TECHNISCHE UNIVERSITÄT MÜNCHEN
Zentrum Mathematik

Algorithms for Fields and an Application to a Problem in Computer Vision

Anna Katharina Binder

TECHNISCHE UNIVERSITÄT MÜNCHEN
Zentrum Mathematik

Algorithms for Fields and an Application to a Problem in Computer Vision

Anna Katharina Binder

Vollständiger Abdruck der von der Fakultät für Mathematik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Vorsitzender:		Univ.-Prof. Dr. Peter Rentrop
Prüfer der Dissertation:	1.	Univ.-Prof. Dr. Gregor Kemper
	2.	Univ.-Prof. Dr. Dr. Jürgen Richter-Gebert
	3.	Univ.-Prof. Dr. Peter Müller Julius-Maximilians-Universität Würzburg

Die Dissertation wurde am 26. 03. 2009 bei der Technischen Universität eingereicht und durch die Fakultät für Mathematik am 13. 07. 2009 angenommen.

Für meine Eltern.

Abstract

This thesis is composed of several different parts. We start with an investigation of an important problem in computer vision. An appropriate mathematical modeling of this problem motivates a problem in invariant theory, the examination of the natural action of the group $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$ on the set of n-point configurations $(\mathbb{P}^m_K)^n$ (for some infinite field K and some $m, n \in \mathbb{N}$).
This in turn leads to an investigation of algorithms for fields. We develop an algorithm for the intersection of fields (in special cases) and a method for testing whether a field is algebraically closed in another field. Moreover, we give an algorithm for testing simpleness of a field extension as well as finding – if applicable – a generating element. The latter leads to a new proof of a generalized version of the Theorem of Lüroth.
Another approach to solve problems in field theory is given by the theory of cross-sections of rational maps. We provide a survey on cross-sections and give a criterion for their existence. This yields an algorithm for testing field membership.
Finally, we come back to the examination of the natural action of the group $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$ on the set of n-point configurations. We determine generators of the corresponding invariant field and investigate their separating properties.

Zusammenfassung

Die vorliegende Arbeit setzt sich aus verschiedenen Teilen zusammen. Wir beginnen mit der Untersuchung eines wichtigen Problems aus der *computer vision*. Eine mathematische Modellierung dieses Problems motiviert ein Problem aus der Invariantentheorie, nämlich die Untersuchung der natürlichen Operation der Gruppe $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$ auf der Menge der n-Punktkonfigurationen $(\mathbb{P}^m_K)^n$ (für einen unendlichen Körper K und $m, n \in \mathbb{N}$).
Das wiederum motiviert eine Untersuchung von Algorithmen für Körper. Wir entwickeln einen Algorithmus zur Berechnung des Schnittes von Körpern (für spezielle Fälle) und ein Verfahren um zu testen, ob ein Körper in einem anderen Körper algebraisch abgeschlossen ist. Ferner geben wir einen Algorithmus an, der eine Körpererweiterung auf Einfachheit testet und gegebenenfalls ein erzeugendes Element findet. Letzteres führt zu einem neuen Beweis einer verallgemeinerten Version des Satzes von Lüroth.
Eine weitere Herangehensweise, um Probleme aus der Körpertheorie zu lösen, liefert die Theorie der Sektionen von rationalen Abbildungen. Wir geben einen Überblick über Sektionen und entwickeln ein Kriterium für deren Existenz. Dies führt zu einem Algorithmus, der das Enthaltensein in einem Körper testet.
Schließlich kommen wir auf die Untersuchung der Operation der Gruppe $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$ auf der Menge der n-Punktkonfigurationen zurück. Wir bestimmen Erzeuger des zugehörigen Invariantenkörpers und untersuchen deren Trennungseigenschaften.

Contents

Introduction

The original question which eventually lead to this thesis was a problem placed in the field of computer vision. Computer vision may be best described as the science which is concerned with the problem of obtaining information from images in an algorithmic way. Its ultimate goal is the construction of computer programs that 'see'. These programs can then be used in a variety of applications including search engines for image databases and 'seeing' robots, just to name two of them.
It comes as no surprise that computer vision – as a very practical discipline – heavily depends on the concrete fields of application. In particular, there does not exist the one and central problem of computer vision which can be written down in a formal way. Quite the contrary, there are various rather different interesting questions and areas of research. The problem which will play a central role in my thesis is the following.

> Given two (two-dimensional) images of flat objects in three-dimensional space, is it possible to decide whether they show the same objects or not? To put it more practically, is it possible for a machine to recognize a flat object in three-dimensional space from a two-dimensional picture as it is provided for example from a digital camera?

It turns out that algebraic methods can be used to give an answer to this problem. For doing this, the flat object is replaced by a finite set of points lying in a plane. This set of, say n, points may be thought of as a description of the boundary of the flat object. Rephrasing* this simplified problem in mathematical language and formulating it for arbitrary dimensions leads to the following situation.

> Let $P_1, \dots, P_n,\ Q_1, \dots, Q_n \in \mathbb{P}^m$ be points in a projective space. Does there exist a projectivity $\sigma \in \mathrm{PGL}_{m+1}$ such that $P_i = \sigma(Q_i)$ for all $i \in \{1, \dots, n\}$? Since – as will be seen – the concrete numbering of the points is not known in the applications, this question should be posed more generally. Does there exist a projectivity $\sigma \in \mathrm{PGL}_{m+1}$ and a permutation $\pi \in \mathrm{S}_n$ such that $P_i = \sigma(Q_{\pi(i)})$ for all $i \in \{1, \dots, n\}$? In fact, the concrete elements σ and π are not of particular interest. Therefore, it would be sufficient to just be able to answer this question with yes or no.

As this formulation might suggest, methods of invariant theory can be used to examine this problem. Kemper and Boutin have already done this partially, they have treated a

*A detailed treatment of how this translation from computer vision to mathematical language can be done will be given in the next chapter. This will also include precise definitions of the terms which are used intuitively in this introduction.

special case thereof in [BK05]. In this thesis, I have followed their path and have specified a set of (rational) invariants which separate orbits of almost all n-point configurations under a certain group action of $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$.

Rational invariants of n-point configurations tend to be very large when writing them down. Therefore, I have used computer algebra systems for various concrete computations. Needless to say, the computer has also been used to do experiments with the given mathematical data. In fact, this experiments made me realize that there are still open questions for dealing with finitely generated field extensions algorithmically. This in turn caused me to temporarily digress from the path of computer vision and invariant theory and enter the world of computational algebra. Consequently, a big part of this thesis will be devoted to computational problems in field theory.

Another aspect which attracted my attention during research is the notion of a cross-section of a rational map in algebraic geometry. Historically, cross-sections of rational maps have been used extensively for the solutions of problems in invariant theory. In fact, the solution of the invariant theoretical problem from above is also based on the concept of a cross-section. I have thus included a thorough examination of cross-sections in this thesis, too.

Main Results

Computational field theory. The notion of a field is one of the most basic and important concepts of algebra. It therefore comes as no surprise that significant effort has been put into the development of algorithms for dealing with fields computationally. Müller-Quade and Steinwandt who provided several algorithms for fields on the basis of the theory of Gröbner bases perfectly deserve to be mentioned in this context. In this thesis, their ideas are carried on and some new algorithms for fields are developed.
Except for the special case treated in [SMQ00] – to the best of my knowledge – there has not been published any method for computing intersections of fields. In this thesis, an algorithm is presented for intersecting fields of characteristic zero which are algebraically closed in some surrounding field. In fact, the algorithm is not limited to fields with this property, it yields correct results for arbitrary fields in arbitrary characteristic as long as it terminates. Furthermore, a method is given for testing whether a field is algebraically closed in another field or not. Apart from being useful on its own, the latter method turns out to be very convenient for verifying the input data of the former algorithm about the intersection of fields.
Another part of computational field theory in this thesis is devoted to simple field extensions, i. e. extensions which are generated by one single element. These examinations not only produce an algorithm for testing simpleness of a field extension as well as finding – if applicable – a generating element, but also lead to a novel proof of a generalized version of the well-known Theorem of Lüroth.

Theory of cross-sections – computational aspects. Closely related to field theory,

another topic of this thesis is the notion of a cross-section of a rational map. Classically, cross-sections have been used in invariant theory, but in fact, they are also a valuable tool for algebraic geometry in general. In this thesis, a basic examination of cross-sections of rational maps is given. In particular, this includes a criterion about the existence of a cross-section. For a special class of fields, the results about cross-sections lead to an alternative algorithm for testing field membership.

Application in computer vision – a result in invariant theory. Finally, as an important application of the developed theory, a real-world problem of computer vision is examined. This includes both a mathematical modeling as well as a solution of the resulting problem. To be more explicit, the final solution consists of an explicit construction of the generators of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$. It has been put some effort on this construction to work for arbitrary infinite fields K and for arbitrary $n, m \in \mathbb{N}$.

Structure of the Thesis

In the first chapter, an introduction to computer vision is given. There is a special focus on the problem of recognizing flat objects from their images, as indicated above. It will be shown in a detailed way how this real-world problem translates to a problem in abstract algebra.

In the second chapter, field theory is examined from a computational point of view. A method is given for testing whether a field is algebraically closed in another field. Moreover, this chapter includes an algorithm for the computation of the intersection of two subfields of a field (in special cases). Finally, it is shown how the simpleness of a field extension can be checked algorithmically. Interestingly enough, the construction of this latter algorithm produces a complete proof of the Theorem of Lüroth.

The notion of a cross-section of a rational map plays a central role in chapter three. First, an introduction to algebraic geometry is given which covers the basic material which is needed for defining and using cross-sections. Then a criterion about when cross-sections exist is established. As will be seen, cross-sections can be used for computational methods in field theory, too. In particular, an algorithm for deciding field membership and finding a representation of a given element in certain generators of the field is presented. This extends the toolbox of algorithms for fields as introduced in the second chapter. Finally, the chapter closes with some additional information about cross-sections in the context of invariant theory.

In Chapter four, the concrete mathematical questions formulated in chapter one are reconsidered. Using the methods developed in the second and third chapter, a thorough examination of these questions is given.

An implementation of the algorithm for intersecting fields from Chapter 2 can be found in the appendix.

Requirements. For all parts of this thesis, it is assumed that the reader has a background in commutative algebra. The understanding of Chapter 4 requires a basic knowledge of Galois theory for finite field extensions. An introduction to commutative algebra can be found in [Eis95], field theory (including the theory of Galois) is treated in detail in [Lan02].

Acknowledgements

I would like to express my gratitude to my advisor Prof. Dr. Gregor Kemper for his excellent mentoring of my dissertation. I appreciated his valuable comments which saved me from unpromising paths and motivated me to keep on with my research. On the other hand, I also very much enjoyed the independence that I was granted. This combination gave me a perfect medium for research.
Special thank goes to Prof. Dr. Vladimir L. Popov for our fruitful conversations about sections of rational maps.
It was an honour for me that I have been supported by the programme "TopMath – Angewandte Mathematik mit Promotion" which not only funded conference visits but also offered interesting workshops in many different disciplines of mathematical science. I would like to thank Dr. Christian Kredler, Dr. Ralph Franken and Andrea Echtler for their great commitment within this program.
Last but not least, I thank the Konrad-Adenauer-Stiftung which supported this dissertation financially. I very much enjoyed being part of this foundation, especially being a member of the group of scholarship holders in Munich ("Gruppe 5"). In this context, I cordially thank Prof. Dr. Dieter Witt for his perfect supervision of this group.

1 A Problem in Computer Vision

A key requirement for a universal robot which can move freely in three-dimensional space is the ability to interact with the environment in a reasonable way. But how can the robot gather information about the environment? How can it be provided with basic 'human' sensing capabilities? As most biological systems use vision as their primary sense for orientation, it seems to be reasonable to concentrate on the visual capabilities. From a technical point of view this amounts to the processing of images generated by cameras installed on the robot. It is the scientific discipline of computer vision where the problems evolving from such situations are investigated.
Computer vision – as the science which examines the problem of obtaining information from images algorithmically – has many different fields of application and of course is not restricted to robotics. For example, search engines for the internet heavily use techniques of computer vision to index images.
Usually, the problems of computer vision strongly vary with the concrete fields of applications. But what is common to all questions of computer vision is the fact that they work with (photographic) images of objects. Of course, such images depend on many factors. It thus comes as no surprise that invariant theory – as a theory which examines the inherent characteristics of objects – comes in when we want to understand images.

In this chapter, we want to examine one concrete problem of computer vision from the invariant theoretical point of view. For a comprehensive introduction to computer vision and a detailed treatment of various other problems in this field, see for example [Fau93]. This book also served as a basis for this chapter.

'Our' problem shall be given as follows.

Problem 1.1. *Consider two (photographic) images of a flat object in three-dimensional real space. Is there a way to decide whether the two images show the same object (possibly from a different perspective) or not?*

Note that a solution of this problem could be relevant for a variety of applications, for example the recognition of road signs, just to name one of them.
Usually, invariant theory comes in as a second stage method which means the following. First, various heuristics are applied to the raw image to detect points and/or edges. Then a simplified version of the image – given in the form of a set of points and/or edges – is passed to the invariant theoretical part of the 'problem solver' as a second step. Regarding

just the second stage, i. e. the set of points, the above problem can be simplified to the following situation.

Problem 1.2. *Consider a set of n points in three-dimensional real space $\mathbb{R}^3$. We say that such a set of n points is* **flat** *if all its points lie in a plane. Given two (photographic) images of a flat set of n points, is there a way to decide whether the two images show the same flat n-point set (possibly from a different perspective) or not?*

The aim of this chapter is the formulation of this problem in the language of invariant theory. For doing this, we first investigate the operation of taking photographs from a mathematical point of view. After this, we will be able to systematically analyze the operation of taking photographs of flat objects from different perspectives. This will finally lead to an invariant theoretical characterization of Problem 1.2.

1.1 Some Projective Geometry

We give a rough survey on the concepts of projective geometry over the real numbers $\mathbb{R}$ which are needed for the material presented in this chapter. Note that the following carries over word by word to arbitrary infinite fields. Later, in Chapter 3, where we provide an introduction to algebraic geometry, we will work with projective geometry over arbitrary algebraically closed fields.

The central object in projective geometry over the real numbers is the **projective n-space** over $\mathbb{R}$, denoted by $\mathbb{P}^n_{\mathbb{R}}$ or simply $\mathbb{P}^n$. In brief, it is defined as the set of pointed lines through the origin in the $(n+1)$-dimensional real space $\mathbb{R}^{n+1}$. A more formal definition of $\mathbb{P}^n_{\mathbb{R}}$ is the following. The projective n-space is the set of equivalence classes of points in $\mathbb{R}^{n+1}\setminus\{0\}$, where two points $(\xi_1,\ldots,\xi_{n+1}),(\zeta_1,\ldots,\zeta_{n+1})\in\mathbb{R}^{n+1}\setminus\{0\}$ are equivalent if and only if there exists $\lambda\in\mathbb{R}^\times := \mathbb{R}\setminus\{0\}$ such that $\zeta_i=\lambda\cdot\xi_i$ for all $i\in\{1,\ldots,n+1\}$. For a point $(\xi_1,\ldots,\xi_{n+1})\in\mathbb{R}^{n+1}\setminus\{0\}$, the corresponding equivalence class, say P, is written as $(\xi_1:\ldots:\xi_{n+1})$. We then also say that P has **homogeneous coordinates** $(\xi_1:\ldots:\xi_{n+1})$.

The space $\mathbb{R}^n$ can be embedded in a natural way in the projective n-space $\mathbb{P}^n$ by sending $(\xi_1,\ldots,\xi_n)\in\mathbb{R}^n$ to the point $(\xi_1:\ldots:\xi_n:1)\in\mathbb{P}^n$. The points of $\mathbb{P}^n$ which are not contained in the image of this embedding, i. e. the points of the form $(\zeta_1:\ldots:\zeta_n:0)\in\mathbb{P}^n$, are called the **points at infinity**. In case that $n=2$, the set of points at infinity is called the **line at infinity**.

Let $\sim$ be the equivalence relation on the set of elements of the general linear group $\mathrm{GL}_{n+1}(\mathbb{R})$ of degree $n+1$, where two elements $A,B\in\mathrm{GL}_{n+1}(\mathbb{R})$ are equivalent with respect to $\sim$ if and only if there exists $\lambda\in\mathbb{R}^\times$ such that $B=\lambda\cdot A$. Then every equivalence class in $\mathrm{GL}_{n+1}(\mathbb{R})/\sim$ defines a map $\mathbb{P}^n\longrightarrow\mathbb{P}^n$. A map of this type is called a **projectiv-**

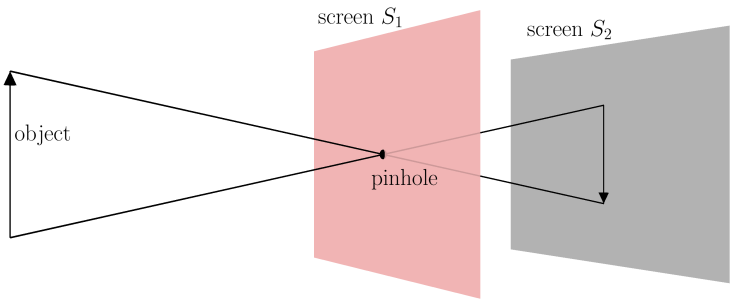

Figure 1.1: Model of the pinhole camera

ity. The set of all projectivities over the real numbers is called the **projective general linear group** of degree $n+1$ over $\mathbb{R}$ and denoted by $\mathrm{PGL}_{n+1}(\mathbb{R})$ or simply PGL_{n+1}. The projective general linear group plays the role of the group of automorphisms of the projective space $\mathbb{P}^n$.

1.2 The Pinhole Camera Model

Problem 1.2 is concerned with (photographic) images of certain objects. We therefore first have to investigate how the process of taking a photograph can be modelled mathematically. We will do this with a simple model of a camera, the so-called **pinhole camera**. Surprisingly – despite its simpleness – this model pretty accurately describes the geometry and optics of a typical camera used in practice.

Consider the system of figure 1.1. There are two screens S_1 and S_2. Screen S_1 has a small hole, letting the light rays emitted or reflected by the object pass through screen S_1 onto screen S_2. This creates an image of the object on screen S_2. Note that by construction, this image is aligned upside down, as indicated in the figure.

This optical system can be turned into a geometric model quite easily. So let $\mathcal{R}$ (corresponding to S_1) and $\mathcal{F}$ (corresponding to S_2) be two parallel planes in the three-dimensional space $\mathbb{R}^3$. The plane $\mathcal{R}$ resp. $\mathcal{F}$ is called the **retinal** resp. the **focal plane**. Let $C \in \mathcal{F}$ correspond to the hole in screen S_1. With this notation, taking a photograph of a point $P \in \mathbb{R}^3$ then corresponds to the mapping which sends P to the point of intersection P' of the line $\overline{PC}$ with the plane $\mathcal{R}$. We say that P' is the image of the **perspective projection** of P on $\mathcal{R}$ with respect to the **optical centre** C. The line perpendicular to $\mathcal{R}$ going through the optical centre C is called the **optical axis**. The distance of $\mathcal{R}$ and C is also referred to as the **focal length** f.

For a more detailed examination of this model, we fix two coordinate systems – one for the three-dimensional space $\mathbb{R}^3$, the other for the two-dimensional retinal plane $\mathcal{R}$. Let e_1, e_2, e_3 denote the standard basis of $\mathbb{R}^3$. Without loss of generality we may assume

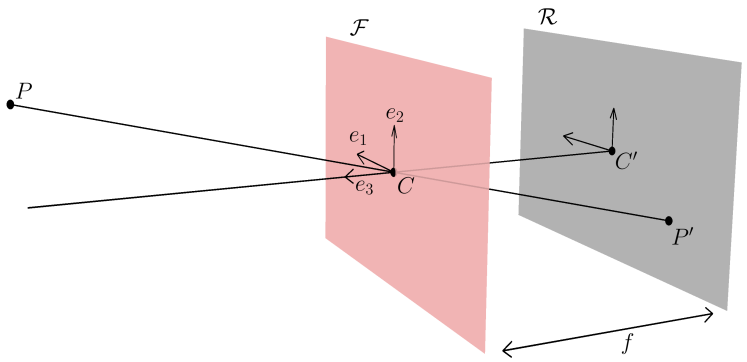

Figure 1.2: A geometric model of the pinhole camera

that the optical centre C lies in the origin of $\mathbb{R}^3$. Furthermore, if X_1, X_2, X_3 denote the coordinate functions of $\mathbb{R}^3$, then – according to figure 1.2 – we may assume that the focal plane is given by $X_3 = 0$. This coordinate system of $\mathbb{R}^3$ with origin C is called the **camera coordinate system**. We will denote it with the letter $\mathfrak{B}$.
Let C' be the point of intersection of the optical axis with the retinal plane $\mathcal{R}$. We can equip the two-dimensional space $\mathcal{R}$ with coordinates in such a way that C' is the origin and the two base vectors of the coordinate system are e_1 and e_2. This coordinate system shall be denoted by $\mathfrak{B}'$.
Having fixed this, a point P of $\mathbb{R}^3$ can be written as

$$P = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix}_{\mathfrak{B}}$$

with $\xi_1, \xi_2, \xi_3 \in \mathbb{R}$ where the subscript $\mathfrak{B}$ is just a reminder for the fact that ξ_1, ξ_2, ξ_3 are coordinates with respect to the coordinate system $\mathfrak{B}$. Analogously, a point $P' \in \mathcal{R}$ shall be written as

$$P' = \begin{pmatrix} \zeta_1 \\ \zeta_2 \end{pmatrix}_{\mathfrak{B}'}$$

with $\zeta_1, \zeta_2 \in \mathbb{R}$. Again, the subscript $\mathfrak{B}'$ means that ζ_1, ζ_2 are coordinates with respect to the coordinate system $\mathfrak{B}'$. With this explicit notation, it is not hard to establish a mathematical relation between the object point P and the image point P' in terms of their coordinates. In fact – assuming that $\xi_3 \neq 0$, i. e. $P \notin \mathcal{F}$ – we have

$$\zeta_1 = -\frac{f \cdot \xi_1}{\xi_3} \quad \text{and} \quad \zeta_2 = -\frac{f \cdot \xi_2}{\xi_3}.$$

This can be written linearly as

$$\begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{pmatrix} = M \cdot \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ 1 \end{pmatrix} \tag{1.1}$$

with

$$M := \begin{pmatrix} -f & 0 & 0 & 0 \\ 0 & -f & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

where $\zeta_1 = \eta_1/\eta_3$ and $\zeta_2 = \eta_2/\eta_3$. Note that $(\eta_1 : \eta_2 : \eta_3)$ can be interpreted as homogeneous coordinates of $(\zeta_1, \zeta_2)^T_{\mathfrak{B}'}$ via the usual embedding $\mathbb{R}^2 \longrightarrow \mathbb{P}^2$. Similarly, regarding $(\xi_1 : \xi_2 : \xi_3 : 1)^T$ as a homogeneous coordinate vector of the point $(\xi_1, \xi_2, \xi_3)^T_{\mathfrak{B}}$ as well, equation (1.1) is a relation of homogeneous coordinates. To sum up, an application of M to the object point P, given in homogeneous coordinates, exactly corresponds to the operation of taking a photograph of P, the image point again being given in homogeneous coordinates. Needless to say, the resulting map $M : \mathbb{P}^3 \setminus \mathcal{F} \longrightarrow \mathbb{P}^2$ is well-defined: Applying M to two different representations of an object point yields representations which only differ by a scalar multiple and hence define the same image point.
This projective point of view proves to be very useful, since this also makes sense when photographing points that lie in $\mathcal{F} \setminus \{C\}$, the focal plane without the optical centre. For, multiplying the matrix M with a point of $\mathcal{F} \setminus \{C\}$ yields coordinates $(\eta_1 : \eta_2 : \eta_3)$ with $\eta_3 = 0$. But this means that $(\eta_1 : \eta_2 : \eta_3)$ lies in the line at infinity of $\mathcal{R}$ which perfectly reflects the reality. We may hence extend the domain of definition of the map M and get a map (again denoted by M)

$$M : \mathbb{P}^3 \setminus \{(0:0:0:1)\} \longrightarrow \mathbb{P}^2.$$

Because of this and the nice linear structure of equation (1.1), we usually use homogeneous coordinates for describing the pinhole camera model.

Note that we have assumed that the optical centre C is equal to the origin of $\mathbb{R}^3$. Moreover, the coordinates have been chosen in such a way that the focal plane $\mathcal{F}$ coincides with the X_1-X_2-plane. For practical reasons, it is often more convenient to use other coordinate systems. Such an alternative coordinate system is then – in contrary to the camera-centric point of view of the camera coordinate system – usually referred to as the **world coordinate system**. Note that we may assume that the camera and the world coordinate system just differ by a rotation and a translation. We do not go into the details here, nonetheless, it should be clear from the mathematical viewpoint how these additional practical factors can be included in the model.

Remark. The mathematics describing the perspective projection does not distinguish between points which lie in front of resp. behind the camera. In practice of course, only

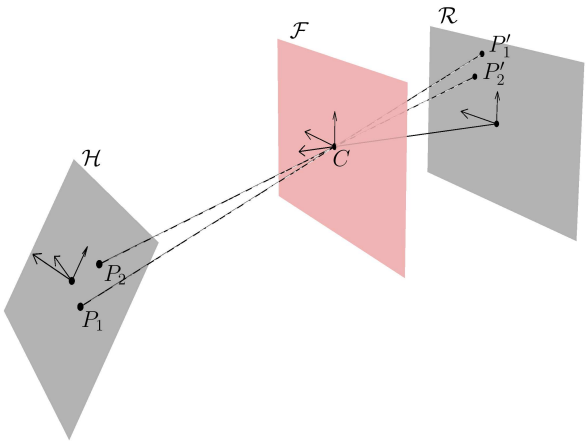

Figure 1.3: Model of the pinhole camera for flat objects

those points which are in front of the camera have an image point on the photograph. ♢

1.3 Images of Flat Objects under Changing Camera Perspectives

In this section, we want to examine how the results about the operation of taking a photograph can be applied to the special case of taking images of flat objects. So assume that our object, given by a tuple $(P_1, \ldots, P_n)$ of points in three-dimensional space, is contained in a plane $\mathcal{H}$. In the following, a tuple of n points will be called an ***n*-point configuration**. Moreover, an n-point configuration is called **flat** if all its points lie in a plane. So in this manner of speaking, the object $(P_1, \ldots, P_n)$ is a flat n-point configuration. According to figure 1.3, we can choose a two-dimensional orthonormal coordinate system of the plane $\mathcal{H}$. This coordinate system shall be denoted by $\mathfrak{C}$. It can be extended to a three-dimensional orthonormal coordinate system of the whole space $\mathbb{R}^3$, which will be called $\mathfrak{D}$. Note that we can choose $\mathfrak{D}$ in such a way that $\mathfrak{D}$ and the camera coordinate system $\mathfrak{B}$ of $\mathbb{R}^3$ (see previous section) only differ by a rotation* $A = (u, v, w) \in \mathrm{SO}_3$, (where $u = (u_1, u_2, u_3)^T, v = (v_1, v_2, v_3)^T, w = (w_1, w_2, w_3)^T \in \mathbb{R}^3$) followed by a translation $t = (t_1, t_2, t_3)^T \in \mathbb{R}^3$.

Putting these information together yields the following mathematical description of taking a photograph of a point contained in $\mathcal{H}$, say $P = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix}_{\mathfrak{C}}$, in terms of the coordinate

*As usual, $\mathrm{SO}_3(\mathbb{R})$ or simply SO_3 denotes the special orthogonal group of dimension 3 over $\mathbb{R}$.

systems $\mathfrak{C}$, $\mathfrak{D}$ and $\mathfrak{B}$:

$$\begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix}_{\mathfrak{C}} \longrightarrow \begin{pmatrix}\xi_1\\ \xi_2\\ 0\end{pmatrix}_{\mathfrak{D}} \overset{\text{Rotation \& translation}}{\longrightarrow} \left(A\begin{pmatrix}\xi_1\\ \xi_2\\ 0\end{pmatrix} + \begin{pmatrix}t_1\\ t_2\\ t_3\end{pmatrix}\right)_{\mathfrak{B}}$$
$$= \left(\begin{pmatrix}u_1 & v_1 & w_1\\ u_2 & v_2 & w_2\\ u_3 & v_3 & w_3\end{pmatrix}\begin{pmatrix}\xi_1\\ \xi_2\\ 0\end{pmatrix} + \begin{pmatrix}t_1\\ t_2\\ t_3\end{pmatrix}\right)_{\mathfrak{B}} = \begin{pmatrix}u_1\xi_1 + v_1\xi_2 + t_1\\ u_2\xi_1 + v_2\xi_2 + t_2\\ u_3\xi_1 + v_3\xi_2 + t_3\end{pmatrix}_{\mathfrak{B}}$$
$$\overset{\text{Embedding into } \mathbb{P}^3}{\longrightarrow} \begin{pmatrix}u_1\xi_1 + v_1\xi_2 + t_1\\ u_2\xi_1 + v_2\xi_2 + t_2\\ u_3\xi_1 + v_3\xi_2 + t_3\\ 1\end{pmatrix} \overset{\text{Application of } M}{\longrightarrow} \begin{pmatrix}-f(u_1\xi_1 + v_1\xi_2 + t_1)\\ -f(u_2\xi_1 + v_2\xi_2 + t_2)\\ u_3\xi_1 + v_3\xi_2 + t_3\end{pmatrix}$$

This last vector can also be written as

$$\begin{pmatrix}-f & 0 & 0\\ 0 & -f & 0\\ 0 & 0 & 1\end{pmatrix} \cdot (u, v, t) \cdot \begin{pmatrix}\xi_1\\ \xi_2\\ 1\end{pmatrix}.$$

Again, we may think of $\overline{P} := (\xi_1 : \xi_2 : 1)$ as the homogeneous version of $P := (\xi_1, \xi_2)^T \in \mathcal{H}$ via the standard embedding $\mathbb{R}^2 \longrightarrow \mathbb{P}^2$. To sum up, the operation of taking a photo of P corresponds to the application of the linear map given by the matrix

$$\begin{pmatrix}-f & 0 & 0\\ 0 & -f & 0\\ 0 & 0 & 1\end{pmatrix} \cdot (u, v, t)$$

to the point $\overline{P}$. Note that by definition of M, this yields homogeneous coordinates of the image point (with respect to the coordinates $\mathfrak{B}'$). By construction, the set of all possible 'photographing matrices' which can occur in this context is given by

$$\left\{\begin{pmatrix}-f & 0 & 0\\ 0 & -f & 0\\ 0 & 0 & 1\end{pmatrix} \cdot (u, v, t);\ u, v, t \in \mathbb{R}^3, f \in \mathbb{R} \setminus \{0\}, \|u\| = \|v\| = 1, \langle u, v\rangle = 0\right\}$$

The brackets $\langle \cdot, \cdot \rangle$ resp. $\| \cdot \|$ denote the standard scalar product resp. the standard norm in $\mathbb{R}^3$. Note that these last conditions about u und v originate from $A \in \mathrm{SO}_3$ being a rotation. Actually – as we have seen – the elements of the above set describe maps from $\mathcal{H} \setminus C$ to $\mathcal{R}$ where both $\mathcal{H}$ and $\mathcal{R}$ are given the structure of $\mathbb{P}^2$ with respect to the coordinates $\mathfrak{C}$ and $\mathfrak{B}'$. We may now define the set of (projective) 'photographing matrices' as the set of equivalence classes

$$\Omega := \left\{\begin{pmatrix}-f & 0 & 0\\ 0 & -f & 0\\ 0 & 0 & 1\end{pmatrix} \cdot (u, v, t);\ u, v, t \in \mathbb{R}^3, f \in \mathbb{R} \setminus \{0\}, \|u\| = \|v\|, \langle u, v\rangle = 0\right\} / \sim,$$

where two matrices are equivalent under $\sim$ if they only differ by a scalar multiple. Note that then still every equivalence class in Ω describes a well-defined map $\mathcal{H} \setminus C \longrightarrow \mathcal{R}$. If we

use a camera with a known focal length f for taking all the images, then the set Ω can be specialized to the set of all possible 'photographing matrices for a specific focal length' by simply putting f equal to the concrete value of f. Nonetheless, we want to solve Problem 1.2 even if the images are taken with different cameras. We hence let f be unspecified and use the set Ω as defined above.

In the first section of this chapter, we have noticed that the elements of PGL_3, the projectivities, are the automorphisms of projective space $\mathbb{P}^2$. We hence are primarily interested in such matrices of Ω which belong to the group PGL_3. Otherwise, if we take a camera position such that the corresponding matrix is not contained in PGL_3 then this means that we have chosen a 'bad' position in the sense that distinct points of $\mathcal{H}$ are mapped to the same image point in $\mathcal{R}$. We do not want to consider such cases. More explicitly, we want to examine only those camera positions such that the corresponding matrices are contained in $\Omega \cap \mathrm{PGL}_3$.

Let $(P'_1, \ldots, P'_n), (Q'_1, \ldots, Q'_n) \in (\mathbb{P}^2)^n$ be two photographs of the flat n-point configuration $(P_1, \ldots, P_n)$ in the sense that P'_i resp. Q'_i is the image point of P_i under the first resp. the second camera position. Assuming that neither $(P'_1, \ldots, P'_n)$ nor $(Q'_1, \ldots, Q'_n)$ are 'bad' photographs in the above sense, we know by construction that there exist $\sigma, \tau \in \Omega \cap \mathrm{PGL}_3$ such that

$$P'_i = \sigma\tau^{-1}(Q'_i) \qquad \text{for all } i \in \{1, \ldots, n\}.$$

In particular, the n-point configurations[†] $(P'_1, \ldots, P'_n)$ and $(Q'_1, \ldots, Q'_n)$ lie in the same orbit under the action of the group PGL_3 on $(\mathbb{P}^2)^n$ by pointwise multiplication , i. e. under the action

$$\sigma(P_1, \ldots, P_n) := (\sigma(P_1), \ldots, \sigma(P_n)) \quad \text{for all } \sigma \in \mathrm{PGL}_3,\ (P_1, \ldots, P_n) \in (\mathbb{P}^2)^n.$$

In the next section, we will see that this group action will play a central role for the invariant theoretical formulation of Problem 1.2.

1.4 Invariant Theoretical Formulation of the Problem

According to Problem 1.2, we want to be able to decide whether two given n-point configurations consisting of points in $\mathbb{P}^2$ can be (photographic) images of the same flat n-point configuration of points in three-dimensional space $\mathbb{R}^3$ or not. Clearly, this can be achieved by checking whether there exist elements $\sigma, \tau \in \Omega \cap \mathrm{PGL}_3$ such that one of the point configurations can be transformed to the other by an application of $\sigma\tau^{-1}$. But doing this for many pairs of point configurations can be very cumbersome and time-consuming. Therefore, as mentioned earlier, we will use methods of invariant theory to give an alternative and more elegant solution of this problem. An essential ingredient for this will be the

[†]The photographic image of an n-point configuration is – as a sequence of n points – itself an n-point configuration consisting of points contained in $\mathbb{P}^2$. Therefore, if we speak of an n-point configuration, this may mean both, the original object as well as the image of this object. Nonetheless, it should be clear from the context, whether we refer to the objects or the images.

group action of PGL_3 on $(\mathbb{P}^2)^n$ as defined in the previous section. This will become clear with the following proposition.

Proposition 1.3. *The group* PGL_3 *is generated by the set*

$$\{\sigma\tau^{-1};\ \sigma,\tau \in \Omega \cap \mathrm{PGL}_3\}.$$

Proof. As the identity matrix I_3 is in $\Omega \cap \mathrm{PGL}_3$, it is sufficient to show that PGL_3 is generated by $\Omega \cap \mathrm{PGL}_3$. Note that the equivalence classes of all permutation matrices, i. e. matrices which have the property that they have exactly one entry '1' in each column and in each row, are contained in $\Omega \cap \mathrm{PGL}_3$. Moreover, the equivalence classes defined by the set of representatives

$$\left\{ \begin{pmatrix} 1 & 0 & \lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};\ \lambda \in \mathbb{R} \right\} \tag{1.2}$$

are obviously contained in $\Omega \cap \mathrm{PGL}_3$, too.

Consider the set

$$T := \{I_3 + E_{ij}(\lambda);\ i,j \in \{1,2,3\}, i \neq j, \lambda \in \mathbb{R}\}$$

where I_3 denotes the identity matrix and $E_{ij}(\lambda)$ denotes the matrix with λ in the entry (i,j) and zero elsewhere. It can be checked without difficulties that all elements of T can be written as products of permutation matrices and the matrices contained in the set (1.2). By a theorem of group theory, the special linear group SL_3 is generated by the set T (cf. [Hup67], Chapter II, Satz 6.7). In particular, this implies that PGL_3 is generated by the set of equivalence classes defined by T. Since the equivalence classes defined by the permutation matrices and the set (1.2) are contained in $\Omega \cap \mathrm{PGL}_3$, it follows by the above that PGL_3 is generated by $\Omega \cap \mathrm{PGL}_3$. ∎

Corollary 1.4. *Let* $f : (\mathbb{P}^2)^n \longrightarrow \mathbb{R}$ *be an arbitrary function such that*

$$f(\sigma\tau^{-1}(P_1,\ldots,P_n)) = f(P_1,\ldots,P_n) \quad \text{for all } \sigma,\tau \in (\Omega \cap \mathrm{PGL}_3),\ (P_1,\ldots,P_n) \in (\mathbb{P}^2)^n.$$

Then f *is constant on the orbits of the group* PGL_3 *acting on the set of* n*-point configurations by pointwise multiplication. In this case we say that* f *is an* **invariant** *under the action of* PGL_3 *on* $(\mathbb{P}^2)^n$.

Proof. Let $\rho \in \mathrm{PGL}_3$ and $(P_1,\ldots,P_n) \in (\mathbb{P}^2)^n$ be arbitrary. We have to show that

$$f(\rho(P_1,\ldots,P_n)) = f(P_1,\ldots,P_n).$$

If $\rho \in \Omega \cap \mathrm{PGL}_3$, this follows by setting $\sigma = \rho$ and $\tau = 1_{\mathrm{PGL}_3}$. Furthermore, if $\rho^{-1} \in \Omega \cap \mathrm{PGL}_3$, then – knowing this – it follows that $f(\rho(P_1, \ldots, P_n)) = f(\rho^{-1}\rho(P_1, \ldots, P_n)) = f(P_1, \ldots, P_n)$.
By the previous proposition, we know for all other ρ that there exist $\rho_1, \ldots, \rho_s \in \Omega \cap \mathrm{PGL}_3$ and $i_1, \ldots, i_s \in \{1, -1\}$ such that $\rho = \rho_1^{i_1} \ldots \rho_s^{i_s}$. By what we did a few lines above, we have

$$\begin{aligned} f(\rho(P_1, \ldots, P_n)) &= f(\rho_1^{i_1}\rho_2^{i_2} \ldots \rho_s^{i_s}(P_1, \ldots, P_n)) \\ &= f(\rho_2^{i_2} \ldots \rho_s^{i_s}(P_1, \ldots, P_n)) \\ &= f(\rho_3^{i_3} \ldots \rho_s^{i_s}(P_1, \ldots, P_n)) \\ &= \ldots = f(P_1, \ldots, P_n) \end{aligned}$$

and the assertion follows. ∎

Therefore, a function $(\mathbb{P}^2)^n \longrightarrow K$ which is constant on the sets of good photographs of point configurations in $(\mathbb{P}^2)^n$ actually is an invariant under the action of PGL_3 on $(\mathbb{P}^2)^n$ (as defined in the previous section).
In practice though, another aspect has to be taken into account. Usually, it is not known which point of the original flat n-point configuration maps to a given point in the image. In particular, if we have two images $(P_1, \ldots, P_n)$ and $(Q_1, \ldots, Q_n) \in (\mathbb{P}^2)^n$ of an n-point-configuration, it is not known which point P_i of the first image corresponds to which point Q_j of the second image. For an answering of the question whether $(P_1, \ldots, P_n)$ and $(Q_1, \ldots, Q_n)$ are images of the same object or not – which is the content of our Problem 1.2 – it is therefore reasonable to include this unknown point correspondence in the mathematical model. This can be done as follows. We know that there exists a permutation $\pi \in \mathrm{S}_n$, where S_n denotes the symmetric group in n symbols, such that

$$P_i = \sigma\tau^{-1}(Q_{\pi(i)}) \qquad \text{for all } i \in \{1, \ldots, n\}$$

with $\sigma, \tau \in \Omega \cap \mathrm{PGL}_3$ appropriate. Therefore, if $(P_1, \ldots, P_n)$ and $(Q_1, \ldots, Q_n)$ are photographs of the same set of n points lying in a plane, it follows that both point configurations $(P_1, \ldots, P_n)$ and $(Q_1, \ldots, Q_n)$ are contained in the same orbit under the action of the group $\mathrm{PGL}_3 \times \mathrm{S}_n$ on $(\mathbb{P}^2)^n$ given by

$$\begin{aligned} (\sigma, \pi)(P_1, \ldots, P_n) := (\sigma(P_{\pi^{-1}(1)}), \ldots, \sigma(P_{\pi^{-1}(n)})) \text{ for all} \\ (\sigma, \pi) \in \mathrm{PGL}_3 \times \mathrm{S}_n,\ (P_1, \ldots, P_n) \in (\mathbb{P}^2)^n. \end{aligned}$$

It is our aim to find functions which are invariant under this action. In fact, we are not interested in arbitrary functions $(\mathbb{P}^2)^n \longrightarrow \mathbb{R}$ which are invariant under $\mathrm{PGL}_3 \times S_n$, but only in functions which are contained in a special class of functions, the so-called **rational functions** on $(\mathbb{P}^2)^n$. Precise definitions of the notion of a rational function, an invariant rational function etc. will be given in Chapter 3. The set of rational functions on $(\mathbb{P}^2)^n$ will be denoted by $\mathbb{R}((\mathbb{P}^2)^n)$, the set of those rational functions which are invariant under the action of $\mathrm{PGL}_3 \times S_n$ will be written as $\mathbb{R}((\mathbb{P}^2)^n)^{\mathrm{PGL}_3 \times S_n}$. We will see that both sets

have the structure of a field which is finitely generated over $\mathbb{R}$.

Assume for a moment that we know a finite set of generators of the invariant field $\mathbb{R}((\mathbb{P}^2)^n)^{\mathrm{PGL}_3 \times \mathrm{S}_n}$, say $\{f_1, \ldots, f_s\} \subset \mathbb{R}((\mathbb{P}^2)^n)^{\mathrm{PGL}_3 \times \mathrm{S}_n}$. How can this be used for a solution of Problem 1.2? Obviously, we have the following. If $P := (P_1, \ldots, P_n), Q := (Q_1, \ldots, Q_n) \in (\mathbb{P}^2)^n$ are images of flat n-point configurations and if there exists $i \in \{1, \ldots, s\}$ such that $f_i(P) \neq f_i(Q)$, then P and Q cannot be images of the same flat n-point configuration. Moreover – as we will see – the converse is also true for 'general enough' $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$-orbits in the set of point configurations $(\mathbb{P}^2)^n$. More precisely, we will show that for 'almost all' point configurations $P := (P_1, \ldots, P_n)$ and $Q := (Q_1, \ldots, Q_n)$ the equality $f_i(P) = f_i(Q)$ for all $i \in \{1, \ldots, s\}$ implies that P and Q are images of the same object. We can hence decide whether P and Q are images of the same object without explicitly checking for the existence of $\sigma, \tau \in \Omega \cap \mathrm{PGL}_3$ and $\pi \in \mathrm{S}_n$ such that $P = \sigma\tau^{-1}(\pi(Q))$, as it has been suggested at the beginning of this section.

In this thesis, the examinations of this invariant theoretical problem will actually take place in a more general setting. We will consider arbitrary infinite fields K – not just the field of real numbers – and arbitrary dimensions m of the space where the object points are contained. We will compute a finite set of generators of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$. Moreover, we will examine the separation properties of these generating rational invariants. More explicitly, we will examine which point configurations can be separated by rational invariants in the sense whether $f(P_1, \ldots, P_n) = f(Q_1, \ldots, Q_n)$ for all $f \in K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$ does imply that $(P_1, \ldots, P_n)$ and $(Q_1, \ldots, Q_n)$ lie in the same $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$-orbit.
Summarizing this gives the following invariant theoretical problem. Note that all terms used here will be defined precisely later on.

Problem 1.5. *Let $m, n \in \mathbb{N}$, let K be an infinite field and let the group $\mathrm{PGL}_{m+1}(K) \times \mathrm{S}_n$ act on the set of n-point configurations $(\mathbb{P}^m_K)^n$ by*

$$(\sigma, \pi)(P_1, \ldots, P_n) := (\sigma(P_{\pi^{-1}(1)}), \ldots, \sigma(P_{\pi^{-1}(n)})) \text{ for all } (\sigma, \pi) \in \mathrm{PGL}_{m+1} \times \mathrm{S}_n,\ (P_1, \ldots, P_n) \in (\mathbb{P}^m_K)^n.$$

Then

- *Compute generators of $K((\mathbb{P}^m_K)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$, the field of invariant rational functions.*
- *Find a set $H \subset (\mathbb{P}^m_K)^n$ (as large as possible) such that all $\mathrm{PGL} \times \mathrm{S}_n$-orbits of points contained in H can be separated by rational invariants.*

Note that the case $m = 2$ has already been treated by Boutin and Kemper in [BK05].

2 Algorithms for Fields

Algorithmic problems are a rather new field of research in field theory. Whereas the incipiencies of classical field theory go back to the second part of the nineteenth century, algorithmic aspects basically came into mind with the advent of Gröbner bases. They first appeared in the sixties of the last century (see [Buc65]). In order to use Gröbner basis techniques in the context of field theory, it is necessary to put the theory of fields down to the theory of ideals. An important contribution to this was made by Sweedler [Swe93] as well as Kemper [Kem93]. Using additional variables, so-called tag variables, they assigned to each intermediate field L of K and a finitely generated field extension $K(x_1, \ldots, x_n)$ over K a special ideal in a polynomial ring. On the basis of that assignment, they solved several algorithmic problems in field theory. Their works include an algorithm for computing the transcendental respectively the algebraic degree of the field extension $K(x_1, \ldots, x_n)|L$, an algorithm for finding the minimal polynomial of an element over L and a field membership test for L.
As algorithms involving Gröbner basis computations behave quite sensitive to the number of variables, it was a matter of interest to find alternative methods which work without the usage of additional variables. Following a different approach, Müller-Quade and Steinwandt got by without using tag variables (see [MQS99] and [MQS00a]). They presented solutions for many further algorithmic problems in field theory such as finding a transcendence basis and – if applicable – a separable basis of $K(x_1, \ldots, x_n)|L$, computing – if applicable – the elements of the Galois group $\mathrm{Gal}(K(x_1, \ldots, x_n)|L)$ and computing the intersection of intermediate fields L_1 and L_2 in case that they are linearly disjoint over their intersection (see [SMQ00]). The works of Müller-Quade and Steinwandt are based on a special field-ideal correspondence. That correspondence will play a central role in this chapter.

In the following, an algorithmic approach to field theory based on the ideas of Müller-Quade and Steinwandt will be given. We will characterize the lattice of intermediate fields of K and $K(x_1, \ldots, x_n)$ on the basis of their concepts. After that we will give an algorithm to compute the intersection of two intermediate fields L_1 and L_2. Unlike the algorithm of Müller-Quade and Steinwandt, the algorithm presented here works in general, provided that it terminates. We will show that it certainly terminates in characteristic zero if both fields L_1 and L_2 are algebraically closed in $K(x_1, \ldots, x_n)$. Therefore, we will indicate a way to test algebraic closedness in the field $K(x_1, \ldots, x_n)$. Finally, we will examine simple field extensions. We will give an algorithm to decide whether an intermediate field L is simple over K or not and – in the affirmative case – to compute a generating element. This will lead to a new proof of a generalized version of the well-known Theorem of Lüroth.

Throughout this chapter we will use the following notation.

Notation 2.1.

(i) K shall denote a field. Unless otherwise stated this field can be of arbitrary characteristic.

(ii) $K(x_1, \ldots, x_n)$ shall denote a finitely generated field extension over K. Note that unless otherwise stated the elements $x_1, \ldots, x_n$, abbreviated by $\underline{x}$, need not be algebraically independent.

(iii) $X_1, \ldots, X_n$, abbreviated by $\underline{X}$, shall denote indeterminates over K.

(iv) $Z_1, \ldots, Z_n$, abbreviated by $\underline{Z}$, shall denote indeterminates over $K(x_1, \ldots, x_n)$.

(v) L, L_1 and L_2 shall denote intermediate fields of K and $K(x_1, \ldots, x_n)$, i. e. $K \leq L, L_1, L_2 \leq K(x_1, \ldots, x_n)$.

(vi) $f(\underline{x}) := g(\underline{x})/h(\underline{x}), f_1(\underline{x}) := g_1(\underline{x})/h_1(\underline{x}), \ldots, f_m(\underline{x}) := g_m(\underline{x})/h_m(\underline{x}) \in K(x_1, \ldots, x_n)$ shall denote field elements with polynomials $g(\underline{X}), g_1(\underline{X}), \ldots, g_m(\underline{X})$ and polynomials $h(\underline{X}), h_1(\underline{X}), \ldots, h_m(\underline{X})$ in $K[X_1, \ldots, X_n]$, where $h(\underline{x}), h_1(\underline{x}), \ldots, h_m(\underline{x}) \neq 0$.

2.1 Some Computational Algebra

Gröbner bases are one of the most powerful tools in computational algebra. As we will see later, they also play an essential role in this work. In this section, we give a brief introduction to the basic concepts of the theory of Gröbner bases. For more details, see [BW93].

Definition 2.2. *A* **monomial**[*] *in the indeterminates $X_1, \ldots, X_n$ is a product of the form*

$$X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n}$$

with $\alpha_1, \ldots, \alpha_n \in \mathbb{N}_0$. A monomial $X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n}$ will be abbreviated by $\underline{X}^{\alpha}$, where α stands for the multi-index $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$.
A **monomial order** *on $X_1, \ldots, X_n$ is a linear order $\leq$ on the set of monomials in $X_1, \ldots, X_n$ such that*

(i) $1 \leq \underline{X}^{\alpha}$ *for all* $\alpha \in \mathbb{N}_0^n$.

(ii) $\underline{X}^{\alpha} \leq \underline{X}^{\beta}$ *implies that* $\underline{X}^{\alpha} \cdot \underline{X}^{\gamma} \leq \underline{X}^{\beta} \cdot \underline{X}^{\gamma}$ *for all* $\alpha, \beta, \gamma \in \mathbb{N}_0^n$.

In fact, there exists a great variety of monomial orders on $X_1, \ldots, X_n$ (cf. [BW93], Chapter 5, Section 1). Depending on the type of problem, different monomial orders are used. We will need the following types.

[*] In literature, a monomial is sometimes also called a term.

Definition 2.3. *A monomial order of* **i-elimination type** *is a monomial order such that any monomial involving one of $X_1, \ldots, X_i$ is greater than all monomials in $X_{i+1}, \ldots, X_n$. Let $M = \{X_{i_1}, \ldots, X_{i_s}\} \subset \{X_1, \ldots, X_n\}$ and denote the elements of $\{X_1, \ldots, X_n\} \setminus M$ by $X_{j_1}, \ldots, X_{j_{n-s}}$. An* **inverse block order with respect to M** *is a monomial order such that for all monomials m_1, m_2 in the indeterminates $X_{i_1}, \ldots, X_{i_s}$ and monomials n_1, n_2 in the indeterminates $X_{j_1}, \ldots, X_{j_{n-s}}$ we have*

$$m_1 \cdot n_1 \leq m_2 \cdot n_2$$

if and only if

$$\begin{aligned} &n_1 < n_2 \text{ or} \\ &n_1 = n_2 \text{ and } m_1 \leq m_2. \end{aligned}$$

Definition 2.4. *Let $p(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ be a polynomial, that means*

$$p(X_1, \ldots, X_n) = \sum_{\beta \in \mathbb{N}_0^n} c_\beta \underline{X}^\beta \in K[X_1, \ldots, X_n]$$

for some $c_\beta \in K$, $\beta \in \mathbb{N}_0^n$, where all but finitely many c_β, $\beta \in \mathbb{N}_0^n$ are equal to zero. We say that the monomial $\underline{X}^\alpha$ with $\alpha \in \mathbb{N}_0^n$ **is involved in $\mathbf{p}(\mathbf{X_1}, \ldots, \mathbf{X_n})$** *if $c_\alpha \neq 0$.*

Definition 2.5. *Let $p(\underline{X}) \in K[X_1, \ldots, X_n]$ be a polynomial and let $\leq$ be a monomial order on $X_1, \ldots, X_n$. Then the* **leading monomial** *of $p(\underline{X})$ with respect to $\leq$, abbreviated by $\mathrm{LM}_{\leq}(\mathbf{p}(\underline{\mathbf{X}}))$, is the maximal monomial with respect to $\leq$ involved in $p(\underline{X})$.*
The coefficient of $\mathrm{LM}_{\leq}(p(\underline{X}))$ in $p(\underline{X})$ is called the **leading coefficient** *of $p(\underline{X})$ with respect to $\leq$. It is abbreviated by $\mathrm{LC}_{\leq}(\mathbf{p}(\underline{\mathbf{X}}))$.*

Remark 2.6. It is not hard to see that the operator $\mathrm{LM}_{\leq}$ is multiplicative, more precisely, we have the equality $\mathrm{LM}_{\leq}(p(\underline{X}) \cdot q(\underline{X})) = \mathrm{LM}_{\leq}(p(\underline{X})) \cdot \mathrm{LM}_{\leq}(q(\underline{X}))$ for all polynomials $p(\underline{X}), q(\underline{X}) \in K[X_1, \ldots, X_n]$. ♢

Definition 2.7. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let $\leq$ be a monomial order on $X_1, \ldots, X_n$. A* **Gröbner basis** *of I with respect to $\leq$ is a finite subset $\mathcal{G} \subset I$ such that for every $p(\underline{X}) \in I$ there exists $g(\underline{X}) \in \mathcal{G}$ with*

$$\mathrm{LM}_{\leq}(g(\underline{X})) \mid \mathrm{LM}_{\leq}(p(\underline{X})).$$

A Gröbner basis $\mathcal{G}$ is called **reduced**, *if*

(i) $\mathrm{LC}_{\leq}(g(\underline{X})) = 1$ *for all $g(\underline{X}) \in \mathcal{G}$.*

(ii) no monomial involved in $g(\underline{X}) \in \mathcal{G}$ is divisible by one of the leading monomials of $\mathcal{G} \setminus \{g(\underline{X})\}$.

Proposition 2.8. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal and let $\leq$ be a monomial order on $X_1, \ldots, X_n$. Then there exists a Gröbner basis of I w. r. t. $\leq$. Moreover, there exists a unique reduced Gröbner basis of I w. r. t. $\leq$.*

Proof. See [BW93], Chapter 5, Section 2. ∎

For simplicity, we often say 'Gröbner basis of I' instead of 'Gröbner basis of I with respect to $\leq$', when the monomial order $\leq$ can be deduced from the context or may be chosen arbitrarily.

Remarks 2.9. (a) A Gröbner basis $\mathcal{G}$ of an ideal I is a basis of I, indeed, i. e. $(\mathcal{G}) = I$.

(b) A Gröbner basis as well as reduced Gröbner basis of I w. r. t. an arbitrary monomial order $\leq$ can be found algorithmically (see [Buc65]). ♢

There exists a variety of algorithms which are based on the theory of Gröbner bases. For the execution of these algorithms on a computer, it is required that the field K can be handled computationally. More precisely, the operations multiplication, addition and inversion (of elements in K) need to be realizable on a computer. If this is the case, we say that K is a **computable** field. Within this thesis, we do not explicitly state this computability condition on K at the various places where algorithms are developed – we implicitly assume that the coefficients of the involved polynomial data are contained in a computable field.

Proposition and Definition 2.10. *Let $p(\underline{X}) \in K[X_1, \ldots, X_n]$ be a polynomial and let $\mathcal{G}$ be a Gröbner basis of an ideal $I \trianglelefteq K[X_1, \ldots, X_n]$. Then there exists a unique polynomial $q(\underline{X}) \in K[X_1, \ldots, X_n]$ such that*

(i) no monomial involved in $q(\underline{X})$ is divisible by one of the leading monomials of $\mathcal{G}$.

(ii) $p(\underline{X}) = h(\underline{X}) + q(\underline{X})$ for some $h(\underline{X}) \in I$.

The polynomial $q(\underline{X})$ is called the **normal form** *of $p(\underline{X})$ with respect to $\mathcal{G}$. It is denoted by $\mathrm{NF}_{\mathcal{G}}(\mathbf{p}(\underline{\mathbf{X}}))$.*

Proof. See [BW93], Chapter 5, Section 2. ∎

Remark 2.11. Let $\mathcal{G}$ be a Gröbner basis of an ideal $I \trianglelefteq K[X_1, \ldots, X_n]$.

(a) By [BW93], Chapter 5, Theorem 5.35, we have

$$p(\underline{X}) \in I \iff \mathrm{NF}_{\mathcal{G}}(p(\underline{X})) = 0.$$

(b) It can be shown that the operator $\mathrm{NF}_{\mathcal{G}}$ is additive and K-linear, i.e.

$$\mathrm{NF}_{\mathcal{G}}(\lambda \cdot p(\underline{X}) + \mu \cdot q(\underline{X})) = \lambda \cdot \mathrm{NF}_{\mathcal{G}}(p(\underline{X})) + \mu \cdot \mathrm{NF}_{\mathcal{G}}(q(\underline{X}))$$

for all scalars $\lambda, \mu \in K$ and polynomials $p(\underline{X}), q(\underline{X}) \in K[X_1, \ldots, X_n]$.

(c) If the elements of the Gröbner basis $\mathcal{G}$ only have coefficients in a subfield L of K, then

$$\mathrm{NF}_{\mathcal{G}}(p(\underline{X})) \in L[X_1, \ldots, X_n]$$

for all $p(\underline{X}) \in L[X_1, \ldots, X_n]$. ♢

Proposition 2.12. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal, let $i \in \{1, \ldots, n\}$ and let $\mathcal{G}$ be a Gröbner basis of I with respect to a monomial order of i-elimination-type. Then*

$$I \cap K[X_{i+1}, \ldots, X_n] = (\mathcal{G} \cap K[X_{i+1}, \ldots, X_n]) \trianglelefteq K[X_{i+1}, \ldots, X_n].$$

Proof. See [BW93], Chapter 6, Proposition 6.15. ∎

Definition 2.13. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal. The* **dimension** *of the ideal I is defined as*

$$dim(I) := \max\{|M| \,;\, M = \{X_{i_1}, \ldots, X_{i_s}\} \subset \{X_1, \ldots, X_n\} \text{ and } I \cap K[X_{i_1}, \ldots, X_{i_s}] = (0)\}.$$

Proposition 2.14. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal. Then $dim(I)$ is the supremum of the lengths of chains of prime ideals ascending strictly from I, where the length of a chain*

$$I \subset Q_0 \subsetneq \ldots \subsetneq Q_d \subsetneq K[X_1, \ldots, X_n]$$

with prime ideals $Q_0, \ldots, Q_d \trianglelefteq K[X_1, \ldots, X_n]$ is taken to be d.

Proof. For a proof see [ZS75b], Chapter VII, §7, Theorem 20. ∎

Proposition 2.15. *Let $I \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal. Then* $\dim(I)$ *can be computed with Gröbner bases.*

Proof. See [BW93], Chapter 9, Proposition 9.29. ∎

2.2 MQS Ideals

As outlined at the beginning of the chapter, Müller-Quade and Steinwandt assigned to each intermediate field of K and $K(x_1, \ldots, x_n)$ a certain ideal (see [MQS99] and [MQS00a]). This proved to be useful for the algorithmic solution of various problems for intermediate fields. We mimic their approach, although our field-ideal assignment is slightly different. The following definition makes the idea of assigning an ideal to each intermediate field of K and $K(x_1, \ldots, x_n)$ precise. Later, we will see that this assignment is injective in the sense that two different intermediate fields yield two different ideals.

Definition 2.16. *Let K, $K(x_1, \ldots, x_n)$, L and $Z_1, \ldots, Z_n$ be as in Notation 2.1. The* **MQS[†] ideal of $\mathbf{x_1}, \ldots, \mathbf{x_n}$ over $\mathbf{L}$**, *denoted by $J_L^{x_1,\ldots,x_n}$ or simply $J_L^{\underline{x}}$, is the ideal generated in the polynomial ring $K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ by the relations of $x_1, \ldots, x_n$ over L, i.e.*

$$J_L^{\underline{x}} := (p(Z_1, \ldots, Z_n) \in L[Z_1, \ldots, Z_n];\ p(x_1, \ldots, x_n) = 0)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}\,.$$

Proposition 2.17. *Let K, $K(x_1, \ldots, x_n)$, L and $Z_1, \ldots, Z_n$ be as in Notation 2.1. The relations of the elements $x_1, \ldots, x_n$ over L are given by*

$$(Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n].$$

In particular,

$$J_L^{\underline{x}} = \left((Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n]\right)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}\,.$$

Proof. We start with proving that the ideal $(Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$ is exactly the ideal of relations of the elements $x_1, \ldots, x_n$ over $K(x_1, \ldots, x_n)$. Clearly, we have

$$p(x_1, \ldots, x_n) = 0$$

for all $p(\underline{Z}) \in (Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$. Conversely, let the polynomial $p(\underline{Z}) \in K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ be a relation of $x_1, \ldots, x_n$ over $K(x_1, \ldots, x_n)$, i. e.

[†]We call them MQS ideals in honour of Müller-Quade and Steinwandt. They were probably the first who examined these ideals more closely with regard to algorithmic aspects. Actually, they regarded slightly different ideals. Details about the close relationship of their ideals with MQS ideals as defined here will be given later.

$p(x_1, \ldots, x_n) = 0$. Then we have

$$\begin{aligned} p(Z_1, \ldots, Z_n) &= p((Z_1 - x_1) + x_1, \ldots, (Z_n - x_n) + x_n)) \\ &= p(x_1, \ldots, x_n) + \sum_{i=1}^{n} (Z_i - x_i) \cdot q_i(Z_1, \ldots, Z_n) \\ &= \sum_{i=1}^{n} (Z_i - x_i) \cdot q_i(Z_1, \ldots, Z_n) \end{aligned}$$

for some $q_1(\underline{Z}), \ldots, q_n(\underline{Z}) \in K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$. It follows that $p(\underline{Z}) \in (Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$.
It is now immediate that the relations of $x_1, \ldots, x_n$ over L are given by

$$(Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n].$$

The rest of the proposition follows from the definition of $J_L^{\underline{x}}$. ∎

Corollary 2.18. *Let K, $K(x_1, \ldots, x_n)$, L and $Z_1, \ldots, Z_n$ be as in Notation 2.1. Then*

$$J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n] = (Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n],$$

the ideal of relations of $x_1, \ldots, x_n$ over L.

Proof. By Proposition 2.17, the MQS ideal $J_L^{\underline{x}}$ is clearly contained in the ideal $(Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$. Therefore, we have the inclusion

$$J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n] \subset (Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n].$$

For the reverse inclusion recall from Proposition 2.17 that the ideal $J_L^{\underline{x}}$ is generated by the elements of the ideal $(Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n]$. In particular,

$$(Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n] \subset J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n],$$

which proves the assertion. ∎

We can now establish the close relationship between MQS ideals and the ideals as defined by Müller-Quade and Steinwandt in [MQS00a]. By the above, there is an inclusion-preserving 1-1-correspondence between $\{J_L^{\underline{x}};\ K \leq L \leq K(x_1, \ldots, x_n)\}$ and the set of ideals $\{(Z_1 - x_1, \ldots, Z_n - x_n) \cap L[Z_1, \ldots, Z_n];\ K \leq L \leq K(x_1, \ldots, x_n)\}$. It was this latter set of ideals which was used for the field-ideal correspondence in [MQS00a]. In contrast to [MQS00a], our ideals all live in $K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$. For computational reasons our viewpoint seems to be simpler in practice.

Definition 2.19. *Let I and J be ideals in a ring R. Then the* **colon ideal** $I : J$ *is defined*

to be

$$I : J := \{r \in R;\ r \cdot J \subset I\}.$$

The **saturation** $I : J^\infty$ *of* I *by* J *is defined to be*

$$I : J^\infty := \{r \in R;\ r \cdot J^n \subset I \text{ for some } n \in \mathbb{N}\}.$$

As the name suggests, the set $I : J$ *as well as the set* $I : J^\infty$ *has the structure of an ideal. If* J *is a principal ideal generated by an element* $q \in R$*, then we also write* $I : q$ *instead of* $I : J$ *and* $I : q^\infty$ *instead of* $I : J^\infty$*.*

Lemma 2.20. *Let* K' *be a subfield of a field* L'*, let* $Y_1, \ldots, Y_n$ *be indeterminates over* L'*, let* $I \trianglelefteq K'[Y_1, \ldots, Y_n]$ *be an ideal and* $q(Y_1, \ldots, Y_n) \in K'[Y_1, \ldots, Y_n]$ *be a polynomial. Then*

$$(I : q(Y_1, \ldots, Y_n)^\infty)_{L'[Y_1,\ldots,Y_n]} = (I)_{L'[Y_1,\ldots,Y_n]} : q(Y_1, \ldots, Y_n)^\infty.$$

Proof. Let T be an indeterminate over L' and let $p_1(Y_1, \ldots, Y_n), \ldots, p_s(Y_1, \ldots, Y_n) \in I$ be generators of the ideal I. As before, we abbreviate $Y_1, \ldots, Y_n$ by $\underline{Y}$. It is commonly known (e. g. see [BW93], Chapter 6, Proposition 6.37) that the saturation ideals are given by

$$I : q(\underline{Y})^\infty = (p_1(\underline{Y}), \ldots, p_s(\underline{Y}), 1 - Tq(\underline{Y}))_{K'[Y_1,\ldots,Y_n,T]} \cap K'[Y_1, \ldots, Y_n]$$

and

$$(I)_{L'[Y_1,\ldots,Y_n]} : q(\underline{Y})^\infty = (p_1(\underline{Y}), \ldots, p_s(\underline{Y}), 1 - Tq(\underline{Y}))_{L'[Y_1,\ldots,Y_n,T]} \cap L'[Y_1, \ldots, Y_n].$$

Let $\mathcal{G}$ be a Gröbner basis of the ideal $(p_1(\underline{Y}), \ldots, p_s(\underline{Y}), 1 - Tq(\underline{Y}))_{K'[Y_1,\ldots,Y_n,T]}$. Clearly, $\mathcal{G}$ is also a Gröbner basis of $(p_1(\underline{Y}), \ldots, p_s(\underline{Y}), 1 - Tq(\underline{Y}))_{L'[Y_1,\ldots,Y_n,T]}$. So the assertion follows by Proposition 2.12. ∎

Proposition 2.21. *Let* K*,* $K(x_1, \ldots, x_n)$*,* $f_1(\underline{x}), \ldots, f_m(\underline{x})$ *and* $Z_1, \ldots, Z_n$ *be as in Notation 2.1. Let* L *be the field generated by the elements* $f_1(\underline{x}), \ldots, f_m(\underline{x})$ *over* K*. Moreover, let* $p_1(\underline{Z}), \ldots, p_s(\underline{Z}) \in K[Z_1, \ldots, Z_n]$ *be generators of the ideal* $J_K^{\underline{x}}$*, let*

$$h(\underline{Z}) := \prod_{i=1}^{m} h_i(\underline{Z})$$

and let I *be the ideal generated in the polynomial ring* $K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ *by the elements*

$$g_1(\underline{Z}) - f_1(\underline{x})h_1(\underline{Z}), \ldots, g_m(\underline{Z}) - f_m(\underline{x})h_m(\underline{Z}),$$
$$p_1(\underline{Z}), \ldots, p_s(\underline{Z}).$$

Then we have

$$J_L^{\underline{x}} = I : h(\underline{Z})^\infty.$$

Proof. Denote by I' the ideal generated in the polynomial ring $L[Z_1, \ldots, Z_n]$ by the elements $g_1(\underline{Z}) - f_1(\underline{x})h_1(\underline{Z}), \ldots, g_m(\underline{Z}) - f_m(\underline{x})h_m(\underline{Z}), p_1(\underline{Z}), \ldots, p_s(\underline{Z})$. By Lemma 2.20, it is equivalent to show that

$$J_L^{\underline{x}} = \left(I' : h(\underline{Z})^\infty\right)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}.$$

We claim that $I' : h(\underline{Z})^\infty$ is the ideal of relations of $x_1, \ldots, x_n$ over L. By definition of $J_L^{\underline{x}}$, this then proves the proposition. To prove the claim, let first $p(\underline{Z}) \in I' : h(\underline{Z})^\infty$. Then there exists $n' \in \mathbb{N}$ such that $p(\underline{Z})h(\underline{Z})^{n'} \in I'$. It follows that $p(\underline{x})h(\underline{x})^{n'} = 0$. Since $h(\underline{x})$ is not equal to zero, this implies that $p(\underline{x}) = 0$, which means that $p(\underline{Z})$ is a relation of $x_1, \ldots, x_n$ over L, indeed.
For the reverse inclusion suppose that $p(\underline{Z}) \in L[Z_1, \ldots, Z_n]$ is a relation of $x_1, \ldots, x_n$ over L. We need to show that $p(\underline{Z}) \in I' : h(\underline{Z})^\infty$. Let q be a polynomial in m indeterminates such that

$$q(f_1(\underline{x}), \ldots, f_m(\underline{x})) \cdot p(\underline{Z}) \in K[f_1(\underline{x}), \ldots, f_m(\underline{x})][Z_1, \ldots, Z_n],$$

and let p' be a polynomial in $m + n$ indeterminates such that

$$p'(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n) = q(f_1(\underline{x}), \ldots, f_m(\underline{x})) \cdot p(\underline{Z}).$$

From the fact that $p(\underline{Z}) = 1/q(f_1(\underline{x}), \ldots, f_m(\underline{x})) \cdot p'(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n)$ it follows that it is sufficient to show that $p'(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n)$ lies in $I' : h(\underline{Z})^\infty$.
Observe that firstly,

$$\begin{aligned} &p'(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n) \\ &\quad = p'((f_1(\underline{x}) - f_1(\underline{Z})) + f_1(\underline{Z}), \ldots, (f_m(\underline{x}) - f_m(\underline{Z})) + f_m(\underline{Z}), Z_1, \ldots, Z_n) \\ &\quad = \sum_{i=1}^{m} (f_i(\underline{x}) - f_i(\underline{Z})) \cdot q_i(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n) \\ &\qquad\qquad + p'(f_1(\underline{Z}), \ldots, f_m(\underline{Z}), Z_1, \ldots, Z_n). \end{aligned} \tag{2.1}$$

for certain elements $q_1(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n), \ldots, q_m(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n)$ in $K[f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n]$. Secondly, by definition of $h(\underline{Z}) \in K[Z_1, \ldots, Z_n]$, there exists $n' \in \mathbb{N}$ such that not only

$$\begin{aligned} &h(\underline{Z})^{n'} \cdot \sum_{i=1}^{m} (f_i(\underline{x}) - f_i(\underline{Z})) \cdot q_i(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n) \\ &\qquad\qquad \in (g_1(\underline{Z}) - f_1(\underline{x})h_1(\underline{Z}), \ldots, g_m(\underline{Z}) - f_m(\underline{x})h_m(\underline{Z}))_{L[Z_1,\ldots,Z_n]} \subset I' \end{aligned} \tag{2.2}$$

but also

$$h(\underline{Z})^{n'} \cdot p'(f_1(\underline{Z}), \ldots, f_m(\underline{Z}), Z_1, \ldots, Z_m) \in K[Z_1, \ldots, Z_n]. \tag{2.3}$$

By definition of p', we have $p'(f_1(\underline{x}), \ldots, f_m(\underline{x}), x_1, \ldots, x_n) = 0$. Therefore, it follows by (2.3) that thirdly

$$h(\underline{Z})^{n'} \cdot p'(f_1(\underline{Z}), \ldots, f_m(\underline{Z}), Z_1, \ldots, Z_n) \in J_K^{\underline{x}} = (p_1(\underline{Z}), \ldots, p_s(\underline{Z})). \tag{2.4}$$

Combining (2.1), (2.2) and (2.4) finally shows that

$$h(\underline{Z})^{n'} \cdot p'(f_1(\underline{x}), \ldots, f_m(\underline{x}), Z_1, \ldots, Z_n) \in I',$$

as asserted. ∎

Remarks. (a) The proposition can be used for the computation of MQS ideals. All we need is an algorithm for computing saturation ideals. But this can be done with Gröbner basis methods. An algorithm is formulated for example in [BW93], Chapter 6, Proposition 6.37.
An implementation of an algorithm for computing MQS ideals in the computer algebra system MAGMA can be found in the appendix.

(b) In the previous proposition, we assumed that L is generated by a finite number of elements $f_1(\underline{x}), \ldots, f_m(\underline{x}) \in K(x_1, \ldots, x_n)$. Note that in fact any intermediate field of K and $K(x_1, \ldots, x_n)$ is finitely generated. For a proof of this see [Lan02], Chapter V, § 1.

(c) In [MQS00a], Müller-Quade and Steinwandt proved a similar statement to the previous proposition, namely – with the notation of the previous proposition – that

$$(x_1 - Z_1, \ldots, x_n - Z_n) \cap L[Z_1, \ldots, Z_n] = \\ (g_1(\underline{Z}) - f_1(\underline{x})h_1(\underline{Z}), \ldots, g_m(\underline{Z}) - f_m(\underline{x})h_m(\underline{Z}), p_1(\underline{Z}), \ldots, p_s(\underline{Z}))_{L[Z_1,\ldots,Z_n]} : h(\underline{Z})^{\infty}.$$

The proof given here simplifies their ideas slightly. For algorithmic purposes, our statement is more convenient, since computations can be done in $K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$, which seems to be easier than in $L(Z_1, \ldots, Z_n)$.

(d) By definition, the MQS ideal $J_K^{\underline{x}}$ is generated by the relations of $x_1, \ldots, x_n$ over K. If we assume that $K(x_1, \ldots, x_n)$ is given by generators and relations, then clearly no further computation is required for $J_K^{\underline{x}}$.

MQS ideals have some nice properties. We will examine two of them in the following propositions. Originally, they have been proven in [MQS00a]. Nonetheless, we give a proof here for the benefit of being self-contained. We start with a lemma.

Lemma 2.22. *Let K' be a subfield of a field L', let $Y_1, \ldots, Y_m$ be indeterminates over L'*

and let I be an ideal in the polynomial ring $K'[Y_1, \ldots, Y_m]$. Then

$$\dim(I) = \dim((I)_{L'[Y_1,\ldots,Y_m]}).$$

Proof. Note that if $\mathcal{G}$ is a Gröbner basis of the ideal I, then it is also one of the ideal $(I)_{L'[Y_1,\ldots,Y_m]}$. So the equality is an immediate consequence of the standard algorithm for the computation of the dimension of an ideal in a polynomial ring from a Gröbner basis of the ideal (cf. [BW93], Chapter 9, Proposition 9.29). ∎

Proposition 2.23. *Let K, $K(x_1, \ldots, x_n)$, L and $Z_1, \ldots, Z_n$ be as in Notation 2.1. Then*

$$\dim(J_L^x) = \dim(J_L^x \cap L[Z_1, \ldots, Z_n]) = \operatorname{trdeg}_L(K(x_1, \ldots, x_n)),$$

the transcendental degree of $K(x_1, \ldots, x_n)$ over the field L.

Proof. By the previous lemma, the first equality follows directly from Proposition 2.17 and Corollary 2.18. For the second equality, recall that by Proposition 2.17 and Corollary 2.18, the ideal $J_L^x \cap L[Z_1, \ldots, Z_n]$ is equal to the ideal of relations of $x_1, \ldots, x_n$ over L. Therefore, the map

$$\begin{aligned} \operatorname{Quot}(L[Z_1, \ldots, Z_n]/(J_L^x \cap L[Z_1, \ldots, Z_n])) &\longrightarrow L(x_1, \ldots, x_n), \\ Z_i + (J_L^x \cap L[Z_1, \ldots, Z_n]) &\longmapsto x_i \qquad \text{for } i \in \{1, \ldots, n\}, \end{aligned}$$

where $\operatorname{Quot}(L[Z_1, \ldots, Z_n]/(J_L^x \cap L[Z_1, \ldots, Z_n]))$ as usual denotes the quotient field, is an L-isomorphism of fields. Since $K(x_1, \ldots, x_n) = L(x_1, \ldots, x_n)$, it follows that

$$\begin{aligned} \operatorname{trdeg}_L(K(x_1, \ldots, x_n)) &= \operatorname{trdeg}_L(\operatorname{Quot}(L[Z_1, \ldots, Z_n]/(J_L^x \cap L[Z_1, \ldots, Z_n]))) \\ &= \dim(J_L^x \cap L[Z_1, \ldots, Z_n]). \end{aligned}$$

For details about the above formula, see for example [BW93], Chapter 7, Section 1. ∎

The following proposition shows how we get the field L back from the MQS ideal J_L^x of $x_1, \ldots, x_n$ over L. It is an essential ingredient for the field-ideal correspondence which will be given in the next section.

Proposition 2.24. *Let K, $K(x_1, \ldots, x_n)$, L and $Z_1, \ldots, Z_n$ be as in Notation 2.1 and let $\leq$ be an arbitrary monomial order on $Z_1, \ldots, Z_n$. Then the coefficients of the reduced Gröbner basis of the MQS ideal $J_L^x \trianglelefteq K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ w. r. t. $\leq$ generate the field L over K.*

Proof. Let $\mathcal{G}$ be the reduced Gröbner basis of J_L^x with respect to $\leq$ and let L' be the field generated by the coefficients of the elements of $\mathcal{G}$. We need to show that $L' = L$.
Clearly, J_L^x has a finite generating set in $L[Z_1, \ldots, Z_n]$. Since the computation of the reduced Gröbner basis from a given generating set with the Buchberger algorithm (cf.

[Buc65]) does not extend the field of coefficients, L' is contained in L.
Conversely, let $f(\underline{x}) = g(\underline{x})/h(\underline{x}) \in L$. Then $g(\underline{Z}) - f(\underline{x})h(\underline{Z}) \in L[Z_1, \ldots, Z_n]$ is a relation of $x_1, \ldots, x_n$ over L and therefore,

$$g(\underline{Z}) - f(\underline{x})h(\underline{Z}) \in J_L^{\underline{x}}.$$

By Remark 2.11 (a), we see that $\mathrm{NF}_{\mathcal{G}}(h(\underline{Z})) \neq 0$ and furthermore that $\mathrm{NF}_{\mathcal{G}}(g(\underline{Z}) - f(\underline{x})h(\underline{Z})) = 0$. From the equation

$$\mathrm{NF}_{\mathcal{G}}(g(\underline{Z})) - f(\underline{x})\,\mathrm{NF}_{\mathcal{G}}(h(\underline{Z})) = \mathrm{NF}_{\mathcal{G}}(g(\underline{Z}) - f(\underline{x})h(\underline{Z})) = 0$$

(cf. Remark 2.11 (b)) and the fact that $\mathrm{NF}_{\mathcal{G}}(g(\underline{Z}))$ and $\mathrm{NF}_{\mathcal{G}}(h(\underline{Z}))$ are in $L'[Z_1, \ldots, Z_n]$ it follows that

$$f(\underline{x}) = \frac{\mathrm{NF}_{\mathcal{G}}(g(\underline{Z}))}{\mathrm{NF}_{\mathcal{G}}(h(\underline{Z}))} \in L'(\underline{Z}) \cap K(x_1, \ldots, x_n) = L',$$

as desired. ∎

The content of the following corollary seems to be well-known. Nonetheless, we state it here for creating a reference. It will be proved with similar methods as Proposition 2.24.

Corollary 2.25. *Let K' be a subfield of a field L', let $Y_1, \ldots, Y_n$ be indeterminates over L', let $Z_1, \ldots, Z_n$ be indeterminates over $L'(Y_1, \ldots, Y_n)$ and let $f_1, \ldots, f_m$ be elements in the field $K'(Y_1, \ldots, Y_n)$. Then we have*

$$L'(f_1, \ldots, f_m) \cap K'(Y_1, \ldots, Y_n) = K'(f_1, \ldots, f_m).$$

Proof. By Proposition 2.21 and Lemma 2.20, it follows that

$$J^{Y_1,\ldots,Y_n}_{L'(f_1,\ldots,f_m)} = \left(J^{Y_1,\ldots,Y_n}_{K'(f_1,\ldots,f_m)}\right)_{L'(Y_1,\ldots,Y_n)[Z_1,\ldots,Z_n]}.$$

Therefore, a reduced Gröbner basis $\mathcal{G}$ of the ideal $J^{Y_1,\ldots,Y_n}_{K'(f_1,\ldots,f_m)}$ is also a reduced Gröbner basis of the ideal $J^{Y_1,\ldots,Y_n}_{L'(f_1,\ldots,f_m)}$. Let $f(\underline{Y}) = g(\underline{Y})/h(\underline{Y})$ with polynomials $g(\underline{Y}), h(\underline{Y}) \in K'[Y_1, \ldots, Y_n]$ be an element in the intersection $L'(f_1, \ldots, f_m) \cap K'(Y_1, \ldots, Y_n)$. Then we have

$$g(\underline{Z}) - f(\underline{Y})h(\underline{Z}) \in J^{Y_1,\ldots,Y_n}_{L'(f_1,\ldots,f_m)},$$

which implies that

$$f(\underline{Y}) = \frac{\mathrm{NF}_{\mathcal{G}}(g(\underline{Z}))}{\mathrm{NF}_{\mathcal{G}}(h(\underline{Z}))}.$$

By Proposition 2.24, the coefficients of the elements of the reduced Gröbner basis $\mathcal{G}$ all lie in the field $K'(f_1, \ldots, f_m)$. So the previous equation shows that the element $f(\underline{Y})$ lies in $K'(f_1, \ldots, f_m)(Z_1, \ldots, Z_n) \cap L'(f_1, \ldots, f_m) = K'(f_1, \ldots, f_m)$, as asserted. ∎

2.3 The Lattice of MQS Ideals

Let $\mathcal{J} := \{J_L^x;\ K \leq L \leq K(x_1, \ldots, x_n)\}$ be the set of MQS ideals of $x_1, \ldots, x_n$ over the intermediate fields of K and $K(x_1, \ldots, x_n)$ and let $\mathcal{L} := \{L \subset K(x_1, \ldots, x_n);\ K \leq L \leq K(x_1, \ldots, x_n)\}$ be the set of intermediate fields of K and $K(x_1, \ldots, x_n)$. $\mathcal{L}$ together with $\cdot$ and $\cap$, which denote the composition and the intersection of fields, carries the structure of a lattice. In this section, we aim to give $\mathcal{J}$ the structure of a lattice and to establish an isomorphism of lattices between $\mathcal{J}$ and $\mathcal{L}$.

Lemma 2.26. *Let $\mathcal{I}$ and $\mathcal{J}$ be the sets as defined above. The map*

$$\mathcal{L} \longrightarrow \mathcal{J},\ L \longrightarrow J_L^x$$

is an inclusion-preserving 1-1-correspondence.

Proof. By definition of $\mathcal{J}$, the map is certainly surjective. Furthermore, it follows by Proposition 2.24 that the map is also injective. Thus it is in fact a bijection. Moreover, it is an immediate consequence of Definition 2.16 that the map is inclusion-preserving. ∎

Proposition and Definition 2.27. *Let K, $K(x_1, \ldots, x_n)$, L_1 and L_2 be as in Notation 2.1. Let the* **join** *of $J_{L_1}^x$ and $J_{L_2}^x$, denoted by $J_{L_1}^x \vee J_{L_2}^x$, be defined as*

$$J_{L_1}^x \vee J_{L_2}^x := J_{L_1 \cdot L_2}^x$$

and let the **meet** *of $J_{L_1}^x$ and $J_{L_2}^x$, denoted by $J_{L_1}^x \wedge J_{L_2}^x$, be defined as*

$$J_{L_1}^x \wedge J_{L_2}^x := J_{L_1 \cap L_2}^x.$$

The triple $(\mathcal{J}, \vee, \wedge)$ is a lattice. We call it the **lattice of MQS ideals of $\mathbf{x_1}, \ldots, \mathbf{x_n}$ over the intermediate fields of K and $\mathbf{K}(\mathbf{x_1}, \ldots, \mathbf{x_n})$**.

Proof. By Lemma 2.26, it is immediate that $(\mathcal{J}, \vee, \wedge)$ is a lattice. ∎

Proposition 2.28. *The lattice $(\mathcal{J}, \vee, \wedge)$ of MQS ideals of $x_1, \ldots, x_n$ over the intermediate fields of K and $K(x_1, \ldots, x_n)$ is isomorphic to the lattice $(\mathcal{L}, \cdot, \cap)$ of intermediate fields of K and $K(x_1, \ldots, x_n)$ via*

$$\mathcal{L} \longrightarrow \mathcal{J},\ L \longmapsto J_L^x.$$

Proof. The assertion follows directly from the definition of $\vee$ and $\wedge$. ∎

2.4 The Composition and the Intersection of Fields

In this section we want to examine how the composition and the intersection of intermediate fields of K and $K(x_1, \ldots, x_n)$ can be computed algorithmically. By the previous section, this problem is equivalent to computing the join and the meet in the lattice $(\mathcal{J}, \vee, \wedge)$ algorithmically. Whereas this problem is very easy for the join operator, several attempts have been made to find an algorithm for computing the meet. To the best of my knowledge, the last recent publication dealing with this problem is [SMQ00]. In that paper an algorithm was given for computing the meet $J^{\underline{x}}_{L_1} \wedge J^{\underline{x}}_{L_2}$ for the special case that L_1 and L_2 are linearly disjoint over their intersection. Here we will present a solution for another case, namely the case that L_1 and L_2 are algebraically closed in $K(x_1, \ldots, x_n)$ and the characteristic of the field K is zero. In fact, this situation is not as special as it seems at first sight. A variety of examples appear in invariant theory: For instance, the field of invariants of a connected group acting on a variety X is algebraically closed in $K(X)$. We will give a concrete example of such a situation later on.
The impulse to focus on this case was given by Harm Derksen. He communicated to me that he even found an algorithm – which he has not published yet – for computing the intersection of intermediate fields of K and $K(x_1, \ldots, x_n)$ in the case that just one of the intermediate fields is algebraically closed in $K(x_1, \ldots, x_n)$. I have not studied his ideas in detail, nonetheless they seem to be closely related to those presented here.

As already mentioned, the problem of the computation of the join is straightforward:

Remark. Let K, $K(x_1, \ldots, x_n)$ and $f_1(\underline{x}), \ldots, f_m(\underline{x})$ be as in Notation 2.1 and let $L_1 := K(f_1(\underline{x}), \ldots, f_s(\underline{x}))$ and $L_2 := K(f_{s+1}(\underline{x}), \ldots, f_m(\underline{x}))$ for some $s \in \{1, \ldots, m\}$. Then the join $J^{\underline{x}}_{L_1} \vee J^{\underline{x}}_{L_2}$ is given by

$$J^{\underline{x}}_{L_1 \cdot L_2} = (g_1(\underline{Z}) - f_1(\underline{x})h_1(\underline{Z}), \ldots, g_m(\underline{Z}) - f_m(\underline{x})h_m(\underline{Z}), p_1(\underline{Z}), \ldots, p_s(\underline{Z})) : h(\underline{Z})^\infty,$$

where again $h(\underline{Z}) := \prod_{i=1}^m h_i(\underline{Z})$. ♢

Before we present the algorithm for computing the meet, some more work has to be done. We begin with the definition of a primary ideal.

Definition 2.29. *Let R be a ring and let $I \trianglelefteq R$ be an ideal in R. The ideal I is called* **primary** *if for all $a, b \in R$*

$$ab \in I,\ a \notin I \Rightarrow b^n \in I \text{ for some } n \in \mathbb{N}.$$

In particular, if I is a primary ideal, then its radical $\sqrt{I}$ is a prime ideal. We say that I is **$\sqrt{\text{I}}$-primary**.

Proposition and Definition 2.30. *Let R be a noetherian ring and let $I \trianglelefteq R$ be a proper ideal in R. Then there exist primary ideals $Q_1, \ldots, Q_t \trianglelefteq R$ such that*

(a) $I = \bigcap_{i=1}^{t} Q_i$.

(b) $Q_j \notin \bigcap_{i=1, i\neq j}^{t} Q_i$ *for all* $j \in \{1, \ldots, t\}$.

(c) $\sqrt{Q_i} \neq \sqrt{Q_j}$ *for all distinct* $i, j \in \{1, \ldots, t\}$.

Such a representation is called a **primary decomposition** *of the ideal I.*

Proof. See for example [BW93], Chapter 8, Theorem 8.54. ∎

The following statements are true in a more general context. Let K' be a subfield of a field L' which is algebraically closed in L'. Moreover, let $Y_1, \ldots, Y_n$ be indeterminates over L'. We aim to prove that in characteristic zero, the extension of a prime ideal in $K'[Y_1, \ldots, Y_n]$ to $L'[Y_1, \ldots, Y_n]$ is again a prime ideal. As we will see later, this plays a central role in our algorithm for computing the meet. We will proceed as follows:
First, we will prove that in characteristic zero, the extension of a zero-dimensional radical ideal in $K'[Y_1, \ldots, Y_n]$ to $L'[Y_1, \ldots, Y_n]$ is again radical and that the extension of a zero-dimensional primary ideal in $K'[Y_1, \ldots, Y_n]$ to $L'[Y_1, \ldots, Y_n]$ is again primary. Since a radical primary ideal actually is a prime ideal, the assertion thus follows for zero-dimensional ideals. Then we will deduce the assertion for arbitrary dimensions.

Lemma 2.31. *Let K' be a subfield of a field L' which is algebraically closed in L' and let Y be an indeterminate over L'. Then a monic polynomial $p(Y) \in K'[Y]$ is irreducible over K', i. e. it is non-constant and it cannot be written as the product of two non-constant polynomials in K'[Y], if and only if it is irreducible over L'.*

Proof. If the monic polynomial $p(Y) \in K'[Y]$ is irreducible over L', then in particular, it is irreducible over K'. Conversely, suppose that $p(Y) \in K'[Y]$ is a monic polynomial which is irreducible over K'. Clearly – with $d := \deg(p(Y))$ the degree of $p(Y)$ – the polynomial $p(Y)$ splits up into

$$p(Y) = \prod_{i=1}^{d} (Y - a_i)\,,$$

for certain $a_1, \ldots, a_d \in \overline{L'}$, the algebraic closure of the field L'. Suppose now that

$$p(Y) = p_1(Y) \cdot p_2(Y)$$

for some monic polynomials $p_1(Y), p_2(Y) \in L'[Y]$. Then there exists $M \subset \{1, \ldots, d\}$ such that

$$p_1(Y) = \prod_{i \in M} (Y - a_i)\,.$$

The coefficients of $p_1(Y) \in L'[Y]$ are hence contained in the field $L' \cap K'(a_i;\ i \in M)$. From the fact that $a_1, \ldots, a_d$ are roots of the polynomial $p(Y) \in K'[Y]$ it follows that they are

algebraic over K'. This implies that the coefficients of the polynomial $p_1(Y) \in L'[Y]$ are algebraic over K', too. Since K' is algebraically closed in L', this actually means that

$$p_1(Y) \in K'[Y].$$

In the same way it follows that $p_2(Y) \in K'[Y]$. By assumption, either $p_1(Y)$ or $p_2(Y)$ is equal to 1. So $p(Y)$ is irreducible over L'. ∎

Lemma 2.32. *Let K' be a subfield of a field L' which is algebraically closed in L', let $\mathrm{char}(L') = 0$ and let $Y_1, \ldots, Y_n$ be indeterminates over L'. If $\hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]$ is a zero-dimensional radical ideal, then $I := (\hat{I})_{L'[Y_1,\ldots,Y_n]}$ is a radical ideal, too.*

Proof. Let $i \in \{1, \ldots, n\}$. Since $\hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]$ is a zero-dimensional ideal, we have

$$\hat{I} \cap K'[Y_i] \neq (0).$$

Let $q_i(Y_i) \in K'[Y_i] \setminus \{0\}$ be the unique monic generator of $\hat{I} \cap K'[Y_i]$. Since $\hat{I}$ is a radical ideal, the ideal $\hat{I} \cap K'[Y_i]$ is clearly radical, too. Therefore, the polynomial $q_i(Y_i)$ is squarefree. By definition of the ideal I, a Gröbner basis of $\hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]$ is also a Gröbner basis of $I \trianglelefteq L'[Y_1, \ldots, Y_n]$. Hence by Proposition 2.12, there exists a basis of $\hat{I} \cap K'[Y_i]$ which also generates the ideal $I \cap L'[Y_i]$. This implies that

$$I \cap L'[Y_i] = (\hat{I} \cap K'[Y_i])_{L'[Y_i]} = (q_i(Y_i))_{L'[Y_i]}.$$

Moreover, it follows by Lemma 2.31 that the polynomial $q_i(Y_i)$, is squarefree over L', too. Since we assumed K' and hence L' to be of characteristic zero, we therefore have

$$\gcd_{L'[Y_i]}(q_i(Y_i), q_i'(Y_i)) = 1,$$

where as usual $q_i'(Y_i)$ denotes the derivative of the polynomial $q_i(Y_i)$ with respect to Y_i and $\gcd_{L'[Y_i]}(q_i(Y_i), q_i'(Y_i))$ denotes the greatest common divisor of the polynomials $q_i(Y_i)$ and $q_i'(Y_i)$ in $L'[Y_i]$ (e. g. see [BW93], Chapter 2, Lemma 2.85). As $i \in \{1, \ldots, n\}$ was chosen arbitrarily and I is clearly zero-dimensional, too, the assertion follows by Seidenberg's Lemma 92 (e. g. see [BW93], Chapter 8, Lemma 8.13). ∎

Definition 2.33. *Let K' be an arbitrary field, let $Y_1, \ldots, Y_n$ be indeterminates over K' and let $i \in \{1, \ldots, n\}$. An ideal $I \trianglelefteq K'[Y_1, \ldots, Y_n]$ is called* **in normal position with respect to $\mathbf{Y_i}$** *if the Y_i-components of the zeroes of I in $(\overline{K'})^n$, where as usual $\overline{K'}$ denotes the algebraic closure of the field K', are pairwise distinct, that means for all points $(\xi_1, \ldots, \xi_n), (\zeta_1, \ldots, \zeta_n) \in (\overline{K'})^n$ with*

$$p(\xi_1, \ldots, \xi_n) = p(\zeta_1, \ldots, \zeta_n) = 0 \ \forall p \in I$$

we have $\xi_i \neq \zeta_i$.

Lemma 2.34. *Let K' be a subfield of a field L' which is infinite and algebraically closed in L'. Moreover, let $Y_1, \ldots, Y_n$ be indeterminates over L'. If $\hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]$ is a zero-dimensional primary ideal, then $I := (\hat{I})_{L'[Y_1,\ldots,Y_n]}$ is a primary ideal, too.*

Proof. First we show that we may assume that I is in normal position w. r. t. Y_i for some $i \in \{1, \ldots, n\}$. Note that by Lemma 2.22 the ideal I is zero-dimensional, too. Since K' has been assumed to be infinite, it follows by [BW93], Chapter 8, Lemma 8.76 that there exists $(c_2, \ldots, c_n) \in (K')^{n-1}$ such that the elements

$$\xi_1 + \sum_{i=2}^{n} c_i \xi_i \in \overline{L'}, \quad \text{for all } (\xi_1, \ldots, \xi_n) \in Z(I) \subset (\overline{L'})^n, \tag{2.5}$$

where $Z(I)$ denotes the set of elements $(\xi_1, \ldots, \xi_n) \in (\overline{L'})^n$ such that $p(\xi_1, \ldots, \xi_n) = 0$ for all $p \in I$, are pairwise distinct. Let $\hat{\phi} : K'[Y_1, \ldots, Y_n] \longrightarrow K'[Y_1, \ldots, Y_n]$ be the K'-automorphism defined by

$$Y_1 \longmapsto Y_1 - \sum_{i=2}^{n} c_i Y_i, \quad Y_j \longmapsto Y_j \quad \text{for } j \in \{2, \ldots, n\}$$

and let $\hat{J} := \hat{\phi}(\hat{I}) \trianglelefteq K'[Y_1, \ldots, Y_n]$. Clearly, $\hat{J}$ primary and by Proposition 2.14 moreover zero-dimensional. Note that the automorphism $\hat{\phi}$ can be extended to an L'-automorphism of $L'[Y_1, \ldots, Y_n]$ in the obvious way. Let $J := (\hat{J})_{L'[Y_1,\ldots,Y_n]} = \hat{\phi}(I)$ and let $\widetilde{\phi}$ be the bijective map defined by

$$\widetilde{\phi} : (\overline{L'})^n \longrightarrow (\overline{L'})^n,\ (\xi_1, \ldots, \xi_n) \longmapsto \left(\xi_1 + \sum_{i=2}^{n} c_i \xi_i, \xi_2, \ldots, \xi_n \right).$$

Then we have $q(\widetilde{\phi}(\xi_1, \ldots, \xi_n)) = 0$ for all $q \in J$ if and only if $p(\xi_1, \ldots, \xi_n) = 0$ for all $p \in I$. It hence follows by (2.5) that J is in normal position w. r. t. Y_1. Finally, since J is primary if and only if I is primary, we may assume that I is in normal position w. r. t. Y_i for some $i \in \{1, \ldots, n\}$, indeed.

Since $\hat{I}$ is zero-dimensional, we have

$$\hat{I} \cap K'[Y_i] \neq (0).$$

Let $p(Y_i) \in K'[Y_i] \setminus \{0\}$ be the unique monic generator of $\hat{I} \cap K'[Y_i]$. From the fact that $\hat{I}$ is a primary ideal it follows that $\hat{I} \cap K'[Y_i]$ is primary, too. So we have

$$p(Y_i) = q(Y_i)^m$$

for some irreducible, monic polynomial $q(Y_i) \in K'[Y_i]$. By definition of the ideal I, a Gröbner basis of $\hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]$ is also a Gröbner basis of $I \trianglelefteq L'[Y_1, \ldots, Y_n]$. Hence by Proposition 2.12, there exists a basis of $\hat{I} \cap K'[Y_i]$ which also generates the ideal $I \cap L'[Y_i]$.

This implies that

$$I \cap L'[Y_i] = (\hat{I} \cap K'[Y_i])_{L'[Y_i]} = (q(Y_i)^m)_{L'[Y_i]}.$$

Note that by Lemma 2.31, the polynomial $q(Y_i)$ is irreducible in $L'[Y_i]$, too. So, finally by [BW93], Chapter 8, Proposition 8.69, it follows that I is primary, as asserted. ∎

Combining the last two lemmas, we get the following proposition.

Proposition 2.35. *Let K' be a subfield of a field L' which is algebraically closed in L', let $\mathrm{char}(L') = 0$ and let $Y_1, \ldots, Y_n$ be indeterminates over L'. If $\hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]$ is a zero-dimensional prime ideal, then $I := (\hat{I})_{L'[Y_1,\ldots,Y_n]}$ is a prime ideal, too.*

Proof. A primary radical ideal is certainly prime. So the proposition is immediate by Lemma 2.32 and Lemma 2.34. ∎

Our next aim is the generalization of Proposition 2.35 to arbitrary dimensions of the ideal I. For this purpose we need the following lemma.

Lemma 2.36. *Let K' be a subfield of a field L' which is algebraically closed in L' and let Y be an indeterminate over L'. Then $K'(Y)$ is algebraically closed in $L'(Y)$.*

Proof. Let $g(Y)/h(Y) \neq 0 \in L'(Y)$ with $g(Y), h(Y) \in L'[Y]$ coprime polynomials be algebraic over $K'(Y)$. We need to show that $g(Y)/h(Y) \in K'(Y)$. Since $g(Y)/h(Y)$ is algebraic over $K'(Y)$, there exists $m \in \mathbb{N}$ and polynomials $p_0(Y), \ldots, p_m(Y) \in K'[Y]$ with $p_m(Y) \neq 0$ such that

$$\sum_{i=0}^{m} p_i(Y) \cdot \left(\frac{g(Y)}{h(Y)}\right)^i = 0.$$

It follows that

$$p_m(Y)g(Y)^m = -\sum_{i=0}^{m-1} p_i(Y)g(Y)^i h(Y)^{m-i}.$$

Since $g(Y)$ and $h(Y)$ were assumed to be coprime, it follows that $h(Y)$ is a divisor of $p_m(Y)$ in the polynomial ring $L'[Y]$. Let $c \in K'$ such that $c \cdot p_m(Y)$ is monic and let $l_1 \in L'$ such that $l_1 \cdot h(Y)$ is monic. Since K' is algebraically closed in the field L', it follows from Lemma 2.31 that a factorization of the polynomial $c \cdot p_m(Y)$ into irreducible monic factors in the polynomial ring $K'[Y]$ is also a factorization of $c \cdot p_m(Y)$ into irreducible monic factors in the polynomial ring $L'[Y]$. This implies

$$l_1 \cdot h(Y) \in K'[Y].$$

From the fact that $h(Y)/g(Y) \in L'(Y)$ is algebraic over $K'(Y)$, too, the same argumentation shows that there exists $l_2 \in L'$ such that $l_2 \cdot g(Y) \in K'[Y]$. Finally, note that any $l \in L' \setminus K'$ is transcendental over $K'(Y)$. Since $l_2/l_1 \cdot g(Y)/h(Y) \in K'(Y)$ is obviously

algebraic over $K'(Y)$, it follows that l_2/l_1 in fact lies in the field K'. This shows

$$\frac{g(Y)}{h(Y)} \in K'(Y),$$

as desired. ∎

Proposition 2.37. *Let K' be a subfield of a field L' which is algebraically closed in L', let* $\mathrm{char}(L') = 0$ *and let $Y_1, \ldots, Y_n$ be indeterminates over L'. If $\hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]$ is a prime ideal, then $I := (\hat{I})_{L'[Y_1,\ldots,Y_n]}$ is a prime ideal, too.*

Proof. Let $M = \{Y_{i_1}, \ldots, Y_{i_s}\} \subset \{Y_1, \ldots, Y_n\}$ be maximal such that

$$I \cap L'[Y_{i_1}, \ldots, Y_{i_s}] = (0).$$

Since $\hat{I} \subset I$, we clearly also have

$$\hat{I} \cap L'[Y_{i_1}, \ldots, Y_{i_s}] = (0).$$

Let $\mathcal{G} \subset K'[Y_1, \ldots, Y_n]$ be a Gröbner basis of the ideal $\hat{I}$, so also of the ideal I, with respect to some inverse block order w. r. t. M (cf. Definition 2.3) and denote the elements of $\{Y_1, \ldots, Y_n\} \setminus M$ by $Y_{j_1}, \ldots, Y_{j_{n-s}}$. Then $\mathcal{G}$ is also a Gröbner basis with respect to the induced monomial order on $Y_{j_1}, \ldots, Y_{j_{n-s}}$ of the ideals

$$\hat{I}^e := (\hat{I}) \trianglelefteq K'(Y_{i_1}, \ldots, Y_{i_s})[Y_{j_1}, \ldots, Y_{j_{n-s}}]$$

and

$$I^e := (I) \trianglelefteq L'(Y_{i_1}, \ldots, Y_{i_s})[Y_{j_1}, \ldots, Y_{j_{n-s}}],$$

that means the extension of the ideal $\hat{I}$ to $K'(Y_{i_1}, \ldots, Y_{i_s})[Y_{j_1}, \ldots, Y_{j_{n-s}}]$ and the extension of the ideal I to $L'(Y_{i_1}, \ldots, Y_{i_s})[Y_{j_1}, \ldots, Y_{j_{n-s}}]$ (cf. [BW93], Chapter 8, Lemma 8.93). We claim that $\hat{I}^e \cap K'[Y_1, \ldots, Y_n] = \hat{I}$ and that $I^e \cap L'[Y_1, \ldots, Y_n] = I$. Let $q(Y_{i_1}, \ldots, Y_{i_s}) \in K'[Y_{i_1}, \ldots, Y_{i_s}]$ be the least common multiple of the leading coefficients of the elements of the Gröbner basis $\mathcal{G} \subset K'(Y_{i_1}, \ldots, Y_{i_s})[Y_{j_1}, \ldots, Y_{j_{n-s}}]$. Then it can be shown that

$$\hat{I}^e \cap K'[Y_1, \ldots, Y_n] = \hat{I} : q(Y_{i_1}, \ldots, Y_{i_s})^\infty \tag{2.6}$$

and

$$I^e \cap L'[Y_1, \ldots, Y_n] = I : q(Y_{i_1}, \ldots, Y_{i_s})^\infty$$

(cf. [BW93], Chapter 8, Lemma 8.91). It follows from Lemma 2.20 that actually

$$I^e \cap L'[Y_1, \ldots, Y_n] = (\hat{I} : q(Y_{i_1}, \ldots, Y_{i_s})^\infty)_{L'[Y_1,\ldots,Y_n]}.$$

So we just need to show that $\hat{I}^e \cap K'[Y_1, \ldots, Y_n] = \hat{I}$, since then $I^e \cap L'[Y_1, \ldots, Y_n] = (\hat{I})_{L'[Y_1,\ldots,Y_n]} = I$. Clearly, we have $\hat{I} \subset \hat{I}^e \cap K'[Y_1, \ldots, Y_n]$. To prove the reverse inclusion,

let $p(\underline{Y}) \in \hat{I}^e \cap K'[Y_1, \ldots, Y_n]$. By equation (2.6), there exists $n' \in \mathbb{N}$ such that

$$p(\underline{Y}) \cdot q(Y_{i_1}, \ldots, Y_{i_s})^{n'} \in \hat{I}.$$

By the choice of $M \subset \{Y_1, \ldots, Y_n\}$, we clearly have $q(Y_{i_1}, \ldots, Y_{i_s})^{n'} \notin \hat{I}$. From the fact that $\hat{I}$ is a prime ideal, it hence follows that $p(\underline{Y}) \in \hat{I}$. Therefore, we have

$$\hat{I}^e \cap K'[Y_1, \ldots, Y_n] = \hat{I}, \tag{2.7}$$

and so also

$$I^e \cap L'[Y_1, \ldots, Y_n] = (\hat{I})_{L[Y_1,\ldots,Y_n]} = I, \tag{2.8}$$

as claimed.
Note that by construction, the ideal $\hat{I}^e$ is zero-dimensional and the ideal I^e is equal to $(\hat{I}^e)_{L'(Y_{i_1},\ldots,Y_{i_s})[Y_{j_1},\ldots,Y_{j_{n-s}}]}$. We aim to apply Proposition 2.35 to $\hat{I}^e$. From Lemma 2.36 it follows by induction that the field $K'(Y_{i_1}, \ldots, Y_{i_s})$ is algebraically closed in $L'(Y_{i_1}, \ldots, Y_{i_s})$. It hence remains to show that $\hat{I}^e \trianglelefteq K'(Y_{i_1}, \ldots, Y_{i_s})[Y_{j_1}, \ldots, Y_{j_{n-s}}]$ is a prime ideal. Let $q_1(Y_{j_1}, \ldots, Y_{j_{n-s}}), q_2(Y_{j_1}, \ldots, Y_{j_{n-s}}) \in K'(Y_{i_1}, \ldots, Y_{i_s})[Y_{j_1}, \ldots, Y_{j_{n-s}}]$ such that

$$q_1(Y_{j_1}, \ldots, Y_{j_{n-s}}) \cdot q_2(Y_{j_1}, \ldots, Y_{j_{n-s}}) \in \hat{I}^e.$$

Clearly, there exist nonzero polynomials $q_1'(Y_{i_1}, \ldots, Y_{i_s}), q_2'(Y_{i_1}, \ldots, Y_{i_s}) \in K'[Y_{i_1}, \ldots, Y_{i_s}]$ such that

$$\begin{aligned} q_1'(Y_{i_1}, \ldots, Y_{i_s}) \cdot q_1(Y_{j_1}, \ldots, Y_{j_{n-s}}) &\in K'[Y_1, \ldots, Y_n], \\ q_2'(Y_{i_1}, \ldots, Y_{i_s}) \cdot q_2(Y_{j_1}, \ldots, Y_{j_{n-s}}) &\in K'[Y_1, \ldots, Y_n]. \end{aligned}$$

By equation (2.7), we then have

$$\begin{aligned} &q_1'(Y_{i_1}, \ldots, Y_{i_s}) \cdot q_1(Y_{j_1}, \ldots, Y_{j_{n-s}}) \\ &\quad \cdot q_2'(Y_{i_1}, \ldots, Y_{i_s}) \cdot q_2(Y_{j_1}, \ldots, Y_{j_{n-s}}) \in \hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]. \end{aligned}$$

Since $\hat{I}$ is a prime ideal, either $q_1'(Y_{i_1}, \ldots, Y_{i_s}) \cdot q_1(Y_{j_1}, \ldots, Y_{j_{n-s}}) \in \hat{I}$ or $q_2'(Y_{i_1}, \ldots, Y_{i_s}) \cdot q_2(Y_{j_1}, \ldots, Y_{j_{n-s}}) \in \hat{I}$. So one of the polynomials $q_1(Y_{j_1}, \ldots, Y_{j_{n-s}})$ or $q_2(Y_{j_1}, \ldots, Y_{j_{n-s}})$ lies in the ideal $\hat{I}^e$. This shows that $\hat{I}^e$ is a prime ideal. By Proposition 2.35, it hence follows that the ideal I^e is prime, too. This finally proves the proposition (cf. equation (2.8)). ∎

Remark. Proposition 2.37 is also true, if we replace prime by primary. The proof is almost the same. ♢

We can now give an algorithm for computing the meet of two MQS ideals $J_{L_1}^{\underline{x}}$ and $J_{L_2}^{\underline{x}}$ in the case that the fields L_1 and L_2 are algebraically closed in $K(x_1, \ldots, x_n)$ and $\mathrm{char}(K) = 0$. By Proposition 2.24, this gives an algorithm for computing the intersection of the fields L_1 and L_2.

Algorithm 2.38. (Computing the meet)

Input: A field extension $K(x_1,\ldots,x_n)$ over a field K of characteristic zero, MQS ideals $J^{\underline{x}}_{L_1}, J^{\underline{x}}_{L_2} \trianglelefteq K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]$ of $x_1,\ldots,x_n$ over intermediate fields L_1 and L_2 of K and $K(x_1,\ldots,x_n)$ which are algebraically closed in $K(x_1,\ldots,x_n)$.

Output: The meet $J^{\underline{x}}_{L_1\cap L_2} \trianglelefteq K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]$ of the MQS ideals.

(1) Set $i := 1$, $I_1 := (1)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$, $J_1 := J^{\underline{x}}_{L_1}$

(2) While $J_i \neq I_i$:

- Compute the restriction $J_i \cap L_2[Z_1,\ldots,Z_n]$ (see Remark 2.39) and set
$$I_{i+1} := (J_i \cap L_2[Z_1,\ldots,Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}.$$
- Compute the restriction $I_{i+1} \cap L_1[Z_1,\ldots,Z_n]$ (see Remark 2.39) and set
$$J_{i+1} := (I_{i+1} \cap L_1[Z_1,\ldots,Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}.$$
- Set $i := i+1$

(3) Return J_i.

Remark 2.39. An algorithm for computing the ideal restrictions in step (2) can be found in [BMQS06]. As input data this algorithm requires the ideal in the polynomial ring $K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]$ which shall be restricted and the MQS ideal of $x_1,\ldots,x_n$ over the new coefficient field, i. e. in our case the MQS ideal $J^{\underline{x}}_{L_2}$ resp. the MQS ideal $J^{\underline{x}}_{L_1}$. $\diamondsuit$

Proof of Correctness. First, we will prove that the algorithm terminates. Then we will show that the returned ideal is indeed equal to $J^{\underline{x}}_{L_1\cap L_2}$.
Assume for a contradiction that the while loop does not terminate. By Proposition 2.17, we have the equality
$$J_1 = ((x_1 - Z_1,\ldots,x_n - Z_n) \cap L_1[Z_1,\ldots,Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}.$$
Note that the ideal $(x_1 - Z_1,\ldots,x_n - Z_n) \trianglelefteq K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]$ is clearly prime and that the intersection of a prime ideal with a subalgebra gives again a prime ideal. So it follows by Proposition 2.37 that the ideal J_1 is prime, too. Let $i \in \mathbb{N}$ and suppose that the ideal J_i is prime. Then – again by Proposition 2.37 – it can be seen that the ideal
$$I_{i+1} = (J_i \cap L_2[Z_1,\ldots,Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$$

is also prime. In the same way it hence follows that the ideal

$$J_{i+1} = (I_{i+1} \cap L_1[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$$

is again prime. By induction, this implies that all the ideals J_i, $i \in \mathbb{N}$ are prime.
Now observe that we have the inclusions

$$\begin{aligned} J_{i+1} =& ((J_i \cap L_2[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L_1[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \\ &\subset (J_i \cap L_2[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} = I_{i+1} \end{aligned}$$

and

$$I_{i+1} = (J_i \cap L_2[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \subset J_i$$

for all $i \in \mathbb{N}$. Moreover, by assumption, we have $J_{i+1} \neq I_{i+1}$ which implies that in fact

$$J_{i+1} \subsetneq J_i$$

for all $i \in \mathbb{N}$. So the chain of prime ideals J_i, $i \in \mathbb{N}$ in the algebra $K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ is descending strictly. Since $K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ is a finite-dimensional algebra, this is clearly a contradiction. It follows that the algorithm terminates after a finite number of steps.
It remains to show that the algorithm actually returns the MQS ideal $J^{\underline{x}}_{L_1 \cap L_2}$. Let $s \in \mathbb{N}, s \geq 2$ such that $J_s = I_s$ (note that we always have $J_1 \neq I_1$). First, we show that the ideal $J^{\underline{x}}_{L_1 \cap L_2}$ is contained in the ideal J_s that we return. By definition, the ideal $J^{\underline{x}}_{L_1 \cap L_2}$ is clearly contained in the MQS ideal $J^{\underline{x}}_{L_1}$, i.e.

$$J^{\underline{x}}_{L_1 \cap L_2} \subset J_1.$$

Let $i \in \mathbb{N}$, $i < s$ and suppose that the ideal $J^{\underline{x}}_{L_1 \cap L_2}$ is contained in the ideal J_i. By Proposition 2.17 and Corollary 2.18, we hence get the inclusion

$$\begin{aligned} J^{\underline{x}}_{L_1 \cap L_2} &= (J^{\underline{x}}_{L_1 \cap L_2} \cap (L_1 \cap L_2)\,[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \\ &\subset (J_i \cap L_2[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} = I_{i+1} \end{aligned}$$

and thus also

$$\begin{aligned} J^{\underline{x}}_{L_1 \cap L_2} &= (J^{\underline{x}}_{L_1 \cap L_2} \cap (L_1 \cap L_2)\,[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \\ &\subset (I_{i+1} \cap L_1[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} = J_{i+1}. \end{aligned}$$

By induction, it follows that the ideal $J^{\underline{x}}_{L_1 \cap L_2}$ is contained in the ideal J_i for all $i \in \mathbb{N}$. In particular, the ideal $J^{\underline{x}}_{L_1 \cap L_2}$ is contained in the ideal J_s that we return.
Finally, we show that J_s is contained in the MQS ideal $J^{\underline{x}}_{L_1 \cap L_2}$, meaning that $J_s = J^{\underline{x}}_{L_1 \cap L_2}$. By construction, the ideal J_s has a generating set in $L_1[Z_1, \ldots, Z_n]$ and the ideal I_s has a generating set in $L_2[Z_1, \ldots, Z_n]$. Since $I_s = J_s$ and the computation of the reduced Gröbner basis from a given generating set with the Buchberger algorithm [Buc65] does not extend the field of coefficients, the reduced Gröbner basis of J_s actually lies

in $(L_1 \cap L_2)[Z_1, \ldots, Z_n]$. Therefore, it follows from the inclusions $J_s \subset J_1 \subset (x_1 - Z_1, \ldots, x_n - Z_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$ that J_s is contained in the ideal

$$\left((x_1 - Z_1, \ldots, x_n - Z_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap (L_1 \cap L_2)[Z_1, \ldots, Z_n]\right)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]},$$

which is equal to $J^x_{L_1 \cap L_2}$ (cf. Proposition 2.17). ∎

Remark. The intersection of intermediate fields of K and $K(x_1, \ldots, x_n)$ which are algebraically closed in $K(x_1, \ldots, x_n)$ is again algebraically closed in $K(x_1, \ldots, x_n)$. Therefore, the intersection of finitely many intermediate fields of K and $K(x_1, \ldots, x_n)$ which are algebraically closed in $K(x_1, \ldots, x_n)$ can be computed with this algorithm. ♢

Example 2.40 (Computing the intersection of two fields with Algorithm 2.38).

Let X_1, X_2, X_3, X_4, X_5 be indeterminates over $\overline{\mathbb{Q}}$. We compute the intersection of the fields

$$L_1 := \overline{\mathbb{Q}}(X_1, X_1X_5 - X_2, -2X_1^2X_3 - X_1X_5^2 + 2X_2X_5, -6X_1^4X_4 + 6X_1^2X_3X_5 + X_1X_5^3 - 3X_2X_5^2)$$

and

$$L_2 := \overline{\mathbb{Q}}(X_1, X_2, X_3).$$

The field L_1 has gained prominence as the first example of an invariant field – of some G_a-variety, where G_a is the additive group – whose corresponding invariant ring is not finitely generated. It was developed by Daigle and Freudenberg (cf. [DF99]). As an invariant field with respect to a connected group action, the field L_1 is algebraically closed in $\overline{\mathbb{Q}}(X_1, \ldots, X_5)$. (For details about the notion of an invariant field and an invariant ring see Chapter 3 and Chapter 4.)
Taking the MQS ideals $J^{X_1,\ldots,X_5}_{L_1}$ and $J^{X_1,\ldots,X_5}_{L_2}$ as input data, Algorithm 2.38 terminates after one loop with the ideal

$$J^{X_1,\ldots,X_5}_{L_1 \cap L_2} = (Z_2^2 - 2X_1^3Z_3 + 2X_1^3X_3 - X_2^2, Z_1 - X_1) \trianglelefteq \overline{\mathbb{Q}}(X_1, \ldots, X_5)[Z_1, \ldots, Z_5],$$

where $Z_1, \ldots, Z_n$ are indeterminates over $\overline{\mathbb{Q}}(X_1, \ldots, X_5)$. By Proposition 2.24, we hence get

$$L_1 \cap L_2 = \mathbb{Q}(X_1, 2X_1^3X_3 - X_2^2).$$ ◁

Apart from the case that we considered, i. e. that the fields L_1 and L_2 are both algebraically closed in $K(x_1, \ldots, x_n)$ and $\mathrm{char}(K) = 0$, the algorithm might work in many further cases. The only problem is that we do not have an a priori criterion for the termination of the while loop. In other words, the algorithm produces correct results for arbitrary fields $L_1, L_2 \leq K(x_1, \ldots, x_n)$ in arbitrary characteristic provided that it terminates. Yet, there are cases, where the while loop does not terminate.

Examples 2.41. (a) Let X_1 be an indeterminate over $\mathbb{Q}$ and let $L_1 := \mathbb{Q}(X_1^2)$ and $L_2 := \mathbb{Q}(X_1^2 + X_1)$. Note that the fields L_1 and L_2 are not algebraically closed in $\mathbb{Q}(X_1)$. We show that Algorithm 2.38 does not terminate for these fields. Let Z_1 be an indeterminate over $\mathbb{Q}(X_1)$. We claim – with the notation of Algorithm 2.38 – that

$$I_{n+1} = \left(\prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \right)$$

and

$$J_{n+1} = \left(\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \right)$$

for all $n \in \mathbb{N}_0$. Assume for a moment that the claim is true. Then we clearly have a strictly descending chain of ideals $I_1 \supsetneq J_1 \supsetneq I_2, \ldots$, which shows that the algorithm does not terminate.
To prove the claim, we use induction on $n \in \mathbb{N}_0$. Note that the ideal I_1 is equal to $(1) \trianglelefteq K(X_1)[Z_1]$. Furthermore by Proposition 2.21, we have

$$J_1 = J_{X_1^2}^{X_1} = (Z_1^2 - X_1^2) \trianglelefteq \mathbb{Q}(X_1)[Z_1].$$

So the assertion is true for $n = 0$.
Now suppose that the claim is true for some $n \in \mathbb{N}_0$. A straightforward calculation shows that

$$\begin{aligned}
&(Z_1^2 - X_1^2 + 2nX_1 - n^2) \cdot (Z_1^2 - X_1^2 - 2(n+1)X_1 - (n+1)^2) \\
&\quad = Z_1^4 + (-2(X_1^2 + X_1) - 2n^2 - 2n - 1)Z_1^2 \\
&\qquad + (X_1^2 + X_1)(X_1^2 + X_1 - 2n^2 - 2n) + n^4 + 2n^3 + n^2 \\
&\quad \in \mathbb{Q}(X_1^2 + X_1)[Z_1]
\end{aligned}$$

and that

$$\begin{aligned}
&(Z_1^2 - X_1^2 - 2(n+1)X_1 - (n+1)^2) \cdot (Z_1^2 - X_1^2 + 2(n+1)X_1 - (n+1)^2) \\
&\quad = Z_1^4 + (-2)(X_1^2 + (n+1)^2)Z_1^2 + X_1^4 - 2(n+1)^2X_1^2 + (n+1)^4 \\
&\quad \in \mathbb{Q}(X_1^2)[Z].
\end{aligned}$$

So by assumption, it can be seen that

$$\begin{aligned}
&\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \\
&\quad = \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \\
&\qquad \cdot (Z_1^2 - X_1^2 - 2(n+1)X_1 - (n+1)^2)
\end{aligned}$$

$$
\begin{aligned}
&= \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \\
&\quad \cdot (Z_1^2 - X_1^2 + 2nX_1 - n^2) \cdot (Z_1^2 - X_1^2 - 2(n+1)X_1 - (n+1)^2) \\
&\in J_{n+1} \cap \mathbb{Q}(X_1^2 + X_1)[Z_1] \subset I_{n+2}
\end{aligned}
$$

and

$$
\begin{aligned}
&\prod_{i=0}^{n+1} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \\
&\quad = \prod_{i=0}^{n} \left(Z^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \\
&\qquad \cdot (Z_1^2 - X_1^2 + 2(n+1)X_1 - (n+1)^2) \\
&\quad = \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \\
&\qquad \cdot (Z_1^2 - X_1^2 + 2(n+1)X_1 - (n+1)^2) \cdot (Z_1^2 - X_1^2 - 2(n+1)X_1 - (n+1)^2) \\
&\quad \in I_{n+2} \cap \mathbb{Q}(X_1^2)[Z_1] \subset J_{n+2}.
\end{aligned}
$$

It remains to show that these polynomials actually generate the ideals I_{n+2} and J_{n+2}. Denote by $p_{n+2}(Z_1) \in \mathbb{Q}(X_1^2 + X_1)[Z_1]$ the generator of the principal ideal I_{n+2} and by $q_{n+2}(Z_1) \in \mathbb{Q}(X_1^2)[Z_1]$ the generator of the principal ideal J_{n+2}. Then

$$
p_{n+2}(Z_1) \mid \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right),
$$

and as the ideal I_{n+2} is contained in the ideal J_{n+1} it follows from the assumption that

$$
\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \mid p_{n+2}(Z_1).
$$

So there are just finitely many candidates for the polynomial $p_{n+2}(Z_1)$. We examine these candidates.

Note that a non-constant polynomial in $\mathbb{Q}[X_1^2]$, so also the constant term of the polynomial $\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \in \mathbb{Q}[X_1^2][Z_1]$, is not contained in $\mathbb{Q}(X_1^2 + X_1)$. Therefore, it follows that the polynomial $\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right)$ is not contained in $\mathbb{Q}(X_1^2 + X_1)[Z_1]$. Moreover, from the fact that the constant term of the polynomial

$$
\begin{aligned}
&\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \\
&\qquad \cdot (Z_1 - (X_1 + (n+1))) \in \mathbb{Q}(X_1)[Z_1]
\end{aligned}
$$

as well as of the polynomial

$$\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n-1} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \cdot (Z_1 + (X_1 + (n+1))) \in \mathbb{Q}(X_1)[Z_1]$$

is a polynomial in $Q[X_1]$ whose degree is odd, it follows that neither of these polynomials is contained in $\mathbb{Q}(X_1^2 + X_1)[Z_1]$. This implies that we actually have

$$p_{n+2}(Z_1) = \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right),$$

as claimed.
The argumentation for the generator $q_{n+2}(Z_1)$ of the ideal J_{n+2} is quite similar. We clearly have

$$q_{n+2}(Z_1) \mid \prod_{i=0}^{n+1} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right),$$

and as the ideal J_{n+2} is contained in the ideal I_{n+2} moreover that

$$\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \mid q_{n+2}(Z_1).$$

Again, there are just finitely many candidates for the polynomial $q_{n+2}(Z_1)$. We examine these candidates.
Since the constant term of the polynomial $p_{n+2}(Z_1) = \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \in \mathbb{Q}(X_1^2 + X_1)[Z_1]$ is a non-constant polynomial in $\mathbb{Q}[X_1^2 + X_1]$ and hence is clearly not contained in $\mathbb{Q}(X_1^2)$, it follows that $p_{n+2}(Z_1)$ is not contained in $\mathbb{Q}(X_1^2)[Z_1]$. Furthermore, since the constant term of the polynomial

$$\prod_{i=0}^{n} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right) \cdot (Z_1 - (X_1 - (n+1)))$$

is a polynomial in $\mathbb{Q}[X_1]$ whose degree is odd, it is not contained in $\mathbb{Q}(X_1^2)[Z_1]$, either. So in fact, we have

$$q_{n+2}(Z_1) = \prod_{i=0}^{n+1} \left(Z_1^2 - X_1^2 + 2iX_1 - i^2\right) \cdot \prod_{i=0}^{n} \left(Z_1^2 - X_1^2 - 2(i+1)X_1 - (i+1)^2\right),$$

as claimed.

(b) Let X_1, X_2 be indeterminates over $\mathbb{Q}$. Clearly, the fields $L_1 := \mathbb{Q}(X_1^2)$ and $L_2 := \mathbb{Q}(X_2^2)$ are not algebraically closed in $\mathbb{Q}(X_1, X_2)$. Let Z_1, Z_2 be indeterminates over

$\mathbb{Q}(X_1, X_2)$. Then by Proposition 2.21,

$$J_{L_1}^{X_1,X_2} = (Z_1^2 - X_1^2) \trianglelefteq \mathbb{Q}(X_1, X_2)[Z_1, Z_2].$$

It is not hard to verify that

$$J_{L_1}^{X_1,X_2} \cap \mathbb{Q}(X_2^2)[Z_1, Z_2] = (0).$$

It follows that the ideal $(J_{L_1}^{X_1,X_2} \cap \mathbb{Q}(X_2^2)[Z_1, Z_2])_{\mathbb{Q}(X_1,X_2)[Z_1,Z_2]}$ as well as the ideal $((J_{L_1}^{X_1,X_2} \cap \mathbb{Q}(X_2^2)[Z_1, Z_2])_{\mathbb{Q}(X_1,X_2)[Z_1,Z_2]} \cap \mathbb{Q}(X_1^2)[Z_1, Z_2])_{\mathbb{Q}(X_1,X_2)[Z_1,Z_2]}$ is equal to zero. In particular, these ideals are equal. So the algorithm terminates, although the fields L_1 and L_2 are not algebraically closed in $\mathbb{Q}(X_1, X_2)$. ◁

Our next aim is to find a method for testing the hypothesis that some subfields L_1 and L_2 of a field $K(x_1, \ldots, x_n)$ are algebraically closed in $K(x_1, \ldots, x_n)$.

Proposition 2.42. *Let K, $K(x_1, \ldots, x_n)$ and L be as in Notation 2.1. Moreover, let* $\mathrm{char}(K(x_1, \ldots, x_n))$ *be equal to zero. The field L is algebraically closed in $K(x_1, \ldots, x_n)$ if and only if the MQS ideal J_L^x is a prime ideal.*

Proof. First, assume that the ideal J_L^x is prime. Denote the algebraic closure of the field L in $K(x_1, \ldots, x_n)$ by $\tilde{L}$. Then we have the inclusion $J_L^x \subset J_{\tilde{L}}^x$ (cf. Definition 2.16) and therefore also

$$J_L^x \cap \tilde{L}[Z_1, \ldots, Z_n] \subset J_{\tilde{L}}^x \cap \tilde{L}[Z_1, \ldots, Z_n]. \tag{2.9}$$

Recall from Proposition 2.23 that

$$\dim(J_L^x \cap L[Z_1, \ldots, Z_n]) = \mathrm{trdeg}_L(K(x_1, \ldots, x_n)).$$

Since by Lemma 2.22 the dimension of the ideal $J_L^x \cap L[Z_1, \ldots, Z_n]$ is the same as the dimension of the ideal $\left(J_L^x \cap L[Z_1, \ldots, Z_n]\right)_{\tilde{L}[Z_1,\ldots,Z_n]}$, it follows that

$$\begin{aligned}
\mathrm{trdeg}_L(K(x_1, \ldots, x_n)) &= \dim(J_L^x \cap L[Z_1, \ldots, Z_n]) = \dim\left(\left(J_L^x \cap L[Z_1, \ldots, Z_n]\right)_{\tilde{L}[Z_1,\ldots,Z_n]}\right) \\
&\geq \dim(J_L^x \cap \tilde{L}[Z_1, \ldots, Z_n]) \geq \dim(J_{\tilde{L}}^x \cap \tilde{L}[Z_1, \ldots, Z_n]) \\
&= \mathrm{trdeg}_{\tilde{L}}(K(x_1, \ldots, x_n)).
\end{aligned}$$

By the fact that $\mathrm{trdeg}_L(K(x_1, \ldots, x_n)) = \mathrm{trdeg}_{\tilde{L}}(K(x_1, \ldots, x_n))$, this implies that

$$\dim(J_L^x \cap \tilde{L}[Z_1, \ldots, Z_n]) = \dim(J_{\tilde{L}}^x \cap \tilde{L}[Z_1, \ldots, Z_n]). \tag{2.10}$$

Note that by Corollary 2.18, the ideal $J_{\tilde{L}}^x \cap \tilde{L}[Z_1, \ldots, Z_n]$ is prime. By assumption, the ideal J_L^x is also prime, thus the ideal $J_L^x \cap \tilde{L}[Z_1, \ldots, Z_n]$ is prime, too. Summarizing this, the ideal $J_L^x \cap \tilde{L}[Z_1, \ldots, Z_n]$ is prime, contained in the prime ideal $J_{\tilde{L}}^x \cap \tilde{L}[Z_1, \ldots, Z_n]$ and

has the same dimension as $J_{\tilde{L}}^{x} \cap \tilde{L}[Z_1, \ldots, Z_n]$. It follows from Proposition 2.14 that

$$J_L^x \cap \tilde{L}[Z_1, \ldots, Z_n] = J_{\tilde{L}}^{x} \cap \tilde{L}[Z_1, \ldots, Z_n].$$

Therefore, the ideal J_L^x is equal to the ideal $J_{\tilde{L}}^{x}$ (cf. Corollary 2.18) and by Lemma 2.26, we finally get $L = \tilde{L}$.

Conversely, assume that the field L is algebraically closed in $K(x_1, \ldots, x_n)$. Observe that the ideal $(x_1 - Z_1, \ldots, x_n - Z_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n]$ is prime. It hence follows by Proposition 2.37 that the ideal

$$J_L^x = \big((x_1 - Z_1, \ldots, x_n - Z_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} \cap L[Z_1, \ldots, Z_n]\big)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$$

(cf. Proposition 2.17) is prime, too. ∎

The previous proposition can easily be turned into an algorithm with methods of Gröbner basis theory, which allows to effectively check whether a given input for Algorithm 2.38 satisfies the required conditions.

Remarks. (a) It can be seen from the proof of the proposition that if the MQS ideal J_L^x is a prime ideal, then L is algebraically closed in the field $K(x_1, \ldots, x_n)$, independent of the characteristic of the field K.

(b) In characteristic zero, Proposition 2.42 gives rise to an algorithm for computing the algebraic closure $\tilde{L}$ of a field L in the field $K(x_1, \ldots, x_n)$. The MQS ideal $J_{\tilde{L}}^{x}$ is one of the minimal primes over J_L^x. An algorithm for the computation of the minimal primes over an ideal can be found in [BW93], Chapter 8, Section 7, Theorem 8.101.

2.5 Some Facts about MQS Ideals

In Section 2.2, we have already pointed out some properties of MQS ideals. In this section, we want to examine the following questions:

- When is an ideal an MQS ideal?
- What properties do MQS ideals have: Are they radical, prime?

It is obvious that not all ideals in $K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ are MQS ideals. By Proposition 2.17, we know that every MQS ideal is contained in the ideal $(Z_1 - x_1, \ldots, Z_n - x_n)_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$. Note that we can actually check algorithmically whether an ideal $J \trianglelefteq K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ is an MQS ideal or not. For, it follows from Proposition 2.21 that if J is an MQS ideal of $x_1, \ldots, x_n$ over some intermediate field of K and $K(x_1, \ldots, x_n)$, then it is the MQS ideal of $x_1, \ldots, x_n$ over the field generated by the coefficients of the elements of a reduced Gröbner basis of J (w. r. t. an arbitrary monomial order on $Z_1, \ldots, Z_n$).

As we have seen, there is not only an algorithm to compute a reduced Gröbner basis of J, but also to compute the MQS ideal of $x_1, \ldots, x_n$ over an intermediate field of K and $K(x_1, \ldots, x_n)$.

For further examinations of the MQS ideal J_L^x of $x_1, \ldots, x_n$ over an intermediate field L of K and $K(x_1, \ldots, x_n)$, recall from Proposition 2.17 that

$$J_L^x = ((Z_1 - x_1, \ldots, Z_n - x_n) \cap L[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}.$$

So the ideal $J_L^x \trianglelefteq K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ is the extension of a prime ideal in $L[Z_1, \ldots, Z_n]$ to $K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$.

The next lemma examines extensions of prime ideals in polynomial rings over a field of characteristic zero. Note that it is a generalization of Proposition 2.37. An alternative proof of this lemma can be found in [ZS75b], Chapter VII, § 11, Corollary, p. 226.

Lemma 2.43. *Let L' be a finitely generated field extension over a field K' of characteristic zero and let $Y_1, \ldots, Y_n$ be indeterminates over L'. If an ideal $\hat{I} \trianglelefteq K'[Y_1, \ldots, Y_n]$ is a prime ideal, then $I := (\hat{I})_{L'[Y_1,\ldots,Y_n]}$ is a radical ideal.*

Proof. Let $x_1, \ldots, x_r \in L'$ be a transcendence basis of the field L' over K'. By Proposition 2.37, the ideal $(\hat{I})_{K'(x_1,\ldots,x_r)[Y_1,\ldots,Y_n]}$ is prime. It is hence sufficient to prove the assertion for the case that $L'|K'$ is a finite field extension.
So assume that L' is a finite extension of the field K'. Since $\mathrm{char}(K') = 0$, the field extension $L'|K'$ is separable. Let Z be an indeterminate over K'. By the Primitive Element Theorem (e.g. see [Lan02], Chapter V, Theorem 4.6), it follows that there exists a (irreducible) separable polynomial $f(Z) \in K'[Z]$ such that $L' \cong K'[Z]/(f(Z))$. Then we have

$$\begin{aligned} L'[Y_1, \ldots, Y_n]/I &\cong L' \otimes_{K'} K'[Y_1, \ldots, Y_n]/\hat{I} \\ &\cong K'[Z]/(f(Z)) \otimes_{K'} K'[Y_1, \ldots, Y_n]/\hat{I} \\ &\subset K'[Z]/(f(Z)) \otimes_{K'} \mathrm{Quot}(K'[Y_1, \ldots, Y_n]/\hat{I}) \\ &\cong \mathrm{Quot}(K'[Y_1, \ldots, Y_n]/\hat{I})[Z]/(f(Z)). \end{aligned}$$

(cf. [ZS75a], Chapter III, Theorem 35). We show that $\mathrm{Quot}(K'[Y_1, \ldots, Y_n]/\hat{I})[Z]/(f(Z))$ does not have any nilpotent elements. Denote by $\hat{K'}$ the algebraic closure of the field $\mathrm{Quot}(K'[Y_1, \ldots, Y_n]/\hat{I})$. Since the polynomial $f(Z)$ is separable, the ideal $(f(Z))_{\hat{K'}[Z]}$ is a radical ideal (cf. [CLO07], Chapter 4, § 2, Proposition 9). It follows that the ideal $(f(Z))_{\mathrm{Quot}(K'[Y_1,\ldots,Y_n]/\hat{I})[Z]}$, which is equal to $(f(Z))_{\hat{K'}[Z]} \cap \mathrm{Quot}(K'[Y_1, \ldots, Y_n]/\hat{I})[Z]$, is radical, too. This implies that $\mathrm{Quot}(K'[Y_1, \ldots, Y_n]/\hat{I})[Z]/(f(Z))$ does not have any nilpotent elements, thus the same is true for $L'[Y_1, \ldots, Y_n]/I$. This shows that I is radical. ∎

By the lemma, it follows that in characteristic zero all MQS ideals $J_L^{\underline{x}}$, $K \leq L \leq K(x_1, \ldots, x_n)$ are radical ideals which are contained in the ideal $(Z_1 - x_1, \ldots, Z_n - x_n)$. Moreover by Proposition 2.37, the ideal $J_L^{\underline{x}}$ is prime if and only if the field L is algebraically closed in $K(x_1, \ldots, x_n)$. Note that by the next example not all radical ideals contained in $(Z_1 - x_1, \ldots, Z_n - x_n) \trianglelefteq K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ are of the 'MQS type'.

Example 2.44. Let X_1, X_2 be indeterminates over $\mathbb{Q}$ and let Z_1, Z_2 be indeterminates over $\mathbb{Q}(X_1, X_2)$. Let

$$I := (Z_1X_2 - Z_2X_1 + 2Z_1Z_2 - 2X_1X_2) \trianglelefteq \mathbb{Q}(X_1, X_2)[Z_1, Z_2].$$

Clearly, the ideal I is contained in $(Z_1 - X_1, Z_2 - X_2) \trianglelefteq \mathbb{Q}(X_1, X_2)[Z_1, Z_2]$. Furthermore, it is not hard to see that the polynomial $Z_1X_2 - Z_2X_1 + 2Z_1Z_2 - 2X_1X_2 \in \mathbb{Q}(X_1, X_2)[Z_1, Z_2]$ is irreducible. It follows that the ideal I is prime, so in particular, I is a radical ideal. Note that the reduced Gröbner basis of I with respect to any monomial order is given by $\{Z_1Z_2 + 1/2 \cdot Z_1X_2 - 1/2 \cdot Z_2X_1 - X_1X_2\}$. It follows by Proposition 2.24 that if I was an MQS ideal of X_1, X_2 over some field L, then it would be equal to $J^{X_1,X_2}_{\mathbb{Q}(X_1,X_2)} = (Z_1 - X_1, Z_2 - X_2)$, which certainly is not the case. ◁

If the characteristic of K is not equal to zero, then the ideal $J_L^{\underline{x}}$ is not necessarily radical, as the following example shows.

Example 2.45. Let K be a field of characteristic 2 and let X_1 be an indeterminate over K. Let $L := K(X_1^2)$, an intermediate field of K and $K(X_1)$. The MQS ideal of X_1 over L is given by

$$J_L^{X_1} = (Z_1^2 - X_1^2) \trianglelefteq K(X_1)[Z_1],$$

which is obviously not radical. ◁

2.6 Simple Field Extensions

A field extension $L|K$ is called **simple** if there exists $l \in L$ such that $L = K(l)$. We then also say that the field L is simple over K. Simple field extensions occur in various parts of mathematics, e. g. a variety of examples can be found in the context of algebraic curves: The function field of an algebraic curve which has a parametrization is simple over K ([Sha94], Chapter I, Section 1.3). In fact, it can be shown that the converse is also true. Essentially, this equivalence is based on the Theorem of Lüroth, which says that each intermediate field of K and a transcendental field extension of K of degree one is simple over K.

In this section we will characterize the notion of simplicity of intermediate fields of K and $K(x_1, \ldots, x_n)$ over K by means of MQS ideals in the case that $x_1, \ldots, x_n$ are algebraically independent over K. Müller-Quade and Steinwandt discussed such a characterization in [MQS00b]. Our investigation will follow a different approach and will finally lead to a

new proof of a generalized version of Lüroth's Theorem[‡]. Moreover, we will provide an algorithm for testing simplicity of field extensions and – if applicable – finding a generating element.

For the remainder of this section, let $x_1, \ldots, x_n$ be algebraically independent over K.

Proposition 2.46. *Let K, $K(x_1, \ldots, x_n)$ and L be as in Notation 2.1. Then $J_L^{\underline{x}}$ is a nonzero principal ideal if and only if the field L has transcendental degree 1 over K.*

Proof. Let $Z_1, \ldots, Z_n$ be indeterminates over $K(x_1, \ldots, x_n)$. Recall from Proposition 2.23 that

$$\dim(J_L^{\underline{x}}) = \dim(J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n]) = \operatorname{trdeg}_L(K(x_1, \ldots, x_n)). \tag{2.11}$$

Suppose first that the MQS ideal $J_L^{\underline{x}} \trianglelefteq K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ is a nonzero principal ideal. We claim that $\dim(J_L^{\underline{x}}) = n - 1$. Clearly, the dimension of the ideal $J_L^{\underline{x}} \neq (0)$ is less than n. On the other hand, there exists a monomial $\underline{Z}^\alpha$ with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \setminus \{(0, \ldots, 0)\}$, that means $\alpha_i \neq 0$ for some $i \in \{1, \ldots, n\}$, which is involved in the generator of the principal ideal $J_L^{\underline{x}}$. Hence $J_L^{\underline{x}} \cap K(x_1, \ldots, x_n)[Z_1, \ldots, Z_{i-1}, Z_{i+1}, \ldots, Z_n]$ is equal to zero. It follows that the dimension of the ideal $J_L^{\underline{x}}$ is at least $n - 1$. This shows that actually

$$n - 1 = \dim(J_L^{\underline{x}}) = \operatorname{trdeg}_L(K(x_1, \ldots, x_n)),$$

as claimed. Since the elements $x_1, \ldots, x_n$ are algebraically independent over K, the transcendental degree of $K(x_1, \ldots, x_n)$ over K is equal to n, and therefore,

$$\operatorname{trdeg}_K(L) = \operatorname{trdeg}_K(K(x_1, \ldots, x_n)) - \operatorname{trdeg}_L(K(x_1, \ldots, x_n)) = n - (n - 1) = 1.$$

Conversely, suppose that the transcendental degree of the field L over K is equal to 1. By equation (2.11), it follows that

$$\begin{aligned} \dim(J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n]) &= \operatorname{trdeg}_L(K(x_1, \ldots, x_n)) \\ &= \operatorname{trdeg}_K(K(x_1, \ldots, x_n)) - \operatorname{trdeg}_K(L) \\ &= n - 1. \end{aligned} \tag{2.12}$$

Since $J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n] = (Z_1 - x_1, \ldots, Z_n - x_n) \cap L[Z_1, \ldots, Z_n]$ (cf. Proposition 2.18) is a nonzero prime ideal, it contains a nonzero, irreducible polynomial $p(\underline{Z})$. It follows that the ideal $J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n]$ contains the nonzero prime ideal $(p(\underline{Z}))_{L[Z_1, \ldots, Z_n]}$. Assume for a contradiction that the ideal $(p(\underline{Z}))_{L[Z_1, \ldots, Z_n]}$ is not equal to $J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n]$. Then it follows from Proposition 2.14 that

$$\dim((p(\underline{Z}))_{L[Z_1, \ldots, Z_n]}) \geq \dim(J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n]) + 1 = n,$$

[‡]The generalized version of the Theorem of Lüroth seems to have first appeared in [Igu51].

which implies that $p(\underline{Z}) = 0$. This is obviously a contradiction. So in fact,

$$J_L^{\underline{x}} = (J_L^{\underline{x}} \cap L[Z_1, \ldots, Z_n])_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]} = (p(\underline{Z}))_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]},$$

i. e. $J_L^{\underline{x}}$ is a principal ideal. ∎

In the following, we aim to show that the ideal $J_L^{\underline{x}}$ is principal if and only if L is simple over K. We start with a lemma.

Lemma 2.47. *Let K, $K(x_1, \ldots, x_n)$ and $Z_1, \ldots, Z_n$ be as in Notation 2.1. Moreover, let $g(\underline{Z}), h(\underline{Z}) \in K[Z_1, \ldots, Z_n]$ be non-constant, coprime polynomials. Then the polynomial*

$$h(\underline{x}) \cdot g(\underline{Z}) - g(\underline{x}) \cdot h(\underline{Z}) \in K[x_1, \ldots, x_n][Z_1, \ldots, Z_n]$$

is primitive as a polynomial in $Z_1, \ldots, Z_n$.

Proof. Let $p(\underline{x}) \in K[x_1, \ldots, x_n]$ such that

$$p(\underline{x}) \cdot q(\underline{Z}) = h(\underline{x}) \cdot g(\underline{Z}) - g(\underline{x}) \cdot h(\underline{Z}) \tag{2.13}$$

for some polynomial $q(\underline{Z}) \in K[x_1, \ldots, x_n][Z_1, \ldots, Z_n]$. We aim to show that the element $p(\underline{x}) \in K[x_1, \ldots, x_n]$ is constant, i. e. $p(\underline{x}) \in K$. First, we show that $p(\underline{x})$ is a divisor of $g(\underline{x})$. Denote the coefficient of the monomial $\underline{Z}^\alpha$, $\alpha \in \mathbb{N}^n$ in the polynomial $g(\underline{Z}) \in K[Z_1, \ldots, Z_n]$ by c_α and its coefficient in the polynomial $h(\underline{Z}) \in K[Z_1, \ldots, Z_n]$ by d_α. Then clearly, $p(\underline{x})$ is a divisor of $c_\alpha h(\underline{x}) - d_\alpha g(\underline{x})$ for all $\alpha \in \mathbb{N}^n$. It follows that

$$p(\underline{x}) \mid \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha (c_\alpha h(\underline{x}) - d_\alpha g(\underline{x}))$$

for all choices of $\lambda_\alpha \in K$ for $\alpha \in \mathbb{N}^n$. Since $g(\underline{Z})$ is a non-constant polynomial, there exists $\alpha \in \mathbb{N}^n$ such that $c_\alpha \neq 0$. By the above, it follows that $p(\underline{x})$ is a divisor of

$$\frac{c_\beta}{c_\alpha} \cdot (c_\alpha h(\underline{x}) - d_\alpha g(\underline{x})) - (c_\beta h(\underline{x}) - d_\beta g(\underline{x})) = \left(\frac{c_\beta}{c_\alpha} \cdot d_\alpha + d_\beta \right) g(\underline{x}) \tag{2.14}$$

for all $\beta \in \mathbb{N}^n$. We claim that there exists $\beta \in \mathbb{N}^n$ such that $((c_\beta/c_\alpha) \cdot d_\alpha + d_\beta) \neq 0 \in K$. Since $h(\underline{Z})$ is a non-constant polynomial, the claim is certainly true if $d_\alpha = 0$. In case that $d_\alpha \neq 0$, assume for a contradiction that $((c_\beta/c_\alpha) \cdot d_\alpha + d_\beta) = 0$ for all $\beta \in \mathbb{N}^n$. Then we have the equality

$$h(\underline{Z}) = \sum_{\beta \in \mathbb{N}^n} d_\beta \cdot \underline{Z}^\beta = - \sum_{\beta \in \mathbb{N}^n} \frac{d_\alpha}{c_\alpha} \cdot c_\beta \underline{Z}^\beta = - \frac{d_\alpha}{c_\alpha} \cdot g(\underline{Z}).$$

By the coprimacy of the polynomial $g(\underline{Z})$ and $h(\underline{Z})$, this is obviously a contradiction.
So there exists $\beta \in \mathbb{N}^n$ such that $((c_\beta/c_\alpha) \cdot d_\alpha + d_\beta) \neq 0 \in K$. It follows that $p(\underline{x})$ is a divisor of $g(\underline{x})$ (cf. (2.14)).
Multiplying equation(2.13) by (-1), the same argumentation shows that $p(\underline{x})$ is also a

divisor of $h(\underline{x})$. Since $g(\underline{x})$ and $h(\underline{x})$ are coprime, it follows that $p(\underline{x})$ is actually constant. This shows that the polynomial $h(\underline{x}) \cdot g(\underline{Z}) - g(\underline{x}) \cdot h(\underline{Z})$ is primitive, indeed. ∎

Theorem 2.48. *Let K, $K(x_1, \ldots, x_n)$, L and $Z_1, \ldots, Z_n$ be as in Notation 2.1. Then $J_L^{\underline{x}}$ is a principal ideal if and only if L is simple over K.*
Moreover, in case that L is simple over K, the form of the reduced Gröbner basis $\mathcal{G}$ of $J_L^{\underline{x}}$ (for some fixed monomial order) can be described explicitly. Namely, there exists a generator $f(\underline{x}) = g(\underline{x})/h(\underline{x}) \in K(x_1, \ldots, x_n)$ of the field L over K – where we may assume that $g(\underline{x})$ and $h(\underline{x})$ are coprime polynomials in $K[x_1, \ldots, x_n]$ – such that $\mathcal{G}$ is given by

$$\mathcal{G} = \{g(\underline{Z}) - f(\underline{x}) \cdot h(\underline{Z})\}.$$

Proof. By assumption, the elements $x_1, \ldots, x_n$ are algebraically independent over K, that means

$$J_K^{\underline{x}} = (0) \trianglelefteq K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n].$$

So the theorem is correct in the case $L = K$. Assume now that $L \neq K$.
Suppose first that L is a simple field extension over K, i. e. $L = K(f(\underline{x}))$ for some $f(\underline{x}) \in K(x_1, \ldots, x_n) \setminus \{0\}$. Since $x_1, \ldots, x_n$ are algebraically independent over K, the element $f(\underline{x})$ is transcendental over K, hence

$$\operatorname{trdeg}_K(L) = 1.$$

By Lemma 2.46, this implies that the ideal $J_L^{\underline{x}}$ is principal.
Conversely, suppose that $J_L^{\underline{x}} \trianglelefteq K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ is a principal ideal. Let $\leq$ be a monomial order on $Z_1, \ldots, Z_n$ and let the reduced Gröbner basis $\mathcal{G}$ of $J_L^{\underline{x}}$ with respect to $\leq$ be given by

$$\mathcal{G} = \left\{ \underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{g_\gamma(\underline{x})}{h_\gamma(\underline{x})} \cdot \underline{Z}^{\gamma} \right\}$$

for some $\alpha \in \mathbb{N}^n$ and coprime polynomials $g_\gamma(\underline{Z})$, $h_\gamma(\underline{Z}) \in K[Z_1, \ldots, Z_n]$ for all $\gamma \in \mathbb{N}^n$ with $\underline{Z}^{\gamma} < \underline{Z}^{\alpha}$. By Proposition 2.24, the field L is generated over K by the coefficients of the elements in $\mathcal{G}$. Therefore, there exists a multi-index $\beta \in \mathbb{N}^n$ with $\underline{Z}^{\beta} < \underline{Z}^{\alpha}$ such that $g_\beta(\underline{x})/h_\beta(\underline{x}) \in L \setminus K$. We claim that $L = K(g_\beta(\underline{x})/h_\beta(\underline{x}))$. By definition of the MQS ideal $J_L^{\underline{x}}$, we clearly have

$$g_\beta(\underline{Z}) - \frac{g_\beta(\underline{x})}{h_\beta(\underline{x})} \cdot h_\beta(\underline{Z}) \in J_L^{\underline{x}}.$$

So let $p(\underline{Z}) \in K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$ such that

$$p(\underline{Z}) \cdot \left(\underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{g_\gamma(\underline{x})}{h_\gamma(\underline{x})} \cdot \underline{Z}^{\gamma} \right) = g_\beta(\underline{Z}) - \frac{g_\beta(\underline{x})}{h_\beta(\underline{x})} \cdot h_\beta(\underline{Z}). \tag{2.15}$$

We aim to show that $p(\underline{Z})$ actually lies in $K(x_1, \ldots, x_n)$. Let $h(\underline{x}) \in K[x_1, \ldots, x_n]$ be the least common multiple of the elements $h_\gamma(\underline{x})$, $\gamma \in \mathbb{N}^n$, $\underline{Z}^{\gamma} < \underline{Z}^{\alpha}$ and let $h'(\underline{x}) \in$

$K[x_1, \ldots, x_n]$ such that

$$h'(\underline{x}) \cdot p(\underline{Z}) \in K[x_1, \ldots, x_n][Z_1, \ldots, Z_n].$$

Multiplying equation (2.15) with $h'(\underline{x})h(\underline{x})$ hence gives

$$\begin{aligned} h'(\underline{x}) \cdot p(\underline{Z}) \cdot \left(h(\underline{x}) \cdot \underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{h(\underline{x}) g_{\gamma}(\underline{x})}{h_{\gamma}(\underline{x})} \cdot \underline{Z}^{\gamma} \right) \\ = \frac{h'(\underline{x})h(\underline{x})}{h_{\beta}(\underline{x})} \cdot (h_{\beta}(\underline{x}) \cdot g_{\beta}(\underline{Z}) - g_{\beta}(\underline{x}) \cdot h_{\beta}(\underline{Z})), \end{aligned} \tag{2.16}$$

an equality of polynomials in $K[x_1, \ldots, x_n][Z_1, \ldots, Z_n]$. Recall that the polynomials $g_{\gamma}(\underline{Z})$, $h_{\gamma}(\underline{Z}) \in K[Z_1, \ldots, Z_n]$ are coprime for all $\gamma \in \mathbb{N}^n$ with $\underline{Z}^{\gamma} < \underline{Z}^{\alpha}$ and that $h(\underline{x})$ is the least common multiple of the elements $h_{\gamma}(\underline{x})$, $\gamma \in \mathbb{N}^n, \underline{Z}^{\gamma} < \underline{Z}^{\alpha}$. Having this in mind, it is not hard to see that the polynomial

$$h(\underline{x}) \cdot \underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{h(\underline{x}) g_{\gamma}(\underline{x})}{h_{\gamma}(\underline{x})} \cdot \underline{Z}^{\gamma} \in K[x_1, \ldots, x_n][Z_1, \ldots, Z_n]$$

is primitive. It follows that the polynomial $h'(\underline{x})h(\underline{x})/h_{\beta}(\underline{x}) \in K[x_1, \ldots, x_n]$ is a divisor of the polynomial $h'(\underline{x}) \cdot p(\underline{Z}) \in K[x_1, \ldots, x_n][Z_1, \ldots, Z_n]$ and hence that

$$\frac{h_{\beta}(\underline{x})}{h(\underline{x})} \cdot p(\underline{Z}) = \frac{h_{\beta}(\underline{x})}{h'(\underline{x})h(\underline{x})} \cdot (h'(\underline{x}) \cdot p(\underline{Z})) \in K[x_1, \ldots, x_n][Z_1, \ldots, Z_n].$$

In the following, we regard $x_1, \ldots, x_n$ as indeterminates over K. Let $\leq'$ be a monomial order on $x_1, \ldots, x_n$. Note that we have the following equation of polynomials

$$\left(\frac{h_{\beta}(\underline{x})}{h(\underline{x})} \cdot p(\underline{Z}) \right) \cdot \left(h(\underline{x}) \cdot \underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{h(\underline{x}) g_{\gamma}(\underline{x})}{h_{\gamma}(\underline{x})} \cdot \underline{Z}^{\gamma} \right) = (h_{\beta}(\underline{x}) \cdot g_{\beta}(\underline{Z}) - g_{\beta}(\underline{x}) \cdot h_{\beta}(\underline{Z})) \tag{2.17}$$

(cf. equation (2.16)). By Remark 2.6, it is not hard to see that

$$\begin{aligned} &\mathrm{LM}_{\leq'} \left(h(\underline{x}) \cdot \underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{h(\underline{x}) \cdot g_{\gamma}(\underline{x})}{h_{\gamma}(\underline{x})} \cdot \underline{Z}^{\gamma} \right) \\ &\quad \leq' \mathrm{LM}_{\leq'} \left(\frac{h_{\beta}(\underline{x})}{h(\underline{x})} \cdot p(\underline{Z}) \right) \cdot \mathrm{LM}_{\leq'} \left(h(\underline{x}) \cdot \underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{h(\underline{x}) \cdot g_{\gamma}(\underline{x})}{h_{\gamma}(\underline{x})} \cdot \underline{Z}^{\gamma} \right) \\ &\quad = \mathrm{LM}_{\leq'} (h_{\beta}(\underline{x}) \cdot g_{\beta}(\underline{Z}) - g_{\beta}(\underline{x}) \cdot h_{\beta}(\underline{Z})), \end{aligned}$$

and on the other hand that

$$\begin{aligned} &\mathrm{LM}_{\leq'} (h_{\beta}(\underline{x}) \cdot g_{\beta}(\underline{Z}) - g_{\beta}(\underline{x}) \cdot h_{\beta}(\underline{Z})) \\ &\quad \leq' \max_{\leq'} \{ \mathrm{LM}_{\leq'} (h_{\beta}(\underline{x})),\ \mathrm{LM}_{\leq'} (g_{\beta}(\underline{x})) \} \\ &\quad \leq' \max_{\leq'} \{ \mathrm{LM}_{\leq'} (h(\underline{x})),\ \mathrm{LM}_{\leq'} \left(\frac{h(\underline{x}) \cdot g_{\gamma}(\underline{x})}{h_{\gamma}(\underline{x})} \right);\ \gamma \in \mathbb{N}^n, \underline{Z}^{\gamma} < \underline{Z}^{\alpha} \} \end{aligned}$$

$$= \mathrm{LM}_{\leq'}\left(h(\underline{x}) \cdot \underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{h(\underline{x}) \cdot g_{\gamma}(\underline{x})}{h_{\gamma}(\underline{x})} \cdot \underline{Z}^{\gamma}\right).$$

It follows that there is equality everywhere and in particular that

$$\mathrm{LM}_{\leq'}\left(\frac{h_{\beta}(\underline{x})}{h(\underline{x})} \cdot p(\underline{Z})\right) = 1,$$

meaning that $h_{\beta}(\underline{x})/h(\underline{x}) \cdot p(\underline{Z})$ is a polynomial in $K[Z_1, \ldots, Z_n]$.
Note that by symmetry, the polynomial $h_{\beta}(\underline{x}) \cdot g_{\beta}(\underline{Z}) - g_{\beta}(\underline{x}) \cdot h_{\beta}(\underline{Z})$ is also primitive as a polynomial in $x_1, \ldots, x_n$ (cf. Lemma 2.47). It hence follows from equation (2.17) that actually

$$\frac{h_{\beta}(\underline{x})}{h(\underline{x})} \cdot p(\underline{Z}) \in K.$$

This shows that $p(\underline{Z})$ lies in $K(x_1, \ldots, x_n)$, indeed. By equation (2.15), this implies

$$J_L^{\underline{x}} = \left(g_{\beta}(\underline{Z}) - \frac{g_{\beta}(\underline{x})}{h_{\beta}(\underline{x})} \cdot h_{\beta}(\underline{x})\right).$$

Since the computation of the reduced Gröbner basis with the Buchberger algorithm does not extend the field of coefficients (cf. [Buc65]), it follows that

$$\underline{Z}^{\alpha} + \sum_{\underline{Z}^{\gamma} < \underline{Z}^{\alpha}} \frac{g_{\gamma}(\underline{x})}{h_{\gamma}(\underline{x})} \cdot \underline{Z}^{\gamma} \in K\left(g_{\beta}(\underline{x})/h_{\beta}(\underline{x})\right)[Z_1, \ldots, Z_n],$$

and an application of Proposition 2.24 shows that L is generated by $g_{\beta}(\underline{x})/h_{\beta}(\underline{x})$ over K. In particular, L is simple over K, as asserted.

For the second assertion about the special form of the Gröbner basis $\mathcal{G}$ of $J_L^{\underline{x}}$ assume that $L \neq K$ is simple over K. By the above, there exist coprime polynomials $g(\underline{x})$ and $h(\underline{x}) \in K[x_1, \ldots, x_n]$ such that $L = K(g(\underline{x})/h(\underline{x}))$ and $J_L^{\underline{x}} = (g(\underline{Z}) - g(\underline{x})/h(\underline{x}) \cdot h(\underline{Z}))$.

Case $\mathrm{LM}_{\leq}(h(\underline{Z})) < \mathrm{LM}_{\leq}(g(\underline{Z}))$. By assumption, we have $\mathrm{LM}_{\leq}(h(\underline{Z})) < \mathrm{LM}_{\leq}(g(\underline{Z}))$. So the reduced Gröbner basis of $J_L^{\underline{x}}$ is given by

$$\left\{\frac{1}{\mathrm{LC}_{\leq}(g(\underline{Z}))} g(\underline{Z}) - \frac{(1/\mathrm{LC}_{\leq}(g(\underline{Z})))g(\underline{x})}{h(\underline{x})} \cdot h(\underline{Z})\right\}.$$

Obviously, L is generated by $(1/\mathrm{LC}_{\leq}(g(\underline{Z})))g(\underline{x})/h(\underline{x})$ over K.

Case $\mathrm{LM}_{\leq}(g(\underline{Z})) = \mathrm{LM}_{\leq}(h(\underline{Z}))$. Denote the leading monomial of $g(\underline{Z})$ and $h(\underline{Z})$ by Z^{α} with $\alpha \in \mathbb{N}^n$ and denote the leading coefficients of $g(\underline{Z})$ and $h(\underline{Z})$ by c_{α} and d_{α}. Observe that since $g(\underline{x})$ and $h(\underline{x})$ are coprime, the element $c_{\alpha} - d_{\alpha} g(\underline{x})/h(\underline{x})$ is certainly nonzero. The reduced Gröbner basis of $J_L^{\underline{x}}$ is hence given by

$$\left\{\frac{1}{c_{\alpha} - d_{\alpha} g(\underline{x})/h(\underline{x})} \cdot \left(g(\underline{Z}) - \frac{g(\underline{x})}{h(\underline{x})} \cdot h(\underline{Z})\right)\right\}$$

It is a straightforward verification that this is equal to

$$\left\{ \frac{1}{c_\alpha} g(\underline{Z}) - \frac{(1/c_\alpha) g(\underline{x})}{c_\alpha h(\underline{x}) - d_\alpha g(\underline{x})} \cdot (c_\alpha h(\underline{Z}) - d_\alpha g(\underline{Z})) \right\}.$$

Note that for all $c, d \in K$, $c \neq 0$ we have the equality

$$K\left(\frac{h(\underline{x})}{g(\underline{x})}\right) = K\left(\frac{1}{c}\left(\frac{h(\underline{x})}{g(\underline{x})} - d\right)^{-1}\right).$$

So in particular, we have

$$K\left(\frac{h(\underline{x})}{g(\underline{x})}\right) = K\left(\frac{1}{c_\alpha}\left(\frac{h(\underline{x})}{g(\underline{x})} - \frac{d_\alpha}{c_\alpha}\right)^{-1}\right) = K\left(\frac{g(\underline{x})}{c_\alpha h(\underline{x}) - d_\alpha g(\underline{x})}\right).$$

Case $\mathrm{LM}_{\leq}(g(\underline{Z})) < \mathrm{LM}_{\leq}(h(\underline{Z}))$. It is not hard to see that the reduced Gröbner basis of $J_L^{\underline{x}}$ is given by

$$\left\{ \frac{1}{\mathrm{LC}_{\leq}(h(\underline{Z}))} h(\underline{Z}) - \frac{(1/\mathrm{LC}_{\leq}(h(\underline{Z})))h(\underline{x})}{g(\underline{x})} \cdot g(\underline{Z}) \right\}.$$

Furthermore, we clearly have the equality

$$K\left(\frac{(1/\mathrm{LC}_{\leq}(h(\underline{Z})))h(\underline{x})}{g(\underline{x})}\right) = K\left(\frac{g(\underline{x})}{h(\underline{x})}\right).$$

In all these cases, the Gröbner basis is of the desired form. This finishes the proof. ∎

The following example shows that the theorem is not true for arbitrary field extensions – more precisely, the condition that the elements $x_1, \ldots, x_n$ are algebraically independent over K can not be omitted.

Example 2.49. Let $\mathbb{Q}(x_1, x_2)$ be a field extension over $\mathbb{Q}$ with the relations of x_1 and x_2 over $\mathbb{Q}$ being given by

$$x_1 = x_2.$$

Then by Proposition 2.21, the MQS ideal of x_1, x_2 over the field $\mathbb{Q}(x_1)$ is equal to

$$J_{\mathbb{Q}(x_1)}^{x_1,x_2} = (Z_1 - x_1, Z_1 - Z_2) \trianglelefteq \mathbb{Q}(x_1, x_2)[Z_1, Z_2],$$

which is clearly a zero-dimensional ideal. By the definition of the dimension of an ideal (cf. Definition 2.13), it follows that the MQS ideal of x_1, x_2 over the field $\mathbb{Q}(x_1)$ is not principal. ◁

Theorem 2.50 (Lüroth). *Let K, $K(x_1, \ldots, x_n)$ and L be as in Notation 2.1. If the transcendental degree of L over K is equal to 1, then L is simple over K.*

Proof. The theorem follows by combining Lemma 2.46 and Theorem 2.48. ∎

Theorem 2.48 together with its proof can also be used for algorithmic purposes. We get an algorithm for deciding whether a given field extension over K is simple or not.

Algorithm 2.51. (Testing whether a field extension is simple)

Input: An intermediate field L of K and a finitely generated field extension $K(x_1, \ldots, x_n)$, where $x_1, \ldots, x_n$ are algebraically independent elements over K. More precisely, these data shall be given in the following form: polynomials $g_1(\underline{x}), \ldots, g_m(\underline{x}) \in K[x_1, \ldots, x_n]$ and polynomials $h_1(\underline{x}), \ldots, h_m(\underline{x}) \in K[x_1, \ldots, x_n] \setminus \{0\}$ such that the field L is equal to $K(g_1(\underline{x})/h_1(\underline{x}), \ldots, g_m(\underline{x})/h_m(\underline{x}))$.

Output: FALSE, if L is not simple over K. Otherwise (TRUE, $f(\underline{x})$), where $f(\underline{x})$ is some generating element of L over K.

(1) Compute the MQS ideal of $x_1, \ldots, x_n$ over L, i. e. compute

$$J_L^{\underline{x}} = \left(g_1(\underline{Z}) - \frac{g_1(\underline{x})}{h_1(\underline{x})} h_1(\underline{Z}), \ldots, g_m(\underline{Z}) - \frac{g_m(\underline{x})}{h_m(\underline{x})} h_m(\underline{Z})) : \left(\prod_{i=1}^{m} h_i(\underline{Z}) \right)^{\infty} \right)$$
$$\trianglelefteq K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n].$$

(2) Compute the reduced Gröbner basis $\mathcal{G}$ of $J_L^{\underline{x}}$ with respect to an arbitrary monomial order $\leq$ on $Z_1, \ldots, Z_n$.

(3) If $|\mathcal{G}| \neq 1$ return FALSE.
Else if $\mathcal{G} = \{0\}$ return (TRUE, 0).
Else return (TRUE, $f(\underline{x})$), where $f(\underline{x})$ is some non-constant coefficient of the polynomial $g \in \mathcal{G}$.

Proof of Correctness. By Theorem 2.48, the field L is simple over K if and only if the ideal $J_L^{\underline{x}}$ is principal. As the ideal $J_L^{\underline{x}}$ is principal if and only if its reduced Gröbner basis has exactly one element, the algorithm is certainly correct if the field extension $L|K$ is not simple.
Now let L be simple over K. Since L is equal to K if and only if the MQS ideal $J_L^{\underline{x}}$ is equal to zero, i. e. $\mathcal{G} = \{0\}$, the algorithm is correct in that case, too. If $L \neq K$, then there exist coprime polynomials $g(\underline{x})$, $h(\underline{x}) \in K[x_1, \ldots, x_n] \setminus \{0\}$ such that

$$\mathcal{G} = \left\{ g(\underline{Z}) - \frac{g(\underline{x})}{h(\underline{x})} \cdot h(\underline{Z}) \right\}$$

and $L = K(g(\underline{x})/h(\underline{x}))$ (cf. Theorem 2.48). By Proposition 2.24 – since L was assumed not to be equal to K – there exists a non-constant coefficient $f(\underline{x}) \in K(x_1, \ldots, x_n)$ in the

polynomial $g(\underline{Z}) - g(\underline{x})/h(\underline{x}) \cdot h(\underline{Z}) \in K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$, say

$$f(\underline{x}) = c + d \cdot \frac{g(\underline{x})}{h(\underline{x})}$$

for some $c, d \in K$, $d \neq 0$. Now observe that

$$K(f(\underline{x})) = K\left(c + d \cdot \frac{g(\underline{x})}{h(\underline{x})}\right) = K\left(d \cdot \frac{g(\underline{x})}{h(\underline{x})}\right) = K\left(\frac{g(\underline{x})}{h(\underline{x})}\right) = L.$$

So indeed, $f(\underline{x})$ generates the field L over K. This proves the correctness of the algorithm.■

Example 2.52. We want to apply Algorithm 2.51 to an example from the theory of plane algebraic curves[§].
Let X_1, X_2 be indeterminates over $\overline{\mathbb{Q}}$, the algebraic closure of the field $\mathbb{Q}$. Let X be the plane algebraic curve defined by the polynomial $p(X_1, X_2) = X_1^2 X_2 + X_1 - 1 \in \overline{\mathbb{Q}}[X_1, X_2]$, i. e.

$$X := \{(\xi_1, \xi_2) \in \overline{\mathbb{Q}}^2;\ \xi_1^2 \xi_2 + \xi_1 - 1 = 0\}.$$

Let $I := (p(X_1, X_2)) \trianglelefteq \overline{\mathbb{Q}}[X_1, X_2]$. We will show that the function field $\overline{\mathbb{Q}}(X)$, which is equal to $\mathrm{Quot}(\overline{\mathbb{Q}}[X_1, X_2]/I)$, is a simple field extension over $\overline{\mathbb{Q}}$.
Let T be an indeterminate over $\overline{\mathbb{Q}}$. It can be verified that the ideal of relations of the elements

$$\phi_1 := \frac{T^2}{T^2 + T + 1},\ \phi_2 := \frac{T^3 + 2T^2 + 2T + 1}{T^4} \in \overline{\mathbb{Q}}(T)$$

over $\overline{\mathbb{Q}}$ is given by the ideal I. (Note that this means that ϕ_1 and ϕ_2 actually define a parametrization of the algebraic curve X.) We get an isomorphism of fields

$$\mathrm{Quot}(\overline{\mathbb{Q}}[X_1, X_2]/I) \cong \overline{\mathbb{Q}}(\phi_1, \phi_2) \leq \overline{\mathbb{Q}}(T).$$

By the Theorem of Lüroth it follows that the function field $\overline{\mathbb{Q}}(X) = \mathrm{Quot}(\overline{\mathbb{Q}}[X_1, X_2]/I)$ is simple over $\overline{\mathbb{Q}}$. In fact, using Algorithm 2.51 it can be verified that

$$J^T_{\overline{\mathbb{Q}}(\phi_1, \phi_2)} = \left(Z^2 - \frac{T^2}{T+1} \cdot (Z+1)\right) \trianglelefteq \overline{\mathbb{Q}}(T)[Z],$$

where Z is an indeterminate over $K(T)$. So we get

$$\overline{\mathbb{Q}}\left(\frac{T^2}{T^2 + T + 1}, \frac{T^3 + 2T^2 + 2T + 1}{T^4}\right) = \overline{\mathbb{Q}}\left(\frac{T^2}{T+1}\right).$$

For finding a generating element of $\overline{\mathbb{Q}}(X)$ over $\overline{\mathbb{Q}}$ we need to find a representation of $T^2/(T+1)$ in the elements $T^2/(T^2+T+1), (T^3+2T^2+2T+1)/T^4$. An algorithm for

[§]An introduction to algebraic geometry can be found in Section 3.1.

this problem has been developed in [MQS99]. An application of this algorithm yields

$$\frac{T^2}{T+1} = \frac{T^2/(T^2+T+1)\cdot(T^3+2T^2+2T+1)/T^4+1}{(T^3+2T^2+2T+1)/T^4)}.$$

It follows that

$$\mathrm{Quot}(\overline{\mathbb{Q}}[X_1,X_2]/I) = \overline{\mathbb{Q}}\left(\frac{(X_1X_2+1)+I}{X_2+I}\right). \qquad \triangleleft$$

3 A Survey on Cross-Sections of Rational Maps

One of the central problems of invariant theory is the determination of the invariant ring or the invariant field of an algebraic group acting on a finite dimensional K-vector space X or – more generally – on a variety X over a field K. Whereas it is common to describe the invariant ring and the invariant field of a group action in the form of generators together with their relations – i. e. in an algebraic way – a more geometric approach is often used to actually find generating sets.
In this context, the notion of a so-called cross-section of a rational quotient of the action comes into the picture. Roughly speaking, it is a subvariety S of the variety X such that it has exactly one point in common with the orbit of each point contained in some nonempty open subset of S and the image of S under the group action is a dense subset of the variety X. It is a model for the field of invariant rational functions, i. e. its function field is isomorphic to the invariant field.
The content of this chapter is the examination of the notion of a cross-section of a rational map – a generalization of the idea of cross-sections in invariant theory. As we will see, we will gain a very useful tool, not only for problems in invariant theory, but also for algorithmic purposes in field theory.
In the literature, cross-sections of rational maps in general and cross-sections in invariant theory in special seem to be quite rare. In 1992, Popov gave a survey on cross-sections in invariant theory (cf. [Pop94]). Moreover, with the theory of moving frames [FO01], Olver and Fels made some contributions to the analytic analogue of the problem, i. e. to the case where a Lie transformation group acts analytically on a manifold. Based on these ideas, Hubert and Kogan recently published a work about cross-sections in invariant theory (cf. [HK07]). They focused on more algorithmic aspects. We will come back to that later.

We start with a brief survey on the basics of algebraic geometry, which is indispensable for the theory of cross-sections of rational maps. Then we will define the notion of a cross-section of a rational map, furthermore, we will give a criterion when a cross-section exists. In the third part of this chapter, we will use cross-sections of rational maps to solve some algorithmic problems in field theory. We will present a new algorithm, based on cross-sections of rational maps, for testing subfield membership and for finding a representation of an element of that subfield in a special set of generators of the subfield. Finally, we will examine the notion of a cross-section of a rational map in the context of invariant theory.

3.1 Some Algebraic Geometry

The following crash course on algebraic geometry differs from other survey-like texts about this topic in the way that it strongly emphasizes concrete constructions. For example, some effort has been spent to actually describe how morphisms resp. rational maps between varieties can be written down concretely. For a more comprehensive and advanced introduction to algebraic geometry, see [Har77].

Let K be an algebraically closed field, let $\mathbb{A}^n_K$ or simply $\mathbb{A}^n$ be the **affine n-space** over K and let $\mathbb{P}^n_K$ or simply $\mathbb{P}^n$ be the **projective n-space** over K.
Let $X_1, \ldots, X_n$ be indeterminates over K. Note that every polynomial $p \in K[X_1, \ldots, X_n]$ defines a function on $\mathbb{A}^n$ via

$$\mathbb{A}^n \longrightarrow K,\ (\xi_1, \ldots, \xi_n) \longmapsto p(\xi_1, \ldots, \xi_n).$$

The **Zariski topology** on $\mathbb{A}^n$ is defined as follows. The closed subsets of $\mathbb{A}^n$ are the zero sets of sets of polynomials in $K[X_1, \ldots, X_n]$. For a set of polynomials $I \subset K[X_1, \ldots, X_n]$, the set of zeroes of I in $\mathbb{A}^n$ shall be written as

$$\mathrm{Z}(I) := \{P \in \mathbb{A}^n;\ p(P) = 0\ \forall p \in I\}.$$

Conversely, for a set $X \subset \mathbb{A}^n$ let

$$\mathrm{Id}(X) := \{p \in K[X_1, \ldots, X_n];\ p(P) = 0\ \forall P \in X\}$$

be the vanishing ideal of X. Note that $\mathrm{Id}(X)$ is an ideal in $K[X_1, \ldots, X_n]$ for every $X \subset \mathbb{A}^n$.
For the projective case, let X_0 be a further indeterminate over K. As in Chapter 1, we represent a point $P \in \mathbb{P}^n$ by homogeneous coordinates $P = (\xi_0 : \ldots : \xi_n)$ where $\xi_0, \ldots, \xi_n \in K$ are not all equal to zero. As usual, $\xi_0, \ldots, \xi_n \in K$ and $\zeta_0, \ldots, \zeta_n \in K$ represent the same point i.e.

$$(\xi_0 : \ldots : \xi_n) = (\zeta_0 : \ldots : \zeta_n)$$

if and only if there exists $\lambda \in K^\times$ such that $\zeta_i = \lambda \cdot \xi_i$ for all $i \in \{0, \ldots, n\}$.
Note that by the non-uniqueness of homogeneous coordinates, a polynomial $p \in K[X_0, \ldots, X_n]$ in general does not define a function on $\mathbb{P}^n$. If however p is assumed to be a homogeneous* polynomial of degree m, then it follows that

$$p(\lambda \cdot \xi_0, \ldots, \lambda \cdot \xi_n) = \lambda^m \cdot p(\xi_0, \ldots, \xi_n) \qquad \text{for all } \lambda \in K^\times,\ (\xi_0 : \ldots : \xi_n) \in \mathbb{P}^n.$$

In particular, if $p(\xi_0, \ldots, \xi_n) = 0$ for some $\xi_0, \ldots, \xi_n \in K$, not all zero, then $p(\lambda \cdot \xi_0, \ldots, \lambda \cdot \xi_n) = 0$ for all $\lambda \in K^\times$. It therefore makes sense to write $p(\xi_0 : \ldots : \xi_n) = 0$ and to speak of the zero set of a homogeneous polynomial in the projective case.

*with respect to the usual grading on $K[X_0, \ldots, X_n]$

Analogously to the affine case, we define the **Zariski topology** on $\mathbb{P}^n$ as follows. The closed subsets of $\mathbb{P}^n$ are the zero sets of sets of homogeneous polynomials in $K[X_0, \ldots, X_n]$. If $I \subset K[X_0, \ldots, X_n]$ is a set of homogeneous polynomials or an homogeneous ideal, i. e. an ideal which is generated by homogeneous elements, then let

$$\mathrm{Z}^+(I) := \{P \in \mathbb{P}^n;\ p(P) = 0\ \forall p \in I \text{ homogeneous}\}$$

be the set of zeroes of I in $\mathbb{P}^n$, and for a set $X \subset \mathbb{P}^n$ let

$$\mathrm{Id}^+(X) := \big(\{p \in K[X_0, \ldots, X_n] \text{ homogeneous};\ p(P) = 0\ \forall P \in X\}\big) \trianglelefteq K[X_0, \ldots, X_n]$$

be the (homogeneous) vanishing ideal of X.
The **Zariski closure** in $\mathbb{A}^n$ respectively $\mathbb{P}^n$ of a subset X of $\mathbb{A}^n$ respectively $\mathbb{P}^n$ is denoted by $\overline{X}$. It is not hard to see that $\overline{X} = \mathrm{Z}(\mathrm{Id}(X))$ respectively $\overline{X} = \mathrm{Z}^+(\mathrm{Id}^+(X))$.
A nonempty subset of a topological space is called **irreducible** if it cannot be expressed as the union of two proper closed subsets. The empty set is not considered to be irreducible. Note that X is an irreducible closed subset of $\mathbb{A}^n$ respectively $\mathbb{P}^n$ if and only if $\mathrm{Id}(X)$ respectively $\mathrm{Id}^+(X)$ is a prime ideal.

Definition 3.1. *An* **affine variety** *is an irreducible closed subset of $\mathbb{A}^n$ endowed with the induced Zariski topology. A* **quasi-affine variety** *is a nonempty open subset of an affine variety, also with the induced Zariski topology. Let V be an open subset of a quasi-affine variety in $\mathbb{A}^n$. A function $f : V \longrightarrow K$ is called* **regular on V** *if it can be written locally as the quotient of polynomials in $K[X_1, \ldots, X_n]$, i. e. if for every point $P \in V$ there exists an open neighbourhood $V_P \subset V$ of P and polynomials $g, h \in K[X_1, \ldots, X_n]$ with $0 \notin h(V_P)$ such that $f(P') = g(P')/h(P')$ for all $P' \in V_P$. Note that the polynomials $X_1, \ldots, X_n$ define functions which are regular on the whole affine space $\mathbb{A}^n$. They are called* **coordinate functions**.
A **projective variety** *is an irreducible closed subset of $\mathbb{P}^n$ endowed with the induced Zariski topology. A* **quasi-projective variety** *is a nonempty open subset of a projective variety, also with the induced Zariski topology. Let V be an open subset of a quasi-projective variety in $\mathbb{P}^n$. A function $f : V \longrightarrow K$ is called* **regular on V** *if it can be written locally as the quotient of homogeneous polynomials in $K[X_0, \ldots, X_n]$ of the same degree. To be more precise, this means that for every point $P \in V$ there exists an open neighbourhood $V_P \subset V$ of P and homogeneous polynomials $g, h \in K[X_0, \ldots, X_n]$ of the same degree with*[†] *$0 \notin h(V_P)$ such that $f(\xi_0 : \ldots : \xi_n) = g(\xi_0, \ldots, \xi_n)/h(\xi_0, \ldots, \xi_n)$ for all $(\xi_0 : \ldots : \xi_n) \in V_P$. (Note that the non-uniqueness of the homogeneous coordinates is no problem here, since we have $g(\lambda \cdot \xi_0, \ldots, \lambda \cdot \xi_n)/h(\lambda \cdot \xi_0, \ldots, \lambda \cdot \xi_n) = g(\xi_0, \ldots, \xi_n)/h(\xi_0, \ldots, \xi_n)$ for all $\lambda \in K^\times$ by the homogeneity of g and h.)*
A **variety over K** *or simply a* **variety** *is any affine, quasi-affine, projective or quasi-projective variety. The set of regular functions on a variety X has the structure of a K-algebra and is denoted by $K[X]$. It is called the* **ring of regular functions** *on X.*
A subset of a variety X which is irreducible and open in its closure in X together with the

[†]The notation $0 \notin h(V_P)$ means that there is no $P' \in V_P$ such that $h(P') = 0$.

induced Zariski topology is called a **subvariety** *of X.*

Remarks 3.2. (a) It can be shown that every regular function on a variety is continuous if K is equipped with the Zariski topology (cf. [Har77], Chapter I, Section 3).

(b) Let V be an open subset of a variety, let f be a regular function on V and let U be an open subset of V. Then the restriction of f to U, denoted by $f_{|U}$, is a regular function on U.

(c) A nonempty open subset of a variety X is a subvariety of X. Furthermore, it is not hard to see that if Y and Z are subvarieties of X such that $Y \cap Z$ is nonempty and irreducible, then $Y \cap Z$ is a subvariety of X, of Y and of Z.

(d) A subvariety of a variety is again a variety. ♢

Definition 3.3. *Let X and Y be varieties. A* **morphism** *$\phi : X \longrightarrow Y$ is a continuous map such that for every open subset $V \subset Y$ and every regular function f on V, the function*

$$f \circ \phi : \phi^{-1}(V) \longrightarrow K$$

is regular on $\phi^{-1}(V)$. An **isomorphism** *$\phi : X \longrightarrow Y$ is a morphism which admits an inverse morphism $\phi^{-1} : Y \longrightarrow X$, where 'inverse' is meant in the usual sense that $\phi^{-1} \circ \phi : X \longrightarrow X$ is the identity map on X and $\phi \circ \phi^{-1} : Y \longrightarrow Y$ is the identity map on Y.*

Remarks 3.4. (a) A nonempty open subset of an irreducible set is dense and irreducible. It follows from Remark 3.2 (a) that if f and g are regular functions on a nonempty open subset V of a variety X such that f and g coincide on a nonempty open subset of V, then $f = g$ as regular functions on V. Similarly, if $\phi : V \longrightarrow Y$ and $\psi : V \longrightarrow Y$ are morphisms from a nonempty open subset V of a variety X to a variety Y such that ϕ and ψ coincide on a nonempty open subset of V, it follows that $\phi = \psi$ as morphisms from V to Y.

(b) Let X and Y be varieties and let $\phi : X \longrightarrow Y$ be a morphism. Then the restriction of ϕ to a subvariety S of X, i. e. $\phi_{|S} : S \longrightarrow Y$ is a morphism, too. Let S' be a subvariety of Y and assume that $\phi(X) \subset S'$. Then again, the map $\phi : X \longrightarrow S'$ is a morphism of varieties.

(c) **Morphisms into affine space.** Let X be an arbitrary variety and let $Y \subset \mathbb{A}^m$ be a quasi-affine variety. It is a straightforward verification that a map $\phi : X \longrightarrow Y$ is a morphism if and only if there exist $f_1, \ldots, f_m \in K[X]$ such that

$$\phi(P) = (f_1(P), \ldots, f_m(P))$$

for all $P \in X$. Because of that, a morphism from a variety X to a quasi-affine variety Y can always be written as an m-tuple

$$\phi = (f_1, \ldots, f_m)$$

for some regular functions $f_1, \ldots, f_m \in K[X]$.

(d) **Morphisms into projective space.** Let X and Y be quasi-projective varieties, say $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$. A map $\phi : X \longrightarrow Y$ is a morphism if and only if for every $P \in X$ there exist polynomials $q_{P,0}, \ldots, q_{P,m} \in K[X_0, \ldots, X_n]$ which are homogeneous of the same degree such that

$$\phi(\xi_0 : \ldots : \xi_n) = (q_{P,0}(\xi_0, \ldots, \xi_n) : \ldots : q_{P,m}(\xi_0, \ldots, \xi_n))$$

for all $(\xi_0 : \ldots : \xi_n)$ in an open neighbourhood of P. Note that since the polynomials $q_{P,0}, \ldots, q_{P,m}$ are homogeneous of the same degree, the expression $(q_{P,0}(\xi_0, \ldots, \xi_n) : \ldots : q_{P,m}(\xi_0, \ldots, \xi_n))$ is independent of the concrete choice of homogeneous coordinates, indeed.
Therefore by (a), a morphism from a quasi-projective variety X to a quasi-projective variety Y can always be represented by an $(m+1)$-tuple

$$\phi = (q_0 : \ldots : q_m)$$

for some polynomials $q_0, \ldots, q_m \in K[X_0, \ldots, X_n]$ which are homogeneous of the same degree (cf. [Sha94], Chapter I, Section 4). ♢

The next definition shows how an ideal of a polynomial ring can be transformed to a homogeneous ideal. As we will see, this will be useful for passing from projective geometry to affine geometry and vice versa.

Definition 3.5. *Let I be an ideal in $K[X_1, \ldots, X_n]$ and let T be an indeterminate over K. Then the* **homogenization of I with respect to T**, *denoted by I_T^h, is defined as the homogeneous ideal in $K[T, X_1, \ldots, X_n]$ generated by*

$$\left\{T^{d_p} \cdot p(X_1/T, \ldots, X_n/T);\ p \in I\right\}$$

where d_p denotes the total degree of the polynomial $p \in I$.

There is a common method to cover the projective n-space with affine varieties. The next lemma makes that precise. For a proof, see e. g. [Har77], Chapter I, Corollary 2.3.

Lemma 3.6. *Let $i \in \{0, \ldots, n\}$ and $U_i := \mathbb{P}^n \setminus \mathrm{Z}^+(X_i)$. Then*

$$\psi_i : U_i \longrightarrow \mathbb{A}^n,\ (\xi_0 : \ldots : \xi_n) \longmapsto \left(\frac{\xi_0}{\xi_i}, \ldots, \frac{\xi_{i-1}}{\xi_i}, \frac{\xi_{i+1}}{\xi_i}, \ldots, \frac{\xi_n}{\xi_i}\right)$$

is an isomorphism of varieties. The inverse of ψ_i is given by

$$\psi_i^{-1} : \mathbb{A}^n \longrightarrow U_i,\ (\zeta_1, \ldots, \zeta_n) \longmapsto (\zeta_1 : \ldots : \zeta_i : 1 : \zeta_{i+1} : \ldots : \zeta_n). \qquad \blacksquare$$

Note that $U_0, \ldots, U_n$ cover the projective n-space, i. e. $\mathbb{P}^n = \bigcup_{0=1}^n U_i$. Therefore – because of the previous lemma – the sets $U_i = \mathbb{P}^n \setminus \mathrm{Z}^+(X_i)$, $i \in \{0, \ldots, n\}$ are also called the **affine pieces** of $\mathbb{P}^n$.

Remarks 3.7. (a) Let $Y_1, \ldots, Y_n$ be indeterminates over K, let $i \in \{0, \ldots, n\}$ and let $Q \trianglelefteq K[X_0, \ldots, X_n]$ be a homogeneous ideal. Consider the ideal $\widetilde{Q} \trianglelefteq K[Y_1, \ldots, Y_n]$ generated by the set of polynomials

$$\{p(Y_1, \ldots, Y_i, 1, Y_{i+1}, \ldots, Y_n);\ p \in Q\}.$$

Then – with the notation of Lemma 3.6 – it can be verified that

$$\psi_i(\mathrm{Z}^+(Q) \cap U_i) = \mathrm{Z}(\widetilde{Q}).$$

Conversely, let $\widetilde{Q} \trianglelefteq K[Y_1, \ldots, Y_n]$ be arbitrary. Then

$$\psi_i^{-1}(\mathrm{Z}(\widetilde{Q})) = \mathrm{Z}^+\big((\widetilde{q}(X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n);\ \widetilde{q} \in \widetilde{Q})^h_{X_i}\big) \cap U_i.$$

(b) With the same notation as in (a), we have

$$\overline{\psi_i^{-1}(\mathrm{Z}(\widetilde{Q}))} = \mathrm{Z}^+\big((\widetilde{q}(X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n);\ \widetilde{q} \in \widetilde{Q})^h_{X_i}\big).$$

(c) Quasi-projectiveness is the most general notion among the four types of varieties in the sense that every variety is isomorphic to a quasi-projective variety. $\diamondsuit$

Definition 3.8. *Let X be a variety. A* **rational function** *on X is the equivalence class of an element in the set of pairs $\{(V, f);\ V \subset X$ nonempty open, $f \in K[V]\}$, where two pairs (V_1, f_1) and (V_2, f_2) are equivalent if $f_1(P) = f_2(P)$ for all $P \in V_1 \cap V_2$. Note that by Remark 3.4 (a), this is indeed an equivalence relation. We denote the equivalence class of (V, f) by $\langle V, f \rangle$. The* **function field** *$K(X)$ of X is defined as the set of rational functions on X.*

Remarks 3.9. (a) It is not hard to see that $K(X)$ together with the obvious addition and multiplication has the structure of a field over K, indeed. Further details can be found in [Har77], Chapter I, Section 3.

(b) Let X be a variety. Clearly, every rational function of the form $\langle X, f\rangle$ can be regarded as a regular function on X. In fact, there is an embedding of the ring of regular functions in the function field of X given by $K[X] \longrightarrow K(X),\ f \longmapsto \langle X, f\rangle$.

(c) Let X be a variety and let $V \subset X$ be a nonempty open subset of X. Then, by definition of the function field, $K(V)$ can be identified with $K(X)$.

(d) Let $X \subset \mathbb{A}^n$ be an affine variety and let $I := \mathrm{Id}(X) \trianglelefteq K[X_1, \ldots, X_n]$. Then $K(X)$ is isomorphic to the field $\mathrm{Quot}(K[X_1, \ldots, X_n]/I)$. For, note that for $g, h \in K[X_1, \ldots, X_n]$, $h \notin I$, the map

$$\begin{aligned}(g + I)/(h + I) : X \setminus \mathrm{Z}(h) &\longrightarrow K,\\ P &\longmapsto g(P)/h(P)\end{aligned}$$

is a well-defined regular function on $X \setminus Z(h)$. Then it is not hard to verify that

$$\begin{aligned}\theta : \mathrm{Quot}(K[X_1, \ldots, X_n]/I) &\longrightarrow K(X),\\ (g + I)/(h + I) &\longmapsto \langle X \setminus \mathrm{Z}(h), (g + I)/(h + I)\rangle\end{aligned}$$

is a well-defined isomorphism of fields.

(e) Let $X \subset \mathbb{P}^n$ be a projective variety and let $I := \mathrm{Id}^+(X) \trianglelefteq K[X_0, \ldots, X_n]$. Then $K(X)$ is isomorphic to the subfield of $\mathrm{Quot}(K[X_0, \ldots, X_n]/I)$ given by the elements of the form $(g + I)/(h + I)$, where $g, h \in K[X_0, \ldots, X_n]$, $h \notin I$ are homogeneous polynomials of the same degree. Similarly as in the affine case, an element $(g+I)/(h+I) \in \mathrm{Quot}(K[X_0, \ldots, X_n]/I)$, where $g, h \in K[X_0, \ldots, X_n]$, $h \notin I$ are homogeneous polynomials of the same degree, corresponds to the rational function $\langle X \setminus \mathrm{Z}^+(h), (g + I)/(h+I)\rangle \in K(X)$. Note again that – in spite of the non-uniqueness of homogeneous coordinates – the expression $(g+I)/(h+I)$ gives a well-defined function on $X \setminus \mathrm{Z}^+(h)$. As before, it is a straightforward verification that this correspondence is in fact an isomorphism of fields.

(f) Let $X \subset \mathbb{A}^n$ be a quasi-affine variety with $I := \mathrm{Id}(X) \trianglelefteq K[X_1, \ldots, X_n]$. Because of (c) and (d) the fields $K(X)$ and $\mathrm{Quot}(K[X_1, \ldots, X_n]/I)$ are isomorphic.
Now let $X \subset \mathbb{P}^n$ be a quasi-projective variety with $I := \mathrm{Id}^+(X) \trianglelefteq K[X_0, \ldots, X_n]$. Similarly as in the affine case, it follows by (c) and (e) that there is an isomorphism between $K(X)$ and the subfield of $\mathrm{Quot}(K[X_0, \ldots, X_n]/I)$ given by the elements of the form $(g+I)/(h+I)$, where $g, h \in K[X_0, \ldots, X_n]$, $h \notin I$ are homogeneous polynomials of the same degree.

(g) If $X \subset \mathbb{A}^n$ is an affine or, more generally, a quasi-affine variety with $I := \mathrm{Id}(X) \trianglelefteq K[X_1, \ldots, X_n]$, then according to (d) and (f), we will often write $f = (g+I)/(h+I) \in K(X)$ with $g, h \in K[X_1, \ldots, X_n]$, $h \notin I$ instead of $\langle V, f\rangle \in K(X)$.

Similarly – according to (e) and (f), if $X \subset \mathbb{P}^n$ is a projective or, more generally, a quasi-projective variety with $I := \mathrm{Id}^+(X)$, then the rational function $\langle V, f\rangle$ will usually be written as $f = (g+I)/(h+I) \in K(X)$ with $g, h \in K[X_0, \ldots, X_n]$, $h \notin I$ homogeneous polynomials of the same degree.

(h) **Morphisms into projective space revisited.** With the notion of rational functions in hand, we can give another characterization of morphisms between quasi-projective varieties (cf. Remark 3.4 (d)). Let X and Y be quasi-projective varieties, say $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$. We know by Remark 3.4 (d) that a map $\phi : X \longrightarrow Y$ is a morphism if and only if for every $P \in X$ there exist polynomials $q_{P,0}, \ldots, q_{P,m} \in K[X_0, \ldots, X_n]$ which are homogeneous of the same degree such that

$$\phi(\xi_0 : \ldots : \xi_n) = (q_{P,0}(\xi_0, \ldots, \xi_n) : \ldots : q_{P,m}(\xi_0, \ldots, \xi_n))$$

for all $(\xi_0 : \ldots : \xi_n)$ in an open neighbourhood of P. Clearly, there is an index $i \in \{0, \ldots, m\}$ such that $q_{P,i}(P) \neq 0$. It follows that there exists a nonempty open subset V' of V with $0 \notin q_{P,i}(V')$ such that

$$\phi(\xi_0, \ldots, \xi_n) = \left(\frac{q_{P,0}(\xi_0, \ldots, \xi_n)}{q_{P,i}(\xi_0, \ldots, \xi_n)} : \ldots : \frac{q_{P,m}(\xi_0, \ldots, \xi_n)}{q_{P,i}(\xi_0, \ldots, \xi_n)} \right)$$

for all $(\xi_0 : \ldots : \xi_n) \in V'$. Note that the elements $(q_{P,0} + \mathrm{Id}^+(X))/(q_{P,i} + \mathrm{Id}^+(X)), \ldots, (q_{P,m} + \mathrm{Id}^+(X))/(q_{P,i} + \mathrm{Id}^+(X))$ are rational functions on X. Therefore, we have shown that if $\phi : X \longrightarrow Y$ is a morphism, then for every $P \in X$ there exist rational functions $f_{P,0}, \ldots, f_{P,m} \in K(X)$ such that

$$\phi(P') = (f_{P,0}(P') : \ldots : f_{P,m}(P'))$$

for all P' in some open neighbourhood of P. A very similar argumentation shows that conversely, a map $\phi : X \longrightarrow Y$ is a morphism if for every $P \in X$ there exist rational functions $f_{P,0}, \ldots, f_{P,m} \in K(X)$ such that

$$\phi(P') = (f_{P,0}(P') : \ldots : f_{P,m}(P'))$$

for all P' in some open neighbourhood of P. ♢

Definition 3.10. *Let X, Y and Z be varieties. A* **rational map** *from X to Y is the equivalence class of an element in the set of pairs $\{(V, \phi);\ V \subset X$ nonempty open, $\phi : V \longrightarrow Y$ a morphism$\}$, where two pairs (V_1, ϕ) and (V_2, ψ) are equivalent if $\phi(P) = \psi(P)$ for all $P \in V_1 \cap V_2$. Note that by Remark 3.4 (a), this indeed defines an equivalence relation. We denote the equivalence class of (V, ϕ) by $\langle V, \phi\rangle$.*
A rational map $\langle V, \phi\rangle$ is called **dominant** *if $\phi(V)$ is dense in Y. If $\langle V_1, \phi\rangle$ is a dominant rational map from X to Y and $\langle V_2, \psi\rangle$ is a rational map from Y to Z, then the composition $\langle V_2, \psi\rangle \circ \langle V_1, \phi\rangle$ can be defined in the obvious way which then yields a rational map from*

X to Z.
A dominant rational map $\langle V_1, \phi\rangle$ from X to Y is called a **birational isomorphism** *if there exists an inverse dominant rational map $\langle V_2, \phi^{-1}\rangle$ from Y to X, in the sense that*

$$\langle V_2, \phi^{-1}\rangle \circ \langle V_1, \phi\rangle = \langle X, \mathrm{id}_X\rangle \text{ and } \langle V_1, \phi\rangle \circ \langle V_2, \phi^{-1}\rangle = \langle Y, \mathrm{id}_Y\rangle,$$

where id_X denotes the identity map on X and id_Y denotes the identity map on Y. If there exists a birational isomorphism from X to Y, then the varieties X and Y are called **birationally equivalent**.

Remark 3.11. Let X, Y and Z be varieties. By Remark 3.7 (c), we may assume that $Y \subset \mathbb{P}^m$ for some $m \in \mathbb{N}$.

(a) Let $\langle V, \phi\rangle$ be a rational map from X to Y. Then there is a unique maximal (with respect to inclusion) open subset V' of X such that there exists a morphism $\psi : V' \longrightarrow Y$ with $\langle V', \psi\rangle = \langle V, \phi\rangle$. We call V' the **domain of definition** of the rational map $\langle V, \phi\rangle$. If a point P lies in V', then we say that the rational map $\langle V, \phi\rangle$ is **defined at P**.

(b) The composition of dominant rational maps again gives a dominant rational map. The composition of birational isomorphisms gives a birational isomorphism.

(c) The restriction of a rational map $\langle V, \phi\rangle$ from X to Y to a subvariety S of X with $S \cap V \neq \emptyset$ obviously defines a rational map from S to Y, namely $\langle S \cap V, \phi_{|S\cap V}\rangle$. Let $S' \subset Y$ be a subvariety of Y and assume that $\phi(V) \subset S'$. Then again, $\langle V, \phi\rangle$ is a rational map from X to S'.

(d) As the name suggests, a rational map $\langle V, \phi\rangle$ from X to Y defines a partial map from X to Y which is defined at all points of the domain of definition of $\langle V, \phi\rangle$ in the obvious way. For ease of notation we will write the rational map $\langle V, \phi\rangle$ from X to Y simply as $\phi : X \dashrightarrow Y$. The composition of a dominant rational map $\phi : X \dashrightarrow Y$ and a rational map $\psi : Y \dashrightarrow Z$ will be written as $\psi \circ \phi : X \dashrightarrow Z$. The restriction of a rational map $\phi : X \dashrightarrow Y$ to a subvariety S of X, which has a nonempty intersection with the domain of definition of ϕ, will be written as $\phi_{|S} : S \dashrightarrow Y$.

(e) **Rational maps into affine space.** Let $Y \subset A^m$ be quasi-affine. If $\phi : X \dashrightarrow Y$ is a rational map, then it follows by Remark 3.4 (c) and Remarks 3.9 (b) and (c) that there exist rational functions $f_1, \ldots, f_m \in K(X)$ such that

$$\phi(P) = (f_1(P), \ldots, f_m(P))$$

for all P in some nonempty open subset of X. For that reason every rational map ϕ from X to Y can be represented by an m-tuple

$$\phi = (f_1, \ldots, f_m)$$

for some rational functions $f_1, \ldots, f_m \in K(X)$. In fact, for all points P in the domain of definition of ϕ there exist rational functions $f_1, \ldots, f_m \in K(X)$ which are regular at P such that $\phi = (f_1, \ldots, f_m)$.
Conversely, if $f_1, \ldots, f_m \in K(X)$ are rational functions, then it follows again from Remark 3.4 (c) that

$$\begin{aligned}(f_1, \ldots, f_m) : X &\dashrightarrow \mathbb{A}^m, \\ P &\longmapsto (f_1(P), \ldots, f_m(P)),\end{aligned}$$

for all P in some nonempty open subset of X, defines a rational map.

(f) **Rational maps into projective space.** Let X and Y be quasi-projective varieties, say $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ and let $\phi : X \dashrightarrow \mathbb{P}^m$ be a rational map. Since a nonempty open subset of a quasi-projective variety is quasi-projective again, we know by Remarks 3.9 (h) and (c) that there exist rational functions $f_0, \ldots, f_m \in K(X)$ such that

$$\phi(P) = (f_0(P) : \ldots : f_m(P))$$

for all P in some nonempty open subset V of X. For that reason every rational map ϕ from X to Y can be represented by an m-tuple

$$\phi = (f_0 : \ldots : f_m)$$

for some rational functions $f_0, \ldots, f_m \in K(X)$. In fact, for all points P in the domain of definition of ϕ there exist rational functions $f_0, \ldots, f_m \in K(X)$ which are defined at P such that $\phi = (f_0 : \ldots : f_m)$.
Conversely, if $f_0, \ldots, f_m \in K(X)$ are rational functions, then it follows again from Remark 3.9 (h) that

$$\begin{aligned}(f_0 : \ldots : f_m) : X &\dashrightarrow \mathbb{P}^m, \\ P &\longmapsto (f_0(P) : \ldots : f_m(P))\end{aligned}$$

for all P in some nonempty open subset of X defines a rational map.

(g) **Rational maps from quasi-affine varieties into projective space.** By Lemma 3.6, it should be clear how a rational map from a quasi-affine variety to a quasi-projective variety looks like. Nonetheless, we give an explicit form of this map here, since we need this later on. Let X be a quasi-affine and Y be a quasi-projective variety, say $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{P}^m$. By Lemma 3.6, X is isomorphic to a quasi-projective variety in $\mathbb{P}^n$ via $\phi_0^{-1} : \mathbb{A}^n \longrightarrow U_0$. Using this isomorphism and (f) above, it follows that a map ϕ from X to Y is a rational map if and only if there exist rational functions $f_0, \ldots, f_m \in K(X)$ such that

$$\phi(P) = (f_0(P) : \ldots : f_m(P))$$

for all P in some nonempty open subset of X. In fact, for all points P in the domain

of definition of ϕ there exist rational functions $f_0, \ldots, f_m \in K(X)$ which are defined at P such that $\phi = (f_0 : \ldots : f_m)$.

(h) Let X be a variety and let $\phi = (f_1, \ldots, f_m) : X \dashrightarrow \mathbb{A}^m$ be a rational map with some rational functions $f_1, \ldots, f_m \in K(X)$. Sometimes, it is useful to know the image of X under ϕ. The image of X under ϕ is defined as the image of the domain of definition V' of ϕ and written as $\phi(X)$, i. e. $\phi(X) := \phi(V')$.
In practice, it is often sufficient to know the closure of the image of ϕ. Actually, this can be defined independently of the concrete choice of a representative of the rational map ϕ. Let (V, ϕ_V) and (U, ϕ_U) be two representatives of ϕ. We claim that $\overline{\phi_V(V)} = \overline{\phi_U(U)}$. For, note that

$$\overline{\phi_U(U \cap V)} \supset \phi_U(\overline{U \cap V}) = \phi_U(U) \quad \text{and} \quad \phi_V(V) \supset \phi_V(U \cap V) = \phi_U(U \cap V).$$

It follows that $\overline{\phi_V(V)} \supset \overline{\phi_U(U)}$ and thus – by symmetry – $\overline{\phi_V(V)} = \overline{\phi_U(U)}$, as claimed. In particular, we have $\overline{\phi(X)} = \overline{\phi_V(V)}$ for all representatives (V, ϕ_V) of ϕ.
Let $Q \trianglelefteq K[Y_1, \ldots, Y_m]$ with indeterminates $Y_1, \ldots, Y_m$ over K be the ideal of relations of the elements $f_1, \ldots, f_m$ over K. Then it can be shown that

$$\overline{\phi(X)} = \mathrm{Z}(Q) \subset \mathbb{A}^m, \tag{3.1}$$

where obviously $Y_1, \ldots, Y_m$ play the role of the coordinate functions on $\mathbb{A}^m$ (cf. [CLO07], Chapter 3, § 3).
For the examination of the projective case, let $\phi' = (f_0 : \ldots : f_m) : X \dashrightarrow \mathbb{P}^m$ be a rational map with some rational functions $f_0, \ldots, f_m \in K(X)$. Let $Y_0, \ldots, Y_m$ be indeterminates over K, let $i \in \{0, \ldots, m\}$ such that $f_i \neq 0 \in K(X)$ and let $Q \trianglelefteq K[Y_0, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_m]$ be the ideal of relations of the elements $f_0/f_i, \ldots, f_{i-1}/f_i$, $f_{i+1}/f_i, \ldots, f_m/f_i$ over K. Then it can be shown (cf. Remark 3.7 (b) and equation (3.1)) that

$$\overline{\phi(X)} = \mathrm{Z}^+(Q^h_{Y_i}) \subset \mathbb{P}^m. \qquad \diamondsuit$$

Proposition 3.12. *Let X and Y be varieties and $\phi : X \dashrightarrow Y$ a dominant rational map. Then ϕ induces a K-homomorphism ϕ^* of fields in the following way*

$$\phi^* : K(Y) \longrightarrow K(X),\ f \longmapsto f \circ \phi.$$

Proof. See for example [Har77], Chapter I, Section 4. ∎

Remarks 3.13. (a) Actually, the set of dominant rational maps from X to Y is in one-to-one-correspondence with the set of K-homomorphisms of fields from $K(Y)$ to $K(X)$ in the way as described in Proposition 3.12. It can be checked that $\phi^* : K(Y) \longrightarrow K(X)$ is an isomorphism of fields if and only if $\phi : X \dashrightarrow Y$ is a birational isomorphism. For details, see [Har77], Chapter I, Corollary 4.5.

(b) It follows from (a) and Remark 3.9 (c) that if V is a nonempty open subset of a variety X, then V and X are birationally equivalent. More precisely, the natural embedding $\iota : V \hookrightarrow X$ is a birational isomorphism. In particular, a subvariety Y of a variety X and its Zariski closure $\overline{Y} \cap X$ in X are birationally equivalent via the natural embedding $\iota_Y : Y \hookrightarrow \overline{Y} \cap X$.

(c) Let X and Y be varieties with $Y \subset \mathbb{A}^m$ quasi-affine and let $\phi = (f_1, \ldots, f_m) : X \dashrightarrow Y$ with some rational functions $f_1, \ldots, f_m \in K(X)$ be a dominant rational map. It is not hard to see that
$$\phi^*(K(Y)) = K(f_1, \ldots, f_m).$$

(d) Let X and Y be varieties with $Y \subset \mathbb{P}^m$ quasi-projective, let $\phi = (f_0 : \ldots : f_m) : X \dashrightarrow Y$ be a dominant rational map with some rational functions $f_0, \ldots, f_m \in K(X)$ and let $i \in \{0, \ldots, m\}$ such that $f_i \neq 0 \in K(X)$. Then it can be shown that
$$\phi^*(K(Y)) = K(f_0/f_i, \ldots, f_m/f_i). \qquad \diamondsuit$$

For the remainder of this chapter we use the following notation:

Notation 3.14.

(i) K shall denote an algebraically closed field.

(ii) X, Y shall denote varieties over K, where $X \subset \mathbb{A}^n_K$ or $X \subset \mathbb{P}^n_K$ and $Y \subset \mathbb{A}^m_K$ or $Y \subset \mathbb{P}^m_K$.

(iii) $\phi : X \dashrightarrow Y$ shall denote a dominant rational map.

(iv) $L \leq K(X)$ shall denote the field $\phi^*(K(Y))$.

(v) $X_0, \ldots, X_n$ and $Y_0, \ldots, Y_m$ shall denote indeterminates over K. Usually, the sets of variables $X_0, \ldots, X_n$ correspond to coordinates of $\mathbb{A}^n$ resp. $\mathbb{P}^n$ and the sets of variables $Y_0, \ldots, Y_m$ correspond to coordinates of $\mathbb{A}^m$ resp. $\mathbb{P}^m$.

3.2 Cross-Sections of Rational Maps

In the following, the notion of a cross-section of a rational map will be introduced. As we will see, the existence of a cross-section of a rational map is not guaranteed in general – it has to be checked specifically for each rational map whether it admits a cross-section or not. The standard way for doing this is nice in theory but not really handy in practice. In this section, we will develop a better manageable criterion for the existence of a cross-section of a rational map. Moreover, it will turn out that this criterion provides a way to actually find one.

Definition 3.15. *Let X, Y and ϕ be as in Notation 3.14. A subvariety S of X is called a* **cross-section** *of the rational map ϕ if*

$$\phi_{|S} : S \dashrightarrow Y$$

is a birational isomorphism.

So in particular, a cross-section of a dominant rational map $\phi : X \dashrightarrow Y$ is a model of the field $K(Y)$, i. e. a variety such that its function field is isomorphic to $K(Y)$. Note that the condition on S to be a cross-section is rather strong – in fact, as mentioned above and as it will be demonstrated in the following examples, not all rational maps actually have a cross-section. Later, we will see that a cross-section of a rational map is advantageous for the solution of various problems concerning the field $\phi^*(K(Y))$.

Examples 3.16. (a) Let X_1, X_2 be indeterminates over K, let ϕ be the rational map

$$\phi : \mathbb{A}^2 \dashrightarrow \mathbb{A}^1,\ (\xi_1, \xi_2) \longmapsto \frac{\xi_1}{\xi_2} \quad \text{for all } (\xi_1, \xi_2) \in \mathbb{A}^2 \setminus \mathrm{Z}(X_2)$$

and let S be the subvariety of $\mathbb{A}^2$ defined by the ideal $(X_2 - 1) \trianglelefteq K[X_1, X_2]$. Obviously, the restriction of the rational map ϕ to the subvariety S is a birational isomorphism with its inverse being given by the morphism

$$\mathbb{A}^1 \longrightarrow S,\ \xi \longmapsto (\xi, 1).$$

Therefore, it follows that S is a cross-section of ϕ.

(b) Let ϕ be the morphism

$$\phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^1,\ \xi \longmapsto \xi^2.$$

Clearly, ϕ is a dominant rational map. We claim that there does not exist a cross-section of ϕ. To see this, assume for a contradiction that a subvariety S of $\mathbb{A}^1$ is a cross-section of ϕ. Then since the restriction $\phi_{|S}$ is a birational isomorphism, the function fields $K(S)$ and $K(\mathbb{A}^1)$ are K-isomorphic. It follows from Remark 3.9 (d) that the ideal $I := \mathrm{Id}(S) \trianglelefteq K[X_1]$ (where X_1 is an indeterminate over K) satisfies $\mathrm{Quot}(K[X_1]/I) \cong K(X_1)$. By comparing transcendental degrees, this implies that I is equal to $(0) \trianglelefteq K[X_1]$, and thus we have

$$\overline{S} = \mathbb{A}^1.$$

It follows that the rational map ϕ itself must be a birational isomorphism. But on the other hand, it is not hard to see that the rational map ϕ does not have a rational inverse – a contradiction. This shows that ϕ does not admit a cross-section. $\lhd$

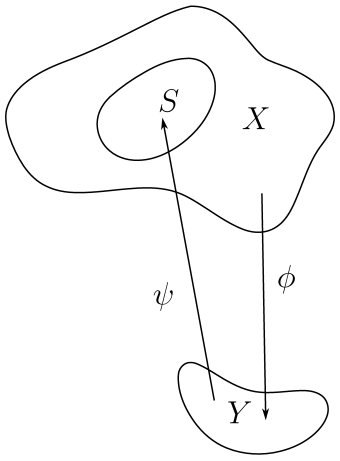

Figure 3.1: A cross-section S of a rational map ϕ

How can the notion of a cross-section of a rational map be interpreted geometrically? Let X, Y and ϕ be as in Notation 3.14 and let a subvariety S of X be a cross-section of ϕ. By definition, there exists a rational map $\psi : Y \dashrightarrow S$ (see figure 3.2) such that $\psi \circ \phi_{|S} = \mathrm{id}_S$ and $\phi_{|S} \circ \psi = \mathrm{id}_Y$.
Let $\mathcal{O}$ be the (nonempty) open subset of points P in X such that ϕ is defined at P, ψ is defined at $\phi(P)$ and again ϕ is defined at $(\psi \circ \phi)(P)$. Obviously, the composition $\pi := \psi \circ \phi : X \dashrightarrow S$ is constant on the fibres of the rational map ϕ in $\mathcal{O}$. Observe that $\pi(P) \in \mathcal{O}$ and that P and $\pi(P)$ are in the same fibre of ϕ for all points $P \in \mathcal{O}$. Therefore – with $\pi_{|S}$ being equal to the identity map on S – the rational map π can be interpreted as some kind of projection which maps all fibres F of the rational map ϕ in the open set $\mathcal{O}$ to a distinguished point of the fibre, namely to the single point of the intersection $F \cap S$.

In the next proposition, we give another characterization of cross-sections of rational maps. Although this characerization seems to be almost obvious, we want to point it out here explicitly, since it is the key to many applications of cross-sections of rational maps.

Proposition 3.17. *Let X, Y, ϕ and L be as in Notation 3.14. A subvariety S of X is a cross-section of ϕ if and only if the restriction of the rational functions in L to S defines an isomorphism of the fields L and $K(S)$.*

Proof. First, assume that the subvariety S is a cross-section of the rational map ϕ. By definition, the K-homomorphism $\phi^* : K(Y) \longrightarrow K(X)$ induces an isomorphism of the fields $K(Y)$ and L. Moreover, since S is a cross-section, the rational map $\phi_{|S} : S \dashrightarrow Y$ is a birational isomorphism. So we have

$$L \xleftarrow[\phi^*]{\cong} K(Y) \xrightarrow[(\phi_{|S})^*]{\cong} K(S).$$

It follows that the composition

$$\theta := (\phi_{|S})^* \circ (\phi^*)^{-1} : L \longrightarrow K(S)$$

is an isomorphism, too. Now observe that for every $f \in L$, which by definition of L is equal to $\phi^*(\hat{f})$ for some $\hat{f} \in K(Y)$, the image of f under the map θ satisfies

$$\theta(f) = (\phi_{|S})^* \circ (\phi^*)^{-1}(f) = (\phi_{|S})^*(\hat{f}) = \hat{f} \circ \phi_{|S} = (\hat{f} \circ \phi)_{|S} = f_{|S}.$$

It follows that the restriction of the rational functions in L to S coincides with the map $\theta : L \longrightarrow K(S)$ and hence is an isomorphism of the fields L and $K(S)$.

Conversely, suppose that the restriction of the rational functions in L to S defines an isomorphism of the fields L and $K(S)$. In particular, this means that every rational function in L is defined somewhere on S. As the rational map ϕ can be represented on a nonempty open subset of X by a finite number of rational functions in L (cf. Remark 3.11 (e), (f) and (g)), it follows that the domain of definition of ϕ has a nonempty intersection with the subvariety S. So the restriction $\phi_{|S} : S \dashrightarrow Y$ is a well-defined rational map. By definition of L, we furthermore have the equality

$$(\phi_{|S})^*(K(Y)) = \{l_{|S};\ l \in L\},$$

the right hand side being equal to $K(S)$ by assumption. It follows that $\phi_{|S} : S \dashrightarrow Y$ is a birational isomorphism (cf. Remark 3.13 (a)). ∎

In the examples above, we have seen that not every rational map admits a cross-section. As mentioned before, we will now develop an easy-to-handle criterion for the existence of a cross-section of a rational map.

Proposition 3.18. *Let X, Y and ϕ be as in Notation 3.14 and let Z be a subvariety of X which is open in X. Furthermore, let S be a subvariety of X with $S \cap Z \neq \emptyset$. Then the following are equivalent:*

(a) S is a cross-section of ϕ.

(b) $S \cap Z$ is a cross-section of ϕ.

(c) $S \cap Z$ is a cross-section of $\phi_{|Z}$.

Proof. First of all, note that by Remark 3.2 (c), the set $S \cap Z$ is a subvariety of X and a subvariety of Z. The equivalence of (b) and (c) is an immediate consequence of the fact that $(\phi_{|Z})_{|S\cap Z} = \phi_{|S\cap Z} : S \cap Z \dashrightarrow Y$.
By Remark 3.13 (b), the varieties S and $S \cap Z$ are birationally equivalent via the natural embedding $\iota : S \cap Z \hookrightarrow S$, since $S \cap Z$ is open in S. Thus by Remark 3.11 (b), the equality

$$\phi_{|S\cap Z} = \phi_{|S} \circ \iota : S \cap Z \dashrightarrow Y$$

shows the equivalence of (a) and (b). ∎

The proposition makes clear that there exists a cross-section of a rational map $\phi : X \dashrightarrow Y$ if and only if there exists a cross-section of the rational map[‡] $\phi : \overline{X} \dashrightarrow Y$ which has a nonempty intersection with X. Therefore, in the first instance, we aim to develop a criterion for the existence of a cross-section of a rational map $\phi : X \dashrightarrow Y$ with $X = \overline{X}$.

Corollary 3.19. *Let X, Y and ϕ be as in Notation 3.14. Let S be a subvariety of X. Then S is a cross-section of ϕ if and only if $\overline{S} \cap X$, the Zariski-closure of S in X, is a cross-section of ϕ.*

Proof. By definition of a subvariety, S is an open subset of its closure $\overline{S} \cap X$ in X. Hence there exists $Z \subset X$ open such that $S = (\overline{S} \cap X) \cap Z$. Now the assertion is exactly the equivalence of (a) and (b) in Proposition 3.18. ∎

Because of this corollary, we will assume in various places in what follows that cross-sections of rational maps are closed.

Corollary 3.20. *Let X, Y and ϕ be as in Notation 3.14 with $X \subset \mathbb{P}^n$ a quasi-projective variety. Let $U_i \subset \mathbb{P}^n$, $i \in \{0, \ldots, n\}$ be the affine pieces of $\mathbb{P}^n$. Then a subvariety S of X is a cross-section of $\phi : X \dashrightarrow Y$ if and only if for some – and in fact for any – $i \in \{0, \ldots, n\}$ with $S \cap U_i \neq \emptyset$ the variety $S \cap U_i$ is a cross-section of $\phi_{|X \cap U_i} : X \cap U_i \dashrightarrow Y$.*

Proof. Let $i \in \{0, \ldots, n\}$ with $S \cap U_i \neq \emptyset$. Recall from Remark 3.2 (c) that $Z := X \cap U_i$ is a subvariety of X. By construction, the subvariety Z is open in X and its intersection with S is nonempty. So the assertion follows from the equivalence of (a) and (c) of Proposition 3.18. ∎

Recall from Lemma 3.6 that the affine pieces $U_i \subset \mathbb{P}^n$, $i \in \{0, \ldots, n\}$ are isomorphic to the affine space $\mathbb{A}^n$. More generally, it is not hard to see that if $X \subset \mathbb{P}^n$ is a (quasi-)projective variety, then the intersections $X \cap U_i$, $i \in \{0, \ldots, n\}$ have the structure of (quasi-)affine varieties. By Corollary 3.20, the existence of a cross-section of a rational map $\phi : X \dashrightarrow Y$ where X is a (quasi-)projective variety is hence equivalent to the existence of a cross-section of $\phi' := \phi_{|X'} : X' \dashrightarrow Y$ with $X' \subset X$ an appropriate (quasi-)affine variety. This in turn – as we have seen - is equivalent to the existence of a cross-section of $\phi' : \overline{X'} \dashrightarrow Y$ where $\overline{X'}$ is the closure of X' in affine space.

Summarizing the above, it is our main object to find a criterion for the existence of a (closed) cross-section of a rational map $\phi : X \dashrightarrow Y$ for the case that X is an affine variety.

[‡]As before, $\overline{X}$ denotes the Zariski-closure of X in $\mathbb{A}^n$ respectively $\mathbb{P}^n$ depending on whether $X \subset \mathbb{A}^n$ or $X \subset \mathbb{P}^n$.

Let X, Y, ϕ and L be as in Notation 3.14 with $X \subset \mathbb{A}^n$ an affine variety. Let a closed subvariety $S \subset X$ be a cross-section of $\phi : X \dashrightarrow Y$. Again, we denote by $\psi : Y \dashrightarrow S$ the inverse of the birational isomorphism $\phi_{|S} : S \dashrightarrow Y$ and by $\pi : X \dashrightarrow S$ the composition of the dominant rational maps ψ and ϕ. Let $I := \mathrm{Id}(X) \trianglelefteq K[X_1, \ldots, X_n]$ and write $x_1, \ldots, x_n$ as abbreviations for $X_1 + I, \ldots, X_n + I$. From the equality

$$\pi^*(K(S)) = \phi^*(K(Y)) = L$$

it follows that the dominant rational map π can be represented by a finite number of rational functions in L, i. e. that there exist rational functions $l_1, \ldots, l_n \in L$ such that

$$\pi = (l_1, \ldots, l_n) : X \dashrightarrow S$$

(cf. Remark 3.11 (e) and Remark 3.13 (c)). Recall from Remark 3.11 (h) that the cross-section S then coincides with the affine variety which is defined by the ideal of relations of the elements $l_1, \ldots, l_n$ over K. The cross-section S is hence determined by the tuple $(l_1, \ldots, l_n) \in L^n$. But what conditions characterize L-tuples in L^n that define a cross-section of the rational map ϕ?
Note that by construction of the rational map $\pi = \psi \circ \phi : X \dashrightarrow S$, the restriction $\pi_{|S} : S \dashrightarrow Y$ is equal to the identity map on S. It follows that we have

$$l_{1|S} = x_{1|S}, \ldots, l_{n|S} = x_{n|S} \in K(S).$$

By Proposition 3.17, any L-relation of the elements $x_1, \ldots, x_n$ gives a $K(S)$-relation of the elements $x_{1|S}, \ldots, x_{n|S} = l_{1|S}, \ldots, l_{n|S}$ if we restrict the involved elements of the relation to S. It follows – again by Proposition 3.17 – that $p(l_1, \ldots, l_n) = 0$ for all L-relations p of $x_1, \ldots, x_n$ and therefore that

$$p(l_1, \ldots, l_n) = 0 \in K(X) \text{ for all } p \in J_L^x \trianglelefteq K(X)[Z_1, \ldots, Z_n],$$

the MQS ideal of $x_1, \ldots, x_n$ over L, which by Corollary 2.18 is the ideal generated by the relations of the elements $x_1, \ldots, x_n$ over L. This property of $l_1, \ldots, l_n$ will be the content of the first condition for the elements $l_1, \ldots, l_n \in L$ to define a cross-section of the rational map ϕ.
Moreover, by definition of a cross-section, the intersection of the cross-section S with the domain of definition of the rational map ϕ is nonempty, i. e. the rational map ϕ is defined somewhere on the variety $Z(Q) = S$, where Q is the ideal of relations of the elements $l_1, \ldots, l_n$ over K. In fact, as we will see in a minute, this property together with the condition outlined a few lines above already characterizes the set of L-tuples that define a cross-section of ϕ.

Proposition 3.21. *Let X, Y, ϕ and L be as in Notation 3.14 with $X \subset \mathbb{A}^n$ an affine variety and $I := \mathrm{Id}(X) \trianglelefteq K[X_1, \ldots, X_n]$ (where $X_1, \ldots, X_n$ are indeterminates over K). Let $x_1, \ldots, x_n$ be abbreviations for $X_1 + I, \ldots, X_n + I$, let $\underline{x}$ be an abbreviation for $x_1, \ldots, x_n$*

and let $Z_1, \ldots, Z_n$ be indeterminates over $K(X)$. There exists a cross-section of ϕ if and only if there exist $l_1, \ldots, l_n \in L = \phi^*(K(Y))$ satisfying the following conditions:

(a) For all $p \in J_L^x \trianglelefteq K(X)[Z_1, \ldots, Z_n]$, we have

$$p(l_1, \ldots, l_n) = 0 \in K(X).$$

(b) The rational map ϕ is defined somewhere on $\mathrm{Z}(Q) \subset X$, where $Q \trianglelefteq K[X_1, \ldots, X_n]$ is the ideal of relations of the elements $l_1, \ldots, l_n$ over K.

In fact, if these conditions are satisfied, then the variety $\mathrm{Z}(Q) \subset X$ is a cross-section of the rational map ϕ.

Remark 3.22. Let $l_1, \ldots, l_n$ be elements in L such that condition (a) of Proposition 3.21 is satisfied. Let $Q \trianglelefteq K[X_1, \ldots, X_n]$ be the ideal of relations of the elements $l_1, \ldots, l_n$ over K. If p is a polynomial in $I \trianglelefteq K[X_1, \ldots, X_n]$, the ideal of relations of the elements $x_1, \ldots, x_n$ over K, then the polynomial $p(Z_1, \ldots, Z_n)$ clearly lies in the MQS ideal $J_L^x \trianglelefteq K(X)[Z_1, \ldots, Z_n]$, the ideal generated by the relations of the elements $x_1, \ldots, x_n$ over L. It follows that the polynomials of the ideal I vanish at $l_1, \ldots, l_n$. Therefore, the ideal I is contained in Q, which shows that $\mathrm{Z}(Q)$ is a subvariety of X, indeed. $\diamondsuit$

Proof. Suppose first that there exists a cross-section of ϕ. Then by Corollary 3.19, there exists a cross-section S of ϕ which is closed in X. Let $Q \trianglelefteq K[X_1, \ldots, X_n]$ be its vanishing ideal, i. e. $Q := \mathrm{Id}(S)$, let $\psi : Y \dashrightarrow S$ be the inverse of the rational map $\phi_{|S} : S \dashrightarrow Y$ and let $l_1, \ldots, l_n \in L$ such that $\psi \circ \phi = (l_1, \ldots, l_n) : X \dashrightarrow S$. As in the discussion above, it can be shown that the elements $l_1, \ldots, l_n$ vanish at all polynomials of the MQS ideal $J_L^x \trianglelefteq K(X)[Z_1, \ldots, Z_n]$. Therefore, the elements $l_1, \ldots, l_n$ satisfy condition (a). Furthermore, we know by Remark 3.11 (h) that the ideal Q is exactly the ideal of relations of the elements $l_1, \ldots, l_n$ over K and hence that the rational map ϕ is defined somewhere on $\mathrm{Z}(Q) = S$. It follows that the elements $l_1, \ldots, l_n$ satisfy condition (b), too.

Conversely, suppose that there exist $l_1, \ldots, l_n \in L$ which satisfy conditions (a) and (b). Let $Q \trianglelefteq K[X_1, \ldots, X_n]$ be the ideal of relations of $l_1, \ldots, l_n$ over K. We claim that $S := \mathrm{Z}(Q) \subset X$ is a cross-section of ϕ, i. e. that $\phi_{|S} : S \dashrightarrow Y$ is a birational isomorphism. We first show that $\phi_{|S} : S \dashrightarrow Y$ is dominant. By Remark 3.7 (c), we may assume that Y is a quasi-projective variety in $\mathbb{P}^m$. Since the rational map ϕ is defined somewhere on S (cf. condition (b)), there exist rational functions $f_0, \ldots, f_m \in L$ which are defined somewhere on S such that

$$\phi = (f_0 : \ldots : f_m) : X \dashrightarrow Y$$

(cf. Remark 3.11 (g) and Remark 3.13 (d)). Let $g_0, \ldots, g_m \in K[X_1, \ldots, X_n]$ and $h_0, \ldots, h_m$

$\in K[X_1, \ldots, X_n] \setminus Q$ be polynomials such that

$$f_i = \frac{g_i + I}{h_i + I} \in L \subset K(X)$$

for all $i \in \{0, \ldots, m\}$. Then the polynomials $g_i(\underline{Z}) - f_i \cdot h_i(\underline{Z}) \in L[Z_1, \ldots, Z_n]$, $i \in \{0, \ldots, m\}$ lie in the MQS ideal $J_L^{\underline{x}}$ (cf. Definition 2.16). By condition (a), it follows that

$$g_i(l_1, \ldots, l_n) - \frac{g_i + I}{h_i + I} \cdot h_i(l_1, \ldots, l_n) = 0 \in K(X)$$

for all $i \in \{0, \ldots, m\}$. Thus the rational function $g_i(l_1, \ldots, l_n)/h_i(l_1, \ldots, l_n) \in K(X)$ is equal to the rational function $(g_i + I)/(h_i + I) = f_i \in K(X)$ for all $i \in \{0, \ldots, m\}$. Let

$$\pi := (l_1, \ldots, l_n) : X \dashrightarrow S$$

be the dominant rational map defined by $l_1, \ldots, l_n$ (cf. Remark 3.11 (h)). By the above, we have the equality

$$(f_i)_{|S} \circ \pi = \frac{(g_i + Q)}{(h_i + Q)} \circ (l_1, \ldots, l_n) = \frac{g_i(l_1, \ldots, l_n)}{h_i(l_1, \ldots, l_n)} = \frac{(g_i + I)}{(h_i + I)} = f_i \in K(X) \tag{3.2}$$

for all $i \in \{0, \ldots, m\}$ and therefore,

$$\phi_{|S} \circ \pi = \phi : X \dashrightarrow Y. \tag{3.3}$$

Since the rational map $\phi : X \dashrightarrow Y$ is dominant, it follows that the rational map $\phi_{|S} : S \dashrightarrow Y$ is dominant, too.

We now show that $\phi_{|S} : S \dashrightarrow Y$ is a birational isomorphism. Since $L = \phi^*(K(Y))$, there clearly exist rational functions $\hat{f}_1, \ldots, \hat{f}_n \in K(Y)$ such that

$$l_i = \hat{f}_i \circ \phi$$

for $i \in \{1, \ldots, n\}$. Let $\psi : Y \dashrightarrow \mathbb{A}^n$ be the rational map defined by

$$\psi := (\hat{f}_1, \ldots, \hat{f}_n) : Y \dashrightarrow \mathbb{A}^n.$$

We claim that the rational map ψ maps into S and that $\psi : Y \dashrightarrow S$ is the inverse of the rational map $\phi_{|S} : S \dashrightarrow Y$. By definition of ψ, the composition $\psi \circ \phi$ coincides with the dominant rational map $\pi : X \dashrightarrow S$. Observe first that since ϕ was assumed to be dominant, it follows that $\psi(P) \in \overline{S} = S$ for all $P \in Y$ in the domain of definition of ψ. Moreover, we clearly have the equality

$$\psi \circ \phi_{|S} = \pi_{|S}. \tag{3.4}$$

Recall from (3.3) that the rational map $\phi_{|S} \circ \pi : X \dashrightarrow Y$ is equal to the rational map

$\phi : X \dashrightarrow Y$. Therefore, we have

$$\begin{aligned}\pi_{|S} \circ \pi &= \psi \circ \phi_{|S} \circ \pi \\ &= \psi \circ \phi \\ &= \pi.\end{aligned}$$

Since $\pi(X)$ is dense in the set S, it follows that the restriction $\pi_{|S}$ of the rational map π to S is equal to the identity map on S. By equation (3.4) this shows that $\psi \circ \phi_{|S} = \pi_{|S}$ is equal to id_S. So the rational map $\phi_{|S} : S \dashrightarrow Y$ has $\psi : Y \dashrightarrow S$ as a left inverse. Furthermore, observe that

$$\phi_{|S} \circ \psi \circ \phi_{|S} = \phi_{|S} : S \dashrightarrow Y.$$

Since $\phi_{|S} : S \dashrightarrow Y$ is dominant, it follows that the map $\phi_{|S} \circ \psi : Y \dashrightarrow Y$ is equal to the identity map id_Y. This shows that $\phi_{|S}$ is a birational isomorphism. So $S = \mathrm{Z}(Q)$ is a cross-section of the rational map ϕ, as claimed. ∎

Remarks 3.23. The following remarks use the notation of Proposition 3.21.

(a) By the previous proof it can be seen that there exist generators of the field L which are contained in the field generated by the elements $l_1, \ldots, l_n$ over K. In other words, the elements $l_1, \ldots, l_n$ generate the field $L = \phi^*(K(Y))$ over K.

(b) It follows from the proof of the proposition that every cross-section S of $\phi : X \dashrightarrow Y$ which is closed in X can be realized as $S = Z(Q)$, where Q is the ideal of relations of $l_1, \ldots, l_n$ over K for some elements $l_1, \ldots, l_n$ satisfying the conditions (a) and (b). Furthermore, for every such set of elements $l_1, \ldots, l_n$, we have $l_{1|S} = X_1 + Q, \ldots, l_{n|S} = X_n + Q$.

(c) For a given set of rational functions $l_1, \ldots, l_n \in L$ it is possible to check the conditions (a) and (b) algorithmically. By Proposition 2.21, it is clear how this can be done for the first condition (cf. [BW93], Chapter 6, Corollary 6.38). Observe that in case that $Y \subset \mathbb{A}^m$ is a quasi-affine variety, condition (b) can be checked as follows: Let $Q \trianglelefteq K[X_1, \ldots, X_n]$ be the ideal of relations of $l_1, \ldots, l_n$ over K and let $g_1, \ldots, g_m \in K[X_1, \ldots, X_n]$ and $h_1, \ldots, h_m \in K[X_1, \ldots, X_n] \setminus I$ be polynomials such that

$$\phi = \left(\frac{g_1 + I}{h_1 + I}, \ldots, \frac{g_m + I}{h_m + I} \right) : X \dashrightarrow Y.$$

Then the rational map ϕ is defined somewhere on the subvariety $\mathrm{Z}(Q)$ if and only if there exist polynomials $\hat{g}_1, \ldots, \hat{g}_m \in K[X_1, \ldots, X_n]$, $h \in K[X_1, \ldots, X_n] \setminus Q$ such that $\phi = (\hat{g}_1 + I/h + I, \ldots, \hat{g}_m + I/h + I)$, i. e. such that

$$\frac{\hat{g}_i + I}{h + I} = \frac{g_i + I}{h_i + I} \qquad \text{for all } i \in \{1, \ldots, m\}.$$

It is not hard to verify that this is equivalent to the existence of a polynomial h in $\bigcap_{i=0}^{m}((h_i)+I) : (g_i)$ which is not in Q. Note that the ideal $\bigcap_{i=0}^{m}((h_i)+I) : (g_i)$ can be found algorithmically (cf. [BW93], Chapter 6, Corollary 6.34 and Corollary 6.20). An element h with the required properties – if it exists – can then be identified by simply testing membership in Q of the elements of a generating set of the ideal $\bigcap_{i=0}^{m}((h_i)+I) : (g_i)$.

If Y is a quasi-projective variety in $\mathbb{P}^m$, then condition (b) can be checked by restricting the map ϕ to the ϕ-preimages of the quasi-affine pieces $Y \cap U_i$, $i \in \{0,\ldots,m\}$ of Y. We do not go into the details about this here.

(d) By condition (a), the elements $l_1,\ldots,l_n$ vanish at the ideal $J_L^x \trianglelefteq K(X)[Z_1,\ldots,Z_n]$. In other words, $(l_1,\ldots,l_n) \in L^n$ is a so-called L-rational point of the variety

$$Z(J_L^x) \subset \mathbb{A}^n_{\overline{K(X)}},$$

where $\overline{K(X)}$ denotes the algebraic closure of the field $K(X)$. In general, finding L-rational points of a variety algorithmically is known to be a hard (number-theoretic) problem. Nonetheless for concrete situations in practice, a solution of this problem is often possible (see the examples below).
From a conceptual viewpoint, the following deserves an explicit mention. If ϕ is a morphism, then the MQS ideal $J_L^x \trianglelefteq K(X)[Z_1,\ldots,Z_n]$ is equal to the ideal corresponding to the generic fibre of the morphism $\phi : X \longrightarrow Y$. Proposition 3.21 can thus be reformulated as follows. There exists a cross-section of a morphism $\phi : X \longrightarrow Y$ if and only if the generic fibre of ϕ contains an L-rational point.
I thank Robin Hartshorne for pointing that out to me.

(e) It seems that in general, it is not possible to check the existence of a cross-section of a rational map $\phi : X \dashrightarrow Y$ algorithmically. For special problems though, such as those situations motivated by invariant theory, there seems to be some recent (not yet published) development for finding cross-sections computationally. I thank Vladimir Popov for our conversations about this question. ♢

Examples 3.24. a) We reconsider Example 3.16 (a). So let X be the affine space $\mathbb{A}^2$ and let ϕ be the dominant rational map given by

$$\phi : X \dashrightarrow \mathbb{A}^1,\ (\xi_1,\xi_2) \longmapsto \frac{\xi_1}{\xi_2} \qquad \text{for all } (\xi_1,\xi_2) \in X \setminus \mathrm{Z}(X_2).$$

Then $L := \phi^*(\mathbb{A}^1)$ is equal to the field $K(X_1/X_2)$. By Proposition 2.21, the MQS ideal $J_L^{X_1,X_2}$ of X_1, X_2 over L is given by

$$J_L^{X_1,X_2} = \left(\left(Z_1 - \frac{X_1}{X_2}\cdot Z_2\right) : Z_2^\infty\right) = \left(Z_1 - \frac{X_1}{X_2}\cdot Z_2\right) \trianglelefteq K(X)[Z_1,Z_2].$$

It is immediate that $p(X_1/X_2, 1) = 0$ for all polynomials $p \in J_L^{X_1,X_2}$. So the elements

$$l_1 := \frac{X_1}{X_2},\ l_2 := 1 \in L$$

satisfy condition (a) of Proposition 3.21. The ideal of relations of l_1 and l_2 over K is given by $Q := (X_2 - 1) \trianglelefteq K[X_1, X_2]$. Obviously, the rational map ϕ is defined at all points of the subvariety $\mathrm{Z}(Q) \subset \mathbb{A}^2$. So it follows by Proposition 3.21 that the affine variety $\mathrm{Z}(X_2 - 1)$ is a cross-section of the rational map ϕ.
Apart from that, we clearly also have $p((X_1/X_2)^2, X_1/X_2) = 0$ for all polynomials $p \in J_L^{X_1,X_2}$. So the elements

$$l_1' := \left(\frac{X_1}{X_2}\right)^2,\ l_2' := \frac{X_1}{X_2} \in L$$

satisfy condition (a) of Proposition 3.21, too. The ideal of relations over K of the elements l_1' and l_2' is given by $Q' := (X_2^2 - X_1) \trianglelefteq K[X_1, X_2]$. It is immediate that the rational map ϕ is defined somewhere on $\mathrm{Z}(Q')$. Hence the affine variety $\mathrm{Z}(X_2^2 - X_1)$ defines another cross-section of the rational map ϕ. This shows that there may exist several different cross-sections for one and the same rational map. In particular, cross-sections of rational maps are not unique.
Now consider the elements $l_1'' := 0$, $l_2'' := 0 \in L$. Clearly, $p(0, 0) = 0$ for all $p \in J_L^{X_1,X_2}$, which shows that the elements l_1'', l_2'' satisfy condition (a) of Proposition 3.21. But obviously, the rational map ϕ is not defined on $\mathrm{Z}(X_1 - 0, X_2 - 0) = \{(0, 0)\}$. So the elements l_1'' and l_2'' do not define a cross-section of ϕ. In particular, this demonstrates that condition (b) of Proposition 3.21 is not superfluous.

b) Let X_1, X_2 be indeterminates over K, let X be the affine space $\mathbb{A}^2$ and let ϕ be the dominant morphism given by

$$\phi : X \longrightarrow \mathbb{A}^2,\ (\xi_1, \xi_2) \longmapsto (\xi_1 + \xi_2, \xi_1\xi_2).$$

We claim that the rational map ϕ does not have a cross-section.
Assume for a contradiction that there exists a cross-section of ϕ. Let $L := \phi^*(K(\mathbb{A}^2)) = K(X_1 + X_2, X_1X_2)$. By Proposition 2.21, the MQS ideal $J_L^{X_1,X_2}$ of X_1, X_2 over L is given by

$$J_L^{X_1,X_2} = (Z_1 + Z_2 - X_1 - X_2, Z_1Z_2 - X_1X_2) \trianglelefteq K(X)[Z_1, Z_2],$$

where Z_1, Z_2 are indeterminates over $K(X)$. Let $l_1, l_2 \in L$ such that condition (a) of Proposition 3.21 is satisfied. Then in particular,

$$l_1l_2 - X_1X_2 = 0 \in K(X)$$

and

$$l_1 + l_2 - X_1 - X_2 = 0 \in K(X).$$

Substituting l_1 in the first equation by $-l_2 + X_1 + X_2$ (cf. second equation) gives

$$-l_2^2 + l_2(X_1 + X_2) - X_1X_2 = 0 \in K(X).$$

This implies that l_2 is either equal to X_1 or equal to X_2. In both cases, it follows that l_2 is not contained in the field $L = K(X_1 + X_2, X_1X_2)$ – a contradiction. Hence ϕ does not have a cross-section.

c) Let $X_1, \ldots, X_5$ be indeterminates over K and let X be the affine variety

$$X := \mathrm{Z}((X_1X_4 - X_2X_3)X_5 - 1) \subset \mathbb{A}^5,$$

which can be interpreted as the set of all regular 2×2-matrices over K. We use the abbreviations $x_i := X_i + ((X_1X_4 - X_2X_3)X_5 - 1)$ for $i \in \{1, \ldots, 5\}$. Let ϕ be the dominant morphism

$$\phi : X \longrightarrow \mathbb{A}^1,\ (\xi_1, \xi_2, \xi_3, \xi_4, \xi_5) \longmapsto \frac{1}{\xi_5},$$

i. e. the morphism which maps a regular matrix to its determinant. Then $L := \phi^*(\mathbb{A}^1)$ is equal to the field $K(1/x_5)$. By Proposition 2.21, the MQS ideal $J_L^{x_1,\ldots,x_5}$ of $x_1, \ldots, x_5$ over L is given by

$$J_L^{x_1,\ldots,x_5} = \left(\left(1 - \frac{1}{x_5} \cdot Z_5, (Z_1Z_4 - Z_2Z_3)Z_5 - 1\right) : Z_5^\infty\right) \trianglelefteq K(X)[Z_1, \ldots, Z_5],$$

where $Z_1, \ldots, Z_5$ are indeterminates over $K(X)$. It is a straightforward verification that $p(1, 0, 0, 1/x_5, x_5) = 0$ for all $p \in J_L^{x_1,\ldots,x_5}$. So the elements

$$l_1 := 1,\ l_2 := 0,\ l_3 := 0,\ l_4 := 1/x_5,\ l_5 := x_5$$

satisfy condition (a) of Proposition 3.21. The ideal of relations of the elements l_1, l_2, l_3, l_4 and l_5 over K is given by $Q := (X_1 - 1, X_2, X_3, X_4X_5 - 1) \trianglelefteq K[X_1, \ldots, X_5]$. Obviously, the rational map ϕ is defined at all points of the subvariety $\mathrm{Z}(Q) \subset X$. By Proposition 3.21, it follows that the affine variety $\mathrm{Z}(X_1 - 1, X_2, X_3, X_4X_5 - 1)$ is a cross-section of the rational map ϕ. In other words, the set of all matrices of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix} \text{ with } \xi \in K^\times$$

is a cross-section of the morphism which maps a regular matrix to its determinant. $\lhd$

Proposition 3.21 provides a criterion for the existence of a cross-section of a rational map $\phi : X \dashrightarrow Y$ where X is an affine variety. As indicated before (cf. Proposition 3.18 and Corollary 3.20), it should be clear by now how this can be used to construct a criterion for the general case where X is an arbitrary variety. Nonetheless, carrying out this generalization explicitly can be rather tedious. We will hence only give a sketch-proof of the following corollary – particularly as this result will not be used in the following

chapters of this thesis.

Corollary 3.25. *Let X, Y, ϕ and L be as in Notation 3.14 with $X \subset \mathbb{P}^n$ a quasi-projective variety and $I := \mathrm{Id}^+(X) \trianglelefteq K[X_0, \ldots, X_n]$ (where $X_0, \ldots, X_n$ are indeterminates over K). Let $x_0, \ldots, x_n$ be abbreviations for $X_0 + I, \ldots, X_n + I$ and let $Z_1, \ldots, Z_n$ be indeterminates over $K(X)$. There exists a cross-section of the rational map $\phi : X \dashrightarrow Y$ if and only if there exist $i \in \{0, \ldots, n\}$ and $l_1, \ldots, l_n \in L = \phi^*(K(Y))$ satisfying the following conditions:*

(a) The intersection of X with the affine piece U_i is nonempty.

(b) For all $p \in J_L^{x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i} \trianglelefteq K(X)[Z_1, \ldots, Z_n]$ (the MQS ideal of the elements $x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i$ over L), we have

$$p(l_1, \ldots, l_n) = 0 \in K(X).$$

(c) The rational map ϕ is defined somewhere on the variety $\tilde{S} := \mathrm{Z}^+(\widetilde{Q}^h_{X_i})$, where $\widetilde{Q} \trianglelefteq K[X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ is the ideal of relations of $l_1, \ldots, l_n$ over K.

(d) The variety $\tilde{S}$ from the previous item has a nonempty intersection with the variety X, i. e. $\tilde{S} \cap X \neq \emptyset$.

In fact, if these conditions are satisfied, then the variety $\mathrm{Z}^+(\widetilde{Q}^h_{X_i}) \cap X$ is a cross-section of the rational map ϕ.

Proof (Sketch). Let $U_i \subset \mathbb{P}^n$, $i \in \{0, \ldots, n\}$ be the affine pieces of the space $\mathbb{P}^n$.
Suppose that a closed subvariety $S \subset X$ is a cross-section of the rational map ϕ. Let $i \in \{0, \ldots, n\}$ such that the intersection of S and U_i is nonempty. By Proposition 3.18, the variety $S \cap U_i$ is a cross-section of the restriction of the rational map ϕ to the subvariety $X \cap U_i$. Observe that ϕ can be regarded as a rational map ϕ_Z on the variety $Z := \overline{(X \cap U_i)} \cap U_i$, the closure of $X \cap U_i$ in U_i, and that $S \cap U_i$ is a cross-section of ϕ_Z, too. By Lemma 3.6, it follows that Z is isomorphic to an affine variety $\tilde{Z}$ via the map $\psi_i : U_i \longrightarrow \mathbb{A}^n$. Applying Proposition 3.21 to this affine variety $\tilde{Z}$, the subvariety $\overline{\psi_i(S \cap U_i)}$ and the rational map $\phi_Z \circ (\psi_i^{-1})_{|\tilde{Z}}$ yields elements which satisfy conditions (a) and (b) of Proposition 3.21. It then can be checked that translating this back to the subvariety Z via the isomorphism induced by ψ_i gives elements $l_1, \ldots, l_n \in L$ which satisfy conditions (b) and (c). Furthermore, it can be verified that the intersection of the subvariety defined by these elements with X is equal to S. So condition (d) is satisfied, too.

The converse can be proved with very similar methods, i. e. with the method of reducing the general case to the affine one and applying Proposition 3.21. We do not go into the details about this here. ∎

Example 3.26. Let X_0, X_1, X_2, X_3 be indeterminates over K and let X be the projective variety

$$X := \mathrm{Z}^+(X_0X_1 - X_2X_3) \subset \mathbb{P}^3,$$

a so-called quadric surface in $\mathbb{P}^3$. As before, let x_0, x_1, x_2, x_3 be abbreviations for $X_0 + (X_0X_1 - X_2X_3), \ldots, X_3 + (X_0X_1 - X_2X_3)$. Let ϕ be the dominant rational map given by

$$\phi : X \longrightarrow \mathbb{A}^1,\ (\xi_0 : \xi_1 : \xi_2 : \xi_3) \longmapsto \frac{\xi_2}{\xi_0} \qquad \text{for all } (\xi_0 : \xi_1 : \xi_2 : \xi_3) \in X \setminus \mathrm{Z}^+(X_0).$$

In the following, we aim to find a cross-section of ϕ. According to Corollary 3.25, let $L := \phi^*(\mathbb{A}^1) = K(x_2/x_0)$. Note that the intersection $X \cap U_i$ is nonempty for all $i \in \{0, \ldots, 3\}$. Let $i := 0$. By Proposition 2.21, the MQS ideal of the elements $x_1/x_0, x_2/x_0, x_3/x_0$ over L is given by

$$J_L^{x_1/x_0, x_2/x_0, x_3/x_0} = (Z_2 - x_2/x_0, Z_1 - Z_2Z_3) \trianglelefteq K(X)[Z_1, Z_2, Z_3],$$

where $Z_1, \ldots, Z_3$ are indeterminates over $K(X)$. Obviously, we have $p(x_2/x_0, x_2/x_0, 1) = 0$ for all $p \in J_L^{x_1/x_0, x_2/x_0, x_3/x_0}$. So the elements

$$l_1 := x_2/x_0,\ l_2 := x_2/x_0,\ l_3 := 1 \in L$$

satisfy condition (b) of Corollary 3.25. The homogenization with respect to X_0 of the ideal of relations of $l_1, \ldots, l_3$ is given by $(X_1 - X_2, X_3 - X_0) \trianglelefteq K[X_0, X_1, X_2, X_3]$. Clearly, the rational map ϕ is defined somewhere on the projective variety $\mathrm{Z}^+(X_1 - X_2, X_3 - X_0)$. So condition (c) is satisfied, too. Since $\mathrm{Z}^+(X_1 - X_2, X_3 - X_0)$ is contained in the projective variety X – which gives condition (d) – it follows from the previous Corollary 3.25 that $S := \mathrm{Z}^+(X_1 - X_2, X_3 - X_0)$ is a cross-section of the rational map ϕ. In fact, it is not hard to verify directly that $\phi_{|S} : S \longrightarrow Y$ is a birational isomorphism, indeed. $\triangleleft$

3.3 Algorithmic Aspects of Cross-Sections of Rational Maps

In the second chapter, we have seen various algorithmic methods for the solution of problems in field theory. These methods all used the field-ideal correspondence of Lemma 2.26 as a central tool. In what follows, we will show how some of these problems in field theory can also be solved algorithmically with methods based on the theory of cross-sections of rational maps.

Hubert and Kogan have used concepts of the theory of cross-sections of rational maps for testing membership in a field of invariants (cf. [HK07]). We will present an algorithm based on cross-sections of rational maps for testing membership in an arbitrary field and finding – if applicable – a representation of the respective element in certain generators of the field. Since cross-sections of rational maps do not always exist, the algorithm can not be applied in all situations. Nonetheless, if an appropriate cross-section of a certain rational map exists and is given, then the algorithm presented below is a valuable tool.

Let $K(x_1,\dots,x_n)$ be a finitely generated field extension over K and let $I \trianglelefteq K[X_1,\dots,X_n]$ (where $X_1,\dots,X_n$ are indeterminates over K) be the ideal of relations of $x_1,\dots,x_n$ over K. As before, $\underline{x}$ shall be an abbreviation for $x_1,\dots,x_n$. Let L be a subfield of $K(x_1,\dots,x_n)$ given by

$$L := K(f_1,\dots,f_m) \subset K(x_1,\dots,x_n)$$

with $f_1,\dots,f_m \in K(x_1,\dots,x_n)$ and let $J \trianglelefteq K[Y_1,\dots,Y_m]$ (where $Y_1,\dots,Y_n$ are indeterminates over K) be the ideal of relations of the elements $f_1,\dots,f_m$ over K. It is our aim to test whether an element $f \in K(x_1,\dots,x_n)$ is contained in L or not. For this, we define varieties X and Y by

$$X := \mathrm{Z}(I) \subset \mathbb{A}^n \text{ and}$$
$$Y := \mathrm{Z}(J) \subset \mathbb{A}^m$$

and a rational map $\phi : X \dashrightarrow Y$ by

$$\phi := (f_1,\dots,f_m) : X \dashrightarrow Y.$$

Note that by Remark 3.11 (h), the rational map $\phi : X \dashrightarrow Y$ is well-defined and dominant. Moreover, by Remark 3.9 (f), the field $K(X)$ is isomorphic to the field $K(x_1,\dots,x_n) \cong \mathrm{Quot}(K[X_1,\dots,X_n]/I)$. Finally, observe that the field $\phi^*(K(Y))$ is equal to $K(f_1,\dots,f_m) = L$ (cf. Remark 3.13 (c)).

The algorithm below provides a way to test membership in the field L. As input data the algorithm requires a cross-section of the rational map $\phi : X \dashrightarrow Y$. More precisely, it requires elements $l_1,\dots,l_n \in L$ which satisfy the conditions of Proposition 3.21 (applied to X, Y and ϕ). If applicable, the algorithm computes a representation of the respective element in $l_1,\dots,l_n$. Note that the latter perfectly makes sense since L is generated by $l_1,\dots,l_n$ (cf. Remark 3.23 (a)).

Algorithm 3.27. (Testing field membership and finding a representation)

Input: A field extension $K(x_1,\dots,x_n)$ over the field K given by the ideal of relations $I \trianglelefteq K[X_1,\dots,X_n]$ of the elements $x_1,\dots,x_n$ over K, a subfield $L = K(f_1,\dots,f_m)$ of $K(x_1,\dots,x_n)$ with $f_1,\dots,f_m \in K(x_1,\dots,x_n)$. Moreover, a cross-section S of the dominant rational map $\phi := (f_1,\dots,f_m) : \mathrm{Z}(I) \dashrightarrow Y$ with $Y \subset \mathbb{A}^m$ an appropriate variety, given by elements $l_1,\dots,l_n \in L$ in the sense of Proposition 3.21, and an element $f(\underline{x}) = g(\underline{x})/h(\underline{x}) \in K(x_1,\dots,x_n)$ with $h \in K[X_1,\dots,X_n]$ and $g \in K[X_1,\dots,X_n] \setminus I$, whose membership in L shall be tested.

Output: If $f \in L$, then $(\hat{g},\hat{h})$, where $\hat{g},\hat{h} \in K[X_1,\dots,X_n]$ are polynomials such that

$\hat{h}(l_1, \ldots, l_n) \neq 0 \in K(x_1, \ldots, x_n)$ and

$$f = \frac{\hat{g}(l_1, \ldots, l_n)}{\hat{h}(l_1, \ldots, l_n)}.$$

Else FALSE.

(1) Compute generators $\hat{h}_1, \ldots, \hat{h}_s \in K[X_1, \ldots, X_n]$ of the ideal

$$((h) + I) : (g) \trianglelefteq K[X_1, \ldots, X_n].$$

(2) If for some $i \in \{1, \ldots, s\}$ the element $\hat{h}_i(l_1, \ldots, l_n) \in K(x_1, \ldots, x_n)$ is not equal to zero, then set $\hat{h} := \hat{h}_i$ and find $\hat{g} \in K[X_1, \ldots, X_n]$ such that

$$\hat{h} \cdot g = \hat{g} \cdot h + r$$

for some $r \in I$ (see Remark 3.28 (b)).
Else return FALSE.

(3) If

$$\hat{h}(l_1, \ldots, l_n) \cdot g(\underline{x}) - \hat{g}(l_1, \ldots, l_n) \cdot h(\underline{x}) = 0 \in K(x_1, \ldots, x_n)$$

return $(\hat{g}, \hat{h})$.
Else return FALSE.

Remarks 3.28. (a) Note that the ideal $H := ((h) + I) : (g) \trianglelefteq K[X_1, \ldots, X_n]$ of the first step of the algorithm can be interpreted as the set of all possible representatives of the denominator of the element $f = g(\underline{x})/h(\underline{x})$. More precisely, if $\hat{h}$ lies in $H \setminus I$, then there exists $\hat{g} \in K[X_1, \ldots, X_n]$ such that $g(\underline{x})/h(\underline{x}) = \hat{g}(\underline{x})/\hat{h}(\underline{x})$.

(b) In step (2) of the algorithm, an element $\hat{g}$ such that $\hat{h} \cdot g = \hat{g} \cdot h + r$ (for some $r \in I$) can be found by testing membership of $\hat{h} \cdot g$ in the ideal $(h) + I \trianglelefteq K[X_1, \ldots, X_n]$ with the Extended Buchberger Algorithm (cf. [BW93], Chapter 5, Section 5.6). For, if $\{p_1, \ldots, p_s\} \subset I$ is a given set of generators of the ideal I, then an application of this algorithm yields elements $\hat{g}, q_1, \ldots, q_s \in K[X_1, \ldots, X_n]$ such that $\hat{h} \cdot g = \hat{g} \cdot h + \sum_{i=1}^{s} q_i \cdot p_i$.

(c) If $K[x_1, \ldots, x_n]$ is a unique factorization domain, then the first step of the algorithm can be replaced by cancelling out common factors of $g(\underline{x})$ and $h(\underline{x})$ until the new numerator $\hat{g}(\underline{x}) \in K[x_1, \ldots, x_n]$ and the new denominator $\hat{h}(\underline{x}) \in K[x_1, \ldots, x_n]$ are coprime, since then

$$((h) + I) : (g) = ((\hat{h}) + I).$$

On the other hand, cancelling out common factors usually is a nontrivial task. Hence for algorithmic purposes it seems to be more convenient to compute the colon ideal

$((h) + I) : (g)$ directly. Nonetheless, this alternative method is often useful when the algorithm is carried out by hand. ♢

The idea of the algorithm is based on the following characterization of the field L: Using the notation of the algorithm, a rational function on $X := Z(I) \subset K^n$ is contained in L if and only if there exists an open subset of X contained in the domain of definition of f and in the domain of definition of ϕ such that its intersection with the cross-section S is nonempty and such that f is constant on the fibres of ϕ in this open subset. The correctness of this characterization will be a consequence of the following discussion. It should be mentioned that the following discussion is not a complete proof of correctness, it is a geometric interpretation of Algorithm 3.27. For a complete proof, see below.

First of all note that since S is a cross-section of ϕ, the domain of definition of the rational map ϕ has a nonempty intersection with S.
In steps (1) and (2), the algorithm checks whether the rational function $f \in K(X)$ is defined somewhere on the cross-section S, i. e. whether the domain of definition of f has a nonempty intersection with S. If this is not the case, then FALSE is returned since in this case f cannot be contained in L.
Otherwise, step (3) is executed, which may be best described as some kind of transformation which maps f to the rational function $f(l_1, \ldots, l_n) = f_{|S} \circ \pi \in K(X)$. Recall that π can be interpreted as a projection which maps all fibres F of $\phi_{|\mathcal{O}}$, for some open subset $\mathcal{O} \subset X$ with $\mathcal{O} \cap S \neq \emptyset$, to a distinguished point of the fibre F, namely to the single point in $F \cap S$ (cf. the discussion before Proposition 3.17). It follows that the rational function $f_{|S} \circ \pi$ is constant on the fibres of ϕ in some open subset of X which has a nonempty intersection with S. Note that if f has already been constant on the fibres of $\phi_{|\mathcal{O}'}$ for some open subset $\mathcal{O}' \subset X$ with $\mathcal{O}' \cap S \neq \emptyset$, then $f_{|S} \circ \pi_{|\mathcal{O}'} = f_{|\mathcal{O}'}$, meaning that $f_{|S} \circ \pi = f$. Therefore, we have $f = f_{|S} \circ \pi$ if and only if there exists an open subset of X contained in the domain of definition of f and in the domain of definition of ϕ such that its intersection with S is nonempty and such that f is constant on the fibres of ϕ in this open subset.
Note that every element of L by definition can be written as $g \circ \phi$ for some $g \in K(Y)$ and thus is constant on the fibres of $\phi_{|\mathcal{O}'}$ for some open subset $\mathcal{O}' \subset X$ with $\mathcal{O}' \cap S \neq \emptyset$. On the other hand, if the rational function $f \in K(X)$ is constant on the fibres of $\phi_{|\mathcal{O}'}$ for some open subset $\mathcal{O}' \subset X$ contained in the domain of definition of f and in the domain of definition of ϕ with $\mathcal{O}' \cap S \neq \emptyset$, then $f = f_{|S} \circ \pi \in L$ is obviously contained in L. Summarizing this, the rational function f is contained in L if and only if there exists an open subset of X contained in the domain of definition of f and in the domain of definition of ϕ such that its intersection with S is nonempty and such that f is constant on the fibres of ϕ in this open subset.
Coming back to the algorithm, it is thus checked in step (3) whether f is mapped to itself or not, i. e. whether we have $f = f(l_1, \ldots, l_n)$ or not. As explained above, this is the case if and only if f is contained in L.

Proof of Correctness. Let $X := \mathrm{Z}(I) \subset \mathbb{A}^n$ and let $Q \trianglelefteq K[X_1, \ldots, X_n]$ be the ideal of relations of the elements $l_1, \ldots, l_n$ over K, that means $S := \mathrm{Z}(Q) \subset X$ is a cross-section

of the rational map $\phi : X \dashrightarrow Y$ (cf. Proposition 3.21).
Suppose that the algorithm terminates with $(\hat{g}, \hat{h})$. It follows by steps (2) and (3) that $\hat{h}(l_1, \ldots, l_n) \neq 0 \in K(x_1, \ldots, x_n)$ and $\hat{h}(l_1, \ldots, l_n) \cdot g(\underline{x}) - \hat{g}(l_1, \ldots, l_n) \cdot h(\underline{x}) = 0 \in K(x_1, \ldots, x_n)$. But this means that

$$f = \frac{g(\underline{x})}{h(\underline{x})} = \frac{\hat{g}(l_1, \ldots, l_n)}{\hat{h}(l_1, \ldots, l_n)} \in L,$$

as desired.

Conversely, suppose that $f \in K(x_1, \ldots, x_n)$ is an element of L. We show that in this case the algorithm terminates with an output which is not equal to FALSE. By the argument a few lines above, this proves the correctness of the algorithm.
Since the restriction map $\theta : L \longrightarrow K(S)$ of the rational functions in L to the cross-section S is a well-defined isomorphism of fields (cf. Proposition 3.17), there are polynomials $\tilde{g} \in K[X_1, \ldots, X_n]$, $\tilde{h} \in K[X_1, \ldots, X_n] \setminus Q$ such that $\tilde{g}(\underline{x})/\tilde{h}(\underline{x}) = g(\underline{x})/h(\underline{x}) \in K(x_1, \ldots, x_n)$. It follows that there exists an element $r \in I$ such that

$$\tilde{h} \cdot g = \tilde{g} \cdot h + r \in K[X_1, \ldots, X_n].$$

This means that the polynomial $\tilde{h}$ is contained in the colon ideal $((h) + I) : (g)$. Furthermore, since the polynomial $\tilde{h}$ is not contained in Q, the ideal of relations of $l_1, \ldots, l_n$ over K, it follows that

$$\tilde{h}(l_1, \ldots, l_n) \neq 0 \in K(x_1, \ldots, x_n).$$

Therefore, at least one of $\hat{h}_1, \ldots, \hat{h}_s$, the generators of the colon ideal $((h) + I) : (g)$, does not vanish at $l_1, \ldots, l_n$. In particular, this means that the algorithm does not return FALSE in the second step.
Let $\hat{h} \in \{\hat{h}_1, \ldots, \hat{h}_s\}$ such that $\hat{h}(l_1, \ldots, l_n) \neq 0 \in K(x_1, \ldots, x_n)$ and let $\hat{g} \in K[X_1, \ldots, X_n]$ such that $\hat{h} \cdot g = \hat{g} \cdot h + \hat{r}$ for some $\hat{r} \in I$. Then we have the equality

$$\frac{g(\underline{x})}{h(\underline{x})} = \frac{\hat{g}(\underline{x})}{\hat{h}(\underline{x})}.$$

By definition of the MQS ideal $J_L^{\underline{x}}$ of $x_1, \ldots, x_n$ over L, the polynomial

$$\hat{g}(\underline{Z}) - \frac{g(\underline{x})}{h(\underline{x})} \cdot \hat{h}(\underline{Z}) \in L[Z_1, \ldots, Z_n]$$

lies in $J_L^{\underline{x}}$. It follows that the rational function $\hat{g}(l_1, \ldots, l_n) - g(\underline{x})/h(\underline{x}) \cdot \hat{h}(l_1, \ldots, l_n) \in K(x_1, \ldots, x_n)$ is equal to zero (cf. Proposition 3.21 (a)). Thus the algorithm does not terminate with FALSE, as desired. ∎

Examples 3.29. (a) Let X_1, X_2, X_3 be indeterminates over K and let L be the subfield of $K(X_1, X_2, X_3)$ defined by $L := K(X_2/X_1, X_3/X_1)$. We use Algorithm 3.27 to test

whether the element

$$\frac{X_1X_2}{X_3^2} \in K(X_1, X_2, X_3)$$

lies in the subfield $L \leq K(X_1, X_2, X_3)$ or not. We first have to specify the input data. So let $g := X_1X_2 \in K[X_1, X_2, X_3]$ and $h := X_3^2 \in K[X_1, X_2, X_3]$. It is a straightforward verification that the elements

$$l_1 := 1,\ l_2 := \frac{X_2}{X_1},\ l_3 := \frac{X_3}{X_1} \in L$$

satisfy the conditions (a) and (b) of Proposition 3.21 with respect to the dominant rational map

$$\phi := \left(\frac{X_2}{X_1}, \frac{X_3}{X_1}\right) : \mathbb{A}^3 \dashrightarrow \mathbb{A}^2.$$

So we can apply Algorithm 3.27 to the data $K(X_1, X_2, X_3)$, L, (l_1, l_2, l_3) and (g, h). Obviously, the elements X_1X_2 and $X_3^2 \in K[X_1, \ldots, X_n]$ are coprime. It hence follows that the colon ideal $(X_3^2) : (X_1X_2) \trianglelefteq K[X_1, X_2, X_3]$ is equal to $(X_3^2) \trianglelefteq K[X_1, X_2, X_3]$. Evaluating the generator $\hat{h} := X_3^2 \in K[X_1, X_2, X_3]$ of this ideal at $(l_1, l_2, l_3) \in L^3$ gives

$$X_3^2(1, X_2/X_1, X_3/X_1) = (X_3/X_1)^2 \neq 0 \in K(X_1, X_2, X_3).$$

Let $\hat{g}$ be the polynomial $\hat{g} := X_1X_2$. Then $\hat{h}/\hat{g} = h/g$ and

$$\begin{aligned}
&\hat{h}(l_1, l_2, l_3) \cdot g - \hat{g}(l_1, l_2, l_3) \cdot h \\
&\quad = X_3^2 \left(1, \frac{X_2}{X_1}, \frac{X_3}{X_1}\right) \cdot X_1X_2 - X_1X_2 \left(1, \frac{X_2}{X_1}, \frac{X_3}{X_1}\right) \cdot X_3^2 \\
&\quad = \left(\frac{X_3}{X_1}\right)^2 \cdot X_1X_2 - \frac{X_2}{X_1} \cdot X_3^2 \\
&\quad = 0 \in K(X_1, X_2, X_3),
\end{aligned}$$

which implies that the element $(X_1X_2)/X_3^2$ satisfies

$$\frac{X_1X_2}{X_3^2} = \frac{X_2/X_1}{(X_3/X_1)^2} \in L.$$

(b) The next example has its origins in invariant theory. It makes use of some invariant theoretical terms which have not been defined yet. Nonetheless, it should be possible to understand the following intuitively. In any case, an introduction to invariant theory is given in the next section of this chapter.
Let $X_{1,1}, X_{1,2}, X_{2,1}, X_{2,2}, X_{3,1}, X_{3,2}, X_{4,1}, X_{4,2}$ be indeterminates over K and let L be the subfield of $K(X_{1,1}, X_{1,2}, X_{2,1}, X_{2,2}, X_{3,1}, X_{3,2}, X_{4,1}, X_{4,2})$ generated over K by the elements

$$\begin{aligned}
f_1 &:= X_{1,1}X_{3,2} - X_{3,1}X_{1,2},\ f_2 := X_{1,1}X_{4,2} - X_{4,1}X_{1,2}, \\
f_3 &:= X_{2,1}X_{3,2} - X_{3,1}X_{2,2},\ f_4 := X_{2,1}X_{4,2} - X_{4,1}X_{2,2}.
\end{aligned}$$

Note that the elements $f_1, \ldots, f_4$ are invariants under the linear action of the group SL_2 on $(\mathbb{A}^2)^4$ by componentwise multiplication. The polynomial $(X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2})$ is an invariant under that action of SL_2, too. We use Algorithm 3.27 to show that it is actually already contained in the field generated by the invariants f_1, f_2, f_3 and f_4 over K, i. e. that

$$f := (X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2})$$

lies in the field L. Let $g := (X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2})$ and $h := 1$, i. e. $f = g/h$. It is a straightforward verification that the elements

$$\begin{aligned} l_{1,1} &:= f_1,\ l_{2,1} := f_3,\ l_{3,1} := 0,\ l_{4,1} := -1, \\ l_{1,2} &:= f_2,\ l_{2,2} := f_4,\ l_{3,2} := 1,\ l_{4,2} := 0 \ \in L \end{aligned}$$

satisfy the conditions (a) and (b) of Proposition 3.21 with respect to the dominant morphism

$$\phi := (f_1, f_2, f_3, f_4) : \mathbb{A}^8 \longrightarrow \mathbb{A}^4.$$

We can hence apply Algorithm 3.27 to the data $K(X_{1,1}, \ldots, X_{4,2})$, L, $(l_{1,1}, \ldots, l_{4,2})$ and (g, h). With polynomials $\hat{g} := (X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2})$ and $\hat{h} := 1$ in the polynomial ring $K[X_{1,1}, X_{1,2}, X_{2,1}, X_{2,2}, X_{3,1}, X_{3,2}, X_{4,1}, X_{4,2}]$, it can moreover be verified that

$$\begin{aligned} &\hat{h}(l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l_{3,1}, l_{3,2}, l_{4,1}, l_{4,2}) \cdot g - \hat{g}(l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l_{3,1}, l_{3,2}, l_{4,1}, l_{4,2}) \cdot h \\ &\quad = 1(f_1, f_2, f_3, f_4, 0, 1, -1, 0) \cdot (X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2}) \\ &\qquad - ((X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2}))(f_1, f_2, f_3, f_4, 0, 1, -1, 0) \cdot 1 \\ &\quad = (X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2}) - (f_1 f_4 - f_3 f_2) \\ &\quad = (X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2}) \\ &\qquad - (X_{1,1}X_{3,2} - X_{3,1}X_{1,2})(X_{2,1}X_{4,2} - X_{4,1}X_{2,2}) \\ &\qquad + (X_{2,1}X_{3,2} - X_{3,1}X_{2,2})(X_{1,1}X_{4,2} - X_{4,1}X_{1,2}) \\ &\quad = 0. \end{aligned}$$

It follows that the element $(X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2})$ satisfies the equation[§]

$$\begin{aligned} &(X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2}) \\ &\quad = (X_{1,1}X_{3,2} - X_{3,1}X_{1,2}) \cdot (X_{2,1}X_{4,2} - X_{4,1}X_{2,2}) \\ &\qquad - (X_{2,1}X_{3,2} - X_{3,1}X_{2,2}) \cdot (X_{1,1}X_{4,2} - X_{4,1}X_{1,2}). \end{aligned}$$

In particular, this shows that the element $(X_{1,1}X_{2,2} - X_{2,1}X_{1,2}) \cdot (X_{3,1}X_{4,2} - X_{4,1}X_{3,2})$ lies in the field $K(f_1, f_2, f_3, f_4)$. ◁

[§]In the literature, this equation is known as one of the Grassmann-Plücker-relations (cf. e. g. [DK02], Chapter 4, Theorem 4.4.5).

Given a cross-section $S = \mathrm{Z}(Q)$ of a rational map $\phi : X \dashrightarrow Y$, it would be nice – according to the input specification of Algorithm 3.27 – to have a method for explicitly finding elements $l_1, \ldots, l_n$ in the sense of Proposition 3.21. Recall that the restrictions of the elements $l_1, \ldots, l_n$ to the subvariety S are equal to $X_1 + Q, \ldots, X_n + Q$. Often, this property is sufficient for a determination of the elements $l_1, \ldots, l_n$. Nonetheless in some cases, the next proposition might be helpful.

Proposition 3.30. *Let X, Y, ϕ and L be as in Notation 3.14 with $X \subset \mathbb{A}^n$ an affine variety. Let $X_1, \ldots, X_n$ be indeterminates over K and let $Q \trianglelefteq K[X_1, \ldots, X_n]$ be an ideal such that $\mathrm{Z}(Q) \subset \mathbb{A}^n$ is a cross-section of $\phi : X \dashrightarrow Y$. Then one of the minimal primes over the ideal*

$$(Q)_{L[Z_1,\ldots,Z_n]} + (J_L^x \cap L[Z_1, \ldots, Z_n]) \trianglelefteq L[Z_1, \ldots, Z_n]$$

(where $Z_1, \ldots, Z_n$ are indeterminates over $K(X)$) is of the form $(Z_1 - l_1, \ldots, Z_n - l_n) \trianglelefteq L[Z_1, \ldots, Z_n]$ such that $l_1, \ldots, l_n \in L$ satisfy the conditions (a) and (b) of Proposition 3.21 and the ideal of relations of $l_1, \ldots, l_n$ over K is equal to Q.

Recall from Proposition 2.21 that there is an algorithmic way to find generators of the MQS ideal $J_L^x \cap L[Z_1, \ldots, Z_n]$ (see e. g. [BW93], Chapter 6, Corollary 6.38). It follows by the proposition that one of the finitely many ideals of a primary decomposition of the ideal $(Q)_{L[Z_1,\ldots,Z_n]} + (J_L^x \cap L[Z_1, \ldots, Z_n])$ must be $(Z_1 - l_1, \ldots, Z_n - l_n)$-primary, i. e. its radical is equal to $(Z_1 - l_1, \ldots, Z_n - l_n)$ (cf. [Eis95], Chapter 3, Theorem 3.1 and Theorem 3.10). Note that this could be used to find $l_1, \ldots, l_n$ algorithmically.

Proof. Let $l_1, \ldots, l_n \in L = \phi^*(K(Y))$ such that condition (a) and condition (b) of Proposition 3.21 are satisfied and the ideal Q is equal to the ideal of relations of $l_1, \ldots, l_n$ over K (cf. Remark 3.23 (b)). We show that the prime ideal $(Z_1 - l_1, \ldots, Z_n - l_n) \trianglelefteq L[Z_1, \ldots, Z_n]$ is minimal prime over $(Q)_{L[Z_1,\ldots,Z_n]} + (J_L^x \cap L[Z_1, \ldots, Z_n])$.
From condition (a) of Proposition 3.21 it follows that

$$p(l_1, \ldots, l_n) = 0 \qquad \text{for all } p \in (Q)_{L[Z_1,\ldots,Z_n]} + (J_L^x \cap L[Z_1, \ldots, Z_n])$$

and hence $(Z_1 - l_1, \ldots, Z_n - l_n) \supset (Q)_{L[Z_1,\ldots,Z_n]} + (J_L^x \cap L[Z_1, \ldots, Z_n])$. Let $J \trianglelefteq L[Z_1, \ldots, Z_n]$ be a prime ideal such that

$$(Q)_{L[Z_1,\ldots,Z_n]} + (J_L^x \cap L[Z_1, \ldots, Z_n]) \subset J \subset (Z_1 - l_1, \ldots, Z_n - l_n) \trianglelefteq L[Z_1, \ldots, Z_n].$$

In the following we show that $J = (Z_1 - l_1, \ldots, Z_n - l_n)$. Let $i \in \{1, \ldots, n\}$. Since the restriction of the elements in the field L to the cross-section S is well-defined (cf. Proposition 3.17), there exist polynomials $g_i \in K[X_1, \ldots, X_n]$ and $h_i \in K[X_1, \ldots, X_n] \setminus Q$

such that

$$l_i = \frac{(g_i + I)}{(h_i + I)} \in K(X).$$

By definition of the MQS ideal J_L^x, this implies

$$g_i(Z_1, \ldots, Z_n) - l_i \cdot h_i(Z_1, \ldots, Z_n) \in J_L^x \cap L[Z_1, \ldots, Z_n].$$

Since the elements $l_1, \ldots, l_n$ satisfy condition (a) of Proposition 3.21, it follows that the polynomial $g_i(Z_1, \ldots, Z_n) - Z_i \cdot h_i(Z_1, \ldots, Z_n) \in K[Z_1, \ldots, Z_n]$ is contained in Q, the ideal of relations of $l_1, \ldots, l_n$ over K. The equation

$$\begin{aligned}(Z_i - l_i) \cdot h_i(Z_1, \ldots, Z_n) = {} & (Z_i \cdot h_i(Z_1, \ldots, Z_n) - g_i(Z_1, \ldots, Z_n)) \\ & + (g_i(Z_1, \ldots, Z_n) - l_i \cdot h_i(Z_1, \ldots, Z_n))\end{aligned}$$

hence implies that the element $(Z_i - l_i) \cdot h_i(Z_1, \ldots, Z_n) \in L[Z_1, \ldots, Z_n]$ is contained in the ideal $(Q)_{L[Z_1,\ldots,Z_n]} + (J_L^x \cap L[Z_1, \ldots, Z_n]) \trianglelefteq L[Z_1, \ldots, Z_n]$. In particular, it is contained in the prime ideal J. Therefore, either $Z_i - l_i$ or $h_i(Z_1, \ldots, Z_n)$ must be contained in J. It can be verified by definition that the ideal $Q \trianglelefteq K[Z_1, \ldots, Z_n]$ is equal to the intersection

$$Q = (Z_1 - l_1, \ldots, Z_n - l_n) \cap K[Z_1, \ldots, Z_n],$$

which obviously contains the intersection $J \cap K[Z_1, \ldots, Z_n]$. So since by assumption, the polynomial $h_i(Z_1, \ldots, Z_n) \in K[Z_1, \ldots, Z_n]$ is not contained in the ideal Q, it is also not contained in the ideal J. It follows that the polynomial $Z_i - l_i \in L[Z_1, \ldots, Z_n]$ must be contained in J. Since $i \in \{1, \ldots, n\}$ was chosen arbitrarily, this shows

$$J \supset (Z_1 - l_1, \ldots, Z_n - l_n).$$

So in fact, the ideal $(Z_1 - l_1, \ldots, Z_n - l_n)$ is minimal prime over the ideal $(Q)_{L[Z_1,\ldots,Z_n]} + (J_L^x \cap L[Z_1, \ldots, Z_n])$, as asserted. ∎

Example 3.31. Let X_1, X_2 be indeterminates over K, let X be the affine 2-space $\mathbb{A}^2$ and let ϕ be the dominant rational map given by

$$\phi : X \dashrightarrow \mathbb{A}^1,\ (\xi_1, \xi_2) \longmapsto \frac{\xi_1}{\xi_2} \qquad \text{for all } (\xi_1, \xi_2) \in \mathbb{A}^2 \setminus \mathrm{Z}(X_2).$$

Then $L := \phi^*(K(\mathbb{A}^1))$ is equal to the field $K(X_1/X_2)$. By Example 3.24 (a), the elements $l_1 := X_1/X_2$, $l_2 := 1$ satisfy the conditions (a) and (b) of Proposition 3.21. Hence the ideal of relations of l_1 and l_2 over K, namely $(Z_2 - 1) \trianglelefteq K[Z_1, Z_2]$ (where Z_1, Z_2 are indeterminates over $K(X)$) defines a cross-section of the rational map ϕ. By Proposition

2.21, it can be verified that

$$\begin{aligned}(Z_2-1)_{L[Z_1,Z_2]}+(J_L^{X_1,X_2}\cap L[Z_1,Z_2]) &= (Z_2-1)_{L[Z_1,Z_2]}+\left(Z_1-\frac{X_1}{X_2}Z_2\right)_{L[Z_1,Z_2]}\\ &= \left(Z_1-\frac{X_1}{X_2},Z_2-1\right)_{L[Z_1,Z_2]}\\ &= (Z_1-l_1,Z_2-l_2)_{L[Z_1,Z_2]}.\end{aligned}$$

Furthermore by Example 3.24 (a), the elements $l_1' := (X_1/X_2)^2$, $l_2' := X_1/X_2$ satisfy the conditions (a) and (b) of Proposition 3.21, too, that means the ideal of relations of l_1' and l_2' over K, namely $(Z_2^2-Z_1)\trianglelefteq K[Z_1,Z_2]$, defines another cross-section of the rational map ϕ. By Proposition 2.21, it follows that

$$\begin{aligned}(Z_2^2-Z_1)_{L[Z_1,Z_2]}+(J_L^{X_1,X_2}\cap L[Z_1,Z_2]) &= (Z_2^2-Z_1)_{L[Z_1,Z_2]}+\left(Z_1-\frac{X_1}{X_2}Z_2\right)_{L[Z_1,Z_2]}\\ &= \left(Z_1-\frac{X_1}{X_2}\cdot Z_2, Z_2^2-\frac{X_1}{X_2}\cdot Z_2\right)_{L[Z_1,Z_2]},\end{aligned}$$

a zero-dimensional ideal which can easily be checked to be contained in the prime ideal $(Z_1-l_1',Z_2-l_2')\trianglelefteq L[Z_1,Z_2]$. Note that this inclusion actually is strict. This follows for example from the fact that

$$\left(Z_1-\frac{X_1}{X_2}\cdot Z_2, Z_1^2-\frac{X_1}{X_2}\cdot Z_2\right)\subset (Z_1,Z_2)\trianglelefteq L[Z_1,Z_2].$$

In particular, this last inclusion shows that – with the notation of Proposition 3.30 – there may exist $l_1,\ldots,l_n\in L$ such that $(Z_1-l_1,\ldots,Z_n-l_n)$ is minimal over $(Q)_{L[Z_1,\ldots,Z_n]}+(J_L^x\cap L[Z_1,\ldots,Z_n])$, but which do not define a cross-section in the sense of Proposition 3.21. ◁

Remark 3.32. In [HK07], Hubert and Kogan defined the notion of a cross-section of degree d with $d\in\mathbb{N}$. We do not go into the details about their definition of cross-sections here – for those readers who know the paper [HK07], we just want to note that cross-sections of rational maps are not necessarily cross-sections of degree 1 in the sense of [HK07]. This can be seen for example by Example 3.31.
In this context, it should be mentioned that Algorithm 3.27 seems to be similar to the idea of a replacement invariant as defined in [HK07]. Yet, the idea of a replacement invariant does not work in general. This can be seen for instance from Example 3.31. ♢

We close this section with a remark which is often useful for algorithmic problems. It summarizes some field theoretic properties in the context of cross-sections. Although most of the following is almost obvious, we have included this remark for creating a reference for the next chapter.

Remark 3.33. Let X, Y, ϕ and L be as in Notation 3.14. If S is a cross-section of the rational map $\phi : X \dashrightarrow Y$, then the fields $K(S)$ and L are K-isomorphic via restricting the rational functions in L to S (cf. Proposition 3.17). This implies that all properties, which are invariant under K-isomorphisms of fields, such as the transcendental degree over K, rationality, etc. coincide. In particular, if $X \subset \mathbb{A}^n$ is affine and S is equal to $Z(Q)$ for some prime ideal $Q \trianglelefteq K[X_1, \ldots, X_n]$ then $\operatorname{trdeg}(K(S)) = \operatorname{trdeg}_K(\operatorname{Quot}(K[X_1, \ldots X_n]/Q)) = \dim(Q)$ and hence

$$\operatorname{trdeg}_K(L) = \dim(Q).$$

Since there are algorithms to compute the dimension of the ideal Q, that provides a way to compute the transcendental degree of the field L over K.

Sometimes, the isomorphism $K(S) \cong L$ can be used to check whether a given set $\{l_1, \ldots, l_n\}$ of elements of L already generates L or not. This is because $\{l_1, \ldots, l_n\} \subset L$ is a generating set of L over K if and only if the set of the restrictions $\{l_{1|S}, \ldots, l_{t|S}\} \subset K(S)$ generates the field $K(S)$ over K. ♢

3.4 Cross-Sections in Invariant Theory

As mentioned before, the original motivation for the theory of cross-sections of rational maps comes from invariant theory. In this section, cross-sections in invariant theory will be examined in more detail. It will turn out that there is a convenient criterion for a subvariety to be a cross-section of a so-called rational quotient of a G-variety. We will see that cross-sections of rational quotients are a useful tool for finding generators of the invariant field of a G-variety.
Before we can go into the details, we need a brief survey on the concepts of invariant theory. This survey will also include some more basics in algebraic geometry.

The first proposition is about products of projective respectively quasi-projective varieties. It is the well-known Segre embedding. More details about products of varieties in general and the Segre embedding in special can be found for example in [Har77], Chapter I, Section 2.

Proposition 3.34 (Segre embedding). *Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be projective varieties. The set $X \times Y \subset \mathbb{P}^n \times \mathbb{P}^m$ has the structure of a projective variety via its embedding into the projective $nm + n + m$-space given by*

$$\psi : \mathbb{P}^n \times \mathbb{P}^m \longrightarrow \mathbb{P}^{nm+n+m},$$
$$((\xi_0 : \ldots : \xi_n), (\rho_0 : \ldots : \rho_m)) \longmapsto (\xi_0\rho_0 : \ldots : \xi_0\rho_m : \ldots : \xi_n\rho_0 : \ldots : \xi_n\rho_m).$$

Proof (Sketch). Let $Z_{i,j}$, $i \in \{0, \ldots, n\}$, $j \in \{0, \ldots, m\}$ be indeterminates over K. It is not hard to verify that $\psi(\mathbb{P}^n \times \mathbb{P}^m) \subset \mathbb{P}^{nm+n+m}$ is the zero set of the set of homogeneous

polynomials

$$\{Z_{i,j}Z_{k,l} - Z_{i,l}Z_{k,j};\ i,k \in \{0,\dots,n\},\ j,l \in \{0,\dots,m\}\} \\ \subset K[Z_{i,j};\ i \in \{0,\dots,n\},\ j \in \{0,\dots,m\}],$$

where

$$Z_{i,j}(\zeta_{0,0},\dots,\zeta_{0,m},\dots,\zeta_{n,0},\dots,\zeta_{n,m}) = \zeta_{i,j}$$

for all $i \in \{0,\dots,n\}$, $j \in \{0,\dots,m\}$ and $(\zeta_{0,0} : \dots : \zeta_{0,m} : \dots : \zeta_{n,0} : \dots : \zeta_{n,m}) \in \mathbb{P}^{nm+n+m}$. Let $p_1,\dots,p_s \in K[X_0,\dots,X_n]$ and $q_1,\dots,q_t \in K[Y_0,\dots,Y_m]$ be homogeneous polynomials such that $X = \mathrm{Z}^+(p_1,\dots,p_s) \subset \mathbb{P}^n$ and $Y = \mathrm{Z}^+(q_1,\dots,q_t) \subset \mathbb{P}^m$. It can be checked that $\psi(X \times Y) \subset \mathbb{P}^{nm+n+m}$ is then equal to the zero set in $\psi(\mathbb{P}^n \times \mathbb{P}^m)$ defined by the homogeneous polynomials

$$p_1(Z_{0,0},\dots,Z_{n,0}),\dots,p_1(Z_{0,m},\dots,Z_{n,m}),\dots,p_s(Z_{0,0},\dots,Z_{n,0}),\dots,p_s(Z_{0,m},\dots,Z_{n,m}),$$
$$q_1(Z_{0,0},\dots,Z_{0,m}),\dots,q_1(Z_{n,0},\dots,Z_{n,m}),\dots,q_t(Z_{0,0},\dots,Z_{0,m}),\dots,q_t(Z_{n,0},\dots,Z_{n,m}).$$

For the irreducibility of $\psi(X \times Y) \subset \mathbb{P}^{nm+n+m}$, see e. g. [Sha94], Chapter I, Section 5. ∎

Corollary 3.35. *Let X and Y be quasi-projective varieties. Then $X \times Y$ has the structure of a quasi-projective variety.*

Proof. Let X resp. Y be an open subset of the projective variety $X' \subset \mathbb{P}^n$ resp. $Y' \subset \mathbb{P}^m$. Let $\psi : \mathbb{P}^n \times \mathbb{P}^m$ be defined as in the previous proposition. By the equality

$$\psi(X \times Y) = \psi(X' \times Y') \setminus \psi\left((X' \setminus X) \times Y' \ \cup\ X' \times (Y' \setminus Y)\right)$$

it follows that $\psi(X \times Y)$ is an open subset of the projective variety $\psi(X' \times Y')$. ∎

Remarks 3.36. (a) By Remark 3.7 (c), any variety can be regarded as a quasi-projective variety. Therefore, $X \times Y$ has the structure of a variety for any two varieties X and Y.

(b) Let X and Y be varieties. Then $X \times Y$ is a product in the category of varieties (cf. [Har77], Chapter I, Section 3).

(c) Let $X', X'', \dots, X^{(k)}$ be varieties. An easy induction argument shows that the set $X' \times X'' \times \dots \times X^{(k)}$ has the structure of a variety, too.

(d) Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be projective varieties and let $p_1,\dots,p_s \in K[X_0,\dots,X_n]$ as well as $q_1,\dots,q_t \in K[Y_0,\dots,Y_m]$ be homogeneous polynomials such that $X = \mathrm{Z}^+(p_1,\dots,p_s) \subset \mathbb{P}^n$ and $Y = \mathrm{Z}^+(q_1,\dots,q_t) \subset \mathbb{P}^m$. Let H be the ideal given by $H := (p_1,\dots,p_s,q_1,\dots,q_t) \trianglelefteq K[X_0,\dots,X_n,Y_0,\dots,Y_m]$. It can be verified that the

kernel of the map

$$\begin{aligned}\theta : K[Z_{i,j};\ i \in \{0,\dots,n\},\ j \in \{0,\dots,m\}] &\longrightarrow K[X_0,\dots,X_n,Y_0,\dots,Y_m]/H,\\ Z_{i,j} &\longmapsto X_iY_j + H \qquad \text{for } i \in \{0,\dots,n\},\ j \in \{0,\dots,m\}\end{aligned}$$

is equal to $\mathrm{Id}^+(\psi(X \times Y))$. In particular, the ring

$$K[Z_{i,j};\ i \in \{0,\dots,n\},\ j \in \{0,\dots,m\}]/(\mathrm{Id}^+(X \times Y))$$

can be identified with the subring of $K[X_0,\dots,X_n,Y_0,\dots,Y_m]/H$ which is generated by the elements $X_iY_j + H$, $i \in \{0,\dots,n\}$, $j \in \{0,\dots,m\}$. Therefore, statements involving homogeneous coordinates of points in $X \times Y$, i. e. statements in terms of $Z_{i,j}$, $i \in \{0,\dots,n\}$, $j \in \{0,\dots,m\}$, can be transformed to statements in terms of $X_0,\dots,X_n$ and $Y_0,\dots,Y_m$. For example, recall that by Remark 3.9 (e), rational functions on a projective variety are given by quotients of polynomials of the same degree. Therefore, via the natural extension of θ to the quotient fields

$$\begin{aligned}\theta : \mathrm{Quot}(K[Z_{i,j};\ i \in \{0,\dots,n\},\ j \in \{0,\dots,m\}]/\mathrm{Id}^+(X \times Y))\\ \longrightarrow \mathrm{Quot}(K[X_0,\dots,X_n,Y_0,\dots,Y_m]/H),\end{aligned}$$

the elements of the function field $K(X \times Y)$ can be identified with the set of elements in $\mathrm{Quot}(K[X_0,\dots,X_n,Y_0,\dots,Y_m]/H)$ of the form $(g+H)/(h+H)$, where $g,h \in K[X_0,\dots,X_n,Y_0,\dots,Y_m]$, $h \notin H$ are homogeneous of the same degree as polynomials in $X_0,\dots,X_n$ and homogeneous of the same degree as polynomials in $Y_0,\dots,Y_m$.

(e) **Morphisms from product varieties into projective space.** Let $X \subset \mathbb{P}^n$, $Y \subset \mathbb{P}^m$ and $Z \subset \mathbb{P}^r$ be quasi-projective varieties. It follows from (d) and Remark 3.4 (d) that a map $\phi : X \times Y \longrightarrow Z$ is a morphism if and only if for every $P \in X \times Y$ there exist polynomials $g_{P,0},\dots,g_{P,r} \in K[X_0,\dots,X_n,Y_0,\dots,Y_m]$ which are homogeneous of the same degree as polynomials in $X_0,\dots,X_n$ and homogeneous of the same degree as polynomials in $Y_0,\dots,Y_m$ such that

$$\phi(P_1',P_2') = (g_{P,0}(P_1',P_2') : \dots : g_{P,r}(P_1',P_2'))$$

for all (P_1',P_2') in some open neighbourhood of P.

(f) **Products of morphisms between quasi-projective varieties.** Let X,X',Y,Y' be quasi-projective varieties and let $\phi : X \longrightarrow Y$ and $\phi' : X' \longrightarrow Y'$ be morphisms. Using the Segre embedding, it can be shown with similar methods as above that

$$\phi \times \phi' : X \times X' \longrightarrow Y \times Y',\ (P_1,P_2) \longmapsto (\phi(P_1),\phi'(P_2))$$

is a morphism of quasi-projective varieties, again. For details, see [Har77], Chapter I, Section 3.

(g) **Morphisms from affine product varieties into affine space.** Observe that if $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ and $Z \subset \mathbb{A}^r$ are affine varieties, then the description of a morphism

$\phi : X \times Y \longrightarrow Z$ can be simplified as follows. The map ϕ is a morphism if and only if there exist polynomials $g_1, \ldots, g_r \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ such that

$$\phi(P_1, P_2) = (g_1(P_1, P_2), \ldots, g_r(P_1, P_2))$$

for all (P_1, P_2) in $X \times Y$. ♢

Example 3.37. By the above, the n-fold product of the projective m-space, i. e. $X = (\mathbb{P}^m)^n$, is a projective variety in the projective $\big((m+1)^n - 1\big)$-space. To specify the function field $K(X)$, let $X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}$ be indeterminates over K. For $i \in \{1, \ldots, n\}$, let $X_{i,0}, \ldots, X_{i,m}$ correspond to the coordinates of the ith factor of $(\mathbb{P}^m)^n = \mathbb{P}^m \times \ldots \times \mathbb{P}^m$. Then an iterated application of Remark 3.36 (d) shows that the function field $K(X)$ can be identified with the subfield of $K(X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m})$ which is generated by the set of fractions, where the numerator and the denominator are polynomials in $K[X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}]$ which for every $i \in \{1, \ldots, n\}$ are homogeneous of the same degree in $X_{i,0}, \ldots, X_{i,m}$. It is therefore not hard to see that

$$K(X) \cong K\left(\frac{X_{1,1}}{X_{1,0}}, \ldots, \frac{X_{1,m}}{X_{1,0}}, \ldots, \frac{X_{n,1}}{X_{n,0}}, \ldots, \frac{X_{n,m}}{X_{n,0}}\right). \qquad \triangleleft$$

We now have seen enough algebraic geometry to give a short introduction to invariant theory. We will only cover material which will be needed for the understanding of the following chapter. A comprehensive introduction to invariant theory can be found in the books [MFK94] and [DK02].

Definition 3.38. *An* **algebraic group** *G is a variety which is endowed with the structure of a group where the group operations inversion $\iota : G \longrightarrow G$ and multiplication $\mu : G \times G \longrightarrow G$ are morphisms.*

Example 3.39. (a) The multiplicative group $K^\times = K \setminus \{0\} = K \setminus \mathrm{Z}(X_1) \subset \mathbb{A}^1$ is an algebraic group. For, let Y_1 be a further indeterminate over K (corresponding to the coordinate function of another copy of $\mathbb{A}^1 \supset K^\times$). The multiplication in $K^\times$ is given by

$$\mu = (X_1 Y_1) : K^\times \times K^\times \longrightarrow K^\times,$$

which is a morphism by Remark 3.36 (g) and Remark 3.4 (b). The inversion in $K^\times$ is given by

$$\iota = (1/X_1) : K^\times \longrightarrow K^\times.$$

By Remark 3.4 (c), this is a morphism, too.

(b) The group $\mathrm{PGL}_{m+1}(K)$ or simply PGL_{m+1}, the projective general linear group over

K, is an algebraic group. In fact, $\mathrm{PGL}_{m+1}(K)$ is the quasi-projective variety given by

$$\mathbb{P}^{m^2-1} \setminus \mathrm{Z}^+(\det(X_{i,j})_{i,j=0,\dots,m}),$$

where $X_{i,j}$, $i,j \in \{0,\dots,m\}$ are indeterminates over K (corresponding to the coordinates on $\mathbb{P}^{m^2-1}$ in the usual way of indexing when points of $\mathbb{P}^{m^2-1}$ are written as $(m+1)\times(m+1)$-matrices) and $\det(X_{i,j})_{i,j=0,\dots,m}$ denotes the determinant of the matrix $(X_{i,j})_{i,j=0,\dots,m}$. Let $Y_{i,j}$, $i,j \in \{0,\dots,m\}$ be further indeterminates over K corresponding to the coordinates of another copy of $\mathbb{P}^{m^2-1} \supset \mathrm{PGL}_{m+1}$. Then the multiplication of the group is given by the map

$$\mu = \begin{pmatrix} \sum_{j=0}^m X_{0,j}Y_{j,0} & \dots & \sum_{j=0}^m X_{0,j}Y_{j,m} \\ \vdots & & \vdots \\ \sum_{j=0}^m X_{m,j}Y_{j,0} & \dots & \sum_{j=0}^m X_{m,j}Y_{j,m} \end{pmatrix} : \mathrm{PGL}_{m+1} \times \mathrm{PGL}_{m+1} \longrightarrow \mathrm{PGL}_{m+1},$$

which by Remark 3.36 (e) certainly is a morphism.
For the inversion recall that the inverse and the adjoint of a regular matrix only differ by a (nonzero) scalar factor and hence are representatives of the same element of the group PGL_{m+1}. Since the entries of the adjoint of a matrix can be written as homogeneous polynomials in the entries of the original matrix, it follows – again by Remark 3.36 (e) – that the inversion is a morphism, too. ◁

For the definition of a G-variety, which is a central concept of invariant theory, we need the following preparatory lemma.

Lemma 3.40. *Let X, Y and Z be varieties and let $\phi : X \times Y \longrightarrow Z$ be a morphism. For $P \in X$ the map*

$$\phi(P,-) : Y \longrightarrow Z,\ P' \longmapsto \phi(P,P')$$

is a morphism from Y to Z.

Proof. It is a straightforward verification that $\iota_P : Y \longrightarrow X \times Y,\ P' \longmapsto (P,P')$ is a morphism. Being equal to the composition of morphisms $\phi \circ \iota_P : Y \longrightarrow Z$, it follows that $\phi(P,-)$ is a morphism, too. ■

Definition 3.41. *Let G be an algebraic group, X a variety and $\nu : G \times X \longrightarrow X$ a morphism. If the morphism ν defines an action of G on X, i. e. if*

$$\nu(1_G,-) = \mathrm{id}_X$$

and

$$\nu(\sigma\cdot\tau,-) = \nu(\sigma,-)\circ\nu(\tau,-),$$

where 1_G denotes the identity element of the group G, then the variety X is called a **G-variety** *(with respect to ν). If there is no danger of confusion, we sometimes write $\sigma(P)$ instead of $\nu(\sigma, P)$ for $\sigma \in G, P \in X$.*

Examples 3.42. (a) Clearly the morphism $\nu : K^\times \times \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ given by

$$\nu : \ K^\times \times \mathbb{A}^2,\ (\lambda, (\xi_1, \xi_2)) \longmapsto (\lambda\xi_1, \lambda\xi_2) \ \text{ for all } \lambda \in K^\times, (\xi_1, \xi_2) \in \mathbb{A}^2$$

defines an action of the algebraic group $K^\times$ on $\mathbb{A}^2$, that means the affine 2-space $\mathbb{A}^2$ is a $K^\times$-variety with respect to ν.

(b) Let $\mu : \mathrm{PGL}_{m+1} \times \mathbb{P}^m \longrightarrow \mathbb{P}^m$ be the morphism defined by the multiplication of PGL_{m+1} and $\mathbb{P}^m$, i.e.

$$\mu : \mathrm{PGL}_{m+1} \times \mathbb{P}^m \longrightarrow \mathbb{P}^m,$$
$$\big((\xi_{i,j})_{i,j=0,\ldots,m}, (\zeta_0 : \ldots : \zeta_m)\big) \longmapsto \left(\sum_{i=0}^{m} \xi_{0,i}\zeta_i : \ldots : \sum_{i=0}^{m} \xi_{m,i}\zeta_i\right).$$

Furthermore, let $\iota : \mathrm{PGL}_{m+1} \times (\mathbb{P}^m)^n \longrightarrow (\mathrm{PGL}_{m+1} \times \mathbb{P}^m)^n$ be the morphism given by

$$\iota : \mathrm{PGL}_{m+1} \times (\mathbb{P}^m)^n \longrightarrow (\mathrm{PGL}_{m+1} \times \mathbb{P}^m)^n,$$
$$(\sigma, (P_1, \ldots, P_n)) \longmapsto (\sigma, P_1, \ldots, \sigma, P_n).$$

Consider the composition $\nu := (\mu \times \ldots \times \mu) \circ \iota : \mathrm{PGL}_{m+1} \times (\mathbb{P}^m)^n \longrightarrow (\mathbb{P}^m)^n$ of ι and the n-fold product of the morphism μ. It defines an action of PGL_{m+1} on $(\mathbb{P}^m)^n$ which can be interpreted as the pointwise multiplication of PGL_{m+1} on the set of point configurations $(\mathbb{P}^m)^n$. So $(\mathbb{P}^m)^n$ is a PGL_{m+1}-variety with respect to ν. ◁

Lemma 3.43. *Let G be an algebraic group and let X be a G-variety with respect to a morphism $\nu : G \times X \longrightarrow X$. Then the map*

$$\nu_\sigma := \nu(\sigma, -) : X \longrightarrow X$$

is an isomorphism for all $\sigma \in G$.

Proof. Obviously, the morphism $\nu_{\sigma^{-1}} : X \longrightarrow X$ is the inverse of the morphism ν_σ. ∎

Proposition and Definition 3.44. *Let G be an algebraic group and let X be a G-variety with respect to $\nu : G \times X \longrightarrow X$. Then there is an induced action of G on the function field $K(X)$ given by*

$$\sigma(f) := f \circ \nu_{\sigma^{-1}}.$$

An element $f \in K(X)$ is called a **(rational) invariant** *under the action of G if*

$$\sigma(f) = f \qquad \text{for all } \sigma \in G.$$

The set of all rational invariants under the action of G has the structure of a field (over K) and is called the **invariant field** *under the action of G. It is denoted by $K(X)^G$.*
If a rational invariant $f \in K(X)^G$ is defined at a point $P \in X$, then it is defined at all points of the **G-orbit** *$G(P) := \{\nu(\sigma, P);\ \sigma \in G\}$ and $f(P) = f(\nu(\sigma, P))$ for all $\sigma \in G$.*
Let P and P' be points in the variety X. We say that the orbits $G(P)$ and $G(P')$ can be **separated** *by a set $L \subset K(X)^G$ of rational invariants if there exists $f \in L$ such that either f is defined both at P and at P' and $f(P) \neq f(P')$, or f is defined at exactly one of the points P and P'.*

Since subfields of finitely generated fields are finitely generated (e. g. see [Lan02], Chapter V, § 1), the invariant field $K(X)^G \subset K(X)$ has a finite generating set over K. The problem of finding a set of generating rational invariants has quite a long tradition. Especially in the very beginnings of invariant theory, which goes back to the second half of the nineteenth century, great efforts have been put into the development of methods for finding a generating set of $K(X)^G$. Whereas today there exist convenient algorithms to compute generators of the invariant field $K(X)^G$ for all kinds of algebraic groups G and G-varieties X (e. g. see [Kem07]), the possibilities in the early phase of invariant theory were limited to a pool of ad hoc methods for solving this problem. An important tool in this context was a cross-section of a certain rational map – to be more precise, a cross-section of a so-called rational quotient.

Definition 3.45. *Let G be an algebraic group and let X be a G-variety. If $f_1, \ldots, f_m \in K(X)^G$ generate the invariant field $K(X)^G$, then the dominant rational map*

$$(f_1, \ldots, f_m) : X \dashrightarrow Y$$

with $Y \subset \mathbb{A}^m$ appropriate is called a **rational quotient** *of the G-variety X.*

Remarks 3.46. (a) By definition, rational quotients of a G-variety X depend on the choice of a generating set of $K(X)^G$ and therefore cannot be unique in general. Nonetheless, for any two rational quotients $\phi_1 : X \dashrightarrow Y_1$ and $\phi_2 : X \dashrightarrow Y_2$ there exists a birational isomorphism $\psi : Y_1 \dashrightarrow Y_2$ such that $\psi \circ \phi_1 = \phi_2$.

(b) Let a subvariety $S \subset X$ be a cross-section of a rational quotient $\phi : X \dashrightarrow Y$ of a G-variety X. Then it follows from (a) that S is a cross-section of all rational quotients $\phi' : X \dashrightarrow Y'$ of the G-variety X. Therefore, S is simply called a **cross-section of the G-variety** X. ♢

A cross-section of a G-variety X can sometimes be found without the knowledge of a rational quotient. By definition of a rational quotient, this seems to be impossible at first

sight. But in fact, there is a geometric criterion for a subvariety to be a cross-section of the G-variety X which just uses the orbits of the action of G on X. This will be examined in the following. Before we can go into the details though, we need a preparatory lemma.

Lemma 3.47. *Let X, Y and ϕ be as in Notation 3.14 and let ϕ be injective on some nonempty open subset $\mathcal{O}$ of X.*

(i) If $\mathrm{char}(K) = 0$, then $\phi^*(K(Y)) = K(X)$. In particular, the rational map ϕ is a birational isomorphism.

(ii) If $\mathrm{char}(K) = p$ for some $p > 0$, then $K(X)$ is a purely inseparable field extension of $\phi^*(K(Y))$, i. e. for every element $f \in K(X)$ there exists $s \in \mathbb{N}_0$ such that $f^{p^s} \in \phi^*(K(Y))$.

Proof. For the case that X and Y are affine varieties and ϕ is a morphism, a proof of this lemma can be found in [Hum75], Proposition 4.8. The general case where X and Y are arbitrary varieties and $\phi : X \dashrightarrow Y$ is a rational map can be proved by a reduction argument. For, by definition of a rational map, there exists a nonempty open subset $V \subset X$ such that $\phi_{|V}$ is a morphism. Clearly, the restriction of ϕ to the nonempty open subset $V \cap \mathcal{O}$ is a morphism, too. Since ϕ was assumed to be dominant and $V \cap \mathcal{O}$ is open in X, it follows that $\phi_{|V\cap\mathcal{O}} : V \cap \mathcal{O} \longrightarrow Y$ is a dominant morphism (cf. Remark 3.11 (h)). Let $Y' \subset Y$ be an open, affine subset of Y (cf. [Har77], Chapter I, Proposition 4.3). By continuity of $\phi_{|V\cap\mathcal{O}}$, the preimage $\phi^{-1}_{|V\cap\mathcal{O}}(Y')$ is open in $V \cap \mathcal{O}$ and hence open in X. Moreover, since $\phi_{|V\cap\mathcal{O}}$ is dominant, it is nonempty. Let $X' \subset \phi^{-1}_{|V\cap\mathcal{O}}(Y')$ be an open affine subset of X. By Remark 3.11 (h),

$$\phi_{|X'} : X' \longrightarrow Y'$$

is a dominant, injective morphism between the affine varieties X' and Y'. By the fact that $K(X') = K(X)$ and $K(Y') = K(Y)$, the assertion now follows from the special case mentioned at the beginning of this proof. ∎

Proposition 3.48. *Let G be an algebraic group, let X be a G-variety and let S be a subvariety of X which satisfies the following conditions:*

(i) $|G(P) \cap S| = 1$ for all P in some nonempty open subset $\mathcal{O}$ of S.

(ii) $\overline{G(S)} = X$.

Let $\phi : X \dashrightarrow Y$ be a rational quotient of the G-variety X. Then $\phi_{|S} : S \dashrightarrow Y$ is a dominant rational map which is injective on some nonempty open subset $\mathcal{O}'$ of S. In particular, if K is a field of characteristic zero, then S is a cross-section of the G-variety X.

Proof. By definition, the rational quotient $\phi : X \dashrightarrow Y$ is dominant. Since $G(S)$ is a dense subset of X, it follows by a theorem of Chevalley (cf. [Har77], Chapter II, Exercise 3.18

and Exercise 3.19) that there exists $\widetilde{\mathcal{O}} \subset G(S)$ which is nonempty and open in X. By Remark 3.11 (h), we know that $\phi(\widetilde{\mathcal{O}})$ is dense in Y. As a rational quotient, ϕ is clearly constant on the G-orbits, therefore defined on some nonempty subset of S and

$$\phi(S) \supset \phi(\widetilde{\mathcal{O}}).$$

So $\phi_{|S} : S \dashrightarrow Y$ is a dominant rational map.
By the Theorem of Rosenlicht (see [Ros63]), there exists a G-stable nonempty open subset $\mathcal{R}$ of X such that ϕ is defined everywhere on $\mathcal{R}$ and

$$G(P) = G(P') \iff \phi(P) = \phi(P') \qquad \text{for all points } P, P' \in \mathcal{R}. \tag{3.5}$$

Let $\mathcal{O}' \subset S$ be the open subset of S given by

$$\mathcal{O}' := \mathcal{O} \cap \mathcal{R} \subset S.$$

We show that $\mathcal{O}'$ is nonempty and that the restriction $\phi_{|\mathcal{O}'} : \mathcal{O}' \dashrightarrow Y$ is injective.
Since $G(S)$ is dense in X, the intersection $G(S) \cap \mathcal{R}$ must be nonempty. From the fact that $\mathcal{R}$ is G-stable it hence follows that $\mathcal{R} \cap S$ is a nonempty open subset of S. Therefore, we have

$$\mathcal{O} \cap \mathcal{R} = \mathcal{O} \cap (\mathcal{R} \cap S) \neq \emptyset,$$

i. e. $\mathcal{O}'$ is nonempty.
Let P and P' be points in $\mathcal{O}'$ such that $\phi(P) = \phi(P')$. Since $\mathcal{O}'$ is contained in the set $\mathcal{R}$ and therefore also $P, P' \in \mathcal{R}$, the orbits $G(P)$ and $G(P')$ must be equal (cf. (3.5)). By condition (i), it follows that

$$P = G(P) \cap S = G(P') \cap S = P'.$$

This shows that $\phi_{|\mathcal{O}'} : \mathcal{O}' \dashrightarrow Y$ is injective, indeed.
The remaining statement of the proposition is an immediate consequence of the previous lemma. ∎

With the previous proposition we get a valuable tool for the identification of a cross-section of a G-variety X. In the following examples it will be utilized to find generators of the invariant field $K(X)^G$.

Examples 3.49. (a) Let K be a field of characteristic zero and let X be the $K^\times$-variety $\mathbb{A}^2$ of Example 3.42 (a). Note that the $K^\times$-orbits under this action are given by the origin and the pointed lines through the origin. Let $S_1 \subset X$ be the subvariety given by

$$S_1 := \{(\xi_1, \xi_2);\ \xi_2 = 1\}.$$

It is not hard to see that $G(S_1)$ is equal to the dense open subset $X \setminus \mathrm{Z}(X_2) \subset X$ and that the G-orbit $G(\xi_1, \xi_2)$ of a point $(\xi_1, \xi_2) \in S_1$ intersects S_1 exactly at (ξ_1, ξ_2). By

the previous proposition, it follows that S_1 is a cross-section of the $K^\times$-variety X. Let $S_2 \subset X$ be the parabola given by

$$S_2 := \{(\xi_1, \xi_2);\ \xi_2 = \xi_1^2\}.$$

As before, it can easily be verified that $G(S_2)$ is a dense open subset of X, namely $(X \setminus Z(X_1X_2)) \cup (0,0)$, and that the G-orbit $G(\xi_1, \xi_2)$ of a point $(\xi_1, \xi_2) \in S_2$ intersects S_2 exactly at (ξ_1, ξ_2). Again, it follows that S_2 is a cross-section of the $K^\times$-variety X. By Remark 3.33, a set of generators of the invariant field $K(X)^{K^\times}$ is therefore given by any set of rational invariants whose restrictions to one of the cross-sections S_1 or S_2 generate the function field $K(S_1)$ resp. $K(S_2)$ over K. Obviously, the rational function $X_1/X_2 \in K(X)$ is invariant under the action of $K^\times$. Its restriction to the subvariety $S_1 = \mathrm{Z}(X_2 - 1)$ is equal to the rational function $X_1 + (X_2 - 1)_{K[X_1,X_2]} \in K(S_1)$, which obviously generates the function field $K(S_1)$. This implies that the invariant field $K(X)^{K^\times}$ is equal to the field $K(X_2/X_1)$.

Note that the very same situation has already been examined in Example 3.24 (a). Unlike to the treatment there where we have tried to find a cross-section of the rational map $(X_1/X_2) : \mathbb{A}^2 \longrightarrow \mathbb{A}^1$ (which retrospectively has turned out to be a rational quotient), the motivation here is the other way round: we have found the invariant field and thus a rational quotient just by identifying a cross-section of a rational quotient at first.

(b) Let K be a field of characteristic zero and let X be the PGL_2-variety $(\mathbb{P}^1)^3$ of Example 3.42 (b). Let $S \subset X$ be the subvariety given by the single point

$$S := ((1:0), (0:1), (1:1)) \in (\mathbb{P}^1)^3.$$

Since S consists of just one single point, we obviously have $\mathrm{PGL}_2(P) \cap S = \{P\}$ for all points $P \in S$. Furthermore, it is a standard result from projective geometry (e. g. see Lemma 4.4) that for any point $P = (P_1, P_2, P_3)$ in $(\mathbb{P}^1)^3$ such that P_1, P_2 and $P_3 \in \mathbb{P}^1$ are pairwise distinct, there exists $\sigma \in \mathrm{PGL}_2$ such that

$$\sigma(P_1, P_2, P_3) = ((1:0), (0:1), (1:1)).$$

Since the set of all such points is equal to

$$\Big\{((\xi_{1,0} : \xi_{1,1}), (\xi_{2,0} : \xi_{2,1}), (\xi_{3,0} : \xi_{3,1})) \in (\mathbb{P}^1)^3;\ \prod_{\substack{i,j \in \{1,2,3\} \\ i \neq j}} \xi_{i,0}\xi_{j,1} - \xi_{i,1}\xi_{j,0} \neq 0\Big\},$$

which obviously is a nonempty open subset of $(\mathbb{P}^1)^3$, it follows that $\mathrm{PGL}_2(S)$ is dense in $(\mathbb{P}^1)^3$. By Proposition 3.48, the subvariety S thus is a cross-section of the PGL_2-variety $(\mathbb{P}^1)^3$.
Since S is a one-point-set, it is immediate that the invariant field $K((\mathbb{P}^1)^3)^{\mathrm{PGL}_2}$ is equal to K (cf. Remark 3.33).
A generalization of this problem will be examined in the next chapter. $\lhd$

4 Invariants of the Action of the Group $\mathbf{PGL}_{m+1} \times \mathbf{S}_n$ on $(\mathbb{P}^m)^n$

In this chapter, we come back to Problem 1.5 in Chapter 1 which was motivated by the recognition of flat objects by means of photographic images of the objects. Let K be an infinite field and consider the action of the group $\mathrm{PGL}_{m+1}(K) \times \mathrm{S}_n$ on the set of point configurations $(\mathbb{P}^m_K)^n$ given by

$$(\sigma, \pi)(P_1, \ldots, P_n) = (\sigma(P_{\pi^{-1}(1)}), \ldots, \sigma(P_{\pi^{-1}(n)}))$$

for all $\sigma \in \mathrm{PGL}_{m+1}$, $\pi \in \mathrm{S}_n$ and $(P_1, \ldots, P_n) \in (\mathbb{P}^m)^n$. Recall that the action of PGL_{m+1} on $\mathbb{P}^m$ is just the standard multiplication. It is our aim to find generators of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$ and to examine which orbits of this action can be separated by rational invariants (see below for a definition of invariant field, separation etc. in this generalized situation). Kemper and Boutin examined this problem for the case $m = 2$ in their paper [BK05]. Here we will generalize their ideas to arbitrary dimensions m.

For a precise treatment of Problem 1.5 in its generality for arbitrary infinite fields K, we have to (re-)define some terms which have already been defined for algebraically closed fields in the previous chapter. Essentially, the following is just a straight generalization of the respective terms and definitions which have been introduced before.

Let K be an infinite field, let $m \in \mathbb{N}$ and let $n \in \mathbb{N}$. We define a topology on $(\mathbb{P}^m_K)^n$ for arbitrary infinite fields K as follows. Let $X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}$ be indeterminates over K where $X_{i,0}, \ldots, X_{i,m}$ correspond to the coordinates on the ith factor of $(\mathbb{P}^m)^n = \mathbb{P}^m \times \ldots \times \mathbb{P}^m$ for $i \in \{1, \ldots, n\}$. We take the closed sets of $(\mathbb{P}^m_K)^n$ to be the zero sets of sets of polynomials in $K[X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}]$ which are homogeneous in $X_{i,0}, \ldots, X_{i,m}$ for all $i \in \{1, \ldots, n\}$. It is an easy verification that this in fact defines a topology on $(\mathbb{P}^m_K)^n$. Note that for algebraically closed fields K this is just the Zariski topology on $(\mathbb{P}^m_K)^n$.

The **function field** $K((\mathbb{P}^m_K)^n)$ of the set of point configurations $(\mathbb{P}^m_K)^n$ is defined to be

$$K((\mathbb{P}^m_K)^n) := K\left(\frac{X_{1,1}}{X_{1,0}}, \ldots, \frac{X_{1,m}}{X_{1,0}}, \ldots, \frac{X_{n,1}}{X_{n,0}}, \ldots, \frac{X_{n,m}}{X_{n,0}}\right).$$

An element f of the function field is called a **rational function**. Obviously, f defines a partial function from $(\mathbb{P}^m_K)^n$ to K. The **domain of definition** of f is defined to be the set of all points $P \in (\mathbb{P}^m_K)^n$ such that there exist polynomials $g_P, h_P \in K[X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}]$ which are homogeneous in $X_{i,0}, \ldots, X_{i,m}$ for all $i \in \{1, \ldots, n\}$ such that $h_P(P) \neq 0$ and $f = g_P/h_P$. It is not hard to see that the

domain of definition of f is an open subset of X.
If it is desired to emphasize the "functional" point of view of a rational function $f \in K((\mathbb{P}^m_K)^n)$, we sometimes write $f : (\mathbb{P}^m_K)^n \dashrightarrow K$. In fact, we do not loose any information when identifying the element $f \in K((\mathbb{P}^m_K)^n)$ with the respective partial function $f : (\mathbb{P}^m_K)^n \dashrightarrow K$, as the following two results show.

Lemma 4.1. *Let $\overline{K}$ be the algebraic closure of the field K and let ι be the natural embedding $\iota : (\mathbb{P}^m_K)^n \longrightarrow (\mathbb{P}^m_{\overline{K}})^n$. Then ι induces a homeomorphism between $(\mathbb{P}^m_K)^n$ and $\iota((\mathbb{P}^m_K)^n)$. Moreover, $\iota((\mathbb{P}^m_K)^n)$ is dense in $(\mathbb{P}^m_{\overline{K}})^n$. In particular, $(\mathbb{P}^m_K)^n$ is irreducible and it follows that $\iota(\mathcal{O})$ is dense in $(\mathbb{P}^m_{\overline{K}})^n$ for every nonempty open subset $\mathcal{O}$ of $(\mathbb{P}^m_K)^n$.*

Proof. We first show that ι maps closed subsets of $(\mathbb{P}^m_K)^n$ to closed subsets (with respect to the subspace topology) of $\iota((\mathbb{P}^m_K)^n)$. Let $p_1, \ldots, p_t \in K[X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}]$ be polynomials which are homogeneous in $X_{i,0}, \ldots, X_{i,m}$ for all $i \in \{1, \ldots, n\}$ and let $\mathcal{C} \subset (\mathbb{P}^m_K)^n$ be the zero set of the polynomials $p_1, \ldots, p_t$. Then clearly $\iota(\mathcal{C})$ is the intersection of the embedding $\iota((\mathbb{P}^m_K)^n)$ with the zero set of the polynomials $p_1, \ldots, p_t$ in $(\mathbb{P}^m_{\overline{K}})^n$, hence is the intersection of the set $\iota((\mathbb{P}^m_K)^n)$ with a closed subset of $(\mathbb{P}^m_{\overline{K}})^n$, as desired. Note that the same is true for open sets, i. e. for any open set $\mathcal{O} \subset (\mathbb{P}^m_K)^n$ the set $\iota(\mathcal{O}) \subset (\mathbb{P}^m_{\overline{K}})^n$ is the intersection of the set $\iota((\mathbb{P}^m_K)^n)$ with an open subset $\hat{\mathcal{O}}$ of $(\mathbb{P}^m_{\overline{K}})^n$.

Next we show that $\iota((\mathbb{P}^m_K)^n)$ is dense in $(\mathbb{P}^m_{\overline{K}})^n$. As a preliminary consideration, let $k \in \mathbb{N}_0$, let $Y_1, \ldots, Y_k$ be indeterminates over K and let $p \in \overline{K}[Y_1, \ldots, Y_k]$ be a nonzero polynomial. We claim that there exist $\xi_1, \ldots, \xi_k \in K$ such that $p(\xi_1, \ldots, \xi_k) \neq 0$. If $k = 0$, then there is nothing to show. Otherwise, there exists $\xi_k \in K$ such that $p(Y_1, \ldots, Y_{k-1}, \xi_k) \neq 0$. For, the polynomial p can be regarded as a (nonzero) element of the univariate polynomial ring $\mathrm{Quot}(\overline{K}[Y_1, \ldots, Y_{k-1}])[Y_k]$. But then, since K is infinite and a nonzero polynomial over a field cannot have infinitely many roots, there exists $\xi_k \in K$ such that $0 \neq p(X_1, \ldots, X_{k-1}, \xi_k) \in \mathrm{Quot}(\overline{K}[X_1, \ldots, X_{k-1}])$. Moreover, observe that by construction $p(X_1, \ldots, X_{k-1}, \xi_k) \in \overline{K}[X_1, \ldots, X_{k-1}]$ and so the claim follows by induction.
We can now show that $\iota((\mathbb{P}^m_K)^n)$ is dense in $(\mathbb{P}^m_{\overline{K}})^n$. Let $p \in \overline{K}[X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}]$ be a nonzero polynomial which is homogeneous in $X_{i,0}, \ldots, X_{i,m}$ for all $i \in \{1, \ldots, n\}$. By what we have proved a few lines above, p does not vanish at all points of $\iota((\mathbb{P}^m_K)^n)$, i. e. $p(P_1, \ldots, P_n) \neq 0$ for some $(P_1, \ldots, P_n) \in \iota((\mathbb{P}^m_K)^n)$. It follows that the zero polynomial is the only polynomial that vanishes on $\iota((\mathbb{P}^m_K)^n)$. Therefore, the closure of the set $\iota((\mathbb{P}^m_K)^n)$ is equal to $(\mathbb{P}^m_{\overline{K}})^n$.

Since $(\mathbb{P}^m_{\overline{K}})^n$ is irreducible and $\iota((\mathbb{P}^m_K)^n)$ is a dense subspace of $(\mathbb{P}^m_{\overline{K}})^n$, it follows that $\iota((\mathbb{P}^m_K)^n)$ and hence $(\mathbb{P}^m_K)^n$ is irreducible, too. In particular, every nonempty open subset $\mathcal{O}$ of $(\mathbb{P}^m_K)^n$ is dense in $(\mathbb{P}^m_K)^n$. It follows that $\iota(\mathcal{O})$ is dense in $\iota((\mathbb{P}^m_K)^n)$ and thus – since $\iota((\mathbb{P}^m_K)^n)$ is dense in $(\mathbb{P}^m_{\overline{K}})^n$ – the set $\iota(\mathcal{O})$ is also dense in $(\mathbb{P}^m_{\overline{K}})^n$. ∎

Corollary 4.2. *Let $f_1, f_2 \in K((\mathbb{P}^m)^n)$ be rational functions. If f_1 and f_2 define the same*

function on a nonempty open subset of $(\mathbb{P}^m)^n$*, then* $f_1 = f_2 \in K((\mathbb{P}^m)^n)$.

Proof. Let $\mathcal{O} \subset (\mathbb{P}^m_K)^n$ be a nonempty open set such that f_1 and f_2 define the same function on $\mathcal{O}$. As in the previous lemma, let ι be the embedding of $(\mathbb{P}^m_K)^n$ into $(\mathbb{P}^m_{\overline{K}})^n$. If we regard f_1 and f_2 as rational functions on $(\mathbb{P}^m_{\overline{K}})^n$, then f_1 and f_2 clearly define the same function on the set $\iota(\mathcal{O})$. Since this set is dense in $(\mathbb{P}^m_{\overline{K}})^n$, it is also dense in the intersection of the domains of definition of $f_1, f_2 \in \overline{K}((\mathbb{P}^m)^n)$ and hence it follows that f_1 and f_2 define the same function on $(\mathbb{P}^m_{\overline{K}})^n$. This implies that $f_1 = f_2 \in \overline{K}((\mathbb{P}^m_{\overline{K}})^n)$ and hence also $f_1 = f_2 \in K((\mathbb{P}^m_K)^n)$. ∎

In particular, it makes no difference whether we regard a rational function as a formal element of $K((\mathbb{P}^m_K)^n)$ or as a partial function from $(\mathbb{P}^m_K)^n$ to K. In the following, both viewpoints will be used interchangeably.
Let a group G act on the set of point configurations $(\mathbb{P}^m)^n$ in such a way that any $\sigma \in G$ induces an automorphism of the function field $K((\mathbb{P}^m)^n)$, i. e. such that $f \circ \sigma \in K((\mathbb{P}^m)^n)$ for all $f \in K((\mathbb{P}^m)^n)$ and for all $\sigma \in G$. In this context, σ stands for the map $(\mathbb{P}^m)^n \longrightarrow (\mathbb{P}^m)^n$, $P \longmapsto \sigma(P)$. Note in passing that the action of the group $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$ as defined above is of that type.
Assuming an arbitrary G-action of this type, there is an induced action of G on the function field $K((\mathbb{P}^m)^n)$ via $\sigma(f) := f \circ \sigma^{-1}$ for all $\sigma \in G$. We call a rational function $f \in K((\mathbb{P}^m)^n)$ a **(rational) invariant** under the action of G if

$$\sigma(f) = f \qquad \text{for all } \sigma \in G.$$

The **invariant field** $K((\mathbb{P}^m)^n)^G$ is defined to be the set of all rational invariants. It is not hard to see that it has the structure of a field.
Note that if a rational invariant f is defined at a point $P \in (\mathbb{P}^m)^n$, then it is defined on its whole **G-orbit** $G(P) := \{\sigma(P);\ \sigma \in G\}$ and $f(P) = f(\sigma(P))$ for all $\sigma \in G$. Let P and P' be in $(\mathbb{P}^m)^n$. We say that the orbits $G(P)$ and $G(P')$ can be **separated** by a set $L \subset K((\mathbb{P}^m)^n)^G$ of rational invariants if there exists $f \in L$ such that either f is defined both at P and at P' and $f(P) \neq f(P')$ or f is defined at exactly one of the points P and P'.

As mentioned at the very beginning of this chapter, it is our aim to find generators of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$ and to examine which orbits of this action can be separated by rational invariants. The agenda for doing this is as follows. First, we will restrict to the action of the (normal) subgroup $\mathrm{PGL}_{m+1} \trianglelefteq \mathrm{PGL}_{m+1} \times S_n$ on the set of point configurations $(\mathbb{P}^m)^n$ and determine generators of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$. Then we will examine the action of the group $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$ on the field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ as induced by the action of $\mathrm{PGL}_{m+1} \times S_n$ on $(\mathbb{P}^m)^n$. By construction, this action can be interpreted as an action of the finite group S_n on the field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$. The field of fixed elements $(K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}})^{\mathrm{S}_n}$ is then equal to the desired invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$.

We will use the following notation.

Notation 4.3.

(i) Unless otherwise stated, K shall denote an infinite field.

(ii) m and n shall be in $\mathbb{N}$.

(iii) Unless otherwise stated, the projective m-space $\mathbb{P}^m$ and the projective general linear group PGL_{m+1} shall be over K, i. e. $\mathbb{P}^m := \mathbb{P}^m_K$ and $\mathrm{PGL}_{m+1} := \mathrm{PGL}_{m+1}(K)$.

(iv) $X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}$ shall be indeterminates over K. Usually, the indeterminates $X_{i,0}, \ldots, X_{i,m}$ correspond to the coordinates of the ith factor of $(\mathbb{P}^m)^n = \mathbb{P}^m \times \ldots \times \mathbb{P}^m$ for $i \in \{1, \ldots, n\}$.

(v) $P_1, P_2, P_3, \ldots$ shall denote points in $\mathbb{P}^m$, $P = (P_1, \ldots, P_n) \in (\mathbb{P}^m)^n$ shall denote a point configuration.

(vi) p. d. shall be an abbreviation for pairwise distinct.

4.1 The Fundamental Theorems for the Group PGL_{m+1}

As outlined above, we start with an examination of the action of the group PGL_{m+1} on the set of point configurations $(\mathbb{P}^m)^n$. We will determine generators of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ and describe all K-relations among these generators. In classical invariant theory, the determination of a generating set of invariants is usually referred to as the first fundamental theorem for that group. In this manner of speaking, the description of the relations among a set of generators is called the second fundamental theorem for that group.

For a better readability, it is convenient to introduce the following notation. We define the bracket $[d_1, \ldots, d_{m+1}]$ to be the determinant

$$[d_1, \ldots, d_{m+1}] := \begin{vmatrix} X_{d_1,0} & \cdots & X_{d_{m+1},0} \\ \vdots & & \vdots \\ X_{d_1,m} & \cdots & X_{d_{m+1},m} \end{vmatrix} \in K[X_{1,0}, \ldots, X_{1,m}, \ldots, X_{n,0}, \ldots, X_{n,m}]$$

for $d_1, \ldots, d_{m+1} \in \{1, \ldots, n\}$. Obviously, every such bracket is a homogeneous polynomial in $X_{i,0}, \ldots, X_{i,m}$ for all $i \in \{1, \ldots, n\}$.

It is not hard to specify at least some rational invariants. A straightforward verification shows that for all pairwise distinct elements $d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\}$ the rational function

$$c_{d_1,\ldots,d_{m-1},i,j,k,l} := \frac{[d_1, \ldots, d_{m-1}, i, j][d_1, \ldots, d_{m-1}, k, l]}{[d_1, \ldots, d_{m-1}, i, k][d_1, \ldots, d_{m-1}, j, l]} \in K((\mathbb{P}^m)^n)$$

is a non-constant invariant under the action of the group PGL_{m+1}. In the literature, a rational function of that type is called **cross-ratio**. In fact, we will show that the set of all cross-ratios already generates the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$.

To prove this, we use the theory of cross-sections of rational maps. Our first task thus will be the identification of a cross-section of a rational quotient of the PGL_{m+1}-variety $(\mathbb{P}^m_K)^n$ where $K = \overline{K}$. Such a cross-section will evolve from the following lemma.

Lemma 4.4. *Let $X_0, \ldots, X_m$ be indeterminates over the field K and let $P_1, \ldots, P_{m+2} \in \mathbb{P}^m$ be points in the projective m-space such that no $m+1$ of them are in a hypersurface of $\mathbb{P}^m$, i. e. in the zero set of a nonzero polynomial of the form $\sum_{i=0}^m \lambda_i X_i \in K[X_0, \ldots, X_m]$ with $\lambda_0, \ldots, \lambda_m \in K$. Then there exists a (unique) $\sigma \in \mathrm{PGL}_{m+1}$ such that*

$$\begin{aligned} \sigma(P_1) &= (1 : 0 : \ldots : 0) \\ \sigma(P_2) &= (0 : 1 : 0 : \ldots : 0) \\ &\vdots \\ \sigma(P_{m+1}) &= (0 : \ldots : 0 : 1) \qquad \textit{and} \\ \sigma(P_{m+2}) &= (1 : 1 : \ldots : 1). \end{aligned}$$

Proof. For $i \in \{1, \ldots, m+2\}$, let $(\xi_{i,0} : \ldots : \xi_{i,m})$ with $\xi_{i,0}, \ldots, \xi_{i,m} \in K$ be the homogeneous coordinates of the point P_i. The fact that no $m+1$ of the points $P_1, \ldots, P_{m+2}$ are in a hypersurface of $\mathbb{P}^m$ translates to the fact that the matrix

$$\begin{pmatrix} \xi_{1,0} & \cdots & \xi_{j-1,0} & \xi_{j+1,0} & \cdots & \xi_{m+2,0} \\ \vdots & & \vdots & \vdots & & \vdots \\ \xi_{1,m} & \cdots & \xi_{j-1,m} & \xi_{j+1,m} & \cdots & \xi_{m+2,m} \end{pmatrix} \tag{4.1}$$

is regular for all $j \in \{1, \ldots, m+2\}$. It follows that there exist $\lambda_1, \ldots, \lambda_{m+1} \in K^\times$ such that

$$\begin{pmatrix} \xi_{1,0} & \cdots & \xi_{m+1,0} \\ \vdots & & \vdots \\ \xi_{1,m} & \cdots & \xi_{m+1,m} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{m+1} \end{pmatrix} = \begin{pmatrix} \xi_{m+2,0} \\ \vdots \\ \xi_{m+2,m} \end{pmatrix}.$$

Furthermore, as the diagonal matrix $\mathrm{diag}(\lambda_1, \ldots, \lambda_{m+1})$ is regular, too, there exists $\hat{\sigma} \in \mathrm{GL}_{m+1}$ such that

$$\hat{\sigma} \cdot \begin{pmatrix} \xi_{1,0} & \cdots & \xi_{m+1,0} \\ \vdots & & \vdots \\ \xi_{1,m} & \cdots & \xi_{m+1,m} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_{m+1} \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}.$$

It follows by construction that the equivalence class defined by $\hat{\sigma} \in \mathrm{GL}_{m+1}$, say $\sigma \in \mathrm{PGL}_{m+1}$, satisfied (4.4). In particular, we certainly also have $\sigma(P_{m+2}) = (1 : \ldots : 1)$.
To show the uniqueness of such an element $\sigma \in \mathrm{PGL}_{m+1}$, it is enough to consider the case where $P_{m+2} = (1 : \ldots : 1)$ and* $P_i = (\delta_{1,i} : \ldots : \delta_{m+1,i})$ for $i \in \{1, \ldots, m+1\}$. But for this case, the uniqueness of such a group element $\sigma \in \mathrm{PGL}_{m+1}$ is immediate, the only element

*as usual, $\delta_{-,-}$ denotes the Kronecker symbol

in PGL_{m+1} which has the desired properties is the element $\sigma = 1_{\mathrm{PGL}_{m+1}}$. ∎

Let H be the open subset of $(\mathbb{P}^m)^n$ given by

$$H := \Big\{(P_1, \ldots, P_n) \in (\mathbb{P}^m)^n; \prod_{\substack{d_1,\ldots,d_{m+1} \in \{1,\ldots,n\} \\ d_1 < \ldots < d_{m+1}}} [d_1, \ldots, d_{m+1}](P_1, \ldots, P_n) \neq 0\Big\},$$

the set of point configurations of length n such that no $m+1$ of these points lie in a hypersurface of the projective space $\mathbb{P}^m$. The set H is nonempty. For, let $\lambda_1, \ldots, \lambda_{m+1} \in K^\times$ and consider the matrix

$$\begin{pmatrix} \lambda_1^0 & \cdots & \lambda_{m+1}^0 \\ \vdots & & \vdots \\ \lambda_1^m & \cdots & \lambda_{m+1}^m \end{pmatrix}$$

(also known as the Vandermonde matrix). It is a well-known fact that this matrix is regular if and only if $\lambda_1, \ldots, \lambda_{m+1}$ are pairwise distinct (see for example [CLO07], Chapter 1, § 5, Exercise 2). So, let $\xi_1, \ldots, \xi_n \in K^\times$ be pairwise distinct elements. It then follows that $((1 : \xi_1 : \ldots : \xi_1^m), \ldots, (1 : \xi_m : \ldots : \xi_m^m)) \in H$.
Furthermore, we define a closed subset S of $(\mathbb{P}^m)^n$. In case that n is greater than $m+2$, let S be given by

$$S := \{(1 : 0 : \ldots : 0), \ldots, (0 : \ldots : 0 : 1), (1 : \ldots : 1), P_{m+3}, \ldots, P_n)\,;\; P_{m+3}, \ldots, P_n \in \mathbb{P}^m\}\,.$$

In case that $n \leq m+2$, we define S to be the one-point subset of $(\mathbb{P}^m)^n$ having the point configuration given by the first n points of $(1 : 0 : \ldots : 0), \ldots, (0 : \ldots : 0 : 1), (1 : \ldots : 1)$ as its only element.

Lemma 4.5. *Let S be the subset of the PGL_{m+1}-variety $(\mathbb{P}^m)^n$ as defined a few lines above. Then S has the following properties:*

(a) $|\mathrm{PGL}_{m+1}(P) \cap S| = 1$ *for all* $P \in S$.

(b) $\mathrm{PGL}_{m+1}(S)$ *contains a nonempty open subset.*

Proof. Suppose first that $n \leq m+2$. Then S consists of just one single point, hence (a) is obviously true. By the previous lemma, the set $\mathrm{PGL}_{m+1}(S)$ contains all point configurations $(P_1, \ldots, P_n) \in (\mathbb{P}^m)^n$ which can be supplemented by points $P_{n+1}, \ldots, P_{m+2} \in \mathbb{P}^m$ such that no $m+1$ of the points $P_1, \ldots, P_{m+2}$ are in a hypersurface. This is equivalent to saying that at least one of the $n \times n$ minors of the $(m+1) \times n$ matrix whose ith column is given by homogeneous coordinates of the point P_i for $i \in \{1, \ldots, n\}$ is nonzero. Obviously, this condition characterizes a nonempty and open set, which shows (b).
Suppose now that $n > m+2$. Let $P \in S$. Then by Lemma 4.4, there exists a unique $\sigma \in \mathrm{PGL}_{m+1}$, namely $\sigma = 1_{\mathrm{PGL}_{m+1}}$, such that $\sigma(P) \in S$. Hence (a) is proven. To show (b), observe that for all points P in the open set H (as defined a few lines above), there

exists an element $\sigma \in \mathrm{PGL}_{m+1}$ such that $\sigma(P) \in S$ (cf. Lemma 4.4). In other words, the PGL_{m+1}-image of S contains the open set H. ∎

In case that K is an algebraically closed field of characteristic zero, it follows by Proposition 3.48 that S is a cross-section of a rational quotient of the PGL_{m+1}-variety $(\mathbb{P}^m)^n$. In fact, as will become clear in a minute, this holds for positive characteristic of the field K, too.

Proposition 4.6. *Let the field K be algebraically closed and let S be as defined before Lemma 4.5. Then S is a cross-section of the PGL_{m+1}-variety $(\mathbb{P}^m)^n$. Moreover, the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ is generated by the set of invariants*

$$C := \{c_{d_1,\ldots,d_{m-1},i,j,k,l};\ d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\}\ p.\,d.\}$$

as a field over K.

Proof. If the number of points n is at most $m+2$, then S consists of just one single point. By Lemma 4.5 (b), there exists a dense PGL_{m+1}-orbit in the PGL_{m+1}-variety $(\mathbb{P}^m)^n$ (cf. Examples 3.49 (b)), hence the only rational invariants are the constants, that means

$$K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}} = K.$$

It follows that $\phi : (\mathbb{P}^m)^n \longrightarrow \mathbb{A}^0,\ P \longmapsto 0$ for all $P \in (\mathbb{P}^m)^n$ is a rational quotient of the PGL_{m+1}-variety $(\mathbb{P}^m)^n$, hence the one-point set S is obviously a cross-section of the PGL_{m+1}-variety $(\mathbb{P}^m)^n$. Furthermore, we have $C = \emptyset$, so $K(C)$ is equal to $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}} = K$, as asserted.
Suppose now that the number of points n is at least $m+3$. Consider the set of functions

$$\tilde{C} := \{c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,k,1};\ k \in \{m+3,\ldots,n\}, i \in \{2,\ldots,m+1\}\} \subset C,$$

where the hat symbolizes that the corresponding index is omitted. As the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ is finitely generated, there exist rational invariants $f_1,\ldots,f_t \in K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ such that

$$K(\tilde{C} \cup \{f_1,\ldots,f_t\}) = K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}.$$

Let $\phi : (\mathbb{P}^m)^n \dashrightarrow Y \subset \mathbb{A}^{t+m(n-(m+2))}$ (where Y is an appropriate affine variety) be a rational quotient of $(\mathbb{P}^m)^n$, say

$$\begin{aligned}\phi := (&c_{3,\ldots,m+1,2,m+2,m+3,1},\ldots,c_{2,\ldots,m,m+1,m+2,m+3,1},\ldots,c_{3,\ldots,m+1,2,m+2,n,1},\ldots,\\ &c_{2,\ldots,m,m+1,m+2,n,1},f_1,\ldots,f_t) :\\ &(\mathbb{P}^m)^n \dashrightarrow Y \subset \mathbb{A}^{t+m(n-(m+2))},\end{aligned}$$

By Lemma 4.5 and Proposition 3.48, the restriction of the rational quotient ϕ to the

subvariety S gives a dominant rational map $\phi_{|S} : S \dashrightarrow Y$. Note that since $\mathrm{PGL}_{m+1}(S)$ is dense in $(\mathbb{P}^m)^n$, the restrictions $c_{|S}$, $c \in \tilde{C}$ and $f_{1|S}, \ldots, f_{t|S}$ are well-defined rational functions $S \longrightarrow K$. Therefore, the embedding of $K(Y)$ into $K(S)$ by $(\phi_{|S})^*$ is given by

$$(\phi_{|S})^*(K(Y)) = K(f_{1|S}, \ldots, f_{t|S}, c_{|S};\ c \in \tilde{C}) \subset K(S).$$

(cf. Remark 3.13 (c)). We show that the image $(\phi_{|S})^*(K(Y))$ actually is equal to $K(S)$. Let $k \in \{m+3, \ldots, n\}$, $i \in \{2, \ldots, m+1\}$ and let $(P_1, \ldots, P_n)$ be a point configuration in S such that $P_k \in U_0 := \{(\xi_0 : \ldots : \xi_m) \in \mathbb{P}^m;\ \xi_k \neq 0\}$. Let $\xi_{k,0}, \ldots, \xi_{k,m}$ be homogeneous coordinates of P_k, i. e. $P_k = (\xi_{k,0} : \ldots : \xi_{k,m})$. Then we have

$$(c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,k,1})(P_1, \ldots, P_n) =$$

$$\frac{\begin{vmatrix} 0 & \cdots & \cdots & 0 & \delta_{1,i} & 1 \\ 1 & \ddots & & \vdots & \delta_{2,i} & 1 \\ 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & \delta_{m+1,i} & 1 \end{vmatrix}_{\widehat{i-1}} \cdot \begin{vmatrix} 0 & \cdots & \cdots & 0 & (\xi_{k,0})_{|S} & 1 \\ 1 & \ddots & & \vdots & (\xi_{k,1})_{|S} & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & (\xi_{k,m})_{|S} & 0 \end{vmatrix}_{\widehat{i-1}}}{\begin{vmatrix} 0 & \cdots & \cdots & 0 & \delta_{1,i} & (\xi_{k,0})_{|S} \\ 1 & \ddots & & \vdots & \delta_{2,i} & (\xi_{k,1})_{|S} \\ 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & \delta_{m+1,i} & (\xi_{k,m})_{|S} \end{vmatrix}_{\widehat{i-1}} \cdot \begin{vmatrix} 0 & \cdots & \cdots & 0 & 1 & 1 \\ 1 & \ddots & & \vdots & 1 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 1 & 0 \end{vmatrix}_{\widehat{i-1}}} = \frac{\xi_{k,i-1}}{\xi_{k,0}}.$$

Again, $\delta_{-,-}$ denotes the Kronecker symbol and $\widehat{i-1}$ at the right bottom of the matrices means that the $(i-1)$th column is omitted. Since the set of all point configurations $(P_1, \ldots, P_n) \in S$ such that $P_k \in U_0$ is a nonempty open subset of S, we get

$$(c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,k,1})_{|S} = \left(\frac{X_{k,i-1}}{X_{k,0}}\right)_{|S} \tag{4.2}$$

Similarly as in Example 3.37, it can be verified that the function field $K(S)$ is the field generated over the field K by the elements $(X_{k,j}/X_{k,0})_{|S}$ for $k \in \{m+3, \ldots, n\}$, $j \in \{1, \ldots, m\}$ and thus

$$K(S) = K(c_{|S};\ c \in \tilde{C}).$$

In particular, the image of $K(Y)$ under $(\phi_{|S})^*$ is equal to $K(S)$. It follows that the rational map $\phi_{|S} : S \dashrightarrow Y$ is a birational isomorphism (cf. Remark 3.13 (a)) and hence that S is a cross-section of a rational quotient of the PGL_{m+1}-variety $(\mathbb{P}^m)^n$. Furthermore by Remark 3.33, the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ is generated over K by the rational invariants contained in the set $\tilde{C}$, so clearly also by the rational invariants contained in the larger

set C. ∎

We can generalize this to the case where K is an arbitrary infinite field.

Theorem 4.7 (First fundamental theorem for the group $\mathbf{PGL_{m+1}}$). *The invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ is generated by the set of invariants*

$$C := \{c_{d_1,\dots,d_{m-1},i,j,k,l};\ d_1,\dots,d_{m-1},i,j,k,l \in \{1,\dots,n\}\ p.\,d.\}$$

as a field over K.

Proof. For the case that K is algebraically closed this has been shown in Proposition 4.6. Otherwise, let $\overline{K}$ be the algebraic closure of the field K. Clearly, the field $K(C)$ is contained in the invariant field $K((\mathbb{P}^m_K)^n)^{\mathrm{PGL}_{m+1}(K)}$. So it remains to show that

$$K((\mathbb{P}^m_K)^n)^{\mathrm{PGL}_{m+1}(K)} \subset K(C). \tag{4.3}$$

Note that every rational function on $(\mathbb{P}^m_K)^n$ can be regarded naturally as a rational function on $(\mathbb{P}^m_{\overline{K}})^n$, hence we have the inclusion

$$K((\mathbb{P}^m_K)^n) \subset \overline{K}((\mathbb{P}^m_{\overline{K}})^n).$$

We first show that the invariant field $K((\mathbb{P}^m_K)^n)^{\mathrm{PGL}_{m+1}(K)}$ is contained in the invariant field $\overline{K}((\mathbb{P}^m_{\overline{K}})^n)^{\mathrm{PGL}_{m+1}(\overline{K})}$, i. e. we show that

$$K((\mathbb{P}^m_K)^n)^{\mathrm{PGL}_{m+1}(K)} \subset \overline{K}((\mathbb{P}^m_{\overline{K}})^n)^{\mathrm{PGL}_{m+1}(\overline{K})} = \overline{K}(C). \tag{4.4}$$

Assuming this, the inclusion (4.3) is not hard to see. For, recall that by Remark 2.25, we have the equality

$$K(C) = \overline{K}(C) \cap K(X_{1,1}/X_{1,0},\dots,X_{1,m}/X_{1,0},\dots,X_{n,1}/X_{n,0},\dots,X_{n,m}/X_{n,0})$$

and thus it follows

$$\begin{aligned}
&K((\mathbb{P}^m_K)^n)^{\mathrm{PGL}_{m+1}(K)}\\
&\quad= K((\mathbb{P}^m_K)^n)^{\mathrm{PGL}_{m+1}(K)} \cap K(X_{1,1}/X_{1,0},\dots,X_{1,m}/X_{1,0},\dots,X_{n,1}/X_{n,0},\dots,X_{n,m}/X_{n,0})\\
&\quad\subset \overline{K}(C) \cap K(X_{1,1}/X_{1,0},\dots,X_{1,m}/X_{1,0},\dots,X_{n,1}/X_{n,0},\dots,X_{n,m}/X_{n,0})\\
&\quad= K(C),
\end{aligned}$$

as desired.

For the proof of (4.4), let $f \in K((\mathbb{P}^m_K)^n)^{\mathrm{PGL}_{m+1}(K)}$ and let $\sigma \in \mathrm{PGL}_{m+1}(K)$. Then the rational function $f \in K((\mathbb{P}^m_K)^n)$ is equal to the rational function $\sigma(f) \in K((\mathbb{P}^m_K)^n)$. It follows by Lemma 4.2 that $f = \sigma(f) \in \overline{K}((\mathbb{P}^m_{\overline{K}})^n)$ as rational functions on $(\mathbb{P}^m_{\overline{K}})^n$ which

shows that $f \in \overline{K}((\mathbb{P}^m_{\overline{K}})^n)$ is invariant under the action of $\mathrm{PGL}_{m+1}(K)$.
It can be seen by a standard argument that the rational function f is also invariant under the action of all group elements in the Zariski closure $\overline{\mathrm{PGL}_{m+1}(K)} \subset \mathrm{PGL}_{m+1}(\overline{K})$ of $\mathrm{PGL}_{m+1}(K)$. We claim that

$$\begin{aligned} T :=& \big\{ \{ I_{m+1} + E_{i,j}(\lambda);\ i,j \in \{1,\dots,m+1\}, i \neq j, \lambda \in \overline{K} \} / \sim \big\} \\ & \subset \overline{\mathrm{PGL}_{m+1}(K)}, \end{aligned} \tag{4.5}$$

where I_{m+1} denotes the identity matrix of degree $m+1$, $E_{i,j}(\lambda)$ denotes the matrix with λ in the entry (i,j) and zero elsewhere and where as before two $(m+1)\times(m+1)$-matrices are equivalent under $\sim$ if and only if they differ by a nonzero multiplicative constant. Assume for a moment that (4.5) is true. Since the elements of T generate the group $\mathrm{PGL}_{m+1}(\overline{K})$ (cf. [Hup67], Chapter II, Satz 6.7), it is not hard to see that the rational function f is actually invariant under the action of the whole group $\mathrm{PGL}_{m+1}(\overline{K})$ (for some hints about how this can be deduced, see Corollary 1.4). Therefore, the rational function f is an element of $\overline{K}((\mathbb{P}^m_{\overline{K}})^n)^{\mathrm{PGL}_{m+1}(\overline{K})}$ and (4.4) follows.

It remains to prove (4.5). Suppose that a homogeneous polynomial p vanishes at all elements of the group $\mathrm{PGL}_{m+1}(K)$, i. e. $p \in \mathrm{Id}^+(\mathrm{PGL}_{m+1}(K))$. Fix some distinct elements $i,j \in \{1,\dots,m+1\}$. By the choice of p, we must have

$$p(I_{m+1} + E_{i,j}(\lambda)) = 0 \quad \text{for all } \lambda \in K.$$

This implies that the polynomial $p(I_{m+1} + E_{i,j}(Y)) \in \overline{K}[Y]$, where Y is an indeterminate over $\overline{K}$, has infinitely many zeroes. It follows that $p(I_{m+1} + E_{i,j}(Y)) \in \overline{K}[Y]$ is the zero polynomial and hence that

$$p(I_{m+1} + E_{i,j}(\lambda)) = 0 \text{ for all } \lambda \in \overline{K}.$$

But this shows that $T \subset \mathrm{Z}^+(\mathrm{Id}^+(\mathrm{PGL}_{m+1}(K))) = \overline{\mathrm{PGL}_{m+1}(K)}$, as claimed. ∎

Remark 4.8. It can be seen from the proofs of Proposition 4.6 and Theorem 4.7 that the transcendental degree $\mathrm{trdeg}_K(K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}})$ of the invariant field is equal to $m \cdot (n - (m+2))$. The set of invariants

$$\tilde{C} := \{ c_{2,\dots,\hat{i},\dots,m+1,i,m+2,k,1};\ k \in \{m+3,\dots,n\}, i \in \{2,\dots,m+1\} \}.$$

gives a system of K-algebraically independent generators of the invariant field. Nonetheless – as we will see – it is often more convenient to work with the larger generating set C. ♢

Knowing generators of the invariant field, we can now examine their separating properties. In case that the field K is algebraically closed, it is known (cf. [Ros63]) that the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ separates the PGL_{m+1}-orbits of points contained in a nonempty open subset $\mathcal{O}$ of $(\mathbb{P}^m)^n$. In the following proposition, we show that this is true

as well if K is an arbitrary infinite field. Moreover, an open subset $\mathcal{O}$ with the desired properties will be given explicitly.

Proposition 4.9. *If $n \leq m+2$, then the PGL_{m+1}-orbit of the point configuration given by the first n points of $(1:0:\ldots:0),\ldots,(0:\ldots:0:1),(1:\ldots:1)$ is open in $(\mathbb{P}^m)^n$. In particular, the invariant field separates orbits in this nonempty open set.*
If $n > m+2$, then the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ separates the orbits in the PGL_{m+1}-stable nonempty open set

$$H := \{(P_1,\ldots,P_n) \in (\mathbb{P}^m)^n; \prod_{\substack{d_1,\ldots,d_{m+1}\in\{1,\ldots,n\}\\ d_1<\ldots<d_{m+1}}} [d_1,\ldots,d_{m+1}](P_1,\ldots,P_n) \neq 0\},$$

the set of point configurations $(P_1,\ldots,P_n) \in (\mathbb{P}^m)^n$ such that no $m+1$ of the points are in a hypersurface.

Proof. Let $n \leq m+2$. By Lemma 4.4, the orbit of the point configuration given by the first n points of $(1:0:\ldots:0),\ldots,(0:\ldots:0:1),(1:\ldots:1)$ can be seen to be the set of point configurations $(P_1,\ldots,P_n) \in (\mathbb{P}^m)^n$ such that at least one $n \times n$-minor of the $(m+1) \times n$-matrix whose ith column is given by homogeneous coordinates of the point P_i for $i \in \{1,\ldots,n\}$ is not zero. This is clearly an open set.
Let now $n > m+2$. Again, we consider the subset S of $(\mathbb{P}^m)^n$ as defined before Lemma 4.5. By Lemma 4.4, the intersection of the orbit $\mathrm{PGL}_{m+1}(P)$ with S is a one-point set for all points $P \in H$. Therefore, it is enough to show that the field of invariants separates the points in $S \cap H$. Let $(P_1,\ldots,P_n)$ and $(P'_1,\ldots,P'_n) \in (\mathbb{P}^m)^n$ be distinct points in $S \cap H$. Then there exists $k \in \{m+3,\ldots,n\}$ such that $P_k \neq P'_k$. Similarly as in the proof of 4.7 it can be verified that

$$c_{1,\ldots,\hat{l},\ldots,\hat{i},\ldots,m+1,i,m+2,k,l|S} = \left(\frac{X_{k,i-1}}{X_{k,l-1}}\right)_{|S}$$

for all $l \in \{1,\ldots,m+1\}$ and $i \in \{1,\ldots,\hat{l},\ldots,m+1\}$, where as usual the hat symbolizes that the corresponding index is omitted. It follows that the point configurations $(P_1,\ldots,P_n)$ and $(P'_1,\ldots,P'_n)$ can be separated by the invariants $c_{1,\ldots,\hat{l},\ldots,\hat{i},\ldots,m+1,i,m+2,k,l}$, $l \in \{1,\ldots,m+1\}$, $i \in \{1,\ldots,\hat{l},\ldots,m+1\}$. This shows that $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ separates the points in $S \cap H$, as desired. ∎

Theorem 4.7 provides a generating set C of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$. As mentioned before, actually a strictly smaller set of invariants is sufficient for generation of the invariant field. In the following, we want to analyse the redundancy of C, i. e. we aim to find the K-relations among the elements of C.
Let $C_{d_1,\ldots,d_{m-1},i,j,k,l}$ with $d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\}$ pairwise distinct be indeterminates over K and denote by R the polynomial ring over K in these indeterminates. We

want to find generators of the kernel of the K-homomorphism given by

$$\begin{aligned} R &\longrightarrow K((\mathbb{P}^m)^n)^{PGL_{m+1}}, \\ C_{d_1,\ldots,d_{m-1},i,j,k,l} &\longmapsto c_{d_1,\ldots,d_{m-1},i,j,k,l} \quad \text{for all } d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\} \text{ p. d.} \end{aligned} \tag{4.6}$$

First, we consider a special case, the $\mathrm{PGL}_2(\overline{\mathbb{Q}})$-variety $(\mathbb{P}^1_{\overline{\mathbb{Q}}})^4$. As we already know, the invariant field $\overline{\mathbb{Q}}((\mathbb{P}^1)^4)^{\mathrm{PGL}_2}$ is a simple field over $\overline{\mathbb{Q}}$ which is generated by the element $c_{2,3,4,1}$. Representing an element $c_{i,j,k,l}$ with $i,j,k,l \in \{1,2,3,4\}$ p. d. by means of $c_{2,3,4,1}$ clearly gives a $\overline{\mathbb{Q}}$-relation among the c's. Having such representations for all $c_{i,j,k,l}$ with $i,j,k,l \in \{1,2,3,4\}$ p. d., we will finally be able to completely describe the ideal of relations of the c's.
By definition, the invariant field $\overline{\mathbb{Q}}((\mathbb{P}^1)^4)^{\mathrm{PGL}_2}$ is a subfield of the field

$$\overline{\mathbb{Q}}((\mathbb{P}^1)^4) = \overline{\mathbb{Q}}(X_{1,1}/X_{1,0}, X_{2,0}/X_{2,1}, X_{3,1}/X_{3,0}, X_{4,1}/X_{4,0}).$$

We use Algorithm 3.27 for our problem of finding representations in the element $c_{2,3,4,1} \in \overline{\mathbb{Q}}((\mathbb{P}^1)^4)^{\mathrm{PGL}_2}$. Let $Y_1,\ldots,Y_4$ be indeterminates over $\overline{\mathbb{Q}}$ and let $F \in \overline{\mathbb{Q}}(Y_1,Y_2,Y_3,Y_4)$ be given by

$$F := \frac{Y_1Y_2Y_3 - Y_2Y_3Y_4 - Y_1 + Y_4}{Y_2Y_4Y_1 - Y_2Y_3Y_4 - Y_1 + Y_3}.$$

It is not hard to verify that F is a representation of the rational function $c_{2,3,4,1}$ in the elements $X_{1,1}/X_{1,0}$, $X_{2,0}/X_{2,1}, X_{3,1}/X_{3,0}, X_{4,1}/X_{4,0}$, i. e. that

$$F(X_{1,1}/X_{1,0}, X_{2,0}/X_{2,1}, X_{3,1}/X_{3,0}, X_{4,1}/X_{4,0}) = c_{2,3,4,1}.$$

Consider the rational map defined by

$$\phi : \mathbb{A}^4 \dashrightarrow \mathbb{A}^1,\ (\xi_1,\xi_2,\xi_3,\xi_4) \longmapsto F(\xi_1,\xi_2,\xi_3,\xi_4)$$

for all $(\xi_1,\xi_2,\xi_3,\xi_4)$ in some nonempty open subset of $\mathbb{A}^4$. We claim that the elements $l_1 = 0$, $l_2 = 0$, $l_3 = 1$ and $l_4 = F$ satisfy the conditions (a) and (b) of Proposition 3.21. Let Z_1,Z_2,Z_3 and Z_4 be indeterminates over $\overline{\mathbb{Q}}(Y_1,Y_2,Y_3,Y_4)$. By Proposition 2.21, the MQS ideal $J^{Y_1,Y_2,Y_3,Y_4}_{\overline{\mathbb{Q}}(F)} \trianglelefteq \overline{\mathbb{Q}}(Y_1,Y_2,Y_3,Y_4)[Z_1,Z_2,Z_3,Z_4]$ is given by the saturation ideal

$$\begin{aligned} J^{Y_1,Y_2,Y_3,Y_4}_{\overline{\mathbb{Q}}(F)} =& ((Z_1Z_2Z_3 - Z_2Z_3Z_4 - Z_1 + Z_4) \ - \ F \cdot (Z_2Z_4Z_1 - Z_2Z_3Z_4 - Z_1 + Z_3)) \\ & : (Z_2Z_4Z_1 - Z_2Z_3Z_4 - Z_1 + Z_3)^\infty. \end{aligned}$$

By definition of the saturation, it is not hard to verify that $p(l_1,l_2,l_3,l_4) = 0$ for all polynomials $p \in J^{Y_1,Y_2,Y_3,Y_4}_{\overline{\mathbb{Q}}(F)}$. Furthermore, the rational map ϕ is certainly defined on the whole subvariety $\hat{S} := \{(0,0,1,\xi_4);\ \xi_4 \in \overline{\mathbb{Q}}\} \subset \mathbb{A}^4$, the subvariety of $\mathbb{A}^4$ which is defined by the ideal of relations of the elements l_1,l_2,l_3,l_4 over $\overline{\mathbb{Q}}$.
We can hence represent the elements $c_{i,j,k,l}$ with $i,j,k,l \in \{1,2,3,4\}$ pairwise distinct as rational functions in $c_{2,3,4,1}$: We just need to find a representation $F_c \in \overline{\mathbb{Q}}(Y_1,Y_2,Y_3,Y_4)$

of the respective element c in $X_{1,1}/X_{1,0}, X_{2,0}/X_{2,1}, X_{3,1}/X_{3,0}, X_{4,1}/X_{4,0}$, i.e.

$$F_c(X_{1,1}/X_{1,0}, X_{2,0}/X_{2,1}, X_{3,1}/X_{3,0}, X_{4,1}/X_{4,0}) = c,$$

such that the denominator of F_c does not vanish if we replace Y_1 by 0, Y_2 by 0, Y_3 by 1 and Y_4 by F.
Exemplarily, we do this for the element $c_{1,2,3,4}$. First, we write $c_{1,2,3,4}$ in the elements $X_{1,1}/X_{1,0}, X_{2,0}/X_{2,1}, X_{3,1}/X_{3,0}, X_{4,1}/X_{4,0}$. It can be checked without difficulties that

$$c_{1,2,3,4} = \frac{\frac{X_{4,1}}{X_{4,0}} - \frac{X_{3,1}}{X_{3,0}} - \frac{X_{1,1}}{X_{1,0}} \cdot \frac{X_{2,0}}{X_{2,1}} \cdot \frac{X_{4,1}}{X_{4,0}} + \frac{X_{1,1}}{X_{1,0}} \cdot \frac{X_{2,0}}{X_{2,1}} \cdot \frac{X_{3,1}}{X_{3,0}}}{\frac{X_{2,0}}{X_{2,1}} \cdot \frac{X_{3,1}}{X_{3,0}} \cdot \frac{X_{4,1}}{X_{4,0}} - \frac{X_{1,1}}{X_{1,0}} \cdot \frac{X_{2,0}}{X_{2,1}} \cdot \frac{X_{4,1}}{X_{4,0}} - \frac{X_{3,1}}{X_{3,0}} + \frac{X_{1,1}}{X_{1,0}}}. \tag{4.7}$$

So let

$$F_{c_{1,2,3,4}} := \frac{Y_4 - Y_3 - Y_1Y_2Y_4 + Y_1Y_2Y_3}{Y_2Y_3Y_4 - Y_1Y_2Y_4 - Y_3 + Y_1}.$$

Replacing Y_1 by 0, Y_2 by 0, Y_3 by 1 and Y_4 by F gives

$$F_{c_{1,2,3,4}} = 1 - F,$$

which – after a replacement of $Y_1, \ldots, Y_4$ by $X_{1,1}/X_{1,0}, X_{2,0}/X_{2,1}, X_{3,1}/X_{3,0}, X_{4,1}/X_{4,0}$ – means that

$$c_{1,2,3,4} = 1 - c_{2,3,4,1}.$$

Doing this with all the c's gives

$$\begin{array}{llll}
c_{1,4,3,2} = & c_{2,3,4,1} = & c_{3,2,1,4} = & c_{4,1,2,3} = \quad c_{2,3,4,1} \\
c_{1,2,4,3} = & c_{2,1,3,4} = & c_{3,4,2,1} = & c_{4,3,1,2} = \quad \dfrac{c_{2,3,4,1} - 1}{c_{2,3,4,1}} \\
c_{1,3,2,4} = & c_{2,4,1,3} = & c_{3,1,4,2} = & c_{4,2,3,1} = \quad \dfrac{1}{1 - c_{2,3,4,1}} \\
c_{1,3,4,2} = & c_{2,4,3,1} = & c_{3,1,2,4} = & c_{4,2,1,3} = \quad \dfrac{1}{c_{2,3,4,1}} \\
c_{1,4,2,3} = & c_{2,3,1,4} = & c_{3,2,4,1} = & c_{4,1,3,2} = \quad \dfrac{c_{2,3,4,1}}{c_{2,3,4,1} - 1} \\
c_{1,2,3,4} = & c_{2,1,4,3} = & c_{3,4,1,2} = & c_{4,3,2,1} = \quad 1 - c_{2,3,4,1}
\end{array}$$

From that we can deduce all K-relations of the elements $c_{i,j,k,l}$ with $i, j, k, l \in \{1, 2, 3, 4\}$ pairwise distinct. This will not be carried out here explicitly. Instead, we move along to the next theorem which gives a general description of all relations of the c's for arbitrary dimensions.

Theorem 4.10 (Second fundamental theorem for the group $\mathbf{PGL_{m+1}}$). *With the notation of* (4.6)*, the ideal of relations*

$$I \trianglelefteq K[C_{d_1,\ldots,d_{m-1},i,j,k,l};\ d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\}\ p.\,d.]$$

of the elements in the set $C := \{c_{d_1,\ldots,d_{m-1},i,j,k,l};\ d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\}\ p.\,d.\}$ *is generated by the following relations:*

$$C_{d_1,\ldots,d_{m-1},i,j,k,l} - C_{\pi(d_1),\ldots,\pi(d_{m-1}),i,j,k,l} \quad \text{for all } \pi \in \mathrm{S}_{\{d_1,\ldots,d_{m-1}\}} \tag{4.8}$$

$$\begin{aligned} &C_{d_1,\ldots,d_{m-1},i,j,k,l} - C_{d_1,\ldots,d_{m-1},j,i,l,k} \\ &C_{d_1,\ldots,d_{m-1},i,j,k,l} - C_{d_1,\ldots,d_{m-1},k,l,i,j} \\ &C_{d_1,\ldots,d_{m-1},i,j,k,l} - C_{d_1,\ldots,d_{m-1},l,k,j,i} \end{aligned} \tag{4.9}$$

$$C_{d_1,\ldots,d_{m-1},i,j,k,l} \cdot C_{d_1,\ldots,d_{m-1},i,k,j,l} - 1 \tag{4.10}$$

$$C_{d_1,\ldots,d_{m-1},i,j,k,l} + C_{d_1,\ldots,d_{m-1},i,l,k,j} - 1 \tag{4.11}$$

$$C_{d_1,\ldots,d_{m-1},i,j,k,l} - C_{i,d_2,\ldots,d_{m-1},d_1,j,k,l} \cdot C_{l,d_2,\ldots,d_{m-1},i,j,k,d_1} \tag{4.12}$$

$$C_{d_1,\ldots,d_{m-1},i,j,k,l} - C_{d_1,\ldots,d_{m-1},r,j,k,l} \cdot C_{d_1,\ldots,d_{m-1},i,j,k,r} \tag{4.13}$$

for all pairwise distinct $d_1,\ldots,d_{m-1},i,j,k,l,r \in \{1,\ldots,n\}$*, where* $\mathrm{S}_{\{d_1,\ldots,d_{m-1}\}}$ *denotes the symmetric group on the set* $\{d_1,\ldots,d_{m-1}\}$*.*

Proof. First, we show that (4.8)-(4.13) actually are relations. For (4.8)-(4.10), (4.12) and (4.13) this is a straightforward verification. Only relation (4.11) requires some more attention. Let $d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\}$ be pairwise distinct. We claim that the rational function $c_{d_1,\ldots,d_{m-1},i,j,k,l} + c_{d_1,\ldots,d_{m-1},i,l,k,j} - 1$ is equal to zero on the nonempty open subset

$$H = \Big\{(P_1,\ldots,P_n) \in (\mathbb{P}^m)^n;\ \prod_{\substack{\hat{d}_1,\ldots,\hat{d}_{m+1} \in \{1,\ldots,n\} \\ \hat{d}_1 < \ldots < \hat{d}_{m+1}}} [\hat{d}_1,\ldots,\hat{d}_{m+1}](P_1,\ldots,P_n) \neq 0\Big\} \subset (\mathbb{P}^m)^n,$$

which by Lemma 4.2 proves the correctness of relation (4.11).
Let $S_{d_1,\ldots,d_{m-1},i,j,k}$ be the subvariety of $(\mathbb{P}^m)^n$ given by

$$\begin{aligned} S_{d_1,\ldots,d_{m-1},i,j,k} := \{&(P_1,\ldots,P_n) \in (\mathbb{P}^m)^n; \\ &P_{d_1} = (1:0:\ldots:0),\ldots,P_{d_{m-1}} = (0:\ldots:0:1:0:0), \\ &P_i = (0:\ldots:0:1:0), \\ &P_j = (0:\ldots:0:1), \\ &P_k = (1:\ldots:1)\}. \end{aligned}$$

By Lemma 4.4, it follows that $\mathrm{PGL}_{m+1}(S_{d_1,\ldots,d_{m-1},i,j,k}) \supset H$. Since the rational maps $c_{d_1,\ldots,d_{m-1},i,j,k,l}$ and $c_{d_1,\ldots,d_{m-1},i,l,k,j}$ are invariants, we see that

$$(c_{d_1,\ldots,d_{m-1},i,j,k,l} + c_{d_1,\ldots,d_{m-1},i,l,k,j} - 1)_{|H} = 0$$

if and only if

$$(c_{d_1,\ldots,d_{m-1},i,j,k,l} + c_{d_1,\ldots,d_{m-1},i,l,k,j} - 1)_{|S_{d_1,\ldots,d_{m-1},i,j,k}} = 0.$$

Let $(P_1,\ldots,P_n)$ be a point in $S_{d_1,\ldots,d_{m-1},i,j,k}$ where $P_l = (\xi_{l,0} : \ldots : \xi_{l,m})$ with $\xi_{l,m-1} \neq 0$. It can be checked that

$$(c_{d_1,\ldots,d_{m-1},i,j,k,l} + c_{d_1,\ldots,d_{m-1},i,l,k,j} - 1)(P) = \left(\frac{\xi_{l,m} - \xi_{l,m-1}}{-\xi_{l,m-1}} + \frac{\xi_{l,m}}{\xi_{l,m-1}}\right) - 1 = 0.$$

Since the set of all such points $(P_1,\ldots,P_n) \in S_{d_1,\ldots,d_{m-1},i,j,k}$ is a nonempty open subset of the subvariety $S_{d_1,\ldots,d_{m-1},i,j,k}$, it follows by the above that (4.11) is a relation, indeed.

It remains to show that the given relations actually generate the whole ideal of relations $I \trianglelefteq K[C_{d_1,\ldots,d_{m-1},i,j,k,l};\ d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\},\ \text{p. d.}]$. As before, let R be the polynomial ring over K in the indeterminates $C_{d_1,\ldots,d_{m-1},i,j,k,l}$, $d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\}$ pairwise distinct. We denote by $\hat{I} \trianglelefteq R$ the ideal generated by the relations (4.8)-(4.13). Let $\hat{R}$ be the subalgebra of R defined by

$$\hat{R} := K[C_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,k,1};\ k \in \{m+3,\ldots,n\}, i \in \{2,\ldots,m+1\}] \subset R$$

and let $Q\hat{R}$ be the subalgebra of $R/\hat{I}$ given by

$$Q\hat{R} := (K[\hat{r} + \hat{I};\ \hat{r} \in \hat{R}] \cap (R/\hat{I})^\times)^{-1} \cdot K[\hat{r} + \hat{I};\ \hat{r} \in \hat{R}] \subset R/\hat{I}.$$

We claim that every $C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I}$ with $d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\}$ pairwise distinct lies in $Q\hat{R}$. Assume for a moment that this is true. Let $p \in I$ be a relation. It follows from the claim that there exist polynomials $g, h \in \hat{R}$ with $h + \hat{I} \in K[\hat{r} + \hat{I};\ \hat{r} \in \hat{R}] \cap (R/\hat{I})^\times$ such that

$$(h + \hat{I}) \cdot (p + \hat{I}) = g + \hat{I}.$$

From the fact that p is a relation it follows that g is a relation, too, i. e. $g \in I$. Since by Remark 4.8 the elements $c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,k,1}$, $k \in \{m+3,\ldots,n\}$, $i \in \{2,\ldots,m+1\}$ are algebraically independent over K, we have $\hat{R} \cap I = 0$. It follows that actually $g = 0 \in R$. Thus we have

$$(h + \hat{I}) \cdot (p + \hat{I}) = g + \hat{I} = 0 \in R/\hat{I}.$$

By the choice of h, this implies $p + \hat{I} = 0 \in R/\hat{I}$ and hence $p \in \hat{I}$. This proves that the ideal I is equal to $\hat{I}$, as desired.

It remains to prove the claim. Let $d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\}$ be pairwise distinct. We will proceed in several steps. First, we show that

$$C_{d_1,\ldots,d_{m-1},\pi(i),\pi(j),\pi(k),\pi(l)} + \hat{I} \in Q\hat{R} \implies C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I} \in Q\hat{R} \tag{4.14}$$

for all $\pi \in \mathrm{S}_{\{i,j,k,l\}}$. If π is one of the permutations $(i,j)(k,l), (i,l)(j,k), (i,k)(j,l)$ or (j,l), then the assertion is immediate by the relations (4.9) and (4.11). Furthermore, note that in case that π is equal to (j,k), the element $C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I} \in R/\hat{I}$ is just the inverse of the element $C_{d_1,\ldots,d_{m-1},\pi(i),\pi(j),\pi(k),\pi(l)} + \hat{I} \in Q\hat{R} \subset R/\hat{I}$. Let $g + \hat{I} \in K[\hat{r} + \hat{I};\ \hat{r} \in \hat{R}]$ and $h + \hat{I} \in K[\hat{r} + \hat{I};\ \hat{r} \in \hat{R}] \cap (R/\hat{I})^\times$ such that

$$C_{d_1,\ldots,d_{m-1},i,k,j,l} + \hat{I} = (h + \hat{I})^{-1} \cdot (g + \hat{I}).$$

Since $h + \hat{I}$ and $C_{d_1,\ldots,d_{m-1},i,k,j,l} + \hat{I}$ are elements in $(R/\hat{I})^\times$ (cf. relation (4.10)) and $g + \hat{I}$ is an element in $K[\hat{r} + \hat{I};\ \hat{r} \in \hat{R}]$, this implies

$$(g + \hat{I}) = (h + \hat{I}) \cdot (C_{d_1,\ldots,d_{m-1},i,k,j,l} + \hat{I}) \in K[\hat{r} + \hat{I};\ \hat{r} \in \hat{R}] \cap (R/\hat{I})^\times,$$

and hence

$$C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I} = (g + \hat{I})^{-1} \cdot (h + \hat{I}) \in Q\hat{R}.$$

So the assertion (4.14) is true in that case, too. As the symmetric group $\mathrm{S}_{\{i,j,k,l\}}$ is generated by the permutations $(i,j)(k,l), (i,l)(j,k), (i,k), (j,l), (j,k) \in \mathrm{S}_{\{i,j,k,l\}}$, the validity of (4.14) follows by a straightforward induction argument.

Next we show that for all $s \in \{2, \ldots, m+1\}$ we have the implication

$$\begin{aligned} &\{C_{d'_1,\ldots,d'_{m-1},i',j',k',l'} + \hat{I};\ d'_1, \ldots, d'_{m-1}, i', j', k', l' \in \{1, \ldots, n\} \text{ p. d. with} \\ &\qquad \{2, \ldots, s\} \subset \{d'_1, \ldots, d'_{m-1}, i'\}\} \subset Q\hat{R} \\ \implies &\{C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I};\ d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\} \text{ p. d. with} \\ &\qquad \{2, \ldots, s-1\} \subset \{d_1, \ldots, d_{m-1}, i\}\} \subset Q\hat{R}. \end{aligned} \tag{4.15}$$

Note that if we assume the validity of (4.15), then we clearly also have the implication

$$\begin{aligned} &\{C_{d'_1,\ldots,d'_{m-1},i',j',k',l'} + \hat{I};\ d'_1, \ldots, d'_{m-1}, i', j', k', l' \in \{1, \ldots, n\} \text{ p. d. with} \\ &\qquad \{2, \ldots, m+1\} = \{d'_1, \ldots, d'_{m-1}, i'\}\} \subset Q\hat{R} \\ \implies &\{C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I};\ d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\} \text{ p. d.}\} \subset Q\hat{R}. \end{aligned} \tag{4.16}$$

To prove (4.15), let $s \in \{2, \ldots, m+1\}$ and assume that $C_{d'_1,\ldots,d'_{m-1},i',j',k',l'} + \hat{I} \in Q\hat{R}$ for all pairwise distinct elements $d'_1, \ldots, d'_{m-1}, i', j', k', l' \in \{1, \ldots, n\}$ with $\{2, \ldots, s\} \subset \{d'_1, \ldots, d'_{m-1}, i'\}$. Let $d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\}$ be pairwise distinct elements with $\{2, \ldots, s-1\} \subset \{d_1, \ldots, d_{m-1}, i\}$ but $s \notin \{d_1, \ldots, d_{m-1}, i\}$. Assume first that actually

$\{2,\dots,s-1\} \subset \{d_1,\dots,d_{m-1}\}$. If $s \in \{j,k,l\}$, then the assertion follows from implication (4.14) by the assumption, since there exists a permutation $\pi \in \mathrm{S}_{\{i,j,k,l\}}$ such that $\pi(i) = s$. Otherwise, we have by relation (4.13) the equality

$$C_{d_1,\dots,d_{m-1},i,j,k,l} + \hat{I} = \left(C_{d_1,\dots,d_{m-1},s,j,k,l} \cdot C_{d_1,\dots,d_{m-1},i,j,k,s}\right) + \hat{I}. \tag{4.17}$$

By what we have already proved, the element $C_{d_1,\dots,d_{m-1},i,j,k,s} + \hat{I}$ is in $Q\hat{R}$. Moreover by assumption, the element $C_{d_1,\dots,d_{m-1},s,j,k,l} + \hat{I}$ is in $Q\hat{R}$. It follows that the element on the right hand side of equation (4.17) is in $Q\hat{R}$ and hence also $C_{d_1,\dots,d_{m-1},i,j,k,l} + \hat{I} \in Q\hat{R}$. So the assertion is true if $\{2,\dots,s-1\} \subset \{d_1,\dots,d_{m-1}\}$. Note that if $s = 2$, then $\{2,\dots,s-1\} = \emptyset$, which is contained in any set, in particular in the set $\{d_1,\dots,d_{m-1}\}$. So the claim (4.15) is proved for that case.
Let now s be at least 3, that means m is at least 2, and assume that $\{2,\dots,s-1\} \subset \{d_1,\dots,d_{m-1},i\}$ but $\{2,\dots,s-1\} \nsubseteq \{d_1,\dots,d_{m-1}\}$. Observe that this means that $i \in \{2,\dots,s-1\}$. Moreover, at least one of $d_1,\dots,d_{m-1}$, say d_t with $t \in \{1,\dots,m-1\}$, is not in $\{2,\dots,s-1\}$. For, otherwise we had $\{d_1,\dots,d_{m-1}\} \subset \{2,\dots,s-1\} \setminus \{i\}$ and thus $m-1 = |\{d_1,\dots,d_{m-1}\}| \leq |\{2,\dots,s-1\} \setminus \{i\}| \leq s-3 \leq m-2$, a contradiction. Let $\tau \in \mathrm{S}_{\{d_1,\dots,d_{m-1}\}}$ such that $\tau(d_1) = d_t$.
If $l = s$, then by relation (4.8) and by relation (4.12), we get the equality

$$\begin{aligned} C_{d_1,\dots,d_{m-1},i,j,k,l} + \hat{I} &= C_{\tau(d_1),\dots,\tau(d_{m-1}),i,j,k,s} + \hat{I} \\ &= \left(C_{i,\tau(d_2),\dots,\tau(d_{m-1}),\tau(d_1),j,k,s} \cdot C_{s,\tau(d_2),\dots,\tau(d_{m-1}),i,j,k,\tau(d_1)}\right) + \hat{I}. \end{aligned}$$

By what we have already proved, the element $C_{i,\tau(d_2),\dots,\tau(d_{m-1}),\tau(d_1),j,k,s} + \hat{I}$ is in $Q\hat{R}$. Furthermore by assumption, the element $C_{s,\tau(d_2),\dots,\tau(d_{m-1}),i,j,k,\tau(d_1)} + \hat{I}$ is in $Q\hat{R}$. It follows that the element on the right hand side of the equation is in $Q\hat{R}$ and hence also $C_{d_1,\dots,d_{m-1},i,j,k,l} + \hat{I} \in Q\hat{R}$.
Next, suppose that at least $s \in \{j,k,l\}$. Let $\pi \in \mathrm{S}_{\{i,j,k,l\}}$ be a permutation with $\pi(i) = i$ and $\pi(l) = s$. Since by the above the element $C_{d_1,\dots,d_{m-1},\pi(i),\pi(j),\pi(k),\pi(l)} + \hat{I}$ is in $Q\hat{R}$, it follows by the implication (4.14) that we also have $C_{d_1,\dots,d_{m-1},i,j,k,l} + \hat{I} \in Q\hat{R}$. Otherwise, if $s \notin \{j,k,l\}$, then relation (4.13) yields the equality

$$C_{d_1,\dots,d_{m-1},j,i,k,l} + \hat{I} = (C_{d_1,\dots,d_{m-1},s,i,k,l} \cdot C_{d_1,\dots,d_{m-1},j,i,k,s}) + \hat{I}. \tag{4.18}$$

Let $\pi_1 \in \mathrm{S}_{\{s,i,k,l\}}$ and $\pi_2 \in \mathrm{S}_{\{j,i,k,s\}}$ be permutations with $\pi_1(s) = i$, $\pi_1(l) = s$ and $\pi_2(j) = i$, $\pi_2(s) = s$. By the cases that we have already proved we know that the elements $C_{d_1,\dots,d_{m-1},\pi_1(s),\pi_1(i),\pi_1(k),\pi_1(l)} + \hat{I}$ and $C_{d_1,\dots,d_{m-1},\pi_2(j),\pi_2(i),\pi_2(k),\pi_2(s)}) + \hat{I}$ are both in $Q\hat{R}$. Therefore, we deduce by the implication (4.14) that the element on the right hand side of equation (4.18) is in $Q\hat{R}$. Hence also $C_{d_1,\dots,d_{m-1},j,i,k,l} \in Q\hat{R}$. It follows again by the implication (4.14) that the element $C_{d_1,\dots,d_{m-1},i,j,k,l} + \hat{I}$ lies in $Q\hat{R}$, too. This proves assertion (4.15).

Finally, we show that the set of elements $\{C_{d_1,\dots,d_{m-1},i,j,k,l} + \hat{I};\ d_1,\dots,d_{m-1},i,j,k,l \in \{1,\dots,n\}$ p. d. with $\{2,\dots,m+1\} = \{d_1,\dots,d_{m-1},i\}\}$ is a subset of $Q\hat{R}$.

Let $d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\}$ be pairwise distinct with $\{d_1, \ldots, d_{m-1}, i\} = \{2, \ldots, m+1\}$. If $j = m+2$ and $l = 1$, then by definition of $Q\hat{R}$ and of $\hat{R}$ we clearly have $C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I} \in Q\hat{R}$. If at least $m+2$ and 1 are in the set $\{j, k, l\}$, then it follows from (4.14) by taking $\pi \in \mathrm{S}_{\{i,j,k,l\}}$ with $\pi(j) = m+2$ and $\pi(l) = 1$ that $C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I}$ is in $Q\hat{R}$. In case that 1 is not in $\{j, k, l\}$ but at least $m+2 \in \{j, k, l\}$, we take a permutation $\pi \in \mathrm{S}_{\{i,j,k,l\}}$ with $\pi(j) = i$ and $\pi(k) = m+2$. By relation (4.13), we have

$$\begin{aligned} C_{d_1,\ldots,d_{m-1},\pi(i),\pi(j),\pi(k),\pi(l)} + \hat{I} &= C_{d_1,\ldots,d_{m-1},\pi(i),i,m+2,\pi(l)} + \hat{I} \\ &= (C_{d_1,\ldots,d_{m-1},1,i,m+2,\pi(l)} \cdot C_{d_1,\ldots,d_{m-1},\pi(i),i,m+2,1}) + \hat{I}. \end{aligned}$$

Again by (4.14) – since the elements $C_{d_1,\ldots,d_{m-1},i,m+2,\pi(l),1} + \hat{I}$ and $C_{d_1,\ldots,d_{m-1},i,m+2,\pi(i),1} + \hat{I}$ are in $Q\hat{R}$ – we see that the element $C_{d_1,\ldots,d_{m-1},1,i,m+2,\pi(l)} + \hat{I}$ as well as the element $C_{d_1,\ldots,d_{m-1},\pi(i),i,m+2,1} + \hat{I}$ is in $Q\hat{R}$. This shows that the element $C_{d_1,\ldots,d_{m-1},\pi(i),\pi(j),\pi(k),\pi(l)} + \hat{I}$ lies in $Q\hat{R}$ and by implication (4.14) also that $C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I}$ is in $Q\hat{R}$.
Suppose now that $m+2 \notin \{j, k, l\}$. Let $\pi \in \mathrm{S}_{\{i,j,k,l\}}$ such that $\pi(j) = i$. Then by relation (4.13),

$$\begin{aligned} C_{d_1,\ldots,d_{m-1},\pi(i),\pi(j),\pi(k),\pi(l)} + \hat{I} &= C_{d_1,\ldots,d_{m-1},\pi(i),i,\pi(k),\pi(l)} + \hat{I} \\ &= C_{d_1,\ldots,d_{m-1},m+2,i,\pi(k),\pi(l)} \cdot C_{d_1,\ldots,d_{m-1},\pi(i),i,\pi(k),m+2} + \hat{I}. \end{aligned}$$

It follows from implication (4.14) and from what we have already proved that the element on the right hand side of the equation is in $Q\hat{R}$. Hence also $C_{d_1,\ldots,d_{m-1},\pi(i),\pi(j),\pi(k),\pi(l)} + \hat{I} \in Q\hat{R}$. Finally, a last application of the implication (4.14) shows that $C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I}$ is in $Q\hat{R}$, too.
This proves that all the elements $C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I}$, $d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\}$ p. d. with $\{d_1, \ldots, d_{m-1}, i\} = \{2, \ldots, m+1\}$ are contained in $Q\hat{R}$.
By the implication (4.16), this proves that all the elements $C_{d_1,\ldots,d_{m-1},i,j,k,l} + \hat{I}$ with $d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\}$ pairwise distinct are in $Q\hat{R}$, as claimed. ∎

Recall that by Remark 4.8, the set

$$\tilde{C} := \{c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,k,1};\ k \in \{m+3, \ldots, n\}, i \in \{2, \ldots, m+1\}\}$$

gives a system of algebraically independent generators of $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$. As we will see later, it is sometimes convenient to know representations of all c's in terms of the elements of $\tilde{C}$. Now – knowing the relations among the c's by the previous theorem – it is not a hard task to find these representations. In the following example, this will be done for the case $m = 3$, $n = 6$.

Example 4.11. Let $K := \overline{\mathbb{Q}}$. We know that the invariant field $K((\mathbb{P}^3)^6)^{\mathrm{PGL}_4}$ is generated by the elements of $C := \{c_{d_1,d_2,i,j,k,l};\ d_1, d_2, i, j, k, l \in \{1, \ldots, 6\}$ p. d.$\}$. Moreover, we

know that by Remark 4.8, any such element can be represented as a rational function in the elements $c_{3,4,2,5,6,1}, c_{2,4,3,5,6,1}, c_{2,3,4,5,6,1}$. In the following, Algorithm 3.27 and Theorem 4.10 will be used to determine these representations.
Consider the inclusion of fields

$$\begin{aligned} K(c_{3,4,2,5,6,1}, c_{2,4,3,5,6,1}, c_{2,3,4,5,6,1}) \\ \subset K\Bigg(&\frac{X_{1,1}}{X_{1,0}}, \frac{X_{1,2}}{X_{1,0}}, \frac{X_{1,3}}{X_{1,0}}, \frac{X_{2,0}}{X_{2,1}}, \frac{X_{2,2}}{X_{2,1}}, \frac{X_{2,3}}{X_{2,1}}, \frac{X_{3,0}}{X_{3,2}}, \frac{X_{3,1}}{X_{3,2}}, \frac{X_{3,3}}{X_{3,2}}, \\ &\frac{X_{4,0}}{X_{4,3}}, \frac{X_{4,1}}{X_{4,3}}, \frac{X_{4,2}}{X_{4,3}}, \frac{X_{5,1}}{X_{5,0}}, \frac{X_{5,2}}{X_{5,0}}, \frac{X_{5,3}}{X_{5,0}}, \frac{X_{6,1}}{X_{6,0}}, \frac{X_{6,2}}{X_{6,0}}, \frac{X_{6,3}}{X_{6,0}}\Bigg). \end{aligned}$$

Let $Y_1, \ldots, Y_{18}$ be indeterminates over K and let $F_{c_{3,4,2,5,6,1}}$, $F_{c_{2,4,3,5,6,1}}$ and $F_{c_{2,3,4,5,6,1}} \in K(Y_1, \ldots, Y_{18})$ be representations of the elements $c_{3,4,2,5,6,1}$, $c_{2,4,3,5,6,1}$ and $c_{2,3,4,5,6,1}$ in $X_{1,1}/X_{1,0}, \ldots, X_{6,3}/X_{6,0}$, i.e.

$$\begin{aligned} c = F_c\Bigg(&\frac{X_{1,1}}{X_{1,0}}, \frac{X_{1,2}}{X_{1,0}}, \frac{X_{1,3}}{X_{1,0}}, \frac{X_{2,0}}{X_{2,1}}, \frac{X_{2,2}}{X_{2,1}}, \frac{X_{2,3}}{X_{2,1}}, \frac{X_{3,0}}{X_{3,2}}, \frac{X_{3,1}}{X_{3,2}}, \frac{X_{3,3}}{X_{3,2}}, \\ &\frac{X_{4,0}}{X_{4,3}}, \frac{X_{4,1}}{X_{4,3}}, \frac{X_{4,2}}{X_{4,3}}, \frac{X_{5,1}}{X_{5,0}}, \frac{X_{5,2}}{X_{5,0}}, \frac{X_{5,3}}{X_{5,0}}, \frac{X_{6,1}}{X_{6,0}}, \frac{X_{6,2}}{X_{6,0}}, \frac{X_{6,3}}{X_{6,0}}\Bigg) \end{aligned}$$

for $c \in \{c_{3,4,2,5,6,1}, c_{2,4,3,5,6,1}, c_{2,3,4,5,6,1}\}$. We may assume that the elements F_c, $c \in \{c_{3,4,2,5,6,1}, c_{2,4,3,5,6,1}, c_{2,3,4,5,6,1}\}$ are minimal in the sense that the numerator and the denominator are coprime.
The field $K(Y_1, \ldots, Y_{18})$ can be regarded as the function field of the affine space $\mathbb{A}^{18}$. Let $\phi : \mathbb{A}^{18} \dashrightarrow \mathbb{A}^3$ be the rational map given by

$$\phi := (F_{c_{3,4,2,5,6,1}}, F_{c_{2,4,3,5,6,1}}, F_{c_{2,3,4,5,6,1}}) : \mathbb{A}^{18} \longrightarrow \mathbb{A}^3$$

Though straightforward, a quite lengthy verification shows that the elements

$$\begin{aligned} &l_1, \ldots, l_{12} := 0 \\ &l_{13}, \ldots, l_{15} := 1 \\ &l_{16} := F_{c_{3,4,2,5,6,1}},\ l_{17} := F_{c_{2,4,3,5,6,1}},\ l_{18} := F_{c_{2,3,4,5,6,1}} \end{aligned}$$

in the field $K(F_{c_{3,4,2,5,6,1}}, F_{c_{2,4,3,5,6,1}}, F_{c_{2,3,4,5,6,1}}) \subset K(Y_1, \ldots, Y_{18})$ satisfy the conditions of Proposition 3.21 with respect to the rational map ϕ. In the same way as above, let $F_c \in K(Y_1, \ldots, Y_{18})$, $c \in C$ be representations of the elements in the set C in $X_{1,1}/X_{1,0}, \ldots, X_{6,3}/X_{6,0}$. By Algorithm 3.27 we get representations of the rational functions $F_c \in K(Y_1, \ldots, Y_{18})$ in $F_{c_{3,4,2,5,6,1}}$, $F_{c_{2,4,3,5,6,1}}$ and $F_{c_{2,3,4,5,6,1}}$ by replacing Y_i by l_i for

$i \in \{1, \ldots, 18\}$. Substituting $Y_1, \ldots, Y_{18}$ in the results by $X_{1,1}/X_{1,0}, \ldots, X_{6,3}/X_{6,0}$ yields

$$c_{5,6,1,2,3,4} = \frac{(-C_2 + C_3)(C_1 - 1)}{(-C_3 + C_1)(-C_2 + 1)} \qquad c_{1,4,2,3,5,6} = \frac{C_1 - C_2}{C_1} \qquad c_{4,5,1,2,3,6} = \frac{1 - C_1}{1 - C_2}$$
$$c_{3,6,1,2,4,5} = \frac{C_3(C_1 - 1)}{-C_1(1 - C_3)} \qquad c_{3,5,1,2,4,6} = \frac{1 - C_1}{1 - C_3} \qquad c_{3,4,1,2,5,6} = 1 - C_1$$
$$c_{2,6,1,3,4,5} = \frac{-C_3(1 - C_2)}{C_2(C_3 - 1)} \qquad c_{1,5,2,3,4,6} = \frac{C_1 - C_2}{C_1 - C_3} \qquad c_{2,4,1,3,5,6} = 1 - C_2$$
$$c_{1,6,2,3,4,5} = \frac{C_3(C_2 - C_1)}{-C_2(C_1 - C_3)} \qquad c_{1,2,3,4,5,6} = \frac{C_2 - C_3}{C_2 C_3} \qquad c_{2,5,1,3,4,6} = \frac{1 - C_2}{1 - C_3}$$
$$c_{4,6,1,2,3,4} = \frac{-C_2(1 + C_1)}{C_1(C_2 - 1)} \qquad c_{1,3,2,4,5,6} = \frac{C_1 - C_3}{C_1} \qquad c_{2,3,1,4,5,6} = 1 - C_3,$$

where we use the abbreviations $C_1 := c_{3,4,2,5,6,1}$, $C_2 := c_{2,4,3,5,6,1}$ and $C_3 := c_{2,3,4,5,6,1}$. Representations of the remaining elements in the set C can be deduced from these representations according to the relations given in Theorem 4.10. More explicitly, we have the equations

$$c_{d_1,d_2,i,j,l,k} = \frac{c_{d_1,d_2,i,j,k,l}}{c_{d_1,d_2,i,j,k,l} - 1}, \qquad c_{d_1,d_2,i,l,j,k} = \frac{c_{d_1,d_2,i,j,k,l} - 1}{c_{d_1,d_2,i,j,k,l}}$$
$$c_{d_1,d_2,i,l,k,j} = 1 - c_{d_1,d_2,i,j,k,l}, \qquad c_{d_1,d_2,i,k,j,l} = \frac{1}{c_{d_1,d_2,i,j,k,l}}$$
$$c_{d_1,d_2,i,k,l,j} = \frac{1}{1 - c_{d_1,d_2,i,j,k,l}}$$

for all pairwise distinct $d_1, d_2, i, j, k, l \in \{1, \ldots, 6\}$. Having these identities, it should be clear how to get representations of the remaining c's as rational functions in the elements C_1, C_2 and C_3. ◁

The previous proposition describes the set of all K-relations among the c's, which is convenient for calculations in the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$. Later, we will also need some 'non-relations' of the c's. Some of these are written down in the next proposition. As a useful tool for the following proofs, we define for all distinct elements $i, j \in \{1, \ldots, n\}$ a homomorphism of groups

$$\omega_{i,j} : K(X_{k,l};\ k \in \{1, \ldots, n\}, l \in \{0, \ldots, m\})^\times \longrightarrow (\mathbb{Z}, +).$$

Let $I_{i,j}$ be the ideal defined by

$$I_{i,j} := ((X_{i,0} - X_{j,0}), \ldots, (X_{i,m} - X_{j,m})) \trianglelefteq K[X_{k,l};\ k \in \{1, \ldots, n\}, l \in \{0, \ldots, m\}].$$

For a nonzero irreducible polynomial $p \in K[X_{k,l};\ k \in \{1, \ldots, n\}, l \in \{0, \ldots, m\}]$, the

homomorphism $\omega_{i,j}$ shall be specified by

$$\omega_{i,j} : p \longmapsto \begin{cases} 1 & \text{if } p \in I_{i,j} \\ 0 & \text{otherwise.} \end{cases} \tag{4.19}$$

Note that this defines the homomorphism $\omega_{i,j}$ uniquely. More precisely, if $p_1, \ldots, p_s$, $q_1, \ldots, q_t \in K[X_{k,l};\ k \in \{1, \ldots, n\}, l \in \{0, \ldots, m\}]$ are irreducible polynomials, then

$$\omega_{i,j}\left(\frac{\prod_{k=1}^{s} p_k}{\prod_{k=1}^{t} q_k}\right) = \sum_{k=1}^{s} \omega_{i,j}(p_k) - \sum_{k=1}^{t} \omega_{i,j}(q_k).$$

Lemma 4.12. *For some $i, j \in \{1, \ldots, n\}$ distinct, let $\omega_{i,j}$ be the map as defined a few lines above. Then*

$$\omega_{i,j}(c_{d'_1,\ldots,d'_{m-1},i',j',k',l'}) = \begin{cases} 1 & \text{if } \{i,j\} \in \{\{i',j'\},\{k',l'\}\} \\ -1 & \text{if } \{i,j\} \in \{\{i',k'\},\{j',l'\}\} \\ 0 & \text{otherwise} \end{cases} \tag{4.20}$$

for all pairwise distinct elements $d'_1, \ldots, d'_{m-1}, i', j', k', l' \in \{1, \ldots, n\}$.

Proof. Let $d_1, \ldots, d_{m+1} \in \{1, \ldots, n\}$ be pairwise distinct. Observe first that the bracket $[d_1, \ldots, d_{m+1}] \in K[X_{k,l};\ k \in \{1, \ldots, n\}, l \in \{0, \ldots, m\}]$ is an irreducible polynomial. If either i or j is not in the set $\{d_1, \ldots, d_{m+1}\}$, then the bracket $[d_1, \ldots, d_{m+1}]$ is clearly not contained in the ideal $I_{i,j} = ((X_{i,0} - X_{j,0}), \ldots, (X_{i,m} - X_{j,m}))$, hence $\omega_{i,j}([d_1, \ldots, d_{m+1}]) = 0$ in that case.
Suppose now that i and j are contained in the set $\{d_1, \ldots, d_{m+1}\}$. Since the bracket $[\pi(d_1), \ldots, \pi(d_{m+1})]$ with $\pi \in \mathrm{S}_{\{d_1,\ldots,d_{m+1}\}}$ is in the ideal $I_{i,j}$ if and only if $[d_1, \ldots, d_{m+1}]$ is in $I_{i,j}$, we may assume – by possibly changing the notation – that $d_1 = i$ and $d_2 = j$. From the equality

$$[d_1, \ldots, d_{m+1}] = [i, j, d_3, \ldots, d_{m+1}] - [j, j, d_3, \ldots, d_{m+1}]$$

it follows by Laplace expansion along the first columns of the elements on the right hand side of the equation that the bracket $[d_1, \ldots, d_{m+1}]$ lies in the ideal $I_{i,j}$. The lemma is now a straightforward verification. ∎

Proposition 4.13. *Let $n > m + 2$ and let $d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\}$ be pairwise distinct elements, let $d'_1, \ldots, d'_{m-1}, i', j', k', l' \in \{1, \ldots, n\}$ be pairwise distinct elements and let $d''_1, \ldots, d''_{m-1}, i'', j'', k'', l'' \in \{1, \ldots, n\}$ be pairwise distinct elements.*

(a) If $c_{d_1,\ldots,d_{m-1},i,j,k,l} = c_{d'_1,\ldots,d'_{m-1},i',j',k',l'}$, then we have

$$\{d'_1, \ldots, d'_{m-1}\} = \{d_1, \ldots, d_{m-1}\} \text{ and}$$
$$(i', j', k', l') \in \{(i,j,k,l), (j,i,l,k), (k,l,i,j), (l,k,j,i)\}.$$

(b) If $c_{d_1,\dots,d_{m-1},i,j,k,l} = c_{d'_1,\dots,d'_{m-1},i',j',k',l'} \cdot c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}$*, then we have*

$$\left|\{i,j,k,l,i',j',k',l',i'',j'',k'',l''\}\right| \in \{4,5\}$$

Proof. We use the maps $\omega_{i,j}$ with $i,j \in \{1,\dots,n\}$ distinct as defined in the discussion above. First, suppose that

$$c_{d_1,\dots,d_{m-1},i,j,k,l} = c_{d'_1,\dots,d'_{m-1},i',j',k',l'}.$$

By Lemma 4.12, we have

$$\begin{aligned}\omega_{i',j'}(c_{d_1,\dots,d_{m-1},i,j,k,l}) &= \omega_{i',j'}(c_{d'_1,\dots,d'_{m-1},i',j',k',l'}) = 1\\ \omega_{i',k'}(c_{d_1,\dots,d_{m-1},i,j,k,l}) &= \omega_{i',k'}(c_{d'_1,\dots,d'_{m-1},i',j',k',l'}) = -1,\end{aligned}$$

and hence

$$\begin{aligned}\{i',j'\} &\in \{\{i,j\},\{k,l\}\}\\ \{i',k'\} &\in \{\{i,k\},\{j,l\}\}.\end{aligned}$$

By a combinatorial argument it follows that the tuple (i',j',k',l') is one of

$$(i,j,k,l),(j,i,l,k),(k,l,i,j),(l,k,j,i).$$

In case that the dimension m is equal to 1, (a) is proved. So assume that m is at least 2. Recall the definition of $c_{d_1,\dots,d_{m-1},i,j,k,l}$ and $c_{d'_1,\dots,d'_{m-1},i',j',k',l'}$ and observe that the polynomial defined by the bracket $[d'_1,\dots,d'_{m-1},i',j']$ must be a divisor of $[d_1,\dots,d_{m-1},i,j] \cdot [d_1,\dots,d_{m-1},k,l]$, i.e.

$$[d'_1,\dots,d'_{m-1},i',j'] \mid [d_1,\dots,d_{m-1},i,j] \cdot [d_1,\dots,d_{m-1},k,l]. \tag{4.21}$$

Let $s \in \{d'_1,\dots,d'_{m-1}\}$. Since $X_{s,0}$ appears in the polynomial $[d'_1,\dots,d'_{m-1},i',j']$, it follows by (4.21) that $X_{s,0}$ appears in the polynomial $[d_1,\dots,d_{m-1},i,j] \cdot [d_1,\dots,d_{m-1},k,l]$, too. But this means that $s \in \{d_1,\dots,d_{m-1},i,j,k,l\}$. As this is true for all $s \in \{d'_1,\dots,d'_{m-1}\}$, this implies that $\{d'_1,\dots,d'_{m-1}\} \subset \{d_1,\dots,d_{m-1},i,j,k,l\}$. By the above, we already know that the set $\{i',j',k',l'\}$ is equal to $\{i,j,k,l\}$. Since we assumed $d'_1,\dots,d'_{m-1},i',j',k',l'$ to be pairwise distinct, it therefore follows that $\{d'_1,\dots,d'_{m-1}\}$ is contained in the set $\{d_1,\dots,d_{m-1}\}$, which is equivalent to

$$\{d'_1,\dots,d'_{m-1}\} = \{d_1,\dots,d_{m-1}\}.$$

For the proof of (b) let now

$$c_{d_1,\dots,d_{m-1},i,j,k,l} = c_{d'_1,\dots,d'_{m-1},i',j',k',l'} \cdot c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}.$$

Applying the group homomorphism $\omega_{i,j}$ yields the equality

$$1 = \omega_{i,j}(c_{d_1,\dots,d_{m-1},i,j,k,l}) = \omega_{i,j}(c_{d'_1,\dots,d'_{m-1},i',j',k',l'}) + \omega_{i,j}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}).$$

It follows that one of $\omega_{i,j}(c_{d'_1,\dots,d'_{m-1},i',j',k',l'})$ and $\omega_{i,j}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''})$ must be positive. Therefore, Lemma 4.12 implies

$$\{i,j\} \in \{\{i',j'\},\{k',l'\},\{i'',j''\},\{k'',l''\}\}.$$

By symmetry, we may assume that $\{i,j\} \in \{\{i',j'\},\{k',l'\}\}$. Furthermore, by possibly changing the notation, we may assume by relation (4.9) that actually $(i,j) = (i',j')$. So we get

$$c_{d_1,\dots,d_{m-1},i,j,k,l} = c_{d'_1,\dots,d'_{m-1},i,j,k',l'} \cdot c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}. \tag{4.22}$$

Applying the group homomorphism $\omega_{k,l}$ to this equality yields

$$1 = \omega_{k,l}(c_{d_1,\dots,d_{m-1},i,j,k,l}) = \omega_{k,l}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'}) + \omega_{k,l}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}).$$

In the same way as above it follows that one of the elements $\omega_{k,l}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'})$ and $\omega_{k,l}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''})$ must be positive and hence

$$\{k,l\} \in \{\{i,j\},\{k',l'\},\{i'',j''\},\{k'',l''\}\}.$$

Note that since the elements i,j,k and l are pairwise distinct, $\{k,l\}$ is actually contained in $\{\{k',l'\},\{i'',j''\},\{k'',l''\}\}$. Moreover, again by possibly changing the notation, we may assume by relation (4.9) that

$$\{k,l\} \in \{\{k',l'\},\{k'',l''\}\}. \tag{4.23}$$

Suppose first that we have $\{k,l\} = \{k',l'\}$, i. e. $\{i,j,k,l\} = \{i',j',k',l'\}$. Applying the group homomorphisms $\omega_{i'',j''}$ and $\omega_{k'',l''}$ to equality (4.22) then gives

$$\begin{aligned}
\omega_{i'',\,j''}(c_{d_1,\dots,d_{m-1},i,j,k,l}) &= \omega_{i'',\,j''}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'}) + \omega_{i'',\,j''}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}) \\
&= \omega_{i'',\,j''}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'}) + 1, \\
\omega_{k'',\,l''}(c_{d_1,\dots,d_{m-1},i,j,k,l}) &= \omega_{k'',\,l''}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'}) + \omega_{k'',\,l''}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}) \\
&= \omega_{k'',\,l''}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'}) + 1.
\end{aligned}$$

By Lemma 4.12, it follows that the elements i'' and j'' must be contained in $\{i,j,k,l\} = \{i,j,k',l'\}$. For, otherwise both $\omega_{i'',\,j''}(c_{d_1,\dots,d_{m-1},i,j,k,l})$ and $\omega_{i'',\,j''}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'})$ would be zero, a contradiction. Similarly, it follows that $k'',l'' \in \{i,j,k,l\}$. Thus we have

$$\{i,j,k,l,i',j',k',l',i'',j'',k'',l''\} = \{i,j,k,l\},$$

showing that (b) is true in that case.
Suppose now that we have $\{k,l\} = \{k'',l''\}$. Applying the group homomorphism $\omega_{i'',j''}$ to

the equation (4.22) gives

$$\begin{aligned}\omega_{i'',j''}(c_{d_1,\dots,d_{m-1},i,j,k,l}) &= \omega_{i'',j''}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'}) + \omega_{i'',j''}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}) \\ &= \omega_{i'',j''}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'}) + 1.\end{aligned}$$

Again, it follows by Lemma 4.12 that the elements i'' and j'' must be contained in the set $\{i,j,k,l,k',l'\}$. For, otherwise both $\omega_{i'',j''}(c_{d_1,\dots,d_{m-1},i,j,k,l})$ and $\omega_{i'',j''}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'})$ would be zero, a contradiction. Since $i = i'$, $j = j'$ and by assumption $\{k,l\} = \{k'',l''\}$, this gives

$$\{i,j,k,l,i',j',k',l',i'',j'',k'',l''\} = \{i,j,k,l,k',l'\}. \tag{4.24}$$

Applying the group homomorphism $\omega_{k',l'}$ to equation (4.22) yields

$$\begin{aligned}\omega_{k',l'}(c_{d_1,\dots,d_{m-1},i,j,k,l}) &= \omega_{k',l'}(c_{d'_1,\dots,d'_{m-1},i,j,k',l'}) + \omega_{k',l'}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}) \\ &= 1 + \omega_{k',l'}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''}).\end{aligned} \tag{4.25}$$

The only possible values for $\omega_{k',l'}(c_{d_1,\dots,d_{m-1},i,j,k,l})$ and $\omega_{k',l'}(c_{d''_1,\dots,d''_{m-1},i'',j'',k'',l''})$ are $-1, 0$ and 1 (cf. Lemma 4.12). It follows from equation (4.25) that either $\omega_{k',l'}(c_{d_1,\dots,d_{m-1},i,j,k,l})$ is equal to 1 or $\omega_{k',l'}(c_{d'_1,\dots,d'_{m-1},i'',j'',k'',l''})$ is equal to -1, which by Lemma 4.12 means that $\{k',l'\}$ is either one of $\{i,j\}$ and $\{k,l\}$ or one of $\{i'',k''\}$ and $\{j'',l''\}$. Since the elements i', j', k' and l' are pairwise distinct and $i' = i$, $j' = j$, this implies

$$\{k',l'\} \in \{\{k,l\},\{i'',k''\},\{j'',l''\}\}.$$

By the assumption $\{k'',l''\} = \{k,l\}$ and equation (4.24), it follows that in any of these cases we have

$$\big|\{i,j,k,l,i',j',k',l',i'',j'',k'',l''\}\big| \in \{4,5\},$$

as asserted. ∎

4.2 The Invariant Field $K((\mathbb{P}^m)^n)^{\mathbf{PGL}_{m+1} \times \mathbf{S}_n}$

In this section, we tackle the actual problem of finding a generating set of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$. By the previous section, we already know that the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}}$ of the action of the normal subgroup $\mathrm{PGL}_{m+1} \trianglelefteq \mathrm{PGL}_{m+1} \times \mathrm{S}_n$ is given by

$$K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}} = K(C),$$

where $C := \{c_{d_1,\dots,d_{m-1},i,j,k,l};\ d_1,\dots,d_{m-1},i,j,k,l \in \{1,\dots,n\} \text{ p. d.}\}$. As mentioned before, we have the equality

$$K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n} = (K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n} = K(C)^{\mathrm{S}_n},$$

where the action of the group S_n on $K(C)$ is defined by the action of the subgroup $1 \times \mathrm{S}_n \trianglelefteq \mathrm{PGL}_{m+1} \times \mathrm{S}_n$ on $K(C) \subset K((\mathbb{P}^m)^n)$, i.e.

$$\pi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) := c_{\pi(d_1),\ldots,\pi(d_{m-1}),\pi(i),\pi(j),\pi(k),\pi(l)}$$

for all $\pi \in \mathrm{S}_n$. Hence it remains to find all rational functions in the field $K(C)$ which are invariant under this action of the symmetric group S_n.

We will start with the case where the number of points n is equal to $m+3$. After that we will be able to solve the general case by considering the $\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}$-invariants of the sub-configurations of the point configurations in $(\mathbb{P}^m)^n$ of length $m+3$. At the end of this section, we will examine the separating properties of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}\times \mathrm{S}_n}$.

4.2.1 The Case $n = m + 3$

In this section, we will consider the special case where the number of points n is equal to $m+3$. It is our aim to find generators of the invariant field $K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1}\times \mathrm{S}_{m+3}} = K(C)^{\mathrm{S}_{m+3}}$. A central tool for finding such a generating set will be the following lemma.

Lemma 4.14 (Permutation lemma). *Let ϕ be a K-automorphism of the field $K(C)$ which permutes the elements of the set $C = \{c_{d_1,\ldots,d_{m-1},i,j,k,l};\ d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,n\}$ p. d.$\}$. Then there exists a permutation $\pi \in \mathrm{S}_{m+3}$ such that*

$$\phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = c_{\pi(d_1),\ldots,\pi(d_{m-1}),\pi(i),\pi(j),\pi(k),\pi(l)}$$

for all $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C$.

Proof. The plan of the proof is as follows. In advance, we will prove the case $m = 1$ – a straightforward argumentation. For the cases $m > 2$, we will consider special subsets of $\{1,\ldots,m+3\}$ of size 5 which cover the whole set $\{1,\ldots,m+3\}$. These 5-sets will be constructed in a way such that the automorphism $\phi : K(C) \longrightarrow K(C)$ induces a map from each of these sets into the set $\{1,\ldots,m+3\}$. As we then will see, these maps can be "glued" together to give a permutation $\pi : \{1,\ldots,m+3\} \longrightarrow \{1,\ldots,m+3\}$. Finally, we will show that the K-automorphism of the field $K(C)$ given by

$$c_{d_1,\ldots,d_{m-1},i,j,k,l} \longmapsto c_{\pi(d_1),\ldots,\pi(d_{m-1}),\pi(i),\pi(j),\pi(k),\pi(l)}$$

for all $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C$ is equal to ϕ.

We start with some preliminary considerations and the proof of the case $m = 1$. Let $d_1,\ldots,d_{m-1},i,j,k,l \in \{1,\ldots,m+3\}$ be arbitrary pairwise distinct elements. Note that by comparing cardinalities, we have $\{d_1,\ldots,d_{m-1},i,j,k,l\} = \{1,\ldots,m+3\}$. It is therefore reasonable to call a sequence such as $d_1,\ldots,d_{m-1},i,j,k,l$ a labelling of the elements in the set $\{1,\ldots,m+3\}$. In this manner of speaking, let $e_1,\ldots,e_{m-1},s,t,u,v \in \{1,\ldots,m+3\}$

be another labelling such that $\phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = c_{e_1,\ldots,e_{m-1},s,t,u,v}$. We claim that for all permutations $\eta \in \mathrm{S}_{\{i,j,k,l\}}$ of the elements i, j, k and l there exists a permutation $\hat{\eta} \in \mathrm{S}_{\{s,t,u,v\}}$ such that

$$\phi(c_{d_1,\ldots,d_{m-1},\eta(i),\eta(j),\eta(k),\eta(l)}) = c_{e_1,\ldots,e_{m-1},\hat{\eta}(s),\hat{\eta}(t),\hat{\eta}(u),\hat{\eta}(v)}. \tag{4.26}$$

More precisely, $\hat{\eta}$ is the permutation which arises from η by replacing i by s, j by t, k by u and l by v. If η is one of the permutations $(i,j)(k,l)$, $(i,k)(j,l)$ or $(i,l)(j,k) \in \mathrm{S}_{\{i,j,k,l\}}$, the claim is immediate, since then $c_{d_1,\ldots,d_{m-1},\eta(i),\eta(j),\eta(k),\eta(l)} = c_{d_1,\ldots,d_{m-1},i,j,k,l}$ and $c_{e_1,\ldots,e_{m-1},\hat{\eta}(s),\hat{\eta}(t),\hat{\eta}(u),\hat{\eta}(v)} = c_{e_1,\ldots,e_{m-1},s,t,u,v}$ (cf. Theorem 4.10, relation (4.9)). If η is equal to (j,k), then applying the K-automorphism ϕ to relation (4.10) of Theorem 4.10 shows that

$$\begin{aligned} 1 &= \phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) \cdot \phi(c_{d_1,\ldots,d_{m-1},i,k,j,l}) \\ &= c_{e_1,\ldots,e_{m-1},s,t,u,v} \cdot \phi(c_{d_1,\ldots,d_{m-1},\eta(i),\eta(j),\eta(k),\eta(l)}). \end{aligned}$$

Since by relation (4.10) the inverse of the element $c_{e_1,\ldots,e_{m-1},s,t,u,v}$ is given by the element $c_{e_1,\ldots,e_{m-1},s,u,t,v}$, it follows that $\phi(c_{d_1,\ldots,d_{m-1},\eta(i),\eta(j),\eta(k),\eta(l)})$ must be equal to the element $c_{e_1,\ldots,e_{m-1},s,u,t,v}$. So the claim is true in this case, too. Let now η be equal to (j,l). Applying the K-automorphism ϕ to relation (4.11) of Theorem 4.10 yields the equation

$$\begin{aligned} 1 &= \phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) + \phi(c_{d_1,\ldots,d_{m-1},i,l,k,j}) \\ &= c_{e_1,\ldots,e_{m-1},s,t,u,v} + \phi(c_{d_1,\ldots,d_{m-1},\eta(i),\eta(j),\eta(k),\eta(l)}). \end{aligned}$$

On the other hand, we have the equality $1 = c_{e_1,\ldots,e_{m-1},s,t,u,v} + c_{e_1,\ldots,e_{m-1},s,v,u,t}$ (cf. relation (4.11)). Thus the element $\phi(c_{d_1,\ldots,d_{m-1},\eta(i),\eta(j),\eta(k),\eta(l)})$ must be equal to $c_{e_1,\ldots,e_{m-1},s,v,u,t}$, and the claim is also true in this case.
Now observe that the permutations $(i,j)(k,l), (i,k)(j,l), (i,l)(j,k), (j,k)$ and (j,l) generate the group $\mathrm{S}_{\{i,j,k,l\}}$. Knowing this, the claim follows by a straightforward induction argument.

For the special case that $m = 1$, the correctness of the lemma is now not hard to see. For, observe that for $m = 1$, that means $m+3 = 4$, we have $\{i,j,k,l\} = \{s,t,u,v\} = \{1,2,3,4\}$. Let $\pi : \{1,2,3,4\} \longrightarrow \{1,2,3,4\}$ be the permutation defined by $i \longmapsto s$, $j \longmapsto t$, $k \longmapsto u$ and $l \longmapsto v$. Then it it immediate by the claim (4.26) that $\phi(c_{i',j'.k'.l'}) = c_{\pi(i'),\pi(j'),\pi(k'),\pi(l')}$, which proves the lemma for this case.
For the remainder of the proof we assume that m is at least 2. Observe that if we take another labelling $d'_1, \ldots, d'_{m-1}, i', j', k', l'$ of the elements in the set $\{1, \ldots, m+3\}$ such that the sets $\{i', j', k', l'\}$ and $\{i,j,k,l\}$ are equal and so also $\{d'_1, \ldots, d'_{m-1}\} = \{d_1, \ldots, d_{m-1}\}$, then by relation (4.8), there exists a permutation $\eta \in \mathrm{S}_{\{i,j,k,l\}}$ such that

$$c_{d'_1,\ldots,d'_{m-1},i',j',k',l'} = c_{d_1,\ldots,d_{m-1},\eta(i),\eta(j),\eta(k),\eta(l)}$$

Therefore, we get a well-defined map ψ from the set of all 4-subsets of $\{1, \ldots, m+3\}$ to the set of all 4-subsets of $\{1, \ldots, m+3\}$ by taking the value of ψ at a 4-subset $\{i,j,k,l\} \subset$

$\{1, \ldots, m+3\}$ to be

$$\psi(\{i,j,k,l\}) := \{s,t,u,v\}$$

if $\phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = c_{e_1,\ldots,e_{m-1},s,t,u,v}$ for some arbitrary labelling $d_1, \ldots, d_{m-1} \in \{1, \ldots, m+3\} \backslash \{i,j,k,l\}$ of the elements in the set $\{1, \ldots, m+3\} \backslash \{i,j,k,l\}$ and some $e_1, \ldots, e_{m-1}$, $s,t,u,v \in \{1, \ldots, m+3\}$.
It is not hard to see that ψ is injective (and thus surjective). For, note that the inverse ϕ^{-1} of the map ϕ is again a K-automorphism of the field $K(C)$ which permutes the elements of the set C. So it follows by the discussion of (4.26) that for all permutations $\hat{\eta} \in \mathrm{S}_{\{s,t,u,v\}}$ there exists a permutation $\eta \in \mathrm{S}_{\{i,j,k,l\}}$ such that

$$\phi^{-1}(c_{e_1,\ldots,e_{m-1},\hat{\eta}(s),\hat{\eta}(t),\hat{\eta}(u),\hat{\eta}(v)}) = c_{d_1,\ldots,d_{m-1},\eta(i),\eta(j),\eta(k),\eta(l)}.$$

But this obviously shows the injectivity of ψ.

Consider the subsets $T_3, \ldots, T_{m+1} \subset \{1, \ldots, m+3\}$ of size 5 defined by

$$T_i := \{1, 2, i, m+2, m+3\},\ i \in \{3, \ldots, m+1\}.$$

Obviously, the sets T_i, $i \in \{3, \ldots, m+1\}$ cover the whole set $\{1, \ldots, m+3\}$. In the following, we will construct a family of maps $\pi_i : T_i \longrightarrow \{1, \ldots, m+3\}$ for all $i \in \{3, \ldots, m+1\}$. These maps will finally be "glued" together to give the desired permutation corresponding to ϕ.
Fix some $i \in \{3, \ldots, m+1\}$. Note that by relation (4.12) of Theorem 4.10, we get the equations

$$\begin{aligned}
\phi(c_{i,3,\ldots,\hat{i},\ldots,m+1,2,m+2,m+3,1}) &= \phi(c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,m+3,1}) \cdot \phi(c_{1,3,\ldots,\hat{i},\ldots,m+1,2,m+2,m+3,i}) \\
\phi(c_{i,3,\ldots,\hat{i},\ldots,m+1,m+2,2,m+3,1}) &= \phi(c_{m+2,3,\ldots,\hat{i},\ldots,m+1,i,2,m+3,1}) \cdot \phi(c_{1,3,\ldots,\hat{i},\ldots,m+1,m+2,2,m+3,i}) \\
\phi(c_{i,3,\ldots,\hat{i},\ldots,m+1,m+3,m+2,2,1}) &= \phi(c_{m+3,3,\ldots,\hat{i},\ldots,m+1,i,m+2,2,1}) \cdot \phi(c_{1,3,\ldots,\hat{i},\ldots,m+1,m+3,m+2,2,i}),
\end{aligned}$$

where as usual the hat means that the respective element is omitted. By definition of the map ψ, it follows by Proposition 4.13 (b) that

$$\begin{aligned}
&|\psi(\{1,2,m+2,m+3\}) \cup \psi(\{1,i,m+2,m+3\}) \cup \psi(\{2,i,m+2,m+3\})| \in \{4,5\} \\
&|\psi(\{1,2,m+2,m+3\}) \cup \psi(\{1,2,i,m+3\}) \cup \psi(\{2,i,m+2,m+3\})| \in \{4,5\} \\
&|\psi(\{1,2,m+2,m+3\}) \cup \psi(\{1,2,i,m+2\}) \cup \psi(\{2,i,m+2,m+3\})| \in \{4,5\}.
\end{aligned} \tag{4.27}$$

On the other hand, since ψ is injective, we already have

$$|\psi(\{1,2,m+2,m+3\}) \cup \psi(\{2,i,m+2,m+3\})| \geq 5.$$

It follows from the equations (4.27) that the size of the set $\psi(\{1,2,m+2,m+3\}) \cup$

$\psi(\{2, i, m+2, m+3\})$ actually must be equal to 5. Moreover, the set

$$\begin{aligned} B_i := \psi(\{1,2,m+2,m+3\}) \cup \psi(\{2,i,m+2,m+3\}) \cup \psi(\{1,i,m+2,m+3\}) \\ \cup \psi(\{1,2,i,m+3\}) \cup \psi(\{1,2,i,m+2\}) \end{aligned} \tag{4.28}$$

has size 5, too. We thus can define a map $\pi_i : T_i \longrightarrow B_i \subset \{1, \ldots, m+3\}$ by sending $\nu \in T_i$ to the (single) element in the set $B_i \setminus \psi(T_i \setminus \{\nu\})$. Note that by the injectivity of the map ψ, the map π_i must be injective and thus surjective, too. So π_i maps the set T_i bijectively to the set B_i. Therefore, it follows that

$$\pi_i(T_i \setminus \{\nu\}) = \pi_i(T_i) \setminus \{\pi_i(\nu)\} = \pi_i(T_i) \setminus (\pi_i(T_i) \setminus \psi(T_i \setminus \{\nu\})) = \psi(T_i \setminus \{\nu\}). \tag{4.29}$$

As mentioned before, it is our aim to "glue" the maps π_i, $i \in \{3, \ldots, m+1\}$ together to a map $\pi : \{1, \ldots, m+3\} \longrightarrow \{1, \ldots, m+3\}$. For this to make sense, we need to show that $(\pi_i)_{|T_i \cap T_j} = (\pi_j)_{|T_i \cap T_j}$ for all $i, j \in \{3, \ldots, m+1\}$.
Observe that the intersection $T_i \cap T_j$ is equal to $\{1, 2, m+2, m+3\}$ for all distinct $i, j \in \{3, \ldots, m+1\}$. Fix some distinct elements $i, j \in \{3, \ldots, m+1\}$. We claim that

$$\pi_i(\{1,2,m+2,m+3\} \setminus \{\nu\}) = \pi_j(\{1,2,m+2,m+3\} \setminus \{\nu\})$$

for all $\nu \in \{1, 2, m+2, m+3\}$. Assume for the moment that this is true. Then by equality (4.29) and the injectivity of π_i and π_j, we get

$$\begin{aligned} \{\pi_i(\nu)\} &= \pi_i(\{1,2,m+2,m+3\}) \setminus \pi_i(\{1,2,m+2,m+3\} \setminus \{\nu\}) \\ &= \psi(\{1,2,m+2,m+3\}) \setminus \pi_j(\{1,2,m+2,m+3\} \setminus \{\nu\}) \\ &= \pi_j(\{1,2,m+2,m+3\}) \setminus \pi_j(\{1,2,m+2,m+3\} \setminus \{\nu\}) \\ &= \{\pi_j(\nu)\} \end{aligned}$$

for all $\nu \in \{1, 2, m+2, m+3\}$. This then shows that $(\pi_i)_{|T_i \cap T_j} = (\pi_j)_{|T_i \cap T_j}$, as desired.

For the proof of the claim, let $d_2, \ldots, d_{m-1}, a_1, a_2, a_3, a_4, a_5 \in \{1, \ldots, m+3\}$ be some labelling of the elements in the set $\{1, \ldots, m+3\}$. Then by relation (4.12), we have

$$\phi(c_{a_5,d_2,\ldots,d_{m-1},a_1,a_2,a_3,a_4}) = \phi(c_{a_1,d_2,\ldots,d_{m-1},a_5,a_2,a_3,a_4}) \cdot \phi(c_{a_4,d_2,\ldots,d_{m-1},a_1,a_2,a_3,a_5}).$$

By definition of the map ψ, it thus follows from Proposition 4.13 (b) that

$$|\psi(\{a_1,a_2,a_3,a_4\}) \cup \psi(\{a_5,a_2,a_3,a_4\}) \cup \psi(\{a_1,a_2,a_3,a_5\})| \in \{4,5\}$$

and therefore

$$|\psi(\{a_1,a_2,a_3,a_4\}) \cup \psi(\{a_1,a_2,a_3,a_5\})| \in \{4,5\}.$$

This implies

$$|\psi(\{a_1,a_2,a_3,a_4\}) \cap \psi(\{a_1,a_2,a_3,a_5\})| \in \{4,3\}.$$

By the fact that ψ is an injective map, we moreover know that the cardinality of the set $\psi(\{a_1, a_2, a_3, a_4\}) \cap \psi(\{a_1, a_2, a_3, a_5\})$ is at most 3, which shows that actually

$$|\psi(\{a_1, a_2, a_3, a_4\}) \cap \psi(\{a_1, a_2, a_3, a_5\})| = 3.$$

It follows that

$$|\psi(\{1, 2, i, m+2, m+3\} \setminus \{\nu\}) \cap \psi(\{1, 2, j, m+2, m+3\} \setminus \{\nu\})| = 3.$$

for all $\nu \in \{1, 2, m+2, m+3\}$.
Consider the subsets B_i and $B_j \subset \{1, \ldots, m+3\}$ as defined in (4.28). Since ψ is a bijection and hence injective, it follows from the definition of B_i that the different 4-subsets of B_i are given by $\psi(T_i \setminus \{\nu\})$, $\nu \in T_i$. Therefore, again by injectivity of the map ψ, the set B_i cannot contain the ψ-image of the set $\{2, j, m+2, m+3\}$, i. e. $\psi(\{2, j, m+2, m+3\}) \nsubseteq B_i$. In particular, this means that

$$B_j \nsubseteq B_i \quad \text{and} \quad B_i \nsubseteq B_j.$$

By definition of B_i and B_j, the set $\psi(\{1, 2, m+2, m+3\})$ is contained both, in B_i and in B_j, so it follows from the definition of the maps π_i and π_j that

$$\begin{aligned} B_i &\not\supseteq B_j \setminus \psi(\{1, 2, m+2, m+3\}) = \{\pi_j(j)\} \\ B_j &\not\supseteq B_i \setminus \psi(\{1, 2, m+2, m+3\}) = \{\pi_i(i)\}. \end{aligned}$$

Note that this means that $\pi_j(j)$ is not contained in $\{\pi_i(1), \pi_i(2), \pi_i(i), \pi_i(m+2), \pi_i(m+3)\}$ and that $\pi_i(i)$ is not contained in $\{\pi_j(1), \pi_j(2), \pi_j(j), \pi_j(m+2), \pi_j(m+3)\}$. Together with (4.29), we therefore have for all $\nu \in \{1, 2, m+2, m+3\}$

$$\begin{aligned} &|\pi_i(\{1, 2, m+2, m+3\} \setminus \{\nu\}) \cap \pi_j(\{1, 2, m+2, m+3\} \setminus \{\nu\})| \\ &= |\pi_i(\{1, 2, i, m+2, m+3\} \setminus \{\nu\}) \cap \pi_j(\{1, 2, j, m+2, m+3\} \setminus \{\nu\})| \\ &= |\psi(\{1, 2, i, m+2, m+3\} \setminus \{\nu\}) \cap \psi(\{1, 2, j, m+2, m+3\} \setminus \{\nu\})| \\ &= 3, \end{aligned}$$

which shows that $\pi_i(\{1, 2, m+2, m+3\} \setminus \{\nu\})$ is equal to $\pi_j(\{1, 2, j, m+2, m+3\} \setminus \{\nu\})$, as claimed.

So there exists a (unique) map $\pi : \{1, \ldots, m+3\} \longrightarrow \{1, \ldots, m+3\}$ such that

$$\pi_{|T_i} = \pi_i \quad \text{for all } i \in \{3, \ldots, m+1\}.$$

Since the sets B_i, $i \in \{3, \ldots, m+1\}$ are pairwise distinct but all contain the set $\psi(\{1, 2, m+2, m+3\}$ of size 4, the union $\bigcup_{i=3}^{m+1} B_i$ is equal to the whole set $\{1, \ldots, m+3\}$. From the surjectivity of the maps $\pi_i : T_i \longrightarrow B_i$ it hence follows that the map π is surjective, too, and thus is a permutation of the elements in the set $\{1, \ldots, m+3\}$. Then π gives an

automorphism ϕ_π of the field $K(C)$ by

$$\phi_\pi : c_{d_1,\dots,d_{m-1},i,j,k,l} \longmapsto c_{\pi(d_1),\dots,\pi(d_{m+1}),\pi(i),\pi(j),\pi(k),\pi(l)}$$

for all $c_{d_1,\dots,d_{m-1},i,j,k,l} \in C$. We will show that ϕ_π is equal to the map ϕ, or equivalently that the map

$$\hat{\phi} := \phi_\pi^{-1} \circ \phi$$

is equal to the identity map $\mathrm{id}_{K(C)}$. Since $K(C)$ is generated by $c_{2,\dots,\hat{i},\dots,m+1,i,m+2,m+3,1}$, $i \in \{2,\dots,m+1\}$ (cf. Remark 4.8), it is enough to show that $\hat{\phi}$ maps each of these elements to itself.
So let $i \in \{2,\dots,m+1\}$. If i is equal to 2, let $j := 3$, otherwise, let j be equal to 2. Note that by definition of the permutation π, it follows from equation (4.29) that we have

$$\begin{aligned}
\pi(\{i, m+2, m+3, 1\}) &= \psi(\{i, m+2, m+3, 1\}) \\
\pi(\{j, m+2, m+3, 1\}) &= \psi(\{j, m+2, m+3, 1\}) \\
\pi(\{i, m+2, m+3, j\}) &= \psi(\{i, m+2, m+3, j\}) \\
\pi(\{i, 1, m+3, j\}) &= \psi(\{i, 1, m+3, j\}).
\end{aligned}$$

and thus

$$\begin{aligned}
\{i, m+2, m+3, 1\} &= \pi^{-1}(\psi(\{i, m+2, m+3, 1\})) \\
\{j, m+2, m+3, 1\} &= \pi^{-1}(\psi(\{j, m+2, m+3, 1\})) \\
\{i, m+2, m+3, j\} &= \pi^{-1}(\psi(\{i, m+2, m+3, j\})) \\
\{i, 1, m+3, j\} &= \pi^{-1}(\psi(\{i, 1, m+3, j\})).
\end{aligned}$$

Note that the map ϕ_π^{-1} is equal to the map $\phi_{\pi^{-1}}$, the automorphism of the field $K(C)$ induced by the permutation π^{-1}. By definition of the map ψ and relation (4.8) of Theorem 4.10, it hence follows that there exist permutations $\eta_1 \in \mathrm{S}_{\{i,m+2,m+3,1\}}$, $\eta_2 \in \mathrm{S}_{\{j,m+2,m+3,1\}}$, $\eta_3 \in \mathrm{S}_{\{i,m+2,m+3,j\}}$ and $\eta_4 \in \mathrm{S}_{\{i,1,m+3,j\}}$ such that

$$\begin{aligned}
\hat{\phi}(c_{2,\dots,\hat{i},\dots,m+1,i,m+2,m+3,1}) &= \phi_{\pi^{-1}}(\phi(c_{2,\dots,\hat{i},\dots,m+1,i,m+2,m+3,1})) \\
&= c_{2,\dots,\hat{i},\dots,m+1,\eta_1(i),\eta_1(m+2),\eta_1(m+3),\eta_1(1)} \\
\hat{\phi}(c_{2,\dots,\hat{j},\dots,m+1,j,m+2,m+3,1}) &= \phi_{\pi^{-1}}(\phi(c_{2,\dots,\hat{j},\dots,m+1,j,m+2,m+3,1})) \\
&= c_{2,\dots,\hat{j},\dots,m+1,\eta_2(j),\eta_2(m+2),\eta_2(m+3),\eta_2(1)} \\
\hat{\phi}(c_{1,\dots,\hat{j},\dots,\hat{i},\dots,m+1,i,m+2,m+3,j}) &= \phi_{\pi^{-1}}(\phi(c_{1,\dots,\hat{j},\dots,\hat{i},\dots,m+1,i,m+2,m+3,j})) \\
&= c_{1,\dots,\hat{j},\dots,\hat{i},\dots,m+1,\eta_3(i),\eta_3(m+2),\eta_3(m+3),\eta_3(j)} \\
\hat{\phi}(c_{m+2,2,\dots,\hat{j},\dots,\hat{i},\dots,m+1,i,1,m+3,j}) &= \phi_{\pi^{-1}}(\phi(c_{m+2,2,\dots,\hat{j},\dots,\hat{i},\dots,m+1,i,1,m+3,j})) \\
&= c_{m+2,2,\dots,\hat{j},\dots,\hat{i},\dots,m+1,\eta_4(i),\eta_4(1),\eta_4(m+3),\eta_4(j)}.
\end{aligned} \tag{4.30}$$

Note that by relation (4.9), we may assume without loss of generality that $\eta_1(i)$, $\eta_3(i)$ and

$\eta_4(i)$ are equal to i. By relation (4.12) and relation (4.8) of Theorem 4.10, we have the equation

$$\hat{\phi}(c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,m+3,1}) = \hat{\phi}(c_{2,\ldots,\hat{j},\ldots,m+1,j,m+2,m+3,1}) \cdot \hat{\phi}(c_{1,\ldots,\hat{j},\ldots,\hat{i},\ldots,m+1,i,m+2,m+3,j}).$$

According to the above equations we can rewrite this as

$$\begin{aligned} &c_{2,\ldots,\hat{i},\ldots,m+1,i,\eta_1(m+2),\eta_1(m+3),\eta_1(1)} \\ &\quad = c_{2,\ldots,\hat{j},\ldots,m+1,\eta_2(j),\eta_2(m+2),\eta_2(m+3),\eta_2(1)} \cdot c_{1,\ldots,\hat{j},\ldots,\hat{i},\ldots,m+1,i,\eta_3(m+2),\eta_3(m+3),\eta_3(j)}. \end{aligned}$$

We apply now the maps $\omega_{i,\eta_1(m+2)}$ and $\omega_{i,\eta_1(m+3)}$ as defined in the previous section. By Lemma 4.12, we have the equality

$$\begin{aligned} 1 &= \omega_{i,\eta_1(m+2)}(c_{2,\ldots,\hat{i},\ldots,m+1,i,\eta_1(m+2),\eta_1(m+3),\eta_1(1)}) \\ &= \omega_{i,\eta_1(m+2)}(c_{2,\ldots,\hat{j},\ldots,m+1,\eta_2(j),\eta_2(m+2),\eta_2(m+3),\eta_2(1)}) \\ &\qquad + \omega_{i,\eta_1(m+2)}(c_{1,\ldots,\hat{j},\ldots,\hat{i},\ldots,m+1,i,\eta_3(m+2),\eta_3(m+3),\eta_3(j)}) \\ &= 0 + \omega_{i,\eta_1(m+2)}(c_{1,\ldots,\hat{j},\ldots,\hat{i},\ldots,m+1,i,\eta_3(m+2),\eta_3(m+3),\eta_3(j)}). \end{aligned}$$

It follows that $\eta_1(m+2)$ is equal to $\eta_3(m+2)$, which lies in the set $\{j, m+2, m+3\}$. Similarly, we see that

$$\begin{aligned} -1 &= \omega_{i,\eta_1(m+3)}(c_{2,\ldots,\hat{i},\ldots,m+1,i,\eta_1(m+2),\eta_1(m+3),\eta_1(1)}) \\ &= \omega_{i,\eta_1(m+3)}(c_{2,\ldots,\hat{j},\ldots,m+1,\eta_2(j),\eta_2(m+2),\eta_2(m+3),\eta_2(1)}) \\ &\qquad + \omega_{i,\eta_1(m+3)}(c_{1,\ldots,\hat{j},\ldots,\hat{i},\ldots,m+1,i,\eta_3(m+2),\eta_3(m+3),\eta_3(j)}) \\ &= 0 + \omega_{i,\eta_1(m+3)}(c_{1,\ldots,\hat{j},\ldots,\hat{i},\ldots,m+1,i,\eta_3(m+2),\eta_3(m+3),\eta_3(j)}). \end{aligned}$$

This implies that $\eta_1(m+3)$ is equal to $\eta_3(m+3)$, which is also an element of the set $\{j, m+2, m+3\}$. Since by definition the elements $\eta_1(m+2)$ and $\eta_1(m+3)$ both lie in the set $\{1, m+2, m+3\}$, which does not contain the element j, it follows that the set $\{\eta_1(m+2), \eta_1(m+3)\}$ is equal to $\{m+2, m+3\}$. It particular, this implies that $\eta_1(1)$ is equal to 1. Hence we have

$$\hat{\phi}(c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,m+3,1}) = c_{2,\ldots,\hat{i},\ldots,m+1,i,\eta_1(m+2),\eta_1(m+3),1} \tag{4.31}$$

with $\{\eta_1(m+2), \eta_1(m+3)\} = \{m+2, m+3\}$.

By relation (4.11) and the equations (4.30), it is not hard to see that

$$\begin{aligned} \hat{\phi}(c_{2,\ldots,\hat{i},\ldots,m+1,i,1,m+3,m+2}) &= 1 - \hat{\phi}(c_{2,\ldots,\hat{i},\ldots,m+1,i,m+2,m+3,1}) \\ &= 1 - c_{2,\ldots,\hat{i},\ldots,m+1,i,\eta_1(m+2),\eta_1(m+3),1} \\ &= c_{2,\ldots,\hat{i},\ldots,m+1,i,1,\eta_1(m+3),\eta_1(m+2)} \end{aligned}$$

and

$$\begin{aligned}\hat{\phi}(c_{2,\dots,\hat{j},\dots,m+1,j,1,m+3,m+2}) &= 1 - \hat{\phi}(c_{2,\dots,\hat{j},\dots,m+1,j,m+2,m+3,1}) \\ &= 1 - c_{2,\dots,\hat{j},\dots,m+1,\eta_2(j),\eta_2(m+2),\eta_2(m+3),\eta_2(1)} \\ &= c_{2,\dots,\hat{j},\dots,m+1,\eta_2(j),\eta_2(1),\eta_2(m+3),\eta_2(m+2)}.\end{aligned}$$

Together with relation (4.12) and relation (4.8) of Theorem 4.10, we have

$$\begin{aligned}c_{2,\dots,\hat{i},\dots,m+1,i,1,\eta_1(m+3),\eta_1(m+2)} &= \hat{\phi}(c_{2,\dots,\hat{i},\dots,m+1,i,1,m+3,m+2}) \\ &= \hat{\phi}(c_{2,\dots,\hat{j},\dots,m+1,j,1,m+3,m+2}) \cdot \hat{\phi}(c_{m+2,2,\dots,\hat{j},\dots,\hat{i},\dots,m+1,i,1,m+3,j}) \\ &= c_{2,\dots,\hat{j},\dots,m+1,\eta_2(j),\eta_2(1),\eta_2(m+3),\eta_2(m+2)} \cdot c_{m+2,2,\dots,\hat{j},\dots,\hat{i},\dots,m+1,i,\eta_4(1),\eta_4(m+3),\eta_4(j)}.\end{aligned}$$

Applying the map $\omega_{i,\eta_1(m+3)}$ to this equation, it follows by Lemma 4.12 that

$$\begin{aligned}-1 &= \omega_{i,\eta_1(m+3)}(c_{2,\dots,\hat{i},\dots,m+1,i,1,\eta_1(m+3),\eta_1(m+2)}) \\ &= \omega_{i,\eta_1(m+3)}(c_{2,\dots,\hat{j},\dots,m+1,\eta_2(j),\eta_2(1),\eta_2(m+3),\eta_2(m+2)}) \\ &\quad + \omega_{i,\eta_1(m+3)}(c_{m+2,2,\dots,\hat{j},\dots,\hat{i},\dots,m+1,i,\eta_4(1),\eta_4(m+3),\eta_4(j)}) \\ &= 0 + \omega_{i,\eta_1(m+3)}(c_{m+2,2,\dots,\hat{j},\dots,\hat{i},\dots,m+1,i,\eta_4(1),\eta_4(m+3),\eta_4(j)}).\end{aligned}$$

Again, Lemma 4.12 shows that $\eta_1(m+3)$ is equal to $\eta_4(m+3)$, which is an element of the set $\{1, j, m+3\}$. Since by the above $\eta_1(m+3)$ lies in the set $\{m+2, m+3\}$, it follows that $\eta_1(m+3) = m+3$ and $\eta_1(m+2) = m+2$. Thus

$$\hat{\phi}(c_{2,\dots,\hat{i},\dots,m+1,i,m+2,m+3,1}) = c_{2,\dots,\hat{i},\dots,m+1,i,m+2,m+3,1},$$

as desired. This finishes the proof. ∎

Equipped with that lemma, we can now find a set of generating invariants of the invariant field $K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}}$.

Theorem 4.15. *Let C be the set of invariants given by*

$$C := \{c_{d_1,\dots,d_{m-1},i,j,k,l};\ d_1,\dots,d_{m-1},i,j,k,l \in \{1,\dots,m+3\}\ p.\,d.\}$$

and let Y be an indeterminate over $K(C)$. Then the coefficients of the polynomial $F \in K(C)[Y]$ defined by

$$F := \prod_{c \in C} (Y - c) \in K(C)[Y].$$

generate the invariant field $K(C)^{\mathrm{S}_{m+3}} = K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}}$ over K.

Proof. Let L be the field generated by the coefficients of the polynomial $F \in K(C)[Y]$ over K. We need to show that L is equal to $K(C)^{\mathrm{S}_{m+3}}$.

First we show that L is contained in $K(C)^{\mathrm{S}_{m+3}}$. Let $\pi \in \mathrm{S}_{m+3}$. Then π acts on $K(C)$ by the K-automorphism ϕ_π given by

$$\phi_\pi : c_{d_1,\ldots,d_{m-1},i,j,k,l} \longmapsto c_{\pi(d_1),\ldots,\pi(d_{m-1}),\pi(i),\pi(j),\pi(k),\pi(l)}$$

for all pairwise distinct $d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, m+3\}$. By Proposition 4.13 (a), it is not hard to see that the automorphism of the polynomial ring $K(C)[Y]$ which fixes Y and is equal to ϕ_π on $K(C)$ permutes the zeroes of the polynomial $F \in K(C)[Y]$. It follows that the coefficients of the polynomial F are fixed by the automorphism ϕ_π. Thus the coefficients of the polynomial F are invariant under the action of the group S_{m+3}, which shows that $L \subset K(C)^{\mathrm{S}_{m+3}}$.
It remains to show $L \supset K(C)^{\mathrm{S}_{m+3}}$. By construction, the polynomial $F \in L[Y]$ is separable. Since $K(C)$ is the splitting field of the polynomial $F \in L[Y]$, it follows from Galois theory that the field extension $K(C)|L$ is Galois. Let ϕ be an L-automorphism of the field $K(C)$, i. e. $\phi \in \mathrm{Gal}(K(C)/L)$. As the polynomial F has coefficients in L, the automorphism ϕ permutes the roots of the polynomial F, i. e. ϕ permutes the elements of the set C. By Lemma 4.14, there exists a permutation $\pi \in \mathrm{S}_{m+3}$ such that $\phi = \phi_\pi$. So we have

$$\mathrm{Gal}(K(C)/L) \subset \{\phi_\pi;\ \pi \in \mathrm{S}_{m+3}\}.$$

It follows that the field $L = K(C)^{\mathrm{Gal}(K(C)/L)}$ contains the field $K(C)^{\mathrm{S}_{m+3}}$, as desired. ∎

The previous theorem provides an explicit way of finding a generating set of the invariant field $K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}}$. Unfortunately, apart from the cases where m is small, the computation of the generators turns out to be too complex in practice. In the applications though, it may be not necessary to know a generating set of rational invariants explicitly. For example, if we are only interested in the values of the generating set of rational invariants of Theorem 4.15 at a certain point P, the problem of explicitly computing invariants can be avoided. By construction, their values at a point P are perfectly represented by the distribution of the values of the rational functions in the set C at the point P. For, denote the elements of the set C by $c_1, \ldots, c_d$. Furthermore, let $Z_1, \ldots, Z_d$ be indeterminates over K and consider the elementary symmetric polynomials $e_0, \ldots, e_d$ in d variables, i.e.

$$e_k(Z_1, \ldots, Z_d) := \sum_{1 \le j_1 \le \ldots \le j_k \le d} Z_{j_1} \cdot \ldots \cdot Z_{j_k} \qquad \text{for all } k \in \{0, \ldots, d\}.$$

Assuming that all c's are defined at P, it follows that the coefficients of F, that means $e_0(c_1, \ldots, c_d)$, $\ldots$, $e_d(c_1, \ldots, c_d)$, are defined at P, too. Moreover, it follows that

$$e_k(c_1(P), \ldots, c_d(P)) = e_k(c_1, \ldots, c_d)(P) \quad \text{for all } k \in \{0, \ldots, d\}.$$

But this means nothing else than that the values of the generating set of rational invariants of Theorem 4.15 at P are defined by the distribution of the values of the rational functions in the set C at P.

Nonetheless, it would be desirable on its own to find a simpler generating set of the invariant field $K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}}$. By Remark 4.8, the field $K(C)$ has transcendental degree m over K. Since S_{m+3} is a finite group, the same is true for the invariant field $K(C)^{\mathrm{S}_{m+3}} = (K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}}$. So there might be a chance that the generating set can be reduced to a total of m elements.
In case that $m = 1$, this is in fact true, since the invariant field is a subfield of transcendental degree one of $K(C)$ – the latter being a purely transcendental field extension over K (cf. Theorem 2.50). In the following example, we will examine this case in more detail for $K = \overline{\mathbb{Q}}$.
The case that $m = 2$ is treated extensively in the paper [BK05]. Kemper and Boutin provide a generating set of the invariant field $K((\mathbb{P}^2)^5)^{\mathrm{PGL}_3 \times \mathrm{S}_5}$ consisting of two elements.
In the cases where m is greater than two, the amount of data exceeded our computing capabilities. Nonetheless, for the case that m is equal to 3, we have given explicit representations of all elements in the set C in terms of the elements $c_{3,4,2,5,6,1}, c_{2,4,3,5,6,1}$ and $c_{2,3,4,5,6,1}$ (cf. Example 4.11). Having these representations is advantageous in practice if we want to compute the values of the elements in the set C at some concrete point.

Example 4.16. Let $K := \overline{\mathbb{Q}}$. We examine the invariant field $K((\mathbb{P}^1_K)^4)^{\mathrm{PGL}_2 \times \mathrm{S}_4}$. By the theorem of Lüroth (Theorem 2.50), the invariant field

$$K((\mathbb{P}^1_K)^4)^{\mathrm{PGL}_2 \times \mathrm{S}_4} \subset K\left(c_{2,3,4,1}\right) = K((\mathbb{P}^2_K)^4)^{\mathrm{PGL}_2}$$

is simple over K, that means it is generated by just one element over K. Let c be an abbreviation for the element $c_{2,3,4,1}$ and let Z be an indeterminate over the field $K(c)$. Since the previous theorem provides an explicit generating set of $K((\mathbb{P}^1_K)^4)^{\mathrm{PGL}_2 \times \mathrm{S}_4}$, the MQS ideal $J^c_{K((\mathbb{P}^1_K)^4)^{\mathrm{PGL}_2 \times \mathrm{S}_4}}$ of the element c over the invariant field $K((\mathbb{P}^1_K)^4)^{\mathrm{PGL}_2 \times \mathrm{S}_4}$ can be computed explicitly, too. With Proposition 2.21, the computer algebra system Magma (cf. [BCP97]) yields

$$\begin{aligned} J^c_{K((\mathbb{P}^1_K)^4)^{\mathrm{PGL}_2 \times \mathrm{S}_4}} = \Big(& Z^6 - 3Z^5 + \frac{-c^6 + 3c^5 - 5c^3 + 3c - 1}{c^4 - 2c^3 + c^2} \cdot Z^4 \\ & + \frac{2c^6 - 6c^5 + 5c^4 + 5c^2 - 6c + 2}{c^4 - 2c^3 + c^2} \cdot Z^3 \\ & + \frac{-c^6 + 3c^5 - 5c^3 + 3c - 1}{c^4 - 2c^3 + c^2} \cdot Z^2 - 3Z + 1 \Big) \trianglelefteq K(c)[Z]. \end{aligned}$$

By Algorithm 2.51, the invariant field $K((\mathbb{P}^1_K)^4)^{\mathrm{PGL}_2 \times \mathrm{S}_4}$ is generated by the element

$$\frac{-c^6 + 3c^5 - 5c^3 + 3c - 1}{c^4 - 2c^3 + c^2} \in K(c)$$

over K. By the way, this is a coefficient of the polynomial

$$F := (Y - c_{2,3,4,1})(Y - c_{2,3,1,4})(Y - c_{2,4,3,1})(Y - c_{2,4,1,3})(Y - c_{2,1,3,4})(Y - c_{2,1,4,3}),$$

more precisely, it is the second elementary polynomial in the set of all c's.
With similar computations it can be verified that an alternative generating set of the invariant field $K((\mathbb{P}^1_K)^4)^{\mathrm{PGL}_2 \times \mathrm{S}_4}$ is given by the sum of the squares of the c's. $\lhd$

4.2.2 The General Case

Having solved the problem of finding generators of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$ for the special case that n is equal to $m+3$, we will now give a solution of the general case. For arbitrary $n \in \mathbb{N}$, a set of generating invariants will be constructed by considering sub-configurations of the point configurations in $(\mathbb{P}^m)^n$ of length $m+3$.

We use the following notation. Denote by $\tilde{M}$ the set of all $(m+3)$-subsets of the set $\{1, \ldots, n\}$, i.e.

$$\tilde{M} := \{M \subset \{1, \ldots, n\};\ |M| = m+3\}.$$

The symmetric group on $\tilde{M}$ shall be written as $S_{\tilde{M}}$. Moreover, as before we denote by C the set given by

$$C := \{c_{d_1,\ldots,d_{m-1},i,j,k,l};\ d_1, \ldots, d_{m-1}, i, j, k, l \in \{1, \ldots, n\},\ \text{p. d.}\}.$$

As in the special case $n = m+3$, we start with a lemma which will turn out to be a central tool for finding a set of generating invariants. The proof will be similar to the proof of Lemma 4.26.

Lemma 4.17 (Second permutation lemma). *Let ϕ be a K-automorphism of the field $K(C)$ such that there exists a permutation $\psi \in \mathrm{S}_{\tilde{M}}$ and for each set $M \in \tilde{M}$ a bijection $\rho_M : M \longrightarrow \psi(M)$ which for all $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C$ with $\{d_1, \ldots, d_{m-1}, i, j, k, l\} = M$ satisfies the equality*

$$\phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = c_{\rho_M(d_1),\ldots,\rho_M(d_{m-1}),\rho_M(i),\rho_M(j),\rho_M(k),\rho_M(l)}.$$

Then there exists a permutation $\pi \in \mathrm{S}_n$ such that

$$\phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = c_{\pi(d_1),\ldots,\pi(d_{m-1}),\pi(i),\pi(j),\pi(k),\pi(l)}$$

for all $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C$.

Proof. If $n \leq m+3$, there is nothing to show. So let n be at least $m+4$. The plan of the proof is as follows. We will consider subsets of $\{1, \ldots, n\}$ of size $m+4$. We will present a construction where for each of these sets, the automorphism ϕ will induce a map from that set into $\{1, \ldots, n\}$. As we will see, these maps can then be "glued" together to give a permutation $\pi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$. Finally, we will show that the induced

K-automorphism of the field $K(C)$ given by

$$c_{d_1,\dots,d_{m-1},i,j,k,l} \longmapsto c_{\pi(d_1),\dots,\pi(d_{m-1}),\pi(i),\pi(j),\pi(k),\pi(l)}$$

for all $c_{d_1,\dots,d_{m-1},i,j,k,l} \in C$ is equal to ϕ.

Let T be a subset of the set $\{1,\dots,n\}$ of size $m+4$. In the following, we denote the set $T \setminus \{\nu\}$ by $T_{\hat{\nu}}$ for all $\nu \in T$. We claim that

$$\left| \bigcup_{\nu \in T} \psi(T_{\hat{\nu}}) \right| = m+4. \tag{4.32}$$

Since ψ is a permutation and hence injective, we already have $\left|\psi(T_{\hat{i}}) \cup \psi(T_{\hat{l}})\right| \geq m+4$ for all distinct elements $i, l \in T$. Therefore, it is enough to show that

$$\left|\psi(T_{\hat{i}}) \cup \psi(T_{\hat{l}}) \cup \psi(T_{\hat{r}})\right| = m+4$$

for all $i, l, r \in T$ pairwise distinct. So fix some $i, l, r \in T$ pairwise distinct. Recall that by the definition of the bijections $\rho_{T_{\hat{i}}}$, $\rho_{T_{\hat{l}}}$ and $\rho_{T_{\hat{r}}}$ we have

$$\psi(T_{\hat{i}}) = \rho_{T_{\hat{i}}}(T_{\hat{i}}), \quad \psi(T_{\hat{l}}) = \rho_{T_{\hat{l}}}(T_{\hat{l}}) \quad \text{and} \quad \psi(T_{\hat{r}}) = \rho_{T_{\hat{r}}}(T_{\hat{r}}).$$

Assume for a contradiction that $\left|\psi(T_{\hat{i}}) \cup \psi(T_{\hat{l}}) \cup \psi(T_{\hat{r}})\right|$ is at least $m+5$. Since $|\psi(T_{\hat{r}})|$ is equal to $m+3$, it follows that the set $\big(\psi(T_{\hat{i}}) \cup \psi(T_{\hat{l}}) \cup \psi(T_{\hat{r}})\big) \setminus \psi(T_{\hat{r}})$ contains at least two elements. Consider two of these elements and denote them by s and t. Then s and t are both contained in the set $\psi(T_{\hat{i}}) \cup \psi(T_{\hat{l}}) = \rho_{T_{\hat{i}}}(T_{\hat{i}}) \cup \rho_{T_{\hat{l}}}(T_{\hat{l}})$. We consider different cases to choose elements $j, k \in T \setminus \{i, l, r\}$.
If neither s nor t is contained in the set $\{\rho_{T_{\hat{i}}}(l), \rho_{T_{\hat{i}}}(r), \rho_{T_{\hat{l}}}(i), \rho_{T_{\hat{l}}}(r)\}$, then let $j, k \in T \setminus \{i, l, r\}$ such that $s, t \in \{\rho_{T_{\hat{i}}}(j), \rho_{T_{\hat{i}}}(k), \rho_{T_{\hat{l}}}(j), \rho_{T_{\hat{l}}}(k)\}$. Otherwise, in case that exactly one of s and t, say s, is not contained in the set $\{\rho_{T_{\hat{i}}}(l), \rho_{T_{\hat{i}}}(r), \rho_{T_{\hat{l}}}(i), \rho_{T_{\hat{l}}}(r)\}$, then let $j \in T \setminus \{i, l, r\}$ such that $s \in \{\rho_{T_{\hat{i}}}(j), \rho_{T_{\hat{l}}}(j)\}$ and let $k \in T \setminus \{i, j, l, r\}$ arbitrary. In case that both s and t are contained in the set $\{\rho_{T_{\hat{i}}}(l), \rho_{T_{\hat{i}}}(r), \rho_{T_{\hat{l}}}(i), \rho_{T_{\hat{l}}}(r)\}$, then let $j, k \in T \setminus \{i, l, r\}$ be arbitrary distinct elements. Note that since $|T| \geq 5$, these choices of j and k are in fact possible. Summarizing this, in any of these cases we can choose $j, k \in T \setminus \{i, l, r\}$ such that

$$s, t \in \{\rho_{T_{\hat{i}}}(l), \rho_{T_{\hat{i}}}(r), \rho_{T_{\hat{i}}}(j), \rho_{T_{\hat{i}}}(k), \rho_{T_{\hat{l}}}(i), \rho_{T_{\hat{l}}}(r), \rho_{T_{\hat{l}}}(j), \rho_{T_{\hat{l}}}(k)\}. \tag{4.33}$$

Denote the elements of the set $T \setminus \{i, j, k, l, r\}$, by $d_1, \dots, d_{m-1}$. Applying the automorphism ϕ to relation (4.13) of Theorem 4.10 then gives the equation

$$\phi(c_{d_1,\dots,d_{m-1},i,j,k,l}) = \phi(c_{d_1,\dots,d_{m-1},r,j,k,l}) \cdot \phi(c_{d_1,\dots,d_{m-1},i,j,k,r}).$$

By definition of the maps $\rho_{T_{\hat{i}}}$, $\rho_{T_{\hat{l}}}$ and $\rho_{T_{\hat{r}}}$, this equation can be rewritten as

$$c_{\rho_{T_{\hat{r}}}(d_1),\ldots,\rho_{T_{\hat{r}}}(d_{m-1}),\rho_{T_{\hat{r}}}(i),\rho_{T_{\hat{r}}}(j),\rho_{T_{\hat{r}}}(k),\rho_{T_{\hat{r}}}(l)} = c_{\rho_{T_{\hat{i}}}(d_1),\ldots,\rho_{T_{\hat{i}}}(d_{m-1}),\rho_{T_{\hat{i}}}(r),\rho_{T_{\hat{i}}}(j),\rho_{T_{\hat{i}}}(k),\rho_{T_{\hat{i}}}(l)} \cdot c_{\rho_{T_{\hat{l}}}(d_1),\ldots,\rho_{T_{\hat{l}}}(d_{m-1}),\rho_{T_{\hat{l}}}(i),\rho_{T_{\hat{l}}}(j),\rho_{T_{\hat{l}}}(k),\rho_{T_{\hat{l}}}(r)}.$$

By Proposition 4.13 (b), it hence follows that the set

$$\{\rho_{T_{\hat{r}}}(i), \rho_{T_{\hat{r}}}(j), \rho_{T_{\hat{r}}}(k), \rho_{T_{\hat{r}}}(l), \rho_{T_{\hat{i}}}(r), \rho_{T_{\hat{i}}}(j), \rho_{T_{\hat{i}}}(k), \rho_{T_{\hat{i}}}(l), \rho_{T_{\hat{l}}}(i), \rho_{T_{\hat{l}}}(j), \rho_{T_{\hat{l}}}(k), \rho_{T_{\hat{l}}}(r)\}$$

has either four or five elements. On the other hand, this set contains the elements $\rho_{T_{\hat{r}}}(i), \rho_{T_{\hat{r}}}(j), \rho_{T_{\hat{r}}}(k), \rho_{T_{\hat{r}}}(l)$ and moreover, by (4.33), the elements s and t. By the choice of s and t, these six elements are pairwise distinct which is obviously a contradiction. Therefore, the set B_T given by

$$B_T := \bigcup_{\nu \in T} \psi(T_{\hat{\nu}}) \tag{4.34}$$

is of size $m+4$ for all $T \subset \{1,\ldots,n\}$ with $|T| = m+4$.

We can now define a map $\pi_T : T \longrightarrow B_T$ for all $T \subset \{1,\ldots,n\}$, $|T| = m+4$, which maps $\nu \in T$ to the (single) element of the set $B_T \setminus \psi(T_{\hat{\nu}})$. Note that since ψ is a permutation and hence injective, the maps π_T are injective and thus surjective, too. Therefore, it follows that

$$\pi_T(T_{\hat{\nu}}) = \pi_T(T) \setminus \{\pi_T(\nu)\} = \pi_T(T) \setminus (\pi_T(T) \setminus \psi(T_{\hat{\nu}})) = \psi(T_{\hat{\nu}}) \tag{4.35}$$

for all $\nu \in T$.

As mentioned before, it is our aim to "glue" the maps π_T, $T \subset \{1,\ldots,n\}$ with $|T| = m+4$ together to a map $\pi : \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$. For this to make sense, we need to show that

$$(\pi_T)_{|T \cap T'} = (\pi_{T'})_{|T \cap T'} \tag{4.36}$$

for any two subsets $T, T' \subset \{1,\ldots,n\}$ with $|T| = |T'| = m+4$.
Fix some subsets T and T' of size $m+4$. If $|T \cap T'| = m+4$, i. e. if T is equal to T', then the assertion is immediate. Suppose now that the intersection $T \cap T'$ is a set of size $m+3$. Let $i \in T \setminus T'$ and $r \in T' \setminus T$. We claim that

$$\pi_T(T \setminus \{i, \nu\}) = \pi_{T'}(T' \setminus \{r, \nu\})$$

for all $\nu \in T \cap T'$. Assume for a moment that this is true. Then it follows by equality (4.35) and the injectivity of the maps π_T and $\pi_{T'}$ that

$$\begin{aligned}
\{\pi_T(\nu)\} &= \pi_T(T \setminus \{i\}) \setminus \pi_T(T \setminus \{i, \nu\}) \\
&= \psi(T \setminus \{i\}) \setminus \pi_{T'}(T' \setminus \{r, \nu\}) \\
&= \psi(T' \setminus \{r\}) \setminus \pi_{T'}(T' \setminus \{r, \nu\}) \\
&= \pi_{T'}(T' \setminus \{r\}) \setminus \pi_{T'}(T' \setminus \{r, \nu\}) \\
&= \{\pi_{T'}(\nu)\}
\end{aligned}$$

for all $\nu \in T \cap T'$, thus showing (4.36) in case that $|T \cap T'| = m+3$.
For the proof of the claim we first show that

$$\left|\psi(T \setminus \{\nu\}) \cap \psi(T' \setminus \{\nu\})\right| = m+2 \tag{4.37}$$

for all $\nu \in T \cap T'$. Fix some $\nu \in T \cap T'$. As above, we denote the set $T \setminus \{\nu\}$ by $T_{\hat{\nu}}$ and the set $T' \setminus \{\nu\}$ by $T'_{\hat{\nu}}$. Since ψ is a permutation and hence is injective, it is clear that the number of elements in the set $\psi(T_{\hat{\nu}}) \cap \psi(T'_{\hat{\nu}})$ is at most $m+2$. Assume for a contradiction that $|\psi(T_{\hat{\nu}}) \cap \psi(T'_{\hat{\nu}})|$ is strictly smaller than $m+2$. Then the set $\psi(T_{\hat{\nu}}) \setminus \psi(T'_{\hat{\nu}})$ contains at least two elements. We consider two of these elements and denote them by s and t. Recall that by definition of the maps $\rho_{T_{\hat{\nu}}}$ and $\rho_{T'_{\hat{\nu}}}$, the set $\psi(T_{\hat{\nu}})$ is equal to $\rho_{T_{\hat{\nu}}}(T_{\hat{\nu}})$ and the set $\psi(T'_{\hat{\nu}})$ is equal to $\rho_{T'_{\hat{\nu}}}(T'_{\hat{\nu}})$, that means $s, t \in \rho_{T_{\hat{\nu}}}(T_{\hat{\nu}}) \setminus \rho_{T'_{\hat{\nu}}}(T'_{\hat{\nu}})$. We consider different cases to choose elements $j, k \in T_{\hat{\nu}} \setminus \{i\}$.
If neither s nor t is equal to $\rho_{T_{\hat{\nu}}}(i)$, then let $j, k \in T_{\hat{\nu}} \setminus \{i\}$ such that $\{s,t\} = \{\rho_{T_{\hat{\nu}}}(j), \rho_{T_{\hat{\nu}}}(k)\}$. Otherwise, if one of s and t, say t, is equal to $\rho_{T_{\hat{\nu}}}(i)$, then let $j \in T_{\hat{\nu}} \setminus \{i\}$ such that $s = \rho_{T_{\hat{\nu}}}(j)$ and let $k \in T_{\hat{\nu}} \setminus \{i,j\}$ arbitrary. Summarizing this, in any case, we can choose $j, k \in T_{\hat{\nu}} \setminus \{i\}$ such that

$$s, t \in \{\rho_{T_{\hat{\nu}}}(i), \rho_{T_{\hat{\nu}}}(j), \rho_{T_{\hat{\nu}}}(k)\}. \tag{4.38}$$

Denote the elements of the set $(T \cap T') \setminus \{j,k,\nu\}$, by $d_1, \ldots, d_{m-1}$ and l. We then have $T_{\hat{\nu}} = \{d_1, \ldots, d_{m-1}, i, j, k, l\}$ and $T'_{\hat{\nu}} = \{d_1, \ldots, d_{m-1}, r, j, k, l\}$. Applying the automorphism ϕ to relation (4.13) of Theorem 4.10 gives the equation

$$\phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = \phi(c_{d_1,\ldots,d_{m-1},r,j,k,l}) \cdot \phi(c_{d_1,\ldots,d_{m-1},i,j,k,r}).$$

According to the definition of the maps $\rho_{T_{\hat{\nu}}}$ and $\rho_{T'_{\hat{\nu}}}$, we can rewrite this as

$$\begin{aligned} &c_{\rho_{T_{\hat{\nu}}}(d_1),\ldots,\rho_{T_{\hat{\nu}}}(d_{m-1}),\rho_{T_{\hat{\nu}}}(i),\rho_{T_{\hat{\nu}}}(j),\rho_{T_{\hat{\nu}}}(k),\rho_{T_{\hat{\nu}}}(l)} \\ &\quad = c_{\rho_{T'_{\hat{\nu}}}(d_1),\ldots,\rho_{T'_{\hat{\nu}}}(d_{m-1}),\rho_{T'_{\hat{\nu}}}(r),\rho_{T'_{\hat{\nu}}}(j),\rho_{T'_{\hat{\nu}}}(k),\rho_{T'_{\hat{\nu}}}(l)} \cdot \phi(c_{d_1,\ldots,d_{m-1},i,j,k,r}). \end{aligned}$$

By Proposition 4.13 (b), it follows that the set

$$\{\rho_{T_{\hat{\nu}}}(i), \rho_{T_{\hat{\nu}}}(j), \rho_{T_{\hat{\nu}}}(k), \rho_{T_{\hat{\nu}}}(l), \rho_{T'_{\hat{\nu}}}(r), \rho_{T'_{\hat{\nu}}}(j), \rho_{T'_{\hat{\nu}}}(k), \rho_{T'_{\hat{\nu}}}(l)\}$$

has at most five elements. On the other hand, this set contains the elements $\rho_{T'_{\hat{\nu}}}(r), \rho_{T'_{\hat{\nu}}}(j)$, $\rho_{T'_{\hat{\nu}}}(k), \rho_{T'_{\hat{\nu}}}(l) \in \psi(T'_{\hat{\nu}})$ and moreover, by (4.38), the elements s and t. By the choice of s and t, these six elements are pairwise distinct which is clearly a contradiction. Therefore, the assertion (4.37) is true.
Consider the subsets B_T and $B_{T'} \subset \{1, \ldots, n\}$ as defined in (4.34). Since ψ is a bijection and hence injective, it follows from the definition of B_T that the different $m+3$-subsets of B_T are given by $\psi(T_{\hat{\nu}})$, $\nu \in T$. Therefore, again by injectivity of the map ψ, the set B_T cannot contain the ψ-image of the set $T'_{\hat{\nu}}$ for $\nu \in T \cap T'$, i. e. $\psi(T'_{\hat{\nu}}) \nsubseteq B_T$ for all $\nu \in T \cap T'$. By definition of the sets B_T and $B_{T'}$, this shows that

$$B_{T'} \nsubseteq B_T \quad \text{and} \quad B_T \nsubseteq B_{T'}.$$

Since the set $\psi(T \cap T')$ is contained both in B_T and in $B_{T'}$, it follows from the definition of the maps π_T and $\pi_{T'}$ that

$$\begin{aligned} B_T &\not\supseteq B_{T'} \setminus \psi(T \cap T') = \{\pi_{T'}(r)\} \text{ and} \\ B_{T'} &\not\supseteq B_T \setminus \psi(T \cap T') = \{\pi_T(i)\}. \end{aligned}$$

Furthermore, since π_T maps into B_T and $\pi_{T'}$ maps into $B_{T'}$, it follows by (4.37) that

$$\begin{aligned} &\left|\pi_T\left((T \cap T') \setminus \{\nu\}\right) \cap \pi_{T'}\left((T \cap T') \setminus \{\nu\}\right)\right| \\ &\quad = \left|\left(\pi_T\left((T \cap T') \setminus \{\nu\}\right) \cup \{\pi_T(i)\}\right) \cap \left(\pi_{T'}\left((T \cap T') \setminus \{\nu\}\right) \cup \{\pi_{T'}(r)\}\right)\right| \\ &\quad = \left|\pi_T(T \setminus \{\nu\}) \cap \pi_{T'}(T' \setminus \{\nu\})\right| \\ &\quad = \left|\psi(T \setminus \{\nu\}) \cap \psi(T' \setminus \{\nu\})\right| \\ &\quad = m + 2 \end{aligned}$$

for all $\nu \in T \cap T'$. This shows that the set $\pi_T(T \setminus \{i, \nu\}) = \pi_T\left((T \cap T') \setminus \{\nu\}\right)$ must be equal to $\pi_{T'}(T' \setminus \{r, \nu\}) = \pi_{T'}\left((T \cap T') \setminus \{\nu\}\right)$, as claimed.

Let now the size of the intersection $T \cap T'$ be arbitrary. If $T \cap T' = \emptyset$, then for (4.36) to be true there is nothing to show. Otherwise, there exist subsets $T_0 = T, T_1, \ldots, T_{m+2}, T_{m+3} = T' \subset \{1, \ldots, n\}$ of size $m + 4$ such that

$$T \cap T' \subset T_i \quad \text{and} \quad |T_i \cap T_{i-1}| \geq m + 3$$

for all $i \in \{1, \ldots, m + 3\}$. The assertion that $(\pi_T)_{|T \cap T'}$ is equal to $(\pi_{T'})_{|T \cap T'}$ then follows by an iterated application of the proof for the case $|T \cap T'| = m + 3$.

So there exists a (unique) map $\pi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ such that

$$\pi_{|T} = \pi_T \quad \text{for all } T \subset \{1, \ldots, n\}, |T| = m + 4.$$

Since ψ is a permutation of $\tilde{M}$, the union $\bigcup_{T \subset \{1,\ldots,n\},\, |T|=m+4} B_T = \bigcup_{M \in \tilde{M}} \psi(M)$ clearly is equal to the whole set $\{1, \ldots, n\}$. From the surjectivity of the maps $\pi_T : T \longrightarrow B_T$ it hence follows that the map π is surjective, too, and thus is a permutation of the elements in the set $\{1, \ldots, n\}$. The permutation π defines an automorphism ϕ_π of the field $K(C)$ by

$$\phi_\pi : c_{d_1,\ldots,d_{m-1},i,j,k,l} \longmapsto c_{\pi(d_1),\ldots,\pi(d_{m+1}),\pi(i),\pi(j),\pi(k),\pi(l)} \quad \text{for all } c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C.$$

We claim that the map ϕ_π is equal to ϕ, or equivalently, that the map

$$\hat{\phi} := \phi_\pi^{-1} \circ \phi,$$

is equal to the identity map $\mathrm{id}_{K(C)}$. Note that if this claim is true, then the lemma is proved. To prove the claim, observe first that the map ϕ_π^{-1} is equal to the map $\phi_{\pi^{-1}}$. Let $M = \{d_1, \ldots, d_{m-1}, i, j, k, l\} \in \tilde{M}$. Then the $\hat{\phi}$-image of the element $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C$

is given by

$$\begin{aligned}\hat{\phi}(c_{d_1,\ldots,d_{m-1},i,j,k,l}) &= \phi_\pi^{-1} \circ \phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) \\ &= \phi_{\pi^{-1}} \circ \phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) \\ &= c_{\pi^{-1}(\rho_M(d_1)),\ldots,\pi^{-1}(\rho_M(d_{m-1})),\pi^{-1}(\rho_M(i)),\pi^{-1}(\rho_M(j)),\pi^{-1}(\rho_M(k)),\pi^{-1}(\rho_M(l))}.\end{aligned}$$

Recall that by definition the set $\rho_M(M)$ is equal to $\psi(M)$. Hence the set $\pi^{-1}(\rho_M(M))$ is equal to M. It follows that the map $(\pi^{-1})_{|\rho_M(M)} \circ \rho_M$ actually is a permutation of the set M. For $M \in \tilde{M}$, let $\hat{\pi}_M : M \longrightarrow M$ be the permutation defined by

$$\hat{\pi}_M := (\pi^{-1})_{|\rho_M(M)} \circ \rho_M.$$

Then we have $\hat{\phi}(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = c_{\hat{\pi}_M(d_1),\ldots,\hat{\pi}_M(d_{m-1}),\hat{\pi}_M(i),\hat{\pi}_M(j),\hat{\pi}_M(k),\hat{\pi}_M(l)}$ for all $M = \{d_1,\ldots,d_{m-1},i,j,k,l\} \in \tilde{M}$.
Before we start to prove the claim that $\hat{\phi}$ is equal to $\mathrm{id}_{K(C)}$, we analyze the maps $\hat{\pi}_M$, $M \in \tilde{M}$. Let $M \in \tilde{M}$. Suppose first that $\hat{\pi}_M(i) = i$ for some $i \in M$. We show that this implies that $\hat{\pi}_M = \mathrm{id}_M$, i.e.

$$\hat{\pi}_M(i) = i \text{ for some } i \in M \implies \hat{\pi} = \mathrm{id}_M\,. \tag{4.39}$$

Assume for a contradiction that there exists $l \in M \setminus \{i\}$ such that $\hat{\pi}_M(l) \neq l$. Then there exists $k \in M \setminus \{i,l\}$ such that $\hat{\pi}_M(k) = l$. Denote the elements of the set $M \setminus \{i,k,l\}$ by $d_1,\ldots,d_{m-1}$ and j. Let r be an arbitrary element in the nonempty set $\{1,\ldots,n\} \setminus M$ and denote by M' the set given by $M' := \{d_1,\ldots,d_{m-1},r,j,k,l\}$ and by M'' the set given by $M'' := \{d_1,\ldots,d_{m-1},i,j,k,r\}$. Applying the automorphism $\hat{\phi}$ to relation (4.13) of Theorem 4.10 gives the equation

$$\hat{\phi}(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = \hat{\phi}(c_{d_1,\ldots,d_{m-1},r,j,k,l}) \cdot \hat{\phi}(c_{d_1,\ldots,d_{m-1},i,j,k,r}),$$

which by definition of the maps $\hat{\pi}_M, \hat{\pi}_{M'}$ and $\hat{\pi}_{M''}$ can be rewritten as

$$\begin{aligned}&c_{\hat{\pi}_M(d_1),\ldots,\hat{\pi}_M(d_{m-1}),i,\hat{\pi}_M(j),l,\hat{\pi}_M(l)} \\ &\quad= c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),\hat{\pi}_{M'}(l)} \\ &\qquad\cdot c_{\hat{\pi}_{M''}(d_1),\ldots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(j),\hat{\pi}_{M''}(k),\hat{\pi}_{M''}(r)}.\end{aligned}$$

By Lemma 4.12, an application of the map $\omega_{i,l}$ (as defined before Lemma 4.12) to this equation gives

$$\begin{aligned}-1 &= \omega_{i,l}\big(c_{\hat{\pi}_M(d_1),\ldots,\hat{\pi}_M(d_{m-1}),i,\hat{\pi}_M(j),l,\hat{\pi}_M(l)}\big) \\ &= \omega_{i,l}\big(c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),\hat{\pi}_{M'}(l)}\big) \\ &\qquad+ \omega_{i,l}\big(c_{\hat{\pi}_{M''}(d_1),\ldots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(j),\hat{\pi}_{M''}(k),\hat{\pi}_{M''}(r)}\big).\end{aligned}$$

Since neither the set M' nor the set M'' contain both of the elements i and l, it follows

that the sum in the previous equation, i.e.

$$\omega_{i,l}\big(c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),\hat{\pi}_{M'}(l)}\big) + \omega_{i,l}\big(c_{\hat{\pi}_{M''}(d_1),\ldots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(j),\hat{\pi}_{M''}(k),\hat{\pi}_{M''}(r)}\big)$$

is equal to zero. Obviously, this is a contradiction. Therefore, $\hat{\pi}_M$ is equal to id_M, indeed. Next, we show that for all $i \in M$ we have the implication

$$\hat{\pi}_M(i) = l \neq i \implies \hat{\pi}_M(l) = i. \tag{4.40}$$

Let $i \in M$ such that $\hat{\pi}_M(i) = l \neq i$. Assume for a contradiction that $\hat{\pi}_M(l) \neq i$. Then there exists $k \in M \setminus \{i,l\}$ such that $\hat{\pi}_M(k) = i$. Again, we denote the elements of the set $M\backslash\{i,k,l\}$ by $d_1,\ldots,d_{m-1}$ and j. Let r be an element of the (nonempty) set $\{1,\ldots,n\}\backslash M$. As before, set $M' := \{d_1,\ldots,d_{m-1},r,j,k,l\}$ and $M'' := \{d_1,\ldots,d_{m-1},i,j,k,r\}$. Applying the automorphism $\hat{\phi}$ to relation (4.13) of Theorem 4.10 gives the equation

$$\hat{\phi}(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = \hat{\phi}(c_{d_1,\ldots,d_{m-1},r,j,k,l}) \cdot \hat{\phi}(c_{d_1,\ldots,d_{m-1},i,j,k,r}),$$

which by definition of the maps $\hat{\pi}_M, \hat{\pi}_{M'}$ and $\hat{\pi}_{M''}$ can be rewritten as

$$\begin{aligned} &c_{\hat{\pi}_M(d_1),\ldots,\hat{\pi}_M(d_{m-1}),l,\hat{\pi}_M(j),i,\hat{\pi}_M(l)} \\ &\quad = c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),\hat{\pi}_{M'}(l)} \\ &\qquad \cdot c_{\hat{\pi}_{M''}(d_1),\ldots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(j),\hat{\pi}_{M''}(k),\hat{\pi}_{M''}(r)}. \end{aligned}$$

Again by Lemma 4.12, an application of the map $\omega_{l,i}$ to this equation yields

$$\begin{aligned} -1 &= \omega_{l,i}\big(c_{\hat{\pi}_M(d_1),\ldots,\hat{\pi}_M(d_{m-1}),l,\hat{\pi}_M(j),i,\hat{\pi}_M(l)}\big) \\ &= \omega_{l,i}\big(c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),\hat{\pi}_{M'}(l)}\big) \\ &\quad + \omega_{l,i}\big(c_{\hat{\pi}_{M''}(d_1),\ldots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(j),\hat{\pi}_{M''}(k),\hat{\pi}_{M''}(r)}\big). \end{aligned}$$

As before, since neither the set M' nor the set M'' do contain both of the elements i and l, we get a contradiction.

We can now prove the claim that $\hat{\phi}$ is equal to $\mathrm{id}_{K(C)}$. Suppose first that m is equal to 1. Then for all pairwise distinct $i,j,k,l \in \{1,\ldots,n\}$ we have the equality

$$\hat{\phi}(c_{i,j,k,l}) = c_{\hat{\pi}_{\{i,j,k,l\}}(i),\hat{\pi}_{\{i,j,k,l\}}(j),\hat{\pi}_{\{i,j,k,l\}}(k),\hat{\pi}_{\{i,j,k,l\}}(l)}.$$

From (4.39) and (4.40), it follows that the map $\hat{\pi}_{\{i,j,k,l\}} : \{i,j,k,l\} \longrightarrow \{i,j,k,l\}$ is one of $\mathrm{id}_M, (i,j)(k,l), (i,k)(j,l), (i,l)(j,k)$. In any of these cases, it follows by relation (4.9) of Theorem 4.10 that $\hat{\phi}(c_{i,j,k,l})$ is equal to $c_{i,j,k,l}$. But this means that the map $\hat{\phi}$ is equal to $\mathrm{id}_{K(C)}$, and so the claim is true in this case.
If m is equal to 2, then it follows from implication (4.40) that for all $M \subset \{1,\ldots,n\}$ with $|M| = m+3 = 5$ there must be $i \in M$ such that $\hat{\pi}_M(i) = i$. By (4.39), this means that $\hat{\pi}_M = \mathrm{id}_M$ and again the claim that $\hat{\phi}$ is equal to $\mathrm{id}_{K(C)}$ is true.

Let now m be at least 3. Let $M \in \tilde{M}$ and assume for a contradiction that there exists an element $i \in M$ such that $l := \hat{\pi}_M(i) \neq i$ and hence $\hat{\pi}_M(l) = i$ (cf. (4.40)). Let $r \in \{1, \ldots, n\} \setminus M$ and let M' be the set given by $M' := (M \setminus \{i\}) \cup \{r\}$. We claim that these assumptions imply

$$\begin{aligned} &\hat{\pi}_{M'}(r) = \hat{\pi}_M(i) = l, \\ &\hat{\pi}_{M'}(l) = r, \\ &\hat{\pi}_{M'}(j) = \hat{\pi}_M(j) \text{ for all } j \in (M \cap M') \setminus \{l\}. \end{aligned} \tag{4.41}$$

Denote the remaining elements of $M \cap M'$, that is the elements in $(M \cap M') \setminus \{l\}$ by $d_1, \ldots, d_{m-1}, j$ and k. We then have $M = \{d_1, \ldots, d_{m-1}, i, j, k, l\}$ and $M' = \{d_1, \ldots, d_{m-1}, r, j, k, l\}$. Moreover, denote the set $\{d_1, \ldots, d_{m-1}, i, j, k, r\}$ by M''. Again, we apply the automorphism $\hat{\phi}$ to relation (4.13) of Theorem 4.10. This gives

$$\hat{\phi}(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = \hat{\phi}(c_{d_1,\ldots,d_{m-1},r,j,k,l}) \cdot \hat{\phi}(c_{d_1,\ldots,d_{m-1},i,j,k,r}),$$

which by the definition of the maps $\hat{\pi}_M$ and $\hat{\pi}_{M'}$ and $\hat{\pi}_{M''}$ can be rewritten as

$$\begin{aligned} &c_{\hat{\pi}_M(d_1),\ldots,\hat{\pi}_M(d_{m-1}),l,\hat{\pi}_M(j),\hat{\pi}_M(k),i} \\ &\quad = c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),\hat{\pi}_{M'}(l)} \\ &\qquad \cdot c_{\hat{\pi}_{M''}(d_1),\ldots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(j),\hat{\pi}_{M''}(k),\hat{\pi}_{M''}(r)}. \end{aligned}$$

Applying the map $\omega_{l,\hat{\pi}_M(j)}$ to this equation hence gives

$$\begin{aligned} 1 &= \omega_{l,\hat{\pi}_M(j)}\big(c_{\hat{\pi}_M(d_1),\ldots,\hat{\pi}_M(d_{m-1}),l,\hat{\pi}_M(j),\hat{\pi}_M(k),i}\big) \\ &= \omega_{l,\hat{\pi}_M(j)}\big(c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),\hat{\pi}_{M'}(l)}\big) \\ &\qquad + \omega_{l,\hat{\pi}_M(j)}\big(c_{\hat{\pi}_{M''}(d_1),\ldots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(j),\hat{\pi}_{M''}(k),\hat{\pi}_{M''}(r)}\big) \\ &= \omega_{l,\hat{\pi}_M(j)}\big(c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),\hat{\pi}_{M'}(l)}\big) + 0. \end{aligned} \tag{4.42}$$

Note that (4.42) is true for arbitrary labellings $d_1, \ldots, d_{m-1}, j, k$ of the elements in the set $(M \cap M') \setminus \{l\}$. Therefore – by Lemma 4.12 – it follows that $l \in \{\hat{\pi}_{M'}(r), \hat{\pi}_{M'}(j), \hat{\pi}_{M'}(k), \hat{\pi}_{M'}(l)\}$ for arbitrary choices of j and $k \in (M' \cap M) \setminus \{l\}$. Assume for a contradiction that l is not contained in $\{\hat{\pi}_{M'}(r), \hat{\pi}_{M'}(l)\}$. Then l must be contained in the set $\{\hat{\pi}_{M'}(j), \hat{\pi}_{M'}(k)\}$ for arbitrary choices of j and $k \in (M' \cap M) \setminus \{l\}$. Since $(M' \cap M) \setminus \{l\}$ is a set with at least four elements and $\hat{\pi}_{M'}$ is a permutation of the set M' and hence injective, this is a contradiction. It follows that $l \in \{\hat{\pi}_{M'}(r), \hat{\pi}_{M'}(l)\}$.
Suppose that $l = \hat{\pi}_{M'}(l)$. Then – again by Lemma 4.12 – if follows from equation (4.42) that $\hat{\pi}_{M'}(k)$ is equal to $\hat{\pi}_M(j)$. As before, this must be true for all choices of $k \in (M \cap M') \setminus \{l, j\}$, a set which has at least three elements. By the fact that $\hat{\pi}_{M'}$ is a permutation of the set M' and hence injective, we get a contradiction. Therefore, $l = \hat{\pi}_{M'}(r)$ and hence also $\hat{\pi}_{M'}(l) = r$ (cf. (4.40)). We can thus rewrite equation (4.42) as

$$\begin{aligned} 1 &= \omega_{l,\hat{\pi}_M(j)}\big(c_{\hat{\pi}_M(d_1),\ldots,\hat{\pi}_M(d_{m-1}),l,\hat{\pi}_M(j),\hat{\pi}_M(k),i}\big) \\ &= \omega_{l,\hat{\pi}_M(j)}\big(c_{\hat{\pi}_{M'}(d_1),\ldots,\hat{\pi}_{M'}(d_{m-1}),l,\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k),r}\big) + 0. \end{aligned}$$

As before, this is true for arbitrary labellings $d_1,\dots,d_{m-1},j,k$ of the elements in the set $(M\cap M')\setminus\{l\}$. In particular, $j\in(M\cap M')\setminus\{l\}$ can be chosen arbitrarily. Therefore, by Lemma 4.12, it follows that $\hat{\pi}_{M'}(j)$ is equal to $\hat{\pi}_M(j)$ for all $j\in(M\cap M')\setminus\{l\}$ and the claim (4.41) is proved.

Let $k\in(M\cap M')\setminus\{l\}$, where again $M':=(M\setminus\{i\})\cup\{r\}$ for some $r\in\{1,\dots,n\}\setminus M$. By the assumption that $\hat{\pi}_M(i)$ is not equal to i, it follows that $d_1:=\hat{\pi}_M(k)$ is an element in $(M\cap M')\setminus\{l\}$ which is not equal to k (cf. (4.39)). By (4.40), we hence have $k=\hat{\pi}_M(d_1)$. Let $j\in(M\cap M')\setminus\{l,k,d_1\}$, a set which has at least two elements. Since $\hat{\pi}_M$ is not the identity map on M, it follows that $d_2:=\hat{\pi}_M(j)$ is an element in $(M\cap M')\setminus\{l,k,d_1\}$ which is not equal to j (cf. (4.39)). Denote the elements in the set $(M\cap M')\setminus\{j,k,l,d_1,d_2\}$ by $d_3,\dots,d_{m-1}$. We then have $M=\{d_1,\dots,d_{m-1},i,l,j,k\}$ and $M'=\{d_1,\dots,d_{m-1},r,l,j,k\}$. Furthermore, denote the set $\{d_1,\dots,d_{m-1},i,l,j,r\}$ by M''. Consider the equation

$$\hat{\phi}(c_{d_1,\dots,d_{m-1},i,l,j,k})=\hat{\phi}(c_{d_1,\dots,d_{m-1},r,l,j,k})\cdot\hat{\phi}(c_{d_1,\dots,d_{m-1},i,l,j,r}),$$

which by definition of the maps $\hat{\pi}_M$, $\hat{\pi}_{M'}$ and $\hat{\pi}_{M''}$ can be rewritten as

$$\begin{aligned}c_{\hat{\pi}_M(d_1),\dots,\hat{\pi}_M(d_{m-1}),\hat{\pi}_M(i),\hat{\pi}_M(l),\hat{\pi}_M(j),\hat{\pi}_M(k)}&=\\ =c_{\hat{\pi}_{M'}(d_1),\dots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(l),\hat{\pi}_{M'}(j),\hat{\pi}_{M'}(k)}&\\ \cdot c_{\hat{\pi}_{M''}(d_1),\dots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(l),\hat{\pi}_{M''}(j),\hat{\pi}_{M''}(r)}.&\end{aligned}$$

Note that $M'=(M\setminus\{i\})\cup\{r\}$ and $M''=(M\setminus\{k\})\cup\{r\}$. It hence follows from (4.41) that

$$\begin{aligned}\hat{\pi}_{M'}(j)&=\hat{\pi}_M(j)=d_2\\ \hat{\pi}_{M'}(k)&=\hat{\pi}_M(k)=d_1\\ \hat{\pi}_{M''}(r)&=\hat{\pi}_M(k)=d_1\\ \hat{\pi}_{M''}(j)&=\hat{\pi}_M(j)=d_2.\end{aligned}$$

So the above equation can be written as

$$\begin{aligned}c_{\hat{\pi}_M(d_1),\dots,\hat{\pi}_M(d_{m-1}),\hat{\pi}_M(i),\hat{\pi}_M(l),d_2,d_1}&\\ =c_{\hat{\pi}_{M'}(d_1),\dots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(l),d_2,d_1}&\\ \cdot c_{\hat{\pi}_{M''}(d_1),\dots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(l),d_2,d_1}.&\end{aligned}$$

Applying the map ω_{d_2,d_1} to this equation then gives

$$\begin{aligned}1&=\omega_{d_2,d_1}(c_{\hat{\pi}_M(d_1),\dots,\hat{\pi}_M(d_{m-1}),\hat{\pi}_M(i),\hat{\pi}_M(l),d_2,d_1})\\ &=\omega_{d_2,d_1}(c_{\hat{\pi}_{M'}(d_1),\dots,\hat{\pi}_{M'}(d_{m-1}),\hat{\pi}_{M'}(r),\hat{\pi}_{M'}(l),d_2,d_1})\\ &\quad+\omega_{d_2,d_1}(c_{\hat{\pi}_{M''}(d_1),\dots,\hat{\pi}_{M''}(d_{m-1}),\hat{\pi}_{M''}(i),\hat{\pi}_{M''}(l),d_2,d_1})\\ &=1+1,\end{aligned}$$

clearly a contradiction.
This shows that the map $\hat{\pi}_M$ is equal to id_M and hence that $\hat{\phi}$ is equal to $\mathrm{id}_{K(C)}$, as desired. ∎

With the preceding lemma we are now in the situation where we finally can construct a set of generating elements of the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$. For better readability of the following theorem, we introduce some more notation. Let

$$\begin{aligned} &a_1(X_{1,0}, \ldots, X_{1,m}, \ldots, X_{m+3,0}, \ldots, X_{m+3,m}), \ldots, \\ &\quad a_d(X_{1,0}, \ldots, X_{1,m}, \ldots, X_{m+3,0}, \ldots, X_{m+3,m}) \\ &\qquad \in K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}} \subset K(X_{1,1}/X_{1,0}, \ldots, X_{m+3,m}/X_{m+3,0}) \\ &\qquad\quad \subset K(X_{1,0}, \ldots, X_{1,m}, \ldots, X_{m+3,0}, \ldots, X_{m+3,m}) \end{aligned}$$

be pairwise distinct non-constant generators of the field $K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}}$ over K (e. g. those of Theorem 4.15). For $M \in \tilde{M}$, define the set C_M to be

$$C_M := \{c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C;\ \{d_1, \ldots, d_{m-1}, i, j, k, l\} = M\}.$$

Moreover, if $M = \{i_1, \ldots, i_{m+3}\} \in \tilde{M}$, let the rational function $a_{j,M} \in K((\mathbb{P}^m)^n) = K(X_{1,1}/X_{1,0}, \ldots, X_{n,m}/X_{n,0})$ with $j \in \{1, \ldots, d\}$ be defined by

$$a_{j,M} := a_j(X_{i_1,0}, \ldots, X_{i_1,m}, \ldots, X_{i_{m+3},0}, \ldots, X_{i_{m+3},m}) \in K(C_M).$$

Note that since $a_j \in K((\mathbb{P}^m)^{m+3})^{\mathrm{PGL}_{m+1} \times \mathrm{S}_{m+3}}$ is invariant under permutation of variables induced by the action of S_{m+3}, this definition of $a_{j,M}$ does only depend on M and not on the concrete order of the elements $i_1, \ldots, i_{m+3}$. Consider the natural action of the symmetric group S_M on $K(C_M)$ which is given by

$$\pi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = c_{\pi(d_1),\ldots,\pi(d_{m-1}),\pi(i),\pi(j),\pi(k),\pi(l)}$$

for all $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C_M$ and $\pi \in \mathrm{S}_M$. Clearly, the invariant field with respect to this action is given by $K(C_M)^{\mathrm{S}_M} = K(a_{1,M}, \ldots, a_{d,M})$.
Let $M \in \tilde{M}$, let Y be an indeterminate over $K(C)$ and define $t := |C_M|$ (in fact, t is independent of $M \in \tilde{M}$). Furthermore, let $Z_1, \ldots, Z_d$ be indeterminates over K. By Theorem 4.15, it follows that there exist functions $f_0, \ldots, f_{t-1} \in K(Z_1, \ldots, Z_d)$ such that $f_i(a_{1,M}, \ldots, a_{d,M}) \in K(C_M)$ is defined for $i \in \{0, \ldots, t-1\}$ and

$$\prod_{c \in C_M} (Y - c) = Y^t - \sum_{i=0}^{t-1} f_i(a_{1,M}, \ldots, a_{d,M}) Y^i \in K(C_M)[Y] \qquad \text{for all } M \in \tilde{M}.$$

Theorem 4.18. *Let $Y_1, \ldots, Y_{d+1}$ be indeterminates over $K(C)$ and let*

$$F := \prod_{M\in\tilde{M}} (Y_{d+1} + \sum_{i=1}^{d} a_{i,M}Y_i) \in K(C)[Y_1, \ldots, Y_{d+1}].$$

Then the coefficients of the polynomial F generate the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}\times \mathrm{S}_n}$ over K.

Proof. Let L be the field generated by the coefficients of F over K. We need to show that L is equal to $K(C)^{\mathrm{S}_n} = K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}\times \mathrm{S}_n}$.
First we show that $L \subset K(C)^{\mathrm{S}_n}$. Let $\pi \in \mathrm{S}_n$ be a permutation of the set $\{1, \ldots, n\}$ and let ϕ_π be the induced K-automorphism of the field $K(C)$, that is

$$\phi_\pi : c_{d_1,\ldots,d_{m-1},i,j,k,l} \longmapsto c_{\pi(d_1),\ldots,\pi(d_{m-1}),\pi(i),\pi(j),\pi(k),\pi(l)} \text{ for all } c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C.$$

Note that $\phi_\pi(a_{i,M}) = a_{i,\pi(M)}$ for all $i \in \{1, \ldots, d\}$, $M \in \tilde{M}$. It follows that the extension of the map ϕ_π to the polynomial ring $K(C)[Y_1, \ldots, Y_{d+1}]$ by setting $\phi_\pi(Y_i) = Y_i$ for all $i \in \{1, \ldots, d+1\}$ permutes the factors $(Y_{d+1} + \sum_{i=1}^{d} a_{i,M}Y_i)$, $M \in \tilde{M}$ of the polynomial F. Hence the coefficients of the polynomial F are invariant under the action of the symmetric group S_n, which shows $L \subset K(C)^{\mathrm{S}_n}$.

For the reverse inclusion we first show that $K(C)|L$ is Galois. We start with proving that the field extension $K(a_{i,M};\ i \in \{1, \ldots, d\}, M \in \tilde{M})|L$ is Galois. Let Y be an indeterminate over K. Consider the separable polynomial

$$\tilde{F} := \prod_{i=1}^{d} \prod_{M\in\tilde{M}} (Y - a_{i,M}) \in K(C)[Y].$$

Let $i \in \{1, \ldots, d\}$ and let ψ_i be the L-algebra homomorphism

$$\psi_i : L[Y_1, \ldots, Y_{d+1}] \longrightarrow L[Y]$$

defined by $Y_{d+1} \longmapsto Y$, $Y_i \longmapsto -1$ and $Y_j \longmapsto 0$ for all $j \in \{1, \ldots, d\} \setminus \{i\}$. Then the ψ_i-image of the polynomial $F \in L[Y_1, \ldots, Y_{d+1}]$ is given by

$$\psi_i(F) = \prod_{M\in\tilde{M}} (Y - a_{i,M})$$

It follows that each of the factors $\prod_{M\in\tilde{M}}(Y - a_{i,M})$ of the polynomial $\tilde{F}$ lies in $L[Y]$, so also $\tilde{F} \in L[Y]$. As the field $K(a_{i,M};\ i \in \{1, \ldots, d\}, M \in \tilde{M})$ is the splitting field of the separable polynomial $\tilde{F}$, this shows that the field extension $K(a_{i,M};\ i \in \{1, \ldots, d\}, M \in \tilde{M})|L$ is Galois, indeed.

Let ϕ be an element of the Galois group $\mathrm{Gal}(K(a_{i,M};\ i \in \{1, \ldots, d\}, M \in \tilde{M})|L)$. Then the extension of the automorphism ϕ to the polynomial ring $K(a_{i,M};\ i \in \{1, \ldots, d\}, M \in \tilde{M})[Y_1, \ldots, Y_{d+1}]$ by setting $\phi(Y_i) = Y_i$ for all $i \in \{1, \ldots, d+1\}$ clearly fixes the polynomial

$F = \prod_{M \in \tilde{M}} (Y_{d+1} + \sum_{i=1}^{d} a_{i,M} Y_i)$. Note that the factors of F, i. e. $(Y_{d+1} + \sum_{i=1}^{d} a_{i,M} Y_i)$ are irreducible. It follows that there exists a permutation $\psi_\phi \in \mathrm{S}_{\tilde{M}}$ such that

$$\phi\left(Y_{d+1} + \sum_{i=1}^{d} a_{i,M} Y_i\right) = Y_{d+1} + \sum_{i=1}^{d} a_{i,\psi_\phi(M)} Y_i \qquad \text{for all } M \in \tilde{M},$$

which implies $\phi(a_{i,M}) = a_{i,\psi_\phi(M)}$ for all $i \in \{1, \ldots, d\}$, $M \in \tilde{M}$.
Consider the polynomial

$$\begin{aligned}\hat{F} :&= \prod_{M \in \tilde{M}} \left(\prod_{c \in C_M} (Y - c) \right) = \prod_{M \in \tilde{M}} \left(Y^t - \sum_{i=0}^{t-1} f_i(a_{1,M}, \ldots, a_{d,M}) Y^i \right) \\ &\in K(a_{i,M};\ i \in \{1, \ldots, d\}, M \in \tilde{M})[Y].\end{aligned}$$

Then we have

$$\begin{aligned}\phi(\hat{F}) &= \prod_{M \in \tilde{M}} \left(Y^t - \sum_{i=0}^{t-1} f_i(\phi(a_{1,M}), \ldots, \phi(a_{d,M})) Y^i \right) \\ &= \prod_{M \in \tilde{M}} \left(Y^t - \sum_{i=0}^{t-1} f_i(a_{1,\psi_\phi(M)}, \ldots, a_{d,\psi_\phi(M)}) Y^i \right) \\ &= \hat{F}.\end{aligned}$$

It follows that the polynomial $\hat{F}$ has only coefficients in the fixed field of the Galois group $\mathrm{Gal}(K(a_{i,M};\ i \in \{1, \ldots, d\}, M \in \tilde{M})|L)$ which is equal to L and hence $\hat{F} \in L[Y]$. Since $K(C)$ is the splitting field of the separable polynomial $\hat{F} \in L[Y]$, the field extension $K(C)|L$ is Galois, indeed.

Let now ϕ be an element of the Galois group $\mathrm{Gal}(K(C)|L)$. Then ϕ fixes the polynomial $F \in L[Y_1, \ldots, Y_{d+1}]$. In the same way as above, it follows that there exists a permutation $\psi_\phi \in \mathrm{S}_{\tilde{M}}$ such that $\phi(a_{i,M}) = a_{i,\psi_\phi(M)}$ for all $i \in \{1, \ldots, d\}$, $M \in \tilde{M}$. Hence for $M \in \tilde{M}$ we have

$$\begin{aligned}\phi\left(\prod_{c \in C_M} (Y - c) \right) &= \phi\left(Y^t - \sum_{i=0}^{t-1} f_i(a_{1,M}, \ldots, a_{d,M}) Y^i \right) \\ &= Y^t - \sum_{i=0}^{t-1} f_i(a_{1,\psi_\phi(M)}, \ldots, a_{d,\psi_\phi(M)}) Y^i \\ &= \prod_{c \in C_{\psi_\phi(M)}} (Y - c).\end{aligned}$$

It follows that for all $M \in \tilde{M}$ the automorphism ϕ maps the set C_M bijectively onto the set $C_{\psi_\phi(M)}$, which implies that $\phi_{|K(C_M)}$ is an isomorphism of the fields $K(C_M)$ and $K(C_{\psi_\phi(M)})$.

Let $M \in \tilde{M}$, let $\tau_M : \psi_\phi(M) \longrightarrow M$ be some bijection and let $\phi_{\tau_M} : K(C_{\psi_\phi(M)}) \longrightarrow K(C_M)$ be the induced isomorphism of fields, i.e.

$$\phi_{\tau_M} : c_{d_1,\ldots,d_{m-1},i,j,k,l} \longmapsto c_{\tau_M(d_1),\ldots,\tau_M(d_{m-1}),\tau_M(i),\tau_M(j),\tau_M(k),\tau_M(l)}$$

for all $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C_{\psi_\phi(M)}$. Then the map $\phi_{\tau_M} \circ \phi_{|K(C_M)}$ is an automorphism of the field $K(C_M)$ which permutes the elements of the set C_M. It follows by Lemma 4.14 that there exists a permutation $\pi_M : M \longrightarrow M$ such that the induced automorphism

$$\begin{aligned} \phi_{\pi_M} &: K(C_M) \longrightarrow K(C_M) \\ c_{d_1,\ldots,d_{m-1},i,j,k,l} &\longmapsto c_{\pi_M(d_1),\ldots,\pi_M(d_{m-1}),\pi_M(i),\pi_M(j),\pi_M(k),\pi_M(l)} \end{aligned}$$

for all $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C_M$ coincides with the map $\phi_{\tau_M} \circ \phi_{|K(C_M)}$. So we get the equality $\phi_{|K(C_M)} = \phi_{\tau_M}^{-1} \circ \phi_{\pi_M}$. Let $\rho_M : M \longrightarrow \psi(M)$ be the bijection given by $\rho_M := \tau_M^{-1} \circ \pi_M : M \longrightarrow \psi_\phi(M)$. Then

$$\phi(c_{d_1,\ldots,d_{m-1},i,j,k,l}) = c_{\rho_M(d_1),\ldots,\rho_M(d_{m-1}),\rho_M(i),\rho_M(j),\rho_M(k),\rho_M(l)}$$

for all $c_{d_1,\ldots,d_{m-1},i,j,k,l} \in C_M$.
It follows by Lemma 4.17, that there exists a permutation $\pi \in \mathrm{S}_n$ such that $\phi = \phi_\pi$. Therefore, the Galois group $\mathrm{Gal}(K(C)|L)$ is contained in the group $\{\phi_\pi;\ \pi \in \mathrm{S}_n\}$ and hence by Galois theory, $K(C)^{\mathrm{S}_n}$ is contained in $L = K(C)^{\mathrm{Gal}(K(C)|L)}$. This proves the proposition. ∎

Remark 4.19. As before, if we are interested in computing the values of the coefficients of the polynomial F at some point $P \in (\mathbb{P}^m)^n$, then we actually do not have to know the coefficients of the polynomial F explicitly. By the special form of the polynomial F we see that the distribution of the tuples $(a_{1,M}(P), \ldots, a_{d,M}(P)) \in K^d,\ M \in \tilde{M}$, i. e. $(a_{1,M}(P), \ldots, a_{d,M}(P)) \in K^d;\ M \in \tilde{M}$, is a perfect representation of these values. For more details about a similar consideration, see the discussion after Theorem 4.15. ♢

Now we come to our final task, the examination of the separating properties of the elements in the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}\times \mathrm{S}_n}$.

Proposition 4.20. *If $n \leq m+2$, then the $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$-orbit of the point configuration given by the first n points of $(1:0:\ldots:0), \ldots, (0:\ldots:0:1), (1:\ldots:1)$ is open in $(\mathbb{P}^m)^n$. In particular, the invariant field separates orbits in this nonempty open set.*
If $n > m+2$, then the invariant field $K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1}\times \mathrm{S}_n}$ separates the orbits in the $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$-stable nonempty open set

$$H := \{(P_1, \ldots, P_n) \in (\mathbb{P}^m)^n;\ \prod_{\substack{d_1,\ldots,d_{m+1}\in\{1,\ldots,n\} \\ d_1<\ldots<d_{m+1}}} [d_1, \ldots, d_{m+1}](P_1, \ldots, P_n) \neq 0\},$$

the set of point configurations $(P_1, \ldots, P_n) \in (\mathbb{P}^m)^n$ such that no $m+1$ of the points are

in a hypersurface.

Proof. Suppose first that $n \leq m+2$. As in Proposition 4.9, it can be verified that the PGL_{m+1}-orbit of the point configuration given by the first n points of $(1:0:\ldots:0), \ldots, (0:\ldots:0:1), (1:\ldots:1)$ is the set of point configurations $(P_1, \ldots, P_n) \in (\mathbb{P}^m)^n$ such that at least one $n \times n$-minor of the $(m+1) \times n$-matrix whose ith column is given by homogeneous coordinates of the point P_i for $i \in \{1, \ldots, n\}$ is not equal to zero. This is clearly an open set. Moreover, it is not hard to see that this set is $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$-stable. Therefore, it is in fact an open $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$-orbit.
Let now n be at least $m+3$ and let Y_1, Y_2 be indeterminates over K. Denote the elements of the set C by $c_1, \ldots, c_d$ with $d \in \mathbb{N}$ appropriate, and consider the polynomial

$$\tilde{F} := \prod_{\pi \in \mathrm{S}_n} \left(Y_1 - \sum_{i=1}^{d} \pi(c_i) Y_2^i \right) \in K(C)[Y_1, Y_2]$$

whose coefficients clearly are invariant under the action of the group $\mathrm{PGL}_{m+1} \times \mathrm{S}_n$, i. e. $\tilde{F} \in K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}[Y_1, Y_2]$. Let P and P' be point configurations contained in the open subset H such that the orbits $\mathrm{PGL}_{m+1} \times \mathrm{S}_n(P)$ and $\mathrm{PGL}_{m+1} \times \mathrm{S}_n(P')$ cannot be separated by rational invariants $f \in K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$. As P and P' were assumed to be in H, all rational functions in the set C are defined at these points. Hence by construction of the polynomial $\tilde{F}$, the coefficients of $\tilde{F} \in K((\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}[Y_1, Y_2]$ are defined at P and P', too. So we have

$$\prod_{\pi \in \mathrm{S}_n} \left(Y_1 - \sum_{i=1}^{d} \pi(c_i)(P) Y_2^i \right) = \prod_{\pi \in \mathrm{S}_n} \left(Y_1 - \sum_{i=1}^{d} \pi(c_i)(P') Y_2^i \right).$$

It follows that there exists a permutation $\pi \in \mathrm{S}_n$ such that

$$\sum_{i=1}^{d} c_i(P) Y_2^i = \sum_{i=1}^{d} \pi(c_i)(P') Y_2^i = \sum_{i=1}^{d} c_i(\pi^{-1}(P')) Y_2^i.$$

In particular, this means that $c_i(P) = c_i(\pi^{-1}(P'))$ for all $i \in \{1, \ldots, d\}$. From the fact that $\pi^{-1}(P')$ is again in H, it follows by Proposition 4.9 that the point $\pi^{-1}(P')$ is in the same PGL_{m+1}-orbit as the point P. In other words, we have $(\mathrm{PGL}_{m+1} \times \mathrm{S}_n)(P) = (\mathrm{PGL}_{m+1} \times \mathrm{S}_n)(P')$. Thus the elements in the invariant field $K((\mathbb{P}^m)^n)$ separate the orbits contained in the nonempty open set H, as asserted. ∎

By the previous proposition, a point configuration P contained in the nonempty open set H – or more precisely its orbit – can be recognized by the values of the rational invariants evaluated at P. As mentioned before, if it is only desired to check whether two point configurations can be separated by a set of generating invariants or not – as it is usually the case in the applications – it is not necessary to know any invariants explicitly. For example, as we have seen, the values of the elements of the set of generating invariants as given in Theorem 4.18 at a point configuration P are perfectly represented by the distribution of the tuples $(a_{1,M}(P), \ldots, a_{d,M}(P))$, $M \in \tilde{M}$. In particular, if two point configurations P and P' have different such distributions, then they cannot be contained

in the same $\mathrm{PGL}_{m+1} \times S_n$-orbit. Furthermore, it is worth mentioning from an applied point of view that – as we have seen exemplarily for the cases that $m \in \{1, 2, 3\}$ – this distribution can be computed in an efficient way.

This completes our examination of the invariant field $(K(\mathbb{P}^m)^n)^{\mathrm{PGL}_{m+1} \times \mathrm{S}_n}$.

A Code

At various places in the thesis, computations have been done with the computer algebra sytem Magma. Some of the code that was used for these computations is listed below.

```
/*

FUNCTION AnyRepresentative

Let K be a field, X_1, ..., X_n be indeterminates over K and I an
ideal of K[X_1, ..., X_n]. Let g be an element of the affine algebra
K[X_1, ..., X_n]/I.

The function AnyRepresentative computes a representative of g+I, i.e.
a polynomial h in K[X_1, ..., X_n] such that h+I = g+I. Of course
such a h is not unique (unlike I is the zero ideal).

Input (g):
- g: an element of an affine algebra K[X_1, ..., X_n]/I.

Output (h):
- h: a polynomial in K[X_1, ..., X_n] as described above.

*/


AnyRepresentative:=function(g)

  if (Type(Parent(g)) eq RngMPol) then
    return g;
  elif (Type(Parent(g)) eq RngMPolRes) then
    return PreimageRing(Parent(g))!g;
  else
    error "Wrong types.";
  end if;

end function;
```

```
/*

FUNCTION MQSIdeal

Let K be a field, X_1, ..., X_n be indeterminates over K and I a
prime ideal of K[X_1, ..., X_n]. Let genL be a list of elements of
Quot(K[X_1, ..., X_n]/I).

The function MQSIdeal computes the MQS ideal of X_1+I, ..., X_n+I
over the field L:=K(genL).

Input (KX,I,genL):
- KX: a polynomial ring over K.
- I: a prime ideal of KX.
- genL: a list of elements of Quot(KX/I).


Optional, an instance of the ring Quot(K[X_1, ..., X_n]/I)[Z_1, ..., Z_n],
in which the resulting MQS ideal lies may be specified via the
parameter KfxZ. If the parameter KfxZ is not set, a new instance of
Quot(K[X_1, ..., X_n]/I)[Z_1, ..., Z_n] is created.


Output J:
- J: the MQS ideal as described above. This lives in the ring
     Quot(K[X_1, ..., X_n]/I)[Z_1, ..., Z_n].

*/


MQSIdeal:=function(KX,I,genL: KfxZ:=1)

  // Error Handling
  if (Generic(I) ne KX) then
    error "Wrong types.";
  end if;

  if genL eq [] then
    error "Cannot have an empty list (genL) as argument.";
  end if;

  Kfx:=FieldOfFractions(KX/I);

  n:=Rank(KX);
  KfxWZ:=PolynomialRing(Kfx,1+n);
```

```
  genLN:=[AnyRepresentative(Numerator(genL[i])): i in [1..#genL]];
  genLD:=[AnyRepresentative(Denominator(genL[i])): i in [1..#genL]];

  phi:=hom<KX->KfxWZ | [KfxWZ.(1+i): i in [1..n]]>;
  d:=&*genLN;
  HI:=ideal<KfxWZ | [KfxWZ.1*phi(d)-1] cat
    [phi(genLN[i])-KfxWZ!genL[i]*phi(genLD[i]): i in [1..#genL]] cat
    [phi(g): g in Basis(I)]>;

  delete genLD;
  delete genLN;
  delete d;
  delete phi;

  J:=EliminationIdeal(HI,{KfxWZ.i: i in [2..1+n]});
  if KfxZ cmpeq 1 then
      KfxZ:=PolynomialRing(Kfx,n);
  end if;

  phi:=hom<KfxWZ->KfxZ | [KfxZ!0] cat [KfxZ.i: i in [1..n]]>;
  J:=ideal<KfxZ | [phi(g): g in Basis(J)]>;
  delete phi;

  return J;

end function;



/*

FUNCTION MQSIdealTaggedVersion

Let K be a field, X_1, ..., X_n be indeterminates over K and I a
prime ideal of K[X_1, ..., X_n]. Let genL be a list of elements of
Quot(K[X_1, ..., X_n]/I).

The function MQSIdealTaggedVersion computes the tagged MQS ideal of
X_1+I, ..., X_n+I over the field K(genL) and the ideal of relations
of the elements of genL over K.

Input (KX,I,genL):
- KX: a polynomial ring over K.
- I: a prime ideal of KX.
```

```
- genL: a list of elements of Quot(KX/I).


Optionally, instances of the rings K[Z_1, ..., Z_n,T_1, ..., T_m]
(where m is the length of genL), in which the resulting tagged MQS
ideal lies, and K[T_1, ..., T_m], in which the resulting relation
ideal lies, may be specified via the parameters KZT and KT. If the
parameters KZT resp. KT are not set, new instances of
K[Z_1, ..., Z_n,T_1, ..., T_m] resp. K[T_1, ..., T_m] are created.


Output (J,S):
- J: the tagged MQS ideal of X_1+I, ..., X_n+I over K(genL). This
     lives in the ring K[Z_1, ..., Z_n,T_1, ..., T_m].
- S: the relation ideal of the elements of genL over K. This lives
     in K[T_1, ..., T_m].

*/


MQSIdealTaggedVersion:=function(KX,I,genL: KZT:=1,KT:=1)

  // Error Handling
  if (Generic(I) ne KX) then
    error "Wrong types.";
  end if;

  if genL eq [] then
    error "Cannot have an empty list (genL) as argument.";
  end if;

  n:=Rank(KX);
  m:=#genL;

  KWZT:=PolynomialRing(CoefficientRing(KX),1+n+m);

  genLN:=[AnyRepresentative(Numerator(genL[i])): i in [1..#genL]];
  genLD:=[AnyRepresentative(Denominator(genL[i])): i in [1..#genL]];

  phi:=hom<KX->KWZT | [KWZT.(1+i): i in [1..n]]>;
  d:=&*genLN;
  HI:=ideal<KWZT | [KWZT.1*phi(d)-1] cat
    [KWZT.(1+n+i)*phi(genLD[i])-phi(genLN[i]): i in [1..m]] cat
    [phi(g): g in Basis(I)]>;
  J:=EliminationIdeal(HI,{KWZT.i: i in [2..1+n+m]});
```

```
  delete genLN;
  delete genLD;
  delete d;
  delete phi;

  if KZT cmpeq 1 then
    KZT:=PolynomialRing(CoefficientRing(KX),n+m);
  end if;

  phi:=hom<KWZT->KZT | [KZT!0] cat [KZT.i: i in [1..n+m]]>;
  J:=ideal<KZT | [phi(g): g in Basis(J)]>;
  delete phi;

  S:=EliminationIdeal(HI,{KWZT.i: i in [1+n+1..1+n+m]});

  if KT cmpeq 1 then
    KT:=PolynomialRing(CoefficientRing(KX),m);
  end if;

  phi:=hom<KWZT->KT | [KT!0] cat [KT!0: i in [1..n]] cat
  [KT.i: i in [1..m]]>;
  S:=ideal<KT | [phi(g): g in Basis(S)]>;
  delete phi;

  return J,S;

end function;



/*

FUNCTION MembershipSubRationalFieldTaggedVersion

Let K be a field, X_1, ..., X_n be indeterminates over K and I a
prime ideal of K[X_1, ..., X_n]. Let genL be a list of elements of
Quot(K[X_1, ..., X_n]/I) and f be an element of
Quot(K[X_1, ..., X_n]/I).

The function MembershipSubRationalFieldTaggedVersion checks, whether
f lies in the subfield of Quot(K[X_1, ..., X_n]/I) generated by genL.
If this is the case, then a representation of f (as a rational
function) in the generators genL is computed.
```

```
Input f:
- f: an element of Quot(K[X_1, ..., X_n]/I).

and as parameters EITHER (KX,I,L)
- KX: a polynomial ring over K.
- I: a prime ideal of KX.
- genL: a list of elements of Quot(KX/I).

OR (J,S)
- J: the tagged MQS ideal of X_1+I, ..., X_n+I over K(genL).
- S: the relation ideal of the elements of genL over K.

In the first case, when (KX,I,L) is set, the function computes (J,S)
via the MQSIdealTaggedVersion function. If
MembershipSubRationalFieldTaggedVersion has to be applied to several
elements f, then it should be invoked with the parameters (J,S), as
otherwise these have to be computed each time again.


Output (b,r,S):
- b: a boolean value indicating, whether f is contained in K(genL)
     or not.
- r: in case b equals true, a rational function contained in
     K(T_1, ..., T_m) (m the number of elements in genL), such that
     f=b(genL[1], ..., genL[m]), 0 otherwise
- S: the relation ideal of the elements of genL over K (see also
     MQSIdealTaggedVersion).

*/


MembershipSubRationalFieldTaggedVersion:=function(f: KX:=1,I:=1,
genL:=1,J:=1,S:=1)

  if (J cmpeq 1 or S cmpeq 1) then
    if (KX cmpeq 1 or I cmpeq 1 or genL cmpeq 1) then
      error "(KX,I,L) or (J,S) must be defined.";
    end if;
    m:=#genL;
    n:=Rank(KX);
    J,S:=MQSIdealTaggedVersion(KX,I,genL);
  else
    m:=Rank(Generic(S));
    n:=Rank(Generic(J))-m;
  end if;
```

```
  KT:=Generic(S);
  KZT:=Generic(J);

  KftZ:=PolynomialRing(FieldOfFractions(KT/S),n);

  phi:=hom<KZT->KftZ | [KftZ.i: i in [1..n]] cat
    [CoefficientRing(KftZ).i: i in [1..m]]>;

  JS:=ideal<KftZ | [phi(g): g in Basis(J)]>;
  delete phi;

  phi:=hom<KX->KftZ | [KftZ.i: i in [1..n]]>;

  N:=NormalForm(phi(AnyRepresentative(Numerator(f))),JS);
  D:=NormalForm(phi(AnyRepresentative(Denominator(f))),JS);

  delete phi;

  KfT:=FieldOfFractions(KT);

  if (N-(LeadingCoefficient(N)/LeadingCoefficient(D))*D ne 0) then
    return false,KfT!0,S;
  else
    r:=LeadingCoefficient(N)/LeadingCoefficient(D);
    return true,
      (KfT!AnyRepresentative(Numerator(r)))/(KfT!AnyRepresentative
      (Denominator(r))),S;
  end if;

end function;



/*

FUNCTION IdealRestriction

Let K be a field, X_1, ..., X_n be indeterminates over K and I a
prime ideal of K[X_1, ..., X_n]. Let genL be a list of elements of
Quot(K[X_1, ..., X_n]/I). Let furthermore genJ be a list of elements
of Quot(K[X_1, ..., X_n]/I)[Z_1, ..., Z_l].

The function IdealRestriction computes generators of the intersection
of the ideal (genJ) (in Quot(K[X_1, ..., X_n]/I)[Z_1, ..., Z_l]) with
```

```
K(genL)[Z_1, ..., Z_l].
("IdealRestriction" since the coefficients of the polynomials in the
ideal (genJ) are restricted to K(genL).)

Input (KX,I,genL,genJ):
- KX: a polynomial ring over K.
- I: a prime ideal of KX.
- genL: a list of elements of Quot(KX/I).
- genJ: a list of elements of Quot(KX/I)[Z_1, ..., Z_l].


Output (genJRes):
- genJRes: a list of elements of Quot(KX/I)[Z_1, ..., Z_l]. These
           elements generate the intersection of the ideal (genL)
           with K(genL)[Z_1, ..., Z_l] regarded as an ideal in
           K(genL)[Z_1, ..., Z_l]. In particular, all coefficients
           of the elements of genJRes lie in K(genL).

*/


IdealRestriction:=function(KX,I,genL,genJ)

  if (genJ eq []) then
    return genJ;
  end if;

  m:=#genL;
  n:=Rank(Generic(I));
  l:=Rank(Parent(genJ[1]));

  JQ,S:=MQSIdealTaggedVersion(KX,I,genL);
  L:=FieldOfFractions(Generic(S)/S);

/*
  Since S is the relation ideal of genL, the field L is a field
  isomorphic to K(genL). L is used in the sequel to calculate within
  K(genL). By construction, all elements of K(genL) are represented
  in L as rational functions in the elements of genL.
*/

  LXZ:=PolynomialRing(L,n+l);

  phi:=hom<Generic(JQ)->LXZ | [LXZ.i: i in [1..n]] cat
    [CoefficientRing(LXZ).i: i in [1..m]]>;
```

```
genJQS:=[phi(g): g in Basis(JQ)];
delete phi;

KXZ:=PolynomialRing(CoefficientRing(KX),n+l);
KfxZ:=Parent(genJ[1]);

phi:=hom<KX->KXZ | [KXZ.i: i in [1..n]]>;
Kxz := KXZ/ideal<KXZ | [phi(g): g in Basis(I)]>;
delete phi;

Kfxz:=FieldOfFractions(Kxz);

phi:=hom<KfxZ->Kfxz | hom<CoefficientRing(KfxZ)->Kfxz |
  [Kfxz.i: i in [1..n]]>, [Kfxz.(n+i): i in [1..l]]>;
genJ:=[phi(g): g in genJ];
delete phi;

genJ:=[AnyRepresentative(Kxz!Numerator(g)): g in genJ];

phi:=hom<KXZ->LXZ | [LXZ.i: i in [1..n+l]]>;
H:=ideal<LXZ | [phi(g): g in genJ] cat genJQS>;
delete phi;

PD:=PrimaryDecomposition(H);

LX:=PolynomialRing(L,n);

phi:=hom<Generic(JQ)->LX | [LX.i: i in [1..n]] cat
  [CoefficientRing(LX).i: i in [1..m]]>;
JQSS:=ideal<LX | [phi(g): g in Basis(JQ)]>;

delete phi;

phi:=hom<LXZ->LX | [LX.i: i in [1..n]] cat [0: i in [1..l]]>;
ResI:=ideal<LXZ|1>;
for j in [1..#PD] do
  if (ideal<LX | [phi(g): g in Basis(EliminationIdeal(PD[j],
    SequenceToSet([LXZ.i: i in [1..n]])))]> subset JQSS) then
    ResI:=ResI meet PD[j];
  end if;
end for;

delete phi;
delete PD;
delete H;
```

```
  ResI:=EliminationIdeal(ResI, SequenceToSet([LXZ.(n+i): i in [1..l]]));

  phi:=hom<LXZ->KfxZ | hom<CoefficientRing(LXZ)->KfxZ | genL>,
    [0: i in [1..n]] cat [KfxZ.i: i in [1..l]]>;

  return [phi(g): g in Basis(ResI)];

end function;



/*

FUNCTION FieldIntersection

Let K be a field of characteristic zero, X_1, ..., X_n be
indeterminates over K and I be a prime ideal of K[X_1, ..., X_n].
Let genL1, genL2 be lists of elements of Quot(K[X_1, ..., X_n]/I),
such that K(genL1) and K(genL2) are algebraically closed in
Quot(K[X_1, ..., X_n]/I).

The function FieldIntersection computes generators of the
intersection of the fields K(genL1) and K(genL2).

Input (KX,I,genL1,genL2):
- KX: a polynomial ring over K.
- I: a prime ideal of KX.
- genL1: a list of elements of Quot(KX/I).
- genL2: a list of elements of Quot(KX/I).


Output (genLRes):
- genLRes: generators of the MQS ideal of X_1+I, ..., X_n+I over the
           intersection of the fields K(genL1) and K(genL2). This
           ideal lives in Quot(K(X_1, ..., X_n)/I)[Z_1, ..., Z_n].
           In particular, the coefficients of these generators
           generate the intersection of the fields K(genL1) and
           K(genL2).

*/


FieldIntersection:=function(KX,I,genL1,genL2)
```

```
  n:=Rank(KX);

  KfxZ:=PolynomialRing(FieldOfFractions(KX/I),n);

  J1:=Basis(MQSIdeal(KX,I,genL1: KfxZ:=KfxZ));
  J2:=[1];

  while (ideal<KfxZ | [g: g in J1]> ne ideal<KfxZ | [g: g in J2]>) do

    J2:=IdealRestriction(KX,I,genL2,J1);
    J1:=IdealRestriction(KX,I,genL1,J2);

  end while;

  return J1;

end function;
```

Bibliography

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BK05] Mireille Boutin and Gregor Kemper. On reconstructing configurations of points in $\mathbb{P}^2$ from a joint distribution of invariants. *Appl. Algebra Engrg. Comm. Comput.*, 15(6):361–391, 2005.

[BMQS06] Thomas Beth, Jörn Müller-Quade, and Rainer Steinwandt. Computing restrictions of ideals in finitely generated k-algebras by means of Buchberger's algorithm. *J. Symbolic Comput.*, 41(3-4):372–380, 2006.

[Buc65] Bruno Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. *Dissertation*, 1965.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[CLO07] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[DF99] Daniel Daigle and Gene Freudenburg. A counterexample to Hilbert's fourteenth problem in dimension 5. *J. Algebra*, 221(2):528–535, 1999.

[DK02] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[Fau93] Olivier Faugeras. *Three-dimensional computer vision: a geometric viewpoint*. MIT Press, Cambridge, MA, USA, 1993.

[FO01] Mark Fels and Peter J. Olver. Moving frames and coframes. In *Algebraic methods in physics (Montréal, QC, 1997)*, CRM Ser. Math. Phys., pages 47–64. Springer, New York, 2001.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, 1977. Graduate Texts in Mathematics, No. 52.

[HK07] Evelyne Hubert and Irina A. Kogan. Rational invariants of a group action. Construction and rewriting. *J. Symbolic Comput.*, 42(1-2):203–217, 2007.

[Hum75] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[Hup67] Bertram Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[Igu51] Jun-ichi Igusa. On a theorem of Lueroth. *Mem. Coll. Sci. Univ. Kyoto Ser. A. Math.*, 26:251–253, 1951.

[Kem93] Gregor Kemper. An algorithm to determine properties of field extensions lying over a ground field. *Preprint, IWR, Heidelberg*, 58, 1993.

[Kem07] Gregor Kemper. The computation of invariant fields and a constructive version of a theorem by Rosenlicht. *Transform. Groups*, 12(4):657–670, 2007.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[MFK94] David Mumford, John Fogarty, and Frances Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]*. Springer-Verlag, Berlin, third edition, 1994.

[MQS99] Jörn Müller-Quade and Rainer Steinwandt. Basic algorithms for rational function fields. *J. Symbolic Comput.*, 27(2):143–170, 1999.

[MQS00a] Jörn Müller-Quade and Rainer Steinwandt. Gröbner bases applied to finitely generated field extensions. *J. Symbolic Comput.*, 30(4):469–490, 2000.

[MQS00b] Jörn Müller-Quade and Rainer Steinwandt. Recognizing simple subextensions of purely transcendental field extensions. *Appl. Algebra Engrg. Comm. Comput.*, 11(1):35–41, 2000.

[Pop94] Vladimir Popov. Sections in invariant theory. In *The Sophus Lie Memorial Conference (Oslo, 1992)*, pages 315–361. Scand. Univ. Press, Oslo, 1994.

[Ros63] Maxwell Rosenlicht. A remark on quotient spaces. *An. Acad. Brasil. Ci.*, 35:487–489, 1963.

[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.

[SMQ00] Rainer Steinwandt and Jörn Müller-Quade. Freeness, linear disjointness, and implicitization—a classical approach. *Beiträge Algebra Geom.*, 41(1):57–66, 2000.

[Swe93] Moss Sweedler. Using Groebner bases to determine the algebraic and transcendental nature of field extensions: return of the killer tag variables. In *Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993)*, volume 673 of *Lecture Notes in Comput. Sci.*, pages 66–75. Springer, Berlin, 1993.

[ZS75a] Oscar Zariski and Pierre Samuel. *Commutative algebra. Vol. 1.* Springer-Verlag, New York, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.

[ZS75b] Oscar Zariski and Pierre Samuel. *Commutative algebra. Vol. II.* Springer-Verlag, New York, 1975. Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

Index

Notation

$\emptyset$	the empty set
$\mathbb{N}, \mathbb{N}_0$	the set of natural numbers (excluding resp. including 0)
$\mathbb{Z}$	the set of integers
$\mathbb{Q}$	the field of rational numbers

1_G, 96
$\langle \cdot, \cdot \rangle$, 11
$\mathbb{A}^n$, 58
$\mathbb{A}^n_K$, 58
$(\cdot)_{\mathfrak{B}}$, 8
$[d_1, \ldots, d_{m+1}]$, 104
$\deg(p(y))$, 31
$\delta_{-,-}$, 105
$\det(X_{i,j})_{i,j=0,\ldots,m}$, 95
$\mathrm{diag}(\lambda_1, \ldots, \lambda_{m+1})$, 105
$\dim(I)$, 21
$\mathrm{Gal}(K(x_1, \ldots, x_n)|L)$, 17
$\gcd_{L'[Y_i]}(q_i(Y_i), q_i'(Y_i))$, 32
$\mathrm{GL}_{n+1}(\mathbb{R})$, 6
I_3, 13
$\mathrm{Id}^+(X)$, 59
$\mathrm{Id}(X)$, 58
id_X, 65
I_T^h, 61
$I : J$, 23
$I : J^\infty$, 24
$I : q$, 24
$I : q^\infty$, 24
$J^{\underline{x}}_L$, 22
$J^{\underline{x}}_{L_1} \vee J^{\underline{x}}_{L_2}$, 29
$J^{\underline{x}}_{L_1} \wedge J^{\underline{x}}_{L_2}$, 29
$\overline{K'}$, 32
$K^\times$, 94
$K(X)$, 62
$K[X]$, 59
$K(x_1, \ldots, x_n)$, 17
$K(x_1, \ldots, x_n)|L$, 17
$K(X)^G$, 97
$K(x_1, \ldots, x_n)[Z_1, \ldots, Z_n]$, 22
$\mathrm{LC}_{\leq}(\mathbf{p}(\underline{\mathbf{X}}))$, 19
$\mathrm{LM}_{\leq}(\mathbf{p}(\underline{\mathbf{X}}))$, 19
$\mathrm{NF}_{\mathcal{G}}(\mathbf{p}(\underline{\mathbf{X}}))$, 20
$(p_1(\underline{Z}), \ldots, p_s(\underline{Z}))_{K(x_1,\ldots,x_n)[Z_1,\ldots,Z_n]}$, 22
p. d., 104
PGL_{n+1}, 7
$\mathrm{PGL}_{n+1}(\mathbb{R})$, 7
ϕ^*, 67
$\mathbb{P}^n$, 58
$\mathbb{P}^n_K$, 58
$\mathbb{P}^n_{\mathbb{R}}$, 6
$\mathrm{Quot}(\cdot)$, 27
$\mathbb{R}$, 6
$\mathbb{R}^n$, 6
$\mathbb{R}^\times$, 6
SL_3, 13
SO_n, 10
$\mathrm{S}_{\{d_1,\ldots,d_{m-1}\}}$, 114
S_n, 14
$\mathrm{trdeg}_L(K(x_1, \ldots, x_n))$, 27
$\underline{X}$, 18
$\underline{x}$, 18
$\underline{X}^\alpha$, 18
$(\xi_1 : \ldots : \xi_{n+1})$, 6
$\overline{X}$, 59
$\underline{Z}$, 18
$\mathrm{Z}(I)$, 58
$\mathrm{Z}^+(I)$, 59