FFC 7.4.08

Separable Körpererweiterungen

Def: Irred Polyn. $f \in K[x]$ heißt separabel wenn f in seinem Zerf.kö über K deg f viele verschiedene Nullstellen hat (äquiv.: in keiner Körpererw. vorkommt eine mehrf. Nullstelle hat).

Zur Erinnerung: $f \in K[x]$ hat in keiner Erw vorkommt mehrf. Nullstelle $\Leftrightarrow ggT(f,f')=1$ mehrf Nullstelle $u \Rightarrow$ Nullst von f und f' Minimalp. von u müßte in $K[x]$ f und f teilen umgekehrt: $ggT(f,f')=g \neq 1$ im Zerf kö von g mehrf. Nullst.

Bem: f irred $\in K[x] \Rightarrow$ (f hat in irgendeiner Erw von K mehrf. Nst $\Leftrightarrow f'=0$). Weil für f irred: $ggT(f,f') \neq 1 \Leftrightarrow ggT(f,f')=f$
$f \mid f'$ mit $\deg f' < \deg f \Rightarrow f'=0$.

Satz: K Körper. Alle f irred $\in K[x]$ separabel $\Leftrightarrow \chi(K)=0 \vee$
$\vee (\chi(K)=p \wedge \psi: K \to K \quad \psi(x)=x^p$ surj.)

Bew: „$\in$" Wenn $\exists f$ irred nicht separabel, dann $f'=0$
$f=\sum_{k=0}^{n} a_k x^k \quad a_n \neq 0 \qquad f'=\sum_{k=0}^{n} k a_k x^{k-1}=0$ d.h. $\forall k: (k+1)a_k=0$
Da K kein Nullteiler hat, folgt $\chi(K)=p \neq 0$ und für alle k mit $a_k \neq 0$ gilt $p \mid k$
D.h. $\chi(K)=p$ prim und $f=\sum_{k=0}^{m} a_{kp} x^{kp}$.
Wenn jedes $a \in K$ eine p-te Potenz ist, dann sei b_k sod $a_{kp}=(b_k)^p$
Dann $f=\sum_{k=0}^{m} (b_k)^p x^{kp} = (\sum_{k=0}^{n} b_k x^k)^p$ also f nicht irred. Also folgt aus Existenz einer nicht sep. irred Polyn. dass $K^p \subsetneq K$, nicht jedes El. von K p-te Potenz.

„$\Leftarrow$" Aus $\chi(K)=p$ und $K^p \subsetneq K$, dann existiert nicht sep. irred. Polyn. $\in K[x]$. Sei $a \in K \setminus K^p$, betrachte $f=X^p-a$. Im Zerf kö Erw f über K sei b ein Nullstelle von f d.h. b sod $b^p=a$ dann
$f=X^p-a=X^p-b^p=(X-b)^p$. f hat in seinem Zerf kö über K ein p-fache Nullstelle.

Def: ein Körper heißt vollkommen/perfekt wenn jedes f irred $\in K[x]$ separabel ist.

Insb: jeder Körper mit $\chi(K)=0$ ist perfekt. Jede endl. Körper ist perfekt.

Bsp für nicht perfekten Körper: $\mathbb{F}_q(X)$, z.B in $\mathbb{Z}_p(X)$ ist x kein p-te Potenz, daher y^p-x ein nicht separables Polynom in $\mathbb{Z}_p(X)[Y]$

Def: $F:K$ algebraische Körpererw. heißt separabel, wenn jedes f irred $\in K[x]$, das in F eine Nullstelle hat, separabel ist.

[Körper perfekt $\Leftrightarrow$ jede alg Erw separabel]

Bem: für nicht alg Erw separabel anders definieren.

normale Körpererweiterungen

Def: $F:K$ Körpererw heißt normal, wenn jedes irred $f \in K[x]$ das in F eine Nullst hat, über F zerfällt.

Satz: $F:K$ alg Körpererw. Dann äquivalent

1) $F:K$ normal
2) F ist Zerfk. einer Menge von Polynom. in $K[x]$ über K
3) $\forall$ K-Monomorph. $\psi: F \to \bar{K}$ ($\bar{K}$ über alg Abschl von K) gilt $\psi(F)=F$.

Bew: 1→2 Sei F über K erzeugt von S ($F=K[S]$) dann F Zerfk. der Menge der Minimalp. $\in K[x]$ der El von S.

2→3 F Zerf. k. von $\mathcal{F} \subseteq K[x]$. Sei S die Menge aller Nullstellen aller $f \in \mathcal{F}$ in F, $F=K[S]$

Sei $a \in F$ dann $\exists s_1 \dots s_n \in S$ $\exists g \in K[x_1,\dots,x_n]$: $a = g(s_1,\dots,s_n)$

$\psi(a) = g(\psi(s_1),\dots,\psi(s_n)) = g(t_1,\dots,t_n)$ mit $t_1 \dots t_n \in S$ also $\psi(a) \in K[S] = F$

Verwendet: ψ lässt El von K punktw. fest. d.h. ψ lässt Koeff von jedem $f \in \mathcal{F} \subseteq K[x]$ fix, daher bildet ψ Nullst. von $f \in \mathcal{F}$ wieder auf Nullstellen von f ab, $\psi(S) \subseteq S$, ψ injektiv $\Rightarrow$ ψ auf Nullstell. einer jeden $f \in \mathcal{F}$ bijektiv, $\forall t_1 \dots t_n \in S$ $\exists s_1 \dots s_n \in S$: $\psi(s_i) = t_i$

Also $\forall a \in F \quad a = g(s_1, \dots s_n) \quad g \in K[x_1 \dots x_n], s_i \in S$

$\exists t_1 \dots t_n \in S$ mit $\varphi(t_i) = s_i$ also für $b = g(t_1 \dots t_n)$: $\varphi(b) = a$. $\varphi: F \to F$ surj.

3 → 1: f irred $\in K[x]$, $K \subseteq F \subseteq \overline{K}$ f hat Nullstelle $a \in F$

Seien $a = a_1, \dots, a_n$ alle Nullstellen von f in $\overline{K}$, dann

$\exists$ Isom $\psi: K[a] \to K[a_i]$ (für bel. i) mit $\psi(a) = a_i$

$\psi(k) = k$ für $k \in K$. $\overline{K}$ ist alg Abschluss von $K[a]$ und von $K[a_i]$, ψ lässt sich auf Alg. Abschluss fortsetzen zu

$\overline{\psi}: \overline{K} \to \overline{K}$ Iso mit $\overline{\psi}|_{K[a]} = \psi$ insb. mit $\overline{\psi}(a) = a_i$

$\overline{\psi}|_F = \overline{\psi}: F \to \overline{K}$ K-Monom. Nach Vor $\overline{\psi}(F) = F$ also

$a_i = \psi(a) = \overline{\psi}(a) \in F$. Jede Nullstelle von f in $\overline{K}$ schon in F,

also zerfällt f über F.

Vor: F, K endl. Körper mit $K \subseteq F$ dann $F:K$ normal (weil F Zerfk von $x^{|F|} - x$ über K).

Def: eine alg Körpererw. $F:K$, die normal und separabel ist heißt Galois-Erweiterung.

Einheitswurzel, Kreisteilungskörper

Def: K Körper $w \in K$ heißt n-te Einheitswurzel wenn $w^n = 1$ und w heißt primitive n-te Einheitswurzel, wenn die Ordnung von w in $(K \setminus \{0\}, \cdot)$ gleich n ist. d.h. $w^n = 1$ $w^k \neq 1$ für $0 < k < n$

Bem: n-te Einheitswurzeln gibt es immer, da 1 ein n-te Einheitswurzel für jedes n. Primitive n-te Einheitswurzeln gibt es nicht immer z.B. in $\mathbb{Q}$ nur $1, -1$, keine Primitive 3. Einheitswurzel. Aber in Zerf.kö von $x^n - 1$ über $\mathbb{Q}$ gibt es primitive n-te Einheitswurzeln $e^{\frac{2\pi i}{n}}$. Nicht über jedem Körper kann man durch adjunktion von Nullstellen $x^n - 1$ n versch. n-te Einheitsw. bekommen z.B. K endl. Körper mit $\chi(K) = p$, $|K| = p^m$ $|(K \setminus \{0\}, \cdot)| = p^m - 1$

Jedes El in $(K\setminus\{0\},\cdot)$ hat als Ordnung einen Teiler von p^m-1 z.B Ord p m. möpl.

Ü: K Körper $n\in\mathbb{N}$ $n>0$ die n-te EHW in K bilden endl. zykl. Gruppe, deren Ord ein Teiler von n ist.

Lem: K Körper, $n\in\mathbb{N}$ Wenn $\chi(K)\nmid n$ ($\chi(K)=0$ oder $\chi(K)=p\nmid n$)
dann hat x^n-1 in seinem Zerfk-Kö über K n versch. Nullstellen;
wenn $\chi(K)=p\mid n$, $n=p^m k$ $p\nmid k$ dann $x^n-1=(x^k-1)^{p^m}$
und x^n-1 hat in seinem Zerfk-Kö K versch Nullst (die Nullst von x^k-1),
jede von Vielf. p^m.

Bew: $\chi(K)\nmid n$ $(x^n-1)'=nx^{n-1}$ ggT $(x^n-1, nx^{n-1})=1$ x^n-1 hat in Zerf-Kö-Körper mehrf. Nullstellen $\to$ n verschiedene Nst.
$\chi(K)=p$ $n=p^m k$ Frobenius: $(x^{p^m k}-1)=(x^k-1)^{p^m}$
Rechte 1 anwenden auf x^k-1.

Def: ω primitive n-te Einheitswurzel in K, dann sei
$\varphi_n(x):=\prod_{\substack{1\le k\le n\\ ggT(k,n)=1}}(x-\omega^k)=\prod_{\omega \text{ primitive n-te EW in } K}(x-\omega)$ das n-te Kreisteilungspolynom $\in K[x]$
Offenbar $\deg(\varphi_n)=\varphi(n)=|\{k\mid 1\le k\le n, ggT(k,n)=1\}|$

Satz: 1) Das n-te Kreisteilungspolynom $\varphi_n=\prod_{\substack{1\le k\le n\\ ggT(k,n)=1}}(x-\omega^k)$ [ω primitive n-te EW in K]
ist in $R[x]$, R Primring von K ($\frac{\varphi(n)}{d}$ Stück (oder von 1K erz. Ring).
2) $\varphi_n\in\mathbb{F}_q[x]\supseteq\mathbb{Z}_p[x]$ zerfällt in $\frac{\varphi(n)}{d}$ irred Faktoren vom Grad d
$d\in\mathbb{N}$ minimal sod $n\mid q^d-1$

Bew: Ad 1) Ind v. n: $\varphi_1=x-1$ ✓ $x^n-1=\prod_{d\mid n}\varphi_d(x)=\varphi_n(x)\cdot\prod_{\substack{d\mid n\\ d<n}}\varphi_d(x)$
Nach I.V. $g(x)=\prod_{\substack{d\mid n\\ d<n}}\varphi_d(x)\in R[x]$. Wegen Eind von Quotient und Rest
bei Polynomdiv.: $\varphi_n(x)\in R[x]$ ($\chi(K)=p$ $R=\mathbb{Z}_p$ Polynom d. in $\mathbb{Z}_p[x]$,
$\chi(K)=0$, $R=\mathbb{Z}$, Division durch normiert Poly. $\in\mathbb{Z}[x]$ und $g(x)$ normiert).
~~x^n-1~~, $g(x)$ normiert in $R[x]$, Div mit Rest in $R[x]$ $x^n-1=q(x)g(x)+r(x)$
$\deg r<\deg g$ in $K[x]$ liefert Vg. Eind. $g=\varphi_n$, $r=0$.

Ad 2) primitive n-te EW in Körper F der $\mathbb{F}_q$ enthält $\Rightarrow F = \mathbb{F}_{q^d}$ und $n \mid q^d - 1$. Für minimales d mit $n \mid q^d - 1$: kleinster Körper erw. von $\mathbb{F}_q$ der ein primitive n-te EW enthält.

Dh. wenn man eine Nullst. w eines irred. Faktors von $\Phi_n \in \mathbb{F}_q[x]$ adjungiert, dann $[\mathbb{F}_q[w] : \mathbb{F}_q] = d$ (d minimal so $n \mid q^d - 1$), daher auch Grad dieses irred. Faktors $= d$.

Def: K Körper, der Zerfällungskörper von $x^n - 1$ ü. K heißt n-ter Kreisteilungskörper über K.