KAPITEL 2

Monoide

1. Verknüpfungen

DEFINITION. *Unter einer* **Verknüpfung** *auf einer nichtleeren Menge M versteht man eine Abbildung*

$$\varphi : M \times M \to M, \quad (a, b) \mapsto \varphi(a, b),$$

d.h. zwei Elementen a und b der Menge M wird ein Element $\varphi(a, b) \in M$ zugeordnet. Will man andeuten, dass man M mit der Verknüpfung φ betrachtet, schreibt man auch (M, φ).

Beispiele:

(1) Die Addition von zwei natürlichen Zahlen ist eine Verknüpfung auf der Menge der natürlichen Zahlen:
$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a + b.$$
(Zur Erinnerung: $\mathbb{N} = \{1, 2, 3, \dots\}$ und $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\} = \{0\} \cup \mathbb{N}$.)

(2) Die Multiplikation zweier natürlicher Zahlen definiert eine Verknüpfung auf $\mathbb{N}$:
$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a \cdot b.$$

(3) Das Potenzieren zweier natürlicher Zahlen liefert eine Verknüpfung auf $\mathbb{N}$:
$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a^b.$$

(4) Die Subtraktion definiert keine Verknüpfung auf $\mathbb{N}$, da die Differenz zweier natürlicher Zahlen nicht in jedem Fall eine natürliche Zahl liefert.

(5) Die Subtraktion definiert aber eine Verknüpfung auf $\mathbb{Z}$, der Menge der ganzen Zahlen:
$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto a - b.$$
(Wir schreiben dann auch $(\mathbb{Z}, -)$.)

Bemerkungen:

(1) Wir werden eine allgemeine Verknüpfung auf einer Menge M oft in der Form $a * b$ (statt $\varphi(a, b)$) schreiben. $(M, *)$ ist dann die Menge mit der Verknüpfung $*$.

(2) Damit $*$ eine Verknüpfung auf M definiert, muss $a * b$ für alle $a, b \in M$ definiert sein und $a * b \in M$ gelten. M muss also „abgeschlossen“ unter der Verknüpfung sein.

(3) Oft ist für eine Verknüpfung die **multiplikative** Schreibweise als **Produkt** sinnvoll, also $a \cdot b$ oder einfach nur ab.

(4) In vielen Situationen ist auch eine **additive Schreibweise** angebracht, also $a + b$.

(5) Ist $*$ eine Verknüpfung auf einer endlichen Menge $M = \{a_1, a_2, a_3, \dots, a_n\}$, so beschreibt man die Verknüpfung manchmal durch eine **Verknüpfungstabelle**:

$*$	a_1	a_2	a_3	$\dots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$	$\dots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$	$\dots$	$a_2 * a_n$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$	$\dots$	$a_3 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	$a_n * a_1$	$a_n * a_2$	$a_n * a_3$	$\dots$	$a_n * a_n$

Datei: alg_monoide.tex. Version vom 1.11.2023

Manche Eigenschaften einer Verknüpfung kann man auch gut an der Verknüpfungstabelle ablesen.

Beispiel: Multipliziert man die ganzen Zahlen ± 1 mit ± 1, so erhält man wieder ± 1, d.h. die Menge $\{1, -1\} \subseteq \mathbb{Z}$ ist abgeschlossen unter Multiplikation. Daher definiert die Multiplikation eine Verknüpfung auf der Menge $\{1, -1\}$, was auch durch $(\{1, -1\}, \cdot)$ beschrieben wird. Hier ist eine Verknüpfungstabelle:

$\cdot$	1	-1
1	1	-1
-1	-1	1

Verknüpfungen haben oft bestimmte Eigenschaften, für die es eigene Bezeichnungen gibt:

DEFINITION. *Sei M eine Menge mit einer Verknüpfung $* : M \times M \to M$, $(a, b) \mapsto a * b$, kurz $(M, *)$.*

(1) *Die Verknüpfung heißt* **assoziativ**, *wenn gilt*
$$a * (b * c) = (a * b) * c \text{ für alle } a, b, c \in M,$$
d.h. wenn das „Assoziativgesetz“ gilt.

(2) *Die Verknüpfung heißt* **kommutativ**, *wenn gilt*
$$a * b = b * a \text{ für alle } a, b \in M,$$
d.h. wenn das „Kommutativgesetz“ gilt.

(3) *Ein Element $e \in M$ heißt* **neutrales Element** *(oder* **Einselement***) der Verknüpfung, wenn gilt*
$$a * e = e * a = a \text{ für alle } a \in M.$$

Beispiele:

(1) Addition und Multiplikation natürlicher Zahlen sind assoziative und kommutative Verknüpfungen. (Um anzudeuten, mit welcher Verknüpfung wir $\mathbb{N}$ betrachten, schreiben wir $(\mathbb{N}, +)$ bzw $(\mathbb{N}, \cdot)$.)

(2) Potenzieren natürlicher Zahlen ist weder assoziativ noch kommutativ, was folgende Beispiele zeigen:
$$\left(2^2\right)^3 = 64, \text{ aber } 2^{\left(2^3\right)} = 256 \quad \text{und} \quad 2^3 \neq 3^2.$$

(3) Wir betrachten $(\mathbb{Z}, -)$, also $\mathbb{Z}$ mit der Subtraktion als Verknüpfung. Würde das Assoziativgesetz gelten, so hätte man $a - (b - c) = (a - b) - c$ für alle $a, b, c \in \mathbb{Z}$, was aber für $c \neq 0$ falsch ist. Ebenso gilt das Kommutativgesetz nicht, denn die Gleichung $a - b = b - a$ gilt nur dann, wenn $a = b$ ist.

(4) Die Multiplikation natürlicher Zahlen besitzt als neutrales Element die 1, denn es gilt $m \cdot 1 = 1 \cdot m = m$ für alle $m \in \mathbb{N}$.

(5) Für die Addition natürlicher Zahlen existiert kein neutrales Element, denn es gibt keine natürliche Zahl e mit $e + 2 = 2$. Dagegen ist die Addition eine Verknüpfung auf $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, die 0 als neutrales Element besitzt.

LEMMA. *Hat eine Verknüpfung $*$ auf einer Menge M ein neutrales Element e, so ist dies das einzige neutrale Element.*

Beweis: Ist e' ein neutrales Element, so gilt $e = e * e' = e' * e$ wegen der Neutralität von e' und $e' = e * e' = e' * e$ wegen der Neutralität von e, woraus sofort $e = e'$ folgt. ■

Bemerkung: Hat man eine Verknüpfungstabelle für $(M, *)$, so kann man einige Eigenschaften der Verknüpfung leicht ablesen:

- Die Verknüpfung ist kommutativ, wenn die Verknüpfungstabelle symmetrisch bezüglich der Diagonalen ist: $a_i * a_j = a_j * a_i$.

- e ist ein neutrales Element, wenn die entsprechende Zeile und Spalte so aussieht:

$*$	a_1	a_2	a_3	$\dots$	a_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
e	a_1	a_2	a_3	$\dots$	a_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$

$*$	$\dots$	e	$\dots$
a_1	$\dots$	a_1	$\dots$
a_2	$\dots$	a_2	$\dots$
a_3	$\dots$	a_3	$\dots$
$\vdots$		$\vdots$	
a_n	$\dots$	a_n	$\dots$

- Ich sehe nicht, wie man Aussagen über die Assoziativität direkt an der Verknüpfungstabelle ablesen könnte.

Beispiele: Wir betrachten eine 2-elementige Menge $M = \{\mathrm{a}, \mathrm{b}\}$ und alle möglichen Verknüpfungen, d.h. Abbildungen $f : M \times M \to M$. Man kann sich

$$f(\mathrm{a},\mathrm{a}) \in \{\mathrm{a},\mathrm{b}\}, \quad f(\mathrm{a},\mathrm{b}) \in \{\mathrm{a},\mathrm{b}\}, \quad f(\mathrm{b},\mathrm{a}) \in \{\mathrm{a},\mathrm{b}\}, \quad f(\mathrm{b},\mathrm{b}) \in \{\mathrm{a},\mathrm{b}\}$$

beliebig vorgeben, sodass es insgesamt $2^4 = 16$ Möglichkeiten gibt. Für jeden Fall haben wir untersucht, ob die Verknüpfung assoziativ, kommutativ ist, und ob es ein neutrales Element gibt.

(1)

$*$	a	b
a	a	a
b	a	a

assoziativ	ja
kommutativ	ja
neutrales Element	nein

(2)

$*$	a	b
a	b	a
b	a	a

assoziativ	nein
kommutativ	ja
neutrales Element	nein

(3)

$*$	a	b
a	a	b
b	a	a

assoziativ	nein
kommutativ	nein
neutrales Element	nein

(4)

$*$	a	b
a	a	a
b	b	a

assoziativ	nein
kommutativ	nein
neutrales Element	nein

(5)

$*$	a	b
a	a	a
b	a	b

assoziativ	ja
kommutativ	ja
neutrales Element	b

(6)

$*$	a	b
a	b	b
b	a	a

assoziativ	nein
kommutativ	nein
neutrales Element	nein

(7)

$*$	a	b
a	b	a
b	b	a

assoziativ	nein
kommutativ	nein
neutrales Element	nein

(8)

$*$	a	b
a	b	a
b	a	b

assoziativ	ja
kommutativ	ja
neutrales Element	b

(9)

$*$	a	b
a	a	b
b	b	a

assoziativ	ja
kommutativ	ja
neutrales Element	a

(10)

$*$	a	b
a	a	b
b	a	b

assoziativ	ja
kommutativ	nein
neutrales Element	nein

(11)

$*$	a	b
a	a	a
b	b	b

assoziativ	ja
kommutativ	nein
neutrales Element	nein

(12)

$*$	a	b
a	b	b
b	b	a

assoziativ	nein
kommutativ	ja
neutrales Element	nein

(13)

$*$	a	b
a	b	b
b	a	b

assoziativ	nein
kommutativ	nein
neutrales Element	nein

(14)

$*$	a	b
a	b	a
b	b	b

assoziativ	nein
kommutativ	nein
neutrales Element	nein

(15)

$*$	a	b
a	a	b
b	b	b

assoziativ	ja
kommutativ	ja
neutrales Element	a

(16)

$*$	a	b
a	b	b
b	b	b

assoziativ	ja
kommutativ	ja
neutrales Element	nein

In der Vorlesung spielen assoziative Verknüpfungen, die ein neutrales Element besitzen, eine wichtige Rolle. Sie haben einen eigenen Namen.

2. Monoide

DEFINITION. *Eine Menge M zusammen mit einer Verknüpfung $*$, also $(M, *)$ wird ein* **Monoid** *genannt, wenn die Verknüpfung assoziativ ist und ein neutrales Element besitzt. (Wir haben bereits gesehen, dass das neutrale Element dann eindeutig bestimmt ist.) Das Monoid wird* **kommutativ** *genannt, wenn die Verknüpfung kommutativ ist.*

Beispiele:

(1) $(\mathbb{N}, +)$ ist kein Monoid, da es kein neutrales Element bezüglich der Addition gibt. Dagegen ist $(\mathbb{N}_0, +)$ ein (kommutatives) Monoid mit der 0 als neutralem Element.
(2) Ist K ein Körper - wie $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$, so ist $(K, +)$ ein kommutatives Monoid bezüglich der Addition mit neutralem Element 0 und $(K, \cdot)$ ein kommutatives Monoid bezüglich der Multiplikation mit neutralem Element 1.

Bemerkung: Da die Verknüpfung $*$ eines Monoids $(M, *)$ assoziativ ist, d.h. es gilt

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

kann man auch die „Klammern weglassen“, d.h. man kann

$$a * b * c$$

schreiben. Dies verallgemeinert sich dann auch auf n Elemente:

$$a_1 * a_2 * \cdots * a_n.$$

Bemerkungen: Häufig wird die Verknüpfung eines Monoids als Multiplikation oder Addition geschrieben.

(1) Schreibt man die Verknüpfung eines Monoids als Multiplikation, so spricht man auch von einem **multiplikativ geschriebenen Monoid**. Dann ist die Verknüpfung $(a, b) \mapsto a \cdot b$ oder einfach $(a, b) \mapsto ab$. Das neutrale Element wird häufig e oder 1 geschrieben. Also:

$$a(bc) = (ab)c \quad \text{und} \quad ae = ea = a \text{ bzw. } a \cdot 1 = 1 \cdot a = a.$$

Die Verknüpfung von n Elementen schreibt man als Produkt

$$a_1 \cdot a_2 \cdot \cdots \cdot a_n \quad \text{oder} \quad \prod_{i=1}^{n} a_i.$$

(2) Schreibt man die Verknüpfung als Addition, so sprechen wir auch von einem **additiv geschriebenen Monoid**. Die Verknüpfung ist $(a, b) \mapsto a + b$. Das neutrale Element wird meist als 0 beschrieben. Also:

$$a + (b + c) = (a + b) + c \quad \text{und} \quad a + 0 = 0 + a = a.$$

Die Verknüpfung von n Elementen schreibt man als Summe

$$a_1 + a_2 + \cdots + a_n \quad \text{oder} \quad \sum_{i=1}^{n} a_i.$$

Verwendet man eine additive Schreibweise, ist das Monoid meist kommutativ.

Oft ist das Assoziativgesetz automatisch erfüllt, wenn man es mit Abbildungen zu tun hat. Dies geht aus dem Beweis des nachfolgenden Satzes hervor.

Satz. *Sei M eine nichtleere Menge und $\mathrm{Abb}(M, M) = \{f : M \to M\}$ die Menge aller Abbildungen von M in M. Die Hintereinanderausführung von Abbildungen, d.h.*

$$\mathrm{Abb}(M, M) \times \mathrm{Abb}(M, M) \to \mathrm{Abb}(M, M) \quad (f, g) \mapsto f \circ g \text{ mit } (f \circ g)(x) = f(g(x))$$

definiert dann eine assoziative Verknüpfung auf $\mathrm{Abb}(M, M)$ und hat als neutrales Element id_M (mit $\mathrm{id}_M(x) = x$). Insbesondere ist dann $(\mathrm{Abb}(M, M), \circ)$ ein Monoid.

Beweis: Für alle $x \in M$ gilt

$$\begin{aligned} ((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) = f(g(h(x))), \\ (f \circ (g \circ h))(x) &= f(g \circ h)(x) = f(g(h(x))), \end{aligned}$$

also $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$, und damit

$$(f \circ g) \circ h = f \circ (g \circ h).$$

Weiter folgt aus

$$(f \circ \mathrm{id}_M)(x) = f(\mathrm{id}_M(x)) = f(x) = \mathrm{id}_M(f(x)) = (\mathrm{id}_M \circ f)(x)$$

sofort

$$f \circ \mathrm{id}_M = \mathrm{id}_M \circ f = f.$$

Dies war zu zeigen. ■

Beispiel: Wir betrachten das Monoid $(\mathrm{Abb}(\{0,1\},\{0,1\}),\circ)$. Ein Element $f \in \mathrm{Abb}(\{0,1\},\{0,1\})$ beschreiben wir durch eine Tabelle:

$$f = \begin{pmatrix} 0 & 1 \\ f(0) & f(1) \end{pmatrix}.$$

Die 4 Elemente von $\mathrm{Abb}(\{0,1\},\{0,1\})$ sind dann

$$f_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \mathrm{id}_{\{0,1\}}, \quad f_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Die zugehörige Verknüpfungstabelle ist

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_1	f_1	f_1
f_2	f_1	f_2	f_3	f_4
f_3	f_4	f_3	f_2	f_1
f_4	f_4	f_4	f_4	f_4

Man sieht, dass f_2 das neutrale Element und das Monoid nicht kommutativ ist.

Beispiele aus der Linearen Algebra: Wir erinnern noch an Verknüpfungen, die in der Linearen Algebra behandelt wurden. Dabei sei K ein Körper (wie $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$).

(1) **Vektoraddition** $(K^n,+)$**:** Die Menge der Spaltenvektoren mit n Einträgen

$$K^n = \{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_1,\dots,a_n \in K\}$$

wird mit der komponentenweisen Addition

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{pmatrix}$$

zu einem kommutativen Monoid mit dem Nullvektor $0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in K^n$ als neutralem Element.

(2) **Matrizenaddition** $(\mathrm{Mat}(m\times n,K),+)$ **oder** $(K^{m\times n},+)$**:** Matrizen gleicher Gestalt kann man addieren, d.h. die Addition von Matrizen liefert eine Verknüpfung:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ \vdots & & \vdots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}.$$

Die Matrizenaddition ist assoziativ und kommutativ, sie hat als neutrales Element die Nullmatrix 0. (Wir schreiben die $m\times n$-Nullmatrix $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$ in der Regel einfach als 0.) Damit ist $(\mathrm{Mat}(m\times n,K),+)$ ein kommutatives Monoid.

(3) **Matrizenmultiplikation** $(\mathrm{M}_n(K),\cdot)$ **oder** $(K^{n\times n},\cdot)$**:** Für Matrizen A und B ist das Matrizenprodukt AB definiert, wenn die Spaltenzahl von A gleich der Zeilenzahl von B ist. Multipliziert man also zwei $n\times n$-Matrizen, so erhält man wieder eine $n\times n$-Matrix. Daher definiert die Matrizenmultiplikation eine Verknüpfung auf der Menge der $n\times n$-Matrizen $\mathrm{M}_n(K)$:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n a_{1j}b_{j1} & \dots & \sum_{j=1}^n a_{1j}b_{jn} \\ \vdots & & \vdots \\ \sum_{j=1}^n a_{nj}b_{j1} & \dots & \sum_{j=1}^n a_{nj}b_{jn} \end{pmatrix}.$$

Für 2×2-Matrizen sieht dies so aus:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Die Matrizenmultiplikation ist assoziativ und hat als neutrales Element die Einheitsmatrix

$$\mathbf{1}_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Die Matrizenmultiplikation ist im Fall $n \geq 2$ nicht kommutativ. Also ist $\mathrm{M}_n(K), \cdot)$ ein Monoid mit neutralem Element $\mathbf{1}_n$.

Ist $n \in \mathbb{N}$, so ist der Rest der Division durch n immer ein Element aus $\{0, 1, \dots, n-1\}$, d.h.

$$a \bmod n \in \{0, 1, \dots, n-1\} \text{ für alle } a \in \mathbb{Z}.$$

Daher ist folgende Definition sinnvoll:

DEFINITION. *Für $n \in \mathbb{N}$ sei*

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}.$$

$(\mathbb{Z}_n, +_{\bmod n})$ wird definiert durch die Verknüpfung

$$(a, b) \mapsto a +_{\bmod n} b := (a + b) \bmod n,$$

$(\mathbb{Z}_n, \cdot_{\bmod n})$ durch die Verknüpfung

$$(a, b) \mapsto a \cdot_{\bmod n} b := (ab) \bmod n.$$

Da sich $+_{\bmod n}$ und $\cdot_{\bmod n}$ nicht schön schreiben lässt, werden wir dafür auch einfach $+$ und $\cdot$ schreiben, also $(\mathbb{Z}_n, +)$ und $(\mathbb{Z}_n, \cdot)$.

Beispiele: Für kleine n kann man $(\mathbb{Z}_n, +_{\bmod n})$ und $(\mathbb{Z}_n, \cdot_{\bmod n})$ noch gut durch Verknüpfungstabellen beschreiben:

$(\mathbb{Z}_1, +_{\bmod 1})$	0
0	0

$(\mathbb{Z}_1, \cdot_{\bmod 1})$	0
0	0

$(\mathbb{Z}_2, +_{\bmod 2})$	0	1
0	0	1
1	1	0

$(\mathbb{Z}_2, \cdot_{\bmod 2})$	0	1
0	0	0
1	0	1

$(\mathbb{Z}_3, +_{\bmod 3})$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$(\mathbb{Z}_3, \cdot_{\bmod 3})$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$(\mathbb{Z}_4, +_{\bmod 4})$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_4, \cdot_{\bmod 4})$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(\mathbb{Z}_5, +_{\bmod 5})$	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

$(\mathbb{Z}_5, \cdot_{\bmod 5})$	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

$(\mathbb{Z}_6, +_{\bmod 6})$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$(\mathbb{Z}_6, \cdot_{\bmod 6})$	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

$(\mathbb{Z}_7, +_{\bmod 7})$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$(\mathbb{Z}_7, \cdot_{\bmod 7})$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$(\mathbb{Z}_8, +_{\bmod 8})$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$(\mathbb{Z}_8, \cdot_{\bmod 8})$	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

LEMMA. *Für $n \in \mathbb{N}$ gilt:*

(1) $(\mathbb{Z}_n, +_{\bmod n})$ *ist ein kommutatives Monoid mit neutralem Element* 0.
(2) $(\mathbb{Z}_n, \cdot_{\bmod n})$ *ist ein kommutatives Monoid mit neutralem Element* 1.

Beweis: Wir zeigen zunächst die Assoziativität der Addition. Seien $a, b, c \in \mathbb{Z}_n$.

- Sei $a +_{\bmod n} b = d$ und $d +_{\bmod n} c = e$. Dann ist
$$(a +_{\bmod n} b) +_{\bmod n} c = d +_{\bmod n} c = e.$$
Sei $b +_{\bmod n} c = f$ und $a +_{\bmod n} f = g$. Dann ist
$$a +_{\bmod n} (b +_{\bmod n} c) = a +_{\bmod n} f = g.$$
Wir müssen zeigen, dass $e = g$ gilt.
- Es ist $d = (a + b) \bmod n$, also gibt es ein $h \in \mathbb{Z}$ mit $a + b = hn + d$. Es ist $e = (d + c) \bmod n$, also gibt es ein $i \in \mathbb{Z}$ mit $d + c = in + e$. Insgesamt ist
$$e = d + c - in = (a + b - hn) + c - in = a + b + c - (h + i)n.$$
- Es ist $f = (b + c) \bmod n$, also gibt es ein $j \in \mathbb{Z}$ mit $b + c = jn + f$. Es ist $g = (a + f) \bmod n$, also gibt es ein $k \in \mathbb{Z}$ mit $a + f = kn + g$. Daraus folgt
$$g = a + f - kn = a + (b + c - jn) - kn = a + b + c - (j + k)n.$$
- Wir fassen zusammen:
$$a + b + c = (h + i)n + e \quad \text{und} \quad a + b + c = (j + k)n + g.$$
Wegen $e, g \in \mathbb{Z}_n$, also $0 \leq e, g < n$ und der Eindeutigkeit der Division mit Rest folgt nun
$$e = g = (a + b + c) \bmod n.$$
Dies beweist die Assoziativität der Addition.

Der vorangegangene Beweis ist mathematisch sicher nicht sehr elegant, er zeigt aber, wie man die Assoziativität systematisch angehen kann. Die Assoziativität der Multiplikation sieht man ganz genauso. Da die Aussagen über die neutralen Elemente klar sind, ist alles bewiesen. ■

3. Untermonoide

Sei $(M, *)$ ein Monoid und $U \subseteq M$ eine (nichtleere) Teilmenge von M.

- Ist U abgeschlossen unter der Verknüpfung $*$, d.h. gilt
$$a, b \in U \quad \Longrightarrow \quad a * b \in U,$$
so definiert $*$ auch eine Verknüpfung auf U. Das hat einfache Konsequenzen:
- Da in M das Assoziativgesetz gilt, gilt es natürlich auch in U. (Dies ist ein großer Vorteil.)
- Gilt für $(M, *)$ das Kommutativgesetz, so auch automatisch für $(U, *)$.
- Ist $e \in M$ das neutrale Element von $(M, *)$ und gilt $e \in U$, so besitzt auch $(U, *)$ das neutrale Element e. Dann ist also $(U, *)$ selbst ein Monoid. Man nennt U dann ein **Untermonoid** von M.

Wir formulieren das Ergebnis als Lemma.

LEMMA. *Sei $(M, *)$ ein Monoid und $U \subseteq M$ eine Teilmenge mit folgenden Eigenschaften:*

- *Für $a, b \in U$ gilt $a * b \in U$.*
- *Das neutrale Element e von M liegt auch in U, d.h. $e \in U$.*

Dann ist auch $(U, *)$ ein Monoid (mit neutralem Element e).

Beispiele:

(1) $(\mathbb{N}_0, +)$ ist ein Untermonoid von $(\mathbb{Z}, +)$.
(2) $(\mathbb{N}, \cdot)$ und $(\mathbb{N}_0, \cdot)$ sind Untermonoide von $(\mathbb{Z}, \cdot)$.
(3) **Achtung:** $(\mathbb{Z}_n, +_{\bmod n})$ ist **kein** Untermonoid von $(\mathbb{Z}, +)$ und $(\mathbb{Z}_n, \cdot_{\bmod n})$ ist kein Untermonoid von $(\mathbb{Z}, \cdot)$, da sich die Verknüpfungen stark unterscheiden.

4. Invertierbare Elemente

DEFINITION. *Sei $(M, *)$ ein Monoid mit neutralem Element e. Ein Element $a \in M$ heißt* **invertierbar**, *wenn es ein Element $b \in M$ gibt mit*
$$ab = ba = e.$$
b heißt dann ein zu a **inverses Element**. *(Natürlich ist dann auch a ein zu b inverses Element.)*

Beispiel: Das Monoid $(\mathbb{Q}, \cdot)$ hat 1 als neutrales Element. Alle Elemente $\neq 0$ sind invertierbar: Für $a, b \in \mathbb{Z} \setminus \{0\}$ gilt $\frac{a}{b} \cdot \frac{b}{a} = \frac{b}{a} \cdot \frac{a}{b} = 1$, also ist $\frac{b}{a}$ invers zu $\frac{a}{b}$.

LEMMA. *Ist $(M, *)$ ein Monoid mit neutralem Element e und ist $a \in M$ invertierbar, so gibt es genau ein zu a inverses Element.*

Beweis: Sind $b, c \in M$ zu a invers, so gilt
$$ab = ba = e \quad \text{und} \quad ac = ca = e.$$
Es folgt
$$b = be = b(ac) = (ba)c = ec = c,$$
was die Behauptung beweist. ■

Bemerkungen:

(1) Sei $(M, \cdot)$ ein multiplikativ geschriebenes Monoid mit neutralem Element e. Ist $a \in M$ invertierbar, so schreibt man meist a^{-1} für das zu a inverse Element. Es gilt also
$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$
Da a das zu a^{-1} inverse Element ist, gilt
$$\left(a^{-1}\right)^{-1} = a.$$
(2) Sei $(M, +)$ ein additiv geschriebenes Monoid mit neutralem Element 0. Ist a invertierbar, so schreibt man meist $-a$ für das zu a inverse Element. Es gilt
$$a + (-a) = (-a) + a = 0.$$
Analog wie eben gilt
$$-(-a) = a.$$

Bemerkung: Der Begriff **invertierbar** ist schon aus der Linearen Algebra bekannt. Eine quadratische Matrix $A \in \mathrm{M}_n(K)$ ist invertierbar, wenn es eine Matrix B gibt mit $AB = BA = \mathbf{1}_n$. (Hier rechnet man im Monoid $(\mathrm{M}_n(K), \cdot)$.)

Wir betrachten unsere Monoide $(\mathbb{Z}_n, +_{\bmod n})$ und $(\mathbb{Z}_n, \cdot_{\bmod n})$.

Satz. *Sei $n \in \mathbb{N}$. In $(\mathbb{Z}_n, +)$ ist jedes Element invertierbar. Es gilt*
$$-a = (-a) \bmod n = \begin{cases} 0, & \text{falls } a = 0, \\ n - a, & \text{falls } 0 < a < n. \end{cases}$$

Beweis: Für $a = 0$ ist die Aussage klar. Für $0 < a < n$ gilt
$$a +_{\bmod n} (n - a) = (a + (n - a)) \bmod n = n \bmod n = 0,$$
was die Behauptung beweist. ■

Satz. *Sei $n \in \mathbb{N}$. Im Monoid $(\mathbb{Z}_n, \cdot_{\bmod n})$ ist ein Element $a \in \mathbb{Z}_n$ genau dann invertierbar, wenn $\mathrm{ggT}(n, a) = 1$ gilt. Bestimmt man mit dem erweiterten euklidischen Algorithmus $x, y \in \mathbb{Z}$ mit $xn + ya = 1$, so ist*
$$a^{-1} = y \bmod n.$$

Beweis:

- Sei a invertierbar in $(\mathbb{Z}_n, \cdot_{\bmod n})$, d.h. es gibt ein $b \in \mathbb{Z}_n$ mit $(ab) \bmod n = 1$. Dann gibt es ein $k \in \mathbb{Z}$ mit $ab = kn + 1$. Aus $1 = ab - kn$ folgt sofort $\mathrm{ggT}(n, a) = 1$.
- Sei nun umgekehrt $\mathrm{ggT}(n, a) = 1$. Mit dem erweiterten euklidischen Algorithmus findet man $x, y \in \mathbb{Z}$ mit $xn + ya = 1$. Sei $z = y \bmod n$. Dann gibt es ein $l \in \mathbb{Z}$ mit $y = ln + z$. Es folgt
$$(y \bmod n)a = za = (y - ln)a = ya - lan = 1 - xn - lan,$$
und damit
$$(y \bmod n) \cdot_{\bmod n} a = ((y \bmod n)a) \bmod n = 1.$$
Dies beweist die Behauptung. ■

Beispiel: Wir betrachten im Monoid $(\mathbb{Z}_7, \cdot)$ das Element 5. Wegen $\mathrm{ggT}(7, 5) = 1$ ist 5 invertierbar. Wegen
$$3 \cdot 7 + (-4) \cdot 5 = 1$$
gilt
$$5^{-1} = (-4) \bmod 7 = 3.$$

Lemma. *Ist M eine nichtleere Menge, so ist $f \in \mathrm{Abb}(M, M)$ genau dann invertierbar (bezüglich der Komposition $\circ$), wenn f bijektiv ist. Invers zu f ist f^{-1}.*

Beweis:

- Ist $f : M \to M$ bijektiv, ist $f^{-1} : M \to M$ die inverse Funktion, so gilt bekanntlich
$$f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}_M.$$
f ist also invertierbar im Monoid $(\mathrm{Abb}(M, M), \circ)$ und f^{-1} das Inverse von f.
- Ist $f \in \mathrm{Abb}(M, M)$ invertierbar, so gibt es eine Funktion $g : M \to M$ mit
$$g \circ f = \mathrm{id}_M \quad \text{und} \quad f \circ g = \mathrm{id}_M.$$
Mit Standardargumenten folgt aus $g \circ f = \mathrm{id}_M$ die Injektivität von f, aus $f \circ g = \mathrm{id}_M$ die Surjektivität von f. Also ist f bijektiv; die Umkehrabbildung f^{-1} erfüllt natürlich
$$f \circ f^{-1} = \mathrm{id}_M \quad \text{und} \quad f^{-1} \circ f = \mathrm{id}_M.$$
Dies beweist die Behauptung. ■

LEMMA. *Sei $(M, *)$ ein Monoid mit neutralem Element e. Ist $a \in M$ und gibt es Elemente $b, c \in M$ mit*
$$ba = e \quad \textit{und} \quad ac = e,$$
so gilt $b = c$, a ist invertierbar und
$$a^{-1} = b = c.$$

Beweis: Es ist
$$b = be = b(ac) = (ba)c = ec = c,$$
sodass $ba = ab = e$ gilt. Also ist a invertierbar, woraus der Rest folgt. ■

Bemerkung: Die Bedingung $ba = e$ des vorangegangenen Lemmas alleine garantiert nicht die Invertierbarkeit von a. (In den Hausaufgaben findet man ein einfaches Gegenbeispiel mit dem Monoid $(\mathrm{Abb}(\mathbb{N}, \mathbb{N}), \circ)$.)

Bemerkung: Kennt man für das Monoid $(M, *)$ eine Verknüpfungstabelle, so ist $a \in M$ genau dann invertierbar, wenn in der zu a gehörigen Zeile und in der zu a gehörigen Spalte das neutrale Element e vorkommt.

SATZ. *Sei $(M, *)$ ein Monoid mit neutralem Element e.*

(1) *Sind $a, b \in M$ invertierbar, so ist auch ab invertierbar, und es gilt*
$$(ab)^{-1} = b^{-1}a^{-1}.$$
(2) *Ist a invertierbar, so auch a^{-1}, und es gilt*
$$(a^{-1})^{-1} = a.$$
(3) *Die durch*
$$M^* = \{a \in M : a \textit{ ist invertierbar}\}$$
definierte Teilmenge von M ist ein Untermonoid von M, in dem jedes Element invertierbar ist. Außerdem gilt: $a \in M \Longrightarrow a^{-1} \in M$.

Beweis:

(1) Dies folgt sofort aus
$$b^{-1}a^{-1}ab = e \quad \text{und} \quad abb^{-1}a^{-1} = e.$$
(2) Dies haben wir bereits zuvor bemerkt.
(3) Nach (1) ist M^* unter der Verknüpfung abgeschlossen. Da trivialerweise $e \in M^*$ gilt, ist M^* ein Untermonoid. Die letzte Eigenschaft folgt aus (2). ■

Bemerkung: M^* ist ein Monoid, in dem jedes Element invertierbar ist. Solche Monoide heißen **Gruppen** und werden im nächsten Kapitel behandelt.

5. Potenzieren - Multiplizieren

Potenzieren: Ist $(M, *)$ ein Monoid, so kann man für $n \in \mathbb{N}$ die Potenz

$$a^n = \underbrace{a * a * \cdots * a}_{n \text{ Faktoren}}$$

bilden, da es auf die Klammersetzung nicht ankommt. Es gelten dann die üblichen Rechenregeln für $m, n \in \mathbb{N}$

$$a^m * a^n = a^{m+n} \quad \text{und} \quad (a^m)^n = a^{mn}.$$

Kurze Begründung:

$$a^m * a^n = (\underbrace{a * a * \cdots * a}_{m \text{ Faktoren}}) * (\underbrace{a * a * \cdots * a}_{n \text{ Faktoren}}) = \underbrace{a * a * \cdots * a}_{m+n \text{ Faktoren}} = a^{m+n}$$

und

$$\begin{aligned}(a^m)^n &= \underbrace{a^m * a^m * \cdots * a^m}_{n \text{ Faktoren}} = \\ &= \underbrace{(\underbrace{a * a * \cdots * a}_{m \text{ Faktoren}}) * (\underbrace{a * a * \cdots * a}_{m \text{ Faktoren}}) * \cdots * (\underbrace{a * a * \cdots * a}_{m \text{ Faktoren}})}_{n \text{ Faktoren}} = \\ &= \underbrace{a * a * \cdots * a}_{mn \text{ Faktoren}} = a^{mn}.\end{aligned}$$

Ist e das neutrale Element von $(M, *)$, definiert man

$$a^0 = e,$$

so bleiben obige Rechenregeln auch für $m, n \in \mathbb{N}_0$ gültig.

Hat man es mit einem additiv geschriebenen Monoid $(M, +)$ zu tun, so schreibt man für $n \in \mathbb{N}$ und $a \in M$

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ Summanden}}.$$

Die obigen Rechenregeln schreiben sich dann in der Form

$$m \cdot a + n \cdot a = (m + n) \cdot a \quad \text{und} \quad n \cdot (m \cdot a) = (mn) \cdot a.$$

Ist 0 das neutrale Element von $(M, +)$, so definiert man

$$0 \cdot a = 0.$$

(Die 0 taucht hier in verschiedenen Bedeutungen auf: Links ist $0 \in \mathbb{N}_0$, rechts $0 \in M$.)

Das folgende Lemma gibt ein wichtiges Beispiel.

LEMMA. *Für $n \in \mathbb{N}$ betrachten wir das additiv geschriebene Monoid $(\mathbb{Z}_n, +_{\bmod n})$. Für $a \in \mathbb{Z}_n$ und $m \in \mathbb{N}_0$ gilt*

$$m \cdot a = (ma) \bmod n.$$

Beweis: Wir beweisen dies durch Induktion nach m. Die Fälle $m = 0$ und $m = 1$ folgen aus den Definitionen:

$$0 \cdot a = 0, \quad 1 \cdot a = a.$$

Sei nun $m \geq 1$ und die Aussage bereits für m bewiesen, d.h.

$$m \cdot a = (ma) \bmod n.$$

Schreiben wir $r = (am) \bmod n$, so ist $am = qn + r$ mit $q \in \mathbb{Z}$. Dann gilt

$$(m + 1) \cdot a = (m \cdot a) +_{\bmod n} a = r +_{\bmod n} a = (r + a) \bmod n.$$

Nun ist

$$r + a = am - qn + a = m(a + 1) - qn, \quad \text{also} \quad (r + a) \bmod n = (m(a + 1)) \bmod n,$$

und damit

$$(m+1)\cdot a = (m(a+1)) \bmod n,$$

was zu zeigen war. ■

6. Potenzieren von invertierbaren Elementen

Potenzieren für invertierbare Elemente: Sei $(M,*)$ ein Monoid mit neutralem Element e. Wir $n \in \mathbb{N}$ und $a \in M$ hatten wir definiert

$$a^n = \underbrace{a * a * \cdots * a}_{n \text{ Faktoren}} \quad \text{und} \quad a^0 = e.$$

Ist a invertierbar, so definieren wir für $n \in \mathbb{N}$

$$a^{-n} := (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ Faktoren}}.$$

(Dies erweitert die Schreibweise a^{-1} auf a^{-n}.)
Ist $(M,+)$ ein additiv geschriebenes Monoid mit neutralem Element 0, so hatten wir für $n \in \mathbb{N}$ definiert

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ Summanden}} \quad \text{und} \quad 0 \cdot a = 0.$$

Ist a invertierbar, so definieren wir für $n \in \mathbb{N}$

$$(-n)\cdot a = n \cdot (-a) = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ Summanden}}.$$

Die Rechenregeln für das Potenzieren verallgemeinern sich nun wie folgt:

LEMMA. *Ist $(M,\cdot)$ ein (multiplikativ geschriebenes) Monoid mit neutralem Element e und $a \in M$ invertierbar, so gilt für alle $m,n \in \mathbb{Z}$*

$$a^m \cdot a^n = a^{m+n} \quad \textit{und} \quad (a^m)^n = a^{mn}.$$

Insbesondere ist auch a^m invertierbar; invers dazu ist a^{-m}.
Ist $(M,+)$ ein (additiv geschriebenes) Monoid mit neutralem Element 0 und $a \in M$ invertierbar, so gilt für alle $m,n \in \mathbb{Z}$

$$m \cdot a + n \cdot a = (m+n)\cdot a \quad \textit{und} \quad n \cdot (m \cdot a) = (mn) \cdot a.$$

Da mir im Augenblick nur ein Beweis mit einer Reihe von Fallunterscheidungen einfällt, führe ich diesen hier nicht aus.

7. Schnelles Potenzieren - Eine square-and-multiply-Methode

Sei $(M,*)$ ein Monoid und $n \in \mathbb{N}$. Will man a^n berechnen, braucht man mittels der Definition

$$a^n = \underbrace{a * a * a * \cdots * a}_{n \text{ Faktoren}}$$

$n-1$ Multiplikationen, also beispielsweise für $n = 10$ neun Multiplikationen:

$$a^{10} = (((((((a * a) * a) * a) * a) * a) * a) * a) * a) * a.$$

Dies geht mit folgender Idee auch schneller. In der Rechnung ergeben sich zwischendurch Ausdrücke der Form $b * c^n$, die wie folgt behandelt werden:

- Ist n gerade, so gilt
$$b * c^n = b * (c^2)^{\frac{n}{2}}.$$
Wir müssen für den nächsten Schritt c quadrieren.
- Ist n ungerade, so gilt
$$b * c^n = (b * c) * c^{n-1}.$$
Wir müssen für den nächsten Schritt das Produkt $b * c$ berechnen.

Am Ende haben wir wieder einen Ausdruck $\overline{b} * \overline{c}^{\overline{n}}$, allerdings nun mit kleinerem Exponenten.
Bevor wir das Vorgehen algorithmisch beschreiben, starten wir mit Beispielen:

Beispiele:

(1) In $(\mathbb{Z}, \cdot)$ wollen wir 3^{33} berechnen:

$$\begin{aligned} 3^{33} &= 3 \cdot 3^{32} = 3 \cdot (3^2)^{16} = 3 \cdot 9^{16} = 3 \cdot (9^2)^8 = 3 \cdot 81^8 = 3 \cdot (81^2)^4 = 3 \cdot 6561^4 = \\ &= 3 \cdot (6561^2)^2 = 3 \cdot 43046721^2 = 3 \cdot 1853020188851841 = 5559060566555523 \end{aligned}$$

(2) Wir wollen in $(\mathbb{Z}_{10}, \cdot)$ die Potenz 4^{20} berechnen:

$$4^{20} = (4^2)^{10} = 6^{10} = (6^2)^5 = 6^5 = 6 \cdot 6^4 = 6 \cdot (6^2)^2 = 6 \cdot 6^2 = 6 \cdot 6 = 6.$$

Wir schreiben die Vorgehensweise nun als mathematischen Satz auf:

Satz. *Gegeben sei ein Monoid $(M, *)$ mit neutralem Element e, ein Element $a \in M$ und eine Zahl $n \in \mathbb{N}_0$. Rekursiv werden Größen $b_i, c_i \in M$ und $n_i \in \mathbb{N}_0$ wie folgt definiert:*
Man beginnt mit

$$b_0 = e, \quad c_0 = a, \quad n_0 = n.$$

Seien nun b_i, c_i, n_i bereits definiert. Man unterscheidet drei Fälle:

- *Ist $n_i = 0$, so bricht man ab. Es gilt dann*
$$a^n = b_i.$$
- *Ist $n_i > 0$ und $n_i \bmod 2 = 0$, so definiert man*
$$b_{i+1} = b_i, \quad c_{i+1} = c_i^2, \quad n_{i+1} = \left\lfloor \frac{n_i}{2} \right\rfloor.$$
- *Ist $n_i > 0$ und $n_i \bmod 2 = 1$, so definiert man*
$$b_{i+1} = b_i * c_i, \quad c_{i+1} = c_i, \quad n_{i+1} = n_i - 1.$$

Mit Hilfe der Folgen b_i, c_i, n_i wurde a^n berechnet.

Beweis: Wir zeigen, dass für alle definierten Indizes i die Beziehung

$$b_i * c_i^{n_i} = a^n$$

gilt. Für $i = 0$ stimmt dies nach Definition von b_0, c_0, n_0. Die Beziehung gelte nun für i, d.h.

$$b_i * c_i^{n_i} = a^n.$$

- Ist $n_i = 0$, so gilt
$$a^n = b_i,$$
wie behauptet.
- Ist $n_i > 0$ und $n_i \bmod 2 = 0$, so gilt
$$b_{i+1} * c_{i+1}^{n_{i+1}} = b_i * (c_i^2)^{\frac{n_i}{2}} = b_i * c_i^{n_i} = a^n.$$
- Ist $n_i > 0$ und $n_i \bmod 2 = 1$, so gilt
$$b_{i+1} * c_{i+1}^{n_{i+1}} = (b_i * c_i) * c_i^{n_i - 1} = b_i * c_i^{n_i} = a^n.$$

Damit folgt die Behauptung durch Induktion. ■

Das im Satz dargestellte Verfahren lässt sich auch gut in Tabellenform beschreiben. In den folgenden Beispielen haben wir auch noch die Binärdarstellung von n_i angegeben.

Beispiele:

(1) Wir berechnen nochmals 3^{33} in $(\mathbb{Z}, \cdot)$:

i	b_i	c_i	n_i	n_i binär
0	1	3	33	$(100001)_2$
1	3	3	32	$(100000)_2$
2	3	9	16	$(10000)_2$
3	3	81	8	$(1000)_2$
4	3	6561	4	$(100)_2$
5	3	43046721	2	$(10)_2$
6	3	1853020188851841	1	$(1)_2$
7	5559060566555523	1853020188851841	0	$(0)_2$

Es ist

$$3^{33} = 5559060566555523.$$

(2) Wir berechnen nochmals 4^{20} in $(\mathbb{Z}_{10}, \cdot)$:

i	b_i	c_i	n_i	n_i binär
0	1	4	20	$(10100)_2$
1	1	6	10	$(1010)_2$
2	1	6	5	$(101)_2$
3	6	6	4	$(100)_2$
4	6	6	2	$(10)_2$
5	6	6	1	$(1)_2$
6	6	6	0	$(0)_2$

Es ist

$$4^{20} = 6 \text{ in } \mathbb{Z}_{10}.$$

(3) Wir berechnen 13^{17} in $(\mathbb{Z}_{19}, \cdot)$:

i	b_i	c_i	n_i	n_i binär
0	1	13	17	$(10001)_2$
1	13	13	16	$(10000)_2$
2	13	17	8	$(1000)_2$
3	13	4	4	$(100)_2$
4	13	16	2	$(10)_2$
5	13	9	1	$(1)_2$
6	3	9	0	$(0)_2$

Es ist

$$13^{17} = 3 \text{ in } \mathbb{Z}_{19}.$$

(4) Wir berechnen $79^{123456789}$ in $(\mathbb{Z}_{101}, \cdot)$:

i	b_i	c_i	n_i	n_i binär
0	1	79	123456789	$(111010110111100110100010101)_2$
1	79	79	123456788	$(111010110111100110100010100)_2$
2	79	80	61728394	$(11101011011110011010001010)_2$
3	79	37	30864197	$(11101011011110011010000101)_2$
4	95	37	30864196	$(11101011011110011010000100)_2$
5	95	56	15432098	$(11101011011110011010000010)_2$
6	95	5	7716049	$(11101011011110011010001)_2$
7	71	5	7716048	$(11101011011110011010000)_2$
8	71	25	3858024	$(11101011011110011010000)_2$
9	71	19	1929012	$(11101011011110011010100)_2$
10	71	58	964506	$(1110101101111001101 0)_2$
11	71	31	482253	$(1110101101111001101)_2$
12	80	31	482252	$(1110101101111001100)_2$
13	80	52	241126	$(111010110111100110)_2$
14	80	78	120563	$(11101011011110011)_2$
15	79	78	120562	$(11101011011110010)_2$
16	79	24	60281	$(1110101101111001)_2$
17	78	24	60280	$(1110101101111000)_2$
18	78	71	30140	$(111010110111100)_2$
19	78	92	15070	$(11101011011110)_2$
20	78	81	7535	$(1110101101111)_2$
21	56	81	7534	$(1110101101110)_2$
22	56	97	3767	$(111010110111)_2$
23	79	97	3766	$(111010110110)_2$
24	79	16	1883	$(11101011011)_2$
25	52	16	1882	$(11101011010)_2$
26	52	54	941	$(1110101101)_2$
27	81	54	940	$(1110101100)_2$
28	81	88	470	$(111010110)_2$
29	81	68	235	$(11101011)_2$
30	54	68	234	$(11101010)_2$
31	54	79	117	$(1110101)_2$
32	24	79	116	$(1110100)_2$
33	24	80	58	$(111010)_2$
34	24	37	29	$(11101)_2$
35	80	37	28	$(11100)_2$
36	80	56	14	$(1110)_2$
37	80	5	7	$(111)_2$
38	97	5	6	$(110)_2$
39	97	25	3	$(11)_2$
40	1	25	2	$(10)_2$
41	1	19	1	$(1)_2$
42	19	19	0	$(0)_2$

Daher ist

$$79^{1234567890} = 19 \text{ in } \mathbb{Z}_{101}.$$

(5) Im Monoid $(\mathrm{M}_2(\mathbb{Q}), \cdot)$ (mit dem neutralem Element $\mathbf{1}_2$) berechnen wir $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{100}$:

i	b_i	c_i	n_i	n_i binär
0	$\mathbf{1}_2$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	100	$(1100100)_2$
1	$\mathbf{1}_2$	$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$	50	$(110010)_2$
2	$\mathbf{1}_2$	$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$	25	$(11001)_2$
3	$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$	24	$(11000)_2$
4	$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix}$	12	$(1100)_2$
5	$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 610 & 987 \\ 987 & 1597 \end{pmatrix}$	6	$(110)_2$
6	$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 1346269 & 2178309 \\ 2178309 & 3524578 \end{pmatrix}$	3	$(11)_2$
7	$\begin{pmatrix} 9227465 & 14930352 \\ 14930352 & 24157817 \end{pmatrix}$	$\begin{pmatrix} 1346269 & 2178309 \\ 2178309 & 3524578 \end{pmatrix}$	2	$(10)_2$
8	$\begin{pmatrix} 9227465 & 14930352 \\ 14930352 & 24157817 \end{pmatrix}$	$\begin{pmatrix} 6557470319842 & 10610209857723 \\ 10610209857723 & 17167680177565 \end{pmatrix}$	1	$(1)_2$
9	$\begin{pmatrix} 218922995834555169026 & 354224848179261915075 \\ 354224848179261915075 & 573147844013817084101 \end{pmatrix}$	$\begin{pmatrix} 6557470319842 & 10610209857723 \\ 10610209857723 & 17167680177565 \end{pmatrix}$	0	$(0)_2$

Es ist also

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{100} = \begin{pmatrix} 218922995834555169026 & 354224848179261915075 \\ 354224848179261915075 & 573147844013817084101 \end{pmatrix}.$$

Hier ist eine algorithmische Variante des vorangegangenen Satzes:

Potenzieren mit der square-and-multply-Methode:

Eingabe: Monoid $(M, *)$ mit neutralem Element e, $a \in M$, $n \in \mathbb{N}_0$

Ausgabe: a^n

1: $b \leftarrow e$, $c \leftarrow a$
2: **while** $n > 0$ **do**
3: **if** $n \bmod 2 = 0$ **then**
4: $c \leftarrow c^2$, $n \leftarrow \left\lfloor \frac{n}{2} \right\rfloor$
5: **else**
6: $b \leftarrow b * c$, $n \leftarrow n - 1$
7: **end if**
8: **end while**
9: **return** b

Bemerkungen:

(1) Die wesentlichen Elemente des vorangegangenen Algorithmus sind das Quadrieren (square) in Zeile 4 und das Multiplizieren (multiply) in Zeile 6. Deswegen spricht man auch von einer **square-and-multiply-Methode**.
(2) Es gibt auch andere Varianten der square-and-multiply-Methode, auf die wir aber hier nicht eingehen.
(3) Schaut man sich die vorangegangenen Beispiele an, so entdeckt man, dass die Anzahl der Zeilen der Tabellen genau die Summe aus der Anzahl der Binärstellen von n und aus der Anzahl der Einsen in der Binärdarstellung von n ist. Das kann man auch allgemein zeigen. Dies bewirkt, dass das Verfahren gerade für große Exponenten schnell ist.