Cayley's Ω-Process And The Reynolds Operator

Bert Lorke

January 16, 2018

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, which he 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. We look at the group of all transformations which leave angles unchanged, which are called conformal transformations. 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 specifically: In invariant theory, we try to find invariant polynomial-like functions.

One of the most important concept is the cross ratio: The cross ratio is a rational polynomial which takes as its input four collinear points. This is invariant under projective transformations. Is this the only invariant polynomial? 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 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.

[1] I read somewhere that it is not certain

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? 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 the 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, 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 Pre-work

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.

Definition 2.1
We denote by m the group multiplication of the group G. We want to view the pullback of m as a map $m^* : K[G] \longrightarrow K[G] \otimes K[G]$, which makes sense, because m and $\otimes$ are associative. The strict pullback, which I will call $\hat{m}$, should be a map of the type $K[G] \longrightarrow K[G \times G]$, where $f \mapsto f \circ m$. If we want to give the variables names, we can equivalently say it is a map $K[Z]|_G \longrightarrow K[X,Y]|_{G \times G}$, where $Z = \{Z_1, \ldots, Z_k\}$, X and Y analogously (here, m canonically takes its

left input via X and its right input via Y). Define

$$\begin{aligned} t\colon\ K\left[X,Y\right]\big|_{G\times G} &\longrightarrow K\left[Z\right]\big|_{G}\otimes K\left[Z\right]\big|_{G} \\ \sum_i \lambda_i \prod_j X_j^{d_{i,j}} \prod_j Y_j^{e_{i,j}} &\mapsto \sum_i \lambda_i \prod_j Z_j^{d_{i,j}} \otimes \prod_j Z_j^{e_{i,j}} \end{aligned} \tag{1}$$

This is independant of the choice of the representatives and therefore well-defined. It is even an isomorphism. Now, finally, define $m^* := t \circ \hat{m} : K[G] \longrightarrow K[G] \otimes K[G]$.

Remark 2.1.1
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 $f \in K[Z]\big|_G$, we will write $\mathrm{id} \otimes \frac{\partial}{\partial Z_i}(m^* f)$ as in [DK15], whereas [Stu08] would write $\frac{\partial}{\partial Y_i} f(XY)$.

Definition 2.2: Rational Representation
Let V be a vector space (not necessarily finite dimensional), and $\mu : G \times V \longrightarrow V$ an action. We call μ a **rational representation** iff there exists a linear map $\mu'\colon V \longrightarrow K[G] \otimes V$ such that $\mu(\sigma, v) = ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu')(v)$.

Remark 2.2.1
If $\tilde{\mu}$ is the action defined by $\tilde{\mu}(\sigma, x) = \mu(\sigma^{-1}, x)$, then $\mu' = \tilde{\mu}^*$, where μ^* denotes the algebraic cohomomorphism.

Definition 2.3: Regular Action, Regular Representation
Let G be a linear algebraic group, X an affine variety. We call an action $G \times X \longrightarrow X$ a **regular action**, iff it is a morphism of affine varieties. We say G **acts regularly on** X.
For a finite-dimensional vector space V, if $\mu\colon G \times V \longrightarrow V$ is a representation in the classical sense, that is for all $g \in G$ we have $D_\mu(g) := (v \mapsto g.v) \in \mathrm{GL}(V)$, we call μ a **regular representation** iff it is regular.

Proposition 2.4
An action $\mu\colon G \times V \longrightarrow V$ is a rational representation if and only if the action is locally finite (id est for every $v \in V$, $\mathrm{span}(G.v)$ is finite-dimensional), and every finite-dimensional G-stable subspace W, $\mu|_{G\times W}$ is a regular representation.

Proof. See [DK15, A.1.8] and [DK15, 2.2.5(b) $\Longrightarrow$ (c),2.2.6]
Assume that μ is a rational representation. Let $v \in V$. We can write $\mu^*(v) = \Sigma_{i=1}^l f_i \otimes v_i$. We then easily see that $K(G.v) \subseteq \mathrm{span}\{v_i\}_{i=1}^l$, showing that the action is locally finite. Now let W be a finite-dimensional subrepresentation with the basis $\{w_i\}_{i=1}^r$. By assummption, we have $p_{i,j} \in K[G]$ with $\mu^*(w_j) =$

$\Sigma_{i=1}^{r} p_{i,j} \otimes w_i$. Now let $w = \Sigma_{j=1}^{r} \lambda_j w_j \in W$. Then for all $\sigma \in G$ we have

$$\begin{aligned} \mu(\sigma, w) &= ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu^*)(w) \\ &= \sum_{j=1}^{N} \lambda_j \sum_{i=1}^{N} p_{i,j}(\sigma) \cdot w_i \end{aligned} \tag{2}$$

from which we immediately notice that $D_{\mu|_{G\times W}}(\sigma) \in \mathrm{GL}(W)$. Therefore $\mu|_{G\times W}$ is a regular representation.
Now let μ be an action such that for every finite-dimensional G-stable subspace W, $\mu|_{G\times W}$ is a regular representation. Let $v \in V$. There exists a $\square$

Definition 2.5: Rational Representation
Let G be a linear algebraic group. A representation V of G is called a **rational representation**, iff its corresponding action $G \times V \longrightarrow V$ is a regular action.

Claim: If V is finite dimensional, the notions of the definitions coincide.
Proof: First, let V be a rational representation of G with basis $\{v_1, \ldots, v_N\}$ be a basis of V. By our assumption, we have a rational representation, therefore there exist $p_{i,j} \in K[G]$ such that $\mu(\sigma, v_j) = \Sigma_{i=1}^{N} p_{i,j}(\sigma) \cdot v_i$. Define $\mu^*(v_j) := \Sigma_{i=1}^{N} p_{i,j} \otimes v_i$. Now we easily see:

$$\begin{aligned} \mu(\sigma, v) &= \mu\left(\sigma, \Sigma_{j=1}^{N} \lambda_j v_j\right) \\ &= \sum_{j=1}^{N} \lambda_j \sum_{i=1}^{N} p_{i,j}(\sigma) \cdot v_i \\ &= \sum_{j=1}^{N} \lambda_j ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu^*)(v_j) \quad = ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu^*)(v) \end{aligned} \tag{3}$$

which was to show.

Remark 2.5.1
A rational representation $G \longrightarrow \mathrm{GL}(V)$ is of the following form:
If $a_{i,j} : G \longrightarrow K$ is the function of the (i,j)-entry, then $a_{i,j} \in K[G]$.
In fact, it is equivalent to define a representation as rational, iff its map $G \longrightarrow \mathrm{GL}(V)$ is a map of affine varieties.

Definition 2.6: Invariants
Let G act on X regularly.

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

It defines a linear subspace. This given action induces an action $G \times K[X] \longrightarrow K[X]$, where $K[X]$ is the coordinate ring, as follows:

$$(g, f) \longmapsto g \cdot f := \left(x \mapsto f\left(\sigma^{-1}.x\right)\right) \tag{5}$$

The **invariant ring** of the representation is defined as

$$K[X]^G := \{\, f \in K[X] \mid \forall g \in G : g \cdot f = f \,\} \tag{6}$$

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

Definition 3.1: Reynolds Operator
Let V be a rational representation of a linear algebraic group G. A G-invariant linear projection $K[V] \longrightarrow K[V]^G$ is called a **Reynolds Operator**.

Remark 3.1.1
If a Reynolds Operator exists, it is unique (?). See [DK15, p.39f]: In the proof of the equivalences, in the step "(b) $\Longrightarrow$ (c)", only the existence of the Reynolds operator is needed. Therefore, the existence of the Reynolds Operator already implies its uniqueness (?).

Definition 3.2: linearly reductive
A group G is called **linearly reductive** iff there exists a Reynolds operator for the regular action $G \times G \longrightarrow G$ by left multiplication $R_G \colon K[G] \longrightarrow K[G]^G = K$.

Remark 3.2.1
We could have also defined linear reductive groups as such, for which every regular action has a Reynolds Operator. We will prove that this is in fact equivalent.

Now we want to define an algebra structure on bla $K[G]$.

Definition 3.3
Define the multiplication on $K\left[G\right]^*$, denoted by $*$, as follows: For $\alpha, \beta \in K\left[G\right]^*$:

$$\alpha * \beta := (\alpha \otimes \beta) \circ m^* \tag{7}$$

More slowly: For $f \in K\left[G\right]$ we get $m^*\left(f\right) = \Sigma_i g_i \otimes h_i$ (with $g_i, h_i \in K\left[G\right]$), therefore the Kronecker-product gives us

$$(\alpha * \beta)\left(f\right) = \Sigma_i \alpha\left(g_i\right) \otimes \beta\left(h_i\right) = \Sigma_i \alpha\left(g_i\right) \beta\left(h_i\right) \tag{8}$$

As usual, we identify $K \otimes K$ with K canonically.

Example: TODO

Proposition 3.4
The multiplication $*$ makes $K\left[G\right]^*$ into an associative algebra with the neutral element $\epsilon := \epsilon_e$ (Note: $\epsilon_\sigma\left(f\right) = f\left(\sigma\right)$).

Proof. First, a small observation:

$$(m^* \otimes \mathrm{id}) \circ m^* = (\mathrm{id} \otimes m^*) \circ m^* \tag{9}$$

This is true because m (and $\otimes$) is associative. Then, for $\delta, \gamma, \varphi \in K\left[G\right]^*$:

$$\begin{aligned}(\delta * \gamma) * \varphi &= (((\delta \otimes \gamma) \circ m^*) \otimes \varphi) \circ m^* = (\delta \otimes \gamma \otimes \varphi) \circ (m^* \otimes \mathrm{id}) \circ m^* \\ &= (\delta \otimes \gamma \otimes \varphi) \circ (\mathrm{id} \otimes m^*) \circ m^* = (\delta \otimes ((\gamma \otimes \varphi) \circ m^*)) \circ m^* = \delta * (\gamma * \varphi)\end{aligned} \tag{10}$$

showing the associativity. The second equation is easily checked . Also, 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 3.5
Let G act regularly on a vectorspace V via μ, from which we retrieve μ^* as described in definition 2.2. $K[G]^*$ then acts on V as follows:

$$\delta \cdot v := ((\delta \otimes \mathrm{id}) \circ \mu')\,(v) \tag{11}$$

Remark 3.5.1
If we look at definition 2.2, 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:

$$\sigma . v = \epsilon_\sigma \cdot v \tag{12}$$

Remark 3.5.2
The subalgebra

$$\{\, \delta \in K[G]^* \mid \forall f, g \in K[G] : \delta(fg) = \delta(f)g(e) + f(e)\delta(g) \,\} \tag{13}$$

is called the **Lie algebra**.

Proposition 3.6
Let G be linearly reductive, and let G act regularly on an affine variety X, which induces a rational G-action on $K[X]$ (maybe prove this? easy...). Then, the following the map

$$R\colon K[X] \longrightarrow K[X]^G \qquad\qquad f \mapsto R_G \cdot f \tag{14}$$

defines a Reynolds operator.

Proof. As per our construction from definition 3.5, the linearity of this map should be clear. Let us now check that R does map polynomials to invariant polynomials. For this, let $f \in K[X]$, $\sigma \in G$ and $x \in X$. Write $\mu'(f) = \Sigma_i p_i \otimes g_i \in K[G] \otimes K[X]$. Now we compute:

$$\begin{aligned}
\sigma.\left(R_G \cdot f\right)(x) \quad &= \left(R_G \otimes id\right)\left(\mu'(f)\right)\left(\sigma^{-1}.x\right) \\
&= \Sigma_i R_G\left(p_i\right) g_i \left(\sigma^{-1}.x\right) \\
&= \Sigma_i R_G(p_i) \cdot (\sigma.g_i)(x) \\
&= \Sigma_i R_G(\sigma\dot{}p_i) \cdot (\sigma.g_i)(x) \\
&= \left(R_G \otimes \mathrm{id}\right)\left(\Sigma_i \sigma\dot{}p_i \otimes \sigma.g_i\right)(x) \\
&=
\end{aligned} \tag{15}$$

not done yet pls finish ☐

then show lemmas and hilberts finiteness theorem...

4 Cayley's Ω-Process

We want to express the Reynolds Operator in a conrete 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 $I := \left(\left(\sum_{\sigma\in S_n} \mathrm{sgn}\left(\sigma\right) \prod_{i\in\lceil n\rceil} Z_{i,\sigma(i)}\right) \cdot D - 1\right) = \left(\det\left(Z\right) \cdot D - 1\right)$, where $Z := \left[Z_{i,j}\right]_{i,j\in\lceil n\rceil}$. Then $V\left(I\right) = \{\ (z,d) \mid z \in \mathrm{GL}_n, d = \det\left(z\right)^{-1}\ \}$. Equipped with the componentwise multiplication (GL_n and $K\setminus\{0\}$, respectively), this is a linear algebraic group isomorphic to GL_n. The coordinate ring $K\left[\mathrm{GL}_n\right]$ is isomorphic to $K\left[\{Z_{i,j}\}_{i,j\in\lceil n\rceil}, \det\left(Z\right)^{-1}\right] \subseteq K\left(\{Z_{i,j}\}_{i,j\in\lceil n\rceil}\right)$, and we will write it as such from now on.

Definition 4.1: Cayley's Ω-Process
We call

$$\Omega := \sum_{\sigma\in S_n} \mathrm{sgn}\left(\sigma\right) \prod_{i\in\lceil n\rceil} \frac{\partial}{\partial z_{i,\sigma(i)}} \tag{16}$$

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

$$\left(\det\left(Z\right)^{-1} \cdot \otimes\Omega\right) \circ m^* = m^* \circ \Omega = \left(\Omega \otimes \det\left(Z\right)^{-1} \cdot\right) \circ m^* \tag{17}$$

where I 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 I will make use of this notation).

Proof. Here, we will follow the same convention as described in chapter 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

$Y = [Y_{i,j}]_{i,j\in\lceil n\rceil}$ in the occuring polynomials respectively, and the outputs $m = [m_{i,j}]_{i,j\in\lceil n\rceil}$ are indexed the same as the inputs of the polynomials in $Z_{1,1}, Z_{1,2}, \dots Z_{n,n}$.
Let $f \in K[\mathrm{GL}_n]$. Then $f \circ m \in K\left[\{X_{i,j}\}_{i,j\in\lceil n\rceil}, \det(X)^{-1}, \{Y_{i,j}\}_{i,j\in\lceil n\rceil}, \det(Y)^{-1}\right]$.
For fixed $i, j \in \lceil n\rceil$ we have

$$\begin{aligned}\left(\mathrm{id}\otimes\frac{\partial}{\partial Z_{i,j}}\right)(m^*(f)) &= t\left(\frac{\partial}{\partial Y_{i,j}}(f\circ m)\right) = t\left(\sum_{k,l\in\lceil n\rceil}\left(\left(\frac{\partial}{\partial Z_{k,l}}f\right)\circ m\right)\cdot\frac{\partial}{\partial Y_{i,j}}m_{k,l}\right)\\ &= t\left(\sum_{k=1}^{n}\left(\left(\frac{\partial}{\partial Z_{k,j}}f\right)\circ m\right)\cdot X_{k,i}\right) = \sum_{k=1}^{n}(Z_{k,i}\cdot\otimes\mathrm{id})\left(m^*\left(\frac{\partial}{\partial Z_{k,j}}f\right)\right)\end{aligned} \tag{18}$$

Note the use of t as described in chapter 3 to aid in rephrasing terms. Successively applying this yields

$$\begin{aligned}(\mathrm{id}\otimes\Omega)(m^*(f)) &= \sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)\left(\mathrm{id}\otimes\prod_{i=1}^{n}\frac{\partial}{\partial Z_{i,\sigma(i)}}\right)(m^*(f))\\ &= \sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)\sum_{k\in\lceil n\rceil^n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^*\left(\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)\\ &= \sum_{k\in\lceil n\rceil^n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^*\left(\sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)\\ &= \sum_{k\in S_n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^*\left(\sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)\\ &= \sum_{k\in S_n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)(m^*(\mathrm{sgn}(k)\Omega(f))) = (\det(Z)\cdot\otimes\mathrm{id})(m^*(\Omega(f)))\end{aligned} \tag{19}$$

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 $\det(Z)^p = \Sigma_i a_i m_i\left(\{Z_{k,l}\}_{k,l\in\lceil n\rceil}\right)$, where $a_i \in K$ and m_i are (monic) monomials. Then

$$\Omega^p(\det(Z)^p) = \Sigma_i a_i m_i\left(\left\{\frac{\partial}{\partial Z_{k,l}}\right\}_{k,l\in\lceil n\rceil}\right)\left(\Sigma_j a_j m_j\left(\{Z_{k,l}\}_{k,l\in\lceil n\rceil}\right)\right) \tag{20}$$

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

$$c_{p,n} = \sum_i a_i^2 m_i \left(\left\{ \frac{\partial}{\partial Z_{k,l}} \right\}_{k,l \in \lceil n \rceil} \right) \left(m_i \left(\{Z_{k,l}\}_{k,l \in \lceil n \rceil} \right) \right) \in \mathbb{N}_{>0} \tag{21}$$

□

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 $f = \frac{\tilde{f}}{\det(Z)^p}$:

$$R(f) := \frac{\Omega^p \tilde{f}}{c_{p,n}} \tag{22}$$

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. First, I will introduce a notation: For $f \in K[\mathrm{GL}_n]$ and $\alpha \in \mathrm{GL}_n$, define $\alpha\dot{} f := \left(x \mapsto f\left(x\alpha^{-1}\right) \right)$ (again, I assure the reader that this proof contains the only occurence of this notation). This is *not* an action, but a right action (normal actions should be called “left actions”). 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

$$\begin{aligned} R(\beta.f)(\gamma) = R\left(\frac{\det(\beta)^p \cdot \beta.\tilde{f}}{\det(Z)^p} \right)(\gamma) &= \frac{\det(\beta)^p \cdot \Omega^p \left(\beta.\tilde{f}\right)(\gamma)}{c_{p,n}} \\ &= \frac{1}{c_{p,n}} \cdot \left(\epsilon_{\beta^{-1}} \otimes \epsilon_\gamma \right) \left(\left(\left(\det(Z)^{-p} \cdot \otimes \Omega^p \right) \circ m^* \right) \left(\tilde{f} \right) \right) \\ &= \frac{1}{c_{p,n}} \cdot \left(\epsilon_{\beta^{-1}} \otimes \epsilon_\gamma \right) \left(\left(\left(\Omega^p \otimes \det(Z)^{-p} \cdot \right) \circ m^* \right) \left(\tilde{f} \right) \right) \\ = \frac{\Omega^p \left(\gamma^{-1}\dot{}\tilde{f} \right)\left(\beta^{-1}\right) \cdot \det\left(\gamma^{-1}\right)^p}{c_{p,n}} &= R\left(\frac{\gamma^{-1}\dot{}\tilde{f} \cdot \det\left(\gamma^{-1}\right)^p}{\det(Z)^p} \right)\left(\beta^{-1}\right) \\ &= R\left(\gamma^{-1}\dot{} f\right)\left(\beta^{-1}\right) \end{aligned} \tag{23}$$

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 $\alpha \in \mathrm{GL}_n$

$$\begin{aligned} R(\alpha.f) = R(\alpha.f)(I_n) &= R\left(I_n^{-1}\dot{} f\right)\left(\alpha^{-1}\right) \\ &= R\left(I_n^{-1}\dot{} f\right) = R\left(I_n\dot{} f\right) = R(f) \end{aligned} \tag{24}$$

which shows the GL_n-invariance. Finally, the definition immediately gives us that R restricted to K is the identity. As mentioned in 3.1.1, 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 $K[\mathrm{GL}_n] = K\left[\{Z_{k,l}\}_{k,l\in\lceil n\rceil}, \det(Z)^{-1}\right]$, view $K[\mathrm{SL}_n] = K[\mathrm{GL}_n]/I$ where $I = (\det(Z) - 1)$. Now, for $p \in \mathbb{N}$ and $\tilde{f} \in K\left[\{Z_{i,j}\}_{k,l\in\lceil n\rceil}\right]_{pn}$ define for $f = \frac{\tilde{f}}{\det(Z)^p} + I$:

$$R(f) := R_{\mathrm{GL}_n}\left(\frac{\tilde{f}}{\det(Z)^p}\right) + I = \frac{\Omega^p \tilde{f}}{c_{p,n}} + I \tag{25}$$

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

Proof. First, we will show $K[\mathrm{GL}_n]^{\mathrm{SL}_n} = K\left[\det(Z), \det(Z)^{-1}\right]$ (action by left multiplication). Let $g \in K[\mathrm{GL}_n]^{\mathrm{SL}_n}$, and let $\alpha \in \mathrm{GL}_n$. Now for $x \in K \setminus \{0\}$, 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 $M(\det(\alpha))^{-1}\alpha \in \mathrm{SL}_n$. Define $h := (\beta \mapsto g(M(\det(\beta)))) \in K\left[\det(Z), \det(Z)^{-1}\right]$. Now

$$\begin{aligned} g(\alpha) = \left(M(\det(\alpha))^{-1}\alpha\right).g(\alpha) &= g\left(M(\det(\alpha))\,\alpha^{-1}\alpha\right) \\ &= g(M(\det(\alpha))) = h(\alpha) \end{aligned} \tag{26}$$

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

$$\hat{R}(f) := \det(Z)^{r-p} \cdot \frac{\Omega^r \tilde{f}}{c_{r,n}} = \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\tilde{f}}{\det(Z)^r}\right) \tag{27}$$

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 (and $r - p = (r+q) - (p+q)$ for $q \in \mathbb{N}$). This map is the identity on $K[\mathrm{GL}_n]^{\mathrm{SL}_n}$: If $f \in K\left[\{Z_{k,l\in\lceil n\rceil}\}\right]_{rn}$ and $f \in K[\mathrm{GL}_n]^{\mathrm{SL}_n}$, then $\tilde{f} = \lambda \det(Z)^r$ with $\lambda \in K$. Therefore we can say w.l.o.g. either $p = 0$ or $r = 0$. Then it is quite clear that then f gets mapped to f. Finally, the SL_n-invariance also follows from the last theorem: Let $\alpha \in \mathrm{SL}_n$. Then

$$\begin{aligned}\hat{R}(\alpha.f) = \hat{R}\left(\frac{\det(\alpha)^p \cdot \alpha.\tilde{f}}{\det(Z)^p}\right) &= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\det(\alpha)^p \cdot \alpha.\tilde{f}}{\det(Z)^r}\right) \\ &= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\det(\alpha)^r \cdot \alpha.\tilde{f}}{\det(Z)^r}\right) \\ &= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\alpha.\left(\frac{\tilde{f}}{\det(Z)^r}\right)\right) \\ &= \det(Z)^{r-p} \cdot R_{\mathrm{GL}_n}\left(\frac{\tilde{f}}{\det(Z)^r}\right) = \hat{R}(f)\end{aligned} \tag{28}$$

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 Some First Examples

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:

$$\begin{aligned}\mu\colon \quad \mathrm{SL}_2 \times V &\longrightarrow V \\ (S, A) &\longmapsto SAS^T\end{aligned} \tag{29}$$

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

$$\begin{aligned} S &= \begin{bmatrix} s_{1,1} & s_{1,2} \\ s_{2,1} & s_{2,2}\end{bmatrix} \qquad A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2}\end{bmatrix} \\ S^{-1} &= \begin{bmatrix} s_{2,2} & -s_{1,2} \\ -s_{2,1} & s_{1,1}\end{bmatrix}\end{aligned} \tag{30}$$

We then have

$$\begin{aligned} S^{-1}.A &= S^{-1}A\left(S^{-1}\right)^T \\ &= \begin{bmatrix} a_{1,1}s_{2,2}^2 - 2a_{1,2}s_{1,2}s_{2,2} + a_{2,2}s_{1,2}^2 & -a_{1,1}s_{2,1}s_{2,2} + a_{1,2}s_{1,1}s_{2,2} + a_{1,2}s_{1,2}s_{2,1} - a_{2,2}s_{1,1} \\ -a_{1,1}s_{2,1}s_{2,2} + a_{1,2}s_{1,1}s_{2,2} + a_{1,2}s_{1,2}s_{2,1} - a_{2,2}s_{1,1}s_{1,2} & a_{1,1}s_{2,1}^2 - 2a_{1,2}s_{1,1}s_{2,1} + a_{2,2}s_{1,1}^2 \end{bmatrix}\end{aligned} \tag{31}$$

Notice that we also have

$$\begin{aligned}\det\left(\frac{\partial}{\partial S}\right)^n &= \left(\frac{\partial}{\partial S_{1,1}}\frac{\partial}{\partial S_{2,2}} - \frac{\partial}{\partial S_{1,2}}\frac{\partial}{\partial S_{2,1}}\right)^n \\ &= \sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{\partial}{\partial S_{1,1}}^{n-k}\frac{\partial}{\partial S_{1,2}}^{k}\frac{\partial}{\partial S_{2,1}}^{k}\frac{\partial}{\partial S_{2,2}}^{n-k}\end{aligned} \tag{32}$$

Now consider a monomial $f = A_{1,1}^{r_{1,1}}A_{1,2}^{r_{1,2}}A_{2,2}^{r_{2,2}} \in K[V]$. We then have

$$\begin{aligned}&\mu^*(f) \\ &= \sum_{|t_{1,1}|=r_{1,1}}\sum_{|t_{1,2}|=r_{1,2}}\sum_{|t_{2,2}|=r_{2,2}}\binom{r_{1,1}}{t_{1,1}}\binom{r_{1,2}}{t_{1,2}}\binom{r_{2,2}}{t_{2,2}} \\ &= \sum s_{1,1}^{t_{1,2}^{(2)}+t_{1,2}^{(4)}+t_{2,2}^{(2)}+2t_{2,2}^{(3)}}\end{aligned} \tag{33}$$

Example 5.2
Consider the cross ratio. We can view its domain as the affine variety

$$\begin{aligned}X &:= \{\,(a,b,c,d) \in (\mathbb{K}^2)^4 \mid (b_1c_2 - b_2c_1)(d_1a_2 - d_2a_1) \neq 0\,\} \\ &= \{\,(a,b,c,d) \in (\mathbb{K}^2)^4 \mid \det(b,c)\det(d,a) \neq 0\,\}\end{aligned} \tag{34}$$

as described in [**yaboi**]. Now Consider the action of GL_2 on X via pointwise application. The *cross ratio* $\mathrm{cr} \in K[X]$ defined as follows

$$\begin{aligned}\mathrm{cr}\colon \quad & X \longrightarrow K \\ &(a,b,c,d) \longmapsto \frac{\det(a,b)\det(c,d)}{\det(b,c)\det(d,a)}\end{aligned} \tag{35}$$

is an invariant under this action, as is easily seen. Exactly this GL_2-invariance guarantees a coordinate-independent definition of the cross ratio in the projective space.

Example 5.3
(K needs to be algebraically closed for Zariski-denseness of diagonizable matrices...)
Consider GL_n viewed as the group of all change-of-coordinates transformations for endomorphisms on K^n, that is the rational representation

$$\begin{aligned}\mu\colon \quad \mathrm{GL}_n \times K^{n.n} &\longrightarrow K^{n,n} \\ (\sigma, A) &\longmapsto \sigma A \sigma^{-1}\end{aligned} \tag{36}$$

What are its 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

$$\det(tI_n - A) = \sum_{i=0}^{n} p_{n,i}(A)t^i \tag{37}$$

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 $D := \{ \delta \in K^{n,n} \mid \delta \text{ diagonalizable} \} \subseteq K^{n,n}$. Since V is Zariski-dense in $K^{n,n}$, we have $K[K^{n,n}] \simeq K[K^{n,n}]|_D$ via $p \mapsto p|_D$. 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: $\pi\colon K^{n,n} \longrightarrow K^n, [A_{i,j}]_{i,j\in[n]} \longmapsto (X_{i,i})_{i\in[n]}$. Consider $\tilde{p} = p\left([\delta_{i,j}Z_{i,j}]_{i,j\in[n]}\right) \in K[K^n]$. $\tilde{p}$ is S_n-invariant: If $M_\tau \in \mathrm{GL}_n$ is the matrix corresponding to $\tau \in S_n$, then for all $\tau \in S_n$ and for all $X \in K^n$ we have

$$\begin{aligned}\tau.\tilde{p}(X) \quad &= \tilde{p}(\tau^{-1}.X)\\ &= \tilde{p}(\pi(\mathrm{diag}(\tau^{-1}.X)))\\ &= p(\mathrm{diag}(\tau^{-1}.X)\\ &= M_\tau.p(\mathrm{diag}(X))\\ &= p(\mathrm{diag}(X)) \qquad\qquad = \tilde{p}(X)\end{aligned} \tag{38}$$

From the fundamental theorem of symmetric polynomials we can follow that $\tilde{p} \in \mathrm{span}\{ e_n^i \mid i \in [n] \}$, say $\tilde{p} = \Sigma_{i=1}^n \lambda_i e_{n,i}$, where $e_{n,i}$ 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 $s(A) := \sigma_A.A$ get $p = \tilde{p} \circ \pi \circ s$, therefore $p = \Sigma_{i=1}^n \lambda_i e_{n,i} \circ \pi \circ s$. 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

$$\begin{aligned}\sum_{i=1}^{n} (e_{n,i} \circ \pi \circ s)(A)t^i \quad &= \det(t - \sigma_A.A)\\ &= \det(t - A) \qquad = \sum_{i=1}^{n} p_{n,i}(A)t^i\end{aligned} \tag{39}$$

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. . .).

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.