Cayley's Ω-Process And The Reynolds Operator

Bert Lorke

September 26, 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 contruct finite homogenious 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 then 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 $G \times X \longrightarrow X$ 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 $G \times V \longrightarrow V$ 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.

$$X^G := \{\, x \in X \mid \forall g \in G : g.x = x \,\} \tag{1}$$

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:

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

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

$$K[X]^G := \{\, f \in K[X] \mid \forall g \in G : g \cdot f = f \,\} \tag{3}$$

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) $\Longrightarrow$ (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 $K[G]^* \times V \longrightarrow V$. 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 $m^* : K[G] \longrightarrow K[G] \otimes K[G]$, 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

$$t : K[X,Y]|_{G \times G} \longrightarrow K[Z]|_G \otimes K[Z]|_G$$
$$\sum_i \lambda_i \prod_j Z_j^{d_{i,j}} \prod_j Z_j^{e_{i,j}} \mapsto \sum_i \lambda_i \prod_j Z_j^{d_{i,j}} \otimes \prod_j Z_j^{e_{i,j}} \tag{4}$$

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

$$\alpha * \beta := (\alpha \otimes \beta) \circ m^* \tag{5}$$

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

$$(\alpha * \beta)(f) = \Sigma_i \alpha(g_i) \otimes \beta(h_i) = \Sigma_i \alpha(g_i) \beta(h_i) \tag{6}$$

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:

$$(m^* \otimes \mathrm{id}) \circ m^* = (\mathrm{id} \otimes m^*) \circ m^* \tag{7}$$

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

$$(\delta * \gamma) * \varphi = (((\delta \otimes \gamma) \circ m^*) \otimes \varphi) \circ m^* = (\delta \otimes \gamma \otimes \varphi) \circ (m^* \otimes \mathrm{id}) \circ m^*$$
$$= (\delta \otimes \gamma \otimes \varphi) \circ (\mathrm{id} \otimes m^*) \circ m^* = (\delta \otimes ((\gamma \otimes \varphi) \circ m^*)) \circ m^* = \delta * (\gamma * \varphi) \tag{8}$$

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 **rational** iff there exists a linear map $\mu^* : V \longrightarrow K[G] \otimes V$ such that $\mu(\sigma, v) = ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu^*)(v)$.

In our given situation, we have a rational representation $\mu : G \times V \longrightarrow V$.
Claim: There is a linear map $\mu^* : V \longrightarrow K[G] \otimes V$ with $\mu(\sigma, v) = ((\epsilon_\sigma \otimes \mathrm{id}) \circ \mu^*)(v)$.
Proof: Let $\{v_1, \ldots, v_N\}$ 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:

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

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 $K[G]^* \times V \longrightarrow V$:

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

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 $G \longrightarrow \mathrm{GL}(V)$ 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 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 $G \times K[X] \longrightarrow K[X]$, where $K[X]$ is the coordinate ring, as follows:

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

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

$$K[X]^G := \{\, f \in K[X] \mid \forall g \in G : g \cdot f = f \,\} \tag{13}$$

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 $K[V] \longrightarrow K[V]^G$ 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 $G \times G \longrightarrow G$ by left multiplication $R_G : K[G] \longrightarrow K[G]^G = K$.

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 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 $I := \left(\left(\sum_{\sigma \in S_n} \mathrm{sgn}\,(\sigma) \prod_{i \in \lceil n \rceil} Z_{i,\sigma(i)}\right) \cdot D - 1\right) = (\det(Z) \cdot D - 1)$, where $Z := [Z_{i,j}]_{i,j \in \lceil n \rceil}$. Then $V(I) = \{\,(z, d) \mid z \in \mathrm{GL}_n, d = \det(z)^{-1}\,\}$. Equipped with the componentwise multiplication (GL_n and $K \setminus \{0\}$, respectively), this is a linear algebraic group isomorphic to GL_n. The coordinate ring $K[\mathrm{GL}_n]$ 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 5.1: Cayley's Ω-Process
We call
$$\Omega := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i \in \lceil n \rceil} \frac{\partial}{\partial z_{i,\sigma(i)}} \tag{14}$$

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

Lemma 5.2
$$\left(\det(Z)^{-1} \cdot \otimes \Omega\right) \circ m^* = m^* \circ \Omega = \left(\Omega \otimes \det(Z)^{-1} \cdot\right) \circ m^* \tag{15}$$

where I write "p·" for the operation *multiply with p* for a polynomial $p \in K[\operatorname{GL}_n]$ (but don't 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 $X = [X_{i,j}]_{i,j \in \lceil n \rceil}$ 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 $Z_{1,1}, Z_{1,2}, \ldots Z_{n,n}$.
Let $f \in K[\operatorname{GL}_n]$. 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

$$\left(\operatorname{id} \otimes \frac{\partial}{\partial Z_{i,j}}\right)(m^*(f)) = t\left(\frac{\partial}{\partial Y_{i,j}}(f \circ m)\right) = t\left(\sum_{k,l \in \lceil n \rceil}\left(\left(\frac{\partial}{\partial Z_{k,l}}f\right) \circ m\right) \cdot \frac{\partial}{\partial Y_{i,j}}m_{k,l}\right)$$

$$= t\left(\sum_{k=1}^{n}\left(\left(\frac{\partial}{\partial Z_{k,j}}f\right) \circ m\right) \cdot X_{k,i}\right) = \sum_{k=1}^{n}(Z_{k,i} \cdot \otimes \operatorname{id})\left(m^*\left(\frac{\partial}{\partial Z_{k,j}}f\right)\right)$$

$$\tag{16}$$

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

sively applying this yields

$$(\mathrm{id}\otimes\Omega)\,(m^*\,(f)) = \sum_{\sigma\in S_n}\mathrm{sgn}\,(\sigma)\left(\mathrm{id}\otimes\prod_{i=1}^{n}\frac{\partial}{\partial Z_{i,\sigma(i)}}\right)(m^*\,(f))$$

$$=\sum_{\sigma\in S_n}\mathrm{sgn}\,(\sigma)\sum_{k\in\lceil n\rceil^n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^*\left(\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)$$

$$=\sum_{k\in\lceil n\rceil^n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^*\left(\sum_{\sigma\in S_n}\mathrm{sgn}\,(\sigma)\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)$$

$$=\sum_{k\in S_n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)\left(m^*\left(\sum_{\sigma\in S_n}\mathrm{sgn}\,(\sigma)\prod_{j=1}^{n}\frac{\partial}{\partial Z_{k(j),\sigma(j)}}f\right)\right)$$

$$=\sum_{k\in S_n}\left(\prod_{i=1}^{n}Z_{k(i),i}\cdot\otimes\mathrm{id}\right)(m^*\,(\mathrm{sgn}(k)\Omega(f))) = (\det(Z)\cdot\otimes\mathrm{id})\,(m^*\,(\Omega(f)))$$

$$(17)$$

which immediately shows the first equality. The second equality is proven analogously. $\square$

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.