

Lösung 9

Aufgabe 35.

- (1) Die Aussage trifft nicht zu. Denn die Teilkörper von \mathbf{F}_{2^5} sind von der Form \mathbf{F}_{2^d} mit d einem Teiler von 5. Da 5 nur die Teiler 1 und 5 hat, hat \mathbf{F}_{32} nur die Teilkörper \mathbf{F}_2 und \mathbf{F}_{32} .
- (2) Die Aussage trifft nicht zu. Selbe Begründung wie bei (1).
- (3) Die Teilkörper von $\mathbf{F}_{5^{12}}$ sind von der Form \mathbf{F}_{5^d} mit d einem Teiler von 12, i.e. mit $d \in \{1, 2, 3, 4, 6, 12\}$. Also hat $\mathbf{F}_{5^{12}}$ gerade 6 Teilkörper.

Aufgabe 36.

- (1) Als Menge geschrieben besteht C aus den Zeilen der folgenden Matrix.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

In jeder Nichtnullzeile gibt es wenigstens 2 nichtverschwindende Einträge. Und es gibt eine Zeile mit 2 nichtverschwindenden Einträgen. Somit ist der Minimalabstand $d(C)$ gleich 2.

- (2) Bei linearen Codes berechnet sich die Informationsrate als Quotient der Dimension des Unterraumes C , geteilt durch die Dimension des Raumes, in welchem C Unterraum ist. Da M den Rang 3 hat, ist die Informationsrate hier $r(C) = 3/5 = 0.6$.
- (3) Als Menge geschrieben besteht C aus der Nullzeile und den nichtverschwindenden skalaren Vielfachen der Zeilen folgender Matrix.

$$\begin{pmatrix} 0 & 1 & \omega & 1+\omega \\ 1 & 0 & \omega+1 & \omega \\ \omega & 1+\omega & 0 & 1 \\ \omega+1 & \omega & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

In jeder Nichtnullzeile von C gibt es also wenigstens 3 nichtverschwindende Einträge. Und es gibt eine Zeile mit 3 nichtverschwindenden Einträgen. Somit ist der Minimalabstand $d(C)$ gleich 3.

- (4) Es ist $\mathbf{F}_4^2 \simeq C \subseteq \mathbf{F}_4^4$. Also ist die Informationsrate $r(C)$ gleich $2/4 = 0.5$.

Aufgabe 37.

- (1) Hierzu folgende Tabelle. In dieser erstellen wir zunächst die ersten beiden Spalten (Probe: F sollte bijektiv sein!). Mit deren Hilfe erstellen wir dann die restlichen Spalten. Beim Rechnen ist es nützlich, sich daran

zu erinnern, daß stets $F(\xi + \eta) = F(\xi) + F(\eta)$ ist.

ξ	$F(\xi)$	$F^2(\xi)$	$F^3(\xi)$	$F^4(\xi)$
0	0	0	0	0
1	1	1	1	1
γ	γ^2	$\gamma + 1$	$\gamma^2 + 1$	γ
$\gamma + 1$	$\gamma^2 + 1$	γ	γ^2	$\gamma + 1$
γ^2	$\gamma + 1$	$\gamma^2 + 1$	γ	γ^2
$\gamma^2 + 1$	γ	γ^2	$\gamma + 1$	$\gamma^2 + 1$
$\gamma^2 + \gamma$	$\gamma^2 + \gamma + 1$	$\gamma^2 + \gamma$	$\gamma^2 + \gamma + 1$	$\gamma^2 + \gamma$
$\gamma^2 + \gamma + 1$	$\gamma^2 + \gamma$	$\gamma^2 + \gamma + 1$	$\gamma^2 + \gamma$	$\gamma^2 + \gamma + 1$
γ^3	$\gamma^3 + \gamma^2$	$\gamma^3 + \gamma^2 + \gamma + 1$	$\gamma^3 + \gamma$	γ^3
$\gamma^3 + 1$	$\gamma^3 + \gamma^2 + 1$	$\gamma^3 + \gamma^2 + \gamma$	$\gamma^3 + \gamma + 1$	$\gamma^3 + 1$
$\gamma^3 + \gamma$	γ^3	$\gamma^3 + \gamma^2$	$\gamma^3 + \gamma^2 + \gamma + 1$	$\gamma^3 + \gamma$
$\gamma^3 + \gamma + 1$	$\gamma^3 + 1$	$\gamma^3 + \gamma^2 + 1$	$\gamma^3 + \gamma^2 + \gamma$	$\gamma^3 + \gamma + 1$
$\gamma^3 + \gamma^2$	$\gamma^3 + \gamma^2 + \gamma + 1$	$\gamma^3 + \gamma$	γ^3	$\gamma^3 + \gamma^2$
$\gamma^3 + \gamma^2 + 1$	$\gamma^3 + \gamma^2 + \gamma$	$\gamma^3 + \gamma + 1$	$\gamma^3 + 1$	$\gamma^3 + \gamma^2 + 1$
$\gamma^3 + \gamma^2 + \gamma$	$\gamma^3 + \gamma + 1$	$\gamma^3 + 1$	$\gamma^3 + \gamma^2 + 1$	$\gamma^3 + \gamma^2 + \gamma$
$\gamma^3 + \gamma^2 + \gamma + 1$	$\gamma^3 + \gamma$	γ^3	$\gamma^3 + \gamma^2$	$\gamma^3 + \gamma^2 + \gamma + 1$

(2) Mit (1) werden

$$\begin{aligned}
 K_1 &= \{0, 1\} \\
 K_2 &= \{0, 1, \gamma^2 + \gamma, \gamma^2 + \gamma + 1\} \\
 K_3 &= \{0, 1\} \\
 K_4 &= \mathbf{F}_{16}
 \end{aligned}$$

In der Tat hat, für p prim, $n \geq 1$ und $d|n$, der Fixkörper von $(\text{Frob}_p)^d$ in \mathbf{F}_{p^n} gerade p^d Elemente. Dies bestätigt das Ergebnis von K_1 und K_4 , und es macht das Resultat für K_2 plausibel.

(3) Es ist K_2 aus (2) ein vierelementiger Teilkörper von \mathbf{F}_{16} . Es ist

$$\begin{array}{ccc}
 \mathbf{F}_4 & \xrightarrow[\sim]{\varphi} & K_2 \\
 1 & \longmapsto & 1 \\
 \alpha & \longmapsto & \gamma^2 + \gamma
 \end{array}$$

ein auf einer \mathbf{F}_2 -Basis definierter \mathbf{F}_2 -linearer Isomorphismus. Wir behaupten, daß ein Ringmorphismus (und damit insgesamt ein Körperisomorphismus) vorliegt.

Hierbei genügt es zu zeigen, daß $\varphi(\xi \cdot \eta) \stackrel{!}{=} \varphi(\xi) \cdot \varphi(\eta)$ für alle ξ und η aus einer Basis. Denn dies setzt sich dann wegen der schon bekannten Verträglichkeit von φ mit Linearkombinationen distributiv zum allgemeinen Fall fort.

Ist im vorliegenden Fall $\xi = 1$ oder $\eta = 1$, so ist dies unmittelbar einsichtig. Zu zeigen bleibt also, daß $\varphi(\alpha^2) \stackrel{!}{=} \varphi(\alpha)^2$. In der Tat ist auf der einen Seite

$$\varphi(\alpha^2) = \varphi(\alpha + 1) = \varphi(\alpha) + \varphi(1) = \gamma^2 + \gamma + 1,$$

und auf der anderen

$$\varphi(\alpha)^2 = (\gamma^2 + \gamma)^2 = \gamma^4 + \gamma^2 = \gamma^2 + \gamma + 1.$$

Aufgabe 38.

Wir wählen $\xi = \beta$. In folgender Tafel erstellen wir spaltenweise von links nach rechts.

$$\begin{array}{lll}
 \beta^0 = 1 & \beta^0 + 1 = 0 & = - \\
 \beta^1 = \beta & \beta^1 + 1 = \beta + 1 & = \beta^3 \\
 \beta^2 = \beta^2 & \beta^2 + 1 = \beta^2 + 1 & = \beta^6 \\
 \beta^3 = \beta + 1 & \beta^3 + 1 = \beta & = \beta^1 \\
 \beta^4 = \beta^2 + \beta & \beta^4 + 1 = \beta^2 + \beta + 1 & = \beta^5 \\
 \beta^5 = \beta^2 + \beta + 1 & \beta^5 + 1 = \beta^2 + \beta & = \beta^4 \\
 \beta^6 = \beta^2 + 1 & \beta^6 + 1 = \beta^2 & = \beta^2
 \end{array}$$

Entsprechend sind die Zechlogarithmen

k	$\ell(k)$
0	-
1	3
2	6
3	1
4	5
5	4
6	2

Zum Beispiel wird damit $\beta^3 + \beta^5 = \beta^3(\beta^2 + 1) = \beta^3 \cdot \beta^6 = \beta^9 = \beta^2$.

Direkt kann man etwa $\beta^3 + \beta^5 = \beta + 1 + \beta^2(\beta + 1) = \beta + 1 + (\beta + 1 + \beta^2) = \beta^2$ rechnen.