Kapitel 1

Algebraische Strukturen

1.1 Operationen

1.1.A Stelligkeit und Typ

1.1.1 Definition. Sei A eine Menge, $n \in \mathbb{N}_0$, dann heißt eine Abbildung $\omega : A^n \to A$ eine *n-stellige*[1] (oder *n-äre*) *Operation auf A*, d. h.,
für $n \in \mathbb{N}$:

$$\omega : \begin{cases} A^n \to A \\ (x_1, \ldots, x_n) \mapsto \omega x_1 \ldots x_n \text{ oder } \omega(x_1, \ldots, x_n) \end{cases}$$

für $n = 0$:

$$\omega : \begin{cases} A^0 = \{\emptyset\} \to A \\ \emptyset \mapsto \omega\emptyset =: \omega. \end{cases}$$

Wichtigster Fall: $n = 2$. Eine 2-stellige oder binäre Operation ist eine Abbildung

$$\omega : \begin{cases} A^2 \to A \\ (x, y) \mapsto \omega xy \text{ oder } \omega(x, y). \end{cases}$$

Meist bezeichnen wir 2-stellige Operationen mit Symbolen wie $\circ$, $+$, $*$, $\star$ statt mit Buchstaben wie ω; für diese Symbole verwenden wir dann meist „Infixnotation“ statt Präfixnotation (siehe Abschnitt 1.2), also

$$\circ : \begin{cases} A^2 \to A \\ (x, y) \mapsto x \circ y. \end{cases}$$

1.1.2 Beispiele. 1) $+$ und $\cdot$ sind 2-stellige Operationen auf $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}^+$, $\mathbb{R}$, $\mathbb{R}^+$ und $\mathbb{C}$, $-$ ist 2-stellige Operation auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$, $\div$ auf $\mathbb{Q}^+$, $\mathbb{R}^+$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$.

2) $+$ und $\cdot$ (im üblichen Sinn) sind 2-stellige Operationen auf $M_n(\mathbb{C})$, der Menge aller quadratischen $n \times n$-Matrizen über $\mathbb{C}$ (analog mit $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ statt $\mathbb{C}$).

3) Seien M und N Mengen. Mit N^M bezeichnen wir die Menge aller Abbildungen von M nach N: $N^M := \{f \mid f : M \to N\}$.
Für $M = N$ ist die binäre Operation $\circ$ auf N^M wie folgt definiert: $(f \circ g)(x) := f(g(x))$ für alle $x \in M$ (Komposition oder Verkettung von Funktionen). Wir erhalten also:

$$\circ : \begin{cases} M^M \times M^M \to M^M \\ (f, g) \mapsto f \circ g. \end{cases}$$

4) M sei eine Menge und $\mathfrak{P}(M) := \{T \mid T \subseteq M\}$ die Potenzmenge von M. $\cap$, $\cup$ sind binäre Operationen auf $\mathfrak{P}(M)$.

[1] n heißt auch „Stelligkeit“ oder „Arität“ der Operation, englisch „arity“

Weiterer wichtiger Fall: $n = 1$. Eine einstellige (unäre) Operation ist eine Abbildung

$$\omega : \begin{cases} A \to A \\ x \mapsto \omega x. \end{cases}$$

1.1.3 Beispiele. 1) $- : \begin{cases} \mathbb{C} \to \mathbb{C} \\ x \mapsto -x \end{cases}$ ist einstellige Operation auf $\mathbb{C}$.

2) $-$ ist auch einstellige Operation auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $M_n(\mathbb{C})$.

3) $x \mapsto 1/x$ ist einstellige Operation auf $\mathbb{Q} \setminus \{0\}$, $\mathbb{Q}^+$, $\mathbb{R} \setminus \{0\}$, $\mathbb{R}^+$, $\mathbb{C} \setminus \{0\}$.

4) $T \mapsto M \setminus T =: T'$ ist einstellige Operation auf der Potenzmenge $\mathfrak{P}(M)$.

1.1.4 Anmerkung. Das Symbol „$-$“ wird sowohl für die einstellige Operation des „Negativmachens“ (oft: Multiplikation mit -1) als auch für die zweistellige Operation „Differenz“ verwendet. Der Kontext entscheidet, ob die einstellige oder zweistellige Operation gemeint ist.
In den Gleichungen

$$x - y = x + (-y), \qquad x - (-y) = x + y$$

bezeichnet das erste „$-$“ jeweils die zweistellige Operation, das zweite die einstellige.

1.1.5 Definition. Sei A eine Menge, $n \in \mathbb{N}_0$, $D \subseteq A^n$, dann heißt eine Abbildung $\omega : D \to A$ eine *n-stellige partielle Operation auf A*.
1) $-$ ist eine zweistellige partielle Operation auf $\mathbb{N}$.

2) $x \mapsto 1/x$ ist einstellige partielle Operation auf $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ($D = \mathbb{Q} \setminus \{0\}, \ldots$).

Sei $A = \{a_1, \ldots, a_n\}$ eine endliche Menge und $\circ$ eine binäre Operation auf A. Dann kann diese durch eine Operationstafel, die sog. *Cayley-Tafel* angegeben werden. Die Tafel weist im Schnittpunkt der i-ten Zeile mit der j-ten Spalte das Element $a_i \circ a_j$ auf.

1.1.6 Definition. Sei A Menge[2] I (Index-)Menge. Für $i \in I$ sei ω_i eine n_i-stellige Operation auf A, $n_i \in \mathbb{N}_0$. Dann heißt $\mathfrak{A} := (A, (\omega_i)_{i \in I})$ eine (*universelle*) *Algebra* mit der *Grundmenge* A und der *Operationenfamilie* $(\omega_i)_{i \in I} =: \Omega$.

Häufig ist I endlich, etwa $I = \{1, \ldots, n\}$. In diesem Fall schreibt man

$$(A, \Omega) = (A, (\omega_i)_{i \in \{1, \ldots, n\}}) =: (A, \omega_1, \ldots, \omega_n).$$

Die Familie $(n_i)_{i \in I}$ heißt der *Typ* der Algebra (A, Ω). Algebren desselben Typs heißen „ähnlich“. Oft[3] verwenden wir für eine Algebra und ihre Grundmenge dasselbe Symbol, also $A = (A, \Omega)$, sofern keine Verwechslung möglich ist.

1.1.7 Beispiel. $(\mathbb{Z}, +, -, 0)$ ist eine Algebra vom Typ $(2, 1, 0)$, $(\mathbb{Z}, +, -, 0, \cdot, 1)$ ist eine Algebra vom Typ $(2, 1, 0, 2, 0)$.

[2] A kann eine endliche oder unendliche Menge sein. Auch die leere Menge ist a priori zugelassen. Meistens werden wir jedoch Algebren mit nullstelligen Operationen betrachten; diese sind niemals leer.

[3] In der Logik und auch in der universellen Algebra verwendet man oft ein Symbol (A, B, …, oder auch einen komplizierteren Ausdruck wie A', B_1, …) für die Grundmenge einer Algebra und ein entsprechendes Symbol aus einem anderen Zeichensatz ($\mathfrak{A}$, $\mathcal{A}$, $\mathscr{A}$, analog $\mathfrak{B}_1$, …) für die Algebra. Man kann auch die Algebra selbst als das fundamentale Objekt betrachten, und bezeichnet dann die Algebra z.B. mit A, die Grundmenge mit $|A|$ oder $univ(A)$, die Operationen mit ω_i^A.

1.1.B Kommutativität, Assoziativität, Distributivität

1.1.8 Definition. Sei A Menge, $\circ$ binäre Operation. $\circ$ heißt *assoziativ* genau dann, wenn das so genannte *Assoziativgesetz* gilt:

$$\forall x, y, z \in A : (x \circ y) \circ z = x \circ (y \circ z).$$

1.1.9 Beispiel. $+, \cdot$ auf $\mathbb{C}$ und $M_n(\mathbb{C})$ sind assoziativ, ebenso $\circ$ auf M^M und $\cap, \cup$ auf $\mathfrak{P}(M)$. Dagegen sind $-, \div$ im allgemeinen *nicht* assoziativ![4]

1.1.10 Definition. Die binäre Operation $\circ$ auf A heißt *kommutativ* $:\Leftrightarrow$

$$\forall x, y \in A : x \circ y = y \circ x \quad (\textit{Kommutativgesetz})$$

1.1.11 Beispiel. *Nicht* kommutativ sind: $-$ auf $\mathbb{C}$, $\div$ auf $\mathbb{C} \setminus \{0\}$, $\cdot$ auf $M_n(\mathbb{C})$ für $n \geq 2$, $\circ$ auf M^M für $|M| \geq 2$.

1.1.12 Definition. Sind $+, \cdot$ binäre Operationen auf A, dann heißt $\cdot$ *distributiv über* $+ :\Leftrightarrow$ es gelten die *Distributivgesetze*:

$$\forall x, y, z \in A : x \cdot (y + z) = x \cdot y + x \cdot z \quad (\textit{Linksdistributivgesetz})$$
$$\forall x, y, z \in A : (y + z) \cdot x = y \cdot x + z \cdot x \quad (\textit{Rechtsdistributivgesetz})$$

1.1.13 Anmerkung. Um Klammern zu sparen, verwenden wir die Konvention: „Punktrechnung wird vor Strichrechnung ausgeführt."

1.1.14 Beispiel. $\cdot$ ist distributiv über $+$ in $\mathbb{C}$, $M_n(\mathbb{C})$. In $\mathfrak{P}(M)$ ist $\cup$ distributiv über $\cap$ und $\cap$ distributiv über $\cup$.

1.1.C Neutrale und inverse Elemente

1.1.15 Definition. Sei A Menge, $\circ$ eine binäre Operation auf A. Sei $e \in A$, dann heißt e

- ein *Linkseinselement* oder *linksneutrales Element* bezüglich $\circ :\Leftrightarrow \forall x \in A : e \circ x = x$,
- ein *Rechtseinselement* oder *rechtsneutrales Element* bezüglich $\circ :\Leftrightarrow \forall x \in A : x \circ e = x$,
- ein *Einselement* oder *neutrales Element* bezüglich $\circ :\Leftrightarrow \forall x \in A : e \circ x = x \circ e = x$.

1.1.16 Anmerkung. Universell quantifizierte Gleichungen zwischen Termen (also Gleichungen, die die Form $t_1(x, y, z, \ldots) = t_2(x, y, z, \ldots)$ mit geeigneten Termen t_1, t_2 haben und für alle Elemente einer Algebra erfüllt sein sollen, wie z. B. „$\forall x \in A : e \circ x = x$"), heißen *Gesetze*.
Um deutlich zu machen, dass nicht die Terme t_1 und t_2 qua[5] formale Objekte gleich sind, sondern nur ihre Auswertungen an allen Elementen der betrachteten Algebra (zum Beispiel enthält der Term $x \cdot x^{-1}$ die Variable x zwei Mal, der Term 1 enthält sie gar nicht), schreibt man Gesetze oft nicht in der Form $t_1 = t_2$ sondern verwendet die Notation $t_1 \approx t_2$.

[4] Ein weiteres Beispiel aus der Umgangssprache: Nach dem 2.Weltkrieg waren Lebensmittel in Österreich rationiert, und man konnte sie offiziell nur gegen Marken oder „Punkte" eintauschen, die man am Anfang des Monats von einer Behörde erhielt. Diese (Lebensmittel)punkte standen für viele im Lebens(mittelpunkte).

[5] qua=in ihrer Eigenschaft als

1.1.17 Beispiele. 1) Sei $A = \mathbb{C}$ mit der Operation $\circ = +$. Dann ist 0 neutrales Element.
2) Sei $A = \mathbb{C}$ mit der Operation $\circ = \cdot$. Dann ist 1 ist neutrales Element. (Wir sagen: „1 ist neutral *bezüglich* Multiplikation, 0 ist neutral bezüglich Addition.“)

3) Sei $A = M_n(\mathbb{C})$. Dann ist $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$ neutrales Element bezüglich Addition, $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$ ist neutrales Element bezüglich (Matrizen-)Multiplikation.

4) Sei $A = M^M$ mit $\circ =$ Komposition. Dann ist id_M (die identische Abbildung) neutrales Element.

5) Sei $A = \mathfrak{P}(M)$. Dann ist M ist neutrales Element bezüglich der Operation $\cap$, denn $X \cap M = X$ für alle $X \in \mathfrak{P}(M)$. Die leere Menge $\emptyset$ ist neutrales Element bezüglich $\cup$.

1.1.18 Satz. *Sei $\circ$ binäre Operation auf A, e_1 Linkseinselement und e_2 Rechtseinselement. Dann gilt: $e_1 = e_2$, und $e_1 (= e_2)$ ist Einselement.*

Beweis. $e_1 = e_1 \circ e_2 = e_2$. □

1.1.19 Folgerung. Es gibt höchstens ein Einselement.

1.1.20 Definition. Sei A Menge, $\circ$ binäre Operation, e Einselement, $x \in A$; dann heißt ein Element $y \in A$ *linksinvers* zu $x :\Leftrightarrow y \circ x = e$, *rechtsinvers* zu $x :\Leftrightarrow x \circ y = e$, *invers* zu $x :\Leftrightarrow x \circ y = y \circ x = e$.

1.1.21 Beispiel.

Menge	Operation	Element	Inverses
$\mathbb{C}$	$+$	x	$-x$
$\mathbb{C}$	$\cdot$	$x \neq 0$	$1/x$
$M_n(\mathbb{C})$	$+$	(a_{ij})	$(-a_{ij})$
$M_n(\mathbb{C})$	$\cdot$	(a_{ij}) mit $\det(a_{ij}) \neq 0$	$(a_{ij})^{-1}$
M^M	$\circ$	bijektives f	f^{-1}
$\mathfrak{P}(M)$	$\cap$	M	M
$\mathfrak{P}(M)$	$\cup$	$\emptyset$	$\emptyset$
$\mathbb{Z}$	$\cdot$	± 1	± 1

1.1.22 Definition. x heißt *invertierbar* $:\Leftrightarrow$ es gibt ein Inverses zu x.

1.1.23 Satz. *$\circ$ sei assoziative binäre Operation auf A, $x \in A$, y_1 linksinvers zu x, y_2 rechtsinvers zu x bezüglich des neutralen Elementes e. Dann gilt: $y_1 = y_2$.*

Beweis. $y_2 = e \circ y_2 = (y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2) = y_1 \circ e = y_1$. □

1.1.24 Folgerung. Bei einer assoziativen Operation gibt es zu jedem Element x höchstens ein Inverses.

Schreibweise für das Inverse von x: x^{-1} (bezüglich $\circ, \cdot$) oder $-x$ (bezüglich $+$). Ein neutrales Element bezüglich $+$ wird meist mit 0 bezeichnet.

1.1.D Reguläre und invertierbare Operationen

1.1.25 Definition. $\circ$ heißt *invertierbar* auf $A :\Leftrightarrow$

$$\forall (a,b) \in A^2 \; \exists (x,y) \in A^2 : a \circ x = b \text{ und } y \circ a = b.$$

1.1.26 Satz. *Sei $A \neq \emptyset$ und $\circ$ eine assoziative Operation auf A. Dann sind folgende Aussagen äquivalent:*

a) $\circ$ ist invertierbar auf A.

b) Es gibt ein neutrales Element e bezüglich $\circ$, und jedes $x \in A$ ist invertierbar, d. h., $\exists y \in A : x \circ y = y \circ x = e$.

Beweis. b) $\Rightarrow$ a): Für $x \in A$ bezeichne x^{-1} das Inverse von x. Seien $a, b \in A$. Dann gilt: $a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$ und $(b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b$.

a) $\Rightarrow$ b): Sei $a \in A$ beliebig, aber fest. Dann gilt: $\exists e_1, e_2 \in A : e_1 \circ a = a = a \circ e_2$ (setze $b = a$, $y = e_1$, $x = e_2$). Für beliebiges $b \in A$ gilt dann:

$$\exists x \in A : b = a \circ x \Rightarrow e_1 \circ b = e_1 \circ (a \circ x) = (e_1 \circ a) \circ x = a \circ x = b,$$
$$\exists y \in A : b = y \circ a \Rightarrow b \circ e_2 = (y \circ a) \circ e_2 = y \circ (a \circ e_2) = y \circ a = b.$$

Also ist e_1 Linkseinselement, e_2 Rechtseinselement und daher $e_1 = e_1 \circ e_2 = e_2 =: e$ Einselement.

Nun ist noch zu zeigen, dass zu jedem $x \in A$ ein Inverses y existiert. Da $\circ$ invertierbar, gilt:

$$\exists y_1, y_2 \in A : x \circ y_1 = e \text{ und } y_2 \circ x = e.$$

Also ist y_1 Rechtsinverses, y_2 Linksinverses von x, woraus $y_1 = y_2 =: y$ folgt und somit y invers zu x ist. □

1.1.27 Anmerkung. In dem eben bewiesenen Satz haben die Gleichungen $a \circ x = b$ und $y \circ a = b$ genau eine Lösung x, y. Aus $a \circ x_1 = b = a \circ x_2$ folgt nämlich $a^{-1} \circ (a \circ x_1) = a^{-1} \circ (a \circ x_2)$ und daraus (mit Hilfe des Assoziativgesetzes) $x_1 = x_2$. Analog für die zweite Gleichung.

1.1.28 Definition. Die Operation $\circ$ auf A heißt *regulär* oder *kürzbar* $:\Leftrightarrow \forall a, x_1, x_2, y_1, y_2 \in A : (a \circ x_1 = a \circ x_2 \Rightarrow x_1 = x_2)$ und $(y_1 \circ a = y_2 \circ a \Rightarrow y_1 = y_2)$.

Die Gleichungen $a \circ x = b$ und $y \circ a = b$ haben also bei einer kürzbaren Operation $\circ$ *höchstens* eine Lösung, bei einer invertierbaren assoziativen Operation $\circ$ *genau* eine Lösung.

In der Operationstafel: kürzbar $\Leftrightarrow$ jede Zeile (Spalte) enthält jedes Element *höchstens* einmal, invertierbar $\Leftrightarrow$ jede Zeile (Spalte) enthält jedes Element *mindestens* einmal.

Für endliches A gilt: $\circ$ invertierbar $\Leftrightarrow$ $\circ$ regulär (Übung).

Nach obiger Anmerkung gilt: $\circ$ ist invertierbar und assoziativ $\Rightarrow$ $\circ$ ist regulär.

1.1.29 Beispiel. $+, \cdot$ auf $\mathbb{N}$ sind regulär, aber *nicht* invertierbar.

1.1.E Abschluss

1.1.30 Definition. Sei A eine Menge, und sei ω eine partielle (möglicherweise auch totale) einstellige Operation auf A, also eine partielle Funktion von A nach A.
Eine Teilmenge $B \subseteq A$ heißt *abgeschlossen* unter ω, wenn aus $b \in B$ stets $\omega(b) \in B$ folgt.
Sei allgemeiner $\omega : A^n \to A$ eine n-stellige Operation ($n \geq 1$), dann nennen wir B „*abgeschlossen unter* ω“, wenn für alle $b_1, \ldots, b_n \in B$ auch $\omega(b_1, \ldots, b_n) \in B$ gilt.
B heißt *abgeschlossen* unter der nullstelligen Operation ω, wenn der (einzige) Wert von ω in B liegt.

1.1.31 Lemma.

1. *A ist unter jeder partiellen Operation auf A abgeschlossen.*
2. *Für $n \geq 1$ ist die leere Menge unter jeder partiellen n-stelligen Operation abgeschlossen (aber unter keiner nullstelligen Operation).*
3. *Der Durchschnitt von beliebig vielen unter ω abgeschlossenen Mengen ist selbst unter ω abgeschlossen.*
4. *Zu jeder Menge $S \subseteq A$ gibt es eine kleinste Obermenge, den „Abschluss von S unter ω“[6] $\bar{S} \subseteq A$, die unter ω abgeschlossen ist, nämlich den Durchschnitt aller abgeschlossenen Mengen, die S enthalten.*

Der Abschluss $\bar{S}$ von S kann auch so konstruiert werden: Sei $S_0 := S$. Induktiv definieren wir nun eine aufsteigende Folge von Mengen so:

$$S_{k+1} := S_k \cup \{\omega(b_1, \ldots, b_n) \mid b_1, \ldots, b_n \in S_k, (b_1, \ldots, b_k) \in dom(\omega)\}.$$

Wir setzen $S_\infty := \bigcup_{k=0}^{\infty} S_k$. Dann kann man einerseits (induktiv) zeigen, dass $S_k \subseteq \bar{S}$ gelten muss, somit auch $S_\infty \subseteq \bar{S}$, andererseits sieht man leicht, dass S_∞ unter ω abgeschlossen ist, somit $\bar{S} \subseteq S_\infty$. Daher ist S_∞ der Abschluss von S.
Dieses Argument zeigt auch den folgenden Satz:

1.1.32 Satz. *Sei $S \subseteq A$ höchstens abzählbar, das heißt: endlich oder abzählbar. Dann ist der Abschluss von S unter ω auch höchstens abzählbar (weil nämlich die Mengen S_k alle höchstens abzählbar sind und die Vereinigung von abzählbar vielen höchstens abzählbaren Mengen wieder höchstens abzählbar ist).*

Sei nun Ω eine Familie von (partiellen) Operationen auf der Menge A. Dann definieren wir die Begriffe „$S \subseteq A$ ist *abgeschlossen* unter Ω“ und „*Abschluss* von S unter Ω“ ganz analog: S heißt *abgeschlossen* unter Ω, wenn S unter jeder Operation $\omega \in \Omega$ abgeschlossen ist; der *Abschluss* von S ist die kleinste Menge $\bar{S} \subseteq A$, die S als Untermenge enthält und unter Ω abgeschlossen ist.

1.2 Präfix und Postfix

1.2.A Präfix, Infix, Postfix

Es gibt verschiedene Arten, binäre Operationen anzuschreiben.
Sei $\circ$ eine binäre Operation auf der Menge A, also $\circ : A \times A \to A$. Die Operation $\circ$ ordnet jedem Element von $A \times A$ (d.h., jedem geordnetem Paar (x, y) mit $x, y \in A$) ein Element z aus A zu.

[6] Diese Menge nennen wir auch „die von S erzeugte Unteralgebra von (A, ω)“ und schreiben sie als $\langle S \rangle$ oder $\langle S \rangle_\omega$ an, siehe Abschnitt 2.1.

- Wenn wir *Infixnotation* verwenden, schreiben wir das Ergebnis z dieser Operation als $x \circ y$ oder $(x \circ y)$ an.
  Diese Notation wird vor allem dann verwendet, wenn wir die zweistellige Operation als ein abstraktes Symbol (wie $\circ$, $+$, $*$, etc.) anschreiben.

- Wenn wir *Präfixnotation* (auch „polnische Notation“, Łukasiewicz-Notation) verwenden, schreiben wir das Ergebnis z dieser Operation als $\circ xy$ oder $\circ(x, y)$ an.
  Diese Notation wird vor allem dann verwendet, wenn wir die zweistellige Operation durch einen Buchstaben (wie f oder g) oder eine Buchstabengruppe (wie ggT) repräsentieren. Insbesondere werden daher benutzerdefinierte Funktionen in Programmiersprachen meist in Präfixform geschrieben. Auch für einstellige Funktionen wird meistens Präfixnotation verwendet (z.B. $\sin x$). Die Programmiersprache LISP betont diese Notation (z.B. `(cons a b)`).

- Wenn wir *Postfixnotation* (auch „umkehrte polnische Notation“, „reverse Polish notation“, RPN) verwenden, schreiben wir das Ergebnis z dieser Operation als $xy\circ$ an.
  Diese Notation wird in manchen Programmiersprachen verwendet (FORTH, PostScript) sowie auf manchen Taschenrechnern.

Kompliziertere Terme lassen sich ebenfalls in Infix-, Präfix- oder Postfixnotation schreiben. Den Term $(x \cdot y) + (a \cdot b)$ kann man

- in Präfixnotation als $+\cdot xy \cdot ab$ ausdrücken, das kann man von links nach rechts so lesen:

  $+$ die Summe von
  - $\cdot$ erstens dem Produkt aus
    - x
    - y
  - $\cdot$ und zweitens dem Produkt aus
    - a
    - b

- in Postfixnotation als $xy\cdot ab\cdot +$ ausdrücken, das kann man von links nach rechts als einen Algorithmus für die Berechnung des Terms lesen. „Man nehme x, y und bilde das Produkt; dann nehme man a und b und bilde das Produkt. Schließlich bilde man die Summe der beiden letzten Zwischenresultate.“

Auch Terme, in denen nicht nur binäre Operationen sondern auch Operationen mit anderen Stelligkeiten vorkommen, lassen sich in Präfix- oder Postfixnotation schreiben. Der Term $(-x) * (-y)$ (wo „$-$“ eine unäre Operation ist) sieht in Präfix- bzw Postfixnotation so aus:

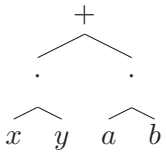
$$*-x-y \qquad x-y-*$$

Terme in Präfix- und Postfixnotation lassen sich ohne Verwendung von Klammern anschreiben. Natürlich muss hier die Stelligkeit der Operationen vorgegeben sein. Wenn etwa f und g zweistellig sind, dann ist mit $f\,x\,g\,y\,z$ der Term $f(x, g(y, z))$ gemeint. Wenn hingegen f dreistellig und g einstellig ist, so ist mit $f\,x\,g\,y\,z$ der Term $f(x, g(y), z)$ gemeint.

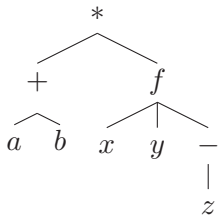
1.2.B Baumdarstellung

Terme in Präfix- und Postfixnotation lassen sich leicht in Baumdiagramme übersetzen. Ein Term t, der eine Summe darstellt (also t_1+t_2, bzw $+(t_1,t_2)$ bzw $t_1\,t_2\,+$), wird in einen Baum transformiert, dessen Wurzel (die traditionell oben geschrieben wird) mit dem Symbol $+$ markiert ist; von der Wurzel führt ein Zweig nach links und einer nach rechts; an diesen beiden Zweigen hängen die Bäume T_1 und T_2, die t_1 und t_2 repräsentieren:

Der Term $(x \cdot y) + (a \cdot b)$ wird durch den Baum



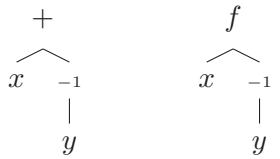
dargestellt, der Term $(a + b) * f(x, y, -z)$ durch den folgenden Baum:



Umgekehrt kann man aus der Baumdarstellung leicht Präfix-, Postfix- und Infixdarstellung ablesen. Wenn etwa der oben dargestellte Baum für $t_1 + t_2$ gegeben ist, übersetzt man zunächst (rekursiv) die Bäume T_1 und T_2 in Infixnotation t_1 und t_2; der Ausdruck $(t_1)+(t_2)$ ist dann die Infixnotation für den gesamten Baum.

1.2.C Gemischte Darstellung

Ein Element y, das (bezüglich einer zweistelligen Operation $*$) invers zu x ist (also $x * y = y * x = e$ erfüllt, mit e neutral), bezeichnet man oft mit x^{-1}. Das Symbol $^{-1}$ kann man hier als einstelliges Operationssymbol auffassen, das *immer* in Postfixnotation geschrieben wird. Es ist üblich, die Postfixnotation für $^{-1}$ auch dann anzuwenden, wenn für die anderen Symbole Präfix- oder Infixnotation verwendet wird. Die Terme mit Baumnotation



schreiben wir also $x+y^{-1}$ (Infix, gemischt mit Postfix) bzw. $f(x, y^{-1})$ (Präfix, gemischt mit Postfix).
Ähnliches gilt für manche anderen einstelligen Operationen, wie z.B. die Operation $x \mapsto x^2$.

1.2.D Terme

Im vorigen Abschnitt haben wir öfters den Ausdruck „Term“ verwendet, aber was genau bedeutet das? Statt einer formalen Definition (siehe dazu Abschnitt 3.1) geben wir eine informelle Beschreibung:

1.2.1 Definition. Ein „Term“ (in Präfixnotation) ist ein Ausdruck, der sich in sinnvoller Weise aus Variablen und/oder Operationssymbolen zusammensetzt. Jede Variable ist bereits ein Term; wenn $t_1, \ldots, t_k$ Terme sind und ω ein k-stelliges Operationssymbol ist, dann ist auch der „String“[7]

$$\omega t_1 \cdots t_k$$

wiederum ein Term. Überdies entstehen alle Terme durch wiederholte Anwendung (endlich oft) der gerade genannten Regeln.

Analog kann man einen Term in Postfix- oder Infix-Notation definieren. Auch Terme in Baumdarstellung lassen sich ähnlich beschreiben.

1.3 Einige wichtige Typen von Algebren

1.3.1 Definition. Eine Algebra $(A, \cdot)$ vom Typ (2) heißt ein *Gruppoid*[8].

Schreibweise: $a \cdot b =: ab, a, b \in A$.

1.3.2 Definition. Ein Gruppoid $(H, \cdot)$ heißt eine *Halbgruppe*[9] $:\Leftrightarrow$ $\cdot$ ist assoziativ.

1.3.3 Beispiel. $(M^M, \circ)$ ist eine Halbgruppe, die so genannte *symmetrische* Halbgruppe von M.

1.3.4 Definition. a) Eine Halbgruppe $(H, \cdot)$ heißt *Monoid* vom Typ (2) $:\Leftrightarrow$ es existiert ein neutrales Element e. (Es kann höchstens ein neutrales Element geben.)

b) Eine Algebra $(H, \cdot, e)$ vom Typ $(2, 0)$ heißt *Monoid* vom Typ $(2, 0)$ $:\Leftrightarrow$ die folgenden Gesetze gelten für alle $x, y, z \in H$:

1) $x(yz) = (xy)z$,

2) $ex = x$, $xe = x$.

Oft sprechen wir einfach von einem Monoid, ohne festzulegen, ob wir nun ein Monoid vom Typ (2) oder ein Monoid vom Typ (2,0) meinen. Dadurch können aber kaum Missverständnisse entstehen, da sich jedes Monoid vom Typ (2) in eindeutiger Weise als Monoid vom Typ (2,0) interpretieren lässt, und umgekehrt.

1.3.5 Definition. a) Ein Monoid $(G, \cdot)$ mit neutralem Element e heißt eine *Gruppe* vom Typ (2) $:\Leftrightarrow$ jedes $x \in G$ ist invertierbar, d. h., $\forall x \in G\ \exists x^{-1} \in G : xx^{-1} = x^{-1}x = e$.

b) Eine Algebra $(G, \cdot, e, {}^{-1})$ vom Typ $(2, 0, 1)$ heißt eine *Gruppe* vom Typ $(2, 0, 1)$ $:\Leftrightarrow$ die folgenden Gesetze gelten für alle $x, y, z \in G$:

[7] Wir begnügen uns hier mit der anschaulichen Vorstellung eines Strings oder einer Zeichenkette: Strings bestehen aus Symbolen, die aneinander gereiht werden; Strings können miteinander „verkettet“ werden und ergeben so einen neuen String. Aus der Verkettung von *abc* und *xyz* entsteht *abcxyz*. Wenn wir uns mit freien Halbgruppen beschäftigen, werden wir dieses Konzept noch genauer untersuchen.

[8] Die Nomenklatur ist nicht ganz einheitlich; in der Kategorientheorie bezeichnet man als Gruppoid etwas ganz anderes, nämlich eine Kategorie, in der alle Morphismen Isomorphismen sind.

[9] englisch: *semigroup*

1) $x(yz) = (xy)z$,

2) $ex = x$, $xe = x$,

3) $xx^{-1} = e$, $x^{-1}x = e$.

c) Eine Gruppe $(G, \cdot)$ bzw. $(G, \cdot, e, ^{-1})$ heißt *kommutativ* oder *abelsch* $:\Leftrightarrow \forall x, y \in G : xy = yx$.

1.3.6 Anmerkung. $(G, \cdot)$ ist Gruppe $\Leftrightarrow G \neq \emptyset$, $\cdot$ assoziativ und invertierbar.

1.3.7 Definition. a) Eine Algebra $(R, +, \cdot)$ vom Typ $(2, 2)$ heißt ein *Ring* vom Typ $(2, 2)$ $:\Leftrightarrow$

1) $(R, +)$ ist eine abelsche Gruppe,

2) $(R, \cdot)$ ist eine Halbgruppe,

3) $\cdot$ ist distributiv über $+$.

b) Eine Algebra $(R, +, 0, -, \cdot)$ vom Typ $(2, 0, 1, 2)$ heißt ein *Ring* vom Typ $(2, 0, 1, 2)$ $:\Leftrightarrow$

1) $(R, +, 0, -)$ ist eine abelsche Gruppe,

2) $(R, \cdot)$ ist eine Halbgruppe,

3) $\cdot$ ist distributiv über $+$.

Das Element 0 heißt „Nullelement“ des Ringes. Weiters vereinbaren wir die Schreibweise: $x - y := x + (-y)$.

Ähnlich wie bei Monoiden „identifizieren“[10] wir oft eine Gruppe vom Typ (2) mit der entsprechenden Gruppe vom Typ $(2, 0, 1)$, ebenso einen Ring vom Typ $(2, 2)$ mit dem entsprechenden Ring vom Typ $(2, 0, 1, 2)$.

1.3.8 Lemma. *Sei $(R, +, 0, -, \cdot)$ ein Ring. Dann gilt für alle $x, y, z \in R$:*

a) $x0 = 0 = 0x$,

b) $x(-y) = (-x)y = -(xy)$,

c) $(-x)(-y) = xy$,

d) $x(y - z) = xy - xz$, $(x - y)z = xz - yz$.

[10] Wenn wir sagen, dass wir X und Y „identifizieren“, dann bedeutet dies Folgendes: X und Y haben gewisse gemeinsame Eigenschaften; solange es nur um diese Eigenschaften geht, ist es egal, ob wir von X oder von Y sprechen. Wir lassen es sogar zu, dass wir von X sprechen, tatsächlich aber Y meinen. Wenn wir zum Beispiel sagen, dass die Gruppe der ganzen Zahlen kommutativ ist, dann spielt es keine Rolle, ob wir von der Gruppe $(\mathbb{Z}, +)$ (vom Typ (2)) oder von der Gruppe $(\mathbb{Z}, +, 0, -)$ (vom Typ $(2, 0, 1)$) sprechen. Auch hat eine Gruppe vom Typ (2) dieselben Untergruppen wie die entsprechende Gruppe vom Typ $(2, 0, 1)$.

Allerdings hat die algebraische Struktur $(\mathbb{Z}, +)$ mehr „Unteralgebren“ (siehe Abschnitt 2.1, Seite 26ff) als die Struktur $(\mathbb{Z}, +, 0, -)$, denn die natürlichen Zahlen bilden eine Unteralgebra (=Unterhalbgruppe) von $(\mathbb{Z}, +)$, nicht aber eine Unteralgebra (=Untergruppe) von $(\mathbb{Z}, +, 0, -)$, weil sie ja nicht unter der unären Operation „$-$“ abgeschlossen sind. Wenn es also um Unter*gruppen* geht, dürfen wir $(\mathbb{Z}, +, 0, -)$ mit $(\mathbb{Z}, +)$ „identifizieren“; wenn es um Unter*algebren* geht (was selten der Fall ist), nicht.

Beweis. a) $0 = 0 + 0 \Rightarrow x0 = x(0 + 0) = x0 + x0 \Rightarrow x0 - x0 = x0 + x0 - x0 \Rightarrow 0 = x0$. Analog für $0 = 0x$.

b) $y + (-y) = 0 \Rightarrow xy + x(-y) = x0 = 0 \Rightarrow xy + (-(xy)) + x(-y) = 0 + (-(xy))$ $\Rightarrow x(-y) = -(xy)$. Analog für $(-x)y = -(xy)$.

c) folgt aus b) und $-(-x) = x$.

d) $x(y - z) = x(y + (-z)) = xy + x(-z) = xy + (-(xz)) = xy - xz$. Analog für $(x - y)z = xz - yz$. □

1.3.9 Beispiele. $(\mathbb{Z}, +, 0, -, \cdot)$ und $(M_n(\mathbb{C}), +, 0, -, \cdot)$ sind Ringe.

1.3.10 Definition. a) Eine Algebra $(R, +, 0, -, \cdot, 1)$ vom Typ $(2, 0, 1, 2, 0)$ heißt ein *Ring mit Einselement* (oder auch *unitärer Ring*[11]) :$\Leftrightarrow$

1) $(R, +, 0, -, \cdot)$ ist ein Ring,

2) 1 ist neutrales Element bezüglich $\cdot$, d. h., $\forall x \in R : 1 \cdot x = x \cdot 1 = x$. (1 heißt „Einselement“ des Ringes.)

b) Ein Ring $(R, +, 0, -, \cdot)$ heißt *kommutativ* :$\Leftrightarrow \forall x, y \in R : xy = yx$.

c) Eine Algebra $(R, +, 0, -, \cdot, 1)$ heißt ein *kommutativer Ring mit Einselement* :$\Leftrightarrow$

1) $(R, +, 0, -, \cdot)$ ist ein kommutativer Ring,

2) 1 ist neutrales Element bezüglich $\cdot$.

1.3.11 Beispiel. $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist kommutativer Ring mit Einselement; ebenso jeder Körper (s. u.).

1.3.12 Definition. Ein kommutativer Ring mit Einselement $(R, +, 0, -, \cdot, 1)$ heißt ein *Integritätsbereich*[12] :$\Leftrightarrow$

1) $R \setminus \{0\} \neq \emptyset$ (d. h., $0 \neq 1$),

2) $\forall x, y \in R$: Wenn $x \neq 0$ und $y \neq 0$, dann $xy \neq 0$. Oder in äquivalenter Form: Wenn $xy = 0$ ist, dann muss $x = 0$ oder $y = 0$ gelten.

1.3.13 Lemma. *Ist $(R, +, 0, -, \cdot, 1)$ ein Integritätsbereich, dann ist $\cdot$ regulär auf $R \setminus \{0\}$.*

Beweis. Es seien $x, y, z \neq 0$. Dann gilt: $xy = xz \Rightarrow xy - xz = 0 \Rightarrow x(y - z) = 0 \Rightarrow y - z = 0$ $\Rightarrow y = z$. □

1.3.14 Anmerkung. In einem Integritätsbereich ist $(R \setminus \{0\}, \cdot, 1)$ ein kommutatives Monoid.

1.3.15 Beispiel. $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist ein Integritätsbereich.

[11] Manche Autoren verstehen unter „Ring“ das, was wir als „Ring mit Einselement“ bezeichnen.
[12] englisch: *integral domain*

1.3.16 Definition. a) Ein Ring mit Einselement $(R, +, 0, -, \cdot, 1)$ heißt ein *Schiefkörper*[13] :⇔

1) $0 \neq 1$,

2) $(R \setminus \{0\}, \cdot)$ ist eine Gruppe.

b) Ein kommutativer Ring mit Einselement $(R, +, 0, -, \cdot, 1)$ heißt ein *Körper*[14] :⇔

1) $0 \neq 1$,

2) $(R \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.

1.3.17 Beispiele. 1) $(\mathbb{Q}, +, 0, -, \cdot, 1)$, $(\mathbb{R}, +, 0, -, \cdot, 1)$, $(\mathbb{C}, +, 0, -, \cdot, 1)$ sind Körper.

2) Ohne Beweis: Jeder endliche Schiefkörper ist Körper (Satz von Wedderburn).

3) Ist p Primzahl, dann ist $(\mathbb{Z}_p, +, 0, -, \cdot, 1)$ Körper (mit p Elementen). (Zur genauen Definition des Restklassenrings $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ modulo n siehe Abschnitt 2.2.B)

1.3.18 Anmerkung. $\mathbb{Z}_n$ Körper $\Leftrightarrow$ n prim $\Leftrightarrow$ $\mathbb{Z}_n$ Integritätsbereich. (Siehe Abschnitt 5.3.)

1.3.19 Satz. *Jeder Körper ist ein Integritätsbereich. Jeder endliche Integritätsbereich ist ein Körper.*

Beweis. Die erste Aussage ist klar.

Sei nun $R = \{a_1, \ldots, a_n\}$ endlicher Integritätsbereich $\Rightarrow \cdot$ ist eine assoziative, reguläre Operation auf der endlichen Menge $R \setminus \{0\}$ $\Rightarrow \cdot$ ist invertierbar $\Rightarrow (R \setminus \{0\}, \cdot)$ ist abelsche Gruppe. □

1.3.20 Definition. Sei $(K, +, 0, -, \cdot, 1)$ ein Körper, $I = \{a, b, c\} \cup K$ mit $a, b, c \notin K$, a, b, c paarweise verschieden. Eine Algebra $(V, (\omega_i)_{i \in I})$ vom Typ $(2, 0, 1, (1)_{\lambda \in K})$ heißt *Vektorraum über*[15] K :⇔

1) $(V, \omega_a, \omega_b, \omega_c) =: (V, +, 0, -)$ ist eine abelsche Gruppe,

2) $\forall x, y \in V, \lambda, \mu \in K$:
$\omega_\lambda(x + y) = \omega_\lambda(x) + \omega_\lambda(y)$,
$\omega_{\lambda+\mu}(x) = \omega_\lambda(x) + \omega_\mu(x)$,
$\omega_{\lambda\mu}(x) = \omega_\lambda(\omega_\mu(x))$,
$\omega_1(x) = x$.

Im folgenden schreiben wir statt $\omega_\lambda(x)$ einfach $\lambda \cdot x$ oder nur[16] λx. setzen wir $\omega_\lambda =: \lambda$ und schreiben für den Vektorraum $(V, +, 0, -, K)$. Die Gesetze unter 2) lauten dann: $\lambda(x+y) = \lambda x + \lambda y$, $(\lambda + \mu)x = \lambda x + \mu x$, $(\lambda\mu)x = \lambda(\mu x)$, $1x = x$.
Die Elemente der Algebra nennen wir „Vektoren“. Die Elemente des Körpers (den wir uns meist als disjunkt zu unserer Algebra vorstellen) heißen Skalare. Wenn wir im Zusammenhang mit Vektorräumen von Homomorphismen, Unteralgebren, Kongruenzen etc. sprechen, beziehen wir uns immer auf den selben Körper.

[13] englisch: *skew field oder division ring*
[14] englisch: *field*
[15] englisch: *vector space*
[16] Dadurch wird also eine Abbildung $(\lambda, x) \mapsto \omega_\lambda(x)$ von $K \times V$ nach V definiert, die „Multiplikation mit Skalaren“. Man beachte, dass diese (so genannte „externe“) Verknüpfung zwar ähnlich notiert wird wie die Multiplikation in K, nämlich durch das Symbol $\cdot$ oder durch Nebeneinanderschreiben, aber dennoch keine „Operation“ (in unserem Sinne) auf der Menge V ist, denn Operationen müssen von einer endlichen Potenz von V (z.B. von V oder von V^2) nach V abbilden. In der Gleichung $(\lambda \cdot \mu) \cdot x = \lambda \cdot (\mu \cdot x)$ kommt links zunächst die Operation $\cdot$ des Körpers und dann die externe Verknüpfung vor, rechts zweimal die externe Verknüpfung.

1.4 Die komplexen Zahlen

Es gibt verschiedene Möglichkeiten, die komplexen Zahlen zu definieren; sie führen alle auf isomorphe Strukturen. Im Kapitel Körpertheorie werden wir die komplexen Zahlen als Faktorring des Polynomrings $\mathbb{R}[x]$ nach dem von x^2+1 erzeugten Ideal wiederfinden. In diesem Abschnitt skizzieren wir eine Konstruktion, die sich auf Vorkenntnisse aus der linearen Algebra stützt.

1.4.1 Definition. Sei $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ die 2×2-Einheitsmatrix über den reellen Zahlen, und sei $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Sei $\mathbb{C} := \{aE + bI \mid a, b \in \mathbb{R}\} = \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$.

Für $a, b \in \mathbb{R}$ nennen wir die Wurzel aus der Determinante von $z := aE + bI$, also die nichtnegative Zahl $\sqrt{a^2+b^2}$, den „absoluten Betrag“ von z, abgekürzt $|z|$. Offenbar gilt $|z| = 0$ genau dann, wenn $z = \mathbf{0}$. Weiters ist $|aE|$ der absolute Betrag (im üblichen Sinn) der reellen Zahl a.

1.4.2 Satz. *1. $\mathbb{C}$ (mit der üblichen Addition und Multiplikation von Matrizen) ist ein Unterring (siehe Abschnitt 2.1) des Rings der 2×2-Matrizen. Eingeschränkt auf $\mathbb{C}$ ist die Multiplikation kommutativ.*

2. Die Nullmatrix $\mathbf{0}$ ist neutral bezüglich Addition, die Matrix E ist neutral bezüglich Multiplikation. Weiters gilt $I^2 = -E$.

3. $\mathbb{C}$ ist Körper; wenn $aE + bI \neq \mathbf{0}$, dann ist $(aE + bI)(aE - bI) = (a^2 + b^2)E$, somit ist $\frac{a}{a^2+b^2}E + \frac{-b}{a^2+b^2}I$ das multiplikative Inverse zu $aE + bI$.

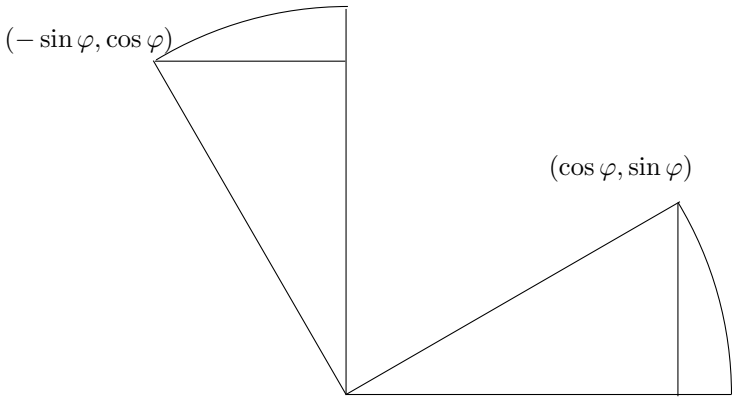
4. Die Abbildung $a \mapsto aE$ ist ein Isomorphismus zwischen $\mathbb{R}$ und einem Unterkörper von $\mathbb{C}$.

Wir schreiben ab jetzt statt $aE + bI$ einfach $a + bi$; das heißt, wir identifizieren ab jetzt jede reelle Zahl a mit der Matrix aE, und wir verwenden für die Matrix I einen Kleinbuchstaben, um von der Tatsache abzulenken, dass I eine Matrix ist, und um zu betonen, dass man mit i wie mit einer Zahl rechnen kann. In dieser Schreibweise übersetzt sich $I^2 = -E$ in $i^2 = -1$.

1.4.3 Satz.

(1) *Der absolute Betrag ist multiplikativ: $|x \cdot y| = |x| \cdot |y|$ für alle $x, y \in \mathbb{C}$.*

(2) *Wenn $|a + bi| = 1$, dann gibt es einen eindeutig bestimmten Winkel $\varphi \in [0, 2\pi)$ mit $a = \cos\varphi$, $b = \sin\varphi$. Die Matrix $aE + bI$, also $\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$, stellt in diesem Fall eine Drehung um den Winkel φ dar.*



(3) *Matrizenmultiplikation entspricht einer Hintereinanderausführung von Drehungen, das heißt:* $(\cos\varphi + i\,\sin\varphi)\cdot(\cos\psi + i\,\sin\psi) = \cos(\varphi+\psi) + i\,\sin(\varphi+\psi)$.

(4) *φ verhält sich also wie ein Logarithmus der Zahl $\cos\varphi + i\,\sin\varphi$. Da die Funktion $f(\varphi) = \cos\varphi + i\,\sin\varphi$ die Differentialgleichung $f'(\varphi) = -\sin\varphi + i\,\cos\varphi = i\cdot f(\varphi)$ mit der Anfangsbedingungs $f(0) = 1$ erfüllt — ebenso[17] wie die Funktion $\varphi \mapsto e^{i\varphi}$ — ist die Schreibweise $e^{i\varphi}$ für $\cos\varphi + i\,\sin\varphi$ sinnvoll.*[18]

(5) *$e^{\frac{\pi}{2}i} = i$, $e^{\pi i} = -1$, $e^{2\pi i} = 1$. Weiters gilt $e^{i\varphi} = e^{i\psi}$ genau dann, wenn die Differenz $\varphi - \psi$ ein ganzzahliges Vielfaches von 2π ist.*

(6) *Jedes Element $z \in \mathbb{C}\setminus\{0\}$ lässt sich eindeutig in der Form $z = r\cdot e^{i\varphi}$ mit $r \in \mathbb{R}$, $r > 0$, $\varphi \in [0, 2\pi)$ darstellen.*
Für die Multiplikation gilt $re^{i\varphi}\cdot se^{i\psi} = (rs)\cdot e^{i(\varphi+\psi)}$.

(7) *Sei $n \geq 1$ eine natürliche Zahl. Dann hat die Gleichung $z^n = 1$ genau n Lösungen in den komplexen Zahlen:*

$$z^n = 1 \;\Leftrightarrow\; z \in \{\, 1 = e^{\frac{2\pi i 0}{n}},\, e^{\frac{2\pi i}{n}},\, \ldots,\, e^{\frac{2\pi i(n-1)}{n}} \,\}.$$

Die Lösungen dieser Gleichungen heißen n-te Einheitswurzeln.

(8) *Sei $s\cdot e^{i\psi}$ eine beliebige komplexe Zahl $\neq 0$, s eine positive reelle Zahl, $\psi \in [0, 2\pi)$. Dann hat die Gleichung $x^n = s\,e^{i\psi}$ genau n Lösungen in $\mathbb{C}$; eine Lösung ist die Zahl $\sqrt[n]{s}\,e^{i\frac{\psi}{n}}$, die weiteren Lösungen erhält man durch Multiplikation dieser Lösung mit den Einheitswurzeln:*

$$x^n = s\,e^{i\psi} \;\Leftrightarrow\; \exists k \in \{0,\ldots,n-1\}\; x = \sqrt[n]{s}\,e^{i\frac{\psi+2\pi k}{n}}.$$

Beweis. (1) ist leicht nachzurechnen. (2) setzen wir als aus der Analysis bekannt voraus.
(3) folgt direkt aus der geometrischen Anschauung oder aus den Additionstheoremen für die trigonometrischen Funktionen.
(5) ergibt sich durch Einsetzen, z.B. $e^{i\pi} = \cos\pi + i\sin\pi = -1 + 0\cdot i = -1$.
Die Beziehung $e^{i\varphi} = e^{i\psi}$ gilt genau dann, wenn $e^{i\varphi}\,e^{-i\psi} = 1$ ist, also wenn $\cos(\varphi-\psi) = 1$ ist.
(6) Man muss offenbar $r := |z|$ wählen; Existenz und Eindeutigkeit von φ folgt aus (2) und (5).
(7) Jede Lösung der Gleichung $z^n = 1$ in den komplexen Zahlen muss $|z|^n = 1$, also $|z| = 1$ erfüllen, hat also die Form $e^{i\varphi}$. Weiters gilt $z^n = e^{i\varphi n} = 1$, daher muss $i\varphi n$ von der Form $2\pi ik$ mit $k \in \mathbb{Z}$ sein, also $\varphi = \frac{2\pi k}{n}$. Für $\varphi \in [0, 2\pi)$ muss $k \in \{0,\ldots,n-1\}$ gelten.
(8) folgt aus (6) und (7). □

1.5 Äquivalenzrelationen und Klasseneinteilungen

1.5.1 Definition. Für Mengen A, B bezeichnen wir mit $A\times B$ die Menge aller „geordneten Paare“ (a, b), die $a \in A$ und $b \in B$ erfüllen.
Insbesondere ist $A \times A$ die Menge aller geordneten Paare (a, b) mit $a, b \in A$.

[17] Die Frage, wie diese Funktion definiert ist, und ob die Ableitung erstens existiert und zweitens die üblichen Regeln erfüllt, überlassen wir der Analysis

[18] Je nach Zugang bzw. nach Geschmack kann man die Beziehung $e^{i\varphi} = \cos\varphi + i\,\sin\varphi$ als abkürzende *Schreibweise*, als wichtige *Eigenschaft* der Exponentialfunktion (die man etwa mit Hilfe der Reihendarstellung beweisen kann) oder als Teil der *Definition* der Exponentialfunktion auf den komplexen Zahlen sehen.

Wenn A und B endliche Mengen mit k bzw. n Elementen sind, dann hat $A \times B$ $n \cdot k$ Elemente.

1.5.2 Definition. Ist M eine Menge, dann heißt jede Teilmenge R von $M \times M$ eine *binäre* oder *zweistellige Relation* auf M. (Eine binäre Relation ist also eine Menge von geordneten Paaren.)
Statt $(x, y) \in R$ schreibt man meist xRy.
Eine *einstellige* (*unäre*) Relation ist einfach eine Teilmenge von M.

Spezielle Relationen: $\alpha_M := M \times M$ heißt *Allrelation*, $\iota_M := \{(x, x) \mid x \in M\}$ heißt *identische Relation*, *Gleichheitsrelation* oder *Diagonale*.[19]
Die leere Menge ist eine Relation (auf jeder Menge M).[20]

1.5.3 Definition. Eine Relation $R \subseteq M \times M$ heißt:

1) *reflexiv (auf M)* $:\Leftrightarrow \iota_M \subseteq R$, d. h., $\forall x \in M : xRx$.

2) *symmetrisch* $:\Leftrightarrow \forall x, y \in M : xRy \Rightarrow yRx$.

3) *antisymmetrisch* $:\Leftrightarrow \forall x, y \in M : (xRy \text{ und } yRx) \Rightarrow x = y$.

4) *transitiv* $:\Leftrightarrow \forall x, y, z \in M : (xRy \text{ und } yRz) \Rightarrow xRz$.

Eine Relation mit 1), 2) und 4) heißt *Äquivalenzrelation*, eine mit 1), 3) und 4) *Halbordnung* oder *partielle Ordnung*.

1.5.4 Beispiele. 1) α_M und ι_M sind stets Äquivalenzrelationen. $\leq$ auf $\mathbb{R}$, $\subseteq$ auf $\mathfrak{P}(M)$ und $|$ („teilt“) auf $\mathbb{N}$ sind Halbordnungen.

2) Sei $m \in \mathbb{Z}$, $m \geq 2$ gegeben. Dann ist die Relation $\equiv \bmod m$ auf $\mathbb{Z}$ definiert durch

$$a \equiv b \bmod m \ :\Leftrightarrow \ m|(b - a)$$

eine Äquivalenzrelation auf $\mathbb{Z}$. Für $a \equiv b \bmod m$ sagt man: *a ist kongruent zu b modulo m*, m heißt in diesem Zusammenhang *Modul*.

Für Äquivalenzrelationen verwenden wir meistens die griechischen Buchstaben θ, π, ρ, σ, oder aber Symbole wie $\sim$, $\equiv$, $\approx$, etc. Die Symbole sind vor allem dann praktisch, wenn wir die Äquivalenzrelation als *Prädikat* oder Eigenschaft betrachten, also uns dafür interessieren, welche Elemente zu einander in Relation stehen: $a \sim b$, $a \not\sim c$, etc. Buchstaben sind hingegen dann typographisch passender, wenn wir uns für die Äquivalenzrelationen als *Objekte* und für die Beziehungen zwischen diesen Relationen interessieren, z.B. $\theta \neq \omega_A$, $\rho \subseteq \sigma$, etc.
Wenn θ eine Äquivalenzrelation auf der Menge M ist, a ein Element von M, dann nennen wir die Menge

$$[a]_\theta := \{x \in M \mid x \ \theta \ a\}$$

die „(Äquivalenz-)Klasse von a“. Statt $[a]_\theta$ schreibt man manchmal nur $[a]$, manchmal auch a/θ.

[19] Die Allrelation bezeichnet man manchmal auch mit ω_A oder ∇_A, die Gleichheitsrelation mit „=“ oder Δ_A.

[20] Der leeren Menge wird entweder keine Stelligkeit zugeordnet, oder aber eine Stelligkeit, die sich aus dem Kontext ergibt. Gelegentlich wird auch zwischen der „einstelligen“ leeren Menge $\emptyset \subseteq M$ und der „zweistelligen“ leeren Menge $\emptyset \subseteq M^2$ unterschieden.

1.5.5 Beispiel. Für die Äquivalenzrelation $\equiv \mathrm{mod} m$ auf $\mathbb{Z}$ ist die Äquivalenzklasse eines Elements $a \in \mathbb{Z}$ gegeben durch $[a] = \{a + km \mid k \in \mathbb{Z}\}$. Falls über den Modul m kein Zweifel besteht, schreibt man für die Klasse $[a]$ auch kurz $\bar{a}$.

1.5.6 Definition. Sei M eine Menge. $\mathcal{P} \subseteq \mathfrak{P}(M)$ heißt *Klasseneinteilung* oder *Partition* $:\Leftrightarrow$

1) $\bigcup_{C \in \mathcal{P}} C = M$,

2) $\emptyset \notin \mathcal{P}$,

3) $A, B \in \mathcal{P} \Rightarrow A = B$ oder $A \cap B = \emptyset$ (d. h., die Mengen in $\mathcal{P}$ sind paarweise disjunkt).

Die Elemente der Partition P (die also alle nichtleere Teilmengen von M sein müssen) heißen *Klassen* von P.

1.5.7 Satz. *Sei π Äquivalenzrelation auf der Menge M, $a \in M$ und $M/\pi := \{[a]_\pi \mid a \in M\}$ die Menge aller Äquivalenzklassen bezüglich π. (M/π heißt auch* Faktor- *oder* Quotientenmenge *von M nach π.)*
Dann ist M/π Klasseneinteilung von M.

Ist umgekehrt $\mathcal{P}$ eine Klasseneinteilung von M und π definiert durch $a \,\pi\, b :\Leftrightarrow \exists C \in \mathcal{P} : a, b \in C$, dann ist π eine Äquivalenzrelation auf M, und es gilt $M/\pi = \mathcal{P}$.

$\pi \mapsto M/\pi$ ist eine bijektive Abbildung von der Menge aller Äquivalenzrelationen von M auf die Menge aller Klasseneinteilungen von M. Die Umkehrabbildung ist gegeben durch obige Vorschrift $\mathcal{P} \mapsto \pi$.

Beweis. Übungsaufgabe. □

1.5.8 Satz. *Seien M, N Mengen, $f : M \to N$ eine Abbildung und $x \,\pi_f\, y :\Leftrightarrow f(x) = f(y)$. Dann gilt:*

a) π_f ist eine Äquivalenzrelation auf M, genannt der Kern von f.

b) Die Abbildung

$$\begin{cases} M/\pi_f \to f(M) := \{f(x) \mid x \in M\} \subseteq N \\ [x]_{\pi_f} \mapsto f(x) \end{cases}$$

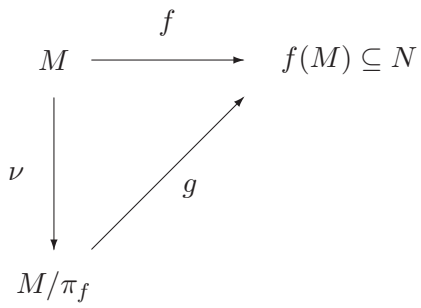
ist wohldefiniert und bijektiv.

Umgekehrt gilt: Sei θ eine beliebige Äquivalenzrelation auf M. Dann gibt es eine Menge N (nämlich M/θ) und eine Abbildung $f : M \to N$ (die so genannte kanonische Abbildung) sodass $\theta = \pi_f$.

Kurz gesagt: Jede Abbildung induziert eine Äquivalenzrelation, ihren Kern; umgekehrt wird jede Äquivalenzrelation durch ihre kanonische Abbildung induziert.

Beweis. Übungsaufgabe. □

1.5.9 Anmerkung. Der in obigem Satz beschriebene Sachverhalt lässt sich durch das folgende *kommutative Diagramm* veranschaulichen:



Hier ist

$$\nu : \begin{cases} M \to M/\pi_f \\ x \mapsto [x]_{\pi_f} \end{cases}$$

die *kanonische* oder *natürliche* Abbildung und g die Abbildung

$$\begin{cases} M/\pi_f \to f(M) \\ [x]_{\pi_f} \mapsto f(x). \end{cases}$$

Es gilt: $f = g \circ \nu$.

1.6 Partielle Ordnungen und Verbände

1.6.1 Definition. Eine „partielle Ordnung“ ist eine Menge P zusammen mit einer zweistelligen Relation R auf P, die antisymmetrisch, transitiv und reflexiv ist (siehe 1.5.3).

Für die Relation R verwendet man meistens eines der Symbole $\leq$, $\sqsubseteq$, $\precsim$, ...; damit ergibt sich die übliche Schreibweise $x \leq y$ (statt $(x, y) \in \leq$ oder $\leq(x, y)$).

1.6.2 Definition. Sei $(P, \leq)$ partielle Ordnung, $A \subseteq P$, $s \in P$. s heißt *obere Schranke* für A, wenn $a \leq s$ für alle $a \in A$ gilt. s heißt „*größtes Element* von A“, wenn s erstens obere Schranke für A und zweitens sogar Element von A ist. Analog sind die Begriffe „*untere Schranke*“ und „*kleinstes Element*“ definiert.
Die kleinste obere Schranke einer Menge A (so etwas muss nicht existieren; es kann zum Beispiel sein, dass A gar keine obere Schranken hat, oder auch, dass die Menge der oberen Schranken kein kleinstes Element hat) nennen wir $\sup A$, das Supremum von A. Die größte untere Schranke heißt $\inf A$, das Infimum von A.

Man beachte: Eine obere Schranke für A kann (muss aber nicht) in A liegen. Weiters gilt: Jedes Element $s \in P$ ist obere Schranke für die leere Menge, und jede einelementige Menge ist (durch ihr einziges Element) beschränkt.

1.6.3 Beispiel. Sei $P = \{1, 2, 3, 4, 6\}$. Die Relation

$$| \;:=\; \{(1,1),(2,2),(3,3),(4,4),(6,6)\} \cup \{(1,2),(1,3),(1,4),(1,6),\ (2,4),(2,6),(3,6)\},$$

die man üblicherweise als „Teilbarkeitsrelation“ bezeichnet, ist eine partielle Ordnung auf P. Bezüglich dieser Ordnung gilt: Die Menge $\{1, 2\}$ ist nach oben beschränkt, sowohl durch 2 als auch durch 4 als auch durch 6. (2 ist die kleinste aller dieser oberen Schranken.)
Die einzige (und daher auch kleinste) obere Schranke der Menge $\{2, 3\}$ ist die Zahl 6.
Die Menge $\{3, 4\}$ hat keine obere Schranke.

1.6.4 Definition. Sei $(P, \leq)$ partielle Ordnung. P heißt „*Verband*“,[21,22] wenn jede zweielementige Teilmenge von P sowohl eine kleinste obere als auch eine größte untere Schranke hat.
Schreibweise: $x \vee y := \sup\{x, y\}$. $x \wedge y := \inf\{x, y\}$.
P heißt *vollständiger Verband*, wenn jede Teilmenge von P sowohl eine kleinste obere als auch eine größte untere Schranke hat.

1.6.5 Satz. *Sei P eine partielle Ordnung, in der jede Teilmenge eine größte untere Schranke hat. Dann hat in P auch jede Teilmenge eine kleinste obere Schranke.*

Beweis. Übungsaufgabe. □

1.6.6 Beispiel. Sei X eine Menge, und sei V eine Familie von Teilmengen von X, die unter beliebigen Schnitten abgeschlossen ist, mit $X \in V$. Dann ist $(V, \subseteq)$ ein vollständiger Verband, denn für jede[23] Teilmenge $T \subseteq V$ ist $Z := \bigcap T := \bigcap_{Y \in T} Y$ in V. Nach Definition ist Z untere Schranke für T (d.h., $Z \subseteq Y$ für alle $Y \in T$, und es ist auch klar, dass Z die größte untere Schranke ist.
Konkrete Beispiele für diese Situation: V könnte die Menge aller Untergruppen einer Gruppe sein (siehe Abschnitt 2.1) oder die Menge aller abgeschlossenen Teilmengen eines topologischen oder metrischen Raums auf der Grundmenge X.

1.7 Grundbegriffe der Gruppentheorie

1.7.1 Definition. Sei $(G, \cdot)$ ein Gruppoid, $a_1, \ldots, a_n \in G$ $(n \in \mathbb{N})$, dann ist das *Produkt* $a_1 \cdots a_n$ induktiv definiert durch $a_1 \cdots a_n := (a_1 \cdots a_{n-1})a_n$.

1.7.2 Beispiel. $a_1a_2a_3a_4 = (a_1a_2a_3)a_4 = ((a_1a_2)a_3)a_4$.

1.7.3 Definition. Sei $(G, \cdot)$ ein Gruppoid, $a \in G$, dann sind die *Potenzen*[24] von a definiert durch: $a^1 := a$, $a^{n+1} := (a^n)a$ $(n \in \mathbb{N})$.

1.7.4 Anmerkungen. 1) Beim Rechnen mit Produkten in einer Halbgruppe dürfen Klammern beliebig eingeführt werden. (Übungsbeispiel)

2) In einer kommutativen Halbgruppe gilt: $a_1 \cdots a_n = a_{\pi(1)} \cdots a_{\pi(n)}$, wann immer π eine Permutation der Menge $M = \{1, \ldots, n\}$ ist.

1.7.5 Satz. *Sei $(G, \cdot, e, {}^{-1})$ eine Gruppe, $a, b \in G$. Dann gilt $(ab)^{-1} = b^{-1}a^{-1}$.*

Beweis. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = a(ea^{-1}) = aa^{-1} = e$. □

1.7.6 Folgerung. $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ (Induktion nach n).

1.7.7 Definition. Sei $(G, \cdot, e, {}^{-1})$ eine Gruppe, $a \in G$. Für $n \in \mathbb{N}$ sei a^n wie oben definiert. Weiters sei $a^0 := e$ und $a^{-n} := (a^{-1})^n$, $n \in \mathbb{N}$.

1.7.8 Satz (Rechenregeln für Potenzen in Gruppen). *Für alle $a, b \in G$, $n, m \in \mathbb{Z}$ gilt:*

[21] englisch: *lattice*
[22] Genauer: Verband im ordnungstheoretischen Sinn. Später werden wir eine algebraische Version dieser Definition kennenlernen.
[23] Für $T = \emptyset$ definieren wir $\bigcap T := X$; mit dieser Definition treffen die nun folgenden Überlegungen auch auf diesen Fall zu.
[24] englisch: *power*

a) $a^n a^m = a^{n+m}$,

b) $(a^m)^n = a^{mn}$,

c) $(ab)^n = a^n b^n$, *falls* $\cdot$ *kommutativ ist.*

Beweis. Durch Fallunterscheidungen. Z. B. b) für $n > 0$:

$$(a^m)^n = \underbrace{a^m \cdots a^m}_{n \text{ mal}} = a^{\overbrace{m+\cdots+m}^{n \text{ mal}}} = a^{nm}.$$

□

1.7.9 Anmerkung. Diese Regeln gelten für $m, n \in \mathbb{N}$ auch in Halbgruppen.

1.7.10 Definition. Sei $(G, \cdot, e, ^{-1})$ eine Gruppe, $a \in G$. Dann heißt

$$|\{a^0 = e, a^1, a^{-1}, a^2, a^{-2}, \ldots\}| = |\{a^k \mid k \in \mathbb{Z}\}|$$

die *Ordnung*[25] *von* a, symbolisch $\mathrm{o}(a)$.

1.7.11 Anmerkung. $\mathrm{o}(a) \in \mathbb{N}$ oder $\mathrm{o}(a) = |\mathbb{N}| = \aleph_0 (= \infty)$.

1.7.12 Beispiele. 1) In $(\mathbb{Z}, +, 0, -)$ schreiben wir (ebenso wie in allen Gruppen, bei denen „+“ als Operationszeichen verwendet wird) na anstelle von a^n. Die obigen Rechenregeln lauten dann: (i) $ma + na = (m + n)a$, (ii) $n(ma) = (mn)a$, (iii) $n(a + b) = na + nb$. („Additive Schreibweise“.) Es gilt $\mathrm{o}(0) = 1$, $\mathrm{o}(k) = \infty$ für alle $k \in \mathbb{Z}$, $k \neq 0$. (In jeder Gruppe gilt $\mathrm{o}(e) = 1$.)

2) In der Gruppe $(\mathbb{C} \setminus \{0\}, \cdot, 1, ^{-1})$ gilt: $\mathrm{o}(1) = 1$, $\mathrm{o}(-1) = 2$, $\mathrm{o}(i) = \mathrm{o}(-i) = 4$.

1.7.13 Anmerkung. Die additive Schreibweise $(G, +, 0, -)$ wird meist nur für kommutative Gruppen verwendet, die multiplikative Schreibweise $(G, \cdot, 1, ^{-1})$ für beliebige Gruppen.

1.7.14 Definition. Sei $(G, \cdot, e, ^{-1})$ eine Gruppe. Dann heißt $|G|$ (die Mächtigkeit von G) die *Ordnung* der Gruppe. Allgemeiner heißt für eine Algebra $(A, (\omega_i)_{i \in I})$ die Mächtigkeit $|A|$ die *Ordnung* der Algebra.

Für alle $a \in G$ gilt: $\mathrm{o}(a) \leq |G|$.

1.7.15 Lemma (Division mit Rest).

$$\forall k, l \in \mathbb{Z} : \Big(l \neq 0 \Rightarrow \exists q, r \in \mathbb{Z} : 0 \leq r < |l| \text{ und } k = lq + r \Big).$$

Beweis. Wir betrachten zunächst den Fall $k \geq 0$, $l > 0$. Die Menge

$$\{n \in \mathbb{N}_0 \mid l \cdot n \leq k\}$$

kann nur Zahlen $n \leq k$ enthalten (weil für $n > k$ auch $l \cdot n > k$ gilt). Daher ist diese Menge endlich (und sicher nicht leer), hat also ein maximales Element $q := \max\{n \in \mathbb{N}_0 \mid l \cdot n \leq k\}$. Dann ist $l \cdot q \leq k < l \cdot (q + 1)$, also $0 \leq k - lq < l$. Sei $r := k - lq$, dann ist $k = lq + r$ mit $0 \leq r < l$.

[25] englisch: *order*

Die anderen Fälle ($k < 0$, und/oder $l < 0$) können auf den ersten Fall zurückgeführt werden. Wenn zum Beispiel $k < 0$ und $l > 0$ gilt, dann können wir das Ergebnis des ersten Falls auf $-k$ und l anwenden und erhalten $-k = lq + r$; wenn $r = 0$ ist, dann erhalten wir die Darstellung $k = -lq = lq' + r'$ mit $q' := -q$, $r' := 0$; wenn $0 < r < l$, dann erhalten wir $k = -lq - r = l(-q-1) + l - r = lq' + r'$ mit $q' := -q - 1$, $r' := l - r$. □

1.7.16 Definition. Für $n \in \mathbb{N}_0$, $r, s \in \mathbb{Z}$ ist $r \equiv s \bmod n$ („r kongruent s modulo n“) :$\Leftrightarrow$ $n|(r-s)$ (n teilt $(r-s)$).

Es gilt: 1) $r \equiv s \bmod n \Leftrightarrow r = s + kn$, $k \in \mathbb{Z} \Leftrightarrow r, s$ haben denselben Rest bei Division durch n.

2) $\equiv \bmod n$ ist eine Äquivalenzrelation (siehe später).

1.7.17 Satz. *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe und $a \in G$.*

a) Ist $\mathrm{o}(a) = \infty$, so sind die Potenzen von a paarweise verschieden.

b) Ist $\mathrm{o}(a) = n \in \mathbb{N}$, dann gilt $n = \min\{m \in \mathbb{N} \mid a^m = e\}$ und $\{a^k \mid k \in \mathbb{Z}\} = \{a^0 = e, a^1, \ldots, a^{n-1}\}$. Weiters ist $a^r = a^s \Leftrightarrow r \equiv s \bmod n$.

Beweis. a) Sei $\mathrm{o}(a) = \infty$. Annahme: $\exists r, s \in \mathbb{Z} : r > s$ und $a^r = a^s$. Für $m := r - s \in \mathbb{N}$ gilt dann $a^m = e$. Sei $k \in \mathbb{Z}$. Dann ist $k = mq + l$ mit $q \in \mathbb{Z}$, $l \in \mathbb{N}_0$ und $0 \leq l < m$. Daraus folgt $a^k = a^{mq+l} = (a^m)^q a^l = e^q a^l = a^l$, also $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{m-1}\}$. Widerspruch!

b) Ist $\mathrm{o}(a) = n \in \mathbb{N}$, dann gibt es nach a) ein $m \in \mathbb{N}$ mit $a^m = e$, und weiters gilt $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{m-1}\}$. Sei $n_0 = \min\{m \in \mathbb{N} \mid a^m = e\}$. Dann ist $a^{n_0} = e$ und $n \leq n_0$. Die Elemente $e, a, \ldots, a^{n_0-1}$ sind paarweise verschieden. Denn wäre dies nicht der Fall, also $a^r = a^s$ für $0 \leq s < r < n_0$, dann würde gelten $a^{r-s} = e$ für $0 < r - s < n_0$ — Widerspruch zur Minimalität von n_0. Also gilt auch $n \geq n_0$ und damit $n = n_0$. Es gilt somit $\{a^k \mid k \in \mathbb{Z}\} = \{e, a, \ldots, a^{n-1}\}$.

Wir zeigen nun noch $a^r = a^s \Leftrightarrow r \equiv s \bmod n$.

$\Rightarrow$: $a^r = a^s$, $r > s \Rightarrow a^{r-s} = e$, $r - s > 0$, $r - s = nq + l$, $0 \leq l < n \Rightarrow e = a^{r-s} = (a^n)^q a^l = e^q a^l = a^l \Rightarrow l = 0 \Rightarrow r - s = nq \Rightarrow r \equiv s \bmod n$.
$\Leftarrow$: $r \equiv s \bmod n \Rightarrow r - s = nq \Rightarrow a^{r-s} = a^{nq} = (a^n)^q = e \Rightarrow a^r = a^s$. □

1.7.18 Beispiel. Sei M Menge und $S_M := \{f : M \to M \mid f \text{ bijektiv}\}$. $(S_M, \circ, \mathrm{id}_M, ^{-1})$ ist eine Gruppe, die *symmetrische Gruppe auf M* (Übungsbeispiel). Die Elemente von S_M heißen auch *Permutationen* von M. Ist $M = \{1, 2, \ldots, n\}$, schreibt man S_n anstelle von S_M. Es gilt: $|S_n| = n!$. So ist z. B.

$$S_3 = \left\{ \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} \right\},$$

in *Zyklenschreibweise*:

$$S_3 = \{(1), (123), (132), (23), (13), (12)\}.$$

Die geraden Permutationen bilden die *alternierende* Gruppe A_n. So ist z. B.

$$A_3 = \{(1), (123), (132)\}.$$

(Zur Definition von geraden und ungeraden Permutationen siehe die Vorlesung „Lineare Algebra I“.)

Die Ordnungen der Elemente der S_3:

π	$\mathrm{o}(\pi)$
(1)	1
(123)	3
(132)	3
(23)	2
(13)	2
(12)	2

Es gilt: Jedes Element der S_n lässt sich als Produkt elementfremder Zyklen darstellen. Diese Darstellung ist bis auf die Reihenfolge der Zyklen eindeutig. Z. B. besitzt die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 8 & 5 & 4 & 1 & 3 & 2 & 7 \end{pmatrix}$$

aus der S_9 die Zyklendarstellung (16)(29738)(45). Es ist $\mathrm{o}(\pi) = 2 \cdot 5 = \mathrm{kgV}(2, 5, 2)$. Allgemein: Ein Zyklus der Länge k hat die Ordnung k. Die Ordnung eines Produkts elementfremder Zyklen ist das kleinste gemeinsame Vielfache der Ordnungen der Faktoren.