



Abgabe zu zweit vor der Vorlesung am Di., 03.06.14 um 10:15 Uhr im Raum E 20.

## Aufgabe 13 (Reed-Solomon-Codes)

Gegeben sei der Körper  $\mathbb{F}_8$  und ein primitives Element  $\alpha \in \mathbb{F}_8$  mit Minimalpolynom  $x^3 + x + 1$ . Betrachte im Folgenden den RS-Code  $\mathcal{C}$  mit  $n = 8, k = 3$  und Auswertungsvektor  $a = (0, 1, \alpha, \dots, \alpha^6)$  über  $\mathbb{F}_8$ .

- a) Welches Codewort  $c \in \mathcal{C}$  gehört zu dem Polynom  $f(x) = x^2 + (\alpha^2 + 1)x$ ?
- b) Gib eine Erzeugermatrix von  $\mathcal{C}$  an.
- c) Es wurde  $r = (\alpha, 1, \alpha^2 + 1, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha, 0)$  empfangen. Ist  $r$  ein Codewort?
- d) Nun wurde  $c = (\alpha + 1, \alpha^2 + 1, 1, \alpha^2 + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, 1, \alpha + 1)$  empfangen. Es gilt  $c \in \mathcal{C}$ . Finde ein Polynom  $g \in P_k$ , das zu  $c$  codiert wurde.

(0,5+1+2+1,5 = 5 P)

## Aufgabe 14 (Körpererweiterungen)

Wir suchen Körper  $\mathbb{F}_q$ , die ein Element  $\beta$  ( $q = p^s$ ,  $p$  prim) mit  $\text{ord}(\beta) = 5$  enthalten.

- a) Berechne für  $p = 3$  und  $p = 11$  jeweils ein minimales  $s$ , so dass  $\beta$  existiert.
- b) Zeige, dass für Primzahlpotenzen der Form  $q = 5^s$  kein Element  $\beta$  in  $\mathbb{F}_q$  der Ordnung 5 existiert.
- c) Sei allgemein  $n \in \mathbb{N}_{>1}$ ,  $p$  prim mit  $\text{ggT}(n, p) = 1$ . Zeige, dass eine natürliche Zahl  $s \leq n - 1$  existiert mit

$$n \mid p^s - 1.$$

**Zusatz:** Es gilt sogar  $s \mid g(n) \leq n - 1$  mit einer passenden Funktion  $g(n)$ . Finde  $g$  (1 P).

(1+1+1+1= 4 P)

## Aufgabe 15 (Ordnung von Elementen)

Betrachte den Körper  $\mathbb{F}_{25} := \mathbb{F}_5[x]/(x^2 + x + 1)$ . Das Polynom  $g(x) = x^2 + 3 \in \mathbb{F}_5[x]$  ist irreduzibel (muss nicht gezeigt werden). Sei  $\beta \in \mathbb{F}_{25}$  mit  $\min_{\mathbb{F}_5}(\beta) = g$ .

- a) Bestimme  $|\mathbb{F}_5(\beta)|$ .
- b) Bestimme  $\text{ord}(\beta)$ .

(0,5+0,5= 1 P)

