M. Künzer, J. Marhenke

Lineare Algebra für Informatiker, WS 03/04

# Lösung 3

**Aufgabe 10.** Die Multiplikationstafeln ergeben sich wie folgt.

**Z/5Z**

| $(\cdot)$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

**Z/6Z**

| $(\cdot)$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

**Z/8Z**

| $(\cdot)$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

**Aufgabe 11.**

(1) Es wird $\left\{x \in \mathbf{Z}/13\mathbf{Z} \,\middle|\, \{x^m \mid m \in \mathbf{Z}\} = (\mathbf{Z}/13\mathbf{Z}) \smallsetminus \{0\}\right\} = \{2, 6, 7, 11\}$.

(2) Zunächst überprüfen wir, ob die Multiplikationsabbildung zu einer Abbildung $G \times G \longrightarrow G$ einschränkt. Seien $x, y \in G$. Wegen $(xy)^4 = x^4 y^4 = 1$ ist dann auch $xy \in G$.

(G1) Seien $x, y, z \in G$. Dann gilt $(xy)z = x(yz)$, da $G \subseteq \mathbf{Z}/13\mathbf{Z}$.

(G2) Die 1 aus $\mathbf{Z}/13\mathbf{Z}$ ist auch die 1 in $G$.

(G3) Für jedes $x \in G$ ist $xx^3 = x^3 x = x^4 = 1$. Außerdem ist $(x^3)^4 = (x^4)^3 = 1^3 = 1$, somit ist $x^3$ in $G$ und invers zu $x$.

Die Multiplikationstafel ergibt sich zu

| $(\cdot)$ | 1 | 5 | 8 | 12 |
|---|---|---|---|---|
| 1 | 1 | 5 | 8 | 12 |
| 5 | 5 | 12 | 1 | 8 |
| 8 | 8 | 1 | 12 | 5 |
| 12 | 12 | 8 | 5 | 1 |

**Aufgabe 12.**

(1) Wir zeigen $R \times S$ Ring. Seien $(r, s)$, $(r', s')$, $(r'', s'')$, $(r''', s''') \in R \times S$.

(R1) (i) $((r,s) + (r',s')) + (r'',s'') = (r + r', s + s') + (r'', s'') = (r + r' + r'', s + s' + s'')$
$= (r,s) + (r' + r'', s' + s'') = (r,s) + ((r',s') + (r'',s''))$

(ii) $(r,s) + (0,0) = (r + 0, s + 0) = (r,s)$

(ii) $(r,s) + (-r,-s) = (r + (-r), s + (-s)) = (0,0)$

(iv) $(r,s) + (r',s') = (r + r', s + s') = (r' + r, s' + s) = (r',s') + (r,s)$

(R2) (i) $((r,s)(r',s'))(r'',s'') = (rr', ss')(r'',s'') = (rr'r'', ss's'')$
$= (r,s)(r'r'', s's'') = (r,s)((r',s')(r'',s''))$

(ii) $(r,s)(1,1) = (r \cdot 1, s \cdot 1) = (r,s) = (1 \cdot r, 1 \cdot s) = (1,1)(r,s)$

(R3) $((r,s) + (r',s'))((r'',s'') + (r''',s''')) = (r + r', s + s')(r'' + r''', s'' + s''')$
$= ((r + r')(r'' + r'''), (s + s')(s'' + s''')) = (rr'' + rr''' + r'r'' + r'r''', ss'' + ss''' + s's'' + s's''')$
$= (r,s)(r'',s'') + (r,s)(r''',s''') + (r',s')(r'',s'') + (r',s')(r''',s''')$

Wir zeigen, dass $R \times \{0\}$ ein Ideal in $R \times S$ ist. Wegen $(0,0) \in R \times \{0\}$ ist $R \times \{0\} \neq \emptyset$. Seien $(r,0), (r',0) \in R \times \{0\}$ und $(r'',s'') \in R \times S$. Es gilt $(r,0) - (r',0) = (r - r', 0) \in R \times \{0\}$, und $(r,0)(r'',s'') = (rr'', 0 \cdot s'') = (rr'', 0) \in R \times \{0\}$ sowie $(r'',s'')(r,0) = (r''r, s'' \cdot 0) = (r''r, 0) \in R \times \{0\}$.

(2) Injektivität genügt hier, weil es sich um eine Abbildung zwischen zwei Mengen mit je $uv$ Elementen handelt (vgl. Blatt 1, Aufgabe 2).
Da die Abbildung ein Morphismus der additiven Gruppen ist, genügt es zu zeigen, dass ihr Kern gleich $\{0\}$ ist. Sei also $x + uv\mathbf{Z} \in \mathbf{Z}/uv\mathbf{Z}$ gegeben mit $(x + u\mathbf{Z}, x + v\mathbf{Z}) = (0 + u\mathbf{Z}, 0 + v\mathbf{Z})$. In anderen Worten, es ist $x \in u\mathbf{Z} \cap v\mathbf{Z}$. Nun ist wegen $u$, $v$ teilerfremd aber $u\mathbf{Z} \cap v\mathbf{Z} = uv\mathbf{Z}$, und es folgt $x \in uv\mathbf{Z}$, in anderen Worten, $x + uv\mathbf{Z} = 0 + uv\mathbf{Z}$.

(3) Da nach (2) die Abbildung $\varphi$ surjektiv ist, ist $\varphi^{-1}((a+u\mathbf{Z}, b+v\mathbf{Z})) \neq \emptyset$. Also existiert ein $x \in \mathbf{Z}$ so, dass $\varphi(x+uv\mathbf{Z}) = (a+u\mathbf{Z}, b+v\mathbf{Z})$, d.h. $x+u\mathbf{Z} = a+u\mathbf{Z}$ und $x+v\mathbf{Z} = b+v\mathbf{Z}$. D.h. $x \equiv_u a$ und $x \equiv_v b$, wie verlangt.

(4) Zum Beispiel leistet $x = 155$ das Gewünschte: $155 \equiv_{15} 5$ und $155 \equiv_{22} 1$.
Allgemein ist $\{x \in \mathbf{Z} \mid x \equiv_{15} 5\,,\ \ x \equiv_{22} 1\} = 155 + 330\mathbf{Z}$.

**Aufgabe 13.**

(1) Es ist $(0,0,0)$ sicher eine Lösung. Wir haben zu zeigen, dass keine weiteren Lösungen existieren. Dazu treffen wir die Annahme, es gebe eine Lösung $(x_0, y_0, z_0) \neq (0,0,0)$, und haben einen Widerspruch herzuleiten. Sei $g$ der größte gemeinsame Teiler von $(x_0, y_0, z_0)$. Aus $x_0^5 + 2y_0^5 = 5z^5$ folgt nun $\left(\frac{x_0}{g}\right)^5 + 2\left(\frac{y_0}{g}\right)^5 = 5\left(\frac{z_0}{g}\right)^5$, d.h. wir haben eine Lösung $(x,y,z) := (\frac{x_0}{g}, \frac{y_0}{g}, \frac{z_0}{g}) \neq 0$ derart, dass keine Primzahl $x$, $y$ und $z$ teilt. Man spricht von einem *teilerfremden* Tupel $(x,y,z)$, oder auch von einem Tupel mit $\mathrm{ggT}(x,y,z) = 1$.

Es sei das Repräsentantensystem $\{-5,-4,\ldots,4,5\}$ von $\mathbf{Z}/11\mathbf{Z}$ gewählt. Für jedes $x \in \mathbf{Z}/11\mathbf{Z}$ gilt $x^5 \in \{-1,0,1\}$. Wir erhalten folgende mögliche Werte von $x^5 + 2y^5$ in $\mathbf{Z}/11\mathbf{Z}$.

| $x^5$ | $y^5$ | $x^5 + 2y^5$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 2 |
| 0 | $-1$ | $-2$ |
| 1 | 0 | 1 |
| 1 | 1 | 3 |
| 1 | $-1$ | $-1$ |
| $-1$ | 0 | $-1$ |
| $-1$ | 1 | 1 |
| $-1$ | $-1$ | $-3$ |

Für $z \in \mathbf{Z}/11\mathbf{Z}$ kann $5z^5$ nur Werte aus $\{-5,0,5\}$ annehmen. Folglich sehen wir aus der Tabelle, dass $x \equiv_{11} 0$, $y \equiv_{11} 0$ und $z \equiv_{11} 0$ gelten muss, dass also 11 sowohl $x$, $y$ als auch $z$ teilt, und wir sind bei einem Widerspruch angelangt.

(2) Wie in (1) haben wir die Existenz einer teilerfremden Lösung $(x,y,z) \neq (0,0,0)$ zum Widerspruch zu führen. Betrachtet man die Gleichung $x^3 + 2y^3 = 4z^3$ modulo 2, so erhält man $x^3 = 4z^3 - 2y^3 \equiv_2 0$, also muss $x \equiv_2 0$ sein. Eine Betrachtung der Gleichung modulo 4 liefert nun $2y^3 \equiv_8 x^3 + 2y^3 = 4z^3 \equiv_4 0$ wegen $x^3 \equiv_8 0$, mithin $y \equiv_2 0$. Eine Betrachtung der Gleichung modulo 8 liefert nun $4z^3 = x^3 + 2y^3 \equiv_8 0$, also auch $z \equiv_2 0$. Damit teilt 2 sowohl $x$, $y$ als auch $z$, und wir haben einen Widerspruch.

(3) Wie in (1) haben wir die Existenz einer teilerfremden Lösung $(x,y,z) \neq (0,0,0)$ zum Widerspruch zu führen. Man betrachte die Gleichung modulo $p$. In $\mathbf{Z}/p\mathbf{Z}$ ist $a^{p-1} = 0$ für $a = 0$, und $a^{p-1} = 1$ für alle $a \in (\mathbf{Z}/p\mathbf{Z}) \smallsetminus \{0\}$. Also kann $x^{p-1} + y^{p-1}$ in $\mathbf{Z}/p\mathbf{Z}$ nur die Werte 0, 1 oder 2 annehmen, und $3z^{p-1}$ kann dort nur 0 oder 3 werden. Wegen $p \geq 5$ ist $3 \not\equiv_p 0,1,2$. Es folgt $x \equiv_p 0$, $y \equiv_p 0$ und $z \equiv_p 0$, und wir haben einen Widerspruch.

**Aufgabe 14.**

(1) Die Aussage ist wahr. Man schreibt zunächst $\sigma$ in Zykelschreibweise:
$\sigma = (1,4n)(2,4n-1)(3,4n-2)\cdots(2n-1,2n+2)(2n,2n+1)$. Daraus entnimmt man $\varepsilon_\sigma = (-1)^{2n} = 1$.

(2) Die Aussage ist wahr. Die Ordnung $m$ eines $\sigma \in \mathcal{S}_n$ teilt $n! = \#\mathcal{S}_n$ nach Lagrange, d.h. es ist $mm' = n!$ für ein $m' \in \mathbf{Z}$. Nun ist $\sigma^{n!} = \sigma^{mm'} = (\sigma^m)^{m'} = 1^{m'} = 1$.

(3) Die Aussage ist falsch. Betrachte $x = 3$ in $\mathbf{Z}/6\mathbf{Z}$. Es ist $x^3 = 9 \equiv_6 3$, aber $x \not\equiv_6 0,1$.

(4) Die Aussage ist wahr. Wegen $\#R < \infty$ kann der Ring $R$ auch nur endlich viele Ideale haben. Wir behaupten, es existiert ein *maximales Ideal* $M$, i.e. ein Ideal, für welches kein Ideal $I'$ existiert mit $M \subsetneq I' \subsetneq R$.

Angenommen, dies sei nicht so. Wegen $\#R > 1$ ist $\{0\} \subsetneq R$, und ausgehend davon können wir eine Folge von Idealen $\{0\} \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$ mit $I_i \subsetneq R$ für alle $i \in \mathbf{N}$ konstruieren. Dies ist ein Widerspruch, da es nur endlich viele Ideale in $R$ gibt.

Sei also $M$ ein solches maximales Ideal. Wir behaupten, dass $R/M$ nur die Ideale $\{\bar{0}\}$ und $R/M$ enthält. Sei $\{0\} \subsetneq I \subseteq R/M$ ein Ideal. Wir haben $I = R/M$ zu zeigen. Sei $J := \{\, x \in R \mid \bar{x} \in I \} \subseteq R$. Dann ist wegen $\bar{0} \in I$ sicher $M \subseteq J$, und wegen $\{\bar{0}\} \subsetneq I$ sogar $M \subsetneq J$. Ferner ist $J$ ein Ideal in $R$, da mit $x, x' \in J$ und $r \in R$ wegen $\overline{x - x'} = \overline{x'} - \overline{x} \in I$ und $\overline{rx} = \overline{r} \cdot \overline{x} \in I$ auch $x - x' \in J$ und $rx \in J$. Wegen der Maximalität von $M$ folgt nun $J = R$, und also auch $I = R/M$. Wir bemerken noch, dass in $R/M$ wegen $M \subsetneq R$ auch $\bar{0} \neq \bar{1}$ gilt, da sonst $1 \in M$ wäre, und somit $R = M$.

Bleibt zu zeigen, dass $R/M$ ein Körper ist. Dafür genügt es zu zeigen, dass jeder kommutative Ring $S$, in welchem $0 \neq 1$, und in welchem $\{0\}$ und $S$ die einzigen Ideale sind, ein Körper ist. Sei $x \in S \smallsetminus \{0\}$. Es ist das Ideal $xS \neq \{0\}$, also $xS = S$, speziell $1 \in xS$, d.h. es gibt ein $y \in S$ mit $xy = 1$.