Kapitel IV: Invariantenberechnung für endliche Gruppen

10 Ist der Invariantenring einer endlichen Gruppe stets endlich erzeugt?

In diesem Abschnitt sei K ein Körper, V endlich-dimensionaler K-Vektorraum mit Basis $\{x_1, \ldots x_n\}$, sei $G \subseteq \mathrm{GL}_n(K)$ endliche Gruppe die auf V lineare operiert und sei $P = K[x_1, \ldots, x_n]$ standard-graduiert. Es gelte:

- Die Operation von G werde auf P fortgesetzt durch $f(x) \mapsto f(Ax)$
- $\mathrm{char}(K) \nmid \#G$ (nicht-modularer Fall)
- P^G sei der Invariantenring

10.1 Definition

Die Abbildung

$$\begin{aligned} \rho_G : P &\rightarrow P \\ f &\mapsto \frac{1}{\#G} \sum_{A \in G} f(Ax) \end{aligned}$$

heißt der **Reynolds-Operator** der Operation von G auf P.

10.2 Satz

Der Reynolds-Operator $\rho_G : P \to P$ hat die folgenden Eigenschaften:

(a) ρ_G ist K-linear und homogen.

(b) Für $f \in P^G$ gilt $\rho_G(f) = f$.

(c) Für $f \in P^G$ und $g \in P$ gilt

$$\rho_G(fg) = f\rho_G(g)$$

d.h. ρ_G ist sogar P^G-linear.

(d) $\rho_G^2 = \rho_G$, d.h. ρ_G ist eine Projektion auf P^G. Also gilt $\mathrm{Bild}(\rho_G) = P^G$.

Beweis:
Zu (a): K-linear: klar.
Homogen: Klar, da für homogenes f auch $f(Ax)$ homogen vom gleichen Grad ist.
Zu (b): Für $f \in P^G$ gilt:

$$\rho_G(f) = \frac{1}{\#G} \sum_{A \in G} f(Ax) \overset{(1)}{=} \frac{1}{\#G} \sum_{A \in G} f(x) = f(x)$$

Zu (1): Da f invariant ist.

Zu (c): Für $f \in P^G$ und $g \in P$ gilt:

$$\begin{aligned}\rho_G(fg) &= \frac{1}{\#G}\sum_{A\in G} f(Ax)\,g(Ax)\\ &= \frac{1}{\#G}\sum_{A\in G} f(x)\,g(Ax)\\ &= f(x)\,\frac{1}{\#G}\sum_{A\in G} g(Ax)\\ &= f(x)\,\rho_G(g)\end{aligned}$$

Zu (d):

$$\begin{aligned}\rho_G^2(f) &= \rho_G\left(\frac{1}{\#G}\sum_{A\in G} f(Ax)\right)\\ &= \frac{1}{\#G}\sum_{A\in G}\frac{1}{\#G}\sum_{B\in G} f(ABx)\\ &\overset{(1)}{=} \frac{1}{\#G}\sum_{A\in G}\frac{1}{\#G}\sum_{C\in G} f(Cx)\\ &= \frac{1}{\#G}\sum_{A\in G}\rho_G(f)\\ &\overset{(b)}{=} \rho_G(f)\end{aligned}$$

Zu (1): $C = AB$ und B durchläuft die Gruppe. □

10.3 Theorem (Hilberts Endlichkeitssatz)

Der Invariantenring P^G einer endlichen Gruppe G ist eine endlich erzeugte K-Algebra.
Beweis: Sei $I = \left\langle f \mid f \in P^G \backslash K\right\rangle$ das von den Invarianten positiven Grades erzeugte Ideal. Nach dem Hilbertschen Basissatz gibt es homogene Elemente $f_1, \ldots, f_s \in P^G$ positiven Grades mit $I = \langle f_1, \ldots, f_s\rangle$. Sei $A = K[f_1, \ldots, f_s] \subseteq P^G$.
Angenommen, es gilt gilt $\subsetneqq$. Sei $f \in P^G\backslash A$ homogen von minimalem Grad. Schreibe

$$f = \sum_{i=1}^{s} g_i f_i \in I$$

mit $g_i \in P$ homogen vom Grad $\deg(f) - \deg(f_i)$. Wende ρ_G an und erhalte

$$f = \rho_G(f) = \sum_{i=1}^{s} \rho_G(g_i)\, f_i$$

mit $\rho_G(g_i) \in P^G$ homogen von einem Grad $< \deg(f)$. Nach Konstruktion folgt $\rho_G(g_i) \in A$, also $f \in A$. Dies ist ein Widerspruch zur Annahme. □

10.4 Bemerkung

a) Ist G eine unendliche Gruppe für die es einen Reynolds-Operator mit den in Satz 10.2 angegebenen Eigenschaften gibt (d.h. eine **reduktive** Gruppe) so bleibt der Beweis von Theorem 10.3 korrekt und zeigt, dass P^G eine endlich erzeugte K-Algebra ist.

b) Der Beweis von Theorem 10.3 ist nicht konstruktiv. Er wird erst mit Hilfe des nächsten Theorems zu einem Algorithmus.

10.5 Theorem (Noethers Gradschranke)

Sei $\operatorname{char}(K) = 0$. Der Invariantenring P^G besitzt ein K-Algebra-Erzeugendensystem bestehend aus $\leq \binom{n + \#G}{n}$ homogenen fundamentalen Invarianten vom Grad $\leq \#G$.

Der Beweis verwendet das folgende Lemma:

10.6 Lemma

Für $1 \leq d \leq n$ sei s_d das elementarsymmetrische Polynom vom Grad d und für $d \geq 1$ sei $p_d = x_1^d \dots x_n^d$

a) Es gilt:

$$p_d - s_1 p_{d-1} + \dots + (-1)^{d-1} s_{d-1} p_1 + (-1)^d d s_d = 0$$

b) Gilt $d > n$ oder $\operatorname{char}(K) > d$ oder $\operatorname{char}(K) > n$, so folgt $s_d \in K[p_1, \dots, p_n]$.

Beweis:

Zu (a): Wir schließen mit vollständiger Induktion nach n.

$n = 1$: $p^d = x_1^d$, $s_1 = x_1$. Die Behauptung ist erfüllt, denn $x_1^d - x_1^d = 0$.

$n > 1$: Es gilt: $p_d = x_n^d + p_d'$ und $s_i = s_i' + x_n s_{i-1}'$. Dann folgt: