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

Invariantentheorie

Vorlesung 7

Wir haben schon vereinzelt die Standardgraduierung auf dem Polynomring verwendet. In dieser Vorlesung führen wir graduierte Ringe allgemein ein und erläutern den engen Zusammenhang zwischen Graduierungen und Gruppenoperationen vom kommutativen Gruppen.

Graduierungen

Definition 7.1. Es sei R ein kommutativer Ring und D eine kommutative Gruppe. Eine R-Algebra A heißt D-*graduiert*, wenn es eine direkte Summenzerlegung

$$A = \bigoplus_{d \in D} A_d$$

mit R-Untermoduln A_d gibt derart, dass $R \subseteq A_0$ ist und für die Multiplikation auf A die Beziehung

$$A_d \cdot A_e \subseteq A_{d+e}$$

gilt.

Eine einfache Überlegung zeigt, dass $1 \in A_0$ ist und dass somit A_0 eine R-Unteralgebra von A ist. Häufig spricht man einfach von einem D-graduierten Ring A. Statt R kann man stets $\mathbb{Z}$ oder A_0 als Grundring wählen.

Bemerkung 7.2. In einer D-graduierten R-Algebra besitzt jedes Element $a \in A$ eine eindeutige Darstellung

$$a = \sum_{d \in D} a_d \text{ mit } a_d \in A_d \, ,$$

wobei nur endlich viele der a_d ungleich 0 sein können. Die a_d heißen dabei die *homogenen Komponenten* von a, die A_d heißen ebenfalls die *homogenen Komponenten* von A (oder d-ten Stufen) und Elemente $a \in A_d$ heißen *homogen* vom *Grad* d. Die Gruppe D heißt die *graduierende Gruppe*. Der Fall $A_d = 0$ ist erlaubt.

Durch eine Graduierung wird die Multiplikation auf einer Algebra A übersichtlicher strukturiert. Man muss lediglich für homogene Elemente $a \in A_d$ und $b \in A_e$ die Produkte $ab \in A_{d+e}$ kennen, dadurch ist schon die gesamte Multiplikation distributiv festgelegt.

Beispiel 7.3. Es sei R ein kommutativer Ring und $R[X_1, \ldots, X_n]$ der Polynomring in n Variablen über R. Dieser ist in naheliegender Weise $\mathbb{Z}$-graduiert. Man definiert für ein Monom $X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ den Grad durch $k_1 + k_2 + \ldots + k_n$

und setzt A_d als den R-Modul aller Polynome an, die R-Linearkombinationen von Monomen von Grad d sind. Bei der Multiplikation von zwei Monomen verhält sich der Grad offensichtlich additiv, so dass dadurch eine graduierte R-Algebra entsteht. Es ist $A_0 = R$ und $A_n = 0$ für negativen Grad n. Diese Graduierung heißt auch die *Standardgraduierung* auf dem Polynomring.

Beispiel 7.4. Es sei R ein kommutativer Ring und $R[X_1, \ldots, X_n]$ der Polynomring in n Variablen über R. Die additive Gruppe des Polynomrings ist einfach

$$\bigoplus_{\nu \in \mathbb{N}^n} R \cdot X^\nu .$$

Daher ist der Polynomring $\mathbb{Z}^n$-graduiert, wobei die $\nu = (\nu_1, \ldots, \nu_n)$-te Stufe einfach aus allen R-Vielfachen des Monoms

$$X^\nu \, = \, X_1^{\nu_1} \cdots X_n^{\nu_n}$$

besteht. Die Stufen zu $\nu \in \mathbb{N}^n$ sind also isomorph zu R, die anderen Stufen, bei denen mindestens eine Komponente negativ ist, sind 0. Diese Graduierung nennt man die *feine Graduierung* des Polynomringes.

Durch einen (surjektiven) Gruppenhomomorphismus

$$\mathbb{Z}^n \longrightarrow D$$

kann man aus der feinen Graduierung des Polynomrings wiederum „gröbere Graduierungen“ gewinnen. In Beispiel 7.13 wird diese Konstruktion eingesetzt.

Beispiel 7.5. Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Dann besitzt die Restklassenalgebra $A = K[X]/(X^n - a)$ eine Graduierung mit der graduierenden Gruppe $D = \mathbb{Z}/(n)$, und zwar setzt man (wobei x die Restklasse von X sei)

$$A_d = \left\{ \lambda x^d | \, \lambda \in K \right\} .$$

Jedes Element $f \in A$ kann man durch ein Polynom repräsentieren, das maximal den Grad $n-1$ besitzt. Daher besitzt jedes f eine Summendarstellung mit Summanden aus den A_d. Diese Summenzerlegung ist direkt, da man mit der einzigen gegebenen Gleichung $X^n = a$ nicht weiter reduzieren kann. Die Multiplikationseigenschaft folgt aus $\lambda x^d \cdot \mu x^e \, = \, \lambda \mu x^{d+e}$, und dies ist gleich $\lambda \mu a x^{d+e-n}$, falls $d + e \geq n$ ist, und andernfalls gleich $\lambda \mu x^{d+e}$. So oder so ist es ein Element aus A_{d+e}.

Lemma 7.6. *Es sei D eine kommutative Gruppe und A ein kommutativer D-graduierter Ring. Dann ist $A_0 \subseteq A$ ein direkter Summand.*

Beweis. Die Stufen A_d sind A_0-Moduln, daher ist

$$A \, = \, A_0 \oplus \left(\bigoplus_{d \in D, \, d \neq 0} A_d \right)$$

eine direkte Summenzerlegung. $\square$

Wir nennen die Stufe A_0 auch die *neutrale Stufe* des graduierten Ringes.

Homogene Ideale

DEFINITION 7.7. Es sei R ein kommutativer Ring, D eine kommutative Gruppe und

$$A = \bigoplus_{d \in D} A_d$$

eine D-graduierte R-Algebra. Ein Ideal $\mathfrak{a} \subseteq A$ heißt *homogen*, wenn zu $f \in \mathfrak{a}$ auch die homogenen Komponenten $f_d \in \mathfrak{a}$ sind.

Für ein homogenes Ideal liegt die Summenzerlegung

$$\mathfrak{a} = \bigoplus_{d \in D} \mathfrak{a}_d$$

mit

$$\mathfrak{a}_d = \mathfrak{a} \cap A_d$$

vor.

LEMMA 7.8. *Es sei R ein kommutativer Ring, D eine kommutative Gruppe und A eine D-graduierte R-Algebra. Es sei $\mathfrak{a} \subseteq A$ ein homogenes Ideal. Dann ist auch der Restklassenring $R/\mathfrak{a}$ D-graduiert. Dabei ist*

$$(R/\mathfrak{a})_d = R_d/\mathfrak{a}_d.$$

Beweis. Siehe Aufgabe 7.7. □

Graduierungen und Gruppenoperationen

Wir kommen nun zu der Beziehung zwischen D-Graduierungen und Operationen der Charaktergruppe $D^\vee$.

LEMMA 7.9. *Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Dann gibt es einen Gruppenhomomorphismus*

$$D^\vee = \operatorname{Char}(D, K) \longrightarrow \operatorname{Aut}_K(A),\ \chi \longmapsto (a_d \mapsto \chi(d)a_d),$$

der Charaktergruppe von D in die (homogene) K-Automorphismengruppe von A. Wenn alle $A_d \neq 0$ sind, so ist diese Zuordnung injektiv.

Beweis. Zu jedem Charakter

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

ist die durch $\varphi_\chi\left(\sum_{d \in D} a_d\right) = \sum_{d \in D} \chi(d) \cdot a_d$ definierte Abbildung φ_χ mit der Addition verträglich. Die Verträglichkeit mit der Multiplikation folgt für homogene Elemente $a_d \in A_d$ und $a_e \in A_e$ aus

$$\varphi_\chi(a_d \cdot a_e) = \chi(d+e)a_d \cdot a_e = \chi(d) \cdot \chi(e)a_d \cdot a_e = \varphi_\chi(a_d) \cdot \varphi_\chi(a_e),$$

woraus sich aufgrund des Distributivgesetzes auch der allgemeine Fall ergibt. Für $a \in A_0$ (und insbesondere für $a \in K$) ist ferner $\varphi_\chi(a) = \chi(0)a = a$, so dass ein K-Algebrahomomorphismus vorliegt. Der triviale (konstante) Charakter geht bei dieser Zuordnung auf die Identität. Es seien nun zwei Charaktere $\chi_1, \chi_2 \in \operatorname{Char}(D, K)$ gegeben. Für ein homogenes Element $a_d \in A_d$ ist

$$\begin{aligned} \varphi_{\chi_1 \cdot \chi_2}(a_d) &= (\chi_1 \cdot \chi_2)(d) \cdot a_d \\ &= \chi_1(d) \cdot \chi_2(d) \cdot a_d \\ &= \chi_1(d) \cdot \varphi_{\chi_2}(a_d) \\ &= \varphi_{\chi_1}(\varphi_{\chi_2}(a_d)) \\ &= (\varphi_{\chi_1} \circ \varphi_{\chi_2})(a_d), \end{aligned}$$

so dass die Gesamtzuordnung mit den Verknüpfungen verträglich ist. Daher gilt auch

$$\varphi_\chi \circ \varphi_{\chi^{-1}} = \varphi_{\chi \circ \chi^{-1}} = \varphi_1 = \mathrm{id}_A,$$

so dass jedes φ_χ ein K-Algebraautomorphismus und die Gesamtzuordnung ein Gruppenhomomorphismus ist. Die Injektivität ergibt sich unter Verwendung von Lemma 4.9 (Körper- und Galoistheorie (Osnabrück 2011)) folgendermaßen. Bei $\chi \neq 1$ gibt es ein $d \in D$ mit $\chi(d) \neq 1$. Nach Voraussetzung ist $A_d \neq 0$, sei also $a \in A_d$, $a \neq 0$. Damit ist $\varphi_\chi(a) = \chi(d)a \neq a$, da $\chi(d) - 1$ eine Einheit ist. Also ist $\varphi_\chi \neq \mathrm{id}_A$. □

Aufgrund dieses Lemmas operiert also die Charaktergruppe zur graduierenden Gruppe auf A als Gruppe von (homogenen) K-Algebraautomorphismen. Der zugehörige Invariantenring zu dieser Operation fällt unter schwachen Bedingungen mit dem Ring der neutralen Stufe der Graduierung zusammen.

Satz 7.10. *Es sei K ein Körper, D eine kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Zu jedem $d \in D$, $d \neq 0$, gebe es einen Charakter $\chi \in D^\vee$ mit*

$$\chi(d) \neq 1.$$

Dann ist A_0 der Invariantenring unter der natürlichen Operation der Charaktergruppe $G = D^\vee$ auf A.

Beweis. Für ein Element $f \in A_0$ und einen beliebigen Charakter χ ist offenbar

$$\varphi_\chi(f) = \chi(0)f = f,$$

so dass $A_0 \subseteq A^G$ ist. Da die Operation der Charaktergruppe homogen ist, sind die homogenen Komponenten eines invarianten Elements $f \in A^G$ ebenfalls invariant. Sei $f \in A_d \cap A^G$ und $d \neq 0$. Aufgrund der Voraussetzung gibt es einen Charakter

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

mit $\chi(d) \neq 1$. Dann ist

$$\varphi_\chi(f) = \chi(d)f \neq f,$$

also sind solche Elemente nicht invariant. □

KOROLLAR 7.11. *Es sei K ein Körper, D eine endliche kommutative Gruppe und A eine D-graduierte kommutative K-Algebra. Der Körper enthalte hinreichend viele Einheitswurzeln, so dass die Charaktergruppe $G = D^\vee$ von D isomorph zu D sei. Dann ist A_0 der Invariantenring unter der natürlichen Operation der Charaktergruppe G auf A.*

Beweis. Dies folgt direkt aus Satz 7.10. □

BEISPIEL 7.12. Es sei K ein Körper der positiven Charakteristik p und der Polynomring $K[X]$ sei durch $D = \mathbb{Z}/(p)$ über $\mathbb{Z} \to \mathbb{Z}/(p)$ graduiert. Die neutrale Stufe ist offenbar $K[X^p]$. Die Charaktergruppe zu $\mathbb{Z}/(p)$ ist aber trivial, da es wegen

$$(x-1)^p = x^p - 1$$

neben der 1 keine weiteren p-ten Einheitswurzeln in K gibt. Damit ist natürlich auch die induzierte Operation trivial und der Invariantenring ist $K[X]$.

Wir besprechen abschließend zwei wichtige Beispiele für Invariantenringe, die die sogenannten A- bzw. die D-Singularitäten repräsentieren.

BEISPIEL 7.13. Es sei K ein Körper, der eine primitive n-te Einheitswurzel ξ enthalte. Wir betrachten die Untergruppe

$$G = \left\{ \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \mid \zeta^n = 1 \right\} \subseteq \mathrm{GL}_2(K)$$

und die zugehörige Operation auf K^2 bzw. auf $K[U, V]$. Es handelt sich um eine zyklische Gruppe der Ordnung n, die von

$$g = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}$$

erzeugt wird. Die Operation von g auf $K[U, V]$ ist durch $U \mapsto \xi U$ und $V \mapsto \xi^{-1} V$ gegeben. Offenbar sind

$$X = U^n,\ Y = V^n,\ Z = UV$$

invariante Polynome unter dieser Gruppenoperation, die in der Beziehung

$$XY = Z^n$$

stehen. Dass diese drei Invarianten den Invariantenring erzeugen, sieht man am besten, wenn man die Situation graduiert realisiert. Dazu sei der Polynomring $\mathbb{Z} \times \mathbb{Z}$-graduiert, wobei U den Grad $(1, 0)$ und V den Grad $(0, 1)$ besitze. Wir betrachten den Gruppenhomomorphismus

$$\delta \colon \mathbb{Z}^2 \longrightarrow \mathbb{Z}/(n) =: D,\ (a, b) \longmapsto a - b,$$

und die zugehörige D-Graduierung des Polynomringes. Wir identifizieren die Charaktergruppe $D^\vee$ mit der obigen Gruppe G, indem wir

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

mit $\begin{pmatrix} \chi(1) & 0 \\ 0 & \chi(-1) \end{pmatrix}$ identifizieren. Bei dieser Identifizierung entspricht die obige explizite Operation von G auf $K[U,V]$ der natürlichen Operation der Charaktergruppe gemäß Lemma 7.9. Nach Korollar 7.11 ist der Invariantenring unter der G-Operation gleich der neutralen Stufe unter der D-Graduierung. Der Kern von δ wird durch $(n,0),(0,n),(1,1)$ erzeugt. Die zugehörigen Stufen bilden somit den Invariantenring. Der Invariantenring ist also $K[U^n,V^n,UV]$.

Im vorstehenden Beispiel haben wir einen surjektiven Ringhomomorphismus

$$K[X,Y,Z]/(XY-Z^n) \longrightarrow K[U^n,V^n,UV] = K[U,V]^G.$$

Dies ist in der Tat ein Isomorphismus, d.h. $XY = Z^n$ ist die einzige relevante Gleichung. Dies liegt daran, dass das Polynom $XY - Z^n$ irreduzibel ist und dadurch der Restklassenring $K[X,Y,Z]/(XY-Z^n)$ ein Integritätsbereich ist. Die Übereinstimmung mit dem Invariantenring folgt nun aus der Dimensionstheorie, die wir aber nicht systematisch entwickeln werden. Jedenfalls ist dieser Restklassenring und der gesuchte Invariantenring zweidimensional, so dass sie übereinstimmen müssen.

Beispiel 7.14. Es sei $m \in \mathbb{N}_+$ und es sei K ein Körper der Charakteristik $\neq 2$, der eine vierte primitive Einheitswurzel i und eine $2m$-te primitive Einheitswurzel ζ enthalte. Wir betrachten die von den Matrizen

$$A = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ und } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

erzeugte Untergruppe G (die man auch als BD_{2m} bezeichnet) der $\mathrm{GL}_2(K)$ mit ihrer natürlichen Operation auf $R = K[U,V]$. Es sei $H \subseteq G$ die von A erzeugte zyklische Untergruppe der Ordnung $2m$. Da G die Ordnung $4m$ besitzt, ist H ein Normalteiler in G. Daher können wir mit Hilfe von Proposition 5.1 (3) und Beispiel 7.13 den Invariantenring $K[U,V]^G$ ausrechnen. Es ist ja

$$S := = K[U,V]^H = K[U^{2m},V^{2m},UV] = K[X,Y,Z]/(XY-Z^{2m}).$$

Die Operation des nichttrivialen Elementes aus $G/H \cong \mathbb{Z}/(2)$ auf diesem Invariantenring wird durch die Operation von B auf $K[U,V]$ repräsentiert. Sie ist also durch $U \mapsto iV$ und $V \mapsto iU$ gegeben und induziert

$$X = U^{2m} \longmapsto i^{2m}V^{2m} = \rho Y\,,$$

$$Y = V^{2m} \longmapsto i^{2m}U^{2m} = \rho X\,,$$

$$Z = UV \longmapsto i^2UV = -Z\,,$$

wobei $\rho = \pm 1$ ist, je nachdem, ob m gerade oder ungerade ist.

Durch diese Operation ist S $\mathbb{Z}/(2)$-graduiert. Bei m gerade sind

$$X+Y, Z^2, Z(X-Y)$$

invariante Polynome (bei m ungerade $X-Y, Z^2, Z(X+Y)$) und Z und $X-Y$ sind semiinvariante Polynome. Mittels $X = \frac{1}{2}(X+Y)+\frac{1}{2}(X-Y)$ und $Y = \frac{1}{2}(X+Y)-\frac{1}{2}(X-Y)$ lässt sich für jedes Monom $X^iY^jZ^k$ die homogene Zerlegung bezüglich dieser Graduierung angeben (wegen $(X-Y)^2 = (X+Y)^2-4Z^{2m}$ kann diese Invariante durch die anderen ausgedrückt werden). Deshalb bilden $L = X+Y$, $M = Z^2$, $N = Z(X-Y)$ ein Algebraerzeugendensystem des Invariantenringes

$$R^G \;=\; S^{\mathbb{Z}/(2)}.$$

Es besteht die Relation

$$\begin{aligned} N^2 &= Z^2(X-Y)^2 \\ &= M\left(X^2+Y^2-2XY\right) \\ &= M\left(L^2-4XY\right) \\ &= ML^2-4MM^m \\ &= ML^2-4M^{m+1}. \end{aligned}$$

Da das Polynom

$$N^2-ML^2+4M^{m+1}$$

irreduzibel ist, und der Invariantenring zweidimensional sein muss, ist

$$R^G \;\cong\; K[L,M,N]/(N^2-ML^2+4M^{m+1}).$$

Unter schwachen Bedingungen an den Körper K ist dieser Ring isomorph zu

$$K[X,Y,Z]/(X^2+YZ^2+Z^{m+1})\,.$$