Why $\operatorname{Ring}(A,k)/G$ injects into $\operatorname{Ring}\left(A^G,k\right)$

Darij Grinberg

January 30, 2020

I shall use the following notations:

- If G is a group, and if S is a G-set, then S^G shall denote the set of all fixed points under G in S. (In other words, $S^G = \{s \in S \mid gs = s \text{ for all } g \in G\}$.)
- If G is a group, and if S is a G-set, then S/G shall denote the set of all G-orbits on S. (In other words, $S/G = \{Gs \mid s \in S\}$.)
- If U and V are two rings, then $\operatorname{Ring}(U,V)$ denotes the set of all ring homomorphisms from U to V.

The crux of [KucSch16, Lemma 4.9] is the following elementary fact:

Proposition 0.1. Let A be a commutative ring. Let G be a finite group acting on A by ring automorphisms. Let k be an integral domain. Notice that $\operatorname{Ring}(A,k)$ becomes a G-set in an obvious way (namely, by setting $(gx)(a) = x\left(g^{-1}a\right)$ for all $g \in G$, $x \in \operatorname{Ring}(A,k)$ and $a \in A$). Then, the map

$$\operatorname{Ring}(A,k)/G \to \operatorname{Ring}\left(A^G,k\right),$$
$$Gx \mapsto x\mid_{A^G}$$

is injective.

In other words, this says that if two ring homomorphisms $x : A \to k$ and $y : A \to k$ are identical on the invariant ring A^G (that is, we have $x\mid_{A^G} = y\mid_{A^G}$), then x and y are in the same G-orbit on $\operatorname{Ring}(A,k)$.

I shall give an elementary proof of Proposition 0.1 (using nothing but Viete's formulas and basic properties of polynomial rings). First, let me prove a lemma:

Lemma 0.2. Let A be a commutative ring. Let G be a finite group acting on A by ring automorphisms. Let k be an integral domain. Let x and y be two elements of Ring (A,k) such that $x\mid_{A^G} = y\mid_{A^G}$. Let $a \in A$. Then, there exists some $g \in G$ such that $x(a) = y(ga)$.

Proof of Lemma 0.2. If S is a finite set, if R is a commutative ring, if $(b_s)_{s\in S} \in R^S$ is a family of elements of R, and if $\ell \in \mathbb{N}$, then we shall let $e_\ell\left((b_s)_{s\in S}\right)$ denote the ℓ-th elementary symmetric polynomial of the elements b_s (with $s \in S$). Explicitly, it is given by

$$e_\ell\left((b_s)_{s\in S}\right) = \sum_{\substack{T\subseteq S;\\ |T|=\ell}} \prod_{t\in T} b_t.$$

For example,

$$e_0\left((b_s)_{s\in S}\right) = 1 \qquad \text{and} \qquad e_1\left((b_s)_{s\in S}\right) = \sum_{s\in S} b_s$$

$$\text{and} \qquad e_{|S|}\left((b_s)_{s\in S}\right) = \prod_{s\in S} b_s.$$

The following fact is a form of Viete's relations:

> *Fact 1:* Let S be a finite set. Let R be a commutative ring. Let $(b_s)_{s\in S} \in R^S$ be a family of elements of R. Let $t \in R$. Then,
>
> $$\prod_{s\in S}(t-b_s) = \sum_{\ell=0}^{|S|} t^{|S|-\ell}(-1)^\ell e_\ell\left((b_s)_{s\in S}\right).$$

(Fact 1 follows easily by expanding the product $\prod_{s\in S}(t-b_s)$ and collecting like powers of t.)

Now, let us return to the proof of Lemma 0.2. Fix $\ell \in \mathbb{N}$. Set $\varepsilon_\ell = e_\ell\left((ga)_{g\in G}\right) \in A$.

Each element of the group G merely permutes the elements of the family $(ga)_{g\in G}$. Thus, the element $e_\ell\left((ga)_{g\in G}\right)$ is invariant under G (being defined as a symmetric polynomial in this family), and thus lies in A^G. Thus, $e_\ell\left((ga)_{g\in G}\right) \in A^G$, so that $\varepsilon_\ell = e_\ell\left((ga)_{g\in G}\right) \in A^G$. Hence,

$$x(\varepsilon_\ell) = \underbrace{(x\mid_{A^G})}_{=y\mid_{A^G}}(\varepsilon_\ell) = (y\mid_{A^G})(\varepsilon_\ell) = y(\varepsilon_\ell). \tag{1}$$

But from $\varepsilon_\ell = e_\ell\left((ga)_{g\in G}\right)$, we obtain

$$x(\varepsilon_\ell) = x\left(e_\ell\left((ga)_{g\in G}\right)\right) = e_\ell\left((x(ga))_{g\in G}\right) \tag{2}$$

(since x is a ring homomorphism while e_ℓ is a natural transformation) and similarly

$$y(\varepsilon_\ell) = e_\ell\left((y(ga))_{g\in G}\right). \tag{3}$$

Hence, (2) yields

$$e_\ell\left((x(ga))_{g\in G}\right) = x(\varepsilon_\ell) = y(\varepsilon_\ell) = e_\ell\left((y(ga))_{g\in G}\right). \tag{4}$$

Now, forget that we fixed ℓ. We thus have shown that (4) holds for every $\ell \in \mathbb{N}$. In the polynomial ring $k[t]$, we have

$$\prod_{g\in G}(t - x(ga)) = \sum_{\ell=0}^{|G|} t^{|G|-\ell}(-1)^\ell e_\ell\left((x(ga))_{g\in G}\right) \tag{5}$$

(by Fact 1, applied to $R = k[t]$ and $S = G$ and $(b_s)_{s\in S} = (x(ga))_{g\in G}$) and similarly

$$\prod_{g\in G}(t - y(ga)) = \sum_{\ell=0}^{|G|} t^{|G|-\ell}(-1)^\ell e_\ell\left((y(ga))_{g\in G}\right). \tag{6}$$

From (4), we see that the right hand sides of (5) and (6) are equal. Hence, so are the left hand sides. In other words,

$$\prod_{g\in G}(t - x(ga)) = \prod_{g\in G}(t - y(ga))$$

in $k[t]$. If we evaluate both sides of this equality at $t = x(a)$, we obtain

$$\prod_{g\in G}(x(a) - x(ga)) = \prod_{g\in G}(x(a) - y(ga)). \tag{7}$$

The factor of the product $\prod_{g\in G}(x(a) - x(ga))$ for $g = 1$ is 0. Thus, the whole product is 0. In other words, the left hand side of (7) is 0. Hence, so is the right hand side. In other words, $\prod_{g\in G}(x(a) - y(ga)) = 0$. Since k is an integral domain, this shows that there exists some $g \in G$ such that $x(a) - y(ga) = 0$. In other words, there exists some $g \in G$ such that $x(a) = y(ga)$. Lemma 0.2 is proven. □

Proof of Proposition 0.1. We must show that if x and y are two elements of Ring (A, k) such that $x\mid_{A^G} = y\mid_{A^G}$, then $Gx = Gy$.

Indeed, assume the contrary. Then, there exist two elements x and y of Ring (A, k) such that $x\mid_{A^G} = y\mid_{A^G}$ but $Gx \neq Gy$. Consider these x and y. From $Gx \neq Gy$, we obtain $x \notin Gy$. Hence, for every $g \in G$, we have $x \neq gy$. Hence, for every $g \in G$, there exists some $a_g \in A$ such that $x(a_g) \neq (gy)(a_g)$. Consider this a_g.

For each $g \in G$, introduce a new indeterminate s_g. For each commutative ring B, we let $\widetilde{B}$ denote the polynomial ring $B\left[s_g \mid g \in G\right]$ in all these indeterminates.

The polynomial ring $\widetilde{k} = k\left[s_g \mid g \in G\right]$ is an integral domain (since k is an integral domain). The polynomial ring $\widetilde{A} = A\left[s_g \mid g \in G\right]$ is equipped with a G-action by automorphisms: namely, we let G act on the coefficients (that is, the inclusion $A \to \widetilde{A}$ should be G-equivariant), while leaving all indeterminates s_g unchanged (that is, we have $hs_g = s_g$ for all $g, h \in G$; not $hs_g = s_{hg}$).

Thus, a polynomial $f \in \widetilde{A} = A\left[s_g \mid g \in G\right]$ is a fixed point under G if and only if all its coefficients are fixed points under G. In other words, $\widetilde{A}^G = A^G\left[s_g \mid g \in G\right]$.

Define an element a of $\widetilde{A}$ by $a = \sum\limits_{h \in G} a_h s_h$.

Any ring homomorphism $f : A \to k$ canonically induces a ring homomorphism $\widetilde{f}$ from $\widetilde{A} = A\left[s_g \mid g \in G\right]$ to $\widetilde{k} = k\left[s_g \mid g \in G\right]$ which homomorphism acts as f on the coefficients (that is, $\widetilde{f}(\alpha) = f(\alpha)$ for each $\alpha \in k$) while leaving the indeterminates s_g unchanged (that is, $\widetilde{f}\left(s_g\right) = s_g$ for each $g \in G$). Thus, in particular, the two ring homomorphisms x and y from A to k canonically induce two ring homomorphisms $\widetilde{x}$ and $\widetilde{y}$ from $\widetilde{A} = A\left[s_g \mid g \in G\right]$ to $\widetilde{k} = k\left[s_g \mid g \in G\right]$ (which homomorphisms act as x and y (respectively) on the coefficients while leaving the indeterminates unchanged). These new ring homomorphisms $\widetilde{x}$ and $\widetilde{y}$ have the property that

$$\widetilde{x}\mid_{A^G\left[s_g \mid g \in G\right]} = \widetilde{y}\mid_{A^G\left[s_g \mid g \in G\right]}$$

(since $x\mid_{A^G} = y\mid_{A^G}$ and since $\widetilde{x}\left(s_g\right) = s_g = \widetilde{y}\left(s_g\right)$ for each $g \in G$). This rewrites as

$$\widetilde{x}\mid_{\widetilde{A}^G} = \widetilde{y}\mid_{\widetilde{A}^G}$$

(since $\widetilde{A}^G = A^G\left[s_g \mid g \in G\right]$). Hence, Lemma 0.2 (applied to $\widetilde{A}$, $\widetilde{k}$, $\widetilde{x}$ and $\widetilde{y}$ instead of A, k, x and y) shows that there exists some $g \in G$ such that $\widetilde{x}(a) = \widetilde{y}(ga)$. Consider this g.

From $a = \sum\limits_{h \in G} a_h s_h$, we obtain

$$\widetilde{x}(a) = \widetilde{x}\left(\sum_{h \in G} a_h s_h\right) = \sum_{h \in G} x\left(a_h\right) s_h \tag{8}$$

(by the definition of $\widetilde{x}$), but also

$$ga = g \sum_{h \in G} a_h s_h = \sum_{h \in G} g a_h s_h.$$

Applying the map $\widetilde{y}$ to the latter equality, we find

$$\widetilde{y}(ga) = \widetilde{y}\left(\sum_{h \in G} g a_h s_h\right) = \sum_{h \in G} y\left(g a_h\right) s_h \qquad \text{(by the definition of } \widetilde{y}\text{)}.$$

Hence, (8) yields

$$\sum_{h \in G} x\left(a_h\right) s_h = \widetilde{x}(a) = \widetilde{y}(ga) = \sum_{h \in G} y\left(g a_h\right) s_h.$$

Comparing coefficients before s_h in this equality, we conclude that

$$x(a_h) = y(ga_h) \qquad \text{for all } h \in G. \tag{9}$$

Applying this to $h = g^{-1}$, we find $x\left(a_{g^{-1}}\right) = y\left(ga_{g^{-1}}\right)$. But the definition of $a_{g^{-1}}$ yields $x\left(a_{g^{-1}}\right) \neq (g^{-1}y)\left(a_{g^{-1}}\right) = y\left(\underbrace{\left(g^{-1}\right)^{-1}}_{=g} a_{g^{-1}}\right) = y\left(ga_{g^{-1}}\right)$, which contradicts $x\left(a_{g^{-1}}\right) = y\left(ga_{g^{-1}}\right)$. This contradiction completes our proof. □

References

[KucSch16] Robert A. Kucharczyk, Peter Scholze, *Topological realisations of absolute Galois groups*, arXiv:1609.04717v2.