

7. Übung Codierungstheorie

1. Aufgabe Idempotente

(5 Punkte)

Sei $R_n := \mathbb{F}_q[X]/(X^n - 1)$ und C_1 und C_2 Ideale in R_n mit Idempotenten e_1 und e_2 . Zeige folgende Aussagen:

- (i) Ist $C_1 \cap C_2 \neq 0$, so besitzt $C_1 \cap C_2$ die Idempotente $e_1 e_2$.
- (ii) Ist $q = 2^m$, so besitzt $C_1 + C_2$ die Idempotente $e_1 + e_2 + e_1 e_2$.

2. Aufgabe Spur-Codes

(5 Punkte)

Sei C ein Code der Länge n über $E := \mathbb{F}_{q^m}$ und $K := \mathbb{F}_q$. Zeige, dass $(C|_K)^\perp = \text{Tr}_{E/K}(C^\perp)$ ist.

3. Aufgabe Primitive Idempotente

(6 Punkte)

Sei $R_n = \mathbb{F}_q[X]/(X^n - 1)$ mit $(q, n) = 1$ und $X^n - 1 = f_1(X) \cdots f_r(X)$ die Faktorisierung von $X^n - 1$ in irreduzible Polynome. Zeige folgende Aussagen:

- (a) Die $M_i := R_n f_i$ sind maximale Ideale in R_n ,
- (b) Die $\tilde{M}_i := R_n \prod_{j=1, j \neq i}^n f_j = R_n \tilde{f}_i$ sind minimale Ideale in R_n ,
- (c) \tilde{M}_i ist orthogonal zu M_i ,
- (d) \tilde{M}_i ist isomorph zu einem Körper.