

Themenvorschläge für die kleinen Übungen am 6./7. Mai 2002

- a) *Richtig oder falsch:* Die Vektoren $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ aus \mathbb{F}_2^3 sind linear unabhängig.
- b) *Richtig oder falsch:* Die Vektoren $\begin{pmatrix} \alpha \\ 1 \end{pmatrix}$ und $\begin{pmatrix} \alpha + 1 \\ \alpha \end{pmatrix}$ aus \mathbb{F}_4^2 sind linear unabhängig.
- c) *Richtig oder falsch:* Die Abbildung $\varphi: \mathbb{F}_4 \rightarrow \mathbb{F}_4$, die α und $\alpha + 1$ miteinander vertauscht und 0, 1 auf sich selbst abbildet, ist \mathbb{F}_2 -linear.
- d) *Richtig oder falsch:* Für ein Polynom mit Koeffizienten in \mathbb{F}_2 ist

$$(a_0 + a_1x + a_2x^2 + \dots + a_nx^n)^2 = a_0 + a_1x^2 + a_2x^4 + \dots + a_nx^{2n}.$$

- e) Was ist $(x^6 + x^5 + x^3 + x^2 + 1)(x^2 + x + 1)$, wenn man Koeffizienten aus \mathbb{F}_2 rechnet?
- f) Zeigen Sie: Das Polynom $x^4 + 1$ ist irreduzibel über \mathbb{Q} , aber reduzibel über \mathbb{F}_2 .
- g) Stellen Sie den ggT von 2001 und 290 als Linearkombination dieser Zahlen dar!
- h) Bestimmen Sie im Körper \mathbb{F}_{1031} das multiplikative Inverse von zehn!
- i) Bestimmen Sie im Körper \mathbb{F}_{1031} das multiplikative Inverse von zwanzig!
- j) Bestimmen Sie im Körper \mathbb{F}_{1031} das multiplikative Inverse von zwei!
- k) Berechnen Sie den ggT der beiden Polynome $x^4 + 1$ und $x^3 + 1$ sowohl über \mathbb{R} als auch über \mathbb{F}_2 !
- l) Berechnen Sie über \mathbb{F}_2 den ggT der beiden Polynome

$$f = x^4 + x^2 + 1 \quad \text{und} \quad g = x^3 + 1,$$

und stellen Sie ihn in der Form $\alpha f + \beta g$ dar!

Multiplikation in $\mathbb{F}_8 = \mathbb{F}_2^3$ mit Basis $1, \alpha, \alpha^2$ sei über die Relation $\alpha^3 = \alpha + 1$ definiert.

- m) Was ist $(\alpha^2 + 1)(\alpha + 1)$?
- n) Was ist $(\alpha^2 + 1)^3$?
- o) Was ist $\frac{1}{\alpha}$?

Multiplikation in $\mathbb{F}_{64} = \mathbb{F}_2^6$ mit Basis $1, \alpha, \alpha^2, \dots, \alpha^5$ sei über die Relation $\alpha^6 = \alpha + 1$ definiert.

- p) Was ist $(\alpha^2 + 1)^3$?
- q) Was ist $(\alpha^3 + 1)^3$?
- r) Was ist $\frac{1}{\alpha + 1}$?

- s) Was ist der diskrete Logarithmus von 3 modulo 5 zur Basis 2?
- t) Was ist der diskrete Logarithmus von 5 modulo 7 zur Basis 3?