Proseminar Körpertheorie
Vortrag 5

Borislav Vlajic

23.Mai 2013

5. Vortrag - Die Galoissche Gruppe

5.1 Einfache und separable Erweiterungen

Definition 5.1.1. Sei L/K eine Körpererweiterung. Man nennt die Erweiterung *einfach*, wenn ein $x \in L$ ex. mit $L = K[x]$.

Proposition 5.1.2. (Korollar von Satz von Kronecker) Sei L/K eine einfache algebraische Erweiterung, $x \in L$, s.d. $L = K[x]$ und P das Minimalpolynom bzgl. x über K. Sei weiter Ω/K ein alg. 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 die Abbildung $f \mapsto f(x)$ Es gibt mindestens einen solcher Homomorphismen und höchstens $[L : K]$ viele.

Beweis. Erster Teil der Aussage folgt direkt aus dem Satz von Kronecker (Vortrag 4). Hat P n verschiedene Nullstellen in Ω, so gibt es n Möglichkeiten x abzubilden. Also ist $[L : K] = \deg(P) \leq n$. □

Bemerkung 5.1.3. Jeder dieser Homomorphismen erlaubt es uns Ω als algebraischen Abschluss zu bezeichnen. Alle diese Homomorphismen sind verschieden und aus diesem Grund ist es besser Körpererweiterungen als injektive Homomorphismen zu betrachten, statt als Inklusionen von Unterkörpern. Sobald aber einer dieser Homomorphismen gewählt wurde, gibt es keinen Grund mehr L nicht durch sein Bild in Ω zu ersetzen, was uns wieder in die möglich vertrautere Anschauung von Unterkörpern bringt $K \subset L \subset \Omega$.

Definition 5.1.4. Sei K ein Körper. Ein Polynom $P \in K[X]$ heißt *separabel*, wenn seine Nullstellen ein einem algebraischen Abschluss von K einfach sind. (also wenn P keine Mehrfachnullstellen hat)

Lemma 5.1.5. Sei K ein Körper. Ein Polynom $P \in K[X]$ ist genau dann separabel, wenn P und seine Ableitung P' teilerfremd sind.

Beweis. Sei $\alpha \in K$ eine n-fache Nullstelle von $P, Q \in K[X]$ mit $Q(\alpha) \neq 0$, ohne Einschränkung Q separabel und P sei von der Form $P(x) = (x - \alpha)^n \cdot Q(x)$. Dann gilt:

$$P'(x) = n(x - \alpha)^{n-1} \cdot Q(x) + (x - \alpha)^n \cdot Q'(x) = (x - \alpha)^{n-1} \cdot (nQ(x) + (x - \alpha)Q'(x))$$

Wir sehene also: P, P' teilerfremd $\iff n = 1 \iff P$ separabel □

Definition 5.1.6. Sei L/K eine algebraische Erweiterung. Ein Element $\alpha \in L$ heist separabel über K wenn es Nullstelle eines separablen Polynoms über K ist. ($\iff$ das Minimalpolynom von α über K separabel ist)

Lemma 5.1.7. Sei L/K eine algebraische Erweiterung und sei Ω ein algebraischer Abschluss von L. Ist $\alpha \in \Omega$ separabel über K, so ist α auch separabel über L.

Beweis. Sei P das Minimalpolynom bzgl. α über L und Q das Minimalpolynom bzgl. α über K. Da Q(α)=0 teilt P offensichtlich Q. Hat dann Q nur einfache Nullstellen, dann hat P auch nur einfache Nullstellen. □

Satz 5.1.8. Sei K ein Körper, L/K eine endliche Körpererweiterung und Ω/K ein algebraischer Abschluss von K. Die Anzahl N der verschiedenen K-Homomorphismen von L nach Ω erfüllt die Ungleichung $1 \leq N \leq [L:K]$. Ferner sind die folgenden drei Eigenschaften äquivalent:

(i) $N = [L/K]$

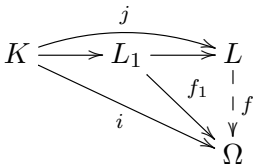
(ii) es gibt Elemente $x_1, .., x_n \in L$, separabel über K, s.d $L = K[x_1, .., x_n]$

(iii) jedes Element aus L ist separabel über K

Beweis. Den Beweis führen wir induktiv über n. Für n=1 ist L eine einfache Körpererweiterung und nach Proposition 5.1.2. ist N dann gleich der Anzahl der verschiedenen Nullstellen des Minimalpolynoms bzgl. x_1 in Ω. Da das Minimalpolynom Grad $[L:K]$ hat, wissen wir zwei sachen:

- N liegt zwischen 1 und $[L:K]$
- $N = [L:K]$ genau dann, wenn x_1 separabel über K ist.

Angenommen $x_1 \notin K$. Sei P_1 das Minimalpolynom bzgl. x_1, $d = \deg(P_1)$ und setze $L_1 = K[x_1]$. Die Einschränkung auf L_1 von jedem K-Homomorphismus $f : L \to \Omega$ ist ein K-Homomorphismus f_1 von L_1 nach Ω und hängt von der Wahl einer Nullstelle von P_1 in Ω ab. Daher gibt es 1 bis d solcher Homomorphismen f_1 und jeder von ihnen erlaubt es uns Ω als algebraischen Abschluss von L_1 zu betrachten. Die Situation wird von folgendem Diagramm beschrieben:



Der Grad der Erweiterung $L_1 \to L$ bestimmt sich zu:

$$[L:K] = [L:L_1][L_1:K] = [L:L_1] \cdot d \Longrightarrow [L:L_1] = [L:K]/d$$

Also ist $[L:L_1]$ kleiner als $[L:K]$. Nach Induktionsannahme liegt die Zahl der L_1-Homomorphismen von L nach Ω zwischen 1 und $[L:L_1]$. Auf diese Weise haben wir verschiedene K-Homomorphismen von L nach Ω konstruiert und zwar zwischen einem und $[L:K] = d \cdot [L:L_1]$ vielen. Da jeder K-Homomorphismus von L nach Ω auf diese Weise konstruiert werden kann, zeigt dies den ersten Teil des Satzes. Es bleibt die Äquivalenzen zu zeigen:

$(iii) \Rightarrow (ii)$: Nach Vor. ist L/K eine endliche Körpererweiterung. Also gibt es Elemente $x_1, .., x_n \in L$ mit $L = [x_1, .., x_n]$. Da jedes Element aus L separabel über K ist, sind es auch $x_1, .., x_n$.

$(ii) \Rightarrow (i)$: $K \subset K[x_1] \subset K[x_1, x_2] \subset ... \subset K[x_1, .., x_n] = L$ sind jeweils einfache und seperable Erweiterungen. Die vorangegangene Induktion zeigt, dass die Gleichung $N = [L:K]$ erfüllt ist wenn x_1 separabel über K ist, x_2 separabel über $K[x_1]$ ist usw.. Damit folgt Aussage (i).

$(i) \Rightarrow (iii)$: sein $N = [L:K]$ und $x \in L$. Dann ist $L = K[x_1, .., x_n] = K[x, x_1, .., x_n]$. Die vorangegangene Induktion zeigt dann auch, dass x separabel über K ist. □

Bemerkung. Eine Erw. welche den äquivalenten Eigenschaften aus 5.1.8. genügt, nennt man *separabel*.

5.2 Galoissche Erweiterungen

Definition 5.2.1. Sei L/K eine Körpererweiterung. Ein K-Automorphismus von L ist ein Körperautomorphismus, $\sigma : L \to L$, der Elemente aus K fest lässt, für den also gilt: $\sigma(x) = x$ für alle $x \in K$.

Bemerkung. Die Menge der K-Automorphismen von L ist eine Gruppe. Wir bezeichnen sie mit $Aut(L/K)$. Sei $\sigma \in Aut(L/K)$. Für ein $P \in K[X]$ gilt: $P(\sigma(x)) = \sigma(P(x))$ für jedes $x \in L$. D.h falls x eine Nullstelle von P ist, so ist $\sigma(x)$ ebenfalls eine Nullstelle von P. Also permutiert σ die Nullstellen von P in L.

Proposition 5.2.2. Sei L/K eine endliche Erweiterung. Die Kardinalität von $Aut(L/K)$ ist höchstens $[L : K]$. Gilt Gleichheit, also $Aut(L/K) = [L : K]$, ist die Erweiterung separabel.

Beweis Sei Ω/L ein algebraischer Abschluss von L. Jeder K-Automorphismus $\sigma \in Aut(L/K)$ induziert einen eindeutigen K-Homomorphismus von L nach Ω. Nach Satz 5.1.8. ist die Anzahl dieser Homomorphismen kleiner oder gleich $[L : K]$ und falls Gleichheit gilt ist die Erweiterung separabel. □

Definition 5.2.3. Man nennt eine endliche Erweiterung L/K *galoissch* oder *Galoiserweiterung* falls $Aut(L/K)$ Kardinalität $[L : K]$ besitzt. Die Gruppe $Aut(L/K)$ wird dann *Galoisgruppe* dieser Erweiterung gennant und wird als $Gal(L/K)$ notiert.

5.3 Beispiele

Beispiel 1 Wir betrachten die Erweiterung $\mathbb{C}/\mathbb{R}$.
Sei σ ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$ und $z = a + ib \in \mathbb{C}$ mit $a, b \in \mathbb{R}$. Dann gilt:

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

Da

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$$

besteht $Aut(\mathbb{C}/\mathbb{R})$ aus 2 Elementen, nämlich der Identität $\sigma(i) = i$ und der komplexen Konjugation $\sigma(i) = -i$. Man sieht leicht, dass die Erweiterung $\mathbb{C}/\mathbb{R}$ galoissch ist. Dazu überlegt man sich, dass man $\mathbb{C}$ durch $\mathbb{R}$ erhält in dem man z.B. i zu $\mathbb{R}$ adjungiert. Das Minimalpolynom von i bzgl. dieser Erweiterung wäre dann gegeben durch $X^2 + 1$. Dieses ist trivialerweise irreduzibel über $\mathbb{R}[X]$ und hat den Grad 2. Damit gilt $\#Aut(\mathbb{C}/\mathbb{R}) = 2 = [\mathbb{C} : \mathbb{R}]$ und nach Definition ist die Erweiterung galoissch.

Beispiel 2 Wir betrachten die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.
Jedes Element aus $\mathbb{Q}(\sqrt[3]{2})$ kann geschrieben werden als $a+b\sqrt[3]{2}+c\sqrt[3]{2}^2$, wobei $a, b, c \in \mathbb{Q}$. Ein $\mathbb{Q}$-Automorphismus σ von $\mathbb{Q}(\sqrt[3]{2})$ ist wohldefiniert, sobald das Bild von $\sqrt[3]{2}$ gegeben ist. Da:

$$\sigma(\sqrt[3]{2})^3 = \sigma(\sqrt[3]{2}^3) = \sigma(2) = 2$$

und die Gleichung $x^3 = 2$ nur eine reelle Nullstelle hat, nämlich $\sqrt[3]{2}$, besteht die Automorphismengruppe $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ nur aus dem trivialen Element, der Identität: $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$.
Man sieht leicht, dass diese Körpererweiterung nicht galoissch ist, da die Kardinalität der Automorphismengruppe $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$ ist und eine echte Körpererweiterung stets Grad ungleich 1 hat. Man könnte aber auch einfach das Minimalpolynom der Erweiterung bestimmen, was in diesem Fall $X^3 - 2$ wäre, und den Grad des Minimalpolynoms mit der Kardinalität von $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ vergleichen, was uns

zum gleichen Ergebnis führen würde.
Hätten wir hier eine Galoiserweiterung erhalten wollen, müssten wir nach weiteren Nullstellen von X^3-2 suchen und sie zu $\mathbb{Q}(\sqrt[3]{2})$ adjungieren. Dies würde uns auf die dritten Einheitswurzeln, die in $\mathbb{C}$ liegen, bringen. Natürlich müssten wir vorher noch die Irreduzibilität von X^3-2 über $\mathbb{Q}[X]$ zeigen, um auch wirklich zu verifizieren, dass es sich hier um das Minimalpolynom handelt. Die dritten Einheitswurzeln sind gegeben durch ζ und ζ^2, wobei $\zeta = \exp(\frac{2\pi i}{3})$ und die weiteren Nullstellen des Minimalpolynoms durch $\zeta\sqrt[3]{2}$ und $\zeta^2\sqrt[3]{2}$. Man sollte sich klar machen, dass es reicht nur $\zeta\sqrt[3]{2}$ zu $\mathbb{Q}(\sqrt[3]{2})$ zu adjungieren, da man $\zeta^2\sqrt[3]{2}$ durch Lineakombination von den beiden anderen Nullstellen erhält.
Die erhieltene Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2})/\mathbb{Q}$ wäre dann galoissch.
Es ist anzumerken, dass der Grad der Körpererweiterung nicht erhalten bleiben muss beim hinzuadjungieren weiterer Nullstellen. In unserem Fall würde sich dieser von 3 zu 6 vergrößern, wie man leicht mit der Gradformel nachprüfen kann. Außerdem müsste man hier auch explizit die Automorphismengruppe $Aut(\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2})/\mathbb{Q})$ bestimmen, insbesondere die Kardinalität und diese mit dem Grad der Körpererweiterung vergleichen um einzusehen, dass es sich hier wirklich um eine Galoiserweiterung handelt.