Algebra B III

Kuhlmann

28. Vorlesung

Beweis (Steinitz)

"$\Rightarrow$" $E = F(u)$; sei $F \subseteq K \subseteq E$; $f(x)$ Min Pol von u über F
und $g(x)$ " " " " " K

Es ist $g(x) \mid f(x)$. Sei K' Unterk. von E/F erzeugt durch die Koeff. 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 Koeffz. der normierten Faktoren von $f(x)$; da es nur endlich viele davon gibt haben wir die Behauptung bewiesen.

"$\Leftarrow$" Fall 1: F endlich ✓ (Kor. 1.27 Vor)

Also $\mathbb{O}$ Fall 2: F unendlich.

Wir zeigen $E = F(u,v)$ hat ein primitives Element;

der allgemeine Fall $E = F(u_1, \dots, u_k)$ folgt dann

per Induktion. Betrachte die Unterkörper

$F(u + av)$; $a \in F$, da ist 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

$E = F(u,v) = F(Z)$. ∎

§ Fundamentaler Satz der Algebra

Satz. $\mathbb{C}$ ist alg. abg.

Beweis: wir werden die folgende Eigenschaften von $\mathbb{R}$ benötigen [diese werden allgemeiner für reell abgeschlossene Körper in der RAG I Vorlesung im 7. Semester gezeigt].

(i) : $a \in \mathbb{R}$; $a \geq 0$ hat ein Quadratwurzel in $\mathbb{R}$

(ii) jedes $f \in \mathbb{R}[x]$ ungeraden Grades hat eine NS in $\mathbb{R}$.

Beh (i) hat zu Folge daß jedes Polynom 2. Grades aus $\mathbb{C}[x]$ hat eine NS in $\mathbb{C}$.

Dafür genügt es z.z daß $z \in \mathbb{C}$ hat eine Quadratwurzel in $\mathbb{C}$.

Sei also $z = x + iy \in \mathbb{C}$; $x, y \in \mathbb{R}$

wir wollen lösen: $z = x + iy = (a+ib)^2$, $a, b \in \mathbb{R}$
$= (a^2 - b^2) + i\,2ab$

also $x = a^2 - b^2$ und $y = 2ab$

Die Gleichungen sind, abgesehen von der Wahl des Vorzeichens von a und b äquivalent zu

$$a^2 = \tfrac{1}{2} x \pm \tfrac{1}{2}\sqrt{x^2+y^2}$$
$$b^2 = -\tfrac{1}{2} x \pm \tfrac{1}{2}\sqrt{x^2+y^2}$$

$\pm$ bedeutet das man für beide Gleichungen einheitlich entweder das + oder das − auswählt.

Beh

Betrachte nun

$\mathbb{R} \subseteq \mathbb{C} \subseteq L$ wobei $L/\mathbb{C}$ endlich ist.

Es ist : $[\mathbb{C} : \mathbb{R}] = 2$.

z.z : $L = \mathbb{C}$. $\Leftrightarrow$ $L/\mathbb{R}$ ist Galois.

Setze $G := \mathrm{Gal}(L/\mathbb{R})$.

Es ist

$[L : \mathbb{R}] = |G| = 2^k m$ mit $k \in \mathbb{N}$ und $2 \nmid m$.

G enthält eine 2-Sylow $H \leq G$

FSGT $\Rightarrow$ $[L : \mathrm{Inv}\, H] = |H| = 2^k$ bzw

$[\mathrm{Inv}\ H : \mathbb{R}] = m$.

Da aber jedes reelle Polynom ung. Grades eine NS 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 $G' := \mathrm{Gal}(L|\mathbb{C})$. Wenn $L \neq \mathbb{C}$

also $k \geq 2$, Sylow 1 liefert $H' \leq G'$

mit $|H'| = 2^{k-2}$.

Also ist $[L : \mathrm{Inv}\ H'] = 2^{k-2}$

so $[\mathrm{Inv}\ H' : \mathbb{C}] = 2$. $\lightning$ ∎

---

§ Auflösbare Erweiterungen.

Definition (a) $L|K$ endl. ist **auflösbar** wenn es einen Oberkörper $E \supset L$ gibt so daß $E|K$ eine endl. Galois Erw. mit auflösbarer $\mathrm{Gal}(E|K)$

Satz (Galois Gruppe als Untergruppen von S_n).

Sei $f \in K[x]$ separable, $\deg f = n \in \mathbb{N}$

L/K Zerfällungskörper. Seien $a_1, \dots, a_n \in L$

NS von f, so definiert

$$\varphi : Gal(L/K) \longrightarrow Sym\{a_1, \dots, a_n\}$$

$$\sigma \longmapsto \sigma | \{a_1, \dots, a_n\}$$

einen injektiven Gruppenhom.

Beweis. $\sigma \in Gal(L/K)$, $f(a_i) = 0 \Rightarrow$

$0 = \sigma(f(a_i)) = f(\sigma(a_i))$; also $\sigma(a_i)$ NS von S.

da
σ die
Koeff. von f
fest läßt.

Da nun σ injektiv ist $\sigma : \{a_1, \dots, a_n\} \longrightarrow \{a_1, \dots, a_n\}$

ist auch surjektiv; also bijektiv. Damit ist

φ wohldefiniert. Da $L = K(a_1, \dots, a_n)$

und $\sigma \in Gal(L/K)$ ist bereits eindeutig durch seine

Werte auf $\{a_1, \dots, a_n\}$ bestimmt ist,

ist φ injektiv. ∎

Korollar 1. Sei L/K endl. Galois Erw. vom Grad n; so läßt sich $Gal(L/K)$ als Untergruppe von S_n auffassen. ∎

Korollar 2: Sei L/K eine separable Erw. vom Grad ≤ 4; dann ist L/K auflösbar

Beweis: Satz. Prim. El $\Rightarrow L = K(a)$.

Sei $f \in K[x]$ Min Pol_K a

Sei L' Zerfallungskörp von f über K;

$Gal(L'/K)$ läßt sich als Untergruppe von S_4 auffassen. Da S_4 und alle ihre Untergr. auflösbar sind, so sind L'/K und L/K auflösbar. ∎

Korollar 3 Es gibt endl. sep. Körpererw. die nicht auflösbar sind.

Beweis: Sei k Körper und

$$L = k(T_1, \dots, T_n) = \mathrm{Quot}\left(k[T_1, \dots, T_n]\right)$$

Körper der rationalen Funkt. in endlich vielen Variablen $T_1, \dots, T_n$.

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

$$k(T_1, \dots, T_n) \longrightarrow k(T_1, \dots, T_n)$$

$$\frac{g(T_1, \dots, T_n)}{h(T_1, \dots, T_n)} \longmapsto \frac{g(T_{\pi(1)}, \dots, T_{\pi(n)})}{h(T_{\pi(1)}, \dots, T_{\pi(n)})}$$

Sei $K := \mathrm{Inv}\, S_n \subseteq L$

Es ist (Satz 0.6 25. Vor)

$L|K$ Galois und $\mathrm{Gal}(L|K) = S_n$.

Wähle nun $n \geq 5$; dann ist $\mathrm{Gal}(L|K)$ nicht auflösbar. ∎