Why invariants?

Cohomology: $H^*(G,K) = H^*(N,K)^H$
if $1 \to N \to G \to H \to 1$ exact, $\mathrm{char}(K) \nmid |H|$.

Galois group computation: Need permutation invariants for Stauduhar's method.

Coding theory: Weight enumerators of self-dual codes are invariants.

Finite-dimensional algebras: Automorphism groups are linear algebraic groups.
$(V, \mathsf{mult}_1) \cong (V, \mathsf{mult}_2) \Leftrightarrow \mathsf{mult}_i$ are in same orbit of $\mathsf{GL}(V)$ on $V^* \otimes V^* \otimes V$.

Why arithmetic invariant theory?

$G \subseteq \mathrm{GL}_n(\mathcal{O})$ with $\mathcal{O}$ ring. For $\mathcal{O} \to K$, *often* have

$$K[x_1, \ldots, x_n]^G = K \otimes_{\mathcal{O}} \mathcal{O}[x_1, \ldots, x_n]^G$$

("universal" invariant ring, specializes to all characteristics).

Multiplicative invariants: $G \subseteq \mathrm{GL}_n(\mathbb{Z})$ acts on $\mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ by application to exponent vectors. Without loss: G finite.

Problem 7 in Martin Lorenz' book:

Find an algorithm for computing $\mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]^G$.

Setup

$R = K[a_1, \ldots, a_n]$: finitely generated domain over a ring K.

$G \subseteq \mathrm{Aut}_K(R)$: a group consisting of automorphisms.

$L = \mathrm{Quot}(R)$: field of fractions.

$y_1, \ldots, y_n$: indeterminates (with trivial G-action).

$\mathfrak{D} := \bigcap_{\sigma \in G} \big(y_1 - \sigma(a_1), \ldots, y_n - \sigma(a_n)\big) \subsetneqq L[y_1, \ldots, y_n]$: *Derksen ideal*. (depends on the a_i)

$\mathfrak{E} \subsetneqq L[y_1, \ldots, y_n]$ G-stable s.t. $\mathfrak{D} \subseteq \mathfrak{E}$: *extended Derksen ideal*. (a matter of choice)

$\mathfrak{B}$: reduced Gröbner basis of $\mathfrak{E}$ (w.r.t. an arbitrary monomial ordering).

$A \subseteq L$: subalgebra generated by the coefficients of all polynomials in $\mathfrak{B}$.

Example 1

$R = \mathbb{Z}[x, x^{-1}]$, $G \cong C_2$ generated by $x \mapsto -x^{-1}$.

$$\mathfrak{D} = (y_1 - x, y_2 - x^{-1}) \cap (y_1 + x^{-1}, y_2 + x)$$

$$= \Big(\underbrace{y_1^2 - (x - x^{-1})y_1 - 1, y_2 - y_1 + (x - x^{-1})}_{=\mathfrak{B}}\Big) =: \mathfrak{E}.$$

$A = \mathbb{Z}\big[x - x^{-1}\big] = R^G$.

Example 2

The multiplicative group $G = \mathbb{G}_m = K \setminus \{0\}$ over an infinite field K acts on $R = K[x_1, x_2]$ with weight $(1, -1)$. Obtain

$$\mathfrak{D} = \bigcap_{\lambda \in K \setminus \{0\}} (y_1 - \lambda x_2, y_2 - \lambda^{-1} x_2) = \Big(y_1 y_2 - x_1 x_2\Big).$$

May choose $\mathfrak{E} = \mathfrak{D}$ or

$$\mathfrak{E} := \mathfrak{D} + (y_1 - 1) = \Big(y_1 - 1, y_2 - x_1 x_2\Big).$$

In both cases $A = K[x_1 x_2] = R^G$.

Setup

$R = K[a_1, \ldots, a_n]$: domain over a ring K, $L := \mathrm{Quot}(R)$.
$G \subseteq \mathrm{Aut}_K(R)$.
$y_1, \ldots, y_n$: indeterminates.

$\mathfrak{D} := \bigcap_{\sigma \in G} \big(y_1 - \sigma(a_1), \ldots, y_n - \sigma(a_n)\big) \subsetneqq L[y_1, \ldots, y_n]$: *Derksen ideal*.

$\mathfrak{E} \subsetneqq L[y_1, \ldots, y_n]$ G-stable with $\mathfrak{D} \subseteq \mathfrak{E}$: *extended Derksen ideal*.

$A \subseteq L$: subalgebra generated by the coefficients of all polynomials in the reduced Gröbner basis $\mathfrak{B}$ of $\mathfrak{E}$.

Theorem (K., versions due to Müller-Quade & Beth, Hubert & Kogan, Kamke): $R^G \subseteq A \subseteq L^G$.

If $0 \neq c \in R^G$ with $A \subseteq R_c := R[c^{-1}]$, then

$$\boxed{R_c^G = A_c}$$

Geometry and computation

G: linear algebraic group over a field $K = \overline{K}$.
X: irreducible affine variety with G-action.
$R = K[X] = K[a_1, \ldots, a_n]$.
$g_1, \ldots, g_n \in K[G] \otimes K[X]$: defining the G-action on the a_i.

$Y \subseteq X$: closed subset s.t. $G(Y) \subseteq X$ is dense.
Y is called a *cross-section* (first used by Hubert & Kogan).

Write $Y = \mathrm{Var}\Big(f_1(a_1, \ldots, a_n), \ldots, f_s(a_1, \ldots, a_n)\Big)$ with $f_j \in K[y_1, \ldots, y_n]$, set

$$\widehat{\mathfrak{E}} := \Big(y_1 - g_1, \ldots, y_n - g_n, f_1, \ldots, f_s\Big) \subseteq K[G] \otimes K(X)[y_1, \ldots, y_n].$$

Theorem: $\mathfrak{E} := K(X)[y_1, \ldots, y_n] \cap \widehat{\mathfrak{E}}$ (elimination ideal) is an extended Derksen ideal.

Theorem: The f_j can be chosen as $f_j = y_{i_j} - \beta_j$ with $\beta_j \in K$, $s =$ maximal dimension of a G-orbit. Reduce number of variables!

Invariantization

Let $r \in R$, write $r = f(a_1, \ldots, a_n)$ with $f \in K[y_1, \ldots, y_n]$. Define

$$\varphi_{\mathfrak{B}}(r) = \Big(\mathsf{NF}_{\mathfrak{B}}(f)\Big)(y_1 = \cdots = y_n = 0) \in A$$

invariantization of r (term coined by Fels & Olver).

Theorem (K.): $\varphi_{\mathfrak{B}}$: $R_c \twoheadrightarrow R_c^G$ is a projection of R_c^G-modules. In particular, R_c^G is a direct summand of R_c.

Corollary: If R_c is regular and contains a field, then R_c^G is Cohen-Macaulay.

Example

The multiplicative group $G = \mathbb{G}_m = K \setminus \{0\}$ over an infinite field K acts on $R = K[x_1, x_2]$ with weight $(1, -1)$. Derksen ideal:

$$\mathfrak{D} = \big(y_1 y_2 - x_1 x_2\big).$$

First choice: $\mathfrak{E} = \mathfrak{D}$, $\mathfrak{B} = \{y_1 y_2 - x_1 x_2\}$. Then for $t \in K[x_1, x_2]$ a monomial have

$$\varphi_{\mathfrak{B}}(t) = \begin{cases} t & \text{if } t \in R^G, \\ 0 & \text{otherwise,} \end{cases}$$

This is the Reynolds operator, not a ring homomorphism.

Second choice: $\mathfrak{E} = \mathfrak{D} + (y_1 - 1)$, $\mathfrak{B} = \{y_1 - 1, y_2 - x_1 x_2\}$. Then for $g \in K[x_1, x_2]$ have

$$\varphi_{\mathfrak{B}}(g) = g(1, x_1 x_2).$$

This is a ring homomorphism!

Perfect cross-sections

G: linear algebraic group over a field $K = \overline{K}$.
X: irreducible affine variety with G-action.
$R = K[X] = K[a_1, \ldots, a_n]$.
Suppose there exist $\emptyset \neq U \subseteq X$ open, G-stable, and $Y \subseteq U$ closed such that

$$|G(x) \cap Y| = 1 \quad \text{for} \quad x \in U$$

("*perfect cross-section*"). Then the morphism

$$U \to Y, \quad x \to G(x) \cap Y$$

defines a geometric quotient of U by G.

• The embedding $Y \to U$ induces the invariantization $K[U] \to K[U]^G$, which in this case is a projection of $K[U]^G$-algebras.

• If G is connected and solvable, there always exists a perfect cross-section. $\to$ van den Essen's algorithm for $\mathbb{G}_a$-invariants.

Retrieving R^G from R_c^G

Recall $R_c^G = A_c$ with A computed. By changing A, may assume $c \in A \subseteq R$. Then

$$R^G = A \quad \Leftrightarrow \quad R \cdot c \cap A \subseteq A \cdot c.$$

The latter can be checked using Gröbner bases.

If there is $r \in (R \cdot c \cap A) \setminus A \cdot c$, then $r/c \in R^G \setminus A$
$\rightarrow$ new generator, include it into A!

Obtain a semi-algorithm for computing R^G. It terminates iff R^G is finitely generated.

Gröbner bases can be computed over *Zacharias rings*. Example: Euclidean rings. Implementation in MAGMA for $K = \mathbb{Z}$. Adams and Loustaunau's book treats Gröbner bases over rings.

Finite groups

If G is finite, there is good news:

- The Gröbner basis $\mathfrak{B}$ of $\mathfrak{E} = \mathfrak{D}$ can be just written down ("closed formula"); no Buchberger necessary!
- $0 \neq c \in R^G$ with $A \subseteq R_c$ can be found.
- If K is Noetherian, R^G is finitely generated, so the semi-algorithm will terminate.

Obtain an algorithm for computing invariants of a finite group acting on a finitely generated domain over a Zacharias ring, such as $\mathbb{Z}$.

Example: universal invariant ring

$G \cong C_2$ acts on $R = \mathbb{Z}[x_1, x_2, x_3, y_1, y_2, y_3]$ by $x_i \leftrightarrow y_i$.

Result (computed with MAGMA in the blink of an ):

$$R^G = \mathbb{Z}[s_1, s_2, s_3, p_1, p_2, p_3, u_{12}, u_{13}, u_{23}, f]$$

with

$$s_i = x_i + y_i,\ \ p_i = x_i y_i,\ \ u_{ij} = x_i y_j + y_i x_j,\ \ f = x_1 y_2 x_3 + y_1 x_2 y_3.$$

Have

$$2f = s_1 u_{23} - s_2 u_{13} + s_3 u_{12}, \qquad (*)$$

so f can be dropped if $2 \in K^\times \rightarrow$ Noether's degree bound.

The relation $(*)$ shows that R^G is not Cohen-Macaulay.

Example: multiplicative invariants

$G = \left\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle \cong D_8$ acts on $R = \mathbb{Z}[x^{\pm 1}, y^{\pm 1}]$ by $x \mapsto x^{-1}$, $y \mapsto y$, and $x \leftrightarrow y$.

Result (computed with MAGMA in the blink of an ):

$$R^G = \mathbb{Z}\left[x + y + x^{-1} + y^{-1}, xy + xy^{-1} + x^{-1}y + x^{-1}y^{-1}\right].$$

There are 13 finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ (up to conjugacy). For all, the multiplicative invariants can be computed by pressing RETURN $\rightarrow$ perfect agreement with data in Lorenz' book.

Open problems

G algebraic group acting on an affine variety X over $K = \overline{K}$.

- Decide if $K[X]^G$ is finitely genrated.
- Find a (semi-)algorithm that computes $K[X]^G$ if finitely generated.
- Compute a quasi-affine variety Y with $K[X]^G = K[Y]$.
- G reductive, R nonreduced K-algebra with G-action: Compute R^G.

Thank you!