FFC 10.3.08

Forts. von Körperiso auf Zerf.ks eines Polynom.

Satz: $\varphi: K \to F$ Körperiso. $f \in K[x]$ $(\deg f \geq 1)$

E Zerfällungskörper von f über K, L Zerf. Körp. von $\varphi(f)$ über F,

Dann $\exists\ \bar{\varphi}: E \to L$ Körperiso mit $\bar{\varphi}|_K = \varphi$

Bew: Ind^v $[E:K]$ (evtl das $\leq(\deg f)$!)

$[E:K]=1$ heißt $E=K$, f zerfällt über K

$f = a(x-b_1)\cdot\ldots\cdot(x-b_n)$ mit $a, b_i \in K$

Da φ Körperhom ist $\varphi(f) = \varphi(a)(x-\varphi(b_1))\cdot\ldots\cdot(x-\varphi(b_n))$

und $\varphi(f)$ zerfällt über F, also F Zerf körper $\varphi(f)$ über F, $\bar{\varphi}=\varphi$ Iso

zwischen den beiden Zerf kö.

$[E:K]>1$ $\quad E \xrightarrow{\bar{\varphi}} L$] IV.

$K(b) \xrightarrow{\psi} F(\varphi(b))$] Forts. von φ auf einf. alg. Erw.

$K \xrightarrow{\varphi} F$

f zerfällt nicht über K; sei $b \in F \setminus K$ Nullstelle von f und zwar

b Nullstelle eines irred Faktors $g \in K[x]$ von f. Dann $\varphi(b)$ Nullstelle

von $\varphi(g)$ irred $\in F[x]$ mit $\varphi(g) \mid \varphi(f)$ [weil φ Homom.]

Können φ fortsetzen zu $\psi: K[b] \to F[\varphi(b)]$ Isom. mit $\psi|_K = \varphi$

Da $[K(b):K]>1$ ist $[E:K(b)] < [E:K]$. E ist Zerf kö. von f auch über

$K(b)$, L Zerf kö von $\varphi(f)$ auch über $F(\varphi(b))$, ψ fortsetzbar

nach IV. zu $\bar{\varphi}$ $\bar{\varphi}: E \to L$ Körperiso mit $\bar{\varphi}|_{K(b)} = \psi$ also $\bar{\varphi}|_K = \psi|_K = \varphi$.

Lem. $E \subseteq F$ endl. Körper, $|E|=q$, $|F|=q^n$ dann ist F Zerf. kö von $x^{q^n}-x$ ü. E.

Bew: $|F|=q^n$ → jedes $a \in F$ erfüllt $a^{q^n}=a$, ist also Nullstelle v. $x^{q^n}-x$.

Dieses Polyn. hat also $\deg f$ versch. Nullst. in F und zerfällt daher ü. F.

[Vervollst, dass $F[x]$ ZPE-Ring als Nullst von f, dann f durch $(x-a)$

und durch $(x-b)$ teilbar, daher f durch $\text{kgV}((x-a),(x-b)) = (x-a)(x-b)$ teilb.

insb: $\deg f = n$, f hat versch. Nst. $a_1 \ldots a_n$, dann $f = c(x-a_1)\cdot\ldots\cdot(x-a_n)$]

Da F nur aus Nst von $x^{q^n}-x$ bestellt und E enthält, ist F Zerf kö von

$x^{q^n}-x$ über E.

Kor Je zwei Erweiterungskörper desselben Grades über einem endl. Körper E sind E-isomorph. d.h. E endl. Körper $F_1 \supseteq E$, $F_2 \supseteq E$, $[F_1:E]=[F_2:E]$ dann $\exists \varphi$ $\varphi: F_1 \to F_2$ Körperiso mit $\varphi|_E = id_E$

Notation: E-Isom zwischen zwei Erweiterungskörpern von E ist Körperiso das Elemente fix lässt.

Kor: Je zwei endl. Körper mit p^n El sind isomorph (weil beide Zerfällungskörper von $X^{p^n}-X$ über $\mathbb{Z}_p$).

Nachtrag zu Körpererweiterungen im Allgemeinen

endlich-dim $\Leftrightarrow$ algebraisch u. endl. erzeugt

Prop: $[F:K]=n$ endl. $\Rightarrow$ $F:K$ algebraisch (jedes El. von F alg vom Grad $\leq n$ über K) und F endl. erz. über K ($F=K[a_1,\dots,a_m]$).

Bew: $\forall$ $n+1$ El von F sind K-l.a., insb für jedes $a \in F$: $1, a, a^2, \dots, a^n$ K-l.a., d.h. $\exists\, c_0, c_1, \dots, c_n \in K$ nicht alle 0 mit $c_0 + c_1 a + \dots + c_n a^n = 0$

$f = \sum_{k=0}^{n} c_k x^k$ ist Polyn. $\in K[x] \setminus \{0\}$ mit $f(a)=0$ deg $f \leq n$

F erzeugt als K-VR vom n Basisel. $a_1 \dots a_n \in F$ jedes $a \in F$ ist K-lineare Komb. der a_i, insb. jedes $a \in F$ in $K[a_1 \dots a_n]$.

Prop: Sei $K \subseteq F$, $F = K(a_1, \dots, a_n)$ mit $a_1 \dots a_n \in F$ alg. über $K \Rightarrow [F:K]$ endl.

(„endl. erzeugt von alg. El $\Rightarrow$ endl. dim")

Bew: Sei $K_i = K(a_1, \dots a_i)$, $K_0 = K$, $K_n = F$

$K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n \subseteq F$ $\quad K_{i+1} = K_i(a_{i+1})$

a_{i+1} alg über K_i da alg über K, daher $[K_{i+1}:K_i] = \deg f_i$ f_i Minimalpolyn. von a_{i+1} über K_i, insb. endlich. $[F:K] = [F:K_{n-1}] \cdot \dots \cdot [K_1:K]$ endlich.

Kor: $F:K$ sei $F = K(S)$ $S \subseteq F$ sei jedes $s \in S$ alg über K dann $F:K$ algebraisch.

Bew: Jedes $a \in F$ ist der Form $a = f(s_1, \dots s_n)$ für gewisse $s_1 \dots s_n \in S$ (endl. viele!) und $f \in K[x_1, \dots, x_n]$ daher $a \in K[s_1, \dots, s_n]$ mit $[K[s_1 \dots s_n]:K]$ endlich, daher a alg über K.

Kor $K \subseteq F$ Körpererw. $E = \{a \in F \mid a \text{ alg. ü. } K\}$ dann E Körper

Beu: $E = K(E)$ weil $E \subseteq K(E)$ und andererseits jedes El. von $K(E)$ alg. ü. K also $K(E) \subseteq E$

Bspi: $\mathbb{A}$ die Menge aller El in $\mathbb{C}$ die alg ü. $\mathbb{Q}$ sind, dann $A: \mathbb{Q}$ Bsp einer unendl. dim. alg Körpererw. (unendlich dim., da es nach Eisenstein $\forall n \in \mathbb{N}$ ein $f \in \mathbb{Q}[x]$ irred mit deg $f = n$ gibt.)

Algebraischer Abschluss eines Körpers.

Def: K Körper, $S \subseteq K[x]$ eine Menge von Polynomen mit deg ≥ 1, $F \supseteq K$ heißt Zerfk. der Menge S von Polynom. in $K[x]$ wenn

1) jedes $f \in S$ zerfällt ü. F

2) $F = K(W)$ W besteht nur aus Nullstellen von Polyn. $\in S$.

[Für $S = \{f_1, \dots, f_n\}$ endlich ist Zerf.kö von S ü. K einfach der Zerfkö von $f_1 \cdot f_2 \cdot \dots \cdot f_n$ über K]

Def: K heißt alg abgeschlossen, wenn jedes $f \in K[x]$ mit deg $f \geq 1$ über K zerfällt. [genau: jedes $f \in K[x]$ mit deg $f \geq 1$ ein Nullst in K hat]

Def: $F \subseteq K$, F heißt alg. Abschluss von K, wenn

1) $F:K$ algebr. und 2) F alg abgeschlossen

Ü: $F \supseteq K$ F ist alg Abschluss von $K \Leftrightarrow F$ Zerfkö der Menge aller Polyn. $\in K[x]$ mit deg ≥ 1 [genau: Zerfkö der Menge aller normierten Polyn $\in K[x]$].

Zerfkö einer bel. Menge $S \subseteq K[x]$ über K existiert und ist bis auf K-Isom. eindeutig

Zuerst Eindeutigkeit

Satz: $\varphi: K \to F$ Körperiso $S \subseteq K[x]$ (mit deg $f \geq 1$ für alle $f \in S$)

E Zerfkö von S über K, L Zerfkö von $\varphi(S) = \{\varphi(f) \mid f \in S\}$ über F.

dann $\exists\, \bar{\varphi}: E \to L$ Körperiso mit $\bar{\varphi}|_K = \varphi$

Bew: Betrachte Menge T aller (E_i, L_i, φ_i) mit $K \subseteq E_i \subseteq E$, $F \subseteq L_i \subseteq L$
$\varphi_i : E_i \to L_i$ Körperiso mit $\varphi_i|_K = \varphi$; geordnet durch $(E_i, L_i, \varphi_i) \leq (E_k, L_k, \varphi_k)$
$:\Leftrightarrow E_i \subseteq E_k$, $L_i \subseteq L_k$, $\varphi_k|_{E_i} = \varphi_i$. Da jede Kette in dieser Menge T eine
obere Schranke in T hat $(\bigcup_{i\in I} E_i, \bigcup_{i\in I} L_i, \bigcup_{i\in I} \varphi_i)$ für $\{(E_i, L_i, \varphi_i) \mid i \in I\}$ Kette
Also hat T max El. $(\tilde{E}, \tilde{L}, \tilde{\varphi})$.
Beh. $\tilde{E} = E$, $\tilde{L} = L$. Ag $\tilde{E} \subsetneq E$, dann $\exists$ Nullstelle b eines $f \in S$ die in $E \setminus \tilde{E}$ liegt.
$\tilde{E} = E_0$, da E über K von der Nullstelle erzeugt wird.]
Dann $\tilde{\varphi}$ ein Iso $\Psi : \tilde{E}(b) \to \tilde{L}(\tilde{G}(b))$ fortsetzbar auf $\tilde{E}(b), \tilde{L}(\tilde{G}(b)), \Psi) >$
$> (\tilde{E}, \tilde{L}, \tilde{\varphi})$ in T, Widerspr zur Max.
Wenn $\tilde{L} \neq L$, dann analog $\tilde{\varphi}^{-1} : \tilde{L} \to \tilde{E}$ fortsetzbar zu $\Psi : \tilde{L}(c) \to \tilde{E}(\tilde{\varphi}(c))$ ..

Lem: K Körper, $F : K$ alg Erw. $\Rightarrow |F| \leq \aleph_0 |K| = \begin{cases} |K| & \text{falls } K \text{ unendl.} \\ \aleph_0 & \text{falls } K \text{ endl.} \end{cases}$ $\quad$ Alef.

Bew: El von F sind Nullst von irred. Polyno. $\in K[x]$, jedes Polyn. hat nur endl.
viele Nst; $|F| \leq \left|\sum_{n\in\mathbb{N}} n \cdot |\{f \in K[x] \mid \deg f = n\}|\right| = \left|\sum_{n\in\mathbb{N}} n |K|^{n+1}\right| \leq \aleph_0 \cdot \aleph_0 \cdot |K| \leq \aleph_0 |K|$

Satz Jeder Körper K hat alg. Abschluss $\bar{K}$

Bew Sei S Menge mit $S > \aleph_0 \cdot |K|$ (existiert, z.B. Potenzmge von $\mathbb{N} \times K$).
K eingebettet als Teilmenge in S: $K \subseteq S$. Betrachten Körpererw. von K,
die in S eingebettet sind: $K \subseteq E \subseteq S$, wobei $\cdot : E \times E \to E$, $+ : E \times E \to E$
so daß sie $\cdot|_{K\times K} \to K$, $+|_{K\times K} \to K$ fortsetzen.
Betrachten Menge T aller Tripel $(E, +, \cdot)$ mit $K \subseteq E \subseteq S$ Funktion $+, \cdot : E \times E \to E$
und E alg ü. K.
sod Körperaxiome erfüllt und $+, \cdot$ die Op $K \times K \to K$ fortsetzen.
Axiome der Mengenlehre (ZF) garantieren dass T tatsächl. eine Menge ist.
Auf T Ordnungsrel $\leq$ $(E_1, +_1, \cdot_1) \leq (E_2, +_2, \cdot_2)$ wenn $E_1 \subseteq E_2$ und $+_2$ Fortsetz. von $+_1$
$\cdot_2$ Fortsetz. von $\cdot_1$ Zornsches Lemma anwendbar: Jede Kette hat obere Schranke
$(\bigcup E_i, \bigcup +_i, \bigcup \cdot_i)$ also $\exists$ max El von T.

Beh: max El $(F, +, \cdot)$ von T ist alg Abschluss von K $F : K$ alg., da
$(F, +, \cdot) \in T$ Ag F nicht alg abg. Dann sei $E : F$ eine einfache alg.
Körpererweiterung, $[E : F] = n > 1$

In S ist ganz Platz um eine Kopie von E einzubetten $|E \setminus F| \leq \aleph_0 \cdot |K|$, $|S \setminus F| > \aleph_0 \cdot |K|$, Verwirkliche E auf einer Teilmenge von S, die F ganz umfasst, so dass Null und Add von E die Op von F fortsetzen, dann $(E,+,\cdot) \in T$ echt größer als $(F,+,\cdot)$, Widerspruch zur Maximalität von $(F,+,\cdot)$

Kor: K Körper $S \subseteq K[x]$ (sd. $\forall f \in S$ $\deg f \neq 1$) dann $\exists F : K$ Zerfk von S über K.

Bew: ~~Alg~~ Alg. Abschluss $\bar{K}$ bilde $F = K(w)$ mit $V = \{v \in \bar{K} \mid \exists f \in S\, f(v) = 0\}$ ist Zerf kö von S über K.