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

Körper- und Galoistheorie

Vorlesung 13

Automorphismen und Nullstellen

Lemma 13.1. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von F. Es seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von F in L. Dann gibt es einen natürlichen injektiven Gruppenhomomorphismus*

$$\mathrm{Gal}\,(L|K) \longrightarrow S(\{\alpha_1, \ldots, \alpha_n\})$$

der Galoisgruppe in die Permutationsgruppe der Nullstellen.

Beweis. Sei $\varphi \in \mathrm{Gal}\,(L|K)$. Nach Lemma 8.15 ist $\varphi(\alpha_i)$ wieder eine Nullstelle von F, daher muss $\varphi(\alpha_i) = \alpha_j$ für ein gewisses j sein. Dies definiert ein Abbildung der Nullstellenmenge in sich selbst. Da φ injektiv ist, ist auch diese induzierte Abbildung injektiv, also nach Lemma 3.14 (Mathematik (Osnabrück 2009-2011)) bijektiv und somit eine Permutation. Die Gesamtzuordnung ist offenbar ein Gruppenhomomorphismus. Da die Nullstellen ein Erzeugendensystem des Zerfällungskörpers bilden, liegt nach Lemma 8.14 ein injektiver Homomorphismus vor. □

Definition 13.2. 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 13.3. *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-Algebra-Automorphismus φ von L mit $\varphi(\alpha) = \beta$.*

Beweis. Zunächst gibt es wegen

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

einen K-Algebra-Homomorphismus φ von $K[\alpha]$ nach $K[\beta]$. Der Körper L ist über diesen beiden Unterkörpern der Zerfällungskörper von F. Daher gibt es nach Satz 11.5 einen K-Algebra-Homomorphismus von L nach L, der φ fortsetzt. □

Das Lemma von Dedekind

Richard Dedekind (1831-1916)

Die Menge der Charaktere auf einem Monoid G in einen Körper K, also $\mathrm{Char}\,(G, K)$, 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.*

Satz 13.4. *Es sei G ein Monoid, K ein Körper und $\chi_1, \ldots, \chi_n \in \mathrm{Char}\,(G, K)$ seien n Charaktere. Dann sind diese Charaktere linear unabhängig (als Elemente in $\mathrm{Hom}_K(G, K)$).*

Beweis. Es sei

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

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)

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

Für ein beliebiges $h \in G$ ist nämlich

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

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 $\chi_2, \ldots, \chi_n$ 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 13.5. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist*

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

Beweis. Nach Satz 8.16 ist $\#(\mathrm{Gal}\,(L|K))$ endlich. Wir setzen

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

und $n = \mathrm{grad}_K\, L$ und müssen $m \leq n$ zeigen. Nehmen wir also $m > n$ an. Es sei $v_1, \ldots, v_n$ eine K-Basis von L und die Elemente in der Galoisgruppe seien $\varphi_1, \ldots, \varphi_m$. 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 nicht-triviale Relation zwischen den m Spalten, sagen wir

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

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

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

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 13.4 nicht sein kann. □

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

Definition 13.6. Sei $K \subseteq L$ eine endliche Körpererweiterung. Sie heißt eine *Galoiserweiterung*, wenn

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

gilt.

Lemma 13.7. *Es sei K ein Körper mit einer Charakeristik $\neq 2$ und sei $K \subseteq L$ eine quadratische Körpererweiterung. Dann ist $K \subseteq L$ eine Galoiserweiterung.*

Beweis. Siehe Aufgabe 13.6. □

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 13.8. *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 $G^\vee$ isomorphe[1] Gruppen.*

Beweis. Nach Lemma 9.10 und Korollar 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 zyklische Gruppe der Ordnung n. Also gibt es n solche Homomorphismen.

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

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 13.9. *Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Zu jedem Primpotenzteiler p^r von $\#(D)$ enthalte K eine p^r-te primitive Einheitswurzel. Dann ist $K \subseteq L$ eine Galoiserweiterung mit Galoisgruppe $D^\vee = \operatorname{Char}(D, K)$.*

Beweis. Die Voraussetzung über die primitiven Einheitswurzeln in Verbindung mit Lemma 13.8 und Lemma 9.7 sichern

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

Nach Lemma 9.11 ist

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

Also ist

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

und somit haben wir nach Satz 13.5 hier Gleichheit, also liegt eine Galoiserweiterung vor. Damit ist auch der nach Lemma 9.11 injektive Gruppenhomomorphismus

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

bijektiv. $\square$

BEISPIEL 13.10. 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 9.4 $D = \mathbb{Z}/(n)$-graduierte Körpererweiterung, und nach Satz 13.9 handelt es sich um eine Galoiserweiterung mit Galoisgruppe

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

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 13.1 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 graduierende Gruppe D, sein Charakterdual $D^\vee$, die Gruppe der n-ten Einheitswurzeln $\mu_n(K)$, die Galoisgruppe $\operatorname{Gal}(L|K)$ 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 ist die Multiplikation mit $\chi(1)$. Bei $\chi(1) = -1$ ist das die Permutation $1 \leftrightarrow -1$, $i \leftrightarrow -i$, bei $\chi(1) = i$ ist das die Permutation $1 \to i \to -1 \to -i$ und bei $\chi(1) = -i$ ist das die Permutation $1 \to -i \to -1 \to i$. Unter den 24 Permutationen rühren also nur 4 von einem Charakter her, eine Permutation wie $1 \leftrightarrow 1$, $-1 \leftrightarrow -1$, und $i \leftrightarrow -i$ z.B. nicht.

Abbildungsverzeichnis