Invariant Theory of Commutative Rings

Aryaman Maithani

August 13, 2024

Introduction

Notes I made for my talk at the commutative algebra seminar at IIT Bombay. Talk abstract:

> Given a group G acting on a ring R, we consider the subring R^G, the subring of elements fixed by G. It's a natural question to ask what "good" properties of R are inherited by R^G. Some of these questions were considered by Hilbert and Noether, and were a motivation to study noetherian rings. We will discuss some of these results.
> This talk should be accessible to someone who's done a first course in module theory.

§1. Group actions

Throughout the talk, k will denote an arbitrary field, R a commutative ring with unity, and G a group. An action of G on R is a group homomorphism $G \to \operatorname{Aut}(R)$. The fixed subring is defined as

$$R^G := \{r \in R : g(r) = r \text{ for all } g \in G\}.$$

Some natural questions to ask are:

Question 1.1. Are "good" properties of R inherited by R^G?
Some examples of properties: noetherian, domain, normal, PID, UFD, polynomial, regular, Gorenstein, Cohen-Macaulay, F-regular, etc.

Question 1.2. What can we say about the inclusion $R^G \hookrightarrow R$?
Is it integral? Module-finite? Algebra-finite? Split?
Recall that an inclusion of $\iota \colon R \hookrightarrow S$ is said to be split if it is split in the category of R-modules, i.e., if there an R-linear map $p \colon S \to R$ such that $p \circ \iota = \mathrm{id}_R$.

Example 1.3 (Symmetric group acting on the polynomial ring)**.**
S_n acts naturally on $R := k[x_1, \ldots, x_n]$ by permuting the variables.
We have $R^{S_n} = k[e_1, \ldots, e_n]$, where $e_1, \ldots, e_n$ are the elementary symmetric polynomials. In this case, the fixed subring is again a polynomial ring as the e_i are algebraically independent and the inclusion $R^{S_n} \hookrightarrow R$ is split[1], independent of characteristic.
This is also an integral extension since

$$(T - x_1) \cdots (T - x_n) \in R^{S_n}[T].$$

Observation 1.4. If $|G| < \infty$, then $R^G \hookrightarrow R$ is integral: every $r \in R$ satisfies the monic polynomial

$$\prod_{g \in G} (x - g(r)) \in R^G[x].$$

§2. Noetherian and Splitting

The answer to the invariant subring inheriting the property of being noetherian is "no" is general:

Example 2.1 (Nagarajan [Nag68])**.** Let $R := \mathbb{F}_2(a_1, a_2, \ldots)[\![x, y]\!]$ and $G := \mathbb{Z}/2$. There is an action of G on R such that R^G is not noetherian.

Note that in the above example, R is a really nice ring: a regular local ring. Note that the order of the group is not invertible in the ring.

Remark 2.2. The above also implies that $R^G \hookrightarrow R$ is not a module-finite extension.

This is due to the Eakin-Nagata theorem which states: if $R \hookrightarrow S$ is a module-finite extension of rings, then R is noetherian iff S is so.

Thus, Nagarajan's example 2.1 shows that $R^G \hookrightarrow R$ need not be algebra-finite either. (An algebra-finite integral extension is module-finite.)

Note that by Galois theory, $\mathrm{Frac}(R)^G \hookrightarrow \mathrm{Frac}(R)$ *is* a module-finite extension. A rank two extension, in fact.

[1] There are multiple ways of seeing this: One is the fact that $R \hookrightarrow S$ always splits if the extension is finite and R is a polynomial ring. The other is that R is a free R^{S_n}-module with a basis given by elements of the form $x_1^{<1} x_2^{<2} \cdots x_n^{<n}$.

Theorem 2.3. Let G be a finite group acting on a ring R containing $\frac{1}{|G|}$. Then,

$$R^G \hookrightarrow R$$

splits with a splitting being given as

$$\frac{1}{|G|}\sum_{g\in G} g(r) \mapsfrom r.$$

The above is called the Reynolds operator.

Consequently, for any ideal $I \subseteq R^G$, one has that

$$IR \cap R^G = I.$$

In particular, if R is noetherian, then so is R^G.

The above is not a necessary condition for splitting, as witnessed by Example 1.3.

Example 2.4. The alternating group $A_3 \leqslant S_3$ acts on $R := k[x, y, z]$ by permuting the variables. If $\operatorname{char}(k) \neq 2$, then $R^{A_3} = k[e_1, e_2, e_3, \Delta]$, where $\Delta := (x-y)(y-z)(z-x)$.

Note that $|A_3| = 3$ and thus, $R^{A_3} \hookrightarrow R$ splits if $\operatorname{char}(k) \neq 3$.

Claim. If $\operatorname{char}(k) = 3$, then $R^{A_3} \hookrightarrow R$ is *not* split.

Proof. Assume $\operatorname{char}(k) = 3$. It suffices to construct an ideal $I \subseteq R^{A_3}$ such that $IR \cap R^{A_3} \neq I$. To this end, consider $I := (e_1, e_2, e_3)R^{A_3}$. It is not difficult to check that $\Delta \notin I$.

We show that $\Delta \in IR$. In fact, we show that $\Delta \in (e_1, e_2)R$. First, note that

$$\begin{aligned}
(e_1,\ e_2)R &= (x+y+z,\ xy+(x+y)z)R \\
&= (x+y+z,\ xy-(x+y)^2)R \\
&= (x+y+z,\ (x+y)^2-xy)R \\
&= (x+y+z,\ x^2+xy+y^2)R && \Big\downarrow \operatorname{char}(k)=3 \\
&= (x+y+z,\ (x-y)^2)R.
\end{aligned}$$

Now, modulo $(e_1, e_2)R$, we note that

$$\begin{aligned}
\Delta &= (x-y)(y-z)(z-x) && \Big\downarrow z \equiv -(x+y) \\
&\equiv -(x-y)(2y+x)(2x+y) \\
&= (x-y)^3 \equiv 0. \qquad \square
\end{aligned}$$

Remark 2.5. It is known (cf. [Sin98]) that $R^{A_n} \hookrightarrow R$ splits precisely if $\operatorname{char}(k) \nmid |A_n|$.

These questions about finiteness were some forms of one of Hilbert's question (see Question 3.2). The following result is due to Emmy Noether, which helped motivate her development of noetherian rings.

Theorem 2.6 (Noether)**.** Let A be a noetherian ring, R a finitely generated A-algebra, and G a finite group acting on R via A-algebra automorphisms. Then, R^G is a finitely generated A-algebra and hence, noetherian.

Proof. This follows, for example, from [AM69, Proposition 7.8]: consider the tower of extensions $A \subseteq R^G \subseteq R$; the latter extension is integral as noted before. □

Of particular interest is the case when $A = k$ is a field, and $R = k[x_1, \ldots, x_n]$ is the polynomial algebra. In fact, even restricting to graded automorphisms of R is of considerable interest. Note that such an action is determined by the the images of the variables x_i, which must necessarily be mapped to (homogeneous) linear polynomials. This gives a natural identification

$$\mathrm{GL}_n(k) \cong \text{graded-}\mathrm{Aut}_k(R).$$

§3. Infinite groups

A subgroup $G \leqslant \mathrm{GL}_m(k)$ is called a linear algebraic group if G is closed in the Zariski topology, i.e., G is "cut out by polynomials". We can consider graded actions of G on $k[x_1, \ldots, x_n]$ by looking at homomorphisms $G \to \mathrm{GL}_n(k)$.[2] Such an action is called k-rational if the homomorphism is a morphism of varieties. Henceforth, if G is a linear algebraic group, then its actions will be assumed to be k-rational.

Example 3.1. $\mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$, $\mathrm{O}_n(k)$, and $\mathrm{Sp}_{2n}(k)$ are some examples of linear algebraic groups. In particular, the multiplicative group $k^\times \cong \mathrm{GL}_1(k)$ is a linear algebraic group. So is the additive group k via

$$k \cong \left\{ \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} : \alpha \in k \right\} \leqslant \mathrm{GL}_2(k).$$

Question 3.2 (Hilbert's 14th Problem)**.** If G is a linear algebraic group acting (rationally) on $k[x_1, \ldots, x_n] =: R$, is R^G a finitely generated k-algebra?

[2] Note that m and n may be different.

Answer. No. Nagata [Nag60] gave a (characteristic-independent) counterexample. The group was a product of copies of the additive group k. □

Similar to how requiring $|G|$ be invertible in R had solved the issue earlier, the corresponding analogue here is to consider the algebraic groups that are *linearly reductive*.[3] In particular, one has the following.

Theorem 3.3. If G is a linearly reductive group acting on a finitely generated k-algebra R, the ring R^G is finitely generated as a k-algebra. Moreover, the inclusion $R^G \hookrightarrow R$ splits.

Example 3.4. $\mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$, $\mathrm{O}_n(k)$, and $\mathrm{Sp}_{2n}(k)$ are linearly reductive in characteristic zero, but generally not in positive characteristic.

A linear algebraic group over $\mathbb{C}$ is linearly reductive precisely if it has a Zariski dense subgroup that is a compact real Lie group; average over the compact subgroup with respect to the Haar measure to obtain the splitting. Elements fixed by a (Zariski) dense subgroup are fixed by everything.

For concreteness, we now focus on a specific example. Let k be a field, $G \coloneqq \mathrm{SL}_2(k)$, and $R \coloneqq k[X_{2\times 3}]$. Here, R is a polynomial ring in six variables labeled x_{ij} for $1 \leqslant i \leqslant 2$ and $1 \leqslant j \leqslant 3$.
G acts on R, where the action is given by

$$M\colon X \mapsto MX.$$

By the above, we mean that $M \in G$ acts via the automorphism that maps x_{ij} to the (i,j)th entry of MX. For example, if $M = \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1/2 \end{smallmatrix}\right)$, then M acts via

$$\begin{aligned} x_{11} &\mapsto 2x_{11} + x_{21}, & x_{12} &\mapsto 2x_{12} + x_{22}, & x_{13} &\mapsto 2x_{13} + x_{23} \\ x_{21} &\mapsto \tfrac{1}{2}x_{21}, & x_{22} &\mapsto \tfrac{1}{2}x_{22}, & x_{23} &\mapsto \tfrac{1}{2}x_{23}. \end{aligned}$$

It is not difficult to check that the three 2×2 minors $\Delta_1, \Delta_2, \Delta_3$ of X are fixed by G. It also happens to be the case that these are algebraically independent, i.e., $k[\underline{\Delta}]$ is a polynomial ring.

Theorem 3.5. If k is infinite, then $R^G = k[\Delta_1, \Delta_2, \Delta_3]$.

[3] Loosely speaking, those l.a.g. G which have the following property: every inclusion of G-modules splits.

Now, if $\operatorname{char}(k) = 0$, then by the earlier remarks, we know that

$$k[\underline{\Delta}] \hookrightarrow k[X]$$

splits. In contrast, one has the following.

Theorem 3.6. If $\operatorname{char}(k) > 0$, then

$$k[\underline{\Delta}] \hookrightarrow k[X]$$

is *not* split. Note that the subring is also a polynomial ring.

Sketch. Let $R \coloneqq k[X]$, $S \coloneqq k[\underline{\Delta}]$, $I \coloneqq (\underline{\Delta})S$. We wish to show that $S \hookrightarrow R$ does not split.

One can check that $(\Delta_1\Delta_2\Delta_3)^{p-1} \in I^{[p]}R \setminus I^{[p]}$ showing that $I^{[p]}R \cap S \neq I^{[p]}$.

Alternately, it suffices to show that the local cohomology module $H^3_{IR}(R)$ vanishes. To do this, note that R/IR has an R-free resolution of length two which can be given the form

$$0 \to R \xrightarrow{\begin{pmatrix} x_{11} \\ x_{12} \\ x_{13} \end{pmatrix}} R^3 \xrightarrow{(\Delta_1 \; \Delta_2 \; \Delta_3)} R \to 0.$$

By flatness of Frobenius, we see that each $R/I^{[p^e]}R$ has a free resolution of length two. Thus, $H^3_{IR}(R) = \underrightarrow{\operatorname{colim}}_e \operatorname{Ext}^3_R(R/I^{[p^e]}R, R) = 0$. □

Remark 3.7. A more general fact is true: Consider the analogous action $SL_t(k) \curvearrowright k[X_{t\times n}]$ with $t \leqslant n$. If k is infinite, then the fixed subring is precisely the k-algebra generated by the $t \times t$ minors of X (this may not be a polynomial ring).

This ring R^G is of independent interest since $\operatorname{Proj}(S^G) = \operatorname{Grass}(t, n)$ is the Grassmannian variety.

In characteristic zero, the inclusion $R^G \hookrightarrow R$ is always split. In positive characteristic, the inclusion splits precisely if $t \in \{1, n\}$ as was shown in the recent work [Hoc+23].

The above has an interesting consequence: Let $\pi \colon \mathbb{Q}[X] \twoheadrightarrow \mathbb{Q}[\underline{\Delta}]$ be a $\mathbb{Q}[\underline{\Delta}]$-linear splitting. Note that the set of monomials acts as a $\mathbb{Q}[\underline{\Delta}]$-generating set for $\mathbb{Q}[X]$. For every prime $p > 0$, there is some monomial X^α such that p shows in the denominator of $\pi(X^\alpha)$; for if not, then we could go modulo p and obtain a splitting for $\mathbb{F}_p[\underline{\Delta}] \hookrightarrow \mathbb{F}_p[X]$.

$SL_2(\mathbb{C})$ is a small enough example where I could explicitly work out—to an extent—the splitting by integrating with respect to the Haar measure.

As before, let $R \coloneqq \mathbb{C}\left[\begin{smallmatrix} a & b & c \\ s & t & u \end{smallmatrix}\right]$.[4] Consider the larger polynomial ring $S \coloneqq R[z, w, \overline{z}, \overline{w}]$. Even though we use suggestive notation, we intend for S to be a polynomial ring over R with $z, w, \overline{z}, \overline{w}$ being indeterminates.

[4] R could more generally be of the form $R[X_{2\times n}]$. We use the letters $a, \ldots$ for ease of writing.

Let $\varphi \colon R \to S$ be the k-algebra map defined by

$$\begin{bmatrix} a & b & c \\ s & t & u \end{bmatrix} \mapsto \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix} \begin{bmatrix} a & b & c \\ s & t & u \end{bmatrix}$$

For example, $\varphi(a) = az - s\overline{w}$ and $\varphi(t) = bw + t\overline{z}$.

Let $\mathbb{I} \colon S \to R$ be the R-linear map defined as following:

$$(z\overline{z})^m (w\overline{w})^n \mapsto \frac{m!n!}{(m+n+1)!}.$$

Monomials in S not of the above form are mapped to 0.
For reasons to be explained later, $\mathbb{I}$ is to be thought of the *integration* operator.

Then, the splitting $S \to R$ is given by

$$\pi = \mathbb{I} \circ \varphi.$$

Example 3.8. We have

$$\varphi(at) = abzw + atz\overline{z} - bsw\overline{w} - st\overline{zw}.$$

Integrating the above gives us

$$\pi(at) = 0 + at \cdot \frac{1!0!}{2!} - bs \cdot \frac{0!1!}{2!} + 0 = \frac{at - bc}{2}.$$

Thus, $\pi(at) = \frac{\Delta_1}{2}$.

With some more effort, one can show that

$$\pi\left((at)^n\right) = \frac{1}{n+1} \Delta_1^n.$$

Thus, every positive integer—and hence, every prime—shows up in the denominator.

The above description of the splitting follows essentially from the following: SU_2 is a Zariski dense subgroup of SL_2 that is a real Lie group. We have the paramaterisation

$$SU_2 = \left\{ \begin{bmatrix} z & -\overline{w} \\ w & z \end{bmatrix} : z, w \in \mathbb{C},\ |z|^2 + |w|^2 = 1 \right\}.$$

Monomials in these coordinate functions can be integrated as

$$\int_{SU_2} z^a \overline{z}^b w^c \overline{w}^d \, dSU_2 = \mathbb{I}(z^a \overline{z}^b w^c \overline{w}^d),$$

where dSU_2 is the Haar measure on SU_2. (Note that the monomial on the left is being treated as a complex-valued function on the Lie group SU_2, whereas the monomial on the right is an element in the formal polynomial ring S.)

§4. Back to Finite Groups

We now return to the finite group setup.

Setup.

k is a field, $R := k[x_1, \ldots, x_n]$, G is a finite subgroup of $GL_n(k)$ acting on R in the natural way.

The case when $\mathrm{char}(k)$ divides $|G|$ is called the modular case.

Example 4.1. Consider $R := \mathbb{C}[x, y]$ and

$$G = \left\langle \begin{bmatrix} -1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ & -1 \end{bmatrix} \right\rangle.$$

Then,

$$R^G = \mathbb{C}[x^2, y^2],$$

which is again a polynomial ring.

By Theorem 2.6, we know in general that the invariant subring in this setup is a finitely generated k-algebra. A few relevant questions now are as follows.

Question 4.2. Given G, what are (minimal) generators of R^G as a k-algebra? What are the relations between these generators? What is the largest degree of such a generator?

Theorem 4.3 (Noether's bound)**.** If $\mathrm{char}(k) \nmid |G|$, then R^G is generated (as a k-algebra) by the elements of degree at most $|G|$.

In 1915, Noether had proven the above in the chase that $\mathrm{char}(k) \nmid |G|!$ (the factorial). For many years, the result as stated above was not known (called "Noether's gap"). It was finally solved independently by Fleischmann in 2000 and Fogarty in 2001. These proofs were substantially simplified by Benson.

Example 4.4 (Noether's bound failing in the modular case)**.**
Let $R := \mathbb{F}_2[x_1, x_2, x_3, y_1, y_2, y_3]$, and σ be the order two automorphism given by $x_i \leftrightarrow y_i$. Then, $R^{\langle \sigma \rangle}$ needs a generator in degree three. Specifically, the invariant

$$x_1x_2x_3 + y_1y_2y_3$$

is not in the algebra generated by the invariants of degree $\leqslant 2$.

As it happens, this subring is not Cohen-Macaulay.

Noether's bound gives a naïve method for computing generators for R^G in the nonmodular case: take the set of all monomials of degree $\leqslant |G|$ and apply the Reynolds operator. In fact, one can be more efficient by making use of the Molien series which describes the Hilbert series of the invariant ring as

$$H(R^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - tg)}.$$

As written, the above strictly only makes sense in characteristic zero. (Indeed, the left side is an element of $\mathbb{Q}(t)$ or $\mathbb{Z}[\![t]\!]$ whereas the right is an element of $k(t)$.) However, it can be made sense of in the positive characteristic (nonmodular) case by the use of *Brauer lifts*.

Interestingly, the following equality holds in the modular and nonmodular case both:

$$\lim_{t \to 1} (1-t)^n H(R^G, t) = \frac{1}{|G|}.$$

We now look at some homological properties.

Example 4.5. Consider $R \coloneqq \mathbb{C}[x, y]$, and

$$\sigma = \begin{bmatrix} -1 & \\ & -1 \end{bmatrix} : \begin{cases} x \mapsto -x, \\ y \mapsto -y. \end{cases}$$

Then, $R^{\langle \sigma \rangle} = \mathbb{C}[x^2, xy, y^2]$. Thus, being a UFD is not inherited by the invariant subring.

More generally, if

$$\sigma = \begin{bmatrix} \zeta & \\ & \zeta \end{bmatrix}, \qquad \text{where } \zeta \coloneqq \exp\left(\frac{2\pi\imath}{d}\right),$$

then $R^{\langle \sigma \rangle} = R^{(d)} = \mathbb{C}[x^d, x^{d-1}y, \ldots, xy^{d-1}, y^d]$ is the d-th Veronese of R.

These subrings are all Cohen-Macaulay.

Remark 4.6. If $|G|^{-1} \in k$, then R^G is Cohen-Macaulay since $R^G \hookrightarrow R$ is a finite split extension and R is Cohen-Macaulay.

Recall that an element $g \in GL_n(k)$ is called a pseudoreflection if $\operatorname{rank}(g - I) = 1$.

Theorem 4.7 (Watanabe)**.** Suppose $\mathrm{char}(k)$ and $|G|$ are coprime. Then,

$$G \leqslant \mathrm{SL}_n(k) \quad \Rightarrow \quad k[x_1, \ldots, x_n]^G \text{ is Gorenstein.}$$

If G contains no psuedoreflections, then the converse holds as well.

> **Exercise 4.8.** Using the above, check that if $n \geqslant 2$, then
>
> $$\mathbb{C}[x_1, \ldots, x_n]^{(d)} \text{ is Gorenstein} \quad \Leftrightarrow \quad d \mid n.$$
>
> The above gives a family of rings which are Cohen-Macaulay but not Gorenstein.

Theorem 4.9 (Chevalley-Shephard-Todd)**.** Suppose $\mathrm{char}(k)$ and $|G|$ are coprime. Then,

$$R^G \text{ is a polynomial ring} \quad \Leftrightarrow \quad G \text{ is generated by pseudoreflections.}$$

The case of $k = \mathbb{C}$ was first proved by Shephard and Todd who gave a case-by-case proof. Soon afterwards, Chevalley gave a uniform proof. The general proof in the nonmodular setup was given by Serre.

References

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, pp. ix+128.

[Hoc+23] Melvin Hochster, Jack Jeffries, Vaibhav Pandey, and Anurag K. Singh. “When are the natural embeddings of classical invariant rings pure?” In: *Forum Math. Sigma* 11 (2023), Paper No. e67, 43.

[Nag60] Masayoshi Nagata. “On the fourteenth problem of Hilbert”. In: *Proc. Internat. Congress Math. 1958*. Cambridge Univ. Press, New York, 1960, pp. 459–462.

[Nag68] K. R. Nagarajan. “Groups acting on Noetherian rings”. In: *Nieuw Arch. Wisk. (3)* 16 (1968), pp. 25–29.

[Sin98] Anurag K. Singh. “Failure of F-purity and F-regularity in certain rings of invariants”. In: *Illinois J. Math.* 42.3 (1998), pp. 441–448.