Wolfgang K. Seiler
Tel. 2515

A5, C201

14. Mai 2004

4. Übungsblatt Höhere Mathematik I

Fragen: *(je ein Punkt)*
Die Antworten auf die nachfolgenden Fragen sollten nicht länger als etwa zwei Zeilen sein und lediglich eine kurze *Begründung enthalten. Antworten ohne Begründung werden nicht gewertet.*

1) Richtig oder falsch: Für $x, y \in \mathbb{F}_{1024}$ ist $(x+y)^6 = x^6 + y^6$.

2) Richtig oder falsch: Jeder Vektorraum über $\mathbb{F}_2$ ist auch ein Vektorraum über $\mathbb{F}_4$.

3) Richtig oder falsch: $\mathbb{F}_8$ ist ein zweidimensionaler $\mathbb{F}_4$-Vektorraum.

4) Richtig oder falsch: Jeder Vektorraum über $\mathbb{F}_{16}$ ist auch ein Vektorraum über $\mathbb{F}_4$.

Aufgabe 1: *(5 Punkte)*
Ein Teilnehmer eines RSA-Netzwerks hat den öffentlichen Schlüssel (N, e) mit $N = 8\,539\,900\,738\,813$ und $e = 5\,693\,263\,252\,587$. Dabei ist N das Produkt der beiden Primzahlen $3\,141\,641$ und $2\,718\,293$.

a) Berechnen Sie den geheimen Exponenten dieses Teilnehmers!

b) Entschlüsseln Sie das an ihn gerichtete Kryptogramm $3\,878\,527\,951\,880$!

c) Das Original entspricht einer Folge von ASCII-Zeichen (deutscher Zeichensatz), die als Ziffern einer Zahl zur Basis 256 aufgefaßt wurden. Was war die Nachricht?

Aufgabe 2: *(5 Punkte)*

a) Zeigen Sie: Für alle $a \in \mathbb{F}_4$ ist $a^4 = a$.

b) Finden Sie alle Lösungen der Gleichung $x^6 = x$ in $\mathbb{F}_4$!

c) Finden Sie alle Lösungen der Gleichung $x^6 = 1$ in $\mathbb{F}_4$!

Aufgabe 3: *(6 Punkte)*
Addition und Multiplikation im Körper $\mathbb{F}_{256}$ seien über das Polynom $P = x^8+x^4+x^3+x+1$ erklärt, und $\alpha \in \mathbb{F}_{256}$ sei so gewählt, daß $P(\alpha) = 0$ ist. Stellen Sie die folgenden Potenzen und Produkte in der Form

$$a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\alpha^5 + g\alpha^6 + h\alpha^7$$

dar:

a) α^{15} *b)* $(1+\alpha^4)(1+\alpha^5)$ *c)* $(\alpha^2+\alpha^3+\alpha^4+\alpha^6)^2$ *d)* $(1+\alpha+\alpha^2+\alpha^3)^2$

Abgabe bis zum Freitag, dem 21. Mai 2004, um 12.00 Uhr