

## Invariantentheorie

### Vorlesung 19

#### Die Hilbert-Reihe und die Formel von Molien

Wir setzen nun die Untersuchung der Invariantenringe  $K[X_1, \dots, X_n]^G$  zu einer endlichen Gruppe  $G \subseteq \mathrm{GL}_n(K)$  fort. Insbesondere wollen wir charakterisieren, wann der Invariantenring ein Polynomring ist, wie das beispielsweise bei der symmetrischen Gruppe der Fall ist. Für diese Fragestellung ist das Konzept der Hilbert-Reihe hilfreich.

DEFINITION 19.1. Es sei  $K$  ein Körper und  $R$  eine positiv-graduierte kommutative  $K$ -Algebra mit der Eigenschaft, dass für jedes  $d \in \mathbb{N}$  die Stufe  $R_d$  endlichdimensional ist. Dann nennt man die Potenzreihe

$$\sum_{d=0}^{\infty} \dim_K(R_d) z^d$$

die *Hilbert-Reihe* von  $R$ .

Es handelt sich also um eine Potenzreihe mit Koeffizienten aus  $\mathbb{N}$ . Wir werden sie als formale Potenzreihe handhaben, Konvergenzuntersuchungen werden keine Rolle spielen. Die Hilbert-Reihe eines Polynomringes, wobei die Variablen positiven Grad besitzen, hat folgende Gestalt.

LEMMA 19.2. *Es sei  $K$  ein Körper und es sei  $R = K[X_1, \dots, X_n]$  der Polynomring über  $K$ , wobei die  $X_i$  den positiven Grad  $d_i \in \mathbb{N}_+$  haben mögen. Dann ist die Hilbert-Reihe dieses Ringes gleich*

$$H(R, z) = \frac{1}{(1 - z^{d_1}) \cdots (1 - z^{d_n})}.$$

*Beweis.* Die Monome  $X_1^{\nu_1} \cdots X_n^{\nu_n}$  vom Gesamtgrad  $d = \sum_{j=1}^n d_j \nu_j$  bilden eine  $K$ -Basis von  $R_d$ . Die Dimension der  $d$ -ten Stufe  $R_d$  ist also die Anzahl der Elemente in der Menge

$$A_d := \{(\nu_1, \dots, \nu_n) \in \mathbb{N}^n \mid \nu_1 d_1 + \dots + \nu_n d_n = d\}.$$

Die Behauptung folgt somit aus

$$\begin{aligned} \sum_{d=0}^{\infty} |A_d| z^d &= \sum_{d=0}^{\infty} \sum_{(\nu_1, \dots, \nu_n) \in A_d} z^d \\ &= \left( \sum_{\nu_1=0}^{\infty} z^{\nu_1 d_1} \right) \cdots \left( \sum_{\nu_n=0}^{\infty} z^{\nu_n d_n} \right) \end{aligned}$$

$$= \frac{1}{1 - z^{d_1}} \cdots \frac{1}{1 - z^{d_n}},$$

wobei wir im letzten Schritt die Formel für die geometrische Reihe verwendet haben.  $\square$

Die lineare Operation von einer endlichen Gruppe  $G$  auf einem  $K$ -Vektorraum  $V$  bzw. auf dem zugehörigen Polynomring  $R = K[V]$  induziert eine  $K$ -lineare Operation  $R_d \rightarrow R_d$  in jeder Stufe und der Invariantenring  $R^G$  ist selbst graduiert. Dies ermöglicht folgende Definition.

DEFINITION 19.3. Die endliche Gruppe  $G$  operiere linear auf dem Polynomring  $R = K[X_1, \dots, X_n]$ . Dann nennt man die Potenzreihe

$$\Phi_G(z) = \sum_{d=0}^{\infty} \dim_K (R_d^G) z^d$$

die *Hilbert-Reihe* (oder *Molien-Reihe*) zu dieser Operation.

Die Dimensionen der homogenen Stufen sind endlich und daher ist diese Definition sinnvoll. Die Hilbert-Reihe zur Operation ist einfach die Hilbert-Reihe des Invariantenringes.

Die Dimension des Fixraumes zu einer linearen Operation kann man über die Spur der einzelnen Automorphismen berechnen. Wir erinnern an die Definition der *Spur* einer Matrix und eines Endomorphismus.

DEFINITION 19.4. Es sei  $K$  ein Körper und sei  $M = (a_{ij})_{ij}$  eine  $n \times n$ -Matrix über  $K$ . Dann heißt

$$\text{Spur}(M) := \sum_{i=1}^n a_{ii}$$

die *Spur* von  $M$ .

DEFINITION 19.5. Es sei  $K$  ein Körper und sei  $V$  ein endlichdimensionaler  $K$ -Vektorraum. Es sei  $\varphi: V \rightarrow V$  eine lineare Abbildung, die bezüglich einer Basis durch die Matrix  $M$  beschrieben werde. Dann nennt man  $\text{Spur}(M)$  die *Spur* von  $\varphi$ , geschrieben  $\text{Spur}(\varphi)$ .

Diese Definition ist unabhängig von der gewählten Basis, siehe Aufgabe 19.5.

LEMMA 19.6. *Es sei  $K$  ein Körper und  $V$  ein endlichdimensionaler  $K$ -Vektorraum, auf dem eine endliche Gruppe  $G$  linear und treu operiere. Die Gruppenordnung sei kein Vielfaches der Charakteristik von  $K$ . Dann besitzt der Fixraum der Operation (also der gemeinsame Eigenraum zum Eigenwert 1) die Dimension*

$$\dim_K (V^G) = \frac{1}{|G|} \sum_{\sigma \in G} \text{Spur}(\sigma).$$

*Beweis.* Wir betrachten die lineare Abbildung

$$\pi = \frac{1}{|G|} \sum_{\sigma \in G} \sigma.$$

Zu  $w \in V$  ist  $\pi(w)$   $G$ -invariant und für  $v \in V^G$  ist  $\pi(v) = v$ . Daher ist  $\pi$  eine lineare Projektion

$$V \longrightarrow V^G.$$

Eine lineare Projektion wird in einer geeigneten Basis durch eine Diagonalmatrix beschrieben, in der  $m = \dim_K(V^G)$  Einsen und sonst Nullen stehen. Also ist  $\text{Spur}(\pi) = m$ . Die Behauptung folgt daraus, dass die Spur additiv ist.  $\square$

Der folgende Satz berechnet die Hilbert-Reihe (Formel von Molien).

**SATZ 19.7.** *Es sei  $K$  ein algebraisch abgeschlossener Körper der Charakteristik 0. Die endliche Gruppe  $G$  operiere linear auf einem endlichdimensionalen  $K$ -Vektorraum  $V$ . Dann ist*

$$\Phi_G(z) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det(\text{Id} - z\sigma)}.$$

*Beweis.* Der lineare Automorphismus  $\sigma$  ist nach Satz 3.19 diagonalisierbar, da er endliche Ordnung hat. In einer geeigneten Basis besitzt die duale Abbildung  $\sigma^*$  die Gestalt

$$X_i \longmapsto \xi_i X_i.$$

Auf der  $d$ -ten Stufe induziert dies den linearen Automorphismus

$$\sigma^{(d)}: K[V]_d \longrightarrow K[V]_d$$

mit  $X^\nu \longmapsto \xi^\nu X^\nu$ . Die Eigenvektoren von  $\sigma^{(d)}$  sind die  $\binom{n+d-1}{d}$  verschiedenen Monome

$$X_1^{\nu_1} \cdots X_n^{\nu_n}$$

(es sei  $n = \dim_K(V)$ ) mit  $\nu_1 + \dots + \nu_n = d$  mit den Eigenwerten  $\xi_1^{\nu_1} \cdots \xi_n^{\nu_n}$ . Die Spur von  $\sigma^{(d)}$  ist daher

$$\text{Spur}(\sigma^{(d)}) = \sum_{|\nu|=d} \xi^\nu.$$

Nach Lemma 19.6 ergibt sich

$$\dim_K(K[V]_d^G) = \frac{1}{|G|} \sum_{\sigma \in G} \text{Spur}(\sigma^{(d)})$$

mit

$$\text{Spur}(\sigma^{(d)}) = \sum_{\nu_1 + \dots + \nu_n = d} \xi_1^{\nu_1} \cdots \xi_n^{\nu_n}.$$

Damit ist unter Verwendung der geometrischen Reihe

$$\begin{aligned}
\Phi_G(z) &= \sum_{d=0}^{\infty} \left( \frac{1}{|G|} \sum_{\sigma \in G} \text{Spur}(\sigma^{(d)}) \right) z^d \\
&= \frac{1}{|G|} \sum_{d=0}^{\infty} \left( \sum_{\sigma \in G} \sum_{\nu_1 + \dots + \nu_n = d} \xi_{\sigma,1}^{\nu_1} \dots \xi_{\sigma,n}^{\nu_n} \right) z^d \\
&= \frac{1}{|G|} \sum_{\sigma \in G} \sum_{(\nu_1, \dots, \nu_n) \in \mathbb{N}^n} \xi_{\sigma,1}^{\nu_1} \dots \xi_{\sigma,n}^{\nu_n} z^{\nu_1 + \dots + \nu_n} \\
&= \frac{1}{|G|} \sum_{\sigma \in G} \left( \sum_{\nu_1=0}^{\infty} \xi_{\sigma,1}^{\nu_1} z^{\nu_1} \right) \dots \left( \sum_{\nu_n=0}^{\infty} \xi_{\sigma,n}^{\nu_n} z^{\nu_n} \right) \\
&= \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{(1 - z\xi_{\sigma,1}) \dots (1 - \xi_{\sigma,n})} \\
&= \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det(\text{Id} - z\sigma)}.
\end{aligned}$$

□

Die Formel besagt insbesondere, dass diese Potenzreihe eine rationale Funktion (also ein Quotient aus zwei Polynomen) ist und daher nur endlich viele Polstellen hat. Die Nennerpolynome in den Summanden erinnern an die charakteristischen Polynome der Gruppenelemente, doch steht hier die Variable bei der linearen Abbildung, nicht bei der Identität.

### Der Satz von Chevalley-Shephard-Todd

Wir wenden uns nun der Charakterisierung derjenigen linearen Operationen auf dem Polynomring zu, die zu einem Invariantenring führen, der selbst ein Polynomring ist.

DEFINITION 19.8. Ein linearer Automorphismus auf einem endlichdimensionalen  $K$ -Vektorraum heißt *Pseudoreflektion* (oder *Pseudospiegelung*), wenn er in einer geeigneten Basis durch eine Matrix der Form

$$\begin{pmatrix}
1 & 0 & \dots & \dots & 0 \\
0 & 1 & 0 & \dots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & \dots & 0 & 1 & 0 \\
0 & \dots & \dots & 0 & \zeta
\end{pmatrix},$$

wobei  $\zeta \neq 1$  eine Einheitswurzel ist, beschrieben werden kann.

Eine Pseudoreflektion besitzt also eine Hyperebene (einen  $(n-1)$ -dimensionalen Untervektorraum), auf der sie fix ist (der Eigenraum zum Eigenwert 1) und einen weiteren dazu linear unabhängigen Eigenvektor zum Eigenwert  $\zeta$ .

Die Ordnung der Einheitswurzel  $\zeta$  bestimmt auch die Ordnung der Pseudoreflektion. Das Inverse einer Pseudoreflektion ist wieder eine Pseudoreflektion.

**DEFINITION 19.9.** Eine endliche Untergruppe  $G \subseteq \mathrm{GL}_n(K)$  heißt *Reflektionsgruppe* (oder *Spiegelungsgruppe*), wenn sie durch Pseudoreflektionen erzeugt wird.

Man beachte, dass dies keine Eigenschaft der (abstrakten) Gruppe  $G$  ist, sondern eine Eigenschaft der Untergruppe  $G \subseteq \mathrm{GL}_n(K)$ . In einer Reflektionsgruppe kann man jedes Element  $\tau$  als ein Produkt  $\tau = \sigma_1 \cdots \sigma_k$  mit Pseudoreflektionen  $\sigma_j$  schreiben.

Die Bedeutung von Reflektionsgruppen in der Invariantentheorie kommt im folgenden wichtigen Satz, dem *Satz von Chevalley-Shephard-Todd*, zum Ausdruck.

**SATZ 19.10.** *Es sei  $K$  ein algebraisch abgeschlossener Körper der Charakteristik null. Die endliche Gruppe  $G$  operiere linear und treu auf dem  $K$ -Vektorraum  $V$ . Dann sind folgende Aussagen äquivalent.*

- (1)  $G \subseteq \mathrm{GL}_n(K)$  ist eine Reflektionsgruppe.
- (2) Der Invariantenring  $K[X_1, \dots, X_n]^G$  ist (isomorph zu einem) ein Polynomring (in  $n$  Variablen).

Aus Dimensionsgründen ist klar, dass wenn der Invariantenring ein Polynomring ist, dieser  $n$  Variablen besitzt. Der Beweis dieses Satzes benutzt verschiedene Lemmata und verwendet die Theorie der Hilbert-Reihen. Hierbei werden verschiedene elementare Hilfsmittel aus der Theorie der Potenzreihen verwendet.

**LEMMA 19.11.** *Es sei  $K$  ein algebraisch abgeschlossener Körper und  $\sigma \in \mathrm{GL}_n(K)$  eine Pseudoreflektion. Es sei  $H_\sigma$  der Fixraum zu  $\sigma$  und  $L_\sigma$  eine Linearform  $\neq 0$ , die auf  $H_\sigma$  verschwindet. Dann ist  $L_\sigma$  für jedes Polynom  $f \in K[X_1, \dots, X_n]$  ein Teiler von  $f\sigma - f$ .*

*Beweis.* Für  $v \in H_\sigma$  ist

$$(f\sigma - f)(v) = f(\sigma v) - f(v) = f(v) - f(v) = 0.$$

Das Polynom  $f\sigma - f$  verschwindet also auf der Nullstellenmenge von  $L_\sigma$ . Wir können  $L_\sigma$  zu einer Variablenmenge  $L_\sigma, L_2, \dots, L_n$  ergänzen und

$$f\sigma - f = P(L_\sigma, L_2, \dots, L_n)L_\sigma + Q(L_2, \dots, L_n)$$

schreiben. Das Polynom  $Q$  verschwindet auf  $H_\sigma$  und ist somit die Nullfunktion, also muss es auch das Nullpolynom sein, da der Körper unendlich ist.  $\square$

**LEMMA 19.12.** *Es sei  $K$  ein algebraisch abgeschlossener Körper der Charakteristik 0 und  $G \subseteq \mathrm{GL}_n(K)$  eine Reflektionsgruppe. Es sei  $I_G$  das Ideal in*

$K[X_1, \dots, X_n]$ , das durch die homogenen Invarianten von einem positiven Grad erzeugt wird. Es gelte

$$g_1 h_1 + \dots + g_m h_m = 0,$$

wobei die  $h_1, \dots, h_m \in K[X_1, \dots, X_n]$  homogene Polynome und die  $g_1, \dots, g_m \in K[X_1, \dots, X_n]^G$  invariante Polynome seien. Dann ist  $h_1 \in I_G$  oder  $g_1 \in (g_2, \dots, g_m)$ .

*Beweis.* Wir führen Induktion über den Grad von  $h_1$ . Bei  $h_1 = 0$  gehört natürlich  $h_1$  zu  $I_G$ . Für  $h_1 \neq 0$  und  $\text{grad}(h_i) = 0$  ist  $g_1 \in (g_2, \dots, g_m)$ . Sei also  $\text{grad}(h_1) \geq 1$  und die Aussage für kleineren Grad bewiesen. Es sei  $g_1 \notin (g_2, \dots, g_m)$  vorausgesetzt und es sei  $\sigma \in G$  eine Pseudoreflektion. Dann ist

$$\sum_{i=1}^m g_i \cdot (h_i \sigma) = \left( \sum_{i=1}^m g_i h_i \right) \sigma = 0 \sigma = 0.$$

Nach Lemma 19.11 kann man

$$h_i \sigma = h_i + L_\sigma \cdot \tilde{h}_i$$

schreiben, wobei  $L_\sigma$  eine beschreibende Linearform des Fixraumes zu  $\sigma$  ist und  $\tilde{h}_i$  einen kleineren Grad als  $h_i$  besitzt. Wir schreiben die obige Gleichung als

$$0 = \sum_{i=1}^m g_i (h_i + L_\sigma \tilde{h}_i) = L_\sigma \sum_{i=1}^m g_i \tilde{h}_i.$$

Daher ist die Summe rechts gleich 0 und nach Induktionsvoraussetzung ist  $\tilde{h}_1 \in I_G$ , also auch  $h_1 \sigma - h_1 = \tilde{h}_1 L_\sigma \in I_G$ .

Sei nun  $\tau = \sigma_1 \cdots \sigma_k \in G$  ein Produkt von Pseudoreflektionen. Dann ist

$$\begin{aligned} h_1 \tau - h_1 &= \sum_{i=1}^k (h_1 \sigma_i \cdots \sigma_k - h_1 \sigma_{i+1} \cdots \sigma_k) \\ &= \sum_{i=1}^k (h_1 \sigma_i - h_1) (\sigma_{i+1} \cdots \sigma_k). \end{aligned}$$

Da  $h_1 \sigma_i - h_1$  zu  $I_G$  gehört und  $I_G$  unter  $G$  invariant ist, gehört auch  $h_1 \tau - h_1$  zu  $I_G$ . Mit dem Reynolds-Operator  $\rho$  ist

$$\rho(h_1) - h_1 = \left( \frac{1}{|G|} \sum_{\tau \in G} h_1 \tau \right) - h_1 = \frac{1}{|G|} \sum_{\tau \in G} (h_1 \tau - h_1).$$

Dies gehört zu  $I_G$  und wegen  $\rho(h_1) \in I_G$  ist auch  $h_1 \in I_G$ . □