Invariantentheorie

Bald auch in einem Computeralgebrasystem in
Ihrer Nähe verfügbar!

Johannes Schmitt
TU Kaiserslautern
12. August 2021

Invarianten

K: Körper, $\operatorname{char} K = 0$
G: endliche Gruppe
V: G-Modul, $\dim_K V = n$

Invarianten

K: Körper, $\operatorname{char} K = 0$	$\mathbb{Q}$
G: endliche Gruppe	$G := \langle -I_2 \rangle \subseteq \mathrm{GL}_2(\mathbb{Q})$
V: G-Modul, $\dim_K V = n$	$V := \mathbb{Q}^2$, $n = 2$

Invarianten

K: Körper, $\operatorname{char} K = 0$ $\qquad$ $\mathbb{Q}$
G: endliche Gruppe $\qquad$ $G := \langle -I_2 \rangle \subseteq \mathrm{GL}_2(\mathbb{Q})$
V: G-Modul, $\dim_K V = n$ $\qquad$ $V := \mathbb{Q}^2$, $n = 2$

Für $f \in K[V] := S(V^*)$ und $\gamma \in G$ definiere $\gamma \cdot f \in K[V]$ durch

$$(\gamma \cdot f)(v) := f(\gamma^{-1} \cdot v) ,$$

für alle $v \in V$.

Invarianten

K: Körper, char $K = 0$ — $\mathbb{Q}$

G: endliche Gruppe — $G := \langle -I_2 \rangle \subseteq \mathrm{GL}_2(\mathbb{Q})$

V: G-Modul, $\dim_K V = n$ — $V := \mathbb{Q}^2$, $n = 2$

Für $f \in K[V] := S(V^*)$ und $\gamma \in G$ definiere $\gamma \cdot f \in K[V]$ durch

$$(\gamma \cdot f)(v) := f(\gamma^{-1} \cdot v)\ ,$$

für alle $v \in V$.

$$K[V] = \mathbb{Q}[x, y]$$
$$(-I_2) \cdot x = -x$$
$$(-I_2) \cdot y = -y$$
$$(-I_2) \cdot (x + y) = -x - y$$

Invarianten

K: Körper, $\operatorname{char} K = 0$ — $\mathbb{Q}$

G: endliche Gruppe — $G := \langle -I_2 \rangle \subseteq \mathrm{GL}_2(\mathbb{Q})$

V: G-Modul, $\dim_K V = n$ — $V := \mathbb{Q}^2$, $n = 2$

Für $f \in K[V] := S(V^*)$ und $\gamma \in G$ definiere $\gamma \cdot f \in K[V]$ durch

$$(\gamma \cdot f)(v) := f(\gamma^{-1} \cdot v)\ ,$$

für alle $v \in V$.

$K[V] = \mathbb{Q}[x, y]$

$(-I_2) \cdot x = -x$

$(-I_2) \cdot y = -y$

$(-I_2) \cdot (x + y) = -x - y$

Ein Polynom $f \in K[V]$ heißt invariant, wenn $\gamma \cdot f = f$ für alle $\gamma \in G$.

Invarianten

K: Körper, $\operatorname{char} K = 0$
G: endliche Gruppe
V: G-Modul, $\dim_K V = n$

$\mathbb{Q}$
$G := \langle -I_2 \rangle \subseteq \mathrm{GL}_2(\mathbb{Q})$
$V := \mathbb{Q}^2$, $n = 2$

Für $f \in K[V] := S(V^*)$ und $\gamma \in G$ definiere $\gamma \cdot f \in K[V]$ durch

$$(\gamma \cdot f)(v) := f(\gamma^{-1} \cdot v) \ ,$$

für alle $v \in V$.

$K[V] = \mathbb{Q}[x, y]$
$(-I_2) \cdot x = -x$
$(-I_2) \cdot y = -y$
$(-I_2) \cdot (x + y) = -x - y$

Ein Polynom $f \in K[V]$ heißt invariant, wenn $\gamma \cdot f = f$ für alle $\gamma \in G$.

$(-I_2) \cdot x^2 = x^2$
$(-I_2) \cdot (xy) = xy$

Invarianten

Für $f \in K[V] := S(V^*)$ und $\gamma \in G$ definiere $\gamma \cdot f \in K[V]$ durch

$$(\gamma \cdot f)(v) := f(\gamma^{-1} \cdot v) \ ,$$

für alle $v \in V$.

$$K[V] = \mathbb{Q}[x, y]$$
$$(-I_2) \cdot x = -x$$
$$(-I_2) \cdot y = -y$$
$$(-I_2) \cdot (x + y) = -x - y$$

Ein Polynom $f \in K[V]$ heißt invariant, wenn $\gamma \cdot f = f$ für alle $\gamma \in G$.

$$(-I_2) \cdot x^2 = x^2$$
$$(-I_2) \cdot (xy) = xy$$

Der Invariantenring von G ist $K[V]^G := \{f \in K[V] \text{ invariant}\}$.

Invarianten

Für $f \in K[V] := S(V^*)$ und $\gamma \in G$ definiere $\gamma \cdot f \in K[V]$ durch

$$(\gamma \cdot f)(v) := f(\gamma^{-1} \cdot v) \ ,$$

für alle $v \in V$.

$$K[V] = \mathbb{Q}[x, y]$$
$$(-I_2) \cdot x = -x$$
$$(-I_2) \cdot y = -y$$
$$(-I_2) \cdot (x + y) = -x - y$$

Ein Polynom $f \in K[V]$ heißt invariant, wenn $\gamma \cdot f = f$ für alle $\gamma \in G$.

$$(-I_2) \cdot x^2 = x^2$$
$$(-I_2) \cdot (xy) = xy$$

Der Invariantenring von G ist $K[V]^G := \{f \in K[V] \text{ invariant}\}$.

$$\mathbb{Q}[V]^G = \{f = \textstyle\sum_i f_i \mid f_i \text{ homogen}, \deg f_i \text{ gerade}\}$$

Endlichkeitssatz

Hilberts Endlichkeitssatz (1890)

Der Invariantenring $K[V]^G$ ist eine endlich erzeugte K-Algebra.

Endlichkeitssatz

Hilberts Endlichkeitssatz (1890)

Der Invariantenring $K[V]^G$ ist eine endlich erzeugte K-Algebra.

$G = \langle -I_2 \rangle$

$$\begin{aligned}\mathbb{Q}[V]^G &= \{f = \textstyle\sum_i f_i \mid f_i \text{ homogen}, \deg f_i \text{ gerade}\} \\ &= \mathbb{Q}[x^2, xy, y^2]\end{aligned}$$

Endlichkeitssatz

Hilberts Endlichkeitssatz (1890)

Der Invariantenring $K[V]^G$ ist eine endlich erzeugte K-Algebra.

Endlichkeitssatz

Hilberts Endlichkeitssatz (1890)

Der Invariantenring $K[V]^G$ ist eine endlich erzeugte K-Algebra.

S_n

Die Gruppe S_n operiert auf $V := K^n$ durch Permutation der Variablen.

Endlichkeitssatz

Hilberts Endlichkeitssatz (1890)

Der Invariantenring $K[V]^G$ ist eine endlich erzeugte K-Algebra.

S_n

Die Gruppe S_n operiert auf $V := K^n$ durch Permutation der Variablen. Entsprechend ist $K[V]^{S_n}$ erzeugt von den elementarsymmetrischen Polynomen

$$f_k := \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}, \quad 1 \leq k \leq n \ .$$

Endlichkeitssatz

Hilberts Endlichkeitssatz (1890)

Der Invariantenring $K[V]^G$ ist eine endlich erzeugte K-Algebra.

S_n

Die Gruppe S_n operiert auf $V := K^n$ durch Permutation der Variablen. Entsprechend ist $K[V]^{S_n}$ erzeugt von den elementarsymmetrischen Polynomen

$$f_k := \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}, \quad 1 \leq k \leq n \; .$$

Problem

Finde Erzeuger von $K[V]^G$ als K-Algebra.

Hilbert Reihen

Der Ring $K[V]^G$ erbt die Graduierung (via Totalgrad) von $K[V] = K[x_1, \ldots, x_n]$.

Hilbert Reihen

Der Ring $K[V]^G$ erbt die Graduierung (via Totalgrad) von $K[V] = K[x_1, \ldots, x_n]$. Insbesondere gilt

$$(K[V]_d)^G \subseteq K[V]_d \quad \text{für } d \in \mathbb{Z}_{\geq 0} \; .$$

Hilbert Reihen

Der Ring $K[V]^G$ erbt die Graduierung (via Totalgrad) von $K[V] = K[x_1, \dots, x_n]$. Insbesondere gilt

$$(K[V]_d)^G \subseteq K[V]_d \;\text{ für } d \in \mathbb{Z}_{\geq 0} \;.$$

Die Hilbert Reihe von $K[V]^G$ ist die Potenzreihe

$$H(K[V]^G, t) := \sum_{d=0}^{\infty} \dim_K K[V]_d^G \, t^d \;.$$

Hilbert Reihen

Der Ring $K[V]^G$ erbt die Graduierung (via Totalgrad) von $K[V] = K[x_1, \ldots, x_n]$. Insbesondere gilt

$$(K[V]_d)^G \subseteq K[V]_d \quad \text{für } d \in \mathbb{Z}_{\geq 0} \ .$$

Die Hilbert Reihe von $K[V]^G$ ist die Potenzreihe

$$H(K[V]^G, t) := \sum_{d=0}^{\infty} \dim_K K[V]_d^G \, t^d \ .$$

Moliens Formel

Im Fall $\operatorname{char} K = 0$ gilt

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{\gamma \in G} \frac{1}{\det(1 - t \cdot \gamma)} \ .$$

Hilbert Reihen

Moliens Formel

Im Fall char $K = 0$ gilt

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{\gamma \in G} \frac{1}{\det(1 - t \cdot \gamma)} \ .$$

Hilbert Reihen

Moliens Formel

Im Fall char $K = 0$ gilt

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{\gamma \in G} \frac{1}{\det(1 - t \cdot \gamma)} \ .$$

$G = \langle -I_2 \rangle$

$$H(\mathbb{Q}[V]^G, t) = \frac{1}{2} \frac{1}{(1-t)^2} + \frac{1}{2} \frac{1}{(1+t)^2}$$

Hilbert Reihen

Moliens Formel

Im Fall char $K = 0$ gilt

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{\gamma \in G} \frac{1}{\det(1 - t \cdot \gamma)} .$$

$G = \langle -I_2 \rangle$

$$\begin{aligned} H(\mathbb{Q}[V]^G, t) &= \frac{1}{2} \frac{1}{(1-t)^2} + \frac{1}{2} \frac{1}{(1+t)^2} \\ &= \frac{1}{2} \sum_{d=0}^{\infty} d t^{d-1} + \frac{1}{2} \sum_{d=0}^{\infty} d(-t)^{d-1} \end{aligned}$$

Hilbert Reihen

Moliens Formel

Im Fall char $K = 0$ gilt

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{\gamma \in G} \frac{1}{\det(1 - t \cdot \gamma)} \ .$$

$G = \langle -I_2 \rangle$

$$\begin{aligned} H(\mathbb{Q}[V]^G, t) &= \frac{1}{2}\frac{1}{(1-t)^2} + \frac{1}{2}\frac{1}{(1+t)^2} \\ &= \frac{1}{2}\sum_{d=0}^{\infty} dt^{d-1} + \frac{1}{2}\sum_{d=0}^{\infty} d(-t)^{d-1} = \sum_{\substack{d=0 \\ d \text{ gerade}}}^{\infty} (d+1)t^d \end{aligned}$$

Ein erster Algorithmus
Nicht zuhause nachmachen!

Algorithmus

$S := \emptyset$
while $H(K[S], t) \neq H(K[V]^G, t)$ **do**
    Finde den minimalen Grad d, in dem sich $H(K[S], t)$ und $H(K[V]^G, t)$ unterscheiden.
    Füge homogene Invarianten von Grad d zu S hinzu.
end while
return S

Ein erster Algorithmus

Nicht zuhause nachmachen!

Algorithmus

$S := \emptyset$
while $H(K[S], t) \neq H(K[V]^G, t)$ **do**
    Finde den minimalen Grad d, in dem sich $H(K[S], t)$ und $H(K[V]^G, t)$ unterscheiden.
    Füge homogene Invarianten von Grad d zu S hinzu.
end while
return S

Problem

Finde homogene Invarianten von gegebenem Grad d.

Etwas Theorie

Invariantensuche

Primärinvarianten

Sekundärinvarianten

Invariantensuche

Reynolds-Operator

Die Abbildung

$$\mathcal{R}_G : K[V] \to K[V]^G,\ f \mapsto \frac{1}{|G|} \sum_{\gamma \in G} \gamma \cdot f$$

ist der Reynolds-Operator von G.

Invariantensuche
Reynolds-Operator

Die Abbildung

$$\mathcal{R}_G : K[V] \to K[V]^G,\ f \mapsto \frac{1}{|G|} \sum_{\gamma \in G} \gamma \cdot f$$

ist der Reynolds-Operator von G.

Algorithmus

1: Wähle $f \in K[V]_d$.
2: **return** $\mathcal{R}_G(f)$

Die Abbildung

$$\mathcal{R}_G : K[V] \to K[V]^G,\ f \mapsto \frac{1}{|G|} \sum_{\gamma \in G} \gamma \cdot f$$

ist der Reynolds-Operator von G.

Algorithmus

1: Wähle eine Basis $h_1, \ldots, h_k \in K[V]_d$.
2: **return** $\mathcal{R}_G(h_1), \ldots, \mathcal{R}_G(h_k)$, ein Erzeugendensystem für $K[V]_d^G$

Die Abbildung

$$\mathcal{R}_G : K[V] \to K[V]^G,\ f \mapsto \frac{1}{|G|} \sum_{\gamma \in G} \gamma \cdot f$$

ist der Reynolds-Operator von G.

Algorithmus

1: Wähle eine Basis $h_1, \ldots, h_k \in K[V]_d$.
2: **return** $\mathcal{R}_G(h_1), \ldots, \mathcal{R}_G(h_k)$, ein Erzeugendensystem für $K[V]_d^G$

Erfordert allerdings die Operation jedes Gruppenelements.

Invariantensuche

Reynolds-Operator für Fortgeschrittene

Für $H \leq G$ und $f \in K[V]^H$ sei

$$\mathcal{R}_{G/H}(f) := \frac{1}{[G:H]} \sum_{\gamma \in G/H} \gamma \cdot f \ .$$

Invariantensuche

Reynolds-Operator für Fortgeschrittene

Für $H \leq G$ und $f \in K[V]^H$ sei

$$\mathcal{R}_{G/H}(f) := \frac{1}{[G:H]} \sum_{\gamma \in G/H} \gamma \cdot f \ .$$

Gegeben sei eine Kette von Untergruppen

$$1 = G_1 \leq G_2 \leq \cdots \leq G_{m-1} \leq G_m = G \ .$$

Invariantensuche

Reynolds-Operator für Fortgeschrittene

Für $H \leq G$ und $f \in K[V]^H$ sei

$$\mathcal{R}_{G/H}(f) := \frac{1}{[G:H]} \sum_{\gamma \in G/H} \gamma \cdot f \ .$$

Gegeben sei eine Kette von Untergruppen

$$1 = G_1 \leq G_2 \leq \cdots \leq G_{m-1} \leq G_m = G \ .$$

Algorithmus

1: Wähle $f \in K[V]_d$.
2: **for** $i = 1, \ldots, m-1$ **do**
3: $\quad f := \mathcal{R}_{G_{i+1}/G_i}(f) \in K[V]_d^{G_{i+1}}$
4: **end for**
5: **return** f

Invariantensuche

Reynolds-Operator für Fortgeschrittene

Für $H \leq G$ und $f \in K[V]^H$ sei

$$\mathcal{R}_{G/H}(f) := \frac{1}{[G:H]} \sum_{\gamma \in G/H} \gamma \cdot f \ .$$

Gegeben sei eine Kette von Untergruppen

$$1 = G_1 \leq G_2 \leq \cdots \leq G_{m-1} \leq G_m = G \ .$$

Algorithmus

1: Wähle $f \in K[V]_d$.
2: **for** $i = 1, \ldots, m-1$ **do**
3: $\quad f := \mathcal{R}_{G_{i+1}/G_i}(f) \in K[V]_d^{G_{i+1}}$
4: **end for**
5: **return** f

Erfordert lediglich $\sum_{i=1}^{m-1} [G_{i+1} : G_i]$ Gruppenoperationen.

Invariantensuche
Via linearer Algebra

Seien $\gamma_1, \ldots, \gamma_m \in G$ Erzeuger von G.

Invariantensuche

Via linearer Algebra

Seien $\gamma_1, \ldots, \gamma_m \in G$ Erzeuger von G. Die lineare Abbildung

$$\varphi_d : K[V]_d \to \bigoplus_{i=1}^{m} K[V]_d,\ f \mapsto (\gamma_1 \cdot f - f, \ldots, \gamma_m \cdot f - f)$$

hat Kern $K[V]_d^G$.

Seien $\gamma_1, \dots, \gamma_m \in G$ Erzeuger von G. Die lineare Abbildung

$$\varphi_d : K[V]_d \to \bigoplus_{i=1}^{m} K[V]_d,\ f \mapsto (\gamma_1 \cdot f - f, \dots, \gamma_m \cdot f - f)$$

hat Kern $K[V]_d^G$.

Algorithmus

1: Wähle eine Basis von $K[V]_d$ (etwa alle Monome).
2: Schreibe φ_d als Matrix M in dieser Basis.
3: **return** $\ker M$

Seien $\gamma_1, \ldots, \gamma_m \in G$ Erzeuger von G. Die lineare Abbildung

$$\varphi_d : K[V]_d \to \bigoplus_{i=1}^{m} K[V]_d,\ f \mapsto (\gamma_1 \cdot f - f, \ldots, \gamma_m \cdot f - f)$$

hat Kern $K[V]_d^G$.

Algorithmus

1: Wähle eine Basis von $K[V]_d$ (etwa alle Monome).
2: Schreibe φ_d als Matrix M in dieser Basis.
3: **return** ker M

Aber: $\dim_K K[V]_d = \binom{n+d-1}{n-1}$.

Primärinvarianten

Der Ring $K[V]^G$ hat eine Noether Normalisierung, d. h. es existieren $f_1, \ldots, f_n \in K[V]^G$ mit

a. die $f_1, \ldots, f_n$ sind algebraisch unabhängig und
b. $K[V]^G$ is ein endlich erzeugter Modul über $K[f_1, \ldots, f_n]$,

die Primärinvarianten.

Primärinvarianten

Der Ring $K[V]^G$ hat eine Noether Normalisierung, d. h. es existieren $f_1, \dots, f_n \in K[V]^G$ mit

a. die $f_1, \dots, f_n$ sind algebraisch unabhängig und
b. $K[V]^G$ is ein endlich erzeugter Modul über $K[f_1, \dots, f_n]$,

die Primärinvarianten.

$G = \langle -I_2 \rangle$

Primärinvarianten von $\mathbb{Q}[V]^G = \mathbb{Q}[x^2, xy, y^2]$ sind x^2 und y^2.

Primärinvarianten

Der Ring $K[V]^G$ hat eine Noether Normalisierung, d. h. es existieren $f_1, \ldots, f_n \in K[V]^G$ mit

a. die $f_1, \ldots, f_n$ sind algebraisch unabhängig und
b. $K[V]^G$ is ein endlich erzeugter Modul über $K[f_1, \ldots, f_n]$,

die Primärinvarianten.

$G = \langle -I_2 \rangle$

Primärinvarianten von $\mathbb{Q}[V]^G = \mathbb{Q}[x^2, xy, y^2]$ sind x^2 und y^2. Allerdings nicht eindeutig: x^4 und y^4 sind ebenfalls Primärinvarianten.

Primärinvarianten

Der Ring $K[V]^G$ hat eine Noether Normalisierung, d. h. es existieren $f_1, \dots, f_n \in K[V]^G$ mit

a. die $f_1, \dots, f_n$ sind algebraisch unabhängig und
b. $K[V]^G$ is ein endlich erzeugter Modul über $K[f_1, \dots, f_n]$,

die Primärinvarianten.

$G = \langle -I_2 \rangle$

Primärinvarianten von $\mathbb{Q}[V]^G = \mathbb{Q}[x^2, xy, y^2]$ sind x^2 und y^2. Allerdings nicht eindeutig: x^4 und y^4 sind ebenfalls Primärinvarianten.

Problem

Finde Primärinvarianten $f_1, \dots, f_n$ mit $d_i := \deg f_i$ "optimal", insbesondere $d_1 \cdots d_n$ minimal.

Primärinvarianten

Nenne $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$ "Primärgrade", wenn Primärinvarianten von diesem Grad existieren.

Primärinvarianten

Nenne $d_1, \dots, d_n \in \mathbb{Z}_{\geq 0}$ "Primärgrade", wenn Primärinvarianten von diesem Grad existieren.

Algorithmische Idee

1: Finde Primärgrade $d_1, \dots, d_n$.
2: Wähle zufällige $f_i \in K[V]^G_{d_i}$.

Primärinvarianten

Nenne $d_1, \dots, d_n \in \mathbb{Z}_{\geq 0}$ "Primärgrade", wenn Primärinvarianten von diesem Grad existieren.

Algorithmische Idee

1: Finde Primärgrade $d_1, \dots, d_n$.
2: Wähle zufällige $f_i \in K[V]^G_{d_i}$.

Zu Schritt 2:

Kemper, 1999

Die Menge

$$\{(f_1, \dots, f_n) \in K[V]^G_{d_1} \times \cdots \times K[V]^G_{d_n} \mid \dim(f_1, \dots, f_n) = n\}$$

ist eine Zariski offene Teilmenge von $K[V]^G_{d_1} \times \cdots \times K[V]^G_{d_n}$.

Primärinvarianten

Wie entscheided man, ob $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$ Primärgrade sind?

Primärinvarianten

Wie entscheided man, ob $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$ Primärgrade sind?

Notwendige Bedingungen

- $|G|$ teilt das Produkt $d_1 \cdots d_n$.

Primärinvarianten

Wie entscheided man, ob $d_1, \dots, d_n \in \mathbb{Z}_{\geq 0}$ Primärgrade sind?

Notwendige Bedingungen

- $|G|$ teilt das Produkt $d_1 \cdots d_n$.
- $H(K[V]^G, t)$ lässt sich als

$$\frac{f(t)}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}$$

mit $f(t) \in \mathbb{Z}_{\geq 0}[t]$ schreiben.

Primärinvarianten

$G = \langle (12)(34), (14)(23) \rangle$

Mit Moliens Formel gilt

$$H(\mathbb{Q}(V)^G, t) = \frac{1}{4}\frac{1}{(1-t)^4} + \frac{1}{4}\frac{3}{(1-t^2)^2}$$

Primärinvarianten

$G = \langle (12)(34), (14)(23) \rangle$

Mit Moliens Formel gilt

$$H(\mathbb{Q}(V)^G, t) = \frac{1}{4}\frac{1}{(1-t)^4} + \frac{1}{4}\frac{3}{(1-t^2)^2}$$
$$= \frac{t^2 - t + 1}{(1-t)^2(1-t^2)^2} = \frac{1+t^3}{(1-t)(1-t^2)^3}$$

Primärinvarianten

$G = \langle (12)(34), (14)(23) \rangle$

Mit Moliens Formel gilt

$$\begin{aligned} H(\mathbb{Q}(V)^G, t) &= \frac{1}{4}\frac{1}{(1-t)^4} + \frac{1}{4}\frac{3}{(1-t^2)^2} \\ &= \frac{t^2 - t + 1}{(1-t)^2(1-t^2)^2} = \frac{1+t^3}{(1-t)(1-t^2)^3} \end{aligned}$$

In der Tat findet man Primärinvarianten

$$\begin{aligned} f_1 &= x_1 + x_2 + x_3 + x_4 \ , & f_2 &= (x_1 - x_2 + x_3 - x_4)^2 \ , \\ f_3 &= (x_1 - x_2 - x_3 + x_4)^2 \ , & f_4 &= (x_1 + x_2 - x_3 - x_4)^2 \ . \end{aligned}$$

Primärinvarianten

Aber wie entscheided man jetzt wirklich, ob $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$ Primärgrade sind?

Primärinvarianten

Aber wie entscheided man jetzt wirklich, ob $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$ Primärgrade sind?

Abstraktion zwecks Rekursion

Für eine graduierte Algebra A mit $\dim A = n$ seien $d_1, \ldots, d_k \in \mathbb{Z}_{\geq 0}$ Primärgrade, wenn $f_i \in A_{d_i}$ mit $\dim(f_1, \ldots, f_k) = k$ existieren.

Primärinvarianten

Aber wie entscheided man jetzt wirklich, ob $d_1, \dots, d_n \in \mathbb{Z}_{\geq 0}$ Primärgrade sind?

Abstraktion zwecks Rekursion

Für eine graduierte Algebra A mit $\dim A = n$ seien $d_1, \dots, d_k \in \mathbb{Z}_{\geq 0}$ Primärgrade, wenn $f_i \in A_{d_i}$ mit $\dim(f_1, \dots, f_k) = k$ existieren.

Kemper, 1999

Die Zahlen $d_1, \dots, d_k \in \mathbb{Z}_{\geq 0}$ sind Primärgrade genau dann, wenn für jede Teilmenge $M \subseteq \{1, \dots, k\}$ gilt

$$\dim\left(A \Big/ \Big(\bigcup_{i \in M} A_{d_i} \Big)\right) \leq n - |M| \ .$$

Primärinvarianten

Aber wie entscheided man jetzt wirklich, ob $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$ Primärgrade sind?

Abstraktion zwecks Rekursion

Für eine graduierte Algebra A mit $\dim A = n$ seien $d_1, \ldots, d_k \in \mathbb{Z}_{\geq 0}$ Primärgrade, wenn $f_i \in A_{d_i}$ mit $\dim(f_1, \ldots, f_k) = k$ existieren.

Kemper, 1999

Die Zahlen $d_1, \ldots, d_k \in \mathbb{Z}_{\geq 0}$ sind Primärgrade genau dann, wenn für jede Teilmenge $M \subseteq \{1, \ldots, k\}$ gilt

$$\dim\left(A \Big/ \Big(\bigcup_{i \in M} A_{d_i} \Big)\right) \leq n - |M| \ .$$

Erfordert allerdings 2^k Gröbner Basen!

Primärinvarianten

Algorithmus (Kemper, 1999)

Input: Graduierte Algebra A, $\dim A = n$, $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 1}$.

$k := 0$
for $f_1 \in A_{d_1} \setminus \{0\}$ **do**
  if $k > 0$ **then**
    if $d_2, \ldots, d_k$ sind keine Primärgrade für $A/(f_1)$ **then continue**
  Sei R Ergebnis der Rekursion mit $A/(f_1)$ und $d_2, \ldots, d_n$.
  if $R = f_2, \ldots, f_n$ **then return** $f_1, \ldots, f_n$
  if $R \geq k$ **then**
    $k := R + 1$
    if $d_1, \ldots, d_k$ sind keine Primärgrade für A **then break**
if $k \leq 1$ **and** $\dim A > n$ **then** $k := 0$ **else** $k := 1$
if $n = 0$ **and** $k = 1$ **then return** leere Liste
return k

Sekundärinvarianten

Erinnerung: Sind $f_1, \ldots, f_n \in K[V]^G$ Primärinvarianten, so ist $K[V]^G$ ein endlich erzeugter $K[f_1, \ldots, f_n]$-Modul.

Sekundärinvarianten

Erinnerung: Sind $f_1, \ldots, f_n \in K[V]^G$ Primärinvarianten, so ist $K[V]^G$ ein endlich erzeugter $K[f_1, \ldots, f_n]$-Modul.

Erzeuger $g_1, \ldots, g_m \in K[V]^G$ von $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul heißen Sekundärinvarianten.

Sekundärinvarianten

Erinnerung: Sind $f_1, \dots, f_n \in K[V]^G$ Primärinvarianten, so ist $K[V]^G$ ein endlich erzeugter $K[f_1, \dots, f_n]$-Modul.

Erzeuger $g_1, \dots, g_m \in K[V]^G$ von $K[V]^G$ als $K[f_1, \dots, f_n]$-Modul heißen Sekundärinvarianten.

$G = \langle -I_2 \rangle$

Für $f_1 = x^2$ und $f_2 = y^2$ sind $g_1 = 1$ und $g_2 = xy$ Sekundärinvarianten.

Sekundärinvarianten

Erinnerung: Sind $f_1, \ldots, f_n \in K[V]^G$ Primärinvarianten, so ist $K[V]^G$ ein endlich erzeugter $K[f_1, \ldots, f_n]$-Modul.

Erzeuger $g_1, \ldots, g_m \in K[V]^G$ von $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul heißen Sekundärinvarianten.

$G = \langle -I_2 \rangle$

Für $f_1 = x^2$ und $f_2 = y^2$ sind $g_1 = 1$ und $g_2 = xy$ Sekundärinvarianten.

Also: Primärinvarianten und Sekundärinvarianten erzeugen $K[V]^G$ als K-Algebra.

Sekundärinvarianten

Erinnerung: Sind $f_1, \ldots, f_n \in K[V]^G$ Primärinvarianten, so ist $K[V]^G$ ein endlich erzeugter $K[f_1, \ldots, f_n]$-Modul.

Erzeuger $g_1, \ldots, g_m \in K[V]^G$ von $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul heißen Sekundärinvarianten.

$G = \langle -I_2 \rangle$

Für $f_1 = x^2$ und $f_2 = y^2$ sind $g_1 = 1$ und $g_2 = xy$ Sekundärinvarianten.

Also: Primärinvarianten und Sekundärinvarianten erzeugen $K[V]^G$ als K-Algebra.

Problem

Finde Sekundärinvarianten $g_1, \ldots, g_m$ gegeben Primärinvarianten $f_1, \ldots, f_n$ mit $d_i := \deg f_i$.

Sekundärinvarianten

Nakayama

Homogene Polynome $g_1, \ldots, g_m \in K[V]^G$ erzeugen genau dann $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul, wenn sie $K[V]^G/(f_1, \ldots, f_n)K[V]^G$ als K-Vektorraum erzeugen.

Sekundärinvarianten

Nakayama

Homogene Polynome $g_1, \ldots, g_m \in K[V]^G$ erzeugen genau dann $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul, wenn sie $K[V]^G/(f_1, \ldots, f_n)K[V]^G$ als K-Vektorraum erzeugen.

Hochster–Eagon, 1971

Der Ring $K[V]^G$ ist Cohen-Macaulay.

Sekundärinvarianten

Nakayama

Homogene Polynome $g_1, \ldots, g_m \in K[V]^G$ erzeugen genau dann $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul, wenn sie $K[V]^G/(f_1, \ldots, f_n)K[V]^G$ als K-Vektorraum erzeugen.

Hochster–Eagon, 1971

Der Ring $K[V]^G$ ist Cohen-Macaulay.
Insbesondere ist $K[V]^G$ frei als $K[f_1, \ldots, f_n]$-Modul.

Sekundärinvarianten

Nakayama

Homogene Polynome $g_1, \dots, g_m \in K[V]^G$ erzeugen genau dann $K[V]^G$ als $K[f_1, \dots, f_n]$-Modul, wenn sie $K[V]^G/(f_1, \dots, f_n)K[V]^G$ als K-Vektorraum erzeugen.

Hochster–Eagon, 1971

Der Ring $K[V]^G$ ist Cohen-Macaulay.
Insbesondere ist $K[V]^G$ frei als $K[f_1, \dots, f_n]$-Modul.

Damit folgt schon

$$m = \frac{d_1 \cdots d_n}{|G|}$$

für ein freies Erzeugendensystem!

Sekundärinvarianten

Nakayama + $m = d_1 \cdots d_n / |G|$

Homogene Polynome $g_1, \ldots, g_m \in K[V]^G$ erzeugen genau dann $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul, wenn sie in $K[V]^G/(f_1, \ldots, f_n)K[V]^G$ linear unabhängig sind.

Sekundärinvarianten

Nakayama + $m = d_1 \cdots d_n / |G|$

Homogene Polynome $g_1, \ldots, g_m \in K[V]^G$ erzeugen genau dann $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul, wenn sie in $K[V]^G/(f_1, \ldots, f_n)K[V]^G$ linear unabhängig sind.

Die Abbildung

$$K[V]^G \to K[V]/(f_1, \ldots, f_n)K[V], \; f \mapsto f + (f_1, \ldots, f_n)K[V]$$

induziert eine Einbettung

$$K[V]^G/(f_1, \ldots, f_n)K[V]^G \hookrightarrow K[V]/(f_1, \ldots, f_n)K[V] \, .$$

Sekundärinvarianten

Nakayama + $m = d_1 \cdots d_n/|G|$

Homogene Polynome $g_1, \ldots, g_m \in K[V]^G$ erzeugen genau dann $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul, wenn sie in $K[V]^G/(f_1, \ldots, f_n)K[V]^G$ linear unabhängig sind.

Die Abbildung

$$K[V]^G \to K[V]/(f_1, \ldots, f_n)K[V], \; f \mapsto f + (f_1, \ldots, f_n)K[V]$$

induziert eine Einbettung

$$K[V]^G/(f_1, \ldots, f_n)K[V]^G \hookrightarrow K[V]/(f_1, \ldots, f_n)K[V] \, .$$

Nakayama + $m = d_1 \cdots d_n/|G|$ + Einbettung

Homogene Polynome $g_1, \ldots, g_m \in K[V]^G$ erzeugen genau dann $K[V]^G$ als $K[f_1, \ldots, f_n]$-Modul, wenn sie in $K[V]/(f_1, \ldots, f_n)K[V]$ linear unabhängig sind.

Sekundärinvarianten

Algorithmus

Input: Primärinvarianten $f_1, \ldots, f_n$ mit $d_i := \deg f_i$

1: Berechne eine Gröbnerbasis $\mathcal{G}$ von $(f_1, \ldots, f_n) \subseteq K[V]$.

2: $m := \frac{d_1 \cdots d_n}{|G|}$

3: **for** $i = 1, \ldots, m$ **do**

4: Finde $g_i \in K[V]^G$, sodass $\mathrm{NF}_{\mathcal{G}}(g_i)$ linear unabhängig von den Polynomen $\mathrm{NF}_{\mathcal{G}}(g_1), \ldots, \mathrm{NF}_{\mathcal{G}}(g_{i-1})$ ist.

5: **end for**

6: **return** $g_1, \ldots, g_m$

Sekundärinvarianten

Algorithmus

Input: Primärinvarianten $f_1, \ldots, f_n$ mit $d_i := \deg f_i$

Berechne eine Gröbnerbasis $\mathcal{G}$ von $(f_1, \ldots, f_n) \subseteq K[V]$.
$m := \frac{d_1 \cdots d_n}{|G|}$
for $i = 1, \ldots, m$ **do**
    Finde $g_i \in K[V]^G$, sodass $\mathrm{NF}_{\mathcal{G}}(g_i)$ linear unabhängig von den Polynomen $\mathrm{NF}_{\mathcal{G}}(g_1), \ldots, \mathrm{NF}_{\mathcal{G}}(g_{i-1})$ ist.
end for
return $g_1, \ldots, g_m$

Die Gröbnerbasis $\mathcal{G}$ is schon aus der Berechnung von $f_1, \ldots, f_n$ bekannt!

Sekundärinvarianten

4: Finde $g_i \in K[V]^G$, sodass ...

Sekundärinvarianten

4: Finde $g_i \in K[V]^G$, sodass ...

- Mit $H(K[V]^G, t)$ und $d_1, \ldots, d_n$ sind auch die Grade $e_i := \deg g_i$ der Sekundärinvarianten bekannt.

Sekundärinvarianten

4: Finde $g_i \in K[V]^G$, sodass ...

- Mit $H(K[V]^G, t)$ und $d_1, \ldots, d_n$ sind auch die Grade $e_i := \deg g_i$ der Sekundärinvarianten bekannt.
- Konstruiere Sekundärinvarianten von hohem Grad als Produkte von solchen mit kleinem Grad.

Sekundärinvarianten

4: Finde $g_i \in K[V]^G$, sodass ...

- Mit $H(K[V]^G, t)$ und $d_1, \ldots, d_n$ sind auch die Grade $e_i := \deg g_i$ der Sekundärinvarianten bekannt.
- Konstruiere Sekundärinvarianten von hohem Grad als Produkte von solchen mit kleinem Grad.
- Wende $\mathcal{R}_G$ nur auf Monome von Grad e_i an, die nicht durch ein Leitmonom in $\mathcal{G}$ teilbar sind.