M. Künzer, J. Marhenke

Lineare Algebra für Informatiker, WS 03/04

Lösung 4

Aufgabe 15.

$(\mathbf{F}_4,+)$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$(\mathbf{F}_4,\cdot)$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

$(\mathbf{F}_8,\cdot)$	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
0	0	0	0	0	0	0	0	0
1	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
β	0	β	β^2	$\beta+\beta^2$	$1+\beta$	1	$1+\beta+\beta^2$	$1+\beta^2$
$1+\beta$	0	$1+\beta$	$\beta+\beta^2$	$1+\beta^2$	$1+\beta+\beta^2$	β^2	1	β
β^2	0	β^2	$1+\beta$	$1+\beta+\beta^2$	$\beta+\beta^2$	β	$1+\beta^2$	1
$1+\beta^2$	0	$1+\beta^2$	1	β^2	β	$1+\beta+\beta^2$	$1+\beta$	$\beta+\beta^2$
$\beta+\beta^2$	0	$\beta+\beta^2$	$1+\beta+\beta^2$	1	$1+\beta^2$	$1+\beta$	β	β^2
$1+\beta+\beta^2$	0	$1+\beta+\beta^2$	$1+\beta^2$	β	1	$\beta+\beta^2$	β^2	$1+\beta$

$(\mathbf{F}_9,\cdot)$	0	1	-1	ι	$\iota+1$	$\iota-1$	$-\iota$	$-\iota+1$	$-\iota-1$
0	0	0	0	0	0	0	0	0	0
1	0	1	-1	ι	$\iota+1$	$\iota-1$	$-\iota$	$-\iota+1$	$-\iota-1$
-1	0	-1	1	$-\iota$	$-\iota-1$	$-\iota+1$	ι	$\iota-1$	$\iota+1$
ι	0	ι	$-\iota$	-1	$\iota-1$	$-\iota-1$	1	$\iota+1$	$-\iota+1$
$\iota+1$	0	$\iota+1$	$-\iota-1$	$\iota-1$	$-\iota$	1	$-\iota+1$	-1	ι
$\iota-1$	0	$\iota-1$	$-\iota+1$	$-\iota-1$	1	ι	$\iota+1$	$-\iota$	-1
$-\iota$	0	$-\iota$	ι	1	$-\iota+1$	$\iota+1$	-1	$-\iota-1$	$\iota-1$
$-\iota+1$	0	$-\iota+1$	$\iota-1$	$\iota+1$	-1	$-\iota$	$-\iota-1$	ι	1
$-\iota-1$	0	$-\iota-1$	$\iota+1$	$-\iota+1$	ι	-1	$\iota-1$	1	$-\iota$

Aufgabe 16.

(1) In $\mathbf{C}$ ist $(1+i)^3 = 1+3i+3i^2+i^3 = -2+2i$ und

$$(1+2i)^{-1} \;=\; \frac{1}{1+2i}\cdot\frac{1-2i}{1-2i} \;=\; \frac{1-2i}{1+4} \;=\; \frac{1}{5}-\frac{2}{5}i\,.$$

(2) Zum Beispiel kann man $(1+\alpha)^5 = ((1+\alpha)^2)^2(1+\alpha) = \alpha^2(1+\alpha) = \alpha$ rechnen. Ferner folgt aus $\alpha^3 = 1$, daß $\alpha^{-2} = \alpha$.

(3) In $\mathbf{F}_9$ gilt $x^8 = 1$ für alle $x \neq 0$. Daher ist $(1+\iota)^7 = (\iota+1)^{-1} = \iota - 1$. Aus der in Aufgabe 15 erstellten Tabelle liest man ab, daß $\sum_{x\in\mathbf{F}_9} x^2 = 0+1+1-1-\iota+\iota-1+\iota-\iota = 0$.

(4) Man erhält aus obiger Tabelle für $\mathbf{F}_8$, dass $(1+\beta+\beta^2)^{-1} = \beta^2$. Weiter ist $0^{14} = 0$ und $x^{14} = (x^7)^2 = 1^2 = 1$ für alle $x \in \mathbf{F}_8 \smallsetminus \{0\}$.

Aufgabe 17.

(1) Es liegt kein Körper vor, da $119 = 7\cdot 17$ keine Primzahl ist. Der Ring $\mathbf{Z}/119\mathbf{Z}$ hat 119 Elemente.

(2) In $\mathbf{C}[X]$ gilt $X^2+1 = (X+i)(X-i)$. Das Polynom X^2+1 ist also reduzibel und damit ist (der unendliche Ring) $\mathbf{C}[X]/(X^2+1)\mathbf{C}[X]$ kein Körper.

(3) In diesem Fall ist R ein Körper, da X^3+X^2+1 ein Polynom von Grad 3 ist, das keine Nullstellen in $\mathbf{F}_5$ besitzt, und somit irreduzibel ist. Der Körper hat $5^3 = 125$ Elemente.

(4) In $\mathbf{F}_2[X]$ ist $X^4+X^2+1 = (X^2+X+1)^2$ reduzibel. Damit ist R ein Ring mit $2^4 = 16$ Elementen, aber kein Körper.

(5) Das Polynom $X^3+\alpha \in \mathbf{F}_4[X]$ besitzt in $\mathbf{F}_4$ keine Nullstelle, da $0^3 = 0$ und $x^3 = 1$ für alle $x \in \mathbf{F}_4 \smallsetminus \{0\}$. Da das Polynom von Grad 3 ist, ist es irreduzibel und somit ist R ein Körper mit $4^3 = 64$ Elementen.

(6) Wir zeigen, dass R ein Körper ist. Zunächst stellt man fest, dass X^4+X^2+X+1 keine Nullstellen in $\mathbf{F}_3$ besitzt. Achtung: Dies zeigt noch nicht, dass das Polynom irreduzibel ist, da es von Grad 4 ist! Aber es zeigt, dass keine Faktorisierung des Polynoms existiert, die einen Faktor von Grad 1 enthält. Somit genügt es, alle irreduziblen Polynome von Grad 2 aufzulisten, namentlich X^2+X-1, X^2-X-1 und X^2+1, und nachzurechnen, dass X^4+X^2+X+1 nicht das

Produkt zweier solcher Faktoren ist.

$(\cdot)$	X^2+X-1	X^2-X-1	X^2+1
X^2+X-1	$X^4-X^3-X^2+X+1$	X^4+1	X^4+X^3+X-1
X^2-X-1		$X^4+X^3-X^2-X+1$	X^4-X^3-X-1
X^2+1			X^4-X^2+1

Damit sehen wir, dass X^4+X^2+X+1 irreduzibel ist. Somit ist R ein Körper mit $3^4=81$ Elementen.

Aufgabe 18.

(1) In $\mathbf{F}_2[X]$ gibt es nur ein irreduzibles Polynom von Grad 2, und zwar X^2+X+1. Alle anderen normierten Polynome von Grad 2, als da wären X^2, X^2+1, X^2+X, haben eine Nullstelle in $\mathbf{F}_2$. Nur X^2+X+1 hat keine Nullstelle, und da es von Grad ≤ 3 ist, genügt dies, um darauf schließen zu können, daß es irreduzibel ist.

(2) Es genügt, alle normierten Polynome aus $\mathbf{F}_4[X]$ aufzulisten, die keine Nullstellen in $\mathbf{F}_4$ besitzen. Hierbei kann die Nullstelle 0 durch einen nichtverschwindenden konstanten Term ausgeschlossen werden, sowie von Vorteil verwandt werden, daß $x^3=1$ für $x\in\mathbf{F}_4\smallsetminus\{0\}$. Die irreduziblen Polynome sind gegeben durch: $X^3+\alpha$, $X^3+(1+\alpha)$, X^3+X+1, $X^3+\alpha X+1$, $X^3+(1+\alpha)X+1$, X^3+X^2+1, $X^3+X^2+X+\alpha$, $X^3+X^2+X+(1+\alpha)$, $X^3+X^2+\alpha X+(1+\alpha)$, $X^3+X^2+(1+\alpha)X+\alpha$, $X^3+\alpha X^2+1$, $X^3+(1+\alpha)X^2+1$, $X^3+\alpha X^2+X+(1+\alpha)$, $X^3+(1+\alpha)X^2+X+\alpha$, $X^3+\alpha X^2+\alpha X+\alpha$, $X^3+(1+\alpha)X^2+(1+\alpha)X+(1+\alpha)$, $X^3+\alpha X^2+(1+\alpha)X+\alpha$, $X^3+(1+\alpha)X^2+\alpha X+(1+\alpha)$, $X^3+\alpha X^2+(1+\alpha)X+(1+\alpha)$, $X^3+(1+\alpha)X^2+\alpha X+\alpha$. Das sind insgesamt 20 Stück.

(3) Zunächst muss man bestimmen, wieviele irreduzible Polynome von Grad 2 es in $\mathbf{F}_p[X]$ gibt. Es gibt p^2 normierte Polynome von Grad 2. Außerdem gibt es in $\mathbf{F}_p[X]$ nur p mögliche Faktoren von Grad 1. Es gibt p Polynome von Grad 2, die Quadrat eines solchen Faktors sind. Ferner gibt es noch $\frac{p(p-1)}{2}$ Polynome von Grad 2, die Produkt zweier verschiedener Faktoren sind. Also gibt es $p^2-\frac{p^2-p}{2}-p=(p^2-p)/2$ irreduzible Polynome von Grad 2.
Ein normiertes Polynom von Grad 3 kann irreduzibel sein, oder es kann zerfallen in drei irreduzible Faktoren, die jeweils von Grad 1 sind, oder es kann zerfallen in ein Produkt aus einem irreduziblen Faktor von Grad 2 und einem von Grad 1. Insgesamt gibt es p^3 normierte Polynome von Grad 3 in $\mathbf{F}_p[X]$. Davon zerfallen mit obiger Überlegung $p\cdot p(p-1)/2$ Polynome in ein Produkt, das einen irreduziblen Faktor von Grad 2 enthält.
Ist ein Polynom Produkt von 3 Faktoren von Grad 1, so können alle Faktoren identisch sein, es können zwei gleiche auftreten oder es können alle drei verschieden sein. Für 3 gleiche Faktoren gibt es p Möglichkeiten, für zwei gleiche Faktoren gibt es $p(p-1)$ Möglichkeiten, und $\frac{p(p-1)(p-2)}{3!}$ Polynome besitzten eine Zerlegung in 3 verschiedene Faktoren. Also gibt es $p+p(p-1)+\frac{p(p-1)(p-2)}{3!}$ Polynome, die in 3 Faktoren von Grad 1 zerfallen.
Insgesamt gibt es also

$$p^3-\left[p+p(p-1)+\frac{p(p-1)(p-2)}{3!}+p^2(p-1)/2\right]\;=\;\frac{p^3-p}{3}$$

irreduzible Polynome von Grad 3 in $\mathbf{F}_p[X]$. (Bemerkung: Dieselben Überlegungen kann man auch in $\mathbf{F}_4[X]$ anwenden und erhält $(4^3-4)/3=20$ irreduzible Polynome von Grad 3 — das ist eine alternative Lösung von (2), die ohne die Berechnung aller dieser Polynome auskommt.)

Aufgabe 19.

(1) Die Aussage ist falsch. Für $p=2$ ist das Polynom $f(X)=(X^2+X+1)^2\in\mathbf{F}_2[X]$ nicht irreduzibel, wohl aber ohne Nullstelle in $\mathbf{F}_2$.

(2) Die Aussage ist falsch. Sei p prim beliebig gewählt. Für die Polynome $f(X)=X$ und $g(X)=X^p$ in $\mathbf{F}_p[X]$ ist $f(X)\neq g(X)$, aber $f(x)=g(x)$ für alle $x\in\mathbf{F}_p$.

(3) Die Aussage ist wahr. $\Longrightarrow$: Ist $f(X)=g(X)$, so ist auch $f(x)=g(x)$ für alle $x\in\mathbf{R}$. $\Longleftarrow$: Ist $f(x)=g(x)$ für alle $x\in\mathbf{R}$, so ist $h(X):=f(X)-g(X)$ ein Polynom mit $h(x)=0$ für alle $x\in\mathbf{R}$. Wir nehmen an, es sei $h(X)\neq 0$ und schreiben $m=\deg h$. Seien $x_1,\ldots,x_{m+1}$ paarweise verschiedene Elemente von $\mathbf{R}$. Durch Abspalten der zu diesen Nullstellen von $h(X)$ gehörigen Linearfaktoren $(X-x_1),\ldots,(X-x_{m+1})$ erkennt man, daß das Produkt $(X-x_1)\cdots(X-x_{m+1})$ ein Teiler von $h(X)$ sein muß, insbesondere also, daß $\deg h\geq m+1$, Widerspruch. Also ist $h(X)=0$, und mithin $f(X)=g(X)$.

(4) Die Aussage ist falsch. Bezeichne $K:=\mathbf{F}_4[X]/(X^3+\alpha)\mathbf{F}_4[X]$ den Körper aus Aufgabe 18 (5). Sei $\gamma:=\bar{X}$ in K. Es lässt sich jedes Element aus K eindeutig in der Form $(a+b\alpha)+(c+d\alpha)\gamma+(e+f\alpha)\gamma^2$ mit $a,b,c,d,e,f\in\mathbf{F}_2$ schreiben. Insbesondere werden $\gamma^0=1$, $\gamma^1=\gamma$, $\gamma^2=\gamma^2$, $\gamma^3=\alpha$, $\gamma^4=\alpha\gamma$, $\gamma^5=\alpha\gamma^2$ und $\gamma^6=1+\alpha$. Daraus erkennt man zum einen, dass kein Polynom $g(X)\in\mathbf{F}_2[X]$ mit $\deg g\leq 5$ existiert mit $g(\gamma)=0$, und zum anderen, daß für $f(X):=X^6+X^3+1\in\mathbf{F}_2[X]$ gilt, daß $f(\gamma)=0$. Wir behaupten, daß $f(X)$ irreduzibel ist. Angenommen, es gelte $f(X)=g(X)\cdot h(X)$ für $g(X),h(X)\in\mathbf{F}_2[X]$ mit $\deg g,\deg h\leq 5$. Dann ist $0=f(\gamma)=g(\gamma)\cdot h(\gamma)$. Da K ein Körper ist, folgt $g(\gamma)=0$ oder $h(\gamma)=0$, was wir eben ausgeschlossen haben, Widerspruch. Dies zeigt die Behauptung, daß $f(X)=X^6+X^3+1\in\mathbf{F}_2[X]$ in der Tat irreduzibel ist — und dies, ohne alle irreduziblen Polynome von Grad ≤ 3 daraufhin zu testen, ob sie $f(X)$ teilen.