

Splitting the difference: Computations of the Reynolds operator in classical invariant theory

Aryaman Maithani 

Department of Mathematics, University of Utah, Salt Lake City, Utah, USA

Correspondence

Aryaman Maithani, Department of Mathematics, University of Utah, 155 South 1400 East, Salt Lake City, UT 84112, USA.

Email: maithani@math.utah.edu

Funding information

NSF, Grant/Award Numbers: DMS 2101671, DMS 2349623

[Correction added on 15 October, 2025 after first online publication: copyright line was updated.]

Abstract

If G is a linearly reductive group acting rationally on a polynomial ring S , then the inclusion $S^G \hookrightarrow S$ possesses a unique G -equivariant splitting, called the Reynolds operator. We describe algorithms for computing the Reynolds operator for the *classical actions* as in Weyl's book. The groups are the general linear group, the special linear group, the orthogonal group, and the symplectic group, with their classical representations: direct sums of copies of the standard representation and copies of the dual representation.

MSC 2020

13A50 (Primary) 13P99, 14L24, 14L35 (Secondary)

Contents

| | |
|--|----|
| 1. INTRODUCTION | 2 |
| 2. NOTATIONS AND DEFINITIONS. | 3 |
| 3. THE CLASSICAL GROUP ACTIONS | 4 |
| 4. LINEARLY REDUCTIVE GROUPS | 5 |
| 5. THE REYNOLDS OPERATOR FOR A LIE GROUP | 7 |
| 6. THE REYNOLDS OPERATOR FOR THE CLASSICAL ACTIONS | 9 |
| 7. EXPLICIT FORMULAE | 13 |
| 8. COMPARISON WITH POSITIVE CHARACTERISTIC | 17 |
| APPENDIX A: PROOF OF THE DENSITY THEOREM. | 18 |
| APPENDIX B: MULTINOMIAL COEFFICIENT AND INTEGRATION IDENTITIES | 20 |
| ACKNOWLEDGEMENTS. | 23 |
| REFERENCES. | 23 |

1 | INTRODUCTION

Consider a group G acting on a ring S by ring automorphisms. The [ring of invariants](#) for this group action is defined as

$$S^G := \{s \in S : g(s) = s \text{ for all } g \in G\},$$

that is, S^G is the subring of elements that are fixed by each group element. We have the inclusion of rings

$$S^G \hookrightarrow S. \quad (1.1)$$

The above is also then an inclusion of S^G -modules. A natural question to ask is whether (1.1) splits in the category of S^G -modules — in which case S^G is a direct summand of S . A positive answer to this question often implies good properties about the subring; for example, a direct summand of a noetherian ring is again noetherian. A deeper result is the Hochster–Roberts theorem [16], which states that a direct summand of a polynomial ring is Cohen–Macaulay. The inclusion (1.1) does not always split; a simple example is the alternating group A_3 acting on $\mathbb{F}_3[x, y, z]$ by permuting the variables, see Example 4.4. A more dramatic example was given by Nagarajan [22], where a group of order two acts on a regular ring for which the ring of invariants is not noetherian. For finite groups, a simple condition that ensures the existence of a splitting is having order invertible in S ; the inclusion (1.1) then splits with an S^G -linear splitting given by

$$s \mapsto \frac{1}{|G|} \sum_{g \in G} g(s).$$

The above is the *Reynolds operator* and has the additional property of being *G-equivariant* (Definition 2.1).

In this paper, our groups of interest are certain linear algebraic groups over a field k , that is, Zariski-closed subgroups of $\mathrm{GL}_n(k)$. If such a group G acts (rationally) on a k -vector space V , then we get a (rational) degree-preserving k -algebra action of G on the polynomial ring $S := \mathrm{Sym}(V)$. Hilbert’s fourteenth problem asked if S^G is always a finitely generated k -algebra — a question answered in the negative by Nagata [23] by giving an example where S^G is not noetherian. For linear algebraic groups, the analogue to having invertible order is to be *linearly reductive*. These groups admit a similar Reynolds operator, see Theorem 4.2; in particular, the inclusion (1.1) splits G -equivariantly and S^G -linearly.

We focus on the following titular *classical groups* of Weyl’s book [32]: the general linear group $\mathrm{GL}_n(k)$, the special linear group $\mathrm{SL}_n(k)$, the orthogonal group $\mathrm{O}_n(k)$, and the symplectic group $\mathrm{Sp}_{2n}(k)$. As in the book, we look at their classical actions, corresponding to the direct sum of copies of the standard representation and possibly copies of the dual representation. We record the rings of invariants for some of these actions in Theorem 3.1. This includes infinite fields of positive characteristic as in [2, 13]. There is, however, a stark difference between characteristics zero and positive: if k is a field of characteristic zero, then the groups listed above are all linearly reductive. This is typically not the case in positive characteristic wherein these groups admit representations for which the ring of invariants is not Cohen–Macaulay [18]. Moreover — while the classical rings of invariants continue to be Cohen–Macaulay even in positive characteristic — the inclusion (1.1)

is rarely split [15]. This has the interesting consequence that given any splitting over \mathbb{Q} , every prime must appear in the denominator of the image of any basis; see Remark 8.3 for a precise statement.

For the most part, we consider these classical groups in characteristic zero. Because these are then linearly reductive, the inclusion (1.1) splits. We give an algorithm for explicitly computing the Reynolds operator in each case in terms of certain integrals of monomial functions. We do this by reducing the computation to one over a compact Lie group, in which case we may integrate with respect to the Haar measure akin to averaging over a finite group. Methods to compute these integrals are of interest in mathematical physics due to their important role in areas such as mesoscopic transport, quantum chaos, and quantum information and decoherence. This interest has led to the development of various algorithms — such as the *invariant method* and the *column vector method* — to compute these integrals; see the introduction of [10] for more on this topic.

We remark that there are conditions weaker than having invertible order or being linearly reductive that imply finite generation of S^G . Indeed, Noether [24] showed that if G is a finite group acting on a finitely generated k -algebra S by k -algebra automorphisms, then S^G is a finitely generated k -algebra. Similarly, Haboush [11] proved that if G is a *reductive group* acting rationally on a finitely generated k -algebra S , then S^G is finitely generated. While the classical groups are no longer linearly reductive in positive characteristic, they continue to be reductive, and hence the invariant subrings are known to be finitely generated.

The paper is arranged as follows. After setting up the notations and definitions in Section 2, we define the classical group actions in Section 3 and record the rings of invariants. In Section 4, we recall the relevant facts about linearly reductive groups. Section 5 discusses the computation of the Reynolds operator for a compact Lie group. We discuss facts about the Haar measure and set up the required machinery to integrate functions that take values in polynomial rings. Section 6 begins by describing how the computation of the Reynolds operator for a classical group over an arbitrary field of characteristic zero can be reduced to that for a compact Lie group. With this reduction in place, we then give algorithms that one may implement on a computer algebra system. We use these algorithms in Section 7 to provide explicit formulae for the Reynolds operators for the SL and GL actions. These algorithms have been implemented in SageMath [31], and we note some conjectures arising out of these computations. Lastly, we compare with the situation in positive characteristic in Section 8.

2 | NOTATIONS AND DEFINITIONS

The letter k will denote a field. For $n \geq 1$, \mathbb{A}_k^n denotes the topological space k^n with the Zariski topology. We recall the following classical groups of invertible matrices.

- (a) (General linear group) $GL_n(k)$ is the group of $n \times n$ invertible matrices over k .
- (b) (Special linear group) $SL_n(k) := \{M \in GL_n(k) : \det(M) = 1\}$.
- (c) (Orthogonal group) $O_n(k) := \{M \in GL_n(k) : M^{\text{tr}}M = I_n\}$, where I_n denotes the identity matrix.
- (d) (Symplectic group) $Sp_{2n}(k) := \{M \in GL_{2n}(k) : M^{\text{tr}}\Omega M = \Omega\}$, where $\Omega := \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$.

When the field k is taken to be the complex numbers, we have the following additional subgroups.

- (e) (Unitary group) $U_n(\mathbb{C}) := \{U \in GL_n(\mathbb{C}) : UU^* = I_n\}$, where U^* denotes the conjugate transpose of U .

- (f) (Special unitary group) $SU_n(\mathbb{C}) := U_n(\mathbb{C}) \cap SL_n(\mathbb{C})$.
 (g) (Symplectic unitary group) $SpU_{2n}(\mathbb{C}) := U_{2n}(\mathbb{C}) \cap Sp_{2n}(\mathbb{C})$.

All the above groups inherit the subspace topology from $\mathbb{A}_k^{n^2}$, and we refer to this as the Zariski topology. These are all topological groups — though typically not Hausdorff — because the product and inversion functions are continuous in the Zariski topology, being given by rational functions in the entries of the matrices.

When $k = \mathbb{C}$, these groups also have the Euclidean topology and moreover are smooth submanifolds of \mathbb{C}^{n^2} . In this case, the product and inversion functions are smooth; hence, these are all Lie groups.

Definition 2.1. Let G be a group acting by ring automorphisms on a ring S . A **splitting** for the inclusion $S^G \hookrightarrow S$ is an additive function $\mathcal{R} : S \rightarrow S^G$ such that $\mathcal{R}(r) = r$ for all $r \in S^G$. The splitting is **G -equivariant** if $\mathcal{R}(g(s)) = \mathcal{R}(s)$ for all $g \in G$ and $s \in S$. The splitting is **S^G -linear** if $\mathcal{R}(rs) = r\mathcal{R}(s)$ for all $r \in S^G$ and $s \in S$.

3 | THE CLASSICAL GROUP ACTIONS

Let k be a field, and t, m, n be positive integers. We use the notation

$$k[Y_{t \times n}] := k[y_{ij} : 1 \leq i \leq t, 1 \leq j \leq n],$$

that is, $k[Y_{t \times n}]$ is a polynomial ring over k in tn variables. Once the dimensions have been specified, we write $k[Y]$ for brevity. We use the letter Y for the $t \times n$ matrix $[y_{ij}]_{i,j}$. The notation naturally extends to $k[X_{m \times t}, Y_{t \times n}]$.

Let G be one of the groups $GL_t(k)$, $SL_t(k)$, $O_t(k)$, or $Sp_t(k)$, where for the last case, we assume that t is even. We will consider the following two types of rational actions of G .

- (R1) The group G acts on $k[Y_{t \times n}]$, where the action of $M \in G$ is given by

$$M : Y \mapsto MY;$$

by the above, we mean that $[Y]_{ij} \mapsto [MY]_{ij}$.

- (R2) The group G acts on $k[X_{m \times t}, Y_{t \times n}]$, where the action of $M \in G$ is given by

$$M : \begin{cases} X \mapsto XM^{-1}, \\ Y \mapsto MY. \end{cases}$$

The first action corresponds to the direct sum of n copies of the standard representation, whereas the second has an additional m copies of the dual representation. We will describe the splittings for all of these actions.

We recall below the *classical rings of invariants* as in Weyl's book [32] where they were originally discussed in characteristic zero. A characteristic-free proof of the following theorem can be found in [2, 13].

Theorem 3.1. *Let k be an infinite field. With the above actions, we have the following rings of invariants.*

(a) (General linear group) For positive integers t, m, n , the equality

$$k[X_{m \times t}, Y_{t \times n}]^{\mathrm{GL}_t(k)} = k[XY]$$

holds, that is, the invariant ring is generated, as a k -algebra, by the entries of the matrix product XY .

(b) (Special linear group) For positive integers t, n with $t \leq n$, the equality

$$k[Y_{t \times n}]^{\mathrm{SL}_t(k)} = k[\text{size } t \text{ minors}]$$

holds, that is, the invariant ring is generated, as a k -algebra, by the size t minors of the matrix Y .

(c) (Orthogonal group) For positive integers t, n and $\mathrm{char}(k) \neq 2$, the equality

$$k[Y_{t \times n}]^{\mathrm{O}_t(k)} = k[Y^{\mathrm{tr}}Y]$$

holds, that is, the invariant ring is generated, as a k -algebra, by the entries of the matrix product $Y^{\mathrm{tr}}Y$.

(d) (Symplectic group) For positive integers t, n , the equality

$$k[Y_{2t \times n}]^{\mathrm{Sp}_{2t}(k)} = k[Y^{\mathrm{tr}}\Omega Y]$$

holds, that is, the invariant ring is generated, as a k -algebra, by the entries of the matrix product $Y^{\mathrm{tr}}\Omega Y$.

Remark 3.2. For each of the above actions, the fixed subring is of independent interest for the reasons described below. We denote the invariant subring in the respective cases by R .

- (a) (General linear group) The ring R is isomorphic to the determinantal ring $k[Z_{m \times n}]/I_{t+1}(Z)$, where $I_{t+1}(Z)$ is the ideal generated by the size $t+1$ minors of Z .
- (b) (Special linear group) The ring R is the Plücker coordinate ring of the Grassmannian of t -dimensional subspaces of an n -dimensional space.
- (c) (Orthogonal group) The ring R is isomorphic to $k[Z]/I_{t+1}(Z)$, where Z is an $n \times n$ symmetric matrix of indeterminates.
- (d) (Symplectic group) The ring R is isomorphic to $k[Z]/\mathrm{Pf}_{2t+2}(Z)$, where Z is an $n \times n$ alternating matrix of indeterminates, and $\mathrm{Pf}_{2t+2}(Z)$ the ideal generated by its principal $(2t+2)$ -Pfaffians.

4 | LINEARLY REDUCTIVE GROUPS

This section contextualises our results with the broader theory of linearly reductive groups. For the most part, this is only for theoretical interest, as we will compute the Reynolds operator concretely by integrating over a compact Lie group. For an introduction to linear algebraic groups and rational actions, we refer the reader to one of [3, 7, 14, 21]. We record the relevant facts here.

Definition 4.1. Let G be a linear algebraic group over the field k , and V a rational representation of G . A **Reynolds operator** is a k -linear, G -equivariant splitting $\mathcal{R} : k[V] \rightarrow k[V]^G$.

Theorem 4.2. If G is linearly reductive, then for every rational representation V , there exists a unique Reynolds operator $\mathcal{R} : k[V] \rightarrow k[V]^G$. Moreover, \mathcal{R} is $k[V]^G$ -linear.

Proof. The statements are Theorem 2.2.5 and Corollary 2.2.7 in [3], respectively. \square

Example 4.3. We give an example of a group G acting on a polynomial ring S for which there exists an S^G -linear splitting but no G -equivariant splitting. Let G be the symmetric group on two element, and $S := \mathbb{F}_2[x, y]$. The group G acts on S by permuting the variables, and the invariant subring is $\mathbb{F}_2[x + y, xy]$. Because S is a free S^G -module with $\{1, x\}$ as a basis, the inclusion $S^G \hookrightarrow S$ splits S^G -linearly. Suppose that $\pi : S \rightarrow S^G$ is a G -equivariant splitting. Then, $\pi(x) = \pi(y)$ because x and y are in the same orbit. But then,

$$x + y = \pi(x + y) = \pi(x) + \pi(y) = 2\pi(x) = 0,$$

a contradiction. Thus, $S^G \hookrightarrow S$ admits no G -equivariant splitting even though it splits S^G -linearly. This example extends mutatis mutandis to any positive characteristic p by considering the permutation action of Σ_p — the symmetric group on p elements — on the polynomial ring $\mathbb{F}_p[x_1, \dots, x_p]$.

Example 4.4. We now give an example of a group action for which no S^G -linear splitting exists. Consider the action of the alternating group $G := A_3$ on the polynomial ring $S := \mathbb{F}_3[x, y, z]$ by permuting the variables. If we let e_1, e_2, e_3 denote the elementary symmetric polynomials in x, y, z and set $\Delta := (x - y)(y - z)(z - x)$, then one can check that $\Delta \in S^G$, $\Delta \notin (e_1, e_2, e_3)S^G$, but $\Delta \in (e_1, e_2, e_3)S$. This implies that $S^G \hookrightarrow S$ does not split over S^G . More generally, if A_n acts on $S = \mathbb{F}_p[x_1, \dots, x_n]$ by permuting variables, the inclusion $S^{A_n} \hookrightarrow S$ splits if and only if p does not divide $|A_n|$; the nontrivial implication was proven in [8, Theorem 12.2] for $p \nmid n(n - 1)$, and the general case can be found in [9, Corollary 4.2; 17, Theorem 2.18; 29, Theorem 5.5; 30].

Example 4.5. If k is a field of characteristic zero, then the classical groups $\mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$, $\mathrm{O}_n(k)$, and $\mathrm{Sp}_{2n}(k)$ are all linearly reductive, as are all finite groups. For a finite group G , the Reynolds operator is just averaging over the group: $\mathcal{R}(f) = \frac{1}{|G|} \sum_{g \in G} g(f)$.

The above Reynolds operator extends naturally to smooth actions of a compact Lie group; see Theorem 5.6. The following theorem, in conjunction with Proposition 6.4, tells us how the computation of the Reynolds operator for a linearly reductive group over \mathbb{C} can be reduced to that for a compact Lie group.

Theorem 4.6. Let G be a linear algebraic group over \mathbb{C} . The following are equivalent.

- (a) G is linearly reductive.
- (b) G has a Zariski-dense subgroup that is a compact Lie group (in the Euclidean topology).

We will deduce the above theorem for the classical groups of interest by producing Zariski-dense subgroups in Theorem 6.1.

5 | THE REYNOLDS OPERATOR FOR A LIE GROUP

We will now describe the Reynolds operator for a compact Lie group acting on a polynomial ring. Strictly speaking, the term “Reynolds operator” was defined for the rational action of a linear algebraic group, but we continue to use this term to mean a (\mathbb{C}) -linear G -equivariant splitting. We first recall some theory of integration over such a group.

In this section, a finite-dimensional vector space over \mathbb{R} will have its canonical structure of a real differentiable manifold. Examples include \mathbb{C} and finite-dimensional vector spaces over \mathbb{C} . Let G be a compact real Lie group and dG denote the (normalised) Haar measure on G . Given an element $g \in G$, we denote by L_g and R_g the left and right translation maps:

$$\begin{aligned} L_g : G &\rightarrow G, & R_g : G &\rightarrow G, \\ h &\mapsto gh, & h &\mapsto hg. \end{aligned} \tag{5.1}$$

For an introduction to the Haar measure, we refer the reader to one of [12, 20, 27]. We next recall the properties of interest to us.

Theorem 5.1. *Let $\psi : G \rightarrow \mathbb{R}$ be smooth, and $g \in G$. Then,*

$$\int_G \psi \, dG = \int_G (\psi \circ L_g) \, dG = \int_G (\psi \circ R_g) \, dG.$$

If ψ is constant and takes the value 1, then

$$\int_G \psi \, dG = 1.$$

We may naturally extend the integration of scalar-valued functions to vector-valued functions:

Definition 5.2. Let V be a finite-dimensional \mathbb{R} -vector space, and $\psi : G \rightarrow V$ a smooth function. Fix a basis $\{v_1, \dots, v_n\}$ of V . Let $\psi_i : G \rightarrow \mathbb{R}$ be the corresponding coordinate functions, satisfying $\psi(g) = \sum \psi_i(g)v_i$. We define

$$\int_G \psi := \sum_{i=1}^n \left(\int_G \psi_i \, dG \right) v_i \in V.$$

One checks that the above definition is independent of the choice of basis. Note that our notation above drops the “ dG ” when integrating vector-valued functions. This is for ease of notation as we will always be integrating with respect to the Haar measure. The linearity of scalar integration and the properties of the Haar measure readily extend to the following.

Lemma 5.3. *Let $T : V \rightarrow W$ be a linear map of finite-dimensional vector spaces, and let $\psi : G \rightarrow V$ be a smooth function. Then,*

$$\int_G (T \circ \psi) = T \left(\int_G \psi \right).$$

Lemma 5.4. Let $\psi : G \rightarrow V$ be smooth, and $g \in G$. Then,

$$\int_G \psi = \int_G (\psi \circ L_g) = \int_G (\psi \circ R_g).$$

If ψ is constant and takes the value v , then

$$\int_G \psi = v.$$

Definition 5.5. Suppose V is an infinite-dimensional vector space, and $\Psi : G \rightarrow V$ a function such that the vector space spanned by the image of Ψ is finite-dimensional. Let $W \subset V$ be any finite-dimensional subspace containing the image of Ψ , and let $\psi : G \rightarrow W$ be the restriction of Ψ . We say that Ψ is **smooth** if ψ is smooth, and define

$$\int_G \Psi := \int_G \psi,$$

where we note that the above definitions are independent of the choice of W .

Let $S = \mathbb{C}[x_1, \dots, x_n]$ be a polynomial ring, and let $[S]_1$ denote the \mathbb{C} -vector space of homogeneous degree one polynomials. There is a natural isomorphism of groups:

$$\{\text{degree-preserving } \mathbb{C}\text{-algebra automorphisms of } S\} \longleftrightarrow \{\mathbb{C}\text{-linear automorphisms of } [S]_1\}.$$

A degree-preserving \mathbb{C} -algebra action of G on S is called **smooth** if the corresponding action $G \times [S]_1 \rightarrow [S]_1$ is smooth. In this case, the corresponding action $G \times [S]_d \rightarrow [S]_d$ is smooth for all $d \geq 0$, where $[S]_d$ denotes the space of homogeneous polynomials of degree d . For $f \in S$, define the orbit map

$$\begin{aligned} \psi_f : G &\rightarrow S \\ g &\mapsto g(f). \end{aligned}$$

The function ψ_f takes values within a finite-dimensional subspace of S , for example, the space of polynomials of degree at most the degree of f . If the G -action is smooth, then ψ_f is a smooth function.

Theorem 5.6. Let G be a compact Lie group acting smoothly on the polynomial ring $S := \mathbb{C}[x_1, \dots, x_n]$ by degree-preserving \mathbb{C} -algebra automorphisms. Then, $S^G \hookrightarrow S$ splits with a degree-preserving, G -equivariant, S^G -linear splitting $\mathcal{R} : S \twoheadrightarrow S^G$ given by

$$\mathcal{R} : f \mapsto \int_G \psi_f.$$

Suggestively, the above may be written as

$$\mathcal{R}(f) = \int_{g \in G} g(f),$$

resembling the Reynolds operator for finite groups.

Proof. The \mathbb{C} -linearity of \mathcal{R} is clear. If f is homogeneous, then ψ_f takes values in subspace $[S]_{\deg(f)}$ and in turn, $\mathcal{R}(f) \in [S]_{\deg(f)}$. Thus, \mathcal{R} is a degree-preserving \mathbb{C} -linear map.

For the rest of the proof, we will make repeated use of Lemmas 5.3 and 5.4. Recall that L_g and R_g denote the translation maps, defined in (5.1). For $f \in S$ and $g \in G$, we define the \mathbb{C} -linear functions $S \xrightarrow{\rho_f} S$ and $S \xrightarrow{\mu_g} S$ given by left multiplication and the G -action, respectively. Consequently,

$$\begin{aligned} \mathcal{R}(f) &= \int_G \psi_f = \int_G \psi_f \circ R_g = \int_G \psi_{g(f)} = \mathcal{R}(g(f)) \\ &= \int_G \psi_f \circ L_g = \int_G \mu_g \circ \psi_f = \mu_g \left(\int_G \psi_f \right) = g(\mathcal{R}(f)). \end{aligned}$$

The above shows that \mathcal{R} takes values in S^G and is G -equivariant. Lastly, if $f \in S^G$ and $h \in S$, then

$$\mathcal{R}(fh) = \int_G \psi_{fh} = \int_G \rho_f \circ \psi_h = \rho_f \left(\int_G \psi_h \right) = f \mathcal{R}(h),$$

and ψ_f is identically equal to f , giving us

$$\mathcal{R}(f) = \int_G \psi_f = f.$$

This finishes the proof that \mathcal{R} is an S^G -linear splitting. □

6 | THE REYNOLDS OPERATOR FOR THE CLASSICAL ACTIONS

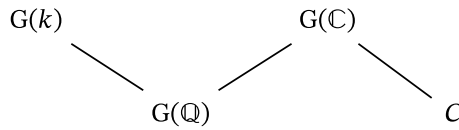
Fix an integer $t \geq 1$ and let $G(-)$ be one of $GL_t(-)$, $SL_t(-)$, $O_t(-)$, or $Sp_t(-)$, where we assume that t is even in the last case. Define $C := G(\mathbb{C}) \cap U_t(\mathbb{C})$. The intersections in the respective cases are $U_n(\mathbb{C})$, $SU_n(\mathbb{C})$, $O_n(\mathbb{R})$, and $SpU_n(\mathbb{C})$. Let k be an arbitrary field of characteristic zero.

Theorem 6.1 (The density theorem). *With the above notation, we have*

- (a) C is a Zariski-dense subgroup of $G(\mathbb{C})$; and
- (b) $G(\mathbb{Q})$ is a Zariski-dense subgroup of $G(k)$.

Proof. For (a), see the proof of [19, Anhang II, Satz 4]. We give a more elementary proof for GL and SL in Appendix A; see Propositions A.5 and A.6. We also prove (b) in Appendix A; see Theorem A.7. □

By $k[Z]$, we will mean one of $k[Y]$ or $k[X, Y]$. In either case, we have a rational action of $G(k)$ on $k[Z]$, as described in Section 3. Note that C is a compact Lie group, and the action of $G(\mathbb{C})$ on $\mathbb{C}[Z]$ restricts to a smooth action of C . We have the following group extensions.



We will first show how the computation of the Reynolds operator for $G(k)$ reduces to that for C . The key point is that the action is rational, and each inclusion above is Zariski-dense by Theorem 6.1. This reduction is useful because C is a compact Lie group; thus, we have its Reynolds operator by Theorem 5.6.

Proposition 6.2. *Let $f_1, \dots, f_n \in \mathbb{Q}[Z]^{G(\mathbb{Q})}$ be generating invariants, that is, we have $\mathbb{Q}[Z]^{G(\mathbb{Q})}$ equals $\mathbb{Q}[f_1, \dots, f_n]$. Then, the equality $k[Z]^{G(k)} = k[f_1, \dots, f_n]$ holds. In particular, we have the inclusion $\mathbb{Q}[Z]^{G(\mathbb{Q})} \subset k[Z]^{G(k)}$ as subsets of $k[Z]$.*

Proof. We first show that each f_i is $G(k)$ -invariant. To this end, note that the equation

$$\sigma(f_i) - f_i = 0$$

holds for each fixed i and for all $\sigma \in G(\mathbb{Q})$. Because the action is rational and $G(\mathbb{Q})$ is Zariski-dense in $G(k)$ by Theorem 6.1, the above equation must hold for all $\sigma \in G(k)$. In other words, each f_i is $G(k)$ -invariant.

We now prove the inclusion $k[Z]^{G(k)} \subset k[f_1, \dots, f_n]$. Let B be a \mathbb{Q} -basis for k . Given an element $h \in k[Z]^{G(k)}$, write

$$h = \sum_{b \in B} b h_b$$

for $h_b \in \mathbb{Q}[Z]$. If we apply $\sigma \in G(\mathbb{Q})$ to the above equation, we get

$$h = \sum_{b \in B} b \sigma(h_b)$$

because $\sigma(h) = h$ and $\sigma(b) = b$ for all $b \in k$. Comparing the two displayed equations above gives us that each h_b is fixed by $G(\mathbb{Q})$ and thus $h_b \in \mathbb{Q}[f_1, \dots, f_n]$ for all b . In turn, $h \in k[f_1, \dots, f_n]$, as desired. \square

Proposition 6.3. *Let $\mathcal{R}_k : k[Z] \rightarrow k[Z]^{G(k)}$ denote the Reynolds operator over the field k . The following diagram commutes*

$$\begin{array}{ccc}
 k[Z] & \xrightarrow{\mathcal{R}_k} & k[Z]^{G(k)} \\
 \uparrow & & \uparrow \\
 \mathbb{Q}[Z] & \xrightarrow{\mathcal{R}_{\mathbb{Q}}} & \mathbb{Q}[Z]^{G(\mathbb{Q})}.
 \end{array}$$

In particular, if $\mu \in k[Z]$ is a monomial, then

$$\mathcal{R}_k(\mu) = \mathcal{R}_{\mathbb{C}}(\mu). \quad (6.1)$$

The above equation makes sense by interpreting μ as an element of $\mathbb{C}[Z]$.

Proof. In view of Proposition 6.2, we may extend $\mathcal{R}_{\mathbb{Q}}$ k -linearly to obtain a retraction π making the diagram

$$\begin{array}{ccc} k[Z] & \xrightarrow{\pi} & k[Z]^{G(k)} \\ \uparrow & & \uparrow \\ \mathbb{Q}[Z] & \xrightarrow{\mathcal{R}_{\mathbb{Q}}} & \mathbb{Q}[Z]^{G(\mathbb{Q})}. \end{array}$$

commute. We need to show that $\pi = \mathcal{R}_k$. By the uniqueness of the Reynolds operator, Theorem 4.2, it suffices to show that π is $G(k)$ -equivariant. Note that $G(k)$ -equivariance can be checked on monomials, where it is true again by the Zariski-density of $G(\mathbb{Q})$. This proves that the diagram commutes. Now, if $\mu \in \mathbb{Q}[Y]$ is a monomial, then the diagram gives us $\mathcal{R}_k(\mu) = \mathcal{R}_{\mathbb{Q}}(\mu)$. Because k was arbitrary, we get (6.1). \square

The Zariski-density of C in $G(\mathbb{C})$ similarly yields the following proposition.

Proposition 6.4. *The equality $\mathbb{C}[Z]^{G(\mathbb{C})} = \mathbb{C}[Z]^C$ holds, and the splitting $\mathcal{R} : \mathbb{C}[Z] \rightarrow \mathbb{C}[Z]^C$ described in Theorem 5.6 is $G(\mathbb{C})$ -equivariant. In other words, \mathcal{R} is the Reynolds operator for the $G(\mathbb{C})$ -action, by Theorem 4.2.*

Remark 6.5. The above has now made the computation of \mathcal{R}_k clear: because the Reynolds operator \mathcal{R}_k is a k -linear map, it suffices to compute it on monomials; and for monomials, \mathcal{R}_k agrees with the Reynolds operator for the Lie group C by (6.1) and Proposition 6.4.

In the following two subsections, we describe algorithms to implement this splitting on a computer algebra system.

6.1 | Computing the Reynolds operator for copies of the standard representation

Continuing our notation from earlier, let $G(k) \leq GL_t(k)$ be one of the classical groups, and $C := G(\mathbb{C}) \cap U_t(\mathbb{C})$ the corresponding compact Lie group. For a positive integer n , the group $G(k)$ acts on $k[Y_{t \times n}]$ as described in (R1). We describe the Reynolds operator for this action. Consider the larger polynomial ring $k[Y][U_{t \times t}]$, and define the k -algebra map

$$\begin{aligned} \phi : k[Y] &\rightarrow k[Y][U] \\ Y &\mapsto UY. \end{aligned}$$

For $f \in k[Y]$, write

$$\phi(f) = \sum_I \alpha_I(f) u^I,$$

where $\alpha_I(f) \in k[Y]$; in the above, the sum is over multi-indices $I \in \mathbb{N}^{t^2}$, and u^I is the corresponding monomial. Each u^I can be naturally interpreted as a smooth function $C \rightarrow \mathbb{C}$ and the Reynolds operator is then given as

$$\begin{aligned} \mathcal{R} : k[Y] &\rightarrow k[Y]^{G(k)} \\ f &\mapsto \sum_I \alpha_I(f) \int_C u^I. \end{aligned} \quad (6.2)$$

6.2 | Computing the Reynolds operator for copies of the standard and the dual representations

We now consider the action of $G(k)$ on $k[X_{m \times t}, Y_{t \times n}]$ as described in (R2). Note that while the action of $G(k)$ involves an inverse, C is a subgroup of the unitary group and thus, $U^{-1} = \overline{U}^{\text{tr}}$ for $U \in C$. We now consider the larger polynomial ring $k[X, Y][U_{t \times t}, \overline{U}_{t \times t}]$ with $2t^2$ additional indeterminates; explicitly, the new variables are the symbols $\{u_{ij} : 1 \leq i, j \leq n\} \cup \{\overline{u}_{ij} : 1 \leq i, j \leq n\}$. Define the k -algebra map

$$\begin{aligned} \phi : k[X, Y] &\rightarrow k[X, Y][U, \overline{U}] \\ X &\mapsto X \overline{U}^{\text{tr}}, \\ Y &\mapsto UY. \end{aligned}$$

For $f \in k[X, Y]$, write

$$\phi(f) = \sum_{I, J} \alpha_{I, J}(f) u^I \overline{u}^J.$$

Each monomial $u^I \overline{u}^J$ can again be interpreted as a smooth function on C and the Reynolds operator is given as

$$\begin{aligned} \mathcal{R} : k[X, Y] &\rightarrow k[X, Y]^{G(k)} \\ f &\mapsto \sum_{I, J} \alpha_{I, J}(f) \int_C u^I \overline{u}^J. \end{aligned} \quad (6.3)$$

6.3 | Some remarks

We stress that the only nonalgebraic calculations above are the integrals of monomial functions over C , where C is one of $U_t(\mathbb{C})$, $SU_t(\mathbb{C})$, $O_t(\mathbb{R})$, or $\text{Sp}U_t(\mathbb{C})$. Note moreover that these are scalar functions. While we discussed the theory of integration of vector-valued functions to prove the above, one needs only to work with \mathbb{C} -valued functions in practice.

The integration of these monomial functions over $U_t(\mathbb{C})$, $O_t(\mathbb{R})$, and $\text{Sp}U_t(\mathbb{C})$ is of interest in various fields of mathematical physics, see the introduction of [10]. Methods to compute these

integrals are described in [1, 10]. In particular, the integration of arbitrary monomial functions over $U_t(\mathbb{C})$ has been implemented in the *Mathematica* package *IntU* [26]. Using this package, we have implemented the splitting (6.3) for the action (R2) of $GL_t(\mathbb{C})$ in the computer algebra system *SageMath* [31]. We have also implemented the splitting (6.2) for the action (R1) of $SL_2(\mathbb{C})$ using Theorem 7.5.

For $SL_t(k)$ and $O_t(k)$, the method described in Section 6.2 for the action (R2) may be modified as follows.

- (a) (Special linear group) If $C = SL_t(\mathbb{C}) \cap U_t(\mathbb{C})$, then the inverse of $U \in C$ is given by the adjugate $\text{adj}(U)$. Note that the entries of $\text{adj}(U)$ are polynomials in the entries of U , so we may modify ϕ as

$$\begin{aligned}\phi : k[X, Y] &\rightarrow k[X, Y][U] \\ X &\mapsto X \text{adj}(U), \\ Y &\mapsto UY.\end{aligned}$$

- (b) (Orthogonal group) If $C = O_t(\mathbb{C}) \cap U_t(\mathbb{C})$, then the inverse of $U \in C$ is just the transpose U^{tr} , so we may modify ϕ as

$$\begin{aligned}\phi : k[X, Y] &\rightarrow k[X, Y][U] \\ X &\mapsto XU^{\text{tr}}, \\ Y &\mapsto UY.\end{aligned}$$

7 | EXPLICIT FORMULAE

In this section, we use the formulae of Section 6 to compute the Reynolds operators for SL_2 and GL_t . We give expressions for these in terms of the invariants described in Theorem 3.1.

7.1 | The Reynolds operator for SL_2

We use formula (6.2) to compute the Reynolds operator \mathcal{R} for the standard action (R1) of $SL_2(k)$ on $k[Y_{2 \times N}]$; the relevant monomial integrals are determined in Theorem 7.5 and we can thus compute \mathcal{R} on any element of $k[Y]$. We begin the section by recording the value of \mathcal{R} on various families of monomials, postponing the proofs until the end of the section. By Theorem 3.1, we know that $k[Y]^{\text{SL}_2(k)}$ is generated by the size 2 minors of Y . For ease of notation, we write

$$Y = \begin{bmatrix} a_1 & a_2 & \cdots & a_N \\ b_1 & b_2 & \cdots & b_N \end{bmatrix}, \quad \{\Delta\} := \{\text{size 2 minors of } Y\}, \quad \text{and} \quad \Delta_{i,j} := a_i b_j - a_j b_i.$$

The next theorem describes the Reynolds operator on $k[Y_{2 \times 2}]$.

Theorem 7.1. *Let $\mathcal{R} : k[Y_{2 \times 2}] \rightarrow k[\{\Delta\}]$ be the Reynolds operator and $\mu \in k[Y_{2 \times 2}]$ a monomial.*

(a) If μ is of the form $(a_1 b_2)^n (a_2 b_1)^m$ for some nonnegative integers n and m , then

$$\mathcal{R}(\mu) = \mathcal{R}((a_1 b_2)^n (a_2 b_1)^m) = \frac{n!m!}{(n+m+1)!} \Delta_{1,2}^n \Delta_{2,1}^m; \quad (7.1)$$

in particular, for $n \geq 0$, we have

$$\mathcal{R}((a_1 b_2)^n) = \frac{1}{n+1} \Delta_{1,2}^n. \quad (7.2)$$

(b) If μ is not of the above form, then

$$\mathcal{R}(\mu) = 0.$$

We give $k[Y_{2 \times N}]$ a multi-grading by defining $\deg(a_i) = (1, 0)$ and $\deg(b_i) = (0, 1)$ for all $1 \leq i \leq N$.

Theorem 7.2. Let $\mu \in k[Y]$ be a monomial such that $\deg(\mu) = (m, n)$ with $m \neq n$. Then, $\mathcal{R}(\mu) = 0$.

Computations suggest that (7.1) generalises as follows.

Conjecture 7.3. For all nonnegative integers i, j, k , we have

$$\mathcal{R}((a_1 b_2)^i (a_1 b_3)^j (a_2 b_3)^k) = \frac{(i+j)!(k+j)!}{(i+j+k+1)!j!} \Delta_{1,2}^i \Delta_{1,3}^j \Delta_{2,3}^k.$$

Conjecture 7.4. For all nonnegative integers n , we have

$$\mathcal{R}((a_1 a_2 a_3 b_1 b_2 b_3)^{2n+1}) = 0.$$

Theorem 7.5. For all nonnegative integers a, b, c, d , we have

$$\int_{\mathrm{SU}_2(\mathbb{C})} u_{11}^a u_{12}^b u_{21}^c u_{22}^d = \begin{cases} (-1)^b \frac{a!b!}{(a+b+1)!} & \text{if } a = d \text{ and } b = c, \\ 0 & \text{else.} \end{cases}$$

Proof. See Identity B.5. □

We say that a monomial in $k[Y]$ is **balanced** if it is a product of monomials of the form $a_i b_j$ with $i \neq j$, and **unbalanced** otherwise. The following are straightforward observations.

- (a) The algebra of minors $k[\{\Delta\}]$ sits inside the k -subalgebra generated by the balanced monomials.
- (b) If $\mu \in k[Y]$ is a balanced monomial, then $\deg(\mu) = (d, d)$ for some $d \geq 0$.

Note however that $\deg(a_1 b_1) = (1, 1)$, yet $a_1 b_1$ is unbalanced.

Remark 7.6. Assuming Conjecture 7.3, the $k[\{\Delta\}]$ -linearity of \mathcal{R} would then determine the value of \mathcal{R} on any balanced monomial in $k[Y_{2 \times 3}]$. For example, one may verify Conjecture 7.3 in the two cases needed for the following computation and obtain

$$\mathcal{R}((a_1 b_2)(a_2 b_3)(a_3 b_1)) = \mathcal{R}((a_1 b_2)(a_2 b_3)(a_1 b_3 - \Delta_{1,3})) = \left(\frac{1}{6} - \frac{1}{6}\right) \Delta_{1,2} \Delta_{1,3} \Delta_{2,3} = 0.$$

The above gives us the case $n = 0$ in Conjecture 7.4. In particular, it shows that a balanced monomial may be in the kernel of \mathcal{R} ; Theorem 7.1 tells us that this does not happen for $k[Y_{2 \times 2}]$, where the monomials in the kernel are precisely the unbalanced ones.

Remark 7.7. It is not true that the image of a monomial is again a monomial in the $\Delta_{i,j}$. One checks that

$$\mathcal{R}(a_1 b_2 a_3 b_4) = \frac{1}{3} \Delta_{1,2} \Delta_{3,4} - \frac{1}{6} \Delta_{1,3} \Delta_{2,4}.$$

The expression on the right is not divisible by any $\Delta_{i,j}$ and thus cannot be expressed as a monomial in the $\{\Delta\}$.

Proof of Theorem 7.1 (a). The map ϕ from Section 6.1 is given by

$$\begin{bmatrix} a_1 & \cdots & a_N \\ b_1 & \cdots & b_N \end{bmatrix} \mapsto \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \begin{bmatrix} a_1 & \cdots & a_N \\ b_1 & \cdots & b_N \end{bmatrix}.$$

Thus,

$$\begin{aligned} \phi(a_1) &= a_1 u_{11} + b_1 u_{12}, \text{ and} \\ \phi(b_2) &= a_2 u_{21} + b_2 u_{22}. \end{aligned}$$

Because ϕ is a ring homomorphism, we have

$$\phi((a_1 b_2)^n) = \sum_{i+j+k+\ell=n} \binom{n}{i, j, k, \ell} (a_1 a_2 u_{11} u_{21})^i (a_1 b_2 u_{11} u_{22})^j (a_2 b_1 u_{12} u_{21})^k (b_1 b_2 u_{12} u_{22})^\ell.$$

Theorem 7.5 tells us that if we integrate the above over $\mathrm{SU}_2(\mathbb{C})$, the only terms that remain are those with $i = \ell$. Integrating those terms, we get

$$\begin{aligned} \mathcal{R}((a_1 b_2)^n) &= \sum_{2i+j+k=n} \binom{n}{i, j, k, i} (a_1 b_2)^{i+j} (a_2 b_1)^{i+k} (-1)^{i+k} \frac{(i+j)!(i+k)!}{(n+1)!} \\ &= \frac{1}{n+1} (a_1 b_2 - a_2 b_1)^n = \frac{\Delta_{1,2}^n}{n+1}, \end{aligned}$$

where the penultimate equality uses Identity B.2, proving (7.2). For (7.1), note that $a_2 b_1 = a_1 b_2 + \Delta_{2,1}$. Because \mathcal{R} is $k[\{\Delta\}]$ -linear and $\Delta_{1,2} = -\Delta_{2,1}$, we get

$$\mathcal{R}((a_1 b_2)^n (a_2 b_1)^m) = \mathcal{R}((a_1 b_2)^n (a_1 b_2 + \Delta_{2,1})^m)$$

$$\begin{aligned}
&= \sum_{k=0}^m \binom{m}{k} \Delta_{2,1}^{m-k} \mathcal{R}((a_1 b_2)^{n+k}) \\
&= \sum_{k=0}^m \binom{m}{k} \Delta_{2,1}^{m-k} \cdot \frac{\Delta_{1,2}^{n+k}}{n+k+1} \\
&= \Delta_{1,2}^n \Delta_{2,1}^m \sum_{k=0}^m \binom{m}{k} \frac{(-1)^k}{n+k+1}.
\end{aligned}$$

Identity B.3 finishes the proof. \square

Proof of Theorem 7.2. Consider the element $\sigma = \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix} \in \mathrm{SL}_2(k)$. We have $\sigma(\mu) = 2^{m-n}\mu$ and thus, the $\mathrm{SL}_2(k)$ -equivariance of \mathcal{R} implies that $\mathcal{R}(\mu) = 2^{m-n}\mathcal{R}(\mu)$. Because $m \neq n$, we get that $\mathcal{R}(\mu) = 0$. \square

Proof of Theorem 7.1 (b). We first prove the statement when μ is of the form $(a_1 b_1)^m (a_1 b_2)^n$ for some $m > 0$ and $n \geq 0$. We have

$$\phi(\mu) = (a_1^2 u^* + a_1 b_1 u^* + a_1 b_1 u^* + b_1^2 u^*)^m \cdot (a_1 a_2 u^* + a_1 b_2 u^* + a_2 b_1 u^* + b_1 b_2 u^*)^n,$$

where each u^* denotes some monomial in the u_{ij} . Because $m > 0$, when we expand the above, each monomial that appears will be unbalanced in the sense that we may write

$$\phi(\mu) = \sum_I \alpha_I \mu_I u_I,$$

where $\alpha_I \in k$, $\mu_I \in k[Y]$ is an unbalanced monomial, and $u_I \in k[U]$ is a monomial. Integrating the above yields

$$\mathcal{R}(\mu) = \sum_I (\alpha_I \int u_I) \mu_I.$$

Now, note that $\mathcal{R}(\mu) \in k[\{\Delta\}] \subset k[\text{balanced monomials}]$, whereas each μ_I above is unbalanced. Thus, the terms above must cancel out to give us $\mathcal{R}(\mu) = 0$.

The $k[\{\Delta\}]$ -linearity of \mathcal{R} then implies the statement for μ of the form $(a_1 b_1)^m \nu$ with $m > 0$ and $\nu \in k[a_1 b_2, a_2 b_1]$. By symmetry, the statement also holds for μ of the form $(a_2 b_2)^m \nu$. Theorem 7.2 takes care of unbalanced monomials not of the above form. \square

7.2 | The Reynolds operator for GL_t

Let t, n, m be positive integers, and $\mathcal{R} : k[X_{m \times t}, Y_{t \times n}] \rightarrow k[X, Y]^{\mathrm{GL}_t(k)}$ the Reynolds operator for the action (R2). By Theorem 3.1, we know the image of \mathcal{R} to lie in $k[XY]$, the subalgebra of $k[X, Y]$ generated by the entries of XY . Experimenting with the package IntU [26] suggests a formula similar to (7.2).

Conjecture 7.8. *For $t = 2$ and $n \geq 0$, we have*

$$\mathcal{R}((x_{11}y_{11})^n) = \frac{1}{n+1}(x_{11}y_{11} + x_{12}y_{21})^n = \frac{1}{n+1}([XY]_{1,1})^n.$$

More generally, for $t \geq 1$ and $n \geq 0$, we have

$$\mathcal{R}((x_{11}y_{11})^n) = \binom{n+t-1}{t-1} ([XY]_{1,1})^n.$$

8 | COMPARISON WITH POSITIVE CHARACTERISTIC

The classical groups GL, SL, O, Sp are typically *not* linearly reductive in positive characteristic. Thus, there is no guarantee of the existence of splittings that are linear over the fixed subring. In fact, the following theorem tells us that this is essentially never the case.

Theorem 8.1 [15, Theorem 1.1]. *Let k be a field of characteristic $p > 0$. Fix positive integers m, n , and t , and let $R \subset S$ denote one of the following inclusions:*

- (a) $k[XY] \subset k[X_{m \times t}, Y_{t \times n}]$;
- (b) $k[\{\Delta\}] \subset k[Y_{t \times n}]$ with $t \leq n$, where $\{\Delta\}$ is the set of size t minors of Y ;
- (c) $k[Y^{\text{tr}}Y] \subset k[Y_{t \times n}]$;
- (d) $k[Y^{\text{tr}}\Omega Y] \subset k[Y_{2t \times n}]$.

Then the inclusion $R \subset S$ splits R -linearly if and only if, in the respective cases,

- (a) $t = 1$ or $\min\{m, n\} \leq t$;
- (b) $t = 1$ or $t = n$;
- (c) $t = 1$; $t = 2$ and p is odd; $p = 2$ and $n \leq (t+1)/2$; or p is odd and $n \leq (t+2)/2$;
- (d) $n \leq t+1$.

Remark 8.2. The above theorem does not reference any group (action). However, compare with Theorem 3.1 to see the connection for infinite fields of positive characteristic.

Remark 8.3. We describe a curious implication of Theorem 8.1. We revisit formula (7.2):

$$\mathcal{R}((a_1b_2)^n) = \frac{1}{n+1}\Delta_{1,2}^n.$$

Note the denominator ‘ $n+1$ ’. This means that each prime number shows up as a factor of the denominator for some monomial. Said differently, \mathcal{R} does not restrict to a map $\mathbb{Z}_{(p)}[Y] \rightarrow \mathbb{Z}_{(p)}[\{\Delta\}]$ for any prime $p > 0$, where $\mathbb{Z}_{(p)}$ is the subring of \mathbb{Q} defined as

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z} \text{ with } p \nmid b \right\}.$$

Theorem 8.1 tells us that this must essentially always happen for any of the Reynolds operators described in the paper. More generally, the above must happen for essentially any splitting that is linear over the subring.

Indeed, pick a situation in Theorem 8.1 where the inclusion does not split in positive characteristic. For example, $\mathbb{F}_p[\{\Delta\}] \hookrightarrow \mathbb{F}_p[Y_{t \times n}]$ with $1 < t < n$. As discussed earlier, the inclusion $\mathbb{Q}[\{\Delta\}] \hookrightarrow \mathbb{Q}[Y_{t \times n}]$ does split. Moreover, if we are only interested in splittings that are linear over the subring, then there are typically more than one. Let $\pi : \mathbb{Q}[Y_{t \times n}] \rightarrow \mathbb{Q}[\{\Delta\}]$ be any such $\mathbb{Q}[\{\Delta\}]$ -linear splitting. The following must hold: given any prime $p > 0$, there exists some monomial $\mu = \mu(p) \in \mathbb{Q}[Y]$ such that when we express $\pi(\mu)$ as a polynomial in the $\{\Delta\}$ with rational coefficients, then one of the coefficients has denominator divisible by p . Indeed, if this were not the case for some prime p , then π would restrict to a splitting $\mathbb{Z}_{(p)}[Y] \rightarrow \mathbb{Z}_{(p)}[\{\Delta\}]$, and we could go mod p to obtain an $\mathbb{F}_p[\{\Delta\}]$ -linear splitting, contradicting Theorem 8.1.

APPENDIX A: PROOF OF THE DENSITY THEOREM

Definition A.1. For X a topological space and Y a subspace of X , a **retraction** of X onto Y is a continuous function $r : X \rightarrow Y$ satisfying $r(y) = y$ for all $y \in Y \subset X$.

Lemma A.2. Let k be a field, and $S \subset k$ be an infinite subset. If $f \in k[x_1, \dots, x_n]$ is a polynomial vanishing on the product $S^n \subset \mathbb{A}_k^n$, then f is the zero polynomial. Equivalently, S^n is Zariski-dense in \mathbb{A}_k^n .

Proof. We prove the statement by induction on n . It is clear for $n = 1$. Assume $n > 1$ and suppose f is nonzero. Write $f = f_0 + f_1 x_n + \dots + f_d x_n^d$ with $d \geq 0$, $f_d \neq 0$, and $f_i \in k[x_1, \dots, x_{n-1}]$. By induction, there exists $\mathbf{s} = (s_1, \dots, s_{n-1}) \in S^{n-1}$ with $f_d(\mathbf{s}) \neq 0$. Then, $f(\mathbf{s}, x_n)$ is a nonzero polynomial in one variable, and this finishes the proof. \square

Lemma A.3. Let X be a topological space, $Z \subset X$ a dense subspace, and $Y \subset X$ a subspace such that there exists a retraction $r : X \rightarrow Y$ with $r(Z) \subset Z$. Then, $Z \cap Y$ is dense in Y .

Proof. Let $y \in Y$ be arbitrary. As Z is dense in X , there exists a net $\langle z_\lambda \rangle_{\lambda \in \Lambda}$ in Z with $z_\lambda \rightarrow y$. In turn, $\langle r(z_\lambda) \rangle_\lambda$ is a net in $Z \cap Y$ converging to y . \square

For the next few proofs, we define the function

$$r : \mathrm{GL}_n(k) \rightarrow \mathrm{SL}_n(k)$$

$$U = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n1} & u_{n2} & \cdots & u_{nn} \end{bmatrix} \mapsto \begin{bmatrix} \frac{u_{11}}{\det U} & \frac{u_{12}}{\det U} & \cdots & \frac{u_{1n}}{\det U} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n1} & u_{n2} & \cdots & u_{nn} \end{bmatrix}. \quad (\text{A.1})$$

That is, r scales the first row of U by $\frac{1}{\det U}$.

Lemma A.4. For any field k , the function r defined by (A.1) is a retraction of $\mathrm{GL}_n(k)$ onto $\mathrm{SL}_n(k)$.

Proof. The multilinearity of \det implies that $\det(r(U)) = 1$ for all $U \in \mathrm{GL}_n(\mathbb{C})$, that is, r indeed takes values in $\mathrm{SL}_n(k)$. The function r is continuous in the Zariski topology because it is given by rational functions. It is clear that the restriction of r to $\mathrm{SL}_n(k)$ is the identity. \square

Proposition A.5. *For all $n \geq 1$, the subgroup $U_n(\mathbb{C})$ is Zariski-dense in $GL_n(\mathbb{C})$.*

Proof. Let C be the Zariski closure of $U_n(\mathbb{C})$ in $GL_n(\mathbb{C})$. Write $C = V(\mathfrak{a}) \cap GL_n(\mathbb{C})$ for \mathfrak{a} an ideal. Let $f \in \mathfrak{a}$. Note that if z_1, \dots, z_n are elements of the unit circle \mathbb{S}^1 , then $\text{diag}(z_1, \dots, z_n)$ is an element of U_n . Thus, f vanishes on all diagonal matrices with entries coming from \mathbb{S}^1 . By Lemma A.2, we see that f must vanish on *all* diagonal matrices. Thus, C contains all invertible diagonal matrices.

Because $GL_n(\mathbb{C})$ is a topological group in the Zariski topology, and $U_n(\mathbb{C})$ is a subgroup, it follows that C is a subgroup. As every invertible matrix can be decomposed as UDV with $U, V \in U_n(\mathbb{C})$ and D invertible diagonal, we are done. \square

Proposition A.6. *For all $n \geq 1$, the subgroup $SU_n(\mathbb{C})$ is Zariski-dense in $SL_n(\mathbb{C})$.*

Proof. We use Lemma A.3 with $X = GL_n(\mathbb{C})$, $Z = U_n(\mathbb{C})$, $Y = SL_n(\mathbb{C})$, and r given by (A.1). The density of Z then follows from Proposition A.5. All that is left to be shown is that $r(U_n(\mathbb{C})) \subset U_n(\mathbb{C})$. To this end, note that a matrix is unitary if and only if its rows form an orthonormal basis. If $U \in U_n(\mathbb{C})$, then $\det(U) \in \mathbb{S}^1$ and thus, the rows of $r(U)$ continue to be orthonormal. \square

Theorem A.7. *Let k be a field of characteristic zero. For each of the following inclusions, the subgroup is Zariski-dense in the larger group.*

- (a) $GL_n(\mathbb{Q}) \subset GL_n(k)$,
- (b) $SL_n(\mathbb{Q}) \subset SL_n(k)$,
- (c) $O_n(\mathbb{Q}) \subset O_n(k)$, and
- (d) $Sp_{2n}(\mathbb{Q}) \subset Sp_{2n}(k)$.

Proof. General linear group: By Lemma A.2, the subspace \mathbb{Q}^{n^2} is dense in $\mathbb{A}_k^{n^2}$. Intersecting with the open set $GL_n(k)$ gives us (a).

Special linear group: (b) then follows by use of Lemma A.3 with $X = GL_n(k)$, $Y = SL_n(k)$, $Z = GL_n(\mathbb{Q})$, and r given by (A.1).

Orthogonal group: We note that the orthogonal group $O_n(k)$ is generated by the set of reflections

$$R(k) := \left\{ I - \frac{2uu^{\text{tr}}}{u^{\text{tr}}u} : u \in k^n \text{ with } u^{\text{tr}}u \neq 0 \right\},$$

in fact the Cartan–Dieudonné theorem states that every orthogonal matrix is a product of at most n such reflections, see [4, 28]. Because the closure of $O_n(\mathbb{Q})$ must be a subgroup of $O_n(k)$, it suffices to show that $R(\mathbb{Q})$ is dense in $R(k)$. To this end, note that $I(k) := \{u \in k^n : u^{\text{tr}}u \neq 0\}$ is an open subset of \mathbb{A}_k^n and thus intersecting with the dense set \mathbb{Q}^n , we get that $I(\mathbb{Q})$ is dense in $I(k)$. Now, $R(k)$ is the image of $I(k)$ under the continuous map $u \mapsto I - \frac{2uu^{\text{tr}}}{u^{\text{tr}}u}$ and hence $R(\mathbb{Q})$ is dense in $R(k)$.

Symplectic group: (d) follows similarly by using the fact that the symplectic group $Sp_{2n}(k)$ is generated by

$$\begin{bmatrix} A & O \\ O & (A^{\text{tr}})^{-1} \end{bmatrix}, \quad \begin{bmatrix} I & B \\ O & I \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} O & I \\ -I & O \end{bmatrix},$$

where A varies over $SL_n(k)$, and B over all symmetric $n \times n$ matrices. This description is originally due to Dieudonné [5] and can also be found in [25, Section 2.2]. \square

APPENDIX B: MULTINOMIAL COEFFICIENT AND INTEGRATION IDENTITIES

Identity B.1. For integers $a, b \geq 0$, we have

$$\int_0^1 t^a (1-t)^b dt = \frac{a!b!}{(a+b+1)!}.$$

Proof. The formula is readily verified if $b = 0$. For $a \geq 0$ and $b > 0$, integration by parts yields

$$\int_0^1 t^a (1-t)^b dt = \frac{b}{a+1} \int_0^1 t^{a+1} (1-t)^{b-1} dt.$$

Repeated application of the above gives the desired formula. □

Identity B.2. Let $n \geq 0$ be an integer. One has the identity

$$\frac{(x+y)^n}{n+1} = \sum_{2i+j+k=n} \binom{n}{i, i, j, k} \frac{(i+j)!(i+k)!}{(n+1)!} x^{i+j} y^{i+k},$$

where, explicitly, the sum is taken over all triples $(i, j, k) \in \mathbb{N}^3$ satisfying $2i + j + k = n$.

Proof. Note that

$$\binom{n}{i, i, j, k} \frac{(i+j)!(i+k)!}{(n+1)!} = \frac{n!}{i!i!j!k!} \frac{(i+j)!(i+k)!}{(n+1)!} = \frac{1}{n+1} \binom{i+j}{i} \binom{i+k}{k}.$$

Thus, the identity of interest is equivalent to

$$(x+y)^n = \sum_{2i+j+k=n} \binom{i+j}{i} \binom{i+k}{k} x^{i+j} y^{i+k}.$$

Because both sides of the equation are homogeneous of degree n , it suffices to verify that

$$(x+1)^n = \sum_{2i+j+k=n} \binom{i+j}{i} \binom{i+k}{k} x^{i+j}. \quad (\star)$$

To prove the above identity, we need to show that the coefficient of x^a is the same on both sides for each $0 \leq a \leq n$. The coefficient of x^a on the right-hand side of (\star) is given by

$$\sum_{\substack{2i+j+k=n \\ i+j=a}} \binom{i+j}{i} \binom{i+k}{k} = \sum_{i+k=n-a} \binom{a}{i} \binom{i+k}{i} = \sum_i \binom{a}{i} \binom{n-a}{i}.$$

Thus, it suffices to prove that

$$\binom{n}{a} = \sum_i \binom{a}{i} \binom{n-a}{i}. \quad (\dagger)$$

To this end, note that

$$(1+X)^a(1+Y)^{n-a} = \sum_{i,j} \binom{a}{i} \binom{n-a}{j} X^i Y^j.$$

Substituting $Y = 1/X$ gives

$$(1+X)^a \left(1 + \frac{1}{X}\right)^{n-a} = \sum_{i,j} \binom{a}{i} \binom{n-a}{j} X^{i-j}.$$

Thus,

$$\frac{1}{X^{n-a}}(1+X)^n = \sum_{i,j} \binom{a}{i} \binom{n-a}{j} X^{i-j}.$$

Comparing the coefficient of X^0 on both sides gives us (\dagger) . □

Identity B.3. For integers $m, n \geq 0$, one has the identity

$$\sum_{k=0}^n \binom{n}{k} \frac{(-1)^k}{m+k+1} = \frac{m!n!}{(m+n+1)!}.$$

Proof. We note

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} \frac{(-1)^k}{m+k+1} &= \sum_{k=0}^n \binom{n}{k} (-1)^k \int_0^1 t^{m+k} dt \\ &= \int_0^1 t^m \cdot \sum_{k=0}^n \binom{n}{k} (-t)^k dt \\ &= \int_0^1 t^m (1-t)^n dt \\ &= \frac{m!n!}{(m+n+1)!}, \end{aligned}$$

where the last step uses Identity B.1. □

Identity B.4. For integers $a, b \geq 0$, we have

$$\int_0^{\pi/2} \cos^{2a}(\theta) \sin^{2b}(\theta) \sin(2\theta) d\theta = \frac{a!b!}{(a+b+1)!}.$$

Proof. The integrand can be rewritten as

$$\begin{aligned} \cos^{2a}(\theta) \sin^{2b}(\theta) \sin(2\theta) &= 2 \cos^{2a+1}(\theta) \sin^{2b+1}(\theta) \\ &= 2(\cos^2(\theta))^a (\sin(\theta))^{2b+1} \cos(\theta) \\ &= 2(1 - \sin^2(\theta))^a (\sin(\theta))^{2b+1} \cos(\theta). \end{aligned}$$

The substitution $u = \sin(\theta)$ gives us

$$\begin{aligned} \int_0^{\pi/2} \cos^{2a}(\theta) \sin^{2b}(\theta) \sin(2\theta) d\theta &= \int_0^1 2(1-u^2)^a u^{2b+1} du \\ &= \int_0^1 (1-u^2)^a (u^2)^b (2u du) \\ &= \int_0^1 (1-t)^a t^b dt. \end{aligned}$$

The desired identity now follows from Identity B.1. □

Identity B.5. For nonnegative integers a, b, c, d , we have

$$\int_{\mathrm{SU}_2(\mathbb{C})} u_{11}^a u_{12}^b u_{21}^c u_{22}^d = \begin{cases} (-1)^b \frac{a!b!}{(a+b+1)!} & \text{if } a = d \text{ and } b = c, \\ 0 & \text{else.} \end{cases}$$

Proof. We use the formula for the Haar measure on $\mathrm{SU}_2(\mathbb{C})$ from [6, Proposition 7.4.1]. Given a smooth function $f : \mathrm{SU}_2(\mathbb{C}) \rightarrow \mathbb{C}$, we have

$$\begin{aligned} \int_{\mathrm{SU}_2(\mathbb{C})} f &= \frac{1}{2\pi^2} \int_0^{\pi/2} \int_0^\pi \int_{-\pi}^\pi f \left(\begin{bmatrix} e^{i\psi} & \\ & e^{-i\psi} \end{bmatrix} \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} e^{i\varphi} & \\ & e^{-i\varphi} \end{bmatrix} \right) \sin(2\theta) d\psi d\varphi d\theta \\ &= \frac{1}{2\pi^2} \int_0^{\pi/2} \int_0^\pi \int_{-\pi}^\pi f \left(\begin{bmatrix} e^{i(\psi+\varphi)} \cos(\theta) & e^{i(\psi-\varphi)} \sin(\theta) \\ -e^{i(-\psi+\varphi)} \sin(\theta) & e^{i(-\psi-\varphi)} \cos(\theta) \end{bmatrix} \right) \sin(2\theta) d\psi d\varphi d\theta. \end{aligned}$$

Rewriting in terms of the above coordinates, we get

$$u_{11}^a u_{12}^b u_{21}^c u_{22}^d = (-1)^c \exp(i\psi(a+b-c-d)) \exp(i\varphi(a-b+c-d)) \cos^{a+d}(\theta) \sin^{b+c}(\theta).$$

We integrate using Fubini's theorem to obtain

$$\begin{aligned} &2\pi^2 \int_{\mathrm{SU}_2(\mathbb{C})} u_{11}^a u_{12}^b u_{21}^c u_{22}^d \\ &= (-1)^c \cdot \int_{-\pi}^\pi \exp(i\psi(a+b-c-d)) d\psi \cdot \int_0^\pi \exp(i\varphi(a-b+c-d)) d\varphi \\ &\quad \cdot \int_0^{\pi/2} \cos^{a+d}(\theta) \sin^{b+c}(\theta) \sin(2\theta) d\theta. \end{aligned}$$

For the first integral to be nonzero, we must have $a+b-c-d=0$. This implies that $a-b+c-d$ is even and hence must be zero if the second integral is to be nonzero. Solving these two equations simultaneously gives us $a=d$ and $b=c$. Assume now that these two equations hold.

We then have

$$\begin{aligned} & 2\pi^2 \int_{\mathrm{SU}_2(\mathbb{C})} u_{11}^a u_{12}^b u_{21}^c u_{22}^d \\ &= (-1)^b \cdot \int_{-\pi}^{\pi} 1 \, d\psi \cdot \int_0^{\pi} 1 \, d\varphi \cdot \int_0^{\pi/2} \cos^{2a}(\theta) \sin^{2b}(\theta) \sin(2\theta) \, d\theta \\ &= (-1)^b (2\pi^2) \cdot \frac{a!b!}{(a+b+1)!}, \end{aligned}$$

where the last equality follows from Identity B.4. □

ACKNOWLEDGEMENTS

The author was supported by NSF grants DMS 2101671 and DMS 2349623.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

ORCID

Aryaman Maithani  <https://orcid.org/0009-0002-8419-1483>

REFERENCES

1. B. Collins and P. Śniady, *Integration with respect to the Haar measure on unitary, orthogonal and symplectic group*, Comm. Math. Phys. **264** (2006), no. 3, 773–795.
2. C. De Concini and C. Procesi, *A characteristic free approach to invariant theory*, Adv. Math. **21** (1976), no. 3, 330–354.
3. H. Derksen and G. Kemper, *Computational invariant theory*, Encyclopaedia of Mathematical Sciences, vol. 130, enlarged ed., Springer, Heidelberg, 2015, xxii+366 pp. With two appendices by Vladimir L. Popov, and an addendum by Norbert A'Campo and Popov. Invariant Theory and Algebraic Transformation Groups, VIII.
4. J. Dieudonné, *Sur les groupes classiques*, Publ. Inst. Math. Univ. Strasbourg (N.S.) **1** (1945), iii+82, Hermann & Cie, Paris, 1948. Actualités Scientifiques et Industrielles, no. 1040. [Current Scientific and Industrial Topics].
5. J. Dieudonné, *Sur les générateurs des groupes classiques*, Summa Brasil. Math. **3** (1955), 149–179.
6. J. Faraut, *Analysis on Lie groups*, Cambridge Studies in Advanced Mathematics, vol. 110, Cambridge University Press, Cambridge, 2008, x+302 pp.
7. J. Fogarty, *Invariant theory*, W. A. Benjamin, Inc., New York, 1969, xvi+216 pp.
8. D. Glassbrenner, *The Cohen–Macaulay property and F-rationality in certain rings of invariants*, J. Algebra **176** (1995), no. 3, 824–860.
9. K. Goel, J. Jeffries, and A. K. Singh, *Local cohomology of modular invariant rings*. Transformation Groups (Mar. 2024).
10. T. Gorin and G. V. López, *Monomial integrals on the classical groups*, J. Math. Phys. **49** (2008), no. 1, 20.
11. W. J. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. (2) **102** (1975), no. 1, 67–83.
12. P. R. Halmos, *Measure theory*, D. Van Nostrand, New York, 1950, xi+304 pp.
13. M. Hashimoto, *Another proof of theorems of De Concini and Procesi*, J. Math. Kyoto Univ. **45** (2005), no. 4, 701–710.

14. M. Hochster, *Invariant theory of commutative rings*, Group actions on rings (Brunswick, Maine, 1984), Contemporary Mathematics, vol. 43, American Mathematical Society, Providence, RI, 1985, 161–179.
15. M. Hochster, J. Jeffries, V. Pandey, and A. K. Singh, *When are the natural embeddings of classical invariant rings pure?* Forum Math. Sigma **11** (2023), 43.
16. M. Hochster and J. L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Adv. Math. **13** (1974), 115–175.
17. K. C. Jeffries, *Rings of invariants, F -regularity, and local cohomology*, Ph.D. thesis, The University of Utah, Ann Arbor, MI, 2015, 55 pp.
18. M. Kohls, *Non-Cohen–Macaulay invariant rings of infinite groups*, J. Algebra **306** (2006), no. 2, 591–609.
19. H. Kraft, *Geometrische Methoden in der Invariantentheorie*, Aspects of Mathematics, vol. D1, Friedr. Vieweg & Sohn, Braunschweig, 1984, x+308 pp.
20. S. Lang, *Real and functional analysis*, Graduate Texts in Mathematics, vol. 142, 3rd ed., Springer, New York, 1993, xiv+580 pp.
21. D. Mumford, *Hilbert's fourteenth problem-the finite generation of subrings such as rings of invariants*, Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Northern Illinois Univ., De Kalb, Ill., 1974), Proc. Sympos. Pure Math., vol. XXVIII, American Mathematical Society, Providence, RI, 1976, pp. 431–444.
22. K. R. Nagarajan, *Groups acting on Noetherian rings*, Nieuw Arch. Wisk. (3) **16** (1968), 25–29.
23. M. Nagata, *On the fourteenth problem of Hilbert*, Proc. Internat. Congr. Math. 1958, Cambridge Univ. Press, New York, 1960, pp. 459–462.
24. E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1915), no. 1, 89–92.
25. O. T. O'Meara, *Symplectic groups*, Mathematical Surveys, vol. 16, American Mathematical Society, Providence, RI, 1978, xi+122 pp.
26. Z. Puchała and J. A. Miszczyk, *Symbolic integration with respect to the Haar measure on the unitary group*, Bull. Pol. Acad. Sci. Tech. Sci. **65** (2017), <https://journals.pan.pl/Content/105697/PDF/10.1515bpasts-2017-0003.pdf>
27. H. L. Royden, *Real analysis*, The Macmillan Company, New York, 1963, xvi+284 pp.
28. P. Scherk, *On the decomposition of orthogonalities into symmetries*, Proc. Amer. Math. Soc. **1** (1950), 481–491.
29. A. K. Singh, *Failure of F -purity and F -regularity in certain rings of invariants*, Illinois J. Math. **42** (1998), no. 3, 441–448.
30. L. Smith, *On alternating invariants and Hilbert ideals*, J. Algebra **280** (2004), no. 2, 488–499.
31. The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.8)*, <https://www.sagemath.org>, 2023.
32. H. Weyl, *The classical groups. Their invariants and representations*, Princeton University Press, Princeton, NJ, 1939, xii+302 pp.