**Aufgabe 1**

Es sei $M$ eine Menge mit $n$ Elementen. Wieviele Abbildungen von $M \times M$ nach $M$ gibt es?
Angenommen, jemand will diese Aufgabe durch Experimentieren am Rechner lösen. Um einen kleinen Überblick zu bekommen, schreibt er ein Programm, das mit Hilfe von Schleifen alle inneren Abbildungen einer Menge durchläuft und bei jeder neuen Abbildung einen Zähler hochsetzt. Nehmen wir an, daß das Programm pro Abbildung nur ein Rechnertakt benötigt, was natürlich viel zu schnell ist, aber für eine erste optimistische Abschätzung taugt. Bei einem mit 1000 MHz getakteten Rechner dauert ein Takt $10^{-9}$ Sekunden. Wie lange dauert es, bis das Programm alle inneren Abbildungen einer Menge mit 10 Elementen gezählt hat? Wie lange dauert es bei 5 Elementen? Speicherplatzprobleme und ähnliches werden nicht berücksichtigt.

**Lösung**: Ist $M$ eine endliche Menge mit $n$ Elementen, so enthält $M \times M$ genau $n^2$ Elemente,

$$|M| = n, \qquad |M \times M| = n^2.$$

Jedes der $n^2$ Elemente von $M \times M$ kann auf $n$ Werte abgebildet werden; insgesamt gibt es somit

$$\underbrace{n \cdot n \cdot \ldots \cdot n}_{n^2 \text{ Faktoren}} = n^{n^2}$$

unterschiedliche Möglichkeiten für Abbildungen von $M \times M$ nach $M$. (Man beachte, daß $n^{n^2} = n^{(n^2)}$ bedeutet.)

(a) Bei einer Menge mit 10 Elementen gibt es also $10^{100}$ Abbildungen. Wenn eine Abbildung $10^{-9}$ s braucht, benötigen alle Abbildungen $10^{100} \cdot 10^{-9}\,\mathrm{s} \approx 3{,}2 \cdot 10^{83}$ Jahre.

(b) Enthält die Menge $M$ nur 5 Elemente, gibt es $5^{25} \approx 2{,}98 \cdot 10^{17}$ Abbildungen. Dann dauert es $5^{25} \cdot 10^{-9}\,\mathrm{s} \approx 9{,}5$ Jahre.

**Aufgabe 2**

Warum liegt keine algebraische Struktur in dem von uns definierten Sinne vor bei a) den natürlichen Zahlen mit der Subtraktion, b) den reellen Zahlen mit der Division, c) dem Skalarprodukt von Vektoren?

**Lösung**: Es seien $A$ und $M$ Mengen. Eine Abbildung $f : M \times M \longrightarrow M$ heißt *innere Verknüpfung* und eine Abbildung $f : A \times M \longrightarrow M$ *äußere Verknüpfung.* Eine algebraische Struktur ist eine Menge $M$ mit mindestens einer solchen Verknüpfung.

(a) $(\mathbb{N}, -)$ ist keine algebraische Struktur, da nicht nach $\mathbb{N}$ abgebildet wird. (Zum Beispiel ist $1 - 2 = -1 \notin \mathbb{N}$.)

(b) $(\mathbb{R}, :)$ ist keine algebraische Struktur, da die Division durch Null nicht definiert ist. (Zum Beispiel ist $1/0$ ein sinnloser Ausdruck.)

(c) $(V_n, \cdot)$ ist keine algebraische Struktur, da $\vec{a} \cdot \vec{b} \in \mathbb{R}$ ist, und nicht aus $V_n$.

**Aufgabe 3**

Zeigen Sie, daß durch $f((a, b)) = a^b$ eine innere Verknüpfung der natürlichen Zahlen gegeben ist, die weder assoziativ noch kommutativ ist.

**Lösung**: Sind $a$ und $b$ natürliche Zahlen, so ist auch $a^b$ eine natürliche Zahl; also haben wir eine innere Verknüpfung. Um zu zeigen, daß diese weder assoziativ noch kommutativ ist, genügt es, Gegenbeispiele zu finden. Es ist

$$(2 * 3) * 4 = 2^3 * 4 = 8 * 4 = 8^4 = 4096,$$

aber

$$2 * (3 * 4) = 2 * 3^4 = 2 * 81 = 2^{81} \approx 2,4 \cdot 10^{24}.$$

Also ist die Verknüpfung nicht assoziativ. Wegen

$$2 * 3 = 2^3 = 8$$

und

$$3 * 2 = 3^2 = 9$$

ist die Verknüpfung auch nicht kommutativ.

**Aufgabe 4**

Es sei $\mathcal{P}(M) = \{A \mid A \subseteq M\}$ die Potenzmenge von $M$. Zeigen Sie, daß $\mathcal{P}(M)$ mit der Mengenoperation der Durchschnittsbildung zu einer assoziativen und kommutativen algebraischen Struktur wird, ebenso mit der Operation der Mengenvereinigung. Zeigen Sie, daß mit der Mengensubtraktion eine algebraische Struktur entsteht, die weder assoziativ noch kommutativ ist.

**Lösung**: Es seien $A$, $B$, $C \in \mathcal{P}(M)$. Wegen

$$\begin{aligned}(A \cap B) \cap C &= \{x \in M \,|\, x \in A \wedge x \in B\} \cap C \\ &= \{x \in M \,|\, (x \in A \wedge x \in B) \wedge x \in C\} \\ &= \{x \in M \,|\, x \in A \wedge (x \in B \wedge x \in C)\} \\ &= A \cap (B \cap C)\end{aligned}$$

ist die Durchschnittsbildung assoziativ, und wegen

$$\begin{aligned}A \cap B &= \{x \in M \,|\, x \in A \wedge x \in B\} \\ &= \{x \in M \,|\, x \in B \wedge x \in A\} \\ &= B \cap A\end{aligned}$$

ist sie auch kommutativ. Völlig analog kann man Assoziativität und Kommutativität für die Mengenvereinigung zeigen.

Die Herleitung geschieht also durch Rückführung auf die Assoziativität und Kommutativität von Und-Verknüpfungen (bzw. Oder-Verknüpfungen) in der Aussagenlogik.

Um zu zeigen, daß die Mengensubtraktion weder assoziativ noch kommutativ ist, genügt die Angabe eines Gegenbeispiels. Für die Mengen $A = \{1, 2, 3\}$ und $B = \{3\}$ aus $\mathcal{P}(\mathbb{N})$ gilt

$$A \setminus B = \{1, 2\}$$

und

$$B \setminus A = \emptyset,$$

wir haben also keine Kommutativität. Nehmen wir noch $C = \{3, 4, 5\}$ dazu, sehen wir an

$$(A \setminus B) \setminus C = \{1, 2\} \setminus C = \{1, 2\}$$

und

$$A \setminus (B \setminus C) = A \setminus \emptyset = \{1, 2, 3\},$$

daß die Mengensubtraktion auch nicht assoziativ ist.

### Aufgabe 5

Es sei $M = \{z \in \mathbb{C} \,|\, z^4 = 1\} = \{1, i, -1, -i\}$.

(a) Was ist $M \times M$ ?

(b) Warum ist die Abbildung $f((x, y)) = x + y$ mit $(x, y) \in M \times M$ keine innere Verknüpfung von $M$?

(c) Warum definiert $f((x, y)) = x \cdot y$ mit $(x, y) \in M \times M$ eine innere Verknüpfung von $M$? Stellen Sie diese Verknüpfung vollständig durch eine Tabelle dar. Zeigen Sie, daß es sich um eine abelsche Gruppe handelt.

**Lösung**:

(a) $M \times M$ ist das kartesische Produkt der Menge $M$ mit sich selbst, d.h. es ist die Menge

$$\begin{array}{rcl} M \times M & = & \{ \quad \begin{array}{rrrr} (1,1), & (1,i), & (1,-1), & (1,-i), \\ (i,1), & (i,i), & (i,-1), & (i,-i), \\ (-1,1), & (-1,i), & (-1,-1), & (-1,-i), \\ (-i,1), & (-i,i), & (-i,-1), & (-i,-i) \end{array} \quad \}, \end{array}$$

die aus 16 Paaren besteht,

$$|M \times M| = 16.$$

(b) Zum Beispiel wird $(1,1) \in M \times M$ auf $1+1=2$ abgebildet, und $2 \notin M$, d.h. die Abbildung $f$ mit $f((x,x)) = x+y$ bildet *nicht* nach $M$ ab.

(c) $f((x,y)) = xy$ ist eine Abbildung mit $f: M \times M \longrightarrow M$, wie man unmittelbar an der Verknüpfungstabelle erkennt.

| | $1$ | $i$ | $-1$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $i$ | $-1$ | $-i$ |
| $i$ | $i$ | $-1$ | $-i$ | $1$ |
| $-1$ | $-1$ | $-i$ | $1$ | $i$ |
| $-i$ | $-i$ | $1$ | $i$ | $-1$ |

Um zu zeigen, daß eine abelsche Gruppe vorliegt, müssen wir nachweisen, daß die Gruppeneigenschaften VANIK erfüllt sind.

(V) Verknüpfungsabgeschlossenheit:
Bei der multiplikativen Verknüpfung entstehen nur Elemente aus $M$ (siehe Tabelle).

(A) Assoziativität:
Für beliebige komplexe Zahlen $z_1$, $z_2$, $z_3$ gilt

$$(z_1 z_2) z_3 = z_1 (z_2 z_3),$$

also gilt das auch bei einer Teilmenge von $\mathbb{C}$.

(N) Neutrales Element:
Die 1 ist offensichtlich das neutrale Element.

(I) Inverse Elemente:

Jedes Element von $M$ hat ein inverses Element, wie unmittelbar aus der Verknüpfungstabelle abgelesen werden kann.

| Element | Inverses | Begründung |
|---|---|---|
| $1$ | $1$ | $1 \cdot 1 = 1$ |
| $i$ | $-i$ | $i \cdot (-i) = 1$ |
| $-1$ | $-1$ | $(-1) \cdot (-1) = 1$ |
| $-i$ | $i$ | $(-i) \cdot i = 1$ |

(K) Kommutativität:

Die Verknüpfungstabelle ist symmetrisch zur Hauptdiagonalen, d.h. für alle $x$, $y \in M$ gilt $xy = yx$.

Also ist $(M, \ \cdot \ )$, die Menge $M$ mit der üblichen Multiplikation im Komplexen, eine abelsche Gruppe.

**Aufgabe 6**

Für $a$, $b \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$ sei die Verknüpfung $a * b = |a - b|$ definiert. Zeigen Sie, daß damit eine algebraische Struktur entsteht, die alle Gesetze einer Gruppe außer der Assoziativität erfüllt.

**Lösung**:

(V) Verknüpfungsabgeschlossenheit.

Offensichtlich ist $|a - b| \in \mathbb{N}_0$ für alle $a$, $b \in \mathbb{N}_0$.

(A) Assoziativität.

Es gilt

$$\begin{aligned}(1 * 1) * 2 &= |1 - 1| * 2 = 0 * 2 = |0 - 2| = 2, \\ 1 * (1 * 2) &= 1 * |1 - 2| = 1 * 1 = |1 - 1| = 0.\end{aligned}$$

Die Verknüpfung ist nicht assoziativ.

(N) Neutrales Element.

Wegen

$$\begin{aligned}a * 0 &= |a - 0| = |a| = a, \\ 0 * a &= |0 - a| = |-a| = a\end{aligned}$$

ist 0 das neutrale Element.

(I) Inverse Elemente.

Jedes Element ist invers zu sich selbst, weil für alle $a \in \mathbb{N}_0$

$$a * a = |a - a| = |0| = 0$$

gilt.

(K) Kommutativität.

Da

$$a * b = |a - b| = |b - a| = b * a$$

gilt, ist die Verknüpfung kommutativ.

**Aufgabe 7**

Es sei $M$ die Menge der $(n \times n)$-Matrizen. Durch die Bedingungen

$$\begin{array}{lll} \det(A) \geq 0, & \det(A) \geq 1, & \det(A) \geq 2, \\ \det(A) < 0, & \det(A) > 0, & \det(A) = 1 \end{array}$$

werden sechs Teilmengen von $M$ definiert. Hierbei bezeichnet $\det(A)$ die Determinante der Matrix $A$.

Untersuchen Sie, welche dieser Teilmengen zusammen mit der üblichen Matrizenmultiplikation eine algebraische Struktur, eine Halbgruppe, ein Monoid oder eine Gruppe bildet.

Hinweis: Für Determinanten von $(n \times n)$-Matrizen gilt

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

**Lösung**: Es muß überprüft werden, ob Verknüpfungsabgeschlossenheit (V), Assoziativität (A), Existenz eines neutralen Elementes (N) und Existenz der inversen Elemente (I) vorliegt.

Daß die Multiplikation von Matrizen assoziativ ist, wurde in der Vorlesung erwähnt, kann also ohne Beweis übernommen werden. Ansonsten ergeben sich die folgenden Resultate.

| $\det(A)$ | (V) | (A) | (N) | (I) | |
|---|---|---|---|---|---|
| $\geq 0$ | ja | ja | ja | nein | Monoid |
| $\geq 1$ | ja | ja | ja | nein | Monoid |
| $\geq 2$ | ja | ja | nein | nein | Halbgruppe |
| $< 0$ | nein | ja | nein | nein | keine alg. Struktur |
| $> 0$ | ja | ja | ja | ja | Gruppe |
| $= 1$ | ja | ja | ja | ja | Gruppe |

Die Ergebnisse zur Verknüpfungsabgeschlossenheit ergeben sich unmittelbar aus

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

Das neutrale Element der Matrizenmultiplikation ist die Einheitsmatrix $E$, für die

$$\det(E) = 1$$

gilt. Also ist $E$ nicht in den Teilmengen mit $\det(A) \geq 2$ und $\det(A) < 0$ enthalten. Wenn kein neutrales Element existiert, macht der Begriff des inversen Elementes keinen Sinn, so daß die Eigenschaft (I) für diese beiden Teilmengen ebenfalls nicht erfüllt ist. Ebenso gilt (I) nicht bei der ersten Teilmenge, da Matrizen mit $\det(A) = 0$ nicht invertierbar sind. Bei den anderen Teilmengen ist folgendes zu beachten: Wegen

$$AA^{-1} = E$$

gilt

$$\det(AA^{-1}) = \det(E) = 1,$$

und ferner ist

$$\det(AA^{-1}) = \det(A)\det(A^{-1}).$$

Zusammen ergibt sich

$$\det(A)\det(A^{-1}) = 1,$$

woraus die Beziehung

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

für die Determinaten von $A$ und $A^{-1}$ folgt.

**Aufgabe 8**

Bestimmen Sie die Nullteiler von $(\mathbb{Z}_n, \oplus, \odot)$ für $n = 3, 4, \ldots, 10$.

**Lösung**: In der Vorlesung wurde (ohne Beweis) mitgeteilt, daß gilt:

1. $(\mathbb{Z}_n, \oplus, \odot)$ ist ein Körper. $\iff$ $n$ ist eine Primzahl.
2. Ein Körper enthält keine Nullteiler. (Das ist klar, denn sonst hätte man in $(K \setminus \{0\}, \cdot)$ keine Verknüpfungsabgeschlossenheit.)

Damit sind für $(\mathbb{Z}_n, \oplus, \odot)$ schon einige der Fälle $n = 3, 4, \ldots, 10$ erledigt: $(\mathbb{Z}_n, \oplus, \odot)$ besitzt *keine* Nullteiler für $n = 3$, $n = 5$ und $n = 7$. Die restlichen Fälle untersuchen wir einzeln.

- $n = 4$

  Für welche Werte von $a$ und $b$ aus der Menge $\{1, 2, 3\}$ ergibt die Multiplikation modulo 4 den Wert Null, d.h. für welche $a$, $b$ ist die Gleichung

  $$a \odot b = 0 \qquad \text{mit} \qquad a, b \in \{1, 2, 3\}$$

  erfüllt? Durch Ausprobieren sieht man, daß dies nur für $a = b = 2$ der Fall sein kann. Statt auszuprobieren kann man sich aber auch überlegen, daß $a \odot b = 0$ ist, wenn $a \cdot b$ durch 4 teilbar ist, also zweimal den Faktor 2 enthält, was eben nur bei $a = b = 2$ möglich ist.

  Also enthält $(\mathbb{Z}_4, \oplus, \odot)$ nur den Nullteiler 2.

- $n = 6$

  Welche Lösungen hat die Gleichung

  $$a \odot b = 0 \qquad \text{mit} \qquad a, b \in \{1, 2, 3, 4, 5\}?$$

  Es ist $a \odot b = 0$, wenn $a \cdot b$ durch 6 teilbar ist, also die Faktoren 2 und 3 enthält. Das ist bei den vier Wertepaaren

  | $a$ | 2 | 3 | 3 | 4 |
  |---|---|---|---|---|
  | $b$ | 3 | 2 | 4 | 3 |

  der Fall.

  Somit enthält $(\mathbb{Z}_6, \oplus, \odot)$ die Nullteiler 2, 3 und 4.

- $n = 8$

  Damit die Gleichung

  $$a \odot b = 0 \qquad \text{mit} \qquad a, b \in \{1, 2, 3, 4, 5, 6, 7\}$$

  erfüllt ist, muß das Produkt $a \cdot b$ durch 8 teilbar sein, also

  $$2 \cdot 2 \cdot 2 \mid ab$$

  gelten. Das ist bei den fünf Wertepaaren

  | $a$ | 2 | 4 | 4 | 4 | 6 |
  |---|---|---|---|---|---|
  | $b$ | 4 | 2 | 4 | 6 | 4 |

  der Fall.

  Also hat $(\mathbb{Z}_8, \oplus, \odot)$ die Nullteiler 2, 4 und 6.

- $n = 9$

  Für
  $$a \odot b = 0 \qquad \text{mit} \qquad a, b \in \{1, 2, 3, 4, 5, 6, 7, 8\}$$
  muß $9 \,|\, ab$ oder $3 \cdot 3 \,|\, ab$ gelten. Nur bei den Paaren

  | $a$ | 3 | 3 | 6 | 6 |
  |---|---|---|---|---|
  | $b$ | 3 | 6 | 3 | 6 |

  ist im Produkt zweimal der Primfaktor 3 enthalten.

  Die Nullteiler von $(\mathbb{Z}_9, \oplus, \odot)$ sind also 3 und 6.

- $n = 10$

  Damit
  $$a \odot b = 0 \qquad \text{mit} \qquad a, b \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
  gilt, muß das Produkt $ab$ durch 10 teilbar sein. Mit Primfaktoren geschrieben, muß
  $$2 \cdot 5 \,|\, ab$$
  gelten. Die Faktoren 2 und 5 sind beide in $ab$ enthalten, wenn wir eines der acht Paare

  | $a$ | 2 | 4 | 5 | 5 | 5 | 5 | 6 | 8 |
  |---|---|---|---|---|---|---|---|---|
  | $b$ | 5 | 5 | 2 | 4 | 6 | 8 | 5 | 5 |

  haben.

  Also hat $(\mathbb{Z}_{10}, \oplus, \odot)$ die Nullteiler 2, 4, 5, 6 und 8.

**Aufgabe 9**

Berechnen Sie über dem Körper $(\mathbb{Z}_5, \oplus, \odot)$ die Determinante und die Inverse der Matrix
$$\begin{pmatrix} 1 & 2 \\ 4 & 0 \end{pmatrix}.$$
Machen Sie für die Inverse die Probe. (Alle Rechnungen sind modulo 5 durchzuführen.)

**Lösung**: Für die Determinante gilt
$$\begin{vmatrix} 1 & 2 \\ 4 & 0 \end{vmatrix} = 1 \cdot 0 - 2 \cdot 4.$$
Nun ist aber
$$1 \cdot 0 = 0 \equiv 0 \pmod 5$$

und

$$2 \cdot 4 = 8 \equiv 3 \pmod 5.$$

Ferner ist $-3$ das additive inverse Element zu 3, also wegen

$$3 + 2 = 5 \equiv 0 \pmod 5$$

die Zahl 2. Da $0 + 2 = 2$ auch im Körper $(\mathbb{Z}_5, \oplus, \odot)$ gilt, ist schließlich

$$\begin{vmatrix} 1 & 2 \\ 4 & 0 \end{vmatrix} \equiv 2 \pmod 5.$$

Zur Berechnung der inversen Matrix kann man die Formel

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}} \cdot \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}^{T} = \frac{1}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

verwenden. Die Determinante wurde bereits berechnet. Durch $1/2$ wird die multiplikative Inverse von 2 bezeichnet. Im Körper $(\mathbb{Z}_5, \oplus, \odot)$ ist dies wegen

$$2 \cdot 3 = 6 \equiv 1 \pmod 5$$

die Zahl 3. Diese muß dann noch mit der Matrix

$$\begin{pmatrix} 0 & -2 \\ -4 & 1 \end{pmatrix}$$

multipliziert werden. Durch $-2$ und $-4$ werden dabei die additiven Inversen von 2 und 4 bezeichnet. Da

$$2 + 3 = 5 \equiv 0 \pmod 5$$

ist, haben wir $-2 = 3$, und wegen

$$4 + 1 = 5 \equiv 0 \pmod 5$$

ist $-4 = 1$. Schließlich folgt aus

$$\begin{aligned} 3 \cdot 0 = 0 &\equiv 0 \pmod 5, \\ 3 \cdot 3 = 9 &\equiv 4 \pmod 5, \\ 3 \cdot 1 = 3 &\equiv 3 \pmod 5 \end{aligned}$$

das Endergebnis

$$\begin{pmatrix} 1 & 2 \\ 4 & 0 \end{pmatrix}^{-1} = 3 \odot \begin{pmatrix} 0 & -2 \\ -4 & 1 \end{pmatrix} = 3 \odot \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 3 & 3 \end{pmatrix}.$$

Zur Probe werden die Matrizen im Körper $(\mathbb{Z}_5, \oplus, \odot)$ multipliziert; das Ergebnis ist die Einheitsmatrix.