

Cayley's Ω -Process And The Reynolds Operator

Bert Lorke

October 10, 2017

1 Introduction

In a seminar, I discussed Hilbert's finiteness theorem for the group GL_n . The proof I presented was a version of Hilbert's non-constructive proof, which, apparently (it is not known how true this is), was responsible for Gordan's famous quote "Das ist Theologie und nicht Mathematik". The central idea of the proof is the existence of the Reynolds Operator. After the dirty work is done and some useful properties are shown, the proof of the theorem is very straightforward. In fact, if we are able to construct finite homogenous generators of the nullcone, all that is left to do is apply the Reynolds Operator to each generator, and the resulting polynomials will be generators of the invariant ring. But even this step is easier said than done. In my presentation at the seminar, I constructed a Haar measure, which gives me a unitary GL_n -invariant inner product, which allows us to define the Reynolds Operator. If one wants to explicitly calculate the image under the Reynolds Operator of a concrete polynomial, following these steps is not really feasible. For the group GL_n , there is an operator called *Cayley's Ω -Process* which allows us to compute the Reynold's Operator. This is the main focus of my work.

2 Invariant Theory and the Reynolds Operator

In this section, we will explain and discuss some terminology and underlying theorems. This is very general, and since we really only focus on $\mathbb{C}[\mathrm{GL}_n]$, we can formulate a lot of this stuff more specifically and without the need to introduce some of these notions. Still though, I feel that it is beneficial to talk about the general framework to aid some readers to categorize this specific case.

This loosely follows [DK15, p.31].

Definition 2.1: Regular Action

Let G be a linear algebraic group, X an affine variety. We call an action $G \times X \rightarrow X$ a **regular action**, iff it is a morphism of affine varieties. We say G **acts regularly on X** .

Definition 2.2: Rational Representation

Let G be a linear algebraic group. A representation V of G is called a **rational representation**, iff its corresponding action $G \times V \rightarrow V$ is a regular action.

Remark 2.2.1

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, $a_{i,j} \in K[G]$.

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 2.3: Invariants

Let G act on X regularly.

$$X^G := \{ x \in X \mid \forall g \in G : g.x = x \} \quad (1)$$

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:

$$(g, f) \longmapsto g \cdot f := (x \mapsto f(\sigma^{-1}.x)) \quad (2)$$

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

$$K[X]^G := \{ f \in K[X] \mid \forall g \in G : g \cdot f = f \} \quad (3)$$

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.

Definition 2.4: 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 2.4.1

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

Definition 2.5: 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 $R_G : K[G] \longrightarrow K[G]^G = K$.

Remark 2.5.1

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.

3 Pre-work

In this section, we will define an algebra structure on $K[G]^*$ and construct an action $K[G]^* \times V \rightarrow V$. We closely follow [DK15, p. 299-302].

We denote by m the group multiplication of the group G . We want to view the pullback of m as a map $m^* : K[G] \rightarrow K[G] \otimes K[G]$, 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 $K[G] \rightarrow K[G \times G]$, where $f \mapsto f \circ m$. If we want to give the variables names, we can equivalently say it is a map $K[Z]|_G \rightarrow K[X, Y]|_{G \times G}$, where $Z = \{Z_1, \dots, Z_k\}$, X and Y analogously (here, m canonically takes its “left” input via X and its “right” input via Y). Define

$$t : K[X, Y]|_{G \times G} \rightarrow K[Z]|_G \otimes K[Z]|_G$$

$$\sum_i \lambda_i \prod_j Z_j^{d_{i,j}} \prod_j Z_j^{e_{i,j}} \mapsto \sum_i \lambda_i \prod_j Z_j^{d_{i,j}} \otimes \prod_j Z_j^{e_{i,j}} \quad (4)$$

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

One might ask, why we want to look at these objects $m^*(f)$ instead of $\hat{m}(f)$. Really, these objects are hardly different, but it helps to formalize performing operations only on “left part” or the “right part”, as we will see right now.

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

$$\alpha * \beta := (\alpha \otimes \beta) \circ m^* \quad (5)$$

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

$$(\alpha * \beta)(f) = \sum_i \alpha(g_i) \otimes \beta(h_i) = \sum_i \alpha(g_i) \beta(h_i) \quad (6)$$

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

Example: TODO

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

Proof: First, a small observation:

$$(m^* \otimes \text{id}) \circ m^* = (\text{id} \otimes m^*) \circ m^* \quad (7)$$

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

$$\begin{aligned} (\delta * \gamma) * \varphi &= (((\delta \otimes \gamma) \circ m^*) \otimes \varphi) \circ m^* = (\delta \otimes \gamma \otimes \varphi) \circ (m^* \otimes \text{id}) \circ m^* \\ &= (\delta \otimes \gamma \otimes \varphi) \circ (\text{id} \otimes m^*) \circ m^* = (\delta \otimes ((\gamma \otimes \varphi) \circ m^*)) \circ m^* = \delta * (\gamma * \varphi) \end{aligned} \quad (8)$$

showing the associativity. The second equation is easily checked (rewrite as described in the beginning of chapter 3). Also, it should be clear that ϵ is the neutral element. This concludes that $K[G]^*$ is an associative algebra, *which was to show*.

Definition 3.1: 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 $\mu^* : V \longrightarrow K[G] \otimes V$ such that $\mu(\sigma, v) = ((\epsilon_\sigma \otimes \text{id}) \circ \mu^*)(v)$.

Claim: If V is finite dimensional, the notions of the definitions coincide.

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

$$\begin{aligned} \mu(\sigma, v) &= \mu(\sigma, \sum_{j=1}^N \lambda_j v_j) \\ &= \sum_{j=1}^N \lambda_j \sum_{i=1}^N p_{i,j}(\sigma) \cdot v_i \\ &= \sum_{j=1}^N \lambda_j ((\epsilon_\sigma \otimes \text{id}) \circ \mu^*)(v_j) = ((\epsilon_\sigma \otimes \text{id}) \circ \mu^*)(v) \end{aligned} \tag{9}$$

which was to show.

Now, with this μ^* , we can extend the operation from $\{\epsilon_\sigma \mid \sigma \in G\}$ to $K[G]^*$, defining an action $K[G]^* \times V \longrightarrow V$:

$$\delta \cdot v := ((\delta \otimes \text{id}) \circ \mu^*)(v) \tag{10}$$

4 Invariant Theory, Hilbert's Finiteness Theorem And The Reynolds Operator

Definition 4.1: Regular Action

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 .

Definition 4.2: 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.

Remark 4.2.1

A rational representation $G \longrightarrow \text{GL}(V)$ is of the following form:

If $a_{i,j} : G \longrightarrow K$ is the function of the (i, j) -entry, $a_{i,j} \in K[G]$.

In fact, it is equivalent to define a representation as rational, iff its map $G \longrightarrow \text{GL}(V)$ is a map of affine varieties.

Definition 4.3: Invariants

Let G act on X regularly.

$$X^G := \{x \in X \mid \forall g \in G : g.x = x\} \tag{11}$$

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

$$(g, f) \mapsto g \cdot f := (x \mapsto f(\sigma^{-1}.x)) \quad (12)$$

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

$$K[X]^G := \{ f \in K[X] \mid \forall g \in G : g \cdot f = f \} \quad (13)$$

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.

Definition 4.4: Reynolds Operator

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

Remark 4.4.1

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

Definition 4.5: linearly reductive

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

Remark 4.5.1

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.

5 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 $K[\{Z_{i,j}\}_{i,j \in [n]}, D]$. Now define $I := \left(\left(\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i \in [n]} Z_{i,\sigma(i)} \right) \cdot D - 1 \right) = (\det(Z) \cdot D - 1)$, where $Z := [Z_{i,j}]_{i,j \in [n]}$. Then $V(I) = \{ (z, d) \mid z \in \mathrm{GL}_n, d = \det(z)^{-1} \}$. 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 $K[\mathrm{GL}_n]$ is isomorphic to $K[\{Z_{i,j}\}_{i,j \in [n]}, \det(Z)^{-1}] \subseteq K(\{Z_{i,j}\}_{i,j \in [n]})$, and we will write it as such from now on.

Definition 5.1: Cayley's Ω -Process

We call

$$\Omega := \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i \in [n]} \frac{\partial}{\partial z_{i, \sigma(i)}} \quad (14)$$

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

Lemma 5.2

$$\left(\det(Z)^{-1} \cdot \otimes \Omega\right) \circ m^* = m^* \circ \Omega = \left(\Omega \otimes \det(Z)^{-1} \cdot\right) \circ m^* \quad (15)$$

where I write “ $p \cdot$ ” for the operation *multiply with p* for a polynomial $p \in K[\text{GL}_n]$ (but don't worry, this is the only time I will make use of this notation).

a

Proof. Here, we will follow the same convention as described in chapter 3: The “left” and “right” inputs of m will be represented by $X = [X_{i,j}]_{i,j \in [n]}$ and $Y = [Y_{i,j}]_{i,j \in [n]}$ in the occurring polynomials respectively, and the outputs $m = [m_{i,j}]_{i,j \in [n]}$ are indexed the same as the inputs of the polynomials in $Z_{1,1}, Z_{1,2}, \dots, Z_{n,n}$.

Let $f \in K[\text{GL}_n]$. Then $f \circ m \in K[\{X_{i,j}\}_{i,j \in [n]}, \det(X)^{-1}, \{Y_{i,j}\}_{i,j \in [n]}, \det(Y)^{-1}]$.

For fixed $i, j \in [n]$ we have

$$\begin{aligned} \left(\text{id} \otimes \frac{\partial}{\partial Z_{i,j}}\right) (m^*(f)) &= t \left(\frac{\partial}{\partial Y_{i,j}} (f \circ m) \right) = t \left(\sum_{k,l \in [n]} \left(\left(\frac{\partial}{\partial Z_{k,l}} f \right) \circ m \right) \cdot \frac{\partial}{\partial Y_{i,j}} m_{k,l} \right) \\ &= t \left(\sum_{k=1}^n \left(\left(\frac{\partial}{\partial Z_{k,j}} f \right) \circ m \right) \cdot X_{k,i} \right) = \sum_{k=1}^n (Z_{k,i} \cdot \text{id}) \left(m^* \left(\frac{\partial}{\partial Z_{k,j}} f \right) \right) \end{aligned} \quad (16)$$

Note the use of t as described in chapter 3 to aid in rephrasing terms. Succes-

sively applying this yields

$$\begin{aligned}
(\text{id} \otimes \Omega)(m^*(f)) &= \sum_{\sigma \in S_n} \text{sgn}(\sigma) \left(\text{id} \otimes \prod_{i=1}^n \frac{\partial}{\partial Z_{i,\sigma(i)}} \right) (m^*(f)) \\
&= \sum_{\sigma \in S_n} \text{sgn}(\sigma) \sum_{k \in [n]^n} \left(\prod_{i=1}^n Z_{k(i),i} \cdot \otimes \text{id} \right) \left(m^* \left(\prod_{j=1}^n \frac{\partial}{\partial Z_{k(j),\sigma(j)}} f \right) \right) \\
&= \sum_{k \in [n]^n} \left(\prod_{i=1}^n Z_{k(i),i} \cdot \otimes \text{id} \right) \left(m^* \left(\sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{j=1}^n \frac{\partial}{\partial Z_{k(j),\sigma(j)}} f \right) \right) \\
&= \sum_{k \in S_n} \left(\prod_{i=1}^n Z_{k(i),i} \cdot \otimes \text{id} \right) \left(m^* \left(\sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{j=1}^n \frac{\partial}{\partial Z_{k(j),\sigma(j)}} f \right) \right) \\
&= \sum_{k \in S_n} \left(\prod_{i=1}^n Z_{k(i),i} \cdot \otimes \text{id} \right) (m^*(\text{sgn}(k)\Omega(f))) = (\det(Z) \cdot \otimes \text{id})(m^*(\Omega(f)))
\end{aligned} \tag{17}$$

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

Lemma 5.3

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 $\det(Z)^p = \sum_i a_i m_i(\{Z_{k,l}\}_{k,l \in [n]})$, where $a_i \in K$ and m_i are (monic) monomials. Then

$$\Omega^p(\det(Z)^p) = \sum_i a_i m_i \left(\left\{ \frac{\partial}{\partial Z_{k,l}} \right\}_{k,l \in [n]} \right) \left(\sum_j a_j m_j(\{Z_{k,l}\}_{k,l \in [n]}) \right) \tag{18}$$

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

$$c_{p,n} = \sum_i a_i^2 m_i \left(\left\{ \frac{\partial}{\partial Z_{k,l}} \right\}_{k,l \in [n]} \right) (m_i(\{Z_{k,l}\}_{k,l \in [n]})) \in \mathbb{N}_{>0} \tag{19}$$

in particular $c_{p,n} \neq 0$. \square

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

Theorem 5.4

For $p \in \mathbb{N}$ and $\tilde{f} \in K \left[\{Z_{i,j}\}_{i,j \in [n]} \right]_{pn}$, define for $f = \frac{\tilde{f}}{\det(Z)^p}$:

$$R(f) := \frac{\Omega^p \tilde{f}}{c_{p,n}} \tag{20}$$

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

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 $\alpha \cdot f := (x \mapsto f(x\alpha^{-1}))$. 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

$$\begin{aligned}
R(\beta \cdot f)(\gamma) &= R\left(\frac{\det(\beta)^p \cdot \beta \cdot \tilde{f}}{\det(Z)^p}\right)(\gamma) = \frac{\det(\beta)^p \cdot \Omega^p(\beta \cdot \tilde{f})(\gamma)}{c_{p,n}} \\
&= \frac{1}{c_{p,n}} \cdot (\epsilon_{\beta^{-1}} \otimes \epsilon_\gamma) \left(((\det(Z)^{-p} \cdot \otimes \Omega^p) \circ m^*) (\tilde{f}) \right) \\
&= \frac{1}{c_{p,n}} \cdot (\epsilon_{\beta^{-1}} \otimes \epsilon_\gamma) \left(((\Omega^p \otimes \det(Z)^{-p} \cdot) \circ m^*) (\tilde{f}) \right) \quad (21) \\
&= \frac{\Omega^p(\gamma^{-1} \cdot \tilde{f})(\beta^{-1}) \cdot \det(\gamma^{-1})^p}{c_{p,n}} = R\left(\frac{\gamma^{-1} \cdot \tilde{f} \cdot \det(\gamma^{-1})^p}{\det(Z)^p}\right)(\beta^{-1}) \\
&= R(\gamma^{-1} \cdot f)(\beta^{-1})
\end{aligned}$$

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

$$\begin{aligned}
R(\alpha \cdot f) &= R(\alpha \cdot f)(I_n) = R(I_n^{-1} \cdot f)(\alpha^{-1}) \\
&= R(I_n^{-1} \cdot f) = R(I_n \cdot f) = R(f)
\end{aligned} \quad (22)$$

which shows the GL_n -invariance. Finally, the definition immediately gives us that R restricted to K is the identity. As mentioned in 4.4.1, the uniqueness of the Reynolds Operator implies $R = R_{\mathrm{GL}_n}$. \square

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

Corollary 5.4.1

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

$$R(f) := \frac{\Omega^p \tilde{f}}{c_{p,n}} + I \quad (23)$$

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

Proof. First, we will show $K[\mathrm{GL}_n]^{\mathrm{SL}_n} = K[\det(Z), \det(Z)^{-1}]$. Let $g \in K[\mathrm{GL}_n]^{\mathrm{SL}_n}$, and let $\alpha \in \mathrm{GL}_n$. Note that $\frac{1}{n \det(\alpha)} \alpha \in \mathrm{SL}_n$. Define $h := \beta \mapsto g(n \det(\beta) I_n) \in K[\det(Z), \det(Z)^{-1}]$. Now

$$\begin{aligned} g(\alpha) &= \left(\frac{1}{n \det(\alpha)} \alpha \right) \cdot g(\alpha) = g(n \det(\alpha) \alpha^{-1} \alpha) \\ &= g(n \det(\alpha) I_n) = h(\alpha) \end{aligned} \tag{24}$$

Therefore $g = h \in K[\det(Z), \det(Z)^{-1}]$. Conversely it is easy to see that $K[\det(Z), \det(Z)^{-1}] \subseteq K[\mathrm{GL}_n]^{\mathrm{SL}_n}$ \square

6 Test

This part of my master file is for testing my environment.

Theorem 6.1

Hero

Theorem 6.2

haroooo

Remark 6.2.1

whaaaaa

Remark 6.2.2

okaydoakes!

Definition 6.3

shiawia

Theorem 6.4

yesss

Corollary 6.4.1

okok whatevs mcshmeves

Remark 6.4.1.1

you got dis?

References

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