$q = p^m,\ K = GF(q) \subseteq L = GF(q^n),\ n = [E:F]$

$Q_i = X^{q^i} - X \in \mathbb{F}[X]$

$\Pi : L \to L$ mit $a \mapsto a^q$

$\Pi^i(a) = a^{q^i}$

$L_i = \{a \in \mathbb{F} : \Pi^i(a) = a\}$

$K = L_1 \subseteq L_i \subseteq L = L_n$

$G = \langle \Pi \rangle = \{\mathrm{id} = \Pi^0, \Pi, \Pi^2, ..., \Pi^{n-1}\}$ zyklische Gruppe der Ordnung

8.15. a) $\Pi \in \mathrm{Aut}_K\, 2$

b) $A^\Pi = A,\ A \in L[X] \quad \Rightarrow \quad A \in K[X]$

Die Untergruppen U von G haben die Form $U = \langle \Pi^i \rangle$, wobei i Teiler von u ist.

$n = i \cdot k$

$|U| = k$

Wir schreiben: $U = U_k$

$\mathrm{Fix}\, U = \{a \in L \,|\, \eta(a) = a \ \ \forall \eta \in U\} = L_i$

8.16. Ist $U = U_k$ Untergruppe der Ordnung von G, so ist $\mathrm{Fix}\, U = L_{\frac{n}{k}}$

$U_i \leq U_j \quad \Leftrightarrow \quad \mathrm{Fix}\, U_j \subseteq \mathrm{Fix}\, U_i$ **Galoiskorrespondenz**

Bezeichnungen:

Für $v \in L$

$B_v = \{\eta(v) \,|\, \eta \in G\} \subseteq L$ **Klasse konjugierter Elemente (Bahn)**

$= \{v^{q^i} \,|\, i \in \mathbb{N}_0\}$

$\mathbb{B} = \{B_v \,|\, v \in L\}$ **Menge aller Klassen** k.E

$M_B = \prod_{w \in B} (X - w) \in L[X]$

Zum Beispiel: $v \in K \quad B_v = \{v\},\ M_{B_v} = X - v$

8.17. a) $B_v = B_w \quad \forall w \in B_v$

b) $L = \bigcup_{B \in \mathbb{B}} B$ disjunkte Vereinigung

c) $|B| = \mathrm{grad}\, M_B$ Teiler von n

Beweis: a) $w=\eta_1(v),\ \eta_1\in G$

$\eta(w)=\eta(\eta_1(v))=(\eta\eta_1)(v)\in B_v$

$\eta_1^{-1}(w)=\eta_1^{-1}(\eta_1(v))=v$

$\Rightarrow\ v\in B_w\subseteq B_v$

genauso $B_v\subseteq B_w$ $\Rightarrow\ B_v=B_w$

b) $v\in B_v$

$\Rightarrow L=\bigcup B_v$

Sei $v\in B\cap\mathcal{C},\ B,\mathcal{C}\in\mathbb{B}$

a) $\Rightarrow B=B_v=\mathcal{C}$

d.h. $B_1\mathcal{C}\neq\varnothing\ \Rightarrow\ B=\mathcal{C}$

c) $U=\{\eta\in G\,|\,\eta(v)=v\},\ B=B_v$

Untergruppe von G

$w=\eta_1(v)\in B_v$

Für $y\in G$: $\eta(v)=w\ \Leftrightarrow\ \eta(v)=\eta_1(v)$

$\Leftrightarrow\eta^{-1}(\eta_1(v))=v\ \Leftrightarrow\ \eta^{-1}\eta_1\in U\ \Leftrightarrow\ \eta_1^{-1}\eta\in U$

$\Leftrightarrow\eta\in\eta_1 U$

$\Rightarrow|B|=|G:U|$ Index

8.18. Satz

Sei $B\in\mathbb{B}$

Für jedes $v\in B$ mit $M_B=M_v$ das Minimalpolynom

$\mathbb{F}=\mathbb{Z}_2\qquad\mathbb{E}=GF(8)\ \ v\in\mathbb{E}$

$M_v=(X-v)(X-v^2)(X-v^4)$

Beweis: $M:=M_B\quad M(v)=0$

z.z. 1) $M\in K[X]$ 2) M irreduzibel in $K[X]$

1) $M^{\Pi}=\prod_{w\in B}(X-w)^{\Pi}$ 8.13. a)

$=\prod_{v\in B}(X-\Pi(w))=M$ 8.13. d) $\Rightarrow M\in K[X]$

$w=\eta(v)$

Jedes $\eta_1\in G$ hat die Form: $\eta_1=\Pi\eta\quad(\eta=\Pi^{-1}\eta_1)$

Mit η durchläuft auch $\eta_1=\Pi\eta$ ganz G

$B=\{\eta(v)\,|\,\eta\in G\}=\{(\Pi\cdot\eta)(v)\,|\,\eta\in G\}=\{\Pi(w)\,|\,w\in B\}$

2) M ist irreduzibe in $K[X]$

$M = AB$ in $K[X]$

$0 = M(v) = A(v)B(v), \quad \text{Œ } A(v) = 0$

8.13. $0 = A(v) \overset{8.13\,c)}{\Rightarrow} A^{\eta}(\eta(v)) = 0$

$A^{\eta} = A \Rightarrow A(\eta w) = 0$

$X - \eta(v)$ teilt A

$\Rightarrow M_B$ teilt $A \Rightarrow A = M$

$Q_n = \prod_{X \in L}(X - v) = X^{q^n} - X \qquad A = \{v \in L \mid Q_n(v) = 0\}$

8.19. $\overset{8.17\,c)}{\Rightarrow} \underbrace{Q_n = \prod_{B \in \mathbb{B}} M_B}_{\text{Primfaktorzerlegung von } Q \text{ in } K[X]}$ ist das Produkt aller Minimalpolynome

8.20. Sei $M \in K[X]$ irreduzibel und normiert, $i = \operatorname{grad} M$

i) i teilt n

$\Leftrightarrow$ ii) $M = M_B$ für ein $B \in \mathbb{B}$

8.21. $\Rightarrow Q_n$ it das Produkt aller irreduziblen normierten Polynome$\in K[X]$, deren Grad Teiler von n ist

Beweis (8.20.):

i) $\Rightarrow$ ii) L_i Teiler von L L_i Nullstellenmenge von Q_i

8.9. $\Rightarrow M$ teilt Q_i $M(v) = 0$ für ein $v \in L_i \Rightarrow$ ii)

ii) $\Rightarrow$ i) Dies ist 8.17. c)

Pimitive Elemente z von L ($L^* = \langle z \rangle$) $\eta(z^i) = (\eta(z))^i \Rightarrow L^* = \langle \eta(z) \rangle$

8.22. z primitiv, $\eta \in \operatorname{Aut} L \Rightarrow \eta(z)$ ist primitiv

$N \in K[X]$ heißt **primitiv**,

wenn es ein Minimalpolynom eines primitiven Elements z ist.

Dann ist $K(z) = L$ und L isomorph zu K_N

Sei $B = B_z = \{\eta(z) \mid \eta \in G\}$

$\Rightarrow \quad N = \prod_{\eta \in G}(X - \eta(z)) = M_B$

$\eta(z^i) = (\eta(z))^i \quad \Rightarrow \quad L^* = \langle \eta(z) \rangle$

Beispiel: $K = \mathbb{Z}_2$

$N = 1 + X + X^2 + X^3 + X^4 \in K[X]$

$X \in L = K_N$ Körper mit $2^4 = 16$ Elementen

N ist Minimalpolynom von X

X istnicht primitiv

$X, X^2, X^3, \rho(X^4) = 1 + X + X^2 + X^3$

$\rho(X^5) = 1$

Definition: Das Polynom $P_N = \prod_{\substack{z \in L \\ z \text{ primitiv}}} (X - z)$ heißt ***n*-tes Kreisteilungspolynom**

P_n teilt Q_n

$B_{P_N} = \{B \in \mathbb{B} \mid B = B_z\}$

8.23. Satz

a) Die primitiven Polynome $N \in K[X]$ haben die Form $N = M_B$ mit $B \in \mathbb{B}_{\text{prim}}$

b) $P_n = \prod_{B \in \mathbb{B}_{\text{prim}}} M_B \in K[X]$

c) Sei z primitiv $\quad P_n = \prod_{\substack{1 \le i \le n \\ \text{ggT}(i,n)=1}} (X - z^i)$

8.24. $G = \text{Aut}_K L \ (= \text{Galoisgruppe}: \text{Gal}(L|K))$

Beweis: $n \in \text{Aut}_K L$, z primitiv $\Rightarrow \eta(z)$ primitiv

$M = M_z \in K[X]$

$M(z) = 0 \Rightarrow M(\eta(z)) = 0$

$B_z = \{\Pi^i(z) : 0 \le i \le n-1\}$ ist die Nullstellenmenge von $M = M_{B_z}$

$\Rightarrow \exists\ 1 \le k \le n$ mit $\eta(z) = \Pi^k(z)$

$\eta(z^i) = (\eta(z))^i = (\Pi^k(z))^i = \Pi^k(z^i)$

$\forall i: L = \{0\} \cup \{z^i \mid i = 0, \ldots, q^{n-1}\}$

$\Rightarrow \eta = \Pi^k$