FFC 9.6.08

$F:K$ separable Erw. und algebraische endl.-dim Erw, $[F:K]=n$

Norm: $N = N_K^F : F \to K$, Spur $T = T_K^F : F \to K$

$N(u) = \sigma_1(u) \cdot \sigma_2(u) \cdot \ldots \cdot \sigma_n(u)$, $T(u) = \sigma_1(u) + \sigma_2(u) + \ldots + \sigma_n(u)$

wobei $\sigma_1 \ldots \sigma_n$ alle versch. K-einbettungen von F in $\overline{K}$

($\overline{K}$ alg. Abschluss von K, der F enthält) durchläuft.

Statt $\overline{K}$ kann man in Def und N, den normalen Abschluss der Erw

$F:K$ verwenden; N ist der eind. bestimmte Körper mit ~~$\overline{K} \supseteq \overline{F}$~~?

$\overline{K} \supseteq N \supseteq F \supseteq K$ sodass $N:K$ normal; erhält N indem man Zerfkö

über F alle Polyn $\in K[x]$, die ein Nullst in F haben bildet.

Ohne Beweis: $[F:K] = |\{\sigma : F \to N \mid \sigma\ K\text{-Monom.}\}|$ $(= |\sigma : F \to \overline{K} \mid \sigma\ K\text{-Monom.}\}|$

weil K-Monom Nullstellen eines jeden Polyn $f \in K[x]$ permutiert, also $\sigma(F) \subseteq N$)

Es gilt i) $\forall u \in F$ $N_K^F(u)$, $T_K^F(u) \in K$

ii) $N_K^F(uv) = N_K^F(u) \cdot N_K^F(v)$

iii) $\left.\begin{array}{l} T_K^F(u+v) = T_K^F(u) + T_K^F(v) \\ T_K^F(ku) = k \cdot T_K^F(u) \end{array}\right\} \begin{array}{l} T: F \to K \\ K\text{-linear} \end{array}$

iv) für $u \in F$ sei $a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$ das Minimalpoly

von u über K

$T_K^F(u) = -[F:K(u)]\, a_{n-1}$

$N_K^F(u) = \left((-1)^n a_0\right)^{[F:K(u)]}$

v) $F \supseteq E \supseteq K$ dann $N_K^E \circ N_E^F = N_K^F$, $T_K^E \circ T_E^F = T_K^F$

Im Spezialfall $F:K$ endl.-dim Galois

ist $N = F$ und $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Aut}_K F$

vi) für $k \in K$ $N_K^F(k) = k^{[F:K]}$; $T_K^F(k) = [F:K] \cdot k$

Artin-Lemma: F Körper $\varphi_1,\dots,\varphi_n : (G,\cdot) \to (F^*,\cdot)$ versch Gruppenhom,
dann sind $\varphi_1,\dots,\varphi_n$ F-l.u. d.h. wenn für $a_1,\dots,a_n \in F$ gilt
$a_1\varphi_1+\dots+a_n\varphi_n=0$ (die Funktion konstant 0), dann folgt
$a_1=a_2=\dots=0$ (d.h. im F-VR F^G aller Funktionen $G\to F$ mit
elementweisen Operationen)

Bew Ind $\ddot{u}$ n: $n=1$ $(\varphi(e_G)=1\neq 0)$

$n-1 \mapsto n$ $\quad a_1\varphi_1(x)+\dots+a_n\varphi_n(x)=0 \qquad (*)$

oBdA alle $a_i \neq 0$ sonst folgt Beh

$\varphi_1,\dots,\varphi_n$ versch, sei $g\in G$ sd $\varphi_1(g)\neq\varphi_n(g)$

in $(*)$ gx für x einsetzen und mit $\varphi_n(g)^{-1}$ mult.

$a_1\varphi_n(g)^{-1}\varphi_1(g)\varphi_1(x)+\dots+a_n\underbrace{\varphi_n(g)^{-1}\varphi_n(x)}_{=1}=0 \qquad (**)$

Subtraktion $(*)-(**)$ liefert Gleichung

$b_1\varphi_1(x)+\dots+b_{n-1}\varphi_{n-1}(x)=0$

$b_1=a_1-a_1\underbrace{(\varphi_n(g)^{-1}\varphi_1(g))}_{\neq 1}\neq 0$ $\quad$ ↯ zur IV dass $\varphi_1\dots\varphi_{n-1}$ F-l.u.

Cor: versch Autom eines Körpers F sind F-l.u. ($\varphi\in \mathrm{Aut}\,F \to \varphi(0)=0$,
φ bijektiv also $\varphi|_{F^*}: F^*\to F^*$ Autom von $(F^*,\cdot)$)
insb sind die in Def von N,T vorkommende
$\sigma_1\dots\sigma_n$ F-l.u.

Cor: $T_K^F: F\to K$ surj K-lin Funktional. Im T K-Unterraum von
K also K oder (0), nicht (0), weil $T=\sigma_1+\sigma_2+\dots+\sigma_n$ nicht triv.
F-Linearkomb versch Autom von F ist.

Bem: $F:K$ endl Körper, dann sind die K-lin Funktionale
$L: F\to K$ genau die Abb $L_\beta: F\to K$ für $\beta\in F$ def durch
$L_\beta(x)=T_K^F(\beta x)$ (und für versch β,γ ist $L_\beta\neq L_\gamma$.

Bew: $L(x,y)=T_K^F(x\cdot y)$ K-bilinear $L_\beta(y)=L(\beta,y)=T(\beta\cdot y)$ K-linear
L_β $F\to K$ für bel $\beta\in F$. Für $\beta\neq\gamma$ $L_\beta(x)-L_\gamma(x)=T((\beta-\gamma)x)$
nicht 0-Funktion $x\mapsto(\beta-\gamma)x$ bijektiv $F\to F$ und $T: F\to K$ surj
Daher $|F|=|K|^{[F:K]}$ versch L_β. Das sind schon alle K-lin Funktionale $F\to K$

Def ein zyklische Körpererw $F:K$ ist ein Galois-Erw mit zykl Galois-Gr $Aut_K F$

Analog heißt <so und so> Körpererw wobei <so und so> ein Adjektiv ist, das einer Gruppe zukommt, dass Galois Erw mit <so und so> Galois Gr gemeint ist, z.B zyklische, Abelsche, auflösbare, ... Erw

Prop T: $F:K$ endl-dim zyklisch $Aut_K F = \langle\sigma\rangle$ dann gilt für $u \in F$

$T_K^F(u)=0 \Leftrightarrow v\in F\ u = v-\sigma(v)$

$\Leftarrow$ Was sogar für bel Körpererw $\sigma \in Aut_K F$

$T(v-\sigma(v)) = T(v) - T(\sigma(v)) = T(v) - T(v) = 0$

$\Rightarrow$ Weil $T: F \to K$ surj $\exists w \in F$ mit $T(w)=1$

für ein solches w und ein $u \in F$ mit $T(u)=0$

sei $v = uw + (u+\sigma(u))\sigma(w) + \dots + (u+\sigma(u)+\sigma^2(u)+\dots+\sigma^k(u))\sigma^k(w) + \dots + (u+\sigma(u)+\dots+\sigma^{n-2}(u))\sigma^{n-2}(w)$

dann (Ü) $v-\sigma(v) = uT(w)$ d.h für w mit $T(w)=1$ gilt $v-\sigma(v)=u$

Hilberts Satz 90: $F:K$ endl dim zykl Gruppe Erw $Aut_K F = \langle\sigma\rangle$

dann für $u \in F$: $N_K^F(u)=1 \Leftrightarrow \exists v \in F\ u = v\cdot(\sigma(v))^{-1}$

Bew: $\Leftarrow$ für bel Galois erw und $\sigma \in Aut_K F$ und $v \in F$ gilt $N(v\sigma(v)^{-1}) = \dots$

$\dots = N(v)\,N(\sigma(v))^{-1} = N(v)\,N(v)^{-1} = 1$

$\Rightarrow$ Sei $u \in F$ mit $N(u)=1$ (insb $u \neq 0$). Da $id, \sigma, \sigma^2, \dots, \sigma^{n-1}$

($n=[F:K]$) versch, sind sie F-lu also $\exists w \in F$ mit

$u\cdot w + (u\sigma(u))\sigma(w) + (u\sigma(u)\sigma^2(u))\sigma^2(w) + \dots + (u\sigma(u)\cdots\sigma^{n-1}(u))\sigma^{n-1}(w) \neq 0$

für jedes solche w gilt $u = w\sigma(w)^{-1}$ (Ü).

Einfacher Bew v. Prop. T im Spezfall $K=\mathbb{F}_q$ F_{q^n}. Sei $\alpha \in F$ $0=T(\alpha)$, sei β

(in Erweiterung von F) Nullst von $X^q - X - \alpha = 0$ zeige $\beta \in F$, denn

$\alpha = \beta^q - \beta = \sigma(\beta) - \beta$ $Aut_K F = \langle\sigma\rangle$. $0 = T(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{n-1}}$

$= (\beta^q-\beta) + (\beta^q-\beta)^q + (\beta^q-\beta)^{q^2} + \dots + (\beta^q-\beta)^{q^{n-1}} = (\beta^q-\beta) + \beta^{q^2} - \beta^q + \beta^{q^3} - \beta^{q^2} + \dots + \beta^{q^n} - \beta^{q^{n-1}} =$

$= \beta^{q^n} - \beta \Rightarrow \beta \in F_{q^n} = F$

#

Basen: $F:K$ endl-dim Galois Erw $[F:K]=n$

$\alpha_1,\dots,\alpha_n$ K-Basis von F genau dann wenn

$$\det\begin{pmatrix} T(\alpha_1\alpha_1) & \dots & T(\alpha_1\alpha_n) \\ T(\alpha_2\alpha_1) & & T(\alpha_2\alpha_n) \\ \vdots & & \vdots \\ T(\alpha_n\alpha_1) & \dots & T(\alpha_n\alpha_n)\end{pmatrix} = \det\left(T(\alpha_i\alpha_j)\right)_{\substack{1\le i\le n\\1\le j\le n}} \neq 0 \quad \text{wobei } T=T_K^F$$

Kor: $\alpha_1\dots\alpha_n$ w.o sind K-Basis K-Basis von F genau dann wenn

$$\det\begin{pmatrix}\sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n)\\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \dots & \sigma_n(\alpha_n)\end{pmatrix} = \det(\sigma_i(\alpha_j)) \neq 0 \quad \text{wobei } \{\sigma_1=id,\sigma_2,\dots\sigma_n\}=Aut_K F$$

ang $(T(\alpha_i\alpha_j))$ hat n K-lu Zeilen sei $c_1\alpha_1+\dots+c_n\alpha_n=0$ dann auch

$c_1\alpha_1\alpha_k+\dots+\alpha_n c_n\alpha_n=0$ für bel α_k

darauf T angew: $c_1T(\alpha_1\alpha_k)+c_2T(\alpha_2\alpha_k)+\dots+c_nT(\alpha_n\alpha_k)=0$

für alle $k=1..n$ d.h. die entspr K-lineare Komb der Zeile von $(T(\alpha_i\alpha_j))$ ist 0

es folgt alle $c_i=0$.

Umgek.: Wenn $\alpha_1..\alpha_n$ K-l.u ang K-lineare Komb der Zeile von

$(T(\alpha_i\alpha_j))$ mit Koeff $c_i\in K$ ist 0, d.h für $k=1..n$

$c_1T(\alpha_1\alpha_k)+c_2T(\alpha_2\alpha_k)+\dots+c_nT(\alpha_n\alpha_k)=0$

$T((c_1\alpha_1+c_2\alpha_2+\dots+c_n\alpha_n)\alpha_k)=0$ für $k=1..n$

d.h für $\beta=c_1\alpha_1+\dots+c_n\alpha_n$ ist $L_\beta=0$ weil $L_\beta(\alpha_i)=0$ für $\alpha_1..\alpha_n$ ke

K-Basis von F dann folgt $\beta=0$, weiters folgt alle $c_i=0$, da

$\alpha_1..\alpha_n$ K-l.u.

Kor folgt aus $(\sigma_i(\alpha_j))^T\cdot(\sigma_i(\alpha_j))^T=(T(\alpha_i\alpha_j))$ also

$\det(T(\alpha_i\alpha_j)) = (\det(\sigma_i(\alpha_j)))^2$

(i,j)-te Eintragung von $(\sigma_i(\alpha_j))^T(\sigma_i(\alpha_j))$ ist $(\sigma_1(\alpha_i)\,\sigma_2(\alpha_i)\dots\sigma_n(\alpha_i))\begin{pmatrix}\sigma_1(\alpha_j)\\ \sigma_2(\alpha_j)\\ \vdots\\ \sigma_n(\alpha_j)\end{pmatrix}$

$=T(\alpha_i\alpha_j)$

Satz: $F:K$ endl-dim zykl Körpererw $\mathrm{Aut}_K F = \langle \sigma \rangle$ $n = [F:K]$

Dann hat F eine K-Basis der Form , $\alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)$ für ein $\alpha \in F$

Bew: $\sigma^n = id$ und $id, \sigma, \sigma^2, \dots, \sigma^{n-1}$ versch K-Auto von F, also F-lu

Daher σ Nullst von $X^n - 1$ aber nicht Nullst ein Polyn $\in F[X]$ mit

dg $< n$. Daher $X^n - 1$ Minimalpoly von σ als K-lin Abb $F \to F$

Da Grad des Minimalpoly von σ gleich n (= Grad des charakteristischen Polyn)

ist das Minimalpoly gleichzeitig das char Polyn. und σ hat bzgl einer

bestimmten K-Basis von F die Form : Geführtenmatrix des Minipoly

d.h. $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 \cdots & 0 \\ & & & \ddots & \\ & & & & 1 \\ -a_0 & & & & -a_{n-1} \end{pmatrix}$ wobei $a_0, \dots, a_{n-1}$ die Koeff des Minimalpolyn spiell $X^n - 1$ D.h. wenn α das erste Basisel. dann hat die Basis die Form $\alpha, \sigma(\alpha), \sigma^2(\alpha), \dots \sigma^n(\alpha)$