

Invariantentheorie

In dieser Vorlesung möchten wir Monoidringe als Invariantenringe zu einer Gruppenoperation auf einem Polynomring realisieren, wobei wir den Weg über graduierte Ringe beschreiten. Wir zitieren den folgenden Satz, das sogenannte *Lemma von Gordan*, das eine Beziehung zwischen (normalen, torsionsfreien, endlich erzeugten) Monoiden (mit Kürzungsregel) und endlich erzeugten rationalen konvexen Kegeln stiftet. Ein solcher (polyedrischer) Kegel besteht aus allen Linearkombinationen mit nichtnegativen Koeffizienten zu einer endlichen Familie von Vektoren im \mathbb{Q}^n . Er heißt *spitz*, wenn er abgesehen vom Nullpunkt vollständig in einem Halbraum liegt. Ein solcher Kegel ist der Durchschnitt von endlich vielen Halbräumen (auch dies ist ein Satz aus der Theorie der polyedrischen Kegel).

- SATZ 9.1. (1) *Es sei $M \subseteq \mathbb{Z}^n$ ein normales endlich erzeugtes Monoid und $C = \mathbb{Q}_{\geq 0}M$ der zugehörige rationale Kegel. Dann ist $M = \Gamma \cap C$, wobei $\Gamma \subseteq \mathbb{Z}^n$ das Differenzengitter zu M ist.*
- (2) *Wenn umgekehrt $\Gamma \subseteq \mathbb{Q}^n$ eine endlich erzeugte Untergruppe und $C \subseteq \mathbb{Q}^n$ ein endlich erzeugter rationaler Kegel ist, so ist der Durchschnitt $M = \Gamma \cap C$ ein normales endlich erzeugtes Monoid.*

Statt im \mathbb{Q}^n kann man genauso gut im \mathbb{R}^n arbeiten, allerdings wird verlangt, dass die Kegel von Vektoren mit rationalen Koordinaten erzeugt werden.

Normale Monoidringe als Invariantenringe

Wir betrachten auf dem Polynomring $K[X_1, \dots, X_r]$ Graduierungen, die aus der feinen Graduierung, bei der die Variable X_i den Grad $e_i \in \mathbb{Z}^r$ bekommt, hervorgehen, indem man einen Gruppenhomomorphismus

$$\delta: \mathbb{Z}^r \longrightarrow D$$

in eine kommutative Gruppe D fixiert (den man als surjektiv voraussetzen darf). Dies ergibt eine D -Graduierung des Polynomrings, bei der der Grad der Variable X_i durch

$$\delta(X_i) := \delta(e_i)$$

festgelegt ist. Die neutrale Stufe dieses so graduierten Polynomrings besteht aus den Linearkombinationen aller Monome $X_1^{a_1} \cdots X_r^{a_r}$, deren Exponententupel $(a_1, \dots, a_r) \in \mathbb{Z}^r$ unter δ auf $0 \in D$ abgebildet wird. Die neutrale Stufe wird also durch den Kern von δ vollständig beschrieben. Wenn umgekehrt eine Untergruppe $\Delta \subseteq \mathbb{Z}^r$ gegeben ist, so kann man die Restklassenabbildung

$$\mathbb{Z}^r \longrightarrow \mathbb{Z}^r / \Delta =: D$$

betrachten und erhält so einen D -graduierten Ring.

SATZ 9.2. *Es sei K ein Körper. Für eine kommutative K -Algebra R sind folgende Aussagen äquivalent.*

- (1) *R ist ein K -Monoidring zu einem endlich erzeugten, torsionsfreien, normalen, spitzen Monoid mit Kürzungsregel.*
- (2) *R ist die neutrale Stufe einer D -Graduierung eines Polynomringes $K[X_1, \dots, X_r]$, wobei die Graduierung durch einen surjektiven Gruppenhomomorphismus*

$$\delta: \mathbb{Z}^r \longrightarrow D$$

gegeben ist.

Beweis. (1) \Rightarrow (2). Sei $R = K[M]$ mit einem kommutativen Monoid M , das die angegebenen Eigenschaften erfüllt. Dann gibt es nach Satz 9.1 (1) einen reellen Raum \mathbb{R}^n und einen spitzen rationalen polyedrischen Kegel $C \subset \mathbb{R}^n$ derart, dass $M = \mathbb{Z}^n \cap C$ ist (dabei kann man \mathbb{Z}^n als das Differenzengitter zu M wählen). Ein solcher Kegel ist der Durchschnitt von endlich vielen Halbräumen H_j , $j = 1, \dots, r$. Diese Halbräume kann man mit der Hilfe von linearen Abbildungen

$$\pi_j: \mathbb{R}^n \longrightarrow \mathbb{R}$$

durch

$$H_j = \pi_j^{-1}(\mathbb{R}_{\geq 0})$$

realisieren. Wegen der Rationalität kann man die π_j sogar als ganzzahlig, also als Abbildungen von \mathbb{Z}^n nach \mathbb{Z} , ansetzen. Dies führt zu einem Gruppenhomomorphismus

$$\pi: \mathbb{Z}^n \longrightarrow \mathbb{Z}^r,$$

der injektiv ist. Wenn nämlich $\pi(w) = 0$ ist, so gehört $w \in \mathbb{Z}^n \subset \mathbb{R}^n$ zu jedem der Halbräume H_j , und das gleiche gilt für $-w$. Wegen der Spitzheit muss $w = 0$ sein. Es sei $\Delta = \pi(\mathbb{Z}^n)$ das Bild in \mathbb{Z}^r und es sei

$$\delta: \mathbb{Z}^r \longrightarrow \mathbb{Z}^r / \Delta =: D$$

der zugehörige Restklassenhomomorphismus. Insgesamt ist

$$\begin{aligned} M &= \mathbb{Z}^n \cap C \\ &= \mathbb{Z}^n \cap \bigcap_{j=1}^r H_j \\ &= \{(a_1, \dots, a_n) \in \mathbb{Z}^n \mid \pi_j(a_1, \dots, a_n) \geq 0 \text{ für alle } j\} \\ &\cong \{(b_1, \dots, b_r) \in \Delta \subseteq \mathbb{Z}^r \mid b_j \geq 0\} \\ &= \{(b_1, \dots, b_r) \in \Delta \mid (b_1, \dots, b_r) \in \mathbb{N}^r\} \\ &= \mathbb{N}^r \cap \Delta \\ &= \mathbb{N}^r \cap \text{kern } \delta. \end{aligned}$$

Das zuletzt angegebene Monoid besteht aber aus allen Monomen in $K[X_1, \dots, X_r]$, deren δ -Grad gleich 0 ist. Also ist

$$K[M] \cong K[\mathbb{N}^r \cap \Delta] = K[\mathbb{N}^r \cap \text{kern } \delta]$$

der Ring der neutralen Stufe von $K[X_1, \dots, X_r]$ unter der durch δ gegebenen Graduierung. (2) \Rightarrow (1). Die neutrale Stufe besteht aus sämtlichen K -Linearkombinationen zu Monomen, deren Grad unter der Graduierung 0 ist. Diese Monome bilden offenbar ein Monoid, das wir M nennen. Es ist also

$$M = \Delta \cap \mathbb{N}^r$$

mit $\Delta = \ker \delta \cong \mathbb{Z}^r$. Der zugehörige Monoidring stimmt mit der neutralen Stufe überein. Wegen $M \subseteq \mathbb{N}^r$ ist das Monoid spitz, torsionsfrei und genügt der Kürzungsregel. Die Normalität ist ebenfalls klar. Wegen $M = \Delta \cap \mathbb{N}^r = \Delta \cap (\mathbb{R}_{\geq 0}^r)$ folgt die endliche Erzeugtheit aus Satz 9.1 (2). \square

SATZ 9.3. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Für eine kommutative K -Algebra R sind folgende Aussagen äquivalent.*

- (1) R ist ein K -Monoidring zu einem endlich erzeugten, torsionsfreien, normalen, spitzen Monoid mit Kürzungsregel.
- (2) R ist die neutrale Stufe einer D -Graduierung eines Polynomringes $K[X_1, \dots, X_r]$, wobei die Graduierung durch einen surjektiven Gruppenhomomorphismus

$$\delta: \mathbb{Z}^r \longrightarrow D$$

gegeben ist.

- (3) R ist der Invariantenring einer treuen Operation λ der Gruppe

$$\mu_{\ell_1}(K) \times \cdots \times \mu_{\ell_a}(K) \times (K^\times)^b$$

auf dem Polynomring $K[X_1, \dots, X_r]$ der Form

$$\lambda(t_1, \dots, t_{a+b}, X_i) = t_1^{d_{i,1}} \cdots t_{a+b}^{d_{i,a+b}} X_i$$

(mit $d_{i,j} \in \mathbb{Z}/(\ell_j)$ für $j \leq a$ und $d_{i,j} \in \mathbb{Z}$ für $j > a$).

- (4) R ist der Invariantenring zur linearen Operation der Gruppe der invertierbaren Diagonalmatrizen

$$\left\{ \left(\begin{array}{cccc} t_1^{d_{1,1}} \cdots t_{a+b}^{d_{1,a+b}} & 0 & \cdots & 0 \\ 0 & t_1^{d_{2,1}} \cdots t_{a+b}^{d_{2,a+b}} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & t_1^{d_{r,1}} \cdots t_{a+b}^{d_{r,a+b}} \end{array} \right) \mid t_j^{\ell_j} = 1 \text{ für } 1 \leq j \leq a \right\}$$

auf dem K^r (für gewisse ℓ_j für $1 \leq j \leq a$).

Beweis. Die Äquivalenz von (1) und (2) folgt direkt aus Satz 9.2. Von (2) nach (3). Nach dem Hauptsatz über endlich erzeugte kommutative Gruppen ist

$$D = \mathbb{Z}/(\ell_1) \times \cdots \times \mathbb{Z}/(\ell_a) \times \mathbb{Z}^b,$$

daher ist

$$G = D^\vee = \mu_{\ell_1}(K) \times \cdots \times \mu_{\ell_a}(K) \times (K^\times)^b.$$

Die zur Graduierung gemäß Lemma 7.9 gehörende Gruppenoperation der Charaktergruppe ist für $\chi \in G$ durch

$$X_i \mapsto \chi(\delta(e_i))X_i$$

festgelegt. Mit

$$\delta(e_i) = (\delta_{i,1}, \dots, \delta_{i,a+b})$$

und

$$\chi = (t_1, \dots, t_{a+b})$$

(beides entsprechend der Produktzerlegung von D bzw. von D^\vee) ist

$$\chi(\delta(e_i))X_i = \chi(\delta_{i,1}, \dots, \delta_{i,a+b})X_i = t_1^{\delta_{i,1}} \dots t_{a+b}^{\delta_{i,a+b}} X_i.$$

Es liegt also die im Satz beschriebene Form der Operation vor. Aufgrund der Voraussetzung an den Körper sind die Bedingungen von Satz 7.10 erfüllt, also ist die neutrale Stufe der Invariantenring. Nach Lemma 7.9 ist die Operation treu. (3) nach (2). Sei die Operation mit den Daten $d_{i,j}$ gegeben. Wir setzen

$$D := \mathbb{Z}/(\ell_1) \times \dots \times \mathbb{Z}/(\ell_a) \times \mathbb{Z}^b$$

und definieren einen Gruppenhomomorphismus $\delta: \mathbb{Z}^r \rightarrow D$ durch $e_i \mapsto (d_{i,1}, \dots, d_{i,a+b})$. Die Gruppenoperation der durch δ gegebenen Graduierung ist gerade die vorgegebene Operation. Diese Aussage folgt somit aus Satz 7.10. Die Äquivalenz von (3) und (4) ist klar. \square

Beispiel 7.12 zeigt, dass man im vorstehenden Satz auf die Voraussetzung der Charakteristik nicht verzichten kann.

Veronese-Ringe

DEFINITION 9.4. Es sei A eine \mathbb{Z} -graduierte R -Algebra und $s \in \mathbb{N}_+$. Dann nennt man

$$A^{(s)} := \bigoplus_{n \in \mathbb{Z}} A_{sn} \subseteq A$$

den s -ten *Veronese-Ring* von A .

Dabei handelt es sich offenbar um einen Unterring von A . Wegen $A_0 \subseteq A^{(s)}$ liegt eine R -Unteralgebra vor. Die Veroneseringe kann man selbst \mathbb{Z} -graduieren, indem man entweder die Graduierung direkt übernimmt (wobei dann die Stufen, deren Index kein Vielfaches von s ist, gleich 0 sind) oder aber die Graduierung als $(A^{(s)})_d := A_{sd}$ ansetzt.

LEMMA 9.5. *Es sei A eine \mathbb{Z} -graduierte R -Algebra und $s \in \mathbb{N}_+$. Es sei vorausgesetzt, dass R eine s -te primitive Einheitswurzel enthalte. Dann ist $A^{(s)}$ der Invariantenring unter der natürlichen Operation der Charaktergruppe $(\mathbb{Z}/(s))^\vee$.*

Beweis. Wir betrachten A als $\mathbb{Z}/(s)$ -graduier durch den kanonischen Gruppenhomomorphismus $\mathbb{Z} \rightarrow \mathbb{Z}/(s)$. Dann ist der Veronese-Ring $A^{(s)}$ die 0-te Stufe von A in dieser neuen Graduierung. Daher folgt die Aussage aus Korollar 7.11. \square

LEMMA 9.6. *Es sei A eine \mathbb{Z} -graduierete R -Algebra, die von der ersten Stufe A_1 erzeugt sei. Dann wird der Veronese-Ring $A^{(s)}$ von der Stufe A_s erzeugt.*

Beweis. Es genügt zu zeigen, dass jedes homogene Element von $A^{(s)}$ von A_s erzeugt wird. Sei also $f \in A_{sd}$. Nach Voraussetzung ist $f = \sum_{\nu \in \mathbb{N}^n} r_\nu x_1^{\nu_1} \cdots x_n^{\nu_n}$ mit Elementen $x_i \in A_1$ und mit $\sum_{i=1}^n \nu_i = sd$. Diese Summe kann man in d Teilsommen aufspalten, d.h. man kann $x^\nu = x^{\mu_1} \cdots x^{\mu_d}$ schreiben, wobei die μ_j jeweils Gradtupel vom Grad s sind. \square

BEISPIEL 9.7. Es sei K ein Körper, $R = K[X_1, \dots, X_n]$ der Polynomring und $R^{(s)}$ der Veronese-Ring zu $s \in \mathbb{N}_+$. Nach Lemma 7.6 ist $R^{(s)} \subseteq R$ ein direkter Summand. Bei $s \geq 2$ (und $n \geq 1$) gibt es keinen Ringhomomorphismus

$$\psi: R \longrightarrow R^{(s)}$$

mit $\psi \circ \iota = \text{id}_{R^{(s)}}$. Dies liegt daran, dass

$$\psi(X_1) = a_0 + a_s + a_{2s} + \dots + a_{rs} = X_1$$

mit $a_{is} \in R_{is}$ keine Lösung besitzt.

Veronese-Ringe zu Polynomringen

Wir betrachten nun genauer die Veronese-Ringe zum Polynomring mit der Standardgraduierung.

LEMMA 9.8. *Es sei K ein Körper und $R = K[X_1, \dots, X_n]$ der Polynomring über K in n Variablen und $s \in \mathbb{N}_+$. Dann ist der Veronese-Ring $R^{(s)}$ der Monoidring zum Monoid*

$$M = \left\{ m = (m_1, \dots, m_n) \in \mathbb{N}^n \mid \sum_{i=1}^n m_i \in \mathbb{N}s \right\} \subseteq \mathbb{N}^n.$$

Wenn K eine s -te primitive Einheitswurzel enthält, so ist dies zugleich der Invariantenring zur linearen Operation der $\mu_s(K)$ auf dem K^n durch skalare Multiplikation.

Beweis. Dies folgt aus Satz 9.2 zur $D := \mathbb{Z}/(s)$ -Graduierung

$$\mathbb{Z}^n \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/(s).$$

Der Kern dieser Abbildung geschnitten mit \mathbb{N}^n bildet gerade die angegebene Menge. Der Zusatz folgt aus Lemma 9.5. \square

Die in der letzten Aussage angesprochene Gruppenoperation ist besonders einfach, sie wird linear durch Diagonalmatrizen mit konstanten Einträgen realisiert, die s -te Einheitswurzeln sind. Die Determinanten dieser Matrizen sind i.A. nicht 1, d.h. es handelt sich nicht um eine Untergruppe der speziellen linearen Gruppe. Damit hängt der Umstand zusammen, dass die Veronese-Ringe typischerweise ziemlich viele Gleichungen benötigen, um sie als Restklassenring eines Polynomrings zu beschreiben.

BEISPIEL 9.9. Zum Polynomring $K[X]$ über einem Körper K und jedem $s \in \mathbb{N}_+$ ist der s -te Veronese-Ring isomorph zum Polynomring selbst. Es handelt sich einfach um den von X^s über K erzeugten Unterring.

BEISPIEL 9.10. Zum Polynomring $A = K[X, Y]$ über einem Körper K und einem $s \in \mathbb{N}_+$ wird der s -te Veronese-Ring durch die Monome $X^s, X^{s-1}Y, \dots, XY^{s-1}, Y^s$ erzeugt. Bei $s = 2$ handelt es sich um

$$K[X^2, XY, Y^2] \cong K[U, V, W]/(UW - V^2).$$

Bei $s = 3$ handelt es sich um

$$K[X^3, X^2Y, XY^2, Y^3] \cong K[U, V, W, Z]/(UZ - VW, UW - V^2, VZ - W^2).$$

Diese Ringe sind nicht isomorph zum Polynomring in zwei Variablen. Beispielsweise ist $A^{(2)}$ im Gegensatz zum Polynomring nicht faktoriell, die Elemente U, V, W sind irreduzibel, aber nicht prim, und die Gleichung $UW = V^2$ bedeutet, dass zwei wesentlich verschiedene Zerlegungen dieses Elementes vorliegen.