25.2.2008 Endliche Körper u. Kodierung

Körpererweiterungen

Def: $F:K$ Körpererweiterung heißt K, F Körper, $K \subseteq F$

Def: $F:K$ Körpererweiterung $\Rightarrow$ F ist K-VR, $[F:K] = \dim_K F$

$[F:K]$ heißt Index der Körpererweiterung $F:K$

($K \subseteq F \Rightarrow$ Einschränkung der Mult von F auf

$\cdot K \times F \to F$ ist Skalarmultiplikation $(F,+)$ mit dieser

Skalarmultiplikation erfüllt Axiome eines K-VR)

Lemma: $K \overset{B}{\subseteq} E \overset{C}{\subseteq} F$ Körper $\Rightarrow$ $[F:K] = [F:E] \cdot [E:K]$

Beweis: Sei B ein K-Basis von E, C ein E-Basis von F. Zeigen:

die Ausdrücke $b \cdot c$ für $b \in B$, $c \in C$ sind für verschiedene (b,c)

paarweise verschieden und bilden K-Basis von F.

Es folgt $\dim_K F = |\{b \cdot c \mid b \in B, c \in C\}| = |B \times C| = |B| \cdot |C| = \dim_K E \cdot \dim_E F$

1.) Erzeugendensystem: geg $f \in F$ ($e_1, \dots, e_m \in E$ sd) $\exists e_c$, $c \in C$ sd

$f = \sum_{c \in C}^{m} e_c c$ weiters $\exists$ für jeden e_c Koeff

$k_{c,b} \in K$ sd $e_c = \sum_{b \in B} k_{c,b} b$

Also $f = \sum_{c \in C} e_c c = \sum_{c \in C} \sum_{b \in B} k_{c,b} b c$

Haben: jedes f ist K-Linearkomb von El $b \cdot c$ mit $b \in B$, $c \in C$

2.) El $b \cdot c$ sind K-lu und paarweise verschieden

~~ang: $b_1 \dots b_k \in B$ $c_1, \dots, c_m \in$~~

geg: endl viele El $\in B \times C$ sein $b_1 \dots b_k$ alle vorkommenden B-Koordinaten

$c_1 \dots c_m$ alle vorkommenden C-Koord, zeigen $(b_i c_j)$ $i = 1..k$, $j = 1..m$ sind K-lu

ang $0 = \sum_{\substack{1 \le i \le k \\ 1 \le j \le m}} k_{ij} b_i c_j = \sum_{1 \le j \le m} \underbrace{\left(\sum_{1 \le i \le k} k_{ij} b_i \right)}_{\in E} c_j$

Da C E-lu $\Rightarrow \forall j: \sum_{1 \le i \le k} k_{ij} b_i = 0$

Da B K-lu $\Rightarrow \forall i,j$ $k_{ij} = 0$ ✓

Def: $K \subseteq F$ Körper, S Menge $\subseteq F$ dann sei $K[S]$ der von $K \cup S$ erzeugte Unterring von F, def als $K[S] := \bigcap\limits_{\substack{K\cup S \subseteq R \subseteq F \\ R \text{ Ring}}} R$

und $K(S)$ der von $K \cup S$ erzeugte Unterkörper von F def

als $K(S) = \bigcap\limits_{\substack{K\cup S \subseteq E \subseteq F \\ E \text{ Körper}}} E$

Schreibt $K[s_1, .., s_n]$ für $K[\{s_1 .. s_n\}]$
$K(s_1, .., s_n)$ für $K(\{s_1, .., s_n\})$

Lemma: $K \subseteq F$ Körper, S Menge $\subseteq F$ $s_1, .., s_n, s \in F$ Dann

1) $K[s] = \{f(s) \mid f \in K[x]\}$
$= \{a_0 + a_1 s + ... + a_n s^n \mid n \in \mathbb{N}_0, a_i \in K\}$

2) $K[s_1 .. s_n] = \{f(s_1, .., s_n) \mid f \in K[x_1 .. x_n]\}$

3) $K[S] = \{f(s_1 .., s_n) \mid n \in \mathbb{N}_0, s_1 .. s_n \in S, f \in K[x_1 .. x_n]\}$

4.) $K(s) = \{\frac{f(s)}{g(s)} \mid f, g \in K[x], g(s) \neq 0\}$

5.) $K(s_1 .. s_n) = \frac{f(s_1 .. s_n)}{g(s_1 .. s_n)} \mid f, g \in K[x_1 .. x_n], g(s_1 .. s_n) \neq 0\}$

6) $K(S) = \{\frac{f(s_1 .. s_n)}{g(s_1 .. s_n)} \mid n \in \mathbb{N}_0, s_1 .. s_n \in S, f, g \in K[x_1 .. x_n], g(s_1 .. s_n) \neq 0\}$

Bew Skizze: sei M die Menge rechts.

Zuerst zeigen: M enthält $K \cup S$ und ist Unterring (1-3) bzw Unterkörper (4-6) von F

Zeigt: $0 \in M$ $a, b \in M \Rightarrow a - b \in M$ $a, b \in M \Rightarrow a \cdot b \in M$

in (4-6) noch $1 \in M$, $a, b \in M$, $b \neq 0 \Rightarrow a b^{-1} \in M$

Dann ist M unter den Objekten, die in Def von $K[S]$ bzw $K(S)$ geschnitten werden,

also $M \supseteq K[S]$ bzw $M \supseteq K(S)$

Zweitens zeigen: jeder Unterring [bzw Unterkörper] von F, der $K \cup S$ enthält, enthält ganz M; das gilt weil wenn Man $K \cup S$ durch Operationen bzgl dieser Ringe (Körper) abgeschlossen sind, vorkommt

Also $M \subseteq K[S]$ bzw $M \subseteq K[S]$

Def: $K \subseteq F$ Körper $u \in F$

u heißt algebraisch über K, wenn $\exists f \in K[x]$, $f \neq 0$ mit $f(u) = 0$

u heißt transzendent über K, d.h. wenn aus $f(u) = 0$ mit

$f \in K[x]$ folgt $f = 0$

Satz: (Einfache transzendente Körpererweiterung)

Sei $K \subseteq F$, $u \in F$, u transzendent über K dann $K(u) \cong K(x)$ mittels ein Iso:

$\varphi: K(x) \to K(u)$ mit $\varphi|_K = id_K$ und $\varphi(x) = u$

[$K(x)$ der „Körper der rationalen Funktionen über K", d.h. $K(x)$ Quotientenkörper des Polynomrings $K[x]$]

Bew: Einsetzhom $\varphi: K[x] \to F$ mit $\varphi|_K = incl_{K \hookrightarrow F}$ ($\forall k \in K$ $\varphi(k) = k$) und

$\varphi(x) = u$. $\operatorname{Im} \varphi = \{ f(u) \mid f \in K[x] \} = K[u]$

$\operatorname{Ker} \varphi = (0)$ da u transzendent über K

Da jedes Element aus $K[x] \setminus \{0\}$ von φ auf ein Einheit in F abgebildet wird, kann man φ auf $\overline{\varphi}: K(x) \to F$ fortsetzen wobei $\overline{\varphi}$ wieder injektiv, und so aussieht

: $\overline{\varphi}\left(\frac{f}{g}\right) = \varphi(f)(\varphi(g))^{-1} = f(u) \cdot g(u)^{-1} = \frac{f(u)}{g(u)}$. Damit $\operatorname{Im} \overline{\varphi} = \left\{ \frac{f(u)}{f(u)} \mid f, g \in K[x] \right\} = K(u)$

$\operatorname{Ker} \overline{\varphi} = (0)$ also $\overline{\varphi}: K(x) \to K(u)$ Iso mit $\overline{\varphi}(k) = k$ $\overline{\varphi}(x) = u$.

Bem: haben verwendet: R komm Ring, S mult $\subseteq R$, $\varphi: R \to T$ Ringhom sodass

$\forall s \in S$ $\varphi(s)$ Einheit $\in T$ dann $\exists! \, \overline{\varphi}: R_S \to T$ mit $\overline{\varphi}|_R = \varphi$ nämlich $\overline{\varphi}\left(\frac{r}{s}\right) = \varphi(r)(\varphi(s))^{-1}$

und wenn φ injektiv dann auch $\overline{\varphi}$.

Satz: Einfache algebraische Körpererweiterung

$K \leq F$ Körper, $u \in F$ algebr. über K dann:

1) $\exists!$ normierten Polynom $g \in K[x]$ sd

$\forall f \in K[x]: f(u)=0 \Leftrightarrow g \mid f$ in $K[x]$ (d.h. $\exists h \in K[x]$ $f(x)=g(x)h(x)$

und dann g ist irreduzibel in $K[x]$

[Dieses g heißt Minimalpolynom von u über K]

2.) $K(u)=K[u] \simeq K[x]/(g)$ (g das Minpolyn von u über K)

wobei $\varphi: K[x]/(g) \to K[u]$ def durch $\varphi(f+(g))=f(u)$ ein Ring isom

3.) $\{1, u, u^2, \dots u^{n-1}\}$ $n=\deg g$ bildet K-Basis von $K(u)=K[u]$, insb

$[K[u]:K]=\deg g$

Bew: sei $\varphi: K[x] \to F$ Einsetzhomom. mit $\varphi(k)=k$ für alle $k \in K$ und $\varphi(x)=u$,

dann $\operatorname{Im}\varphi = \{f(u) \mid f \in K[x]\} = K[u]$ und $\operatorname{Ker}\varphi$ Ideal $\trianglelefteq K[x]$ Hauptidealring

also $\exists g \in K[x]$ $\operatorname{Ker}\varphi = (g) = g(x) \cdot K[x]$

(El von $K[x]$ erz dasselbe Ideal $\Leftrightarrow$ wenn sie sich nur durch Mult mit

einer Konstante unterscheiden $\Rightarrow$ jedes Ideal $\neq (0) \leq K[x]$ hat eindeutig

bestimmten normierten Erzeuger) $\operatorname{Ker}\varphi \neq (0)$ weil u alg über $K \Rightarrow \operatorname{Ker}\varphi = (g)$

g, normiert, eind. best. Eindeutig bestimmtes normiertes g mit

$f \in \operatorname{Ker}\varphi$ (d.h. $f(u)=0$) $\Leftrightarrow f \in (g)$ (d.h. $g \mid f$ in $K[x]$)..

Zeigen g irred:

$\varphi: K[x] \to F$ mit $\operatorname{Im}\varphi = K[u]$, $\operatorname{Ker}\varphi = (g)$ nach 1. Isom Satz

$K[x]/(g) \simeq K[u]$ Integr. bereich $\leq F$ weil Unterring $\leq$ Körper

R kom Ring mit 1: R/I IB $\Rightarrow$ I Primideal also (g) Primideal $\Rightarrow$

g prim, g prim $\Rightarrow$ g irred.

Zeigen $K[u]=K(u)$.

es genügt z.z. $K[u]$ ist Körper.

$K[u] \simeq K[x]/(g)$ g irred $\in K[x]$

g irred $\Rightarrow$ (g) maximal unter den Hauptideal $\neq R$

$K[x]$ Hauptidealring $\Rightarrow (g)$ maximales Ideal $\trianglelefteq K[x]$

R komm. Ring mit 1 $I \trianglelefteq R \Rightarrow (R/I$ Körper $\Leftrightarrow I$ maximal$)$

also $K[x]/(g)$ Körper, d.h. $K[u]$ Körper.

ad 3) $1, u, \dots u^{n-1}$ erzeugt $K[u]$ als K-VR: jedes El $\in K[u]$ der

Form $f(u)$ für ein $f \in K[x]$ Div mit Rest durch g

$f(x) = q(x)g(x) + r(x)$ $\deg r < \deg g$ und $f(u) = r(u)$ weil $g(u) = 0$

$f(u) = a_0 + a_1 u + \dots + a_{n-1} u^{n-1}$ $a_i \in K$ v

K-l.u. ang $k_0 + k_1 u + \dots + k_{n-1} u^{n-1} = 0$

sei $h(x) = \sum k_i x^i$ $h(u) = 0$ also $g | h$ aber $\deg h < \deg g \Rightarrow h = 0$ also $k_i = 0$