Prof. Dr. H. Brenner **Osnabrück WS 2012/2013**

Invariantentheorie

Vorlesung 6

Die alternierende Gruppe

Wir haben gesehen, dass der Invariantenring zur Operation der symmetrischen Gruppe S_n auf dem Polynomring isomorph zum Polynomring in den elementarsymmetrischen Polynomen ist. Eine wichtige Untergruppe der symmetrischen Gruppe ist die alternierende Gruppe $A_n \subseteq S_n$, an deren Definition wir erinnern.

DEFINITION 6.1. Zu $n \in \mathbb{N}$ heißt die Untergruppe

$$A_n := \{\sigma \in S_n | \operatorname{sgn}(\sigma) = 1\}$$

der geraden Permutationen die *alternierende Gruppe*.

Die alternierende Gruppe ist der Kern des Signumshomomorphismus und damit ein Normalteiler. Die A_n operiert wie die S_n auf dem Polynomring $K[X_1,\ldots,X_n]$. Wir interessieren uns für den Invariantenring $K[X_1,\ldots,X_n]^{A_n}$. Nach Proposition 5.1 (1) haben wir die Inklusionen

$$K[E_1,\ldots,E_n] \cong K[X_1,\ldots,X_n]^{S_n} \subseteq K[X_1,\ldots,X_n]^{A_n} \subseteq K[X_1,\ldots,X_n].$$

Zur Beschreibung des Invariantenringes unter der alternierenden Gruppe ist der Begriff der relativen Invarianten bezüglich eines Charakters sinnvoll.

Relative Invarianten

DEFINITION 6.2. Es sei K ein Körper und R eine kommutative K-Algebra, auf der eine Gruppe G als Gruppe von K-Algebraautomorphismen operiere. Es sei

$$\chi\colon G \longrightarrow K^\times$$

ein Charakter auf G. Dann nennt man

$$R_\chi^G := \{f \in R | f\sigma = \chi(\sigma) \cdot f \text{ für alle } \sigma \in G\}$$

die χ-*relativen Invarianten* oder *Semiinvarianten* bezüglich χ.

Der Invariantenring ist also die Menge der Invarianten relativ zum trivialen Charakter. Die χ-relativen Invarianten sind ein R^G-Untermodul von R. Wenn nämlich g invariant und f χ-invariant ist, so ist

$$(gf)\sigma = (g)\sigma \cdot (f)\sigma = g\chi(\sigma)f.$$

Der Invariantenring zur alternierenden Gruppe

LEMMA 6.3. *Es sei K ein Körper der Charakteristik $\neq 2$. Dann gilt für die natürliche Operation der Permutationsgruppe S_n auf dem K^n die Gleichheit*

$$K[X_1, \ldots, X_n]^{S_n}_{\mathrm{sgn}} \;=\; K[X_1, \ldots, X_n]^{S_n} \cdot \triangle,$$

wobei $\triangle = \prod_{j<i}(X_i - X_j)$ die Vandermondesche Determinante ist.

Beweis. Das Polynom $\triangle$ hat offenbar die Eigenschaft, dass es signumsinvariant ist, dass sich also sein Vorzeichen bei einer ungeraden Permutation umkehrt. Hierzu muss man sich nur klar machen, dass sich bei einer Transposition das Vorzeichen um -1 ändert. Dabei kann man sich sogar auf solche Transpositionen beschränken, die zwei Nachbarn i und $i+1$ miteinander vertauschen. Dann wird aus dem Faktor $X_{i+1} - X_i$ der Faktor $X_i - X_{i+1}$ und alle anderen Faktoren werden allenfalls vertauscht. Insgesamt wird $\triangle$ auf $-\triangle$ abgebildet. Wir müssen also zeigen, dass jedes signumsinvariante Polynom F ein Vielfaches von $\triangle$ ist. Der andere Faktor ist dann automatisch invariant.

Für diese Teilerbeziehung genügt es wegen der Faktorialität von $K[V]$ zu zeigen, dass $X_i - X_j$ ein Teiler von F ist $(i \neq j)$. Wir schreiben F in den neuen Variablen $X_k, k \neq i, j, X_i + X_j, X_i - X_j$ als

$$F \;=\; \sum_{n=0}^{m} G_n\left(X_k, X_i + X_j\right)\left(X_i - X_j\right)^n.$$

Dann ist einerseits

$$F(X_i \mapsto X_j) \;=\; \sum_{n=0}^{m} (-1)^n G_n\left(X_k, X_i + X_j\right)\left(X_i - X_j\right)^n$$

und anderseits (da F signumsinvariant ist)

$$F(X_i \mapsto X_j) \;=\; -F \;=\; -\sum_{n=0}^{m} G_n\left(X_k, X_i + X_j\right)\left(X_i - X_j\right)^n.$$

Daraus folgt wegen $\mathrm{char}(K) \neq 2$, dass für n gerade $G_n = 0$ sein muss. Insbesondere ist $G_0 = 0$. Also ist $F = H\left(X_i - X_j\right)$, wie behauptet. □

Noch einmal explizit: Es geht um die Polynome, die relativ zur Signumsabbildung invariant sind, für die also

$$F\sigma \;=\; \mathrm{sgn}(\sigma) F$$

für alle Permutationen gilt. Für eine gerade Permutation σ muss also

$$F\sigma \;=\; F$$

sein, für eine ungerade Permutation dagegen

$$F\sigma \;=\; -F.$$

Insbesondere sind solche Polynome invariant unter der alternierenden Gruppe.

Satz 6.4. *Es sei K ein Körper der Charakteristik* $\mathrm{char}(K) \neq 2$. *Die alternierende Gruppe A_n operiere natürlich auf $V = K^n$. Dann ist*

$$K[V]^{A_n} = K[V]^{S_n} \oplus K[V]^{S_n}_{\mathrm{sgn}} = K[E_1, \ldots, E_n] \oplus K[E_1, \ldots, E_n] \cdot \triangle.$$

Beweis. Die Gleichheit rechts ergibt sich aus Satz 1.7 und Lemma 6.3. Auf $K[V]^{A_n}$ operiert die Restklassengruppe $S_n/A_n = \{1, -1\} = \mathbb{Z}/(2)$ wie in Proposition 5.1 beschrieben. Sei τ das nichttriviale Element daraus. Dieses wird repräsentiert durch eine beliebige ungerade Permutation, etwa durch eine Transposition. Sei $F \in K[V]^{A_n}$ ein Polynom, das invariant unter der alternierenden Gruppe ist. Nach Proposition 5.1 (3) ist $F\tau$ unabhängig von dem gewählten Repräsentanten τ. Es ist

$$F = \frac{1}{2}(F + F\tau) + \frac{1}{2}(F - F\tau),$$

wobei die beiden Summanden symmetrisch bzw. signumsinvariant sind. Dies überprüft man, indem man die (geraden oder ungeraden) Permutationen darauf anwendet. Die Summe ist direkt, da der Durchschnitt 0 ist: Ein Polynom, das sowohl symmetrisch als auch signumsinvariant ist, muss 0 sein. □

Beispiel 6.5. Die natürliche Operation der alternierenden Gruppe $A_3 \cong \mathbb{Z}/(3)$ auf dem K^3 wird durch den Zykel

$$e_1 \longmapsto e_2,\ e_2 \longmapsto e_3,\ e_3 \longmapsto e_1$$

erzeugt. Besitzt K dritte primitive Einheitswurzeln, so kann man die zugehörige Matrix diagonalisieren und man erhält eine neue Basis mit den Eigenvektoren

$$e_1 + e_2 + e_3,\ e_1 + \zeta e_2 + \zeta^2 e_3,\ e_1 + \zeta^2 e_2 + \zeta e_3\,.$$

Wir führen die neuen Variablen

$$U = X + Y + Z,\ V = X + \zeta Y + \zeta^2 Z,\ W = X + \zeta^2 Y + \zeta Z$$

ein. In dieser Basis ist der erzeugende Automorphismus durch

$$U \longmapsto U,\ V \longmapsto \zeta V,\ W \longmapsto \zeta^2 W$$

gegeben und der Invariantenring ist in dieser Basis gleich

$$K[U, V^3, VW, W^3]\,.$$

Die einzige Relation ist gegeben durch $V^3W^3 = (VW)^3$.

Wie sieht der Unterring der symmetrischen Polynome aus? Die Transposition $Y \leftrightarrow Z$ lässt U unverändert und vertauscht V und W. Das bedeutet für den alternierenden Invariantenring, dass V^3 und W^3 vertauscht werden. Der symmetrische Invariantenring ist daher

$$K[U, VW, V^3 + W^3]\,.$$

Dabei sind

$$VW = X^2 + Y^2 + Z^2 + \zeta XY + \zeta^2 XY + \zeta XZ + \zeta^2 XZ + \zeta YZ + \zeta^2 YZ,$$

$$V^3 = X^3 + Y^3 + Z^3 + 6XYZ + 3\xi^2 XY^2 + 3\xi X^2 Y + 3\xi XZ^2 + 3\xi^2 X^2 Z + 3\xi^2 YZ^2 + 3\xi Y^2 Z$$

und

$$W^3 = X^3 + Y^3 + Z^3 + 6XYZ + 3\xi XY^2 + 3\xi^2 X^2 Y + 3\xi^2 XZ^2 + 3\xi X^2 Z + 3\xi YZ^2 + 3\xi^2 Y^2 Z.$$

Für die Vandermondsche Determinante gilt

$$\begin{aligned} \triangle &= (Y-X)(Z-X)(Z-Y) \\ &= XY^2 - X^2 Y + X^2 Z - XZ^2 + YZ^2 - Y^2 Z \\ &= \frac{1}{3(\xi^2 - \xi)} \left(V^3 - W^3\right). \end{aligned}$$

Reynolds-Operator

DEFINITION 6.6. Es sei $R \subseteq S$ ein Unterring eines kommutativen Ringes S. Man sagt, das R ein *direkter Summand* von S ist, wenn es einen R-Modul M gibt mit $S \cong R \oplus M$ (es liegt also ein R-Modulisomorphismus vor).

Diese Eigenschaft ist äquivalent dazu, dass es einen R-Modulhomomorphismus

$$\psi\colon\ S \longrightarrow R$$

mit $\psi \circ \iota = \mathrm{id}_R$ gibt. Eine stärkere Eigenschaft ist die Existenz eines Ringhomomorphismus

$$\psi\colon\ S \longrightarrow R$$

mit $\psi \circ \iota = \mathrm{id}_R$.

BEISPIEL 6.7. Es sei K ein Körper und A eine von 0 verschiedene K-Algebra. Dann ist K ein direkter Summand von A. Dies beruht darauf, dass man die 1 zu einer K-Basis von A ergänzen kann. Mit dem von den anderen Basiselementen erzeugten K-Untervektorraum $V \subset A$ ist dann $A \cong K \cdot 1 \oplus V$. Im Allgemeinen muss es aber keinen K-Algebrahomomorphismus $A \to K$ geben. Bei einer (nichttrivialen) Körpererweiterung $K \subset L$ gibt es keinen Ringhomomorphismus von L nach K.

Für einen Invariantenring $R^G \subseteq R$ nennt man einen R^G-Modulhomomorphismus

$$\rho\colon\ R \longrightarrow R^G$$

mit $\rho \circ \iota = \mathrm{Id}_{R^G}$ auch einen *Reynolds-Operator*. Ein Reynolds-Operator muss im Allgemeinen nicht existieren, er existiert aber unter der folgenden Bedingung.

LEMMA 6.8. *Es sei G eine endliche Gruppe, die auf einer kommutativen K-Algebra R als Gruppe von K-Algebraautomorphismen operiere. Die Gruppenordnung sei kein Vielfaches der Charakteristik von K. Dann ist die Abbildung*

$$\rho\colon\ R \longrightarrow R^G,\ f \longmapsto \frac{1}{\#(G)} \sum_{\sigma \in G} f\sigma,$$

ein Reynolds-Operator. Insbesondere ist $R^G \subseteq R$ ein direkter Summand.

Beweis. Aufgrund der Voraussetzung an die Charakteristik ist $\#(G)$ eine Einheit in K und damit in R, also ist die angegebene Abbildung wohldefiniert. Die Abbildung ist offenbar ein Gruppenhomomorphismus. Für $g \in R^G$ und $f \in R$ ist ferner

$$\begin{aligned}
\rho(gf) &= \frac{1}{\#(G)} \sum_{\sigma \in G} (gf)\sigma \\
&= \frac{1}{\#(G)} \sum_{\sigma \in G} (g\sigma)(f\sigma) \\
&= \frac{1}{\#(G)} \sum_{\sigma \in G} g(f\sigma) \\
&= g\left(\frac{1}{\#(G)} \sum_{\sigma \in G} f\sigma \right) \\
&= g\rho(f),
\end{aligned}$$

daher liegt ein R^G-Modulhomomorphismus vor. Für $g \in \mathbb{R}^G$ ist

$$\rho(g) \,=\, \frac{1}{\#(G)} \sum_{\sigma \in G} g\sigma \,=\, \frac{1}{\#(G)} \sum_{\sigma \in G} g \,=\, \frac{1}{\#(G)} \left(\#(G)g\right) \,=\, g,$$

also ist

$$\rho \circ \iota \,=\, \mathrm{Id}_{R^G}\,.$$

□

Die Bedingung, dass die Gruppenordnung zur Charakteristik teilerfremd ist, ist für viele Resultate der Invariantentheorie eine wesentliche Voraussetzung. Der andere Fall, dass die Gruppenordnung ein Vielfaches der Charakteristik ist, bildet ein eigenes Kapitel der Invariantentheorie, und besitzt sogar einen eigenen Namen. Man spricht von *modularer Invariantentheorie*.

BEISPIEL 6.9. Es sei K ein Körper der Charakteristik 0 und $A = K[X,Y]$. Auf der A-Algebra

$$B \,=\, A[S,T]/(XS+YT+1) \,=\, K[X,Y,S,T]/(XS+YT+1)$$

operiert die additive Gruppe $(K,+)$, indem ein $\lambda \in K$ durch

$$X \mapsto X,\ Y \mapsto Y,\ S \mapsto S+\lambda Y,\ T \mapsto T-\lambda X$$

wirkt. Wegen

$$X(S+\lambda Y)+Y(T-\lambda X) \;=\; XS+YT \;=\; -1$$

sind diese zunächst auf $K[X,Y,S,T]$ definierten Ringautomorphismen auch auf der Restklassenalgebra Automorphismen. Der Invariantenring ist $A = K[X,Y]$, wobei die Inklusion

$$A \;\subseteq\; B^G$$

unmittelbar klar ist. Zum Beweis der Umkehrung betrachten wir die Nenneraufnahme $A \to A_X$ und $B \to B_X$. Es ist

$$B_X \;=\; \left(K[X,Y,S,T]/(XS+YT+1)\right)_X \;\cong\; \left(A_X[S,T]\right)/(XS{+}YT{+}1) \;\cong\; A_X[T],$$

wobei beim letzten Isomorphismus S auf $\frac{-1-YT}{X}$ abgebildet wird. Ebenso ist $B_Y \cong A_Y[S]$. Die Operation lässt sich auf diese beiden Nenneraufnahmen fortsetzen. Für die Operation auf $B_X = A_X[T]$ ist A_X der Invariantenring. Zu einem $\lambda \in K$, $\lambda \neq 0$, wird ein Polynom

$$F \;=\; a_0 + a_1T + \ldots + a_{n-1}T^{n-1} + a_nT^n$$

auf

$$a_0 + a_1(T-\lambda X) + \ldots + a_{n-1}(T-\lambda X)^{n-1} + a_n(T-\lambda X)^n$$

abgebildet. Bei $n \geq 1$ ist der Koeffizient zu T^{n-1}

$$a_{n-1} - n\lambda X a_n$$

und dies ist bei $\lambda \neq 0$ nicht gleich a_{n-1}. Also ist ein solches Polynom nicht invariant. Das gleiche Argument gilt für $A_Y \subseteq A_Y[S] = B_Y$.

Es sei nun $F \in B$ invariant. Dann ist F auch als Element in B_X bzw. in B_Y invariant und daher ist sowohl $F \in A_Y$ als auch $F \in A_X$. Aus

$$F \;=\; \frac{G}{X^n} \;=\; \frac{H}{Y^m}$$

folgt

$$GY^m \;=\; HX^n$$

und aus der Faktorialität von $K[X,Y]$ ergibt sich, dass G ein Vielfaches von X^n sein muss. Somit gehört F zu A. Der Invariantenring ist also A. Dieser ist aber kein direkter Summand in B. Es ist $1 \notin (X,Y)$ in A, aber $1 \in (X,Y)$ in B, was unmittelbar aus der definierenden Gleichung $XS+YT=-1$ folgt. Nach Aufgabe 6.9 kann daher kein direkter Summand vorliegen.