$|K| = q = p^n$, $p = \operatorname{char} K$, $m = q - 1$

$K = \mathbb{F}_q = GF(q)$ **Galoisfeld** (Galois, 1820)

$K^* = \langle z \rangle = \{1, z, z^2, ..., z^{m-1}\}$, z primitives Element von K

$z^i \cdot z^j = z^{i+j} = z^{i +_m j}$ $\quad i +_m j = \rho_m(i+j)$

Zu jedem $a \in K^*$ existiert genau ein $i \in \mathbb{Z}_m = \{0,1,...,m-1\} \leq \mathbb{Z}$ mit $a = z^i$

Schreibweise: $\operatorname{ld}_z(a) := i$ **diskreter Logarithmus** von a zur Basis z

$a = 0 \quad \operatorname{ld}_z(a) := -\infty$

Verabredung: $a^{-\infty} := 0$, $i +_m (-\infty) := -\infty$

8.4. $\operatorname{ld}_z(ab) = \operatorname{ld}_z(a) +_m \operatorname{ld}_z(b)$

Beweis: $a = z', b = z^j, a \cdot b = z^{i +_m j}$

$z^i + z^j = z^k$ nicht klar

Œ $K = (\mathbb{Z}_P)_N$, $N \in \mathbb{Z}_P[X]$ irreduzibel, grad $N = n$

↑ Primkörper

Sei $v_0, v_1, ..., v_{n-1}$ eine Basis von $K_{\mathbb{Z}_P}$

$(\dim K_{\mathbb{Z}_P} = n \quad K = (\mathbb{Z}_P)_N = K_m[X])$

z.B. Basis $1, X, ..., X^{n-1}$

$a \in K$ hat die Darstellung

$$a = \sum_{i=0}^{n-1} a_i v_i \overset{!}{=} (a_0, a_1, ..., a_{n-1}) \quad a_i \in \mathbb{Z}_P$$

$$a + b = (a_0 +_P b_0, a_1 +_P b_1, ..., a_{n-1} +_P b_{n-1})$$

$$a \cdot b = \left(\sum_{i=0}^{n-1} a_i v_i\right)\left(\sum_{j=0}^{n-1} b_j v_j\right) = \sum_{i,j=0}^{n-1} (a_i \cdot_P b_j)(v_i \cdot_P v_j)$$

$$v_i \cdot v_j = \sum_{k=0}^{n-1} s_{ijk} \cdot v_k, \; s_{ijk} \in \mathbb{Z}_P$$

s_{ijk} : **Strukturkonstanten**

$$a \cdot b = \sum_{i,j,k=0}^{n-1} \left((a_i \cdot_P b_j) \cdot_P s_{ijk}\right) v_k = \left(\sum_{i,j} (a_i \cdot_P b_j) \cdot_P s_{ij0}, ..., \sum_{i,j} (a_i \cdot_P b_j) \cdot_P s_{ij(n-1)}\right)$$

Gute Basis ist eine Basis, so dass $s_{ijk} = 0$ möglichst oft.

Beispiel: Basis: $v_0 = 1,\ v_1 = X,\ v_2 = X^2, ..., v_{n-1} = X^{n-1},\ K = (\mathbb{Z}_P)_N$

$$a = \sum_{i=0}^{n-1} a_i v_i = A \text{ Polynom}$$

$$v_i v_j = X^i X^j = \rho_N\left(X^{i+j}\right)$$

Sei $i + j < n$: $v_i v_j = v_{i+j}$ $\quad s_{ijk} = \begin{cases} 0 & k \neq i+j \\ 1 & k = i+j \end{cases}$ falls

Sei $i + j = n$: $N = \underbrace{d_0 + d_1 X + ... + d_{n-1} X^{n-1}}_{D \subset K} + X^n,\ d \in \mathbb{Z}_P$

$d = (d_0, d_1, ..., d_{n-1})$ hat die Basis $v_0, ..., v_{n-1}$

$\rho_N\left(X^n\right) = -D$, d.h.: $v_1^n = -d$

Sei $i + j = n$: $v_i v_j = v_1^i v_1^j = v_1^n = -d$

$s_{ijk} = -d_k \quad k = 0, ..., n-1$

Sei $i + j = n + 1$

$$v_i \cdot v_j = \left(d_{n-1} d_0, \underbrace{d_{n-1} d_1 + d_0}_{s_{ijk}}, ..., d_{n-1}^2 + d_{n-1} \right)$$

Ein guter Spezialfall $p = 2$ $(a+b)^2 = a^2 + 2ab + b^2$

8.5. Satz

$(a+b)^P = a^P + b^P \quad a, b \in K$

Beweis: Zunächst für $a, b \in \mathbb{Z}$

$$(a+b)^P = a^P + b^P + \sum_{i=1}^{P-1} \rho_P\left(\binom{P}{i}\right) a^i b^{P-i} \in \mathbb{N} \qquad \binom{P}{i} = \frac{P(P-1)\cdots(P-i+1)}{i!}$$

$1 \le i \le P-1$ $\quad P$ teilt $\binom{P}{i} i!$, P teilt nicht $i!$

$$\Rightarrow P \text{ teilt } \binom{P}{i} \quad \rho_P\binom{P}{i} = 0$$

Zusatz: a) $a^q = a \quad \forall a \in K \quad q = P^n$

b) $a^P = a \quad \forall a \in \mathbb{Z}_P$

Beweis: $m = q - 1$ ist die Ordnung von K^*

$\Rightarrow a^m = 1 \quad \forall a \in K^* \quad aa^m = a,\ a^q = a$

$a \in \mathbb{Z}_P \quad a^{P-1} = 1 \quad a^P = aa^{P-1}$

8.6. Satz über die Normalbasis

Es existiert $v \in K$, so dass die Potenzen $v, v^P, v^{P^2}, ..., v^{P^{n-1}} \quad (q = P^n)$

Eine Basis von $K_{\mathbb{Z}_P}$ bilden. (Normalbasis)

$$v_0^P = v_1, v_1^P = v_2, ..., v_{n-2}^P = v_{n-1}, v_{n-1}^P = \left(v^{P^{n-1}}\right)^P = v^{P^n} \overset{a)}{=} v = v_0$$

$$a = (a_0, a_1, ..., a_{n-1}) \qquad = \sum_{i=0}^{n-1} a_i v_i$$

$$a^P = \qquad = \sum_{i=0}^{n-1} \underbrace{(a_i v_i)^P}_{a_i^P v_i^P}$$

zyklische Vertauschung

Allgemein: K endlicher Körper mit $q = P^n$ Elementen, $P = \operatorname{char} K$

$L \in E_{endl}(K), [L:K] = \dim L_K$

(z.B. $K = \mathbb{Z}_P \quad L = (\mathbb{Z}_P)_N \quad N \in \mathbb{Z}_P[X]$ irred.)

Für $i \in \mathbb{N}$ sei $\quad Q_i := X^{q^i} - X \in K[X] \quad (\subseteq L[X])$

$$L_i := \{a \in L \mid Q_i(a) = 0\}$$

8.7. Proposition

a) L_i ist Teilkörper von L

b) $|L_i| \le q^i$

c) Zerfällt Q_i in $L[X]$ in Linearfaktoren, so gilt $|L_i| = q^i$

d) $L_1 = K \subseteq L_i \subseteq L$

e) $L_n = L$, wenn $n = [L:K]$

Beweis: $\quad a \in L_i \Leftrightarrow a^q = a$

a) $\quad 1 \in K, P = \operatorname{char} K \quad \Rightarrow \overline{P} = 0$ in $K \quad \overline{q} = 0 \quad (q = P^n)$

$\overset{8.4.}{\Rightarrow} \quad (a+b)^{q^i} = a^{q^i} + b^{q^i} \qquad (a \cdot b)^{q^i} = a^{q^i} \cdot b^{q^i}$

$$\left(a^{-1}\right)^{q^i} = \left(a^{q^i}\right)^{-1}$$

$$(a+b)^{q^2} = \left((a+b)^q\right)^q = \left(a^q + b^q\right)^q = a^{q^2} + b^{q^2}$$

$\Rightarrow \quad a, b \in L_i \Rightarrow a+b, a \cdot b \in L_i, a^{-1} \in L_i$

L_i ist Teilkörper

c) Es genügt zu zeigen, dass Q_i in L nur einfache Nullstellen besitzt.

Kriterium z.z. $\qquad Q_i' = \underbrace{\overline{q}_i X^{q^i - 1}}_{=0} - 1$

$$Q_i'(a) \neq 0 \quad \forall a \in L$$

d) $a^q = q$, d.h. $K \subseteq L_1$ $\qquad Q_1 = X^q - X$

$|K| = q \quad K = L_1$

$a \in K$ heißt $a^q = q, \; a^{q^2} = a^q = a$

$a^{q^i} = a \quad a \in L_i$

$|L| = q^n \quad L^*$ hat die Ordnung $q^n - 1$

$a^{q^{n-1}} = 1 \,|\cdot a \quad \forall a \in L$

$a^{q^n} = a$

8.8. Satz

Zu jedem $n \in \mathbb{N}$ existiert ein Erweiterungskörper L von K mit $|L| = q^n$

$Q_n = X^{q^n} - X \in K[X]$

7.3. $\Rightarrow \exists L \in E_{\text{endl.}}(K)$ in dem das Polynom Q_n in Linearfaktoren zerfällt

c) $\Rightarrow L_n$ ist Körper mit q^n Elementen