Feruzan Ay (ayferuzan@yahoo.de)
Marco Kunze (makunze@cs.tu-berlin.de)
Sebastian Nowozin (nowozin@cs.tu-berlin.de)

SS 2003
22. 6. 2003

Lösungen zum 5. Übungsblatt
Diskrete und strukturelle Mathematik für Informatiker

Lösung zu Aufgabe 1:

a)

$$a \circ e \stackrel{G3}{=} a \circ (a' \circ a) \stackrel{G1}{=} (a \circ a') \circ a \stackrel{1b)}{=} e \circ a \stackrel{G2}{=} a$$

b) Wegen G3 wissen wir, dass $a' \circ a = e$ ist. Also zu zeigen: $a \circ a' = e$
Sei $x = a'$;

$$\begin{aligned} a \circ a' &= a \circ x \\ &\stackrel{G2}{=} e \circ (a \circ x) \\ &\stackrel{G3}{=} (x' \circ x) \circ (a \circ x) \\ &\stackrel{G1}{=} x' \circ (x \circ (a \circ x) \\ &\stackrel{G1}{=} x' \circ ((x \circ a) \circ x)) \\ &\stackrel{G2}{=} x' \circ (e \circ x) \\ &\stackrel{G2}{=} x' \circ x \\ &\stackrel{G3}{=} e \end{aligned}$$

c)

$$a \circ b = e \stackrel{G3}{=} a' \circ a \stackrel{1b)}{=} a \circ a' \Rightarrow b = a'$$

$$a \circ b = e \stackrel{G3}{=} b' \circ b \Rightarrow b' = a$$

d) $\forall a, c \in G$ gibt es genau ein $b \in G$ mit $a \circ b = c$

- **Existenz:** $\forall a, c \in G\ \exists\ b \in G$ mit $a \circ b = c$
  Sei $b = a' \circ c$. Durch Verknüpfung mit a von der linken Seite erhält man

  $$a \circ b = a \circ (a' \circ c) \stackrel{G1}{=} (a \circ a') \circ c \stackrel{G3}{=} e \circ c \stackrel{G2}{=} c$$

  Also es existiert ein b, das $a \circ b = c$ erfüllt.
- **Eindeutigkeit:**
  Sei $b_1, b_2 \in G$ und $b_1 \neq b_2$ so, dass $a \circ b_1 = c$ und $a \circ b_2 = c$ erfüllt.

Also

$$\begin{array}{rcll} a \circ b_1 & = & a \circ b_2 & \text{(Verknüpfung mit } a' \text{ von der linken Seite)} \\ a' \circ (a \circ b_1) & = & a' \circ (a \circ b_2) & \text{(G1)} \\ (a' \circ a) \circ b_1 & = & (a' \circ a) \circ b_2 & \text{(G3)} \\ e \circ b_1 & = & e \circ b_2 & \text{(G2)} \\ b_1 & = & b_2 & \end{array}$$

Das führt aber zum Widerspruch unserer Annahme, also es existiert genau ein b, das $a \circ b = c$ erfüllt.

Lösung zu Aufgabe 2:

a) Wir definieren den Ring mit der Menge $R = \{\nabla, \triangle, \Box, \Diamond\}$ und mit $\bowtie$ als Multiplikation und $\oslash$ als Addition.

1. Abgeschlossenheit
   Wie leicht zu sehen ist, bilden alle Operationen
   $$R \times R \to R$$
   ab. Damit ist (1) und (2) aus dem Skript erfüllt.
2. Zu (3), Assoziativität bzgl. Addition
   Zunächst ist zu klären, welche Operation die Addition ist.
   Sollte $\bowtie$ die Addition sein, so käme als einziges 0-Element $\Box$ in Frage, da es alle Elemente auf sie selbst zurück abbildet. Da aber auch zu jedem Element ein inverses geben muss, müsste es ein $x \in R$ geben mit $x \bowtie \nabla = \Box$. Dieses ist nicht der Fall, also muss $\oslash$ die Addition darstellen. Hier lässt sich auch $\triangle$ als 0-Element feststellen.
   Man kann durch Überprüfen aller 64 Möglichkeiten feststellen, dass die Assoziativität gegeben ist.
3. Zu (4), Kommutativität bzgl. Addition
   Wie leicht zu sehen ist (wenn man denn die Zeilen und Spalten sinnvoll sortiert und die Symbole von links oben aus in der Titelzeile und -spalte gleich angeordnet sind), ergibt sich eine Symmetrie an der Achse von der Ecke links oben zur Ecke rechts unten. Daran ist die Kommutativität bzgl. der Addition leicht zu sehen.
4. Zu (5), Neutrales Element bzgl. der Addition.
   Wie unter 2.) schon erwähnt, ist $\triangle$ das neutrale Element bzgl. der Addition, da es alle Elemente auf sie selbst zurück abbildet.
5. Zu (6), Inverses Element bzgl. der Addition.
   $$\begin{array}{rcl} \Box \oslash \Diamond & = & \triangle \\ \triangle \oslash \triangle & = & \triangle \\ \nabla \oslash \nabla & = & \triangle \end{array}$$
6. Zu (7), Assoziativität bzgl. der Multiplikation
   Man kann durch Überprüfen aller 64 Möglichkeiten feststellen, dass die Assoziativität gegeben ist.
7. Zu (8), Distributivität
   Man kann durch das Überprüfen aller Kombinationen festellen, dass die Distributivität gegeben ist.

b) Bereits gezeigt unter 2a)

c) Da die Kommutativität bzgl. der Addition bereits unter 2a3 gezeigt wurde, bleibt sie nur noch bzgl. der Multiplikation zu zeigen. Allerdings ist hier genauso wie in 2a3 zu verfahren, womit auch dieses gezeigt wäre.

d) Ja,

$$\diamondsuit \bowtie \diamondsuit = \square$$

e) Es handelt sich nicht um einen Körper, da es kein $x \in R$ gibt mit

$$\nabla \bowtie x = \square$$

, soll heißen. . .

f) . . . es fehlt das inverse Element zu ∇.

g) $\oslash$ definiert eine Gruppe, da alle Gruppeneigenschaften erfüllt sind. Man kann eine echte Teilmenge finden, nämlich $\{\nabla, \triangle\}$.

Bezüglich $\bowtie$ erhält man eine Gruppe, wenn man die Menge auf $\{\square, \diamondsuit\}$ beschränkt.

h) Man kann alle Zeichen die nicht in der Titelzeile oder -spalte stehen durch ein beliebiges Zeichen der Menge ersetzen.

Lösung zu Aufgabe 3:

a) (a) Für jeden Ring R ist R ein Ideal von R

Da die Multiplikation im Ring R definiert ist und damit R nicht verlässt, ist $r \cdot s$ mit $r \in R$, $s \in I = R$ wieder vollständig im Ring.

(b) Für $I = \{0\} \subseteq R$ ist I ein Ideal von R

Zu zeigen ist zunächst einmal, dass I ein Unterring von R ist. Sein dazu $x, y \in I$, also $x = y = 0$, da $|I| = 1$. Dann gilt durch die Definition der Eigenschaften des Nullelements: $(x + y) \in I$ und $(x \cdot y) \in I$. Also ist nach Bedingung (14) des Skripts I ein Unterring von R.

Weiter ist I ein Ideal, da $\forall r \in R, s \in I$, also $s = 0$ gilt:

$$r \cdot s = r \cdot 0 = 0 = 0 \cdot r = s \cdot r$$

und $0 \in I$ ist.

b) Der Beweis der beiden Teilrichtungen erfolgt getrennt.

Sein dazu die folgenden Aussagen definiert:

(1)	R hat zu jedem Element ungleich der Null ein Inverses
(2)	R und $\{0\}$ sind die einzigen Ideale von R
$\neg$(1)	Es gibt ein Element in $R \setminus \{0\}$ zu dem keine Inverse existiert.
$\neg$(2)	Es gibt ein Ideal I von R mit $I \neq \{0\}$ und $I \neq R$

Sei e im weiteren das Einserelement von R.

- "(1) $\Rightarrow$ (2)":

  Wir zeigen die Umkehrung, $\neg(2) \Rightarrow \neg(1)$. Dazu führen wir die Aussage $\neg(2) \Rightarrow (1)$ zu einem Widerspruch: Wenn es ein Ideal I von R mit $I \neq \{0\}$ und $I \neq R$ gibt, dann hat R zu jedem Element ungleich der Null eine Inverse.

  Sei also I ein Ideal von R mit $I \neq \{0\}$ und $I \neq R$. Nehmen wir nun ein beliebiges Element i des Ideals mit $i \neq 0$. Es gibt eine Inverse $i^{-1} \in R$, so dass $i \cdot i^{-1} = e$. Wegen der Definition des Ideals muss damit e Element des Ideals sein. Daraus folgt weiter nach der Definition des Ideals, dass für alle $r \in R$ gilt: $(r \cdot e) \in I$. Damit ist $I = R$, was zum Widerspruch führt.

Da wir die Umkehrung gezeigt haben, gilt (1) $\Rightarrow$ (2).

- "(2) $\Rightarrow$ (1)":

  Beweis durch Umkehrung der Aussage, also $\neg(1) \Rightarrow \neg(2)$: Gibt es ein Element x in $R \setminus \{0\}$, zu dem kein Inverses x^{-1} existiert so dass $x \cdot x^{-1} = e$, so muss ein Ideal I mit $I \neq R$, $I \neq \{0\}$ existieren. Das heißt

  $$\forall a \in R \setminus \{0\} : x \cdot a \neq e$$

  Dann ist der folgendermassen definierte Ring I ein Ideal von R mit $I \neq R$, $I \neq \{0\}$:

  $$\begin{aligned} I &:= (M_I, +, \cdot) \\ M_I &= \{x \cdot a | a \in R\} \end{aligned}$$

  I ist nach Bedingung (14) ein Ring, weil für $p, q \in I$, $p = x \cdot a_1$, $q = x \cdot a_2$ gilt:

  - $p \cdot q$ liegt in I

    $$p \cdot q = x \cdot a_1 \cdot x \cdot a_2 = x \cdot \underbrace{(a_1 \cdot x \cdot a_2)}_{\text{in } R \text{ definiert}} = \underbrace{x \cdot a_3}_{\text{in } M_I \text{ definiert}}$$

  - $p + q$ liegt in I

    $$p + q = x \cdot a_1 + x \cdot a_2 = x \cdot \underbrace{(a_1 + a_2)}_{\text{in } R \text{ definiert}} = \underbrace{x \cdot a_3}_{\text{in } M_I \text{ definiert}}$$

  Aber $M_I \subset M_R$, weil $M_I \cap \{e\} = \emptyset$, was zu zeigen war. Damit ist die Hinrichtung bewiesen.

Damit haben wir gezeigt, dass ein Ring R genau dann ein Körper ist, wenn R und $\{0\}$ die einzigen Ideale des Rings sind.

Lösung zu Aufgabe 4:

a) Sein $a := \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}$, $b := \begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix} \in X$ beliebig gewählt. Zu zeigen ist, dass $c := a + b$ und $d := a \cdot b$ Elemente von X sind.

Es gilt:

$$c := a + b = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ -(a_2 + b_2) & a_1 + b_1 \end{pmatrix}$$

Da mit $x = a_1 + b_1$ und $y = a_2 + b_2$ dies als $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ dargestellt werden kann, gilt $c \in X$.

Es gilt weiter:

$$d = a \cdot b = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix} = \begin{pmatrix} a_1b_1 - a_2b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1b_1 - a_2b_2 \end{pmatrix}$$

Für $x = a_1b_1 - a_2b_2$ und $y = a_1b_2 + a_2b_1$ lässt sich der Ausdruck wieder als $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ darstellen.

Es folgt nach Bedingung (14) im Skript, dass X ein Unterring von $(\mathbb{R}^{2\times 2}, +, \cdot)$ ist.

b) Es ist zu zeigen:

- $(X, +, \cdot)$ ist <u>kommutativ</u>:
  Sei $a, b \in X$ mit $a := \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}$ und $b := \begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix}$ beliebig. Wir zeigen:

$$a \cdot b = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix} = \begin{pmatrix} a_1b_1 - a_2b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1b_1 - a_2b_2 \end{pmatrix} =$$

$$\begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} = b \cdot a$$

- $(X, +, \cdot)$ <u>hat eine Eins</u> mit $1 \neq 0$.
  Sei e das Einserelement mit $e := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Dann ist für jedes $x \in X$ mit $x := \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}$:

$$1 \cdot x = x \cdot 1 = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix} = x$$

- Zu $x \in X$, $x \neq 0$ <u>existiert $x^{-1} \in X$</u> mit $x \cdot x^{-1} = 1$. (Bedingung $(11a)$ im Skript.)
  Sei $x \in X$ mit $x \neq 0$ beliebig. Dann ist für $x := \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}$:

$$x^{-1} = \begin{pmatrix} \frac{x_1}{x_1^2+x_2^2} & -\frac{x_2}{x_1^2+x_2^2} \\ \frac{x_2}{x_1^2+x_2^2} & \frac{x_1}{x_1^2+x_2^2} \end{pmatrix}$$

  das inverse Element, denn

$$x \cdot x^{-1} = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix} \cdot \begin{pmatrix} \frac{x_1}{x_1^2+x_2^2} & -\frac{x_2}{x_1^2+x_2^2} \\ \frac{x_2}{x_1^2+x_2^2} & \frac{x_1}{x_1^2+x_2^2} \end{pmatrix} = \begin{pmatrix} \left(\frac{x_1^2}{x_1^2+x_2^2} + \frac{x_2^2}{x_1^2+x_2^2}\right) & \left(-\frac{x_1x_2}{x_1^2+x_2^2} + \frac{x_1x_2}{x_1^2+x_2^2}\right) \\ \left(-\frac{x_1x_2}{x_1^2+x_2^2} + \frac{x_1x_2}{x_1^2+x_2^2}\right) & \left(\frac{x_1^2}{x_1^2+x_2^2} + \frac{x_2^2}{x_1^2+x_2^2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

- Für $x, y \in X \setminus \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}$ gilt: $x \cdot y \in X \setminus \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}$. (Bedingung $(11b)$ im Skript.)
  Sei $x := \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}$ und $y := \begin{pmatrix} y_1 & y_2 \\ -y_2 & y_1 \end{pmatrix}$. Dann ist:

$$x \cdot y = \begin{pmatrix} (x_1y_1 - x_2y_2) & (x_1y_2 + x_2y_1) \\ -(x_1y_2 + x_2y_1) & (x_1y_1 - x_2y_2) \end{pmatrix}$$

  Als Gleichungssystem aufgefasst ist zu lösen:

$$\begin{aligned} x_1y_1 - x_2y_2 &= 0 \qquad (1) \\ x_1y_2 + x_2y_1 &= 0 \qquad (2) \\ -(x_1y_2 + x_2y_1) &= 0 \qquad (3) \end{aligned}$$

  Gleichung (3) fällt weg, die zwei verbleibenden Gleichungen sind nur für $x_1 = x_2 = y_1 = y_2 = 0$ lösbar. Daher gilt $(11b)$.

Aus den bewiesenen Eigenschaften folgt, dass $(X, +, \cdot)$ ein Körper ist.

Lösung zur Zusatzaufgabe:

a) Um zu zeigen, dass $\sim_I$ eine Äquivalenzrelation auf R definiert, müssen wir zeigen, dass die Eigenschaften der *Symmetrie*, *Reflexivität* und *Transitivität* erfüllt sind.

- *Symmetrie*

  Sei $x, y \in R$ und gelte $x \sim_I y$. Dann $\exists s \in I$ mit $xs = y$. Nach Definition des Ideals ist damit $y \in I$. Dadurch ist für jedes $r \in R$ auch $ry \in I$, also erst recht für $r = x$, so daß gilt: $ys = x$. Also ist auch $y \sim_I x$.

- *Reflexivität*

  Für die Reflexivität müsste ein neutrales Element bzgl. der Addition und der Multiplikation gegeben sein. Da die Definition eines Ringes dieses aber nur für die Addition voraussetzt, jedoch nicht für die Multiplikation, konnten wir die Reflexivität nicht nachweisen.

- *Transitivität*

  Zu zeigen für $x, y, z \in R$ ist: $x \sim_I y, y \sim_I z \Rightarrow x \sim_I z$. Sei $x \sim_I y$, dann $\exists s_1 \in I$ mit $xs_1 = y$ und $\exists s_2 \in I$ mit $ys_2 = z$. Daraus folgt dass gilt: $xs_1s_2 = z$. Da für $r \in R$ nach Definition des Ideals auch $rs_2 \in I$ ist, ist für $r = s_1$ erst recht $s_1s_2 \in I$. Daher ist mit $s_3 = s_1s_2$ sofort $s_3 \in I$ und es gilt: $xs_3 = z$, also $x \sim_I z$.

b) Da die Operationen $+, \cdot$ keine Definitionslücken aufweisen, also wohldefiniert sind, bleibt nur noch zu zeigen, dass auch $\sim_I$ keine Definitionslücke enthält.

   Das ist aber explizit dadurch gegeben, dass die Äquivalenzrelation auf $\forall x, y \in R$ definiert wurde, und dass die Eigenschaft als Ideal voraussetzt, dass $\exists s \in I : xs = y$.

   Somit sind die beiden Verknüpfungen wohldefiniert.

c) TODO

d) TODO