Emmy Noether's Theorem on the Finite Generation of Invariants

Marin Genov

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences

Algebra & Logic Seminar, 13. Oct 2023

Outline

Introduction

Problem Setting

Given:

- K a field;
- V a K-vector space, $\dim_K V = n < \infty$;
- G a group with $G \curvearrowright V$;

Then:

- $G \curvearrowright V \Leftrightarrow \rho\colon G \to \mathrm{GL}(V)$.
- $G \curvearrowright V$ induces $G \curvearrowright V^*$ via
$$\forall\, \lambda \in V^*\ \forall\, v \in V\colon (g \cdot \lambda)(v) := \lambda(g^{-1} \cdot v).$$
- $G \curvearrowright V^*$ extends to $G \curvearrowright \mathcal{O}(V) = \mathrm{Sym}(V^*) = K[V^*]$ via
$$(g \cdot F)(v) := F(g^{-1} \cdot v).$$
- $x_1, \ldots, x_n \in V^*$ dual basis $\Rightarrow \mathcal{O}(V) = K[x_1, \ldots, x_n]$, hence
$$G \curvearrowright K[x_1, \ldots, x_n]$$
$$g \cdot P(x_1, \ldots, x_n) = P(g \cdot x_1, \ldots, g \cdot x_n).$$
- In other words, $G \leq \mathrm{Aut}_K(K[x_1, \ldots, x_n])$ acting *linearly*.

One wants to understand $K[x_1, \ldots, x_n]^G$.

Very Brief History

- Originated in the 19th century with the work of Boole and Cayley on the invariance of algebraic forms under linear transformations.
- Felix Klein's work (19th century) on the invariant rings of finite group actions on $\mathbb{C}^2$ lead later to the ADE classification (Arnold,70s) of Du Val singularities (Du Val,30s) (nowadays understood in the framework of McKay correspondence,80s).
- Hilbert discovered the eponymous **Basissatz**, **Nullstellensatz**, and **Syzygy Theorem** while pursuing Invariant Theory.
- Hilbert was mainly interested in the invariants of continuous groups (e.g. GL, SL), whereas Emmy Noether was more interested in the *invariants of finite groups*.

This talk is about a theorem of Emmy Noether on $K[x_1, \ldots, x_n]^G$ (slightly generalized).

The Original Proof (Slightly Modified)

Elementary Symmetric Polynomials & Newton Functions

Fix $R \in \text{CRing}$ with $R \supseteq \mathbb{Q}$ and $n \in \mathbb{N}$.

In $R[x_1, \ldots, x_n]$ one defines:

Definition (Elementary Symmetric Polynomials)

$$e_0(x_1, \ldots, x_n) \coloneqq 1$$

$$e_k(x_1, \ldots, x_n) \coloneqq \sum_{1 \leq j_1 < \cdots < j_k \leq n} x_{j_1} \ldots x_{j_k},\ 1 \leq k \leq n$$

and

Definition (Power Sums / Newton Functions)

$$p_k(x_1, \ldots, x_n) \coloneqq \sum_{i=1}^{n} x_i^k,\ k \in \mathbb{N}.$$

Newton's Identities

Proposition (Girard-Newton,1629,1666)

We have

$$ke_k(x_1, \ldots, x_n) = \sum_{i=1}^{k} (-1)^{i-1} p_i(x_1, \ldots, x_n) e_{k-i}(x_1, \ldots, x_n)$$

for all $1 \leq k \leq n$. *(As written, already true in characteristic 0.)*

$\Rightarrow e_k$ can be expressed via p_i recursively.

Example

$$e_1 = p_1$$
$$e_2 = \frac{1}{2}(p_1^2 - p_2)$$
$$e_3 = \frac{1}{6}(p_1^3 - 3p_1p_2 + p_3) \text{ etc.}$$

A Familiar Example of Invariants

$\mathfrak{S}_n \curvearrowright R[x_1, \dots, x_n]$ via permutation of the variables.

Theorem (Fundamental Theorem of Symmetric Polynomials)

$$R[x_1, \dots, x_n]^{\mathfrak{S}_n} = R[e_1, \dots, e_n]$$

Corollary

$$R[x_1, \dots, x_n]^{\mathfrak{S}_n} = R[p_1, \dots, p_n]$$

In particular: $\forall\, N > n \colon p_N \in R[p_1, \dots, p_n]$.

A Lemma

Notation:

- $R \in$ CRing with $R \supseteq \mathbb{Q}$;
- $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$ multi-index, $|\alpha| = \alpha_1 + \dots + \alpha_n$;
- $G \leq \mathrm{Aut}_R(R[x_1, \dots, x_n])$ finite, e.g. $G = \{g_1, \dots, g_m\}$;

Definition (Generic Invariants)

$$F_\alpha \coloneqq \sum_{g \in G} g \cdot (x_1^{\alpha_1} \dots x_n^{\alpha_n}) \stackrel{\text{def}}{=} \sum_{g \in G} (g \cdot x_1)^{\alpha_1} \dots (g \cdot x_n)^{\alpha_n}.$$

Lemma

$$\forall\, \beta \in \mathbb{N}_0^n \colon F_\beta \in R[\{F_\alpha : |\alpha| \leq m\}].$$

Remark

G is not assumed to act linearly.

Proof of the Lemma

Proof.

(i) $G \curvearrowright R[t_1, \ldots, t_n, x_1, \ldots, x_n]$ via $g \cdot t_i = t_i$, $1 \leq i \leq n$.

(ii) Define $\lambda := t_1 x_1 + \cdots + t_n x_n \in R[t_1, \ldots, t_n, x_1, \ldots, x_n]$.

(iii) Put $P_k := p_k(g_1 \cdot \lambda, \ldots, g_m \cdot \lambda)$, $k \in \mathbb{N}$. Then:

$$P_k \stackrel{\text{def}}{=} \sum_{g \in G} g \cdot (t_1 x_1 + \cdots + t_n x_n)^k =$$

$$= \sum_{g \in G} g \cdot \sum_{|\beta|=k} \frac{k!}{\beta_1! \ldots \beta_n!} t_1^{\beta_1} \ldots t_n^{\beta_n} x_1^{\beta_1} \ldots x_n^{\beta_n} =$$

$$= \sum_{|\beta|=k} \frac{k!}{\beta_1! \ldots \beta_n!} t_1^{\beta_1} \ldots t_n^{\beta_n} F_\beta, \ k \in \mathbb{N}.$$

(iv) $\forall\, k\colon P_k \in R[P_1, \ldots, P_m] \subseteq R[\{t_i\}_{1 \leq i \leq n}, \{F_\alpha : |\alpha| \leq m\}]$.

(v) Thus $\forall\, |\beta| > m\colon F_\beta$ is a polynomial in F_α-s with $|\alpha| \leq m$.

□

Emmy Noether's Theorem

Theorem (E. Noether, Erlangen, 1915)

Let $G \leq \mathrm{Aut}_R(R[x_1, \ldots, x_n])$ with $|G| < \infty$. Then $R[x_1, \ldots, x_n]^G$ is generated by elements of the form F_α, $|\alpha| \leq |G|$. In particular, if the action is linear, then $R[x_1, \ldots, x_n]^G$ is f.g. by elements of degree $\leq |G|$.

Proof.

Let $F = \sum_\beta c_\beta x_1^{\beta_1} \ldots x_n^{\beta_n} \in R[x_1, \ldots, x_n]^G$. Then

$$F = \frac{1}{|G|} \sum_{g \in G} g \cdot F = \frac{1}{|G|} \sum_{g \in G} \sum_\beta c_\beta g \cdot (x_1^{\beta_1} \ldots x_n^{\beta_n}) =$$

$$= \frac{1}{|G|} \sum_\beta c_\beta \sum_{g \in G} g \cdot (x_1^{\beta_1} \ldots x_n^{\beta_n}) = \frac{1}{|G|} \sum_\beta c_\beta F_\beta$$

□

Second Proof by Commutative Algebra

Two Facts from Commutative Algebra

Let $A, B, C \in \mathsf{CRing}$.

Proposition

Let $A \xrightarrow{\varphi} B$ be a morphism of rings. We have:

$$\varphi \text{ integral and of finite type} \Leftrightarrow \varphi \text{ finite.}$$

Lemma (Artin-Tate)

Let $A \subseteq B \subseteq C$ be ring extensions such that:

(i) *A is Noetherian;*

(ii) *C is a finitely generated A-algebra (i.e. of finite type over A);*

(iii) *C is a finite B-module ($\Leftrightarrow B \subseteq C$ integral).*

Then B too is a finitely generated A-algebra.

Integrality over R^G

Recall: $\prod_{k=1}^{n}(t - x_k) = \sum_{k=0}^{n}(-1)^{n-k}e_{n-k}(x_1, \ldots, x_n)t^k$

Now fix:

- $R \in$ CRing;
- $G := \{g_1, \ldots, g_n\} \curvearrowright R$, i.e. $G \leq \mathrm{Aut}(R)$ finite;
- For $\alpha \in R$ denote $\alpha_k := g_k \cdot \alpha$, $1 \leq k \leq n$.

Lemma

Every $\alpha \in R$ is integral over $R[e_1(\alpha_1, \ldots, \alpha_n), \ldots, e_n(\alpha_1, \ldots, \alpha_n)]$. In particular, $R \supseteq R^G$ is an integral extension.

Proof.

Consider $P_\alpha(t) := \prod_{k=1}^{n}(t - \alpha_k)$, which is monic and of degree $n = |G|$. □

Emmy Noether's Theorem

Theorem

Given:

(i) A *a Noetherian ring;*

(ii) $B \supseteq A$ *a finitely generated* A*-algebra;*

(iii) $G \leq \mathrm{Aut}_A(B)$ **finite** *subgroup;*

Then B^G *too is a finitely generated* A*-algebra.*

Proof.

(i) B f.g. A-algebra $\Rightarrow B$ f.g. B^G-algebra.

(ii) $B \supseteq B^G$ integral (by prev. Lemma) $\Rightarrow B$ finite B^G-module.

$$\Rightarrow A \subseteq B^G \subseteq B \text{ is as in Artin-Tate (since } A \text{ Noetherian).}$$

$$\Rightarrow B^G \text{ is a f.g. } A\text{-algebra.}$$

□

An Example: $\mathbb{C}[x, y]^{D_{2n}}$

The Action of D_{2n}

$D_{2n} = \langle \rho, \sigma \mid \rho^n = \sigma^2 = 1, \sigma\rho\sigma = \rho^{n-1} \rangle$ - the dihedral group of order $2n$ (symmetry group of the regular n-gon), $n \geq 3$.

$D_{2n} \curvearrowright \mathbb{R}^2 \cong \mathbb{C}$ via the rotation ρ of a vector (x, y) by $2\pi/n$ and the relfection σ of (x, y) with respect to the x-axis.

$\Rightarrow$ linear action of D_{2n} on the pair of functionals (x, y).

Want to determine $\mathbb{C}[x, y]^{D_{2n}}$.

Ansatz:

- $z := x + iy$, $\bar{z} := x - iy \Rightarrow \mathbb{C}[x, y] = \mathbb{C}[z, \bar{z}]$.
- Hence $\mathbb{C}[x, y]^{D_{2n}} = \mathbb{C}[z, \bar{z}]^{D_{2n}}$.
- $\zeta := e^{2\pi i/n} \Rightarrow \rho(z) = \zeta z$ and $\rho(\bar{z}) = \bar{\zeta}\bar{z} = \zeta^{-1}\bar{z}$.
- $\sigma(z) = \bar{z}$ and $\sigma(\bar{z}) = z$.
- $f(z, \bar{z}) \in \mathbb{C}[z, \bar{z}]^{D_{2n}} \Leftrightarrow \rho \cdot f = f$ **and** $\sigma \cdot f = f$.

Comparison of Coefficients in Degree d

$f(z,\bar{z}) \in \mathbb{C}[z,\bar{z}]^{D_{2n}} \Leftrightarrow f$ symmetric **and** $f(\zeta z, \zeta^{-1}\bar{z}) = f(z,\bar{z})$.

(i) $d = 1$: **none**, since $a(\zeta z + \zeta^{-1}\bar{z}) \neq a(z + \bar{z})$;

(ii) $d = 2$: $a\zeta z \zeta^{-1}\bar{z} + b(\zeta^2 z^2 + \zeta^{-2}\bar{z}^2) \stackrel{?}{=} az\bar{z} + b(z^2 + \bar{z}^2) \Rightarrow$ $z\bar{z} = x^2 + y^2$ is the only invariant in degree 2 (up to scaling).

(iii) More generally for degree d:

$$\sum_{\substack{k+\ell=d \\ k<\ell}} c_{k\ell}(\zeta^{k-\ell} z^k \bar{z}^\ell + \zeta^{\ell-k} z^\ell \bar{z}^k) \stackrel{?}{=} \sum_{\substack{k+\ell=d \\ k<\ell}} c_{k\ell}(z^k \bar{z}^\ell + z^\ell \bar{z}^k)$$

if and only if $c_{k\ell} = 0$ or $n|(\ell - k)$.

(iv) In other words, the invariants are linear combinations of

$$z^k \bar{z}^{mn+k} + z^{mn+k} \bar{z}^k = (z\bar{z})^k \big((z^n)^m + (\bar{z}^n)^m\big) = (z\bar{z})^k p_m(z^n, \bar{z}^n),$$

where $k, m \in \mathbb{N}_0$.

Recursion for $p_m(z^n, \bar{z}^n)$ and m odd

(v) Next notice that

$$p_m(z^n, \bar{z}^n) = (z^n + \bar{z}^n)^m - \sum_{k=1}^{m} \binom{m}{k} (z^n)^k (\bar{z}^n)^{m-k} =$$

$$= p_1(z^n, \bar{z}^n)^m - \underbrace{\sum_{k=1}^{m} \binom{m}{k} (z^k \bar{z}^{m-k})^n}_{=:q_m(z,\bar{z})}$$

Express $q_m(z, \bar{z})$ in terms of $z\bar{z}$ and $p_j(z^n, \bar{z}^n)$, $1 \leq j < m$.

(vi) If m is odd, then:

$$q_m(z, \bar{z}) = \sum_{k=1}^{\frac{m-1}{2}} \binom{m}{k} \left((z^k \bar{z}^{m-k})^n + (z^{m-k} \bar{z}^k)^m \right) =$$

$$= \sum_{k=1}^{\frac{m-1}{2}} \binom{m}{k} (z\bar{z})^{kn} p_{m-2k}(z^n, \bar{z}^n).$$

Recursion for $p_m(z^n, \bar{z}^n)$ and m even

(vii) If m is even, then

$$q_m(z, \bar{z}) = \sum_{k=1}^{\frac{m}{2}-1} \binom{m}{k} \left((z^k \bar{z}^{m-k})^n + (z^{m-k} \bar{z}^k)^n \right) + \binom{m}{m/2} (z\bar{z})^{\frac{mn}{2}}$$

$$= \sum_{k=1}^{\frac{m}{2}-1} \binom{m}{k} (z\bar{z})^{kn} p_{m-2k}(z^n, \bar{z}^n) + \binom{m}{m/2} (z\bar{z})^{\frac{mn}{2}}$$

(viii) Thus, every $p_m(z^n, \bar{z}^n)$ can always be expressed via $z\bar{z}$ and $p_1(z^n, \bar{z}^n), \ldots, p_{m-1}(z^n, \bar{z}^n)$. Therefore, we have:

$$\forall\, m \in \mathbb{N} \colon p_m(z^n, \bar{z}^n) \in \mathbb{C}[z\bar{z}, p_1(z^n, \bar{z}^n)].$$

$$\Rightarrow \mathbb{C}[z, \bar{z}]^{D_{2n}} = \mathbb{C}[z\bar{z}, z^n + \bar{z}^n] = \mathbb{C}[|z|^2, \mathrm{Re}(z^n)].$$

$\square$

Concluding Remarks

Remarks

(1) *Even though we've deviated from the original setting by complexifying the problem, it became easier and we still obtained "real" generators.*

(2) $D_{2n} = \{\rho^k \sigma^\ell : 1 \leq k \leq n,\, 1 \leq \ell \leq 2\}$ *as a set* $\Rightarrow$ *we could've calculated the orbit of each* $z^\alpha \bar{z}^\beta$, $\alpha + \beta \leq |D_{2n}| = 2n$, *and from there the generic invariants (but didn't).*

(3) *In particular, we got away with only 2 generators.*

(4) *Noether's bound* $|G|$ *on the degree of the invariant generators is not always optimal.*

Thank You!