Bachelor's thesis

The Shephard–Todd–Chevalley–Serre Theorem

Torben Bürger

September 2024

Supervisor: Prof. U. Thiel

RPTU Kaiserslautern-Landau

Department of mathematics

Declaration

I, Torben Bürger, avouch that I have created this thesis titled 'The Shephard–Todd–Chevalley–Serre Theorem' on my own and without help or sources but those explicitly mentioned and that I have marked any and all citations as such.

Kaiserslautern, September 2024

Torben Bürger

Contents

Chapter 1. Introduction 1
1. A brief overview of the subjects and results 1
2. Prerequisites 1
3. General assumptions 2
4. The history of the main theorem and its provenance 2

Chapter 2. The affine orbit variety 5
1. Affine algebraic varieties and the equivalence of geometry and algebra 5
2. Important notions and results from commutative algebra 11
3. Quotients of topological spaces and varieties 11
4. Basics of multilinear algebra 16
5. The algebra of polynomial invariants 21
6. The orbit space V/G as affine variety 29

Chapter 3. The Shephard-Todd-Chevalley-Serre Theorem 35
1. Key facts about unitary reflection groups 35
2. The main theorem 39
3. Chevalley's lemma and the proof of (a) $\Rightarrow$ (b) 39
4. The proof of (b) $\Rightarrow$ (a) using Molien's formula 43
5. The proof of (b) $\Leftrightarrow$ (c) 50
6. Computations of concrete generators for the algebra of invariants 60

Chapter 4. Outlook 65

Bibliography 67

CHAPTER 1

Introduction

1. A brief overview of the subjects and results

In this thesis, the main talking point is the *Shephard–Todd–Chevalley–Serre Theorem*. However, we will not only show the classical equivalence of $G \leq GL(V)$ being a unitary reflection group and the corresponding algebra of invariant polynomial functions on the n-dimensional vector space V denoted by $S^G := \{P \in S \mid gP = P \text{ for all } g \in G\}$ being a polynomial algebra, but we will also give a link to algebraic geometry. This will be achieved by the third equivalent statement: the orbit space $\mathbb{C}^n/G$ is a smooth variety. Note that we identified the n-dimensional complex vector space V with $\mathbb{C}^n$ in this case.

The precise formulation is as follows:

Theorem 1.1 (Shephard–Todd–Chevalley–Serre)**.** *Let V be a finite dimensional vector space over the complex numbers $\mathbb{C}$ and let G be a finite subgroup of the general linear group $GL(V)$. Then the following are equivalent:*

(a) The group G is a unitary reflection group.
(b) The algebra of G-invariant polynomials $S^G := \mathbb{C}[V]^G$ is a polynomial algebra.
(c) The orbit space V/G is a smooth variety.

After this introduction whose biggest component is the history of the origins of the main theorem, the second chapter 2 will treat the *affine orbit variety*. We will investigate the orbit space $\mathbb{C}^n/G$ which is at first equipped with the Euclidean topology and due to the topological definition, it is the set of orbits. Then, the main result is that this space is homeomorphic to the at this point introduced *affine orbit variety* which is even a quotient space with respect to the Zariski topology. Subsequently, the third chapter 3 is dedicated to the main theorem in several steps, and to the mathematical tools from various mathematical branches required to prove it.

2. Prerequisites

This work shall be accessible to advanced undergraduate students after visiting several introductory lectures to algebra. Sometimes, we will use advanced results, in particular from commutative algebra, for these the books of Lang [**36**] as well as Atiyah–Macdonald [**1**] are recommendable general references. Moreover, we assume that the reader is familiar with fundamental category theory as we will use the basic objects like categories, functors, and morphisms without introducing them beforehand. A brief introduction to this topic is given by Lang [**36**, Chapter 1, §11] or Eisenbud [**19**, Appendix 5]. Even though it can be helpful, no prior knowledge in algebraic geometry or homological algebra is presumed. When results or concepts from these topics are useful or necessary, they will be introduced beforehand.

3. General assumptions

When we speak about a ring R in this work, we assume that is has a unit element 1 with respect to the multiplication, and that it is commutative. Therefore, we will simply use the term of an R-module and not differentiate between right- and left-modules. Moreover, any vector space is supposed to be of finite dimension, usually denoted by n.

4. The history of the main theorem and its provenance

4.1. The Shephard–Todd-classification and its consequences. The history of the main theorem 1.1 begins with the equivalence of (a) and (b) which is also known as the *Shephard-Todd theorem*. It was originally shown in a paper of Shephard and Todd [**57**] and published in 1954. L. Smith [**60**, p. 177] describes their course of action as follows: to obtain the proof, they used their classification of all irreducible reflection groups—which is also achieved in this paper—to compute all the examples of generators for all unitary reflection groups. They only classified all the irreducible ones but this already suffices to treat this matter, since every unitary reflection group can be decomposed into irreducible parts. For a sophisticated treatment of this decomposition see Flatto [**21**, Chapter II, Section 4].

At the time of publication of the paper from Shephard and Todd, the concept of reflections on a unitary space had only recently been established by Shephard [**56**]. Previously, orthogonal reflections on a euclidean space were commonly considered. Until then, a sizable study on this type of reflections was available, Coxeter made a particularly large contribution to this (cf. Shephard-Todd [**57**, p. 274]). As unitary reflections are an extension of real orthogonal reflections, it is not surprising that they behave similarly, and that there are various analogues or extensions of the real case (cf. Coxeter [**16**] and Shephard–Todd [**57**, p. 275]). For the classification, the authors were "able to draw on the considerable literature which exist[ed] on collineation groups generated by homologies" (Shephard–Todd [**57**, p. 275]) for the so-called *primitive* unitary reflection groups. For the other type, the *imprimitive* ones, the generators were "determined without difficulty" (loc. cit.). Kane [**32**, §15] provides a clear overview of the classification and the methods to achieve it. Another approach to attain this classification is presented by Cohen in [**13**].

The second part of the aforementioned paper of Shepard and Todd [**57**] is devoted to prove some properties of unitary reflection groups by using the classification. Its application leads to the equivalence of (a) and (b). Their proof heavily depends on the classification and thus, as previously mentioned, draws from existing literature on collineation groups. This is why I believe that the following quote points out accurately how many known results were gathered to be able to prove the said equivalence: "The theorem of G. C. Shephard and J. A. Todd on the invariants of complex pseudoreflection groups culminated a century of work on these groups and their classification." (Neusel–Smith [**45**, p. 185]).

The original proof of the implication (a) $\Rightarrow$ (b) is only given for the unitary reflection groups not equivalent to any real orthogonal group as Coxeter had already proven it for them in [**15**]. For the remaining groups, the generating invariants were gained either by explicitly constructing them, or based on knowledge about related collineation groups (cf. Shephard–Todd [**57**, p. 283]). To be precise, there is an additional intermediate step, demonstrating that the degrees of the generators are unique and indicating their connection to $|G|$. For the converse (b) $\Rightarrow$ (a) the classification was not necessary and the proof worked without any case distinctions. It used the concept of *Poincaré series* and an until then already over 50 year old theorem of Molien [**43**]. However, it remained

quite computational, although the first implication using the classification was even more enumerative. This explains why Benson describes that proof in a, in my opinion, very suitable way as a "tour de force of combinatorics and geometry" ([**3**, p. viii]).

4.2. Chevalley's lemma and Serre's remark. For the implication (a) ⇒ (b) there is a uniform proof that does not need the classification. At first, only the statement was published in a paper from Chevalley [**11**] for the International Congress of Mathematicians in 1950. However, this statement was just for the case of real orthogonal reflections (cf. Lehrer–Taylor [**37**, p. 47]). As this precedes the publication of the extension of reflections onto unitary spaces by Shephard [**56**], the orthogonal reflections were the only existing reflections at the time.

A full proof of this statement by Chevalley was published in 1955 [**12**]. It does not use the classification established by Shephard-Todd but it is still "heavily computational" (L. Smith [**60**, p. 205]) and "involve[s] the combinatorics of differential operators" (Benson [**3**, p. viii]). Moreover, L. Smith even refers to the proof as "unmotivated" ([**60**, p. 205]), which is rather harsh to my mind, since it remains the first case-free proof for this implication, even though it is computational and technical. On the other hand, instead of using Chevalley's proof, L. Smith gives his own proof [**59**] that relies heavily on homological machinery. Moreover, Chevalley's statement was at first proven in an unpublished manuscript (cf. Borel [**4**, p. 154 footnote 5]) and was initially mentioned by Chevalley in 1950 [**11**] predating the Shephard–Todd theorem. This may be an explanation why the paper does not include any connection to the Shephard–Todd theorem.

The lack of motivation might be explained by the history of the origins of this paper that is presented by Borel [**4**, p. 154 footnote 5]. Even though the paper was published under Chevalley's name, it was in fact published by Borel. This came about as follows: the proof was already finished in all details in a manuscript by Chevalley, however this "manuscript did not have all the trimmings of a full-fledged paper" (Borel [**4**, p. 154 footnote 5]), in other words, some adaptions would have been necessary to publish it. Since Borel wanted to quote the proof from Chevalley's manuscript, he tried unsuccessfully to convince Chevalley to publish it as an independent paper. On the other hand, Chevalley handed the manuscript to Borel with the words " 'Fais-en ce que tu veux' "[1](loc. cit.). This was cleverly interpreted by Borel as a permission to adapt and publish the manuscript as a paper. According to Borel, Chevalley did notice the publication and was briefly taken back, but he quickly understood what had happened and paid no further attention (cf. Borel [**4**, p. 154 footnote 5]). This is how the proof of Chevalley found its way to the public, and had a much larger impact than just being an auxiliary result in a paper by Borel.

As mentioned before, this proof initially considered only real reflections. However, in [**53**], Serre later pointed out that this proof was not only applicable in the complex case, but that it even "was adequate to handle the nonmodular case" (Neusel–Smith [**45**, p. 187]). This is only relevant if the base field is different from $\mathbb{C}$ which we excluded as a general assumption in this work, yet it demonstrates how powerful this proof is. So, this way to prove the implication is completed by Serre's remark.

Finally, we observe that these preceding two subsections already justify the inclusion of all four names of those influential mathematicians in the title of this work and the main theorem. Note that their surnames are not ordered alphabetically, which is slightly uncommon. This has the purpose to highlight that Shephard and Todd already completed

[1]The quote can be translated to: "Do with it whatever you want".

the proof while Chevalley and Serre improved the way to show one implication. On the other hand, Serre will take on the leading role in the next subsection.

4.3. Serre's homological link between algebraic geometry and invariant theory. In order to prove the last equivalence (b) $\Leftrightarrow$ (c) nearly all the work has to be put into demonstrating that (c) $\Rightarrow$ (b) whilst the other implication is almost trivial.

There is no complete of the proof given for the mentioned advanced implication, but we can look at the single steps taken on the way to prove it. The first step is a short excursion to algebraic geometry by using the fact that smooth varieties afford regular coordinate rings.

The biggest part in the proof of (c) $\Rightarrow$ (b) is an equivalence first given by Serre [**52**] on a conference in 1955. There, he showed that a local Noetherian ring is regular if and only if its global dimension is finite (cf. Serre [**52**, Théorème 3]). Since the implication that a local regular ring is of finite global dimension was shown before by Auslander and Buchsbaum [**2**], "[t]he main original result of this paper is that a local ring of finite global dimension is regular" (Buchsbaum [**9**, p. 439]). In order to prove this, a large toolkit of homological algebra was applied, namely the concepts of *Koszul complexes* and *minimal resolutions* are necessary (cf. Matsumura [**40**, p. 140]). On the path of the original proof a theorem and multiple lemmas are proven as intermediate results. I find it remarkable that the proof relies very little on existing literature, the only quoted result is a characterization of regular rings.

At this point it is important to note that we only need the implication of Auslander–Buchsbaum directly and will therefore exclusively present a proof for this part of the equivalence. However, Serre's converse will be hidden in a proof of a theorem whose result we will just cite. Moreover, it is an interesting characterization of properties whose relation is not apparent at first glance.

To complete the proof of (c) $\Rightarrow$ (b) we make use of a theorem from Serre [**55**, Chapter IV, Appendix III, Theorem 1]. It asserts that for a connected graded algebra over a field, being regular and being isomorphic to a polynomial algebra are equivalent. However, the origin of this theorem remains unclear. To begin with, the mentioned book is based on a lecture given by Serre in 1957 and 1958, and was at first published as a french edition [**54**] in which the appendix including the theorem stated above is missing. This was only added in the english edition [**55**] from the year 2000. Moreover, in the preface, the addition of this appendix is just mentioned (cf. [**55**, p. v]), but there is no explanation whether this result was already given in the original lecture or only attached later on.

Nevertheless, this equivalence must have been known before as, for example, a very similar statement was provided as an exercise in a book from Bruns and Herzog [**8**, Exercise 2.2.25] that was originally published in 1993. Another indication that this result was already known before can be found in Serre's earlier mentioned paper [**53**] from 1967, where a part of the equivalence is stated as lemma. Specifically, it is asserted that for a graded algebra R over a field, the localized ring R_m is regular if and only R is a so-called *graded-polynomial* algebra. However, this is not the whole set of equivalent characterizations in Serre's book [**55**]. Since neither a proof nor a reference to its origin is provided in Serre's 1967 paper, it remains unclear whether this was a new result at the time or a well-known fact. Hence, this chapter on the history of the main theorem has to end with this unsatisfying result.

CHAPTER 2

The affine orbit variety

In this first part of the work, we will discuss the affine orbit variety. That is, the orbit space—from which we will show that it can be viewed as variety—of the group action of a, in our case, finite subgroup G of the general linear group $GL(V)$ for some finite-dimensional vector space V over $\mathbb{C}$. So, we have $V \cong \mathbb{C}^n$ and will hence identify V with $\mathbb{C}^n$. In order to treat this object we need a basis of algebraic geometry and invariant theory. First, we give some fundamental definitions of algebraic geometry and will present the relations between algebra and geometry. Next, there will be a section on quotients to provide a further understanding of the quotient space $\mathbb{C}^n/G$ and quotients of varieties. Subsequently, we will define the algebra of invariant polynomials S^G. To study this subject, we will recall some important definitions and results of ring theory as well commutative algebra. Aiming at a rigorous definition of the algebra of invariants S^G, we first establish the symmetric algebra, and give an exposition of basic facts from multilinear algebra.

Subsequently, there will be a part on invariant theory treating some properties of the algebra of invariants accompanied by an interlude on the historical development of this branch of mathematics. In particular, it will be shown that S^G is a finitely generated algebra in case that the group G is finite. Furthermore, if it is additionally non-modular, S^G is a Cohen-Macaulay ring. Finally, the main result of this section will be presented. Following Lamotke [**35**, Chapter II, §9], we will show that the orbit space $\mathbb{C}^n/G$ is homeomorphic to the so-called *affine orbit variety* which depends on the generators of S^G and that it is thus also a quotient of varieties.

1. Affine algebraic varieties and the equivalence of geometry and algebra

The aim of this first section is to create an overview of the geometric objects, their algebraic counterparts, and the interrelations between these two classes. For this purpose, most of the time, we will adhere closely to the first two chapters of K. Smith et al. [**58**], providing a well-understood introduction to algebraic geometry.

1.1. The geometric objects. First, we determine all objects to be considered in a finite-dimensional vector space over the complex numbers $\mathbb{C}$. Later on, it will emerge that it is useful to choose an infinite, algebraically closed field with characteristic zero. However, one can also study algebraic geometry over other fields, e. g., finite fields or the p-adic numbers. The first foundational object defined below is the *affine algebraic variety.*

Definition 2.1. An *affine algebraic variety* V is the common zero locus of a collection of polynomials with complex coefficients $\{f_i\}_{i\in I}$, where I is an arbitrary, possibly even uncountable, index set. That is,

$$V = \mathbb{V}\left(\{f_i\}_{i\in I}\right) = \{x \in \mathbb{C}^n \mid \forall i \in I\colon f_i(x) = 0\} \subseteq \mathbb{C}^n.$$

If $W \subseteq \mathbb{C}^n$ is an affine algebraic variety and W is contained in V, we call W a subvariety of V.

For example, in $\mathbb{C}^3$ the x_1x_2-plane can be expressed as the variety $\mathbb{V}(x_3)$. Furthermore, the whole affine space $\mathbb{C}^n = \mathbb{V}(\varnothing)$ and the empty set $\varnothing = \mathbb{V}(1)$ are trivial examples for affine algebraic varieties.

Next up, we will present the *Zariski topology* $\mathcal{Z}$ on $\mathbb{C}^n$, in which the open sets are defined to be the complements of affine algebraic varieties. The axioms of a topology are fulfilled as

$$\mathbb{V}\left(\{f_i\}_{i\in I}\right) \cap \mathbb{V}\left(\{f_j\}_{j\in J}\right) = \mathbb{V}\left(\{f_i\}_{i\in I\cup J}\right),$$

which remains true for arbitrary intersections. Moreover, the whole space $\mathbb{C}^n$ as well as the empty set are open as they correspond to the trivial varieties. Finally,

$$\mathbb{V}\left(\{f_i\}_{i\in I}\right) \cup \mathbb{V}\left(\{f_j\}_{j\in J}\right) = \mathbb{V}\left(\{f_if_j\}_{(i,j)\in I\times J}\right).$$

Thus, $\mathbb{C}^n$ equipped with the Zariski topology $\mathcal{Z}$ becomes a topological space. This space is denoted by $\mathbb{A}^n$ and is called the *affine n-space*, where affine means that it cannot "see" any origin, i.e., there is no special point defined as the origin and there is neither an addition of points nor a scalar multiplication.

As usually in algebra when there is a structure, it is intuitive ask for mappings which preserve this structure. Below, we will define *morphisms of affine algebraic varieties*.

Definition 2.2. A *polynomial map* between the affine spaces $\mathbb{A}^n$ and $\mathbb{A}^m$ is a map

$$\begin{aligned} F\colon \mathbb{A}^n &\longrightarrow \mathbb{A}^m \\ x &\longmapsto (F_1(x), \dots, F_m(x)), \end{aligned}$$

where all components F_i are complex polynomials in n variables. Moreover, a map F from $V \subseteq \mathbb{A}^n$ into $W \subseteq \mathbb{A}^m$ is called a *morphism of affine algebraic varieties* if it is the restriction of a polynomial map $F_P\colon \mathbb{A}^n \to \mathbb{A}^m$. The morphism F is called an *isomorphism*, if it is bijective and its inverse is a morphism, too.

Example 2.3. An easy example for a morphism is the projection map. For $n \geq m$ we have

$$\begin{aligned} \pi\colon \mathbb{A}^n &\longrightarrow \mathbb{A}^m \\ (x_1, \dots, x_m, \dots, x_n) &\longmapsto (x_1, \dots, x_m). \end{aligned}$$

The final property that we will define is the *dimension* of a an affine algebraic variety. Afterwards, in Lemma 2.11, we will see a connection to the Krull dimension of a certain ring. Before introducing the dimension, we have to define another property of affine varieties, the *irreducibility*.

Definition 2.4. An affine algebraic variety V is said to be *irreducible* if there exist no proper non-empty subvarieties $V_1 \subsetneq V$ and $V_2 \subsetneq V$, such that $V = V_1 \cup V_2$.

Definition 2.5. The *dimension* of an algebraic variety is the length d of the longest possible chain of properly contained irreducible subvarieties in V,

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_d.$$

Intuitively, one would assume that the dimension $\dim(\mathbb{A}^n)$ of the affine n-space is n, but this is not clear at first glance. However, in Lemma 2.11, we will see that this statement is in fact true.

1.2. The algebraic objects. The basic algebraic objects which will be consulted in this chapter are polynomial rings, in particular the polynomial ring with n variables over the complex numbers $\mathbb{C}[x_1, \ldots, x_n]$. For some general results of ring theory see Atiyah–Macdonald [1, Chapter 1]. Furthermore we recall, that the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ is even a $\mathbb{C}$-algebra, i.e., a ring containing $\mathbb{C}$ as a subring. It is finitely generated by $\{x_1, \ldots, x_n\}$.

For this use case, we additionally need the notion of a *reduced* ring, that is, a ring where all nilpotent elements are already zero. A quotient ring R/I is reduced if and only if the ideal I is radical (cf. Eisenbud [19, p. 36]).

An important theorem which has to be mentioned in this context is *Hilbert's basis theorem* (cf. Atiyah–Macdonald [1, Theorem 7.5]). It states that for a Noetherian ring R—that is, a ring where all ideals are finitely generated—the polynomial ring $R[x]$ is also Noetherian. In particular $\mathbb{C}[x_1, \ldots, x_n]$ is Noetherian.

1.3. The equivalence of geometry and algebra. In the following, we will create the link between geometry, represented by affine algebraic varieties, and algebra, represented by ideals of polynomial rings.

Definition 2.6. The *vanishing ideal* of an affine algebraic variety $V \subseteq \mathbb{A}^n$ is defined to be

$$\mathbb{I}(V) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(x) = 0 \text{ for all } x \in V\}.$$

It is straightforward to verify that $\mathbb{I}(\mathbb{V})$ is indeed an ideal of $\mathbb{C}[x_1, \ldots, x_n]$. By Hilbert's basis theorem this ideal is finitely generated, so let $\mathbb{I}(V) = (f_1, \ldots, f_m)$.

Lemma 2.7. *Let $V \subseteq \mathbb{A}^n$ be an affine algebraic variety. Then*

$$V = \mathbb{V}(\mathbb{I}(V)) = \mathbb{V}((f_1, \ldots, f_m)) = \mathbb{V}(f_1, \ldots, f_m),$$

where $f_1, \ldots, f_m$ denote the generators of the ideal $\mathbb{I}(\mathbb{V})$.

Proof. See K. Smith et al. [58, p. 19] □

In order to detect whether this also works for $\mathbb{I}(\mathbb{V}(I))$ with any ideal $I \trianglelefteq \mathbb{C}[x_1, \ldots, x_n]$, one has to look at *Hilbert's Nullstellensatz*. As it is nicely formulated by K. Smith et al., this "theorem is the first entry in a dictionary that will help us translate statements about geometry into the language of algebra" ([58, p. 23]).

Theorem 2.8 (Hilbert's Nullstellensatz)**.** *For an arbitrary ideal $I \trianglelefteq \mathbb{C}[x_1, \ldots, x_n]$,*

$$\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$$

Proof. See, for example, Harris [26, Theorem 5.1 and p. 57–59]. □

Thus, for radical ideals, it follows immediately that $\mathbb{I}(\mathbb{V}(I)) = I$. With the results above, this yields the bijection

$$\{\text{Affine algebraic varieties of } \mathbb{A}^n\} \longleftrightarrow \{\text{Radical ideals of } \mathbb{C}[x_1, \ldots, x_n]\}. \tag{1}$$

Note that this bijection mapping a variety V onto the ideal $\mathbb{I}(V)$, which is clearly radical, and conversely a radical ideal I onto the variety $\mathbb{V}(I)$ is order-reversing. So, if $W \subseteq V$ is a subvariety, we get $\mathbb{I}(W) \supseteq \mathbb{I}(V)$. Since an arbitrary maximal ideal of $\mathbb{C}[x_1, \ldots, x_n]$ has the form

$$\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n),$$

where $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ (cf. Matsumura [40, Corollary 14.4]) and $\mathbb{V}(\mathfrak{m}_a) = \{a\}$, the maximal ideals $\mathfrak{m}$ of the polynomial ring correspond bijectively to singletons of the affine n-space.

Hilbert's Nullstellensatz is also the reason why we only consider $\mathbb{C}$, or more generally an algebraically closed field, as base field. For example, over $\mathbb{R}$ its statement is no longer true: we have $\mathbb{V}(x^2+1) = \mathbb{V}(1)$, and one can easily verify that both ideals are radical. So, the mapping $I \mapsto \mathbb{V}(I)$ in (1) is no longer injective.

Now we will take the next step in creating our dictionary of algebra and geometry by constructing a corresponding $\mathbb{C}$-algebra to a given affine algebraic variety.

Definition 2.9. For any $V \subseteq \mathbb{A}^n$, we define the *coordinate ring* of V to be the restriction $\mathbb{C}[x_1, \ldots, x_n]|_V$. Its elements are complex polynomials in n variables restricted to the variety V. Under pointwise operations, they form a finitely generated $\mathbb{C}$-algebra as well, which will be denoted by $\mathbb{C}[V]$.

The restriction defines a natural surjective $\mathbb{C}$-algebra homomorphism

$$\mathbb{C}[x_1, \ldots, x_n] \longrightarrow \mathbb{C}[x_1, \ldots, x_n]|_V \,,$$

whose kernel is exactly $\mathbb{I}(V)$. For example, if $V = \{0\}$, the functions of $\mathbb{C}[V]$ are determined by their constant term, so $\mathbb{C}[V] \cong \mathbb{C}$. In general, we get the natural isomorphism

$$\mathbb{C}[x_1, \ldots, x_n]/\mathbb{I}(V) \cong \mathbb{C}[V].$$

This means that the equivalence classes of $\mathbb{C}[V]$ and the functions on V are in a one-to-one correspondence. Moreover, the affine algebraic variety V determines a unique $\mathbb{C}$-algebra, its coordinate ring. Additionally, we want to define a similar relation for morphims of varieties and $\mathbb{C}$-algebra homomorphisms.

Definition 2.10. For any morphism $F\colon V \to W$, the *pullback* is the induced map

$$\begin{aligned} \mathbb{C}[W] &\longrightarrow \mathbb{C}[V] \\ g &\longmapsto g \circ F, \end{aligned}$$

for a polynomial function g on W. It will often be denoted by $F^{\#}$.

This is well-defined because the composition of the polynomial map F and the polynomial function g is again a polynomial, but now on V. Furthermore, it is a simple task to check that this defines a $\mathbb{C}$-algebra homomorphism.

So, for the geometric objects, we have shown in which way they determine their unique algebraic counterparts. Next, we will present the converse direction. Given an arbitrary affine algebraic variety, the coordinate ring is a reduced (since $\mathbb{I}(V)$ is radical) and finitely generated $\mathbb{C}$-algebra. Hence, we start with a reduced finitely generated $\mathbb{C}$-algebra R. For more details see K. Smith et al. [**58**, Section 2.5], but the idea how to determine a variety, that is unique up to isomorphism, is the following: let I be the kernel of the map $\mathbb{C}[x_1, \ldots, x_n] \to R$ sending x_j onto the jth generator of R. Then, $\mathbb{V}(I)$ is an affine algebraic variety with coordinate ring isomorphic to R.

Finally, given a $\mathbb{C}$-algebra homomorphism σ between two reduced finitely generated $\mathbb{C}$-algebras R and S, one can show that σ is the pullback of a polynomial map F between the corresponding affine algebraic varieties, which is unique up to isomorphism. A version of the rather technical proof can be looked up in K. Smith et al. [**58**, Section 2.5].

The first conclusion we can draw is that two affine algebraic varieties are isomorphic if and only if their coordinate rings are isomorphic. Another conclusion will follow as an application of the following lemma.

Lemma 2.11. *Let $V \subseteq \mathbb{A}^n$ be an affine algebraic variety and let $\mathbb{C}[V]$ be its coordinate ring.*

(a) *The variety V is irreducible if and only if the ideal $\mathbb{I}(V) \trianglelefteq \mathbb{C}[x_1, \dots, x_n]$ is prime.*
(b) *The dimension of V is equal to the Krull dimension of $\mathbb{C}[V]$, in particular* $\dim(\mathbb{A}^n) = n$.

Proof. For (a) see Harris [**26**, p. 52]. Then by definition, (b) follows immediately from (a) and the fact that $\mathbb{C}[\mathbb{A}^n] = \mathbb{C}[x_1, \dots, x_n]$. □

As a last part of our dictionary between algebra and geometry, we want to elaborate how the Zariski topology can be translated. While discussing Hilbert's Nullenstellensatz we have already seen that any point of an affine algebraic variety V corresponds to a maximal ideals of the coordinate ring $\mathbb{C}[V]$. Therefore, given any Zariski closed set $W \subseteq V$, due to the order-reversing bijection in (1), we can identify W with the set of maximal ideals containing $\mathbb{I}(W)$. So, we have transported the Zariski topology onto the set of maximal ideals of $\mathbb{C}[V]$. In general, for a ring R we call this set the *maximum spectrum of* R and write $\operatorname{maxSpec}(R) = \{\mathfrak{m} \subseteq R \mid \mathfrak{m} \text{ is a maximal ideal}\}$.

This transfer of topology is compatible with $\mathbb{C}$-algebra homomorphisms as well: for finitely generated reduced $\mathbb{C}$-algebras R and S with $\sigma\colon R \to S$ we obtain the order-reversing correspondence

$$\sigma^{\#}\colon \operatorname{maxSpec}(S) \to \operatorname{maxSpec}(R), \quad \mathfrak{m} \mapsto \sigma^{-1}(\mathfrak{m}).$$

This arises from the varieties satisfying $\mathbb{C}[V] = S$ and $\mathbb{C}[W] = R$, as well as the associated morphism $F\colon V \to W$ mapping a point of V that is considered as a maximal ideal $\mathfrak{m}$ of $\operatorname{maxSpec}(S)$ onto its preimage under the pullback $(F^{\#})^{-1}(\mathfrak{m})$.

However, a possible generalization fails because for an arbitrary commutative ring R, the preimages of maximal ideals are no longer maximal. For example, consider the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$: in $\mathbb{Q}$, the ideal $\{0\}$ is maximal, but in $\mathbb{Z}$ only prime not maximal. Since the preimages of prime ideals are primes themselves, we introduce the following generalization.

Definition 2.12. For a commutative ring R, where the *spectrum* of R is denoted by $\operatorname{Spec}(R) = \{\mathfrak{p} \subseteq R \mid \mathfrak{p} \text{ is a prime ideal}\}$, we define the *Zariski closed* sets to be the sets $\mathbb{V}(I) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \supseteq \mathfrak{p}\}$ for all ideals I of R. In this way, the spectrum equipped with the Zariski topology is transformed into a topological space.

Remark 2.13. The above relation between algebra and geometry can be concluded that for a reduced finitely generated $\mathbb{C}$-algebra R, the affine variety with coordinate ring R corresponds to $\operatorname{Spec}(R)$ and is often also denoted by this expression, i.e., $\operatorname{Spec}(\mathbb{C}[V]) = V$.

This subsection is completed by the introduction of regular functions on a variety which are needed in the third section, see K. Smith et al. [**58**, Chapter 4.3] for more details.

Definition 2.14. Let V be an affine variety. We say that a complex valued function $f\colon U \to \mathbb{C}$ on an open subset $U \subseteq V$ is *regular at a point* p if there exist functions $g, h \in \mathbb{C}[V]$ such that $h(p) \neq 0$, and $f = g/h$ in some neighborhood of p. If f is regular at every point of U, f is called a *regular function* on U. For the set of all regular functions on U, we write $\mathcal{O}_V(U)$.

If V is a closed set of $\mathbb{A}^n$ with respect to the Zariski topology, then the regular functions coincide with the restriction of polynomials to V, i.e., $\mathcal{O}_V(V) = \mathbb{C}[V]$. In general, for any variety V and an arbitrary open set $U \subseteq V$, the set $\mathcal{O}_V(U)$ is even a $\mathbb{C}$-algebra.

1.4. Smooth varieties. This subsection follows K. Smith et al. [**58**, Chapter 6]. Aiming at a definition of smoothness of varieties, let $V \subseteq \mathbb{A}^n$ be an affine algebraic variety of dimension d, and let $\mathbb{I}(V) = (F_1, \dots, F_r)$ be its ideal. Moreover, consider a line

$\ell = \{(ta_1, \ldots, ta_n) \mid t \in \mathbb{C}\}$ in $\mathbb{A}^n$ trough the origin and a fixed point $q = (a_1, \ldots, a_n)$. To compute the intersection $V \cap \ell$, the solutions of $F_i\,(ta_1, \ldots, ta_n) = 0$ have to be determined for all $i = 1, \ldots, r$. This is the question for common roots of these polynomials in one variable t. As the base field is $\mathbb{C}$, they split into linear factors. The *multiplicity* of a point p in $V \cap \ell$ is the maximal power $k \in \mathbb{N}$ of the corresponding linear factor, such that it divides the polynomial $F_i\,(ta_1, \ldots, ta_n)$ for all $i = 1, \ldots, r$.

Definition 2.15. For a line $\ell \subseteq \mathbb{A}^n$, a variety V as above, and a point $p \in V$, we shall say that ℓ is *tangent* to V at p if the multiplicity at p is greater than 1. The space of all points lying on lines tangent to V at p is called the tangent space T_pV.

The aim is to characterize the tangent space using formal derivatives, starting with the introduction of the *differential*.

Definition 2.16. The *differential* $\mathrm{d}f|_p$ of a polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$ at a point $p \in \mathbb{C}^n$ is the linear part of its Taylor series expansion.

In other words, if we write $f(x) = f(p) + L(x-p) + G(x-p)$ uniquely with linear part L and G as the part of terms of degree at least 2, the differential $\mathrm{d}F|_p$ of f at p is the linear function L. This leads to

$$L(x-p) = \mathrm{d}f|_p(x-p) = \sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(p)(x_j - p_j).$$

Furthermore, it can be shown that the set of differentials of all F_i—the generators of $\mathbb{I}(V)$—generates the tangent space as variety (cf. K. Smith et al. [58, p. 89]), i. e.,

$$T_pV = \mathbb{V}\left(\mathrm{d}F_1|_p(x-p), \ldots, \mathrm{d}F_r|_p(x-p)\right) \subseteq \mathbb{A}^n.$$

Note that this way to define the tangent space is well-defined because the same theorem also tells us that the tangent space does not depend on the chosen generators $F_1, \ldots, F_r$.

Definition 2.17. For a point p on an affine algebraic variety V we say that p is a *smooth point* if $\dim(T_pV) = \dim(V)$. Otherwise p is called a *singular point*. If all points of the variety V are smooth, we say that V is a *smooth variety*.

Remark 2.18. As shown by K. Smith et al. ([58, p. 92–93]), the above formula on the differentials leads to the so-called *Jacobi-matrix* J.

$$J(x-p) = \begin{pmatrix} \frac{\partial F_1}{\partial x_1}\big|_p & \cdots & \frac{\partial F_1}{\partial x_n}\big|_p \\ \vdots & \ddots & \vdots \\ \frac{\partial F_r}{\partial x_1}\big|_p & \cdots & \frac{\partial F_r}{\partial x_n}\big|_p \end{pmatrix} \begin{pmatrix} x_1 - p_1 \\ \vdots \\ x_n - p_n \end{pmatrix}$$

is the equation whose zero set is exactly the tangent space T_pV of the variety V corresponding to the f_i at the point $p = (p_1, \ldots, p_n)$. Hence, the tangent space can be viewed as the kernel of this linear map. One can show that the rank of J is bounded upwards by $n - dim(V)$ (cf. Hartshorne [27, proof of 5.3]). Therefore, the dimension of V is a lower bound on the dimension of the tangent space. Then, for a singular point $p \in V$ we have $n - \dim(T_pV) = \mathrm{rk}(J) < n - \dim(V)$. Hence, a point $p \in V$ is a smooth point if and only if the corresponding Jacobi-matrix is of full rank, i. e., $\mathrm{rk}(J) = n - \dim(V)$. This is usually called the *Jacobi-criterion* for smoothness.

Example 2.19.

(a) A simple example for a smooth variety is the whole affine n space. In this case, $\mathbb{I}(\mathbb{A}^n) = \{0\}$ and $\dim(\mathbb{A}^n) = n$. So, $J = (0, \ldots, 0)$ with $\mathrm{rk}(J) = 0 = n - n$.

(b) An example for a singular point is the origin of the so-called cusp $\mathbb{V}\left(y^2 - x^3\right) \subseteq \mathbb{A}^2$. We only have $F_1 = y^2 - x^3$ and therefore $J = \left(-3x^2, 2y\right)$ whence $J(0) = 0$ which is not of rank 1. However, every other point is smooth.

2. Important notions and results from commutative algebra

This section serves as a collection of objects and their properties that will be needed later on. At first, we start with some general results about rings and modules, for a basic introduction see Atiyah–Macdonald [1, Chapter 2]. Throughout, as mentioned in Section 1.2, let R be a commutative ring with unit element.

Lemma 2.20 (Nakayama's lemma)**.**

(a) Let M be a finitely generated R-module. For any ideal I contained in all maximal ideals of R holds the following implication: $IM = M \Rightarrow M = 0$.

(b) Let M and I be as above and let N be a submodule of M. Then if $M = IM + N$, it follows $N = M$.

(c) Let $(R, \mathfrak{m})$ be a local ring, $k = R/\mathfrak{m}$ be its residue field, and M a finitely generated R-module. Then $M/\mathfrak{m}M$ is naturally a k-vector space. Furthermore, if $(x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M)$ form a basis of $M/\mathfrak{m}M$, then $\{x_1, \ldots, x_n\}$ generate M.

Proof. See Atiyah–Macdonald [1, p. 21–22]. □

Next, we want to determine some important notions of ring extensions, for further results see Lang [36, Chapter VII, §1].

Definition 2.21. For a ring R and a ring extension $R \subseteq S$, we say that S is of *finite type* over R if S is a finitely generated R-algebra, and S is *finite* over R if S is a finitely generated R-module.

Definition 2.22. For a ring extension $R \subseteq S$ and an element $a \in S$, we define a to be *integral* over R if there exists a monic polynomial $f \in R[x]$ such that $f(a) = 0$. If all elements of S are integral over R, we say that S is an *integral ring extension* of R.

Propostion 2.23. *Let $R \subseteq S$ be a ring extension. Then the so-called integral closure of R in S, the set $\mathrm{Int}_S(R) \coloneqq \{a \in S \mid a \text{ is integral over } R\}$, is a subring of S.*

Proof. See Lang [36, Chapter VII, Proposition 1.4]. □

Propostion 2.24. *If $R \subseteq S$ is an integral ring extension and S is finitely generated R-algebra, then S is finite over R.*

Proof. See Lang [36, Chapter VII, Proposition 1.2]. □

Definition 2.25. For a field k and a k-algebra A we shall say that a set of elements $\{a_1, \ldots, a_n\} \subseteq A$ is *algebraically independent* over k if the kernel of the canonical map $F\colon k[x_1, \ldots, x_n] \to k[a_1, \ldots, a_n]$, $P \mapsto P\left(a_1, \ldots, a_n\right)$ is trivial.

Theorem 2.26 (Noether normalization)**.** *Let A be a finitely generated nonzero k-algebra for a field k. Then there are $y_1, \ldots, y_r \in A$ such that the extension $k[y_1, \ldots, y_n] \subseteq A$ is integral and the y_i are algebraically independent over k.*

Proof. See Atiyah–Macdonald [1, Chapter 5, Exercise 16]. □

3. Quotients of topological spaces and varieties

After introducing affine algebraic varieties, in order to gain a better understanding of what we mean by $\mathbb{C}^n/G$ in part (c) of the main theorem, we now have to establish *quotients*.

For this purpose, we firstly introduce general quotients in the category of topological spaces. Moreover, we will bring in three further types of quotients for varieties. In order to describe the action of a group on a variety, we have to establish the so-called *linear algebraic groups*. The aim is to prove that the quotient space $\mathbb{C}^n/G$, which is a priori an analytic space with the Euclidean topology, is also a quotient with respect to the Zariski topology in the category of affine varieties. For this purpose, all the preparations will be presented in this section such that these results just have to be applied after demonstrating that $\mathbb{C}^n/G$ can be viewed as an affine variety in Section 2.6.

First, we start with the most basic definition of a quotient: the quotient in the category of sets (cf. Santos–Rittatore [**20**, Chapter 6.4]).

Definition 2.27. Let G be any group acting on an arbitrary set X. We write X/G for the set of orbits of this action and denote the canonical projection mapping $x \in X$ onto its orbit by $\pi\colon X \to X/G$. Then, the pair $(X/G, \pi)$ is called the *set theoretical orbit space*. The categorical characterization is obtained by the following universal property: let $f\colon X \to Z$ be a map that is constant along the orbits, i.e. $f(x) = f(y)$ if and only if x and y lie in the same orbit. Then, one can find a unique map $\hat{f}\colon X/G \to Z$ such that the diagram

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi"'] & Z \\ X/G \arrow[ur, dashed, "\hat{f}"'] & \end{tikzcd}$$

is commutative.

Next, this construction shall be transferred to the category of topological spaces in which the morphisms are continuous maps. Here, we consider quotients given by an action of a group G on the underlying set of the topological space (X, τ). However, we remark that quotients of sets and topological spaces can be defined for general equivalence relations and their classes, too. The following definition and remark are based on Borisovich et al. [**5**, Chapter 2, §3] which also offers a more sophisticated presentation of this topic.

Definition 2.28. Let (X, τ) be a topological space and take the set theoretical quotient space X/G for some group action induced by G. As above, the canonical quotient map is denoted by $\pi\colon X \to X/G$. We define the *quotient topology* τ' on X/G induced by τ as the topology in which the open sets $Y \subseteq X/G$ are exactly those sets such that their preimage $\pi^{-1}(Y) \subseteq X$ is open with respect to τ.

Remark 2.29. In order to prove that this construction is indeed a quotient in the category of topological spaces, it remains to show: if f is continuous in the setup of Definition 2.27, then both π and $\hat{f}$ are continuous such that they are morphisms in the said category. Since the topology τ' of X/G is in Definition 2.28 defined such that π is continuous, it remains to verify the continuity of $\hat{f}$.
We have that $\hat{f}$ is continuous if and only if the preimage $\hat{f}^{-1}(A)$ for every open set $A \subseteq Z$ is open in X/G, and this preimage is in turn open if and only if $\pi^{-1}(\hat{f}^{-1}(A)) = (\hat{f} \circ \pi)^{-1}(A)$ is open in X by Definition 2.28. Hence, using that $f = \hat{f} \circ \pi$ yields that this set is open because f is continuous by assumption which implies that $f^{-1}(A)$ is open.

Remark 2.30. The reason to consider these quotients is that we will demonstrate that the quotient space $\mathbb{C}^n/G$ in part (c) of the main theorem is homeomorphic as analytic space equipped with the Euclidean topology to the later introduced *affine oribt variety* V_{or} (see Theorem 2.88). Therefore, the space $\mathbb{C}^n/G$ can be viewed as a variety itself.

However, it is not clear that it is also a quotient in the category of affine varieties over $\mathbb{C}$. Since we wish that a quotient of an affine variety satisfies properties compatible with the quotient of topological spaces in Remark 2.29, we will subsequently introduce three types of quotients of varieties. Later, after the proof of the aforementioned homeomorphism, we will point out that the variety V_{or} is a so-called *geometric quotient* in the category of affine varieties equipped with the Zariski topology. Based on this, we will demonstrate that V_{or} affords the quotient topology of the space $\mathbb{C}^n/G$ with respect to the Zariski topology. But in order to perform this proof, we firstly have to establish the orbit variety V_{or}. Moreover, its connection to the algebra of invariants $J = S^G$ has to be indicated. Since this will only happen in the later Section 2.6, at this point, we present a general version of the two theorems whose application will yield the desired result. For their proofs, a result from Section 2.5.1 is still needed. Nevertheless, the assertion is so intuitive that we can state it without issue.

The remainder of this section will be devoted to introduce *categorical, good*, and *geometric quotients*. However, we have to firstly introduce a special type of group and their action on varieties. For this presentation, we follow an introductory talk held by Schmitt [**51**], starting with *linear algebraic groups*.

Definition 2.31. A *linear algebraic group* over a field k is an affine variety G such that its set of points possesses a group structure. Moreover, we demand the group operation $G \times G \to G$, $(g, h) \mapsto gh$ and the mapping $g \mapsto g^{-1}$ onto the inverse elements to be morphisms of varieties.

Example 2.32. This example serves as an explanation how the group $GL(k^n)$—for a field—k can be viewed as a linear algebraic group. In the case of $k = \mathbb{C}$, this is the group to which the following theory shall be applied.
We use the identification of $GL(k^n)$ with the set $\{(A, y) \in k^{n\times n} \times k \mid \det(A)y - 1 = 0\}$ which is a variety because the expression $\det(A)^{-1}y$ is polynomial. The corresponding mapping is $A \mapsto \big(A, \det(A)^{-1}\big)$. Note that the coefficients of the product AB are polynomial functions of the coefficients of A and B. Moreover, the coefficients of the inverse A^{-1} are polynomial in the coefficients of A and $\det(A)^{-1}$. Hence, all conditions for a linear algebraic group are fulfilled.

Next, we describe how some linear algebraic group acts on a variety.

Definition 2.33. Let a linear algebraic group G act as a group on the set of points of a variety X. If this action $G \times X \to X$ is a morphism of varieties, we say that the G-action is *regular*. In this case, X is called a G-variety.

Remark 2.34. Now we can formulate which properties we desire to have for a quotient of a variety X is induced by a group action of a linear algebraic group G, and that behaves as in a topological space. We want to determine another affine variety Y which will take the role of the quotient space and a map $p\colon X \to Y$ that shall correspond to the projection π. Therefore, the points of Y shall match the orbits of the group action and p is demanded to be a surjective morphism of varieties that is invariant under the action of G, i.e., for all $g \in G, x \in X$ holds $p(gx) = p(x)$. Then, such a quotient behaves like the quotient of a topological space, and is compatible with the category of affine varieties over a fixed field. Hence, the objective will be to prove that $\mathbb{C}^n/G$ is a later introduced *geometric quotient*.

The first step is the following *categorical quotient*.

Definition 2.35. A *categorical quotient* of a G-variety is a tuple of an affine variety and a G-invariant morphism of varieties $p\colon X \to Y$ satisfying the following universal property: for any G-invariant morphism $f\colon X \to Z$, there exists a unique morphism $\hat{f}\colon Y \to Z$ such

that the diagram

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "p"'] & Z \\ Y \arrow[ur, dashed, "\hat{f}"'] & \end{tikzcd}$$

is commutative.

Note that this quotient is unique, and that the map p is surjective if the categorical quotient exists (cf. Santos–Rittatore [**20**, Chapter 6, Lemma 4.5]). Clearly, the fiber $p^{-1}(\{x\})$ of a point $x \in Y$ consists of a union of the G-orbits. However, this is not necessarily a single orbit whence the desired correspondence of points and orbits in Remark 2.34 is not achieved yet (cf. loc. cit. Chapter 6, Observation 4.3). Furthermore, a categorical quotient does not have to exist, for a counter example see Santos–Rittatore [**20**, Chapter 6, Example 4.10].

Next up, we will introduce some properties of maps from topology.

Definition 2.36. Let $f\colon X \to Y$ be a map between topological spaces, then we shall say
(a) the map f is closed if the image $f(A)$ of any closed set $A \subseteq X$ is closed;
(b) the map f is open if the image $f(B)$ of any open set $B \subseteq X$ is open;
(c) the map f is proper if the preimage $f^{-1}(K)$ of any compact set $K \subseteq Y$ is compact.

Subsequently, we try to fix the missing separation by the introduction of the second type of a quotient of a variety.

Definition 2.37. Let X be a G-variety. Then, we shall say that (Y, p) is a *good quotient* for the group action of G on X if $p\colon X \to Y$ is a closed, G-invariant, and surjective morphism of varities, and fulfills the following: p is demanded to be affine, that is, the preimage of any affine open set in Y is affine algebraic in X as well. Additionally, for every open set $U \subseteq Y$ the map

$$\mathcal{O}_Y(U) \to \mathcal{O}_X\left(p^{-1}(U)\right)^G, \ f \mapsto f \circ p$$

is an isomorphism, where $\mathcal{O}_X\left(p^{-1}(U)\right)^G$ denotes the ring of G-invariant functions which will be investigated more precisely in Section 2.5.1. The last condition is that the images $p(V_1), p(V_2)$ of disjoint closed sets V_1, V_2 are disjoint too.

Propostion 2.38. *A good quotient (Y, p) of a G-variety is a categorical quotient as well.*

Proof. See Schmitt [**51**, slide 17] for a sketch of this proof. □

A good quotient satisfies almost all the desired properties of the quotient of varieties that were postulated in Remark 2.34. However, a good quotient does not separate all orbits but only the closed ones. In order to add this and thereby achieve all the desired properties, the last type of quotient is brought in.

Definition 2.39. A *geometric quotient* (Y, p) of a G-variety X is a good quotient where the fiber $p^{-1}(\{y\})$ of every point $y \in Y$ consists of exactly one G-orbit.

Next, we establish a special type of map between affine varieties, and provide some of its properties that will occur in the following proofs. Note that we assume the base field to be $\mathbb{C}$ as this will be the scenario to which the following results will be applied.

Definition 2.40. A morphism $f\colon X \to Y$ of affine varieties is said to be *finite* if the extension $\mathbb{C}[Y] \subseteq \mathbb{C}[X]$ is a finite ring extension.

Propostion 2.41. *Let $f\colon X \to Y$ be a finite morphism of affine varieties. Then, f is a closed map, and f is surjective if and only if the related pullback $f^{\#}\colon \mathbb{C}[Y] \to \mathbb{C}[X]$ is injective.*

Proof. See Santos–Rittatore [**20**, Chapter 1, Theorem 4.93]. □

Subsequently, we demonstrate the first important result which we will apply onto the situation of $\mathbb{C}^n/G$ later. The ideas of the succeeding proof are taken from Hacking [**25**, Lemma 7.5]. Similarly to the algebra of invariants $J = S^G$, we denote the ring of polynomials on a variety X that are invariant under the action of G by $\mathbb{C}[X]^G$.

Propostion 2.42. *Let X be an affine variety and let the finite group G act on X. Then, the underlying set of the topology of the variety $\operatorname{Spec}(\mathbb{C}[X]^G)$ is the set of orbits and the topology is the quotient topology induced by the Zariski topology.*

Proof. For convenience, we set $Y := \operatorname{Spec}(\mathbb{C}[X]^G)$.
We start with the first claim. In Proposition 2.71 we will see that the ring extension $\mathbb{C}[X]^G \subseteq \mathbb{C}[X]$ is finite. Hence, the morphism of varieties $q\colon X \to Y$ induced by the inclusion map is finite. So, by Proposition 2.41, it follows that q is closed and surjective as the inclusion is clearly injective. Thus, in order to verify that the underlying set of $\operatorname{Spec}(\mathbb{C}[X]^G)$ corresponds to the set of orbits, it remains to show that if $q(x) = q(y)$, then x and y lie in the same orbit. Let $x, y \in X$ such that $x \neq gy$ for all $g \in G$. Analogously to Lemma 2.62 we can find a polynomial $f \in \mathbb{C}[X]$ with $f(x) \neq 0$ and $f(gy) = 0$ for all $g \in G$. Set $h := \prod_{g\in G} gf$ which is clearly G-invariant, i.e., $h \in \mathbb{C}[X]^G$. Call in mind that points $z_1, z_2 \in Y$ are equal if and only if $\alpha(z_1) = \alpha(z_2)$ for all $\alpha \in \mathbb{C}[X]^G$. So, due to the choice of f, it follows that $h(x) \neq 0$ while $h(y) = 0$ which implies $q(x) \neq q(y)$ and hence proves the first claim.
Secondly, we have to show that a set $U \subseteq Y$ is open if and only if its preimage $q^{-1}(U) \subseteq X$ is open. For this purpose, we observe that q is continuous: a closed set in Y is the vanishing locus of some polynomials f_i. Then, its preimage is the vanishing locus of the functions $f_i \circ q$ which are polynomials, too. So, the preimage is closed, and hence q is continuous which implies that if $U \subseteq Y$ is open, then $q^{-1}(U)$ is open.
It remains to confirm that for a set $U \subseteq Y$ such that $q^{-1}(U) \subseteq X$ is open, U is open itself. As q is surjective, we have that $q(q^{-1}(U)) = U$. Moreover, since q is closed, it follows that $q(X \setminus q^{-1}(U)) = Y \setminus U$ is closed whence U is open. Thus, the topology on Y is the quotient topology induced by the Zariski topology. □

In conclusion, we will show that the preceding map q already satisfies all the properties of a geometric quotient. For this purpose we follow Santos–Rittatore [**20**, Theorem 5.2].

Theorem 2.43. *Let G be a finite algebraic linear group acting regularly on an affine variety X. Then the tuple $(\operatorname{Spec}(\mathbb{C}[X]^G), q)$ from Proposition 2.42 is a geometric quotient.*

Proof. At the outset, we observe that we have just seen in the proof of Proposition 2.42 that q is a closed, surjective, and affine morphism. Moreover, since $q(x) = q(y)$ implies $x = gy$ for some $g \in G$, it follows immediately that q separates all the orbits of the G-action. Hence, it remains to verify that q is G-invariant, and that for every open set $U \subseteq Y$ the pullback map $\mathcal{O}_Y(U) \to \mathcal{O}_X\left(q^{-1}(U)\right)^G,\ f \mapsto f \circ q$ is an isomorphism.
So, to start with, the G-equivariance, we have to check that $q(x) = q(gx)$ for all $x \in X$ and all $g \in G$. Hence, we have to verify that $f(q(x)) = f(q(gx))$ for all $f \in \mathbb{C}[Y] = \mathbb{C}[X]^G$. Since q is induced by the inclusion map, it follows that its pullback is the inclusion map, too, and hence $q^{\#}(f) = f \circ q = f$. Thus, the preceding equation translates to $f(x) = f(gx)$ which is clearly true for all G-invariant functions.
For the aforementioned isomorphism, it is sufficient to prove it for an arbitrary elementary

open set $Y_f = \{p \in Y \mid f(p) \neq 0\}$ for a G-invariant polynomial $f \in \mathbb{C}[X]^G$ because any open set can be covered by them. Hence, we aim at proving the isomorphism

$$\mathcal{O}_Y(Y_f) \cong \mathcal{O}_X\left(q^{-1}(Y_f)\right)^G = \mathcal{O}_X(X_f)^G.$$

Under this assumption, the proof is completed by using the equality and the isomorphism

$$\mathcal{O}_X(X_f) = \left\{ \frac{g}{f^r} \middle| g \in \mathbb{C}[X], r \in \mathbb{N} \right\} \cong \mathbb{C}[X]_f$$

(cf. Gathmann [**22**, Proposition 3.8 and Corollary 3.10]), and the fact that $q^{\#}(f) = f$ for all $f \in \mathbb{C}[Y] = \mathbb{C}[X]^G$ as well as the chain

$$q^{\#}(\mathbb{C}[Y]_f) = q^{\#}((\mathbb{C}[X]^G)_f) = (q^{\#}(\mathbb{C}[X]^G))_{q^{\#}(f)} = (\mathbb{C}[X]^G)_f = \left(\mathbb{C}[q^{-1}(Y)]_f\right)^G.$$

For the last equality, we note that $P \in (\mathbb{C}[X]^G)_f$ if and only if $P = \frac{h}{f^r}$, where $r \geq 0$ and h is a G-invariant polynomial. Since f is G-invariant, this is equivalent to $P \in (\mathbb{C}[X]_f)^G$. As $q^{-1}(Y)$ contains at least one representative from each G-orbit, we can conclude that the G-invariant functions on X and $q^{-1}(Y)$ coincide, from which the claimed equality of the sets above follows directly. □

Therefore, the two preceding results jusitify to denote $\operatorname{Spec}(\mathbb{C}[X]G)$ by X/G.

4. Basics of multilinear algebra

In this section, we will follow a book on multilinear algebra by Greub [**24**] to provide an introduction to some useful objects of this area. First, the *tensor algebra* will form the foundation for the *exterior algebra* and the *symmetric algebra*. Here, these notions will only be discussed for vector spaces over a field in characteristic 0, but they can also be generalized for modules, see, for example, Lang [**36**, Chapter XIX, §1 and Chapter XVI, §8]. For this section we assume familiarity with tensor products of finitely many vector spaces and their basic properties, as, e.g., in Lang [**36**, Chapter XVI, §1–2]. The symmetric algebra is needed to define the coordinate ring of a vector space (see Definition 2.59), which is important for the subsequent section. To achieve a better compatibility with the following sections, the notations from Lehrer–Taylor [**37**] are adopted.

Throughout, let V be a vector space over a field of characteristic 0.

4.1. The tensor algebra. The aim of this subsection is the construction of the *tensor algebra* following Greub [**24**, 3.1 and 3.2]. To do so, we first establish some preliminaries.

Definition 2.44. Let $p \geq 2$. The tensor product of $V^p := V \times \cdots \times V$, the p-fold direct product of copies of the vector space V, will be called the *p-fold tensor power* of V, denoted by $T^p(V)$. Its elements are the *tensors of degree p*. If $x \in T^p(V)$ and $x = x_1 \otimes \cdots \otimes x_p$, where all x_i are of degree 1, x is called a *pure tensor*.

The subsequent proposition shows the associativity of the tensor product.

Propostion 2.45. *Let V_1, V_2, V_3 be vector spaces over the same field of characteristic 0. Then*

$$V_1 \otimes V_2 \otimes V_3 \cong (V_1 \otimes V_2) \otimes V_3$$

by sending pure tensors $x_1 \otimes x_2 \otimes x_3$ onto $(x_1 \otimes x_2) \otimes x_3$. This isomorphism is unique.

Proof. See Greub [24, Proposition 1.20.1]. The uniqueness follows from the universal property of the tensor product. □

From this, we can conclude that $T^p \otimes T^q \cong T^{p+q}$ by a unique isomorphism, and that there exists a unique bilinear map, such that for pure tensors

$$\beta\colon T^p \times T^q \to T^{p+q} \quad \beta\left(x_1 \otimes \cdots \otimes x_p, x_{p+1} \otimes \cdots \otimes x_{p+q}\right) = x_1 \otimes \cdots \otimes x_r.$$

Hence, for pure tensors x and y of degree p and q respectively, we can define their tensor product in the following way:

$$x \otimes y = (x_1 \otimes \cdots \otimes x_p) \otimes (y_1 \otimes \cdots \otimes x_q) = (x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes x_q)\,. \tag{2}$$

Since all elements of a p-fold tensor power can be written as sum of pure tensors, this multiplication can be extended linearly.

Definition 2.46. The *tensor algebra* over the vector space V is the direct sum

$$T(V) = \bigoplus_{p=0}^{\infty} T^r(V),$$

with $T^0(V) = k$ and $T^1(V) = V$ for the base field k.

The algebra structure is clear apart from the multiplication of two elements. But in (2) we have already defined the multiplication on pure tensors and extended it for tensors of fixed degree. As every element of $T(V)$ is a formal sum of elements in the tensor powers T^p with only finitely many nonzero entries, the multiplication can be traced back to the case of tensors with fixed degree

$$x \otimes y = \sum_{p,q} x_p \otimes y_q \qquad x = \sum_p x_p, y = \sum_q y_q.$$

The tensor product of x_p and y_q is defined as in (2). Therefore, $T(V)$ is an associative algebra in which V is naturally included. It also admits a grading by assigning the degree p if an element lies in $T^p(V)$.

Recall that for a basis $(v_i)_{i\in I}$ of the vector space V the set of pure tensors $\{v_{i_1} \otimes \cdots \otimes v_{i_p} \mid \text{for all } (i_1, \ldots, i_p \in \{1, \ldots, n\}^p\}$ forms a basis of the p-fold tensor power $T^p(V)$. In particular, if V is of finite dimension n, this leads to $\dim\left(T^p(V)\right) = n^p$.

4.2. The exterior algebra. Aiming at a definition of the *exterior algebra*, the notions of a skew-symmetric map and the exterior product will be introduced. In this subsection we follow Greub [24, 5.1–5.4 and 5.7].

Definition 2.47. Let $p \geq 2$, and let V, W be vector spaces. A p-linear map $\varphi\colon V^p \to W$ is called *skew-symmetric* if the following implication holds:

$$x_i = x_j \text{ for some } i \neq j \quad \Rightarrow \quad \varphi\left(x_1, \ldots, x_n\right) = 0.$$

There are multiple equivalent definitions (cf. Greub [24, 5.1]) but this definition even works in the more general situation that the base field is of positive characteristic.

Example 2.48. The determinant map $\det\colon (k^n)^n \to k$, where the columns of a matrix are considered as individual entries, is a skew symmetric map as equal columns are linearly independent.

Thereafter, we will define a *universal property* for skew-symmetric maps almost analogously to the universal property for tensor products in order to characterize the *exterior product*.

Definition 2.49. Let A be a vector space and $\wedge^p\colon V^p \to A$ be a p-linear skew-symmetric map. We say that $\wedge^p$ has the *universal property* if the following conditions are fulfilled:

(a) The map $\wedge^p$ is surjective, i. e., $\operatorname{im}(\wedge^p) = A$.

(b) For any vector space W and any skew-symmetric map $\varphi\colon V^p \to W$ there exists a linear map $f\colon A \to W$ such that $\varphi = f \circ \wedge^p$, i. e., the diagram commutes:

$$\begin{tikzcd} V^p \arrow[r, "\varphi"] \arrow[d, "\wedge^p"'] & W \\ A. \arrow[ur, dashed, "\exists f"'] & \end{tikzcd}$$

Then we shall say that $(A, \wedge^p)$ is the *p-fold exterior power* of V and may also write $A = \bigwedge^p(V)$.

The succeeding theorem shows that it is justified to denominate it as *the* exterior power since it is unique up to ismorphism.

Theorem 2.50. *For any vector space V and any $p \geq 2$, there exists a p-fold exterior product $\bigwedge^p(V)$ and it is unique up to isomorphism.*

Proof. For the uniqueness assume $\wedge^p\colon V^p \to A$ and $\widetilde{\wedge}^p\colon V^p \to \widetilde{A}$ are two p-linear skew symmetric maps fulfilling the universal property of Definition 2.49. Hence, applied to $W = \widetilde{A}$ and $\widetilde{W} = A$, there exist linear maps $f\colon A \to \widetilde{A}$ and $\widetilde{f}\colon \widetilde{A} \to A$. Then we have

$$f \circ \wedge^p = \widetilde{\wedge}^p \qquad \text{and} \qquad \widetilde{f} \circ \widetilde{\wedge}^p = \wedge^p.$$

This leads to $f \circ \left(\widetilde{f} \circ \widetilde{\wedge}^p\right) = \widetilde{\wedge}^p$ and $\widetilde{f} \circ (f \circ \wedge^p) = \wedge^p$ and as $\wedge^p$ and $\widetilde{\wedge}^p$ are each surjective—so cancellation from the right is applicable—we get that

$$f \circ \widetilde{f} = \mathrm{id} \qquad \text{and} \qquad \widetilde{f} \circ f = \mathrm{id}\,.$$

Thus, we can finally conclude that $A \cong \widetilde{A}$.

For the existence, we only give a sketch of the proof and omit the computations that can be found in Greub [**24**, 4.1, 4.6 and 5.3]. The first step of constructing the p-fold exterior power is to define $N^p(V)$ as the subspace of $T^p(V)$ generated by the set

$$\{x_1 \otimes \cdots \otimes x_p \mid x_k \in V, \exists i \neq j\colon x_i = x_j\}\,.$$

One can show that setting $\bigwedge^p(V) = T^p(V)/N^p(V)$ and defining the map $\wedge^p$ as the concatenation $\pi \circ \tau$, where $\tau\colon V^p \to T^p(V)$ denotes the map belonging to the tensor product and $\pi\colon T^p(V) \to T^p(V)/N^p(V)$ the projection, is a skew symmetric map satisfying the universal property. $\square$

Similarly to the tensor algebra, we can now define the *exterior algebra*.

Definition 2.51. The exterior algebra over a vector space V is the direct sum

$$\bigwedge(V) = \bigoplus_{p=0}^{\infty} \bigwedge^p(V)$$

with $\bigwedge^0(V) = k$ and $\bigwedge^1(V) = V$ for the base field k.

The individual projections $\pi\colon T^p(V) \to \bigwedge^p(V)$ with kernel $N^p(V)$ for each p determine a common projection

$$\pi\colon T(V) \to \bigwedge(V)$$

with kernel $\bigoplus_{p=0}^{\infty} N^p(V) = N(V)$. Hence, $\bigwedge(V) \cong T(V)/N(V)$ which is an associative algebra (cf. Greub [24, 4.6]). The algebra multiplication, denoted by $\wedge$, is induced by the projection π via $x \wedge y = \pi\left(\widetilde{x} \otimes \widetilde{y}\right)$ for preimages under π of x and y respectively. Thus, we have

$$(x_1 \wedge \cdots \wedge x_p) \wedge (y_1 \wedge \cdots \wedge y_q) = x_1 \wedge \cdots \wedge x_p \wedge y_1 \wedge \cdots \wedge y_q.$$

Besides, the ideal $N(V)$ inherits the grading from the tensor algebra, and therefore the exterior algebra is also graded. Moreover, by definition clearly $N^0(V) = 0$ and $N^1(V) = 0$, so we can identify the base field k and the vector space V with their corresponding images under the projection π.

Since we are especially interested in finite dimensional vector spaces, we will conclude with an interesting result on the dimension of the exterior algebra over a finite dimensional vector space.

Propostion 2.52. *Let V be a vector space with basis $(v_i)_{i\in\{1,\dots,n\}}$. Then the products of the shape*

$$v_{i_1} \wedge \cdots \wedge v_{i_p}, \quad i_1 < \cdots < i_p$$

for all permitted combinations of the indices form a basis of $\bigwedge^p(V)$.

Proof. See Greub [24, 5.7]. □

From this, we can immediately conclude that $\dim\left(\bigwedge^p(V)\right) = \binom{n}{p}$ if the vector space V is of finite dimension n. In particular, for $p > n$ this leads to $\bigwedge^p(V) = 0$ and therefore, by the binomial formula, we have $\dim\left(\bigwedge(V)\right) = 2^n$. In this regard, the exterior algebra behaves completely differently from the tensor algebra, which is always of infinite dimension. For example, considering $\mathbb{C}$ as a $\mathbb{C}$-vector space itself leads to $\bigwedge(\mathbb{C}) = \mathbb{C}$, while $T(\mathbb{C})$ is a direct sum of infinitely many finite dimensional spaces.

4.3. The symmetric algebra. The final object to consider in this section is the *symmetric algebra*, which behaves relatively similarly to the exterior algebra, whence we will skip the first proofs and concentrate on the additional properties. For this purpose, we follow Greub [24, Chapter 9].

The difference to the exterior algebra arises from the variation of the foundational map.

Definition 2.53. Let $p \geq 2$ and let V, W be vector spaces. A p-linear map $\varphi\colon V^p \to W$ is called *symmetric* if for all permutations $\sigma \in \mathrm{Sym}(p)$ of the symmetric group and all vectors $(x_1, \dots, x_p) \in V^p$

$$\sigma\varphi\left(x_1, \dots, x_p\right) \coloneqq \varphi\left(x_{\sigma(1)}, \dots, x_{\sigma(p)}\right) = \varphi\left(x_1, \dots, x_p\right).$$

Example 2.54. A simple example for a bilinear symmetric map is an arbitrary scalar product on a vector space V over $\mathbb{R}$.

This allows us to define the *universal property* in a very similar way to Definition 2.49, with a commutative diagram that is omitted as it would look almost exactly the same.

Definition 2.55. Let A be a vector space and $\vee^p\colon V^p \to A$ be a p-linear symmetric map. We say that $\vee^p$ has the *universal property* if the following conditions are fulfilled:

(a) The map $\vee^p$ is surjective, i. e., $\mathrm{im}\left(\vee^p\right) = A$.
(b) For any vector space W and any skew-symmetric map $\varphi\colon V^p \to W$ there exists a linear map $f\colon A \to W$ such that $\varphi = f \circ \vee^p$.

Then we shall say that $(A, \vee^p)$ is the *p-fold symmetric power* of V and may also write $A = S^p(V)$.

The existence and uniqueness of the p-fold symmetric power are shown by using the same methods as for the exterior algebra. Note that the existence can be shown by adapting the proof of Theorem 2.50 so that the subspace is $N^p(V)$ is replaced by $M^p(V)$, which denotes the subspace of $T^p(V)$ generated by the set

$$\left\{x_1 \otimes \cdots \otimes x_p - x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(p)} \mid \text{for all } \sigma \in \mathrm{Sym}(p)\right\}.$$

As for the p-fold exterior power, this enables us to define the *symmetric algebra*.

Definition 2.56. For any vector space V we define $S(V)$, the symmetric algebra over V to be the direct sum

$$S(V) = \bigoplus_{p=0}^{\infty} S^p(V)$$

with $S^0(V) = k$ and $S^1(V) = V$ for the base field k.

Analogously to the exterior algebra, there is a linear isomorphism $f\colon S(V) \to T(V)/M(V)$. This is constructed via the common projection $\pi\colon T(V) \to S(V)$ with kernel $M(V)$ and induces the multiplication on $S(V)$, denoted by $\vee$ via $x \vee y = \pi\left(\widetilde{x} \otimes \widetilde{y}\right)$ for preimages under π of x and y respectively. This is why the symmetric algebra is an associative algebra. Additionally, it is graded and since $M^0(V) = 0 = M^1(V)$, we can identify the base field k and the vector space V with their corresponding images under the projection π (cf. Greub [**24**, 4.14]).

To complete this overview of analogous results to those for the exterior algebra, we add the following proposition for finite dimensional vector spaces.

Propostion 2.57. *For any vector space V with basis $(v_i)_{i\in\{1,\ldots,n\}}$ the products of the form*

$$v_{i_1} \vee \cdots \vee v_{i_p}, \quad i_1 \leq \cdots \leq i_p$$

for all permitted combinations of the indices form a basis of $S^p(V)$.

Proof. See Greub [**24**, 9.7]. □

The above result shows that $\dim\left(S^p(V)\right) = \binom{n+p-1}{p}$ for all $p \geq 0$. Hence, in contrast to the exterior algebra, the symmetric algebra of any nonzero vector space has infinite dimension, even if the vector space itself is finite dimensional. However, its homogeneous parts, the p-fold symmetric powers, are finite dimensional. This gives a hint to the most important result of this section as this property is also fulfilled by a polynomial ring in finitely many variables and its subspaces of fixed degree. We equip the polynomial ring $k[x_1, \ldots, x_n]$ with an associative multiplication on the monomials by

$$p_1 \cdot p_2 = \left(a \cdot x_1^{i_1} \cdots x_n^{i_n}\right) \cdot \left(b \cdot x_1^{j_1} \cdots x_n^{j_n}\right) = a \cdot b \cdot x_1^{i_1+j_1} \cdots x_n^{i_n+j_n}, \tag{3}$$

where all $i_l, j_l \geq 0$ and $a, b \in k$. Since any polynomial is a finite sum of monomials, we can extend this multiplication to the polynomial ring, which then becomes an associative graded algebra, the *polynomial algebra*, denoted by $k[x_1, \ldots, x_n]$. The subsequent proposition shows that these two algebra are in fact isomorphic (cf. Greub [**24**, 9.14]).

Propostion 2.58. *For a vector space V of $\dim(V) = n$ over a field k, its symmetric algebra $S(V)$ is isomorphic to the polynomial algebra in n variables.*

Proof. First, let $(v_1, \ldots, v_n)$ be a fixed basis of V. Then from Proposition 2.57, we know that every element $u \in S^p(V)$ can be uniquely expressed by

$$u = \sum_{(j_1,\ldots,j_n)} a_{(j_1,\ldots,j_n)} \cdot v_1^{j_1} \cdots v_n^{j_n}, \quad \sum_l j_l = p,\ a_{(j_1,\ldots,j_n)} \in k.$$

Here, the exponents j_l stand for the j_l-fold symmetric product $w \vee \cdots \vee w$ of a vector. Following this, we can define the corresponding polynomial P_u by

$$P_u = \sum_{(j_1,\ldots,j_n)} a_{(j_1,\ldots,j_n)} \cdot x_1^{j_1} \cdots x_n^{j_n},$$

which is homogeneous of degree p, that is, it consists only of monomials such that $\sum_l j_l = p$. Conversely, every homogeneous polynomial of degree p can be written uniquely in such way, therefore, it also determines a unique element $u \in S^p(V)$. So, we already have a bijective mapping between the p-fold symmetric power $S^p(V)$ and the homogeneous polynomials of degree p. The linearity $P_{\lambda u+w} = \lambda P_u + P_w$ follows clearly from the construction above as the addition and scalar multiplication only concern the coefficients.
Finally, we have with the notation above

$$u_1 \vee u_2 = \left(a \cdot x_1^{i_1} \cdots x_n^{i_n}\right) \cdot \left(b \cdot x_1^{j_1} \cdots x_n^{j_n}\right) = a \cdot b \cdot x_1^{i_1+j_1} \cdots x_n^{i_n+j_n}$$

for $u_1, u_2 \in S^p(V)$ and comparing to (3) shows that

$$P_{u_1 \vee u_2} = P_{u_1} \cdot P_{u_2}.$$

Hence, the mapping $u \mapsto P_u$ is an algebra isomorphism which extends naturally to an algebra isomorphism $S(V) \overset{\cong}{\to} k[x_1, \ldots, x_n]$. □

Now, following Lehrer–Taylor [**37**, Section 3.1] and sticking to their notation, we will apply this result to the dual vector space V^* of a finite dimensional vector space V over $\mathbb{C}$: we first choose a basis $(v_1, \ldots, v_n)$ of V and let the linear functions $(X_1, \ldots, X_n)$ be the corresponding dual basis. As any X_j sends a vector $v \in V$ onto the uniquely determined coefficient λ_j of v in its basis representation, it is called a *coordinate function*.

Definition 2.59. For an n-dimensional vector space V over $\mathbb{C}$, we shall say that the symmetric algebra of its dual vector space $S := S(V^*)$ is the *coordinate ring* of V.

Note that many authors also use the notation $\mathbb{C}[V]$ in analogy to algebraic geometry. Later, in Remark 2.90 and Remark 3.23 we will see why the coordinate ring is defined as $S(V^*)$ and not as $S(V) = \mathbb{C}[V^*]$.

From Proposition 2.58 we immediately obtain

$$S(V^*) \cong \mathbb{C}[X_1, \ldots, X_n]$$

and therefore, under the identification of the basis elements $X_j \in V^*$ with the variable X_j, we can consider S not as the usual polynomial functions, whose arguments are numbers, but as a generalized version of polynomial functions with arguments in V. For the p-fold symmetric power $S^p(V^*)$—identified with the subspace of homogeneous polynomial functions of degree p—we write S^p.

5. The algebra of polynomial invariants

In order to set the foundation for the next section, the algebra of invariants of a group is presented. Its key property is that it is finitely generated when the underlying group is finite. To show this, we follow Lehrer–Taylor [**37**, Sections 3.1–3.3].

Here, we restrict the considered vector space V to be finite dimensional ($\dim(V) = n$) and to be over the base field $\mathbb{C}$. Let $GL(V)$ be the *general linear group* of V, i. e., the group of invertible linear maps, which acts on V^*. Therefore, it also acts on the coordinate ring S by

$$gP(v) := P\left(g^{-1}v\right) \qquad \text{for all } v \in V$$

for all $P \in S$. For the identity element $1 \in GL(V)$ holds $1P(v) = P\left(1^{-1}v\right) = P(v)$ for all $v \in V$, and for arbitrary $g, h \in GL(V)$ easy computations show that $g(hP) = (gh)P$. So, this defines in fact a group action, which is also compatible with the grading and the algebra structure, i.e., $gS^p = S^p$ and $g(PQ)(v) = (PQ)\left(g^{-1}v\right) = P\left(g^{-1}v\right) \cdot Q\left(g^{-1}v\right) = gP(v) \cdot gQ(v)$ for all $v \in V$.

Example 2.60. Let $n = 3$ and let $g \in GL(V)$ with matrix $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ and inverse $\left(\begin{smallmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, then, since the action of g can be viewed as a basis transformation with g^{-1}, for the canonical monomial, it holds

$$g\left(X_1^r X_2^s X_3^t\right) = (X_1 - X_2 + X_3)^r (X_2 - X_3)^s X_3^t.$$

Definition 2.61. Let G be a subgroup of $GL(V)$. We shall say that a polynomial $P \in S$ is *G-invariant* if $gP = P$ for all $g \in G$. The subalgebra of all these polynomials $S^G := \{P \in S \mid gP = P \text{ for all } g \in G\}$ is called the *algebra of invariants* of G, also denoted by $J = S^G$.

By definition, any $P \in J$ is constant on each orbit $Gv = \{gv \mid g \in G\}$. Hence, we can view P as polynomial that takes arguments from the orbit space V/G, that is, the space of equivalence classes induced by the group action of G.

The subsequent result is a generalized version of the well-known "Lagrange interpolation".

Lemma 2.62. *For arbitrary elements $a_1, \ldots, a_m$ of $\mathbb{C}$ and any set of distinct vectors $\{w_1, \ldots, w_m\} \subseteq V$ there exists a polynomial $P \in S$ such that for all $i = 1, \ldots, m$ holds $P(w_i) = a_i$.*

Proof. Since the finite sum of polynomials is again a polynomial, we can construct P by components P_i with the property that $P_i(w_j) = \delta_{ij}$ (Kronecker delta) by

$$P = \sum_{i=1}^{m} a_i P_i.$$

Therefore, we will inductively prove, that such polynomials P_i for all $i = 1, \ldots, m$ exist. First, for the base case $m = 1$, set $P_1 := 1$. Now, we assume $m > 1$ and take $Q \in S$ with $Q(w_1) = 1$ and $Q(w_i) = 0$ for all $i = 2, \ldots, m-1$. Such a polynomial Q exists by induction. We can express $w_m = \sum_{j=1}^{n} \lambda_j v_j$ in the basis of V, then $L_m = \sum_{j=1}^{n} (X_j - \lambda_j) \in S$ fulfills $L_m(w_m) = 0 \neq L_m(w_1)$ because $w_1 \neq w_m$. Next, set $P_1 := Q\dfrac{L_m}{L_m(w_1)}$ and note that the same construction is applicable not only to $i = 1$ but to all $i = 1, \ldots, m-1$. To construct P_m, we define linear polynomials L_i for $i = 1, \ldots, m-1$ in the same way as L_m. Therefore, $L_i(w_i) = 0 \neq L_i(w_m)$ and the proof is completed by setting $P_m := \prod_{j=1}^{m-1} \dfrac{L_j}{L_j(w_m)}$. □

This lemma is used to prove the next theorem which shows that the algebra of invariants J separates the orbits of the G-action on V.

Propostion 2.63. *Let G be a finite subgroup of $GL(V)$ acting on the vector space V and take arbitrary $v, w \in V$. Then, v and w lie in the same orbit Gv if and only if $P(v) = P(w)$ for all G-invariant polynomials $P \in J$.*

Proof. First, if $w \in Gv$ there exists a $g \in G$ such that $w = g(v)$. Therefore, for any $P \in J$ the statement follows from $P(w) = P(g(v)) = g^{-1}P(v) = P(v)$. In order to establish the converse, assume $w \notin Gv$. Hence, $gv \neq w$ for all $g \in G$ and we can apply Lemma 2.62 (if $g_1 v = g_2 v$, one duplicate is left out) to receive a polynomial $Q \in S$ such that $Q(w) = 0$ and $Q(gv) = 1$ for all $g \in G$. Set $P = \prod_{g \in G} gQ$ and by construction

$hP = \prod_{g\in G} hgQ = \prod_{g\in G} gQ$, so $P \in J$. Furthermore, $P(v) = \prod_{g\in G} Q\left(g^{-1}v\right) = 1$, but $P(w) = 0$. Since P is constant on each orbit, this completes the proof by contraposition. □

5.1. Finite generation of the algebra of invariants. The purpose for this subsection is to answer the question whether the algebra of invariants of G is finitely generated if the group G is finite. This question was already answered positively over one hundred years ago, where first Hilbert [**28**] proved this result in 1890 for the base field $\mathbb{C}$ and the general linear group (cf. Benson [**3**, introduction]). The paper containing this proof is considered by L. Smith as "a paper that broke completely new ground in invariant theory" ([**61**, p. 214]) emphasizing how big a step forward it was for the invariant theory of the 19th century. In particular, the results proven by Hilbert are still viable and relevant in modern invariant theory including vector spaces even though the proof predates the definition of a vector space (cf. L. Smith [**61**, p. 214, footnote 6]). Hilbert's new approach provided an answer to the big question of invariant theory of that time, and hence it "spelled the doom of XIXth Century invariant theory", according to Dieudonné [**18**, p. 2]. On the other hand, the work of Hilbert as well as Noether gave this subject a rigorous mathematical foundation "with the introduction of abstract algebraic machinery for addressing" (Benson [**3**, p. vii]) such questions as the finite generation. This is why Benson states that their work was "the beginning of modern commutative algebra" (loc. cit.).

Then, in 1915 Noether [**46**] gave a proof for an arbitrary finite group and provided an upper bound on the number of generators. Moreover, in 1926 she [**47**] showed that the statement is even true for a base field in arbitrary characteristic (see also Humphreys [**31**]). The approaches of Hilbert and Noether differ greatly: Hilbert's proof contained his famous "Basis Theorem" (cf. Section 2.1.2) but it only gives a proof of the existence of a finite set of generators. This provides a suitable theoretical result, but "[i]n practice it is often very difficult to know where to look for invariants, and / or when we have found all of them" (L. Smith [**60**, p. ix]). On the other hand, Noether's proof provided an explicit set of generating invariants (cf. Flatto [**21**, p. 237]) and it also "introduced fundamental arguments for finite ring extensions" (Neusel–Smith [**45**, p. 29]). The constructive proof of Noether yields an easily implementable algorithm, that, however, is not a very effective way, to determine a generating set (cf. L. Smith [**60**, p. ix–x]). An interesting comparison of both can be found in the first chapter of a paper from Flatto [**21**].

His success in the aforementioned special case might have led Hilbert in 1900 to the formulation of his 14th problem (cf. Humphreys [**31**]), where it is asked, whether the algebra of invariants is finitely generated for all groups. It turned out, that this is in general false due to the famous counterexample of Nagata [**44**]. Furthermore, it can be shown that there exist at least n algebraically independent invariants if $\dim(V) = n$ (cf. Burnside [**10**, 262]). Now the main theorem of this work shows, that there are exactly n algebraically independent generators if and only if G is reflection group (cf. Flatto [**21**, Introduction]). For further concepts and developments of invariant theory the introduction of Benson's book [**3**] offers a good overview and many references. Another interesting work is an article by L. Smith [**61**], where the history of invariant theory as well as more recent problems and developments are highlighted.

After this short historical interlude, we return to the way of Lehrer–Taylor [**37**, Section 3.3], who first present the methods of Hilbert, to prove that—in case of V being a complex n-dimensional vector space—the algebra of invariants $J = S^G$ of a finite subgroup $G \leq GL(V)$ is finitely generated.

Remark 2.64. The set of G-invariant polynomials with zero constant term, that clearly forms an ideal of J, shall be denoted by $J^+ := \{P \in J \mid P(0) = 0\}$. It holds $J/J^+ \cong \mathbb{C}$, hence, J^+ is a maximal ideal. As J is a subalgebra of the symmetric algebra S, we can consider the ideal generated by J^+ and write $F := SJ^+ \trianglelefteq S$ for it. Since we have $S \cong \mathbb{C}[X_1, \dots, X_n]$ (cf. Proposition 2.58), Hilbert's basis theorem says that F is finitely generated, so $F = (I_1, \dots, I_r)$. The generators $I_1, \dots, I_r$ are G-invariant with zero constant term by construction and can be chosen homogeneous, because polynomials in S are finite sums of homogeneous polynomials as seen in the proof of Proposition 2.58 by the bijection between the symmetric power S^p and the homogeneous polynomials of degree p.

Definition 2.65. The *averaging operator* Av is the linear map $S \to J$ defined as

$$\mathrm{Av}(P) := \frac{1}{|G|} \sum_{g \in G} gP.$$

Clearly $\mathrm{Av}(P) \in J$ for all $P \in S$. In addition, if P is already G-invariant, the averaging operator does not change anything, so $\mathrm{Av}(P) = P$ and hence $\mathrm{Av}^2 = \mathrm{Av}$, which indicates that Av is the projector of S onto J. Moreover, as $\deg(gP) = \deg(P)$, if $\mathrm{Av}(P) \neq 0$, the averaging preserves the degree.

Lemma 2.66. *Let $P \in J$ and $Q \in S$, then $\mathrm{Av}(PQ) = P\,\mathrm{Av}(Q)$, hence, the averaging operator is a J-module homomorphism on S considered as J-module.*

Proof. This is a simple computation: let $v \in V$ arbitrary, then

$$\mathrm{Av}(PQ)(v) = \frac{1}{|G|} \sum_{g \in G} gP(v)gQ(v) \overset{P \in J}{=} P(v) \frac{1}{|G|} \sum_{g \in G} gQ(v) = (P\,\mathrm{Av}(Q))(v).$$

□

The following example demonstrates the preceding properties of the averaging operator before they will be applied in the proof of Theorem 2.68.

Example 2.67. Consider a $\mathbb{C}$-vector space V with $\dim(V) = 2$, so $S(V^*) \cong \mathbb{C}[x, y]$ and let $G = \mathbb{Z}/2\mathbb{Z}$ be the cylic group acting by scalar multiplication with ± 1. Let $P = x^2$ and $Q = x^2y$, then we have $P \in J$ and as expected $\mathrm{Av}(P) = \frac{1}{2}\left((1 \cdot x)^2 + (-1 \cdot x)^2\right) = \frac{1}{2}\left(x^2 + x^2\right) = P$. Furthermore, we have $\mathrm{Av}(Q) = \frac{1}{2}\left((1 \cdot x)^2(1 \cdot y) + (-1 \cdot x)^2(-1 \cdot y)\right) = \frac{1}{2}(x^2y - x^2y) = 0$.

Theorem 2.68. *Let G be finite, then the algebra of invariants J of G is a finitely generated $\mathbb{C}$-algebra.*

Proof. By the previous observations with the same notation, there exist G-invariant homogeneous polynomials, such that $F = (I_1, \dots, I_r)$. We will show that J is generated as an algebra by $I_1, \dots, I_r$. First, we assume that all I_i are nonzero. It suffices to show that an arbitrary homogeneous polynomial $P \in J$ is a polynomial in the generators. The proof is by induction on $m := \deg(P)$. Since the case $m = 0$ is trivially fulfilled by taking the corresponding constant polynomial, we may assume $m > 0$.
This implies $P \in J^+ \subseteq F$, so we find $P_1, \dots, P_r \in S$ such that $P = P_1I_1 + \dots + P_rI_r$. As the I_j are homogeneous, we may also choose the P_j homogeneous. This leads to $\deg(P_j) = \deg(P) - \deg(I_j)$ for all $j = 1, \dots, r$. Now the application of Av to P yields

$$P \overset{P \in J}{=} \mathrm{Av}(P) \overset{Lemma\ 2.66}{=} I_1\,\mathrm{Av}(P_1) + \dots + I_r\,\mathrm{Av}(P_r).$$

Finally, by the prior observation, we have for all $j = 1, \dots, r$ with $\mathrm{Av}(P_j) \neq 0$ that $\deg(\mathrm{Av}(P_j)) = \deg(P) - \deg(I_j) < \deg(P)$, and can apply the induction hypothesis to $\mathrm{Av}(P_j)$ which therefore is a polynomial in $I_1, \dots, I_r$. □

There is another proof for this statement, that uses the fact that S is integral over the algebra of invariants $J = S^G$. Indeed, the presented way to prove this (still following Lehrer–Taylor [**37**, Section 3.3], but similar versions are given by, e.g., Kane [**32**, Sections 16-3 and 16-4] or Neusel–Smith [**45**, Propostion 1.7.2 and Theorem 2.1.4]) will also lead to a generalized version of Theorem 2.68. The result is often called *Theorem of Hilbert-Noether* and holds true for arbitrary fields.

First, the *elementary symmetric polynomials* are introduced as they are necessary to prove the following lemma. A good reference is Prasolov [**48**, Section 3.1], where further information on symmetric polynomials can be looked up, too.

Definition 2.69. Let R be a ring and $n > 0$. Then the *elementary symmetric polynomials* in n variables are

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \le i_1 < \dots < i_k \le n} x_{i_1} \cdots x_{i_k} \in R[x_1, \dots, x_n]$$

for $k = 1, \dots, n$.

With this definition, we can give a formula for the coefficients of a monic polynomial $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n \in R[x]$ by $(-1)^k a_k = \sigma_k(x_1, \dots, x_n)$, where $x_1, \dots, x_n$ denote its roots (cf. Prasolov [**48**, p. 77]). This is also a result of *Vieta's formula*, a well-known relation between the roots and the coefficients of a polynomial and is an essential result for the lemma below.

Lemma 2.70. *Let R be a commutative ring and let G be a finite group consisting of R-automorphisms. Denote the subring of G-invariant elements by $R^G := \{r \in R \mid g(r) = r\}$, then the ring extension $R^G \subseteq R$ is integral.*

Proof. Let $r \in R$ arbitrary, then we define the monic polynomial $f(x) := \prod_{g \in G}(x - g(r))$, which has clearly the finite set of roots $\{g(r) \mid g \in G\}$, in particular r is a root of f. By the observations above, the coefficients of f are elementary symmetric polynomials in this set of roots. Hence, in a fixed coefficient, each element $g(r)$ occurs equally often. This implies that all coefficients are G-invariant, and therefore we have $f \in R^G[x]$, which shows that r is integral over R^G. □

With this lemma and the results from Section 2.2 we have all the tools needed to prove the following proposition from which the *Theorem of Hilbert-Noether* can be concluded.

Propostion 2.71. *Let R be a finitely generated k-algebra for field k and let G be a finite group of R-automorphisms. Then the algebra of invariants R^G is a finitely generated k-algebra and the extension $R^G \subseteq R$ is finite.*

Proof. Let $r_1, \dots, r_n$ be generators for R as k-algebra. By Lemma 2.70 each of these finitely many generators is integral over R^G with polynomial f_i. We take the coefficients of all polynomials f_i as generators of a k-algebra S. This is a k-subalgebra of R^G and by construction, all r_i are integral over S. Moreover, the integral closure $\mathrm{Int}_R(S)$, i.e., the subset of elements of R that are integral over S, is a subring by Proposition 2.23 and by definition $k \subseteq S$. Hence, we have $a \cdot r_i^j \in \mathrm{Int}_R(S)$ for all $a \in k, j \in \mathbb{N}$ and $i = 1, \dots, n$ and as every element of R can be expressed as a finite sum of these terms, it follows $\mathrm{Int}_R(S) = R$, in other words, R is integral over S.
On the other hand, S is a finitely generated k-algebra and therefore isomorphic to a quotient of a polynomial ring which is Noetherian and thus it is Noetherian itself (by Hilbert's basis theorem and Atiyah–Macdonald [**1**, Proposition 6.6]). By Proposition 2.24, R is a finitely generated module over the Noetherian ring S. Hence, as shown by Atiyah–Macdonald [**1**, Proposition 6.5], R is a Noetherian module, which implies that all its

submodules, in particular R^G, are finitely generated S-modules. But since S is a finitely generated k-algebra, this shows that R^G is a finitely generated k-algebra, too.
Finally, since $k \subseteq R^G$, we have that R is of finite type over R^G and as this extension is integral by Lemma 2.70, the ring extension $R^G \subseteq R$ it is also finite by Proposition 2.24. □

Corollary 2.72 (Hilbert-Noether)**.** *Let V be a finite dimensional vector space over a field k, and let G be a finite subgroup of $GL(V)$. Then the algebra of invariants $S(V^*)^G$ is a finitely generated k-algebra and $S(V^*)^G \subseteq S(V^*)$ is finite.*

Proof. This follows immediately from Proposition 2.71 by setting $R = S(V^*)$. □

The idea for the following example is taken from a longer list of examples by Benson [**3**, Appendix A].

Example 2.73. Let $G \cong \mathbb{Z}/2\mathbb{Z}$ and V be a 2-dimensional vector space. Then G acts on $S(V^*) = \mathbb{C}[V] \cong \mathbb{C}[X_1, X_2]$ by multiplication with $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Clearly, the polynomials $y_1 = X_1^2$, $y_2 = X_2^2$ and $y_3 = X_1X_2$ are G-invariant as they contain only an even number of variables. But these are already all generators, because a polynomial $P \in S$ is G-invariant if and only if each homogeneous part of P is of even degree. Hence, every such part is a polynomial in y_1, y_2 and y_3 as these are all canonical monomials of degree 2, whence every polynomial of even degree can be build from them.

This is just a straightforward example with a pretty obvious result. However, after studying unitary reflection groups, there will be an own section (Section 3.6) devoted to the computations of more sophisticated examples.

5.2. The Cohen-Macaulay-property of the algebra of invariants. This subsection is devoted to prove that, under light restrictions, the algebra of invariants J has the nice property of being *Cohen-Macaulay*. For this purpose, we mostly follow Kane [**32**, Section 16-4] whilst sticking to the previously established notation. In this part, we deviate once more from the assumption that the base field is $\mathbb{C}$ as the proof holds true for arbitrary fields. It suffices to assume that the finite group $G \leq GL(V)$ is *non-modular*, i.e., the characteristic of the base field k does not divide $|G|$, the order of G.

Definition 2.74. A ring R is said to be *Cohen-Macaulay* (alternatively only CM) if there exists a polynomial subalgebra $k[x_1, \ldots, x_n] \subseteq R$ for a field k and a set of ring elements $\{r_1, \ldots, r_s\} \subseteq R$, such that

$$R = \bigoplus_{i=1}^{s} k[x_1, \ldots, x_n] r_i.$$

This definition can be reformulated to R being free and finite over $k[x_1, \ldots, x_n]$. Note that many authors use a different, more general property to define Cohen-Macaulay rings. That is, for a Noetherian ring the *height* of a prime ideal $\mathrm{ht}(P)$ is defined to be the dimension of the localization R_P. The *grade* (alternatively one uses depth) of P is the maximal length of a so-called *regular sequence* contained in P. That is, a sequence $r_1, \ldots, r_n \in R$, such that $(r_1, \ldots, r_n) R \neq R$ and for all $i = 0, \ldots n-1$ we have that r_{i+1} is not a zero divisor in $R/(r_1, \ldots, r_i) R$. A ring is Cohen-Macaulay if the height and the grade are equal for all prime ideals and there are even more equivalent characterizations (cf. Hochster–Roberts [**30**, p. 127–128] where several equivalent condition can be found).

Remark 2.75. The important remark made in this paper is that the definition via depth and grade of prime ideals and Definition 2.74 coincide for finitely generated graded algebras over a field k (cf. Hochster–Roberts [**30**, p. 128]). A further explanation of this equivalence is given by Hochster–Eagon [**29**, p. 1036]. They also state that there always exists a set

$\{x_1, \ldots, x_n\}$ by the Noether normalization theorem 2.26, such that R is integral and hence finite over $k[x_1, \ldots, x_n]$. This set is called a *system of parameters*, and the authors point out that its cardinality n is equal to the Krull dimension of the ring R, and that the CM-property does not depend on the chosen set of parameters, in particular the freeness does not depend on it (loc. cit.).

The above discussion shows why "[t]he CM property is basically concerned with the freeness property" (Kane [**32**, p. 175]). Note, that the finiteness follows from Proposition 2.24 and the fact that the Noether normalization yields an integral ring extension $k[x_1, \ldots, x_n] \subseteq R$. Before discussing how to prove this, we formulate the statement as the subsequent theorem. It is named after Hochster and Eagon as this result was firstly discussed in two of their papers (cf. Hochster–Roberts [**30**, p. 116]) and also proved that the algebra of invariants "is Cohen-Macaulay in various cases" (Ratliff [**49**]).

Theorem 2.76 (Hochster–Eagon)**.** *Let V be a finite dimensional vector space over an arbitrary field k and let $G \leq GL(V)$ be a finite non-modular subgroup, then the algebra of invariants $J = S(V^*)^G$ is Cohen-Macaulay.*

Proof. First, we recall that the averaging operator Av is a J-module homomorphism projecting $S = S(V^*)$ onto J (cf. Lemma 2.66) and hence produces the decomposition

$$S = J \oplus \ker \mathrm{Av}\,. \tag{4}$$

The proof will need the notion of a projective module, whence we recall the following characterization (cf. Lang [**36**, Chapter III, §4]): an R-module P is projective if and only if there exists an R-module M, such that $P \oplus M$ is a free R-module.
Furthermore, the preceding discussion has already shown, that there exists a polynomial subalgebra $k[x_1, \ldots, x_n] \subseteq J$ over which J is finite. The aim now is to prove that these properties are sufficient for J to be free over $k[x_1, \ldots, x_n]$, too. For this, the first step is to demonstrate that S is free over $k[x_1, \ldots, x_n]$.

From Proposition 2.58 we have $S \cong k[y_1, \ldots, y_n]$. So, clearly S is free over $k[y_1, \ldots, y_n]$ and $\{y_1, \ldots, y_n\}$ is a system parameters. As stated in Remark 2.75, the freeness does not depend on the chosen system of parameters. Hence, we deduce that S is free over $k[x_1, \ldots, x_n]$ as soon as we can show that $\{x_1, \ldots, x_n\}$ also forms a system of parameters. From before we already have that $k[x_1, \ldots, x_n] \subseteq J$ is finite and from Corollary 2.72 we have that $J \subseteq S$ is finite. Hence, by the transitivity of integral ring extensions (Atiyah–Macdonald [**1**, Corollary 5.4]) and Proposition 2.24 we get that $k[x_1, \ldots, x_n] \subseteq S$ is finite. As required, this shows that $\{x_1, \ldots, x_n\}$ is a system of parameters for S.
Finally, S is a free $k[x_1, \ldots, x_n]$-module and therefore (4) implies that J as well as $\ker \mathrm{Av}$ are projective $k[x_1, \ldots, x_n]$-modules. The proof is completed by the subsequent Proposition 2.79 that verifies the freeness of J, as it is a finitely generated $\mathbb{N}$-graded $k[x_1, \ldots, x_n]$-module and $k[x_1, \ldots, x_n]$ is an $\mathbb{N}$-graded connected commutative algebra over the field k. □

Note that we deviate here from Kane's proof (see [**32**, Propositon A of the Appendix] for the more general proof without assuming the module to be graded) by additionally assuming that the considered module admits a grading. This grading allows us to apply an analogues version of Nakayama's lemma 2.20 to this situation. For the rest of this section—except Lemma 2.77—we follow the ideas of Lang [**36**, Chapter X, §4].

For a graded algebra A we will use the notation $A_i := \{a \in A \mid \deg(a) = i\}$ and set $\mathfrak{m} = \bigoplus_{i \geq 1} A_i$ which is a maximal ideal of A. Recall that a *connected* algebra A is an algebra where $A_0 = k \cong A/\mathfrak{m}$. Moreover, for a graded A-module M we write $M = \bigoplus_{i \geq -n} M_i$ for some $n \in \mathbb{N}$.

Lemma 2.77. *Let A be an $\mathbb{N}$-graded connected commutative algebra over the field k. Then for any finitely generated graded A-module M we have $M = \mathfrak{m}M \Rightarrow M = 0$.*

Proof. (Serre [**55**, Chapter 4, Appendix III Lemma 1]) Take the minimal i such that $M_i \neq 0$. If no such i exists, clearly $M = 0$ is already true. But the elements of $\mathfrak{m}M_i$ have degree at least $i+1$. Hence, M_i cannot be a subset of $\mathfrak{m}M$ which is a contradiction to the assumption. □

Now we can formulate the analogues of Nakyama's Lemma 2.20 b) and c).

Lemma 2.78. *Let A be an $\mathbb{N}$-graded connected commutative algebra over the field k and let M be a graded A-module.*

(a) If $N \leq M$ is a submodule such that $M = N + \mathfrak{m}M$, then already $M = N$.
(b) If the residue classes of $x_1, \ldots, x_n$ are basis for $M/\mathfrak{m}M$, the elements $x_1, \ldots, x_n$ already generate M as an A-module.

Proof. For (a) take the quotient $M/N = (N + \mathfrak{m}M)/N = \mathfrak{m}M/N$, then by Lemma 2.77 $M/N = 0$, so $M = N$. For (b) define N to be the submodule generated by $x_1, \ldots, x_n$, then $M = N + \mathfrak{m}M$ and applying (a) to this completes the proof. □

The next proof requires the concept of exact sequences and splitting, for a definition and basic facts see Lang [**36**, Chapter III, §1–3]. Recall that if an exact sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

of modules is split exact at g, i.e., there is a homomorphism $\varphi\colon M'' \to M$ such that $g \circ \varphi = \mathrm{id}$, we can write $M = \ker g \oplus \operatorname{im} \varphi$ and $M \cong M' \oplus M''$ (cf. Lang [**36**, Chapter III, Propostion 3.2]). Moreover, the following equivalent characterization (cf. loc. cit Chapter III, §4) of projective modules will be used: an R-module P is projective if and only if every exact sequence $0 \to M' \to M'' \to P \to 0$ splits.

Propostion 2.79. *Let A be an $\mathbb{N}$-graded connected commutative algebra over the field k, then for any finitely generated graded A-module M holds: M is free if and only M is projective.*

Proof. Clearly, by the first characterization in the proof of Theorem 2.76 every free module is projective. For the converse, we claim that the elements $x_1, \ldots, x_n$ of M whose residue classes $x_i + \mathfrak{m}M$ form a basis of $M/\mathfrak{m}M$ as k-vector space are also a basis of M as A-module.
First, let F be a free A-module with basis $y_1, \ldots, y_n$ and define the homomorphism $f\colon F \to M$ by $y_i \mapsto x_i$ for all $i = 1, \ldots, n$ and extend it linearly. The aim is to show that f is an isomorphism. In order to prove this, we observe that f is already surjective by Lemma 2.78 (b). Hence, the sequence $0 \to \ker f \hookrightarrow F \xrightarrow{f} M \to 0$ is exact and splits because M is projective. Therefore, as previously observed, we get a decomposition $F = M_0 \oplus M_1$ such that $M_0 = \ker f$ and $M_1 = \operatorname{im} f \cong M$ by the surjectivity of f. Note, that since $F = \bigoplus_{i=1}^n Ae_i \cong A^n$, we can view any $x \in F$ as a vector $(a_1, \ldots, a_n)$ and set its degree to the maximum degree of its coordinates. Then $A_j F_i \subseteq F_{i+j}$ and therefore F admits a grading, that is naturally inherited by M_0.
As the residue classes $x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M$ are linearly independent, all elements of F that are mapped onto zero by f have to be a multiple of $\mathfrak{m}$: otherwise, if there was $y = a_1y_1 + \cdots + a_ny_n$ such that $f(y) = a_1x_1 + \cdots + a_nx_n = 0$ and not all $a_i \in \mathfrak{m}$, this would yield a nontrivial linear combination $a_1x_1 + \cdots + a_nx_n \equiv 0 \mod \mathfrak{m}M$ which contradicts the basis property. Hence, $M_0 \subseteq \mathfrak{m}F = \mathfrak{m}M_0 \oplus \mathfrak{m}M_1$, so in particular $M_0 \subseteq \mathfrak{m}M_0$ and hence $M_0 = \mathfrak{m}M_0$. But now by Lemma 2.77 we have $M_0 = 0$, which implies that f injective, and thus an isomorphism which confirms that M is free. □

6. The orbit space V/G as affine variety

What follows will explain why the orbit space V/G of the group action can be considered as an affine algebraic variety. Hence, the result will show why it makes sense to discuss the smoothness of the quotient V/G in the main theorem 1.1. In the preceding section we considered vector spaces over arbitrary fields. At this point, we return to our fundamental assumption that V is an n-dimensional vector space over $\mathbb{C}$, so $V \cong \mathbb{C}^n$. Moreover, we will continue to assume that G is a finite subgroup of the general linear group $GL(\mathbb{C}^n)$. For this section, we follow the path of Lamotke [**35**, Chapter II, §9] and preserve the previously introduced notations.

First, recall that by Theorem 2.68 the algebra of polynomial invariants S^G is finitely generated by polynomials $f_1, \ldots, f_r$. Additionally, in the proof became clear that these polynomials may be chosen homogeneous. Therefore, we assume that f_i is already homogeneous for all $i = 1, \ldots, r$ and set $d_i := \deg(f_i)$. Next we define a polynomial map F that consists of all these generators as components, so

$$F\colon \mathbb{C}^n \longrightarrow \mathbb{C}^r \qquad x = (x_1, \ldots, x_n)^\intercal \longmapsto (f_1(x), \ldots, f_r(x))^\intercal . \tag{5}$$

Lemma 2.80. *Let $\varphi\colon \mathbb{C}[x_1, \ldots, x_r] \to S^G$ be the map defined by $\varphi(h) = h \circ F$ with the polynomial map F from (5). Then φ is surjective.*

Proof. Since S^G is a finitely generated $\mathbb{C}$-algebra and the set $\{f_1, \ldots, f_r\}$ generates S^G, each element $f \in S^G$ can be obtained by plugging the generators into a complex polynomial in r variables. This is exactly what φ does by taking $h \circ F$. □

By taking the quotient with the kernel $k_\varphi := \ker \varphi$ of the above map we get an isomorphism

$$\mathbb{C}[x_1, \ldots, x_r]/k_\varphi \cong S^G.$$

The kernel k_φ is finitely generated as an ideal of the Noetherian ring $\mathbb{C}[x_1, \ldots, x_r]$. Moreover, S^G is an integral domain as subalgebra of the integral domain $S \cong \mathbb{C}[X_1, \ldots, X_n]$. Hence, the kernel of any map into S^G is a prime ideal, so in particular k_φ is prime. This leads to the following definition and the subsequent lemma.

Definition 2.81. Under the previous assumptions the *affine orbit vartiety*, a term coined by Lamotke [**35**, Chapter II, §9], is the variety in $\mathbb{A}^r$ defined by

$$V_{or} := \{x \in \mathbb{C}^r \mid f(x) = 0 \text{ for all } f \in k_\varphi\} .$$

Lemma 2.82. *The affine orbit variety V_{or} is an irreducible affine algebraic variety of dimension n.*

Proof. First, as prime ideals are radical, we get by the correspondence of Hilbert's Nullstellensatz 2.8 that $\mathbb{I}(V_{or}) = k_\varphi$ and $\mathbb{V}(k_\varphi) = V_{or}$. Hence, the application of Lemma 2.11 (a) shows that the variety V_{or} is irreducible since k_φ is a prime ideal.
Second, note that the coordinate ring of V_{or} is $\mathbb{C}[V_{or}] = \mathbb{C}\left[x_1, \ldots, x_r\right]/k_\varphi \cong S^G$. From this we can conclude that $\dim(V_{or}) = n$: to begin with, we utilize Lemma 2.11 (b) to get $\dim(V_{or}) = \dim(\mathbb{C}[V_{or}])$, then the above isomorphism leads to $\dim(\mathbb{C}[V_{or}]) = \dim(S^G)$. Next the extension $S^G \subseteq S \cong \mathbb{C}[x_1, \ldots, x_n]$ is integral by Lemma 2.70 and integral ring extensions have equal dimension (cf. Matsumura [**40**, Theorem 20]). Finally, the proof is completed by combining all the equalities, so $\dim(V_{or}) = \dim\left(\mathbb{C}\left[x_1, \ldots, x_n\right]\right) = n$. □

The aim for the rest of this section is to show that the orbit space V/G is homeomorphic to the orbit variety V_{or} which justifies its name. We assume some basic knowledge of topology which otherwise can be found in, inter alia, Borisovich et al. [**5**, Chapter 2]. In order to check that they are homeomorphic, we show the succeeding properties (cf. Lamotke [**35**,

Chapter II, §9, (6)–(9)]) of the polynomial map from (5), that turns a suitably restricted quotient map of the polynomial map into the desired homoemorphism.

Propostion 2.83. *The image of the polynomial map $F\colon \mathbb{C}^n \to \mathbb{C}^n$ is $F(\mathbb{C}^n) = V_{or}$, the affine orbit variety of Definition 2.81.*

Proof. First, since k_φ is the kernel of the map φ in Lemma 2.80, we have $g \circ F(x) = 0$ for all $g \in k_\varphi$ and $x \in \mathbb{C}^n$ and hence by the definition of V_{or}, it follows that $F(\mathbb{C}^n) \subseteq V_{or}$. To establish the opposite inclusion, let $a = (a_1, \dots, a_r) \in V_{or}$ arbitrary. Consider the ideal $\mathfrak{b} \trianglelefteq \mathbb{C}[x_1, \dots, x_n]$ generated by $f_1 - a_1, \dots, f_r - a_r$, where the f_i are the generators of the algebra of invariants S^G and hence the component functions of F as before. By the weak version of Hilbert's Nullstellensatz (cf. Atiyah–Macdonald [**1**, Chapter 5, exercise 17]) we get that if $\mathfrak{b} \neq \mathbb{C}[x_1, \dots, x_n]$, then the vanishing locus $\mathbb{V}(\mathfrak{b})$ is non-empty. Hence, there is a common zero $b_0 \in \mathbb{C}^n$ such that $f_i(b_0) - a_i = 0$ for all $i = 1, \dots, r$ and we get $F(b_0) = a$. In order to complete the proof, we have to show that never $\mathfrak{b} = \mathbb{C}[x_1, \dots, x_n]$. So assume equality, then one could find polynomials $p_1, \dots, p_r \in \mathbb{C}[x_1, \dots, x_n]$ with $\sum_{i=1}^r p_i(f_i - a_i) = 1$. By the invariance of the f_i, letting $g \in G$ act on this equation and taking the sum leads to $\left(\sum_{g\in G} gp_1\right)(f_1 - a_1) + \dots + \left(\sum_{g\in G} gp_r\right)(f_r - a_r) = |G|$. Now we clearly have for all $i = 1, \dots, r$ that $\sum_{g\in G} gp_i$ is G-invariant, hence, Lemma 2.80 yields a $q_i \in \mathbb{C}[x_1, \dots, x_r]$ such that $\sum_{g\in G} gp_i = q_i \circ F$. As concatenating with the polynomial map F means plugging in f_i instead of x_i, the preceding equations lead to

$$|G| = (q_1 \cdot (x_1 - a_1) + \dots + q_r \cdot (x_r - a_r)) \circ F.$$

Thus, we obtain $h \coloneqq (q_1 \cdot (x_1 - a_1) + \dots + q_1 \cdot (x_1 - a_1)) - |G| \in k_\varphi$ which implies that $h(x) = 0$ for all $x \in V_{or}$. Recall that $a \in V_{or}$ and therefore $h(a) = 0$ from what would follow that $|G| = 0$ as $0 = h(a) = 0 - |G|$, which is a contradiction. □

Lemma 2.84. *For the polynomial map F holds: $F(x) = F(y)$ if and only if there exists a $g \in G$ such that $x = gy$.*

Proof. Note that two functions mapping into multiple coordinates are equal if and only if all of their coordinate functions are equal. Then, the statement follows from Proposition 2.63 for the coordinate functions as being equal on all G-invariant polynomials is equivalent to being equal on all the generators, and these are exactly the coordinate functions of F. □

Before proving the next property of the polynomial map F we introduce an alternative way to multiply a vector $y = (y_1, \dots, y_r) \in \mathbb{C}^r$ by a scalar $t \in \mathbb{C}$. Namely, we define $s(t, y) = \left(t^{d_1} y_1, \dots, t^{d_r} y_r\right)$, where, as before, d_i denotes the degree of the generator f_i. By the homogeneity of the coordinate functions f_i, we have $F(tx) = s(t, F(x))$. This form of scalar multiplication will be used in the following lemma.

Lemma 2.85. *Set $d \coloneqq \operatorname{lcm}(d_1, \dots, d_r)$ and $a_i \coloneqq \frac{d}{d_i}$ for all $i = 1, \dots, r$. Then the map*

$$\sigma(y) = \sqrt[d]{|y_1|^{a_1} + \dots + |y_r|^{a_r}}$$

together with the above defined scalar multiplication by s defines a quasi-norm on $\mathbb{C}^r$. That is a map with the usual properties of a norm, but the normal triangle inequality is replaced by this weaker version $\|x + y\| \leq l(\|x\| + \|y\|)$ for all $x, y \in \mathbb{C}^r$ for some $l \geq 1$ (see Köthe [**33**, Chapter 3, §15.10] *for more details on this subject).*

Proof. Clearly, we have $\sigma(x) \geq 0$ for all $x \in \mathbb{C}^r$ and $\sigma(x) = 0 \Leftrightarrow x = 0$. Moreover, since $a_i \cdot d_i = d$ for all $i = 1, \dots, r$, it follows that $\sigma(s(t, x)) = \sqrt[d]{|t^{d_1} x_1|^{a_1} + \dots + |t^{d_r} x_r|^{a_r}}$ $= \sqrt[d]{|t|^d \left(|x_1|^{a_1} + \dots + |x_r|^{a_r}\right)} = |t|\, \sigma(x)$ for all $t \in \mathbb{C}$ and $x \in \mathbb{C}^r$.

Finally, we claim that $l = 2$ satisfies the weak triangle inequality. This is proven in the case that $r = 2$ but can be generalized for all $r \in \mathbb{N}$. Let $x = (x_1, x_1)^\intercal, y = (y_1, y_2)^\intercal \in \mathbb{C}^2$ arbitrary, then

$$\begin{aligned}
\sigma(x+y)^d &= |x_1+y_1|^{d_1} + |x_2+y_2|^{d_2} \overset{\text{triangle ineq.}}{\leq} (|x_1|+|y_1|)^{d_1} + (|x_2|+|y_2|)^{d_2} \\
&= \sum_{i=0}^{d_1} \binom{d_1}{i} |x_1|^i |y_1|^{d_1-i} + \sum_{i=0}^{d_2} \binom{d_2}{i} |x_2|^i |y_2|^{d_2-i} \\
&\leq \sum_{i=0}^{d_1} \binom{d_1}{i} \max(|x_1|, |y_1|)^{d_1} + \sum_{i=0}^{d_2} \binom{d_2}{i} \max(|x_2|, |y_2|)^{d_2} \\
&\leq 2^{d_1}(|x_1|^{d_1} + |y_1|^{d_1}) + 2^{d_2}(|x_2|^{d_2} + |y_2|^{d_2}) \\
&\overset{d_i \leq d}{\leq} 2^d(|x_1|^{d_1} + |x_2|^{d_2}) + 2^d(|y_1|^{d_1} + |y_2|^{d_2}) \\
&= 2^d(\sigma(x)^d + \sigma(y)^d) \leq 2^d(\sigma(x) + \sigma(y))^d.
\end{aligned}$$

Hence, the proof is completed by taking the d-th root. □

Propostion 2.86. *The polynomial map F is a proper map.*

Proof. At the outset, by the compatibility of the quasi-norm σ and the scalar multiplication by s, we have

$$\sigma(F(t \cdot x)) = \sigma(s(t, F(x))) = |t| \cdot \sigma(F(x)) \tag{6}$$

for all $t \in \mathbb{C}$ and $x \in \mathbb{C}^n$. We write $\|x\| = \sqrt{|x_1|^2 + \cdots + |x_n|^2}$ for the usual hermitean norm on $\mathbb{C}^n$ and $S^{2n-1} = \{x \in \mathbb{C}^n \mid \|x\| = 1\}$ for the compact unit sphere that belongs to the space $\mathbb{C}^n$. Since all component functions of F, the f_i, are continuous, it follows that $F\left(S^{2n-1}\right) \subseteq \mathbb{C}^r$ is also compact. Moreover the origin cannot be contained in this image: we have $F(0) = 0$ because the generators are homogeneous of degree at least one (cf. Remark 2.64), so if there was an $x \in \mathbb{C}^n$ such that $F(x) = 0$, Lemma 2.84 would imply that there is a $g \in G \leq GL(V)$ such that $gx = 0$, which is clearly a contradiction to $g \in GL(V)$. As the image $F\left(S^{2n-1}\right)$ is a compact set, we know that the minimum of σ on it is attained, and that the minimum value is greater than 0. Therefore, one may find a $\delta > 0$ such that $\sigma(F(x)) > \delta$ for all $x \in S^{2n-1}$. As each vector $x \in \mathbb{C}^n$ can be written as a multiple $t \cdot y = x$ of a vector $y \in S^{2n-1}$ and a scalar $t \in \mathbb{C}$, we get

$$\sigma(F(x)) = \sigma(F(t \cdot y)) \overset{(6)}{=} |t|\, \sigma(F(y)) > |t|\, \delta = \|x\|\delta \quad \text{for all } x \in \mathbb{C}^n. \tag{7}$$

Let $B \subseteq \mathbb{C}^r$ be an arbitrary compact set, hence, B is closed as well as it is bounded. Clearly, since F is continuous, we get that the preimage $F^{-1}(B)$ is closed, too. Furthermore, from (7) one can conclude that $F^{-1}(B)$ is bounded as well: let $r \in \mathbb{R}_{>0}$ be an upper bound for B. Then for $x \in F^{-1}(B)$ we have $F(x) \in B$ and therefore $r \geq \sigma(F(x)) > \delta\|x\|$. So, the preimage $F^{-1}(B)$ is bounded and as seen before closed, thus compact. □

Remark 2.87. In the preceding proof we considered $\mathbb{C}^n$ as an analytic space with the Euclidean topology and proved that F is proper with respect to this topology. As explained in Remark 2.30 we will show that $\mathbb{C}^n/G$ is homeomorphic to the orbit variety V_{or} in the category of analytic spaces, i.e., the homeomorphism will be with respect to the quotient topology (cf. Definition 2.28) induced by the Euclidean topology. This is valid because the category of affine varieties is naturally included in the category of analytic spaces. Afterwards, making use of Proposition 2.42 as well as Theorem 2.43, we will conclude

$\mathbb{C}/G$ and V_{or} are also homeomorphic if we equip the involved spaces with the Zariski topology as announced in Remark 2.30.

Now we get to the main result of this chapter which also justifies the notion of the *affine orbit variety.*

Theorem 2.88. *The quotient map $\overline{F}\colon \mathbb{C}^n/G \to V_{or}$ induced by the polynomial map is a homoemorphism. Hence, the orbit space $V/G \cong \mathbb{C}^n/G$ can be viewed as an affine variety.*

Proof. First, the bijectivity of $\overline{F}$ follows immediately from the combination of Proposition 2.83 and Lemma 2.84. Next, the claim is that $\overline{F}$ is a closed map, and that this suffices to prove the theorem. From this we can conclude that it is also an open map because it is bijective, and thus for the complement of an open set A holds $\overline{F}(A^c) = \overline{F}(A)^c$ which is closed, so $\overline{F}(A)$ is open. Since F is continuous, the quotient map $\overline{F}$ is continuous, too. Moreover, as $\overline{F}$ is open, its inverse $\overline{F}^{-1}$ is continuous which can be seen by observing that the preimages under $\overline{F}^{-1}$ are exactly the images of $\overline{F}$. Consequently, it only remains to demonstrate that the quotient map $\overline{F}$ is closed. As noted in Remark 2.87, the topology is the quotient topology induced by the Euclidean topology.
Take an arbitrary closed set $A \subseteq \mathbb{C}^n/G$ and let $c \in V_{or} \setminus \overline{F}(A)$. The aim is to find a neighborhood U of c such that $U \cap \overline{F}(A) = \varnothing$, then the complement $\overline{F}(A)^c$ is open. We start with the neighborhood $W = \{y \in V_{or} \mid \sigma(y) < 2\|c\|\}$. Furthermore, we define the compact set $K = \{x \in \mathbb{C}^n/G \mid \|x\| \leq 2\|c\|/\delta\}$. From (7) we get that all elements of the preimage $\overline{F}^{-1}(W)$ fulfill the inequality $\delta\|x\| < \sigma(\overline{F}(x)) < 2\|c\|$ and hence it follows that $\overline{F}^{-1}(W) \subseteq K$. Since $A \cap K$ is compact, its image $\overline{F}(A \cap K)$ is compact and thus closed. As c lies in the complement $\overline{F}(A)^c \subseteq \overline{F}(A \cap K)^c$, one can find an open set W' containing c such that $W' \cap \overline{F}(A \cap K) = \varnothing$. Then the open set $U := W \cap W'$ has the desired property to have an empty intersection with $\overline{F}(A)$: assume $y \in U \cap \overline{F}(A)$. From $\overline{F}^{-1}(W) \subseteq K$ we get $W \subseteq \overline{F}(K)$, so if $y \in U \subseteq W$ we already get $y \in W \cap \overline{F}(A) \cap \overline{F}(K) = W \cap \overline{F}(A \cap K)$, since $\overline{F}$ is bijective. But $y \in U$ also implies $y \in W'$ which has no common elements with $\overline{F}(A \cap K)$. Therefore, no such y exists and the intersection is empty, hence, the map $\overline{F}$ is closed and the proof is completed. □

After this theorem, the current situation can be illustrated by the following diagram, where $An/\mathbb{C}$ denotes the category of analytic spaces, i.e., the vanishing of analytic functions, and X^{an} stands for the *analytification* of a variety X.

$$\begin{tikzcd}
(An/\mathbb{C}) & X^{an} & \mathbb{C}^n/G \arrow[r, "\cong"] & V_{or}^{an} \\
(Var/\mathbb{C}) \arrow[u, hook] & X \arrow[u, hook] & \mathbb{A}^n/G \arrow[r, "?"] & V_{or}
\end{tikzcd}$$

Note that Theorem 2.88 allows us to view $\mathbb{C}^n/G$ as an affine variety by pulling back the structure by $\overline{F}$ because V_{or} is defined to be an affine variety. As in the introduction of varieties in Section 2.1.1, we can view $\mathbb{C}^n$ as a variety with the Zariski topology and denote it by $\mathbb{A}^n$. The action of G induces also a quotient $\mathbb{A}^n/G$ of this space whose relation to the variety V_{or} is clarified in the next corollary.

Corollary 2.89. *The orbit variety V_{or} affords the quotient topology of $\mathbb{C}^n/G$ with respect to the Zariski topology in the category of affine varieties over $\mathbb{C}$.*

Proof. To begin with, note that we have already observed in the proof of Lemma 2.82 that the coordinate ring of the orbit variety V_{or} is isomorphic to the algebra of invariant functions $S^G = \mathbb{C}[X_1, \ldots, X_n]^G$. Moreover, we have $\mathbb{C}[\mathbb{A}^n] = \mathbb{C}[X_1, \ldots, X_n]$

Therefore, if we apply Proposition 2.42 for $X = \mathbb{A}^n$, it follows that the topology of $V_{or} \cong \operatorname{Spec}(\mathbb{C}[\mathbb{A}^n]^G)$ is the quotient topology induced by the Zariski topology and that its underlying set it the the of G-orbits. By the very definition, the topological space $\mathbb{A}^n/G$ is exactly this set of G-orbits with the quotient topology induced by the Zariski topology. We remark that the group $G \leq GL(V)$ is a linear algebraic group according to Example 2.32, and as it acts linearly on V, it also follows that the action is regular. So, by applying Theorem 2.43 to the same scenario as above, we obtain that V_{or} is a geometric quotient, and hence the type of quotient in the category of varieties that is compatible with quotients of topological spaces (cf. Remark 2.34). The combination of all the previous arguments yields that V_{or} affords the quotient topology of $\mathbb{A}^n/G$, i.e., the quotient topology of $\mathbb{C}^n/G$ with respect to the Zariski topology. □

Remark 2.90. As already seen in the preceding proof, the coordinate ring of the affine orbit variety V_{or} and thereby also of V/G is isomorphic to the algebra of invariant polynomials $S^G = S(V^*)^G = \mathbb{C}[V]^G$. Since we are interested in the variety V/G and not V^*/G, this is the reason why $S(V^*)$ and not $S(V) = \mathbb{C}[V^*]$ is considered (cf. Thiel [**64**, 13.11]). Later on, with another definition we will be able to state in which sense these quotients can differ (cf. Remark 3.23).

This final section and thereby the second chapter will be finished by indicating that conjugated subgroups admit isomorphic orbit varieties. Hence, only a single representative for each conjugacy class has to be viewed in the following considerations.

Propostion 2.91. *Let G and G' be conjugate subgroups of $GL(\mathbb{C}^n)$ and denote the corresponding orbit varieties by V_{or} and V'_{or} respectively. Then the orbit varieties are isomorphic.*

Proof. To begin with, let $h \in GL(\mathbb{C}^n)$ such that $G' = hGh^{-1}$. Since G' is also a finite subgroup of the general linear group, there exist s generators for the algebra of G'-invariants. Hence, as in Equation (5), a polynomial map $F' \colon \mathbb{C}^n \to \mathbb{C}^s$ exists and the orbit variety V'_{or} is defined as in Definition 2.81 for the G'-action. Furthermore, Proposition 2.83 leads to $F'(\mathbb{C}^n) = V'_{or}$. We claim that the following diagram is commutative.

$$\begin{tikzcd}
\mathbb{C}^n \arrow[r, "h"] \arrow[d, "F"] & \mathbb{C}^n \arrow[r, "h^{-1}"] \arrow[d, "F'"] & \mathbb{C}^n \arrow[d, "F"] \\
\mathbb{C}^r \arrow[r, "\Phi"] & \mathbb{C}^s \arrow[r, "\Psi"] & \mathbb{C}^r
\end{tikzcd}$$

In order to prove this, we point out how to obtain the component functions φ_i and ψ_j of Φ and Ψ. From this we will see that both smaller rectangles are commutative. The first step is to show that $f'_i \circ h$ is G-invariant for an arbitrary component function f'_i of F': let $x \in \mathbb{C}^n$ and $g \in G$ arbitrary, then we have by definition $g(f'_i \circ h(x)) = f'_i(h(g^{-1}(x)))$. Since $hG = G'h$, there exists $g' \in G'$ such that $h \circ g^{-1} = g' \circ h$, so we get

$$f'_i(h(g^{-1}(x))) = f'_i(g' \circ h(x)) = (h^{-1}(g')^{-1})(f'_i(x)) = h^{-1}((g')^{-1}(f'_i(x))) = h^{-1}(f'_i(x)),$$

where the second equality is due to the definition of the group action and the identity $g'h = (h^{-1}(g')^{-1})^{-1}$. Then the associativity of the group action and finally the G'-invariance of f'_i are applied. Note that by definition $h^{-1}(f'_i(x)) = f'_i \circ h(x)$, hence, the G-invariance is shown. Clearly, one can show that $f_j \circ h^{-1}$ is G'-invariant in the same way. Now since the components of the polynomial map are the generators of the algebra of invariants, there is a polynomial $\varphi_i \in \mathbb{C}[x_1, \ldots, x_r]$ such that $f'_i \circ h = F \circ \varphi_i$ and similarly $f_j \circ h^{-1} = F' \circ \psi_j$ for a polynomial $\psi_j \in \mathbb{C}[x_1, \ldots, x_s]$ (cf. Lemma 2.80). Therefore, the diagram is commutative.

To terminate the proof, we observe that the outer rectangle implies that

$$F = F \circ h^{-1} \circ h = \Psi \circ \Phi \circ F.$$

As F is surjective by Proposition 2.83, it is right-cancellative, hence, it follows that $\mathrm{id} = \Psi \circ \Phi$. The same considerations with interchanged roles for G and G' and the corresponding polynomial maps leads to $\mathrm{id} = \Phi \circ \Psi$. Hence, the restriction $\Phi|_{V_{or}}$ is an isomorphism between the affine orbit varieties V_{or} and V'_{or} with inverse $\Psi|_{V'_{or}}$. $\square$

CHAPTER 3

The Shephard-Todd-Chevalley-Serre Theorem

In this third chapter the aforementioned main theorem 1.1 whose intriguing history was already presented in Section 1.4 shall be proven. This will be accomplished in several steps as each implication needs its own toolkit. But first of all, we have to introduce the object of unitary reflection groups and various important facts about them.

Subsequently, it will be shown that a unitary reflection group implies that the corresponding algebra of invariants is polynomial. The key part of the necessary toolkit for this proof is a lemma by Chevalley [**12**] that made it possible to provide a case-free proof. Next, the converse will be proven. For this intention, a bigger toolkit including Poincaré series and Molien's theorem [**43**] are required. Lastly, we will demonstrate the equivalence between the algebra of invariants S^G being polynomial and the orbit space V/G being a smooth variety. For this step, a larger toolkit of homological algebra is required, the main part will be a theorem of Auslander–Buchsbaum [**2**] which states that regular local rings are of finite global dimension, and the relation between finite global dimension and being polynomial given by Serre [**55**].

In order to finalize this chapter, the last section will be devoted to some explicit computations of generating systems of invariants. Here, the so-called *exceptional groups* are of particular interest.

1. Key facts about unitary reflection groups

The following first section will treat the foundational object of a unitary reflection group as well as the notion of a root of a reflection. Moreover, we will provide a formula that will later allow us to describe the action of a reflection group on a vector space. For this purpose, we follow Lehrer–Taylor [**37**, Sections 1.1 and 1.2.]. Finally, there will be a short overview on group representations and modules over a group.

At first, we recall the definition of a *Hermitian form* that may already be known from linear algebra.

Definition 3.1. Let V be an n-dimensional vector space over the complex numbers $\mathbb{C}$, then a map $(-,-) : V \times V \to \mathbb{C}$ is called *Hermitian* if

$$(v_1 + v_2, w) = (v_1, w) + (v_2, w)\,, \quad (av, w) = a\,(v, w) \quad \text{and} \quad \overline{(v, w)} = (w, v)$$

for all $v_1, v_2, v, w \in V$ and $a \in \mathbb{C}$. Moreover, it is called *positive definite* if $(v, v) \geq 0$ for all $v \in V$, and $(v, v) = 0$ if and only if $v = 0$.

For example, the standard scalar product $(v, w) = v_1\overline{w}_1 + \cdots + v_n\overline{w}_n$ on $\mathbb{C}^n$ is a positive definite Hermitian form.

Definition 3.2. Let V be an n-dimensional vector space and G be a subgroup of $GL(V)$. A Hermitian form is called *G-invariant*, if

$$(gv, gw) = (v, w) \quad \text{for all } g \in G \text{ and all } v \in V.$$

Remark 3.3. On a vector space V with a given positive definite Hermitian form $[-,-]$, there always exists a G-invariant positive definite Hermitian form as long as the subgroup $G \leq GL(V)$ is finite. This is achieved by defining $(v,w) \coloneqq \sum_{g\in G}[gv,gw]$. The rest follows from an elementary computation; more details are given in Lehrer–Taylor [**37**, Lemma 1.3].

Henceforward, V will always denote an n-dimensional vector space over $\mathbb{C}$ and $(-,-)$ will be a positive definite Hermitian form.

Definition 3.4. Let $g \in GL(V)$. Then we shall say that g is *unitary* if $(gv,gw) = (v,w)$ for all $v,w \in V$. In other words, the form $(-,-)$ is $\langle g\rangle$-invariant. The group of all unitary elements of this form is denoted by $U(V)$.

Consider the matrix M of a unitary element g with respect to an orthonormal basis of V, then we have $M\overline{M}^{\intercal} = I$, where I denotes the identity matrix. The group of all these unitary matrices is denoted by $U_n(\mathbb{C})$, where $n = \dim(V)$.

Note that the group $U(V)$ depends on the form $(-,-)$. However, for two arbitrary forms $(-,-)$ and $[-,-]$, there exists an isomorphism $\varphi\colon V \to V$ such that $(v,w) = [\varphi(v),\varphi(w)]$ for all $v,w \in V$. We say that the forms are *equivalent*. Therefore, the group $U(V)$ is unique up to conjugation in $GL(V)$. Moreover, every finite subgroup of $GL(V)$ is unitary with respect to a suitable form due to Remark 3.3 and hence a subgroup of $U(V)$.

Definition 3.5. For a subset $U \subseteq V$ the *orthogonal complement* $U^{\perp}$ is defined to be the subspace $U^{\perp} \coloneqq \{v \in V \mid (u,v) = 0 \text{ for all } u \in U\}$.

For subspaces $U,W \subseteq V$ we write $U \perp V$, if $V = U \oplus W$ and $(u,w) = 0$ for all $u \in U$ and $w \in W$. A proof that $U^{\perp}$ is in fact a complement of the subspace U is given, e. g., by L. Smith [**62**, Proposition 15.4.2]. Therefore, we have $U \perp W \Leftrightarrow W = U^{\perp}$.

Subsequently, further definitions need to be established to allow us to define the term of a unitary reflection.

Definition 3.6. Let $1 \in GL(V)$ be the identity element on G and let $g \in GL(V)$ and $H \subseteq GL(V)$, then

(a) the *space of fixed points* of g is $\operatorname{Fix} g \coloneqq \ker(1-g) = \{v \in V \mid gv = v\}$;
(b) the *space of fixed points* of H is $V^H \coloneqq \operatorname{Fix}_V(H) \coloneqq \{v \in V \mid hv = v \text{ for all } h \in H\}$;
(c) and the *shifting space* of g is $[V,g] \coloneqq \operatorname{im}(1-g)$.

Lemma 3.7. *For $g \in U(V)$ holds $[V,g] = (\operatorname{Fix} g)^{\perp}$.*

Proof. See Lehrer–Taylor [**37**, Lemma 1.6]. □

At this point, we can define what we mean by a *(unitary) reflection*.

Definition 3.8. A linear map $g \in GL(V)$ will be called a *reflection*, if g is of finite order and if $\dim([V,g]) = 1$. If even $g \in U(V)$, we shall say that g is a *unitary reflection*.

Remark 3.9. We observe that for a reflection g the space of fixed points $\operatorname{Fix} g$ is of codimension 1 and hence a hyperplane, which is called the *reflecting hyperplane*. Moreover, $\dim([V,g]) = 1$ implies that there is a nonzero vector $a \in V$ such that $v - gv = c_v \cdot a$ for a $c_v \in \mathbb{C}$ for all $v \in V$. Thus, a function $\varphi\colon V \to \mathbb{C}$ can be defined by $\varphi(v) \coloneqq c_v$, and it follows that $\operatorname{Fix} g = \ker \varphi$.

Remark 3.10. For a unitary reflection, Lemma 3.7 implies that $[V,g] = (\operatorname{Fix} g)^{\perp}$. But, by Remark 3.3 we already have that any reflection g is unitary for a suitable form $(-,-)$ since g is of finite order m and hence $\langle g\rangle$ is finite. Choosing a basis adapted to the decomposition $V = (\operatorname{Fix} g)^{\perp} \perp \operatorname{Fix} g$ results in the matrix g being $\operatorname{diag}(\zeta,1,\ldots,1)$ for a primitive m^{th} root of unity ζ.

This demonstrates that the matrixes of such form already are unitary reflection which remain true in the one-dimensional case where the matrices only consist of a single entry ζ and the reflecting hypereplane is the origin.

After observing that the one-dimensional space $[V, g]$ is spanned by a single vector a, we will establish a name for a to be able to use this property, for exmaple, to compute the value of a reflection.

Definition 3.11. Let ℓ be a line in V, i.e., ℓ is a one-dimensional subspae of V, then any nonzero vector of ℓ is called a *root* of this line. For a unitary reflection the root of $[V, g]$ is defined to be the root of g, too.

With the terms introduced earlier, we are now able to define the main object of consideration.

Definition 3.12. A finite subgroup of the unitary group $U(V)$ which is generated by reflections is a called a *unitary reflection group*.

Note that several authors refer to unitary reflections and the corresponding groups as *complex* reflections, and *complex* reflection groups, respectively. Furthermore, some authors, e. g., Kane [**32**] call what we have introduced as reflection a pseudo-reflection, and use the notion of reflections only for real (orthogonal) reflections.

Another important observation is that it is only relevant that the generators are reflections, since a suitable Hermitian form can always be found as seen in Remark 3.3. In other words, being a finite group generated by reflections suffices for being a unitary reflection group.

Example 3.13. This example shall be seen as a warning that a group generated by finitely many reflections is not immediately a reflection group. Let $V = \mathbb{C}^2$ and consider

$$r_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \; r_2 = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}.$$

It is easy to compute that $\operatorname{rk}(1 - r_1) = 1$ and $\operatorname{rk}(1 - r_2) = 1$ and that both are of order 2. Hence, they are reflections. Nevertheless, the group $\langle r_1, r_2 \rangle$ is infinite, since

$$r_1 r_2 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \text{ and thus } (r_1 r_2)^k = \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix},$$

which is of infinite order.

Next, a formula to calculate the values of a vector v under a reflection r will be provided. For this, we proceed as follows: given a hyperplane $H \subseteq V$ let $v_1, \ldots, v_{n-1}$ be a basis of H and extend it to a basis of V by adding a matching $w \in V$. Then, the linear map $L_H \colon V \to \mathbb{C}$ defined by $L_H(w) = \lambda \in \mathbb{C} \setminus \{0\}$ and $L_H(v_i) = 0$ for all $i = 1, \ldots, n-1$ has the kernel $\ker L_H = H$.

Lemma 3.14. *Let $r \in GL(V)$ be a reflection of order m, set $H \coloneqq \operatorname{Fix} r$ and take $a \in V$ as a basis of the line $[V, g]$. Using the above defined map L_H one can find a primitive m^{th} root of unity α such that for all $v \in V$ holds*

$$rv = v - (1 - \alpha) \frac{L_H(v)}{L_H(a)} a.$$

Proof. As seen in Remark 3.9, there is a map $\varphi \in V^*$ such that $v - rv = \varphi(v)a$, so equivalently $rv = v - \varphi(v)a$. Moreover, this linear function fulfills $H = \ker \varphi$ and $a \notin H$, since a is an eigenvector of r corresponding to an eigenvalue distinct from 1: first, $a \in [V, g]$, hence, $a = v - rv$ for some $v \in V$. Then we have $ra = rv - r^2 v = 1\,(rv) - r\,(rv) \in [V, g]$,

and therefore $ra = \alpha a$ for some complex number $\alpha \neq 1$ because r is of order m, which implies that α is a primitive m^{th} root of unity.
From $ra = a - \varphi(a)a = \alpha a$, it follows that $\varphi(a) = 1 - \alpha$. Subsequently, from the construction of L_H before the statement of the lemma, it becomes clear that $\varphi = \lambda L_H$ for some nonzero $\lambda \in \mathbb{C}$ and as $\varphi(a) = 1 - \alpha = \lambda L_H(a)$, we get that $\lambda = \frac{(1-\alpha)}{L_H(a)}$. Finally, plug in $\varphi(v) = (1-\alpha)\,\frac{L_H(v)}{L_H(a)}$ to obtain the desired formula. □

This formula can be even simplified, if r is a unitary reflection and the root a is assumed to have length 1, i. e., $(a, a) = 1$.

Corollary 3.15. *Let $r \in U(V)$ be a unitary reflection of order m and let a be a root of r of length 1. Then, there exists a primitive m^{th} root of unity α such that for all $v \in V$ holds*

$$rv = v - (1-\alpha)\,(v, a)\,a.$$

Proof. By Lemma 3.7 we have $H \perp [V, g]$ and can conclude from this that $(-, a)$ has the desired properties for L_H. □

This demonstrates that it suffices to take a nonzero vector and a primitive root of unity to construct a unitary reflection. The following definition is motivated by this observation.

Definition 3.16. Let $a \in V$ be a nonzero vector and let α be a primitive m^{th} root of unity. Then a unitary reflection $r_{a,\alpha} \in U(V)$ is given by

$$r_{a,\alpha}(v) \coloneqq v - (1-\alpha)\,\frac{(v, a)}{(a, a)}a.$$

Subsequently, there will be a short part on representation theory elaborating several necessary definitions to talk about some of the considered objects in a more precise way. The general assumption that V is an n-dimensional vector space over $\mathbb{C}$ is maintained. The following is a collection of the necessary concepts taken from Lehrer–Taylor [**37**, Sections 1.4, 1.5, 1.7 and 2.1], for a detailed look at representation theory see Lang [**36**, Chapters XVII and XVIII].

Definition 3.17. A *linear representation* of a group G in the space V is a homomorphism $\rho\colon G \to GL(V)$. It is called *faithful* if ρ is injective.

Definition 3.18. For such a representation, we can let G act on V via $gv \coloneqq \rho(g)v$. In this situation, we say that V is a *G-module*. Furthermore, if there is a subspace $U \subseteq V$ with the property that $gu \in U$ for all $g \in G$ we say that U is a *G-submodule* of V.

Clearly, the trivial subspaces 0 and V itself are always also a *G-submodule*, but if these two are the only ones, we say that V is an *irreducible* G-module. In the following, we will equip reflection groups with the property of being irreducible.

Definition 3.19. Let G be a unitary reflection group in $U(V)$, then the *natural representation* of G is defined to be the G-module V. If V is irreducible as G-module, we say that G is an *irreducible unitary reflection group*.

In what follows, the character of a group—an important object of representation theory—is introduced because it will later occur in Lemma 3.39 leading to the proof of Molien's forumula (Theorem 3.40).

Definition 3.20. For a subgroup $G \leq GL(V)$ we define the *character* of $g \in G$ to be the function $\chi\colon G \to \mathbb{C}$ mapping $g \in G$ onto its trace, i. e., $\chi(g) \coloneqq \operatorname{tr}(g)$. If V is an irreducible G-module we also say that the character χ is irreducible. This definition can be extended to any group by taking a representation in a space V and setting $\chi(g) = \operatorname{tr}(\rho(g))$.

According to Maschke's theorem (Lehrer–Taylor [**37**, Theorem 1.24]) the representation space V of a finite group G is a direct sum of irreducible components $V = \bigoplus_{i=1}^{m} V_i$.

Definition 3.21. If χ is a character afforded by the subspace V_j in the preceding decomposition we define the *isotypic component* of χ in V to be

$$V_\chi := \bigoplus_{k\colon V_k \cong V_j} V_k.$$

As already indicated in Section 1.4.1, there is a decomposition as a direct product into irreducible unitary reflection groups for every unitary reflection group. However, there exists an even stronger result than in the reference which was given a that point. The following is an improved formulation (cf. Thiel [**65**, Proposition 2.38]) of Theorem 1.27 by Lehrer–Taylor [**37**] where the proof may be found.

Propostion 3.22. *If G is a unitary reflection group acting on the vector space V, then there is an orthogonal decomposition $V = V^G \perp V_1 \perp \cdots \perp V_r$, where V^G denotes the space of fixed points under the action of G, i.e., $gv = v$ for all $g \in G$. Furthermore, there is a direct product decomposition such that*

$$G = G_1 \times \cdots \times G_r$$

and each factor G_i acts as a unitary reflection group on V_i, and as the identity on all other V_j with $j \neq i$.

As a final remark, we can now elaborate on the difference between $S(V^*)$ and $S(V)$, which was already announced in Remark 2.90.

Remark 3.23. To be able to provide a nice counterexample, we deviate from the assumption that the base field is the complex numbers $\mathbb{C}$ and interchange it only for this remark with an arbitrary field k. We have that $k[V] = S(V^*)$ and $k[V^*] = S(V)$ are isomorphic k-algebras. However, they are not necessarily isomorphic as G-modules. There exists an interesting example by Derksen–Kemper [**17**, 3.7.10] where, on the one hand $k[V^*]^G = S(V)^G$ is a polynomial ring whilst, on the other hand, $k[V]^G = S(V^*)^G$ is not even a Cohen-Macaulay-ring; according to Theorem 2.76 this is only possible in the modular case. Hence, there is a difference and since we are interested in V/G and therefore in its coordinate ring $S(V^*)^G$, we only concentrate on exactly this ring (cf. Thiel [**64**, 13.11]).

2. The main theorem

After an exposition of the provenance of the main theorem was already given in Section 1.4, we now only recall the statement itself to prepare the proofs it in the subsequent sections.

Theorem 3.24 (Shephard–Todd–Chevalley–Serre)**.** *For a finite dimensional vector space V over the complex numbers $\mathbb{C}$ and a finite subgroup $G \leq GL(V)$ the following are equivalent:*

(a) The group G is a unitary reflection group.
(b) The algebra of G-invariant polynomials $S^G := \mathbb{C}[V]^G$ is a polynomial algebra.
(c) The orbit space V/G is a smooth variety.

3. Chevalley's lemma and the proof of (a) ⇒ (b)

The aim of this section is to provide a proof for the first implication (a) ⇒ (b) of the main theorem. In the course of the proof, the key steps will involve investigating the action of a

reflection on the polynomial algebra $S(V^*)$ and proving an important auxiliary lemma that was originally established by Chevalley. Then, the proof can be executed and the section is concluded by a result on a certain type of uniqueness of the *fundamental invariants*, a specific type of generators. For this purpose, we follow the exposition of Lehrer–Taylor [**37**, Sections 3.4 and 3.5] who in turn mostly present Chevalley's [**12**] results.

In this section, the algebra of polynomials on the vector space V will be denoted by $S := S(V^*)$ and its subalgebra of G-invariant polynomials for a subgroup $G \leq GL(V)$ is denominated by $J = S^G$. Recall that we already know from Theorem 2.68 that J is a finitely generated $\mathbb{C}$-algebra, and a Cohen-Macaulay-ring by Theorem 2.76. But now the assumption that G is a unitary reflection group is added which will lead to an even stronger result, namely that J is a polynomial algebra.

First, we will have a look at the action of a a reflection on a polynomial $P \in S$.

Lemma 3.25. *Let $r \in GL(V)$ be a reflection, let $H := \operatorname{Fix} r$ be the corresponding hyperplane, and take $L_H \in V^*$ as in Lemma 3.14. Then for all polynomials $P \in S$, one can find a polynomial $Q \in S$ such that*

$$rP = P + L_H Q.$$

Proof. We will proceed in the following way: in the first place, we show that an equation of this type holds for an arbitrary element of V^*. Then we will demonstrate that this relation is also satisfied for the product P_1P_2 for $P_1, P_2 \in S$ if it is already fulfilled in each case. Since S is generated by V^* as an algebra as well as r and L_H are linear, the multiplicativity of P_1 and P_2 to be shown suffices to prove the lemma for all $P \in S$.
Due to the formula in Lemma 3.14, it is straightforward to compute that there is an $\alpha_k \in \mathbb{C}$ for all $k \in \mathbb{N}$ such that $r^k v = v + \alpha_k L_H(v)a$ for a fixed root a of the reflection r. Using the identity $r^{-1} = r^{\operatorname{ord}(r)-1}$ yields a $\beta \in \mathbb{C}$ such that for all $v \in V$ holds $r^{-1}(v) = v + \beta L_H(v)a$. View an arbitrary $\varphi \in V^*$ as an element of S, then by the definition of the G-action on S we have $r\varphi(v) = \varphi\left(r^{-1}(v)\right) = \varphi(v) + \beta L_H(v)\varphi(a)$. Hence, $r\varphi - \varphi = L_H\beta'$ for a $\beta' \in \mathbb{C}$, which is also a polynomial in S of degree 0.
Next, assuming that for $P_1, P_2 \in S$ the matching polynomials Q_1, Q_2 with $rP_1 = P_1 + L_H Q_1$ and $rP_2 = P_2 + L_H Q_2$ have already been found, we can conclude that

$$\begin{aligned} r(P_1P_2) - P_1P_2 &= r(P_1)\cdot r(P_2) + P_1P_2 = r(P_1)\left(r(P_2) - P_2\right) + \left(r(P_1) - P_1\right)P_2 \\ &= r(P_1)L_HQ_2 + L_HQ_1P_2 = L_H\left(r(P_1)Q_2 + Q_1P_2\right). \end{aligned}$$

Thus, the equation also holds for the product P_1P_2 and whence for all $P \in S$ as mentioned in the beginning. □

Before the next lemma, recall from Remark 2.64 that J^+ denotes the G-invariant polynomials with constant term 0, and that the ideal of S generated by this set is denominated by F. These objects will play an important role in the next lemma, which is "the key technical tool needed in Chevalley's proof" (Lehrer–Taylor [**37**, p. 47]) of the desired implication.

Lemma 3.26. *Let G be a unitary reflection group, in particular G is finite. Suppose that there are homogeneous $U_1, \ldots, U_r \in J$ such that U_1 does not lie in the ideal $(U_2, \ldots, U_r)$ of J. Presume there are homogeneous $P_1, \ldots, P_r \in S$ such that*

$$P_1U_1 + \cdots + P_rU_r = 0, \tag{8}$$

then we have that $P_1 \in F$, i.e., P_1 has constant term 0.

Proof. We will prove this by induction on $d := \deg(P_1)$. If $d = 0$ and if we assume P_1 is a nonzero constant polynomial, we get for the averaging operator (cf. Definition 2.65) that $\mathrm{Av}(P_1) = P_1$. But applying Av to (8) leads to $\mathrm{Av}(P_1)U_1 + \cdots + \mathrm{Av}(P_r)U_r = 0$ because the averaging operator is a homomorphism (cf. Lemma 2.66). This would imply that $U_1 \in (U_2, \ldots, U_r)$, contradictory to the assumption. Hence, in the following let $d > 0$.
The case $G = 1$ can be settled because then $J = S$ and $J^+ = F$, so $P_1 \in F$. Otherwise, there is a complex reflection r in G with a corresponding linear map L_H. First, let r act on the equation (8) and then substract (8) from the previously obtained result to obtain—using the invariance of the U_i and the equality of $r(P_iU_i) = (rP_i)(rU_i) = (rP_i)U_i$—that

$$(rP_1 - P_1)\,U_1 + \ldots (rP_1 - P_1)\,U_1 = 0.$$

From Lemma 3.25, it follows that for all P_i there is a homogeneous polynomial $Q_i \in S$ such that $rP_i - P_i = L_H Q_i$. Moreover, since $L_H \in V^*$ is a polynomial of degree 1, it must be $\deg(Q_i) < \deg(P_i)$. As $L_H \neq 0$, we get by canceling it out that

$$Q_1U_1 + \ldots Q_rU_r = 0.$$

Due to the lowered degrees, it follows by induction that $Q_1 \in F$. Hence, we also get that $rP_1 - P_1 = L_H Q_1 \in F$, or in other words, $rP_1 \equiv P_1 \mod F$. By definition, all generators of the group G have the same form as the reflection r, which leads to $gP_1 \equiv P_1 \mod F$ for all $g \in G$. Now, from the definition of the averaging operator we can conclude that $\mathrm{Av}(P_1) \equiv P_1 \mod F$. As P_1 is of strictly positive degree as well as $\mathrm{Av}(P_1)$ is G-invariant and either 0 or of the same degree as P_1 and therefore in F, it follows $P_1 \in F$. □

Before proving the most important result, i.e., the implication (a) ⇒ (b) of the main theorem we need a formula that will be used to attain this result. For the subsequent lemma we follow the ideas of Courant–John [**14**, p. 120] adopted to the situation of polynomials and formal derivatives.

Lemma 3.27 (Euler's formula)**.** *Let $P \in S$ be a homogeneous polynomial in n variables and of degree d. Then the partial differential equation*

$$X_1 \frac{\partial P}{\partial X_1} + \cdots + X_n \frac{\partial P}{\partial X_n} = d \cdot P\,(X_1, \ldots, X_n)$$

is fulfilled.

Proof. Take an arbitrary $t \in \mathbb{C}$, then by the homogeneity of the polynomial P holds $P\,(tX_1, \ldots, tX_n) = t^d P\,(X_1, \ldots, X_n)$. Now, this equation is formally differentiated with respect to t yielding

$$X_1 \frac{\partial P\,(tX_1, \ldots, tX_n)}{\partial X_1} + \cdots + X_n \frac{\partial P\,(tX_1, \ldots, tX_n)}{\partial X_n} = d \cdot t^{d-1} P\,(X_1, \ldots, X_n)$$

due to the multivariate chain rule (cf. Courant–John [**14**, p. 55 equation (18)]) for the left hand side. Finally, the proof is completed by setting $t = 1$. □

With this lemma all the necessary tools to prove the implication (a) ⇒ (b) are established. Hence, we can subsequently prove it in the way it was initially given by Chevalley [**12**] following an expostion of Lehrer–Taylor [**37**, Section 3.5].

Theorem 3.28. *Let G be a unitary reflection group (hence finite) of the n-dimensional vector space V. Then the algebra $J := S^G$ of G-invariant polynomials is a polynomial algebra, that is, it is generated by algebraically independent homogeneous polynomials.*

Proof. Let $I_1, \ldots, I_r$ be a minimal set of homogeneous generators of the ideal $F := SJ^+$ of S, which in turn also generates J as seen in the proof of Theorem 2.68. First of all, observe that if this set is algebraically independent in the sense of Definition 2.25, it turns

the canonical map $\mathbb{C}[Y_1, \dots, Y_r] \to \mathbb{C}[I_1, \dots, I_r]$ injective. Since it is a generating set, this map is surjective as well. So, to prove the algebraic independence is in fact equivalent to proving that J is isomorphic to a polynomial ring.
Next, assume that the generating set $I_1, \dots, I_r$ is algebraically dependent. The aim is to demonstrate that under this assumption there already exists a smaller set of generators, contradictory to the presumed minimality of r. Due to the algebraic dependence, one can find a nonzero polynomial $H \in \mathbb{C}[Y_1, \dots, Y_r]$ that fulfills $H(I_1, \dots, I_r) = 0$. We set $d_i := \deg(I_i)$ for all $i = 1, \dots, r$ and define k_i as the exponents of the monomials $Y_1^{k_1} \cdots Y_r^{k_r}$ occurring in H. As all monomials are canceled out by plugging in $I_1, \dots, I_r$, it is justified to assume that there is an integer h such that $h = k_1 d_1 + \cdots + k_r d_r$ for all monomials. Moreover, we assume H to be chosen such that h is minimal.
Subsequently, we denominate the partial derivatives of H by $H_i := \frac{\partial H}{\partial Y_i}$ for all $i = 1, \dots, r$. If the generators are plugged in, we denote them by $U_i := H_i(I_1, \dots, I_r)$. Since all the I_i are G-invariant and as this property is preserved under multiplication and addition, it follows that all the U_i lie in J. There must be a nonzero partial derivative H_j because otherwise we would have that H is constant but then $H(I_1, \dots, I_r) = 0$ is only true for $H = 0$ which has already been excluded before. Moreover, for a nonzero H_j we have that the corresponding U_j is nonzero, else $k_1 d_1 + \cdots + (k_j - 1) d_j + \cdots + k_r d_r < h$ contradicts the minimality of h.
We may rename the U_i so that the ideal $(U_1, \dots U_r) \trianglelefteq J$ is generated by $U_1, \dots, U_s$ and such that this choice of $s \leq r$ is minimal. Therefore, one can find G-invariant homogeneous polynomials V_{kj} with such that for all $k > s$

$$U_k = \sum_{j=1}^{s} V_{kj} U_j. \tag{9}$$

Since $\deg(U_i) = h - d_i$ for all $U_i \neq 0$, the polynomials V_{kj} must satisfy $\deg(V_{kj}) = d_j - d_k$. Next, as differentiating 0 with respect to an arbitrary variable remains 0 and it holds $H(I_1, \dots, I_r) = 0$, we have for all $i = 1, \dots, n$ that

$$\begin{aligned} 0 = \frac{\partial H(I_1, \dots, I_r)}{\partial X_i} &\overset{\text{chain rule}}{=} \sum_{j=1}^{r} U_j \frac{\partial I_j}{\partial X_i} = \sum_{j=1}^{s} U_j \frac{\partial I_j}{\partial X_i} + \sum_{j=s+1}^{r} U_j \frac{\partial I_j}{\partial X_i} \\ &\overset{(9)}{=} \sum_{j=1}^{s} U_j \frac{\partial I_j}{\partial X_i} + \sum_{k=s+1}^{r} \sum_{j=1}^{s} V_{kj} U_j \frac{\partial I_k}{\partial X_i} = \sum_{j=1}^{s} U_j \left(\frac{\partial I_j}{\partial X_i} + \sum_{k=s+1}^{r} V_{kj} \frac{\partial I_k}{\partial X_i} \right). \end{aligned}$$

Since the indices are renamed such that s is minimal, we get that the polynomial U_j is not contained in the ideal generated by the set $\{U_1, \dots, U_s\} \setminus \{U_j\}$ for all $j \leq s$. Therefore, we can apply Lemma 3.26 to the preceding formula to obtain that

$$\frac{\partial I_j}{\partial X_i} + \sum_{k=s+1}^{r} V_{kj} \frac{\partial I_k}{\partial X_i} \in F$$

for all $j = 1, \dots, s$ and $i = 1, \dots, n$. Clearly, the first summand is of degree $d_j - 1$ and for the second summand we get the same result as $\deg(V_{kj}) + d_k - 1 = d_j - d_k + d_k - 1 = d_j - 1$. So, it is also generated by the I_i and we can write

$$\frac{\partial I_j}{\partial X_i} + \sum_{k=s+1}^{r} V_{kj} \frac{\partial I_k}{\partial X_i} = \sum_{\ell=1}^{r} B_{ij\ell} I_\ell, \tag{10}$$

where the $B_{ij\ell} \in S$ are homogeneous and $B_{ij\ell} = 0$ for all ℓ with $d_\ell \geq d_j$ due to the homogeneity of the I_i and the earlier calculated degree. Recall that the partial derivatives

satisfy

$$\sum_{i=1}^{n} X_i \frac{\partial I_j}{\partial X_i} = d_j I_j$$

by Euler's formula (cf. Lemma 3.27). Hence, if we initially multiply (10) by X_i and then form the sum over i since all the earlier results are valid for all $i = 1, \dots, r$, this leads too.

$$d_j I_j + \sum_{k=s+1}^{r} V_{kj} d_k I_k = \sum_{\ell=1}^{r} A_\ell I_\ell.$$

Since $B_{ij\ell} = 0$ for $j = \ell$ and all $i = 1, \dots, n$, we can conclude that $A_j = \sum_{i=1}^{n} X_i B_{ijj} = 0$. Now, choosing $j = 1$ demonstrates that

$$I_1 = \frac{1}{d_1} \left(\sum_{\ell=2}^{r} A_\ell I_\ell - \sum_{k=s+1}^{r} V_{kj} d_k I_k \right)$$

is contained in the ideal of S generated by $I_2, \dots, I_r$, which is the desired contradiction to the minimality of the generating set. □

Such a minimal set of generators for the algebra of G-invariant polynomials J consisting of algebraically independent homogeneous polynomials is called a set of *basic* or *fundamental invariants* of G. Although such a set is not uniquely determined, it possesses the following uniqueness properties.

Remark 3.29. In addition to the result that the algebra of invariants J is a polynomial algebra, the preceding proof also reveals that a minimal generating set for the ideal $F \trianglelefteq S$ is algebraically independent in S which can be useful to determine an explicit set of generators. Additionally, from this and the fact that $S \cong \mathbb{C}[X_1, \dots, X_n]$ can contain at most n algebraically independent elements we can conclude for the number of generating invariants holds $r \leq n$ (cf. Chevalley [**12**, p. 780-781]).
On the other hand, J is generated as an algebra by r elements $I_1, \dots, I_r$ whence we know that the canonical homomorphism $f \colon \mathbb{C}[x_1, \dots, x_r] \to J$ sending x_i onto I_i is surjective. Hence, J is isomorphic to $\mathbb{C}[x_1, \dots, x_r]/\ker f$ which has Krull dimension of at most r (cf. Broué [**7**, Propostion 2.10]). By Lemma 2.70, the extension $J \subseteq S$ is integral and therefore preserves the Krull dimension (cf. Matsumura [**40**, Theorem 20]). It follows that J has Krull dimension n. Combining these results yields $n \leq r$ and hence with the first inequality, we finally have $n = r$.
Moreover, one can show by investigating J^+ and using Nakayama's lemma 2.20 that the degrees of a fundamental set of invariants are uniquely determined, even though the invariants themselves are not necessarily unique (cf. Thiel [**64**, 13.12]).

4. The proof of (b) ⇒ (a) using Molien's formula

This section is devoted to prove the implication (b) ⇒ (a), i.e., to demonstrate the converse of Theorem 3.28. For this purpose, the concept of a *Poincaré series* of a graded module will be introduced and some useful properties will be presented. Among these, one will find Molien's formula (Theorem 3.40) which provides an explicit equation for the Poincaré series of the algebra of G-invariant polynomials. Moreover, we will present the relationship between the degrees of the fundamental invariants, the group order, and the number of reflections in G, highlighting the connection between the algebraic properties and the geometric representation. In the end, we will be able to prove the desired implication of the main theorem while using some of these relations. To achieve this, we follow the exposition of Lehrer–Taylor [**37**, Sections 4.1–4.3]. The main results at the end of the

section are primarily from a Springer paper [**63**], which in turn presents the results of the original paper by Shephard-Todd [**57**].

Recall that a graded module M over a ring A is denoted by $\bigoplus_{i\geq -m} M_i$ for some $m \in \mathbb{N}$. Since we are interested in the algebra of G-invariant polynomials $J = S^G$ in the following, it suffices to consider the case $m = 0$ for vector spaces. If each subspace M_i of a graded vector space M is of finite dimension and further a G-module for a group G, the space M is a *graded G-module*.

Definition 3.30. Let M be a graded module.

(a) The *Poincaré series* of M is the formal power series in the variable t

$$P_M(t) := \sum_{i\geq 0} \dim(M_i)t^i \in \mathbb{Z}[[t]].$$

(b) For a G-module M and a group element $g \in G$ the *relative Poincaré series* of M with respect to g is defined as the formal power series

$$P_M(g,t) := \sum_{i\geq 0} \operatorname{tr}(g, M_i)t^i \in \mathbb{C}[[t]].$$

Here, $\operatorname{tr}(g, M_i)$ stands for the trace of the matrix that represents the action of g on the finite dimensional subspace M_i.

Remark 3.31. We observe the following: if $g = 1$, the action is trivial, that is, the related matrix is the identity matrix. Hence, we have $\operatorname{tr}(g, M_i) = \dim(M_i)$ and $P_M(1,t) = P_M(t)$.

Example 3.32. Let $M = \mathbb{C}[x]$ be the polynomial ring in a single variable. It admits a natural grading and the kth homogeneous part has a basis of x^k. Therefore, the Poincaré series of it is $P_{\mathbb{C}[x]}(t) = \sum_{k\geq 0} 1 \cdot t^k = \frac{1}{1-t}$ as a formal geometric series.

In the succeeding lemma, the first properties of the relative Poincaré series will be presented, namely the *additivity* and the *multiplicativity*.

Lemma 3.33. *Let G be a group, and let M and N be G-modules. Then, for all g holds $P_{M\oplus N}(g,t) = P_M(g,t) + P_N(g,t)$ as well as $P_{M\otimes N}(g,t) = P_M(g,t) \cdot P_N(g,t)$.*

Proof. For any graded component of $M\oplus N$ we have $(M \oplus N)_k = M_k \oplus N_k$. Consequently, the matrix representing the action of an arbitrary $g \in G$ splits into blocks, and it follows $\operatorname{tr}(g, (M \oplus N)_k) = \operatorname{tr}(g, M_k) + \operatorname{tr}(g, N_k)$. This shows $P_{M\oplus N}(g,t) = P_M(g,t) + P_N(g,t)$ by comparing coefficients.
For the tensor product, we get that the kth graded component of $M\otimes N$ is $\bigoplus_{i=1}^k M_i \otimes N_{k-i}$. Using the *Kronecker product* (see Loan [**38**] for more details on this matter) one may easily verify that the trace of a tensor product of matrices A and B is $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A) \cdot \operatorname{tr}(B)$. Hence, the coefficients of $P_{M\otimes N}(g,t)$ have the form $\sum_{i=1}^k \operatorname{tr}(g, M_i) \cdot \operatorname{tr}(g, N_{k-i})$. Using this formula and the fact that product of two power series is a *Cauchy product* directly leads us to the result. □

Corollary 3.34. *For a group G and G-modules M and N holds $P_{M\oplus N}(t) = P_M(t) + P_N(t)$ and $P_{M\otimes N}(t) = P_M(t) \cdot P_N(t)$.*

Proof. This is clear due to the identity in Remark 3.31 and the previous lemma. □

The following step is to compute the relative Poincaré series of the symmetric algebra of a finite dimensional vector space.

Lemma 3.35. *Let V be an n-dimensional vector space over $\mathbb{C}$ on which the finite group G acts. Then, for all $g \in G$ we have $P_{S(V)}(g,t) = \frac{1}{\det(1-gt)}$.*

Proof. As G is finite, every element $g \in G$ has to be of finite order, and consequently its minimal polynomial has the form $f := X^m - 1 \in \mathbb{C}[X]$ for some $m \in \mathbb{N}$. Therefore, f splits into distinct linear factors which implies that g is diagonalizable (see, e.g., L. Smith [**62**, Theorem 14.5.3 (i)]). Hence, we can choose a basis of V of eigenvectors $v_1, \dots, v_n$ corresponding to the eigenvalues $\lambda_1, \dots, \lambda_n$.
From Proposition 2.57, we know that the monomials $v_1^{m_1} \cdots v_n^{m_n}$ for all combinations of the m_i such that $m_1 + \cdots + m_n = k$ form a basis of $S^k(V)$, the k-fold symmetric power of V, which is the kth homogeneous component of $S(V)$, too. As the identity $g\left(v_1^{m_1} \cdots v_n^{m_n}\right) = g\left(v_1\right)^{m_1} \cdots g\left(v_n\right)^{m_n}$ holds true in the symmetric algebra, the basis monomials are eigenvectors as well. Their eigenvalues are $\lambda_1^{m_1} \cdots \lambda_n^{m_n}$. Since the basis consists of eigenvectors, it follows for the trace

$$\operatorname{tr}(g, S^k(V)) = \sum_{(m_1,\dots,m_n)\in I_k} \lambda_1^{m_1} \cdots \lambda_n^{m_n},$$

where I_k denotes the set of all n-tuples such that $\sum_{i=1}^n m_i = k$. We acquire that this trace is exactly the coefficient of t^k in

$$\sum_{k\geq 0} \left(\sum_{(m_1,\dots,m_n)\in I_k} \lambda_1^{m_1} \cdots \lambda_n^{m_n} \right) t^k \overset{\substack{\text{Cauchy}\\ \text{product}}}{=} \prod_{i=1}^n \sum_{j\geq 0} (\lambda_i t)^j \overset{\substack{\text{geometric}\\ \text{series}}}{=} \prod_{i=1}^n \frac{1}{1-\lambda_i t}.$$

Since g is diagonalizable, the last product is in turn equal to $\frac{1}{\det(1-gt)}$. So, comparing coefficients yields the desired equality $P_{S(V)}(t) = \sum_{k\geq 0} \operatorname{tr}(g, S^k(V)) t^k = \frac{1}{\det(1-gt)}$. □

Example 3.36. In the case of the exterior algebra $\bigwedge(V)$ of an n-dimensional vector space V, the computation of the Poincaré series is greatly simplified by the fact that the kth homogeneous part is of dimension $\binom{n}{k}$ (cf. end of Section 2.4.2 at p. 19). Because of this, the series turns into the finite sum

$$P_{\bigwedge(V)}(t) = \sum_{k=0}^n \binom{n}{k} t^k = (1+t)^n,$$

where the last equality is due to the binomial theorem.

The first part of the next lemma would fit suitably into Section 2.4 on multilinear algebra as well, but it is not used until this point which is why it is included just here. This allows us to compute the Poincaré series of exterior and symmetric algebras more easily.

Lemma 3.37.

(a) *Let $W = W_1 \oplus W_2$ be a direct sum of vector spaces. We get the following vector space isomorphisms $S(W) \cong S(W_1) \otimes S(W_2)$ and $\bigwedge(W) \cong \bigwedge(W_1) \otimes \bigwedge(W_2)$.*

(b) *If $V = \bigoplus_{i\geq 1} V_i$ is a finite dimensional graded vector space where V_i denotes the component of degree i, we have*

$$P_{S(V)}(t) = \prod_{i\geq 1} \left(\frac{1}{1-t^i}\right)^{\dim(V_i)}, \quad P_{\bigwedge(V)}(t) = \prod_{i\geq 1} \left(1+t^i\right)^{\dim(V_i)}.$$

Proof. For (a) see Greub [**24**, 5.15 and 9.8], note that the underlying vector space of the anticommutative tensor product for the exterior algebra is equal to the one of the usual tensor product, so the required vector space isomorphism is shown indeed. For (b), we define U to be a homogeneous vector space of dimension 1 and degree d. Clearly, the degree of all elements of the symmetric algebra $S(U)$ has to be a multiple of d and each of these part is one-dimensional. Since $\dim(U) = 1$, it follows that $\bigwedge(U) = \mathbb{C} \oplus U$, where

$\deg(\mathbb{C}) = 0$. Hence, we get $P_{S(U)}(t) = \sum_{i\geq 0}(t^d)^i = \frac{1}{1-t^d}$ and $P_{\bigwedge(V)}(t) = 1 + t^d$. Finally, the result follows from (a) and Corollary 3.34. □

Using this lemma we can extend Example 3.32 to get that the Poincaré series of the coordinate ring $S = S(V^*) \cong \mathbb{C}[X_1, \ldots, X_n] \cong \mathbb{C}[X_1] \otimes \cdots \otimes \mathbb{C}[X_n]$ of an n dimensional vector space V is $P_S(t) = (1-t)^{-n}$. Moreover, making use of the preceding lemma also allows us to prove the uniqueness of the degrees for a fundamental set of invariants mentioned in Remark 3.29.

Propostion 3.38. *Let $J = S(V^*)^G$ be the algebra of G-invariant polynomials for a unitary reflection group G on a vector space V with $\dim(V) = n$. Then the degrees $d_1, \ldots, d_n$ of a fundamental set of invariants $\{I_1, \ldots, I_n\}$ are uniquely determined. Therefore, they are called the degrees of G.*

Proof. As J inherits the grading of S and since $J \cong \mathbb{C}[I_1] \otimes \cdots \otimes \mathbb{C}[I_n]$, we get that $P_J(t) = \prod_{i=1}^n (1-t^{d_i})^{-1}$. First, we define the inverse of P_J as $Q_J(t) = (P_J(t))^{-1} \in \mathbb{C}[t]$. Then, all of its factors $1 - t^{d_i}$ split into linear factors of the form $\zeta - t$, where the corresponding ζ denotes a d_i^{th} root of unity. For a primitive k^{th} root of unity ζ_k, the multiplicity of $\zeta_k - t$ in $Q_J(t)$ is exactly the number of d_j that are multiples of k.
What will follow is a downwards induction. We start with the largest degree d_m. We notice that the multiplicity of $\zeta_{d_m} - t$ for a primitive d_m^{th} root of unity is exactly the number of occurrences of d_m in $d_1, \ldots, d_n$ because there cannot be any proper multiples of d_m contributing to this number due to the maximality of d_m. For the induction step $0 < k < d_m$ we observe that the number of occurrences of all proper multiples of k in $d_1, \ldots, d_n$ is already uniquely determined by the induction hypothesis, and hence subtracting these from the multiplicity of $\zeta_k - t$ yields the unique number of how often k occurs in $d_1, \ldots, d_n$. Therefore, the degrees only depend on $P_J(t)$ which in turn is an intrinsic property of J. □

Before being able to prove *Molien's formula* from [**43**], we need an auxiliary lemma. Its proof is omitted as it would require some larger machinery, inter alia, the introduction of a further type of Poincaré series, whose only purpose in this work would be to prove this lemma.

Lemma 3.39. *Let G be a finite group and let M be a graded G-module. If χ is an irreducible character of G and M_χ is the χ-isotypic component, i.e., the direct sum of all G-submodules M' isomorphic to V_χ affording χ, then $P_{M_\chi}(t) = \frac{\chi(1)}{|G|}\sum_{g\in G}\overline{\chi(g)}P_M(g,t)$.*

Proof. See Lehrer–Taylor [**37**, Lemma 4.12]. □

Theorem 3.40 (Molien's formula)**.** *For a finite group G acting on the n-dimensional vector space V over $\mathbb{C}$, we have for the ring of G-invariant polynomials $J = S(V^*)^G$ that*

$$P_J(t) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(1-gt)}.$$

Proof. Let χ_1 be the trivial character, that is, $\chi_1(g)P = P$ for all $g \in G$ and $P \in S$. Furthermore, a χ-isotypic component of a G-module M can be equivalently written as $M_\chi = \{v \in M \mid gv = \chi(g)v \text{ for all } g \in G\}$. For the trivial character χ_1 and the G-module of polynomials S this implies $S_{\chi_1} = \{P \in S \mid gP = \chi_1(g)P = P \text{ for all } g \in G\} = J$. Therefore, by Lemma 3.39 and $\chi_1(g) = 1$, it follows that

$$P_J(t) = \frac{1}{|G|}\sum_{g\in G}P_S(g,t).$$

Since V^* is also an n-dimensional vector space, the proof is settled by replacing $P_S(g,t)$ with $\frac{1}{\det(1-gt)}$ due to Lemma 3.35. □

The subsequent theorem is an intermediate step in the original proof of the equivalence between (a) and (b) by Shephard and Todd [**57**, Theorem 5.1 (b) and the following remark]. Not only the results of this theorem but also some of the computations in the course of the proof will be employed to prove the implication (b) ⇒ (a) of the main theorem.

Theorem 3.41 (Shephard–Todd)**.** *Let G be a finite unitary reflection group and let $d_1, \dots, d_n$ be the degrees of G, then*

(a) the order of G satisfies $|G| = d_1 \cdots d_n$;

(b) there are $N = \sum_{i=1}^n (d_i - 1)$ reflections in G.

Proof. (a) Let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of $g \in G$, as g is diagonalizable (cf. the proof of Lemma 3.35). From this, we get $\det(1-gt)^{-1} = ((1-\lambda_1 t)\cdots(1-\lambda_n t))^{-1}$. First, this equation is multiplied by $(1-t)^n$ and afterwards we plug in $t = 1$. This evaluation is 0 as long as there is an eigenvalue different from 1. Else, if all eigenvalues are 1, g must be the identity element and the evaluation at $t = 1$ yields 1.
Due to the geometric sum formula, we have $\frac{1-t}{1-t^{d_i}} = \frac{1}{1+t+\cdots+t^{d_i-1}}$ and setting $t = 1$ yields $\frac{1}{d_i}$ for all $i = 1, \dots, n$. Combining these results via Molien's formula 3.40 and the expression for $P_J(t)$ in Proposition 3.38 we get

$$|G|\, P_J(t) = |G| \prod_{i=1}^n \left(1 - t^{d_i}\right)^{-1} = \sum_{g \in G} \det(1-gt)^{-1}. \tag{11}$$

Once more, we have to multiply this by $(1-t)^n$ and plug in $t = 1$ to get $\frac{|G|}{d_1 \cdots d_n} = 1$ since all summands except the one for $g = 1$ vanish as computed above. Hence, $|G| = d_1 \cdots d_n$.

(b) Let R be the set of all reflections in G. From Remark 3.10, we know that $g \in G$ is a reflection if and only if it has exactly one eigenvalue $\lambda(g)$ that is different from 1. Therefore, the reflections are exactly the $g \in G$ satisfying $\det(1-gt) = (1-t)^{n-1}(1-\lambda(g)t)$. First, substract $(1-t)^{-n}$ from the middle and the right hand side of (11), then multiply by $(1-t)^{n-1}$. In the middle, we get

$$\left(|G| \prod_{i=1}^n (1-t^{d_i})^{-1} - (1-t)^{-n}\right)(1-t)^{n-1} = \frac{|G|}{1-t}\left(\prod_{i=1}^n (1-t^{d_i})^{-1}\right)(1-t)^n - \frac{1}{1-t}$$

$$= \frac{|G|}{1-t}\prod_{i=1}^n \frac{1-t}{1-t^{d_i}} - \frac{1}{1-t} \overset{\substack{\text{geometric sum +}\\ \text{expand the fraction}}}{=} \frac{|G| - \prod_{i=1}^n (1+t+\cdots+t^{d_i-1})}{(1-t)\prod_{i=1}^n (1+t+\cdots+t^{d_i-1})}.$$

For the right hand side of (11), we notice that $\det(1-1t)^{-1} = (1-t)^n$ and for a reflection $g \in R$ holds $\det(1-gt)^{-1}(1-t)^{n-1} = (1-\lambda(g))^{-1}$. Moreover, if neither $g = 1$ nor $g \in R$, it follows that $\det(1-gt)^{-1}(1-t)^{n-1}$ is divisible by $1-t$ because there are at least two eigenvalues different from 1. In other words, the multiplicity of $1-t$ is at most $n-2$ and we can find a rational function $\overline{h} \in \mathbb{C}(t)$ such that $\det(1-gt)^{-1}(1-t)^{n-1} = (1-t)\overline{h}(t)$. Since we may assume all fractions to be completely reduced, the denominator of $\overline{h}$ is not divisible by $(1-t)$. Finally, we can conclude that the right hand side is equal to $\sum_{g \in R}(1-\lambda(g))^{-1} + (1-t)h(t)$, where the denominator of h is not divisible by $1-t$ as it is the sum of all $\overline{h}$ and each of their denominator is not divisible by $1-t$. Hence, we obtain

$$\frac{|G| - \prod_{i=1}^n (1+t+\cdots+t^{d_i-1})}{(1-t)\prod_{i=1}^n (1+t+\cdots+t^{d_i-1})} = \sum_{g \in R} \frac{1}{1-\lambda(g)} + (1-t)h(t), \tag{12}$$

where $h \in \mathbb{C}(t)$ has the aforementioned properties.
We intend to evaluate this equation at $t = 1$. For this purpose, we define the polynomial $H(t) := |G| - \prod_{i=1}^{n}(1+t+\cdots+t^{d_i-1})$ and use the result of (a) to conclude $H(1) = 0$. Thus, we get by the Taylor series expansion at 1 that $H(t) = (t-1)H'(t) + \frac{1}{2}(t-1)^2 H''(t) + \ldots$. Therefore, setting $t = 1$ in (12) eliminates all summands of the Taylor series expansion of H except the first one which turns to $\frac{(t-1)H'(1)}{(1-t)d_1\cdots d_n} = -\frac{H'(1)}{|G|}$. On the right hand side of (12), the first summand remains unchanged whilst the second one is eliminated, too. So, we obtain $-\frac{H'(1)}{|G|} = \sum_{g\in R}\frac{1}{1-\lambda(g)}$ and have to look more precisely at H'.
We get $H'(t) = -\sum_{i=1}^{n}\left((1+2t+3t^2+\cdots+(d_i-1)t^{d_i-2})\prod_{j\neq i}(1+t+\cdots+t^{d_j-1})\right)$ by the product rule for derivatives. If we plug in $t = 1$, we can apply the Gaussian sum formula and use (a) to conclude $H'(t) = -\sum_{i=1}^{n}\left(\frac{1}{2}(d_i-1))d_i\prod_{j\neq i}d_j\right) = -\frac{1}{2}|G|\sum_{i=1}^{n}(d_i-1)$. As we have to multiply this by $\frac{-1}{|G|}$ to plug it into the above formula for $\sum_{g\in R}\frac{1}{1-\lambda(g)}$, it follows that

$$\frac{1}{2}\sum_{i=1}^{n}(d_i-1) = \sum_{g\in R}\frac{1}{1-\lambda(g)}. \tag{13}$$

Initially, we have to consider the special case $n = 1$ and $G = \langle g\rangle$ for a reflection g of order d, where we denote the eigenvalue different from 1 by λ (a primitive d^{th} root of unity). Furthermore, we get $d_1 = d$ and observe that G contains $d-1$ reflections, all elements except $1 \in G$. Hence, their eigenvalues are λ^i for $i = 1,\ldots,d-1$ and we acquire

$$\frac{1}{2}(d-1) = \sum_{i=1}^{d-1}\frac{1}{1-\lambda^i} \tag{14}$$

for (13) in this special case. To finish the proof, we have to return to the general case where the set of all reflections R is a disjoint union of sets of reflections corresponding to cyclic subgroups of G. By (14) each of these cyclic subgroups G' with $|G'| = d$ contributes $\frac{1}{2}(d-1)$ to the right hand side of (13). Hence, taking the sum over all these disjoint sets yields $\frac{1}{2}\sum_{i=1}^{n}(d_i-1) = \frac{1}{2}|R|$, and the proof is completed. □

By the preceding theorem we have shown that the property of G to be a finite unitary reflection group implies that $|G| = d_1\cdots d_n$. But now, we want to demonstrate that G being a unitary reflection group is not only sufficient for the equality of $|G|$ and $d_1\cdots d_n$, but also necessary. Hence, a characterization of unitary reflection groups is achieved by this property which will be used to prove the main objective of this section, the implication (b) ⇒ (a). In order to carry out the proof originally given by Shephard-Todd [**57**] in the version of Springer [**63**, Theorem 2.4], a final preparatory lemma is needed which is due to Springer [**63**, Propostion 2.3], too. Although we mostly follow the presentation of Lehrer–Taylor [**37**, Section 4.3], some supplementary details of the original proof are provided.

Lemma 3.42. *Let V be an n-dimensional vector space over $\mathbb{C}$. If R is the subalgebra of $S := S(V^*)$ generated by n algebraically independent homogeneous polynomials $f_1,\ldots,f_n$ whose degrees are denoted by $d_1,\ldots,d_n$. Moreover, the degrees are assumed to be sorted in increasing order $d_1 \le d_2 \le \cdots \le d_n$. Then*

(a) for all i we have that d_i is the minimal degree of a homogeneous polynomial of R that is not contained in the subalgebra generated by the first $i-1$ generators;
(b) if $g_1,\ldots,g_n \in R$ are homogeneous polynomials and algebraically independent of degrees $e_1 \le e_2 \le \cdots \le e_n$, then $d_i \le e_i$ for all $i = 1,\ldots n$.

Proof. (a) Since R is generated by the f_i, for any homogeneous polynomial $f \in R$ of degree d which is not contained in the subalgebra generated by $f_1, \dots, f_{i-1}$, there exists a polynomial $P \in \mathbb{C}[X_1, \dots, X_n]$ such that $f = P(f_1, \dots, f_n)$. For each monomial $X_1^{m_1} \cdots X_n^{m_n}$ of P holds $d_1 m_1 + \cdots + d_n m_n = d$: due to the homogeneity of f, this sum can either be d or it is evaluated to 0 by plugging in the f_i, but the latter contradicts their algebraic independence. By the choice of f, there exists some $j \geq i$ such that $m_j \geq 1$ and hence we get $d = d_j m_j + x \geq d_j \geq d_i$ for $m_j \geq 1, x \geq 0$, which finishes the proof of (a).

(b) This part is proven by induction on i. For $i = 1$ the statement follows from (a). Now we assume that $d_j \leq e_j$ for all $j = 1, \dots, i-1$. We can find polynomials $G_j \in \mathbb{C}[X_1, \dots, X_n]$ such that $g_j = G_j(f_1, \dots, f_n)$. Due to the algebraic independence of the g_j, the polynomials $G_1, \dots G_i$ cannot involve only the variables $X_1, \dots, X_{i-1}$ because then there would be i algebraic independent polynomials in $i-1$ variables which is impossible for dimension reasons. Thus, in some G_j for $j \leq i$ occurs an X_k with $k \geq i$ whence g_j does not lie in the subalgebra of R generated by $f_1, \dots, f_{k-1}$. From this we can conclude that $e_j \geq d_k$ by (a). Combining this result and the given assumptions we finally obtain $e_i \geq e_j \geq d_k \geq d_i$. □

Theorem 3.43. *Suppose that G is a finite group acting on the n-dimensional vector space V over $\mathbb{C}$. Assume that the algebra of G-invariant polynomials $J := S^G$ is generated by n homogeneous algebraically independent polynomials $f_1, \dots, f_n$ of degrees d_i, respectively. Then*

(a) $|G| \leq d_1 \cdots d_n$;
(b) if $|G| = d_1 \cdots d_n$, it follows that G is a unitary reflection group in V and J is generated by $f_1, \dots, f_n$ as a $\mathbb{C}$-algebra, i.e., J is a polynomial algebra;
(c) if J is generated by $f_1, \dots, f_n$ as a $\mathbb{C}$-algebra, i.e., J is a polynomial algebra, then we obtain equality in (a) and G is a reflection group.

Proof. (a) Denote the ith homogeneous component of J by J_i and set $a_i := \dim(J_i)$. From Molien's formula we obtain

$$\sum_{i \geq 0} a_i t^i = P_J(t) \overset{\text{Theorem 3.40}}{=} \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - gt)}.$$

For the ith homogeneous component of $S = S(V^*)$ we write S_i and get $0 \leq a_i \leq \dim(S_i)$. Since $P_S(t) = (1-t)^{-n}$ by Lemma 3.37 (b), the series $\sum_{i \geq 0} a_i t^i$ is absolutely convergent for all $|t| < 1$ due to the majorant criterion.
Next, let B be the subalgebra of J generated by the homogeneous polynomials $f_1, \dots, f_n$ and define b_i to be the dimension of the ith homogeneous component of B, that is, $b_i = \dim(B \cap S_i)$. We have $b_i \leq a_i$ for all $i = 1, \dots, n$ because $B \cap S_i \subseteq J_i$. From Lemma 3.37 (b), we get that $P_B(t) = \sum_{i \geq 0} b_i t^i = \prod_{j=1}^n (1 - t^{d_j})^{-1}$, and it is absolutely convergent for $|t| < 1$, too, also by the majorant criterion. Hence, we have

$$\prod_{j=1}^n \frac{1}{1 - t^{d_j}} \leq \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - gt)} \tag{15}$$

for all $0 \leq t < 1$ and after multiplying by $(1-t)^n$ we acquire

$$\prod_{i=1}^n (1 + t + \cdots + t^{d_j - 1})^{-1} \leq |G|^{-1} (1-t) h(t).$$

The left hand side is due to the inverse geometric sum formula $\frac{1-t}{1-t^{d_j}} = (1 + t + \cdots + t^{d_j - 1})^{-1}$. For the right hand side, the same arguments as in the proof of Theorem 3.41 are used, and h is once again a rational function whose denominator is not divisible by $1 - t$. Finally,

consider the limit as $t \to 1$ in the above inequality. This leads to $\prod_{j=1}^{n} d_j^{-1} \leq |G|$ and therefore $|G| \leq d_1 \cdots d_n$, which completes the proof of (a).

(b) For this part we assume that equality holds, so we have $|G| = d_1 \cdots d_n$. Initially, we multiply (15) by $|G|$, then subtract $(1-t)^{-n}$ from the result, and consecutively multiply by $(1-t)^{n-1}$. Using similar computations to those in the proof of Theorem 3.41, we obtain

$$\frac{|G| - \prod_{i=1}^{n}(1+t+\cdots+t^{d_i-1})}{(1-t)\prod_{i=1}^{n}(1+t+\cdots+t^{d_i-1})} \leq \sum_{g\in R} \frac{1}{1-\lambda(g)} + (1-t)h(t),$$

where h is a rational function whose denominator is not divisible by $(1-t)$ and R denotes the set of reflections in G. We consider the limit as t approaches 1, then, by the argument at the end of the proof of Theorem 3.41, in particular (14) and what we concluded from this equation at that point, it follows that

$$\frac{1}{2}\sum_{i=1}^{n}(d_i - 1) \leq \frac{1}{2}|R|. \tag{16}$$

Next, define G_1 to be the subgroup of G which is generated by R and denote the degrees of G_1 by $e_1, \ldots, e_n$, i.e., these are the degrees of a set of fundamental invariants. Since the f_i are G-invariant, they are also invariant under the action of the subgroup G_1. But now we are in the situation of Lemma 3.42 (b): the e_i are the degrees of algebraically independent homogeneous generators of $J' := S^{G_1}$ and they may be assumed to be ordered increasingly. Moreover, the f_i (in the role of the g_i) are algebraically independent homogeneous polynomials that lie in J', too, and can be assumed to be ordered by increasing degrees d_i. So, as the roles of the e_i and d_i are interchanged in comparison to the notation of Lemma 3.42, we attain $e_i \leq d_i$ for all $i = 1, \ldots, n$. Additionally, the application of Theorem 3.41 (b) to G_1 yields $|R| = \sum_{i=1}^{n}(d_i - 1)$. Hence, combining all these results leads to

$$\sum_{i=1}^{n}(d_i - 1) \overset{(16)}{\leq} |R| \overset{\textit{Theorem 3.41 (b)}}{=} \sum_{i=1}^{n}(e_i - 1) \overset{e_i \leq d_i}{\leq} \sum_{i=1}^{n}(d_i - 1).$$

Therefore, we have $d_i = e_i$ for all $i = 1, \ldots, n$ and hence $|G_1| \overset{(a)}{=} e_1 \cdots e_n = d_1 \cdots d_n = |G|$. Since G_1 is now a subgroup of G and of order equal to $|G|$, it follows that $G = G_1$. Hence, G is generated by reflections and J is generated by some algebraically independent polynomials. As observed in Theorem 3.28, this is equivalent to J being polynomial.

(c) For this final part we assume J to be generated by the algebraically independent polynomials $f_1, \ldots, f_n$. Thus, we get $B = J$ in the previously introduced notation which also implies that $a_i = b_i$ for all $i = 1, \ldots, n$ and, it follows that we have equality in (15). So, it holds $\prod_{j=1}^{n} \frac{1}{1-t^{d_j}} = \frac{1}{|G|}\sum_{g\in G} \frac{1}{\det(1-gt)}$. Due to the same computations and arguments as in (a), multiplying this equality by $(1-t)^n$ and plugging in $t = 1$ leads to $|G| = d_1 \cdots d_n$. From this point, the result of (c) follows immediately from (b). □

5. The proof of (b) ⇔ (c)

In this section the proof of the main theorem will be completed by demonstrating the equivalence of (b) and (c). First of all, before discussing the following procedure, we will show that we only have to put effort in proving the implication (c) ⇒ (b). We stick to all beforehand introduced notations, in particular, S denotes the symmetric algebra $S(V^*)$ of the dual space of the vector space n-dimensional vector space V over $\mathbb{C}$. Moreover, $J \leq S$ denotes the subalgebra of G-invariant polynomials S^G for a finite group G acting on V.

Remark 3.44. Recall that if $J = S^G$ is generated by r homogeneous polynomials $f_1, \dots, f_r$, the orbit variety $V_{or} \cong V/G$ (cf. Theorem 2.88) is defined to be the vanishing locus in $\mathbb{C}^r$ of the kernel k_φ of the canonical surjective (cf. Lemma 2.80) map $\varphi\colon \mathbb{C}[x_1, \dots, x_r] \to S^G$ mapping x_i onto f_i. Hence, as discussed in Lemma 2.82, its coordinate ring is J and $\mathbb{I}(V_{or}) = k_\varphi$. But now, assuming (b) of the main theorem, i.e., supposing J to be a polynomial algebra equivalently means that J is generated by algebraically independent polynomials. Hence, according to Definition 2.25 the kernel k_φ is 0 and therefore the already surjective map φ is an isomorphism. Since $\dim(J) = n$ (cf. to the proof of Lemma 2.82), we get $n = r$. Furthermore, as $k_\varphi = \{0\}$ it follows immediately that $V_{or} \subseteq \mathbb{A}^n$ is smooth due to the Jacobi-criterion (cf. Example 2.19 (a)) using $\dim(V_{or}) = n$ (cf. Lemma 2.82). So, the proof of (b) ⇒ (c) of the main theorem is completed by this remark.

To establish the converse implication, we first have to create a connection from algebraic geometry to commutative algebra by showing that smooth points of a variety correspond to regular local rings. For the rest of the proof, we will introduce a large toolkit of homological algebra, in particular the addition of two new types of dimension (the projective and the global one). Then, we will demonstrate that regular local rings are already of finite global dimension. Using a fact on the global dimension of localized rings, we will be able to show that J is of finite global dimension. Finally, by a theorem of Serre [**55**] on graded connected algebras, it will be demonstrated that J is isomorphic to a polynomial algebra. Hence, the proof of (c) ⇒ (b) is completed and thus all implications of the main theorem 3.24 are proven.

Remark 3.45. Let $(R, \mathfrak{m})$ be a Noetherian local ring of finite dimension d and denote its residue field by $k := R/\mathfrak{m}$. We recall from commutative algebra that R is said to be *regular* if $\mathfrak{m}$ is generated by d elements. This condition is equivalent to $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$, where $\dim_k$ indicates the k-vector space dimension (cf. Matsumura [**40**, 17.E]).

5.1. From geometry to algebra. Aiming at the prior mentioned link between smooth varieties and local regular rings, we will follow the ideas of a lemma by Görtz–Wedhorn [**23**, Lemma 6.26]. Before advancing to the precise statement, we give an additional lemma that is necessary to prove it (cf. Görtz–Wedhorn[**23**, Proposition B.74 (3)] and see Matsumura [**41**, Theorem 14.2] for a proof).

Lemma 3.46. *Let $(R, \mathfrak{m})$ be a regular local ring and let $r_1, \dots, r_s \in \mathfrak{m}$. Then, the images $\overline{r}_i \in \mathfrak{m}/\mathfrak{m}^2$ are linearly independent over k if and only if the quotient $A/(r_1, \dots, r_s)$ is regular.*

Propostion 3.47. *Let $X \subseteq \mathbb{A}^n$ be an affine variety of dimension d. If $p \in X$ is a smooth point, the corresponding local coordinate ring $\mathbb{C}[X]_{\mathfrak{m}_p}$ is regular.*

Proof. As $dim(X) = d$, we might assume that $\mathbb{C}[X] \cong \mathbb{C}[x_1, \dots, x_n]/(f_1, \dots, f_{n-d})$. Hence, by the Jacobi-criterion, we obtain that $J(p) = \left(\left(\frac{\partial f_i}{\partial x_j}\right)(p)\right)_{i,j}$ is of rank $n - d$. Since $\mathfrak{m}_p = (x_1 - p_1, \dots, x_n - p_n)$ and thus is generated by n elements, it follows that the localized ring $\mathbb{C}[x_1, \dots, x_n]_{\mathfrak{m}_p}$ is regular. We claim that the images of the f_i in $\mathfrak{m}_p/\mathfrak{m}_p^2$ are linearly independent: assume there is a nontrivial linear relation $F := \sum_i^n \lambda_i \overline{f}_i = 0$. Then, $F \in \mathfrak{m}_p^2$ which is the reason why it can be written as a finite sum where each summand contains at least two factors $x_i - p_i$. Therefore, p is a double root of each summand and the partial derivative of $\sum_i^n \lambda_i f_i$ with respect to any variable still vanishes at p, this is a contradiction to the Jacobi-criterion.

As $f_i(p) = 0$, the assumption $f_i \in \mathfrak{m}_p$ is satisfied and we can apply Lemma 3.46 to conclude that $\mathbb{C}[x_1, \ldots, x_n]_{\mathfrak{m}_p} / (f_1, \ldots, f_{n-d})_{\mathfrak{m}_p} \cong (\mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-d}))_{\mathfrak{m}_p} \cong \mathbb{C}[X]_{\mathfrak{m}_p}$ is regular because $\dim(\mathbb{C}[x_1, \ldots, x_n]_{\mathfrak{m}_p}) = n$ and its maximal ideal $\mathfrak{m}_p$ has n generators which turns it into a regular local ring. □

Remark 3.48. This is the localization at exactly all maximal ideals because $\mathbb{C}[X]$ is a quotient ring of the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ whose maximal ideals are exactly the $\mathfrak{m}_p$ of the form $(x_1 - p_1, \ldots, x_n - p_n)$ for a point $p \in \mathbb{C}^n$ (cf. Matsumura [**40**, Corollary 14.4]). But as for any ring R and any ideal I there is a bijection between $\{J \trianglelefteq R \mid I \subseteq J\}$ and $\{\overline{J} \trianglelefteq R/I\}$ (cf. Atiyah–Macdonald [**1**, Proposition 1.1]), the maximal ideals of $\mathbb{C}[X]$ are exactly the $\mathfrak{m}_p$ corresponding to the points of X.

Remark 3.49. Note that a coordinate ring of an affine variety is isomorphic to a quotient ring of a polynomial ring, in particular $J = S^G \cong \mathbb{C}[x_1, \ldots, x_n] / \ker_\varphi$ (cf. Lemma 2.80). Hence, it is the quotient of a Noetherian ring and thus Noetherian itself by Atiyah–Macdonald [**1**, Proposition 6.6], and by [**1**, Proposition 7.3] the localization $J_{\mathfrak{m}_p}$ is also Noetherian. Therefore, the beforehand considered rings satisfy the Noetherian property in the definition of regularity.

Since the orbit variety V/G is assumed to be smooth in (c) of the main theorem, by Proposition 3.47 and Remark 3.48, we obtain the following result.

Corollary 3.50. *Under the assumption of* (c) *of the main theorem it follows that for the algebra of G-invariant polynomials J, the localization at any maximal ideal $J_{\mathfrak{m}_p}$ is a regular local ring.*

5.2. The homological methods. At first, we have to introduce some fundamental objects that will be considered more precisely in the following. The first pair will be projective and injective modules. Even though projective modules have already been introduced while discussing the Cohen-Macaulay property of the algebra of invariants in Section 2.5.2, we will give another definition (see Lang [**36**, Chapter III, §4] for the equivalence). Unless stated otherwise, we will follow Rotman's presentation [**50**] of the subsequently considered objects and properties. For injective and projective modules see Chapter 3, for the succeeding part we mostly refer to the Chapters 6 to 8. In the following, all modules are supposed to be R-modules for a fixed ring R.

Definition 3.51. A module P is said to be *projective* if for all modules B, C with a surjective morphism $\beta\colon B \to C$ and an arbitrary morphism $\alpha\colon P \to C$, there exists a morphism $\gamma\colon P \to B$ such that the following diagram is commutative.

$$\begin{tikzcd} & P \arrow[dl, dashed, "\gamma"'] \arrow[d, "\alpha"] & \\ B \arrow[r, "\beta"'] & C \arrow[r] & 0. \end{tikzcd}$$

Definition 3.52. A module E is defined to be *injective* if for every module B and every submodule $A \leq B$, any morphism $f\colon A \to E$ can be extended to a morphism $g\colon B \to E$ such that the following diagram is commutative.

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & A \arrow[u, "f"] \arrow[r, hook] & B. \arrow[ul, dashed, "g"'] \end{tikzcd}$$

Using these objects, we are now able to introduce a pair of special type of exact sequences.

Definition 3.53. Let M be a module, then we call the exact sequence

$$\cdots \to P_{n+1} \to P_n \to \cdots \to P_1 \to P_0 \to M \to 0$$

a *projective resolution* of M if every module P_i is projective. Analogously, an *injective resolution* of M is an exact sequence

$$0 \to M \to E^0 \to E^1 \to \cdots \to E^n \to E^{n+1} \to \dots$$

where each E^i is an injective module. In this case we use uppercase indices to indicate that the rising indices deviate from the usual notation, where the indices decrease whilst moving to the right.

An important result regarding this topic is that every module has a free and thus projective resolution as well as there always exists an injective resolution (cf. Rotman [**50**, Theorems 3.8 and 3.28]).

Example 3.54. Since any free module is by definition projective as well, we provide an example of a projective resolution by a free resolution. Let $R \neq 0$ be a ring. First, take any non-zero-divisor $x \in R$ and define the R-module $M_1 := R/(x)$. If follows that the sequence

$$0 \hookrightarrow R \xrightarrow{\cdot x} R \twoheadrightarrow M_1 \to 0$$

is exact and as R is clearly free over itself we have a first example of a free resolution. This can be carried on for an arbitrary amount of variables. E.g., for two elements $x, y \in R$ that are no zero-divisors, we have to adapt the previous resolution to gain a free resolution $M_2 := R/(x, y)$ in the following way

$$0 \hookrightarrow R \xrightarrow{\cdot\binom{y}{-x}} R^2 \xrightarrow{\cdot(x,y)} R \twoheadrightarrow M_2 \to 0.$$

If the M in each case is left out, we get the first two *Koszul complexes* which are also a powerful tool in homological algebra and can be defined for any set of elements. The above examples are inspired by Eisenbud [**19**, Chapter 17.1], where further reading on this topic can be found as the whole 17th chapter is about it.

Definition 3.55. A *(chain) complex* $\mathbf{A}$ is a sequence of modules indexed by integers

$$\mathbf{A}\colon \cdots \to A_{n+1} \xrightarrow{d_{n+1}} A_n \xrightarrow{d_n} A_{n-1} \to \dots$$

such that $d_{n+1} \circ d_n = 0$ for all $n \in \mathbb{Z}$. The maps d_n are called *differentiations* and they satisfy equivalently that $\operatorname{im} d_{n+1} \subseteq \ker d_n$ for all $n \in \mathbb{Z}$. Note that we may also denominate a complex by $(\mathbf{A}, d)$.

Definition 3.56. For a complex $(\mathbf{A}, d)$ we define its nth *homology module* as the quotient $H_n(\mathbf{A}) := \ker d_n / \operatorname{im} d_{n+1}$. Due to the inclusion in the prior definition, this is well-defined.

Example 3.57. For the simple Koszul complex $K(x)\colon 0 \to R \xrightarrow{\cdot x} R$ from Example 3.54 the left R is set to be A_1 and the right takes the place of A_0. All other modules in the sequence are 0 and therefore mostly omitted. The preceding definition yields $H_1(K(x)) = \ker(\cdot x)/0 = \operatorname{Ann}(x)$ and $H_0(K(x)) = R/\operatorname{im}(\cdot x) = R/(x)$ and all other homology modules are 0.

For the next part, it is helpful to have some basic knowledge about category theory, in particular, the notion of a functor mapping from the category of R-modules into itself will be used. See Section 1.2 for some introductory literature. Subsequently, we will introduce the Ext- and Tor-*functors* and *-modules* forming the foundation for the further definitions.

Definition 3.58. Let B be a module and define the tensor-functor by $-\otimes_R B$. Then, for a module A, the nth Tor-*module* is defined as $\operatorname{Tor}_n^R(A,B) \coloneqq \ker(d_n\otimes 1)\,/\,\operatorname{im}(d_{n+1}\otimes 1)$ for the complex

$$\mathbf{P}_B\colon \cdots \to P_2\otimes B \xrightarrow{d_2\otimes 1} P_1\otimes B \xrightarrow{d_1\otimes 1} P_0\otimes B \xrightarrow{d_0\otimes 1} A\otimes B \to 0,$$

where $\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} A \to 0$ is a projective resolution of A. In other words, we have $\operatorname{Tor}_n^R(A,B) = H_n(\mathbf{P}_B, d)$. Moreover, leaving the module A variable turns $\operatorname{Tor}_n^R(-,B)$ into the announced Tor-*functor*.

Definition 3.59. Let C be a module and let $\operatorname{Hom}_R(C,-)$ be the homomorphism-functor. Then, the nth Ext-*module* for a module A is defined as $\operatorname{Ext}_R^n(C,A) \coloneqq \ker(d_*^n)\,/\,\operatorname{im}\left(d_*^{n-1}\right)$ for the complex

$$\mathbf{E}_C\colon 0 \to \operatorname{Hom}(C,A) \to \operatorname{Hom}(C,E^0) \xrightarrow{d_*^0} \operatorname{Hom}(C,E^1) \xrightarrow{d_*^1} \operatorname{Hom}(C,E^2) \to \dots,$$

where $0 \to A \to E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \to \dots$ is an injective resolution of A and d_* denotes the dual map. The definition can be reformulated to $\operatorname{Ext}_R^n(C,A) = H_n(\mathbf{E}_C, d)$. Moreover, the Ext-*functor* is derived by $\operatorname{Ext}_R^n(C,-)$.

One could now ask whether Definition 3.58 and Definition 3.59 are well-defined because a resolution has to be chosen whence the modules might depend on this choice. But it can be shown that these definitions are both independent of the chosen resolution (cf. Rotman [**50**, Theorem 6.11 and Corollary 6.15]). Moreover, we remark that it is not straightforward that the prior defined modules are R-modules, because applying $\otimes_R$ and Hom_R to a complex first yields abelian groups and $\mathbb{Z}$-maps. Nevertheless, from our assumptions that a ring is always commutative, it follows that the Ext- and Tor-modules are also R-modules (cf. Rotman [**50**, Theorem 7.15 and 8.12]).

Remark 3.60. Another way to define $\operatorname{Ext}_R^n(C,A)$ is to use the functor $\operatorname{Hom}_R(-,A)$ and to choose a projective resolution of C. For more details on the construction and the precise definition we refer to Rotman [**50**, Definition 6.17]. Since both definitions lead to equal modules (cf. Rotman [**50**, Theorem 7.8]), we can work with either definition depending on the case of usage. Note that there is a similar result for Tor, i.e., the Tor-modules are equal whether the tensor-functor is $-\otimes_R B$ or $A\otimes_R -$ (cf. Rotman [**50**, Theorem 7.9]).

Subsequently, we will introduce two new types of dimension and investigate their relation, for what we firstly follow Serre's approach in [**55**, Chapter IV].

Definition 3.61. Let R be a ring and M be an R-module. Then,

(a) the *projective dimension* $\operatorname{prdim}_R(M)$ of M is defined as the supremum of $p>0$ such that there exists at least one R-module N that satisfies $\operatorname{Ext}_R^p(M,N)\neq 0$;
(b) the *global dimension* $\operatorname{gldim}(R)$ of the ring R as the supremum of $p>0$ such that there is at least one pair of R-modules M,N satisfying $\operatorname{Ext}_R^p(M,N)\neq 0$.

In the case that the underlying ring is Noetherian, there exists a strong connection between a projective resolution of a module and its projective dimension providing a little more intuition for the dimension notion.

Propostion 3.62. *Let R be a Noetherian ring and $n\geq 0$. Then for any R-module M the following are equivalent:*

(a) $\operatorname{prdim}_R(M)\leq n$.
(b) There exists a projective resolution of M of length n, i.e., an exact sequence $0\to P_n\to\cdots\to P_1\to P_0\to M\to 0$, where all P_i are projective.

Proof. See Serre [**55**, Chapter IV, Proposition 17]. □

Remark 3.63. From this characterization, it is even more straightforward to see that an R-module M is of $\operatorname{prdim}_R(M) = 0$ if and only if it is projective. This is still true if R is an arbitrary ring (cf. Serre [**55**, p. 70]).

Before focusing on the global dimension of local Noetherian rings, we present a general result.

Propostion 3.64. *For any ring R holds*

$$\sup\{\operatorname{prdim}_R(M)\} = \operatorname{gldim}(R),$$

where the supremum is taken over all finitely generated R-modules M.

Proof. See Serre [**55**, Chapter IV, Corollary on Proprosition 16]. □

Aiming at the proof that a regular local ring is of finite global dimension, a result originally given by Auslander and Buchsbaum in [**2**], we will provide and prove some results on the projective and global dimension. For this purpose, the principal ideas are taken from Lam [**34**, §5, Sections A, B and F].

Propostion 3.65. *For an exact sequence $0 \to M \to N \to P \to 0$ of R-modules it follows that if two of $\operatorname{prdim}_R(M), \operatorname{prdim}_R(N), \operatorname{prdim}_R(P)$ are finite, so is the third. Moreover,*

(a) if $\operatorname{prdim}_R(M) < \operatorname{prdim}_R(N)$, it follows $\operatorname{prdim}_R(P) = \operatorname{prdim}_R(N)$;
(b) if $\operatorname{prdim}_R(M) > \operatorname{prdim}_R(N)$, it follows $\operatorname{prdim}_R(P) = \operatorname{prdim}_R(M) + 1$;
(c) if $\operatorname{prdim}_R(M) = \operatorname{prdim}_R(N)$, it follows $\operatorname{prdim}_R(P) \leq \operatorname{prdim}_R(M) + 1$.

Proof. See Lam [**34**, Theorem 5.20]. □

Using these relations, we are able to prove the following lemma, denominated as the "Change of Rings Lemma" (Lam [**34**, 5.26]).

Lemma 3.66. *Let R be ring and $x \in R$ be neither a zero-divisor nor a unit. We write $\overline{R} := R/(x)$ for the quotient ring by the principal ideal with generator x. If M is an $\overline{R}$-module of finite projective dimension $n = \operatorname{prdim}_{\overline{R}}(M)$, it follows that $\operatorname{prdim}_R(M) = n+1$.*

Proof. In the course of the proof, we need the following additional fact: for an exact sequence $0 \to K \to P \to M \to 0$ of modules over any fixed ring S, where P is projective and M is *not* projective, according to Lam [**34**, 5.12] we have $\operatorname{prdim}_S(M) = \operatorname{prdim}_S(K) + 1$. The actual proof is an induction on n. We start with the base case $n = 0$, i.e., M is a projective $\overline{R}$-module by Remark 3.63. Therefore, by definition (in the proof of Theorem 2.76) it holds $M \oplus N = \overline{F}$, where N is an $\overline{R}$-module and $\overline{F}$ is a free $\overline{R}$-module. Now consider the canonical exact sequence of R-modules for the quotient $\overline{R}$

$$0 \to (x) \to R \to \overline{R} \to 0.$$

Clearly, (x) and R themselves are projective as R-modules because they are free. Hence, we can apply Proposition 3.65 (c) to obtain that $\operatorname{prdim}_R(\overline{R}) \leq 1$. Using this and the fact that for any free module $F = \bigoplus_i F_i$ holds $\operatorname{prdim}_S(F) = \sup_i \{\operatorname{prdim}_S(F_i)\}$ (cf. Lam [**34**, Proposition 5.25]), we can conclude that $\operatorname{prdim}_R(M) \leq \operatorname{prdim}_R(\overline{F}) \leq 1$. But M cannot be a projective R-module as otherwise $M \neq 0$ would be a direct summand of a free R-module F and for free modules holds $xf \neq 0$ for all nonzero $f \in F$ and all $x \in R$ that are no zero-divisors[1]. However, we have $xM = 0$, and so it follows $\operatorname{prdim}_R(M) = 1$ as required. For the induction step let $n \geq 1$. We firstly consider the exact sequence of $\overline{R}$-modules

$$0 \to K \to \overline{F} \to M \to 0,$$

[1] If $0 = xf = xa_1e_{i_1} + \cdots + xa_ke_{i_k}$, it follows $xa_i = 0$ for all i due to the linear independence of this subset of generators of F and since x is not a zero divisor, we obtain $a_i = 0$, so $f = 0$.

where $\overline{F}$ is a free $\overline{R}$-module. Note that one can always find a free module, even though it might be of infinite rank, such that there is a surjective projection $\overline{F} \to M$ by taking an e_i for each generator a_i of M as an $\overline{R}$-module, then K is the kernel of this projection. Utilizing the remark at the beginning of this proof, it follows that $\operatorname{prdim}_{\overline{R}}(K) = n-1$ and therefore we can apply the induction hypothesis to acquire that $\operatorname{prdim}_R(K) = n$. Initially, we discuss the straightforward case $n \geq 2$. Hence, $\operatorname{prdim}_R(K) = n > 1 = \operatorname{prdim}_R(\overline{F})$ (cf. the base case) and Proposition 3.65 (b) yields the desired result $\operatorname{prdim}_R(M) = n+1$.
It remains to show that the result is also true if $n = 1$. First, by the induction hypothesis and the base case, we have $\operatorname{prdim}_R(K) = 1 = \operatorname{prdim}_R(\overline{F})$. So, Proposition 3.65 (c) yields $\operatorname{prdim}_R(M) \leq 2$. Now, take an exact sequence of R-modules $0 \to T \hookrightarrow F \to M \to 0$, where F is free. By the remark, at the beginning we have $\operatorname{prdim}_R(M) = \operatorname{prdim}_R(T) + 1$ whence it suffices to show that $\operatorname{prdim}_R(T) \geq 1$, that is, T is not projective as an R-module. Since $xM = 0$, we get that $xF \subseteq T$ because of the exactness of the above sequence. This is why

$$0 \to T/xF \to F/xF \to M \to 0$$

is an exact sequence of $\overline{R}$-modules and hence $1 = \operatorname{prdim}_{\overline{R}}(M) = \operatorname{prdim}_{\overline{R}}(T/xF) + 1$, i. e., T/xF is a projective $\overline{R}$-module. Therefore, the exact sequence of $\overline{R}$-modules

$$0 \to xT/xF \to T/xT \to T/xF \to 0$$

splits, i.e., we have $T/xT \cong xT/xF \oplus T/xF$. By multiplying with x, we can identify $M \cong F/T$, which is due to the first exact sequence in this case, with the quotient xF/xT. Therefore, M is a direct summand of T/xT. If $\operatorname{prdim}_R(T) = 0$, that is, if T is projective as R-module, then so is T/xT as $\overline{R}$-module. But in this case, as a direct summand, M is projective as well by the fact already used in the base case that the projective dimension of a direct sum is the supremum of its summands (cf. Lam [**34**, Proposition 5.25]). This contradicts the assumption that $\operatorname{prdim}_{\overline{R}}(M) = 1$ and we have $\operatorname{prdim}_R(T) \geq 1$ as desired, since this implies $\operatorname{prdim}_R(M) = 2$. □

Next, we will introduce the notion of a regular sequence in a ring. Aiming at computing the projective dimension of a regular local ring, we use the definition given by Lam [**34**, Definition 5.31] and the subsequent proposition, but remark that this concept is also used to define the grade or depth of an ideal in Section 2.5.2.

Definition 3.67. Let R be any ring. Then, we shall say that an ordered sequence $x_1, \ldots, x_n \in R$ is a *regular sequence* in R if the ideal $(x_1, \ldots, x_n)$ is not the whole ring and if the image of x_i is not a zero-divisor in $R/(x_1, \ldots, x_{i-1})$ for all $i = 1, \ldots, n$.

Propostion 3.68. *For any ideal $I = (x_1, \ldots, x_n) \trianglelefteq R$ whose generators form a regular sequence in R, it follows* $\operatorname{prdim}_R(R/I) = n$.

Proof. This is shown by induction on n where the base case $n = 0$ and therefore $I = \{0\}$ is trivial. Let $n > 0$ and set $\overline{R} := R/(x_1)$. Then, the images $\overline{x}_2, \ldots, \overline{x}_n$ are already a regular sequence of length $n-1$ in $\overline{R}$. Hence, if we set $\overline{I} := (\overline{x}_2, \ldots, \overline{x}_n) \trianglelefteq \overline{R}$, the induction hypothesis yields $\operatorname{prdim}_{\overline{R}}(\overline{R}/\overline{I}) = n-1$. Moreover, we have $\overline{R}/\overline{I} \cong R/I$ and hence $\operatorname{prdim}_{\overline{R}}(R/I) = n-1$. Since x_1 is not a zero-divisor in R, we can apply Lemma 3.66 to deduce that $\operatorname{prdim}_R(R/I) = n$. □

From now on, we assume R to be a local Noetherian ring $(R, \mathfrak{m})$ with residue field $k = R/\mathfrak{m}$. Before being able to establish a connection between the projective dimension of the residue field and the global dimension of the ring, we need a result about the Tor-modules $\operatorname{Tor}_i(M, k)$ for finitely generated R-modules M and their projective dimension.

Propostion 3.69. *Let $(R, \mathfrak{m})$ be a local Noetherian ring with residue field k and let M be a finitely generated R-module. Then, for any $n \geq 0$, the following are equivalent:*

(a) $\operatorname{prdim}_R(M) \leq n$.
(b) For all $p > n$ and all R-modules N we have $\operatorname{Tor}_p(M, N) = 0$.
(c) $\operatorname{Tor}_{n+1}(M, k) = 0$.

Proof. See Serre [**55**, Chapter IV, Theorem 8]. □

Propostion 3.70. *For a local Noetherian ring $(R, \mathfrak{m})$ with residue field k of projective dimension* $\operatorname{prdim}_R(k) = n$*, it follows* $\operatorname{gldim}(R) = n$.

Proof. We first show that if $\operatorname{prdim}_R(k) \leq n$, then also $\operatorname{gldim}(R) \leq n$. Since R is Noetherian, the quotient $k = R/\mathfrak{m}$ is a Noetherian R-module and hence finitely generated. By setting $p = n + 1$ and letting N be a finitely generated R-module, Proposition 3.69 yields $\operatorname{Tor}_{n+1}(k, N) = 0$ for all finitely generated R-modules N. As R is commutative, we have $\operatorname{Tor}_i(A, B) \cong \operatorname{Tor}_i(B, A)$ for all R-modules A, B and $i \geq 0$ by Rotman [**50**, Corollary 8.6]. Hence, we have $\operatorname{Tor}_{n+1}(N, k) = 0$ and again by Proposition 3.69, it follows

$$\operatorname{prdim}_R(N) \leq n$$

for all finitely generated R-modules N. Now, applying Proposition 3.64 leads to

$$\operatorname{gldim}(R) = \sup\{\operatorname{prdim}_R(N)\} \leq n.$$

Finally, since k is already a finitely generated R-module of projective dimension n, there is equality, so $\operatorname{gldim}(R) = n$. □

At this point, all tools required to prove the succeeding theorem of Auslander and Buchsbaum [**2**] have been introduced. Subsequently, we use the ideas of Lam [**34**, Theorem 5.84].

Theorem 3.71. *(Auslander–Buchsbaum) Let $(R, \mathfrak{m})$ be a local Noetherian ring. If R is regular, then it is also of finite global dimension and* $\operatorname{gldim}(R) = \dim(R)$.

Proof. The aim is to use Proposition 3.68 and Proposition 3.70 whence we have to display that a minimal set of generators for $\mathfrak{m}$ is a regular sequence $x_1, \ldots, x_n$ in R, where $n = \dim(R)$. This is demonstrated by induction on n. For $n = 1$ we use the fact that a regular local ring is an integral domain (cf. Atiyah–Macdonald [**1**, Lemma 11.23]). Hence, x_1 is not a zero-divisor in R. For $n > 1$ we conclude from Lemma 3.46 that $R/(x_1)$ is a regular local ring. Its maximal ideal can be generated by the images of $x_2, \ldots, x_n$. Hence, by induction $x_1, \ldots, x_n$ is a regular sequence in R. In the end, we obtain

$$\dim(R) = n \overset{\textit{Proposition 3.68}}{=} \operatorname{prdim}_R(k) \overset{\textit{Proposition 3.70}}{=} \operatorname{gldim}(R).$$

□

Remark 3.72. In fact, there exists an even stronger result. It can be demonstrated that the converse of Theorem 3.71 is also true, which was originally established by Serre in [**52**], as mentioned in the introduction. Here, we omit a proof of the converse, but using yet a larger machinery of homological algebra, it is given by Serre [**55**, Chapter IV, Theorem 9].

Recall that we have only proven the regularity of the localized rings $J_{\mathfrak{m}_p}$ in Corollary 3.50. Nevertheless, we are able demonstrate that the ring J is of finite global dimension, too, based on the regularity of the $J_{\mathfrak{m}_p}$ using the succeeding proposition.

Propostion 3.73. *Let R be a Noetherian ring, then we have*

$$\operatorname{gldim}(R) = \sup\{\operatorname{gldim}(R_{\mathfrak{m}})\},$$

where the supremum is taken over all maximal ideals of R.

Proof. See Lam [34, Theorem 5.92]. □

As a combination of several preceding results, we are now able to take the next step in proving the implication (c) ⇒ (b).

Corollary 3.74. *Let G be a finite group acting on the n-dimesional vector space V such that the orbit variety V/G is smooth. Then the ring of G-invariant polynomials J is of finite global dimension.*

Proof. First of all, we remember that the ideals $\mathfrak{m}_p$ for all $p \in V/G$ are exactly the maximal ideals of J as explained in Remark 3.48. As seen in Remark 3.49, J and the localizations at all maximal ideals $J_{\mathfrak{m}_p}$ are Noetherian. Hence, by Theorem 3.71, we have $\operatorname{gldim}(J_{\mathfrak{m}_p}) = \dim(J_{\mathfrak{m}_p}) < \infty$. Since the prime ideals of the localized ring $J_{\mathfrak{m}_p}$ correspond bijectively to the primes of J that have empty intersection with $\mathfrak{m}_p$ (cf. Matsumura [40, (1.F)]), it follows $\dim(J_{\mathfrak{m}_p}) \leq \dim(J) = n$. For the last equality see the proof of Lemma 2.82. Finally, we have

$$\operatorname{gldim}(J) \overset{\textit{Proposition 3.73}}{=} \sup_{p \in V/G} \left\{\operatorname{gldim}(J_{\mathfrak{m}_p})\right\} \overset{\textit{Theorem 3.71}}{=} \sup_{p \in V/G} \left\{\dim(J_{\mathfrak{m}_p})\right\} \leq n.$$

□

5.3. Serre's theorem on graded algebras. In this last part of proving the implication (c) ⇒ (b) of the main theorem, we will use that J is also a graded algebra over $\mathbb{C}$. Moreover, we will establish a special type of polynomial algebra, the so-called *graded-polynomial* algebra. In the end, we will present a theorem from Serre indicating that being of finite global dimension and being a polynomial algebra are equivalent. For this purpose, we mostly follow Serre [55, Chapter IV, Appendix III].

Recollect that a commutative connected graded algebra A is a commutative algebra satisfying $A = \bigoplus_{i \geq 0} A_i$ and $A_0 = k$ for a field k. We set $\mathfrak{m} = \mathfrak{m}(A) = \bigoplus_{i \geq 1} A_i$, which is clearly a maximal ideal of A. In the following, we only consider algebras of this type that are finitely generated.

Besides, we have to establish the concept of an $\mathfrak{m}$-adic completion of a ring for an ideal $\mathfrak{m}$. This is a special case of completions, for the generalized definition see Eisenbud [19, Chapter 7.1].

Definition 3.75. Let R be a ring and take an ideal $\mathfrak{m} \trianglelefteq R$. Then the $\mathfrak{m}$-*adic completion* of R is the ring

$$\hat{R} := \{r = (r_1, r_2, \dots) \in \prod_{i \geq 0} R/m^i \mid r_j \equiv r_i \mod m^i \text{ for all } j > i\}.$$

Example 3.76. For the localization $A_{\mathfrak{m}}$, this definition already shows that the $\mathfrak{m}$-adic completion $\hat{A}_{\mathfrak{m}}$ can be identified with the algebra of infinite formal sums consisting of $a_0 + a_1 + \dots$, where $a_i \in A_i$ for every i.

Moreover, a special type of polynomial algebras is defined below.

Definition 3.77. An algebra A satisfying the previous conditions is called a *graded-polynomial algebra* if there exist homogeneous polynomials such that the canonical map

$$k[x_1, \dots, x_d] \to A, \quad x_i \mapsto P_i$$

is an isomorphism. In this case, the monomials $P_1^{c_1} \cdots P_d^{c_d}$ with $\sum c_i \deg(P_i) = n$ form a basis of A_n for all n.

Now we can point out the main result of this subsection.

Theorem 3.78. *Let A be a finitely generated algebra that is commutative, connected and graded. Then, the following are equivalent:*

(a) A is a graded-polynomial algebra.
(b) A is isomorphic to a polynomial algebra (not necessarily as a graded-polynomial algebra).
(c) A considered as a ring is Noetherian and of finite global dimension.
(d) The local ring $A_{\mathfrak{m}}$ is Noetherian and of finite global dimension.

Proof. Clearly, we have (a) ⇒ (b). Moreover, (b) ⇒ (c) follows from Hilbert's basis theorem (cf. Section 2.1.2) and his famous syzygy theorem (see, e.g., Matsumura [**40**, Corollary 18.1]), and (c) ⇒ (d) is given by Proposition 3.73. Hence, it remains to show that (d) ⇒ (a).
Due to the grading of A, it follows that the k-vector space $\mathfrak{m}/\mathfrak{m}^2$ is also graded and since $A_{\mathfrak{m}}$ is Noetherian, $\mathfrak{m}/\mathfrak{m}^2$ is of finite dimension by Nakayama's Lemma 2.20 as $\mathfrak{m}$ is finitely generated. So, we can choose a basis $(p_1, \dots, p_d)$ consisting of homogeneous elements. Set $a_i := \deg(p_i)$, choose an arbitrary representative of the class p_i in A_{a_i}, and denote it by P_i for all $i = 1, \dots, d$. Let A' be the graded-polynomial algebra $k[X_1, \dots, X_d]$ with $\deg(X_i) = a_i$. The aim is to establish an isomorphism between A' and A.
For this purpose, let $f\colon A' \to A$ such that X_i is mapped onto P_i for all i which clearly defines a unique morphism. We have $f(A'_0) = A_0$ and as the P_i generate $\mathfrak{m}$, it follows that $f(A'_n) = A_n$ for all $n \geq 1$, so, f is surjective. For the injectivity, we consider the completed local map $\hat{f}_{\mathfrak{m}}\colon \hat{A}'_{\mathfrak{m}} \to \hat{A}_{\mathfrak{m}}$. Since being of finite global dimenions is preserved under completion (cf. Serre [**55**, Chapter IV, Proposition 24]), it follows that $\operatorname{gldim}(\hat{A}_{\mathfrak{m}}) < \infty$. Note that the completion of the graded-polynomial algebra $A'_{\mathfrak{m}}$ is the formal power series ring. Consequently, $\hat{f}_{\mathfrak{m}}$ is an isomorphism due to a result from Serre [**55**, Chapter IV, Theorem 10] which states that—under the in this case satisfied assumption that $\operatorname{char}(A) = \operatorname{char}(k)$—a complete local ring is of finite global dimension n if and only if the ring is isomorphic to the formal power series ring in n variables. In particular, the map $\hat{f}_{\mathfrak{m}}$ is injective whence its restriction to the local map $f_{\mathfrak{m}}\colon A'_{\mathfrak{m}} \to A_{\mathfrak{m}}$ is injective as well. Since being injective is a local property (cf. Atiyah–Macdonald [**1**, Proposition 3.9]) and $\mathfrak{m}$ is the unique maximal ideal, this implies that f is injective and thereby an isomorphism. □

By applying this theorem, we can finally complete the proof of the main theorem by the subsequent corollary which demonstrates (c) ⇒ (b) of the main theorem.

Corollary 3.79. *Under the assumptions of the main theorem 3.24* (c)*, it follows that the ring of G-invariant polynomials J is a polynomial algebra.*

Proof. From Corollary 3.74, we already know that $\operatorname{gldim}(J) < \infty$ and in Remark 3.49 we have also seen that J is Noetherian. Additionally, J is graded by the degree of the polynomials and $J_0 = \mathbb{C}$. Hence, the conditions for Theorem 3.78 (c) are satisfied and it follows that J is a polynomial algebra. □

Remark 3.80. Supplementary to Remark 3.72, which stated that we only demonstrate that a regular local ring is of finite global dimension (proven by Theorem 3.71), we are now able to explain in which extent the converse (originally due to Serre [**52**]) is required. Although the converse is used in proving Theorem 3.78, its usage is hidden in another theorem may not be apparent at first glance. Namely, the previously stated theorem from Serre (cf. [**55**, Chapter IV, Theorem 10]) about complete local ring requires this characterization of regular local rings. Proving the converse of Theorem 3.71 and the theorem concerning complete local rings involves complex tools beyond the scope of this work, which is why only the proof of Theorem 3.71 is presented whilst the further results are cited.

6. Computations of concrete generators for the algebra of invariants

By Theorem 3.28 we obtained the theoretical result that the algebra of invariants of a finite unitary reflection group is a polynomial algebra, i.e., it is generated by homogeneous algebraically independent polynomials. However, the proof was not constructive at all. But there are ways to compute these generators, and in this section we will present some explicit computations for selected unitary reflection groups.

First of all, the class of reflection groups can be split up into two separate types of groups.

6.1. The imprimitive reflection groups. In this subsection, we establish the so-called imprimitive reflection groups and summarize the results from Lehrer–Taylor [**37**, Chapter 2].

Definition 3.81. We call a subgroup $G \subseteq GL(V)$ *imprimitive* if the G-module V can be decomposed as $V = V_1 \oplus \cdots \oplus V_m$ with $m > 1$, all $V_i \neq 0$, and such that G permutes the subspaces V_i among themselves. Otherwise, we say that G is *primitive*.

The groups of type $G(m,p,n)$, a notation introduced by Shephard and Todd, can be described as generalized symmetric groups. We assume that p is a divisor of m. Then, these groups are constructed by taking the semidirect product of

$$A(m,p,n) = \{(\theta_1, \ldots, \theta_n) \in B \mid (\theta_1 \cdots \theta_n)^{m/p} = 1\},$$

where B denotes the set of vectors in $\mathbb{C}^n$ whose entries are m^{th} roots of unity, and the symmetric group $\mathrm{Sym}(n)$. Intuitively, one can say that the θ_i perform a scalar multiplication on the entries of $\mathbb{C}^n$ whilst the permutations of $\mathrm{Sym}(n)$ permute the coordinates. The following results (cf. Lehrer–Taylor [**37**, Proposition 2.11 and Theorem 2.14], where proofs can be found, too) show that for $m, n > 1$, these groups are, up to conjugacy, precisely the imprimitive reflection groups.

Propostion 3.82. *For $m > 1$ the groups of type $G(m,p,n)$ are imprimitive unitary reflection groups. If $(m,p,n) \neq (2,2,2)$, the group $G(m,p,n)$ is irreducible.*

Theorem 3.83. *Let G be an imprimitive irreducible subgroup of $U(V)$ for a vector space V of dimension n over $\mathbb{C}$ that is generated by reflections. Then, it follows that $n > 1$ and G is conjugate to $G(m,p,n)$ for some $m > 1$ and a matching divisor p of m.*

The groups of type $G(1,1,n)$ are a well-known special case. There is an isomorphism $G(1,1,n) \cong \mathrm{Sym}(n)$ for all n. Although the natural representation $G(1,1,n)$ is a reflection group, it is not irreducible. Nevertheless, there is an irreducible representation such that the symmetric group is a primitive reflection group for $n \geq 5$ fixing the hyperplane generated by $e_1 + \cdots + e_n$.

Remark 3.84. Since the elements of $G(m,p,n)$ are composed of some $h \in A(m,p,n)$ and a permutation $\pi \in \mathrm{Sym}(n)$, it suffices to consider the action on a polynomial for these two components. This action is defined by

$$\begin{aligned}(hP)(X_1, \ldots, X_n) &\coloneqq P(\theta_1^{-1} X_1, \ldots, \theta_n^{-1} X_n) \quad \text{and} \\ (\pi P)(X_1, \ldots, X_n) &\coloneqq P(X_{\pi(1)}, \ldots, X_{\pi(n)}).\end{aligned}$$

We call in mind that the elementary symmetric polynomials in $\mathbb{C}[X_1, \ldots, X_n]$ are defined as $\sigma_k(X_1, \ldots, X_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}$ for all $k = 1, \ldots, n$ (cf. Definition 2.69). It is straightforward by the definition of the action of $G(m,p,n)$ on a polynomial that the symmetric polynomials $s_k \coloneqq \sigma_k(X_1^m, \ldots, X_n^m)$ for $k = 1, \ldots, n-1$ are $G(m,p,n)$-invariant. As we have seen in Theorem 3.28 and the succeeding Remark 3.29, a set of fundamental invariants consists of exactly n algebraically independent generators. Hence, one

last invariant polynomial is missing, this is $s_n := \sigma_n^{m/p}(X_1, \dots, X_m) = (X_1, \dots, X_m)^{m/p}$. One can demonstrate that these n invariants are actually algebraically independent (cf. Lehrer–Taylor [**37**, Proposition 2.22]) and therefore form a set of fundamental invariants. Furthermore, the degrees of $s_1, \dots, s_{n-1}$ are $m, 2m, \dots, (n-1)m$ and s_n is of degree nm/p. As their product is $n!m^n/p\,|G(m.p,n)|$, this is an example for the correctness of Theorem 3.41 (a).

6.2. Imprimitive reflection groups in $U_2(\mathbb{C})$. Now we aim at providing an example for a type of imprimitive reflection groups of rank 2. The partition in the types $\mathcal{T}$ (binary tetrahedral), $\mathcal{O}$ (binary octahedral) and $\mathcal{I}$ (binary icosahedral) arises from the classification of finite subgroups of $SU_2(\mathbb{C})$ (cf. Lehrer–Taylor [**37**, Theorem 5.14]) which are each conjugated to one of these three groups. Then, one can demonstrate that the every imprimitive finite reflection group in $U_2(\mathbb{C})$ is a normal subgroup of one of the central products $\mathcal{C}_{12} \circ \mathcal{T}, \mathcal{C}_{24} \circ \mathcal{O}$ or $\mathcal{C}_{60} \circ \mathcal{I}$ (cf. Lehrer–Taylor [**37**, Theorem 6.1]). Consequently, the emerging reflection groups are called of type $\mathcal{T}, \mathcal{O}$ or $\mathcal{I}$ depending on which group they are a normal subgroup of. Overall, there are 19 primitive reflection groups in $U_2(\mathbb{C})$ of which we will exemplarily consider the four of type $\mathcal{T}$ since the methods to determine a set of fundamental invariants are the same of all types. The ideas and methods used in the following are given by Lehrer–Taylor [**37**, Chapter 6].

First, we state that the generators of $\mathcal{T}$ (cf. Lehrer–Taylor [**37**, Theorem 5.14]) are

$$a := \frac{1}{2}\begin{pmatrix} -1-i & 1-i \\ -1-i & -1+i \end{pmatrix} \quad b := \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Then, for $\mathbf{T} := \mathcal{C}_{12} \circ \mathcal{T}$, it is indicated that there are 5 conjugacy classes of reflections with the succeeding representatives $r := ib, r_1 := \omega a, r_2 := \omega a^2, r_1^2 = \omega^2 a^2$ and $r_2^2 = \omega^2 a$ for $\omega := \exp(2\pi i/3)$. The theoretical background is that the reflections groups are obtained by determining the normal closures of the groups generated by these representatives, i.e., finding the smallest normal subgroup that contains the subgroup generated by one or multiple of these reflections. In the case of $\mathbf{T}$ the succeeding four non-conjugate groups—denoted in the same was in in the Shephard–Todd-classification—arise, where $g^{\mathbf{T}}$ denotes

Table 1. Primitive reflection groups of type $\mathcal{T}$

G	Structure	$\lvert G\rvert$	Degrees
G_4	$\langle r_1, r_1' \rangle = \langle r_1^{\mathbf{T}} \rangle$	24	4, 6
G_5	$\langle r_1, r_2' \rangle = \langle r_1^{\mathbf{T}}, r_2^{\mathbf{T}} \rangle$	72	6, 12
G_6	$\langle r, r_1 \rangle = \langle r^{\mathbf{T}}, r_1^{\mathbf{T}} \rangle$	48	4, 12
G_7	$\langle r, r_1, r_2 \rangle = \langle r^{\mathbf{T}}, r_1^{\mathbf{T}}, r_2^{\mathbf{T}} \rangle$	144	12, 12

the conjugacy class of a group element g in $\mathbf{T}$ and hence $\langle g^{\mathbf{T}} \rangle$ is its normal closure. Moreover, we set $r_i' := r r_i r$ for $i = 1, 2$. For details on the calculations that lead to this table, particulary the order and degrees, including the application of Theorem 3.41, see Lehrer-Taylor [**37**, Chapter 6.2, Table 6.1].

Aiming at explicitly computing fundamental invariants for these four groups, the first newly introduced object will be *semi-invariants*.

Definition 3.85. Let G be a group acting on a vector space V. Then, a *semi-invariant* of G is a polynomial $P \in S(V^*)$ such that there is a $\chi(g) \in \mathbb{C}^\times$ satisfying $gP = \chi(g)P$ for all $\in G$. In other words, $\chi\colon G \to \mathbb{C}^\times$ is a linear character.

Moreover, if such a semi-invariant is the trivial character, it fulfills the conditions for a "usual" invariant of G. Hence, we will proceed as follows: first, we compute semi-invariants of $\mathcal{T}$ using the next lemma. Secondly, since the values of χ will be roots of unity, we take suitable powers of these semi-invariants to obtain invariants.

Lemma 3.86. *Let Δ be an orbit of G on the 1-dimensional subspaces of $S(V^*)$. If we choose a nonzero element φ_L for each $L \in \Delta$, then their product $\prod_{L\in\Delta} \varphi_L$ is a semi-invariant of G.*

Proof. See Lehrer–Taylor [**37**, Lemma 6.4]. □

Since we aim to minimize the degree of the computed semi-invariant, we generally choose Δ such that it is generated by linear forms. In the case of $\mathcal{T}$, we start with an eigenvector $P = c_1X_1 + c_2X_2$ of the generator a satisfying $aP = \lambda \cdot P$ for some $\lambda \in \mathbb{C}$. The choice of P as an eigenvector can be justified by the fact that it helps to minimize the number of images under the group action as, e.g., a and a^2 will lie in the same one-dimensional subspace. Hence, this choice contributes to minimizing the degree of the semi-invariant in Lemma 3.86. This condition leads to

$$\begin{aligned} aP(v) = P(a^{-1}v) &= P\left(\frac{1}{2}\begin{pmatrix} -1+i & -1+i \\ 1+i & -1-i \end{pmatrix}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}\right) \\ &= v_1\left(c_1\frac{1}{2}(-1+i) + c_2\frac{1}{2}(1+i)\right) + v_2\left(c_1\frac{1}{2}(-1+i) + c_2\frac{1}{2}(-1-i)\right) \\ &= \lambda v_1c_1 + \lambda v_2c_2 = \lambda P(v). \end{aligned}$$

Thus, we have to compute an eigenvector of the matrix $\frac{1}{2}\left(\begin{smallmatrix} -1+i & -1+i \\ 1+i & -1-i \end{smallmatrix}\right) = (a^{-1})^\intercal$. This is standard linear algebra and the result is $c_1 = 1$, and $c_2 = -i + (1-i)\omega$, so we obtain $P = X_1 + (-i + (1-i)\omega)X_2$. Moreover, the eigenvalue is also the primitive 3rd root of unity ω.

Next, in order to apply Lemma 3.86, we have to consider the orbit of the action of $\mathcal{T}$ on P. For this purpose, the action gP for all $g \in \mathcal{T}$ is determined and scalar multiples are eliminated yielding the following four representatives of the linear subspaces in this orbit.

$$P_1 = X_1 f\left(-i + (1-i)\omega\right)X_2 = P; \qquad P_2 = \left(\frac{\sqrt{3}}{2} - 1 - \frac{1}{2}i\right)X_1 + \omega i X_2 = abP;$$

$$P_3 = \left(1 - \frac{\sqrt{3}}{2} - \frac{1}{2}i\right)X_1 - \omega^2 X_2 = a^2bP; \quad P_4 = iX_1\left(-1 - (1+i)\omega\right)X_2 = bP.$$

Now, according to Lemma 3.86, their product produces a semi-invariant of $\mathcal{T}$. We have

$$P_1 \cdot P_2 \cdot P_3 \cdot P_4 = \left(-2+\sqrt{3}\right)i \cdot X_1^4 + \left(4\sqrt{3}-6\right)X_1^2X_2^2 + \left(-2+\sqrt{3}\right)i \cdot X_2^4.$$

Since semi-invariants are independent of scalar factors, we multiply by $\left(\left(-2+\sqrt{3}\right)i\right)^{-1}$ to obtain

$$f_T := X_1^4 + 2i\sqrt{3}X_1^2X_2^2 + X_2^4.$$

The next step is to make use of the fact that the *Jacobian*, that is, the determinant of the Jacobi-matrix, of n semi-invariants in n variables as well as the *Hessian*, that is, the Jacobian of the first derivatives, of a semi-invariant are each semi-invariants for the same group (cf. Lehrer–Taylor [**37**, Corollary 6.7]). The Hessian matrix of f_T is

$$H(f_t) = \begin{pmatrix} 12X_1^2 + 4i\sqrt{3}X_2^2 & 8i\sqrt{3}X_1X_2 \\ 8i\sqrt{3}X_1X_2 & 4i\sqrt{3}X_1^2 + 12X_2^2 \end{pmatrix}.$$

Its determinant, the Hessian of f_T, is $\det(H(f_t)) = 48i\sqrt{3}X_1^4 + 288X_1^2X_2^2 + 48i\sqrt{3}X_2^4$, which is also scaled to acquire the semi-invariant

$$h_T \coloneqq X_1^4 - 2i\sqrt{3}X_1^2X_2^2 + X_2^4.$$

Finally, we calculate the Jacobian of f_T and h_T. The corresponding Jacobi-matrix is

$$J(f_T, h_T) = \begin{pmatrix} 4X_1^3 + 4i\sqrt{3}X_1X_2^2 & 4i\sqrt{3}X_1^2X_2 + 4X_2^3 \\ 4X_1^3 - 4i\sqrt{3}X_1X_2^2 & -4i\sqrt{3}X_1^2X_2 + 4X_2^3 \end{pmatrix}$$

with $\det(J(f_T, h_T)) = 32i\sqrt{3}X_1X_2^5 - 32i\sqrt{3}X_1^5X_2$. Normalizing this polynomial leads to the final semi-invariant

$$t_T \coloneqq X_1^5X_2 - X_1X_2^5.$$

Besides, the relation of these semi-invariants can be expressed by

$$f_T^3 - h_T^3 = 12i\sqrt{3}t_T^2.$$

Henceforward, we omit the subscript T to facilitate the notation while looking more precisely at the action of $\mathcal{T}$ on f, h and t. Note that $v = \left(\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right)$ is always supposed to be an arbitrary vector in $\mathbb{C}^2$, where $X_i(v) = v_i$. Since b acts by multiplying the entries of a vector by i and $-i$ respectively, a straightforward calculation shows that f, h and t are invariant under b. Next, the computation of af yields

$$\begin{aligned} af(v) &= f\left(a^2\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}\right) = f\left(\frac{1}{2}\begin{pmatrix} (-1+i)(v_1+v_2) \\ (1-i)(v_1-v_2) \end{pmatrix}\right) \\ &= \frac{(-1+i)^4(v_1+v_2)^4 + 2i\sqrt{3}(-1+i)^2(v_1+v_2)^2(1+i)^2(v_1-v_2)^2 + (1+i)^4(v_1-v_2)^4}{16} \\ &= \frac{-8(v_1^4 + 6v_1^2v_2^2 + v_2^4) + 8i\sqrt{3}(v_1^4 - 2v_1^2v_2^2 + v_2^4)}{16} = \omega\left(v_1^4 + 2i\sqrt{3}v_1^2v_2^2 + v_2^4\right) = \omega f(v). \end{aligned}$$

Similarly, we calculate $ah = \omega f$ and $at = t$. We will demonstrate that f, t, and powers of them suffice to provide fundamental invariants of the groups G_4 through G_7 in Table 1.

$G_4 = \langle r_1, r_1' \rangle$: For the generator $r_1 = \omega a$, it follows that

$$r_1t(v) = t(a^2\omega^2) = \omega^{12}t(a^2v) = at(v) = t(v)$$

due to the homogeneity of t and the prior results. Also due to the homogeneity of f, we get that

$$r_1f(v) = \omega^8af(v) = \omega^8\omega f(v) = f(v).$$

Moreover, for $r = ib = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, it follows that $rf = f$ because all exponents of f are even and conversely $rt = -t$ due to the exclusively odd exponents of t.
Since the action is associative, i.e., $r_1'f = (rr_1r)f = (rr_1)(rf) = r(r_1f) = rf = f$ and $r_1't = (rr_1)(-t) = -rr_1t = -rt = t$, we get that f and t fix both generators. Thus, a set of fundamental invariants is given by f and t.

$G_5 = \langle r_1, r_2' \rangle$: We have already seen that r_1 fixes f and t, and therefore any power of them is invariant under the action of r_1, too.
Since the action of r on f and t was previously investigated, we only have to look at the action of $r_2 = \omega a^2$ to find invariants for $r_2' = rr_2r$. First,

$$r_2t(v) = t(\omega^2a) = \omega^{12}t(av) = a^2t(v) = a(at(v)) = at(v) = t(v)$$

indicates that t is fixed by r_2. On the other hand, for f we have

$$r_2f(v) = f(\omega^2a) = \omega^8f(av) = \omega^8a(af(v)) = \omega^8a\omega f(v) = af(v) = \omega f(v)$$

in the same way as before. Hence, rather than f, since ω is a 3rd root of unity, f^3 is invariant under the action of r_2. Therefore, f^3 and t form a set of fundamental invariants of G_5.

$G_6 = \langle r, r_1 \rangle$: We can now rely on the computations from the two preceding cases. Based on this, since $rf = f$ and $r_1 f = f$, it follows that f is one of the desired fundamental invariants. The other one is t^2 because $rt = -t$ and $r_1 t = t$.

$G_7 = \langle r, r_1, r_2 \rangle$: In this case, by combining all earlier results, we can conclude that f^3 and t^2 are the sought-after fundamental invariants.

Remark 3.87. Recall from the end of Section 3.3 that for a set to qualify as fundamental invariants, the polynomials must be algebraically independent. Therefore, in order justify that they are named as fundamental invariants in the prior enumeration, it remains to verify that the given sets for $G_4 \ldots, G_7$ consist of algebraically independent polynomials. For this purpose, we utilize another Jacobi-criterion: a set of complex polynomials $f_1, \ldots, f_n$ in n variables is algebraically independent if and only if the corresponding Jacobi-matrix is of full rank (cf. Lehrer–Taylor [**37**, Lemma 9.5]).

At first, we show that it suffices to check the algebraic independence of f and t. Suppose that we already know that f and t are algebraically independent. Moreover, assume that, e.g., f^3 and t^2 are algebraically dependent. Hence, we can find a nonzero polynomial $H \in \mathbb{C}[Y_1, Y_2]$ such that $H(f^3, t^2) = 0$. For $i = 1, \ldots, m$, let $a_i Y_1^{k_i} Y_2^{l_i}$ be the monomials of which H consists. Then, the nonzero polynomial H' given as the sum of monomials $a_i Y_1^{3k_i} Y_2^{2l_i}$ satisfies $H'(f, t) = 0$ contradictory to the algebraic independence of f and t. This works similarly for the set $\{f^3, t\}$ as well as $\{f, t^2\}$.

Finally, the Jacobi-matrix of f and t is

$$J(f,t) = \begin{pmatrix} 4X_1^3 + 4i\sqrt{3}X_1X_2^2 & 4i\sqrt{3}X_1^2X_2 + 4X_2^3 \\ 5X_1^4X_2 - X_2^5 & X_1^5 - 5X_1X_2^4 \end{pmatrix}.$$

To check whether it has rank 2, the determinant is considered and since

$$\begin{aligned} \det(J(f,t)) &= (4X_1^3 + 4i\sqrt{3}X_1X_2^2)(X_1^5 - 5X_1X_2^4) - (4i\sqrt{3}X_1^2X_2 + 4X_2^3)(5X_1^4X_2 - X_2^5) \\ &= 4X_1^8 - 16i\sqrt{3}X_1^6X_2^2 - 40X_1^4X_2^4 - 16i\sqrt{3}X_1^2X_2^6 + 4X_2^8 \neq 0, \end{aligned}$$

it follows that the Jacobi-matrix is of rank 2 as desired. Thus, f and t form a fundamental set of invariants of G_4, and so do the further sets of generators because of the preceding observation on the algebraic independence of powers of f and t. The results are summarized by this final table (cf. Lehrer–Taylor [**37**, unnamed table at p. 96]).

TABLE 2. Fundamental invariants for the primitive reflection groups of type $\mathcal{T}$

G	$\lvert G \rvert$	Invariants	Degrees
G_4	24	f, t	4, 6
G_5	72	f^3, t	12, 6
G_6	48	f, t^2	4, 12
G_7	144	f^3, t^2	12, 12

CHAPTER 4

Outlook

This final chapter aims at presenting an outlook on several topics that are related to the previously presented theory.

Positive characteristic

Throughout this work, we usually assumed the base field to be the complex numbers $\mathbb{C}$. This facilitates the previous investigations as $\mathbb{C}$ is algebraically closed and of characteristic 0. However, one could ask whether the previously elaborated results could be transferred to the case of arbitrary fields, in particular those of positive characteristic. For an arbitrary field k one has to distinguish the following alternatives.

(a) The *non-modular* case: $\gcd(|G|, \mathrm{char}(k)) = 1$.
(b) The *modular* case: $|G| \equiv 0 \mod \mathrm{char}(k)$.

In the non-modular case, the result of the main theorem 3.24 remains valid: a group G is a reflection group if and only if the invariant algebra S^G is polynomial. A proof of this equivalence in the general non-modular case can be found, for example, in Kane [**32**, Sections 18-2–18-5]. The proof utilizes the averaging operator (cf. Definition 2.65) and thus requires that $|G|$ is invertible in the base field. Therefore, it is clear that the same methods are not applicable to the modular case, which makes it an interesting topic for further investigation.

It is already known that in the modular case, on the one hand, the implication (b) $\Rightarrow$ (a) remains valid, which was originally proven by Serre [**53**, Théorème 2]. However, the converse is false: there exist reflection groups whose invariant rings are not polynomial. A concrete counter example is presented by Toda [**66**], and Kane offers a brief description [**32**, Section 19-2]. Based on this, an interesting task for further studies might be the investigation on the strictest conditions under which such counterexamples can occur.

On the other hand, we could analyze what happens if the conditions on the invariant polynomials are relaxed: in order to regain some kind of polynomial invariants "in a suitably modified and generalized version" (Kane [**32**, p. 207]), the concept of *generalized invariants*, has been established. In this context, one could explore which further generalizations could be achieved using different relaxations on the condition of G-invariance.

The coinvariant algebra

Recall from Section 2.5.1 that J^+ is the ideal of the algebra of invariants that is formed by the G-invariant polynomials with zero constant term, and that F is the ideal of $S = \mathbb{C}[V]$—the coordinate ring of the vector space on which G acts—generated by J^+. Then, the *coinvariant algebra* of G is the quotient $\mathbb{C}[V]_G := S/F$. Note that this definition translates without changes to the case of an arbitrary field k where it is denoted by $k[V]_G$.

In the study of the relation of reflection groups and representation theory, the coinvariant algebra is valuable as it has the following advantageous property: if $k[V]^G$ is polynomial

for a finite group G, then the representation of G on $k[V]_G$ is the regular representation. As stated by Broer at al. [**6**, p.4], this was proven by Chevalley [**12**] in characteristic 0, and by Mitchell [**42**] in positive characteristic. The relation above is useful as it gives a graded version of the group algebra $k(G)$, a fundamental object in group representations, considered as regular representation (cf. Broer at al. [**6**, p. 4]). In this paper, the authors not only present further results related to this topic, but also prove more general versions of the known results, e.g., the requirement for $k\,[V]^G$ to be polynomial is replaced by a weaker condition (cf. Broer at al. [**6**, Section 1.1]). After having already seen that reflection groups are influential in representation theory, it would be intriguing to continue on this relation be elaborating it in detail in a further work.

Rational invariants

An important concept concerning unitary reflection groups is the field of definition, that is, the subfield of the complex numbers that is generated by the character values of the group. At this point, one can show that any representation of a unitary reflection group can be defined over this field, i.e., the entries of all elements of the groups, when considered as matrices, lie in the field of definition (cf. Lehrer–Taylor [**37**, Section 1.7]).

On the other hand, the question arises in which field the coefficients of fundamental invariants can be chosen. The following partial answer might be unexpected in view of the results of the computations in Section 3.6.2: if $G \subseteq GL(V)$ is an irreducible complex reflection group, where V is a vector space over a suitable field extension k' of the field of definition of G, then there is a $\mathbb{Q}$-tensor product $V = V_0 \otimes_{\mathbb{Q}} k'$ such that the fundamental invariants can be taken in $S(V_0^*)$ and thus have rational coefficients. Marin and Michel [**39**] demonstrated this as a corollary of their efforts on describing the structure of automorphisms in G.

However, there is a trade-off for the rationality of the fundamental invariants: they might be no longer unitary with respect to the standard scalar product but a suitable G-invariant Hermitian form, which must exist according to Remark 3.3. Depending on the application, it must be decided whether a simple G-invariant Hermitian form, such as the standard scalar product, or rational coefficients are more desirable. To delve deeper in this topic, one could classify the complex groups for which both are possible at the same time. Furthermore, if some groups with this property exist, we could carry on this investigation and try to understand what makes these groups distinctive.

Bibliography

1. Michael F. Atiyah and Ian G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley series in mathematics, Addison-Wesley, Reading, MA, 1969.
2. Maurice Auslander and David A. Buchsbaum, *Homological dimension in Noetherian rings*, Proc. Nat. Acad. Sci. U.S.A. **42** (1956), 36–38. MR 75190
3. David J. Benson, *Polynomial Invariants of Finite Groups*, London Mathematical Society lecture note series 190, Cambridge Univ. Press, Cambridge, UK, 1993.
4. Armand Borel, *Essays in the history of Lie groups and algebraic groups*, History of mathematics 21, American Math. Society, London Math. Society, Providence, RI, London, 2001.
5. Yuri G. Borisovich, Nikolai M. Bliznyakov, Tatyana N. Fomenko, and Yakov A. Izrailevich, *Introduction to differential and algebraic topology*, 1st ed., Texts in the Mathematical Sciences 9, Springer Netherlands, Dordrecht, 1995.
6. Abraham Broer, Victor Reiner, Larry Smith, and Peter Webb, *Extending the coinvariant theorems of Chevalley, Shephard–Todd, Mitchell, and Springer*, Proceedings of the London Mathematical Society **103** (2011), no. 5, 747–785.
7. Michel Broué, *Introduction to complex reflection groups and their braid groups*, Lecture notes in mathematics 1988, Springer, Berlin, Heidelberg, 2010.
8. Winfried Bruns and H. Jurgen Herzog, *Cohen-Macaulay rings*, rev. ed., Cambridge studies in advanced mathematics, vol. 39, Cambridge University Press, 2009.
9. David A. Buchsbaum, *Review of the article "Sur la dimension homologique des anneaux et des modules noethériens." by J.-P. Serre*, Bulletin (New Series) of the American Math. Society **34** (2007), no. 3, 439.
10. William Burnside, *Theory of groups of finite order*, reprint of the 2. ed., Dover books on intermediate and advanced mathematics, Dover Publ., New York, 1955.
11. Claude Chevalley, *The betti numbers of the exceptional simple Lie groups*, Proceedings of the international congress of Mathematicians, Cambridge, MA, vol. 2, 1950, pp. 21–24.
12. ———, *Invariants of Finite Groups Generated by Reflections*, American Journal of Mathematics **77** (1955), no. 4, 778–782.
13. Arjeh M. Cohen, *Finite complex reflection groups*, Annales scientifiques de l'École Normale Supérieure **Ser. 4, 9** (1976), no. 3, 379–436.
14. Richard Courant and Fritz John, *Introduction to Calculus and Analysis : Volume ii*, 1st ed., Springer New York, New York, NY, 1989.
15. Harold S. M. Coxeter, *The product of the generators of a finite group generated by reflections*, Duke Mathematical Journal **18** (1951), 765–782.
16. ———, *Review of the article "Finite unitary reflection groups." by G. C. Shephard and J. A. Todd*, Mathematical Reviews **59914** (1954), 1.
17. Harm Derksen and Gregor Kemper, *Computational invariant theory*, 1st ed., Encyclopaedia of Mathematical Sciences, vol. 130, Springer Berlin / Heidelberg, Berlin, Heidelberg, 2002.
18. Jean A. Dieudonné and James B. Carrell, *Invariant theory, old and new*, Advances in Mathematics **4** (1970), no. 1, 1–80.
19. David Eisenbud, *Commutative algebra: With a view toward algebraic geometry*, 1st ed., Graduate Texts in Mathematics, vol. 150, Springer New York, New York, NY, 1995.
20. Walter R. Ferrer Santos and Alvaro Rittatore, *Actions and invariants of algebraic groups*, Pure and applied mathematics 269, Chapman & Hall/CRC, Boca Raton, 2005.
21. Leopold Flatto, *Invariants of finite reflection groups*, L'Enseignement Mathématique **24** (1978), no. 1-2, 237–292.
22. Andreas Gathmann, *Algebraic Geometry*, URL: https://agag-gathmann.math.rptu.de/class/alggeom-2021/alggeom-2021.pdf, last visit on 09.09.2024, winter term 2021/22, Class Notes for a lecture held at TU Kaiserslautern.
23. Ulrich Görtz and Torsten Wedhorn, *Algebraic geometry: Part I: Schemes. With Examples and Exercises*, 1st ed., Advanced Lectures in Mathematics, Vieweg+Teubner Verlag, 2010.
24. Werner H. Greub, *Multilinear algebra*, 2nd ed., Universitext, Springer, New York, 1978.
25. Paul Hacking, *508A Lecture notes*, URL: www.math.umass.edu/~hacking/curves.pdf, last visit on 09.09.2024, march 2008, lecture notes for a second course in Algebraic geometry at the University of Washington.
26. Joe Harris, *Algebraic Geometry: A First Course*, 1st ed., Graduate texts in mathematics, vol. 133, Springer Nature, Netherlands, 2013.

27. Robin Hartshorne, *Algebraic Geometry*, 1st ed., Graduate Texts in Mathematics, vol. 52, Springer Nature, New York, NY, 2013.
28. David Hilbert, *Ueber die Theorie der algebraischen Formen*, Mathematische Annalen **36** (1890), no. 4, 473–534 (ger).
29. Melvin Hochster and John A. Eagon, *Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci*, American Journal of Mathematics **93** (1971), no. 4, 1020–1058.
30. Melvin Hochster and Joel L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Advances in Mathematics **13** (1974), no. 2, 115–175.
31. James E. Humphreys, *Hilbert's Fourteenth Problem*, The American Mathematical Monthly **85** (1978), no. 5, 341–353.
32. Richard Kane, *Reflection Groups and Invariant Theory*, CMS books in mathematics, Springer Nature, Netherlands, 2013.
33. Gottfried Köthe, *Topological Vector Spaces I*, 1st ed., Grundlehren der mathematischen Wissenschaften, A Series of Comprehensive Studies in Mathematics 159, Springer Berlin Heidelberg, Berlin, Heidelberg, 1983.
34. Tsit-Yuen Lam, *Lectures on Modules and Rings*, 1st ed., Graduate Texts in Mathematics, vol. 189, Springer New York, New York, NY, 1999.
35. Klaus Lamotke, *Regular solids and isolated singularities*, Advanced lectures in mathematics, Vieweg, Braunschweig, 1986.
36. Serge Lang, *Algebra*, rev. 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer, 2012.
37. Gustav I. Lehrer and Donald E. Taylor, *Unitary reflection groups*, Australian Mathematical Society Lecture Series 20, Cambridge Univ. Press, Cambridge, UK, 2009.
38. Charles F. Van Loan, *The ubiquitous Kronecker product*, Journal of Computational and Applied Mathematics **123** (2000), no. 1, 85–100, Numerical Analysis 2000. Vol. III: Linear Algebra.
39. Ivan Marin and Jean Michel, *Automorphisms of complex reflection groups*, Represent. Theory **14** (2009), 747–788.
40. Hideyuki Matsumura, *Commutative algebra*, 2nd ed., Mathematics lecture note series 56, Benjamin Cummings, Reading, MA, 1980.
41. ———, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1987.
42. Stephen A. Mitchell, *Finite complexes with A(n)-free cohomology*, Topology **24** (1985), no. 2, 227–246.
43. Theodor Molien, *Über die Invarianten der linearen Substitutionsgruppen*, Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin **Juli-Dec 1897** (1897), 1152–1156 (ger).
44. Masayoshi Nagata, *On the 14-th Problem of Hilbert*, American Journal of Mathematics **81** (1959), no. 3, 766–772.
45. Mara D. Neusel and Larry Smith, *Invariant theory of finite groups*, Mathematical surveys and monographs 94, American Math. Society, Providence, RI, 2002.
46. Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Mathematische Annalen **77** (1915), no. 1, 89–92 (ger).
47. ———, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1926** (1926), 28–35 (ger).
48. Victor V. Prasolov, *Polynomials*, 2004. ed., Algorithms and Computation in Mathematics, vol. 11, Springer Nature, Berlin, Heidelberg, 2004.
49. Louis J. Ratliff Jr, *Review of the article "Cohen-macaulay rings, Invariant Theory, and the Generic Perfection of Determinantal Loci." by M. Hochster and J. A. Eagon*, Mathematical Reviews **302643** (1971), 1.
50. Joseph J. Rotman, *An introduction to homological algebra*, Pure and applied mathematics, a series of monographs and textbooks 85, Academic Press, New York, 1979.
51. Johannes Schmitt, *Quotientenvarietäten — Der Gute, der Kategorielle, der Geometrische*, URL = https://joschmitt.eu/wp-content/uploads/2022/03/Schmitt-Quotientenvarietaten.pdf, last visit on 08.09.2024, September 2020, German slides for an introductory talk on quotient varieties.
52. Jean-Pierre Serre, *Sur la dimension homologique des anneaux et des modules noethériens*, Proceedings of the International Symposium on Algebraic Number Theory (Tokyo and Nikko 1955), 1956, pp. 175–189 (fre).
53. ———, *Groupes finis d'automorphisms d'anneaux locaux réguliers*, Colloque d'Algèbre (Paris) (École Normale Supérieure de Jeunes Filles, ed.), no. 8, 1967, pp. 1–11 (fre).
54. ———, *Algèbre Locale Multiplicités: Cours au Collège de France, 1957–1958 rédigé par Pierre Gabriel*, 3rd ed., Lecture Notes in Mathematics, vol. 11, Springer Berlin Heidelberg, Berlin, Heidelberg, 1975 (fre).
55. ———, *Local Algebra*, 1st ed., Springer Monographs in Mathematics, Springer, Berlin, Heidelberg, 2000, English translation by Chee Whye Chin.
56. Geoffrey C. Shephard, *Unitary Groups Generated by Reflections*, Canadian Journal of Mathematics **5** (1953), 364–383.
57. Geoffrey C. Shephard and John A. Todd, *Finite Unitary Reflection Groups*, Canadian journal of mathematics **6** (1954), 274–304.
58. Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, and William Traves, *An Invitation to Algebraic Geometry*, 1st ed., Universitext, Springer New York, New York, NY, 2000.
59. Larry Smith, *On the invariant theory of finite pseudo reflection groups*, Archiv der Mathematik **44** (1985), no. 3, 225–228.

60. ———, *Polynomial invariants of finite groups*, Research notes in mathematics 6, Peters, Wellesley, MA, 1995.
61. ———, *Polynomial invariants of finite groups. A survey of recent developments*, Bull. Amer. Math. Soc. (N.S.) **34** (1997), no. 3, 211–250. MR 1433171
62. ———, *Linear Algebra*, 3rd ed., Undergraduate Texts in Mathematics, Springer, 2012.
63. Tonny A. Springer, *Regular elements of finite reflection groups*, Inventiones mathematicae **25** (1974), no. 2, 159–198.
64. Ulrich Thiel, *On restricted rational cherednik algebras*, Phd thesis, Technische Universität Kaiserslautern, 2014.
65. ———, *Complex and symplectic reflection groups*, URL: https://ulthiel.com/math/wp-content/uploads/lecture-notes/Complex-and-symplectic-reflection-groups.pdf, last visit on 09.09.2024, march 2023, Notes for 4 lectures during the Spring School on "Real, Complex, and Symplectic Reflection Groups" at Ruhr-Universität Bochum.
66. Hirosi Toda, *Cohomology* mod 3 *of the classifying space* BF_4 *of the exceptional group* $\mathbf{F}_4$, J. Math. Kyoto Univ. **13** (1973), 97–115. MR 321086