Technische Universität Berlin

Fakultät II - Institut für Mathematik

Bachelorarbeit

in englischer Sprache

Cayley's Ω-process and the Reynolds Operator

Berthold Blatt Lorke
Matrikelnr. 361776

Erstgutachter:
Prof. Dr. Peter Bürgisser
Zweitgutachter:
Prof. Dr. Alexander Bobenko

23. März, 2018

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und eigenhändig sowie ohne unerlaubte fremde Hilfe und ausschlielich unter Verwendung der aufgeführten Quellen und Hilfsmittel angefertigt habe.

Die selbständige und eigenständige Anfertigung versichert an Eides statt:

Berlin, den 23. März 2018

____

Berthold Blatt Lorke

Deutsche Zusammenfassung

Ein wichtiges Theorem in der Invariantentheorie ist *Hilberts Endlichkeitssatz*: Ist eine Gruppe G linear reduktiv, so gilt für jede affine G-Varietät X, dass der Invariantenring $K[X]^G$ endlich erzeugt ist, das heißt es gibt $\{f_i\}_{i\in[r]} \subseteq K[X]$ sodass $K[X]^G = K[\{f_i\}_{i\in[r]}]$. Im Beweis ist die Zentrale Idee die Existenz eines *Reynolds Operators* $R\colon K[X] \twoheadrightarrow K[X]^G$, eine G-invariante lineare Projektion von $K[X]$ auf $K[X]^G$. Dieser ermöeglicht uns, Invarianten zu finden.
Eine der wichtigsten Gruppen in der Mathematik ist die allgemeine lineare Gruppe GL_n. Diese ist in der Tat linear reduktiv, was man auf verschiedene Weisen zeigen kann. Eine Möglichkeit die lineare Reduktivität nachzuweisen, ist zu zeigen, dass ein Reynolds Operator der Gruppe existiert. Die Existenz dieses Reynolds Operators wird in dieser Arbeit konstruktiv mit Hilfe von *Cayleys* Ω-*Prozess* nachgewiesen, was nicht nur zur Folge hat, dass GL_n linear reduktiv ist, soncern auch, dass wir eine explizit Formel des Reynolds Operators haben, womit wir konkret Invarianten ausrechnen können.

Contents

1 Introduction **4**

2 Preliminary work **5**
2.1 Notation 5
2.2 Concepts From Algebraic Geometry 5
2.3 Concepts From Invariant Theory 6

3 Linearly reductive groups, the Reynolds operator and Hilbert's finiteness theorem **9**
3.1 Linearly reductive groups and the Reynolds operator 10
3.2 Hilbert's finiteness theorem 14
3.3 The Reynolds operator of a group 18

4 Cayley's Ω-process **21**

5 Further discussion and conclusion **26**
5.1 A complete algorithm for retrieving generators of the invariant ring 26
5.2 Cross Ratio 27
5.3 Conclusion 28

1 Introduction

A very important concept in mathematics is the idea of an *invariant*: An object which does not change under a certain action. In 1872, Felix Klein came up with a then new method of describing geometries with group theory, called the Klein Erlangen program (see [Kle93]). Here, the central idea of a geometry is characterized by its associated symmetry group, the group of transformations which leaves certain objects or properties unchanged, for example angles. The study of these transformations is called conformal geometry.

Let us discuss the following important example in geometry: Consider all transformations which map lines to lines, meaning such transformations under which the property of being a line is invariant. The fundamental theorem of projective geometry gives us that these maps are exactly the projective transformations (see [Aud03, Ex V.44, Ex I.51]).

Conversely, we can consider projective transformations as our given group of transformations. Invariant theory asks: What invariants exist? We can loosely notice a kind of duality between geometries viewed as in the Klein Erlangen program and invariant theory. This discipline of mathematics usually only looks at invariants described with so called regular terms, or more concretely formulated: In invariant theory, we try to find invariant polynomial-like functions.

Staying with our example of considering projective transformations as our given group, a well known example for an invariant is the cross ratio. It is a rational function which takes as its input four collinear points. Is this the only invariant? How can we find other invariants? How big is the ring of all invariants?

Hilbert's finiteness theorem states that for regular actions under certain groups, such that are *linearly reductive*, the invariant ring is finitely generated. If we can find these finite generators, we have a grasp of what all invariants look like. Hilbert's first proof for this theorem, which he published in 1890 (see [Hil90]) was non-constructive. It is claimed that this proof was responsible for Gordan's famous quote "Das ist Theologie und nicht Mathematik" ("This is theology and not mathematics") (see [DK15, p.42]). The central idea of this proof is the existence of a Reynolds operator.

One of the most important and most common groups is the general linear group GL_n. This group is linearly reductive and there are multiple ways to see this. Motivated by averaging for finite groups, for compact groups it is possible to replace the sum by an integral with the Haar-measure, from which we can show that GL_n is linearly reductive (see [Kra85, p. 285-288]). One can also show linear reductivity by the Schur-Weyl-dualty: The symmetric group is finite, from which we can therefore see that in any rational GL_n-representation we can again construct module complements.

Here, we will show that GL_n is linear reductive in an even different way. For one, we want to show that a Reynolds Operator exists, which already means that GL_n is linearly reductive. But we want even more than just its existence. What does it do for our motivation to get a grasp of what all (or even just some) invariants look like, if we merely prove the existence of a finite generator set for the invariants? Since this operator projects polynomials to invariant polynomials, if we can find an explicit formula for computing the Reynolds operator applied to a polynomial, we can more easily obtain concrete invariants. This is possible with *Cayley's Ω-process*, which Arthur Cayley came up with as early as 1846 (see [Cay46]).

If we take a polynomial at random and apply the Reynolds Operator, we might just get a constant polynomial, which is not a very interesting invariant. Similar to the first proof of Hilbert's finiteness theorem (by Hilbert himself, see [DK15, p.41,42]), we can show that there are certain finitely many polynomials whose images under the Reynolds operator will generate the invariant ring. Although this is not what we will be discussing in detail, there is in fact an algorithm to compute these certain polynomials. With the help of Cayley's Ω-process, we then get a complete algorithm that gives us the generators of the invariant ring. (See [DK15, 4.1.9])
The main source of this work is Harm Derksen and Gregor Kemper's *Computational invariant theory* ([DK15]). Section 3 and section 4 in this work are in essence monographs of chapters 2.2.1 and 4.5.3 in this book, respectively.

2 Preliminary work

2.1 Notation

In the following, K is a field of characteristic 0 and G a linear algebraic group, that is a group which is an affine variety, and whose multiplication and inversion are morphisms of affine varieties.
For us, zero is an element of the natural numbers. Furthermore, for $n \in \mathbb{N}$ we write $[n] := \{ m \in \mathbb{N} \mid 1 \leq m \leq n \}$.
For an affine variety X, we denote by $K[X]$ the coordinate ring of X. If $\{f_i\}_{i\in[r]} \subseteq K[X]$ is a set of polynomials, we denote by $K[\{f_i\}_{i\in[r]}]$ the K-subalgebra of $K[X]$ generated by $\{f_i\}_{i\in[r]}$. For a finite-dimensional vector-space V, we denote by X_i, or sometomes Y_i or Z_i, the coordinate functions for a given (often a canonical) basis.
For a set of functions in the coordinate ring $F \subseteq K[X]$ we denote by $Z(F)$ the zero set of F. For a subset of a ring M, (M) denotes the ideal generated by M. If V and W are vector spaces, we denote by $V \otimes W$ the tensor product of V and W, which is equipped with the tensor product mapping $\otimes \colon V \times W \to V \otimes W$. Furhtermore, for a vector space V we denote by V^* the dual space of V, that is $V^* = L(V, K)$.

2.2 Concepts From Algebraic Geometry

Definition 2.1: Linear algebraic group
A group G equipped with the structure of an affine variety whose group operations of the multiplication and inversion are morphisms of affine varieties is called a *linear algebraic group.*

Proposition 2.2: Rabinowitsch trick
Let $V = K^n$ for some $n \in \mathbb{N} \setminus \{0\}$. For a polynomial $p \in K[V] = K[\{X_i\}_{i\in[n]}]$, the set $X_p := \{ v \in V \mid p(v) \neq 0 \}$ has the structure of an affine variety with the coordinate ring $K[X_p] = K[\{X_i\}_{i\in[n]}, p^{-1}]$.
(Compare to [Rab30])

Proof. The set X_p is not an algebraic set itself. The trick (the "Rabinowitsch-trick") is "adding an additional variable X_0". We do this as follows: Consider the algebraic set $\tilde{X}_p := Z\left(X_0 \cdot p - 1\right) \subseteq K \times V$. We then notice that we have

$\tilde{X}_p = \{ (p(v)^{-1}, v) \in K \times V \mid v \in X_p \}$. This means that X_p corresponds to $\tilde{X}_p$ via the bijection $\Phi\colon X_p \to \tilde{X}_p$, $v \leftrightarrow (1/p(v), v)$. The coordinate ring of $\tilde{X}_p$ can be written as $K[\bar{X}_0, \{\bar{X}_i\}_{i\in[n]}]$, where $\bar{X}_i = X_i \operatorname{mod}(X_0 \cdot p - 1)$. If $x \in X_p$, we have $\bar{X}_0(\Phi(v)) = p(x)^{-1}$ and for $i \in [n]$ we have $\bar{X}_i(\Phi(x)) = v_i$. This shows our claim: X_p has the structure of an affine variety with the coordinate ring $K[X] = K[\{X_i\}_{i\in[n]}, p^{-1}]$. □

Example 2.2.1: The general linear group GL_n
One of the most important examples is the general linear group GL_n. By the above proposition, this group is an affine variety with the coordinate ring $K[\{X_{i,j}\}_{i,j\in[n]}, \det^{-1}]$. This makes GL_n into a linear algebraic group.

Definition 2.3: Algebraic cohomomorphism
If $g\colon X \to Y$ is a map of affine varieties, the **algebraic cohomomorphism** of g is defined as $g^*\colon K[Y] \to K[X]$, $f \mapsto g^*(f) := f \circ g$.
Now let $m\colon U_1 \times U_2 \to W$ be a morphism of affine varieties. The algebraic cohomomorphism m^* is a map of the type $m^*\colon K[W] \to K[U_1 \times U_2]$. We have $K[U_1 \times U_2] = K[\{X_k\}_{k\in[r]}, \{Y_l\}_{l\in[s]}]$, where $\{X_k\}_{k\in[r]}$ and $\{Y_l\}_{l\in[s]}$ are generators of $K[U_1]$ and $K[U_2]$ respectively. The map

$$\begin{aligned} K[U_1 \times U_2] &\longrightarrow K[U_1] \otimes K[U_2] \\ \sum_i \lambda_i \prod_j X_j^{d_{i,j}} \prod_k Y_k^{e_{i,k}} &\longmapsto \sum_i \lambda_i \prod_j X_j^{d_{i,j}} \otimes \prod_k Y_k^{e_{i,k}} \end{aligned} \tag{1}$$

is independent of the choice of generators and independent of the representatives and therefore well-defined. This is an isomorphism, and each element of $K[U_1] \otimes K[U_2]$ seen as a polynomial function corresponds to exactly one element in $K[U_1 \times U_2]$, which means that in terms of algebraic geometry, we can view them as equal, in the sense that $K[U_1] \otimes K[U_2]$ describes the coordinate ring $K[U_1 \times U_2]$. We therefore write $m^*\colon K[W] \to K[U_1] \otimes K[U_2]$

Remark 2.3.1
One might ask why we use this notation "$K[U_1] \otimes K[U_2]$". It helps to formalize performing operations only on the "left part" or the "right part", as we will soon see. This notation is found in [DK15], but other literature such as [Stu08] don't take this approach. To give a very simple example: If G is a linear algebraic group and m is its multiplication, for $f \in K[G]$ we would write $\mathrm{id} \otimes \frac{\partial}{\partial Z_i}(m^*(f))$ as in [DK15], whereas [Stu08] would write $\frac{\partial}{\partial Y_i}(m^*(f))$, often also written as $\frac{\partial}{\partial Y_i}(f(XY))$.

2.3 Concepts From Invariant Theory

Our motivation is to look at transformations of spaces. Concretely, we will look at transformations of vector spaces and also more generally on affine varieties. These will be given by a group G that acts on an affine variety, giving the variety an additional structure. This gives rise to the notion of a G-variety. For vector spaces V we are interested in linear G-actions on V, from which we can make many first observations connecting to representation theory.
A given G-variety X induces a linear G-action on the coordinate ring $K[X]$, which equipped with this structure is the main object of interest in this work. The main question of this work is how the ring of all invariants looks like, that is asking which $f \in K[X]$ remain unchanged under the G-action.

Definition 2.4: Regular action, rational representation
Let G be a linear algebraic group and X an affine variety. We call an action $G \times X \to X$ a **regular action**, if and only if μ is a morphism of affine varieties. We say G **acts regularly on** X, and we also call X a G**-variety**.
For a finite-dimensional vector space V, let $\mu\colon G \times V \to V$ be a representation, meaning the map $\rho_\mu\colon G \to \mathrm{GL}(V)$, $\sigma \mapsto \rho_\mu(\sigma) := (v \mapsto \mu(\sigma, v))$ is well defined in the sense that it does map to $\mathrm{GL}(V)$, and it is a group homomorphism. We call a representation μ a **rational representation** if and only if ρ_μ is a morphism of affine varieties. V is also called a G**-module**.
(See [DK15, p. 31])

Example 2.4.1
If G is a linear algebraic group, then the multiplication $m\colon G \times G \to G$ defines a regular action, meaning that G itself is a G-variety.

Definition 2.5
If $\mu\colon G \times V \to V$ is a rational representation, we define for the dual space V^* a rational representation $\hat{\mu}\colon G \times V^* \to V^*$ by $(\sigma, \varphi) \mapsto \sigma.\varphi := (v \mapsto \varphi(\hat{\mu}(\sigma, v)) = \varphi(\sigma^{-1}.v))$.

Definition 2.6: Rational linear action
Let V be a vector space (not necessarily finite dimensional), and $\mu : G \times V \to V$ an action. We call μ a **rational linear action** if and only if there exists a linear map $\mu'\colon V \to K[G] \otimes V$ such that $\mu(\sigma, v) = ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu')(v)$, where $\epsilon_\sigma\colon K[G] \to K$, $p \mapsto p(\sigma)$ denotes the evualuation homomorphism of $\sigma \in G$. In other words, if for $v \in V$ we get $\mu'(v) = \Sigma_{i=1}^r p_i \otimes v_i \in K[G] \otimes V$, we then have $\mu(\sigma, v) = \Sigma_{i=1}^r p_i(\sigma) v_i$ for all $\sigma \in G$. (Compare to [DK15, A.1.7])

Remark 2.6.1
From the definition, it should immediately be apparent that rational linear actions are linear and regular.

We will shortly see that for finite dimensional vector spaces, the terms “rational linear action” and “rational representation” coincide.

Definition 2.7
Let X be an affine G-variety with the regular action $\mu\colon G \times X \to X$. We now define an action $\bar{\mu}\colon G \times K[X] \to K[X]$ via $\bar{\mu}(\sigma, f)(x) := f(\mu(\sigma^{-1}, x))$, and we write $\sigma.f(x) := f(\sigma^{-1}.x)$ for $\sigma \in G$, $f \in K[X]$ and $x \in X$. (Compare to [DK15, p. 31])
This action is obviously regular, but we easily see that it is in fact a rational linear action: If $\tilde{\mu}\colon G \times X \to X$ is the morphism of affine varieties defined by $(\sigma, x) \mapsto \tilde{\mu}(\sigma, x) := \mu(\sigma^{-1}, x)$, we can then define the linear map $\bar{\mu}' := \tilde{\mu}^*\colon K[X] \to K[G] \otimes K[X]$ with the desired properties as described in definition 2.6.

Proposition 2.8
Let X be an affine G-variety. If for $f \in K[X]$ we have $\bar{\mu}'(f) = \Sigma_{i=1}^r p_i \otimes g_i$, then for every $\sigma \in G$ we have $\bar{\mu}'(f) = \Sigma_{i=1}^r \sigma.p_i \otimes \sigma.g_i$.

Proof. Let $\tau \in G$ and $x \in X$. Then

$$\begin{aligned} \sum_{i=1}^r \sigma.p_i \otimes \sigma.g_i(\tau, x) &= \sum_{i=1}^r p_i(\sigma^{-1}\tau) \otimes g_i(\sigma^{-1}.x) \\ &= \sigma^{-1}\tau.f(\sigma^{-1}.x) \\ &= \tau.f(x) \qquad = \bar{\mu}'(f)(\tau, x) \end{aligned} \tag{2}$$

$\square$

Definition 2.9
Let V be a finite-dimensional vector space $\mu\colon G \times V \to V$ a rational representation. We then define an action $\hat{\mu}\colon G \times V^* \to V^*$, $(\sigma, \varphi) \mapsto \sigma.\varphi := (v \mapsto \varphi(\mu(\sigma^{-1}, v)) = \varphi(\sigma^{-1}.v))$, which is a rational representation of G.

Definition 2.10
Let G be a linear algebraic group with the multiplication $m\colon G \times G \to G$. For $\sigma \in G$ and for $p \in K[G]$ we define $\sigma\dot{} p := (\tau \mapsto p(\tau\sigma)) \in K[G]$.

Proposition 2.11
Let X be an affine variety and $\mu\colon G \times X \to X$ a regular action. For $f \in K[X]$, if we have $\bar{\mu}'(f) = \Sigma_{i=1}^r p_i \otimes g_i$ for some $\{g_i\}_{i\in[r]}$, then for $\sigma \in G$ we get $\bar{\mu}'(\sigma.f) = \Sigma_{i=1}^r \sigma\dot{} p_i \otimes g_i$.

Proof. For $f \in K[X]$ we have $\bar{\mu}'(f) = \Sigma_{i=1}^r p_i \otimes g_i$ for some $\{g_i\}_{i\in[r]}$. Now let $\sigma \in G$. Then for all $\tau \in G$ and for all $x \in X$ we have

$$\begin{aligned}
\bar{\mu}'(\sigma.f)(\tau, x) &= ((\epsilon_\tau \otimes \mathrm{id}) \circ \bar{\mu}')(\sigma.f)(x) \\
&= (\tau.(\sigma.f))(x) \\
&= \sum_{i=1}^r p_i(\tau\sigma) g_i(x) \\
&= \sum_{i=1}^r \sigma\dot{} p_i(\tau) g_i(x) \qquad = (\sum_{i=1}^r \sigma\dot{} p_i \otimes g_i)(\tau, x)
\end{aligned} \tag{3}$$

$\square$

Definition 2.12: locally finite
For a vector space V, we call an action $\mu\colon G \times V \to V$ **locally finite**, if and only if for every $v \in V$ there exists a G-stable finite-dimensional vector space $U \subseteq V$ such that $v \in U$.

Definition 2.13
Let V be a vector-space and $\mu\colon G \times V \to V$ an action. For $v \in V$ we define $V_v := \operatorname{span} G.v$.

Remark 2.13.1
V_v is always a G-stable subspace of V. For any G-stable subspace $W \subseteq V$ we have $V_v \subseteq W$. Therefore, an action $\mu\colon G \times V \to V$ is locally finite if and only if V_v is finite-dimensional for all $v \in V$.

Proposition 2.14
Let V be a vector space.

(a) If $\mu\colon G \times V \to V$ is a rational linear action, then the action is locally finite, and every finite-dimensional G-stable subspace W, $\mu|_{G\times W}$ is a rational representation.

(b) If V is a finite-dimensional vector space and $\mu\colon G \times V \to V$ is a rational representation, then μ is also a rational linear action.

(Compare to [DK15, A.1.8, 2.2.5])

Proof.
(a)
Assume that μ is a rational linear action. Let $v \in V$. We can write $\mu'(v) = \Sigma_{i=1}^{l} f_i \otimes v_i$. We then easily see that $V_v \subseteq \operatorname{span}\{v_i\}_{i=1}^{l}$, showing that the action is locally finite. Since μ' is linear, μ is also linear, therefore we immediately get that $\mu|_{G\times W}$ is a rational representation.
(b)
Let V be a finite-dimensional vector-space and $\mu\colon G \times V \to V$ a rational representation. This means that for all $\sigma \in G$ we have $\rho_\mu(\sigma) \in \mathrm{GL}(V)$. Let us now choose a basis $\{v_i\}_{i\in[r]}$ of V. For all $\sigma \in G$ there then exist unique $\{(\rho_\mu)_{i,j}\}_{i,j\in[r]} \subseteq K$ such that for all $i \in [r]$ we have $\mu(\sigma, v_i) = \Sigma_{k=1}^{r} (\rho_\mu)_{i,k}\, v_k$. Since the action is regular, we must have $p_{i,j} := (\mu \mapsto (\rho_\mu)_{i,k}) \in K[G]$. We now define $\mu'\colon V \to K[G] \otimes V$ as the linear extension of $v_i \mapsto \Sigma_{k=1}^{r} p_{i,k} \otimes v_k$ where for $i \in [r]$. It should be clear that μ' satisfies $\mu(\sigma, v) = ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu')(v)$ for all $\sigma \in G$ and $v \in V$. This shows that μ is a rational linear action. $\square$

Remark 2.14.1
This shows that for a finite-dimensional vector space V, an action is a rational linear action if and only if it defines a rational representation. In other words, we have shown that rational representations are exactly defined by rational linear actions on finite-dimensional vector-spaces, which justifies the choice of the names of our definitions.

Remark 2.14.2
A rational representation $\mu\colon G \times V \to V$ is of the following form:
Consider $\rho_\mu\colon G \to \mathrm{GL}(V)$. If then $a_{i,j} : G \to K$ is the function of the (i, j)-entry of ρ_μ, then $a_{i,j} \in K[G]$.

Definition 2.15: Invariants
Let X be an affine G-variety given by $\mu\colon G \times X \to X$, $(\sigma, x) \mapsto \sigma.x$. We define the set of all **invariants** of X as

$$X^G := \{\, x \in X \mid \forall g \in G : g.x = x \,\} \tag{4}$$

The given action μ induces an action $\bar{\mu}\colon G \times K[X] \to K[X]$, $(\sigma, f) \mapsto \sigma.f$ as described in definition 2.7. The **invariant ring** of the representation is defined as

$$K[X]^G := \{\, f \in K[X] \mid \forall g \in G : g.f = f \,\} \tag{5}$$

Its elements are referred to as G-**invariant**. As the name implies, $K[X]^G$ defines a subring (in fact also a K-subalgebra) of $K[X]$.

3 Linearly reductive groups, the Reynolds operator and Hilbert's finiteness theorem

An important theme in this work is the question of whether the invariant ring $K[X]^G$ is finitely generated.
The goal of this section is to prove *Hilbert's finiteness theorem*, which states that if the group G is linearly reductive, $K[V]^G$ is finitely generated. The strict definition of "linearly reductive" is a little unintuitive, but we will discuss

alternate characterizations, which will lay the groundwork for the proof the theorem.
This will also motivate Cayley's Ω-process.

3.1 Linearly reductive groups and the Reynolds operator

Definition 3.1: Linearly reductive group
Let G be a linear algebraic group. We call G **linearly reductive**, if and only if for any rational representation V, the spaces $(V^*)^G$ and V^G are dual to each other with resepct to the canonical pairing $b\colon V^* \times V \to K$, $(\varphi, v) \mapsto \varphi(v)$, that is $b|_{(V^*)^G \times V^G}$ is non-degenerate.
(Compare to [DK15, 2.2.1, 2.2.5 (a) $\Longrightarrow$ (b)])

Definition 3.2
If we have a given action of a group G on a set X, we call a map $A\colon X \to Y$ G**-invariant** if and only if we have $A(\sigma.x) = A(x)$ for all $\sigma \in G$ and $x \in X$.

Definition 3.3: Reynolds operator
Let X be an affine G-variety. A **Reynolds operator** is a G-invariant linear projection $R\colon K[X] \twoheadrightarrow K[X]^G$, that is R is a linear projection of $K[X]$ onto $K[X]^G$ satisfying $R(\sigma.f) = R(f)$ for all $\sigma \in G$ and $f \in K[X]$.
(See [DK15, 2.2.2])

Definition 3.4
Assume that V is a rational G-representation such that there exists a unique subrepresentation W of V with $V = V^G \oplus W$. We define $R_V : V \twoheadrightarrow V^G$ as the linear projection of V onto V^G along W.
(Compare to [DK15, 2.2.5 (b) $\Longrightarrow$ (c)])

Remark 3.4.1
R_V is a G-invariant projection of V onto V^G: If for $v \in V$ we write $v = u + w$ with $u \in V^G$ and $w \in W$, then for $\sigma \in G$ we have $\sigma.v = \sigma.u + \sigma.w = u + \sigma.w$ and $\sigma.w \in W$, therefore we have $R_V(\sigma.v) = u = R_V(v)$.

Lemma 3.5
Assume that G is a linear algebraic group with the following property: For every rational representation V of G there exists a unique subrepresentation W of V such that $V = V^G \oplus W$, and for this W we have $(W^*)^G = \{0\}$. The following properties hold:

(a) If V is a subrepresentation of a rational G-representation V', we then have $R_{V'}|_V = R_V$.

(b) If V is a rational representation of G and $R'_V : V \to Y$ is a G-invariant linear map with $V \subseteq Y$ for some vector space Y and $R'_V|_{V^G} = \mathrm{id}_{V^G}$, we have $R'_V = R_V$, that is R_V is unique with this property[1].

(c) If X is an affine G-variety and $R\colon K[X] \twoheadrightarrow K[X]^G$ is a Reynolds operator, then for every G-stable subspace V of $K[X]$ we have $R|_V = R_V$.

(d) If X is an affine G-variety, $R\colon K[X] \twoheadrightarrow K[X]^G$ a Reynolds operator and W is any G-stable subspace of $K[X]$, we have $R(W) = W^G$. (See [DK15, 2.2.7])

[1]We here view $R_V : V \to V^G$ as $R_V : V \to V$.

(e) If X is an affine G-variety, the Reynolds operator $R\colon K[X] \twoheadrightarrow K[X]^G$ is unique. (See [DK15, 2.2.5 (b) $\implies$ (c)])

Proof.
(a)
Let V be a subrepresentation of a rational representation V' of G. We decompose $V = V^G \oplus W$ and $V' = (V')^G \oplus W'$, where W and W' are each the unique subrepresentations of V and V' repspectively with this property as in our assumption. Let $w \in W$. We write $w = u' + w'$ where $u' \in (V')^G$ and $w' \in W'$. We choose a basis $\{u'_i\}_{i\in[r]}$ of $(V')^G$ and $\{w'_j\}_{j\in[s]}$ of W' and write $w = \Sigma_{i=1}^r \lambda_i u'_i + \Sigma_{j=1}^s \mu_j w'_j$. For $i \in [r]$, let us consider $\hat{u}'_i \in (V')^*$, the dual basis element of u'_i with respect to the basis $\{u'_i\}_{i\in[r]} \cup \{w'_j\}_{j\in[s]}$ of V'. Because of our assumption we have $(W^*)^G = \{0\}$, so we must have $\hat{u}'_i|_W = 0$, and therefore $\lambda_i = \hat{u}'_i(w) = \hat{u}'_i|_W(w) = 0$. We retrieve $u' = 0$, implying $w = w' \in W'$. We have now shown $W \subseteq W'$. Let $v \in V$. With $V^G \subseteq (V')^G$ and $R_V(v) - v \in W \subseteq W'$, we retrieve $R_{V'}(v) - R_V(v) = R_{V'}(v - R_V(v)) = 0$. This concludes $R_{V'}|_V = R_V$.
(b)
Let V be a rational representation of G, and let $R'_V\colon V \to Y$ be a G-invariant linear map where $V \subseteq Y$. Via our assumption, we can find a unique subrepresentation W of V such that $V = V^G \oplus W$. We obviously have $R'_V|_{V^G} = \mathrm{id}_{V^G} = R_V|_{V^G}$. Let $w \in W$. We choose a basis $\{w_i\}_{i\in[r]}$ of $U := \mathrm{span}(W + R'_V(w))$, and we write $R'_V(w) = \Sigma_{i=1}^r \lambda_i w_i$. Let $\{w'_i\}_{i\in[r]}$ be the basis of U^* dual to the previously mentioned basis of U. For $i \in [r]$, we have $(w'_i \circ R'_V)|_W \in (W^*)^G = \{0\}$ via our assumption, and therefore $\lambda_i = w'_i(R'_V(w)) = (w'_i \circ R'_V)|_W(w) = 0$. This means that $R(w) = 0$. We now have shown $R|_W = 0$. This concludes that $R'_V = R_V$.
(c)
This follows immediately from (b): If X is an affine G-variety and $R\colon K[X] \twoheadrightarrow K[X]^G$ is a Reynolds operator and V is a G-stable subspace of $K[X]$, we have that $R|_V : V \to K[X]$ is a linear map with $V \subseteq K[X]$ and $R_V|_{V^G} = \mathrm{id}_{V^G}$. Therefore we have $R|_V = R_V$.
(d)
Let X be an affine G-variety, $R\colon K[X] \twoheadrightarrow K[X]^G$ a Reynolds operator and W any G-stable subspace of $K[X]$. now let $w \in W$. Since W is G-stable we have $V_w \subseteq W$ and with (c) therefore $R(w) = R_{V_w}(w) \in V_w^G \subseteq W^G$. We have therefore shown $R(W) \subseteq W^G$. Also $R|_{W^G} = \mathrm{id}_{W^G}$ since $W^G \subseteq K[X]^G$, concluding $R(W) = W^G$.
(e)
This follows immediately from (c): Let X be an affine G-variety and $R_1, R_2\colon K[X] \twoheadrightarrow K[X]^G$ each a Reynolds operator. Now let $f \in K[X]$. Then $R_1(f) = R_{V_f}(f) = R_2(f)$. □

Remark 3.5.1
$K[V]_d$, that is the subspace of all homogeneous polynomials of degree d, is a G-stable subspace of $K[V]$. Since $K[V] = \bigoplus_{d\geq 0} K[X]_d$, we therefore also have $K[V]^G = \bigoplus_{d\geq 0} K[V]_d^G$, which means that all $R_{K[X]_d}$ characterize R. This is important for the proof of Hilbert's finiteness theorem.

Remark 3.5.2
Note that in lemma 3.5(e) we just showed uniqueness without mentioning ex-

istence. In the following, we see that in fact there always exists a Reynolds operator for groups with the previously described properties.

We now come to the most important theorem of this section before we prove Hilbert's finiteness theorem. We characterize linearly reductive groups in three different ways, the most important one involving the Reynolds operator. Cayley's Ω-process will later give us a concrete formula for the Reynolds operator.

Theorem 3.6
Let G be a linear algebraic group. The following are equivalent:

(a) G is linearly reductive

(b) For every rational representation V of G there exists a unique subrepresentation W with $V = V^G \oplus W$. For this subrepresentation W we have $(W^*)^G = \{0\}$.

(c) For every affine G-variety X there exists a Reynolds operator $R\colon K[X] \twoheadrightarrow K[X]^G$.

(Compare to [DK15, 2.2.5])

Proof.
(a) $\implies$ (b)
Let V be a rational representation of G. Consider the subspace $((V^*)^G)^\perp \subseteq V$. It is easily seen that this is a subrepresentation of V. Since by (a) $(V^*)^G$ and V^G are dual to each other, we have $V = V^G \oplus ((V^*)^G)^\perp$. We have shown the existence, now we shall show uniqueness. Let W be a subrepresentation of V with $V = V^G \oplus W$. Again, it is easily seen that $W^\perp \subseteq V^*$ is a subrepresentation. G must act trivially on $W^\perp \subseteq V^*$: Let $f \in W^\perp$, and let $\sigma \in G$. We have $\sigma.f \in W^\perp$ and therefore $\sigma.f - f \in W^\perp$. Now, let $v \in V$. We write $v = u + w$ for (unique) $u \in V^G$ and $w \in W$ and compute:

$$\begin{aligned}(\sigma.f - f)(v) &= (\sigma.f - f)(u) + (\sigma.f - f)(w) \\ &= f(\sigma^{-1}.u) - f(u) + 0 \\ &= f(u) - f(u) = 0\end{aligned} \tag{6}$$

Which means that $\sigma.f = f$. Hence G does act trivially on $W^\perp$. This means that $W^\perp \subseteq (V^*)^G$. But we also have $\dim W^\perp = \dim V^G = \dim (V^*)^G$, which implies $W^\perp = (V^*)^G$, and therefore also $W = (W^\perp)^\perp = ((V^*)^G)^\perp$, which concludes the claim of uniqueness. Finally, we notice that W and W^* are isomorphic representations, which also means that $(W^*)^G$ and W^G are isomorphic. Since we have $W^G = \{0\}$, we therefore must also have $(W^*)^G = \{0\}$.
(b) $\implies$ (c)
Let X be an affine G-variety. Let $f \in K[X]$. We define the map $R\colon K[X] \to K[X]^G$, $f \mapsto R_{V_f}(f)$. For $f \in K[X]$ we denote by W_f the unique subrepresentation of V_f such that $V_f = V_f^G \oplus W_f$ as in (b). This map is linear: Let $f, g \in K[X]$ and $\lambda \in K$. We notice that $V_f, V_g, V_{\lambda f+g} \subseteq V_f + V_g$, which together with lemma 3.5(a) gives us

$$\begin{aligned}R(\lambda f + g) &= R_{V_{\lambda f+g}}(\lambda f + g) \\ &= R_{V_f+V_g}(\lambda f + g) \\ &= \lambda R_{V_f+V_g}(f) + R_{V_f+V_g}(g) \\ &= \lambda R_{V_f}(f) + R_{V_g}(g) \qquad = \lambda R(f) + R(g)\end{aligned} \tag{7}$$

The map R is a projection onto $K[X]^G$, since for each $f \in K[X]$ we have $V_f^G \subseteq K[X]^G$. R is also G-invariant, since R_{V_f} is G-invariant for all $f \in K[X]$ and $V_f = V_{\sigma.f}$ for all $\sigma \in G$. This concludes that R is a Reynolds operator, which shows (c).

(c) $\Longrightarrow$ (a)

Let V be a rational representation of G and let $v \in V^G \setminus \{0\}$. We choose a basis $\{v_i\}_{i\in[r]}$ of V with $v_1 = v$. Let $\tilde{v} \in V^*$ be the dual basis vector of v with respect the aforementioned basis. We now define $p_v\colon K[V^*] \to K,\ f \mapsto f(\tilde{v})$. Consider the isomorphism of representations $\Phi\colon V \to (V^*)^*,\ w \mapsto (\varphi \mapsto \varphi(w))$. We have $(V^*)^* \subseteq K[V^*]$. Since V^* is a rational representation and since via our assumption (c) there exists a Reynolds operator $R\colon K[V^*] \twoheadrightarrow K[V^*]^G$, we can define $\psi_v := p_v \circ R \circ \Phi\colon V \to K$. Since each map is linear, we have $\psi_v \in V^*$, and since the Reynolds operator is used, we can also see that we have $\psi_v \in (V^*)^G$. We notice that since $v \in V^G$ we have $\Phi(v) \in K[V^*]^G$, implying $R(\Phi(v)) = \Phi(v)$ and therefore $\psi_v(v) = p_v(\Phi(v)) = \Phi(v)(\tilde{v}) = \tilde{v}(v) = 1 \neq 0$. This implies that $b|_{(V^*)^G \times V^G}$ is non-degenerate in the left variable.

By what we just showed, if we take any linear invariant $\varphi \in (V^*)^G \setminus \{0\}$, we receive an $A_\varphi \in ((V^*)^*)^G$ such that $A_\varphi(\varphi) = 1$. Since Φ is an isomorphism of representations, we have $v_\varphi := \Phi^{-1}(A_\varphi) \in V^G$ and $\varphi(v_\varphi) = \varphi(\Phi^{-1}(A_\varphi)) = A_\varphi(\varphi) = 1$. This shows that $b|_{(V^*)^G \times V^G}$ is also non-degenerate in the second variable.

This concludes that G is linearly reductive, showing (a). □

Theorem 3.7

If K is an algebraically closed field, then a linear algebraic group G is linearly reductive if and only if for every rational representation V of G and subrepresentation W of V there exists a subrepresentation Z of V such that $V = W \oplus Z$. (See [DK15, 2.2.5])

Proof. Assume that G is linearly reductive and let V be a rational representation of G.

Let us first assume that we have an irreducible subrepresentation W of V. We can identify $\operatorname{Hom}_K(W,V)^*$ with $\operatorname{Hom}_K(V,W)$ via the isomorphism

$$\begin{array}{rccc} \Phi\colon & \operatorname{Hom}_K(W,V)^* & \longrightarrow & \operatorname{Hom}_K(V,W) \\ & A & \longmapsto & (B \mapsto k^{-1}\operatorname{tr}(A \circ B)) \end{array} \tag{8}$$

where $k \in \mathbb{N}$ is the dimension of W. If we let G act on $\operatorname{Hom}_K(W,V)$ by $\sigma.B := w \mapsto \sigma.(B(w))$ and on $\operatorname{Hom}_K(V,W)$ by $\sigma.A := v \mapsto A(\sigma^{-1}.v)$, we then receive Φ as an isomorphism of representations. Now let $B \in \operatorname{Hom}_K(W,V)^G$ be the inclusion map. Since G is linearly reductive, there exists an $A \in \operatorname{Hom}_K(V,W)^G$ such that $k^{-1}\operatorname{tr}(A \circ B) \neq 0$. Since K is algebraically closed and since W is irreducible, Schur's lemma (see [FH91, 1.7]) gives us that $A \circ B$ must be a non-zero multiple of the identity map. Therefore, if Z is the kernel of A, which is a subrepresentation of V since A is G-invariant, we have $V = W \oplus Z$ as a decomposition of representations.

Now let us prove the claim for an arbitrary subrepresentations W of V by induction over $k := \dim W$. If $k = 0$ the statement is trivial. Assume that for $k \in \mathbb{N}$ the statement is true for all $m \leq k$. Now let $\dim W = k+1$. We choose a non-trivial irreducible subrepresentation of W, say $W' := \operatorname{span} G.w$ for some

$w \in W \setminus \{0\}$. By what we showed, there exists a subrepresentation Z' of V such that $V = W' \oplus Z'$. We also have that $W \cap Z'$ is a subrepresentation V and $W = W' \oplus W \cap Z'$. Since W' is non-trivial, we get $\dim W \cap Z' \leq k$, and therefore by induction hypothesis there exists a subrepresentation Z of Z' such that $Z' = W \cap Z' \oplus Z$. We then have $V = W' \oplus Z' = W' \oplus W \cap Z' \oplus Z = W \oplus Z$. This shows the forwards implication of our initial claim.
Now assume that for every rational representation V of G and subrepresentation W of V there exists a subrepresentation Z of V such that $V = W \oplus Z$. Let V be a rational representation of G. By our assumption there exists a subrepresentation W of V such that $V = V^G \oplus W$. If we have $v \in V^G \setminus \{0\}$, we can extend to a basis B_{V^G} of V^G with $v \in B_{V^G}$. Now we choose any basis B_W of W and can define $\varphi_v \in V^*$ to be the dual vector of v with respect to the basis $B_{V^G} \cup B_W$ of V. We then have $\varphi_v \in (V^*)^G$ and $\varphi_v(v) = 1 \neq 0$. This shows that $b|_{(V^*)^G \times V^G}$ is non-degenerate in the left variable. We use the same steps to show non-degeneracy in the right variable: By assumption, we there exists a subrepresentation Z of V^* with $V^* = (V^*)^G \oplus Z$. If we have $\varphi \in (V^*)^G \setminus \{0\}$, we can choose a basis $B_{(V^*)^G}$ of $(V^*)^G$ with $\varphi \in B_{(V^*)^G}$. Now, for some basis B_Z of Z we define $v_\varphi \in V$ to be the dual vector of φ with respect to the basis $B_{(V^*)^G} \cup B_Z$ of V^*. We notice that $v_\varphi \in V^G$ and $\varphi(v_\varphi) = 1 \neq 0$, showing that $b|_{(V^*)^G \times V^G}$ is non-degenerate in the right variable. This concludes that G is linearly reductive.
We have now proven both implications of our claim. $\square$

3.2 Hilbert's finiteness theorem

Proposition 3.8
Let G be a linearly reductive group, and let $R\colon K[X] \twoheadrightarrow K[X]^G$ be the Reynolds operator for an affine G-variety X. If $f \in K[X]^G$ and $g \in K[X]$ we have $R(fg) = fR(g)$, that is, the Reynolds operator is a $K[X]^G$*-module homomorphism.*
(See [DK15, 2.2.7])

Proof. Let $f \in K[X]^G$ and $g \in K[X]$. By theorem 3.6, we can decompose $V_g = V_g^G \oplus W_g$ uniquely, where W_g is a subrepresentation of V_g, and we also have $(W_g^*)^G = \{0\}$. fV_g is also a representation of G with subrepresentations fV_g^G and fW_g of G and we notice that $(fV_g)^G = fV_g^G$. We easily check that the map $R'_{V_g}: fV_g \to fV_g$, $fh \mapsto fR(h)$ is a G-invariant linear map with $R'_{fV_g}\Big|_{(fV_g)^G} = \mathrm{id}_{(fV_g)^G}$, which by lemma 3.5(b) means that we have $R'_{(fV_g)} = R_{(fV_g)}$, which implies that we have $R(fg) = fR(g)$, concluding that R is a $K[X]^G$-module homomorphism. $\square$

Theorem 3.9: Hilbert's finiteness theorem
If G is linearly reductive and V is a finite-dimensional rational G-representation, the invariant ring $K[V]^G$ is finitely generated.

Proof. Let $I_{>0}$ denote the ideal generated by all non-constant invariants in $K[V]$. Since $K[V]$ is noetherian [Bos13, p. 131], there exist finitely many linearly independent invariants $\{f_i\}_{i\in[r]} \subseteq K[V]^G$ such that $\big(\{f_i\}_{i\in[r]}\big) = I_{i>0}$. We claim $K[\{f_i\}_{i\in[r]}] = K[V]^G$. The inclusion "$\subseteq$" is clear. To show is $\supseteq$". This is equivalent to showing that for all $d \in \mathbb{N}$ we have $K[V]^G_{<d} \subseteq K[\{f_i\}_{i\in[r]}]$. We

will show our claim via induciton over the degree d. For $g \in K[V]^G_{<1} = K$ we are already done since $K \subseteq K[\{f_i\}_{i\in[r]}]$. Now assume that for $d \in \mathbb{N}$ we have $K[V]^G_{<d} \subseteq K[\{f_i\}_{i\in[r]}]$. Let $g \in K[V]^G_{<d+1}$. By construction, $g \in I_{>0}$, therefore there exist $\{g_i\}_{i\in[r]} \subseteq K[V]$ such that $g = \Sigma_{i=1}^r g_i f_i$. Since the f_i are non-constant and linearly independent, and since $\deg g < d+1$, we must have $\deg g_i < d$. We now make use of the Reynolds Operator:

$$g = R(g) = R\left(\sum_{i=1}^{r} g_i f_i\right) = \sum_{i=1}^{r} R(g_i) f_i \tag{9}$$

Since R maps $K[V]_{<d}$ to $K[V]^G_{<d}$, we have $R(g_i) \in K[V]^G_{<d} \subseteq K[\{f_i\}_{i\in[r]}]$ by our induction hypothesis. This finally implies $g \in K[\{f_i\}_{i\in[r]}]$, which concludes our proof: We have $K[V]^G = K[\{f_i\}_{i\in[r]}]$ which means that $K[V]^G$ is finitely generated, which was to show. $\square$

Example 3.9.1
Let K be an algebraically-closed field. Consider GL_n viewed as the group of all change-of-coordinates transformations for endomorphisms on K^n, that is the rational representation

$$\begin{aligned} \mu\colon \quad \mathrm{GL}_n \times V &\longrightarrow V \\ (\sigma, A) &\longmapsto \sigma A \sigma^{-1} \end{aligned} \tag{10}$$

where $V = K^{n\times n}$ We will later show that GL_n is linearly reductive. Hilbert's finiteness theorem then gives us that $K[V]^{\mathrm{GL}_n}$ is finitely generated.
What are the invariants? The invariants are exactly those polynomials that are independent of the choice of the basis. The most well-known invariant is the determinant. From this observation we can find even more: We can follow that the characteristic polynomial of a matrix A, that is $\det(tI_n - A)$, does not change under a change of coordinates. If we write

$$\det(tI_n - A) = \sum_{i=0}^{n} p_i(A) t^i \tag{11}$$

this means that every p_i is an invariant polynomial in $K[V]$. This is how one usually proves that the trace, denoted by tr, is an invariant polynomial after observing that $p_{n-1} = \mathrm{tr}$. This raises the question if there other invariants than these p_i. It is in fact the case that we have $K[V]^{\mathrm{GL}_n} = K[\{p_i\}_{0\le i\le n}]$.

Proof. Consider $D := \{\, \delta \in V \mid \delta \,\text{diagonalizable}\,\} \subseteq K[V]$. Since $M := \{\, A \in V \mid \mathrm{disc}(\det(tI_n - A)) \neq 0 \,\}$ is Zariski-open and therefore Zariski-dense in V, and since $M \subseteq D$, we also have that D is Zariski-dense in V. For this reason, we will look at the evaluation of an invariant polynomial $p \in K[V]$ only on elements in D, and can deduce what polynomial it is.
Let $p \in K[V]^{\mathrm{GL_n}}$. We define a projection onto the diagonal: $\pi\colon K^{n\times n} \twoheadrightarrow K^n, [A_{i,j}]_{i,j\in[n]} \longmapsto (A_{i,i})_{i\in[n]}$. Consider $\tilde{p} := p \circ \mathrm{diag}$[1]. We claim that $\tilde{p}$ is S_n-invariant: If $M_\tau \in \mathrm{GL}_n$ is the permutation matrix corresponding to $\tau \in S_n$,

[1] $\mathrm{diag}\colon K^n \to K^{n\times n}$, $(x_i)_{i\in[n]} \mapsto [\delta_{i,j} x_i]_{i,j\in[n]}$ is the embedding of K^n as diagonal matrices in $K^{n\times n}$.

then for all $\tau \in S_n$ and for all $X \in K^n$ we have

$$\begin{aligned}\tau.\tilde{p}(X) &= \tilde{p}(\tau^{-1}.X) \\ &= p(\operatorname{diag}(\tau^{-1}.X) \\ &= p(M_\tau^{-1} \cdot \operatorname{diag}(X)) \\ &= M_\tau.p(\operatorname{diag}(X)) \\ &= p(\operatorname{diag}(X)) &= \tilde{p}(X)\end{aligned} \tag{12}$$

From the fundamental theorem of symmetric polynomials we can follow that $\tilde{p} \in \operatorname{span}\{e_i\}_{i=0}^n$, say $\tilde{p} = \Sigma_{i=0}^n \lambda_i e_i$, where $\{e_i\}_{i=0}^n$ are the elementary symmetric polynomials of dimension n. Now, for a choice of $\sigma_A \in \mathrm{GL}_n$ such that $\sigma_A.A$ is diagonal, we easily see that for $s(A) := \sigma_A.A$ we get $p = p \circ s = \tilde{p} \circ \pi \circ s$, therefore $p = \Sigma_{i=0}^n \lambda_i e_i \circ \pi \circ s$. Now we want to show that $e_i \circ \pi \circ s = p_i$, which would conclude our claim. For all $A \in D$ we have

$$\begin{aligned}\sum_{i=0}^n (e_i \circ \pi \circ s)(A)t^i &= \det(t - \sigma_A.A) \\ &= \det(t - A) &= \sum_{i=0}^n p_i(A)t^i\end{aligned} \tag{13}$$

This shows our claim. ☐

We have now directly shown that the invariant ring $K[V]^{\mathrm{GL}_n}$ is finiteley generated. We will later show that GL_n is linearly reductive. Hilbert's finiteness theorem then gives us the immediate answer, though without giving us the generators of the invariant ring.

Example 3.9.2
Assume that K is algebraically closed. Consider the group $G = \mathrm{SL}_n$ and the vector space $V = \left\{ A \in K^{n\times n} \mid A^T = A \right\}$. Now we will look at the following action:

$$\begin{aligned}\mu\colon \quad \mathrm{SL}_n \times V &\longrightarrow V \\ (S, A) &\longmapsto SAS^T\end{aligned} \tag{14}$$

which defines a rational representation of SL_n. We claim that $K[V]^{\mathrm{SL}_n} = K[\det(Z)]$[1].

Proof. For $B \in K^{n,n}$, we define $A' := \operatorname{diag}(b_i)_{i\in[n]}$ where $b_1 := \det(B)$ and $a_i := 1$ for $2 \leq i \leq n$ as in corollary 4.4.1. Now assume that $f \in K[V]^{\mathrm{SL}_n}$. Define $h := (B \mapsto f(B')) \in K[\det(Z)]$. We claim that $f = h$. Since $X := \{ A \in V \mid \det(A) \neq 0 \}$ is zariski-dense in V, we have $g_1(A) = g_2(A)$ for all $A \in X$ if and only if $g_1 = g_2$ for $g_1, g_2 \in K[V]$. Now let $A \in X$. There exists a $\sigma \in \mathrm{SL}_n$ such that $\sigma.A = \sigma A \sigma^T$ is a diagonal matrix, say $\sigma.A = \operatorname{diag}(\lambda_i)_{i\in[n]}$ (See [Fis14, p. 325]). We have $\det(A) = \prod_{i=1}^n \lambda_i$. Since $A \in X$, we have $\lambda_i \neq 0$ for all $i \in [n]$. Using that K is algebraically closed, we define $\nu_1 := (\prod_{i=2}^n \lambda_i)^{1/2}$ and $\nu_i := \lambda_i^{-1/2}$ for $2 \leq i \leq n$ and obtain $\tau := \operatorname{diag}(\nu_i)_{i\in[n]} \in \mathrm{SL}_n$. This leads to us having $\tau.\operatorname{diag}(\lambda_i)_{i\in[n]} = A'$, implying $f(A) = (\tau\sigma)^{-1}.f(A) = f(A') = h(A)$, which shows $f = h \in K[\det(Z)]$. Conversely, it should be clear that we have $K[\det(Z)] \subseteq K[V]^{\mathrm{SL}_n}$, which concludes $K[\det(Z)] = K[V]^{\mathrm{SL}_n}$. ☐

[1] $Z = [Z_{\min\{i,j\},\max\{i,j\}}]_{i,j\in[n]}$ is to be viewed as the symmetric matrix of the coordinate functions $\{Z_{i,j}\}_{i,j\in[n],i<j}$ of V.

As in the previous example, we have shown that the invariant ring $K[V]^{\mathrm{SL}_n}$ is finitely generated without Hilbert's finiteness theorem, which after we show that SL_n is linearly reductive, gives us the answer that the invariant ring is finitely generated more quickly.

Lemma 3.10
See [DK15, 2.2.8]
Let K be an algebraically closed filed and V and W be rational representations of a linearly reductuve group G. For a surjective G-equivariant linear map $A\colon V \twoheadrightarrow W$ we then have $A(V^G) = W^G$.

Proof. Let $A\colon V \twoheadrightarrow W$ be a surjective G-equivariant linear map. Let $Z := \ker A$, which is a subrepresentation of V since A is G-equivariant. Since G is linearly reductive and since K is algebraically closed, we can apply theorem 3.7 and get a subrepresentation W' of V such that $V = Z \oplus W'$. This yields an isomorphism of representations $A|_{W'} : W' \xrightarrow{\sim} W$, which implies $A(V^G) = A(Z^G + W'^G) = A(W'^G) = A(W')^G = W^G$. $\square$

Lemma 3.11
See [DK15, A1.9].
Let X be an affine G-variety. Then there exists a rational representation V of G and a G-equivariant embedding $i\colon X \hookrightarrow V$.

Proof. We choose generators $\{f_i\}_{i\in[r]}$ of $K[X]$ and define $W := \sum_{i\in[r]} V_{f_i}$, which is a finite-dimensional G-stable subspace of $K[X]$ containing $\{f_i\}_{i\in[r]}$. This gives us the G-invariant morphism of affine varieties $i\colon X \to W^*$, $x \mapsto (w \mapsto w(x))$. This is injective, since W contains a generating set of $K[X]$, which means that i is an embedding. $\square$

Example 3.11.1: The domain of the cross ratio
We would like to look at four distinct points in the projective line over an algebraically closed field K. Since the projective line isn't an affine variety, we will look at points in K^2 to make the situation affine and regular, which will make some things different from the setting in projective geometry.
Consider $(K^2)^4$ and the coordinate functions $\{(X_i)_k\}_{i\in[4],k\in[2]}$. We write $X_i = \binom{(X_i)_1}{(X_i)_2}$ for $i \in [4]$. Define $q := \prod_{i,j\in[r],i<j} \det(X_i, X_j)$. As described in 2.2, we have an affine variety

$$X := \{\, (x_1, x_2, x_3, x_4) \in (K^2)^4 \mid q(x_1, x_2, x_3, x_4) \neq 0 \,\} \tag{15}$$

with the coordinate ring $K[X] = K[\{(X_i)_k\}_{i\in[4],k\in[2]}, q^{-1}]$. Now consider the rational linear action of GL_2 on X via pointwise application, that is $\mu\colon\ \mathrm{GL}_2 \times X \to X$, $(\sigma, (x_1, x_2, x_3, x_4)) \mapsto (\sigma x_1, \sigma x_2, \sigma x_3, \sigma x_4)$. The Rabinowitsch-trick gives us the inclusion $i\colon X \hookrightarrow K \times (K^2)^4$ as described in proposition 2.2. If we define an action on $K \times (K^2)^4$ by $(\sigma, (z, x_1, x_2, x_3, x_4)) \mapsto (\det(\sigma)^{-6} z, \sigma x_1, \sigma x_2, \sigma x_3, \sigma x_4)$, it should be clear that i is a GL_2-equivariant morphism of affine varieties.

Lemma 3.12
See [DK15, 2.2.9].
Assume that K is algebraically closed and that G is linearly reductive. Let X be an affine G-variety, V a rational representation of G and $i\colon X \hookrightarrow V$ a G-equivariant embedding. The surjective G-equivariant ring homomorphism $i^*\colon K[V] \twoheadrightarrow K[X]$ then has the property $i^*(K[V]^G) = K[X]^G$.

Proof. We obviously have $i^*(K[X]^G) \subseteq K[X]^G$. Now let $f \in K[X]^G$. We have that $V_f = \operatorname{span}(f)$ is a G-stable subspace of $K[X]$, and since i^* is surjective, there exists a $g \in K[V]$ such that $i^*(g) = f$. Since i^* is G-equivariant, $\operatorname{span} g$ is a G-stable subspace of $K[V]$ with $i^*(\operatorname{span} g) = \operatorname{span}(f)$. By lemma 3.10 we have $i^*((\operatorname{span} g)^G) = (\operatorname{span} f)^G$, in particular $f \in i^*((\operatorname{span} g)^G) \subseteq i^*(K[V]^G)$. This concludes $i^*(K[V]^G) = K[X]^G$. $\square$

Theorem 3.13: Hilbert's finiteness theorem for affine varieties
If K is an algebraically closed field, G a linearly reductive group and X is an affine G-variety, $K[X]^G$ is finitely generated.

Proof. By lemma 3.11, there exists a rational representation V of G and and an embedding $i\colon X \hookrightarrow V$. By theorem 3.9 there exist $\{f_i\}_{i\in[r]} \subseteq K[V]$ such that $K[V]^G = K[\{f_i\}_{i\in[r]}]$. By lemma 3.12 we have $K[X]^G = i^*(K[V]^G) = i^*(K[\{f_i\}_{i\in[r]}]) = K[\{i^*(f_i)\}_{i\in[r]}]$, which shows that $K[X]^G$ is finitely generated. $\square$

Example 3.13.1: The domain of the cross ratio
Consider example 3.11.1, that is the affine GL_2-variety $X := \{\, (x_1, x_2, x_3, x_4) \in (K^2)^4 \mid q(x_1, x_2, x_3, x_4) \neq 0 \,\}$, where $q := \prod_{i,j\in[r],i<j} \det(X_i, X_j)$, with the coordinate ring $K[X] = K[\{(X_i)_k\}_{i\in[4],k\in[2]}, q^{-1}]$ and the linear rational action by pointwise application, that is $\mu\colon \mathrm{GL}_2 \times X \to X$, $(\sigma, (x_1, x_2, x_3, x_4)) \mapsto (\sigma x_1, \sigma x_2, \sigma x_3, \sigma x_4)$. Our condition $q(x_1, x_2, x_3, x_4) \neq 0$ is equivalent to saying that for $i \neq j$ we have $x_i \notin \operatorname{span} x_j$, which allows us to define the cross ratio $\mathrm{cr} \in K[X]$ as follows

$$\begin{aligned} \mathrm{cr}\colon \qquad & X \to K \\ (x_1, x_2, x_3, x_4) &\longmapsto \frac{\det(x_1, x_2)\det(x_3, x_4)}{\det(x_2, x_3)\det(x_4, x_1)} \end{aligned} \tag{16}$$

This map, along with the maps $\{\mathrm{cr}(X_{\pi_1}, X_{\pi_2}, X_{\pi_3}, X_{\pi_4})\}_{\pi\in S_4}$, is an invariant. This is very important in projective geometry.
We now ask question of how many other invariants exist. In this affine setting, Hilbert's finiteness theorem gives us that the ring of all invariants $K[X]$ is finitely generated, but it does not give us an idea of what they look like, or if invariants other than the ones mentioned exist.

3.3 The Reynolds operator of a group

In theorem 3.6 we have learned about differnet characterizations of linearly reductive groups, but for a given linear algebraic group, it is still hard to concretely show that it is linearly reductive. We will now learn about an additional way to characterize linearly reductive groups, which will directly motivate Cayley's Ω-process.

Definition 3.14: Reynolds operator of a group
Let G be a linear algebraic group. The multiplication $m\colon G \times G \to G$ makes G a G-variety. Assume that for this action there exists a Reynolds operator $R_G\colon K[G] \twoheadrightarrow K[G]^G = K$ which is G-invariant from the left and from the right, that is for all $\sigma \in G$ and $p \in K[G]$ we not only have $R_G(\sigma.p) = R_G(p)$, but also $R_G(\sigma\dot{}p) = R_G(p)$ (see definition 2.10). We call R_G the *Reynolds operator of* G.

We notice that the Reynolds operator R_G of a group G is an element of the dual space of the coordinate ring $K[G]^*$. In the following, we will define a K-algebra structure on $K[G]^*$, after which we can give any G-module V the structure of a $K[G]^*$-module.

Definition 3.15
Define the multiplication on $K\left[G\right]^*$, denoted by $*$, as follows: For $\alpha, \beta \in K\left[G\right]^*$:

$$\alpha * \beta := (\alpha \otimes \beta) \circ m^* \tag{17}$$

More slowly: If for $f \in K\left[G\right]$ we have $m^*\left(f\right) = \Sigma_i g_i \otimes h_i \in K[G] \otimes K[G]$, we then get $\left(\alpha * \beta\right)\left(f\right) = \Sigma_i \alpha\left(g_i\right)\beta\left(h_i\right)$.

Proposition 3.16
The multiplication $*$ makes $K\left[G\right]^*$ into an associative algebra with the neutral element $\epsilon := \epsilon_e$ (Note: $\epsilon_\sigma\left(f\right) = f\left(\sigma\right)$).
(See [DK15, A2.2])

Proof. From the associativity of the multiplication of the group G, that is for all $\alpha, \beta, \mu \in G$ we have $m(m(\alpha, \beta), \mu) = m(\alpha, m(\beta, \mu))$, we observe that

$$(m^* \otimes \mathrm{id}) \circ m^* = (\mathrm{id} \otimes m^*) \circ m^* \tag{18}$$

holds true.e. Then, for $\delta, \gamma, \varphi \in K\left[G\right]^*$:

$$\begin{aligned} (\delta * \gamma) * \varphi &= (((\delta \otimes \gamma) \circ m^*) \otimes \varphi) \circ m^* \\ &= ((\delta \otimes \gamma) \otimes \varphi) \circ (m^* \otimes \mathrm{id}) \circ m^* \\ &= (\delta \otimes (\gamma \otimes \varphi)) \circ (\mathrm{id} \otimes m^*) \circ m^* \\ &= (\delta \otimes ((\gamma \otimes \varphi) \circ m^*)) \circ m^* \qquad = \delta * (\gamma * \varphi) \end{aligned} \tag{19}$$

showing the associativity. It should be clear that ϵ is the neutral element. This concludes that $K\left[G\right]^*$ is an associative algebra. $\square$

Definition 3.17
Let $\mu \colon G \times V \to V$ be a rational linear action, from which we retrieve $\mu' \colon V \to K[G] \otimes V$ as described in definition 2.6, that is, we have $\mu(\sigma, v) = ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu')(v)$ for all $\sigma \in G$ and $v \in V$, where $\epsilon_\sigma \colon K[G] \to K$, $p \mapsto p(\sigma)$ describes the evaluation homomorphism for $\sigma \in G$. For $\delta \in K[G]^*$ and for $v \in V$ we define:

$$\delta \cdot v := \left((\delta \otimes \mathrm{id}) \circ \mu'\right)(v) \tag{20}$$

Proposition 3.18
Definition 3.17 defines a $K[G]^*$-module structure on V.
(See [DK15, A2.10])

Proof. First, we show that this definition defines a group action. We define $\dot{m} \colon G \times G \to G$ by $(\sigma, \tau) \mapsto m(\tau, \sigma)$. We can then observe that

$$(\mathrm{id} \otimes \mu') \circ \mu' = (\dot{m}^* \otimes \mathrm{id}) \circ \mu' \tag{21}$$

using the fact that μ is an action. For any $\gamma, \delta \in G$ and $v \in V$ we therefore get

$$\begin{aligned} \gamma \cdot (\delta \cdot v) &= ((\gamma \otimes \mathrm{id}) \circ \mu' \circ (\delta \otimes \mathrm{id}) \circ \mu')(v) \\ &= ((\gamma \otimes \mathrm{id}) \circ (\delta \otimes \mathrm{id} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \mu') \circ \mu')(v) \\ &= ((\delta \otimes \gamma \otimes \mathrm{id}) \circ (\dot{m}^* \otimes \mathrm{id}) \circ \mu')(v) \\ &= ((((\gamma \otimes \delta) \circ m^*) \otimes \mathrm{id}) \circ \mu')(v) \qquad = (\gamma * \delta) \cdot v \end{aligned} \tag{22}$$

This concludes that our definition yields an action. Since all operations are linear, we also get that V is a $K[G]^*$-algebra-module. $\square$

If we look at definition 2.6, we can see that for a given G-module V, this newly defined $K[G]^*$-action is an extension of the given G-action in the following way: The subgroup $\{\, \epsilon_\sigma \mid \sigma \in G \,\}$ of $K[G]^*$ is isomorphic to G, and its induced action coincides with the given action: For $\sigma \in G$ and for $v \in V$ we have:

$$\sigma.v = \epsilon_\sigma \cdot v \tag{23}$$

This extension enables us to let R_G act on elements in V, which leads to a quite practical result.

Theorem 3.19
Let G be a group for which a Reynolds operator exists as in defintion 3.14, and let G act regularly on an affine variety X, which induces a rational linear G-action on $K[X]$ as described in definition 2.7, which in turn gives $K[X]$ the structure a $K[G]^*$-algebra-module structure as described in definition 3.17 and proposition 3.18. We notice that we have $R_G \in K[G]^*$. Then the following map

$$\begin{array}{rrcl} R\colon & K[X] & \longrightarrow & K[X]^G \\ & f & \longmapsto & R_G \cdot f \end{array} \tag{24}$$

defines a Reynolds operator.

Proof. As per our construction from definition 3.17, the linearity of this map should be clear. Let $f \in K[X]$, $\sigma \in G$ and $x \in X$. Write $\bar{\mu}'(f) = \Sigma_i p_i \otimes g_i \in K[G] \otimes K[X]$. Now we compute:

$$\begin{aligned} \sigma.\left(R_G \cdot f\right)(x) &= \left(R_G \cdot f\right)\left(\sigma^{-1}.x\right) \\ &= \Sigma_i R_G\left(p_i\right)\sigma.g_i\left(x\right) \\ &= \Sigma_i R_G(\sigma.p_i)\sigma.g_i(x) \\ &= \left(R_G \otimes \mathrm{id}\right)\left(\Sigma_i \sigma.p_i \otimes \sigma.g_i\right)(x) \\ &= (R_G \otimes \mathrm{id})(\bar{\mu}'(f))(x) \qquad\qquad = (R_G \cdot f)(x) \end{aligned} \tag{25}$$

We made use of the G-invariance of R_G and proposition 2.8. This means that we have $R(K[X]) \subseteq K[X]^G$. If $f \in K[V]^G$, we have $\bar{\mu}'(f) = 1 \otimes f$, therefore $R(f) = R_G \cdot f = R_G(1)f = f$. This gives us $R|_{K[X]^G} = \mathrm{id}_{K[X]^G}$, showing that R is a projection of $K[X]$ onto $K[X]^G$.
Now let $\sigma \in G$, $f \in K[X]$, and assume $\bar{\mu}'(f) = \Sigma_{i=1}^r p_i \otimes g_i \in K[G] \otimes K[X]$. Making use of proposition 2.11, we then get

$$\begin{aligned} R_G \cdot \sigma.f &= \left(R_G \otimes \mathrm{id}\right)\left(\bar{\mu}'(\sigma.f)\right) \\ &= \left(R_G \otimes \mathrm{id}\right)\left(\sum_{i=1}^r \sigma^{\cdot} p_i \otimes g_i\right) \\ &= \sum_{i=1}^r R_G(\sigma^{\cdot} p_i) g_i \\ &= \sum_{i=1}^r R_G(p_i) g_i \qquad\qquad = R_G \cdot f \end{aligned} \tag{26}$$

This shows that R is G-invariant, which concludes that R is the Reynolds operator. $\square$

Corollary 3.19.1
If the Reynolds operator of G exists as described in definition 3.14, G is linearly reductive via characterization (c) of theorem 3.6. The Reynolds operator of G is unique by lemma 3.5(e).

This means that to show that a group is linearly reductive, all we need to show is that there exists the Reynolds operator of the group G as in definition 3.14. Additionally, if we have the Reynolds operator R_G of the group, we can then express the Reynolds operator $R\colon K[X] \to K[X]^G$ for any affine G-variety in terms of R_G. *Cayley's Ω-process* will give us an explicit formula for the Reynolds operator of the general linear group GL_n.

4 Cayley's Ω-process

We want to express the Reynolds Operator in a concrete way. For the group GL_n, we can explicitly formulate it with the help of Cayley's Ω-Process, which was pubsished by Arthur Cayley in 1846 ([Cay46]).
The idea is to express the Reynolds operator with formal derivatives of polynomials. For fixed $k, l \in [n]$ and some $g \in K[\{Z_{i,j}\}_{i,j\in[n]}]$ with $Z_{k,l} \nmid g$, the formal partial derivative of $gZ_{k,l}^e \in K[\{Z_{i,j}\}_{i,j\in[n]}]$ with respect to the variable $Z_{k,l}$ is $\frac{\partial}{\partial Z_{k,l}}(gZ_{k,l}^e) = egZ_{k,l}^{e-1} \in K[\{Z_{i,j}\}_{i,j\in[n]}]$ for any $e \in \mathbb{N}$ ($gZ_{k,l}^e$ gets mapped to zero for $e = 0$).
In this section, we abbreviate $K[\{Z_{i,j}\}_{i,j\in[n]}] = K[Z]$.

Definition 4.1: Cayley's Ω-process
We call

$$\begin{aligned} \Omega\colon \quad K[Z] &\longrightarrow K[Z] \\ f &\longmapsto \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} \frac{\partial}{\partial Z_{i,\sigma(i)}} f \end{aligned} \tag{27}$$

Cayley's Ω-process[1]. It can also be thought of as $\Omega = \det\left(\frac{\partial}{\partial Z}\right)$, where $\frac{\partial}{\partial Z} := \left[\frac{\partial}{\partial Z_{i,j}}\right]_{i,j\in[n]}$.

Lemma 4.2
Consider Cayley's Ω-process $\Omega\colon K[Z] \to K[Z]$ as described above and the algebraic cohomomorphism $m^*\colon K[\mathrm{GL}_n] \to K[\mathrm{GL}_n] \otimes K[\mathrm{GL}_n]$ of the group multiplication $m\colon \mathrm{GL}_n \times \mathrm{GL}_n \to \mathrm{GL}_n$. We then have

$$\left(\det(Z)^{-1} \cdot \otimes \Omega\right) \circ m^* = m^* \circ \Omega = \left(\Omega \otimes \det(Z)^{-1} \cdot\right) \circ m^* \tag{28}$$

where $p\cdot\colon K[\mathrm{GL}_n] \to K[\mathrm{GL}_n]$, $f \mapsto pf$ denotes the operation *multiply with* p for a polynomial $p \in K[\mathrm{GL}_n]$, in this case $p = \det(Z)^{-1}$.

[1] $\prod_{i=1}^{n} \frac{\partial}{\partial Z_{i,\sigma(i)}}$ here denotes the successive application of the formal partial derivatives.

Proof. Let $f \in K[\mathrm{GL}_n]$. Consider $m^*(f)$, which we here view as $m^*(f) \in K\left[\{X_{i,j}\}_{i,j\in[n]}, \det(X)^{-1}, \{Y_{i,j}\}_{i,j\in[n]}, \det(Y)^{-1}\right]$, where the $X_{i,j}$ are associated with the "left" input of m and the $Y_{i,j}$ are associated with the "right" input of m. For $k,l \in [n]$, we denote by $m_{k,l}\colon \mathrm{GL}_n \times \mathrm{GL}_n \to K$, $([x_{i,j}]_{i,j\in[n]}, [y_{i,j}]_{i,j\in[n]}) \mapsto \Sigma_{i=1}^n x_{k,i}y_{i,l}$ the (k,l)-entry of the group multiplication m. We have $m_{k,l} = \Sigma_{i=1}^n X_{k,i}Y_{i,l} \in K[\{X_{i,j}\}_{i,j\in[n]}, \{Y_{i,j}\}_{i,j\in[n]}]$.
For fixed $i,j \in [n]$ we have

$$\begin{aligned}
\left(\mathrm{id} \otimes \frac{\partial}{\partial Z_{i,j}}\right)(m^*(f)) &= \frac{\partial}{\partial Y_{i,j}}(f \circ m) \\
&= \sum_{k,l\in[n]} \left(\left(\frac{\partial}{\partial Z_{k,l}} f\right) \circ m\right) \cdot \frac{\partial}{\partial Y_{i,j}} m_{k,l} \\
&= \sum_{k=1}^{n} \left(\left(\frac{\partial}{\partial Z_{k,j}} f\right) \circ m\right) \cdot X_{k,i} \\
&= \sum_{k=1}^{n} (Z_{k,i} \cdot \otimes \mathrm{id}) \left(m^* \left(\frac{\partial}{\partial Z_{k,j}} f\right)\right)
\end{aligned} \tag{29}$$

In the second equation, we made use of the chain rule. Successively applying this result yields

$$\begin{aligned}
(\mathrm{id} \otimes \Omega)(m^*(f)) &= \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \left(\mathrm{id} \otimes \prod_{i=1}^{n} \frac{\partial}{\partial Z_{i,\sigma(i)}}\right)(m^*(f)) \\
&= \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \sum_{k\in[n]^n} \left(\prod_{i=1}^{n} Z_{k(i),i} \cdot \otimes \mathrm{id}\right) \left(m^* \left(\prod_{j=1}^{n} \frac{\partial}{\partial Z_{k(j),\sigma(j)}} f\right)\right) \\
&= \sum_{k\in[n]^n} \left(\prod_{i=1}^{n} Z_{k(i),i} \cdot \otimes \mathrm{id}\right) \left(m^* \left(\sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \prod_{j=1}^{n} \frac{\partial}{\partial Z_{k(j),\sigma(j)}} f\right)\right) \\
&= \sum_{k\in S_n} \left(\prod_{i=1}^{n} Z_{k(i),i} \cdot \otimes \mathrm{id}\right) \left(m^* \left(\sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \prod_{j=1}^{n} \frac{\partial}{\partial Z_{k(j),\sigma(j)}} f\right)\right) \\
&= \sum_{k\in S_n} \left(\prod_{i=1}^{n} Z_{k(i),i} \cdot \otimes \mathrm{id}\right) (m^*(\mathrm{sgn}(k)\Omega(f))) \\
&= (\det(Z) \cdot \otimes \mathrm{id})(m^*(\Omega(f)))
\end{aligned} \tag{30}$$

In the fourth equation, we are able to eliminate all terms with $k \in [n]^n \setminus S_n$ since if there exist $i \neq j$ such that $k(i) = k(j)$, the term $\sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \prod_{j=1}^n \frac{\partial}{\partial Z_{k(j),\sigma(j)}} f$ consists of pairs of sums that cancel each other out, due to the nature of the sign function.
This immediately shows the first equality, and the second equality is proven analogously. □

Lemma 4.3
For $p \in \mathbb{N}$, $c_{p,n} := \Omega^p(\det(Z)^p) = \det\left(\frac{\partial}{\partial Z}\right)^p(\det(Z)^p)$ is a nonnegative integer.

Proof. Write $\det(Z)^p = \Sigma_i a_i q_i \left(\{Z_{k,l}\}_{k,l\in[n]}\right)$, where $a_i \in \mathbb{Z}\setminus\{0\}$ and q_i are (monic) monomials. Then

$$\Omega^p\left(\det(Z)^p\right) = \sum_i a_i q_i \left(\left\{\frac{\partial}{\partial Z_{k,l}}\right\}_{k,l\in[n]}\right)\left(\sum_j a_j q_j\left(\{Z_{k,l}\}_{k,l\in[n]}\right)\right) \tag{31}$$

Notice that $q_i\left(\left\{\frac{\partial}{\partial Z_{k,l}}\right\}_{k,l\in[n]}\right)\left(q_j\left(\{Z_{k,l}\}_{k,l\in[n]}\right)\right)$ is zero for $i\neq j$ and a strictly positive integer for $i=j$. Therefore in particular

$$c_{p,n} = \sum_i a_i^2 q_i\left(\left\{\frac{\partial}{\partial Z_{k,l}}\right\}_{k,l\in[n]}\right)\left(q_i\left(\{Z_{k,l}\}_{k,l\in[n]}\right)\right)\in\mathbb{N}_{>0} \tag{32}$$

□

Now, finally, we have the tools to see the following way of expressing the Reynolds Operator.

Theorem 4.4
For $p\in\mathbb{N}$ and $\tilde{f}\in K[Z]_{pn}$, define for $f=\frac{\tilde{f}}{\det(Z)^p}$:

$$R(f) := \frac{\Omega^p\tilde{f}}{c_{p,n}} \tag{33}$$

The linear extension of this (mapping any $g=\frac{\tilde{g}}{\det(Z)^p}\in K[\mathrm{GL}_n]$ to zero for which $\tilde{g}\in K[Z]_m$ with $m\neq pn$), defines the Reynolds Operator R_{GL_n}, which makes GL_n *linearly reductive.*
(See [DK15, 4.5.27])

Proof. First, check that this is well defined: For any such term, expanding the fraction by $\det(Z)^q$ will yield the same result. Also, Ω^p is linear for any $p\in\mathbb{N}$. We shall now show that R is GL_n-invariant from the left and from the right. Let $p\in\mathbb{N}$, $\tilde{f}\in K[\mathrm{GL}_n]_{pn}$ and $f:=\frac{\tilde{f}}{\det(Z)^p}$. For $\beta,\gamma\in\mathrm{GL}_n$, we notice

$$\begin{aligned}
R(\beta.f)(\gamma) &= R\left(\frac{\det(\beta)^p\cdot\beta.\tilde{f}}{\det(Z)^p}\right)(\gamma)\\
&= \frac{\det(\beta)^p\cdot\Omega^p\left(\beta.\tilde{f}\right)(\gamma)}{c_{p,n}}\\
&= \frac{1}{c_{p,n}}\cdot\left(\epsilon_{\beta^{-1}}\otimes\epsilon_\gamma\right)\left(\left(\left(\det(Z)^{-p}\cdot\otimes\Omega^p\right)\circ m^*\right)\left(\tilde{f}\right)\right)\\
&= \frac{1}{c_{p,n}}\cdot\left(\epsilon_{\beta^{-1}}\otimes\epsilon_\gamma\right)\left(\left(\left(\Omega^p\otimes\det(Z)^{-p}\cdot\right)\circ m^*\right)\left(\tilde{f}\right)\right)\\
&= \frac{\Omega^p\left(\gamma\dot{}\tilde{f}\right)(\beta^{-1})\cdot\det\left(\gamma^{-1}\right)^p}{c_{p,n}}\\
&= R\left(\frac{\gamma\dot{}\tilde{f}\cdot\det\left(\gamma^{-1}\right)^p}{\det(Z)^p}\right)\left(\beta^{-1}\right)\\
&= R\left(\gamma\dot{}f\right)\left(\beta^{-1}\right)
\end{aligned} \tag{34}$$

Since each $\frac{\partial}{\partial Z_{i,j}}$ lowers the degree of a monomial by one or maps it to zero, R maps to K, and therefore for $\delta \in \mathrm{GL}_n$ and $g \in K[\mathrm{GL}_n]$ we have $R(g)(\delta) = R(g) \in K$. We then get for all $\beta, \gamma \in \mathrm{GL}_n$

$$R(\beta.f) = R(\beta.f)(\gamma) = R(\gamma\dot{} f)\left(\beta^{-1}\right) = R(\gamma\dot{} f) \tag{35}$$

This implies that for all $\sigma \in G$ and all $p \in K[\mathrm{GL}_n]$, we have $R(\sigma.p) = R(I_n\dot{} p) = R(p)$ and $R(\sigma\dot{} p) = R(I_n.p) = R(p)$, showing that R is GL_n-invariant from the left and from the right. Finally, the definition immediately gives us that R restricted to K is the identity.
This shows that R is a Reynolds-operator, and as mentioned in lemma 3.5(e), the uniqueness of the Reynolds Operator implies that we can write $R = R_{\mathrm{GL}_n}$. □

Now we will look at the Reynolds Operator R_{SL_n}.

Corollary 4.4.1
With the identification $K[\mathrm{GL}_n] = K\left[\{Z_{k,l}\}_{k,l\in[n]}, \det(Z)^{-1}\right]$, view $K[\mathrm{SL}_n] = K[\mathrm{GL}_n]/I$ where $I = (\det(Z) - 1)$. Now, for $p \in \mathbb{N}$ and $f \in K\left[\{Z_{i,j}\}_{k,l\in[n]}\right]_{pn}$ we define:

$$R(f \bmod I) := R_{\mathrm{GL}_n}\left(\frac{f}{\det(Z)^p}\right) \bmod I = \frac{\Omega^p \tilde{f}}{c_{p,n}} \bmod I \in K[\mathrm{SL}_n] \tag{36}$$

The linear extension of this (mapping $K[\mathrm{SL}_n]_m$ with $n \nmid m$ to zero), defines the Reynolds Operator R_{SL_n}, making SL_n *linearly reductive.*
(See [DK15, 4.5.28])

Proof. First, we will show $K[\mathrm{GL}_n]^{\mathrm{SL}_n} = K\left[\det(Z), \det(Z)^{-1}\right]$ (action by left multiplication). For $B \in K^{n,n}$, define $B' := \mathrm{diag}(b_i)_{i\in[n]}$, where $b_1 := \det(\beta)$ and $b_i := 1$ for $2 \le i \le n$. Let $g \in K[\mathrm{GL}_n]^{\mathrm{SL}_n}$, and let $\alpha \in \mathrm{GL}_n$. Note that $\alpha(\alpha')^{-1} \in \mathrm{SL}_n$. Define $h := (\beta \mapsto g(\beta')) \in K\left[\det(Z), \det(Z)^{-1}\right]$. We claim that $g = h$. This is seen as follows:

$$\begin{aligned} g(\alpha) = \alpha(\alpha')^{-1}.g(\alpha) &= g\left(\alpha'\alpha^{-1}\alpha\right) \\ &= g(\alpha') = h(\alpha) \end{aligned} \tag{37}$$

This shows that $g = h \in K\left[\det(Z), \det(Z)^{-1}\right]$. Conversely it is easy to see that $K\left[\det(Z), \det(Z)^{-1}\right] \subseteq K[\mathrm{GL}_n]^{\mathrm{SL}_n}$.
Now we define a map $\hat{R}\colon K[\mathrm{GL}_n] \longrightarrow K[\mathrm{GL}_n]^{\mathrm{SL}_n}$ as follows:
For $p, r \in \mathbb{N}$, $\tilde{f} \in K\left[\left\{Z_{k,l\in[n]}\right\}\right]_{rn}$, and $f = \frac{\tilde{f}}{\det(Z)^p}$, define

$$\hat{R}(f) := \det(Z)^{r-p} \cdot \frac{\Omega^r \tilde{f}}{c_{r,n}} = \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\tilde{f}}{\det(Z)^r}\right) \tag{38}$$

As before we define the images of the other elements by linear extension. Well-definedness follows from the same observations as in the proof of the theorem. This map is the identity on $K[\mathrm{GL}_n]^{\mathrm{SL}_n}$: If $f \in K[\mathrm{GL}_n]^{\mathrm{SL}_n}$, then f must be a linear combination of terms of the form $\frac{\det(Z)^r}{\det(Z)^p}$. Without loss of generality we can assume that either $p = 0$ or $r = 0$. Then it should be clear that f gets mapped to itself. Finally, we can see that $\hat{R}$ is SL_n-invariant from the left and from the right: Let $\alpha \in \mathrm{SL}_n$. Then

$$\begin{aligned}
\hat{R}(\alpha.f) &= \hat{R}\left(\frac{\det(\alpha)^p \cdot \alpha.\tilde{f}}{\det(Z)^p}\right) \\
&= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\det(\alpha)^p \cdot \alpha.\tilde{f}}{\det(Z)^r}\right) \\
&= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\det(\alpha)^r \cdot \alpha.\tilde{f}}{\det(Z)^r}\right) \\
&= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\alpha.\left(\frac{\tilde{f}}{\det(Z)^r}\right)\right) \\
&= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\tilde{f}}{\det(Z)^r}\right) \qquad = \hat{R}(f)
\end{aligned} \tag{39}$$

We used $\det(\alpha)^p = 1 = \det(\alpha)^r$ and the GL_n-invariance of R_{GL_n}. The GL_n-invariance from the right is shown analogously. Thus we have shown that $\hat{R}$ is the Reynolds-Operator for the action of SL_n on GL_n by left-multiplication, which is also SL_n-invariant from the right.
Noting that $\det(Z) \bmod I = 1 \bmod I$, this shows our proposed statement that $R = R_{\mathrm{SL}_n}$ does define the Reynolds operator of $\mathrm{SL_n}$. □

Example 4.5
We will apply Cayley's Ω-process in the setting of example 3.9.2 for $n = 2$, that is the group $G = \mathrm{SL}_2$ and the representation $V = \left\{ A \in K^{2\times 2} \mid A^T = A \right\}$ with the action

$$\begin{aligned}
\mu\colon \quad \mathrm{SL}_2 \times V &\longrightarrow V \\
(S, A) &\longmapsto SAS^T
\end{aligned} \tag{40}$$

Now consider the following for $S \in \mathrm{SL}_2$ and $A \in V$:

$$\begin{aligned}
S &= \begin{bmatrix} s_{1,1} & s_{1,2} \\ s_{2,1} & s_{2,2} \end{bmatrix} \qquad A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \\
S^{-1} &= \begin{bmatrix} s_{2,2} & -s_{1,2} \\ -s_{2,1} & s_{1,1} \end{bmatrix}
\end{aligned} \tag{41}$$

We then have

$$\begin{aligned}
&S^{-1}.A = S^{-1}A\left(S^{-1}\right)^T \\
&= \begin{bmatrix} \begin{matrix} a_{1,1}s_{2,2}^2 - 2a_{1,2}s_{1,2}s_{2,2} \\ +a_{2,2}s_{1,2}^2 \end{matrix} & \begin{matrix} -a_{1,1}s_{2,1}s_{2,2} + a_{1,2}s_{1,1}s_{2,2} \\ +a_{1,2}s_{1,2}s_{2,1} - a_{2,2}s_{1,1}s_{1,2} \end{matrix} \\ & \\ \begin{matrix} -a_{1,1}s_{2,1}s_{2,2} + a_{1,2}s_{1,1}s_{2,2} \\ +a_{1,2}s_{1,2}s_{2,1} - a_{2,2}s_{1,1}s_{1,2} \end{matrix} & \begin{matrix} a_{1,1}s_{2,1}^2 - 2a_{1,2}s_{1,1}s_{2,1} \\ +a_{2,2}s_{1,1}^2 \end{matrix} \end{bmatrix}
\end{aligned} \tag{42}$$

Notice that we also have

$$\begin{aligned}
\det\left(\frac{\partial}{\partial S}\right)^n &= \left(\frac{\partial}{\partial S_{1,1}}\frac{\partial}{\partial S_{2,2}} - \frac{\partial}{\partial S_{1,2}}\frac{\partial}{\partial S_{2,1}}\right)^n \\
&= \sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{\partial}{\partial S_{1,1}}^{n-k}\frac{\partial}{\partial S_{1,2}}^{k}\frac{\partial}{\partial S_{2,1}}^{k}\frac{\partial}{\partial S_{2,2}}^{n-k}
\end{aligned} \tag{43}$$

It is quite cumbersome to calculate the Reynolds Operator of general polynomials. We will look at the monomial $Z_{1,1}^2 \in K[V]$, for which we have

$$\begin{aligned}
&\bar{\mu}'(Z_{1,1}^2) \\
&= S_{2,2}^4 \otimes Z_{1,1}^2 - 4S_{1,2}S_{2,2}^3 \otimes Z_{1,1}Z_{1,2} + 2S_{1,2}^2S_{2,2}^2 \otimes Z_{1,1}Z_{2,2} \\
&+ 4S_{1,2}^2S_{2,2}^2 \otimes Z_{1,2}^2 - 4S_{1,2}^3S_{2,2} \otimes Z_{1,2}Z_{2,2} + S_{1,2}^4 \otimes Z_{2,2}^2
\end{aligned} \tag{44}$$

We can now apply the Reynolds operator in the way we discussed it in proposition 3.19 in combination with Cayley's Ω-process. Since all terms in $K[\mathrm{SL}_2]$ are already of degree 2, we apply the same to each summand and calculate:

$$\begin{aligned}
&R_G \cdot Z_{1,1}^2 \\
&= \left(\frac{\partial}{\partial S_{1,1}}^2 \frac{\partial}{\partial S_{2,2}}^2 - 2\frac{\partial}{\partial S_{1,1}} \frac{\partial}{\partial S_{1,2}} \frac{\partial}{\partial S_{2,1}} \frac{\partial}{\partial S_{2,2}} + \frac{\partial}{\partial S_{1,2}}^2 \frac{\partial}{\partial S_{2,1}}^2 \right) \cdot Z_{1,1}^2 \\
&= 0
\end{aligned} \tag{45}$$

The zero-polynomial is a trivial invariant, so we see that applying the Reynolds Operator to a polynomial will not always produce interesting results. We will try again for the polynomial $Z_{1,2}^2 \in K[V]$. We calculate

$$\begin{aligned}
&\mu'(Z_{1,2}^2) \\
=&S_{2,1}^2S_{2,2}^2 \otimes Z_{1,1}^2 - 2S_{1,1}S_{2,1}S_{2,2}^2 \otimes Z_{1,1}Z_{1,2} \\
&- 2S_{1,2}S_{2,1}^2S_{2,2} \otimes Z_{1,2}^2 + 2S_{1,1}S_{1,2}S_{2,1}S_{2,2} \otimes Z_{1,1}Z_{2,2} \\
&+ S_{1,1}^2S_{2,2}^2 \otimes Z_{1,2}^2 + 2S_{1,1}S_{1,2}S_{2,1}S_{2,2} \otimes Z_{1,2}^2 \\
&- 2S_{1,1}^2S_{1,2}S_{2,2} \otimes Z_{1,2}Z_{2,2} + S_{1,2}^2S_{2,1}^2 \otimes Z_{1,2}^2 \\
&- 2S_{1,1}S_{1,2}^2S_{2,1} \otimes Z_{1,2}Z_{2,2} + S_{1,1}^2S_{1,2}^2 \otimes Z_{2,2}^2
\end{aligned} \tag{46}$$

Again, all $K[\mathrm{SL}_2]$ terms are of degree 2, therefore we can simplify and calculate

$$\begin{aligned}
&R_G \cdot Z_{1,2}^2 \\
&= \left(\frac{\partial}{\partial S_{1,1}}^2 \frac{\partial}{\partial S_{2,2}}^2 - 2\frac{\partial}{\partial S_{1,1}} \frac{\partial}{\partial S_{1,2}} \frac{\partial}{\partial S_{2,1}} \frac{\partial}{\partial S_{2,2}} + \frac{\partial}{\partial S_{1,2}}^2 \frac{\partial}{\partial S_{2,1}}^2 \right) \cdot Z_{1,2}^2 \\
&= -\frac{4}{12} Z_{1,1}Z_{2,2} + \frac{4}{12} Z_{1,2}^2 - \frac{4}{12} Z_{1,2}^2 + \frac{4}{12} Z_{1,2}^2 \\
&= -\frac{1}{3}\det(Z)
\end{aligned} \tag{47}$$

This is in line with what we expect: $K[V]^{\mathrm{SL}_2} = K[\det(A)]$.

5 Further discussion and conclusion

5.1 A complete algorithm for retrieving generators of the invariant ring

Our motivation for having a construction of the Reynolds operator was to not only see that GL_n is linearly reductive, but also to yield some invariants. It would also be very helpful if we could somehow produce a generating set for the

invariant ring.
In example 4.5, we saw that applying the Reynolds operator to any polynomial does not always result in retrieving a nonzero invariant. It suggests that we somehow need to find the "correct" polynomials to apply the Reynolds operator to. The following proposition (see [DK15, prop. 4.1.1]) gives us exactly that.

Proposition 5.1
Let V be a rational G-representation where G is linearly reductive, and let $I_{>0}$ denote the ideal generated by all non-constant invariants. If $I_{>0} = \big(\{f_i\}_{i\in[r]}\big)$ for some homogeneous polynomials $\{f_i\}_{i\in[r]} \subseteq K[V]$, we then have $I_{>0} = \big(\{R(f_i)\}_{i\in[r]}\big)$ and $K[V]^G = K\left[\{R(f_i)\}_{i\in[r]}\right]$.

In the proof of Hilbert's finiteness theorem (3.9), we made use of the existence of a finite set of invariants generating $I_{>0}$, which was non-constructively given. The previous proposition looks helpful since we have a construction for the Reynolds operator for $G = \mathrm{GL}_n$ via Cayley's Ω-process, but the problem still remains that we need to have a finite set of homogeneous polynomials generating $I_{>0}$, whose existence is here also non-constructively given.
It is in fact possible to compute them with Groebner bases, which is extensively described in [DK15, Algorithm 4.1.9]. This gives us a complete algorithm that takes as its input all of the information necessary to describe our rational representation, which can all be given in terms of polynomials, and outputs a list of generators of the invariant ring.

5.2 Cross Ratio

In examples 3.11.1 and 3.13.1 we discussed the cross ratio. Our setting was affine and in K^2, which makes our results different from the projective setting, where there are not very many other invariants other than the cross ratio.
Using the same conventions and definitions as in the aforementioned examples, we can define the projective cross ratio:

$$\begin{aligned} \mathrm{cr}\colon \qquad\qquad\qquad Y &\longrightarrow K \\ ([x_1],[x_2],[x_3],[x_4]) &\longmapsto \frac{\det(x_1,x_2)\det(x_3,x_4)}{\det(x_2,x_3)\det(x_4,x_1)} \end{aligned} \tag{48}$$

where $Y \subseteq P(K^2)^4$ is the set of all pairwise distinct four-tuples of points in $P(K^2)$. It should be clear that the map cr is well-defined. The action of GL_2 on X induces an action of the projective general linear group PGL_n on Y. In the projective setting, we will get a different looking invariant ring, which we will discuss right now.
Let $f\colon Y \longrightarrow K$ be an invariant regular function. If $X_1, X_2, X_3, Y_1, Y_2, Y_3 \in P(K^2)$ with X_1, X_2 and X_3 pairwise distinct and Y_1, Y_2 and Y_3 pairwise distinct, then an important theorem in projective geometry is that there exists a (unique) projective transformation $\rho \in \mathrm{PGL}(K^2)$ such that $\rho(X_1) = Y_1$, $\rho(X_2) = Y_2$ and $\rho(X_3) = Y_3$ (see [Aud03, prop 5.6]), in other words PGL_2 acts transitively on 3-tuples of pairwise distinct points in $P(K^2)$. Let $A, B, C, D \in Y$, which implies that B, C, D are pairwise distinct. For $x \in K$ we define $x_P := \left[\binom{x}{1}\right]$ and $\infty_P := \left[\binom{1}{0}\right]$. There then exists a $\rho \in \mathrm{PGL}(K^2)$ such that $\rho(B) = 0_P$, $\rho(C) = 1_P$ and $\rho(D) = \infty_P$. Since A is distinct from D we know $\rho(A) \neq \infty_P$,

and therefore there exists some $a \in K$ such that $\rho(A) = [\binom{a}{1}]$. We then compute

$$\begin{aligned} \rho(A) &= \left[\begin{pmatrix} a \\ 1 \end{pmatrix}\right] \\ &= \mathrm{cr}\left(\left[\begin{pmatrix} a \\ 1 \end{pmatrix}\right], \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right], \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right], \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right]\right)_P \\ &= \mathrm{cr}(\rho(A), \rho(B), \rho(C), \rho(D))_P & = \mathrm{cr}(A, B, C, D)_P \end{aligned} \tag{49}$$

We then have

$$\begin{aligned} f(A, B, C, D) &= \rho^{-1}.f(A, B, C, D) \\ &= f(\rho(A), \rho(B), \rho(C), \rho(D)) \\ &= f(\mathrm{cr}(A, B, C, D)_P, 0_P, 1_P, \infty_P) \end{aligned} \tag{50}$$

This shows that in the projective setting, there don't exist many more invariants than the cross ratio.
In our affine setting, it suggests that we can transfer the idea, which would mean that $K[\mathrm{cr}, p(\binom{\mathrm{cr}}{1}, \binom{0}{1}, \binom{1}{1}, \binom{1}{0})^{-1}] = K[\mathrm{cr}, (\mathrm{cr}(\mathrm{cr}-1))^{-1}] = K[\mathrm{cr}, \mathrm{cr}(X_1, X_3, X_4, X_2)]$ are all invariants. This is not true though, since for instance $\frac{\det(X_1, X_2)}{\det(X_3, X_4)} \in K[X]^{\mathrm{GL}_2}$ is an invariant not included in $K[\mathrm{cr}, \mathrm{cr}(X_1, X_3, X_4, X_2)]$.

5.3 Conclusion

References

[Aud03] Michèle Audin. *Geometry.* Springer-Verlag, Berlin Heidelberg, 2003.

[Bos13] Siegfried Bosch. *Algebra.* Springer-Verlag, Berlin Heidelberg, 2013.

[Cay46] Arthur Cayley. On linear transformations. *The Cambridge and Dublin mathematical journal*, 1:104, 1846.

[DK15] Harm Derksen and Gregor Kemper. *Computational Invariant Theory.* Springer-Verlag, Berlin Heidelberg, 2015.

[FH91] William Fulton and Joe Harris. *Representation theory; a first course.* Springer-Verlag, New York, 1991.

[Fis14] Gerd Fischer. *Lineare Algebra.* Springer Fachmedien, Wiesbaden, 2014.

[Hil90] David Hilbert. Über die Theorie der algebraischen Formen. *Annalen der Mathematik*, 36:473, 1890.

[Kle93] Felix Klein. A comparative review of recent researches in geometry, 1893.

[Kra85] Hanspeter Kraft. *Geometrische Methoden in der Invariantentheorie.* Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig, 1985.

[Rab30] J.L. Rabinowitsch. Zum Hilbertschen Nullstellensatz. *Annalen der Mathematik*, 120:520, 1930.

[Stu08] Bernd Sturmfels. *Algorithms in Invariant Theory.* Springer-Verlag, Wien, 2008.