Inhalt

Literatur

- M. Kreuzer und L. Robbiano, Computational Commutative Algebra 2, Springer Verlag 2005
- H. Derksen und G. Kemper, Computational Invariant Theory, Springer Verlag 2002
- B. Sturmfels, Algorithmic Invariant Theory, Texts and Monogr. in Symb. Comput., Springer Verlag 1993
- A.V. Geramita (Hrsg.), The Curves Seminar at Queens, Vol. XII, Queen's Papers in Pure and Applied Math. 114, Kingston 1998

Kapitel I: Einführung

1 Was ist Invariantentheorie?

Im folgenden sei stets K eine Körper, V ein endlichdimensionaler K-Vektorraum und G eine Gruppe, die auf V linear operiert. D.h. es gebe einen Monoid-Homomorphismus

$$\begin{aligned} \rho : G &\rightarrow \operatorname{End}_K(V) \\ \sigma &\mapsto (v \mapsto \sigma(v)) \end{aligned}$$

1.1 Voraussetzung

Durch Übergang zu $\overline{\rho} : G/\ker(\rho) \rightarrow \operatorname{End}_K(V)$ können wir stets voraussetzen, dass ρ injektiv ist. Dann heißt $\rho : G \hookrightarrow \operatorname{End}_K(V)$ auch eine (lineare) **Darstellung** der Gruppe G.

Offenbar gilt sogar: $\rho : G \hookrightarrow \operatorname{Aut}_K(V)$

Nun wählen wir eine K-Basis $\{x_1, \ldots, x_n\}$ von V. Der Polynomring $P = K[V] = K[x_1, \ldots, x_n]$ ist die symmetrische Algebra von V. Wir können V auffassen als die Menge $Kx_1 \oplus \ldots \oplus Kx_n$ der homogenen Polynome vom Grad 1.

1.2 Bemerkung

Die Operation von G auf V lässt sich fortsetzen zu einer Operation von G auf P: Für jedes $\sigma \in G$ und $f \in P$ setze dabei

$$\sigma(f) = f(A \cdot x)$$

wobei A die Darstellungsmatrix von $\rho(\sigma)$ in der Basis $(x_1, \ldots, x_n)$ und $A \cdot x = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ sei. Für $A = (a_{ij})$ gilt also:

$$\sigma(f)(x_1 \ldots x_n) = f(a_{11}x_1 + \ldots + a_{1n}x_n, \ldots, a_{n1}x_1 + \ldots + a_{nn}x_n)$$

1.3 Definition

Die Menge

$$P^G = \{f \in P \mid \sigma(f) = f \ \forall \sigma \in G\}$$

heißt der **Invariantenring** der Operation von G auf V.

1.4 Bemerkung

Die Menge P^G ist eine K-Unteralgebra von P, d.h. für $f, g \in P^G$ und $c \in K$ gilt $f + g \in P^G$, $fg \in P^G$ und $cf \in P^G$.

1.5 Beispiel (Die Invarianten von $\mathcal{O}_2(\mathbb{R})$)

Sei $K = \mathbb{R}$, $V = \mathbb{R}^2$ und die Gruppe $G = \mathcal{O}_2(\mathbb{R}) = \{\mathcal{M} \in \mathrm{GL}_2(\mathbb{R}) \mid \mathcal{M}\mathcal{M}^{\mathrm{tr}} = \mathcal{I}_2\}$ operiere durch Koordinatentransformation bzgl. der Standardbasis $\{x_1, x_2\}$ auf V.

In LA wird gezeigt: $\mathcal{O}_2(\mathbb{R})$ ist die Menge der Kongruenzabbildungen der Ebene, die den Ursprung fest lassen. Sie wird von der Drehung $\mathcal{O} = (0, 0)$ und den Spiegelungen an Ursprungsgeraden erzeugt. Längen und Winkel (bzgl. der euklidischen Norm) sind unter $\mathcal{O}_2(\mathbb{R})$ invariant.

Das Polynom $r = x_1^2 + x_2^2$ ist eine Invariante von $\mathcal{O}_2(\mathbb{R})$:

a) Für $\sigma_\alpha = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix}$ gilt:

$$\begin{aligned} \sigma_\alpha(r) &= [\cos(\alpha)x_1 + \sin(\alpha)x_2]^2 + [-\sin(\alpha)x_1 + \cos(\alpha)x_2]^2 \\ &= \cos^2(\alpha)x_1^2 + \sin^2(\alpha)x_2^2 + \sin^2(\alpha)x_1^2 + \cos^2(\alpha)x_2^2 \\ &= x_1^2 + x_2^2 \\ &= r \end{aligned}$$

b) Für $\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ gilt $\tau(r) = x_1^2 + (-x_2)^2 = r$.

c) Die Matrizen σ_α $(\alpha \in [0, 2\pi[)$ und τ erzeugen $\mathcal{O}_2(\mathbb{R})$.

Später zeigen wir: $P^G = \mathbb{R}\left[x_1^2 + x_2^2\right]$. Jede Invariante von $\mathcal{O}_2(\mathbb{R})$ ist also ein Polynom in $x_1^2 + x_2^2$.

1.6 Beispiel (Die euklidischen Invarianten von n Punkten in $\mathbb{R}^2$)

Sei wieder $K = \mathbb{R}$ und $V = \mathbb{R}^{2n}$. Die Elemente von V entsprechen n-Tupeln $(p_1, \ldots, p_n)$ von Punkten in $\mathbb{R}^2$. Wir betrachten die Gruppe G der Kongruenzabbildungen der Ebene. Sie wird von den Drehungen σ_α, der Spiegelung τ und den Verschiebungen λ_v erzeugt. Der Vektorraum V hat die Basis $\{x_1, y_1, x_2, y_2, \ldots, x_n, y_n\}$.

Die Gruppe G wird erzeugt von den

a) Drehungen

$$\sigma_\alpha = \begin{pmatrix} \mathcal{M}_\alpha & & 0 \\ & \ddots & \\ 0 & & \mathcal{M}_\alpha \end{pmatrix} \quad \text{mit} \quad \mathcal{M}_\alpha = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

b) Spiegelung(en)

$$\tau = \begin{pmatrix} J & & \\ & \ddots & \\ & & J \end{pmatrix} \quad \text{mit} \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

c) Translationen

$$\lambda_v : \begin{pmatrix} x_1 \\ \vdots \\ y_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 + a \\ y_1 + b \\ \vdots \\ x_n + a \\ y_n + b \end{pmatrix} \quad \text{mit} \quad v = (a, b)$$

Hier erhält man einen injektiven Gruppenhomomorphismus $G \hookrightarrow \mathrm{Bij}(V)$, der Menge der bijektiven Abbildungen.

Wir untersuchen nun diverse Polynome, ob sie G-invariant sind:

1) $f_1 = x_1^2 + y_1^2 - 7$ ist nicht translationsinvariant.

2) $f_2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$ (Abstand der ersten beiden Punkte p_1 und p_2) ist G-invariant, denn G ist längentreu.

3) $f_3 = x_1^2 + y_1^2 - x_1x_2 - y_1y_2 - x_1x_3 - y_1y_3 + x_2x_3 + y_2y_3$ ist G-invariant:

$$f_3 = \left\langle \begin{pmatrix} x_1 - x_2 \\ y_1 - y_2 \end{pmatrix}, \begin{pmatrix} x_1 - x_3 \\ y_1 - y_3 \end{pmatrix} \right\rangle$$

ist das Skalarprodukt der Richtungsvektoren der Geraden $\overline{p_1p_2}$ und $\overline{p_1p_3}$. Dieses misst ob die Geraden $\overline{p_1p_2}$ und $\overline{p_1p_3}$ senkrecht zueinander stehen.

Ein klassisches Resultat der Invariantentheorie besagt, dass

$$P^G = K[d_{12}, d_{13}, \ldots, d_{1,n}, d_{23}, \ldots, d_{2,n}, d_{34}, \ldots, d_{nn}] = \mathbb{R}[d_{ij} \mid 1 \le i < j \le n]$$

gilt mit $d_{ij} = (x_i - x_j)^2 + (y_i - y_j)^2 =$ Abstandsquadrat von p_i und p_j.

1.7 Beispiel (Die zyklische Gruppe C_4)

Sei $K = \mathbb{R}$, $V = \mathbb{R}^2$ und

$$G = C_4 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

Die Gruppe G ist zyklisch mit $G = \langle \sigma \rangle$ und $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ = Drehung um 90° im Uhrzeigersinn. Dann gilt

$$P^G = \{ f \in \mathbb{R}[x_1, x_2] \mid f(x_1, x_2) = f(-x_2, x_1) \}$$

Später werden wir zeigen, dass $P^G = \mathbb{R}[f_1, f_2, f_3]$ gilt mit

$$f_1 = x_1^2 + x_2^2, \quad f_2 = x_1^2 x_2^2 \quad \text{und} \quad f_3 = x_1^3 x_2 - x_1 x_2^3$$

Diese Invarianten sind nicht algebraisch unabhängig, denn $f_1^2 f_2 - 4f_2^2 - f_3^2 = 0$.

1.8 Beispiel (Die symmetrische Gruppe S_n)

Sei K ein Körper, $V = K^n$ und $G = S_n$ die symmetrische Gruppe, die auf V operiert durch Permutation der Vektoren der Standardbasis $\{x_1, \ldots, x_n\}$. Die Darstellungsmatrizen sind gerade die Permutationsmatrizen, d.h. für $\sigma \in S_n$ gelte $\sigma(x_i) = x_{\sigma(i)}$. Die invarianten Polynome sind die symmetrischen Polynome. In Alg wird gezeigt, dass die **elementarsymmetrischen Polynome**

$$\begin{aligned}
s_1 &= x_1 + \ldots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_2x_n + \ldots + x_{n-1}x_n \\
&= \sum_{1 \leq i_1 < i_2 \leq n} x_{i_1}x_{i_2} \\
s_3 &= \sum_{1 \leq i_1 < i_2 < i_3 \leq n} x_{i_1}x_{i_2}x_{i_3} \\
\vdots & \quad \vdots \\
s_n &= x_1x_2 \ldots x_{n-1}x_n
\end{aligned}$$

den Invariantenring P^G erzeugen, d.h. dass $P^G = K[s_1, \ldots, s_n]$ gilt. Ferner wird gezeigt, dass $\{s_1, \ldots, s_n\}$ algebraisch unabhängig ist.

1.9 Beispiel (Invarianten binärer Formen)

Sei K ein Körper der Charakteristik 0, sei $d \geq 2$ und sei

$$V_d = \left\{a_0x^d + a_1x^{d-1}y + \ldots + a_dy^d \mid a_0, \ldots, a_d \in K\right\} \subseteq K[x, y]$$

der Vektorraum der **binären Formen** vom Grad d.
Die Gruppe $G = \mathrm{SL}_2(K) = \{\mathcal{M} \in \mathrm{Mat}_2(K) \mid \det(\mathcal{M}) = 1\}$ operiere auf V_d durch

$$(\sigma(f))(x, y) = f(ax + cy, bx + dy) \quad \text{für} \quad \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Eine Invariante von G ist die **Diskriminante** des Polynoms $g = a_0x^d + a_1x^{d-1}y + \ldots + a_dy^d$, die wie folgt definiert ist: Über dem algebraischen Abschluss $\overline{K}$ schreibe

$$g = \prod_{i=1}^{d} (\alpha_i x + \beta_i y) \quad \text{mit} \quad \alpha_i, \beta_i \in \overline{K}$$

Dann setze

$$\Delta_d(g) = \prod_{1 \leq i < j \leq d} (\alpha_i\beta_j - \beta_i\alpha_j)^2 \in K[a_0, a_1, \ldots, a_d]$$

Es gilt: $\Delta_d(g) = 0$ genau dann, wenn g eine mehrfache Nullstelle in $\overline{K}$ besitzt.
Ferner gilt: $\Delta_d(g) \in K[a_0, a_1, \ldots, a_d]^G$.
Folgende Resultate sind bekannt:
a) $K[V_2]^G = K[\Delta_2]$ mit $\Delta_2 = a_1^2 - 4a_0a_2$.
b) $K[V_3]^G = K[\Delta_3]$ mit $\Delta_3 = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3$.
c) $K[V_4]^G = K[f_1, f_2]$ mit

$$\begin{aligned}
f_1 &= a_0a_4 - \frac{1}{4}a_1a_3 + \frac{1}{12}a_2^2 \\
f_2 &= \det \begin{pmatrix} a_0 & \frac{1}{4}a_1 & \frac{1}{6}a_2 \\ \frac{1}{4}a_1 & \frac{1}{6}a_2 & \frac{1}{4}a_3 \\ \frac{1}{6}a_2 & \frac{1}{4}a_3 & a_4 \end{pmatrix}
\end{aligned}$$

Hierbei gilt $\Delta_4 = 256 f_1^3 - 256 \cdot 27 f_2^2$.
d) $K\left[V_5\right]^G$, $K\left[V_6\right]^G$ und $K\left[V_8\right]^G$ sind dann ebenfalls explizit bekannt.