

Körper- und Galoistheorie

Vorlesung 12

Graduierungen

Wir möchten Körpererweiterungen beschreiben, die eine besonders übersichtliche Struktur aufweisen und eng mit einfachen Radikalerweiterungen zusammenhängen. Insbesondere sind ihre Galoisgruppen und ihre Zwischenkörper häufig einfach beschreibbar.

DEFINITION 12.1. Es sei K ein Körper und D eine kommutative Gruppe.¹ Eine K -Algebra A heißt D -graduirt, wenn es eine direkte Summenzerlegung

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

mit K -Untervektorräumen A_d derart gibt, 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 12.2. In einer D -graduirten 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 12.3. Es sei K ein Körper und $K[X_1, \dots, X_n]$ der Polynomring in n Variablen über K . Dieser ist in naheliegender Weise \mathbb{Z} -graduirt. Man definiert für ein Monom $X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ den Grad durch $k_1 + k_2 + \cdots + k_n$ und setzt A_d als den Vektorraum aller Polynome an, die Linearkombinationen von Monomen vom Grad d sind. Bei der Multiplikation von zwei Monomen

¹Diese Gruppe wird fast immer additiv geschrieben.

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 12.4. 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)

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

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

Graduierte Körpererweiterungen

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 12.5. 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.

BEISPIEL 12.6. Die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ ist durch die Gruppe $D = \mathbb{Z}/(2)$ graduiert. 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 12.7. 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. Es liegt also keine graduierte Körpererweiterung vor.

BEISPIEL 12.8. 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 12.9. 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. Das Minimalpolynom zu ζ_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 ζ_8 homogen ist.

LEMMA 12.10. *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 $\text{grad}_K L = \#(D)$.*
- (3) *Es sei $D = (d_1, \dots, d_m)$ ein Erzeugendensystem von D und es sei $x_i \in L_{d_i}$, $x_i \neq 0$, fixiert. Dann ist $L = K[x_1, \dots, x_m]$. 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). \square

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 12.11. 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 bezeichnen wir mit $\text{Char}(G, K)$. 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 $\text{Char}(G, K)$ selbst ein Monoid, und zwar ein Untermonoid des Abbildungsmonoid von G nach K^\times . Da es zu jedem Charakter den inversen Charakter χ^{-1} gibt, der durch

$$\chi^{-1}(g) = (\chi(g))^{-1}$$

definiert ist, bildet $\text{Char}(G, K)$ sogar eine kommutative Gruppe (siehe unten).

DEFINITION 12.12. Es sei G eine Gruppe und K ein Körper. Dann nennt man die Menge der Charaktere

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

die *Charaktergruppe* von G (in K).

BEISPIEL 12.13. Zur Gruppe $G = \mathbb{Z}/(n)$ und zum Körper \mathbb{C} besteht die Charaktergruppe aus allen Gruppenhomomorphismen $\varphi: \mathbb{Z}/(n) \rightarrow \mathbb{C}^\times$. Da ein solcher durch das Bild des Erzeugers 1 festgelegt ist, und dieser auf eine n -te Einheitswurzel geht, besteht eine natürliche Isomorphie zwischen der Charaktergruppe $(\mathbb{Z}/(n))^\vee$ und der Gruppe μ_n der n -ten komplexen Einheitswurzeln. Diese Gruppe ist selbst isomorph zu $\mathbb{Z}/(n)$, aber nicht in kanonischer Weise.

LEMMA 12.14. Sei G eine Gruppe, K ein Körper und $G^\vee = \text{Char}(G, K)$ 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 12.12. □

LEMMA 12.15. *Es sei K ein Körper, D eine kommutative Gruppe und A eine D -graduierte kommutative K -Algebra. Dann gibt es einen Gruppenhomomorphismus*

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

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

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

ist die durch $\varphi_\chi(\sum_{d \in D} a_d) = \sum_{d \in D} \chi(d) \cdot a_d$ definierte Abbildung 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 $\chi_1, \chi_2 \in \text{Char}(D, K)$ 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

$$\varphi_\chi \circ \varphi_{\chi^{-1}} = \varphi_{\chi \circ \chi^{-1}} = \varphi_1 = \text{Id}_A,$$

so dass jedes φ_χ ein K -Algebraautomorphismus und die Gesamtzuordnung ein Gruppenhomomorphismus ist. Die Injektivität ergibt sich unter Verwendung von Lemma 4.9 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 $\varphi_\chi \neq \text{Id}_A$. \square

BEISPIEL 12.16. 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 9.5 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 12.15 den nichttrivialen K -Körperautomorphismus mit $x \mapsto -x$ (wobei x die Restklasse von X sei), also die Konjugation in der quadratischen Körpererweiterung $K \subseteq K[X]/(X^2 - a)$.

Abbildungsverzeichnis

- Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von <http://commons.wikimedia.org>) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren Dateinamen auf Commons angeführt zusammen mit ihrem Autor bzw. Hochlader und der Lizenz. 7
- Lizenzklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 7