1.1.2 Symbolisches Rechnen

Taschenrechner und mathematische Software wie Matlab arbeiten in der Regel numerisch, das heißt das Ergebnis eines Rechenausdrucks zum Beispiel der Form

$$(1 - \frac{1}{4}) \cdot \frac{4}{9}$$

wird etwa als 0.3333333333 ausgegeben, während Terme der Form

$$a^2 - (a - b)(a + b)$$

nur dann ausgewertet werden können, wenn a und b mit bestimmten Zahlwerten belegte Variable sind. Mathematische Software wie Maple, Mathematica oder Singular können dagegen Rechenausdrücke unter Verwendung von Eigenschaften innerer Verknüpfungen wie dem Assoziativ- oder Distributivgesetz in gleichwertige, einfachere Ausdrücke umformen. Ein solches Computeralgebrasystem (CAS) kann im ersten Fall das Ergebnis $\frac{1}{3}$ und im zweiten Fall b^2 liefern.

Im folgenden Abschnitt wird das Rechnen mit Potenzen als Komponente des symbolischen Rechnens diskutiert; das Thema wird im Abschnitt über Gruppen erneut aufgegriffen.

Potenzrechnung in Halbgruppen: Um in einer Halbgruppe $(H, \cdot)$ effizient rechnen zu können, führt man eine Potenzrechnung analog zu der der reellen Zahlen ein. Für jedes $h \in H$ definiert man rekursiv

$$h^1 := h, \quad \forall n \in \mathbb{N} \quad h^{n+1} := h \cdot h^n. \tag{2}$$

Die Regeln für das Rechnen mit Potenzen übertragen sich dann weitgehend:

Satz 16: *In einer Halbgruppe $(H, \cdot)$ gelten die Rechenregeln*

1. $\forall h \in H,\ m, n \in \mathbb{N} \quad h^{m+n} = h^m \cdot h^n$,
2. $\forall h \in H,\ m, n \in \mathbb{N} \quad (h^m)^n = h^{mn}$,
3. *Besitzen $g, h \in H$ die Eigenschaft $g \cdot h = h \cdot g$, so gilt:*
   $\forall m \in \mathbb{N} \quad (g \cdot h)^m = g^m \cdot h^m$.

Beweis: Zu Punkt 1: Man führt eine vollständige Induktion nach $s := m + n$ durch.

Induktionsanfang ($s = 2$): In diesem Fall ist $m = n = 1$ und daher gilt $h^2 = h \cdot h$ nach Definition.

Induktionsschritt: Es sei $s > 2$ und $s = m + n$, $m, n \in \mathbb{N}$. Dann ist ohne Einschränkung der Allgemeinheit $m > 1$ und daher $m - 1 \in \mathbb{N}$. Nach Induktionsannahme gilt

$$h^{m-1+n} = h^{m-1} \cdot h^n$$

und daher

$$h^{m+n} = h \cdot h^{m-1+n} = h \cdot (h^{m-1} \cdot h^n) = (h \cdot h^{m-1}) \cdot h^n = h^m \cdot h^n,$$

wobei man für die erste und vierte Gleichung die Definition (2) benutzt, und für die dritte das Assoziativgesetz.

Zu Punkt 3: Man führt eine vollständige Induktion nach m durch.

Induktionsanfang ($m = 1$): In diesem Fall ist nichts zu beweisen.

Induktionsschritt: Es sei $m > 1$. Dann ergibt sich sukzessive:

$$\begin{aligned}
(g \cdot h)^m &= (g \cdot h) \cdot (g \cdot h)^{m-1} && \text{(Definition (2))} \\
&= (g \cdot h) \cdot (g^{m-1} \cdot h^{m-1}) && \text{(Induktionsannahme)} \\
&= (h \cdot g) \cdot (g^{m-1} \cdot h^{m-1}) && (g \cdot h = h \cdot g) \\
&= (h \cdot (g \cdot g^{m-1})) \cdot h^{m-1} && \text{(Assoziativgesetz)} \\
&= (h \cdot g^m) \cdot h^{m-1} && \text{(Definition (2))} \\
&= (g^m \cdot h) \cdot h^{m-1} && (g^m \cdot h = h \cdot g^m) \\
&= g^m \cdot (h \cdot h^{m-1}) && \text{(Assoziativgesetz)} \\
&= g^m \cdot h^m && \text{(Definition (2)).}
\end{aligned}$$

Die in der sechsten Gleichung verwendete Identität $g^m \cdot h = h \cdot g^m$ für alle $m \in \mathbb{N}$ folgt durch eine sehr einfache vollständige Induktion (Übungsaufgabe) aus der Voraussetzung $g \cdot h = h \cdot g$.

Zu Punkt 2: Man führt eine vollständige Induktion nach $p := mn$ durch.

Induktionsanfang ($p = 1$): In diesem Fall ist $m = n = 1$ und daher gilt $(h^1)^1 = h^1$ nach Definition.

Induktionsschritt: Es sei $p > 1$ und $p = mn$, $m, n \in \mathbb{N}$. Dann ist ohne Einschränkung der Allgemeinheit $m > 1$ und daher $m - 1 \in \mathbb{N}$. Nach Induktionsannahme gilt

$$(h^{m-1})^n = h^{(m-1)n}$$

und daher

$$(h^m)^n = (h \cdot h^{m-1})^n = h^n \cdot h^{(m-1)n} = h^{n+(m-1)n} = h^{mn},$$

wobei man für die erste Gleichung die Definition (2), für die zweite Gleichung den bereits bewiesenen Punkt 3 und für die dritte Gleichung den bereits bewiesenen Punkt 1 benutzt. □

Wir wollen nun die Rechenregeln für Potenzen auch auf negative Exponenten ausweiten, wo immer das möglich ist. Hierzu sei zunächst in Erinnerung gerufen, dass in Analogie zum Fall von Zahlen das (eindeutige) Inverse eines invertierbaren Elements $h \in H$ mit h^{-1} bezeichnet wird. Wir benötigen weiter das folgende auch für sich genommen nützliche Resultat:

FESTSTELLUNG 17: *Es seien $h_1, \ldots, h_r$ invertierbare Elemente des Monoids $(H, \cdot)$. Dann ist auch das Produkt $h_1 \cdot \ldots \cdot h_r$ invertierbar und es gilt die Formel*

$$(h_1 \cdot \ldots \cdot h_r)^{-1} = h_r^{-1} \cdot \ldots \cdot h_1^{-1}.$$

BEWEIS: Die Behauptung wird durch vollständige Induktion nach r bewiesen.

Induktionsanfang ($r = 2$): Es gilt

$$(h_1 \cdot h_2) \cdot (h_2^{-1} \cdot h_1^{-1}) = h_1 \cdot (h_2 \cdot h_2^{-1}) \cdot h_1^{-1} = h_1 \cdot 1 \cdot h_1^{-1} = h_1 \cdot h_1^{-1} = 1$$

und analog bei Vertauschung der beiden Faktoren.

Induktionsschritt: Für $r > 2$ gilt

$$\begin{aligned} h_r^{-1} \cdot \ldots \cdot h_1^{-1} &= (h_r^{-1} \cdot \ldots \cdot h_2^{-1}) \cdot h_1^{-1} \\ &= (h_2 \cdot \ldots \cdot h_r)^{-1} \cdot h_1^{-1} \\ &= (h_1 \cdot h_2 \ldots \cdot h_r)^{-1}, \end{aligned}$$

wobei man die Induktionsannahme zweimal einsetzt, nämlich für $r - 1$ und für 2 Faktoren. □

Als Folge von Feststellung 17 ergibt sich die Invertierbarkeit jeder Potenz h^n, $n \in \mathbb{N}$, falls h invertierbar ist. Damit ist die folgende Definition in jedem Monoid $(H, \cdot)$ sinnvoll:

$$\forall h \in H \quad h^0 := 1. \tag{3}$$

Ist schließlich h in $(H, \cdot)$ invertierbar, so definiert man

$$\forall h \in H^\times, n \in \mathbb{N} \quad h^{-n} := (h^n)^{-1}. \tag{4}$$

Satz 18: *In einem Monoid $(H, \cdot)$ gelten die Rechenregeln aus Satz 16 für alle Exponenten aus der Menge $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.*

Für die invertierbaren Elemente von $(H, \cdot)$ gelten diese Rechenregeln sogar für alle Exponenten aus der Menge $\mathbb{Z}$.

Beweis: Die Behauptung zur Exponentenmenge $\mathbb{N}_0$ ist klar.

Es sei nun $h \in H$ ein invertierbares Element. Um in diesem Fall den Punkt 1 auch für negative Exponenten zu beweisen, betrachtet man zunächst den Fall $m \geq 0$ und $n < 0$. Ist $m + n \geq 0$, so gilt nach Punkt 1

$$h^{-n} \cdot h^{m+n} = h^m.$$

Nach Definition (4) ist $(h^{-n})^{-1} = h^n$, womit sich aus der vorletzten Gleichung durch Linksmultiplikation mit $(h^{-n})^{-1}$ die Gleichung

$$h^{m+n} = h^m \cdot h^n$$

ergibt. Ist $m + n < 0$, so betrachtet man $-(m + n) = (-m) + (-n) > 0$, wobei $-m \leq 0$ und $-n > 0$ gilt. Nach dem eben Bewiesenen gilt dann

$$h^{(-n)+(-m)} = h^{-n} \cdot h^{-m}.$$

Nach Definition (4) gilt $(h^{(-n)+(-m)})^{-1} = h^{n+m}$ sowie $(h^{-n})^{-1} = h^n$ und $h^{-m} = (h^m)^{-1}$. Durch Linksmultiplikation mit $(h^{(-n)+(-m)})^{-1}$ gefolgt von einer Rechtmultiplikation mit h^m gefolgt von einer weiteren Rechtsmultiplikation mit h^n ergibt sich:

$$h^m \cdot h^n = h^{n+m}.$$

Der Fall $m < 0$ und $n \geq 0$ wird analog behandelt.

Es bleibt die Behauptung für den Fall $m < 0$ und $n < 0$ zu zeigen. In diesem Fall gilt nach Punkt 1:

$$h^{(-m)+(-n)} = h^{-m} \cdot h^{-n}.$$

Eine Anwendung der Definition (4) liefert $(h^{(-m)+(-n)})^{-1} = h^{m+n}$ sowie $(h^{-n})^{-1} = h^n$ und $(h^{-m})^{-1} = h^m$. Die Behauptung folgt nun wie oben. □

Schlüsseltausch in der Kryptographie: Die Operation des Potenzierens in einer Gruppe wird in der Kryptographie zur Lösung des so genannten »Schlüsseltauschproblems« genutzt: Zwei Personen, etwa Alice und Bob, möchten die eMails, die sie sich gegenseitig schicken, verschlüsseln, weil sie

befürchten, dass eine dritte Partei – Mallory – die Komunikation zwischen ihnen abhört. Zur Verschlüsselung können sie zum Beispiel das sogenannte »Advanced Encryption Standard«-Verfahren verwenden. Dabei handelt es sich um einen Algorithmus, der auf zwei Arten verwendet werden kann:

- Zur Verschlüsselung eines Texts T wird ein Schlüssel K festgelegt und zusammen mit dem Text als Input für das AES-Verfahren verwendet. Das Verfahren liefert den verschlüsselten Text C als Output. In welcher Weise T verschlüsselt wird, hängt von dem Schlüssel K ab. Dieser Schlüssel ist in der Regel eine (lange) Kombination von Zahlen und Buchstaben, die den AES-Algorithmus in einer bestimmten Weise steuern.

- Zur Entschlüsselung eines verschlüsselten Texts C muss der zur Verschlüsselung benutzte Schlüssel K bekannt sein. Gibt man C und K in das AES-Verfahren ein, so liefert dieses den entschlüsselten Text T.

Um mit Hilfe des AES-Verfahrens verschlüsselte eMails auszutauschen, müssen sich Alice und Bob also auf einen Schlüssel K einigen, den sie beide benutzen. Das kann schwierig sein, wenn Alice und Bob in unterschiedlichen Teilen der Welt leben, denn sie sollten zur Übermittlung von K keine abhörbaren Informationskanäle nutzen, da Mallory sonst den Schlüssel in die Hände bekommen kann.

Nach einer Idee der Mathematiker Whitfield Diffie ($*$ 1944) und Martin Hellman ($*$ 1945) kann dieses Schlüsseltauschproblem wie folgt gelöst werden: Man wählt eine endliche Gruppe $(G, \cdot)$, in der es sehr schwierig ist Gleichungen der Form

$$g^x = h$$

bei bekanntem $g, h \in G$ zu lösen. Solche endlichen Gruppen sind notwendigerweise sehr groß; aktuell haben die von offiziellen Institutionen empfohlenen Gruppen eine Größe von mehr als 10^{57} Elementen. Zur Festlegung eines Schlüssels K legen Alice und Bob eine Gruppe G und ein Element $g \in G$ fest; das können sie offen tun, das heißt diese Information muss nicht geheim gehalten werden. In der Praxis sieht das so aus, dass Alice und Bob eine gemeinsame Verschlüsselungssoftware mit bestimmten Einstellungen nutzen. Danach legen Alice und Bob jeweils für sich natürliche Zahlen a und b fest; diese halten sie geheim. Alice berechnet aus ihrer Zahl das Gruppenelement g^a und schickt es per (unverschlüsselter) eMail an Bob. Bob berechnet g^b

und schickt dieses Element an Alice. Nun kann Alice das Element $(g^b)^a = g^{ab}$ berechnen, denn sie kennt a und hat g^b von Bob erhalten. Bob dagegen kann $(g^a)^b = g^{ab}$ berechnen, denn er kennt b und hat g^a erhalten. Obwohl keiner der beiden die Geheimzahl des anderen kennt, kennen sie beide das Element $K := g^{ab}$, das nun als Schlüssel verwendet werden kann. Mallory kann zwar durch Abhören der eMails die Elemente g^a und g^b in die Hände bekommen, kann daraus aber nach Wahl der Gruppe G die Geheimzahlen a und b nur mit sehr hohem Aufwand, das heißt langer Rechenzeit, ermitteln. Damit kann er auch den Schlüssel K nur mit hohem Aufwand ermitteln.

Welche Gruppen für dieses Verfahren gut geeignet sind, wird in der Kryptographie mit Methoden der Algebra und der Informatik studiert.

Die Bedeutung des Rechnens mit Potenzen mit negativem Exponenten wird klar, wenn man sich das formale Lösen von Gleichungen in Monoiden ansieht:

Lösen von Gleichungen in Monoiden: In einem Monoid $(H, \cdot)$ kann man versuchen Gleichungen der Form

$$g \cdot x = h \text{ oder } x \cdot g = h \tag{5}$$

zu lösen, wobei $g, h \in H$ gegebene Elemente sind. Ist $g \in H^\times$, so erhält man aus der ersten Gleichung

$$x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot h,$$

das heißt es gibt höchstens eine Lösung. Durch Einsetzen verifiziert man, dass $g^{-1} \cdot h$ tatsächlich eine Lösung ist.

Analog ergibt sich im zweiten Fall die Lösung $x = h \cdot g^{-1}$. Man beachte, dass in H das Kommutativgesetz nicht zu gelten braucht.

Ist g nicht invertierbar, so können Gleichungen der Form (5) keine, eine oder mehrere Lösungen besitzen. Man kann dieses Verhalten am Beispiel des Monoids $(\mathbb{R}^{2\times 2}, \cdot)$ gut nachvollziehen: Man betrachte eine Matrixgleichung der Form

$$g \cdot x = \begin{pmatrix} g_{11} & g_{12} \\ 0 & g_{22} \end{pmatrix} \cdot \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} = h.$$

Die Matrix g ist genau dann invertierbar, wenn $g_{11}g_{22} \neq 0$ gilt; in diesem Fall

ist die einzige Lösung dieser Gleichung

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} \\ 0 & g_{22} \end{pmatrix}^{-1} \cdot \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} = \begin{pmatrix} g_{11}^{-1} & -g_{12}g_{11}^{-1}g_{22}^{-1} \\ 0 & g_{22}^{-1} \end{pmatrix} \cdot \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix}.$$

Ist $g_{22} = 0$ und $h_{21} \neq 0$ oder $h_{22} \neq 0$, so besitzt die Gleichung keine Lösung.

Ist $h = 0$ die Nullmatrix und $g_{12} = g_{22} = 0$, so besitzt die Gleichung die unendlich vielen Lösungen

$$\begin{pmatrix} 0 & 0 \\ x_{21} & x_{22} \end{pmatrix}, \quad x_{21}, x_{22} \in \mathbb{R}.$$

Auf der Grundlage dieser allgemeinen Überlegungen kann man in Monoiden auch komplexere Gleichungen zum Beispiel in mehreren Variablen lösen. Das Gleichungssystem

$$g_1 \cdot x_1 \cdot x_2 \cdot g_2 = h_1, \quad x_2 \cdot g_3 = h_2$$

in den Variablen x_1, x_2 beispielsweise besitzt eine eindeutige Lösung sofern die Elemente g_1, g_2, g_3, h_2 alle invertierbar sind: Aus der zweiten Gleichung erhält man dann zunächst $x_2 = h_2 \cdot g_3^{-1}$. Einsetzen in die erste Gleichung liefert

$$g_1 \cdot x_1 \cdot h_2 \cdot g_3^{-1} \cdot g_2 = h_1,$$

aus der sich durch Auflösen nach x_1 die Gleichung

$$x_1 = g_1^{-1} \cdot h_1 \cdot g_2^{-1} \cdot g_3 \cdot h_2^{-1}$$

ergibt. ◇

Zusammenfassend halten wir fest:

FESTSTELLUNG 19: *In einem Monoid $(H, \cdot)$ besitzen Gleichungen der Form*

$$g \cdot x = h, \quad x \cdot g = h, \quad g \cdot x \cdot g' = h$$

stets genau eine Lösung, falls $g, g' \in H^\times$ gilt. Ohne diese Voraussetzung können solche Gleichungen keine oder mehrere Lösungen besitzen.

VERKNÜPFUNGSTAFELN: Neben weit verbreiteten Eigenschaften innerer Verknüpfungen wie dem Assoziativgesetz oder den Regeln des Potenzrechnens, gibt es auch speziellere Eigenschaften, die nur in bestimmten Monoiden gelten. Es stellt sich die Frage, in welcher Weise man solche speziellen Eigenschaften in ein Computeralgebrasystem implementiert, um damit rechnen zu können. Für kleine Halbgruppen, Monoide oder Gruppen ist das Anlegen einer Verknüpfungstafel die einfachste Option. Dabei handelt es sich um eine Tabelle, in deren k-ter Zeile die Elemente $h_k \cdot h_1, \ldots, h_k \cdot h_n$ in der Reihenfolge einer beliebig wählbaren Nummerierung $h_1, \ldots, h_n$ der Elemente von H aufgeführt sind. Entsprechend stehen in der k-ten Spalte der Tabelle die Elemente $h_1 \cdot h_k, \ldots, h_n \cdot h_k$.

Als Beispiel betrachte man das Monoid $(\mathrm{Abb}\,(\{1,2\}), \circ)$. Die identische Abbildung in diesem Monoid wird wie üblich mit id bezeichnet. Weiter seien 1 und 2 diejenigen Abbildungen $\{1,2\} \to \{1,2\}$, die alle Elemente auf die Zahl 1 beziehungsweise die Zahl 2 abbilden. Schließlich sei τ die durch $\tau(1) = 2$ und $\tau(2) = 1$ definierte Abildung. Dann gilt $\mathrm{Abb}\,(\{1,2\}) = \{\mathrm{id}\,, 1, 2, \tau\}$ und man erhält die folgende Verknüpfungstafel:

$\circ$	id	1	2	τ
id	id	1	2	τ
1	1	1	1	1
2	2	2	2	2
τ	τ	2	1	id

Im diesem Beispiel gilt $\mathrm{Abb}\,(\{1,2\})^\times = \{\mathrm{id}\,, \tau\}$, wie man leicht aus der Verknüpfungstafel abliest.

Die Tatsache, dass Gleichungen der Form $g \cdot x = h$ und $x \cdot g = h$ in einer Gruppe $(H, \cdot)$ stets genau eine Lösung besitzen, schlägt sich auch in der Verknüpfungstafel nieder: In der k-ten Zeile stehen nach Definition nämlich gerade die Lösungen der Gleichungen $g_k \cdot x = h$, wobei g_k das in der gewählten Nummerierung k-te Gruppenelement ist, und h alle Gruppenelement durchläuft. Die Lösungen $g_k^{-1} \cdot h$ dieser Gleichungen sind verschieden, denn aus $g_k^{-1} \cdot h = g_k^{-1} \cdot h'$ folgt durch Multiplikation mit g_k von links die Identität $h = h'$. Es folgt: *In jeder Zeile der Verknüpfungstafel kommt jedes Gruppenelement genau einmal vor.* Dieselbe Argumentation mit den Gleichungen $x \cdot g = h$ und den Spalten der Verknüpfungstafel zeigt: *In jeder Spalte der Verknüpfungstafel kommt jedes Gruppenelement genau einmal vor.* Die Verknüpfungstafel einer endlichen Gruppe besitzt also die Eigenschaft eines *Sudokus*.

Zur Illustration dieses Sachverhalts betrachte man zum Beispiel die Menge $\mu_4 := \{1, -1, i, -i\} \subset \mathbb{C}$. Diese Zahlen sind genau die Nullstellen des Polynoms $X^4 - 1$; sie werden deshalb als 4-te Einheitswurzeln bezeichnet. Multipliziert man zwei dieser Zahlen, so erhält man wiederum eine solche. Die Verknüpfungstafel der Multiplikation sieht so aus:

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

Man liest leicht ab, dass es sich bei μ_4 um eine (abelsche) Gruppe handelt.

Neben Verknüpfungstafeln kann man zur IMplementierung von Eigenschaften innerer Verknüpfungen auch charakteristische Gleichungen verwenden. Wir werden auf dieses Vorgehen im Abschnitt über Gruppen zu sprechen kommen.