1 Algebraische Strukturen

1.1 Innere Verknüpfungen

1.1.1 Grundbegriffe und Beispiele

In der Analysis wie auch in der linearen Algebra kommen verschiedene Arten von »Rechenoperationen« vor, bei denen man jeweils (zwei) mathematische Objekte der gleichen Art miteinander »verknüpft« und wieder ein Objekt dieser Art als Ergebnis geliefert bekommt. Die folgende Liste enthält einige Beispiele:

1. Die Addition $m + n$ zweier natürlicher Zahlen $m, n \in \mathbb{N}$.
2. Die Vereinigung $M \cup N$ zweier Mengen M und N.
3. Die Addition $x + y$ zweier Vektoren $x, y \in \mathbb{R}^n$ des n-dimensionalen reellen Raums.
4. Die Multiplikation $A \cdot B$ zweier reeller Matrizen $A, B \in \mathbb{R}^{n \times n}$ mit $n \in \mathbb{N}$ Zeilen und Spalten.
5. Das Vekorprodukt $x \times y = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)$ zweier Vektoren $x = (x_1, x_2, x_3), y = (y_1, y_2, y_3) \in \mathbb{R}^3$ des 3-dimensionalen reellen Raums.

Diese Rechenoperationen oder Verknüpfungen besitzen Gemeinsamkeiten, unterscheiden sich aber auch in einigen Eigenschaften auch erheblich: Für die Addition natürlicher Zahlen gilt die als Assoziativgesetz bekannte Regel

$$(l + m) + n = l + (m + n).$$

Auch die Vereinigung von Mengen gehorcht diesem Gesetz: $(K \cup M) \cup N = K \cup (M \cup N)$. Da die Addition von Vektoren komponentenweise definiert ist, und die Addition reeller Zahlen dem Assoziativgesetz gehorcht, gilt dasselbe auch für die Vektoraddition. Die Matrixmultiplikation ist ebenfalls assoziativ; der Nachweis kann mit einer einfachen aber etwas länglichen Rechnung geführt werden. Das Vektorprodukt dagegen ist *nicht* assoziativ: Nach Definition steht $x \times y$ stets senkrecht auf x und y. Weiter gilt $x \times y = 0$ genau dann, wenn x und y linear abhängig sind. Sind nun x und y linear unabhängige Vektoren, so folgt daher $x \times (x \times y) \neq 0$. Andererseits ist $(x \times x) \times y = 0 \times y = 0$.

Bezeichnet man mit $\emptyset$ die leere Menge, so gilt $M \cup \emptyset = \emptyset \cup M = M$ für eine beliebige Menge M, das heißt die Verknüpfung mit der leeren Menge bewirkt nichts. Analog verhält sich der Nullvektor $0 \in \mathbb{R}^n$ in bezug auf die Vektoraddition, $x + 0 = 0 + x = x$ für einen beliebigen Vektor x, und die Einheitsmatrix $E \in \mathbb{R}^{n \times n}$ in bezug auf die Matrixmultiplikation, $A \cdot E = E \cdot A = A$ für alle Matrizen A. Für die Addition natürlicher Zahlen und das Vektorprodukt gibt es jeweils keine Elemente, die sich in dieser Weise »neutral« verhalten.

Auch in Bezug auf das »neutrale Element«, falls es denn vorhanden ist, verhalten sich die Verknüpfungen verschieden: Für die Vektoraddition gilt stets $x + (-x) = 0$. Zu einer nicht leeren Menge M gibt es aber keine Menge N mit der Eigenschaft $M \cup N = \emptyset$. Im Fall der Matrizen gibt es zu $A \in \mathbb{R}^{n \times n}$ nur manchmal eine Matrix B mit der Eigenschaft $A \cdot B = E$.

Zum Schluss dieser Diskussion sei schließlich festgehalten, dass das Ergebnis einer Verknüpfung in den Beispielen 1 bis 3 nicht von der Reihenfolge, in der man verknüpft, abhängt. Bei den Beispielen 4 und 5 ist das dagegen der Fall. Im Fall des Vektorprodukts gilt dabei stets $x \times y = -(y \times x)$.

Durch *Abstraktion*, also das Wegnehmen aller speziellen Eigenschaften von den obigen Beispielen und das Herausarbeiten der wesentlichen gemeinsamen Eigenschaften, gelangt man zu der folgenden

Definition 1: *Eine innere Verknüpfung einer Menge M ist eine Abbildung*

$$v : M \times M \to M;$$

die Bilder $v(m_1, m_2)$ werden in der Regel als $m_1 \cdot m_2$ geschrieben, um auszudrücken, dass die beiden Elemente $m_1, m_2 \in M$ miteinander verknüpft werden.

Man nennt die innere Verknüpfung v assoziativ, falls das Assoziativgesetz

$$\forall m_1, m_2, m_3 \in M \quad (m_1 \cdot m_2) \cdot m_3 = m_1 \cdot (m_2 \cdot m_3)$$

gilt.

Man nennt v kommutativ, falls das Kommutativgesetz

$$\forall m_1, m_2 \in M \quad m_1 \cdot m_2 = m_2 \cdot m_1$$

gilt.

Ein Element $e \in M$ heißt neutrales Element von v, falls es die Eigenschaft

$$\forall m \in M \quad m \cdot e = e \cdot m = m$$

besitzt.

Besitzt die innere Verknüpfung v ein neutrales Element $e \in M$, so nennt man ein Element $m' \in M$ Inverses zu $m \in M$, falls es die Eigenschaft

$$m \cdot m' = m' \cdot m = e$$

besitzt.

Die Verwendung des Symbols $\cdot$ für eine allgemeine innere Verknüpfung ist zwar willkürlich, hat sich aber in der mathematischen Literatur durchgesetzt, obwohl eine Verwechslungsgefahr mit dem Symbol für die Multiplikation von Zahlen besteht. Wie die oben diskutierten Beispiele zeigen, verwendet man im Fall konkreter Verknüpfungen durchaus auch andere Symbole wie etwa $+$ oder $\cup$.

Die Definition 1 wirft einige Fragen auf:

- Sind für eine assoziative Verknüpfung auch Ausdrücke wie zum Beispiel $(m_1 \cdot m_2) \cdot (m_3 \cdot m_4)$ und $m_1 \cdot ((m_2 \cdot m_3) \cdot m_4)$ gleich?

  Allgemeiner: Darf man in einem Ausdruck, in dem mehrerer Elemente verknüpft werden, die Klammern beliebig setzen, solange die Klammerung ein zulässiger Ausdruck ist?

  Man beachte hierbei, dass die Klammern stets so gesetzt werden müssen, dass die Vorschrift zur Berechnung des Ausdrucks eindeutig erkennbar ist. Die Ausdrücke $m_1 \cdot m_2 \cdot m_3$ und $m_1 \cdot (m_2 \cdot m_3) \cdot m_4$ sind zum Beispiel nicht zulässig, da sie mehrdeutig sind.

- Kann eine innere Verknüpfung mehrere neutrale Elemente besitzen?

- Das Inverse eines Elements hängt vom neutralen Element ab. Kann es bei festem neutralem Element mehrere Inverse zu einem Element geben?

Diese Fragen sollen nun der Reihe nach beantwortet werden.

FESTSTELLUNG 2: *Es seien $v : M \times M \to M$ eine innere Verknüpfung und $m_1, \ldots m_r \in M$.*

Gilt für v das Assoziativgesetz, so liefern für $r \geq 3$ alle zulässig geklammerten Ausdrücke, in denen die m_i in der Reihenfolge ihrer Nummerierung auftreten, dasselbe Ergebnis.

Gilt für v zusätzlich das Kommutativgesetz, so kann man für $r \geq 2$ die m_i in beliebiger Reihenfolge miteinander verknüpfen ohne das Ergebnis zu ändern.

BEWEIS: Beide Behauptungen werden durch vollständige Induktion nach r beweisen. Zunächst zum Assoziativgesetz:

Induktionsanfang ($r = 3$): Dies ist gerade das Assoziativgesetz laut Definition.

Induktionsschritt: Man zeigt, dass das Ergebnis jedes zulässig geklammerten Ausdrucks A aus $r + 1 > 3$ Elementen $m_1, \ldots, m_{r+1} \in M$ gleich dem Ergebnis des Ausdrucks

$$m_1 \cdot (m_2 \cdot (m_3 \cdot (\ldots (m_r \cdot m_{r+1}) \ldots) \tag{1}$$

ist. Am Beispiel $r = 4$ sieht man, wie das gemeint ist: Der Ausdruck $A = (m_1 \cdot m_2) \cdot (m_3 \cdot m_4)$ ist zulässig geklammert. Er ist gleich dem Ausdruck $m_1 \cdot (m_2 \cdot (m_3 \cdot m_4))$, weil man $m_3 \cdot m_4$ als ein Element von $m \in M$ betrachten und das Assoziativgesetz anwenden kann:

$$(m_1 \cdot m_2) \cdot (m_3 \cdot m_4) = (m_1 \cdot m_2) \cdot m = m_1 \cdot (m_2 \cdot m) = m_1 \cdot (m_2 \cdot (m_3 \cdot m_4)).$$

Im allgemeinen Fall argumentiert man so: Da A zulässig geklammert ist, besitzt er die Form $A = A_1 \cdot A_2$ mit zulässig geklammerten Ausdrücken A_1 und A_2. Ist $A_1 = m_1$, so gilt nach Induktionsannahme

$$A_2 = m_2 \cdot (m_3 \cdot (m_4 \cdot (\ldots (m_r \cdot m_{r+1}) \ldots),$$

woraus die Behauptung direkt folgt. Andernfalls gilt für ein $s \in \{2, \ldots, r\}$ nach Induktionsannahme

$$A_1 = m_1 \cdot (m_2 \cdot (m_3 \cdot (\ldots (m_{s-1} \cdot m_s) \ldots),$$

und folglich

$$\begin{aligned} A_1 \cdot A_2 &= (m_1 \cdot (m_2 \cdot (m_3 \cdot (\ldots (m_{s-1} \cdot m_s) \ldots)) \cdot A_2 \\ &= m_1 \cdot ((m_2 \cdot (m_3 \cdot (\ldots (m_{s-1} \cdot m_s) \ldots) \cdot A_2), \end{aligned}$$

wobei man das Assoziativgesetz benutzt. Nach Induktionsannahme gilt

$$(m_2 \cdot (m_3 \cdot (\ldots (m_{s-1} \cdot m_s) \ldots) \cdot A_2 = m_2 \cdot (m_3 \cdot (m_4 \cdot (\ldots (m_r \cdot m_{r+1}) \ldots),$$

woraus wiederum die Behauptung folgt.

Nun zum Kommutativgesetz.

Induktionsanfang ($r = 2$): Dies ist gerade das Kommutativgesetz laut Definition.

Induktionsschritt: Man betrachtet eine Umordnung $k_1, \ldots, k_{r+1}$ der natürlichen Zahlen $1, \ldots, r+1$, $r+1 > 2$. Im Fall $k_1 = 1$ gilt nach Induktionsannahme

$$m_{k_2} \cdot \ldots \cdot m_{k_{r+1}} = m_2 \cdot \ldots \cdot m_{r+1},$$

also wie behauptet

$$m_{k_1} \cdot m_{k_2} \cdot \ldots \cdot m_{k_{r+1}} = m_1 \cdot m_2 \cdot \ldots \cdot m_{r+1}.$$

Andernfalls gilt nach Induktionsannahme zunächst

$$m_{k_2} \cdot \ldots \cdot m_{k_{r+1}} = m_1 \cdot \ldots \cdot m_{r+1},$$

und daher

$$\begin{aligned} m_{k_1} \cdot m_{k_2} \cdot \ldots \cdot m_{k_{r+1}} &= m_{k_1} \cdot m_1 \cdot \ldots \cdot m_{r+1} \\ &= m_1 \cdot m_{k_1} \cdot \ldots \cdot m_{r+1} \\ &= \ldots \\ &= m_1 \cdot m_2 \cdot \ldots \cdot m_{r+1}, \end{aligned}$$

wobei man m_{k_1} solange mit dem jeweils rechts stehenden Faktor tauscht, bis es an der seinem Index k_1 entsprechenden Position im Produkt steht. Hierbei wird das Kommutativgesetz verwendet.

Man beachte, dass wegen der Gültigkeit des Assoziativgesetzes in den oben aufgeführten Produkten keine Klammern gesetzt werden müssen. □

FESTSTELLUNG 3: *Eine innere Verknüpfung besitzt höchstens ein neutrales Element.*

BEWEIS: Es seien e_1 und e_2 zwei neutrale Elemente der inneren Verknüpfung $\cdot$. Dann gilt $e_1 = e_1 \cdot e_2 = e_2$, wobei man für das erste Gleichheitszeichen die Neutralität von e_2 benutzt und für das zweite die Neutralität von e_1. □

Die Feststellung 3 besitzt trotz ihres einfachen Beweises wegen ihrer Allgemeinheit etwas Überraschendes.

Der Begriff des Inversen wird durch die Eindeutigkeit des neutralen Elements selbst wesentlich klarer. Das folgende Ergebnis geht diesbezüglich noch einen Schritt weiter:

FESTSTELLUNG 4: *Besitzt eine innere Verknüpfung ein neutrales Element und gilt das Assoziativgesetz, so besitzt jedes Element höchstens ein Inverses.*

BEWEIS: Es sei $\cdot$ eine assoziative innere Verknüpfung der Menge M mit neutralem Element $e \in M$. Es seien m' und m'' zwei Inverse zu $m \in M$. Dann gilt

$$m' = m' \cdot e = m' \cdot (m \cdot m'') = (m' \cdot m) \cdot m'' = e \cdot m'' = m''.$$

□

Man passt nun auch die mathematische Notation den Ergebnissen an: Ist $\cdot$ eine innere Verknüpfung der Menge M, so bezeichnet man *das* neutrale Element, falls es existiert, nicht mehr mit einem willkürlich gewählten Buchstaben, sondern mit dem Symbol 1, in Übereinstimmung mit dem Multiplikationssymbol für die Verknüpfung.

Besitzt $\cdot$ ein neutrales Element und ist assoziativ, so bezeichnet man entsprechend *das* Inverse eines Elements $m \in M$ mit dem Symbol m^{-1}.

Diese Konventionen gelten für die Untersuchung allgemeiner Verknüpfungen. In speziellen Fällen wird durchaus davon abgewichen.

Entsprechend ihrer Bedeutung zeichnet man assoziative innere Verknüpfungen (mit neutralem Element) besonders aus:

DEFINITION 5: *Eine Halbgruppe ist ein Paar $(H, \cdot)$ bestehend aus einer nicht leeren Menge H und einer assoziativen inneren Verknüpfung $\cdot$ von H. Ein Monoid ist eine Halbgruppe $(H, \cdot)$ für die $\cdot$ ein neutrales Element besitzt. Eine Gruppe ist ein Monoid $(H, \cdot)$, in dem jedes Element ein Inverses besitzt.*

Man nennt eine Halbgruppe, ein Monoid oder eine Gruppe $(H, \cdot)$ *endlich* oder *unendlich*, wenn die Menge H endlich oder unendlich ist. Ist H endlich, so steht das Symbol $|H|$ für die Anzahl der Elemente von H. Diese wird (etwas missverständlich) auch als *Ordnung von H* bezeichnet.

Man nennt eine Halbgruppe oder ein Monoid $(H, \cdot)$ *kommutativ*, wenn das Kommutativgesetz gilt. Eine Gruppe $(H, \cdot)$, in der das Kommutativgesetz gilt, nennt man *abelsch*, zu Ehren des norwegischen Mathematikers Niels Henrik Abel ($*$ 1802, † 1829). Abel zeigte mit Hilfe der Theorie endlicher Gruppen, dass es für die Gleichung fünften Grades

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

mit reellen Koeffizienten *keine* allgemeine Lösungsformel gibt, anders als für die entsprechenden Gleichungen niedrigeren Grades. Man hatte vorher über mehrere Jahrhunderte hinweg versucht eine solche Formel zu finden.

Die folgenden Beispiele von Halbgruppen, Monoiden und Gruppen spielen in der Mathematik wegen ihres häufigen Auftretens eine wichtige Rolle.

Beispiel 6 (Zahlbereiche): In der Schule und zu anfang des Studiums lernt man die folgenden Zahlbereiche kennen. Ihre Struktur ist jeweils angegeben, wobei das Verknüpfungssymbol + für die Addition und das Verknüpfungssymbol $\cdot$ für die Multiplikation im jeweiligen Zahlbereich steht.

- Natürliche Zahlen $(\mathbb{N}, +)$: kommutative Halbgruppe.
- Natürliche Zahlen $(\mathbb{N}, \cdot)$: kommutatives Monoid.
- Ganze Zahlen $(\mathbb{Z}, +)$: abelsche Gruppe.
- Ganze Zahlen $(\mathbb{Z}, \cdot)$: kommutatives Monoid.
- Rationale Zahlen $(\mathbb{Q}, +)$: abelsche Gruppe.
- Rationale Zahlen $(\mathbb{Q} \setminus \{0\}, \cdot)$: abelsche Gruppe.
- Positive rationale Zahlen $(\mathbb{Q}^{>0}, \cdot)$: abelsche Gruppe.
- Reelle Zahlen $(\mathbb{R}, +)$: abelsche Gruppe.
- Reelle Zahlen $(\mathbb{R} \setminus \{0\}, \cdot)$: abelsche Gruppe.
- Positive reelle Zahlen $(\mathbb{R}^{>0}, \cdot)$: abelsche Gruppe.
- Komplexe Zahlen $(\mathbb{C}, +)$: abelsche Gruppe.
- Komplexe Zahlen $(\mathbb{C} \setminus \{0\}, \cdot)$: abelsche Gruppe.

Konvention: In diesem Skript wird das Symbol $\mathbb{K}$ verwendet, wenn *wahlweise* eine der Mengen $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$ gemeint ist.

Beispiel 7 (Vektoraddition): Die Menge $\mathbb{K}^n$ von Vektoren mit Komponenten im Zahlbereich $\mathbb{K}$ bilden zusammen mit der komponentenweisen Addition

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n)$$

eine abelsche Gruppe. Das neutrale Element ist der Nullvektor

$$0 := (0, \ldots, 0),$$

das Inverse eines Vektor $(a_1, \ldots, a_n)$ ist der Vektor

$$-(a_1, \ldots, a_n) := (-a_1, \ldots, -a_n).$$

Beispiel 8 (Matrixoperationen): Die Menge $\mathbb{K}^{m\times n}$ der Matrizen

$$(a_{ik}) := \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

mit m Zeilen und n Spalten sowie Koeffizienten a_{ij} im Zahlbereich $\mathbb{K}$ bilden zusammen mit der koeffizientenweisen Addition

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$$

eine abelsche Gruppe. Das neutrale Element ist die Nullmatrix

$$0 := (a_{ij}), \quad a_{ij} = 0 \text{ für alle } i \text{ und } j.$$

Das Inverse der Matrix (a_{ij}) ist die Matrix

$$-(a_{ij}) := (-a_{ij}).$$

Die Menge $\mathbb{K}^{n\times n}$ der Matrizen mit n Zeilen und n Spalten sowie Koeffizienten a_{ij} im Zahlbereich $\mathbb{K}$ bilden zusammen mit der Matrixmultiplikation

$$(a_{ij}) \cdot (b_{ij}) := (\sum_{k=1}^{n} a_{ik} b_{kj})$$

ein Monoid. Im Fall $n \geq 2$ ist dieses nicht kommutativ. Das neutrale Element ist die Einheitsmatrix

$$E := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \vdots & & & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Beispiel 9 (Punktweise Operationen mit Funktionen): Es sei M eine nicht leere Menge und $\mathrm{Fun}\,(M, \mathbb{R})$ die Menge aller Abbildungen $f : M \to \mathbb{R}$. Solche Abbildungen nennt man auch *Funktionen auf* M; die Fälle $M = (a, b)$, $M = [a, b]$ und $M = \mathbb{R}$ sind aus der Analysis vertraut.

Zwei Funktionen $f, g \in \mathrm{Fun}\,(M, \mathbb{R})$ kann man punktweise addieren und multiplizieren:

$$f + g : M \to \mathbb{R},\ m \mapsto f(m) + g(m),$$

$$f \cdot g : M \to \mathbb{R},\ m \mapsto f(m)g(m)$$

und erhält als Ergebnis wieder eine Funktion $M \to \mathbb{R}$.

Da für die Addition und die Multiplikation reeller Zahlen das Assoziativgesetz und das Kommutativgesetz gelten, gelten diese Gesetze auch für die punktweise Summe und das punktweise Produkt von Funktionen.

Die Nullfunktion $0 : M \to \mathbb{R}$ ist durch $0(m) := 0$ für alle $m \in M$ definiert. Sie ist das neutrale Element der punktweisen Addition.

Die Einsfunktion $1 : M \to \mathbb{R}$ ist durch $1(m) := 1$ für alle $m \in M$ definiert. Sie ist das neutrale Element der punktweisen Multiplikation.

Zu jeder Funktion $f : M \to \mathbb{R}$ kann man die Funktion $-f : M \to \mathbb{R}$ durch $(-f)(m) := -f(m)$ für alle $m \in M$ definieren. Dann gilt $f + (-f) = 0$, das heißt $-f$ ist das Inverse zu f bezüglich der punktweisen Addition.

Insgesamt hat man jetzt bewiesen: $(\mathrm{Fun}\,(M, \mathbb{R}), +)$ ist eine abelsche Gruppe und $(\mathrm{Fun}\,(M, \mathbb{R}), \cdot)$ ist ein kommutatives Monoid.

Beispiel 10 (Verkettung von Abbildungen): Es sei M eine nicht leere Menge und $\mathrm{Abb}\,(M)$ die Menge aller Abbildungen $f : M \to M$. Führt man eine Abbildung $g \in \mathrm{Abb}\,(M)$ *nach* der Abbildung $f \in \mathrm{Abb}\,(M)$ aus, so erhält man insgesamt eine mit $g \circ f$ bezeichnete Abbildung, die häufig als Verkettung von f mit g bezeichnet wird. Nach Definition gilt

$$\forall m \in M \quad (g \circ f)(m) = g(f(m)),$$

woraus das Assoziativgesetz

$$\forall f, g, h \in \mathrm{Abb}\,(M) \quad (h \circ g) \circ f = h \circ (g \circ f)$$

durch einfaches Nachrechnen folgt.

Die identische Abbildung oder Identität $\mathrm{id} : M \to M,\ m \mapsto m$ ist offensichtlich das neutrale Element der inneren Verknüpfung $\circ$.

Besitzt M mehr als zwei Elemente, so ist $(\mathrm{Abb}\,(M), \circ)$ nicht kommutativ: Sind $a, b, c \in M$ nämlich drei verschiedene Elemente von M, so kann man Abbildungen f und g wie folgt definieren:

$$f(a) := b, \quad f(b) := a, \quad \forall m \in M \setminus \{a, b\}\ f(m) := m,$$

$$g(b) := c, \quad g(c) := b, \quad \forall m \in M \setminus \{b, c\}\ g(m) := m.$$

Für diese Abbildungen gilt $(f \circ g)(a) = f(g(a)) = f(a) = b$ und $(g \circ f)(a) = g(f(a)) = g(b) = c$. Es folgt $f \circ g \neq g \circ f$.

Diejenigen Elemente eines Monoids die ein Inverses besitzen, spielen überall in der Mathematik eine besondere Rolle.

Definition 11: *Die Elemente eines Monoids $(H, \cdot)$, die ein Inverses besitzen, nennt man auch invertierbare Elemente von H. Die Menge aller invertierbaren Elemente von $(H, \cdot)$ wird mit $H^\times$ bezeichnet.*

Bei der Bezeichnungsweise $H^\times$ unterdrückt man die eigentlich notwendige Angabe der Verknüpfung $\cdot$, ein übliches Vorgehen um zu komplexe Bezeichnungen zu vermeiden.

Nach Definition sind Gruppen gerade die Monoide $(H, \cdot)$ für die $H = H^\times$ gilt.

Beispiel 12 (Zahlbereiche (Forts.)):

- $(\mathbb{N}, \cdot)^\times = \{1\}$.
- $(\mathbb{Z}, \cdot)^\times = \{-1, 1\}$.

Beispiel 13 (Matrixoperationen (Forts.)): Zu einer Matrix $A \in (\mathbb{K}^{n\times n}, \cdot)^\times$ muss eine Matrix $B \in \mathbb{K}^{n\times n}$ existieren, für die $A \cdot B = B \cdot A = E$ gilt. In der linearen Algebra nennt man Matrizen, die diese Bedingung erfüllen invertierbar, konsistent mit der hier allgemein für Monoide eingeführten Bezeichnung.

Nach dem Determinantenproduktsatz der linearen Algebra gilt

$$\det(A \cdot B) = \det(A)\det(B) = \det(E) = 1$$

und damit $\det(A) \in \mathbb{K} \setminus \{0\}$.

In der linearen Algebra wird bewiesen, dass die Bedingung $\det(A) \neq 0$ auch hinreichend für die Invertierbarkeit von A ist.

Beispiel 14 (Punktweise Operationen mit Funktionen (Forts.)): Die in dem Monoid $(\mathrm{Fun}\,(M,\mathbb{R}),\cdot)$ invertierbaren Elemente sind genau diejenigen Funktionen $f : M \to \mathbb{R}$, die keine Nullstellen besitzen. Besitzt nämlich f keine Nullstelle, so kann man die Funktion $f^{-1} : M \to \mathbb{R}$ durch $f^{-1}(m) := f(m)^{-1}$ definieren und es gilt $f \cdot f^{-1} = 1$. (Vorsicht: f^{-1} ist natürlich(!) nicht die Umkehrfunktion von f.) Ist andererseits f ein invertierbares Element von $(\mathrm{Fun}\,(M,\mathbb{R}),\cdot)$, so gibt es eine Funktion g mit $f \cdot g = 1$. Nach Definition bedeutet das $f(m)g(m) = 1$ für alle $m \in M$, also insbesondere $f(m) \neq 0$ für alle $m \in M$.

Beispiel 15 (Verkettung von Abbildungen (Forts.)): Besitzt $f \in \mathrm{Abb}\,(M)$ ein inverses Element g, so gilt

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

Die Gleichung $g \circ f = \mathrm{id}$ zeigt, dass f injektiv sein muss: Sind nämlich $m, m' \in M$ mit $f(m) = f(m')$, so ergibt sich durch verknüpfen mit g von links die Gleichung $m = m'$.

Die Gleichung $f \circ g = \mathrm{id}$ dagegen liefert die Surjektivität von f: Ist nämlich $m \in M$ so gilt für das Element $g(m) \in M$ die Gleichung $f(g(m)) = m$.

Insgesamt muss ein invertierbares Element von $\mathrm{Abb}\,(M)$ also bijektiv sein und in diesem Fall ist die Umkehrabbildung gerade das Inverse von f.