Übungsblatt 6 LA I SS18

carsten.feldkamp@hhu.de

Aufgabe 1:

Man bemerke: $A \Delta B = B \Delta A$

geg.: symm. Differenz Δ durch
$$A \Delta B := (A \setminus B) \cup (B \setminus A) \quad \forall A, B \subseteq X$$

z.z.: $(\mathcal{P}(X), \Delta)$ ist eine Gruppe

Wir zeigen die Bedingungen von Def. 4.1.1:

$\mathcal{P}(X) \neq \emptyset$ ist klar wegen $\emptyset, X \in \mathcal{P}(X)$.

$\Delta: \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ ist zudem wohldefiniert, denn $(A \setminus B) \cup (B \setminus A) \subseteq A \cup B \subseteq X \quad \forall A, B \subseteq X$.

zu Axiom (1): (Assoziativität)

z.z.: $(A \Delta B) \Delta C = A \Delta (B \Delta C) \quad \forall A, B, C \subseteq X$.

Um dies z.z., benutzen wir eine Wahrheitstabelle. Dazu betrachte man ein beliebiges Element $z \in X$. Der Eintrag 0 bedeutet, dass z kein Element der jeweiligen Menge ist. Beim Eintrag 1 ist z Element der Menge.

A	B	C	$A \Delta B$	$B \Delta C$	$(A \Delta B) \Delta C$	$A \Delta (B \Delta C)$
0	0	0	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	1	1
0	0	1	0	1	1	1
1	1	0	0	1	0	0
1	0	1	1	1	0	0
0	1	1	1	0	0	0
1	1	1	0	0	1	1

alle möglichen Kombinationen — Zwischenrechnung — $\Rightarrow$ Gleichheit der Mengen zu Axiom (2): (neutrales Element)

z.z.: $\exists\, E \in \mathcal{P}(X)$ mit $E \triangle A = A \triangle E = A \quad \forall A \in \mathcal{P}(X)$

Da $\triangle$ symmetrisch ist, reicht es, $E \triangle A = A$ sicher zustellen:

$$E \triangle A \overset{\forall}{\underset{=}{\overset{?}{}}} A \iff (E \setminus A) \cup (A \setminus E) \overset{?}{=} A \qquad (\forall A \in \mathcal{P}(X))$$

Für $E := \emptyset$ gilt:

$$(\emptyset \setminus A) \cup (A \setminus \emptyset) = \emptyset \cup A = A \qquad (\forall A \in \mathcal{P}(X))$$

Somit ist $\emptyset$ das neutrale Element.

zu Axiom (3): (inverses Element)

z.z.: $\forall A \in \mathcal{P}(X)\ \exists\, B \in \mathcal{P}(X)$ mit $A \triangle B = B \triangle A = \emptyset$

Aus Symm.gründen reicht es, $A \triangle B = \emptyset$ zu betrachten:

$$(A \setminus B) \cup (B \setminus A) = \emptyset \iff A \setminus B = \emptyset \text{ und } B \setminus A = \emptyset$$

$$\iff A \subseteq B \text{ und } B \subseteq A \iff A = B$$

Somit ist das inverse Element gefunden.

$\square$

Aufgabe 2:

(a) geg.: Ring K

z.z.: $M(2, K)$ bildet zusammen mit

2x2 Matrizen mit Einträgen aus K

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} \quad \text{und}$$

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}$$

einen Ring.

Wir zeigen die Axiome aus Def. 9.1.1.

Axiome A1 - A4: (Gruppe bzgl. +)

Folgt sofort aus der komponentenweisen Addition der Matrixeinträge und der Tatsache, dass K als Ring zusammen mit seiner Addition eine Gruppe bildet.

<u>Axiom M1:</u> (Assoziativität bzg. „$\cdot$")

Seien $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \in M(2,K)$. Dann gilt:

$$\left(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}\right) \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} = \begin{pmatrix} a_1 b_1 + a_2 b_3 & a_1 b_2 + a_2 b_4 \\ a_3 b_1 + a_4 b_3 & a_3 b_2 + a_4 b_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$

$$= \begin{pmatrix} \overbrace{a_1 b_1 c_1 + a_2 b_3 c_1 + a_1 b_2 c_3 + a_2 b_4 c_3}^{=: *_1} & *_2 \\ *_3 & *_4 \end{pmatrix}$$

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \left(\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}\right) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \left(\begin{pmatrix} b_1 c_1 + b_2 c_3 & b_1 c_2 + b_2 c_4 \\ b_3 c_1 + b_4 c_3 & b_3 c_2 + b_4 c_4 \end{pmatrix}\right)$$

$$= \begin{pmatrix} \underbrace{a_1 b_1 c_1 + a_1 b_2 c_3 + a_2 b_3 c_1 + a_2 b_4 c_3}_{=: \tilde{*}_1} & \tilde{*}_2 \\ \tilde{*}_3 & \tilde{*}_4 \end{pmatrix}$$

Auf diese Weise berechnet man $*_i = \tilde{*}_i \quad \forall i \in \{1,2,3,4\}$

<u>Axiom D1:</u> (Linkes Distributivgesetz)

Seien $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \in M(2,K)$

Dann gilt:

$$\begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \cdot \left(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}\right) = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix}$$

$$= \begin{pmatrix} c_1 a_1 + c_1 b_1 + c_2 a_3 + c_2 b_3 & c_1 a_2 + c_1 b_2 + c_2 a_4 + c_2 b_4 \\ c_3 a_1 + c_3 b_1 + c_4 a_3 + c_4 b_3 & c_3 a_2 + c_3 b_2 + c_4 a_4 + c_4 b_4 \end{pmatrix}$$

und

$$\begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} c_1 a_1 + c_2 a_3 & c_1 a_2 + c_2 a_4 \\ c_3 a_1 + c_4 a_3 & c_3 a_2 + c_4 a_4 \end{pmatrix}$$

$$+ \begin{pmatrix} c_1 b_1 + c_2 b_3 & c_1 b_2 + c_2 b_4 \\ c_3 b_1 + c_4 b_3 & c_3 b_2 + c_4 b_4 \end{pmatrix}$$

$$= \begin{pmatrix} c_1 a_1 + c_2 a_3 + c_1 b_1 + c_2 b_3 & c_1 a_2 + c_2 a_4 + c_1 b_2 + c_2 b_4 \\ c_3 a_1 + c_4 a_3 + c_3 b_1 + c_4 b_3 & c_3 a_2 + c_4 a_4 + c_3 b_2 + c_4 b_4 \end{pmatrix}$$

„="

<u>Axiom D2:</u> (rechtes Distributivgesetz)

analog zu D1

b) geg.: $K \neq \{0\}$

ges.: $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in M(2,K)$

mit $a_i \neq 0 \neq b_i \ \forall i \in \{1,2,3,4\}$

und $A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

existent wegen $K \neq \{0\}$

Wir wählen $a_i = x \neq 0 \ \forall i \in \{1,2,3,4\}$. Dann gilt

$$A \cdot B \underset{K \text{ Ring}}{=} \begin{pmatrix} x(b_1+b_3) & x(b_2+b_4) \\ x(b_1+b_3) & x(b_2+b_4) \end{pmatrix} \overset{!}{=} 0.$$

Dies ist erfüllt für $b_3 = -b_1$, $b_4 = -b_2$

Wähle $b_1 = b_2 = x$:

Schließlich gilt:

$$A \cdot B = \begin{pmatrix} x & x \\ x & x \end{pmatrix} \cdot \begin{pmatrix} x & x \\ -x & -x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Aufgabe 3:

geg.: K kommutativer Ring, I, J Ideale in K

z.z.: $I + J := \{i + j \mid i \in I, j \in J\}$ und $I \cap J$ sind Ideale in K

Wir zeigen jeweils die Axiome 1) und 2) aus Def. 9.1.4: (Wegen $0 \in I$, $0 \in J$ sind $I+J$ und $I \cap J$ nicht leer)

Inverses bzgl. +
I, J Ideale $\Rightarrow \exists x \in I, y \in J$
$\Rightarrow x - x = 0 \in I$, $y - y = 0 \in J$

$I + J$:

zu 1): geg.: $a, b \in I + J$

z.z.: $a - b \in I + J$

$a, b \in I + J \Rightarrow \exists i_1, i_2 \in I, j_1, j_2 \in J$ mit

$$a = i_1 + j_1, \quad b = i_2 + j_2$$

Es gilt:

$$a - b = i_1 + j_1 - i_2 - j_2 \underset{K \text{ komm. Ring}}{=} \underbrace{(i_1 - i_2)}_{=: i_3} + \underbrace{(j_1 - j_2)}_{=: j_3}$$

Da I und J jeweils Ideale sind, gilt nach Def. 9.1.4 1): $i_3 \in I$, $j_3 \in J$

$\Rightarrow a - b = i_3 + j_3 \in I + J$

zu 2): geg.: $a \in I + J$, $b \in K$ z.z.: $a \cdot b \in I + J$

Sei $a = i_1 + j_1$ mit $i_1 \in I$, $j_1 \in J$

Es gilt

$$a \cdot b = (i_1 + j_1) \cdot b \underset{\substack{\uparrow \\ K \text{ Ring (Axiom D2)}}}{=} \overbrace{i_1 \cdot b}^{=: i_2} + \overbrace{j_1 \cdot b}^{=: j_2}$$

Da I, J Jdeale sind; gilt nach Def 9.1.4 2):

$i_2 \in I$, $j_2 \in I$ $\Rightarrow$ $a \cdot b \in I + J$

<u>$I \cap J$:</u>

zu 1): geg.: $a, b \in I \cap J$ z.z.: $a - b \in I \cap J$

$$\begin{array}{ccccc} & \nearrow & a,b \in I \underset{I \text{ Jdeal}}{\Longrightarrow} a-b \in I & \searrow & \\ a,b \in I \cap J & & & & a-b \in I \cap J \\ & \searrow & a,b \in J \underset{J \text{ Jdeal}}{\Longrightarrow} a-b \in J & \nearrow & \end{array}$$

zu 2): geg.: $a \in I \cap J$, $b \in K$. z.z.: $a \cdot b \in I \cap J$

$$\begin{array}{ccccc} & \nearrow & a \in I \underset{I \text{ Jdeal}}{\Longrightarrow} a \cdot b \in I & \searrow & \\ a \in I \cap J & & & & a \cdot b \in I \cap J \\ & \searrow & a \in J \underset{J \text{ Jdeal}}{\Longrightarrow} a \cdot b \in J & \nearrow & \end{array}$$

<u>Aufgabe 4:</u>

(a) ges.: $ggT(162, 126)$ unter Verwendung des Eukl. Alg.

Es gilt:
$$\begin{aligned} 162 &= 1 \cdot 126 + 36 \\ 126 &= 3 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 + 0 \end{aligned}$$

Laut Satz 10.1.3 gilt:

$ggT(162, 126) = 18$

b) ges.: $x, y \in \mathbb{Z}$ mit $x \cdot 162 + y \cdot 126 = ggT(162, 126)$
Wir verfahren wie im Bsp. nach Satz 10.1.4:

$$\begin{aligned} 18 &= 126 - 3 \cdot 36 \\ &= 126 - 3 \cdot (162 - 1 \cdot 126) \\ &= \underbrace{-3}_{=:x} \cdot 162 + \underbrace{4}_{=:y} \cdot 126 \end{aligned}$$

<u>Aufgabe 5:</u>

(a) Existiert ein Inverses zu 45 bzgl. $\cdot_{60}$ im Ring $(\mathbb{Z}_{60}, +_{60}, \cdot_{60})$?

Angenommen ein solches Inverses x zu 45 bzgl. $\cdot_{60}$ existiert, dann gilt:

$$45 \cdot_{60} x = 1 \pmod{60}$$

Also gilt in $\mathbb{Z}$ für ein $k \in \mathbb{Z}$:

$$\underbrace{45 \cdot x}_{\text{durch 5 teilbar}} = \underbrace{1 + k \cdot 60}_{\text{nicht durch 5 teilbar}}$$

↯ Widerspruch

$\Rightarrow$ Es gibt kein solches Inverses.

<u>Bem.:</u> Es lässt sich zeigen, dass zu einem Element m im Ring $(\mathbb{Z}_n, +_n, \cdot_n)$ genau dann ein Inverses bzgl. $\cdot_n$ existiert, wenn $ggT(m, n) = 1$ gilt.

b) ges.: multipl. Inverses zu 17 bzgl. $\cdot_{60}$

Also ist $x \in (\mathbb{Z}_{60}, +_{60}, \cdot_{60})$ ges. mit

$$17 \cdot_{60} x = 1 \pmod{60}$$

$\Leftrightarrow$ ges.: $x, k \in \mathbb{Z}$ mit

$$17x = 1 + 60k$$

$$\Leftrightarrow \quad 17x + 60\overbrace{(-k)}^{=:y} = 1$$

Wegen ggT(60, 17) = 1 existieren laut Satz 10.1.4 solche Elemente $x, y \in \mathbb{Z}$. Wir berechnen analog zum Bsp. aus dem Skript.

$$60 = 3 \cdot 17 + 9$$
$$17 = 1 \cdot 9 + 8$$
$$9 = 1 \cdot 8 + 1$$
$$8 = 8 \cdot 1 + 0$$

Somit

$$1 = 9 - 1 \cdot 8 = 9 - 17 + 9 = 2 \cdot 9 - 17$$
$$= 2(60 - 3 \cdot 17) - 17$$
$$= 2 \cdot 60 \underbrace{- 7}_{=x} \cdot 17$$

Somit ist $-7 =_{60} 53$ das multiplikative Inverse zu 17

4/4