26. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Gabriel Lehéricy, Simon Müller

WS 2016/2017: 17. Februar 2017

Beweis (Steinitz)

"⇒" $E = F(u)$. Sei $F \subseteq K \subseteq E$, $f(x)$ Min. Pol. von u über F und $g(x)$ Min. Pol. von u über K.

Es ist $g(x)/f(x)$. Sei K' ein Unterkörper von E/F, erzeugt durch die Koeffizienten von g. $K' \subset K$ und $g(x)$ ist Min. Pol. von u über K'.

Da $E = K(u) = K'(u)$, haben wir $[E : K] = \deg g(x) = [E : K']$. Also $K' = K$. Jeder Zwischenkörper ist erzeugt durch die Koeffizienten der normierten Faktoren von $f(x)$. Da es nur endlich viele davon gibt, haben wir die Behauptung bewiesen.

"⇐" Fall 1:

F ist endlich (siehe Korollar 1, letzte Vorlesung).

Also ohne Einschränkung Fall 2:

F ist unendlich

Wir zeigen, dass $E = F(u, v)$ ein primitives Element hat. Der allgemeine Fall

$E = F(u_1, \ldots, u_k)$ folgt dann per Induktion.

Betrachte die Unterkörper $F(u + av)$ mit $a \in F$. Da es nur endlich viele davon gibt, aber unendlich viele $a \in F$, muss $a \neq b$ existieren, so dass $F(u + av) = F(u + bv)$. Aber dann ist $v = (a - b)^{-1}(u + av - u - bv) \in F(u + av)$ und $u = u + av - av \in F(u + av)$. Setze $z := u + av$, dann ist $E = F(u, v) = F(z)$. □

Kapitel 7: Fundamentaler Satz der Algebra

Satz
$\mathbb{C}$ ist algebraich abgeschlossen.

Beweis
Wir werden die folgenden Eigenschaften von $\mathbb{R}$ benötigen (diese werden allgemeiner für reell abgeschlossene Körper in der Vorlesung "Reelle algebraische Geometrie I" im 7. Semester gezeigt).

(*i*) $a \in \mathbb{R}$ mit $a \geq 0$ hat eine Quadratwurzel in $\mathbb{R}$.

(*ii*) Jedes $f \in \mathbb{R}[x]$ ungeraden Grades hat eine Nullstelle in $\mathbb{R}$.

Behauptung: (i) hat zur Folge, dass jedes Polynom zweiten Grades aus $\mathbb{C}[x]$ eine Nullstelle in $\mathbb{C}$ hat. Dafür genügt es zu zeigen, dass $z \in \mathbb{C}$ eine Quadratwurzel in $\mathbb{C}$ hat. Sei also $z = x + iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$. Wir wollen lösen:
$z = x + iy = (a + ib)^2 = (a^2 - b^2) + i2ab$ mit $a, b \in \mathbb{R}$. Also $x = a^2 - b^2$ und $y = 2ab$.
Die Gleichungen sind, abgesehen von der Wahl des Vorzeichens von a und b, äquivalent zu

$$a^2 = 1/2x \pm 1/2\sqrt{x^2 + y^2}$$
$$b^2 = 1/2x \pm 1/2\sqrt{x^2 + y^2},$$

wobei $\pm$ bedeutet, dass man für beide Gleichungen einheitlich entweder das $+$ oder das $-$ auswählt.

Betrachte nun $\mathbb{R} \subseteq \mathbb{C} \subseteq L$, wobei $L/\mathbb{C}$ endlich ist. Es ist $[\mathbb{C} : \mathbb{R}] = 2$. Zu zeigen: $L = \mathbb{C}$. Ohne Einschränkung ist $L/\mathbb{R}$ Galois.
Setze $G := \text{Gal}\,(L/\mathbb{R})$. Es ist $[L : \mathbb{R}] = |G| = 2^k m$ mit $k \in \mathbb{N}$ und $2 \nmid m$. G enthält eine 2-Sylow $H \leq G$. Fundamentaler Satz der Galois Theorie $\Rightarrow [L : \text{Inv}\ H] = |H| = 2^k$ beziehungsweise $[\text{Inv}\ H : \mathbb{R}] = m$.
Da aber jedes reelle Polynom ungeraden Grades eine Nullstelle in $\mathbb{R}$ hat, ergibt sich unter Benutzung des Satzes vom primitiven Element notwendig $m = 1$.
Also $[L : \mathbb{R}] = 2^k$ und $[L : \mathbb{C}] = 2^{k-1}$.
Sei $G' := \text{Gal}\,(L/\mathbb{C})$. Wenn $L \neq \mathbb{C}$, also $k \geq 2$, Sylow 1 liefert $H' \leq G'$ mit $|H'| = 2^{k-2}$.
Also ist $[L : \text{Inv}\ H'] = 2^{k-2}$, so $[\text{Inv}\ H' : \mathbb{C}] = 2$. - Widerspruch. $\square$

Kapitel 8: Auflösbare Erweiterungen

Definition
L/K endlich ist *auflösbar*, wenn es einen Oberkörper $E \supset L$ gibt, so dass E/K eine endlische Galois Erweiterung mit auflösbarer Gal (E/K) ist.

Satz (Galois Gruppe als Untergruppen von S_n)
Sei $f \in K[x]$ separabel, $\deg f = n \in \mathbb{N}$ und L/K Zerfällungskörper. Seien $a_1, \ldots, a_n \in L$ Nullstellen von f, so definiert

$$\begin{array}{rccc} \varphi: & \text{Gal } (L/K) & \longrightarrow & Sym\{a_1, \ldots, a_n\} \\ & \delta & \longmapsto & \delta|\{a_1, \ldots, a_n\} \end{array}$$

einen injektiven Gruppenhomomorphismus.

Beweis
$\delta \in \text{Gal } (L/K), f(a_i) = 0 \Rightarrow 0 = \delta(f(a_i)) = f(\delta(a_i))$, da δ die Koeffizienten von f fest lässt. Also ist $\delta(a_i)$ eine Nullstelle von f.
Da nun δ injektiv ist, ist auch $\delta : \{a_1, \ldots, a_n\} \to \{a_1, \ldots, a_n\}$ surjektiv, also bijektiv. Damit ist φ wohldefiniert.
Da $L = K(a_1, \ldots, a_n)$ und $\delta \in \text{Gal } (L/K)$ bereits eindeutig durch seine Werte auf $\{a_1, \ldots, a_n\}$ bestimmt ist, ist φ injektiv. □

Korollar 1
Sei L/K eine endliche Galois-Erweiterung vom Grad n, so lässt sich Gal (L/K) als Untergruppe von S_n auffassen.

Korollar 2
Sei L/K eine separable Erweiterung vom Grad ≤ 4, dann ist L/K auflösbar.

Beweis
Satz vom primitiven Element $\Rightarrow L = K(a)$. Sei $f \in K[x]$ das $Min.Pol._K a$. Sei L' ein Zerfällungskörper von f über K. Gal (L'/K) lässt sich als Untergruppe von S_4 auffassen. Da S_4 und alle ihre Untergruppen auflösbar sind, so sind L'/K und L/K auflösbar. □

Korollar 3

Es gibt endlich separable Körpererweiterungen, die nicht auflösbar sind.

Beweis

Sei k ein Körper und $L = k(T_1, \ldots, T_n) = \text{Quot } (k[T_1, \ldots, T_n])$ Körper der rationalen Funktion in endlich vielen Variablen $T_1, \ldots, T_n$.

Jede $\pi \in S_n$ definiert einen Automorphismus von L, in dem man π auf die Variablen $T_1, \ldots, T_n$ anwendet:

$$\begin{array}{ccc} k(T_1, \ldots, T_n) & \longrightarrow & k(T_1, \ldots, T_n) \\ \frac{g(T_1, \ldots, T_n)}{h(T_1, \ldots, T_n)} & \longmapsto & \frac{g(T_{\pi(1)}, \ldots, T_{\pi(n)})}{h(T_{\pi(1)}, \ldots, T_{\pi(n)})} \end{array}$$

Sei $K := \text{Inv } S_n \subseteq L$. Es ist (Satz 0.6, 23. Vorlesung) L/K Galois und $\text{Gal } (L/K) = S_n$. Wähle nun $n \geq 5$, dann ist $\text{Gal } (L/K)$ nicht auflösbar. $\square$