K endlicher Körper $n = \left|K^*\right| = \left|K\right| - 1$

β primitives Element von K

$\xi_1 = 1 = \beta^0,\ \xi_2 = \beta = 0^1,\ \xi_3 = \beta^3, ...,\ \xi_n = \beta^{n-1}$

$\eta_i = \xi_i^{-1},\ i = 1, ..., n$

$\overline{n} = \underbrace{1 + ... + 1}_{n} \in K$

$n \neq 0$

$y \in K^n$

$\Phi_y = y_1 + y_2 X + ... + y_n X^{n-1} \in K_n[X]$

Erinnerung: 5.8. $\kappa\left(\prod y\right) = \frac{1}{n} \operatorname{val}_{\eta_1, ..., \eta_n}\left(\Phi_y\right)$

6.7. $y \in RS_{\xi_1, ..., \xi_n}(n, R) \quad \Leftrightarrow \quad \operatorname{grad} \Pi y < R$

$\Leftrightarrow\ \Phi_y(\eta_{R+1}) = ... = \Phi_y(\eta_n) = 0$

$\Leftrightarrow\ (X - \eta_{R+1})...(X - \eta_n)$ teilt Φ_y

$\Leftrightarrow$ Es existiert $A \in K_R[X]$ und $\Phi_y = AG$

Unter diesen Voraussetzungen

6.8. $\left(= RS_{\xi_1, ..., \xi_n}(n, R)\right)$ ist ein **zyklischer Code**, d.h.

$(y_1, y_2, ..., y_n) \in C$

$\Rightarrow (y_n, y_1, ..., y_{n-1}) \in C$

$a = (a_0, a_1, ..., a_{k-1})$ Information, $A = a_0 + a_1 X + ... + a_{k-1} X^{k-1} \in K_k[X]$

Mögliche Codierung:

I) $y = \operatorname{val}_{\xi_1, ..., \xi_n}(A),\ y_i = A(\xi_i)$

II) $A \mapsto \kappa(A, G)$

III) $X^{n-k} A = a_0 X^{n-k} + a_1 X^{n-k+1} + ... + a_{k-1} X^{n-1}$

Teile $X^{n-k} A$ durch G

$X^{n-k} A = FG + R,\ \operatorname{grad} R < n - k,\ \operatorname{grad} F < k$

$X^{n-k} A - R = FG$

Code: $A \mapsto y = \kappa\left(X^{n-k} A - R\right) \in RS$

Zu III) Systematische Codierung, d.h. die Information a belegt die letzte $n-k$ Stellen von y

$K=\mathbb{Z}_5,\ n=4,\ \overline{n}=4=-1,\ k=2$

$n-2=2t,\ t=1$

$\beta=3$

$\xi_1=1,\ \xi_2=3,\ \xi_3=4,\ \xi_4=2$ (Potenzen von 3)

$\eta_1=1,\ \eta_2=2,\ \eta_3=4,\ \eta_4=3$

$a=(1,3),\ A=1+3X$

$y=(4,0,3,2)$

I) $\downarrow$ (Übertragung) mit $\tilde{f}=\{2\}$

$\tilde{y}=(4,2,3,2)$

1) Berechnen

$$B=\Pi\tilde{y}=b_1+b_2X+b_3X^2+b_4X^3$$
$$=b_1+b_2X+e_3X^2+e_4X^3$$

$E=B-A$

$\operatorname{grad}A<R$

$\overset{6.6.}{\Rightarrow}$ die höchstens $n-k=2t$ Koeffizienten von B sind die von E

Bilde $\Phi_{\tilde{y}}=4+2X+3X^2+2X^3$

$$b_i=\frac{1}{\overline{n}}\Phi(\eta_i)=-\Phi(\eta_i)$$

$$e_3=-\left(4+2\underset{=3}{\cdot}4+3\underset{=3}{\cdot}4^2+2\underset{=3}{\cdot}4^3\right)=-3=2$$

$$e_4=-\left(4+2\underset{=1}{\cdot}3+3\underset{=2}{\cdot}3^2+2\underset{=4}{\cdot}3^3\right)=-1=4$$

$$N=\prod_{i=1}^{n}(X-\xi_i)=X^n-1=X^4-1$$

Erweiterter euklidischer Algorithmus

$$(X^4-1):(4X^3+2X^2+\ldots)=4X+3$$
$$-X^4+3X^3+\ldots.$$
$$2X^3+\ldots$$
$$2X^3+\ldots$$
$$\text{Rest}=r,\ \operatorname{grad}r=2\quad\Rightarrow\quad r=0$$

$N=(4X+3)\cdot E$

$$QN = PE$$

$Q = 1,\ P = 4X + 3$ Fehlerstellenpolynom

$$P(3) = 0 \quad \Rightarrow \tilde{f} = \{2\}$$

$$\tilde{y}_2 - y_2 = E(\xi_2) = \frac{N'(\xi_2)Q(\xi_2)}{P'(\xi_2)}$$

$$= \frac{(4 \cdot 3^3) \cdot 1}{4} = 3^3 = 2$$

$$y_2 = \tilde{y}_2 - 2 = 2 - 2 = 0$$

$$A(1) = 4 \qquad a_0 + a_1 = 4 \qquad 2a_1 = 1$$

$$A(3) = 0 \qquad a_0 + 3a_1 = 0 \qquad a_1 = 3,\ a_0 = 1$$

II) $G = (X - \eta_3)(X - \eta_4)$

$$= (X - 4)(X - 3) = X^2 + 3X + 2$$

$$AG = (1 + 3X)(X^2 + 3X + 2) = 3X^3 + 4X + 2$$

$$y = (2,4,0,3)$$

$\downarrow$ (Übertragung)

$$\tilde{y} = (2,1,0,3)$$

$$\Phi_{\tilde{y}} = 2 + X + 3X^3$$

$$e_3 = -(2 + 4 + 3 \cdot 4^3) = -3 = 2$$

$$e_4 = -(2 + 3 + 3 \cdot 3^3) = -1 = 4$$

$$(X^4 - 1) : (4X^3 + 2X^2 + \ldots) = 4X + 3$$

$$Q = 1, P = 4X + 3$$

$$\tilde{y}_2 - y_2 = 2 \quad \Rightarrow \quad y_2 = 1 - 2 = 4$$

$$y = (2,4,0,3)$$

$$A = \frac{AG}{G}$$

$$(3X^3 + 4X + 2) : (X^2 + 3X + 2) = 3X + 1$$

$$3X^2 + 4X^2 + X$$

$$X^2 + 3X + 2$$

III) $X^2A = 3X^3 + X^2$

$\left(3X^2 + X^2\right) : \left(X^2 + 3X + 2\right) = 3X + 2$

$3X^2 + 4X^2 + X$

$2X^2 - X$

$2X^2 + X + 4$

$3X + 1 = R$

$X^2 - A - R = 3X^3 + X^2 - 3X - 1$

$y = (4,2,1,3)$

$\downarrow$

$\tilde{y} = (4,2,1,0)$

$\Phi_{\tilde{y}} = 4 + 2X + X^2$

$e_3 = -\Phi_{\tilde{y}}(4) = -\left(4 + 2 \cdot 4 + 4^2\right) = -3 = 2$

$e_4 = \ldots = -\left(4 + 2 \cdot 3 + 3^3\right) = -4 = 1$

$\left(X^4 - 1\right) : \left(X^3 + 2^2 + \ldots\right) = X + 3$

$X^4 + 2X^3$

$3X^3 + \ldots$

$3X^2 + \ldots$

$N = E(X + 3)$

$Q = 1,\ P(X + 3)$

$P(\xi_4) = 2 + 3 = 0$

$\tilde{y}_4 - y_4 = \frac{4 \cdot \xi_4^3}{1} = 4 \cdot 3 = 2$

$y_4 = 0 - 2 = 3$

7. Erweiterungskörper

K sei Teilkörper des Körpers L
L ist Erweiterungskörper von K

$\Rightarrow$ $K[X]$ ist Unterring von $L[X]$

Bemerkung: $\lambda \in K$, $a \in L$, $\lambda \cdot a$ das Produkt von λa in L

$$\left.\begin{array}{l}(\lambda\mu)a = \lambda(\mu a) \\ (\lambda+\mu)a = \lambda a + \mu a \\ 1a = a\end{array}\right\} \begin{array}{l}L \text{ kann als Vektorraum über den Körper } K \text{ aufgefasst werden.} \\ \text{Diesen Vektorraum bezeichnen wir als } L_K\end{array}$$

$[L:K] \overset{\text{def.}}{=} \dim L_K$ Grad von L über K
L heißt endliche Erweiterung von K, wenn $[L:K] < \infty$

7.1. Sei L endliche Erweiterung von K und Z Zwischenkörper, $K \subseteq Z \subseteq L$

$$\Rightarrow [L:K] = [Z:K] \cdot [L:Z] \text{ Gradformel}$$

Z_K Unterraum von L_K
$u_1, ..., u_m$ sei Basis von Z_K
$v_1, ..., v_n$ sei Basis von L_K
Behauptung: Die $n \cdot m$ Elemente u_i, v_j bilden eine Basis von L_K

$a \in L$

$$\left.\begin{array}{l}a = \sum_{i=1}^{n} \lambda_i v_i,\ \lambda_i \in Z \\ \lambda_i = \sum_{j=1}^{n} \mu_{ij} u_j,\ \mu_{ij} \in K\end{array}\right\} a = \sum_{i,j} \mu_{i,j} u_i v_j$$

Sei $0 = \sum_{i,j} \mu_{ij} (v_i u_j) \quad \Rightarrow \quad \mu_{ij} = 0$

$$\sum_{i=1}^{n} \lambda_i v_i,\ \lambda_i \in Z$$

$$\Rightarrow \lambda_i = 0 \Rightarrow \sum_{j=1}^{n} \mu_{ij} u_j = 0,\ \mu_{ij} \in K$$