Wolfgang K. Seiler
Tel. 2515

A5, Zimmer C201

Themenvorschläge für die kleinen Übungen am 20./21. Mai 2003

a) Berechnen Sie die folgenden Summen in $\mathbb{F}_2^3$:

$$\vec{u} = \begin{pmatrix}0\\1\\1\end{pmatrix} + \begin{pmatrix}1\\1\\0\end{pmatrix}, \quad \vec{v} = \begin{pmatrix}1\\1\\1\end{pmatrix} + \begin{pmatrix}1\\1\\1\end{pmatrix} + \begin{pmatrix}1\\1\\1\end{pmatrix}, \quad \vec{w} = \vec{u} + \vec{v} + \vec{u}$$

Lösung:

$$\begin{pmatrix}0\\1\\1\end{pmatrix} + \begin{pmatrix}1\\1\\0\end{pmatrix} = \begin{pmatrix}1\\1+1\\1\end{pmatrix} = \begin{pmatrix}1\\0\\1\end{pmatrix} \quad \text{und}$$

$$\begin{pmatrix}1\\1\\1\end{pmatrix} + \begin{pmatrix}1\\1\\1\end{pmatrix} + \begin{pmatrix}1\\1\\1\end{pmatrix} = (1+1+1)\begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}1\\1\\1\end{pmatrix},$$

denn in $\mathbb{F}_2$ ist $1+1+1=1$.

b) Bestimmen Sie Kern und Bild der linearen Abbildung φ: $\left\{ \begin{array}{c} \mathbb{F}_2^4 \to \mathbb{F}_2^2 \\ \begin{pmatrix}a\\b\\c\\d\end{pmatrix} \mapsto \begin{pmatrix}a+b\\c+d\end{pmatrix} \end{array} \right.$!

Lösung: Die Abbildung ist offensichtlich surjektiv, denn setzt man $b = d = 0$, so erhält man den Vektor $\binom{a}{c}$, d.h. man kann für einen beliebigen Vektor aus $\mathbb{F}_2^2$ (mindestens) ein Urbild finden.

Für einen Vektor aus dem Kern muß $a + b = 0$ und $c + d = 0$ sein; für Elemente von $\mathbb{F}_2$ ist dies äquivalent dazu, daß $a = b$ und $c = d$ ist. Der Kern besteht also aus allen Vektoren aus $\mathbb{F}_2^4$, für die sowohl die ersten beiden als auch die letzten beiden Komponenten übereinstimmen.

c) Richtig oder falsch: Die Vektoren $\begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}$ und $\begin{pmatrix}0\\1\\1\end{pmatrix}$ aus $\mathbb{F}_2^3$ sind linear unabhängig.

Lösung: *Falsch,* denn $\begin{pmatrix}1\\0\\1\end{pmatrix} + \begin{pmatrix}1\\1\\0\end{pmatrix} + \begin{pmatrix}0\\1\\1\end{pmatrix} = \begin{pmatrix}1+1\\1+1\\1+1\end{pmatrix} = \vec{0}$.

(Wenn man die drei Vektoren als Elemente von $\mathbb{R}^3$ definiert hätte, wären sie linear unabhängig.)

d) 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.

Lösung: Zwei Vektoren sind genau dann linear abhängig, wenn einer der beiden ein Vielfaches des anderen ist. Falls, wie hier, keiner der beiden der Nullvektor ist, muß sogar jeder der beiden Vielfaches des anderen sein, denn dann kann in einer Relation $\lambda\vec{u} + \mu\vec{v} = \vec{0}$ keiner der beiden Koeffizienten verschwinden.

Wenn hier $\binom{\alpha+1}{\alpha}$ Vielfaches von $\binom{\alpha}{1}$ ist, sieht man sofort an der zweiten Komponente, daß der Proportionalitätsfaktor gleich α sein muß. Da auch $\alpha \cdot \alpha = \alpha + 1$ ist, gilt dies in der Tat; die beiden Vektoren sind also linear abhängig.

e) Richtig oder falsch: Die Abbildung $\varphi\colon \mathbb{F}_4 \to \mathbb{F}_4$, die α und $\alpha+1$ miteinander vertauscht und $0, 1$ auf sich selbst abbildet, ist $\mathbb{F}_2$-linear.

Lösung: Da es hier um $\mathbb{F}_2$-Linearität geht, ist es zweckmäßig, die Elemente von $\mathbb{F}_4$ als Vektoren über $\mathbb{F}_2$ zu schreiben. Wenn wir α mit dem Basisvektor $\binom{0}{1}$ identifizieren, heißt das

$$0 = \begin{pmatrix}0\\0\end{pmatrix}, \quad 1 = \begin{pmatrix}1\\0\end{pmatrix}, \quad \alpha = \begin{pmatrix}0\\1\end{pmatrix} \quad \text{und} \quad \alpha+1 = \begin{pmatrix}1\\1\end{pmatrix}.$$

φ ist dann gerade die Abbildung, die $\binom{x}{y}$ auf $\binom{x+y}{y}$ abbildet, und die ist natürlich linear.

f) Richtig oder falsch: Für ein Polynom mit Koeffizienten in $\mathbb{F}_2$ ist

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

Lösung: Über jedem Körper ist (nach dem Distributivgesetz)

$$(a_0 + a_1x + a_2x^2 + \cdot + a_nx^n)^2 = \sum_{i=0}^{n}\sum_{j=0}^{n} a_ia_jx^{i+j}.$$

Für $i = j$ ist der Summand gleich $a_i^2x^{2i}$, für $i \neq j$ haben wir außer $a_ia_jx^{i+j}$ auch noch den Summanden $a_ja_ixj + i$, der offensichtlich denselben Wert hat. Da in $\mathbb{F}_2$ wie auch in jedem Vektorraum über $\mathbb{F}_2$ die Addition eines Elements zu sich selbst null ergibt, heben sich diese beiden Terme weg, also ist

$$(a_0 + a_1x + a_2x^2 + \cdot + a_nx^n)^2 = a_0^2 + a_1^2x^2 + a_2^2x^4 + \cdot + a_n^2x^{2n}.$$

Soweit gilt alles auch noch über Körpern wie $\mathbb{F}_4$ oder $\mathbb{F}_{256}$; nur in $\mathbb{F}_2$ aber ist auch noch $a^2 = a$ für alle $a \in \mathbb{F}_2$ – es gibt schließlich nur die beiden Elemente $a = 0$ und $a = 1$. Damit ist die Behauptung richtig.

g) Was ist $(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^2 + 1)$, wenn man mit Koeffizienten aus $\mathbb{F}_2$ rechnet?

Lösung: Multiplikation von $(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ mit x^2 ergibt $x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2$, während die Multiplikation mit eins natürlich nichts ändert. Da $x^i + x^i = 0$ für alle i, folgt

$$(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^2 + 1) = x^{12} + x^{11} + x + 1;$$

alle mittleren Terme heben sich weg.

h) Zeigen Sie: Das Polynom $x^4 + 1$ ist reduzibel über $\mathbb{F}_2$.

Lösung: $x^4 + 1 = (x^2 + 1)(x^2 + 1) = (x + 1)^4$

i) Stellen Sie den ggT von 2010 und 123 als Linearkombination dieser Zahlen dar!

Lösung:

$$2010 : 123 = 16 \text{ Rest } 42 \Longrightarrow 42 = 1 \cdot 2010 - 16 \cdot 123$$

$123 : 42 = 2$ Rest $39 \Longrightarrow 39 = 1{\cdot}123{-}2{\cdot}42 = 1{\cdot}123{-}2(1{\cdot}2010{-}16{\cdot}123) = -2{\cdot}2010{+}33{\cdot}123$

$42 : 39 = 1$ Rest $3 \Longrightarrow 3 = 42{-}39 = (1{\cdot}2010{-}16{\cdot}123){-}(-2{\cdot}2010{+}33{\cdot}123) = 3{\cdot}2010{-}49{\cdot}123$

Da 39 durch drei teilbar ist, ist drei der größte gemeinsame Teiler von 2010 und 123; wir sind also fertig.

j) Bestimmen Sie im Körper $\mathbb{F}_{1031}$ die multiplikativen Inversen von zwei, zehn und zwanzig!

Lösung: Auch hier geht es darum, den größten gemeinsamen Teiler als Linearkombination darzustellen, allerdings wissen wir, daß der ggT von 1031 und jeder der angegebenen Zahlen eins ist, so daß tatsächlich nur die Koeffizienten der Linearkombination interessieren.

$$1031 : 2 = 515 \text{ Rest } 1 \Longrightarrow 1 = 1031 - 515 \cdot 2 \Longrightarrow -515 \cdot 2 \equiv 1 \bmod 1031 .$$

Somit ist $-515 \equiv 1031 - 515 = 516 \bmod 1031$ invers zu zwei.

$$1031 : 10 = 103 \text{ Rest } 1 \Longrightarrow 1 = 1031 - 103 \cdot 10 ,$$

hier ist das Inverse also $-103 \equiv 928 \bmod 1031$. Für zwanzig wird die Rechnung etwas umfangreicher:

$$\begin{aligned} 1031 : 20 = 51 \text{ Rest } 11 &\Longrightarrow 11 = 1 \cdot 1031 - 51 \cdot 20 \\ 20 : 11 = 1 \text{ Rest } 9 &\Longrightarrow 9 = -1 \cdot 1031 + 52 \cdot 20 \\ 11 : 9 = 1 \text{ Rest } 2 &\Longrightarrow 2 = 2 \cdot 1031 - 103 \cdot 20 \\ 9 : 2 = 4 \text{ Rest } 1 &\Longrightarrow 1 = -9 \cdot 1031 + 464 \cdot 20 \end{aligned}$$

Damit ist $464 \cdot 20 \equiv 1 \bmod 1031$, das multiplikative Inverse von 20 in $\mathbb{F}_{1031}$ ist also 464.

k) Berechnen Sie den ggT der beiden Polynome $x^4 + 1$ und $x^3 + 1$ sowohl über $\mathbb{R}$ als auch über $\mathbb{F}_2$!

Lösung: Über den reellen Zahlen ist

$$\begin{aligned} (x^4 + 1) : (x^3 + 1) &= x \text{ Rest } -x + 1 \\ (x^3 + 1) : (-x + 1) &= -x^2 - x - 1 \text{ Rest } 2 , \end{aligned}$$

die Polynome sind also teilerfremd, d.h. der ggT ist Eins (oder jede andere von Null verschiedene Konstante).
Über dem Körper mit zwei Elementen ist

$$\begin{aligned} (x^4 + 1) : (x^3 + 1) &= x \text{ Rest } x + 1 \\ (x^3 + 1) : (x + 1) &= x^2 + x + 1 \text{ Rest } 0 , \end{aligned}$$

der ggT ist also $x + 1$.

l) Berechnen Sie über $\mathbb{F}_2$ den ggT der beiden Polynome $f = x^4 + x^2 + 1$ und $g = x^3 + 1$, und stellen Sie ihn in der Form $\alpha f + \beta g$ dar!

Lösung:

$$\begin{aligned} (x^4 + x^2 + 1) : (x^3 + 1) = x \text{ Rest } x^2 + x + 1 &\Longrightarrow x^2 + x + 1 = 1 \cdot (x^4 + x^2 + 1) + x \cdot (x^3 + 1) \\ (x^3 + 1) : (x^2 + x + 1) = x + 1 \text{ Rest } 0 . & \end{aligned}$$

Damit haben wir bereits in der ersten Division den ggT und seine lineare Darstellung gefunden.

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 $(\alpha^2 + 1)(\alpha + 1)$?

Lösung: $(\alpha^2 + 1)(\alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1$ hat Grad drei, muß also modulo $\alpha^3 + \alpha + 1$ reduziert werden. Bei der Division ist offensichtlich der Quotient eins und der Rest α^2.

n) Was ist $(\alpha^2+1)^2$?

Lösung: $(\alpha^2+1)^2 = \alpha^4+1$ und

$$(\alpha^4+1) : (\alpha^3+\alpha+1) = \alpha \text{ Rest } \alpha^2+\alpha+1\,.$$

Also ist $(\alpha^2+1)^2 = \alpha^2+\alpha+1$.

o) Was ist $\dfrac{1}{\alpha}$?

Lösung: Wir müssen den ggT Eins von $\alpha^3+\alpha+1$ und α linear kombinieren:

$$(\alpha^3+\alpha+1) : \alpha = \alpha^2+1 \text{ Rest } 1 \Longrightarrow \alpha\cdot(\alpha^2+1) \equiv 1 \bmod \alpha^3+\alpha+1\,.$$

Damit ist $\alpha^{-1} = \alpha^2+1$.

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

p) Was ist $(\alpha^2+1)^3$?

Lösung: $(\alpha^2+1)^3 = \alpha^6+\alpha^4+\alpha^2+1$ führt bei Division durch $\alpha^6+\alpha+1$ zum Quotienten Eins und Rest

$$\alpha^4+\alpha^2+\alpha\,,$$

der somit das Ergebnis ist.

q) Was ist $(\alpha^3+1)^3$?

Lösung: $(\alpha^3+1)^3 = \alpha^9+\alpha^6+\alpha^3+1$. Nach der angegebenen Relation ist

$$\alpha^6 = \alpha+1 \Longrightarrow \alpha^9 = \alpha^4+\alpha^3\,.$$

Damit ist $(\alpha^3+1)^3 = (\alpha^4+\alpha^3)+(\alpha+1)+\alpha^3+1 = \alpha^4+\alpha$.

r) Was ist $\dfrac{1}{\alpha+1}$?

Lösung: $(\alpha^6+\alpha+1) : (\alpha+1) = \alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha$ Rest 1, d.h.

$$(\alpha+1)(\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha) = (\alpha^6+\alpha+1)+1$$

(in $\mathbb{F}_2$ sind $+$ und $-$ dieselbe Operation), und

$$\frac{1}{\alpha+1} = \alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha\,.$$