Vortrag 5:

Die Galoische Gruppe

Von: Tobias Sturm M.Nr: 2895977

1.) *einfache* und *separable* Erweiterungen

Sei K im Folgenden stets ein Körper.

Definition 3.1.1:

Eine Körpererweiterung L/K heißt *einfach*, wenn ein $x \in L$ existiert, so dass $L = K[x]$ bzw $L = K(x)$.

Proposition 3.1.2: (Korollar von Satz von Kronecker)

Wiederholung vom Satz von Kronecker: Sei K ein Körper und P ein irreduzibles Polynom aus $K[X]$. Dann existiert eine endliche K.-erweiterung K_1/K und eine Nullstelle x von P in K_1, so dass gilt:

a) $K_1 = K(x)$

b) Wenn L/K eine K.-erweiterung ist, dann gibt es eine Bijektion zwischen der Menge der Einbettungen von K_1 nach L und der Menge der Nullstellen von P in L, diese Bijektion ist gegeben durch: $f \mapsto f(x)$.

Korollar: Sei L/K eine einfache Erweiterung, $x \in L$ mit $L = K(x])$, P das Minimalpolynom von x und sei ferner Ω/L ein algebraischer Abschluss von K. Dann gibt es eine Bijektion zwischen der Menge der K-Homomorphismen von L nach Ω und der Menge der Nullstellen von P in Ω, gegeben durch $f \mapsto f(x)$. Insbesondere gilt für deren Anzahl $N \in \mathbb{N} : 1 \leq N \leq [L : K]$

Beweis: $0 = f(0) = f(P(x)) = P(f(x))$ also wird x von f auf eine Nullstelle von P abgebildet. Da L/K einfach ist, gibt es für jedes $a \in L$ ein $Q \in K[X]$, so dass $a = Q(x)$. Also ist $f(a) = f(Q(x)) = Q(f(x))$. Folglich ist f eindeutig durch $f(x)$ bestimmt. Hat P nun $N \in \mathbb{N}$ verschiedene Nullstellen in Ω, so gibt es N Möglichkeiten x abzubilden. Also ist $[L : K] = deg(P) \geq N$.

□

Bemerkung 3.1.3:

Beachte, dass jeder dieser Homomorphismen es uns ermöglicht Ω als algebraischen Abschluss von L zu betrachten. Diese Hom.-en sind alle von einander verschieden, daher auch die Darstellung der Körpererweiterungen als injektive Hom.-en und nicht als Inklusionen eines Unterkörpers. Allerdings kann man L auch durch sein Bild in Ω darstellen was uns zurück auf eine vertrautere Anschauung von Unterkörpern führen lässt nämlich $K \subseteq L \subseteq \Omega$.

Ein Polynom $P \in K[X]$ heißt *separabel*, wenn seine Nullstellen im algebraischen Abschluss von K *einfach* sind.

Lemma 3.1.4:

Ein Polynom $P \in K[X]$ ist genau dann *separabel*, wenn P zu seiner Ableitung P' *teilerfremd* in $K[X]$ ist.

Beweis: Sei Ω ein algebraischer Abschluss von P. Nach Definition, ist P separabel, wenn die Nullstellen von P im algebraischen Abschluss von K einfach sind, dies ist gleich bedeutend zu P und P' sind teilerfremd in $\Omega[X]$. Nach Korollar 2.4.3, das besagt, dass der $ggT(A, B)$ mit A, B Polynome aus $K[X]$ in $L[X]$ gleich ist dem $ggT(A, B)$ berechnet in $K[X]$, ist dies äquivalent dazu, dass sie auch teilerfremd in $K[X]$ sind.

□

Sei L/K eine algebraische Erweiterung, ein Element $a \in L$ heißt *separabel*, wenn sein Minimalpolynom über K separabel ist.

Lemma 3.1.5:

Sei L/K eine algebraische Erweiterung und Ω ein algebraischer Abschluss von L. Wenn $a \in \Omega$ separabel über K ist, so ist es auch separabel über L.

Beweis: Sei P das Minimalpolynom von a über L und sei Q das Minimalpolynom über K. Da $Q(a) = 0$, ist Q ein Vielfaches von P. Da a separabel über K ist, hat Q nur einfache Nullstellen in Ω, und somit auch P

□

Satz 3.1.6:

Sei L/K eine endliche Erweiterung und Ω/K ein algebraischer Abschluss. Dann gilt für N definiert als die Anzahl der unterschiedlichen K-Homomoprhismen von L nach Ω, dass $1 \leq N \leq [L : K]$.

Darüber hinaus sind folgende 3 Eigenschaften äquivalent:

a) $N = [L : K]$

b) Es existieren: $x_1, \ldots, x_n \in L$ separabel über K mit $L = K[x_1, \ldots, x_n]$

c) Alle Elemente aus L sind separabel über K

Beweis:
Da L eine endliche Erweiterung von K ist, existieren Elemente $x_1, \ldots, x_n \in L$ mit $L = K[x_1, \ldots, x_n]$. Der Beweis erfolgt durch Induktion über n:

Für n = 1 ist L/K einfach und nach Proposition 3.1.2 ist N gleich der Anzahl der verschiedenen Nullstellen des Minimalpolynoms von x_1. Da dieses Polynom vom Grad $[L : K]$ ist, wissen wir:

- Es gilt: $1 \leq N \leq [L:K]$
- $N = [L:K] \Longleftrightarrow x_1$ ist separabel über K.

Angenommen: $x_1 \notin K$ und sei P_1 das Minimalpoylnom von x_1 mit $deg(P_1) = d$ und sei $L_1 = K(x_1)$. Die Einschränkung auf L_1 von jedem K-Homomorphismus $f : L \to \Omega$ ist ein K-Homomorphismus $f_1 : L_1 \to \Omega$ und hängt folglich von der Wahl einer Nullstelle von P_1 in Ω ab. Deswegen, gibt es zwischen 1 und d solcher Homomorphismen f_1 und jeder lässt uns Ω als einen algebraischen Abschluss von L_1 sehen.
Der Grad der Erweiterung von $L_1 \subset L$ ist gleich $[L:K]/d$, ist also kleiner als $[L:K]$. Nach Induktionsannahme liegt die Zahl der L_1-Homomorphismen von L nach Ω, die ein f_1 fortsetzen, zwischen 1 und $[L:L_1]$,
Schließlich haben wir somit zwischen einem und $[L:K] = d \cdot [L:L_1]$ verschiedene K-Homomorphismen von L nach Ω konstruiert. Da jeder K-Homomorphismen von L nach Ω so konstruiert werden kann, zeigt das den ersten Teil des Satzes.

Nun Zeigen wir die Äquivalenz:

b) $\Rightarrow$ a) Seien $x_1, \ldots, x_n \in L$ separabel über K und $L = K(x_1, \ldots, x_n)$. Nach Lemma 3.1.5 gilt ist x separabel über K, so ist es auch separabel über $L \Rightarrow x_2$ ist separabel über $K(x_1)$ und x_3 ist separabel über $K(x_1, x_2)$ usw. Und nach dem vorangegangen Beweis ist die äquivalent zu der Aussage, dass N = [L:K].

a) $\Rightarrow$ c) Sei $N = [L:K]$ und $x \in L$. Dann ist
$L = K[x_1, \ldots, x_n] = K[x, x_1, \ldots, x_n]$. Die vorangegange Induktion zeigt dann auch, dass x separabel über K ist.

c) $\Rightarrow$ b) Da L/K eine endliche Erweiterung ist, gibt es $x_1, \ldots, x_n \in L$, sodass $L = K[x_1, \ldots, x_n]$. Diese x_i sind nach Voraussetzung allesamt separabel über K.

□

Eine Erweiterung L/K, die diesen Eigenschaften genügt, nennt man *separabel*.

2.) *galoische* Erweiterungen

Definition 3.2.1:

Sei L/K eine Körpererweiterung. Ein K-Automorphismus von L ist ein Körperautomorphismus $\sigma : L \to L$ und heißt Erweiterungshomomorphismus.

Die Menge aller K-Autom. von L bilden eine Gruppe [*Notation:* $Aut(L/K)$].
Sei $\sigma \in Aut(L/K)$. Für $P \in K[X]$ gilt: $\sigma(P(x)) = P(\sigma(x))$ für jedes $x \in L$.
Insbesondere gilt, falls x eine Nullstelle von P ist, so ist auch $\sigma(x)$ eine Nullstelle von P. Das heißt, dass σ die Nullstellen von P in L permutiert.

Proposition 3.2.4:

Sei L/K eine *endliche* Erweiterung, dann ist die Kardinalität von $Aut(L/K) \leq [L:K]$. Bei Gleichheit folgt, dass L/K separabel ist.

Beweis: Sei $i : L \to \Omega$ bzw Ω/L ein algebraischer Abschluss von L. Jeder K-Automorphismus $\sigma \in Aut(L/K)$ induziert einen eindeutigen K-Hom.: $i \circ \sigma : L \to \Omega$. Nach Satz 3.1.6, ist deren Anzahl kleiner gleich $[L:K]$ und bei Gleichheit ist L/K separabel.

□

Definition 3.2.5:

Eine endliche Erweiterung L/K nennt man *galoisch*, wenn $|Aut(L/K)| = [L:K]$. Die Automorphismusgruppe wird dann die Galoisgruppe genannt und mit $Gal(L/K)$ bezeichnet

Nach 3.2.4 ist somit eine galoische Erweiterung notwendigerweise *separabel*.

3.) Beispiele

Beispiel 1:

Man betrachte die Erweiterung $\mathbb{C}/\mathbb{R}$. Sei σ ein $\mathbb{R}-Automorphismus$ von $\mathbb{C}$ Für $z = a + ib \in \mathbb{C}$, mit $a, b \in \mathbb{R}$ gilt:

$\sigma(z) = \sigma(a + ib) = \sigma(a) + \sigma(ib) = a + \sigma(i)b$

Da $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1 \Rightarrow \sigma(i) = \pm i \Rightarrow$ es existieren 2 Automorphismen: die Identität und die komplexe Konjugation.
Der Körpergrad $[\mathbb{C}:\mathbb{R}] = 2$, da $(1, i)$ die $\mathbb{R}$-Basis von $\mathbb{C}$ ist und daraus folgt, dass $\mathbb{C}/\mathbb{R}$ eine galoische Erweiterung ist.

Beispiel 2:

Man betrachte die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Jedes Element in $\mathbb{Q}(\sqrt[3]{2})$ kann geschrieben werden, als $a+b\sqrt[3]{2}+c\sqrt[3]{2}^2$. Ein $\mathbb{Q}-Automorphismus\ \sigma$ auf $\mathbb{Q}(\sqrt[3]{2})$ ist wohldefiniert, sobald das Bild von $\sqrt[3]{2}$ gegeben ist. $\sigma(\sqrt[3]{2})^3 = \sigma(\sqrt[3]{2^3}) = \sigma(2) = 2$ und die Gleichung $x^3 = 2$ hat nur eine reelle Nullstelle $\sqrt[3]{2}$, also die einzige Nullstelle von $\mathbb{Q}(\sqrt[3]{2}) \Rightarrow Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = id$. Der Körpergrad $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, da $(1,\ \sqrt[3]{2},\ \sqrt[3]{2^2})$ die $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt[3]{2})$ ist. Und somit ist die Erweiterung nicht galoissch. Des Weiteren existieren aber sehr wohl noch Nullstellen vom Polynom $x^3 = 2 \Rightarrow P := x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2})$ mit der 3. Einheitswurzel ζ mit $\zeta = \exp((2\pi \cdot k \cdot i)/n)$. So sind $\zeta \cdot \sqrt[3]{2}$ und $\zeta^2 \cdot \sqrt[3]{2}$ auch Nullstellen dieses Polynoms. Die Erweiterung $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta)/\mathbb{Q} := L/K$ ist also separabel. Ferner ist L/K normal, da L der Zerfällungskörper von P ist und daraus folgt, dass L/K galoisch ist.(normal $\Leftrightarrow$ alle Minimalpolynome über K von Elementen aus L zerfallen in L vollständig in Linearfaktoren und galoissch $\Leftrightarrow L/K$ ist normal + separabel.)