rightarrow \mathcal{T}_e(G)$ be defined by $(\Theta\delta)(f) = (\delta f)(e)$. Then Θ is a vector space isomorphism.*

PROOF. See [Hum75], Theorem 9.1. □

For an algebraic group G , we denote $\mathfrak{g} = \mathcal{T}_e(G)$ together with the Lie algebra structure carried over by Θ .

The Lie algebra $L(\mathbf{GL}(V))$ with $[V : k] = n$ is $\mathfrak{gl}_n(k)$, the set of all $n \times n$ matrices, where $[x, y] = xy - yx$. If $G \subseteq \mathbf{GL}(V)$ is a linear algebraic group, then $L(G)$ is a subalgebra of $\mathfrak{gl}_n(k)$. For more details see [Bor91, Hum75, Spr98].

PROPOSITION 2.17. *Let $G_1, G_2 \subseteq \mathbf{GL}_m(k)$ be algebraic groups and $\mathfrak{g}_1, \mathfrak{g}_2 \subseteq \mathfrak{gl}_m(k)$ their Lie algebras. If $h \in \mathbf{GL}_m(k)$ is such that $g \mapsto hgh^{-1}$ is an isomorphism from G_1 to G_2 , then its differential is an isomorphism from \mathfrak{g}_1 to \mathfrak{g}_2 given by $x \mapsto h x h^{-1}$.*

PROOF. Let us denote $\varphi: G_1 \rightarrow G_2$, $g \mapsto hgh^{-1}$. We have

$$\varphi(g)_{ij} = (hgh^{-1})_{ij} = \sum_{kl} h_{ik} g_{kl} (h^{-1})_{lj}.$$

By differentiating (i, j) -th coordinate of φ we get

$$d\varphi(x)_{ij} = d(\sum_{kl} h_{ik} g_{kl} (h^{-1})_{lj})(x) = \sum_{kl} h_{ik} x_{kl} (h^{-1})_{lj}.$$

So $d\varphi(x) = h x h^{-1}$. □

COROLLARY 2.18. *Let $\alpha_i: G \rightarrow G_i \subseteq \mathbf{GL}_m(k)$, $i = 1, 2$ be two faithful rational representations of the algebraic group G such that the two m -dimensional modules V_1, V_2 are isomorphic (V_i is the natural G_i -module). Then the isomorphism of G -modules V_1 and V_2 is also an isomorphism of V_1 and V_2 as \mathfrak{g} -modules.*

PROOF. Let μ denote the G -module isomorphism $V_1 \rightarrow V_2$ and let h be the matrix of μ , so $\mu: v \mapsto hv$.

Let $\varphi: G_1 \rightarrow G_2$ be an isomorphism of algebraic groups such that $\mu(gv) = \varphi(g)\mu(v)$. Then for any $g \in G_1$ and $v \in V_1$ we have

$$hgv = \mu(gv) = \varphi(g)\mu(v) = \varphi(g)hv.$$

Since $v \in V_1$ is arbitrary, it follows $\varphi(g) = hgh^{-1}$ for all $g \in G_1$. Now by Proposition 2.17, the isomorphism $d\varphi: \mathfrak{g}_1 \rightarrow \mathfrak{g}_2$ maps $x \mapsto h x h^{-1}$. It is straightforward to check that then $v \mapsto hv$ is a corresponding isomorphism of the \mathfrak{g} -modules. \square

The $G \subset \mathbf{GL}_m(k)$ acts on itself by inner automorphisms

$$\text{Int } h: g \mapsto hgh^{-1}, \quad g, h \in G.$$

The differential of $\text{Int } h$ is denoted by $\text{Ad } h$. By Proposition 2.17 we have that

$$\text{Ad } h(x) = h x h^{-1}, \quad h \in G, x \in \mathfrak{g}.$$

PROPOSITION 2.19. *Let $G_1 \subseteq \mathbf{GL}_n(k), G_2 \subseteq \mathbf{GL}_m(k)$ be algebraic groups and $\mathfrak{g}_1 \subseteq \mathfrak{gl}_n(k), \mathfrak{g}_2 \subseteq \mathfrak{gl}_m(k)$ their Lie algebras. Let $\varphi: G_1 \rightarrow G_2$ be a morphism and $d\varphi: \mathfrak{g}_1 \rightarrow \mathfrak{g}_2$ its differential. Then for every $h \in G_1(k)$ we have*

$$d\varphi \circ \text{Ad } h = \text{Ad } \varphi(h) \circ d\varphi.$$

PROOF. Write $\varphi = (\varphi_{ij})_{i,j=1}^m$, so $d\varphi = (d\varphi_{ij})_{i,j=1}^m$, where

$$d\varphi_{ij}(x) = \sum_{k,l} x_{kl} \frac{\partial}{\partial t_{kl}} \varphi_{ij}(g) \Big|_{g=e}.$$

Further we have

$$\varphi_{ij}(hgh^{-1}) = (\varphi(h)\varphi(g)\varphi(h^{-1}))_{ij} = \sum_{u,v} \varphi_{iu}(h)\varphi_{uv}(g)\varphi_{vj}(h^{-1}).$$

Putting these two together gives

$$d\varphi_{ij}(h x h^{-1}) = (\varphi(h)d\varphi(x)\varphi(h^{-1}))_{ij}$$

and the assertion of the proposition follows. \square

CHAPTER 3

Automorphisms of a variety

This chapter gives a theoretical “basement” for the parametrization method. We introduce the Lie algebra of a variety and give an algorithm for computing it. We will see that k -isomorphic varieties have k -isomorphic Lie algebras. We analyze also the other implication: If two \bar{k} -isomorphic varieties have k -isomorphic Lie algebras, are then these varieties isomorphic also over k ? And how can an isomorphism of Lie algebras be used for finding an isomorphism of the varieties?

1. The Lie algebra of the variety

Let $X \subseteq \mathbb{P}^n$ be an embedded projective variety so that $\mathcal{I}(X) \subset k[x_0, \dots, x_n]$. We define the following linear group:

$$G(X, k) = \{g \in \mathbf{GL}_n(k) \mid f(gp) = 0 \ \forall p \in X \ \forall f \in \mathcal{I}(X)\}.$$

Then the projectivization $\mathbb{P}G(X, k) = G(X, k)/kI_n$, where I_n is the identity matrix, are exactly the automorphisms of \mathbb{P}^n fixing X . Since $G(X, k)$ is described by polynomials, it is an algebraic group, so it has a Lie algebra which we denote $\mathfrak{g}(X, k)$.

DEFINITION 3.1. Let $X \subseteq \mathbb{P}^n$ and let $\mathfrak{g}(X, k)$ be the Lie algebra of $G(X, k)$. We define $\mathfrak{g}_0(X, k) = \mathfrak{g}(X, k)/kI_n$, where $I_n \in \mathfrak{gl}_n(k)$ is the identity matrix. We call $\mathfrak{g}_0(X, k)$ the Lie algebra of the (embedded) variety $X(k)$.

Of course $\mathfrak{g}_0(X, k)$ by this definition depends on the embedding of X . Moreover $\mathbb{P}G(X, k)$ can be a very small subgroup of all automorphisms of X :

EXAMPLE 3.2. Let $C = \mathcal{V}(x^3 + y^3 + z^3 - 3mxyz) \subset \mathbb{P}^2$ with $m^3 \neq 1$, be a curve over $k = \overline{\mathbb{Q}}$. Then C is an elliptic curve, so $\{\alpha_p: C \rightarrow C, q \mapsto pq \mid \forall p \in C\}$ is a continuous subgroup of its automorphisms. Nevertheless, there are only finitely many linear transformations of \mathbb{P}^2 fixing C , as each such transformation has to fix the set of 9 flexes of C . Finally, since $G(C, k)$ is discrete, the Lie algebra of C is trivial.

By $\text{Aut}(X)$ we denote the group of automorphisms of X . To be able to study the structure of $G(X, k)$, we next introduce a subgroup of $\text{Aut}(X)$, which is independent on

the embedding of X :

$$\mathrm{Aut}_0(X) = \{\varphi \in \mathrm{Aut}(X) \mid \varphi^* \text{ acts trivially on } \mathrm{Pic}(X)\}.$$

THEOREM 3.3. *Let X be embedded into \mathbb{P}^n by a map associated to a very ample divisor D on X . Then $\mathrm{Aut}_0(X)$ is embedded into $\mathbb{P}G(\iota_D(X), k)$ as an algebraic variety.*

PROOF. Let D be a very ample divisor, f_0, f_1, \dots, f_n a basis of the Riemann-Roch space $\mathcal{L}(D)$, so $(f_0 : f_1 : \dots : f_n)$ is the associated embedding $\iota_D: X \hookrightarrow \mathbb{P}^n$.

Let $\alpha \in \mathrm{Aut}_0(X)$. Then the pullback $\alpha^*: \mathrm{Div} X \rightarrow \mathrm{Div} X$ maps D into $D - (g)$ for some $g \in k(X)$. Further, the image of an effective divisor under α is again effective. So for $f \in \mathcal{L}(D)$ we have $\alpha^*(D + (f)) = D + (g^{-1}f \circ \alpha) \geq 0$. It follows that $f \mapsto g^{-1}f \circ \alpha$ is a projective transformation of $\mathcal{L}(D)$, i.e. there are $c_{ij} \in k$ such that $g^{-1}f_i \circ \alpha = \sum_{j=0}^n c_{ij} f_j$. Now by assumption $(f_0 : \dots : f_n)$ is the embedding of $X \hookrightarrow \mathbb{P}^n$. Then $\alpha(X)$ is embedded by $(f_0 \circ \alpha : \dots : f_n \circ \alpha) = (g \sum_j c_{0j} f_j : \dots : g \sum_j c_{nj} f_j) = (\sum_j c_{0j} f_j : \dots : \sum_j c_{nj} f_j)$.

Since f_0, \dots, f_n are linearly independent, $\iota_D(X) \subseteq \mathbb{P}^n$ is not contained in any hyperplane. Therefore a transformation of \mathbb{P}^n fixing X pointwise is the identity on \mathbb{P}^n . Hence $\mathrm{Aut}_0(X)$ is injectively mapped into $\mathbf{PGL}_{n+1}(k)$.

Finally, the set of elements $(c_{ij})_{i,j=0}^n \in \mathbf{PGL}_{n+1}(k)$ in the image of $\mathrm{Aut}_0(X)$ is the zero set of polynomials obtained from the ideal generated by $f_i \circ \alpha = g \sum_{j=0}^n x_{ij} f_j$ for $i = 0, \dots, n$, after eliminating all unknowns except x_{ij} 's. So $\mathrm{Aut}_0(X)$ is indeed an algebraic variety. \square

We have seen that the group $\mathrm{Aut}_0(X)$ is algebraic, therefore we can define the Lie algebra of an abstract variety.

DEFINITION 3.4. *The Lie algebra of a variety X such that X has a very ample divisor is the Lie algebra of the algebraic group $\mathrm{Aut}_0(X)$.*

Note that the Lie algebra of an abstract variety X and the Lie algebra of its embedding using a very ample divisor D might differ. Indeed, the image of the group $\mathrm{Aut}_0(X)$ after the embedding ι_D is only a subgroup of (not equal to) $\mathbb{P}G(\iota_D(X), k)$, so the Lie algebra of X can happen to be only a subalgebra of $\mathfrak{g}_0(X, k)$. Nevertheless, in all examples considered in our work these two algebras are isomorphic.

EXAMPLE 3.5. Let $X = \mathbb{P}^n$, $n > 0$, so $\mathrm{Pic}(X) \cong \mathbb{Z}$. Every automorphism of \mathbb{P}^n fixes the Picard group. It follows that $\mathrm{Aut}_0(X) = \mathrm{Aut}(X) = \mathbf{PGL}_{n+1}(k)$, therefore for the Lie algebras we have $\mathfrak{g}(X, k) = \mathfrak{gl}_{n+1}(k)$, and $\mathfrak{g}_0(X, k) = \mathfrak{sl}_{n+1}(k)$.

EXAMPLE 3.6. Let $X = \mathbb{P}^1 \times \mathbb{P}^1$, so $\mathrm{Pic} X \cong \mathbb{Z}^2$. For automorphisms we have $\mathrm{Aut}(\mathbb{P}^1 \times \mathbb{P}^1) = G_1 \times G_2 \rtimes \langle g_0 \rangle$, where $G_1, G_2 \cong \mathbf{PGL}_2(k)$ and g_0 switches the \mathbb{P}^1 's: $g_0 : (s_0 : s_1; t_0 : t_1) \mapsto (t_0 : t_1; s_0 : s_1)$.

The Segre embedding $X \hookrightarrow \mathbb{P}^3$, $(s_0 : s_1; t_0 : t_1) \mapsto (s_0 t_0 : s_0 t_1 : s_1 t_0 : s_1 t_1)$ is the map associated to a divisor of bidegree $(1, 1)$. Here also the automorphism g_0 is represented by a matrix in $\mathbf{PGL}_4(k)$. We conclude that $\text{Aut}(X) = \{g \in \mathbf{PGL}_4(k) \mid gp \in X \ \forall p \in X\}$. The same holds for the anticanonical embedding of $\mathbb{P}^1 \times \mathbb{P}^1$, which is the map associated to a divisor of bidegree $(2, 2)$.

Finally, $\text{Aut}_0(\mathbb{P}^1 \times \mathbb{P}^1) = G_1 \times G_2$ is a subgroup of $\text{Aut}(\mathbb{P}^1 \times \mathbb{P}^1)$ of finite index, therefore the Lie algebras of an abstract variety (as in Definition 3.4) and the embedded ones (as in Definition 3.1) coincide.

EXAMPLE 3.7. Let X be the blowup of \mathbb{P}^2 in $(1 : 0 : 0)$. Then $\text{Pic } X \cong \mathbb{Z}^2$. Every automorphism of X fixes the exceptional line. More precisely, $\text{Aut}(X)$ is a subgroup of $\text{Aut}(\mathbb{P}^2)$ fixing the point $(1 : 0 : 0)$. Therefore $\text{Pic } X$ is fixed by $\text{Aut}(X)$, hence $\text{Aut}(X) = \text{Aut}_0(X)$.

2. Computing $\mathfrak{g}_0(X, k)$

The reason why we define the Lie algebra for an embedded variety is, that such definition immediately delivers also tools for computing $G(X, k)$ and $\mathfrak{g}_0(X, k)$.

Let $\mathcal{I}(X) \subset k[x_0, \dots, x_n]$ be the vanishing ideal of $X \subset \mathbb{P}^n$ and let $\mathcal{B} = \{f_1, \dots, f_k\}$ be a finite set of homogeneous equations generating $\mathcal{I}(X)$. For $g = (g_{ij})_{i,j=1}^{n+1} \in \mathbf{GL}_{n+1}(k)$ we have that

$$\begin{aligned} g \in G(X, k) &\Leftrightarrow f(gp) = 0 \text{ for all } p \in X \text{ and } f \in \mathcal{I} \\ &\Leftrightarrow f \circ g \in \mathcal{I}(X) \text{ for each } f \in \mathcal{B}. \end{aligned}$$

The last expression is valid if $f = \sum a_i f_i$ with $a_i \in k[x_0, \dots, x_n]$ homogeneous and $f_i \in \mathcal{B}$ such that $\deg f_i \leq \deg f$. For each $f \in \mathcal{B}$ therefore we form the following set of polynomials: $\mathcal{S} = \{x^u f_i \mid f_i \in \mathcal{B}, \deg f_i \leq \deg f, |u| = \deg f - \deg f_i\}$, where u is the vector $(u_0, \dots, u_n) \in \mathbb{N}^{n+1}$, $|u| = u_0 + \dots + u_n$ and x^u is a shortcut for $x_0^{u_0} \dots x_n^{u_n}$. Then $f \circ g \in \mathcal{I}(X)$ if $f \circ g = \sum_{h_j \in \mathcal{S}} c_j h_j$ for some c_j 's in k . In this way for each $f \in \mathcal{B}$ we get a polynomial equation in g_{ij} 's and c_j 's defining together an (affine) algebraic variety. Then $G(X, k)$ is its projection discarding all c_j 's. Let J denote the ideal obtained in this way, i.e. $G(X, k) = \mathcal{V}(J)$. To find the Lie algebra of X we have further to compute the radical \sqrt{J} and differentiate its generators.

In the examples we are interested in, the ideal of the variety X is generated by quadratic equations. In this case, we have much more straightforward method for computing the Lie algebra of X .

LEMMA 3.8. *Let $\pi: G \rightarrow \mathbf{GL}(V)$ be a rational representation, and let $N \subset M$ be vector subspaces of V . Put*

$$H = \{g \in G \mid \pi(g)N = N, \pi(g)M = M, \pi(g)_{M/N} = e\}.$$

Then

$$L(H) = \{x \in \mathfrak{g} \mid d\pi(x)M \subset N\}.$$

PROOF. See [Bor91], Lemma 7.4. □

THEOREM 3.9. *Let $X \subset \mathbb{P}^n$ be embedded such that the ideal of X is generated by quadrics $z^t A_i z$, $i = 1, \dots, r$, where A_i 's are symmetric matrices of degree $n + 1$, and $z = (z_0 \ z_1 \ \dots \ z_n)^t$. Let $\mathcal{A} \subset M_{n+1}(k)$ denote the subspace generated by all A_i 's. Then*

$$\mathfrak{g}(X, k) = \{x \in \mathfrak{gl}_{n+1}(k) \mid x^t A_i + A_i x \in \mathcal{A} \ \forall i\}.$$

PROOF. First we describe $G(X, k)$. Let $\lambda_1, \dots, \lambda_s$ be linear forms defining the subspace $\mathcal{A} \subset M_{n+1}(k)$. By definition of $G(X, k)$ for $g \in \mathbf{GL}_{n+1}(k)$ we then have

$$\begin{aligned} g \in G(X, k) &\Leftrightarrow z^t (g^t A_k g) z \in \mathcal{I}(X) \quad \forall k \\ &\Leftrightarrow g^t A_k g \in \mathcal{A} \quad \forall k \\ &\Leftrightarrow \lambda_l (g^t A_k g) = 0 \quad \forall k, \forall l. \end{aligned}$$

So $G(X, k)$ is described by kl quadratic forms in $k[g_{ij} \mid i, j = 0, \dots, n]$.

Except acting on \mathbb{P}^n , $\mathbf{GL}_{n+1}(k)$ acts also on the space $M_{n+1}(k)$ by $g(A) = g^t A g$. Then $G(X, k)$ is exactly the subgroup of $\mathbf{GL}_{n+1}(k)$ fixing \mathcal{A} .

Let $m = (n+1)^2 = [M_{n+1}(k) : k]$. Let V be m -dimensional vector space representing matrices in $M_{n+1}(k)$. We will write v_A for the vector in V representing the matrix A . Let π be the representation of $\mathbf{GL}_{n+1}(k) \rightarrow \mathbf{GL}_m(k)$, so $\pi(g)v_A = v_{g^t A g}$. If we set $M = N = \mathcal{A}$, then by Lemma 3.8 the Lie algebra of $G(X, k)$ is

$$L(G) = \{x \in \mathfrak{gl}_{n+1}(k) \mid d\pi(x)\mathcal{A} \subset \mathcal{A}\}.$$

It remains to compute the differential of π .

For $A = (A_{ij})_{i,j=0}^n \in M_{n+1}(k)$ let v_A be the vector $(A_{00}, A_{01}, \dots, A_{0n}, A_{10}, \dots, A_{nn})^t$. The coordinates in v_A are naturally indexed by vectors: $(v_A)_{(i,j)} = A_{ij}$. Then for $g = (g_{ij})_{i,j=0}^n \in \mathbf{GL}_{n+1}(k)$ we have $(\pi(g))_{(i,j)(k,l)} = g_{ki} g_{lj}$. By differentiating in this

coordinate we get

$$\begin{aligned} (d\pi(x))_{u,v} &= \left(x_{ki} \frac{\partial}{\partial g_{ki}} + x_{lj} \frac{\partial}{\partial g_{lj}} \right) g_{ki} g_{lj} \Big|_{g=e} = (x_{ki} g_{lj} + x_{lj} g_{ki}) \Big|_{g=e} \\ &= x_{ki} g_{lj} + x_{lj} g_{ki} \Big|_{g=e} = \begin{cases} x_{ii} + x_{jj} & \text{if } i = k, j = l \\ x_{lj} & \text{if } i = k, j \neq l \\ x_{ki} & \text{if } i \neq k, j = l \\ 0 & \text{if } i \neq k, j \neq l. \end{cases} \end{aligned}$$

The last tedious computation shows that $(d\pi(x)v_A)_u = (v_{(xA^t+Ax)})_u$ for all $u = 1, \dots, m$ and the assertion of the theorem follows. \square

EXAMPLE 3.10. Let $X \subset \mathbb{P}^2$ be the zero set of $z_0^2 + z_1^2 + z_2^2$ and let $k = \mathbb{Q}$. Though $X(\mathbb{Q}) = \emptyset$, there are still automorphisms of X defined over \mathbb{Q} . We find the Lie algebra $\mathfrak{g}(X, \mathbb{Q})$.

The group $G(X, \mathbb{Q})$ consists of $g \in \mathbf{GL}_3(\mathbb{Q})$ such that $g^t I_3 g = \lambda I_3$ for some $\lambda \in \mathbb{Q}$ where I_3 is the identity matrix. Therefore

$$\mathfrak{g}(X, \mathbb{Q}) = \{x \in \mathfrak{gl}_3(\mathbb{Q}) \mid x^t + x = \lambda I_3 \text{ for some } \lambda \in \mathbb{Q}\},$$

so it is generated by all antisymmetric matrices together with I_3 .

3. Varieties and modules

Let $X_1, X_2 \subseteq \mathbb{P}^n$ be two varieties which are projectively equivalent over k , i.e. there is $\mu: k^{n+1} \rightarrow k^{n+1}$ (and consequently $\mathbb{P}^n \rightarrow \mathbb{P}^n$) given by a matrix $M \in \mathbf{GL}_{n+1}(k)$ such that

$$(1) \quad \mu: p \mapsto Mp \text{ for all } p \in \mathbb{P}^n \text{ and } \mu(X_1) = X_2.$$

Then μ induces a map $\tilde{\mu}: G(X_1, k) \rightarrow G(X_2, k)$ such that the following diagram is commutative:

$$\begin{array}{ccc} X_1 & \xrightarrow{\mu} & X_2 \\ \downarrow g & & \downarrow \tilde{\mu}(g) \\ X_1 & \xrightarrow{\mu} & X_2 \end{array}$$

i.e. $\tilde{\mu}(g) = \mu \circ g \circ \mu^{-1}$. It is straightforward to see that $\tilde{\mu}$ is an isomorphism of groups, mapping g to MgM^{-1} .

PROPOSITION 3.11. *Suppose that X_1 and $X_2 \subseteq \mathbb{P}^n$ are projectively equivalent over k and let M be the matrix as in (1). Then*

- (i) the map $d\tilde{\mu}: x \mapsto MxM^{-1}$ is a Lie algebra isomorphism from $\mathfrak{g}(X_1, k)$ to $\mathfrak{g}(X_2, k)$,
- (ii) $\mu: V_1 \rightarrow V_2, v \mapsto Mp$ is an isomorphism of $(n+1)$ -dimensional natural modules of $\mathfrak{g}_0(X_1, k)$ and $\mathfrak{g}_0(X_2, k)$.

PROOF. The first assertion follows from Proposition 2.17 and the fact that $\tilde{\mu}: g \mapsto MgM^{-1}$ is an isomorphism from $G(X_1, k)$ to $G(X_2, k)$.

The second assertion follows from Corollary 2.18 and the fact that the restriction of φ_L to $\mathfrak{g}_0(X_1, k)$ leads to an isomorphism of $\mathfrak{g}_0(X_1, k)$ and $\mathfrak{g}_0(X_2, k)$. \square

For our purposes, a converse of the last proposition is more useful. Namely, given two algebraic varieties in \mathbb{P}^n , if we can find an isomorphism of their Lie algebras and corresponding modules, can we “lift” it to an isomorphism of the varieties, provided it exists? The following proposition gives a partial answer.

PROPOSITION 3.12. *Suppose that X_1 and X_2 in \mathbb{P}^n are projectively equivalent over k . Assume further that any automorphism of $\mathfrak{g}_0(X_1, k)$ is a conjugation by a matrix from $G(X_1, k)$. Then any isomorphism $\psi: \mathfrak{g}_0(X_1, k) \rightarrow \mathfrak{g}_0(X_2, k)$ leads to an isomorphism ν of their modules. If $N \in M_{n+1}(k)$ is the matrix such that $\nu: v \mapsto Nv$ then the matrix N moreover defines a projective equivalence $X_1 \rightarrow X_2, p \mapsto Np$.*

PROOF. By assumption there is a matrix $M \in \mathbf{GL}_{n+1}(k)$ describing a projective equivalence of X_1 and X_2 , as in (1). By Proposition 3.11 it leads to an isomorphism $d\tilde{\mu}$ of Lie algebras $\mathfrak{g}_0(X_1, k) \rightarrow \mathfrak{g}_0(X_2, k)$ mapping x to MxM^{-1} . Then $d\tilde{\mu}^{-1} \circ \psi$ is an automorphism of $\mathfrak{g}_0(X_1, k)$. By assumption there exists $G \in G(X_1, k)$ such that

$$d\tilde{\mu}^{-1} \circ \psi(x) = GxG^{-1}.$$

It follows that

$$\psi(x) = d\tilde{\mu}(GxG^{-1}) = (MG)x(MG)^{-1}.$$

Hence ψ also leads to an isomorphism of modules, namely $v \mapsto MGv$, so $N = MG$. Finally, the matrix N describes the composition of an automorphism of X_1 and the projective equivalence of X_1 and X_2 , hence the last assertion follows. \square

The last proposition gives an algorithm for deciding existence and finding a linear projective isomorphism of two algebraic varieties provided their Lie algebras satisfy its assumptions:

ALGORITHM: **FindProjectiveEquivalence**

INPUT: $X_1, X_2 \subseteq \mathbb{P}^n$ – projective varieties defined over k such that each automorphism of $\mathfrak{g}_0(X_1, k)$ is a conjugation by a matrix from $G(X_1, k)$,

OUTPUT: $M \in \mathbf{GL}_{n+1}(k)$ such that $Mp \in X_2$ for all $p \in X_1$ if such M exists, **failed** otherwise.

- (1) Compute $\mathfrak{g}_0(X_1, k)$ and $\mathfrak{g}_0(X_2, k)$ as described in Section 2.
- (2) Find a Lie algebra isomorphism $\psi: \mathfrak{g}_0(X_1, k) \rightarrow \mathfrak{g}_0(X_2, k)$. If such isomorphism does not exist, return **failed**.
- (3) Construct an isomorphism μ between the modules V_1 and V_2 of algebras $\mathfrak{g}_0(X_1, k)$ and $\mathfrak{g}_0(X_2, k)$, $\mu: v \mapsto Mv$ for some $M \in \mathbf{GL}_{n+1}(k)$. If such isomorphism does not exist, return **failed**.
- (4) If μ transforms X_1 to X_2 , return M . Otherwise return **failed**.

We will use this algorithm for finding a parametrization of a given variety. More precisely, as the variety X_1 we take a variety with known parametrization. Then we find an isomorphism of X_1 and an implicitly given variety X_2 , obtaining so a parametrization of the latter. Next we illustrate the parametrization algorithm in detail on a simple example of conics.

4. Illustrating example: \mathbb{P}^1 and \mathfrak{sl}_2

Of course there is a lot of ways how to parametrize a given conic. But for the sake of simplicity we use this easy example to illustrate our method.

We will find a parametrization of a conic $C \subset \mathbb{P}^2$ given by a quadratic form in $k[z_0, z_1, z_2]$. We will do so by finding an isomorphism of C and $C_0: z_0z_2 - z_1^2$, where C_0 has a parametrization $(s : t) \mapsto (s^2 : st : t^2)$.

The automorphism group of $\mathbb{P}^1(k)$ is $\mathbf{PGL}_2(k)$, therefore we have $G(\mathbb{P}^1, k) \cong \mathbf{GL}_2(k)$ and the Lie algebra $\mathfrak{g}(\mathbb{P}^1, k) = L(\mathbf{GL}_2(k)) = \mathfrak{gl}_2(k)$. If we factor out the one dimensional subalgebra spanned by the identity matrix, we get

$$\mathfrak{g}_0(\mathbb{P}^1, k) \cong \mathfrak{sl}_2(k).$$

If C has a k -rational parametrization (or equivalently C is over k projectively equivalent to C_0), then also the Lie algebra $\mathfrak{g}_0(C, k)$ is isomorphic to $\mathfrak{sl}_2(k)$.

Next we need to check the assumption of Proposition 3.12. Firstly, Theorem 2.6 asserts that any automorphism of $\mathfrak{sl}_2(k)$ is a conjugation by a regular 2×2 matrix.

We will now examine the conic C_0 . Let v_0, v_1 be the standard basis of $V = k^2$. Let $W = \text{Sym}^2(V)$ with the basis $v_0^2, 2v_0v_1, v_1^2$. Let $\varphi'_0: V \rightarrow W$ be defined by $\varphi'_0(v) = v^2$.

We write the coordinates of an element in W with respect to the basis above. Then the image of the induced map $\varphi_0: \mathbb{P}(V) \rightarrow \mathbb{P}(W)$ in these coordinates is exactly C_0 (see also [FH91], §11.3). The group $G(\mathbb{P}^1, k) = \mathbf{GL}_2(k)$ acts on W by $g \cdot (v_1 v_2) = (g v_1)(g v_2)$. It follows that an automorphism of \mathbb{P}^1 represented by the matrix $g = (g_{ij})_{i,j=0,1}$,

$$gp = \begin{pmatrix} g_{00} & g_{01} \\ g_{10} & g_{11} \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix},$$

is by the parametrization $\varphi_0: (s : t) \mapsto (s^2 : st : t^2)$ transformed to a linear automorphism of \mathbb{P}^2 fixing C_0 :

$$g \cdot \varphi_0(p) = \tilde{\varphi}_0(g)\varphi_0(p) = \begin{pmatrix} g_{00}^2 & 2g_{00}g_{01} & g_{01}^2 \\ g_{00}g_{10} & g_{00}g_{11} + g_{01}g_{10} & g_{01}g_{11} \\ g_{10}^2 & 2g_{10}g_{11} & g_{11}^2 \end{pmatrix} \begin{pmatrix} p_0^2 \\ p_0 p_1 \\ p_1^2 \end{pmatrix},$$

so $\tilde{\varphi}_0$ is a group homomorphism $G(\mathbb{P}^1, k) = \mathbf{GL}_2(k) \rightarrow \mathbf{GL}_3(k)$. The differential of $\tilde{\varphi}_0$ maps the Lie algebra of $G(\mathbb{P}^1, k)$ isomorphically to the Lie algebra of $G(C_0, k)$. It describes the action of the Lie algebra of $G(\mathbb{P}^1, k)$ on W , $x \cdot (v_1 v_2) = d\tilde{\varphi}_0(x)(v_1 v_2) = (x v_1)v_2 + v_1(x v_2)$. Explicitly it is given by

$$(2) \quad d\tilde{\varphi}_0: \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \mapsto \begin{pmatrix} 2a_{00} & 2a_{01} & 0 \\ a_{10} & a_{00} + a_{11} & a_{01} \\ 0 & 2a_{10} & 2a_{11} \end{pmatrix}$$

and maps isomorphically $\mathfrak{sl}_2(k) \rightarrow \mathfrak{g}_0(C_0, k)$.

From Theorem 2.6 and Proposition 2.19 now follows that the algorithm `FindProjectiveEquivalence` can be used to parametrize a given conic C .

In the second step of the algorithm we have to find an isomorphism ψ of Lie algebras of C_0 and C . We have already constructed an isomorphism $d\tilde{\varphi}_0: \mathfrak{sl}_2 \rightarrow \mathfrak{g}_0(C_0, k)$, (see (2)). Therefore it is enough to find an isomorphism $d\tilde{\varphi}: \mathfrak{sl}_2 \rightarrow \mathfrak{g}_0(C, k)$ * and compose $\psi = d\tilde{\varphi} \circ (d\tilde{\varphi}_0)^{-1}$. Finding an isomorphism between Lie algebras is usually the most difficult part of the algorithm, and is discussed in Chapter 6. Nevertheless, assume for now that we can find $d\tilde{\varphi}$. Then the last construction to be made is finding an isomorphism between 3-dimensional natural modules of $\mathfrak{g}_0(C_0, k)$ and $\mathfrak{g}_0(C, k)$.

LEMMA 3.13. *The 3-dimensional \mathfrak{sl}_2 -module afforded by the representation $d\tilde{\varphi}_0: \mathfrak{sl}_2 \rightarrow \mathfrak{g}_0(C_0, k)$ is irreducible with highest weight 2.*

*The prefix “d” in the name of the map $d\tilde{\varphi}$ suggests that $d\tilde{\varphi}$ is a differential of a map between algebraic groups. This indeed is true, nevertheless we don’t prove and don’t use this fact. We look for the map $d\tilde{\varphi}$ independently on that.

PROOF. We have already seen that the 3-dimensional $\mathfrak{g}_0(C_0, k)$ -module is isomorphic to $\text{Sym}^2(V)$, and therefore it is irreducible. The highest weight of this module is 2. \square

Let us fix a Chevalley basis of $\mathfrak{g}_0(C_0, k)$ to be the image of the standard Chevalley basis in $\mathfrak{sl}_2(k)$ under $d\tilde{\varphi}_0$:

$$(3) \quad x_0 = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad y_0 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}, \quad h_0 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

Then the highest weight vector in the $\mathfrak{g}_0(C_0, k)$ -module is

$$(4) \quad v_0^+ = e_1,$$

where by e_i we denote the 3-dimensional column vector with 1 at the i -th place and 0 elsewhere. For the rest of the module we get

$$(5) \quad y_0 \cdot v_0^+ = e_2 \quad \text{and} \quad y_0 \cdot (y_0 \cdot v_0^+) = 2e_3.$$

REMARK 3.14. Surely, the computation just made also shows that the natural $\mathfrak{g}_0(C_0, k)$ -module is irreducible. Nevertheless the conceptual argumentation about the structure of the module is preferable since it easily generalizes to varieties of higher dimension, where the explicit computation would be too lengthy.

The conic C is given implicitly, therefore we have to find its Lie algebra $\mathfrak{g}_0(C, k) \subset \mathfrak{sl}_3(\mathbb{Q})$ by solving the linear system according to Theorem 3.9, and intersecting with $\mathfrak{sl}_3(\mathbb{Q})$.

PROPOSITION 3.15. *The conic $C \subset \mathbb{P}^2$ defined over k has a k -rational parametrization if and only if $\mathfrak{g}_0(C, k) \cong \mathfrak{sl}_2(k)$.*

PROOF. If C has a parametrization over k , then it is projectively equivalent to C_0 (C_0 as above) and hence by Proposition 3.11, $\mathfrak{g}_0(C, k) \cong \mathfrak{sl}_2(k)$.

Let on the other hand $\mathfrak{g}_0(C, k) \cong \mathfrak{sl}_2(k)$. Let $k' \supseteq k$ be a field extension such that C has a k' -rational parametrization. Then the natural modules of $\mathfrak{g}_0(C, k')$ and $\mathfrak{g}_0(C_0, k')$ are two isomorphic $\mathfrak{sl}_2(k')$ -modules. Hence the natural $\mathfrak{g}_0(C, k')$ -module is irreducible with the highest weight 2. But $\mathfrak{g}_0(C, k)$ has a split Cartan subalgebra, therefore the corresponding highest weight vector in the natural $\mathfrak{g}_0(C, k')$ -module is defined over k and so is the isomorphism of modules and of C_0 and C . \square

We can assume that the Lie algebra $\mathfrak{g}_0(C, k) \cong \mathfrak{sl}_2(k)$ since otherwise C does not have a k -rational parametrization. From the proposition it follows that if there is an

isomorphism $\mathfrak{sl}_2 \rightarrow \mathfrak{g}_0(C, k)$, then also the natural $\mathfrak{g}_0(C_0, k)$ - and $\mathfrak{g}_0(C, k)$ -modules are k -isomorphic. Suppose we can find a Chevalley basis x, y, h in $\mathfrak{g}_0(C, k)$, which is equivalent to finding an isomorphism with $\mathfrak{sl}_2(k)$. We find then a module isomorphism by finding the highest weight vector v^+ in the natural $\mathfrak{g}_0(C, k)$ -module and mapping $v_0^+ \mapsto v^+$, $y_0 \cdot v_0^+ \mapsto y \cdot v^+$ and $y_0 \cdot (y_0 \cdot v_0^+) \mapsto y \cdot (y \cdot v^+)$.

EXAMPLE 3.16. Let us parametrize the unit circle $C \subset \mathbb{P}^2$ given by the polynomial $z_1^2 + z_2^2 - z_0^2$ or, equivalently by the diagonal matrix $A \in M_3(\mathbb{Q})$ with entries $(-1, 1, 1)$.

We find $\mathfrak{g}_0(C, \mathbb{Q}) \subset \mathfrak{sl}_3(\mathbb{Q})$ by solving the linear system $x^t A + Ax \in \text{span}_{\mathbb{Q}}\{A\}$ for $x \in \mathfrak{sl}_3(\mathbb{Q})$. A Chevalley basis of $\mathfrak{g}_0(C, \mathbb{Q})$ is for example

$$x = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The maximal weight vector and the derived vectors in the natural $\mathfrak{g}_0(C, k)$ -module are

$$v^+ = e_1 + e_2, \quad y \cdot v^+ = 2e_3 \quad \text{and} \quad y \cdot (y \cdot v^+) = 2(e_1 - e_2).$$

Comparing with (4) and (5) yields that the matrix of an isomorphism of modules is

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 2 & 0 \end{pmatrix},$$

which gives a parametrization of the circle

$$\begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix} = \begin{pmatrix} s^2 + t^2 \\ s^2 - t^2 \\ 2st \end{pmatrix}.$$

5. Conics and their Lie algebras

Here we explain how to use the known algorithms for parametrizing conics when we want to find an isomorphism of a Lie algebra and \mathfrak{sl}_2 .

In the previous example the unexplained step in the algorithm was finding an isomorphism $\mathfrak{sl}_2(\mathbb{Q}) \rightarrow \mathfrak{g}_0(C, \mathbb{Q})$. This is as difficult as finding a rational point on a conic. There are already efficient algorithms for solving the latter (cf. [CR03, Sim05]), some even implemented in Magma. Therefore in the case of conics we usually do a reduction in the other direction: If for a given Lie algebra \mathfrak{g} over \mathbb{Q} we have to find an isomorphism $\mathfrak{sl}_2(\mathbb{Q}) \rightarrow \mathfrak{g}$, then we first find a conic C such that \mathfrak{g} is isomorphic to its Lie algebra, and afterwards we use the known fast algorithms for finding a rational point on C and consequently a parametrization of C , which will lead to constructing an isomorphism of

\mathfrak{g} and $\mathfrak{sl}_2(\mathbb{Q})$. We have to show that for each \mathfrak{g} which is a twist of \mathfrak{sl}_2 it is possible to construct a corresponding conic.

Here again $C_0 \subset \mathbb{P}^2$ is the conic given by the form $z_0z_2 - z_1^2$ and parametrized by monomials $(s : t) \mapsto (s^2 : st : t^2)$.

LEMMA 3.17. *Let \mathfrak{g} be a twist of $\mathfrak{sl}_2(\mathbb{Q})$. There is a basis h, x, y of \mathfrak{g} such that the multiplication in \mathfrak{g} is given by $[h, x] = y$, $[h, y] = ax$, $[x, y] = bh$ for some $a, b \in \mathbb{Q}^*$.*

PROOF. Since \mathfrak{g} is a twist of $\mathfrak{sl}_2(\mathbb{Q})$, it has a 1-dimensional Cartan subalgebra. Let h spans a Cartan subalgebra of \mathfrak{g} . Then we do a Fitting decomposition, $\mathfrak{g} = \text{span}_{\mathbb{Q}}\{h\} + [h, \mathfrak{g}]$. The subalgebra $[h, \mathfrak{g}]$ is generated by two vectors x, y , where x is chosen not to be an eigenvector of $\text{ad } h$, and $y = [h, x]$. Then we also have $[x, y] = bh$ and $[h, y] = ax$ with both $a, b \in \mathbb{Q}$ nonzero. The first multiplication rule can be seen after passing to a splitting field of \mathfrak{g} , the second follows from Jacobi identity. \square

If the Cartan subalgebra, which we find while looking for a basis as in the last lemma, happens to be split, we are done, because we can easily find an isomorphism with $\mathfrak{sl}_2(\mathbb{Q})$, for example by using the method of [dG00], §5.11. Otherwise we continue with the computation.

The adjoint representation of \mathfrak{g} with respect to this basis is a representation by the following 3 by 3 matrices over the rationals:

$$\text{ad } x = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & b & 0 \end{pmatrix}, \quad \text{ad } y = \begin{pmatrix} 0 & 0 & -a \\ 0 & 0 & 0 \\ -b & 0 & 0 \end{pmatrix}, \quad \text{ad } h = \begin{pmatrix} 0 & a & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

It is a straightforward computation to check that this is the Lie algebra of the conic C given by

$$(6) \quad -bz_0^2 + abz_1^2 + az_2^2 = 0, \quad a, b \in \mathbb{Q}^*$$

We use known algorithms to find a rational point on C . If there is none, by Proposition 3.15 the given Lie algebra \mathfrak{g} was a proper twist of \mathfrak{sl}_2 . Otherwise we can construct a Lie algebra isomorphism.

LEMMA 3.18. *Let $(p_0 : p_1 : p_2)$ be a point on the conic*

$$(7) \quad Az_0^2 + Bz_1^2 + Cz_2^2 = 0,$$

such that p_2 is nonzero. Then we have the following parametrization:

$$\begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} Ap_0 & 2Bp_1 & -Bp_0 \\ -Ap_1 & 2Ap_0 & Bp_1 \\ Ap_2 & 0 & Bp_2 \end{pmatrix} \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix}$$

PROOF. Direct verification proves the lemma. When looking for the matrix, we followed the method described in [Mor69]: One looks for the parametrization in the shape $(z_0 : z_1 : z_2) = (s + p_0w : t + p_1w : p_2w)$ and eliminates w . \square

By plugging in $-b, ab, a$ for A, B, C in the lemma we have constructed an isomorphism of C and the conic C_0 given by $z_0z_2 - z_1^2$. Let us denote the matrix describing the isomorphism by M , i.e. for every $p \in C_0$ we have $Mp \in C$. Let x_0, y_0, h_0 be as in (3). Then by Proposition 3.11(i), Mx_0M^{-1} , My_0M^{-1} and Mh_0M^{-1} is a Chevalley basis of \mathfrak{g} , so we have constructed an isomorphism $\mathfrak{sl}_2(\mathbb{Q}) \rightarrow \mathfrak{g}$.

REMARK 3.19. Taking the adjoint representation with respect to the basis as in Lemma 3.17 leads to constructing a conic in the diagonal shape. As pointed out to us by Michael Stoll, this usually introduces additional difficulties when looking for a rational point on the conic (one has to factorize too large integers). Therefore in our algorithms we do not look for the special basis of the Lie algebra but immediately construct the adjoint representation, and then the corresponding conic by solving the linear system in the Theorem 3.9 for an unknown matrix A . The results in this section assure that there is always a conic corresponding to the adjoint representation of the Lie algebra.

6. Variety as an orbit of an algebraic group

The core theorem in the example of the conic (see Section 4) is the first part of Theorem 2.6 saying that each automorphism of \mathfrak{sl}_2 (represented as 2×2 matrices of trace 0) is a conjugation by a regular matrix. Unfortunately this is not true for all algebras appearing in examples we would consider. Therefore in this section we develop another machinery to prove an assertion similar to one in Proposition 3.12.

Let G be an algebraic group and let the variety X be a G -set, i.e. there is an action $G \times X \rightarrow X$, $(g, x) \mapsto g \cdot x$, such that

$$e \cdot x = x \quad \text{and} \quad g \cdot (h \cdot x) = (gh) \cdot x$$

for all $x \in X$ and all $g, h \in G$. Let $x \mapsto g \cdot x$ be an automorphism of X for each $g \in G$. Then we refer to this situation by saying that G acts *morphically on the variety* X or also that X is a G -variety. If both G and X are given over k , we say also that G acts *k -morphically* on X .

As X we will usually take a projective variety $X \subseteq \mathbb{P}^n$ and as the group G a linear subgroup of $\mathbf{GL}_{n+1}(k)$ representing linear transformations of \mathbb{P}^n fixing X , hence the action of G on X is just a multiplication $(g, x) \mapsto gx$. Of course, G acts on the whole $(n+1)$ -dimensional vector space (which we refer to as a G -module) and X is a subset fixed by G .

PROPOSITION 3.20 (Closed orbit lemma). *Let G be an algebraic group acting morphically on a non-empty variety X . Then each orbit is a smooth variety which is open in its closure in X . Its boundary is a union of orbits of strictly lower dimension. In particular, the orbits of minimal dimension are closed.*

PROOF. See [Bor91], Lemma 1.8. □

The *derived series* $\mathcal{D}^n G$ of a group G is defined inductively by:

$$\mathcal{D}^0 G = G, \quad \mathcal{D}^{n+1} G = (\mathcal{D}^n G, \mathcal{D}^n G), \quad n \geq 0,$$

where by $(.,.)$ we denote the commutator subgroup.

A group G is *solvable*, if $\mathcal{D}^n G = \{e\}$ for some n .

A connected solvable group G is *k-split*, if it has a composition series $G = G_0 \supset G_1 \supset \dots \supset G_s = \{e\}$ consisting of connected k -subgroups such that G_i/G_{i+1} is k -isomorphic to \mathbf{G}_a (the additive group of the field) or \mathbf{GL}_1 ($0 \leq i < s$).

THEOREM 3.21 (Borel's fixed point theorem). *Let G be connected, solvable and k -split group acting k -morphically on a projective variety X . If $X(k) \neq \emptyset$, then there is an $x \in X$ with $gx = x$ for all $g \in G$.*

PROOF. See [Bor91], Proposition 15.2. □

Let G be an algebraic group. A maximal connected solvable subgroup of G is called a *Borel subgroup*.

COROLLARY 3.22. *Let $G \subseteq \mathbf{GL}(V)$ be an algebraic group and $B \subseteq G$ a k -split Borel subgroup. If B fixes a unique point in $\mathbb{P}(V)$, then G has a unique closed orbit in $\mathbb{P}(V)$ (i.e. there is a unique projective variety $X \subseteq \mathbb{P}(V)$ on which G acts transitively).*

PROOF. Let $X' = Gx$, where $x \in \mathbb{P}(V)$ is the unique point fixed by B . Let $X \subseteq \mathbb{P}(V)$ be a closed orbit of G . By the Closed orbit lemma X exists and is an algebraic variety. By Borel's fixed point theorem, $x \in X$, so $X' \subseteq X$. Since X itself is an orbit under G , we have that $X' = X$. □

EXAMPLE 3.23. Let us again take the conic C_0 which is the zero set of $z_0 z_2 - z_1^2$, see Section 4. It is the image of \mathbb{P}^1 under the map $\varphi_0: \mathbb{P}^1 \rightarrow \mathbb{P}^2$, $(s : t) \mapsto (s^2 : st : t^2)$. Let $V = k^2$ and let φ'_0 be the map $V \rightarrow \text{Sym}^2(V)$, $v \mapsto v^2$. Let v_1, v_2 be a basis of V and let us take $v_1^2, 2v_1 v_2$ and v_2^2 as the basis of $\text{Sym}^2(V)$. Then for the coordinates of the image $\varphi'_0(V)$ with respect to the fixed basis of $\text{Sym}^2(V)$ we have $\mathbb{P}(\varphi'_0(V)) = C_0$. The group $\mathbf{GL}_2(k)$ acting naturally on V acts on $\text{Sym}^2(V)$ by $g \cdot (v_i v_j) = (g v_i)(g v_j)$ so

that φ'_0 is $\mathbf{GL}_2(k)$ -equivariant. Therefore C_0 is fixed by $\mathbf{GL}_2(k)$ and hence we have a representation $\tilde{\varphi}_0: \mathbf{GL}_2(k) \rightarrow G(C_0, k) \subset \mathbf{GL}_3(k)$.

The group $\mathbf{GL}_2(k)$ has a Borel subgroup

$$B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \mathbf{GL}_2(k) \right\},$$

the group of all upper triangular matrices. Since $\mathbf{GL}_2(k)$ acts transitively on C_0 , the conic is a single orbit of $G(C_0, k)$. On the other hand, via the action $\tilde{\varphi}_0$, B has a unique fixed point in $\mathbb{P}(\mathrm{Sym}^2(V))$, namely $(1 : 0 : 0)$. Therefore C_0 is the unique closed orbit of $G(C_0, k)$ in $\mathbb{P}(\mathrm{Sym}^2(V))$.

PROPOSITION 3.24. *Let X_1 and X_2 in \mathbb{P}^n be projectively equivalent over k . Suppose that $G(X_i, k)$ ($i = 1, 2$) acts transitively on X_i and that a k -split Borel subgroup of $G(X_1, k)$ fixes a unique $x \in \mathbb{P}^n$. Suppose further that the natural $\mathfrak{g}_0(X_i, k)$ -module V_i ($i = 1, 2$) is absolutely irreducible. If there is an isomorphism φ of Lie algebras $\mathfrak{g}_0(X_1, k) \rightarrow \mathfrak{g}_0(X_2, k)$ and an invertible map $\nu: V_1 \rightarrow V_2, v \mapsto Nv$ such that $\nu(xv) = \varphi(x)\nu(v)$ for all $x \in \mathfrak{g}_0(X_1, k)$ and $v \in V_1$, then $p \mapsto Np$ is also a projective equivalence $X_1 \rightarrow X_2$.*

PROOF. We claim that there is an isomorphism ψ of algebraic groups $G(X_1, k) \rightarrow G(X_2, k)$ such that $\varphi = d\psi$ and the natural modules of $G(X_1, k)$ and $G(X_2, k)$ are isomorphic, i.e. there is $\nu': V_1 \rightarrow V_2$ such that $\nu'(gv) = \psi(g)\nu'(v)$ for all $g \in G(X_1, k)$ and $v \in V_1$. Then by Corollary 2.18, ν' is also an isomorphism of natural modules of $\mathfrak{g}_0(X_1, k)$ and $\mathfrak{g}_0(X_2, k)$ with respect to φ , so $\nu'(xv) = \varphi(x)\nu'(v)$. Since the modules are absolutely irreducible, by the Schur's lemma (see e.g. [Hum72], § 6.1) we have $\nu' = \nu$ up to multiplication by scalars.

Now by Corollary 3.22, there is a unique closed orbit in the natural $G(X_1, k)$ -module which is by ν mapped to a unique closed orbit in the natural $G(X_2, k)$ -module. Since $G(X_i, k)$ fixes X_i ($i = 1, 2$) and X_i is a closed orbit of G with respect to the action described by $G(X_i, k)$, we have that ν is also a projective equivalence $X_1 \rightarrow X_2$.

It remains to prove the claim in the beginning of the proof. By assumption there is a projective equivalence $\mu: v \mapsto Mv, \mu(X_2) = X_1$. Then $\psi_\mu: g \mapsto MgM^{-1}$ is an isomorphism $G(X_2, k) \rightarrow G(X_1, k)$ and μ is the associated module isomorphism. Then also the modules of their Lie algebras are isomorphic, $\mu(xv) = d\psi_\mu(x)\mu(v)$ for all $x \in \mathfrak{g}_0(X_2, k)$ and v in the natural $\mathfrak{g}_0(X_2, k)$ -module. (see Corollary 2.18 or Proposition 3.11). For the composition $\mu \circ \nu$ we then get $\mu \circ \nu(xv) = (d\psi_\mu \circ \varphi(x))(\mu \circ \nu(v))$. Let A be a regular matrix such that $\mu \circ \nu(v) = Av$, So $Axv = (d\psi_\mu \circ \varphi(x))Av$. Since the last equality holds for all v in the module, we can conclude that the automorphism $d\psi_\mu \circ \varphi$

of $\mathfrak{g}_0(X_1, k)$ maps x to AxA^{-1} . Then $\psi': g \mapsto AgA^{-1}$ is an injective homomorphism of the group $G(X_1, k)$. The image $\psi'(G(X_1, k))$ is an algebraic group with the same Lie algebra as the one of $G(X_1, k)$, therefore $\psi'(G(X_1, k)) = G(X_1, k)$. If we define $\psi: G(X_1, k) \rightarrow G(X_2, k)$ as the composition $\psi_\mu^{-1} \circ \psi'$, $g \mapsto M^{-1}Ag(M^{-1}A)^{-1}$, then $d\psi = \varphi$. \square

Proposition 3.24 leads to an algorithm for finding a projective equivalence of two varieties under more general assumptions:

ALGORITHM: **FindProjectiveEquivalence**

INPUT: $X_1, X_2 \subseteq \mathbb{P}^n$ – projective varieties defined over k such that at least one of the following conditions is satisfied:

- each automorphism of $\mathfrak{g}_0(X_1, k)$ is a conjugation by a matrix from $G(X_1, k)$,
- $G(X_1, k)$ acts transitively on X_1 , a Borel subgroup of $G(X_1, k)$ fixes a unique point in \mathbb{P}^n , and the natural $\mathfrak{g}_0(X_1, k)$ -module is absolutely irreducible.

OUTPUT: $M \in \mathbf{GL}_{n+1}(k)$ such that $Mp \in X_2$ for all $p \in X_1$ if such M exists, **failed** otherwise.

- (1) Compute $\mathfrak{g}_0(X_1, k)$ and $\mathfrak{g}_0(X_2, k)$ as described in Section 2.
- (2) Find a Lie algebra isomorphism $\psi: \mathfrak{g}_0(X_1, k) \rightarrow \mathfrak{g}_0(X_2, k)$ such that the natural modules of $\mathfrak{g}_0(X_1, k)$ and $\mathfrak{g}_0(X_2, k)$ are isomorphic. If such isomorphism does not exist, return **failed**.
- (3) Construct an isomorphism μ between the natural modules of algebras $\mathfrak{g}_0(X_1, k)$ and $\mathfrak{g}_0(X_2, k)$, $\mu: v \mapsto Mv$ for some $M \in \mathbf{GL}_{n+1}(k)$.
- (4) If μ transforms X_1 to X_2 , return M . Otherwise return **failed**.

Del Pezzo surfaces of degree 8

We illustrate how to use Lie algebras for parametrizing Del Pezzo surfaces of degree 8. As already mentioned, there are two kinds of these surfaces: $\mathbb{P}^1 \times \mathbb{P}^1$ and the blowup of the projective plane in a point. Here we give a parametrization algorithm over k for both of them.

1. Embeddings of $\mathbb{P}^1 \times \mathbb{P}^1$

The automorphism group of $\mathbb{P}^1 \times \mathbb{P}^1$ consists of automorphisms of particular projective lines in the product and automorphisms switching the two factors, the former fixing the Picard group of $\mathbb{P}^1 \times \mathbb{P}^1$, the latter not. So we have $\text{Aut}(\mathbb{P}^1 \times \mathbb{P}^1) = \mathbf{PGL}_2(k) \times \mathbf{PGL}_2(k) \rtimes \mathbb{Z}/2\mathbb{Z}$ and $\text{Aut}_0(\mathbb{P}^1 \times \mathbb{P}^1) = \mathbf{PGL}_2(k) \times \mathbf{PGL}_2(k)$. It follows that $\mathfrak{g}_0(\mathbb{P}^1 \times \mathbb{P}^1, k) = \mathfrak{sl}_2 \oplus \mathfrak{sl}_2$.

The automorphisms of $\mathbb{P}^1 \times \mathbb{P}^1$ can be represented by a linear group $G \subset \mathbf{GL}_4(k)$ in the following way. Let $G = G_0 \times \langle g \rangle$, where $G_0 \cong \mathbf{GL}_2 \times \mathbf{GL}_2(k)$ consists of block diagonal matrices $\text{diag}(g_1, g_2)$ with $g_1, g_2 \in \mathbf{GL}_2(k)$, and

$$g = \begin{pmatrix} 0 & I_2 \\ I_2 & 0 \end{pmatrix}, \quad \text{where } I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The subgroup G_0 acts on $\mathbb{P}^1 \times \mathbb{P}^1$ by $\text{diag}(g_1, g_2) \cdot (u, v) = (g_1u, g_2v)$ and g acts by $g \cdot (u, v) = (v, u)$. This readily gives a surjective group homomorphism $G \rightarrow \text{Aut}(\mathbb{P}^1 \times \mathbb{P}^1)$. The kernel of this homomorphism is a 2-dimensional subgroup consisting of matrices $\text{diag}(c_1I_2, c_2I_2)$ with $c_1, c_2 \in k^*$.

Let $\mathfrak{g}_0 \subseteq \mathfrak{sl}_4(k)$ be the Lie algebra of G with the ideal generated by the identity matrix factored out. It consists of block diagonal matrices, each block being a 2×2 zero trace matrix. The algebra $\mathfrak{g}_0(\mathbb{P}^1 \times \mathbb{P}^1, k)$ is then the image of \mathfrak{g}_0 under the differential of the group homomorphism $G \rightarrow \text{Aut}(\mathbb{P}^1 \times \mathbb{P}^1)$. The automorphism group of \mathfrak{g}_0 is generated by the automorphisms of each of the direct summands of \mathfrak{g}_0 , along with the map switching them. By Theorem 2.6 the former are conjugations by a matrix from G_0 , and the latter is the conjugation by g .

1.1. The basic algorithm. The anticanonical embedding $\varphi_0: \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow X_0 \subset \mathbb{P}^8$ is given by

$$(8) \quad (s_0:s_1; t_0:t_1) \mapsto (s_0^2 t_0^2 : s_0^2 t_0 t_1 : s_0^2 t_1^2 : s_0 s_1 t_0^2 : s_0 s_1 t_0 t_1 : s_0 s_1 t_1^2 : s_1^2 t_0^2 : s_1^2 t_0 t_1 : s_1^2 t_1^2).$$

We want to decide whether a given surface in \mathbb{P}^8 projectively equivalent to X_0 over \bar{k} , is isomorphic to X_0 also over k and if so, to find an isomorphism.

We now analyze the natural $\mathfrak{g}_0(X_0, k)$ -module. Let V_1 and V_2 be two natural 2-dimensional \mathbf{GL}_2 -modules. The action of G on $V_1 \times V_2$ is analogous to the one described on $\mathbb{P}^1 \times \mathbb{P}^1$ in the beginning of the chapter. This action extends to the module $W = \text{Sym}^2(V_1) \otimes \text{Sym}^2(V_2)$ such that the map $\varphi'_0: V_1 \times V_2 \rightarrow W$, $(v_1, v_2) \mapsto v_1^2 \otimes v_2^2$ is G -equivariant. If v_{11}, v_{12} is a basis of V_1 , v_{21}, v_{22} a basis of V_2 , we take the following basis of W :

$$\begin{aligned} &v_{11}^2 \otimes v_{21}^2, 2v_{11}^2 \otimes v_{21}v_{22}, v_{11}^2 \otimes v_{22}^2, 2v_{11}v_{12} \otimes v_{21}^2, 4v_{11}v_{12} \otimes v_{21}v_{22}, 2v_{11}v_{12} \otimes v_{22}^2, \\ &v_{12}^2 \otimes v_{21}^2, 2v_{12}^2 \otimes v_{21}v_{22}, v_{12}^2 \otimes v_{22}^2. \end{aligned}$$

Then after comparing with (8) we see that the projectivization of the image of $V_1 \otimes V_2$ under φ'_0 in coordinates relative to this basis is exactly X_0 . Since the image is fixed by G , we have a map $\tilde{\varphi}_0: G \rightarrow G(X_0, k) \subset \mathbf{GL}_9(k)$. The differential $d\tilde{\varphi}_0$ takes the Lie algebra \mathfrak{g}_0 to $\mathfrak{g}_0(X_0, k)$. By Proposition 2.19 every automorphism of $\mathfrak{g}_0(X_0, k)$ is a conjugation by a matrix from $G(X_0, k)$. Therefore by Proposition 3.12 it follows that the algorithm `FindProjectiveEquivalence` can be applied for finding a parametrization of a surface $X \subset \mathbb{P}^8$ projectively equivalent to X_0 over k .

In the algorithm we have to construct two isomorphisms: an isomorphism of $\mathfrak{g}_0(X, k)$ and $\mathfrak{sl}_2 \oplus \mathfrak{sl}_2$ and isomorphism of two $\mathfrak{sl}_2 \oplus \mathfrak{sl}_2$ -modules afforded by the representations $\mathfrak{g}_0(X_0, k)$ and $\mathfrak{g}_0(X, k)$. For deciding and finding a Lie algebra isomorphism we do the following:

- (1) Check whether $\mathfrak{g}_0(X, k)$ is semisimple.
- (2) Decompose $\mathfrak{g}_0(X, k)$ as a sum of two simple subalgebras, $\mathfrak{g}_0(X, k) = \mathfrak{g}_1 \oplus \mathfrak{g}_2$. (An algorithm for the decomposition can be found in [dG00].)
- (3) Find isomorphisms $\mathfrak{g}_i \rightarrow \mathfrak{sl}_2(k)$, $i = 1, 2$ as described in Chapter 6.

If any step of the algorithm cannot be carried out, the variety X is not isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ over k . Note, that if we work over \mathbb{Q} , the third step in the algorithm reduces to finding rational points on two conics, see Chapter 3, Section 5.

Now we want to find an isomorphism of the natural $\mathfrak{g}_0(X_0, k)$ - and $\mathfrak{g}_0(X, k)$ -modules. In the previous discussion we have seen that the natural $\mathfrak{g}_0(X_0, k)$ -module is the $\mathfrak{sl}_2 \oplus \mathfrak{sl}_2$ -module $\text{Sym}^2(V_1) \otimes \text{Sym}^2(V_2)$, where both V_1 and V_2 are 2-dimensional natural \mathfrak{sl}_2 -modules. It follows that the $\mathfrak{g}_0(X_0, k)$ -module is irreducible and has the highest weight $(2, 2)$.

Hence we can decide module equivalence by checking irreducibility and computing the highest weight. In the affirmative case, we can again construct a module isomorphism using highest weight vectors.

Timings. The algorithm is implemented in Magma. Some statistics about timings for surfaces over \mathbb{Q} can be found in Table 1. For testing, the examples were constructed as follows. We start with the standard embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ into \mathbb{P}^8 (see (8)) which is implicitly given by 20 binomials. Then a 9×9 matrix is generated, containing random integer numbers with absolute values up to a given maximal number (this is written in the first column of Table 1). This matrix is then used as the matrix of a linear transformation of projective space obtaining so a different system of implicit equations.

For a “small” perturbation, almost the whole computational time is spent for finding the Lie algebra of the surface. As the coefficients of the linear transformation grow, finding a rational point on the conic starts to play the main role in the time complexity.

1.2. Proper twists of $\mathbb{P}^1 \times \mathbb{P}^1$. If a surface is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ over an extension of k but not over k itself, it still can have a proper parametrization over k . Here we investigate this case.

THEOREM 4.1. *Let $X \cong C_1 \times C_2$ be defined over k , where C_1 and C_2 are twists of \mathbb{P}^1 . Then X has a k -parametrization if and only if $C_1 \cong \mathbb{P}^1$ and $C_2 \cong \mathbb{P}^1$ over k .*

PROOF. Assume that X has a parametrization. Then in particular there is a k -rational point $p \in X$. The two projections $\pi_i: X \rightarrow C_i$ ($i = 1, 2$) are defined over k , therefore give k -rational points $\pi_1(p) \in C_1$ and $\pi_2(p) \in C_2$. It follows that $C_1 \cong \mathbb{P}^1$ and $C_2 \cong \mathbb{P}^1$ over k . The other direction is trivial. \square

Theorem 4.1 implies that if we are looking for the proper twists of $\mathbb{P}^1 \times \mathbb{P}^1$ with a k -rational parametrization, we have to investigate varieties which do not decompose as a product over k . Let us therefore study, how is the fact, that the variety is a product over k , reflected by its Lie algebra.

THEOREM 4.2. *Let X be a twist of $\mathbb{P}^1 \times \mathbb{P}^1$ defined over k . Then the following are equivalent:*

perturb	eqns max	LA size	prm size	time	LA time	conic time
1	4	11	18	4.56	4.49	0.00
5	73	47	70	21.93	21.66	0.03
10	255	55	84	28.46	28.11	0.09
50	5026	84	130	48.75	48.15	0.22
100	25304	111	166	61.02	60.15	0.34
300	225440	134	200	75.86	73.00	2.14
	208199	136	204	89.52	73.15	15.77
400	335499	143	213	77.99	76.31	0.93
	418185	141	210	152.21	77.91	73.56
	545728	140	208	482.69	74.50	407.53
500	720193	147	222	91.11	82.24	8.10
	525179	145	216	80.95	78.91	1.29
	546787	143	218	176.13	78.51	96.96

perturb – maximal entry allowed in perturbation matrix,

eqns max – maximal absolute value of the coefficients in the implicit equations,

LA size – maximal length of the numerator/denominator of the structure constants of the Lie algebra,

prm size – maximal length of the numerator/denominator of the coefficients in the parametrization,

time – total time (in seconds) needed for parametrizing,

LA time – time (in seconds) needed for finding the Lie algebra (is a part of “time” in the previous column).

conic time – time (in seconds) needed for finding rational points on two conics constructed to identify two summands $\mathfrak{sl}_2(\mathbb{Q})$ (is a part of “time”).

TABLE 1. Parametrizing $\mathbb{P}^1 \times \mathbb{P}^1$.

(i) X is a product of two twists of \mathbb{P}^1 ,

(ii) the Lie algebra $\mathfrak{g}_0(X, k)$ is a direct sum of two twists of \mathfrak{sl}_2 .

PROOF. (i) \Rightarrow (ii): If $X \cong C_1 \times C_2$, then $\text{Aut}_0(X)$ is the direct product of the two normal subgroups $\text{Aut}(C_1)$ and $\text{Aut}(C_2)$. It follows that $\mathfrak{g}_0(X, k) = \mathfrak{g}_0(C_1, k) \oplus \mathfrak{g}_0(C_2, k)$.

(ii) \Rightarrow (i): If X is not a product, we set k' to be a (finite) Galois extension of k such that $X(k') \cong \mathbb{P}^1 \times \mathbb{P}^1$. Then $\text{Pic } X(k') \cong \mathbb{Z}^2$. For any $\sigma \in G$ the image $\sigma(D)$ of a divisor D is again a divisor and if $D_1 \sim D_2$ then $\sigma(D_1) \sim \sigma(D_2)$, so G acts on $\text{Pic } X(k')$. Now we use the following a bit technical

LEMMA 4.3. *Let X be a twist of $\mathbb{P}^1 \times \mathbb{P}^1$ defined over k which is not a product and let k' be a finite Galois extension of k such that $X(k') \cong \mathbb{P}^1 \times \mathbb{P}^1$. Then there is σ in $\text{Gal}(k'|k)$ interchanging the divisor classes $(1, 0)$ and $(0, 1)$.*

Since $\text{Gal}(k'|k)$ interchanges the two classes defining the two projections, it also interchanges the two normal subgroups of $\text{Aut}_0(X(k'))$ of dimension 3, and hence it also interchanges the two ideals of $\mathfrak{g}_0(X, k')$. It follows that these ideals are not defined over k , hence $\mathfrak{g}_0(X, k)$ is simple. \square

PROOF OF LEMMA 4.3. The action of $\text{Gal}(k'|k)$ preserves the intersection numbers and maps effective divisors again to effective divisors. Therefore the divisor classes $(1, 0)$ and $(0, 1)$ can either be fixed or interchanged. We claim, that there is σ in $\text{Gal}(k'|k)$ interchanging these two classes. For, suppose by contradiction that every $\sigma \in \text{Gal}(k'|k)$ fixes $(1, 0)$. Take a divisor $D \in \text{Div } X(k')$ such that its class $[D] = (1, 0)$. Then the divisor $\sum_{\sigma \in \text{Gal}(k'|k)} \sigma(D)$ is fixed by $\text{Gal}(k'|k)$ and its class is $(|\text{Gal}(k'|k)|, 0)$. Therefore the associated map is a projection over k to a twist of \mathbb{P}^1 , contradicting our assumption that X is not a product. \square

The *centroid* of a Lie algebra \mathfrak{g} is the centralizer of $\text{ad } \mathfrak{g}$ in $\mathfrak{gl}(\mathfrak{g})$. The centroid of a Lie algebra \mathfrak{g} is denoted by $\Gamma(\mathfrak{g})$.

LEMMA 4.4. *Let X be a twist of $\mathbb{P}^1 \times \mathbb{P}^1$ defined over k and let Γ_0 be the centroid of $\mathfrak{g}_0(X, k)$.*

- (i) *If X is a product, then $\Gamma_0 = k^2$.*
- (ii) *If X is not a product, then Γ_0 is a quadratic field extension of k and $X(\Gamma_0)$ is a product.*

PROOF. (i) By [Jac79], §X, Theorem 1, the centroid of a simple Lie algebra is a field. If \mathfrak{g} is a twist of $\mathfrak{sl}_2(k)$, we conclude then that $\Gamma(\mathfrak{g}) \cong k$. Write $\mathfrak{g}_0(X, k) = \mathfrak{g}_1 \oplus \mathfrak{g}_2$. Let $T: \mathfrak{g}_0(X, k) \rightarrow \mathfrak{g}_0(X, k)$ be a linear map commuting with all $\text{ad } x$ for $x \in \mathfrak{g}_0(X, k)$. Then $T(\mathfrak{g}_i) \subseteq \mathfrak{g}_i$, $i = 1, 2$. For, let $x \in \mathfrak{g}_1$ and write $T(x) = y_1 + y_2$, $y_i \in \mathfrak{g}_i$. If $y_2 \neq 0$ then take $z \in \mathfrak{g}_2$ such that $[z, y_2] \neq 0$. Then $\text{ad } z \circ T(x) = [z, y_2] \neq 0$. But $T \circ \text{ad } z(x) = T([z, x]) = 0$, a contradiction. It follows, that $\Gamma(\mathfrak{g}_1 \oplus \mathfrak{g}_2) = \Gamma(\mathfrak{g}_1) \oplus \Gamma(\mathfrak{g}_2) = k^2$, since both \mathfrak{g}_1 and \mathfrak{g}_2 are twists of $\mathfrak{sl}_2(k)$.

(ii) Let k' be a field extension of k such that $\mathfrak{g}_0(X, k')$ decomposes as the sum of two ideals. Because computing the centralizer commutes with base field extension, $\Gamma_0 \otimes_k k'$ is equal to the centroid of $\mathfrak{g}_0(X, k')$, which is $(k')^2$. Hence Γ_0 is a 2-dimensional (associative) k -algebra without nilpotent elements. This implies that either Γ_0 is a quadratic field extension of k or $\Gamma_0 \cong k^2$ (with componentwise multiplication).

Since $\mathfrak{g}_0(X, k)$ is simple, the first case is true. To prove the last statement we use again the commuting property of computing the centroid and extending the field to Γ_0 : $\Gamma(\mathfrak{g}_0(X, \Gamma_0)) = \Gamma(\mathfrak{g}_0(X, k)) \otimes_k \Gamma_0 \cong \Gamma_0^2$. The two principal idempotents $(1, 0)$ and $(0, 1)$ in $\Gamma(\mathfrak{g}_0(X, \Gamma_0))$ lead to the desired decomposition of $\mathfrak{g}_0(X, \Gamma_0)$. \square

From Theorem 4.1 and Lemma 4.4 it follows, that a proper twist of $\mathbb{P}^1 \times \mathbb{P}^1$ can have a k -rational parametrization only if X is not a product over k and it decomposes as a product of two projective lines over the centroid of its Lie algebra. In following we will see that this is not only necessary but also a sufficient condition.

PROPOSITION 4.5. *Let X be a twist of $\mathbb{P}^1 \times \mathbb{P}^1$ defined over k which is not a product such that for the centroid $k' = \Gamma(\mathfrak{g}_0(X, k))$ of $\mathfrak{g}_0(X, k)$ we have $X(k') \cong \mathbb{P}^1 \times \mathbb{P}^1$. Then X is k -rational.*

PROOF. By Lemma 4.4, k' is a quadratic extension of k and $\mathfrak{g}_0(X, k') \cong \mathfrak{sl}_2 \oplus \mathfrak{sl}_2$ is the decomposition over k' . Denote by σ the generator of $\text{Gal}(k'|k)$. By Lemma 4.3 then σ interchanges the divisor classes $(1, 0)$ and $(0, 1)$. Let us denote the projection associated to $(1, 0)$ by π . The intersection number of the two classes is 1, therefore for a point $p \in \mathbb{P}^1(k')$ we have that $\pi^{-1}(p) \cap \sigma \circ \pi^{-1}(p)$ is a single point, let us denote it by q . Further we have that q is fixed by $\text{Gal}(k'|k)$, hence $q \in X(k)$. Let $\alpha \in k'$ be such that $k' = k(\alpha)$. The map mapping $\mathbb{P}^1(k') \rightarrow X(k)$ just described is defined by polynomials. Its composition with $\mathbb{P}^2(k) \rightarrow \mathbb{P}^1(k')$ mapping $(s : t : u) \mapsto (s + \alpha t : u)$ is a rational map over k and has a k -rational inverse. \square

The proposition finishes our analysis of proper twists of $\mathbb{P}^1 \times \mathbb{P}^1$. Together with Theorem 4.1 we have that a proper twist X of $\mathbb{P}^1 \times \mathbb{P}^1$ is k -rational if and only if the Lie algebra $\mathfrak{g}_0(X, k)$ is simple and splits completely over its centroid. The proof of the proposition gives also the last step in the process of parametrizing rational proper twists of $\mathbb{P}^1 \times \mathbb{P}^1$. To sum up, we have the following algorithm:

- (1) Check whether $\mathfrak{g}_0(X, k)$ is simple and compute its centroid $k' = \Gamma(\mathfrak{g}_0(X, k))$. By Lemma 4.4 (ii), k' is a quadratic extension of k ; let σ denote the generator of the Galois group $\text{Gal}(k'|k)$.
- (2) Decompose $\mathfrak{g}_0(X, k')$ as a sum of two simple subalgebras, $\mathfrak{g}_0(X, k') = \mathfrak{g}_1 \oplus \mathfrak{g}_2$.
- (3) Find isomorphisms $\mathfrak{g}_i \rightarrow \mathfrak{sl}_2(k')$, $i = 1, 2$ by reducing to a norm equation (see Chapter 6).
- (4) Construct an isomorphism of modules of $\mathfrak{g}_0(X_0, k')$ and $\mathfrak{g}_0(X, k')$ obtaining so a projective equivalence of X_0 and X over k' and also an k' -embedding $\varphi: \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow X$.

- (5) For a fixed $(\alpha:\beta) \in \mathbb{P}^1(k')$, let $l_{(\alpha:\beta)}$ be the line $\varphi(\{(\alpha:\beta; s:t) \mid (s:t) \in \mathbb{P}^1(k')\})$. Then $\mathbb{P}^1(k') \rightarrow X(k)$, $(\alpha:\beta) \mapsto l_{(\alpha:\beta)} \cap \sigma(l_{(\alpha:\beta)})$ together with $\mathbb{P}^2(k) \rightarrow \mathbb{P}^1(k')$, $(s:t:u) \mapsto (s+\alpha t:u)$ leads to a parametrization $\mathbb{P}^2(k) \rightarrow X(k)$.

EXAMPLE 4.6. To illustrate the method we find a parametrization of the unit sphere, which is a twist of Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$. For simplicity we omit here the anti-canonical embedding.

The canonical surface S_0 is parametrized by $(s_0:s_1; t_0:t_1) \mapsto (s_0t_0 : s_0t_1 : s_1t_0 : s_1t_1)$ and implicitly given by the polynomial $z_0z_3 - z_1z_2$. The surface S is given by $z_1^2 + z_2^2 + z_3^2 - z_0^2$. The Lie algebra $\mathfrak{g}_0(S, \mathbb{Q})$ is simple, the centroid $\Gamma(\mathfrak{g}_0(S, \mathbb{Q}))$ is the extension $\mathbb{Q}(i)$, $i^2 = -1$. Over this field the algebra splits as the sum $\mathfrak{g}_0(S, \mathbb{Q}(i)) = \mathfrak{sl}_2(\mathbb{Q}(i)) \oplus \mathfrak{sl}_2(\mathbb{Q}(i))$. We find an isomorphism of the Lie algebras and afterwards the parametrization of S over $\mathbb{Q}(i)$:

$$(9) \quad \begin{pmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ i & 0 & 0 & i \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} s_0t_0 \\ s_0t_1 \\ s_1t_0 \\ s_1t_1 \end{pmatrix} = \begin{pmatrix} -s_0t_1 + s_1t_0 \\ s_0t_0 - s_1t_1 \\ is_0t_0 + is_1t_1 \\ s_0t_1 + s_1t_0 \end{pmatrix}.$$

The line $l_{(\alpha:\beta)}$ is parametrized by fixing $(s_0 : s_1)$ to $(\alpha : \beta) \in \mathbb{P}^1(\mathbb{Q}(i))$ in (9): $l_{(\alpha:\beta)} = (\beta t_0 - \alpha t_1 : \alpha t_0 - \beta t_1 : i\alpha t_0 + i\beta t_1 : \beta t_0 + \alpha t_1)$.

Every point $(\alpha : \beta) \in \mathbb{P}^1(\mathbb{Q}(i))$ can be written as $(a + ib : c)$ such that $a, b, c \in \mathbb{Q}$. A rational parametrization of the sphere S is then obtained by mapping every point $(a : b : c) \in \mathbb{P}^2(\mathbb{Q})$ into the intersection of $l_{(a+ib:c)}$ and its conjugate:

$$\begin{aligned} l_{(a+ib:c)} &= (ct_0 - (a+ib)t_1 : (a+ib)t_0 - ct_1 : i(a+ib)t_0 + ict_1 : ct_0 + (a+ib)t_1), \\ \bar{l}_{(a+ib:c)} &= (cs_0 - (a-ib)s_1 : (a-ib)s_0 - cs_1 : -i(a-ib)s_0 - ics_1 : cs_0 + (a-ib)s_1), \end{aligned}$$

obtaining such

$$(a : b : c) \mapsto l_{(a+ib:c)} \cap \bar{l}_{(a+ib:c)} = (c^2 + a^2 + b^2 : 2ac : -2bc : c^2 - a^2 - b^2).$$

Timings. For testing the algorithm we constructed examples as follows. We have chosen $d \in \mathbb{Z}$ such that $d \notin \mathbb{Q}^2$ (given in the first column of Table 2). Then the quadratic surface in \mathbb{P}^3 given by $z_0^2 - z_1^2 = z_2^2 - dz_3^2$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ over $\mathbb{Q}(\sqrt{d})$ but not over \mathbb{Q} . We anticanonically embedded the surface over \mathbb{Q} into \mathbb{P}^8 obtaining such a surface described by 14 binomials and 6 polynomials with 4 terms. Afterwards we made a linear transformation similar to the previous case, just here the generated matrix is sparser, to obtain examples solvable in practice. Since we have to identify two \mathfrak{sl}_2 's over $\mathbb{Q}(\sqrt{d})$, we have to solve two relative norm equations. This is very time consuming, therefore we were able to parametrize only “small” examples.

discr	perturb (sparse)	eqns max	LA size	prm size	time	LA time	normeq time
-1	1	3	3	9	2.460	0.670	1.010
3	1	5	3	23	3.620	1.030	1.700
8	1	15	5	1135	211.340	1.270	123.230
-1	2	10	5	92	41.690	1.250	38.670

discr – square of the primitive element used for the construction,
normeq time – time (in seconds) needed for solving two relative norm equations (is a part of “time”).

Description of the other columns: as in Table 1.

TABLE 2. Parametrizing the proper twists of $\mathbb{P}^1 \times \mathbb{P}^1$.

2. Blow-up of the projective plane

In this section the surface X is the *blowup* of the projective plane in a single point, i.e. an embedding of

$$\Pi = \{(x_0 : x_1 : x_2; y_1 : y_2) \in \mathbb{P}^2 \times \mathbb{P}^1 \mid x_1 y_2 = x_2 y_1\}.$$

The line $l \subset \Pi$, $l = \{(1 : 0 : 0; s : t)\}$ is the *exceptional line* of Π and it is fixed by every automorphism of Π . Therefore the group of automorphisms of Π is isomorphic to the subgroup of automorphisms of \mathbb{P}^2 fixing the point $(1 : 0 : 0)$. We have the group of matrices representing these automorphisms:

$$H = \left\{ g \in \mathbf{GL}_3(k) \mid g = \begin{pmatrix} g_{00} & g_{01} & g_{02} \\ 0 & g_{11} & g_{12} \\ 0 & g_{21} & g_{22} \end{pmatrix} \right\}.$$

Therefore the Lie algebra of Π (after discarding the identity) is isomorphic to

$$(10) \quad \mathfrak{h}_0 = \left\{ a \in \mathfrak{sl}_3(k) \mid a = \begin{pmatrix} 2a & b_1 & b_2 \\ 0 & c_1 - a & c_2 \\ 0 & c_3 & -c_1 - a \end{pmatrix} \right\}.$$

The semisimple part of the Lie algebra \mathfrak{h}_0 is isomorphic to \mathfrak{sl}_2 . Let \mathfrak{k} denote the Levi subalgebra of \mathfrak{h}_0 consisting of those matrices in (10) where a, b_1 and b_2 vanish. The Lie algebra \mathfrak{h}_0 further contains a three-dimensional solvable radical $\text{Rad } \mathfrak{h}_0$ containing a two-dimensional nilradical \mathfrak{N} . If e_{ij} denotes the matrix having a 1 at (i, j) -th position and zero elsewhere, then \mathfrak{N} is spanned by e_{12} and e_{13} and $\text{Rad } \mathfrak{h}_0$ in addition also by $e = 2e_{11} - e_{22} - e_{33}$.

Now we want to prove a proposition implying that also for embeddings of Π associated to a very ample divisor, we can use the algorithm `FindProjectiveEquivalence`. Before doing that we need some well-known technical lemmata.

LEMMA 4.7. *Let $\mathfrak{g} \subseteq \mathfrak{gl}_m(k)$ be a semisimple Lie algebra. If $x \in \mathfrak{g}$ is nilpotent, then also $\text{ad } x$ is nilpotent.*

PROOF. [Hum72], Lemma 3.2. □

LEMMA 4.8. *Let $G \subseteq \mathbf{GL}_m(k)$ be an algebraic group and let $\mathfrak{g} \subseteq \mathfrak{gl}_m(k)$ be its Lie algebra. If $x \in \mathfrak{g}$ is nilpotent, then $\exp(x) \in G$.*

PROOF. [Bor91], §7.3. □

LEMMA 4.9. *Let $\mathfrak{g} \subset \mathfrak{gl}_m(F)$ be a Lie algebra. Let $x \in \mathfrak{g}$ be such that both $\text{ad } x$ and x are nilpotent. Then $\exp(\text{ad } x)(x') = (\exp x)x'(\exp -x)$.*

PROOF. [Jac79], p. 282. □

PROPOSITION 4.10. *Every automorphism of \mathfrak{h}_0 is a conjugation by a matrix from H .*

PROOF. As before, let \mathfrak{k} be the Levi subalgebra spanned by $h = e_{22} - e_{33}, e_{23}$ and e_{32} . We first show that every automorphism ξ of \mathfrak{h}_0 such that its restriction on \mathfrak{k} is the identity, acts on $\text{Rad } \mathfrak{h}_0$ by $e \mapsto e, e_{12} \mapsto \lambda e_{12}$ and $e_{13} \mapsto \lambda e_{13}$ for some $\lambda \in k$.

The automorphism ξ leaves both \mathfrak{N} and $\text{Rad } \mathfrak{h}_0$ fixed. Therefore $\xi(e) = \alpha_1 e + \alpha_2 e_{12} + \alpha_3 e_{13}$, $\xi(e_{12}) = \beta_2 e_{12} + \beta_3 e_{13}$ and $\xi(e_{13}) = \gamma_2 e_{12} + \gamma_3 e_{13}$. From $\xi([e, h]) = [\xi(e), \xi(h)]$ we get $\alpha_2 = \alpha_3 = 0$. Then from $\xi([e, e_{12}]) = [\xi(e), \xi(e_{12})]$ it follows that $\alpha_1 = 1$. To finish the proof of the claim we use $\xi([e_{32}, e_{12}]) = [\xi(e_{32}), \xi(e_{12})]$, $\xi([e_{23}, e_{13}]) = [\xi(e_{23}), \xi(e_{13})]$ and $\xi([e_{32}, e_{13}]) = [\xi(e_{32}), \xi(e_{13})]$.

Let A be the subgroup of inner automorphisms generated by $\exp(\text{ad } x)$ for $x \in \mathfrak{N}$. Since for x in the nilradical $\text{ad } x$ is nilpotent (see Lemma 4.7), it follows from Lemmata 4.8 and 4.9 that automorphisms in A are conjugations by a matrix from H . Let now σ be any automorphism of \mathfrak{h}_0 . Then $\sigma(\mathfrak{k})$ is a Levi subalgebra and by Theorem of Malcev-Harish-Chandra (cf. [Jac79], §III.) there is an automorphism τ of \mathfrak{h}_0 from A such that $\tau(\mathfrak{k}) = \sigma(\mathfrak{k})$. Together with Theorem 2.6 we obtain the claim of the proposition. □

For finding an isomorphism of \mathfrak{h}_0 and the Lie algebra $\mathfrak{g}_0(X, k)$ of the given surface isomorphic to Π it is useful to note that the nilradical \mathfrak{N} is a 2-dimensional irreducible module of the Levi subalgebra \mathfrak{k} . Thus we have the following algorithm:

- (1) Set \mathfrak{k} to be a Levi subalgebra of $\mathfrak{g}_0(X, k)$.

- (2) Set \mathfrak{N} to be the nilradical of $\mathfrak{g}_0(X, k)$.
- (3) Using the action of \mathfrak{k} on \mathfrak{N} construct an isomorphism $\mathfrak{sl}_2 \rightarrow \mathfrak{k}$.
- (4) Set $E_{12} \in \mathfrak{N}$ to be a vector generating one-dimensional eigenspace of $\text{ad } h$ with eigenvalue -1 , where $h \in \mathfrak{k}$ is a vector generating a split Cartan subalgebra of \mathfrak{k} .
- (5) Similarly one can find the images E_{13} and E of elements e_{13} and e in the Lie algebra \mathfrak{h}_0 . (Note that this step is not necessary for finding a module isomorphism as will become clear soon.)

Next we analyze the 9-dimensional module afforded by the anticanonical embedding of Π . This embedding is given by

$$(x_0:x_1:x_2; y_1:y_2) \mapsto (x_0^2y_1 : x_0^2y_2 : x_0x_1y_1 : x_0x_1y_2 : x_0x_2y_2 : x_1^2y_1 : x_1^2y_2 : x_1x_2y_2 : x_2^2y_2)$$

where $x_1y_2 = x_2y_1$, and Π embedded in this way is parametrized by

$$(11) \quad (s : t : u) \mapsto (s^2t : s^2u : st^2 : stu : su^2 : t^3 : t^2u : tu^2 : u^3),$$

The image of this embedding will be denoted as usual by X_0 .

Let V be a 3-dimensional vector space with basis v_0, v_1, v_2 . Consider the symmetric power $\text{Sym}^3(V)$ with the basis $v_0^3, 3v_0^2v_1, 3v_0^2v_2, 3v_0v_1^2, 6v_0v_1v_2, 3v_0v_2^2, v_1^3, 3v_1^2v_2, 3v_1v_2^2, v_2^3$. Let $\varphi'_0 : V \rightarrow \text{Sym}^3(V)$ be given by $\varphi'_0(v) = v^3$.

Let $G = \mathbf{GL}_3(\mathbb{Q})$ act naturally on V . Then G acts also on $\text{Sym}^3(V)$, making φ'_0 G -equivariant.

Let U be the subspace of $\text{Sym}^3(V)$ spanned by v_0^3 . Let $\pi : \text{Sym}^3(V) \rightarrow \text{Sym}^3(V)/U = W$ be the projection discarding the coordinate at v_0^3 . For $\varphi_0 = \pi \circ \varphi'_0$ we have that X_0 is the projectivization of $\varphi_0(V)$. Note that H is exactly the stabilizer of U in G therefore we have a well-defined action of H on the whole module W .

LEMMA 4.11. *As a \mathfrak{k} -module, W decomposes as a direct sum $W = W_2 \oplus W_3 \oplus W_4$, where W_i is an i -dimensional irreducible \mathfrak{k} -module. As \mathfrak{h}_0 -module, W is irreducible.*

PROOF. When restricting to the Levi subalgebra \mathfrak{k} , the module $\text{Sym}^3(V)$ (see the discussion before the lemma) becomes an \mathfrak{sl}_2 -module and as such decomposes as a sum of four irreducible modules: $W_1 = U$, W_2 is the module spanned by $3v_0^2v_1, 3v_0^2v_2$ and is a 2-dimensional \mathfrak{sl}_2 -module k^2 , W_3 is spanned by $3v_0v_1^2, 6v_0v_1v_2, 3v_0v_2^2$ and isomorphic to $\text{Sym}^2(k^2)$, and lastly W_4 is spanned by $v_1^3, 3v_1^2v_2, 3v_1v_2^2, v_2^3$ and isomorphic to $\text{Sym}^3(k^2)$. It follows that W as \mathfrak{sl}_2 -module decomposes into the sum $W_2 \oplus W_3 \oplus W_4$.

To prove the last assertion of the lemma, let us take any $b \in \mathfrak{N}$, $b = b_1e_{12} + b_2e_{13}$. So if $w \in W_4$ is a basis vector, $w = v_1^i v_2^{3-i}$, then $b \cdot w \in \text{span}\{v_0 v_1^{i-1} v_2^{3-i}, v_0 v_1^i v_2^{2-i}\} \subset W_3$. Similarly for $w \in W_3$ one gets $b \cdot w \in W_2$. \square

Let $\psi: W \rightarrow W$ be an isomorphism of $\mathfrak{g}_0(X_0, k)$ -modules. Then ψ restricted to W_i is multiplication by a scalar λ_i . Let $b = e_{12} \in \mathfrak{N}$, and $w_4 = v_1^3 \in W_4$. Since $b \cdot v_1 = v_0$, it follows $b \cdot w_4 = 3v_0v_1^2 \in W_3$. Hence $\psi(b \cdot w_4) = \lambda_3b \cdot w_4$. On the other hand, $\psi(b \cdot w_4) = b \cdot \psi(w_4) = \lambda_4b \cdot w_4$. We deduce that $\lambda_4 = \lambda_3$. In the same way we find out that $\lambda_3 = \lambda_2$, so that ψ is multiplication by a nonzero scalar.

Now we find an isomorphism of $\mathfrak{g}_0(X_0, k)$ - and $\mathfrak{g}_0(X, k)$ -module for a given surface X as follows.

- (1) Let $\mathfrak{k} \subset \mathfrak{g}_0(X, k)$ be a Levi subalgebra, so $\mathfrak{k} \cong \mathfrak{sl}_2(k)$.
- (2) Using weight vectors find the decomposition $W' = W'_2 \oplus W'_3 \oplus W'_4$ of the natural \mathfrak{k} -module, where $[W'_i : k] = i$.
- (3) Find isomorphisms $\psi_i: W_i \rightarrow W'_i$, ($i = 2, 3, 4$) of \mathfrak{sl}_2 -modules.
- (4) Let E_{12} be the image of the matrix e_{12} in $\mathfrak{g}_0(X, k)$, so E_{12} is in the nilradical of $\mathfrak{g}_0(X, k)$.
- (5) E_{12} maps the highest weight vector of W_i (resp. W'_i) to the highest weight vector of W_{i-1} (resp. W'_{i-1}), ($i = 3, 4$). Use this to finish the construction of an isomorphism of the natural $\mathfrak{g}_0(X_0, k)$ - and $\mathfrak{g}_0(X, k)$ -modules.

Timings. We tried our algorithm on examples which we constructed from the canonical surface (given by the binomial ideal with 20 generators) by a linear transformation of the projective space. The randomly generated matrix of the transformation has integral entries with the given maximal absolute value (the first column in Table 3). We see that almost the whole time is spent for finding the Lie algebra of the surface.

perturb	eqns max	LA size	prm size	time	LA time
1	4	10	46	4.43	4.23
5	85	47	211	21.25	20.76
10	280	59	266	28.21	27.58
50	6372	93	424	51.66	50.43
100	26625	103	475	58.08	56.84
500	599186	145	666	82.81	80.89
1000	1926906	159	724	91.26	89.11
5000	60259495	207	957	118.99	115.94
10000	246171712	219	1008	129.49	126.24

Description of the columns: as in Table 1.

TABLE 3. Parametrizing blow-ups of \mathbb{P}^2 .

Del Pezzo surfaces of degree 9

Another surfaces, where we used Lie algebras for parametrizing, are Del Pezzo surfaces of degree 9. We not only give a parametrization algorithm but also analyze in more detail the algebra associated to the surface constructed during the computation.

1. Severi-Brauer varieties

Severi-Brauer varieties may be defined as twists of a projective space, i.e. they are varieties V such that $V \otimes k' \cong \mathbb{P}^n(k')$ for some extension k' of k .

Though geometrically are these varieties very simple, arithmetically they are rather interesting objects. An alternative definition, giving also more insight, relates the variety to a central simple algebra. Namely, an n -dimensional Severi-Brauer variety is the set of $(n+1)$ -dimensional left ideals of a central simple algebra of degree $n+1$. The variety associated to the algebra A will be denoted by \mathcal{V}_A . For a survey on the topic see [Jah00]

If $A \otimes_k k' \cong M_{n+1}(k')$, then we say that k' is a *splitting field* of A . In such case the variety \mathcal{V}_A is over the field k' isomorphic to the n -dimensional projective space. There is a k' -rational point on \mathcal{V}_A if and only if k' is a splitting field of A . For proofs of these properties see [Jac96], § 3.5. Note that a Severi-Brauer variety is k -isomorphic to a projective space if and only if it contains a k -rational point.

EXAMPLE 5.1. We will construct the Severi-Brauer variety corresponding to the quaternion algebra \mathbb{H} over \mathbb{R} .

Since \mathbb{H} is a division algebra, it has no one-sided nontrivial ideals, therefore there are no real points on $V_{\mathbb{H}}$. The algebra splits over \mathbb{C} as follows:

$$\mathbf{1} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Two-dimensional left ideals in $\mathbb{H} \otimes \mathbb{C}$ are parametrized by points of the projective line $\mathbb{P}^1(\mathbb{C})$. These ideals are of the form

$$\mathcal{L}_{\alpha:\beta} = \left\{ \begin{pmatrix} \alpha x & \beta x \\ \alpha y & \beta y \end{pmatrix} \mid x, y \in \mathbb{C} \right\} = \text{span}_{\mathbb{C}} \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ \alpha & \beta \end{pmatrix} \right\}.$$

In the basis $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ of \mathbb{H} we can write

$$\mathcal{L}_{\alpha;\beta} = \text{span}_{\mathbb{C}} \{ \alpha(\mathbf{1} - \mathbf{i}\mathbf{i}) + \beta(\mathbf{j} - \mathbf{i}\mathbf{k}), -\alpha(\mathbf{j} + \mathbf{i}\mathbf{k}) + \beta(\mathbf{1} + \mathbf{i}\mathbf{i}) \}.$$

After embedding this set into Grassmannian $G(2, 4)$ and afterwards into \mathbb{P}^5 we have

$$\begin{pmatrix} \alpha & \beta \\ -i\alpha & i\beta \\ \beta & -\alpha \\ -i\beta & -i\alpha \end{pmatrix} \mapsto \begin{pmatrix} p_{12} \\ p_{13} \\ p_{14} \\ p_{23} \\ p_{24} \\ p_{34} \end{pmatrix} = \begin{pmatrix} 2i\alpha\beta \\ -\alpha^2 - \beta^2 \\ -i\alpha^2 + i\beta^2 \\ i\alpha^2 - i\beta^2 \\ -\alpha^2 - \beta^2 \\ -2i\alpha\beta \end{pmatrix} \mapsto \begin{pmatrix} p_{12} \\ p_{13} \\ p_{14} \end{pmatrix} = \begin{pmatrix} 2i\alpha\beta \\ -\alpha^2 - \beta^2 \\ -i\alpha^2 + i\beta^2 \end{pmatrix},$$

where the last map is a projection onto linearly independent coordinates. The implicit equation of the Severi-Brauer curve corresponding to the quaternion algebra therefore is

$$p_{12}^2 + p_{13}^2 + p_{14}^2 = 0.$$

2. Parametrizing Del Pezzo surfaces of degree 9

Del Pezzo surfaces of degree 9 are anticanonically embedded Severi-Brauer surfaces, so over an algebraic closure they are isomorphic to the projective plane.

The anticanonical embedding φ_0 of the projective plane into \mathbb{P}^9 is given by

$$(12) \quad (s : t : u) \mapsto (s^3 : t^3 : u^3 : s^2t : t^2u : u^2s : st^2 : tu^2 : us^2 : stu).$$

The image $\varphi_0(\mathbb{P}^2)$ we denote X_0 . Implicitly this surface is given by 27 quadratic forms over the rationals.

For the projective plane we have that $\text{Aut}(\mathbb{P}^2) = \text{Aut}_0(\mathbb{P}^2) = \mathbf{PGL}_3(k)$. Therefore the Lie algebra $\mathfrak{g}_0(\mathbb{P}^2, k) = \mathfrak{sl}_3(k)$. In this example we cannot use Proposition 3.12 since the outer automorphism of $\mathfrak{sl}_3(k)$ mapping the matrix x into $-x^t$ is not a conjugation by any $g \in \mathbf{GL}_3(k)$ (here $\mathfrak{sl}_3(k)$ is represented by 3×3 matrices of trace 0).

LEMMA 5.2. *The 10-dimensional $\mathfrak{g}_0(X_0, k)$ -module is an irreducible \mathfrak{sl}_3 -module.*

PROOF. Let $V = k^3$ and let φ'_0 be the map $V \rightarrow W = \text{Sym}^3(V)$, $v \mapsto v^3$. The group $\mathbf{GL}_3(k)$ acts on V naturally, and on W by $g \cdot (v_1v_2v_3) = (gv_1)(gv_2)(gv_3)$. The map φ'_0 is \mathbf{GL}_3 -equivariant, so the image of V under φ'_0 is left by $\mathbf{GL}_3(k)$ invariant. If we fix bases in V and W , we will obtain a representation of $\mathbf{GL}_3(k)$ in $\mathbf{GL}_{10}(k)$.

Let v_0, v_1, v_2 be the standard basis of $V = k^3$. In $W = \text{Sym}^3(V)$ we take the basis

$$(13) \quad v_0^3, v_1^3, v_2^3, 3v_0^2v_1, 3v_1^2v_2, 3v_2^2v_0, 3v_0v_1^2, 3v_1v_2^2, 3v_2v_0^2, 6v_0v_1v_2,$$

and by $\tilde{\varphi}_0$ we denote the corresponding faithful representation $\mathbf{GL}_3(k) \rightarrow \mathbf{GL}_{10}(k)$. Now if we write the image of V under φ'_0 in coordinates relative to the basis (13), we see that $\mathbb{P}(\varphi'_0(V)) = X_0$. So $\tilde{\varphi}_0$ maps $\mathbf{GL}_3(k)$ to $G(X_0, k)$. Since both groups are algebraic and isomorphic, $\tilde{\varphi}_0$ is an isomorphism. Then $d\tilde{\varphi}_0: \mathfrak{sl}_3(k) \rightarrow \mathfrak{g}_0(X_0, k)$ is an isomorphism of Lie algebras. It is a representation of $\mathfrak{sl}_3(k)$ with underlying module $\mathrm{Sym}^3(V)$. Therefore the 10-dimensional natural $\mathfrak{g}_0(X_0, k)$ -module is irreducible with the highest weight $(3, 0)$. \square

The group $\mathrm{Aut}(\mathbb{P}^2)$ is the projectivization of the linear group $\mathbf{GL}_3(k)$. We take the following Borel subgroup of $\mathbf{GL}_3(k)$:

$$B = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \in \mathbf{GL}_3(k) \right\},$$

i.e. the group of upper triangular matrices. As in the case of conics, $\mathbf{GL}_3(k)$ acts transitively on \mathbb{P}^2 and hence via φ_0 also on X_0 . Therefore X_0 is a single orbit of $\mathbf{GL}_3(k)$ in \mathbb{P}^9 .

LEMMA 5.3. *The Borel subgroup B of the group $\mathbf{GL}_3(k)$ has via the action φ_0 (12) a unique fixed point in \mathbb{P}^9 .*

PROOF. As in the proof of Lemma 5.2, we have that $\mathbb{P}^9 = \mathbb{P}(\mathrm{Sym}^3(V))$, $V = k^3$. The Borel subgroup B fixes the unique line in $\mathrm{Sym}^3(V)$, namely the line spanned by the highest weight vector. Hence in \mathbb{P}^9 there is a unique point fixed by B . \square

Let $H \subset \mathfrak{sl}_3(k)$ be a fixed Cartan subalgebra with basis h_1, h_2 which are part of a Chevalley basis of $\mathfrak{sl}_3(k)$. Let τ be a fixed automorphism of $\mathfrak{sl}_3(k)$, such that $\tau(h_1) = h_2$ and $\tau(h_2) = h_1$ (such an automorphism exists by [dG00], §5.11).

LEMMA 5.4. *Let $d\tilde{\varphi}_0: \mathfrak{sl}_3(k) \rightarrow \mathfrak{g}_0(X_0, k)$ be the isomorphism of Lie algebra as above. Let $X \subset \mathbb{P}^9$ be projectively equivalent to X_0 over an extension of k . If there is a k -isomorphism $\rho: \mathfrak{sl}_3(k) \rightarrow \mathfrak{g}_0(X, k)$, then either $d\tilde{\varphi}_0$ and ρ or $d\tilde{\varphi}_0$ and $\rho \circ \tau$ are isomorphic representations. Further, if μ is the module isomorphism, then μ modulo scalar multiplication is a projective equivalence of X_0 and X defined over k .*

PROOF. Since modules of $\mathfrak{g}_0(X_0, \bar{k})$ and $\mathfrak{g}_0(X, \bar{k})$ are isomorphic (Proposition 3.11), $\mathfrak{g}_0(X, k)$ -module is also irreducible. There are exactly two irreducible \mathfrak{sl}_3 -modules of dimension 10. Let h_1, h_2 be as before the lemma. We represent a weight $\lambda \in H^*$ by the tuple $(\lambda(h_1), \lambda(h_2))$. Then the two irreducible \mathfrak{sl}_3 -modules of dimension 10 have highest weights $(3, 0)$ and $(0, 3)$ respectively. By composing $d\tilde{\varphi}_0$ with τ we change the highest weight of the corresponding module (from $(3, 0)$ to $(0, 3)$ or vice versa). Therefore, after

possibly composing ρ with τ we have that the two representations have the same highest weight, and hence are isomorphic. Now the last assertion follows from Lemma 5.3 and Proposition 3.24. \square

Now we have an algorithm which for a surface X in \mathbb{P}^9 given by quadratic forms over k decides whether it is a Del Pezzo surface of degree 9 containing a k -rational point, and if so, finds a k -parametrization.

- (1) Find the Lie algebra $\mathfrak{g}_0(X, k)$ as described in Chapter 3, Section 2.
- (2) Find an associative algebra A such that $A_{\text{Lie}} \cong \mathfrak{g}_0(X, k) \oplus k$ using the algorithm `EnvelopingAlgebra` in Chapter 2, Section 2.
- (3) Construct an isomorphism $\rho': M_3(k) \rightarrow A$ over k (see Chapter 6), inducing so an isomorphism ρ of Lie algebras $\mathfrak{sl}_3(k) \rightarrow \mathfrak{g}_0(X, k)$. If no such isomorphism exists, then X is not isomorphic to X_0 over k .
- (4) Check whether the modules ρ and $d\tilde{\varphi}_0$ or $\rho \circ \tau$ and $d\tilde{\varphi}_0$ are isomorphic. If none of these isomorphisms exists, then X was not Del Pezzo surface of degree 9.
- (5) In the affirmative case in the previous step let $M \in M_{10}(k)$ be the matrix describing the module isomorphism. If M does not map X_0 to X then X was not Del Pezzo surface of degree 9.

The construction in this section generalizes to finding an isomorphism of Severi-Brauer varieties of arbitrary dimension n . The anticanonical class in \mathbb{P}^n has degree $n+1$, so the associated linear system is the space of all forms of degree $n+1$. Therefore the involved module is the module of $(n+1)$ -th symmetric powers of k^{n+1} , which is an irreducible \mathfrak{sl}_{n+1} -module. As a Borel subgroup we can take the group of upper triangular matrices in $\mathbf{GL}_{n+1}(k) = G(\mathbb{P}^n, k)$. It fixes a unique point in the irreducible representation, namely the highest weight vector. The hardest problem is finding an isomorphism of an associative algebra and $M_{n+1}(k)$. In Chapter 6 we give algorithms for algebras up to degree 4.

Testing the algorithm and timings. In the step (3) of the algorithm, the finding isomorphism of an algebra and the full matrix algebra is reduced to solving a norm equation over a cubic field extension, see Chapter 6. When constructing examples by perturbing coefficients in the implicit equations of the standard embedding (12) as in the case of Del Pezzo surfaces of degree 8, we were able to construct the norm equation but it was too hard to solve. Therefore for generating Severi-Brauer surfaces we used the *Galois descent*, a very efficient method based on Galois cohomology. For expositions of the Galois descent see for example [Jac96, Kra01], an explicit method can be found in [Kan90]. In this case the associative algebra corresponding to the surface is found

in a very neat shape: we can very easily construct the norm equation and moreover this equation is easy to solve, even when the coefficients in the implicit equations of the surface are very large as is shown in Table 4.

When using the Galois descent, one has first to take a cubic field extension of the base field (in our case \mathbb{Q}) which is Galois. This is equivalent to adjoining a root of a cubic irreducible polynomial such that the discriminant of the polynomial is a square in the base field. When generating such polynomial, we bound the absolute value of the coefficients in the polynomial. The bound is given in the first column of the table.

field cfs	eqns size	LA size	prm size	time	LA time	normeq time
100	4	3	18	1.94	1.48	0.16
500	6	7	23	2.56	1.85	0.21
1000	7	8	47	3.26	2.05	0.58
5000	11	13	42	3.63	2.62	0.27
10000	9	9	49	3.17	2.26	0.25
50000	10	10	48	3.14	2.29	0.27
100000	12	14	59	3.76	2.70	0.32
500000	13	15	82	4.33	2.60	0.75

field cfs – maximal entry allowed in the minimum polynomial of an algebraic element generating the extension,

eqns size – maximal length of the numerator/denominator of the coefficients in the implicit equations,

Description of the other columns: as in Tables 1 and 2.

TABLE 4. Parametrizing $\mathbb{P}^1 \times \mathbb{P}^1$.

3. More on the algebra of a Severi-Brauer variety

In the previous section we have seen that a given Severi-Brauer variety was a split one if and only if the associative algebra constructed in our algorithm is isomorphic to a matrix algebra. So in the split case we indeed found the algebra A corresponding to the variety \mathcal{V}_A . Here we investigate the associative algebra also in the case of non-split variety.

Using the construction of a variety as the set of left ideals of a central simple algebra, we will show that for curves, the associative algebra constructed by our method is always the algebra corresponding to the given Severi-Brauer curve. For Severi-Brauer varieties of higher dimensions we are able to prove a similar but slightly weaker assertion.

PROPOSITION 5.5. *Let A be a central simple algebra over k and let \mathcal{V}_A be the associated Severi-Brauer variety. Then the groups of k -automorphisms of A and \mathcal{V}_A are isomorphic.*

PROOF. By d we will denote the degree of A and let k' be a splitting field of A , so $A_{k'} \cong M_d(k')$.

Let α be an automorphism of the algebra A . By the Noether-Skolem Theorem, every automorphism of A is inner (see [Pie82], § 12.6), therefore there is $c \in A$ such that $\alpha: x \mapsto c^{-1}xc$. Since the image of a left ideal in $A_{k'}$ under α is again a left ideal, α permutes the set $\{\mathcal{L}\}$ of all d -dimensional left ideals in $A_{k'}$. Now the situation is illustrated by the following diagram:

$$\begin{array}{ccc} \{\mathcal{L}\} & \xrightarrow{\alpha} & \{\mathcal{L}\} \\ \downarrow P & & \downarrow P \\ \mathcal{V}_A & \xrightarrow{\tilde{\alpha}} & \mathcal{V}_A \end{array}$$

where P stands for Plücker embedding and $\tilde{\alpha}$ is a map of \mathcal{V}_A to itself such that the diagram is commutative. From the commutativity then follows that $\alpha \mapsto \tilde{\alpha}$ is a homomorphism of groups. Since P is a bijection between $\{\mathcal{L}\}$ and \mathcal{V}_A , the map $\alpha \mapsto \tilde{\alpha}$ is injective. We claim that $\tilde{\alpha}$ is the restriction of a linear transformation of the projective space to \mathcal{V}_A and that this transformation is defined over the field k .

Let us fix a k -basis in A . Let b_1, \dots, b_d be vectors spanning \mathcal{L} such that their coordinates are with respect to the fixed k -basis of A . The Plücker embedding is taking all $d \times d$ minors of the $d^2 \times d$ matrix b containing the coordinates of the vectors b_i as columns (compare with Example 5.1).

The automorphism α maps the left ideal \mathcal{L} to $\mathcal{L}c$, since for the invertible $c \in A$ we have that $c^{-1}\mathcal{L} = \mathcal{L}$. Let C be the $d^2 \times d^2$ matrix of the linear transformation $x \mapsto xc$ for all $x \in A$, i.e. if v_x is the vector of coordinates of x then Cv_x is the vector of coordinates of xc . Clearly, C is a matrix over k . The Plücker coordinates of $\alpha(\mathcal{L})$ are all $d \times d$ minors of the matrix Cb .

In following for an $m \times n$ matrix M and subsets $I \subset \{1, \dots, m\}$, $J \subset \{1, \dots, n\}$ such that $|I| = |J| = d$ we by $|M|_{I,J}$ mean the minor of the matrix M which is the determinant of the $d \times d$ matrix obtained from M by omitting all rows not in I and all columns not in J .

The Plücker coordinates of \mathcal{L} are $p_I = |b|_{I, \{1, \dots, d\}}$ ($I \subset \{1, \dots, d^2\}$, $|I| = d$). For the Plücker coordinates p'_I of $\alpha(\mathcal{L})$ we then have

$$p'_I = |Cb|_{I, \{1, \dots, n\}} = \sum_{I'} |C|_{I, I'} |b|_{I', \{1, \dots, n\}} = \sum_{I'} |C|_{I, I'} p'_{I'},$$

where the sum is taken through all subsets I' of $\{1, \dots, d^2\}$ of d elements. Since C is a matrix over k , also all its $d \times d$ minors are in k and the claim is proven.

We have shown that for a k -automorphism α is $\tilde{\alpha}$ a k -automorphism of \mathcal{V}_A . Moreover, the group homomorphism $\text{Aut}_k A \rightarrow \text{Aut}_k \mathcal{V}_A$, $\alpha \mapsto \tilde{\alpha}$ is an algebraic map between twists of $\mathbf{PGL}_d(k)$. We have seen that it is injective and therefore from being algebraic it follows that it is also surjective. For, $\mathbf{PGL}_d(k)$ is an irreducible variety, so if the morphism of groups were not surjective, the image of $\text{Aut } A$ would be a subvariety in $\text{Aut } \mathcal{V}_A$ of positive codimension, hence $\alpha \mapsto \tilde{\alpha}$ would not be injective, a contradiction. \square

LEMMA 5.6. *If A is a central simple algebra, then for the Lie algebra $L(\text{Aut } A)$ of the group $\text{Aut } A$ holds $L(\text{Aut } A) \oplus k \cong A_{\text{Lie}}$.*

PROOF. Since each automorphism of A is inner, $\text{Aut } A$ is a projectivization of A^* , the group of all invertible elements in A . An element $a \in A$ is not invertible, if the matrix of the regular representation of a is singular, therefore A^* is a principal open subset of the linear variety A . The Lie algebra $L(A^*)$ is the tangent space to A^* at e , therefore it consists of elements of A and the multiplication in $L(A^*)$ is $[a, b] = ab - ba$, so $L(A^*) = A_{\text{Lie}}$. The claim of the Lemma now follows from $\text{Aut } A = A^*/\mathbf{C}(A^*)$. \square

Summing up, we have the following:

PROPOSITION 5.7. *Let A be a twist of $M_d(k)$ and \mathcal{V}_A the corresponding Severi-Brauer variety. Further let A' be the associative algebra constructed in our algorithm, (i.e. such that $\mathfrak{g}_0(\mathcal{V}_A, k)$ is embedded into A'_{Lie}).*

- (i) *If $d = 2$ then $A' \cong A$.*
- (ii) *If $d > 2$ then either $A' \cong A$ or $A' \cong A^{op}$, the opposite algebra to A .*

PROOF. First, by Proposition 5.5 there is a k -isomorphism of algebraic groups $\text{Aut}(A) \rightarrow \text{Aut}(\mathcal{V}_A)$. Its differential gives a k -isomorphism of their Lie algebras

$$L(\text{Aut}(A)) \rightarrow L(\text{Aut}(\mathcal{V}_A)) = \mathfrak{g}_0(\mathcal{V}_A, k).$$

Suppose first that $d = 2$. Then by Proposition 2.11 there is a unique enveloping algebra A' of $\mathfrak{g}_0(\mathcal{V}_A, k)$ such that $[A' : k] = 4$. (i.e. an algebra A' with an embedding $\mathfrak{g}_0(\mathcal{V}_A, k) \hookrightarrow (A')_{\text{Lie}}$) and our algorithm finds it (see Lemma 2.10). On the other hand A is by

Lemma 5.6 an enveloping algebra of $L(\text{Aut}(A))$. So again by uniqueness in degree 2 case we conclude that $A' \cong A$.

Now if $d > 2$ then again by Lemma 2.10 the enveloping algebra found by the algorithm has dimension d^2 . But Proposition 2.11 together with Lemma 5.6 in this case give that A and A' are either isomorphic or antiisomorphic. \square

Trivializing central simple algebras

Assume that \mathfrak{g} is a simple Lie algebra which is a twist of $\mathfrak{sl}_n(k)$, i.e. $\mathfrak{g} \otimes \bar{k} \cong \mathfrak{sl}_n(\bar{k})$. We want to decide whether \mathfrak{g} is isomorphic to \mathfrak{sl}_n over k and if so, to find an isomorphism.

Because of the algorithm `EnvelopingAlgebra` in Chapter 2, Section 2.2 this is equivalent to deciding whether a given associative algebra A is isomorphic to $M_n(k)$ (see Corollary 2.12) and finding an isomorphism in the affirmative case. The short algorithm for reducing the problem for Lie algebras to a corresponding one for associative algebras could read as follows:

ALGORITHM: `TrivializeLieAlgebra`

INPUT: \mathfrak{g} – a simple Lie algebra which is a twist of $\mathfrak{sl}_n(k)$.

OUTPUT: an isomorphism $\mathfrak{sl}_n(k) \rightarrow \mathfrak{g}$, if it exists.

- (1) $A, \phi: \mathfrak{g} \hookrightarrow A_{\text{Lie}} := \text{EnvelopingAlgebra}(\mathfrak{g})$;
- (2) if $[A : k] > n^2$ then
 return 'failed'
 end if;
- (3) Let $\varphi: M_n(k) \rightarrow A$ be an isomorphism of associative algebras;
 // now φ is also a Lie algebra isomorphism $\mathfrak{gl}_n(k) \rightarrow A_{\text{Lie}}$
- (4) return restriction of φ to $\mathfrak{sl}_n(k)$.

In this chapter we describe the step (3) of the algorithm: for a given central simple algebra of the degree up to 4 we will construct an isomorphism with $M_n(k)$.

1. Cyclic algebras and left ideals

In this section the role of one-sided ideals in a central simple algebra is explored. We give some hints for finding such ideal by reducing the problem to solving a norm equation. Knowing the solution of the norm equation will make it possible to construct an isomorphism with $M_n(k)$. There are already efficient algorithms for deciding whether a given central simple algebra is a full matrix algebra (see for example [IR93]), therefore

assuming that there exists an isomorphism does not impose much restriction. Nevertheless, the decision algorithms, like the mentioned one, do not give an explicit isomorphism in case it exists.

Assume $A \cong M_n(k)$. Then A contains one-sided ideals of dimension n . We will work here with left ideals. Every minimal left ideal in this algebra has dimension n and any nontrivial left ideal is a direct sum of minimal left ideals.

Let \mathcal{L} be an n -dimensional left ideal in A . For any $a \in A$ we have that $\varphi_a: \mathcal{L} \rightarrow \mathcal{L}$, $x \mapsto ax$ is an endomorphism of \mathcal{L} as a vector space. Let us fix a basis b_1, \dots, b_n of \mathcal{L} . Let $\varphi: A \rightarrow M_n(k)$ assign to $a \in A$ the matrix of φ_a with respect to this basis, i.e. the i -th column of $\varphi(a)$ contains the coordinates of ab_i : $ab_i = \sum_j \varphi(a)_{ji} b_j$.

PROPOSITION 6.1. φ is an isomorphism of algebras.

PROOF. Firstly, φ is a homomorphism of algebras. Further φ is a bijection, since otherwise $\text{Ker } \varphi \neq 0$ would be a nontrivial ideal in A . \square

To make use of the proposition, we have to find an n -dimensional left ideal in the algebra A . It might help, if during our computation we hit a zero divisor d . When for such d we define the vector space endomorphism ρ_d of A , $x \mapsto xd$, then both the kernel and the image of ρ_d are nontrivial left ideals of A . If we are lucky enough, or if the algebra A is of degree 2 or 3, then we have found a left ideal of dimension n .

In following, a finite extension k' of the field k is said to be *cyclic*, if $k' = k(a)$ for some algebraic element a and the minimum polynomial of a factors completely over $k(a)$. Such field is Galois and $\text{Gal}(k(a)|k)$ is cyclic.

In our algorithm for finding left ideals, the crucial is the following

DEFINITION 6.2. The algebra A is a *cyclic* of degree n , if there are elements $c, u \in A$ such that $\{c^i u^j \mid i, j = 0, \dots, n-1\}$ is a basis of A over its ground field k , and the multiplication in A is defined by:

- (i) $1, c, \dots, c^{n-1}$ is a basis of a cyclic field extension $k' = k(c)$ of k ,
- (ii) $uc = \sigma(c)u$, where σ is a fixed generator of the Galois group $\text{Gal}(k'|k)$,
- (iii) $u^n = \gamma 1$, where $0 \neq \gamma \in k$.

We will call c a *cyclic element* and u a *principal generator* of A over $k(c)$.

LEMMA 6.3. A cyclic algebra is central simple. If $c \in A$ is the cyclic element as in Definition 6.2, then the centralizer $\mathbf{C}_A(k(c)) = k(c)$, so it is a maximal subfield of A .

PROOF. cf. [Jac89], Theorem 8.7. \square

The main strategy in finding a minimal left ideal is writing a given algebra A as a cyclic algebra, which means to find a cyclic element c and a principal generator u of A over $k(c)$. The reason for doing so is given by

PROPOSITION 6.4. *Let A be a cyclic algebra generated by c and u as in Definition 6.2. Then $A \cong M_n(k)$ if and only if there exists $s \in k(c) \subset A$ such that*

$$(14) \quad N_{k(c)|k}(s) = s\sigma(s) \dots \sigma^{n-1}(s) = \frac{1}{\gamma}.$$

PROOF. We prove the proposition for degree $n = 2$, the other cases can be proven analogously, the proof is just a bit more technical. A proof for any central simple algebra can also be found for example in [Pie82], § 15.1.

Since A is central simple, by Wedderburn's structure theorem it can be either $M_2(k)$ or a division algebra over k . It is the matrix algebra exactly if it has a 2-dimensional left ideal. Let \mathcal{L} be such an ideal and let $0 \neq c_01 + c_1u \in \mathcal{L}$, $c_i \in k(c)$. Then c_0 is nonzero, for otherwise $u \cdot c_1u$ would be an invertible element in \mathcal{L} . Therefore we may suppose $c_0 = 1$ and then \mathcal{L} is spanned by $1 + c_1u$ and $c(1 + c_1u)$. From $u(1 + c_1u) = \sigma(c_1)\gamma + u \in \mathcal{L}$ we get that c_1 is a solution to the norm equation (14). \square

The proof of the previous proposition delivers also an algorithm for finding an isomorphism of a cyclic algebra A and $M_n(k)$: If the norm equation (14) is solvable, then using a solution we can construct an n -dimensional left ideal. The remaining problem is finding a cyclic element in A . In the following sections we discuss this for degrees 2 and 3 and explain how to use the developed methods in case of algebras of degree 4.

2. Algebras of degree 2

This is a classical method which can be found for example in [TW02]. We shortly describe it here for the sake of completeness.

When looking for a cyclic element c we pick an arbitrary noncentral element in A . Its minimum polynomial $\mu_c(\xi)$ is quadratic. In case it is reducible over k , $\mu_c(\xi) = p_1(\xi)p_2(\xi)$, we have also found a zero divisor, for example $p_1(c)$, and are therefore done. Otherwise c generates in A a quadratic field extension of k . By factoring $\mu_c(\xi)$ over $k' = k(c)$ we find $\sigma(c)$. Then we find a principal generator u by solving a linear system of equations $uc = \sigma(c)u$. There exists such invertible u , because the matrices c and $\sigma(c)$ have the same invariant factors and therefore are similar, cf. [Wed64]. Finally, since c and u are generators of A and $u^2c = cu^2$, $u^2 \in \mathbf{C}(A) \cong k$.

In case the field $k = \mathbb{Q}$, there are already much more effective algorithms for finding an isomorphism $M_2(\mathbb{Q}) \rightarrow A$, see [CR03, IS96, Sim05]. Since there is an efficient

algorithm for finding a rational point on a plane conic over \mathbb{Q} implemented in Magma, in our algorithms we reduce the degree 2 case to this problem, as described in detail in Chapter 3, Section 5.

3. Algebras of degree 3

In this case finding a cyclic element in the algebra is more technical. Throughout the whole section we assume that the given algebra A is isomorphic to $M_3(k)$.

LEMMA 6.5. *Let $a \in A$ be a noncentral element such that the minimal polynomial $\mu_a(\xi) \in k[\xi]$ of a is irreducible over k . Then $\deg \mu_a(\xi) = 3$ and every $b \in A$, $b \neq 0$ such that $\mu_a(b) = 0$ is a conjugate of a .*

PROOF. $a \notin \mathbf{C}(A)$ implies $\deg \mu_a(\xi) > 1$. The case $\deg \mu_a(\xi) = 2$ is not possible. For, let $\deg \mu_a(\xi) = 2$, $\mu_a(\xi)$ irreducible. Then the characteristic polynomial $\chi_a(\xi)$ of a is $\chi_a(\xi) = \mu_a(\xi)l(\xi)$ with $l(\xi)$ linear. The factor $l(\xi)$ of the characteristic polynomial of a is irreducible, therefore it divides the minimal polynomial $\mu_a(\xi)$, a contradiction. Since $\mu_a(\xi)$ is irreducible over k and $\mu_a(b) = 0$, it is also the minimal polynomial of b . Then a and b have the same invariant factors and hence are conjugate (cf. [Wed64]). \square

In a given algebra of degree A we will first try to construct an element $u \in A$ such that $u^3 \in \mathbf{C}(A)$, and afterwards a cyclic element $c \in A$ such that u is a principal generator of A over $k(c)$.

We start by picking an arbitrary noncentral element $x \in A$. If x is not invertible or its minimal polynomial $\mu_x(\xi)$ is reducible over k , then we are done, since we have found a zero divisor. So we may assume that $\mu_x(\xi)$ is irreducible. Then by Lemma 6.5 we have $\deg \mu_x(\xi) = 3$.

In the special case when x is already cyclic, we set $c = x$. Then $k' = \langle 1, c, c^2 \rangle_k$ is a maximal subfield generated by c . Let σ denote a generator of $\text{Gal}(k'|k)$. By factoring the minimal polynomial $\mu_c(\xi)$ over k' we find $\sigma(c)$ and afterwards an element $u \in A$ such that $ucu^{-1} = \sigma(c)$ as a nontrivial solution to the linear system $uc = \sigma(c)u$. By Lemma 6.5 such u exists and since it does not commute with c , we have $u \notin k'$. From $u^3cu^{-3} = c$ follows $u^3 \in \mathbf{C}_A(k') = k'$. We can conclude that $u^3 \in k$ since otherwise u^3 would generate k' and $u^3u = uu^3$ would imply $u \in \mathbf{C}_A(k') = k'$, a contradiction. So in the special case the chosen element $x \in A$ is cyclic, we can easily find a principal generator. Therefore in our construction we may assume that $x \in A$ is non-cyclic.

By $A[\xi]$ we denote the ring of polynomials in ξ over the algebra A , where ξ commutes with all elements in A . As usual we say that $a \in A$ is a root of $p(\xi) = c_0 + c_1\xi + \cdots + c_n\xi^n$,

if $c_0 + c_1a + \cdots + c_na^n = 0$. If a is a root of $p(\xi) \in A[\xi]$, then $p(\xi) = q(\xi)(\xi - a)$ for some $q(\xi) \in A[\xi]$, see [Wed64].

Recall that by $[a, b]$ we mean $ab - ba$.

THEOREM 6.6 (Wedderburn's factorization theorem). *Let $a \in A$ have the minimum polynomial $\mu_a(\xi)$ and $m \in A[\xi]$ be such that $\mu_a(\xi) = m(\xi)(\xi - a)$. Then for any $y \in A$ such that $[y, a]$ is invertible, $a' = [y, a]a[y, a]^{-1}$ is a root of $m(\xi)$.*

PROOF. We partly follow [Jac96], Theorem 2.9.1, where the claim is proven for division algebras.

Since μ_a is a polynomial over the field, we have $\mu_a(\xi)y = y\mu_a(\xi)$ and hence $m(\xi)(y\xi - ay) = ym(\xi)(\xi - a)$. Here the left hand side can be written as $m(\xi)(y\xi - ay) = m(\xi)y(\xi - a) + m(\xi)[y, a]$, therefore together it gives $m(\xi)[y, a] = (ym(\xi) - m(\xi)y)(\xi - a)$. After multiplying by the inverse of $[y, a]$ we get $m(\xi) = (ym(\xi) - m(\xi)y)[y, a]^{-1}(\xi - [y, a]a[y, a]^{-1})$. \square

Using Wedderburn's factorization theorem we can over A factorize the minimal polynomial μ_a of the chosen element $a \in A$ into linear factors

$$(15) \quad \mu_a(\xi) = (\xi - a_3)(\xi - a_2)(\xi - a_1)$$

with $a_i \in A$, $a_1 = a$ and $a_2 = [y, a]a[y, a]^{-1}$ for some $y \in A$, unless we hit a zero divisor. Any factorization obtained in this way has useful properties:

LEMMA 6.7. *For $a \in A$ noncyclic with irreducible minimal polynomial, the factorization (15) fulfills the following:*

- (i) $c = [a_1, a_2] = [a_2, a_3] = [a_3, a_1] \neq 0$,
- (ii) c is invertible and $ca_i c^{-1} = a_{i+1}$ (indices reduced mod 3),
- (iii) $c^3 = \gamma$, $\gamma \in k$.

The lemma can be found in [Jac96] as Lemma 2.9.8 for division algebras. Here we give an alternative proof since it is slightly different for the matrix algebra $M_3(k)$. First we have 2 small technical lemmata

LEMMA 6.8. *Let $f, g \in A[\xi]$ be monic polynomials such that $fg \in k[\xi]$. Then $fg = gf$.*

PROOF. Let us denote $p = fg$ and $q = gf$. Using the facts that $p \in k[\xi]$ and f is monic, after matching coefficients in $pf = fq$ we get that $p = q$. \square

LEMMA 6.9. *Let the minimum polynomial of $a \in A$ be irreducible of degree 3. If there is $y \in A$ such that $yay^{-1} \neq a$ and $[yay^{-1}, a] = 0$, then a is cyclic.*

PROOF. We follow [Jac96]. Since $k(a)$ is a maximal subfield of $A = M_3(k)$, $[yay^{-1}, a] = 0$ implies that $yay^{-1} \in k(a)$. It follows that conjugation by y is a field automorphism of $k(a)$ and from $yay^{-1} \neq a$ we have it is a nontrivial automorphism. Therefore $k(a)$ is Galois over k . \square

PROOF OF LEMMA 6.7. First we show that $[a_1, a_2] \neq 0$. For, let $[a_1, a_2] = 0$ whereas $a_2 = [y, a_1]a_1[y, a_1]^{-1} \neq a_1$. But then by Lemma 6.9 is a_1 cyclic, a contradiction.

Next, since $\mu_a(\xi)$ is a polynomial over the field k , the factors can be permuted cyclically (see Lemma 6.8). Then from

$$\begin{aligned} \mu_a(\xi) &= \xi^3 + \alpha_2\xi^2 + \alpha_1\xi + \alpha_0 = (\xi - a_3)(\xi - a_2)(\xi - a_1) \\ &= (\xi - a_1)(\xi - a_3)(\xi - a_2) \\ &= (\xi - a_2)(\xi - a_1)(\xi - a_3) \end{aligned}$$

we get

$$\alpha_1 = a_3a_2 + a_3a_1 + a_2a_1 = a_1a_3 + a_1a_2 + a_3a_2 = a_2a_1 + a_2a_3 + a_1a_3$$

and (i) follows.

To prove (ii) and (iii) we first observe, that $a_3a_2a_1 = a_2a_1a_3 = a_1a_3a_2 = -\alpha_0$. Using this and the part (i) of the lemma we have

$$[a_3, a_1]a_1 = [a_2, a_3]a_1 = a_2a_3a_1 - a_3a_2a_1 = a_2a_3a_1 - a_2a_1a_3 = a_2[a_3, a_1].$$

Similarly we deduce $[a_1, a_2]a_2 = a_3[a_1, a_2]$ and $[a_2, a_3]a_3 = a_1[a_2, a_1]$. Then $c^3a_i = a_ic^3$ for $i = 1, 2, 3$. Since a_i 's generate the whole A , c^3 is in the center of A and (iii) follows. To finish the proof, it remains to show that c is invertible. For, let $c^3 = 0$. Let $\mathcal{L} = Ac$ be a left ideal. Since $c \neq 0$, also $\mathcal{L} \neq 0$. We observe that $(a_ic)^3 = a_ia_{i+1}a_{i+2}c^3 = 0$ (indices reduced mod 3) and conclude that \mathcal{L} is nilpotent (since a_i 's generate A) and hence contained in a nilpotent two-sided ideal (cf. [Jac43], § 4.10, Lemma 2), a contradiction, since A is simple and not nilpotent. \square

Lemma 6.7 gives an algorithm for finding an element $c \in A$ such that c^3 is in the center of A .

ALGORITHM: **CubicRoot**

INPUT: a – an element in A such that the minimal polynomial μ_a is cubic and irreducible over k .

OUTPUT: c – a noncentral element in A such that

- $c^3 \in k$ and
- $(\xi - a')(\xi - cac^{-1})(\xi - a)$ is a factorization of μ_a as in Lemma 6.7.

- (1) $y :=$ an element in A such that $[y, a]$ is invertible and not commuting with a ;
- (2) $a' := [y, a]a[y, a]^{-1}$;
- (3) **return** $[a, a']$.

LEMMA 6.10. *Let $b \in A$, $b \notin k$ such that $b^3 = \beta$, $\beta \in k^*$. Let $\mu_b(\xi) = \xi^3 - \beta = (\xi - b_3)(\xi - b_2)(\xi - b_1)$, $b_1 = b$ be the factorization of its minimal polynomial as in Lemma 6.7. Let $c = [b_1, b_2]$. Then $a = b_1c$ is a cyclic element not in k .*

PROOF. The proof follows word by word the construction for division algebras which can be found in [Jac96], in the proof of Theorem 2.9.17. \square

ALGORITHM: **GeneratorsOfCyclicAlgebra**

INPUT: A – a central simple algebra.

OUTPUT: c – a cyclic element in A ,
 u – a principal generator of A over $k(c)$.

- (1) $x :=$ a noncentral element in A ;
- (2) **if** a is cyclic **then**
 $c := x$;
 $c^\sigma :=$ any other root of μ_c in $k(c)$;
 $u :=$ a nontrivial solution of a linear system $c^\sigma u = uc$;
return c, u
end if;
- (3) **if** $x^3 \in k$ **then** $u' := x$;
else $u' := \text{CubicRoot}(x)$;
end if;
- (4) $u := \text{CubicRoot}(u')$;
- (5) **return** $u'u$ and u .

To complete the section we add the algorithm which constructs a 3-dimensional left ideal in A in case it exists.

ALGORITHM: **FindMinimalLeftIdeal**

INPUT: A – a central simple algebra.

OUTPUT: \mathcal{L} – a three dimensional left ideal in A .

- (1) $c, u := \text{GeneratorsOfCyclicAlgebra}(A)$;
- (2) $\gamma := u^3$; // $\gamma \in k$
- (3) $k' := k(c)$;

- (4) // solve the norm equation
Let s be such that $N_{k'|k}(s) = 1/\gamma$;
- (5) $b := 1 + su + s^\sigma u^2$, where $s^\sigma = usu^{-1}$;
- (6) Let \mathcal{L} be the 3-dimensional left ideal generated by b ;
- (7) return \mathcal{L} .

For each element $a \in A$ which pops up during the computation it is tested whether a is a zero divisor or whether the minimal polynomial μ_a is reducible. In both cases we would have found a zero divisor d . Then either the kernel or the image of $x \mapsto dx$ is already a 3-dimensional left ideal. If this happens, we can skip the rest of computation, in particular we can avoid time-expensive solving of the norm equation.

4. Algebras of degree 4

The main goal in the algorithm for finding an isomorphism of a given algebra A and $M_4(k)$ is finding a zero divisor. For any $d \in A$ we by ρ_d denote the vector space endomorphism of A , $x \mapsto xd$. Both the kernel and the image of ρ_d are left ideals in A . If $d \in A$ is a zero divisor, $\text{Ker } \rho_d$ is clearly nontrivial, and the same with $\text{Im } \rho_d$, since $1 \cdot d \neq 0$. If $\dim \text{Ker } \rho_d = 4$ or $\dim \text{Im } \rho_d = 4$ or $\dim(\text{Ker } \rho_d \cap \text{Im } \rho_d) = 4$, we are done since we can already use Proposition 6.1 and find an isomorphism $A \rightarrow M_4(k)$. Here we first describe how to use other kinds of zero divisors and afterwards how to find one at all.

LEMMA 6.11. *Let $\varphi: A \rightarrow M_4(k)$ be an isomorphism and let $d \in A$ be a zero divisor such that none of $\text{Ker } \rho_d$, $\text{Im } \rho_d$, $\text{Ker } \rho_d \cap \text{Im } \rho_d$ has dimension 4. Then $\varphi(d)$ is similar to one of the following block matrices:*

- (1) $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$, where $D \in M_2(k)$ is an invertible matrix,
- (2) $\begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix}$, where $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

PROOF. We consider the Jordan normal form of $\varphi(d)$. Since $\dim \text{Ker } \rho_d = 8$, we can conclude that $\varphi(d)$ has at most two nonzero eigenvalues. Therefore the minimum polynomial $\mu_d(\xi)$ is reducible and divisible by ξ^2 . If $\mu_d(\xi) = \xi^4$, then we get the case (2) for the Jordan normal form of $\varphi(d)$. If ξ appears in $\mu_d(\xi)$ in degree 3 (i.e. $\varphi(d)$ has exactly one nonzero eigenvalue), then at least one of the three left ideals $\text{Im } \rho_d$, $\text{Ker } \rho_d$, $\text{Im } \rho_d \cap \text{Ker } \rho_d$ is four-dimensional. Lastly, if ξ appears in $\mu_d(\xi)$ exactly in degree 2, we get that the case (1). \square

If $\text{Ker } \rho_d \cap \text{Im } \rho_d = 0$, then d is a zero divisor of type (1) in Lemma 6.11. We define another vector space endomorphism λ_d of A , $x \mapsto dx$. The intersection $A_1 = \text{Im } \rho_d \cap \text{Im } \lambda_d$ is mapped by φ to the subalgebra of all block matrices, where only the upper left 2×2 block is nonzero, so $A_1 \cong M_2(k)$. We find a zero divisor d_1 in A_1 as mentioned in Section 2. Then $\text{Im } \rho_{d_1}$ is a 4-dimensional left ideal in A .

The second case is a bit more tricky. Let d be a zero divisor of type (2). We denote by A_d the centralizer $C_A(d)$ and by $\mathfrak{R}(A_d)$ the Jacobson radical of A_d . Then there is the natural projection $\pi: A_d \rightarrow A_d/\mathfrak{R}(A_d)$ and for this we have

LEMMA 6.12. *The algebra $\pi(A_d)$ is isomorphic to $M_2(k)$. If $e \in \pi(A_d)$ is a zero divisor, then for a generic element f in $\pi^{-1}(e)$ we have $\dim \text{Ker } \rho_f = 4$.*

REMARK 6.13. By saying that something holds for a “generic element” we mean that all elements, for which the assertion is true, form a nonempty Zariski open subset in the set of all considered elements. Therefore we can easily find an element satisfying the condition.

PROOF. We may suppose that $\varphi(d)$ is actually equal to the matrix (2) in Lemma 6.11. Then the image of $A_d = C_A(d)$ under φ is

$$(16) \quad \varphi(A_d) = \left\{ \left(\begin{array}{cccc} \alpha_1 & \beta_1 & \alpha_2 & \beta_2 \\ 0 & \alpha_1 & 0 & \alpha_2 \\ \alpha_3 & \beta_3 & \alpha_4 & \beta_4 \\ 0 & \alpha_3 & 0 & \alpha_4 \end{array} \right) \mid \alpha_i, \beta_i \in k \right\}.$$

The Jacobson radical in $\mathfrak{R}(\varphi(A_d))$ is the set of all $a \in \varphi(A_d)$ such that $\alpha_i = 0$, ($i = 1, \dots, 4$), and $\varphi(A_d)/\mathfrak{R}(\varphi(A_d)) \cong \{a \in \varphi(A_d) \mid \beta_i = 0, i = 1, \dots, 4\}$, which is clearly isomorphic to $M_2(k)$. Let us denote the natural projection $\varphi(A_d) \rightarrow \varphi(A_d)/\mathfrak{R}(\varphi(A_d))$ by π' . If e is a zero divisor in $M_2(k)$, then the preimage $(\pi')^{-1}(e)$ consists of such elements in (16), that α_i 's are fixed and $\alpha_1\alpha_4 = \alpha_2\alpha_3$.

Now for a matrix f' in $(\pi')^{-1}(e)$ we have that $\dim \text{Ker } \rho_{f'} = 4$ if and only if the rank of f' equals 3. The last is equivalent to $\alpha_1\beta_4 + \alpha_4\beta_1 \neq \alpha_2\beta_3 + \alpha_3\beta_2$. Indeed, the rank of f' equals 3 exactly if there is a 3×3 nonzero minor of f' . Such minor can be found as the determinant of a submatrix containing all β_i 's. Hence for a generic $f' \in (\pi')^{-1}(e)$ we have $\dim \text{Ker } \rho_{f'} = 4$, so $\varphi^{-1}(f')$ gives us a minimal left ideal in A . \square

From the proof of the previous Lemma it also follows that we can compute the the Jacobson radical of A very easily, namely $\mathfrak{R}(A_d) = \text{Ker } \rho_d \cap \text{Ker } \lambda_d$.

FUNCTION: FindMinimalLeftIdeal

INPUT: A – an associative algebra isomorphic to $M_4(k)$,
 d – a zero divisor in A .

OUTPUT: \mathcal{L} – a four-dimensional left ideal in A .

```

(1) if dim Ker  $\rho_d = 4$  then return Ker  $\rho_d$ ;
    elif dim Im  $\rho_d = 4$  then return Im  $\rho_d$ ;
    elif dim Ker  $\rho_d \cap$  Im  $\rho_d = 4$  then return Ker  $\rho_d \cap$  Im  $\rho_d$ ;
    end if;
(2) if dim Ker  $\rho_d \cap$  Im  $\rho_d = 0$  then
     $A_1 :=$  Im  $\rho_d \cap$  Im  $\lambda_d$ ;
     $d_1 :=$  zero divisor in  $A_1$ ;
    return Im  $\rho_{d_1}$  ( $d_1$  dealt here as an element in  $A$ );
    end if;
(3)  $\mathfrak{R} :=$  Ker  $\rho_d \cap$  Ker  $\lambda_d$ ;
     $A_d := A/\mathfrak{R}$ ; let  $\pi$  be the natural projection  $A_d \rightarrow A_d/\mathfrak{R}$ ;
     $e :=$  zero divisor in  $A_d$ ;
    // find  $f' \in \pi^{-1}(e)$  such that dim Ker  $\rho_{f'} = 4$ 
    fix an element  $f'_0 \in \pi^{-1}(e)$  and a basis  $(b_1, b_2, b_3, b_4)$  of  $\pi^{-1}(e) - f'_0$ ;
     $m := 1$ ;
    repeat
    for each  $(c_1, c_2, c_3, c_4)$  such that  $\sum_i |c_i| = m$  do
     $f' := f'_0 + \sum_i c_i b_i$ ;
    if dim Ker  $\rho_{f'} = 4$  then return Ker  $\rho_{f'}$ ; end if;
    end for;
     $m := m + 1$ ;
    until false.

```

Note that the repeat-loop in the last step of the algorithm terminates. Indeed, the preimage $\pi^{-1}(e)$ is a 4-dimensional affine space. For each point in $\pi^{-1}(e)$ with integral coefficients it is tested whether it lies in the Zariski open set given by $\alpha_1\beta_4 + \alpha_4\beta_1 \neq \alpha_2\beta_3 + \alpha_3\beta_2$ ($\alpha_i \in k$ and β_i are indeterminates) with respect to some coordinate system in $\pi^{-1}(e)$. Clearly, the closed complement of this set does not contain a 4-dimensional lattice, therefore a desired element is hit and the loop is left.

The last point to explain is the first step of the algorithm: finding any zero divisor. We start by finding a quadratic element, i.e. an element a such that the minimum polynomial $\mu_a(\xi)$ is irreducible quadratic.

LEMMA 6.14 (Rowen). *Let $c \in A$ have the minimum polynomial $\mu_c(\xi) = \xi^4 + \alpha_2\xi^2 + \alpha_1\xi + \alpha_0$. Then for any factorization $\mu_c(\xi) = (\xi^2 + a'\xi + b')(\xi^2 + a\xi + b)$ in $A[\xi]$ we have $[k(a^2) : k] < 4$.*

PROOF. First denote $\nu(\xi) = (\xi^2 + a\xi + b)(\xi^2 + a'\xi + b') = \xi^4 + \beta_2\xi^2 + \beta_1\xi + \beta_0$ with β_i 's possibly in the algebra. By comparing coefficients in $(\xi^2 + a\xi + b)\mu_c(\xi) = \nu(\xi)(\xi^2 + a\xi + b)$ we obtain $\nu(\xi) = \mu_c(\xi)$. Further we basically follow the proof in [Row78], where a slightly stronger assertion is proven for division algebras.

By matching coefficients in $\mu_c(\xi)$ we get $a' = -a$ and

$$\begin{aligned}\alpha_2 &= b + b' + a'a = b + b' - a^2, \\ \alpha_1 &= a'b + b'a = -ab + b'a, \\ \alpha_0 &= b'b = bb' \quad (\text{from } \alpha_0 = \beta_0).\end{aligned}$$

Case 1: $ab = ba$. Then also $ab' = b'a$ and $\alpha_1 = (b' - b)a$. It follows that $\alpha_1^2 = ((b' + b)^2 - 4\alpha_0)a^2 = ((a^2 + \alpha_2)^2 - 4\alpha_0)a^2 = (a^2)^3 + 2\alpha_2(a^2)^2 + (\alpha_2^2 - 4\alpha_0)a^2$, so $[k(a^2) : k] \leq 3$.

Case 2: $ab \neq ba$. By multiplying $\alpha_2 = b + b' - a^2$ by b from left and right we get $a^2b = ba^2$. Therefore $a \notin k(a^2)$, so $[k(a^2) : k] < [k(a) : k] \leq 4$. \square

The Rowen's lemma gives a recipe for finding a quadratic element as follows. We start with an arbitrary noncentral $c \in A$. If c happens to be a zero divisor or the minimum polynomial μ_c is reducible then we are done and do not need to continue in finding a quadratic element. So we can assume now that neither c is a zero divisor nor μ_c is reducible. Then the minimum polynomial μ_c is not cubic. Indeed, the characteristic polynomial $\chi_c(\xi) = \mu_c(\xi)\lambda(\xi)$, $\lambda \in k[\xi]$ linear, and since every irreducible factor of the characteristic polynomials divides also the minimum polynomial, we have $\lambda(\xi) \mid \mu_c(\xi)$. Hence if c itself is not quadratic, its minimum polynomial is irreducible of degree 4. After applying a linear substitution eliminating the cubic term in $\mu_c(\xi)$ we may use Wedderburn's factorization theorem to construct a factorization as in Rowen's lemma. If a^2 is not a zero divisor and the minimum polynomial of a^2 is not reducible (in which case we would be done), then there are 3 possibilities left:

- (a) $[k(a^2) : k] = 2$, so a^2 is quadratic, or
- (b) $a^2 \in k^*$, then a is quadratic, since otherwise the constructed factorization according to Rowen's lemma would be a factorization over k , or lastly
- (c) $a^2 = a = 0$, then $\mu_c(\xi) = \xi^4 + \alpha_2\xi^2 + \alpha_0$ and c^2 is quadratic.

In sequel we will need the well-known

THEOREM 6.15 (Double Centralizer Theorem). *Let B be a central simple algebra over k and suppose that C is a simple subalgebra of B . Then*

- (i) $\mathbf{C}_B(C)$ is simple,
- (ii) $[C : k] [\mathbf{C}_B(C) : k] = [B : k]$,
- (iii) $\mathbf{C}_B(\mathbf{C}_B(C)) = C$.

PROOF. cf. [Pie82], p. 232. □

Let $a \in A$ be a quadratic element, so $k(a)$ is a subfield of A and $[k(a) : k] = 2$. Then by the Double Centralizer Theorem, the centralizer of a in A is a simple algebra of dimension 8 over k . The center of $\mathbf{C}_A(a)$ is the field $k(a)$, therefore $\mathbf{C}_A(a)$ can be understood as a central simple algebra over $k(a)$. We denote this algebra by A_2 .

LEMMA 6.16. *A_2 is isomorphic to $M_2(k(a))$.*

PROOF. Let \mathcal{L} be a 4-dimensional left ideal in A . If we understand $A_2 = \mathbf{C}_A(a)$ as an algebra over k , then \mathcal{L} is also a 4-dimensional A_2 -module. Let $0 \neq b_1 \in \mathcal{L}$ and let $b_2 \in \mathcal{L}$ be such that $b_2 \notin \mathbf{C}(A_2)b_1$. Then b_1, b_2 is a basis of \mathcal{L} over $k(a)$. So we have a 2-dimensional A_2 -module over $k(a)$, where A_2 is now taken to be an algebra over $k(a)$. Since A_2 acts faithfully on \mathcal{L} , this gives an embedding of A_2 into $M_2(k(a))$. Now the assertion of the Lemma follows from $[A_2 : k(a)] = 4$. □

After finding the algebra A_2 as the centralizer of a quadratic element a , we write A_2 as a cyclic algebra over $k' = k(a)$, so we find a cyclic element $c \in A_2$ and u' such that $(u')^2 = \gamma \in (k')^*$. By Proposition 6.4 there is $s \in k'(c)$ such that $s\sigma(s) = 1/\gamma$. Then also $u = su'$ is a principal generator of A_2 over $k'(a)$ and moreover $u^2 = 1$. We found an element $u \in A$ with the reducible minimum polynomial $\mu_u(\xi) = \xi^2 - 1$, therefore $u + 1$ is a zero divisor.

FUNCTION: FindZeroDivisor

INPUT: A – an associative algebra isomorphic to $M_4(k)$.

OUTPUT: d – a zero divisor in A .

- (1) // find a quadratic element $a \in A$
 - $c :=$ a noncentral element in A ;
 - $c := c + c_3/4 * 1$, where c_3 is the cubic coefficient in μ_c ;
 - if $\deg \mu_c = 2$ then $a := c$;
 - elif $\mu_c(\xi) = \xi^4 + \alpha_2\xi^2 + \alpha_0$ then $a := c^2$; // case (c)
 - else
 - find a factorization $\mu_c(\xi) = (\xi^2 + a'\xi + b')(\xi^2 + a\xi + b)$ over A ;

```

    if  $a^2 \notin k$  then  $a := a^2$ ; end if; // cases (a) and (b)
end if;
(2)  $A_2 :=$  the centralizer of  $a$  in  $A$  regarded as a four-dimensional central algebra
over  $k(a)$ .
(3) // write  $A_2$  as a cyclic algebra over  $k(a)$ 
 $c :=$  a noncentral element in  $A_2$ ;
find  $\sigma(c) \in k(a, c)$  such that  $\mu_c(\xi) = (\xi - c)(\xi - \sigma(c))$ ;
 $u' :=$  a nonzero solution of the linear system  $u'c = \sigma(c)u'$ ;
 $\gamma := (u')^2$ ; // ( $\gamma \in k(a)$ )
(4) if  $\exists r \in k(a)$  such that  $r^2 = \gamma$  then  $u := u'/r$ ;
else
     $s :=$  a solution of the norm equation  $s\sigma(s) = 1/\gamma$ ; // ( $s \in k(a)$ );
     $u := su'$ ;
end if;
(5) return  $u + 1$ .

```

As in the case of algebras of degree 3, for each element popping up during the computation it is tested whether it already accidentally gives a zero divisor. Any kind of the zero divisor would lead to avoiding solving the norm relative equation, which is the most expensive step in the algorithm.

Bibliography

- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24:235–265, 1997. Computational algebra and number theory (London, 1993).
- [Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.
- [Cas78] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978.
- [CR03] J. E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comp.*, 72(243):1417–1441 (electronic), 2003.
- [dG00] Willem A. de Graaf. *Lie algebras: theory and algorithms*, volume 56 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 2000.
- [dGHPS06] W. A. de Graaf, M. Harrison, J. Pílníková, and J. Schicho. A Lie algebra method for rational parametrization of Severi-Brauer surfaces. *Journal of Algebra*, 303(2):514–529, 2006.
- [dGPS] W. A. de Graaf, J. Pílníková, and J. Schicho. Parametrizing Del Pezzo surfaces of degree 8 using Lie algebras. submitted.
- [FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.
- [Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.
- [HS06] M. Harrison and J. Schicho. Rational parametrisation for degree 6 del pezzo surfaces using lie algebras. In *Proc. ISSAC 2006*, 2006.
- [Hum72] James E. Humphreys. *Introduction to Lie algebras and representation theory*. Springer-Verlag, New York, 1972. Graduate Texts in Mathematics, Vol. 9.
- [Hum75] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.
- [IR93] Gábor Ivanyos and Lajos Rónyai. Finding maximal orders in semisimple algebras over \mathbf{Q} . *Comput. Complexity*, 3(3):245–261, 1993.
- [IS96] Gábor Ivanyos and Ágnes Szántó. Lattice basis reduction for indefinite forms and an application. *Discrete Math.*, 153:177–188, 1996.
- [Isk80] V.A. Iskovskih. Minimal models of rational surfaces over arbitrary fields. *Math. USSR Izv.*, 14:17–39, 1980.
- [Jac43] Nathan Jacobson. *The Theory of Rings*. American Mathematical Society Mathematical Surveys, vol. I. American Mathematical Society, New York, 1943.
- [Jac79] Nathan Jacobson. *Lie algebras*. Dover Publications Inc., New York, 1979. Republication of the 1962 original.

- [Jac89] Nathan Jacobson. *Basic algebra. II*. W. H. Freeman and Company, New York, second edition, 1989.
- [Jac96] Nathan Jacobson. *Finite-dimensional division algebras over fields*. Springer-Verlag, Berlin, 1996.
- [Jah00] Jörg Jahnel. The Brauer-Severi variety associated with a central simple algebra: A survey. Linear Algebraic Groups and Related Structures Preprint Server, <http://www.mathematik.uni-bielefeld.de/LAG/man/052.html>, 2000.
- [Kan90] Ming Chang Kang. Constructions of Brauer-Severi varieties and norm hypersurfaces. *Canad. J. Math.*, 42(2):230–238, 1990.
- [Kra01] Daniel Krashen. *Birational isomorphisms between Severi-Brauer varieties*. PhD thesis, The University of Texas at Austin, August 2001.
- [Lan97] Segre Lang. *Survey of Diphantine Geometry*. Springer-Verlag, Berlin Heidelberg, 1997.
- [Man86] Yu. I. Manin. *Cubic forms*, volume 4 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, second edition, 1986. Algebra, geometry, arithmetic, Translated from the Russian by M. Hazewinkel.
- [Mor69] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.
- [Pie82] Richard S. Pierce. *Associative algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982. Studies in the History of Modern Science, 9.
- [PT04] Bjorn Poonen and Yuri Tschinkel, editors. *Arithmetic of higher-dimensional algebraic varieties*, volume 226 of *Progress in Mathematics*, Boston, MA, 2004. Birkhäuser Boston Inc.
- [Row78] Louis Halle Rowen. Central simple algebras. *Israel J. Math.*, 29(2-3):285–301, 1978.
- [SB92] N. I. Shepperd-Barron. The rationality of quintic Del Pezzo surfaces – a short proof. *Bull. London Math. Soc.*, 24:249–250, 1992.
- [Sch98] J. Schicho. Rational parametrization of surfaces. *J. Symbolic Comput.*, 26(1):1–29, 1998.
- [Sch00] J. Schicho. Proper parametrization of surfaces with a rational pencil. In *Proc. ISSAC 2000*, pages 292–299. ACM Press, 2000.
- [Sha94] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.
- [Sim05] Denis Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Math. Comp.*, 74:1531–1543, 2005.
- [Spr98] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, second edition, 1998.
- [TW02] Jacques Tits and Richard M. Weiss. *Moufang polygons*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.
- [Wed64] J. H. M. Wedderburn. *Lectures on matrices*. Dover Publications Inc., New York, 1964.

Jana Pílníková

CONTACT INFORMATION

Address: RICAM, Altenbergerstrasse 52, A-4040 Linz, Austria
Phone: +43 732 2468 5229
E-mail: janka.pilnikova@oeaw.ac.at
Web: www.risc.uni-linz.ac.at/people/janka/

PERSONAL

Born: March 1, 1975 in Žiar nad Hronom, Slovakia
Citizenship: Slovakia

EDUCATION

1999: Magister in mathematics, Comenius University, Bratislava, Slovakia
since 2002: Ph.D. student in mathematics, RISC, Johannes Kepler University, Linz, Austria

POSITIONS

1994–96: Teacher of computer science (on elementary school), Slovakia
1998–99, 2000–02: Software developer, WOC, Slovakia
1999–2000: Ph.D. student, Comenius University, Bratislava, Slovakia
September 2004: Visiting scholar, University of Sydney, Australia
since 2002: Research assistant SFB F013 "Numerical and Symbolic Scientific Computing", Linz, Austria