**Prof. Dr. H. Brenner** **Osnabrück SS 2011**

# Körper- und Galoistheorie

## Vorlesung 9

### Graduierte Körpererweiterungen

Definition 9.1. Es sei $K$ ein Körper und $D$ eine kommutative Gruppe.[1] Eine $K$-Algebra $A$ heißt *$D$-graduiert*, wenn es eine direkte Summenzerlegung

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

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

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

gilt.

Bemerkung 9.2. In einer $D$-graduierten $K$-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 $d$-te Stufe) 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 9.3. Die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ ist graduiert durch die Gruppe $D = \mathbb{Z}/(2)$. Die 0-te homogene Komponente ist $\mathbb{R}$ und die 1-te Komponente ist $\mathbb{R}i$ (das $i$ gehört da dazu, während man unter dem Imaginärteil einer komplexen Zahl die reelle Zahl vor dem $i$ versteht). Die übliche Schreibweise $z = a + bi$ ist also die Zerlegung in die homogenen Komponenten.

Beispiel 9.4. Es sei $K$ ein Körper und $K[X_1, \ldots, X_n]$ der Polynomring in $n$ Variablen über $K$. 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 Vektorraum aller Polynome an, die Linearkombinationen

[1] Diese Gruppe wird fast immer additiv geschrieben.

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

Beispiel 9.5. 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)

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

Jedes Element $f \in A$ kann man durch ein Polynom repräsentieren, das maximal den Grad $n-1$ besitzt. Daher besitzt jedes $f$ eine Summendarstellung in 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 $A_{d+e}$.

Im vorstehenden Beispiel ist es eine nicht-triviale Frage, unter welchen Bedingungen die Algebra $A$ wieder ein Körper ist. Falls ja, so liegt eine graduierte Körpererweiterung im Sinne der folgenden Definition vor.

Definition 9.6. Es sei $K$ ein Körper und $D$ eine endliche kommutative Gruppe. Unter einer *$D$-graduierten Körpererweiterung* versteht man eine Körpererweiterung $K \subseteq L$, bei der auf $L$ eine $D$-Graduierung $L = \bigoplus_{d \in D} L_d$ mit $L_0 = K$ und $L_d \neq 0$ für alle $d \in D$ gegeben ist.

Lemma 9.7. *Es sei $K$ ein Körper, $D$ eine endliche kommutative Gruppe und $K \subseteq L$ eine $D$-graduierte Körpererweiterung. Dann gelten folgende Eigenschaften*

(1) *Jede homogene Stufe $L_d$ besitzt die $K$-Dimension* 1.
(2) *Es ist* $\operatorname{grad}_K L = \#(D)$.
(3) *Es sei $D = (d_1, \ldots, d_m)$ ein Erzeugendensystem von $D$ und es sei $x_i \in L_{d_i}$, $x_i \neq 0$, fixiert. Dann ist $L = K[x_1, \ldots, x_m]$. Insbesondere wird $L$ von homogenen Elementen erzeugt.*
(4) *Jedes homogene Element $x \in L_d$, $x \neq 0$ besitzt ein Minimalpolynom der Form $X^n - a$ mit $a \in K$.*
(5) *Die Körpererweiterung $K \subseteq L$ ist eine Radikalerweiterung.*

*Beweis.* (1). Nach Voraussetzung ist $L_d \neq 0$. Seien $a, b \in L_d$ von 0 verschieden und sei $c \in L_{-d}$ ebenfalls $\neq 0$. Dann sind $ca$ und $cb$ Elemente $\neq 0$ in $L_0 = K$ und daher besteht die Beziehung $ca = \lambda cb$ mit $\lambda \in K$, die sich durch Multiplikation mit $c^{-1}$ (dieses Element gibt es, da wir in einem Körper sind) zurückübersetzt zu $a = \lambda b$. (2) folgt direkt aus (1). (3) ist klar wegen (1). (4). Sei $n \in \mathbb{N}$ die Ordnung von $d \in D$. Für ein homogenes Element $x \in L_d$, $x \neq 0$, ist daher $a = x^n \in L_{nd} = L_0 = K$. Also ist $X^n - a \in K[X]$ ein annullierendes Polynom. Die Potenzen $x^i$, $0 \leq i \leq n-1$, liegen alle in verschiedenen homogenen Stufen. Daher sind sie linear unabhängig und es kann kein annullierendes Polynom von kleinerem Grad geben. (5) folgt aus (3) und (4). □

## Charaktergruppe und Automorphismengruppe bei einer graduierten Körpererweiterung

Wir wollen nun die Automorphismen auf einer graduierten Körpererweiterung kennenlernen. Die Graduierung erlaubt es, die Automorphismen übersichtlich zu beschreiben, was für eine beliebige Körpererweiterung keineswegs selbstverständlich ist. Die Automorphismen hängen eng mit den sogenannten Charakteren der graduierenden Gruppe zusammen, so dass wir zuerst über Charaktere sprechen.

Definition 9.8. Es sei $G$ ein Monoid und $K$ ein Körper. Dann heißt ein Monoidhomomorphismus

$$\chi : G \longrightarrow (K^\times, 1, \cdot)$$

ein *Charakter* von $G$ in $K$.

Die Menge der Charaktere von $G$ nach $K$ bezeichen wir mit $\operatorname{Char}(G, K)$. Mit dem *trivialen Charakter* (also der konstanten Abbildung nach 1) und der Verknüpfung

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$$

ist $\operatorname{Char}(G, K)$ selbst ein Monoid, und zwar ein Untermonoid des Abbildungsmonoid von $G$ nach $K^\times$. Da es zu jedem Charakter den inversen Charakter $\chi^{-1}$ gibt, der durch $\chi^{-1}(g) = (\chi(g))^{-1}$ definiert ist, bildet $\operatorname{Char}(G, K)$ sogar eine kommutative Gruppe (siehe unten).

Definition 9.9. Es sei $G$ ein Gruppe und $K$ ein Körper. Dann nennt man die Menge der Charaktere

$$G^\vee = \operatorname{Char}(G, K) = \{\chi : G \to K^\times \mid \chi \text{ Charakter}\}$$

die *Charaktergruppe* von $G$ (in $K$).

Lemma 9.10. *Sei $G$ eine Gruppe, $K$ ein Körper und $G^\vee = \operatorname{Char}(G, K)$ die Charaktergruppe zu $G$. Dann gelten folgende Aussagen.*

(1) *$G^\vee$ ist eine kommutative Gruppe.*
(2) *Bei einer direkten Gruppenzerlegung $G = G_1 \times G_2$ ist $(G_1 \times G_2)^\vee = G_1^\vee \times G_2^\vee$.*

*Beweis.* Siehe Aufgabe 9.4. □

Lemma 9.11. *Es sei $K$ ein Körper, $D$ eine kommutative Gruppe und $A$ eine $D$-graduierte kommutative $K$-Algebra. Dann gibt es einen Gruppenhomomorphismus*

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

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

*Beweis.* Zu jedem Charakter

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

ist die durch $\varphi_\chi(\sum_{d\in D} a_d) = \sum_{d \in D} \chi(d) \cdot a_d$ definierte Abbildung $\varphi_\chi$ 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 $a \in A_0 = K$ ist ferner $\varphi_\chi(a) = \chi(0)a = a$, so dass ein $K$-Algebra-Homomorphismus vorliegt. Der triviale (konstante) Charakter geht bei dieser Zuordnung auf die Identität. Es seien nun zwei Charaktere $\chi_1, \chi_2 \in \mathrm{Char}\,(D, K)$ 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 $\varphi_\chi$ ein $K$-Algebra-Automorphismus und die Gesamtzuordnung ein Gruppenhomomorphismus ist. Die Injektivität ergibt sich unter Verwendung von Lemma 4.9 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 $\varphi_\chi \neq \mathrm{id}_A$. □

Beispiel 9.12. Es sei $K$ ein Körper, $a \in K$ und $n \in \mathbb{N}$ derart, dass $X^n - a$ irreduzibel ist. Dann ist $K \subseteq K[X]/(X^n - a)$ nach Korollar 7.7 und nach Beispiel 9.4 eine $\mathbb{Z}/(n)$-graduierte Körpererweiterung.

Eine notwendige Voraussetzung für die Irreduzibilität von $X^n - a$ ist, dass $a$ in $K$ keine $n$-te Wurzel besitzt, da sonst das Polynom sofort einen Linearfaktor besitzt. Bei $n = 2$ oder $n = 3$ ist diese Bedingung auch hinreichend. Bei $n = 2$ und wenn die Charakteristik von $K$ nicht gleich 2 ist, so ist $1 \neq -1$ und der nichttriviale Charakter

$$\chi : D = \mathbb{Z}/(2) \longrightarrow K^\times$$

mit $\chi(0) = 1$ und $\chi(1) = -1$ definiert über Lemma 9.11 den nichttrivialen $K$-Körper-Automorphismus mit $x \mapsto -x$ (wobei $x$ die Restklasse von $X$ sei), also die Konjugation in der quadratischen Körpererweiterung $K \subseteq K[X]/(X^2 - a)$.

Beispiel 9.13. Die $\mathbb{Q}$-Algebra $\mathbb{Q}[X]/(X^4 + 4)$ ist eine $\mathbb{Z}/(4)$-graduierte $\mathbb{Q}$-Algebra. Das Polynom $X^4 + 4$ besitzt keine Nullstelle in $\mathbb{Q}$, es ist aber nicht irreduzibel, wie die Zerlegung

$$X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$$

zeigt.

Beispiel 9.14. Wir betrachten den von $\sqrt{2}$ und $\sqrt{3}$ erzeugten Unterkörper $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ von $\mathbb{C}$ (oder von $\mathbb{R}$). Die Elemente $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ bilden dabei unmittelbar ein $\mathbb{Q}$-Erzeugendensystem und sogar eine Basis, da man andernfalls $\sqrt{3}$ als rationale Linearkombination von 1 und $\sqrt{2}$ ausdrücken könnte. Damit liegt insgesamt eine Körpererweiterung vom Grad vier vor. Sei $D = \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Wir setzen

$$L_{(0,0)} = \mathbb{Q},\ L_{(1,0)} = \mathbb{Q} \cdot \sqrt{2},\ L_{(0,1)} = \mathbb{Q} \cdot \sqrt{3}\,, L_{(1,1)} = \mathbb{Q} \cdot \sqrt{6}\,,$$

und erhalten dadurch eine $D$-graduierte Körpererweiterung von $\mathbb{Q}$.

Beispiel 9.15. Wir betrachten die Körpererweiterung $\mathbb{Q} \subseteq L = \mathbb{Q}[i, \sqrt{2}]$ in $\mathbb{C}$. Diese besitzt eine $D = \mathbb{Z}/(2) \times \mathbb{Z}/(2)$-Graduierung, bei der $1, i, \sqrt{2}, i\sqrt{2}$ eine homogene Basis bilden. Das (in dieser Graduierung nicht homogene) Element $\zeta_8 = \frac{1}{2}(\sqrt{2} + \sqrt{2}i)$ ist eine 8-te primitive Einheitswurzel und wegen $\zeta^2 = i$ ist $L = \mathbb{Q}(\zeta_8)$ der achte Kreisteilungskörper.[2] Das Minimalpolynom zu $\zeta_8$ ist $X^4 + 1$, so dass man auch $L \cong \mathbb{Q}[X]/(X^4 + 1)$ schreiben kann. Dies zeigt, dass $L$ auch eine $\mathbb{Z}/(4)$-graduierte Körpererweiterung von $\mathbb{Q}$ ist, bei der $\zeta_8$ homogen ist.

[2] Mit Kreisteilungskörpern werden wir uns später ausführlich beschäftigen.