

AES-Körper:

$$\mathbb{F}_{2^8} = \mathbb{F}_{256}$$

$\mathbb{F}_{p^n}$ Körper: endl.: field

→ Galois-Feld

$$\mathbb{F}_{p^n} = \text{GF}(p^n)$$

Weiter zu A22: Galoisgruppen

Sei $L|K \rightsquigarrow \text{Gal}(L|K) = \{ \sigma \text{ Auto von } L|K; \sigma|_K = \text{id}_K \}$
Galoisgruppe

Endl. $L|K$ galois : $\Leftrightarrow L|K$ normal und separabel

Satz 22.4: $L|K$ galois $\Rightarrow \# \text{Gal}(L|K) = [L:K]$

22.9. Def.: Galoiserw. $L|K$ zyklisch : $\Leftrightarrow \text{Gal}(L|K)$ zyklische Gruppe

" $L|K$ abelsch : $\Leftrightarrow$ " abelsche "

Vgl.: $L = K(x) | K$ heißt einfach $\neg \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) | \mathbb{Q}$ einfach,
 nicht zyklisch, da $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) | \mathbb{Q}) = C_2 \times C_2$
nicht zykl.

22.10. Bsp.: Sei $L|K$ der $\mathbb{Z}K$ eines sep. $f \in K[T]$,

$X := \{x_1, \dots, x_m\} \subseteq L$ die Menge der Wurzeln von f ,

$$\text{also } f = a \prod_{i=1}^m (T - x_i).$$

Dann: $G := \text{Gal}(L|K)$ operiert auf X :

$$G \times X \rightarrow X$$

$$(\sigma, x) \mapsto \sigma x := \sigma(x).$$

Somit: $G \rightarrow \text{Perm}(X) \cong S_m$ Gruppeniso

$\sigma \mapsto \underline{\sigma|_X}$ ist inj. Gruppenhom., vgl. Bsp. A4.19,
 inj., da $L = K(x_1, \dots, x_m)$.

22.11. Def.: Sei $L|K$ der $\mathbb{Z}K$ des sep. $f \in K[T]$, dann heißt $\text{Gal}(L|K)$
 die Galoisgruppe von f (bzw. G -Gr. der Gleichung $f=0$)

22.12. Bem.: $\text{Gal}(L|K)$ Galoisgr. von $f \Rightarrow [L:K] = \# \text{Gal}(L|K) \stackrel{22.4.}{\stackrel{\uparrow}{\leq}} n! \stackrel{22.10.}{\leq} n!$, $n = \deg f$.

22.13. Def.: Ein Kreisteilungskörper der Ordnung n über K | engl.: cyclotomic field
ist ein $\mathbb{Z}K$ von $T^n - 1 \in K[T]$. $\hookrightarrow$ zyklotomischer Körper

22.14. Bsp.: Gelte $\text{Char } K \nmid n$. Dann $(T^n - 1)' = nT^{n-1} \neq 0$ teilerfremd zu $T^n - 1$. $\Rightarrow$ Der KTK L (der Ordn. n über K) ist galois.

22.15. Def.: $E_n := \{x \in L; x \text{ Wurzel von } T^n - 1 \in K[T]\} \subseteq L$,
 $x \in E_n$ heißt n -te Einheitswurzel in L , kurz: n -te EW in L .

22.16. Bem.: * E_n ist zykl. Gruppe der Ordnung n :

$$\xi^n = 1, \quad \zeta^n = 1 \Rightarrow (\xi \cdot \zeta)^n = \xi^n \cdot \zeta^n = 1$$

* Betr. $G = \text{Gal}(L|K) \longrightarrow \text{Perm}(E_n)$

$$\begin{array}{c} \searrow \text{inj.} \quad \cup \\ \text{Aut}(E_n) \end{array}$$

$\sigma \in G \rightarrow \sigma|_{E_n}$ ist Auto der Gruppe E_n .

* Da $\text{Aut}(E_n) \cong (\mathbb{Z}/(n))^*$, wegen $\text{End}(E_n) \cong \mathbb{Z}/(n)$,
ist G isom. einem UG von $(\mathbb{Z}/(n))^*$, d.h. insb. ist G abelsch.
somit $L|K$ abelsche Galois erw.

* Für $K = \mathbb{Q}$ hat man "Gleichheit" (ohne Bew.),

$$\text{d.h. } \text{Gal}(\mathbb{Q}(\xi)|\mathbb{Q}) \cong (\mathbb{Z}/(n))^*,$$

$$\xi = e^{2\pi i/n} \in \mathbb{C}$$

$$\text{also } [\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n),$$

= ist KTK $\mathbb{Q}$ der Ordnung n

wo ξ erz. El. von $E_n|\mathbb{Q}$, etwa $\xi = e^{2\pi i/n}$.

22.17. Def.: Die erzeugenden El. von E_n heißen primitive n -te EWrn.

Das Mipo von $\xi \in E_n$ über K , $\text{Char } K \nmid n$, heißt

n -te Kreisteilungspolynom.

(engl. cyclotomic polynomial).

Bsp.: $K = \mathbb{Q}$

* $n=5$: $T^5 - 1 = (T-1) \cdot \underbrace{(T^4 + T^3 + T^2 + T + 1)}_{\text{irred. in } \mathbb{Q}}$ ← 5-te KTpoly

$= (T-\zeta)(T-\zeta^2)(T-\zeta^3)(T-\zeta^4)$

$\zeta := e^{2\pi i/5}$

→ primitive EW sind $\zeta, \zeta^2, \zeta^3, \zeta^4$

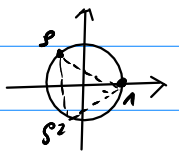
→ KTK: $\mathbb{Q}(\zeta) = \mathbb{Q}(e^{2\pi i/5})$

→ $E_5 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4\}$

* $n=3$: $T^3 - 1 = (T-1)(T^2 + T + 1)$

→ $(T-\zeta)(T-\zeta^2)$, $\zeta := e^{2\pi i/3} = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$
3-te KTpoly

→ $E_3 = \{1, \zeta, \zeta^2\}$



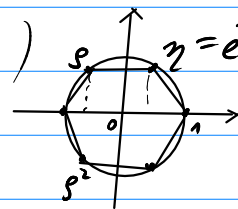
* $n=4$: $T^4 - 1 = (T-1)(T+1)(T-i)(T+i)$, $i := e^{2\pi i/4}$

→ $T^2 + 1$
4-te KTpoly

* $n=6$: $T^6 - 1 = (T-1)(T+1) \cdot \underbrace{(T^2 - T + 1)}_{\text{6-te KTpoly}} \cdot (\dots)$

$\mathbb{Q}(\eta)$

6-te KTpoly



$\eta = e^{2\pi i/6} = \frac{1}{2} + \frac{i}{2}\sqrt{3}$

ist Wurzel von $T^2 - T + 1$

22.18 Bsp.: Sei $p \in \mathbb{N}$ prim, $K = \mathbb{F}_{p^m}$, $L|K$ die Erw. von K vom Grad n , ist galsic.

Sei σ der Frobeniusautom. von L , d.h. $\sigma x = x^p$.

Sei $\tau = \sigma^m \in \text{Gal}(L|K)$: $\tau(x) = x^{p^m} = x$ für alle $x \in \mathbb{F}_{p^m} = K$
↑
 $x^p = x$ für $x \in K$

$\Rightarrow \tau^n(x) = x^{p^{mn}} = x$ für alle $x \in L \cong \mathbb{F}_{p^{mn}} \cong K^n$,

sei $q := p^m$. Für $1 \leq i < n$:

$\tau^i(x) = x^{q^i} \neq x$ für $x \in L$

(Sonst hätte $T^{q^i} - T$ ja $\#L = q^n$ versch. Wurzeln)

$\Rightarrow \tau \in \text{Gal}(L|K)$ hat die Ordnung n .

$\Rightarrow \text{Gal}(L|K) = \langle \tau \rangle = \langle \sigma^m \rangle$ ist zyklisch.

Jede Galoisgr. eines $L|\mathbb{F}_p$ ist zyklisch!

A23: Hauptsatz der Galoistheorie

HS der Galoistheorie

23.1. Einleitung: Körpererw. $\leftrightarrow$ Galoisgruppen

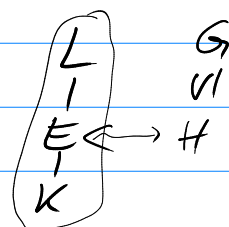


23.2. Def.: Sei L/K Galois'erw., Galoisgruppe sei G , sei $H \leq G$ eine UG.

Dann: $E := \text{Fix}(H) := \{x \in L; \forall \sigma \in H: \sigma x = x\} \subseteq L$

heißt Fixkörper von H .

23.3. Bem.: E ist Zwischenkörper von L/K , $K \subseteq E \subseteq L$.



23.4. Satz: Sei G endl. UG der Autogr. eines Körpers L ,
 $K := \text{Fix}(G)$. Dann: L/K endl. Galois'erw., $\text{Gal}(L/K) = G$.

Bew.: * Sei $m := \#G$, sei $x \in L$.

Sei $x = x_1, x_2, \dots, x_m$ Aufzählung
 von $\{zx; z \in G\}$, dabei $m \leq n$.

* Setze $f(T) := \prod_{i=1}^m (T - x_i)$, $f \in K[T]$, denn:

$$\begin{aligned} \text{Für } \sigma \in G: \{ \sigma x_1, \sigma x_2, \dots, \sigma x_m \} &= \{ x_1, \dots, x_m \}, & (\sigma x_i = (\sigma z)x_1) \\ \text{also } f^\sigma &= \prod_{i=1}^m (T - \sigma x_i) \stackrel{(\sigma \text{ anwenden!})}{=} \prod_{i=1}^m (T - x_i) = f. & \Rightarrow \text{Also } f \in K[T]. \end{aligned}$$

* Resultat: $[K(x):K] \leq m$ für alle $x \in L$. Also: Erw. L/K endlich!

* Sei $x \in L$ mit $[K(x):K]$ maximal.

Dann: $L = K(x)$.

Sonst: Sei $y \in L \setminus K(x) \Rightarrow K(x) \subsetneq K(x, y) = K(z)$

für ein $z \in L$ nach dem S.v. primitiven El. A20.16.

(denn L/K ist sep.), & zur Max. von $x \in L$.

* Somit: $[L:K] \leq m$. Da $G \leq \text{Gal}(L/K)$:

$$m = \#G \leq \# \text{Gal}(L/K) = [L:K] \leq m \Rightarrow [L:K] = m$$

↑

↑

und $\text{Gal}(L/K) = G$. $\square$