Mathematik I für Studierende der Informatik und Wirtschaftsinformatik (Diskrete Mathematik) im Wintersemester 2017/2018

14. Dezember 2017

Definition 6.1

Es sei

$$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} := \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

die Menge der Restklassen modulo m.

Definition 6.2

Für $a, b \in \mathbb{Z}$ sei

$$[a]_m \oplus [b]_m := [a+b]_m$$

und

$$[a]_m \odot [b]_m := [a \cdot b]_m.$$

Satz 6.4

Für alle $a, b, c \in \mathbb{Z}$ gilt:

1. *Kommutativgesetz:*
   - $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$
   - $[a]_m \odot [b]_m = [b]_m \odot [a]_m$
2. *Assoziativgesetz:*
   - $([a]_m \oplus [b]_m) \oplus [c]_m = [b]_m \oplus ([a]_m \oplus [c]_m)$
   - $([a]_m \odot [b]_m) \odot [c]_m = [b]_m \odot ([a]_m \odot [c]_m)$
3. *Existenz neutraler Elemente:*
   - $[a]_m \oplus [0]_m = [a]_m$
   - $[a]_m \odot [1]_m = [a]_m$
4. *Distributivgesetz:*
   - $[a]_m \odot ([b]_m \oplus [c]_m) = ([a]_m \odot [b]_m) \oplus ([a]_m \odot [c]_m)$
5. *Existenz additiver Inverser.*
   - $[a]_m \oplus [-a]_m = [0]_m$

Beweis.

Alle diese Eigenschaften folgen leicht aus den entsprechenden Eigenschaften von $\mathbb{Z}$. Als Beispiel rechnen wir (4) nach.
Es gilt

$$[a]_m \odot ([b]_m \oplus [c]_m) = [a]_m \odot [b+c]_m = [a \cdot (b+c)]_m$$
$$= [a \cdot b + a \cdot c]_m = [a \cdot b]_m \oplus [a \cdot c]_m = ([a]_m \odot [b]_m) \oplus ([a]_m \odot [c]_m).$$

Das zeigt (4). □

Wir geben für $m = 2, 3, 4, 5$ Additionstabellen und Multiplikationstabellen an, wobei wir anstelle von $[r]_m$ zur Abkürzung r schreiben.

$m = 2$:

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

$m = 3$:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$m = 4$:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$m = 5$:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot$	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

Definition 6.5

Sei $[a]_m \in \mathbb{Z}_m$.
Ein Element $[b]_m \in \mathbb{Z}_m$ heißt *multiplikatives Inverses* von $[a]_m$, falls

$$[a]_m \cdot [b]_m = [1]_m$$

gilt.
Besitzt $[a]_m$ ein multiplikatives Inverses, so nennt man $[a]_m$ *invertierbar*.

Beispiel 6.6

$[3]_4$ ist invertierbar. Es gilt nämlich $[3]_4 \cdot [3]_4 = [9]_4 = [1]_4$.

$[2]_4$ ist nicht invertierbar, da in $\mathbb{Z}_4$ kein Element $[b]_4$ existiert, so dass $[2]_4 \cdot [b]_4 = [1]_4$ gilt.
Das liest man an der entsprechenden Multiplikationstabelle ab.

$[2]_5$ ist invertierbar. Es gilt $[2]_5 \cdot [3]_5 = [6]_5 = [1]_5$.

Satz 6.7

Ein Element von $\mathbb{Z}_m$ hat höchstens ein multiplikatives Inverses.

Beweis.

Angenommen, $[b]_m$ und $[c]_m$ sind beide multiplikative Inverse von $[a]_m$.
Dann gilt

$$\begin{aligned}[b]_m = [b]_m \cdot [1]_m &= [b]_m \cdot ([a]_m \cdot [c]_m) \\ &= ([b]_m \cdot [a]_m) \cdot [c]_m = [1]_m \cdot [c]_m = [c]_m.\end{aligned}$$

Also gibt es keine zwei verschiedenen multiplikativen Invsersen von $[a]_m$. □

Satz 6.8

Ein Element $[a]_m \in \mathbb{Z}_m$ ist genau dann invertierbar, wenn a und m teilerfremd sind.
Insbesondere ist jedes Element $[a]_p \in \mathbb{Z}_p \setminus \{[0]_p\}$ invertierbar, wenn p eine Primzahl ist.

Beweis. Sei zunächst $[a]_m \in \mathbb{Z}_m$ invertierbar. Dann existiert $[b]_m \in \mathbb{Z}_m$ mit $[a]_m \cdot [b]_m = [1]_m$. Es gilt also $ab \equiv 1 \pmod{m}$. Damit existiert ein $k \in \mathbb{Z}$ mit $ab - 1 = km$. Es folgt $ab - km = 1$. Ist $g \in \mathbb{Z}$ ein Teiler von a und m, so teilt g auch $ab - km = 1$. Damit ist g entweder 1 oder -1. Also sind a und m teilerfremd.

Nun nehmen wir an, dass a und m teilerfremd sind. Wir betrachten die Restklassen

$$[0 \cdot a]_m, [1 \cdot a]_m, \ldots, [(m-1) \cdot a]_m$$

und zeigen zunächst, dass sie paarweise verschieden sind. Seien nämlich $r, s \in \mathbb{Z}$. Angenommen $[ra]_m = [sa]_m$. Dann ist $ra - sa = (r-s)a$ durch m teilbar. Da a und m teilerfremd sind, folgt daraus, dass $r - s$ durch m teilbar ist. Also gilt $[r]_m = [s]_m$. Es folgt, dass für $r, s \in Z$ mit $r \neq s$ und $0 \leq r, s < m$ die beiden Restklassen $[ra]_m$ und $[sa]_m$ verschieden sind.

Da die m Restklassen

$$[0 \cdot a]_m, [1 \cdot a]_m, \ldots, [(m-1) \cdot a]_m$$

paarweise verschieden sind, muss die Restklasse $[1]_m$ unter ihnen sein. Also gibt es ein $b \in \mathbb{Z}$ mit $0 \leq b < m$ und $[b \cdot a]_m = [1]_m$. Es gilt also $[b]_m \cdot [a]_m = [b \cdot a]_m = [1]_m$ und damit ist $[a]_m$ invertierbar. Das beendet den Beweis von Satz 6.8.

Aus den Sätzen 6.4 und 6.8 folgt sofort das nächste Korollar.

Korollar 6.9

Ist p eine Primzahl, so ist $\mathbb{Z}_p$ ein Körper.

Satz 6.10

Seien $a, b \in \mathbb{N}$ und $d = \mathrm{ggT}(a, b)$. Dann gibt es $\lambda, \mu \in \mathbb{Z}$ mit $d = \lambda a + \mu b$.

Beweis. Wir können annehmen, dass $a \leq b$ gilt und beweisen den Satz durch vollständige Induktion über die Anzahl der Schritte, die im euklidischen Algorithmus durchgeführt werden, um $\mathrm{ggT}(a, b)$ zu berechnen.

Induktionsanfang: Wenn der euklidische Algorithmus bereits nach dem ersten Schritt terminiert, so ist a ein Teiler von b. In diesem Falle ist $\mathrm{ggT}(a, b) = a$ und es gilt $a = 1 \cdot a + 0 \cdot b$.

Induktionsschritt: Sei $n \in \mathbb{N}$ so gewählt, dass der euklidische Algorithmus zur Berechnung von $\mathrm{ggT}(a, b)$ nach n Schritten terminiert und gelte $n > 1$.
Angenommen der Satz gilt für alle $a', b' \in \mathbb{N}$, bei denen der euklidische Algorithmus nach weniger als n Schritten terminiert.

Wir führen den ersten Schritt des euklidischen Algorithmus für a und b durch und wählen $r, q \in \mathbb{Z}$ mit $b = q \cdot a + r$ und $0 \leq r < a$.
Es gilt $d = \mathrm{ggT}(a, b) = \mathrm{ggT}(r, a)$.
Nun lässt sich $\mathrm{ggT}(r, a)$ in weniger als n Schritten berechnen und nach Induktionsannahme existieren $\lambda', \mu' \in \mathbb{Z}$ mit $d = \lambda' r + \mu' a$.
Es gilt $r = b - qa$ und damit

$$d = \lambda'(b - qa) + \mu' a = \lambda' b + (\mu' - \lambda' q)a.$$

Setzt man also $\mu := \lambda'$ und $\lambda := \mu' - \lambda' q$, so ergibt sich $d = \lambda a + \mu b$.
Das beendet den Induktionsschritt und damit den Beweis des Satzes.

Man beachte, dass für teilerfremde $a, m \in \mathbb{N}$ aus Satz 6.10 folgt, dass es $b, k \in \mathbb{Z}$ gibt, so dass $1 = ab + km$ gilt.

Es folgt auf etwas andere Weise als im Satz 6.8, dass $[a]_m$ invertierbar ist, nämlich mit dem multiplikativen Inversen $[b]_m$.

Man kann den euklidischen Algorithmus also auch einsetzen, um Elemente von $\mathbb{Z}_m$ zu invertieren.

Beispiel

a) Seien $a = 228$ und $b = 294$. Es gilt:

$$\begin{aligned} 294 &= 1 \cdot 228 + 66 \\ 228 &= 3 \cdot 66 + 30 \\ 66 &= 2 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0 \end{aligned}$$

Der größte gemeinsame Teiler von 228 und 66 ist also 6. Aus der vorletzten Gleichung erhalten wir $6 = 66 - 2 \cdot 30$. Aus der zweiten Gleichung ergibt sich $30 = 228 - 3 \cdot 66$. Einsetzen liefert $6 = 66 - 2 \cdot (228 - 3 \cdot 66) = 7 \cdot 66 - 2 \cdot 228$. Die erste Gleichung liefert $66 = 294 - 1 \cdot 228$. Durch Einsetzen in $6 = 7 \cdot 66 - 2 \cdot 228$ folgt

$$6 = 7 \cdot (294 - 1 \cdot 228) - 2 \cdot 228 = 7 \cdot 294 - 9 \cdot 228.$$

b) Seien $a = 15$ und $m = 28$. Wir wollen $[a]_m$ invertieren. Der euklidische Algorithmus liefert

$$\begin{aligned} 28 &= 1 \cdot 15 + 13 \\ 15 &= 1 \cdot 13 + 2 \\ 13 &= 6 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Der größte gemeinsame Teiler von 15 und 28 ist also 1. Auflösen der Gleichung in diesem Durchlauf des euklidischen Algorithmus und Rückwärtseinsetzen liefert

$$\begin{aligned} 1 = 13 - 6 \cdot 2 = 13 - 6 \cdot (15 - 1 \cdot 13) = 7 \cdot 13 - 6 \cdot 15 \\ = 7 \cdot (28 - 1 \cdot 15) - 6 \cdot 15 = 7 \cdot 28 - 13 \cdot 15 \end{aligned}$$

Es gilt also $1 \equiv -13 \cdot 15 \pmod{28}$. Damit ist $[-13]_{28} = [15]_{28}$ das multiplikative Inverse von $[15]_{28}$ in $\mathbb{Z}_{28}$.

Für $n \in \mathbb{N}$ sei $\varphi(n)$ die Anzahl der zu n teilerfremden natürlichen Zahlen $\leq n$.

Beispiel 6.11

a) Es gilt $\varphi(1) = 1$, da $\mathrm{ggT}(1,1) = 1$ gilt und damit 1 und 1 teilerfremd sind.
b) Für eine Primzahl p ist $\varphi(p) = p - 1$, da alle kleineren natürlichen Zahlen zu p teilerfremd ist.
c) Die Zahlen $1, 5, 7, 11$ sind zu 12 teilerfremd, während $2, 3, 4, 6, 8, 9, 10$ nichttriviale gemeinsame Teiler mit 12 haben. Also ist $\varphi(12) = 4$.

d) Sind p und q Primzahlen, so gilt

$$\varphi(p \cdot q) = (p-1) \cdot (q-1) = pq - p - q + 1.$$

Eine Zahl $a \leq p \cdot q$ hat nämlich genau dann einen nichttrivialen gemeinsamen Teiler mit $p \cdot q$, wenn a ein Vielfaches von p oder q ist.
Das kleinste gemeinsame Vielfache von p und q ist $p \cdot q$.
Es gibt also p Vielfache von q und q Vielfache von p, die nicht größer als $p \cdot q$ sind.
Dabei wird das gemeinsame Vielfache $p \cdot q$ doppelt gezählt.
Insgesamt gibt es also $p + q - 1$ natürliche Zahlen $\leq p \cdot q$, die nicht zu $p \cdot q$ teilerfremd sind.
Es folgt $\varphi(p \cdot q) = (p-1) \cdot (q-1)$.

Satz 6.12 (Der Satz von Fermat-Euler)

Sei $m, n \in \mathbb{N}$ teilerfremd. Dann gilt

$$n^{\varphi(m)} \equiv 1 \,(\mathrm{mod}\, m).$$

Beweis. Seien $r_1, \ldots, r_{\varphi(m)}$ die natürlichen Zahlen $\leq m$, die zu m teilerfremd sind. Wie im Beweis von Satz 6.8 sind die Restklassen

$$[r_1 \cdot n]_m, [r_2 \cdot n]_m, \ldots, [r_{\varphi(m)} \cdot n]_m$$

paarweise verschieden. Für jedes $i \in \{1, \ldots, \varphi(m)\}$ sind r_i und n beide zu m teilerfremd. Es folgt, dass auch $r_i \cdot n$ zu m teilerfremd ist. Also gilt

$$\{[r_1 \cdot n]_m, [r_2 \cdot n]_m, \ldots, [r_{\varphi(m)} \cdot n]_m\} = \{[r_1]_m, [r_2]_m, \ldots, [r_{\varphi(m)}]_m\}$$

und damit auch

$$[r_1 \cdot n]_m \cdot [r_2 \cdot n]_m \cdot \ldots \cdot [r_{\varphi(m)} \cdot n]_m = [r_1]_m \cdot [r_2]_m \cdot \ldots \cdot [r_{\varphi(m)}]_m.$$

Daher gilt für $v = r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}$ die Kongruenz

$$v \equiv (r_1 \cdot n) \cdot (r_2 \cdot n) \cdot \ldots \cdot (r_{\varphi(m)} \cdot n) \equiv v \cdot n^{\varphi(m)} \pmod{m}.$$

Da v ein Produkt von zu m teilerfremden Zahlen ist, ist auch v selbst zu m teilerfremd. Also ist $[v]_m$ nach Satz 6.8 invertierbar und es existiert $[b]_m \in \mathbb{Z}_m$ mit $[b]_m \cdot [v]_m = [1]_m$. Multiplikation der Gleichung $[v]_m = [v \cdot n^{\varphi(m)}]_m$ mit $[b]_m$ liefert $[1]_m = [n^{\varphi(m)}]_m$, also $n^{\varphi(m)} \equiv 1 \pmod{m}$. Das beendet den Beweis.

Korollar 6.13 (Der kleine Satz von Fermat)

Sei $n \in \mathbb{N}$ und p eine Primzahl, die n nicht teilt. Dann gilt

$$n^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

RSA-Verschlüsselungsverfahren

Die *RSA-Verschlüsselung* wurde 1977 von den Mathematikern Rivest, Shamir und Adleman entwickelt und ist immer noch wichtiger Bestandteil heute gängiger Verschlüsselungsmethoden.
Dabei wird ein Nachrichtentext vom Sender zunächst auf irgendeine sinnvolle Weise als natürliche Zahl m kodiert, so dass sich die Nachricht vom Empfänger aus m leicht wieder dekodieren lässt.
Uns interessiert nur, wie wir nun die Zahl m verschlüsseln und an den Empfänger versenden können, ohne dass Dritte die Nachricht entschlüsseln können.

Es gibt beim RSA-Verfahren zwei Schlüssel, einen *öffentlichen Schlüssel* (*public key*) und einen *privaten Schlüssel* (*private key*). Die beiden Schlüssel werden vom Empfänger der Nachricht erzeugt. Nur der öffentliche Schlüssel wird an den Sender weitergeleitet. Der private Schlüssel ist nur dem Empfänger bekannt. Es ist dabei unwichtig, ob der öffentliche Schlüssel Dritten bekannt wird.

Der öffentliche Schlüssel ist ein Zahlenpaar (e, N) und der private Schlüssel ein Zahlenpaar (d, N), wobei N in beiden Fällen dieselbe Zahl ist.
Man nennt N den *RSA-Modul*, e den *Verschlüsselungsexponenten* und d den *Entschlüsselungsexponenten*.

Die Schlüssel werde wie folgt erzeugt:

1. Wähle zufällig zwei verschiedene Primzahlen p und q.
2. Berechne den RSA-Modul $N = p \cdot q$.
3. Berechne $\varphi(N) = (p-1) \cdot (q-1)$.
4. Wähle eine zu $\phi(N)$ teilerfremde Zahl e mit $1 < e < \varphi(N)$.
5. Berechne das multiplikative Inverse $[d]_{\varphi(N)}$ von $[e]_{\varphi(N)}$.

Die Zahlen p, q und $\varphi(N)$ werden nun nicht mehr benötigt und können gelöscht werden. Die Zahl m, die verschlüsselt werden soll, muss kleiner als das RSA-Modul N sein.

Verschlüsselt wird nun wie folgt:
Der Sender benutzt den öffentlichen Schlüssel (e, N) und berechnet $[m^e]_N$. Die Restklasse $[m^e]_N$ wird dann in Form eines Repräsentanten zwischen 0 und N angegeben und an den Empfänger übermittelt.
Ohne Kenntnis des privaten Schlüssels (d, N) lässt sich m nicht in sinnvoller Zeit aus $[m^e]_N$ rekonstruieren, obwohl man ja eigentlich nur in $\mathbb{Z}_N$ die e-te Wurzel aus $[m^e]_N$ ziehen muss. Aber das geht eben nicht innerhalb eines sinnvollen Zeitrahmens.

Der Empfänger benutzt den privaten Schlüssel (d, N) und berechnet $[(m^e)^d]_N$. Das geht wiederum schnell, da Potenzieren auch in $\mathbb{Z}_N$ einfach ist.
Wegen

$$e \cdot d \equiv 1 \,(\mathrm{mod}\, \varphi(N)$$

existiert ein $q \in \mathbb{Z}$ mit $e \cdot d = q \cdot \varphi(N) + 1$.
Nach Satz 6.12 gilt

$$(m^e)^d \equiv m^{e \cdot d} \equiv m^{q \cdot \varphi(N)+1} \equiv (m^{\varphi(N)})^q \cdot m \equiv 1^q \cdot m \equiv m \,(\mathrm{mod}\, N)$$

und damit $[(m^e)^d]_N = [m]_N$.
Damit ist die Nachricht entschlüsselt.

In der Praxis werden noch diverse weitere Forderungen an p, q und e gestellt, damit das Verfahren effizient und sicher durchgeführt werden kann.
Man beachte, dass man den privaten Schlüssel (d, N) aus (e, N) berechnen kann, indem man N in seine Primfaktoren p und q zerlegt.
Das dauert aber zu lange, wenn p und q ausreichend groß sind.
Im September 2009 wurde eine 232-stellige Zahl (768 Bits) mit einem Rechenaufwand von mehreren Jahren auf hunderten von Rechnern in ihre Primfaktoren zerlegt.
Eine gängige Größe für RSA-Moduln sind 1024 Bit, also etwa 300 Dezimalstellen. Selbst diese Schlüsselgröße wird aber inzwischen nicht mehr für absolut sicher gehalten.

Beispiel 6.14

Wir wählen die zwei Primzahlen $p = 11$ und $q = 13$.
Das liefert den RSA-Modul $N = 143$.
Es gilt $\varphi(N) = (p-1) \cdot (q-1) = 10 \cdot 12 = 120$.
Die Zahl $e = 23$ ist zu 120 teilerfremd.
Wir wählen $(23, 143)$ als den öffentlichen Schlüssel.
Mit dem euklidischen Algorithmus bestimmen wir das multiplikative Inverse von $[23]_{120}$ in $\mathbb{Z}_{120}$.
Es gilt $\mathrm{ggT}(23, 120) = 1 = 23 \cdot 47 - 9 \cdot 120$. Damit ist $23 \cdot 47 \equiv 1 \,(\mathrm{mod}\, 120)$ und wir setzen $d = 47$. Der private Schlüssel ist also $(47, 143)$.

Angenommen, die Zahl 7 soll verschlüsselt werden.
Es gilt

$$7^{23} \mod 143 = 2736874734008091634 3 \mod 143 = 2.$$

Die verschlüsselte Nachricht ist also 2.

Zum Entschlüsseln müssen wir mit $d = 47$ potenzieren.
Es gilt

$$2^{47} \mod 143 = 140737488355328 \mod 143 = 7.$$

Algebraische Strukturen

Einfache Strukturen

Definition 7.1

Eine algebraische Struktur ist eine Menge M zusammen mit endlich vielen endlichstelligen Operationen $f_1, \ldots, f_k$ auf M. Formal schreibt man für die algebraische Struktur $\mathcal{M} = (M, f_1, \ldots, f_k)$. Dabei heißt M die $\mathcal{M}$ *unterliegende Menge*. Oft wird jedoch nicht zwischen einer algebraischen Struktur und ihrer unterliegenden Menge unterschieden. So bezeichnet $\mathbb{R}$ sowohl die Menge der reellen Zahlen als auch die algebraische Struktur $(\mathbb{R}, +, \cdot)$.

Beispiel 7.2

1. Ein Körper ist eine Menge K zusammen mit zwei zweistelligen Operationen $+$ und $\cdot$, sodass die Axiome (K1)–(K5) erfüllt sind. Damit sind Körper algebraische Strukturen. Das gilt insbesondere für $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$.
2. $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{N}, +, \cdot)$ sind ebenfalls algebraische Strukturen.
3. Konstanten in einer Menge M kann man als 0-stellige Operationen auf M interpretieren. Damit können algebraische Strukturen auch Konstanten enthalten. So sind Boolesche Algebren algebraische Strukturen mit zwei zweistelligen Operationen $\sqcup$ und $\sqcap$ sowie einer einstelligen Operation $\neg$ und zwei Konstanten 0 und 1.

4. Für eine Menge A sei $F(A)$ die Menge der Funktionen von A nach A. Dann ist $(F(A), \circ)$ eine algebraische Struktur. Ist $\mathcal{S}(A)$ die Menge der Bijektionen von A nach A, so ist $(\mathcal{S}(A), \circ)$ eine algebraische Struktur. Man beachte, dass die Komposition $\circ$ von Abbildungen tatsächlich eine zweistellige Operation auf $\mathcal{S}(A)$ ist, da die Komposition zweier Bijektionen wieder eine Bijektion ist.

Definition 7.3

Sei $(M, *)$ eine algebraische Struktur mit einem zweistelligen Operator $*$. Ein Element $e \in M$ wird *neutrales Element* (bezüglich $*$) genannt, falls für alle $a \in M$ gilt:

$$e * a = a * e = a$$

Beispiel 7.4

1. Die 0 ist ein neutrales Element bezüglich $+$ in $\mathbb{R}$, $\mathbb{Q}$ und $\mathbb{Z}$. In denselben Strukturen ist 1 ein neutrales Element bezüglich $\cdot$.
2. In einer Booleschen Algebra ist 1 neutral bezüglich $\sqcap$ und 0 ist neutral bezüglich $\sqcup$.
3. In $F(A)$ und $\mathcal{S}(A)$ ist die identische Abbildung

$$\mathrm{id}_A \colon A \to A; x \mapsto x$$

   ein neutrales Element bezüglich $\circ$.
4. Es gibt nicht in jeder algebraischen Struktur mit einer zweistelligen Operation ein neutrales Element. Ein Beispiel ist $(\mathbb{N}, +)$.

Lemma 1

Ist $*$ eine zweistellige Operation auf M, so gibt es höchstens ein neutrales Element bezüglich $*$.

Beweis.

Seien c und d neutrale Elemente bezüglich $*$. Dann gilt $c = c * d = d$. □

Definition 7.5

Sei $*$ eine zweistellige Operation auf M mit einem neutralen Element e. Für $a \in M$ heißt $b \in M$ *invers* zu a (bezüglich $*$), falls $a * b = b * a = e$ gilt. Falls für $a \in M$ ein $b \in M$ existiert, das zu a invers ist, so heißt a *invertierbar*.

Beispiel 7.6

1. Für jedes a in $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$ ist $-a$ das zu a inverse Element bezüglich $+$.
2. Für jedes a in $\mathbb{Q}$ oder $\mathbb{R}$ mit $a \neq 0$ ist a^{-1} das zu a inverse Element bezüglich $\cdot$.
3. Es gibt nicht in jeder algebraischen Struktur mit einer zweistelligen Operation ein neutrales Element. Sei nämlich $A = \{a \in \mathbb{N} \colon a \geq 2\}$, dann ist $(A, +)$ eine algebraische Struktur ohne ein neutrales Element bzgl. $+$.

4. Wenn ein neutrales Element existiert, muss nicht jedes Element Inverse besitzen. So besitzt 0 in $\mathbb{R}$ kein Inverses bezüglich der Multiplikation.
5. Wie wir bereits gesehen haben, hat das Element $[2]_4$ in $\mathbb{Z}_4$ kein Inverses bezüglich der Multiplikation. Andererseits ist $[3]_4$ in $\mathbb{Z}_4$ invertierbar bezüglich $\cdot$ und zu sich selbst invers.
6. Bezüglich $+$ sind alle Elemente $[a]_m$ von $\mathbb{Z}_m$ invertierbar, wobei $[-a]_m$ zu $[a]_m$ invers ist.

Definition 7.7

Es sei $(M, *)$ eine algebraische Struktur mit einer zweistelligen Verknüpfung $*$. Gilt für alle $a, b, c \in M$ das Assoziativgesetz

$$a * (b * c) = (a * b) * c,$$

so ist $(M, *)$ eine *Halbgruppe*.
Hat $(M, *)$ außerdem ein neutrales Element, so nennt man $(M, *)$ ein *Monoid*.

Beispiel 7.8

1. Die Strukturen $(\mathbb{N}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$ und $(F(A), \circ)$ sind Monoide. $(\mathbb{N}, +)$ ist jedoch kein Monoid, da es in $\mathbb{N}$ bezüglich $+$ kein neutrales Element gibt.
2. Für eine Menge A, die wir in diesem Zusammenhang *Alphabet* nennen. sei A^* die Menge aller endlichen Folgen von Zeichen aus A. Die Elemente von A^* nennen wir *Wörter* über A. Für zwei Wörter $v = a_1 \dots a_n$ und $w = b_1 \dots b_m$ definieren wir die *Verkettung* $v^\frown w$ von v und w als das Wort $a_1 \dots a_n b_1 \dots b_m$. Dann ist $(A^*, ^\frown)$ ein Monoid. Dabei ist das leere Wort das neutrale Element.

3. Ist $(K, +, \cdot)$ ein Körper, so ist sowohl $(K \setminus \{0\}, \cdot)$ als auch $(K, \cdot)$ ein Monoid.
4. Für $m \geq 2$ ist $(\mathbb{Z}_m, \cdot)$ ein Monoid. Nach **??** ist $(\mathbb{Z}_m \setminus \{[0]_m\}, \cdot)$ ein Monoid, falls m eine Primzahl ist. Ist m keine Primzahl, so ist $(\mathbb{Z}_m \setminus \{[0]_m\}, \cdot)$ nicht einmal eine algebraische Struktur. Seien nämlich $k, \ell \in \mathbb{N}$ mit $m = k \cdot \ell$ und $k, \ell \neq 1$. Dann gilt $[k]_m \cdot [\ell]_m = [k \cdot \ell]_m = [m]_m = [0]_m$. Damit sind $[k]_m$ und $[\ell]_m$ in $\mathbb{Z}_m \setminus \{[0]_m\}$, während $[k]_m \cdot [\ell]_m$ kein Element von $\mathbb{Z}_m \setminus \{[0]_m\}$ ist. In diesem Falle ist $\cdot$ also gar keine Operation auf $\mathbb{Z}_m \setminus \{[0]_m\}$.

Satz 7.9

Ist $(M, *)$ ein Monoid, so besitzt jedes Element a von M höchstens ein Inverses.

Beweis.

Der Beweis ist eine allgemeine Fassung des Beweises von Satz über die Eindeutigkeit von Inversen in $\mathbb{Z}_m$. Seien $b, c \in M$ Inverse von $a \in M$. Dann gilt

$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$ □