0. Einleitung und Motivation

Ihr habt in eurem bisherigen mathematischen Leben – sei es in der Schule oder an der Universität – sicher schon viele Arten von „Verknüpfungen“ kennengelernt, die zwei Objekten einer gewissen Menge ein drittes zuordnen und dabei gewisse Eigenschaften erfüllen. Das einfachste Beispiel hierfür ist wohl die ganz normale Addition reeller Zahlen: Sind x und y reelle Zahlen, so kann man daraus durch Addition eine neue reelle Zahl $x+y$ bilden. Diese Addition erfüllt gewisse Eigenschaften: So gilt z. B. $x+y=y+x$ für alle x und y (man sagt, die Addition ist *kommutativ*) und $(x+y)+z=x+(y+z)$ für alle x, y und z (man sagt, die Addition ist *assoziativ*).

Natürlich ist dies bei weitem nicht das einzige Beispiel für eine Verknüpfung. Reelle Zahlen lassen sich nicht nur addieren, sondern auch multiplizieren, und auch die Multiplikation ist kommutativ (es gilt $xy=yx$ für alle x und y) und assoziativ (es gilt stets $(xy)z=x(yz)$). Auch Vektoren lassen sich addieren, und vielleicht kennt ihr bereits Matrizen, die man ebenfalls addieren und multiplizieren kann. Es gibt aber auch noch ganz andere Arten von Verknüpfungen: Man kann z. B. zwei Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ verknüpfen, indem man sie „verkettet“, also hintereinander ausführt und so eine neue Funktion von $\mathbb{R}$ nach $\mathbb{R}$ erhält. Auch wenn so eine Verkettung von Funktionen natürlich etwas ganz anderes ist als die Addition zweier reeller Zahlen, hat sie dennoch etwas mit dieser Addition gemeinsam: Sie ist ebenfalls assoziativ (allerdings nicht kommutativ).

Eines der ganz wesentlichen Prinzipien der Mathematik (und in der Tat eine der wichtigsten Fähigkeiten, die ihr in eurem Studium lernen müsst) ist das *abstrakte Denken*. Im Fall unserer eben betrachteten Verknüpfungen heißt das einfach, dass wir von den oben aufgeführten konkreten Beispielen abstrahieren und stattdessen *beliebige* Mengen und Verknüpfungen betrachten sollten, die gewisse Eigenschaften wie z. B. die Kommutativität oder Assoziativität erfüllen. Wenn wir dann nämlich über derartige allgemeine Verknüpfungen irgendwelche Resultate beweisen, können wir diese dann später bei jeder neuen Verknüpfung, die wir kennenlernen (und ihr werdet in dieser Vorlesung und während eures restlichen Studiums noch sehr viele sehen), sofort anwenden, ohne uns erneut darüber Gedanken machen zu müssen.

Eine solche Menge mit einer Verknüpfung, die gewisse Eigenschaften erfüllt, bezeichnet man als eine *algebraische Struktur*. Die wichtigsten dieser algebraischen Strukturen – die sogenannten Gruppen, Ringe und Körper – werden der Inhalt dieser Vorlesung sein.

Auf den ersten Blick werdet ihr nun wahrscheinlich denken, dass die Eigenschaften der Addition reeller Zahlen (oder irgendeiner der anderen oben aufgeführten Verknüpfungen) wohl kaum so spannend sein können, dass sich damit eine ganze Vorlesung füllen lässt. Bevor wir mit dem eigentlichen Stoff beginnen, möchte ich euch daher noch an zwei informellen Beispielen zeigen, dass sich in der Tat schon mit nur einer Verknüpfung auf einer (geeignet gewählten) Menge sehr interessante Strukturen mit konkreten praktischen Anwendungen ergeben können.

Beispiel 0.1 (Prüfziffern)**.** Nehmen wir einmal an, dass wir eine Ziffernfolge wie z. B. den Scancode auf Lebensmitteln oder eine Personalausweisnummer haben, die wir auf irgendeine Art übertragen möchten: Der Scancode wird vielleicht von einem Scanner eingelesen, die Personalausweisnummer möglicherweise von Hand in ein Formular eingetragen und später von einer Person abgetippt, die das Formular bearbeitet. Bei solchen Übertragungen können natürlich Fehler passieren. Man möchte die Ziffernfolgen daher so absichern, dass typische Übertragungsfehler zu einer erkennbar „ungültigen“ Folge führen und die Fehler so entdeckt werden können.

Die einfachste Idee, die man hierfür haben kann, ist die, dass man zu der eigentlichen Ziffernfolge eine weitere Prüfziffer hinzufügt, die sich einfach daraus ergibt, dass man alle Ziffern der gegebenen Folge ohne Übertrag addiert. Etwas mathematischer formuliert heißt das folgendes: Wir definieren

auf der Menge $\{0,\dots,9\}$ aller Ziffern eine Verknüpfung „+“ durch

$$a+b = \text{der Rest der gewöhnlichen Summe von } a \text{ und } b \text{ bei Division durch 10.}$$

Ist nun $a_1,a_2,\dots,a_n$ unsere eigentliche Ziffernfolge, so ist die Idee also, zu dieser Folge einfach die Prüfziffer $a_1+a_2+\dots+a_n$ hinzuzufügen. Betrachten wir z. B. die ursprüngliche Ziffernfolge 1384, so würden wir also $1+3+8+4=6$ rechnen (denn die gewöhnliche Summe dieser Zahlen ist 16) und stattdessen die Ziffernfolge 1384**6** benutzen.

Die Erfahrung zeigt nun, dass der häufigste Übertragungsfehler einfach darin besteht, dass eine der Ziffern falsch gelesen wird, also z. B. statt 13846 die Folge 18846 gelesen wird. Mit Hilfe unserer Prüfziffer können wir diesen Fehler nun sofort erkennen, denn es ist $1+8+8+4=1\neq 6$ (mit der oben definierten Addition, denn die gewöhnliche Summe der vier ersten Ziffern ist 21): Die Prüfziffer am Ende stimmt nicht. Man sieht leicht ein, dass in der Tat jede beliebige Ersetzung einer der Ziffern dazu führt, dass die Prüfsumme nicht mehr stimmt und der Fehler damit erkannt wird. (Wird mehr als eine Ziffer falsch gelesen, kann der Fehler in der Regel nicht mehr erkannt werden, aber das können wir mit nur einer Prüfziffer natürlich auch nicht erwarten.) So weit scheint die Sache mit der Prüfziffer also schon einmal eine gute Idee zu sein.

Der zweithäufigste Übertragungsfehler, der auch noch recht oft vorkommt, ist erfahrungsgemäß einfach ein „Zahlendreher“, d. h. es werden zwei benachbarte Ziffern vertauscht, in unserem Fall also z. B. statt 13846 die Folge 31846 übertragen. Einen solchen Fehler erkennt unsere Prüfziffer bisher natürlich nicht, denn die Summe der Ziffern hängt ja nicht von ihrer Reihenfolge ab: Es ist auch $3+1+8+4=6$ (wieder ohne Übertrag gerechnet).

Durch eine einfache Modifikation können wir unser Prüfziffernsystem jedoch deutlich verbessern, so dass es oft auch derartige Zahlendreher erkennt: Statt der einfachen Summe $a_1+a_2+\dots$ aller Ziffern verwenden wir als Prüfziffer den Ausdruck $a_1+3a_2+a_3+3a_4+\dots$ (wieder mit der obigen Addition, also ohne Übertrag gerechnet), bei dem also jede zweite Ziffer zunächst mit 3 multipliziert wird. Dies ist übrigens genau das Verfahren, das bei den bekannten Waren-Scancodes verwendet wird.

Im Beispiel unserer obigen Ziffernfolge 1384 sieht das dann so aus:

- Die Prüfziffer ist $1+3\cdot 3+8+3\cdot 4=0$ (ohne Übertrag, denn die normale Summe ist 30), unsere Folge mit Prüfziffer also 13840.
- Wird eine Ziffer geändert, also z. B. wie oben statt 13840 die Folge 18840 gelesen, so wird dies weiterhin erkannt: Es ist $1+3\cdot 8+8+3\cdot 4=5\neq 0$, die Prüfziffer stimmt nicht.
- Vertauschen wir die ersten beiden Ziffern und lesen 31840, so wird dieser Fehler nun ebenfalls erkannt: Es ist $3+3\cdot 1+8+3\cdot 4=6\neq 0$, die Prüfziffer stimmt auch hier nicht.
- Vertauschen wir allerdings die zweite mit der dritten Ziffer und lesen 18340, so wird dieser Fehler von der Prüfziffer nicht erkannt, denn es ist $1+3\cdot 8+3+3\cdot 4=0$.

Unser neues System erkennt also *manchmal* auch Zahlendreher, aber nicht immer.

Die Frage ist nun natürlich: Geht es noch besser? Können wir eine Prüfziffer so konstruieren, dass sowohl Fehler in einer der Ziffern als auch beliebige Zahlendreher *immer* erkannt werden? In der Sprache dieser Vorlesung suchen wir also eine Verknüpfung der Ziffern der Folge zu einer Prüfziffer, die eine gewisse Eigenschaft hat.

Die Antwort auf diese Frage ist übrigens ja: Man kann mit einer besonders geschickt konstruierten Prüfziffer beide oben angesprochenen Arten von Fehlern immer entdecken. Die alten DM-Geldscheine hatten zum Beispiel in ihrer Seriennummer ein derartiges Prüfziffernsystem. Das Verfahren hierfür ist jedoch bereits recht kompliziert und soll daher hier nicht näher erläutert werden. Wir erkennen daran aber bereits, dass schon das Studium von Verknüpfungen auf einer Menge von nur 10 Elementen recht interessant werden kann und auch konkrete praktische Anwendungen hat.

Beispiel 0.2 (Einwegfunktionen und Kryptografie)**.** In Beispiel 0.1 haben wir auf der Menge $\{0,\dots,9\}$ die Verknüpfung betrachtet, die man erhält, indem man zwei solche Zahlen addiert und dann den Rest bei Division durch 10 nimmt. Eine analoge Konstruktion wollen wir nun mit der

Multiplikation statt mit der Addition machen und dabei gleichzeitig die Zahl 10 durch eine beliebige andere ersetzen. Wir wählen uns also eine natürliche Zahl $n \geq 2$ und betrachten auf der Menge $\{0,\dots,n-1\}$ die Verknüpfung

$$a \cdot b = \text{der Rest des gewöhnlichen Produkts von } a \text{ und } b \text{ bei Division durch } n.$$

Um ein Gefühl für diese Verknüpfung zu bekommen, betrachten wir einmal ein Beispiel: Wir wählen $n = 11$ und berechnen in der folgenden Tabelle die „Potenzen“ 2^k für $k = 1,\dots,10$ – also die Ergebnisse, die man erhält, wenn man k-mal die Zahl 2 mit sich selbst verknüpft. Man kann die untere Zeile dieser Tabelle also einfach dadurch erhalten, dass man jeweils den vorherigen Eintrag mit 2 multipliziert und vom Ergebnis dann nur den Rest bei Division durch 11 nimmt: Der Eintrag 5 bei 2^4 entsteht z. B. durch die Rechnung $2 \cdot 8 = 16$, was bei Division durch 11 den Rest 5 ergibt.

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	5	10	9	7	3	6	1

Wenn wir uns diese Tabelle ansehen, machen wir eine interessante Beobachtung: Die Werte für 2^k, also die Zahlen in der unteren Reihe, sind einfach alle Zahlen von 1 bis 10, allerdings in einer vertauschten Reihenfolge. Die Abbildung $k \mapsto 2^k$ auf der Menge $\{1,\dots,10\}$ ist also umkehrbar: Man kann k aus 2^k rekonstruieren.

Dies ist kein Zufall – man kann zeigen, dass es zumindest für jede Primzahl n eine Basiszahl a gibt, so dass die Potenzen $a^1, a^2, \dots, a^{n-1}$ in obigem Sinne genau die Zahlen von 1 bis $n-1$ in irgendeiner vertauschten Reihenfolge sind.

Was kann man nun mit dieser Beobachtung anfangen? Stellen wir uns einmal vor, dass wir n sehr sehr groß wählen – irgendeine Zahl mit mehreren hundert oder tausend Stellen. Die Potenzen a^k (mit entsprechend großen Werten für k) lassen sich mit Hilfe der Potenzgesetze dann immer noch recht schnell berechnen: Möchten wir z. B. a^{32} bestimmen, so können wir stattdessen einfach $((((a^2)^2)^2)^2)^2$ rechnen, was nur fünf Rechenoperationen benötigt und somit nicht erfordert, dass wir alle vorhergehenden Potenzen $a^1, a^2, \dots, a^{31}$ auch ausgerechnet haben. Ein allgemeines k, das nicht gerade eine Zweierpotenz ist, kann man mit Hilfe der Binärentwicklung zumindest als Summe von Zweierpotenzen schreiben und somit auch in diesem Fall die Zahl a^k mit den Potenzgesetzen relativ schnell berechnen.

Im Gegensatz dazu ist aber für die Umkehrung, also für die (nach obigen Überlegungen theoretisch mögliche) Rekonstruktion von k aus a^k keine Methode bekannt, die wesentlich schneller ist als ein reines Durchprobieren aller Werte für k. Und ein solches Durchprobieren ist für riesige Zahlen n bzw. k natürlich nicht mehr praktisch durchführbar. Wir haben hier also ein interessantes Phänomen: Eine Funktion (nämlich die Abbildung $k \mapsto a^k$ der Menge $\{1,\dots,n-1\}$ in sich), die einfach zu berechnen ist und die eine Umkehrfunktion besitzt, für die diese Umkehrfunktion aber praktisch nicht berechenbar ist. Eine solche Funktion wird in der Literatur in der Regel als *Einwegfunktion* bezeichnet.

Anwendungen finden solche Einwegfunktionen vor allem in der Kryptografie. Nehmen wir einmal an, ihr müsst am Computer oder für eine Webseite ein Passwort wählen; der Einfachheit halber sei dieses Passwort einfach eine Zahl k aus der Menge $\{1,\dots,n-1\}$. Natürlich muss der Computer dieses Passwort irgendwie speichern, da er beim nächsten Mal, wenn ihr das Passwort eingebt, ja vergleichen können muss, ob die Eingabe korrekt war. Man möchte die Passwörter aber nur ungern ganz normal in einer Datei speichern, da sonst ein Angreifer, der vielleicht diese Datei in die Finger bekommt, sofort die Passwörter aller Benutzer im Klartext lesen könnte.

Eine mögliche Lösung dieses Problems besteht nun einfach darin, statt des eigentlichen Passworts k die Zahl a^k abzuspeichern. Bei einer erneuten Eingabe eines Passworts l kann der Computer dann immer noch einfach überprüfen, ob die Eingabe korrekt war: Er muss einfach a^l berechnen und mit dem gespeicherten Wert a^k vergleichen; es ist dann $l = k$ (also das Passwort korrekt) genau dann wenn $a^l = a^k$. Allerdings ist die Datei mit den gespeicherten Werten a^k jetzt für einen Angreifer

nutzlos, da aus diesen Zahlen a^k nicht mehr die eigentlichen Passwörter rekonstruiert werden können.

Wir sehen also, dass auch diese einfache „Multiplikationsstruktur“ bereits zu interessanten Anwendungen führt.

Nach diesen beiden praktischen Beispielen wollen wir aber nun mit dem eigentlichen Stoff der Vorlesung, dem Studium der algebraischen Strukturen, beginnen. Wir fangen dabei ganz am Anfang an und setzen keine Vorkenntnisse voraus; lediglich die elementaren Notationen zur Logik, Mengenlehre und zu Abbildungen werden wir ohne weitere Erläuterungen in einem Umfang benutzen, wie sie typischerweise in der Vorlesung „Grundlagen der Mathematik 1“ in der ersten Semesterwoche behandelt werden [G, Kapitel 1 und 2.A].