

Körper- und Galoistheorie

Vorlesung 14

Automorphismen und Nullstellen

BEISPIEL 14.1. Wir betrachten den Zerfällungskörper L zum Polynom $X^8 - 1$, also den achten Kreisteilungskörper. Er wird von einer primitiven achten Einheitswurzel ζ erzeugt und besitzt nach Beispiel 12.9 die Darstellungen

$$L = \mathbb{Q}[\zeta]/(\zeta^4 + 1) = \mathbb{Q}[\sqrt{2}, i].$$

Die Nullstellen von $X^8 - 1$ sind die acht verschiedenen Einheitswurzeln, die die Potenzen von ζ sind. Die primitiven Einheitswurzeln besitzen allesamt das Minimalpolynom $X^4 + 1$. Die \mathbb{Q} -Automorphismen

$$\varphi: L \longrightarrow L$$

führen die achten Einheitswurzeln ineinander über, und zwar werden primitive Einheitswurzeln auf primitive Einheitswurzeln abgebildet. Die komplexe Konjugation bildet ζ auf ζ^7 und ζ^3 auf ζ^5 und $\zeta^2 = i$ auf $\zeta^6 = -i$ ab. Der durch $\sqrt{2} \mapsto -\sqrt{2}$ und $i \mapsto i$ gegebene Automorphismus (vergleiche Lemma 12.15) $\zeta = \frac{1}{2}(\sqrt{2} + \sqrt{2}i)$ bildet ζ auf ζ^5 und ζ^3 auf ζ^7 ab. In jedem Fall induziert jeder Automorphismus eine Permutation der achten Einheitswurzeln, also der Nullstellen des Polynoms $X^8 - 1$.

LEMMA 14.2. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von F . Es seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von F in L . Dann gibt es einen natürlichen injektiven Gruppenhomomorphismus*

$$\text{Gal}(L|K) \longrightarrow S(\{\alpha_1, \dots, \alpha_n\})$$

der Galoisgruppe in die Permutationsgruppe der Nullstellen.

Beweis. Sei $\varphi \in \text{Gal}(L|K)$. Nach Lemma 10.15 ist $\varphi(\alpha_i)$ wieder eine Nullstelle von F , daher muss $\varphi(\alpha_i) = \alpha_j$ für ein gewisses j sein. Dies definiert eine Abbildung der Nullstellenmenge in sich selbst. Da φ injektiv ist, ist auch diese induzierte Abbildung injektiv, also nach Lemma 10.5 (Analysis (Osnabrück 2014-2016)) bijektiv und somit eine Permutation. Die Gesamtzuordnung ist offenbar ein Gruppenhomomorphismus. Da die Nullstellen ein Erzeugendensystem des Zerfällungskörpers bilden, liegt nach Lemma 10.14 ein injektiver Homomorphismus vor. \square

BEISPIEL 14.3. Nach Beispiel 11.2 ist

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/(X^3 - 3X + 1) =: L$$

eine Körpererweiterung vom Grad 3 und dabei sind, wenn man die Restklasse von X in L mit α bezeichnet, neben α auch $\beta = \alpha^2 - 2$ und $\gamma = -\alpha^2 - \alpha + 2$ Nullstellen der definierenden Gleichung. Somit besitzen die Elemente α, β, γ das Minimalpolynom $X^3 - 3X + 1$. Durch

$$\varphi: L = \mathbb{Q}[X]/(X^3 - 3X + 1) \longrightarrow L = \mathbb{Q}[X]/(X^3 - 3X + 1), X \longmapsto \beta,$$

wird ein nichtidentischer \mathbb{Q} -Algebraautomorphismus auf L festgelegt. Dieser sendet α auf β , β wegen

$$\begin{aligned} \varphi(\beta) &= \varphi(\alpha^2 - 2) \\ &= \beta^2 - 2 \\ &= (\alpha^2 - 2)^2 - 2 \\ &= \alpha^4 - 4\alpha^2 + 4 - 2 \\ &= \alpha(3\alpha - 1) - 4\alpha^2 + 2 \\ &= -\alpha^2 - \alpha + 2 \\ &= \gamma \end{aligned}$$

auf γ und γ aufgrund einer ähnlichen Rechnung zurück auf α . Die einzigen Automorphismen $\text{Id}, \varphi, \varphi^2$ entsprechen also den geraden Permutationen $\text{Id}, \alpha \mapsto \beta \mapsto \gamma \mapsto \alpha, \alpha \mapsto \gamma \mapsto \beta \mapsto \alpha$ auf der Nullstellenmenge $\{\alpha, \beta, \gamma\}$.

DEFINITION 14.4. Es sei K ein Körper und A eine kommutative K -Algebra. Zwei über K algebraische Elemente $\alpha, \beta \in A$ heißen *konjugiert*, wenn ihre Minimalpolynome übereinstimmen.

SATZ 14.5. *Es sei $K \subseteq L$ eine endliche Körpererweiterung und es seien α und β konjugierte Elemente aus L . Es sei L der Zerfällungskörper des gemeinsamen Minimalpolynoms F dieser beiden Elemente. Dann gibt es einen K -Algebraautomorphismus φ von L mit $\varphi(\alpha) = \beta$.*

Beweis. Zunächst gibt es wegen

$$K[\alpha] \cong K[X]/(F) \cong K[\beta]$$

einen K -Algebrahomomorphismus φ von $K[\alpha]$ nach $K[\beta]$. Der Körper L ist über diesen beiden Unterkörpern der Zerfällungskörper von F . Daher gibt es nach Satz 11.6 einen K -Algebraautomorphismus von L nach L , der φ fortsetzt. \square

Das Lemma von Dedekind

Die Menge der Charaktere auf einem Monoid G in einen Körper K , also $\text{Char}(G, K)$, ist selbst ein Monoid, und zwar ein Untermonoid des Abbildungsmonoids von G nach K^\times . Da Charaktere insbesondere Abbildungen von G nach K sind, kann man von Linearkombinationen von Charakteren sprechen. Diese sind im Allgemeinen keine Charaktere mehr. Es gilt die folgende bemerkenswerte Aussage, das *Lemma von Dedekind*.



Richard Dedekind (1831-1916)

SATZ 14.6. *Es sei G ein Monoid, K ein Körper und $\chi_1, \dots, \chi_n \in \text{Char}(G, K)$ seien n Charaktere. Dann sind diese Charaktere linear unabhängig (als Elemente in $\text{Abb}(G, K)$).*

Beweis. Es sei

$$a_1\chi_1 + \dots + a_n\chi_n = 0,$$

wobei die χ_i verschiedene Charaktere seien und alle $a_i \in K$ von 0 verschieden seien. Darüber hinaus sei n minimal gewählt mit dieser Eigenschaft. Wegen $\chi(e_G) = 1$ ist ein einzelner Charakter nicht die Nullabbildung, also linear unabhängig und somit ist zumindest $n \geq 2$. Wegen $\chi_1 \neq \chi_2$ gibt es auch ein $g \in G$ mit

$\chi_1(g) \neq \chi_2(g)$. Wir behaupten die Gleichheit (wieder von Abbildungen von G nach K)

$$a_1\chi_1(g)\chi_1 + \dots + a_n\chi_n(g)\chi_n = 0.$$

Für ein beliebiges $h \in G$ ist nämlich

$$\begin{aligned} (a_1\chi_1(g)\chi_1 + \dots + a_n\chi_n(g)\chi_n)(h) &= a_1\chi_1(g)\chi_1(h) + \dots + a_n\chi_n(g)\chi_n(h) \\ &= a_1\chi_1(g \cdot h) + \dots + a_n\chi_n(g \cdot h) \\ &= 0 \end{aligned}$$

wegen der Ausgangsgleichung. Wenn man vom $\chi_1(g)$ -fachen der Ausgangsgleichung die zweite Gleichung abzieht, so kann man χ_1 eliminieren und erhält eine nichttriviale (wegen $a_2 \neq 0$ und der Wahl von g) lineare Relation zwischen χ_2, \dots, χ_n im Widerspruch zur Minimalitätseigenschaft von n . \square

Galoiserweiterungen

Aus dem Lemma von Dedekind ergibt sich eine direkte Abschätzung zwischen der Ordnung der Galoisgruppe und dem Grad einer endlichen Körpererweiterung.

SATZ 14.7. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist*

$$\#(\text{Gal}(L|K)) \leq \text{grad}_K L.$$

Beweis. Nach Satz 10.16 ist $\#(\text{Gal}(L|K))$ endlich. Wir setzen

$$m = \#(\text{Gal}(L|K))$$

und $n = \text{grad}_K L$ und müssen $m \leq n$ zeigen. Nehmen wir also $m > n$ an. Es sei v_1, \dots, v_n eine K -Basis von L und die Elemente in der Galoisgruppe seien $\varphi_1, \dots, \varphi_m$. Wir betrachten die Matrix

$$\begin{pmatrix} \varphi_1(v_1) & \cdots & \varphi_m(v_1) \\ \vdots & \ddots & \vdots \\ \varphi_1(v_n) & \cdots & \varphi_m(v_n) \end{pmatrix}.$$

Ihr Rang ist maximal gleich n , da sie nur n Zeilen besitzt. Daher gibt es eine nichttriviale Relation zwischen den m Spalten, sagen wir

$$b_1 \begin{pmatrix} \varphi_1(v_1) \\ \vdots \\ \varphi_1(v_n) \end{pmatrix} + \cdots + b_m \begin{pmatrix} \varphi_m(v_1) \\ \vdots \\ \varphi_m(v_n) \end{pmatrix} = 0,$$

wobei nicht alle b_j gleich 0 sind. Wir betrachten nun

$$\sum_{j=1}^m b_j \varphi_j,$$

wobei wir die Automorphismen φ_j als Charaktere von L^\times nach L^\times auffassen. Für ein beliebiges Element $v \in L$ schreiben wir $v = \sum_{i=1}^n a_i v_i$. Mit diesen Bezeichnungen gilt

$$\begin{aligned} \left(\sum_{j=1}^m b_j \varphi_j \right) (v) &= \left(\sum_{j=1}^m b_j \varphi_j \right) \left(\sum_{i=1}^n a_i v_i \right) \\ &= \sum_{j=1}^m b_j \left(\varphi_j \left(\sum_{i=1}^n a_i v_i \right) \right) \\ &= \sum_{j=1}^m b_j \left(\sum_{i=1}^n a_i \varphi_j(v_i) \right) \\ &= \sum_{i=1}^n a_i \left(\sum_{j=1}^m b_j \varphi_j(v_i) \right) \\ &= 0, \end{aligned}$$

da ja wegen der obigen linearen Abhängigkeit die Zeilensummen

$$\sum_{j=1}^m b_j \varphi_j(v_i) = 0$$

sind für jedes i . Also liegt eine nicht-triviale Relation zwischen Charakteren vor, was nach Satz 14.6 nicht sein kann. \square

Eine wichtige Frage ist, wann in der vorstehenden Abschätzung Gleichheit vorliegt, wann es also so viele Automorphismen wie möglich gibt. Dies machen wir zur Grundlage der folgenden Definition. Wir werden später noch viele äquivalente Eigenschaften kennenlernen.

DEFINITION 14.8. Sei $K \subseteq L$ eine endliche Körpererweiterung. Sie heißt eine *Galoiserweiterung*, wenn

$$\#(\text{Gal}(L|K)) = \text{grad}_K L$$

gilt.

LEMMA 14.9. *Es sei K ein Körper mit einer Charakteristik $\neq 2$ und sei $K \subseteq L$ eine quadratische Körpererweiterung. Dann ist $K \subseteq L$ eine Galoiserweiterung.*

Beweis. Siehe Aufgabe 14.13. \square

Die vorstehende Aussage ist ein Spezialfall der Aussage, dass graduierte Körpererweiterungen unter der Voraussetzung, dass hinreichend viele Einheitswurzeln im Grundkörper vorhanden sind, Galois-Erweiterungen sind. Dazu brauchen wir ein vorbereitendes Lemma.

LEMMA 14.10. *Es sei G eine endliche kommutative Gruppe mit dem Exponenten m , und es sei K ein Körper, der eine primitive m -te Einheitswurzel besitzt. Dann sind G und G^\vee isomorphe¹ Gruppen.*

Beweis. Nach Lemma 12.14 (2) und Satz Anhang 4.2. kann man annehmen, dass $G = \mathbb{Z}/(n)$ eine endliche zyklische Gruppe ist, und dass K eine n -te primitive Einheitswurzel besitzt. Jeder Gruppenhomomorphismus

$$\varphi: G \longrightarrow K^\times$$

ist durch $\zeta = \varphi(1)$ eindeutig festgelegt, und wegen

$$\zeta^n = (\varphi(1))^n = \varphi(n) = \varphi(0) = 1$$

ist ζ eine n -te Einheitswurzel. Umgekehrt kann man zu jeder n -ten Einheitswurzel ζ durch die Zuordnung $1 \mapsto \zeta$ nach Lemma 4.4 und Satz 5.10 einen Gruppenhomomorphismus von $\mathbb{Z}/(n)$ nach K^\times definieren. Die Menge der n -ten Einheitswurzeln ist, da eine primitive Einheitswurzel vorhanden ist, eine

¹Diese Isomorphie ist nicht kanonisch, es gibt keine natürliche Beziehung zwischen den Elementen aus G und den Charakteren auf G .

zyklische Gruppe der Ordnung n . Also gibt es n solche Homomorphismen. Wenn ζ eine primitive Einheitswurzel ist, dann besitzt der durch $1 \mapsto \zeta$ festgelegte Homomorphismus die Ordnung n und ist damit ein Erzeuger der Charaktergruppe, also $(\mathbb{Z}/(n))^\vee \cong \mathbb{Z}/(n)$. \square

SATZ 14.11. *Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D -graduierte Körpererweiterung. Der Körper K enthalte eine m -te primitive Einheitswurzel, wobei m der Exponent von D sei. Dann ist $K \subseteq L$ eine Galoiserweiterung mit Galoisgruppe $D^\vee = \text{Char}(D, K)$.*

Beweis. Die Voraussetzung über die primitiven Einheitswurzeln in Verbindung mit Lemma 14.10 und Lemma 12.10 (2) sichern

$$\#(D^\vee) = \#(D) = \text{grad}_K L.$$

Nach Lemma 12.15 ist

$$\#(D^\vee) \leq \#(\text{Gal}(L|K)).$$

Also ist

$$\text{grad}_K L \leq \#(\text{Gal}(L|K)),$$

und somit haben wir nach Satz 14.7 hier Gleichheit, also liegt eine Galoiserweiterung vor. Damit ist auch der nach Lemma 12.15 injektive Gruppenhomomorphismus

$$D^\vee \longrightarrow \text{Gal}(L|K)$$

bijektiv. \square

BEISPIEL 14.12. Sei $n \in \mathbb{N}_+$ und sei K ein Körper, der eine n -te primitive Einheitswurzel enthält. Es sei $a \in K$ derart, dass das Polynom $X^n - a$ irreduzibel sei. Dann ist

$$K \subseteq L = K[X]/(X^n - a)$$

eine nach Beispiel 9.5 $D = \mathbb{Z}/(n)$ -graduierte Körpererweiterung, und nach Satz 14.11 handelt es sich um eine Galoiserweiterung mit Galoisgruppe

$$\text{Gal}(L|K) = D^\vee \cong \mathbb{Z}/(n).$$

Dabei ist L auch der Zerfällungskörper von $X^n - a$. Wenn x die Restklasse von X bezeichnet, so sind die n verschiedenen Nullstellen dieses Polynoms gleich

$$\zeta x \text{ mit } \zeta \in \mu_n(K) = \{z \in K \mid z^n = 1\},$$

die allesamt homogene Elemente der Stufe $1 \in D$ sind. Ein Charakter $\chi \in D^\vee$ bzw. der zugehörige Automorphismus φ_χ operiert gemäß Lemma 14.2 auf dieser Nullstellenmenge M (die nichtkanonisch isomorph zu $\mu_n(K)$ ist) durch

$$\varphi_\chi: M \longrightarrow M, \zeta x \longmapsto \chi(1)\zeta x.$$

Die graduirende Gruppe D , sein Charakterdual D^\vee , die Gruppe der n -ten Einheitswurzeln $\mu_n(K)$, die Galoisgruppe $\text{Gal}(L|K)$ und die Nullstellenmenge M bestehen aus n Elementen, die Permutationsgruppe von M besteht somit aus $n!$ Elementen. Zu je zwei Nullstellen $x_1 = \zeta_1 x$ und $x_2 = \zeta_2 x$ gibt es

einen eindeutigen Charakter bzw. Automorphismus, dessen zugehörige Permutation x_1 in x_2 überführt, nämlich derjenige Charakter χ mit $\chi(1) = \zeta_2 \zeta_1^{-1}$.

Bei $K = \mathbb{Q}$ und $L = \mathbb{Q}[i] = \mathbb{Q}[X]/(X^2 + 1)$ sind $M = \{i, -i\}$ die beiden Nullstellen und der nichtkonstante Charakter vertauscht die beiden Nullstellen. Wegen $2! = 2$ rührt jede Permutation von einem Automorphismus bzw. einem Charakter her.

Bei $K = \mathbb{Q}[i]$ und $X^4 - 3 \in K[X]$ ist $L = K[X]/(X^4 - 3)$ eine $\mathbb{Z}/(4)$ -graduierte Körpererweiterung. Die vier Nullstellen sind $\sqrt[4]{3}$, $-\sqrt[4]{3}$, $i\sqrt[4]{3}$ und $-i\sqrt[4]{3}$. Die Irreduzibilität von $X^4 - 3$ ergibt sich dadurch, dass das Produkt von je zwei Linearfaktoren nicht zu $K[X]$ gehört. Jeder Charakter χ ist durch $\chi(1)$ bestimmt und die zugehörige Permutation auf der Nullstellenmenge ist die Multiplikation mit $\chi(1)$. Bei $\chi(1) = -1$ ist das die Permutation $\sqrt[4]{3} \leftrightarrow -\sqrt[4]{3}$, $i\sqrt[4]{3} \leftrightarrow -i\sqrt[4]{3}$, bei $\chi(1) = i$ ist das die Permutation $\sqrt[4]{3} \mapsto i\sqrt[4]{3} \mapsto -\sqrt[4]{3} \mapsto -i\sqrt[4]{3}$ und bei $\chi(1) = -i$ ist das die Permutation $\sqrt[4]{3} \mapsto -i\sqrt[4]{3} \mapsto -\sqrt[4]{3} \mapsto i\sqrt[4]{3}$. Unter den 24 Permutationen rühren also nur 4 von einem Charakter her, eine Permutation wie $\sqrt[4]{3} \leftrightarrow \sqrt[4]{3}$, $-\sqrt[4]{3} \leftrightarrow -\sqrt[4]{3}$, und $i\sqrt[4]{3} \leftrightarrow -i\sqrt[4]{3}$ z.B. nicht.

Abbildungsverzeichnis

- Quelle = Dedekind.jpeg , Autor = unbekannt (hochgeladen von Benutzer Jean-Luc W auf Commons), Lizenz = PD 3
- 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. 9
- Lizenzklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 9