Cayley's Ω-Process And The Reynolds Operator

Bert Lorke

March 17, 2018

Contents

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. Here, the central idea of a geometry is characterized by its associated symmetry group, the group of transformations which leaves certain objects unchanged, for example: angles. The study of these transformations is called conformal geometry.

Let us discuss the following important example in projective geometry: Consider all transformations which map lines to lines, id est, such transformations under which the the property of being a line is invariant. In real projective geometry, the fundamental theorem of projective geometry gives us that these maps are exactly the projective transformations.

Conversely, we can now just 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 in 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 polynomial which takes as its input four collinear points. Is this the only invariant? How can we find other invariants? How big is the set (this will be a 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 was non-constructive. It is claimed[1] that this proof was responsible for Gordan's famous quote "Das ist Theologie und nicht Mathematik". 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. It would be great if this group were linearly reductive. But it is! There are multiple ways to see this. In a seminar I held, with the help of the Haar measure, I discussed a way to see that a module complement exists for every representation, making GL_n linearly reductive. One can also show linear reductivity by the Schur-Weyl-dualty: The symmetric group is finite, and therefore we can see that rational GL_n representations are semisimple, from which 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 the existence! What does it help 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 receive concrete invariants. **This is possible with *Cayley's Ω-process*!** This is the main focus of my work.

I say "more easily" receive invariants, because if we take a polynomial at random and apply the Reynolds Operator, we might very likely just get a constant polynomial, which is not a very interesting invariant, and we also want to know if there are more invariants. Similar to the first proof of Hilbert's finiteness theorem (by Hilbert himself), 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 I will be discussing in detail in my work,

[1] I read somewhere that it is not certain

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.

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 whose set is an affine variety, and whose multiplcation 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. For a finite-dimensional vector-space V, we denote by X_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.

2.2 Concepts From Algebraic Geometry

Proposition 2.1: Rabinowitsch Trick
Let $V = K^n$ for some $n \in \mathbb{N}$. 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 $K[X_p] = K[\{X_i\}_{i \in [n]}, p^{-1}]$.

Proof. The set X_p is not an algebraic set itself. The trick (the "Rabinowitsch-trick") is "adding an additional variable X_0", that means to consider X_p as a subset of $K \times V$. 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 notice that $\tilde{X}_p = \{ (p(v)^{-1}, v) \in K \times V \mid v \in X_p \}$. This means that X_p corresponds to $\tilde{X}_p$ via the bijection $\Phi \colon X_p \longrightarrow \tilde{X}_p$, $v \leftrightarrow (1/p(v), v)$. The coordinate ring of $\tilde{X}_p$ can be written as $K[\bar{X}_0, \{\bar{X}_i\}_{i \in [n]}]$, where $\bar{X}_i = X_i \bmod X_0 \cdot p - 1$. Let $x \in X_p$. 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: The General Linear Group GL_n
One of the most important examples is the general linear group GL_n, which will be an essential theme in my work. By the above proposition this group is an affine variety via $p = \det$ with the coordinate ring $K[\{X_{i,j}\}_{i,j \in [n]}, \det^{-1}]$. This makes GL_n into a *linear algebraic group*, that is a group which is an affine variety whose group operations of the multiplication and inversion are morphisms of affine varieties: The multiplication is just a polynomial function in each entry For the inversion each entry is a fraction of polynomials with det as the quotient, which means that each entry is in $K[\mathrm{GL}_n]$.

Definition 2.3: Algebraic Cohomomorphism For Product Spaces
Let $m\colon U_1 \times U_2 \longrightarrow W$ be a morphism of affine varieties. The strict algebraic cohomomorphism, which we shall call $\hat{m}$, is a map of the type $K[W] \longrightarrow K[U_1 \times U_2]$. 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.
We define the following map:

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

This is independent of the choice of generators and independent of the representatives and therefore well-defined. It is even an isomorphism. Now, finally, we define $m^* := t \circ \hat{m} : K[W] \longrightarrow K[U_1] \otimes K[U_2]$. Most literature still also calls m^* the algebraic cohomomorphism of m, the K-algebra of all evaluation maps induced by $K[U_1] \otimes K[U_2]$ is equal to $K[U_1 \times U_2]$.

Remark 2.3.1
One might ask why we want to look at these objects $m^*(f)$ instead of $\hat{m}(f)$. Really, these objects are hardly different (the spaces are isomorphic), but it helps to formalize performing operations only on the "left part" or the "right part", as we will soon see. This is an approach that [DK15] follows, but other literature such as [Stu08] (and probably also Cayley) rather consider $\hat{m}(f)$ written as $\hat{m}(f) = f(XY)$. To give a very simple example: If $f \in K[Z]|_G$, we will write $\mathrm{id} \otimes \frac{\partial}{\partial Z_i}(m^* f)$ as in [DK15], whereas [Stu08] would write $\frac{\partial}{\partial Y_i} f(XY)$.

2.3 Concepts From Invariant Theory

Definition 2.4: Regular Action, Rational Representation
Let G be a linear algebraic group and X an affine variety. We call an action $G \times X \longrightarrow X$ 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 $\mu\colon G \times V \longrightarrow V$ be a representation in the classical sense, that is for all $g \in G$ we have $D_\mu(g) := (v \mapsto \mu(g, v)) \in \mathrm{GL}(V)$. We call μ a *rational representation* if and only if it is regular.
(See [DK15, p. 31])

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

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

Example 2.5.1
A less trivial one

Definition 2.6: Rational Linear Action
Let V be a vector space (not necessarily finite dimensional), and $\mu : G \times V \longrightarrow V$ an action. We call μ a **rational linear action** if and only if there exists a linear map $\mu' \colon V \longrightarrow K[G] \otimes V$ such that $\mu\,(\sigma, v) = ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu')\,(v)$.
(See [DK15, A.1.7])

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

Definition 2.7
Let $\mu \colon G \times X \longrightarrow X$ be a regular action. We define an action $\bar{\mu} \colon G \times K[X] \longrightarrow K[X]$ via $\bar{\mu}(\sigma, f)(x) := f(\mu(\sigma^{-1}, x))$, and we write $\sigma.f(x) := f(\sigma^{-1}.x)$, where $\sigma \in G$, $f \in K[X]$ and $x \in X$.
This action is obviously regular, but it is also easily shown that it is in fact a rational linear action: If $\tilde{\mu} \colon G \times X \longrightarrow X$ is the morphism of affine varieties (it is in fact a right action) defined by $(\sigma, x) \mapsto \tilde{\mu}(\sigma, x) := \mu(\sigma^{-1}, x)$, then we can define $\bar{\mu}' := \tilde{\mu}^*$ with the desired properties.

Definition 2.8
Let V be a finite dimensional vector-space $\mu \colon G \times V \longrightarrow V$ a rational representation. We then define an action $\hat{\mu} \colon G \times V^* \longrightarrow V^*$, $(\sigma, \varphi) \mapsto \sigma.\varphi := (v \mapsto \varphi(\mu(\sigma^{-1}, v)) = \varphi(\sigma^{-1}.v))$, which is a rational represenation of G.

Definition 2.9
let G be a linear algebraic group with the multimplication $m \colon G \times G \longrightarrow G$. We define $\dot{m} \colon G \times G \mapsto G$ by $(\sigma, \tau) \mapsto \dot{m}(\sigma, \tau) := m(\tau, \sigma) = \tau\sigma$.
For $\sigma \in G$ and for $p \in K[G]$ we then also define $\sigma\dot{}p := ((\epsilon_\sigma \otimes \mathrm{id}) \circ \dot{m}^*)(p) = ((\mathrm{id} \otimes \epsilon_\sigma) \circ m^*)(p)$, in other words we have $\sigma\dot{}p(\tau) = p(\tau\sigma)$ for $\sigma, \tau \in G$ and $p \in K[G]$.

Proposition 2.10
Let X be an affine variety and $\mu \colon G \times X \longrightarrow X$ 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

$$\begin{aligned} \bar{\mu}'(\sigma.f)(\tau, x) &= ((\epsilon_\tau \otimes \mathrm{id}) \circ \bar{\mu}')(\sigma.f)(x) \\ &= (\tau.(\sigma.f))(x) \\ &= \Sigma_{i=1}^r p_i(\tau\sigma) g_i(x) \\ &= \Sigma_{i=1}^r \sigma\dot{}p_i(\tau) g_i(x) \qquad = (\Sigma_{i=1}^r \sigma\dot{}p_i \otimes g_i)(\tau, x) \end{aligned} \tag{2}$$

□

Proposition 2.11
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 $\Sigma_{i=1}^{r} \sigma.p_i \otimes \sigma.g_i(\tau, x) = \Sigma_{i=1}^{r} p_i(\sigma^{-1}\tau) \otimes g_i(\sigma^{-1}.x) = \sigma^{-1}\tau.f(\sigma^{-1}.x) = \tau.f(x) = \bar{\mu}'(f)(\tau, x)$. □

Definition 2.12: locally finite
For a vector space V, we call an action $\mu\colon G \times V \longrightarrow V$ **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 $\mu\colon G \times V \longrightarrow V$ 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 $\mu\colon G \times V \longrightarrow V$ is locally finite if and only if V_v is finite-dimensional.

Proposition 2.14
Let V be a vector space.

(a) If $\mu\colon G \times V \longrightarrow V$ 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 $\mu\colon G \times V \longrightarrow V$ is a rational representation, then μ is also a rational linear action.

Proof. See [DK15, A.1.8] and [DK15, 2.2.5(b) $\Longrightarrow$ (c), 2.2.6]
(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 $\mu\colon G \times V \longrightarrow V$ a rational representation. This means that for all $\sigma \in G$ we have $D_\mu(\sigma) \in \mathrm{GL}(V)$. Let us now choose a basis $\{v_i\}_{i \in [r]}$ of V. For all $\sigma \in G$ there then exist unique $\{(D_\mu)_{i,j}\}_{i,j \in [r]} \subseteq K$ such that for all $i \in [r]$ we have $\mu(\sigma, v_i) = \Sigma_{k=1}^{r} (D_\mu)_{i,k} v_k$. Since the action is regular, we must have $p_{i,j} := \left(\mu \mapsto (D_\mu)_{i,k}\right) \in K[G]$. We now define $\mu'\colon V \longrightarrow K[G] \otimes V$ 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. □

Remark 2.14.1
This shows that for a finite-dimensional vector space V, an action is rational 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 $\mu\colon G \times V \longmapsto V$ is of the following form:
Consider $D_\mu\colon G \longmapsto \mathrm{GL}(V)$. If then $a_{i,j} : G \longrightarrow K$ is the function of the (i,j)-entry of D_μ, then $a_{i,j} \in K[G]$.
In fact, it is equivalent to define a representation $\mu\colon G \times V \longrightarrow V$ (V finite dimensional) as rational, iff $D_\mu\colon G \longrightarrow \mathrm{GL}(V)$ is a map of affine varieties.

Definition 2.15: Invariants
Let G act on X regularly.

$$X^G := \{\, x \in X \mid \forall g \in G : g.x = x \,\} \tag{3}$$

This defines a linear subspace. The given action induces an action $\bar{\mu}\colon G \times K[X] \longrightarrow K[X]$ as per definition 2.7. The **invariant ring** of the representation is defined as

$$K[X]^G := \{\, f \in K[X] \mid \forall g \in G : g.f = f \,\} \tag{4}$$

As the name implies, $K[X]^G$ defines a subalgebra of $K[X]^G$.

The general theme of my work revolves around the question of whether the invariant ring $K[X]^G$ is finitely generated.
Hilbert's finiteness theorem states that if the group G is linearly reductive, $K[V]^G$ is finitely generated. The strict definition of "linearly reductive" is quite tricky, but we will give an alternate equivalent definition shortly.

3 Linearly Reductive Groups, The Reynolds Operator And Hilbert's Finiteness Theorem

3.1 The Reynolds Operator And Linearly Reductive Groups

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 $b\colon V^* \times V \longrightarrow K$, $(\varphi, v) \mapsto \varphi(v)$, that is $b|_{(V^*)^G \times V^G}$ is non-degenerate.

Definition 3.2
If we have a given action of a group G on a set X, we call a map $A\colon X \longrightarrow Y$ **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 G-invariant linear projection $R\colon K[X] \twoheadrightarrow K[X]^G$ is called a **Reynolds operator**.

Definition 3.4
Assume that V is a rational representation of V such that there exists a unique subrepresentation W of V such that $V = V^G \oplus W$. We define $R_V\colon V \twoheadrightarrow V^G$ as the linear projection of V onto V^G along W.

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 representation V' of G, we have $R_{V'}|_V = R_V$.

(b) If V is a rational representation of G and $R'_V \colon V \longrightarrow Y$ is a G-invariant linear map with $V \subseteq Y$ and $R'_V|_{V^G} = \mathrm{id}_{V^G}$, we have $R'_V = R_V$, id est R_V is unique with this property (**Do I need to mention that we should then view $R_V \colon V \longrightarrow V$ instead of $\twoheadrightarrow V^G$??**).

(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 $R(W) = W^G$.

(e) If X is an affine G-variety, the Reynolds operator for $K[X]$ is unique

Proof.
(a)
Let V be a subrepresentation of a rational representation V' of G. We write $V = V^G \oplus W$ 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 retreive $u' = 0$, 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 $R'_V \colon V \longrightarrow Y$ 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 $R|_V : V \longrightarrow K[X]$ 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 is 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 existence. In the following, we see that in fact there always exists a Reynolds operator for groups with the previously described properties.

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 $R\colon K[X] \twoheadrightarrow K[X]^G$.

Proof.
(a) $\Longrightarrow$ (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:

$$\begin{aligned}(\sigma.f - f)(v) \quad &=(\sigma.f - f)(u) + (\sigma.f - f)(w) \\ &=f(\sigma^{-1}.u) - f(u) + 0 \\ &=f(u) - f(u) = 0\end{aligned} \tag{5}$$

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 **(How clear is this??)**, 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) $\Longrightarrow$ (c)

Let X be an affine G-variety. Let $f \in K[X]$. We define the map $R\colon K[X] \longrightarrow K[X]^G$, $f \mapsto R_{V_f}(f)$. 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 $R(\lambda f + g) = R_{V_{\lambda f+g}}(\lambda f + g) = R_{V_f + V_g}(\lambda f + g) = \lambda R_{V_f+V_g}(f) + R_{V_f+V_g}(g) = \lambda R_{V_f}(f) + R_{V_g}(g) = \lambda R(f) + R(g)$. The map R is also 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 for all $f \in K[X]$ R_{V_f} is G-invariant and for all $\sigma \in G$ we have $V_f = V_{\sigma.f}$. 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 afore mentioned basis. Now we define $p_v\colon K[V^*] \twoheadrightarrow K$, $f \mapsto f(\tilde{v})$. Consider the isomorphism of representations $\Phi\colon V \longrightarrow (V^*)^*$, $w \mapsto (\varphi \mapsto \varphi(w))$. 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 $\psi_v := p_v \circ R \circ \Phi\colon V \longrightarrow K$. 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 $\psi_v(v) = p_v(\Psi(v)) = \Phi(v)(\tilde{v}) = \tilde{v}(v) = 1 \neq 0$. 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 G is semisimple, that is for every rational representation V of G and subrepresentation W of V there exists a subrepresentation Z of V such that $V = W \oplus Z$.

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 $A \leftrightarrow (B \mapsto k^{-1}\operatorname{tr}(A \circ B))$ 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 see that our identification $A \leftrightarrow (B \mapsto k^{-1}\operatorname{tr}(A \circ B))$ is an isomorphism of representations between $\operatorname{Hom}_K(W,V)^*$ and $\operatorname{Hom}_K(V,W)$. 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 **(CITE!)** 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 $V = W \oplus Z$.
Now let us prove the claim for an arbitrary subrepresentatio 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 earlier, 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 our assumption, we there also exists a subrepresentation Z of V^* such that $V^* = (V^*)^G \oplus Z$. 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. □

3.2 Hilbert's Finiteness Theorem

Proposition 3.8
See [DK15, p.41 Corollary 2.2.7]
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 $R(fg) = fR(g)$, id est the Reynolds operator is a $K[X]^G$*-module homomorphism.*

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 $R'_{V_g}\colon fV_g \longrightarrow fV_g$, $fh \mapsto fR(h)$ 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 means that we have $R(fg) = fR(g)$. □

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, there exist finitely many linearly independent invariants $\{f_i\}_{i\in[r]} \subseteq K[V]^G$ such that $\left(\{f_i\}_{i\in[r]}\right) = I_{i>0}$. 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:

$$g = R(g) = R\left(\sum_{i=1}^r g_i f_i\right) = \sum_{i=1}^r R(g_i) f_i \tag{6}$$

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. □

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

$$\begin{aligned} \mu\colon \quad \mathrm{GL}_n \times V &\longrightarrow V \\ (\sigma, A) &\longmapsto \sigma A \sigma^{-1} \end{aligned} \tag{7}$$

where $V = K^{n,n}$ 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 exactly are the invariants? The invariants are exaclty those polynomials that are independent of the choice of the basis. The most well-known invariant is the determinant. From this obvservation 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

$$\det(tI_n - A) = \sum_{i=0}^{n} p_{n,i}(A)t^i \tag{8}$$

this means that every $p_{n,i}$ is an invariant polynomial in $K[K^{n.n}]$! This is how one usually proves that the trace is an invariant polynomial after observing that $p_{n,n-1} = \mathrm{tr}_n$. Are there other invariants than these $p_{n,i}$? No! To see this, we will use a little trick: Consider $D := \{\, \delta \in V \mid \delta \,\text{diagonalizable}\,\} \subseteq K[V]$. Since K is algebraically closed, D is Zariski-dense in V, and we have $K[V] \simeq= K[V]|_D$ via $p \leftrightarrow p|_D$. 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: $\pi\colon K^{n,n} \twoheadrightarrow K^n, [A_{i,j}]_{i,j\in[n]} \longmapsto (A_{i,i})_{i\in[n]}$. Consider $\tilde{p} := p \circ \mathrm{diag}$ $\tilde{p}$ is S_n-invariant: If $M_\tau \in \mathrm{GL}_n$ is the permutation matrix corresponding to $\tau \in S_n$, then for all $\tau \in S_n$ and for all $X \in K^n$ we have

$$\begin{aligned} \tau.\tilde{p}(X) &= \tilde{p}(\tau^{-1}.X) \\ &= p(\mathrm{diag}(\tau^{-1}.X) \\ &= p(M_\tau^{-1} \cdot \mathrm{diag}(X)) \\ &= M_\tau.p(\mathrm{diag}(X)) \\ &= p(\mathrm{diag}(X)) \qquad = \tilde{p}(X) \end{aligned} \tag{9}$$

From the fundamental theorem of symmetric polynomials we can follow that $\tilde{p} \in \mathrm{span}\{e_{n,i}\}_{i=0}^n$, say $\tilde{p} = \Sigma_{i=0}^n \lambda_i e_{n,i}$, where $\{e_{n,i}\}_{i=0}^n$ 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 $p = \Sigma_{i=0}^n \lambda_i e_{n,i} \circ \pi \circ s$. Now we want to show that $e_{n,i} \circ \pi \circ s = p_{n,i}$, which would conclude our claim. For all $A \in D$ we have

$$\begin{aligned} \sum_{i=0}^{n} (e_{n,i} \circ \pi \circ s)(A)t^i &= \det(t - \sigma_A.A) \\ &= \det(t - A) \qquad = \sum_{i=0}^{n} p_{n,i}(A)t^i \end{aligned} \tag{10}$$

which shows our claim. Note that this is independent of the choice of s, which means that we don't need the axiom of choice.

We now showed that the invariant ring $K[V]^{\mathrm{GL}_n}$ is finiteley generated independently of Hilbert's finiteness theorem, but a priori, Hilbert's finiteness theorem gives us a quicker but not very qualitative answer.

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 $A(V^G) = A(Z^G + {W'}^G) = A({W'}^G) = A(W')^G = W^G$. □

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 $i\colon X \longrightarrow W^*$, $x \mapsto (w \mapsto w(x))$. This is injective, since W contains a generating set of $K[X]$, which means that i is an embedding. □

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, 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 2.1, we have an affine variety

$$X := \{\, (x_1, x_2, x_3, x_4) \in (K^2)^4 \mid q(x_1, x_2, x_3, x_4) \neq 0 \,\} \tag{11}$$

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 $\mu\colon\ \mathrm{GL}_2 \times X \longrightarrow X$, $(\sigma, (x_1, x_2, x_3, x_4)) \mapsto (\sigma x_1, \sigma x_2, \sigma x_3, \sigma x_4)$. The Rabinowitsch-trick gives us the inclusion $i\colon X \hookrightarrow K \times (K^2)^4$ as described in proposition 2.1. 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 $i^*(K[V]^G) = K[X]^G$. □

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. □

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 $\mu\colon \mathrm{GL}_2 \times X \longrightarrow X$, $(\sigma, (x_1, x_2, x_3, x_4)) \mapsto (\sigma x_1, \sigma x_2, \sigma x_3, \sigma x_4)$. 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

$$\begin{aligned} \mathrm{cr}\colon \qquad & X \longrightarrow K \\ (x_1, x_2, x_3, x_4) &\longmapsto \frac{\det(x_1, x_2)\det(x_3, x_4)}{\det(x_2, x_3)\det(x_4, x_1)} \end{aligned} \tag{12}$$

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.

3.3 The Reynolds Operator Of A Group

In theorem 3.6 we have learned about three 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 soon learn about an additional way to characterize linearly reductive groups, which will motivate Cayley's Ω-process.

Definition 3.14: Reynolds Operator Of A Group
Let G be a linear algebraic group. The multiplication $m\colon G \times G \longrightarrow G$ makes G a G-variety. Assume that there exists a Reynolds operator $R_G\colon K[G] \twoheadrightarrow K[G]^G = K$ for this action. We call R_G the *Reynolds operator of* G.

Proposition 3.15
If R_G is a Reynolds Operator of a linear algebraic group G, it is also G-invariant under the action $(\sigma, f) \mapsto \sigma\dot{}f := (\tau \mapsto f(\tau\sigma))$ as described in 2.9, that is we have $R_G(\sigma\dot{}f) = R_G(f)$ for all $\sigma \in G$ and $f \in K[G]$.

Proof. BIG CITE WTH
MAYBE NOT EVEN TRUE □

Definition 3.16
Define the multiplication on $K\left[G\right]^*$, denoted by $*$, as follows: For $\alpha, \beta \in K\left[G\right]^*$:

$$\alpha * \beta := (\alpha \otimes \beta) \circ m^* \tag{13}$$

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

Example: TODO

Proposition 3.17
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

$$(m^* \otimes \mathrm{id}) \circ m^* = (\mathrm{id} \otimes m^*) \circ m^* \tag{14}$$

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

$$\begin{aligned}(\delta * \gamma) * \varphi &= (((\delta \otimes \gamma) \circ m^*) \otimes \varphi) \circ m^* = ((\delta \otimes \gamma) \otimes \varphi) \circ (m^* \otimes \mathrm{id}) \circ m^* \\ &= (\delta \otimes (\gamma \otimes \varphi)) \circ (\mathrm{id} \otimes m^*) \circ m^* = (\delta \otimes ((\gamma \otimes \varphi) \circ m^*)) \circ m^* = \delta * (\gamma * \varphi)\end{aligned} \tag{15}$$

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

Now we can formally define $K[G]^*$-actions.

Definition 3.18
Let $\mu\colon G \times V \longrightarrow V$ be a rational linear action, from which we retrieve μ' as described in definition 2.6. For $\delta \in K[G]^*$ and for $v \in V$ we define:

$$\delta \cdot v := \left(\left(\delta \otimes \mathrm{id}\right) \circ \mu'\right)\left(v\right) \tag{16}$$

Proposition 3.19
Definition 3.18 defines a $K[G]^*$-algebra-module.
See [DK15, A2.10]

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

$$(\mathrm{id} \otimes \mu') \circ \mu' = (\dot{m}^* \otimes \mathrm{id}) \circ \mu' \tag{17}$$

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

$$\begin{aligned} \gamma \cdot (\delta \cdot v) \quad &=((\gamma \otimes \mathrm{id}) \circ \mu' \circ (\delta \otimes \mathrm{id}) \circ \mu')(v) \\ &=((\gamma \otimes \mathrm{id}) \circ (\delta \otimes \mathrm{id} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \mu') \circ \mu')(v) \\ &=((\delta \otimes \gamma \otimes \mathrm{id}) \circ (\dot{m}^* \otimes \mathrm{id}) \circ \mu')(v) \\ &=((((\gamma \otimes \delta) \circ m^*) \otimes \mathrm{id}) \circ \mu')(v) \qquad =(\gamma * \delta) \cdot v \end{aligned} \tag{18}$$

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

Remark 3.19.1
If we look at definition 2.6, we can see that 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:

$$\sigma.v = \epsilon_\sigma \cdot v \tag{19}$$

Remark 3.19.2
The subalgebra

$$\{\, \delta \in K[G]^* \mid \forall f, g \in K[G] : \delta(fg) = \delta(f)g(e) + f(e)\delta(g) \,\} \tag{20}$$

is called the **Lie algebra**.

Theorem 3.20
Let G be linearly reductive, and let G act regularly on an affine variety X, which induces a rational G-action on $K[X]$ as described in definition 2.7. Then, the following the map

$$R\colon K[X] \longrightarrow K[X]^G \qquad\qquad f \mapsto R_G \cdot f \tag{21}$$

defines a Reynolds operator.

Proof. As per our construction from definition 3.18, 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:

$$\begin{aligned} \sigma.\left(R_G \cdot f\right)(x) \quad &= \left(R_G \cdot f\right)(\sigma^{-1}.x) \\ &=\Sigma_i R_G\left(p_i\right) \sigma.g_i\left(x\right) \\ &=\Sigma_i R_G(\sigma.p_i)\sigma.g_i(x) \\ &= \left(R_G \otimes \mathrm{id}\right)\left(\Sigma_i \sigma.p_i \otimes \sigma.g_i\right)(x) \\ &=(R_G \otimes \mathrm{id})(\bar{\mu}'(f))(x) \qquad =(R_G \cdot f)(x) \end{aligned} \tag{22}$$

We made use of the G-invariance of R_G and proposition 2.11. 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 $\sigma \in G$ and let $f \in K[X]$, and let $\bar{\mu}'(f) = \Sigma_{i=1}^r p_i \otimes g_i \subseteq K[G] \otimes K[X]$. We then have

$$\begin{aligned} R_G \cdot \sigma.f \quad &=(R_G \otimes \mathrm{id})\left(\bar{\mu}'(\sigma.f)\right) \\ &=(R_G \otimes \mathrm{id})\left(\sum_{i=1}^{r} \sigma^{\cdot} p_i \otimes g_i\right) \\ &=\sum_{i=1}^{r} R_G(\sigma^{\cdot} p_i) g_i \\ &=\sum_{i=1}^{r} R_G(p_i) g_i \qquad &&=R_G \cdot f \end{aligned} \tag{23}$$

We made use of proposition 2.10 and proposition 3.15. □

Corollary 3.20.1
G is linearly reductive if and only if the Reynolds operator of G exists. The Reynolds operator of G is unique.

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.
First, how is GL_n an affine variety? Consider $K^{n\times n} \times K$, and its coordinate ring $K\left[\{Z_{i,j}\}_{i,j\in\lceil n\rceil}, D\right]$. Now define $I := \left(\left(\sum_{\sigma\in S_n} \mathrm{sgn}\,(\sigma) \prod_{i\in\lceil n\rceil} Z_{i,\sigma(i)}\right) \cdot D - 1\right) = (\det(Z) \cdot D - 1)$, where $Z := \left[Z_{i,j}\right]_{i,j\in\lceil n\rceil}$. Then $V(I) = \{\, (z,d) \mid z \in \mathrm{GL}_n, d = \det(z)^{-1} \,\}$. Equipped with the componentwise multiplication (GL_n and $K\backslash\{0\}$, respectively), this is a linear algebraic group isomorphic to GL_n. The coordinate ring $K\left[\mathrm{GL}_n\right]$ is isomorphic to $K\left[\{Z_{i,j}\}_{i,j\in\lceil n\rceil}, \det(Z)^{-1}\right] \subseteq K\left(\{Z_{i,j}\}_{i,j\in\lceil n\rceil}\right)$, and we will write it as such from now on.

Definition 4.1: Cayley's Ω-Process
We call

$$\Omega := \sum_{\sigma\in S_n} \mathrm{sgn}\,(\sigma) \prod_{i\in\lceil n\rceil} \frac{\partial}{\partial z_{i,\sigma(i)}} \tag{24}$$

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

Lemma 4.2

$$\left(\det\left(Z\right)^{-1}\cdot\otimes\Omega\right)\circ m^{*}=m^{*}\circ\Omega=\left(\Omega\otimes\det\left(Z\right)^{-1}\cdot\right)\circ m^{*}\tag{25}$$

where we write "$p\cdot$" for the operation *multiply with* p for a polynomial $p\in K\left[\mathrm{GL}_n\right]$ (but the reader must not worry, this is the only time we will make use of this notation).

Proof. Here, we will follow the same convention as described in definition 2.3: The "left" and "right" inputs of m will be represented by $X=\left[X_{i,j}\right]_{i,j\in\lceil n\rceil}$ and $Y=\left[Y_{i,j}\right]_{i,j\in\lceil n\rceil}$ in the occuring polynomials respectively, and the outputs $m=\left[m_{i,j}\right]_{i,j\in\lceil n\rceil}$ are indexed in the same way as the inputs of the polynomials in $Z_{1,1},Z_{1,2},\ldots Z_{n,n}$.

Let $f\in K\left[\mathrm{GL}_n\right]$. Then $f\circ m\in K\left[\left\{X_{i,j}\right\}_{i,j\in\lceil n\rceil},\det\left(X\right)^{-1},\left\{Y_{i,j}\right\}_{i,j\in\lceil n\rceil},\det\left(Y\right)^{-1}\right]$. For fixed $i,j\in\lceil n\rceil$ we have

$$\begin{aligned}\left(\mathrm{id}\otimes\frac{\partial}{\partial Z_{i,j}}\right)\left(m^{*}\left(f\right)\right)&=t\left(\frac{\partial}{\partial Y_{i,j}}\left(f\circ m\right)\right)=t\left(\sum_{k,l\in\lceil n\rceil}\left(\left(\frac{\partial}{\partial Z_{k,l}}f\right)\circ m\right)\cdot\frac{\partial}{\partial Y_{i,j}}m_{k,l}\right)\\&=t\left(\sum_{k=1}^{n}\left(\left(\frac{\partial}{\partial Z_{k,j}}f\right)\circ m\right)\cdot X_{k,i}\right)=\sum_{k=1}^{n}\left(Z_{k,i}\cdot\otimes\mathrm{id}\right)\left(m^{*}\left(\frac{\partial}{\partial Z_{k,j}}f\right)\right)\end{aligned}\tag{26}$$

Note the use of t as described in definition 2.3 to aid in rephrasing terms. Successively applying this yields

$$\begin{aligned}\left(\mathrm{id}\otimes\Omega\right)\left(m^{*}\left(f\right)\right)&=\sum_{\sigma\in S_n}\mathrm{sgn}\left(\sigma\right)\left(\mathrm{id}\otimes\prod_{i=1}^{n}\frac{\partial}{\partial Z_{i,\sigma(i)}}\right)\left(m^{*}\left(f\right)\right)\\&=\sum_{\sigma\in S_n}\mathrm{sgn}\left(\sigma\right)\sum_{k\in\lceil n\rceil^{n}}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^{*}\left(\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)\\&=\sum_{k\in\lceil n\rceil^{n}}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^{*}\left(\sum_{\sigma\in S_n}\mathrm{sgn}\left(\sigma\right)\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)\\&=\sum_{k\in S_n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^{*}\left(\sum_{\sigma\in S_n}\mathrm{sgn}\left(\sigma\right)\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)\\&=\sum_{k\in S_n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^{*}\left(\mathrm{sgn}(k)\Omega(f)\right)\right)=\left(\det(Z)\cdot\otimes\mathrm{id}\right)\left(m^{*}\left(\Omega(f)\right)\right)\end{aligned}\tag{27}$$

This immediately shows the first equality, and the second equality is proven analogously. □

Lemma 4.3

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

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

$$\Omega^p\left(\det(Z)^p\right) = \sum_i a_i q_i \left(\left\{\frac{\partial}{\partial Z_{k,l}}\right\}_{k,l\in\lceil n\rceil}\right)\left(\sum_j a_j q_j\left(\{Z_{k,l}\}_{k,l\in\lceil n\rceil}\right)\right) \tag{28}$$

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

$$c_{p,n} = \sum_i a_i^2 q_i\left(\left\{\frac{\partial}{\partial Z_{k,l}}\right\}_{k,l\in\lceil n\rceil}\right)\left(q_i\left(\{Z_{k,l}\}_{k,l\in\lceil n\rceil}\right)\right) \in \mathbb{N}_{>0} \tag{29}$$

□

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 $\tilde{f} \in K\left[\{Z_{i,j}\}_{k,l\in\lceil n\rceil}\right]_{pn}$, define for $f = \frac{\tilde{f}}{\det(Z)^p}$:

$$R(f) := \frac{\Omega^p \tilde{f}}{c_{p,n}} \tag{30}$$

The linear extension of this (mapping anything else in $K[\mathrm{GL}_n]$ to zero), defines the Reynolds Operator R_{GL_n}, which makes GL_n *linearly reductive.*

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 $p \in \mathbb{N}$. Now we show that R is GL_n-invariant. 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

$$\begin{aligned}
R(\beta.f)(\gamma) = R\left(\frac{\det(\beta)^p \cdot \beta.\tilde{f}}{\det(Z)^p}\right)(\gamma) &= \frac{\det(\beta)^p \cdot \Omega^p\left(\beta.\tilde{f}\right)(\gamma)}{c_{p,n}} \\
&= \frac{1}{c_{p,n}} \cdot \left(\epsilon_{\beta^{-1}} \otimes \epsilon_\gamma\right)\left(\left(\left(\det(Z)^{-p} \cdot \otimes \Omega^p\right) \circ m^*\right)\left(\tilde{f}\right)\right) \\
&= \frac{1}{c_{p,n}} \cdot \left(\epsilon_{\beta^{-1}} \otimes \epsilon_\gamma\right)\left(\left(\left(\Omega^p \otimes \det(Z)^{-p} \cdot\right) \circ m^*\right)\left(\tilde{f}\right)\right) \\
= \frac{\Omega^p\left(\gamma^{\cdot}\tilde{f}\right)\left(\beta^{-1}\right) \cdot \det\left(\gamma^{-1}\right)^p}{c_{p,n}} &= R\left(\frac{\gamma^{\cdot}\tilde{f} \cdot \det\left(\gamma^{-1}\right)^p}{\det(Z)^p}\right)\left(\beta^{-1}\right) \\
&= R\left(\gamma^{\cdot} f\right)\left(\beta^{-1}\right)
\end{aligned} \tag{31}$$

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 $g \in K\left[\mathrm{GL}_n\right]$ we have $R(g)(\delta) = R(g) \in K$. We then get for all $\alpha \in \mathrm{GL}_n$

$$\begin{aligned} R\left(\alpha.f\right) &= R\left(\alpha.f\right)\left(I_n\right) = R\left(I_n\dot{}f\right)\left(\alpha^{-1}\right) \\ &= R\left(I_n\dot{}f\right) = R(f) \end{aligned} \tag{32}$$

which shows the GL_n-invariance. Finally, the definition immediately gives us that R restricted to K is the identity. As mentioned in lemma 3.5(e), the uniqueness of the Reynolds Operator implies $R = R_{\mathrm{GL}_n}$. □

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

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

$$R\left(f\right) := R_{\mathrm{GL}_n}\left(\frac{\tilde{f}}{\det(Z)^p}\right) + I = \frac{\Omega^p \tilde{f}}{c_{p,n}} + I \tag{33}$$

The linear extension of this (mapping anything else in $K\left[\mathrm{SL}_n\right]$ to zero), defines the Reynolds Operator R_{SL_n}, making SL_n *linearly reductive.*

Proof. First, we will show $K\left[\mathrm{GL}_n\right]^{\mathrm{SL}_n} = K\left[\det(Z), \det(Z)^{-1}\right]$ (action by left multiplication). Let $g \in K\left[\mathrm{GL}_n\right]^{\mathrm{SL}_n}$, and let $\alpha \in \mathrm{GL}_n$. Now for $z \in K \setminus \{0\}$, define $M(z) = [z_{i,j}]_{i,j\in[n]} \in \mathrm{GL}_n$ to be the matrix with $z_{1,1} = z$ and $z_{i,j} = \delta_{i,j}$ for $(i,j) \neq (1,1)$. Note that $\alpha M\left(\det(\alpha)\right)^{-1} \in \mathrm{SL}_n$. Define $h := \left(\beta \mapsto g\left(M(\det(\beta))\right)\right) \in K\left[\det(Z), \det(Z)^{-1}\right]$. Now

$$\begin{aligned} g(\alpha) = \alpha M\left(\det(\alpha)\right)^{-1}.g\left(\alpha\right) &= g\left(M\left(\det(\alpha)\right)\alpha^{-1}\alpha\right) \\ &= g\left(M\left(\det(\alpha)\right)\right) = h(\alpha) \end{aligned} \tag{34}$$

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

$$\hat{R}(f) := \det(Z)^{r-p} \cdot \frac{\Omega^r \tilde{f}}{c_{r,n}} = \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\tilde{f}}{\det(Z)^r}\right) \tag{35}$$

and 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 $K\left[\mathrm{GL}_n\right]^{\mathrm{SL}_n}$: 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, the SL_n-invariance also follows from the last theorem: Let $\alpha \in \mathrm{SL}_n$. Then

$$\begin{aligned}\hat{R}(\alpha.f) = \hat{R}\left(\frac{\det(\alpha)^p \cdot \alpha.\tilde{f}}{\det(Z)^p}\right) &= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\det(\alpha)^p \cdot \alpha.\tilde{f}}{\det(Z)^r}\right) \\ &= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\det(\alpha)^r \cdot \alpha.\tilde{f}}{\det(Z)^r}\right) \\ &= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\alpha.\left(\frac{\tilde{f}}{\det(Z)^r}\right)\right) \\ &= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\tilde{f}}{\det(Z)^r}\right) = \hat{R}(f)\end{aligned} \tag{36}$$

where we used $\det(\alpha)^p = 1 = \det(\alpha)^r$ and the GL_n-invariance of R_{GL_n}. Thus we have shown that $\hat{R}$ is the Reynolds-Operator for the action of SL_n on GL_n by left-multiplication.

Lastly, this shows our proposed statement $R = R_{\mathrm{SL}_n}$, since $\det(Z) \sim 1$. □

5 Examples (not a section in the final version)

Let us apply the Reynolds operator with respect to an action on concrete polynomials. Before we look at finite generators of Hilbert's nullcone (which we will talk about later), we will just look at generators of the polynomial ring.

Example 5.1

Consider the group $G = \mathrm{SL}_2$ and the vector space $V = \left\{ A \in \mathbb{R}^{2\times 2} \mid A^T = A \right\}$. Now we will look at the following action:

$$\begin{aligned}\mu\colon \quad \mathrm{SL}_2 \times \quad V \quad &\longrightarrow V \\ (\quad S, \quad A) \quad &\longmapsto SAS^T\end{aligned} \tag{37}$$

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

$$\begin{aligned} S &= \begin{bmatrix} s_{1,1} & s_{1,2} \\ s_{2,1} & s_{2,2} \end{bmatrix} \qquad A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \\ S^{-1} &= \begin{bmatrix} s_{2,2} & -s_{1,2} \\ -s_{2,1} & s_{1,1} \end{bmatrix}\end{aligned} \tag{38}$$

We then have

$$\begin{aligned} & S^{-1}.A = S^{-1}A\left(S^{-1}\right)^T \\ & = \begin{bmatrix} a_{1,1}s_{2,2}^2 - 2a_{1,2}s_{1,2}s_{2,2} + a_{2,2}s_{1,2}^2 & -a_{1,1}s_{2,1}s_{2,2} + a_{1,2}s_{1,1}s_{2,2} + a_{1,2}s_{1,2}s_{2,1} - a_{2,2}s_{1,1} \\ -a_{1,1}s_{2,1}s_{2,2} + a_{1,2}s_{1,1}s_{2,2} + a_{1,2}s_{1,2}s_{2,1} - a_{2,2}s_{1,1}s_{1,2} & a_{1,1}s_{2,1}^2 - 2a_{1,2}s_{1,1}s_{2,1} + a_{2,2}s_{1,1}^2 \end{bmatrix}\end{aligned} \tag{39}$$

Notice that we also have

$$\begin{aligned}\det\left(\frac{\partial}{\partial S}\right)^n &= \left(\frac{\partial}{\partial S_{1,1}}\frac{\partial}{\partial S_{2,2}} - \frac{\partial}{\partial S_{1,2}}\frac{\partial}{\partial S_{2,1}}\right)^n \\ &= \sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{\partial}{\partial S_{1,1}}^{n-k}\frac{\partial}{\partial S_{1,2}}^{k}\frac{\partial}{\partial S_{2,1}}^{k}\frac{\partial}{\partial S_{2,2}}^{n-k}\end{aligned} \tag{40}$$

It is quite cumbersome to calculate the Reynolds Operator of general polynomials. We will look at the monomial $A_{1,1}^2$, for which we have

$$\begin{aligned}&\bar{m}u'(A_{1,1}^2) \\ =&S_{2,2}^4 \otimes A_{1,1}^2 - 4S_{1,2}S_{2,2}^3 \otimes A_{1,1}A_{1,2} + 2S_{1,2}^2S_{2,2}^2 \otimes A_{1,1}A_{2,2} \\ &+ 4S_{1,2}^2S_{2,2}^2 \otimes A_{1,2}^2 - 4S_{1,2}^3S_{2,2} \otimes A_{1,2}A_{2,2} + S_{1,2}^4 \otimes A_{2,2}^2 \\ =&\frac{S_{2,2}^4}{\det(S)^2} \otimes A_{1,1}^2 - \frac{4S_{1,2}S_{2,2}^3}{\det(S)^2} \otimes A_{1,1}A_{1,2} \\ &+ \frac{2S_{1,2}^2S_{2,2}^2}{\det(S)^2} \otimes A_{1,1}A_{2,2} + \frac{4S_{1,2}^2S_{2,2}^2}{\det(S)^2} \otimes A_{1,2}^2 \\ &- \frac{4S_{1,2}^3S_{2,2}}{\det(S)^2} \otimes A_{1,2}A_{2,2} + \frac{S_{1,2}^4}{\det(S)^2} \otimes A_{2,2}^2\end{aligned} \tag{41}$$

We can now apply the Reynolds operator in the way we discussed it in proposition 3.20 in combination with Cayley's Ω-process. Since all terms in $K[\mathrm{SL}_2]$ are already of degree 2, apply the same derivatives to each summand and calculate:

$$\begin{aligned}&R_G \cdot A_{1,1}^2 \\ =&\left(\frac{\partial}{\partial S_{1,1}}^2\frac{\partial}{\partial S_{2,2}}^2 - 2\frac{\partial}{\partial S_{1,1}}\frac{\partial}{\partial S_{1,2}}\frac{\partial}{\partial S_{2,1}}\frac{\partial}{\partial S_{2,2}} + \frac{\partial}{\partial S_{1,2}}^2\frac{\partial}{\partial S_{2,1}}^2\right) \cdot A_{1,1}^2 \\ =&0\end{aligned} \tag{42}$$

The zero-polynomial is not very interesting, so applying the Reynolds Operator to any polynomial will not always produce interesting results. We will try again for the polynomial $A_{1,2}^2$. We calculate

$$\begin{aligned}
&\mu'(A_{1,2}^2)\\
=&S_{2,1}^2S_{2,2}^2 \otimes A_{1,1}^2 - 2S_{1,1}S_{2,1}S_{2,2}^2 \otimes A_{1,1}A_{1,2}\\
&- 2S_{1,2}S_{2,1}^2S_{2,2} \otimes A_{1,2}^2 + 2S_{1,1}S_{1,2}S_{2,1}S_{2,2} \otimes A_{1,1}A_{2,2}\\
&+ S_{1,1}^2S_{2,2}^2 \otimes A_{1,2}^2 + 2S_{1,1}S_{1,2}S_{2,1}S_{2,2} \otimes A_{1,2}^2\\
&- 2S_{1,1}^2S_{1,2}S_{2,2} \otimes A_{1,2}A_{2,2} + S_{1,2}^2S_{2,1}^2 \otimes A_{1,2}^2\\
&- 2S_{1,1}S_{1,2}^2S_{2,1} \otimes A_{1,2}A_{2,2} + S_{1,1}^2S_{1,2}^2 \otimes A_{2,2}^2\\
=&\frac{S_{2,1}^2S_{2,2}^2}{\det(S)^2} \otimes A_{1,1}^2 - \frac{2S_{1,1}S_{2,1}S_{2,2}^2}{\det(S)^2} \otimes A_{1,1}A_{1,2}\\
&- \frac{2S_{1,2}S_{2,1}^2S_{2,2}}{\det(S)^2} \otimes A_{1,2}^2 + \frac{2S_{1,1}S_{1,2}S_{2,1}S_{2,2}}{\det(S)^2} \otimes A_{1,1}A_{2,2}\\
&+ \frac{S_{1,1}^2S_{2,2}^2}{\det(S)^2} \otimes A_{1,2}^2 + \frac{2S_{1,1}S_{1,2}S_{2,1}S_{2,2}}{\det(S)^2} \otimes A_{1,2}^2\\
&- \frac{2S_{1,1}^2S_{1,2}S_{2,2}}{\det(S)^2} \otimes A_{1,2}A_{2,2} + \frac{S_{1,2}^2S_{2,1}^2}{\det(S)^2} \otimes A_{1,2}^2\\
&- \frac{2S_{1,1}S_{1,2}^2S_{2,1}}{\det(S)^2} \otimes A_{1,2}A_{2,2} + \frac{S_{1,1}^2S_{1,2}^2}{\det(S)^2} \otimes A_{2,2}^2
\end{aligned} \tag{43}$$

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

$$\begin{aligned}
&R_G \cdot A_{1,2}^2\\
=&\left(\frac{\partial}{\partial S_{1,1}}^2 \frac{\partial}{\partial S_{2,2}}^2 - 2\frac{\partial}{\partial S_{1,1}}\frac{\partial}{\partial S_{1,2}}\frac{\partial}{\partial S_{2,1}}\frac{\partial}{\partial S_{2,2}} + \frac{\partial}{\partial S_{1,2}}^2 \frac{\partial}{\partial S_{2,1}}^2\right) \cdot A_{1,2}^2\\
=&-\frac{4}{12}A_{1,1}A_{2,2} + \frac{4}{12}A_{1,2}^2 - \frac{4}{12}A_{1,2}^2 + \frac{4}{12}A_{1,2}^2\\
=&-\frac{1}{3}\det(A)
\end{aligned} \tag{44}$$

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

Example 5.2
We will now discuss the cross ratio. Since the projective line isn't an affine variety, we will look at points in K^2 to make the situation affine, which will make some things different. Consider $(K^2)^4$ and with the coordinate functions $\{(X_i)_k\}_{i\in[4],k\in[2]}$. (We write $X_i = \left(\begin{smallmatrix}(X_i)_1\\(X_i)_2\end{smallmatrix}\right)$ for $i \in [4]$.) Define $q := \prod_{i,j\in[r],i<j} \det(X_i, X_j)$. As described in 2.1, we have an affine variety

$$X := \{\, (x_1, x_2, x_3, x_4) \in (K^2)^4 \mid q(x_1, x_2, x_3, x_4) \neq 0 \,\} \tag{45}$$

with the coordinate ring $K[X] = K[\{(X_i)_k\}_{i\in[4],k\in[2]}, q^{-1}]$. Nothe that $q(x_1, x_2, x_3, x_4) \neq 0$ is equivalent to saying that for $i \neq j$ we have $x_i \notin \operatorname{span} x_j$, or rather in projective terms $[x_i] \neq [x_j]$. Now consider the action of GL_2 on X via pointwise application. The *cross ratio* $\mathrm{cr} \in K[X]$ defined as follows

$$\begin{aligned} \mathrm{cr}\colon \qquad\qquad & X \longrightarrow K \\ (x_1, x_2, x_3, x_4) & \longmapsto \frac{\det(x_1, x_2)\det(x_3, x_4)}{\det(x_2, x_3)\det(x_4, x_1)} \end{aligned} \tag{46}$$

is an invariant under this action, as well as the same map with permuted inputs, as is easily seen. Together with the fact that the condition $q(x_1, x_2, x_3, x_4) \neq 0$ is also GL_2-invariant, this actually guarantees us a coordinate-free definition of the cross ratio for any two-dimensional vector-space. The invariant ring $K[X]^{\mathrm{GL}_n}$ is finitely generated, as we know by Hilbert's finiteness theorem. In fact, we don't have more invariants than polynomials in the cross ratio (NOT TRUE!): $K[X]^{\mathrm{GL}_n} = K[\{\mathrm{cr}(X_{\pi_1}, X_{\pi_2}, X_{\pi_3}, X_{\pi_4})\}_{\pi \in S_4}]$. We actually have $K[\{\mathrm{cr}(X_{\pi_1}, X_{\pi_2}, X_{\pi_3}, X_{\pi_4})\}_{\pi \in S_4}] = K[\mathrm{cr}, (\mathrm{cr}(\mathrm{cr}-1))^{-1}]$, since we can calculate that for any permutation $\pi in S_4$ we have $\mathrm{cr}(X_{\pi_1}, X_{\pi_2}, X_{\pi_3}, X_{\pi_4}) \in \{\mathrm{cr}, \mathrm{cr}^{-1}, 1-\mathrm{cr}, (1-\mathrm{cr})^{-1}, \mathrm{cr}^{-1}(\mathrm{cr}-1)\}$. To see that the invariant ring looks like what we claimed, we need some results from the projective geometry. The cross ratio is also defined in the projective space: Let Y be defined as those points in $P(K^2)^4$ that are pairwise distinct. Y is equal to $P(X)$, and X itself is already a cone. The projective cross ratio cr_P is then well-defined since it is independent of the choice of representatives because the determinant is multilinear. This means that for any $(a, b, c, d) \in X$ we are allowed to write $\mathrm{cr}(a, b, c, d) = \mathrm{cr}([a], [b], [c], [d])$. For the same reasons as before, this projective cross ratio is also $\mathrm{PGL}(K^2)$-invariant. 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 pairwise y_1, y_2 and y_3 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 $\rho(x_3) = y_3$. 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 $\rho_{B,C,D} \in \mathrm{PGL}(K^2)$ such that $\rho_{B,C,D}(B) = 0_P$, $\rho_{B,C,D}(C) = 1_P$ and $\rho_{B,C,D}(D) = \infty_P$. Since A is distinct from D we know $\rho_{B,C,D}(A) \neq \infty_P$, and therefore there exists some $a \in K$ such that $\rho_{B,C,D}(A) = [\binom{a}{1}]$. We then compute $\rho_{B,C,D}(A) = [\binom{a}{1}] = \mathrm{cr}([\binom{a}{1}], [\binom{0}{1}], [\binom{1}{1}], [\binom{1}{0}])_P = \mathrm{cr}(\rho_{B,C,D}(A), \rho_{B,C,D}(B), \rho_{B,C,D}(C), \rho_{B,C,D}(D))_P = \mathrm{cr}(A, B, C, D)_P$. This means that for $(a, b, c, d) \in X$ we have $\rho_{[b],[c],[d]}([a]) = \mathrm{cr}(a, b, c, d)$, so we can choose a representative $r_{a,b,c,d} \in \rho_{[b],[c],[d]}$ such that $r_{a,b,c,d}(a) = \binom{\mathrm{cr}(a,b,c,d)}{1}$. Let $f \in K[X]^{\mathrm{GL}_2}$. We have $f(a, b, c, d) = r_{a,b,c,d}^{-1} . f(a, b, c, d) = f(r_{a,b,c,d}(a), r_{a,b,c,d}(b), r_{a,b,c,d}(c), r_{a,b,c,d}(d)) =$

Example 5.3

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

$$\begin{aligned} \mu\colon \quad \mathrm{GL}_n \times K^{n.n} & \longrightarrow K^{n,n} \\ (\sigma, A) & \longmapsto \sigma A \sigma^{-1} \end{aligned} \tag{47}$$

What are its invariants? The invariants are exaclty those polynomials that are independent of the choice of basis. The most well-known invariant is the determinant. From this obvservation 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

$$\det(tI_n - A) = \sum_{i=0}^{n} p_{n,i}(A)t^i \tag{48}$$

this means that every $p_{n,i}$ is an invariant polynomial in $K[K^{n.n}]$! This is how one usually proves that the trace is an invariant polynomial after observing that $p_{n,n-1} = \mathrm{tr}_n$. Are there other invariants than these $p_{n,i}$? No! To see this, we will use a little trick: Consider $D := \{\, \delta \in K^{n,n} \mid \delta\,\text{diagonalizable}\,\} \subseteq K[K^{n,n}]$. Since K is algebraically closed, D is Zariski-dense in $K^{n,n}$, and we have $K[K^{n,n}] \simeq= K[K^{n,n}]|_D$ via $p \leftrightarrow p|_D$. For this reason, we will look at the evaluation of an invariant polynomial $p \in K[K^{n.n}]$ only on elements in D, and can deduce what polynomial it is.
Let $p \in K[K^{n,n}]^{\mathrm{GL_n}}$. We define a projection onto the diagonal: $\pi\colon K^{n,n} \twoheadrightarrow K^n, [A_{i,j}]_{i,j\in[n]} \longmapsto (A_{i,i})_{i\in[n]}$. Consider $\tilde{p} := p \circ \mathrm{diag}_n$ $\tilde{p}$ is S_n-invariant: If $M_\tau \in \mathrm{GL}_n$ is the permutation matrix corresponding to $\tau \in S_n$, then for all $\tau \in S_n$ and for all $X \in K^n$ we have

$$\begin{aligned} \tau.\tilde{p}(X) \quad &= \tilde{p}(\tau^{-1}.X) \\ &= p(\mathrm{diag}_n(\tau^{-1}.X) \\ &= p(M_\tau^{-1} \cdot \mathrm{diag}_n(X)) \\ &= M_\tau.p(\mathrm{diag}_n(X)) \\ &= p(\mathrm{diag}_n(X)) \qquad &= \tilde{p}(X) \end{aligned} \tag{49}$$

From the fundamental theorem of symmetric polynomials we can follow that $\tilde{p} \in \mathrm{span}\{e_{n,i}\}_{i=0}^n$, say $\tilde{p} = \Sigma_{i=0}^n \lambda_i e_{n,i}$, where $\{e_{n,i}\}_{i=0}^n$ 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 $p = \Sigma_{i=0}^n \lambda_i e_{n,i} \circ \pi \circ s$. Now we want to show that $e_{n,i} \circ \pi \circ s = p_{n,i}$, which would conclude our claim. For all $A \in D$ we have

$$\begin{aligned} \sum_{i=0}^{n} (e_{n,i} \circ \pi \circ s)(A)t^i \quad &= \det(t - \sigma_A.A) \\ &= \det(t - A) \qquad &= \sum_{i=0}^{n} p_{n,i}(A)t^i \end{aligned} \tag{50}$$

which shows our claim. Note that this is independent of the choice of s, which means that we don't need the axiom of choice (rigorously, as usual, rewrite s as a relation for all possible s instead of a choice of a function…).

6 Further Discussion

fdsafdsa fdsafdsa

References

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

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