Algebraische Strukturen

Andreas Gathmann

Vorlesungsskript TU Kaiserslautern 2019/20

Inhaltsverzeichnis

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].

1. Gruppen

Wie schon in der Einleitung erläutert wollen wir uns in dieser Vorlesung mit Mengen beschäftigen, auf denen algebraische Verknüpfungen mit gewissen Eigenschaften definiert sind. Die in der Mathematik wichtigste derartige Struktur ist die einer Gruppe.

Definition 1.1 (Gruppen)**.**

(a) Eine **Gruppe** ist eine Menge G zusammen mit einer „Verknüpfung“, d. h. einer Abbildung

$$\begin{aligned} \cdot : G \times G &\to G \\ (a,b) &\mapsto a \cdot b \end{aligned}$$

so dass die folgenden Eigenschaften (auch *Gruppenaxiome* genannt) gelten:

(G1) Für alle $a,b,c \in G$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (**Assoziativität**).

(G2) Es gibt ein $e \in G$, so dass $e \cdot a = a$ für alle $a \in G$ gilt (man nennt ein solches e ein **linksneutrales Element**), und für das die folgende Eigenschaft gilt:

(G3) Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $a' \cdot a = e$ (man nennt ein solches a' ein zu a **linksinverses Element**).

Wir schreiben eine solche Gruppe als $(G, \cdot)$, oder manchmal auch einfach nur als G, wenn die betrachtete Verknüpfung aus dem Zusammenhang klar ist. In diesem Fall schreibt man für die Verknüpfung $a \cdot b$ zweier Elemente oft auch einfach nur ab.

(b) Gilt zusätzlich zu den Gruppenaxiomen (G1), (G2) und (G3) noch

(G4) Für alle $a,b \in G$ gilt $a \cdot b = b \cdot a$ (**Kommutativität**),

so heißt $(G, \cdot)$ eine **kommutative** oder **abelsche Gruppe**.

(c) Hat G nur endlich viele Elemente, so heißt G eine **endliche Gruppe** und die Anzahl ihrer Elemente die **Ordnung** von G. Wie für eine beliebige Menge schreibt man diese Anzahl Elemente als $|G|$.

Beispiel 1.2. Wir wollen in dieser Vorlesung die „Standardzahlbereiche“

$\mathbb{N} = \{0,1,2,\dots\}$ der **natürlichen Zahlen**,
$\mathbb{Z} = \{0,\pm 1,\pm 2,\dots\}$ der **ganzen Zahlen**,
$\mathbb{Q}$ der **rationalen Zahlen**,
$\mathbb{R}$ der **reellen Zahlen**

zusammen mit den üblichen darauf definierten Verknüpfungen (z. B. Addition und Multiplikation) und ihren Eigenschaften als aus der Schule bekannt voraussetzen. Man könnte diese Mengen und Verknüpfungen zwar auch allein aus den Prinzipien der Mengenlehre konstruieren und ihre Eigenschaften dann beweisen (siehe z. B. [E, Kapitel 1 und 2]) — dies soll aber nicht der Inhalt dieser Vorlesung sein und würde zum momentanen Zeitpunkt auch mehr verwirren als helfen.

Setzen wir die Eigenschaften dieser Zahlbereiche also als bekannt voraus, so können wir daraus die folgenden einfachen Beispiele für Gruppen gewinnen:

(a) $(\mathbb{R},+)$, also die reellen Zahlen zusammen mit der Addition als Verknüpfung, bilden eine abelsche Gruppe, denn es gilt:

(G1) $(a+b)+c = a+(b+c)$ für alle $a,b,c \in \mathbb{R}$;

(G2) die Zahl 0 ist ein linksneutrales Element, denn es ist $0+a = a$ für alle $a \in \mathbb{R}$;

(G3) zu $a \in \mathbb{R}$ ist $-a \in \mathbb{R}$ ein linksinverses Element, denn es ist stets $(-a)+a = 0$;

(G4) $a+b=b+a$ für alle $a,b\in\mathbb{R}$.

Genauso sind auch $(\mathbb{Q},+)$ und $(\mathbb{Z},+)$ abelsche Gruppen. Im Gegensatz dazu ist $(\mathbb{N},+)$ keine Gruppe: (G1) und (G2) sind zwar weiterhin erfüllt, aber das Gruppenaxiom (G3) ist hier verletzt, da z. B. die Zahl $1\in\mathbb{N}$ kein linksinverses Element besitzt (die hierfür benötigte Zahl -1 liegt nicht in $\mathbb{N}$).

Wenn wir im Folgenden ohne weitere Angaben von $\mathbb{R}$, $\mathbb{Q}$ oder $\mathbb{Z}$ als Gruppe reden, wollen wir vereinbaren, dass immer die Addition als Verknüpfung gemeint ist.

(b) $(\mathbb{R},\cdot)$, also die reellen Zahlen zusammen mit der gewöhnlichen Multiplikation, bilden ebenfalls keine Gruppe: (G1) und (G2) sind hier zwar erfüllt (mit dem einzig möglichen linksneutralen Element 1), aber zu der Zahl 0 gibt es kein linksinverses Element, also kein $a'\in\mathbb{R}$ mit $a'\cdot 0=1$.

Dieses „Problem“ lässt sich jedoch leicht beheben, indem man die 0 einfach aus der Menge herausnimmt: $(\mathbb{R}\backslash\{0\},\cdot)$ ist eine abelsche Gruppe, denn die Assoziativität und die Existenz eines linksneutralen Elementes 1 gelten immer noch, und zusätzlich haben wir:

(G3) Jedes $a\in\mathbb{R}\backslash\{0\}$ hat ein linksinverses Element $a'=\frac{1}{a}$ (mit $\frac{1}{a}\cdot a=1$);

(G4) $a\cdot b=b\cdot a$ für alle $a,b\in\mathbb{R}\backslash\{0\}$.

Genauso ist auch $(\mathbb{Q}\backslash\{0\},\cdot)$ eine abelsche Gruppe. Dagegen sind $(\mathbb{Z}\backslash\{0\},\cdot)$ und $(\mathbb{N}\backslash\{0\},\cdot)$ keine Gruppen: (G1) und (G2) gelten zwar weiterhin (wiederum mit linksneutralem Element 1), aber das Gruppenaxiom (G3) ist verletzt, da z. B. die Zahl 2 kein linksinverses Element besitzt (die hierfür benötigte Zahl $\frac{1}{2}$ liegt nicht in $\mathbb{Z}$ bzw. $\mathbb{N}$).

Analog zu (a) wollen wir vereinbaren, dass immer die Multiplikation gemeint ist, wenn wir ohne Angabe einer Verknüpfung von der Gruppe $\mathbb{R}\backslash\{0\}$ oder $\mathbb{Q}\backslash\{0\}$ sprechen.

(c) Die Menge $G=\{0,\pm1,\pm2\}$ mit der gewöhnlichen Addition ist *keine* Gruppe, obwohl es auf den ersten Blick vielleicht so aussieht, als ob die Gruppenaxiome (G1), (G2) und (G3) erfüllt wären. Die Addition ist nämlich nicht einmal eine Verknüpfung auf G, da sie zwei Elemente von G nicht unbedingt wieder nach G abbildet: Es gilt zwar $1,2\in G$, aber $1+2=3\notin G$. In diesem Sinne steckt in Definition 1.1 also schon in der allerersten Formulierung „eine Gruppe ist eine Menge zusammen mit einer Verknüpfung“ eine Bedingung.

(d) Nach (G2) hat jede Gruppe mindestens ein Element — und zwar ein linksneutrales. Mehr braucht es jedoch nicht: Die einelementige Menge $G=\{e\}$ mit der durch $e\cdot e:=e$ definierten trivialen Verknüpfung ist bereits eine Gruppe (wenn auch keine sehr interessante). Sie wird die **triviale Gruppe** genannt.

Bemerkung 1.3 (Verknüpfungstafeln)**.** Verknüpfungen auf Mengen mit nur wenigen Elementen lassen sich mit Hilfe einer **Verknüpfungstafel** angeben — so wie im Bild rechts, das auf der Menge $G=\{0,1\}$ eine Verknüpfung $*$ definiert, indem die Werte $a*b$ für alle $a,b\in G$ einfach in einer Tabelle angegeben werden. Um festzustellen, ob eine so definierte Verknüpfung alle Gruppenaxiome erfüllt, muss man die Eigenschaften aus Definition 1.1 dann für alle Elemente von G durchgehen.

$*$	0	1
0	0	1
1	1	0

Bei der hier angegebenen Verknüpfungstafel ist dies der Fall, wobei 0 ein linksneutrales Element und jedes Element zu sich selbst linksinvers ist. Die so definierte (abelsche) Gruppe wird mit $\mathbb{Z}_2$ bezeichnet; man kann sie sich vorstellen als „gerade Zahlen (entsprechend 0) und ungerade Zahlen (entsprechend 1) unter Addition“, so dass also z. B. $1*1=0$ bedeutet, dass die Summe zweier ungerader Zahlen gerade ist. Eine deutlich allgemeinere Konstruktion von Gruppen dieser Art werden wir in Beispiel 6.15 kennenlernen.

Beispiel 1.4. Wir definieren auf der Menge $G=\mathbb{R}$ eine Verknüpfung „$*$“ durch

$$a*b:=a+b+1 \quad \text{für } a,b\in\mathbb{R}$$

(wobei „+“ die gewöhnliche Addition reeller Zahlen bezeichnet) und behaupten, dass $(\mathbb{R},*)$ damit zu einer abelschen Gruppe wird. Im Gegensatz zu Beispiel 1.2 (a) und (b), wo wir die Gruppeneigenschaften von $\mathbb{R}$ bezüglich der gewöhnlichen Addition und Multiplikation einfach als bekannt vorausgesetzt haben, müssen wir bei dieser speziell konstruierten Verknüpfung nun natürlich *beweisen*, dass die Gruppenaxiome gelten. Dies rechnet man einfach nach:

(G1) Für alle $a,b,c \in \mathbb{R}$ ist

$$(a*b)*c = (a+b+1)*c = (a+b+1)+c+1 = a+b+c+2$$

und genauso

$$a*(b*c) = a*(b+c+1) = a+(b+c+1)+1 = a+b+c+2,$$

woraus die Assoziativität der Verknüpfung folgt (natürlich haben wir hierbei wieder die Eigenschaften der Addition reeller Zahlen als bekannt vorausgesetzt).

(G2) Die Zahl $e := -1 \in \mathbb{R}$ ist ein linksneutrales Element der Verknüpfung, denn für alle $a \in \mathbb{R}$ gilt

$$(-1)*a = (-1)+a+1 = a.$$

(G3) Zu jedem $a \in \mathbb{R}$ ist $-2-a \in \mathbb{R}$ ein linksinverses Element, denn es gilt

$$(-2-a)*a = (-2-a)+a+1 = -1 = e.$$

(G4) Für alle $a,b \in \mathbb{R}$ gilt

$$a*b = a+b+1 = b+a+1 = b*a.$$

Also ist $(\mathbb{R},*)$ eine abelsche Gruppe — allerdings eine ziemlich langweilige und unwichtige, die euch wohl nie wieder begegnen wird. Der Sinn dieses einfachen Beispiels war es lediglich zu sehen, wie man bei einer konkret gegebenen Verknüpfung die Gruppenaxiome überprüfen kann.

Konstruktion 1.5 (Produkte von Gruppen)**.** Es seien $(G,*)$ und $(H,\circ)$ zwei Gruppen — wir verwenden hier verschiedene Symbole, um die beiden Verknüpfungen unterscheiden zu können. Wir können dann auch auf dem Produkt

$$G \times H = \{(a_1,a_2) : a_1 \in G, a_2 \in H\}$$

eine Verknüpfung definieren, indem wir die beiden gegebenen Verknüpfungen komponentenweise anwenden: Wir setzen einfach

$$(a_1,a_2)\cdot(b_1,b_2) := (a_1*b_1, a_2\circ b_2) \quad \text{für } (a_1,a_2),(b_1,b_2) \in G\times H.$$

Dies macht $G\times H$ zu einer Gruppe, die wir das **Produkt** der Gruppen G und H nennen. In der Tat folgen die Gruppenaxiome für $(G\times H,\cdot)$ sofort aus denen für $(G,*)$ und $(H,\circ)$:

(G1) Für alle $a_1,b_1,c_1 \in G$ und $a_2,b_2,c_2 \in H$ gilt nach Definition der Verknüpfung in $G\times H$

$$\begin{aligned}((a_1,a_2)\cdot(b_1,b_2))\cdot(c_1,c_2) &= (a_1*b_1, a_2\circ b_2)\cdot(c_1,c_2)\\ &= ((a_1*b_1)*c_1, (a_2\circ b_2)\circ c_2)\end{aligned}$$

und

$$\begin{aligned}(a_1,a_2)\cdot((b_1,b_2)\cdot(c_1,c_2)) &= (a_1,a_2)\cdot(b_1*c_1, b_2\circ c_2)\\ &= (a_1*(b_1*c_1), a_2\circ(b_2\circ c_2)).\end{aligned}$$

Wegen der Assoziativität der Verknüpfungen in G und H stimmen diese beiden Ausdrücke überein — was die Assoziativität in $G\times H$ zeigt.

(G2) Das Paar (e_G,e_H) der beiden neutralen Elemente von G und H ist ein linksneutrales Element in $G\times H$, denn es ist

$$(e_G,e_H)\cdot(a_1,a_2) = (e_G*a_1, e_H\circ a_2) = (a_1,a_2)$$

für alle $(a_1,a_2) \in G\times H$.

(G3) Sind a_1' und a_2' linksinverse Elemente zu a_1 in G bzw. zu a_2 in H, so ist (a_1', a_2') linksinvers zu (a_1, a_2) in $G \times H$, denn

$$(a_1', a_2') \cdot (a_1, a_2) = (a_1' * a_1, a_2' \circ a_2) = (e_G, e_H).$$

Sind zudem G und H abelsch, so folgt natürlich auf die gleiche Art, dass dann auch $G \times H$ abelsch ist.

Das einfachste Beispiel für ein Produkt von Gruppen kennt ihr sicher schon aus der Schule: Die Menge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ aller Vektoren in der Ebene mit der komponentenweisen Addition

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2).$$

Es hindert uns aber auch nichts daran, das Produkt von zwei „ganz verschiedenen" Gruppen zu bilden, also z. B. $(\mathbb{Z}, +) \times (\mathbb{R} \backslash \{0\}, \cdot)$. Auch kann man natürlich ganz analog das Produkt von mehr als zwei Gruppen bilden.

Aufgabe 1.6. Untersuche, ob es sich bei den folgenden Mengen und Verknüpfungen um Gruppen handelt. (Man gebe also einen Beweis der Gruppenaxiome oder ein Gegenbeispiel für ein verletztes Axiom an.)

(a) $G = 5\mathbb{Z} := \{5n : n \in \mathbb{Z}\}$, also die Menge aller durch 5 teilbaren ganzen Zahlen, mit der gewöhnlichen Addition als Verknüpfung;

(b) $G = 5\mathbb{Z}$ mit der gewöhnlichen Multiplikation als Verknüpfung;

(c) $G = \mathbb{Q}_{>0}$ mit der Verknüpfung $a * b := \frac{ab}{2}$;

(d) $G = \mathbb{R} \times \mathbb{R}$ mit der Verknüpfung $(a_1, a_2) * (b_1, b_2) := (a_1 + b_2, a_2 + b_1)$;

(e) $G = \mathbb{R} \times \mathbb{R}$ mit der Verknüpfung $(a_1, a_2) * (b_1, b_2) := (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$.

Wir werden später noch mehr Beispiele für Gruppen sehen. Zunächst wollen wir aber ein kleines Resultat beweisen, das es uns erlaubt, etwas einfacher über Gruppen reden zu können. Schauen wir uns dazu einmal das Gruppenaxiom (G2) an: Wir haben hier für $e \in G$ die Beziehung $e \cdot a = a$ für alle $a \in G$ gefordert und e *links*neutral genannt — weil es ein gegebenes a nicht ändert, wenn man es von links mit e verknüpft. Da wir für eine allgemeine Gruppe keine Kommutativität vorausgesetzt haben, folgt daraus natürlich zunächst einmal *nicht*, dass auch $a \cdot e = a$ für alle $a \in G$ gelten muss, dass e also auch *rechts*neutral ist. Wir wollen nun allerdings zeigen, dass dies doch immer der Fall ist und wir e deswegen einfach als *neutrales Element* bezeichnen können. Außerdem wollen wir zeigen, dass ein solches neutrales Element nicht nur existiert (wie es ja in den Gruppenaxiomen gefordert ist), sondern sogar *eindeutig* ist, so dass wir in Zukunft nicht nur von *einem* neutralen Element, sondern von *dem* neutralen Element reden können.

Die gleichen Aussagen gelten übrigens analog auch für inverse Elemente: Ein linksinverses Element ist immer auch rechtsinvers, und ist darüber hinaus auch eindeutig bestimmt. Alles dies besagt der folgende Satz, den wir jetzt beweisen wollen.

Satz 1.7 (Existenz und Eindeutigkeit neutraler und inverser Elemente)**.** *In jeder Gruppe G gilt:*

(a) *Es gibt genau ein linksneutrales Element $e \in G$;*

(b) *dieses linksneutrale Element ist dann auch **rechtsneutral**, d. h. es gilt $a \cdot e = a$ für alle $a \in G$;*

(c) *jedes $a \in G$ besitzt genau ein linksinverses Element $a' \in G$;*

(d) *dieses linksinverse Element ist dann auch **rechtsinvers**, d. h. es gilt $a \cdot a' = e$.*

*Wir können in Zukunft statt von links- und rechtsneutralen bzw. -inversen Elementen also einfach von dem **neutralen** und dem zu einem $a \in G$ **inversen Element** reden.*

Beweis. Nach (G2) existiert in G ein linksneutrales Element e, das (G3) erfüllt. Wir beweisen die vier Aussagen in etwas anderer Reihenfolge, als sie in der Behauptung aufgeführt sind.

(d) Es seien $a \in G$ beliebig und $a' \in G$ ein dazu linksinverses Element, d. h. es gilt $a' \cdot a = e$. Nach (G3) existiert zu diesem a' wiederum ein linksinverses Element $a'' \in G$, es ist also $a'' \cdot a' = e$. Damit folgt nun (wir schreiben zur besseren Verständlichkeit des Beweises hinter jede Gleichheit die zugehörige Begründung)

$$\begin{aligned} a \cdot a' &= e \cdot (a \cdot a') && \text{(G2)} \\ &= (a'' \cdot a') \cdot (a \cdot a') && (a'' \text{ ist linksinvers zu } a') \\ &= a'' \cdot (a' \cdot (a \cdot a')) && \text{(G1)} \\ &= a'' \cdot ((a' \cdot a) \cdot a') && \text{(nochmal G1)} \\ &= a'' \cdot (e \cdot a') && (a' \text{ ist linksinvers zu } a) \\ &= a'' \cdot a' && \text{(G2)} \\ &= e. && (a'' \text{ ist linksinvers zu } a') \end{aligned}$$

Also ist a' auch ein rechtsinverses Element zu a.

(b) Es sei $a \in G$ beliebig. Nach (G3) existiert zu a ein linksinverses Element $a' \in G$, d. h. es gilt $a' \cdot a = e$. Damit folgt

$$\begin{aligned} a \cdot e &= a \cdot (a' \cdot a) && (a' \text{ ist linksinvers zu } a) \\ &= (a \cdot a') \cdot a && \text{(G1)} \\ &= e \cdot a && (a' \text{ ist nach (d) auch rechtsinvers zu } a) \\ &= a, && \text{(G2)} \end{aligned}$$

und damit ist e auch rechtsneutral. (Beachte, dass wir beim Beweis dieser Aussage u. a. den schon bewiesenen Teil (d) des Satzes verwendet haben.)

(a) Es sei $\tilde{e} \in G$ ein weiteres linksneutrales Element. Dann folgt sofort

$$\begin{aligned} e &= \tilde{e} \cdot e && (\tilde{e} \text{ ist linksneutral}) \\ &= \tilde{e}. && (e \text{ ist nach (b) rechtsneutral}) \end{aligned}$$

Also sind e und $\tilde{e}$ notwendigerweise gleich, d. h. es gibt nur ein neutrales Element. 01

(c) Es seien nun $a \in G$ beliebig und $a', \tilde{a}' \in G$ zwei linksinverse Elemente zu a, die dann nach (d) auch beide zu a rechtsinvers sind. Damit ergibt sich

$$\begin{aligned} a' &= e \cdot a' && \text{(G2)} \\ &= (\tilde{a}' \cdot a) \cdot a' && (\tilde{a}' \text{ ist linksinvers zu } a) \\ &= \tilde{a}' \cdot (a \cdot a') && \text{(G1)} \\ &= \tilde{a}' \cdot e && (a' \text{ ist rechtsinvers zu } a) \\ &= \tilde{a}'. && (e \text{ ist rechtsneutral nach (b)}) \end{aligned}$$

Also müssen a' und $\tilde{a}'$ gleich sein, d. h. es gibt zu a nur ein inverses Element. □

Das Symbol „□“ steht hierbei übrigens (wie in der Mathematik üblich) für das Ende eines Beweises.

Bemerkung 1.8. Nach Satz 1.7 hätten wir in Definition 1.1 (a) anstatt der Teile (G2) und (G3) also auch genauso gut schreiben können

(G2′) es gibt *genau ein* $e \in G$ mit $e \cdot a = a \cdot e = a$ für alle $a \in G$;

(G3′) für alle $a \in G$ gibt es *genau ein* $a' \in G$ mit $a' \cdot a = a \cdot a' = e$.

Unser gerade bewiesener Satz zeigt uns, dass die so entstehende Definition zu unserer ursprünglichen äquivalent gewesen wäre. In der Tat wird man wohl auch in manchen Büchern diese abgeänderte Definition finden. Unsere Definition 1.1 (a) hat aber in der Praxis den Vorteil, dass die Bedingungen in konkreten Fällen leichter nachprüfbar sind, weil sie (scheinbar) schwächer sind.

Notation 1.9.

(a) Da neutrale und inverse Elemente in Gruppen nach Satz 1.7 eindeutig sind, gibt man ihnen oft besondere Namen: Das zu einem Element a inverse Element schreibt man als a^{-1}, und das neutrale Element manchmal einfach als 1. Eine Ausnahme macht man hierbei nur, wenn man die Gruppenverknüpfung mit dem Symbol „+“ schreibt: Hier ist es (aufgrund von Beispiel 1.2 (a)) natürlicher, das zu a inverse Element als $-a$ und das neutrale Element als 0 zu schreiben.

(b) Schreibt man die Gruppenverknüpfung als „+“, so verwendet man oft die Notation $a-b$ für $a+(-b)$. Die analoge Notation $\frac{a}{b}$ bei multiplikativ geschriebener Gruppenverknüpfung ist jedoch mit Vorsicht zu genießen, da man sie sowohl als ab^{-1} als auch als $b^{-1}a$ interpretieren könnte — und in allgemeinen Gruppen ist das ja nicht dasselbe. Man sollte diese Schreibweise daher (wenn überhaupt) nur bei abelschen Gruppen anwenden.

(c) Wir haben im Beweis von Satz 1.7 gesehen, dass die Assoziativität (G1) in der Praxis einfach dazu führt, dass Klammern bei mehrfachen Verknüpfungen beliebig umgesetzt werden können, ohne das Resultat zu verändern. Man lässt diese Klammern daher in der Regel einfach ganz weg und schreibt z. B. für $a,b,c \in G$ einfach $a \cdot b \cdot c$ oder abc an Stelle von $(a \cdot b) \cdot c$ oder $a \cdot (b \cdot c)$.

Zum Abschluss dieses Kapitels wollen wir nun noch ein paar allgemeine Rechenregeln herleiten, die in beliebigen Gruppen gelten und die wir später immer wieder benötigen werden. Die wichtigsten dieser Regeln enthält das folgende Lemma („Lemma“ ist griechisch und bedeutet eigentlich „Annahme“, aber in der Mathematik wird dieser Begriff für einen *Hilfssatz* verwendet — also für ein kleines Zwischenresultat, das vielleicht für sich genommen nicht übermäßig schwierig oder spannend ist, aber das in späteren Untersuchungen immer wieder nützlich sein wird).

Lemma 1.10 (Rechenregeln in Gruppen)**.** *Es sei G eine Gruppe. Dann gilt für alle $a,b \in G$:*

(a) $(a^{-1})^{-1} = a$.

(b) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

(c) ***(Kürzungsregel)*** *Für alle $x \in G$ ist*

$$\begin{aligned} & x \cdot a = x \cdot b \quad \text{genau dann wenn} \quad a = b, \\ \text{und analog} \qquad & a \cdot x = b \cdot x \quad \text{genau dann wenn} \quad a = b. \end{aligned}$$

Beweis.

(a) Nach Satz 1.7 (d) ist $aa^{-1} = e$. Dies bedeutet aber genau, dass a das inverse Element zu a^{-1} ist, d. h. dass $(a^{-1})^{-1} = a$ gilt.

(b) ist analog zu (a): Es ist $b^{-1}a^{-1}ab = b^{-1}b = e$. Lesen wir dies als $(b^{-1}a^{-1})(ab) = e$, so bedeutet dies gerade, dass $b^{-1}a^{-1}$ wie behauptet das inverse Element zu ab ist.

(c) Gilt $xa = xb$, so folgt daraus durch Verknüpfung mit x^{-1} von links auch $x^{-1}xa = x^{-1}xb$ und damit $a = b$. Umgekehrt folgt aus $a = b$ durch Verknüpfung mit x von links natürlich $xa = xb$. Die zweite Äquivalenz zeigt man analog. □

Neben diesen elementaren Rechenregeln sind noch mehrfache Verknüpfungen eines Gruppenelements mit sich selbst wichtig. Wir können diese als Potenzen auffassen:

Definition 1.11 (**Potenzen**)**.** Es sei G eine Gruppe, $a \in G$ und $n \in \mathbb{Z}$. Dann setzen wir

$$a^n := \begin{cases} a \cdot \dots \cdot a \quad (n\text{-mal}) & \text{falls } n > 0, \\ e & \text{falls } n = 0, \\ a^{-1} \cdot \dots \cdot a^{-1} \quad ((-n)\text{-mal}) & \text{falls } n < 0. \end{cases}$$

Schreiben wir die Gruppenverknüpfung mit dem Symbol „+“, so verwenden wir die Schreibweise $n \cdot a$ statt a^n, um Verwirrungen zu vermeiden.

Diese Potenzen erfüllen nun die erwarteten Eigenschaften:

Lemma 1.12 (Rechenregeln für Potenzen)**.** *In jeder Gruppe G gilt für alle $a \in G$ und $m,n \in \mathbb{Z}$*

(a) $a^m \cdot a^n = a^{m+n}$;

(b) $(a^m)^n = a^{m\cdot n}$.

(Beachte, dass die Verknüpfung „$\cdot$“ in diesen Gleichungen in zwei Bedeutungen auftritt: als Gruppenverknüpfung auf der linken Seite von (a) und als gewöhnliche Multiplikation zweier ganzer Zahlen auf der rechten Seite von (b).)

Beweis.

(a) Für $m \geq 0$ und $n \geq 0$ ist die Behauptung klar nach Definition 1.11, da dann auf beiden Seiten einfach $(m+n)$-mal das Element a mit sich selbst verknüpft wird. Ebenso ergibt sich die Behauptung sofort für $m < 0$ und $n < 0$, weil dann auf beiden Seiten die $(-m-n)$-fache Verknüpfung von a^{-1} mit sich selbst steht.

Ist hingegen $m \geq 0$ und $n < 0$, so ist die linke Seite der zu beweisenden Gleichung nach Definition 1.11 gleich

$$\underbrace{a \cdot \ldots \cdot a}_{m\text{-mal}} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{(-n)\text{-mal}}.$$

Durch mehrfaches Herauskürzen von $a\,a^{-1}$ in der Mitte erhält man daraus

$$\begin{aligned} a \cdot \ldots \cdot a \quad &((m-(-n))\text{-mal}) && \text{falls } m \geq -n, \\ a^{-1} \cdot \ldots \cdot a^{-1} \quad &((-n-m)\text{-mal}) && \text{falls } m < -n. \end{aligned}$$

In beiden Fällen ist das Ergebnis nach Definition 1.11 wie behauptet gleich a^{m+n}.

Den noch fehlenden Fall $m < 0$ und $n \geq 0$ zeigt man natürlich analog.

(b) Abhängig von n unterscheiden wir die folgenden Fälle:

(1) Für $n \geq 0$ gilt nach Definition

$$(a^m)^n = \underbrace{a^m \cdot \ldots \cdot a^m}_{n\text{-mal}} \overset{\text{(a)}}{=} a^{\overbrace{m+\cdots+m}^{n\text{-mal}}} = a^{mn}.$$

(2) Für $n = -1$ müssen wir $(a^m)^{-1} = a^{-m}$ zeigen, also dass a^{-m} das Inverse zu a^m ist. Dies folgt aber aus Teil (a), da $a^{-m} \cdot a^m = a^{-m+m} = a^0 = e$ gilt.

(3) Für $n < -1$ ergibt sich nun wieder aus der Definition

$$(a^m)^n = \underbrace{(a^m)^{-1} \cdot \ldots \cdot (a^m)^{-1}}_{(-n)\text{-mal}} \overset{(2)}{=} \underbrace{a^{-m} \cdot \ldots \cdot a^{-m}}_{(-n)\text{-mal}} \overset{\text{(a)}}{=} a^{\overbrace{-m-\cdots-m}^{(-n)\text{-mal}}} = a^{mn}.$$

Damit haben wir die Behauptung in allen Fällen gezeigt. □

Aufgabe 1.13. Es sei $G = \{e,a,b\}$ eine Gruppe der Ordnung 3, wobei e wie üblich das neutrale Element bezeichnet. Bestimme alle möglichen Verknüpfungstafeln für G.

Aufgabe 1.14. Man zeige:

(a) Ist G eine Gruppe mit $(ab)^2 = a^2b^2$ für alle $a,b \in G$, so ist G abelsch.

(b) Ist G eine Gruppe mit $a^2 = e$ für alle $a \in G$, so ist G abelsch.

Aufgabe 1.15. Zeige, dass jede nicht-abelsche Gruppe mindestens 5 Elemente haben muss.

Aufgabe 1.16. Es sei G eine Gruppe der Ordnung $|G| = 10$. Zeige, dass es ein $a \in G\backslash\{e\}$ gibt mit $a^{-1} = a$.

Aufgabe 1.17. Es sei G eine Menge mit einer Verknüpfung, von der wir lediglich wissen, dass sie die Assoziativität (G1) und die Existenz eines linksneutralen Elements (G2) erfüllt, aber nicht notwendig die Existenz eines linksinversen Elements (G3). Man zeige:

(a) Ist G endlich, und gilt die rechtsseitige Kürzungsregel

$$ax = bx \Leftrightarrow a = b$$

für alle $a,b,x \in G$, so ist G bereits eine Gruppe.

(b) Ist G endlich, und gilt die linksseitige Kürzungsregel

$$xa = xb \Leftrightarrow a = b$$

für alle $a,b,x \in G$, so muss G nicht notwendig eine Gruppe sein.

(c) Ist G unendlich, so muss G selbst dann keine Gruppe sein, wenn beide Kürzungsregeln gelten.

Aufgabe 1.18. Es sei G eine Gruppe mit endlich vielen Elementen. Man zeige:

(a) Für alle $a \in G$ gibt es ein $n \in \mathbb{N}_{>0}$ mit $a^n = e$.

(b) Zu je zwei Elementen $a,b \in G$ gibt es ein $n \in \mathbb{N}_{>0}$ mit $a^n = b^n$.

Aufgabe 1.19. Es sei $G = \{a_1, \dots, a_n\}$ eine abelsche Gruppe der Ordnung n. Zeige, dass dann $(a_1 \cdot \dots \cdot a_n)^2 = e$ gilt.

2. Symmetrische Gruppen

Im letzten Kapitel haben wir Gruppen eingeführt und ihre elementaren Eigenschaften untersucht. Wir wollen nun eine neue wichtige Klasse von Beispielen von Gruppen — und insbesondere auch unsere ersten nicht-abelschen Gruppen — kennenlernen. Es handelt sich hierbei um die Gruppen aller bijektiven Abbildungen auf gegebenen Mengen.

Konstruktion 2.1 (Symmetrische Gruppen)**.** Zu einer gegebenen Menge M sei

$$S(M) := \{f\colon M \to M \text{ bijektiv}\}$$

die Menge aller bijektiven Abbildungen von M nach M. Wir behaupten, dass $S(M)$ mit der üblichen Verkettung von Abbildungen (die wir mit dem Symbol „$\circ$“ schreiben) eine Gruppe ist. Beachte dazu zunächst, dass die Verkettung zweier bijektiver Abbildungen wieder bijektiv ist und die Verkettung zweier Elemente aus $S(M)$ (also zweier bijektiver Abbildungen von M nach M) damit auch wirklich wieder in $S(M)$ (also wieder bijektiv) ist. Weiterhin gilt:

(G1) Wie wir aus den Grundlagen der Mathematik wissen, ist die Verkettung beliebiger (also insbesondere auch bijektiver) Abbildungen assoziativ [G, Lemma 2.19].

(G2) Die *Identität* $\mathrm{id}_M\colon M \to M$ ist bijektiv und somit ein Element von $S(M)$. Sie ist natürlich ein neutrales Element bezüglich der Verkettung, denn $\mathrm{id}_M \circ f = f$ für alle $f \in S(M)$ (also für alle bijektiven Abbildungen $f\colon M \to M$).

(G3) Zu jeder bijektiven Abbildung $f \in S(M)$ ist die Umkehrabbildung f^{-1} ein inverses Element bezüglich der Verkettung, denn es ist $f^{-1} \circ f = \mathrm{id}_M$. Sie ist bekanntlich auch bijektiv, also ein Element von $S(M)$.

Also ist $(S(M), \circ)$ eine Gruppe. Man nennt sie die **symmetrische Gruppe** auf M. Sie ist im Allgemeinen *nicht* kommutativ: Ist z. B. $M = \mathbb{R}$, so sind

$$f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto x+1 \quad \text{und} \quad g\colon \mathbb{R} \to \mathbb{R},\ x \mapsto 2x$$

zwei bijektive Abbildungen (mit Umkehrabbildungen $f^{-1}(x) = x-1$ und $g^{-1}(x) = \frac{x}{2}$), also gilt $f, g \in S(\mathbb{R})$. Aber die Abbildungen $f \circ g$ und $g \circ f$ sind nicht gleich, denn für alle $x \in \mathbb{R}$ ist

$$(f \circ g)(x) = f(g(x)) = f(2x) = 2x+1,$$

aber

$$(g \circ f)(x) = g(f(x)) = g(x+1) = 2(x+1) = 2x+2.$$

Aufgabe 2.2. Stellt euch vor, ihr seid Übungsleiter für die Algebraischen Strukturen und bekommt von einem Studenten die folgende Abgabe. Was sagt ihr dazu? Stimmt der Beweis so? Stimmt der Satz überhaupt?

> *Satz:* Es sei M eine Menge und $G = \{f\colon M \to M \text{ injektiv}\}$ die Menge aller injektiven Abbildungen von M nach M. Dann ist G zusammen mit der üblichen Verkettung von Abbildungen eine Gruppe.
>
> *Beweis:* Wir prüfen die Gruppenaxiome nach:
>
> (G1) Die Verknüpfung ist assoziativ, weil die Verkettung beliebiger (und damit auch injektiver) Abbildungen immer assoziativ ist.
>
> (G2) Die Identität id_M ist ein (links-)neutrales Element bezüglich der Verkettung von Abbildungen. Sie ist außerdem injektiv, liegt also in G.
>
> (G3) Ist $f\colon M \to M$ injektiv, so existiert eine Abbildung $g\colon M \to M$ mit $g \circ f = \mathrm{id}_M$, also ein linksinverses Element zu f.

Also ist $(G,\circ)$ eine Gruppe.

Aufgabe 2.3. Es sei M eine Menge. Zeige, dass die symmetrische Gruppe $S(M)$ genau dann abelsch ist, wenn M höchstens zwei Elemente besitzt.

Notation 2.4 (Endliche symmetrische Gruppen)**.** Der mit Abstand wichtigste Fall von symmetrischen Gruppen $S(M)$ ist der, wenn M eine *endliche* Menge, also z. B. die Menge $\{1,\dots,n\}$ der natürlichen Zahlen von 1 bis n ist. In diesem Fall setzen wir

$$S_n := S(\{1,\dots,n\}) = \big\{\sigma\colon \{1,\dots,n\} \to \{1,\dots,n\} \text{ bijektiv}\big\},$$

nennen diese Gruppe die **symmetrische Gruppe** der Stufe n und bezeichnen ihre Elemente in der Regel mit kleinen griechischen Buchstaben. Die Elemente von S_n kann man offensichtlich am einfachsten durch eine „Wertetabelle“ angeben: Ist $\sigma \in S_n$, also $\sigma\colon \{1,\dots,n\} \to \{1,\dots,n\}$ eine bijektive Abbildung, so vereinbaren wir dafür die Schreibweise

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Da in der unteren Reihe dieser Matrix eine **Permutation**, d. h. eine Anordnung der Zahlen $1,\dots,n$ steht, kann man S_n auch als die *Gruppe der Permutationen* von n Elementen auffassen. Für Permutationen schreibt man die Gruppenverknüpfung, also die Verkettung $\sigma \circ \tau$, auch oft ohne Verknüpfungssymbol als $\sigma\tau$.

Beispiel 2.5. Wir betrachten die symmetrische Gruppe S_3.

(a) Das neutrale Element in S_3, also die identische Abbildung auf $\{1,2,3\}$, ist $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$. Das Element $\sigma \in S_3$ mit $\sigma(1) = 2$, $\sigma(2) = 3$ und $\sigma(3) = 1$ ist $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$.

(b) Um die Verknüpfung zweier Elemente zu berechnen, z. B. $\sigma\tau$ für

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right) \quad \text{und} \quad \tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right),$$

müssen wir nur verfolgen, welche Zahlen unter dieser Verkettung auf welche anderen abgebildet werden. So wird z. B. die 1 durch τ auf 3 abgebildet, und diese 3 dann durch σ auf 2. Also ist $\sigma\tau(1) = \sigma(3) = 2$ (beachte, dass in einer Verkettung stets die rechts notierte Funktion zuerst ausgeführt wird). Genauso erhalten wir $\sigma\tau(2) = \sigma(1) = 1$ und $\sigma\tau(3) = \sigma(2) = 3$, und damit

$$\sigma\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right).$$

(c) Es ist leicht, alle Elemente von S_3 konkret anzugeben: Listen wir der Reihe nach zuerst alle Permutationen σ auf mit $\sigma(1) = 1$, dann die mit $\sigma(1) = 2$ und schließlich die mit $\sigma(1) = 3$, so erhalten wir für jeden dieser Fälle zwei Möglichkeiten und damit insgesamt

$$S_3 = \left\{\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)\right\}.$$

Die Gruppe S_3 hat also die Ordnung 6.

In der Tat können wir dieses Abzählargument verallgemeinern und damit die Ordnung der symmetrischen Gruppe S_n für alle n bestimmen:

Satz 2.6. *Für alle $n \in \mathbb{N}_{>0}$ gilt $|S_n| = n!$, wobei $n!$ (gesprochen: n-**Fakultät**) als $n! := 1 \cdot 2 \cdot \cdots \cdot n$ definiert ist.*

Wir werden diesen Satz mit dem Beweisprinzip der **(vollständigen) Induktion** zeigen, das ihr inzwischen schon aus den Grundlagen der Mathematik kennen solltet. Dieses Prinzip besagt folgendes: Ist $A(n)$ eine Aussage, die von einer natürlichen Zahl n abhängt, und wollen wir zeigen, dass diese Aussage für alle $n \geq n_0$ gilt (wobei $n_0 \in \mathbb{N}$ ein vorgegebener Startwert ist), so reicht es, die folgenden beiden Aussagen zu zeigen:

- Die Aussage $A(n_0)$ ist wahr („*Induktionsanfang*“);

- für alle $n > n_0$ gilt: Wenn die Aussage $A(m)$ für alle $m < n$ gilt, dann gilt auch die Aussage $A(n)$ („*Induktionsschritt*“).

Die Idee ist also, dass wir nur die erste Aussage $A(n_0)$ wirklich direkt zeigen. Beim Beweis jeder weiteren Aussage $A(n)$ für $n > n_0$ können wir dann voraussetzen, dass wir alle „vorhergehenden“ Aussagen $A(m)$ für $m < n$ schon gezeigt haben (wobei man in der Praxis oft nur die Aussage $A(n-1)$ für den direkt vorhergehenden Wert benötigt). Mit anderen Worten zeigen wir zuerst $A(n_0)$ direkt, beim Beweis von $A(n_0+1)$ können wir dann $A(n_0)$ bereits als bekannt voraussetzen, beim Beweis von $A(n_0+2)$ können wir $A(n_0)$ und $A(n_0+1)$ bereits voraussetzen, und so weiter. Man bezeichnet dabei die Voraussetzung, dass $A(m)$ für $m < n$ schon bekannt ist, als *Induktionsannahme* oder *Induktionsvoraussetzung*. Beachtet dabei bitte insbesondere, dass das Wort „Voraussetzung“ auch nach der neuen deutschen Rechtschreibung nur mit einem „r“ geschrieben wird.

Dass das Beweisprinzip der Induktion funktioniert, liegt offensichtlich daran, dass man alle natürlichen Zahlen irgendwann erreicht, wenn man auf diese Art beliebig oft „eins weiter zählt“.

Aber kehren wir nun zurück zum Beweis des obigen Satzes:

Beweis von Satz 2.6. Wir werden mit Induktion über $n \in \mathbb{N}_{>0}$ die folgende Aussage zeigen: Sind $M = \{x_1, \dots, x_n\}$ und $N = \{y_1, \dots, y_n\}$ zwei n-elementige Mengen, so gibt es genau $n!$ Bijektionen $f\colon M \to N$. (Offensichtlich folgt aus dieser Aussage sofort der Satz, indem man $M = N = \{1, \dots, n\}$ setzt.)

Induktionsanfang: Es ist klar, dass es genau eine Bijektion $f\colon \{x_1\} \to \{y_1\}$ gibt. Da $1! = 1$ ist, ist die Behauptung im Fall $n = 1$ also richtig.

Induktionsschritt: Wir können annehmen, dass wir bereits wissen, dass es zwischen zwei beliebigen $(n-1)$-elementigen Mengen genau $(n-1)!$ Bijektionen gibt (Induktionsannahme). Um zu untersuchen, wie viele Bijektionen $f\colon M \to N$ es zwischen zwei n-elementigen Mengen $M = \{x_1, \dots, x_n\}$ und $N = \{y_1, \dots, y_n\}$ gibt, unterscheiden wir nun n Fälle, je nachdem auf welches Element x_1 abgebildet wird:

1. Fall: $f(x_1) = y_1$. Dann muss f die Menge $\{x_2, \dots, x_n\}$ bijektiv auf $\{y_2, \dots, y_n\}$ abbilden, und jede solche Bijektion liefert auch eine Bijektion $f\colon M \to N$. Nach Induktionsannahme gibt es also genau $(n-1)!$ Bijektionen $f\colon M \to N$ mit $f(x_1) = y_1$.

2. Fall: $f(x_1) = y_2$. Dann bildet f die Menge $\{x_2, \dots, x_n\}$ bijektiv auf $\{y_1, y_3, y_4, \dots, y_n\}$ ab. Wie im 1. Fall erhalten wir nach Induktionsannahme also noch einmal $(n-1)!$ Bijektionen.

Die anderen Fälle $f(x_1) = y_3, \dots, f(x_1) = y_n$ sind offensichtlich analog, liefern also ebenfalls jeweils $(n-1)!$ Bijektionen. Insgesamt erhalten wir also $n \cdot (n-1)! = n!$ Bijektionen, was zu zeigen war. □

Aufgabe 2.7. Es seien $n \in \mathbb{N}_{>0}$, $\sigma \in S_n$ und $i \in \{1, \dots, n\}$. Ferner sei $k \in \mathbb{N}_{>0}$ die kleinste Zahl, so dass

$$\sigma^k(i) \in \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{k-1}(i)\}.$$

Beweise, dass dann $\sigma^k(i) = i$ gilt.

02

Neben der Schreibweise für Permutationen als Wertetabelle wie in Notation 2.4 ist noch eine weitere Schreibweise nützlich und auch oft platzsparender. Hierfür benötigen wir den Begriff eines Zykels.

Notation 2.8 (Zykel)**.** Es sei $n \in \mathbb{N}_{>0}$.

(a) Für $k \in \mathbb{N}_{>0}$ seien $a_1, \dots, a_k$ verschiedene Zahlen zwischen 1 und n. Die Permutation $\sigma \in S_n$ mit

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ \dots,\ \sigma(a_{k-1}) = a_k,\ \sigma(a_k) = a_1$$
$$\text{und} \quad \sigma(a) = a \text{ für alle } a \notin \{a_1, \dots, a_k\},$$

also die die Zahlen $a_1, \dots, a_k$ zyklisch vertauscht und alle anderen Zahlen fest lässt, wird mit $(a_1\ a_2\ \cdots\ a_k)$ bezeichnet. Eine solche Permutation heißt ein k-**Zykel**. Als Spezialfall davon werden 2-Zykel $(a_1\ a_2)$ — also Permutationen, die genau zwei Zahlen a_1 und a_2 miteinander vertauschen und alle anderen fest lassen — **Transpositionen** genannt.

(b) Zwei Zykel $(a_1 \ \cdots \ a_k)$ und $(b_1 \ \cdots \ b_l)$ in S_n heißen **disjunkt**, wenn keine Zahl zwischen 1 und n in beiden Zykeln vorkommt.

Bemerkung 2.9.

(a) Offensichtlich gilt $(a_1 \ a_2 \ \cdots \ a_k) = (a_2 \ \cdots \ a_k \ a_1)$: Beide Zykel beschreiben die Permutation, die a_i auf a_{i+1} für $i < k$, und a_k auf a_1 abbilden. Man sagt: Die Einträge eines Zykels können *zyklisch vertauscht* werden, ohne die Permutation zu ändern. So ist z. B. in S_4

$$(1\ 2\ 4) = (2\ 4\ 1) = (4\ 1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Eine beliebige Vertauschung der Einträge eines Zykels liefert in der Regel jedoch eine andere Permutation: Im Vergleich zu obigem Zykel ist z. B.

$$(2\ 1\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \neq (1\ 2\ 4).$$

(b) Sind die Zykel $\sigma = (a_1 \ \cdots \ a_k)$ und $\tau = (b_1 \ \cdots \ b_l)$ disjunkt, so gilt $\sigma\tau = \tau\sigma$: Beide Verkettungen bilden a_i auf a_{i+1} für $i < k$, a_k auf a_1, b_i auf b_{i+1} für $i < l$, und b_l auf b_1 ab. Man sagt: Disjunkte Zykel vertauschen miteinander. Für Zykel, die nicht disjunkt sind, gilt dies natürlich nicht: So ist z. B. in S_3

$$(1\ 2)(1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \text{aber} \quad (1\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

(beachte, dass wie bei Abbildungen üblich zuerst die rechte und dann die linke Permutation angewendet wird — so bildet z. B. die Verkettung $(1\ 2)(1\ 3)$ die Zahl 3 auf 2 ab, denn die 3 wird zuerst durch die rechte Transposition auf 1 abgebildet, und diese 1 dann durch die linke Transposition auf 2). Also ist $(1\ 2)(1\ 3) \neq (1\ 3)(1\ 2)$ in S_3.

(c) Als Spezialfall ist in Notation 2.8 (a) auch $k = 1$, also ein 1-Zykel zugelassen. Die zugehörige Permutation ist dann aber natürlich gerade die Identität.

(d) Es gilt

$$(a_k \ \cdots \ a_2 \ a_1)(a_1 \ a_2 \ \cdots \ a_k) = \mathrm{id},$$

da diese Verkettung von Zykeln offensichtlich jedes a_i für $i = 1, \ldots, k$ auf sich selbst abbildet (und alle anderen Zahlen in $\{1, \ldots, n\}$ ohnehin durch beide Permutationen unverändert bleiben). Also ist der „umgekehrte" Zykel $(a_k \ \cdots \ a_2 \ a_1)$ genau das Inverse von $(a_1 \ a_2 \ \cdots \ a_k)$. Insbesondere sind Transpositionen damit zu sich selbst invers, da

$$(a_1 \ a_2)^{-1} = (a_2 \ a_1) \overset{\text{(a)}}{=} (a_1 \ a_2).$$

Mit Hilfe von Zykeln können wir jetzt auch beliebige Permutationen einfacher schreiben:

Konstruktion 2.10 (Zykelzerlegung)**.** Wir wollen sehen, dass sich jede Permutation $\sigma \in S_n$ als Verkettung disjunkter Zykel schreiben lässt. Dazu betrachten wir einmal als Beispiel die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 6 & 5 & 3 & 2 \end{pmatrix} \in S_7.$$

Wir versuchen nun, in dieser Permutation einen Zykel zu finden. Dazu starten wir mit einer beliebigen Zahl in $\{1, \ldots, n\}$, z. B. mit 1, und verfolgen sie bei fortlaufender Anwendung von σ:

$$1 \overset{\sigma}{\longmapsto} 4 \overset{\sigma}{\longmapsto} 6 \overset{\sigma}{\longmapsto} 3 \overset{\sigma}{\longmapsto} 1.$$

Da es nur endlich viele Zahlen von 1 bis n gibt, ist klar, dass wir hierbei irgendwann einmal wieder auf eine Zahl stoßen mussten, die wir vorher in der Reihe schon einmal hatten. Nach Aufgabe 2.7 muss dies sogar wieder die Ausgangszahl sein, im Beispiel oben also die 1. Die Abbildung σ lässt sich auf den Zahlen, die in dieser Kette vorkommen, also durch einen Zykel beschreiben — in unserem Fall durch den 4-Zykel $(1\ 4\ 6\ 3)$.

Um die Abbildung σ auch auf den anderen Zahlen korrekt zu beschreiben, müssen wir jetzt auf die gleiche Art noch Zykel konstruieren, die diese anderen Zahlen enthalten. Starten wir z. B. als Nächstes mit 2, so erhalten wir den Zykel

$$2 \overset{\sigma}{\longmapsto} 7 \overset{\sigma}{\longmapsto} 2,$$

also die Transposition $(2\ 7)$ (beachte, dass wir hierbei auch wirklich keine Zahl erhalten können, die schon im vorher betrachteten Zykel enthalten war, weil σ injektiv ist). Die einzige Zahl, die wir nun bisher noch nicht betrachtet haben, ist die 5 — die aber von σ auf sich selbst abgebildet wird und somit den 1-Zykel (5) bildet. Insgesamt können wir σ daher als die Verkettung

$$\sigma = (1\ 4\ 6\ 3)(2\ 7)(5)$$

schreiben. Da der letzte 1-Zykel (5) natürlich nach Bemerkung 2.9 (c) die Identität ist, können wir diesen nun noch weglassen und erhalten

$$\sigma = (1\ 4\ 6\ 3)(2\ 7).$$

Es ist klar, dass man mit diesem Verfahren jede Permutation als Vereinigung disjunkter Zykel schreiben kann (genau genommen müsste man dies jetzt formal beweisen, aber ein solcher formaler Beweis würde hier nur verwirren und keine neuen Erkenntnisse bringen — daher möchte ich euch und mir das ersparen). Man nennt dies eine **Zykelzerlegung** von σ.

Anhand der Konstruktion sieht man auch, dass die Zykelzerlegung einer Permutation eindeutig ist bis auf

(a) zyklisches Vertauschen der Einträge in den Zykeln (siehe Bemerkung 2.9 (a)): Wir hätten im Beispiel oben z. B. auch $\sigma = (6\ 3\ 1\ 4)(7\ 2)$ schreiben können;

(b) Vertauschen der Zykel (siehe Bemerkung 2.9 (b)): Wir hätten die Permutation oben auch als $\sigma = (2\ 7)(1\ 4\ 6\ 3)$ schreiben können;

(c) Hinzufügen bzw. Weglassen von 1-Zykeln (siehe Bemerkung 2.9 (c)): Dies haben wir oben im Beispiel schon gesehen.

(Natürlich müsste man eigentlich auch diese Eindeutigkeitsaussage formal beweisen; auch dies wollen wir aus den oben genannten Gründen hier jedoch nicht tun.)

Unter den Zykeln sind vor allem die Transpositionen besonders wichtig, da wir jetzt sehen wollen, dass man aus ihnen durch geeignete Verkettungen jedes Element der symmetrischen Gruppe S_n bilden kann. Anschaulich ist dies einfach die Aussage, dass sich jede Permutation der Zahlen $1,\dots,n$ dadurch erhalten lässt, dass man mehrfach nacheinander zwei geeignete Zahlen miteinander vertauscht.

Lemma 2.11 (Verkettungen von Transpositionen)**.** *Es sei $n \in \mathbb{N}_{>0}$.*

(a) *Jeder k-Zykel in S_n ist eine Verkettung von $k-1$ Transpositionen.*

(b) *Jede Permutation in S_n ist eine Verkettung von Transpositionen.*

Beweis.

(a) Offensichtlich gilt

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{k-1}\ a_k),$$

da die Permutationen auf beiden Seiten jedes a_i für $i < k$ auf a_{i+1} und a_k auf a_1 abbilden (sowie alle anderen Zahlen in $\{1,\dots,n\}$ unverändert lassen).

(b) Dies folgt sofort aus (a), da jede Permutation nach Konstruktion 2.10 eine Verkettung von Zykeln ist. □

Die Darstellung einer Permutation als Verkettung von Transpositionen ist natürlich keinesfalls eindeutig. So gilt z. B. in S_4

$$\mathrm{id}_{S_4} = (1\ 2)(1\ 2) = (1\ 3)(3\ 4)(1\ 3)(1\ 4) = (1\ 4)(1\ 3)(2\ 4)(3\ 4)(1\ 2)(2\ 3),$$

wie man leicht durch explizite Berechnung jeder dieser Verkettungen überprüfen kann. Überraschenderweise haben aber alle solchen Darstellungen einer gegebenen Permutation σ trotz der vielen Wahlmöglichkeiten eines gemeinsam: Wie wir jetzt zeigen werden, ist die Anzahl der Transpositionen abhängig von σ entweder immer eine gerade Zahl (so wie im Fall der Identität oben, für die wir Darstellungen mit 2, 4 und 6 Transpositionen angegeben haben) oder immer eine ungerade Zahl. Bei der Untersuchung der symmetrischen Gruppe ist es ein sehr wichtiges Unterscheidungsmerkmal für die Permutationen, ob diese Anzahl gerade oder ungerade ist.

Lemma 2.12. *Es sei $n \in \mathbb{N}_{>0}$.*

(a) *Für alle $\sigma \in S_n$ bezeichne $c_\sigma \in \mathbb{N}_{>0}$ die Anzahl der Zykel (inklusive aller 1-Zykel) in der Zykelzerlegung von σ wie in Konstruktion 2.10. Dann gilt*

$$c_{\tau\sigma} = c_\sigma \pm 1$$

für jede Transposition τ.

(b) *Sind*

$$\sigma = \tau_1 \cdots \tau_r \quad \text{und} \quad \sigma = \tilde{\tau}_1 \cdots \tilde{\tau}_s$$

zwei Darstellungen derselben Permutation $\sigma \in S_n$ als Verkettung von Transpositionen $\tau_1, \dots, \tau_r$ bzw. $\tilde{\tau}_1, \dots, \tilde{\tau}_s$, so sind r und s entweder beide gerade oder beide ungerade.

Beweis.

(a) Es sei $\sigma = \sigma_1 \cdots \sigma_m$ die Zerlegung von σ in disjunkte Zykel $\sigma_1, \dots, \sigma_m$ wie in Konstruktion 2.10, so dass also $m = c_\sigma$ gilt. Ferner sei $\tau = (a_1\ b_1)$ mit verschiedenen $a_1, b_1 \in \{1, \dots, n\}$.

Da sowohl a_1 als auch b_1 in genau einem Zykel der Zerlegung vorkommen, können zwei Fälle auftreten:

- Die Zahlen a_1 und b_1 liegen im gleichen Zykel. Nach Konstruktion 2.10 (a) und (b) können wir die Zykel in der Zerlegung dann so anordnen, dass a_1 und b_1 im ersten Zykel σ_1 vorkommen, und a_1 die erste Zahl dieses Zykels ist. Es ist also

$$\sigma = \underbrace{(a_1\ \cdots\ a_k\ b_1\ \cdots\ b_l)}_{=\sigma_1}\, \sigma_2 \cdots \sigma_m$$

für gewisse $a_2, \dots, a_k, b_2, \dots, b_l$. Wie man analog zu Lemma 2.11 (a) sofort nachrechnet, ist dann

$$\begin{aligned} \tau\sigma &= (a_1\ b_1)(a_1\ \cdots\ a_k\ b_1\ \cdots\ b_l)\, \sigma_2 \cdots \sigma_m \\ &= (a_1\ \cdots\ a_k)(b_1\ \cdots\ b_l)\, \sigma_2 \cdots \sigma_m. \end{aligned}$$

Da dies nun die Zykelzerlegung von $\tau\sigma$ ist, und sie aus $m+1$ Zykeln besteht, ist also $c_{\tau\sigma} = c_\sigma + 1$.

- Die Zahlen a_1 und b_1 liegen in verschiedenen Zykeln. Dann können wir die Zykelzerlegung so umschreiben, dass a_1 die erste Zahl im Zykel σ_1 und b_1 die erste Zahl im Zykel σ_2 ist, und wir erhalten durch Nachrechnen diesmal die Zykelzerlegung

$$\begin{aligned} \tau\sigma &= (a_1\ b_1)\, \underbrace{(a_1\ \cdots\ a_k)}_{=\sigma_1}\, \underbrace{(b_1\ \cdots\ b_l)}_{=\sigma_2}\, \sigma_3 \cdots \sigma_m \\ &= (a_1\ \cdots\ a_k\ b_1\ \cdots\ b_l)\, \sigma_3 \cdots \sigma_m \end{aligned}$$

von $\tau\sigma$ mit $m-1$ Zykeln. Damit ergibt sich in diesem Fall $c_{\tau\sigma} = c_\sigma - 1$.

(b) Nach Voraussetzung gilt

$$\begin{aligned}\mathrm{id} &= \sigma^{-1}\sigma \\ &= (\tau_1 \cdots \tau_r)^{-1}\, \tilde{\tau}_1 \cdots \tilde{\tau}_s \\ &= \tau_r^{-1} \cdots \tau_1^{-1}\, \tilde{\tau}_1 \cdots \tilde{\tau}_s \qquad \text{(Lemma 1.10 (b))} \\ &= \tau_r \cdots \tau_1\, \tilde{\tau}_1 \cdots \tilde{\tau}_s\, \mathrm{id}. \qquad \text{(Bemerkung 2.9 (d))}\end{aligned}$$

Die Anzahl der Zykel in der Zykelzerlegung einer Permutation wechselt aber nach (a) bei jeder Verkettung von links mit einer Transposition von gerade auf ungerade und umgekehrt. Da wir ausgehend von der Identität nach einer Verkettung mit $r+s$ Transpositionen wieder die Identität erhalten, muss diese Anzahl $r+s$ von Transpositionen also gerade sein. Damit sind r und s entweder beide gerade oder beide ungerade. □

Definition 2.13 (Signum von Permutationen)**.** Es sei $n \in \mathbb{N}_{>0}$ und $\sigma \in S_n$. Nach Lemma 2.11 (b) können wir σ als Verkettung $\sigma = \tau_1 \cdots \tau_r$ einer gewissen Anzahl r von Transpositionen schreiben. Das **Signum** oder **Vorzeichen** von σ ist dann definiert als

$$\operatorname{sign}\sigma := (-1)^r = \begin{cases} 1 & \text{falls } r \text{ gerade,} \\ -1 & \text{falls } r \text{ ungerade.} \end{cases}$$

Beachte, dass dies nach Lemma 2.12 (b) auch wirklich nur von der gegebenen Permutation σ und nicht von der gewählten Darstellung als Verkettung von Transpositionen $\sigma_1, \ldots, \sigma_r$ abhängt.

Eine unmittelbare, aber sehr wichtige Folgerung aus dieser Definition ist, dass das Vorzeichen *multiplikativ* ist, d. h. dass das Vorzeichen einer Verkettung $\sigma\tau$ von Permutationen gleich dem Produkt der Vorzeichen von σ und τ ist.

Satz 2.14 (Multiplikativität des Signums)**.** *Für alle $n \in \mathbb{N}_{>0}$ und $\sigma, \tau \in S_n$ gilt*

$$\operatorname{sign}(\sigma\tau) = \operatorname{sign}\sigma \cdot \operatorname{sign}\tau.$$

Beweis. Es seien $\sigma = \sigma_1 \cdots \sigma_r$ und $\tau = \tau_1 \cdots \tau_s$ für gewisse Transpositionen $\sigma_1, \ldots, \sigma_r, \tau_1, \ldots, \tau_s$. Dann ist $\sigma\tau = \sigma_1 \cdots \sigma_r \tau_1 \cdots \tau_s$ ein Produkt von $r+s$ Transpositionen, und damit folgt sofort

$$\operatorname{sign}(\sigma\tau) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \operatorname{sign}\sigma \cdot \operatorname{sign}\tau.$$ □

Beispiel 2.15.

(a) Transpositionen haben offensichtlich das Signum -1. Allgemeiner besagt Lemma 2.11 (a), dass ein k-Zykel Signum $(-1)^{k-1}$ hat, also dass sein Signum genau dann -1 ist, wenn k gerade ist.

(b) Wegen der Multiplikativität des Signums aus Satz 2.14 können wir das Signum einer beliebigen Permutation mit Hilfe von (a) leicht aus ihrer Zykelzerlegung berechnen. So gilt z. B. für die Beispielpermutation $\sigma = (1\ 4\ 6\ 3)(2\ 7) \in S_7$ aus Konstruktion 2.10

$$\operatorname{sign}\sigma \overset{2.14}{=} \operatorname{sign}(1\ 4\ 6\ 3) \cdot \operatorname{sign}(2\ 7) \overset{\text{(a)}}{=} (-1) \cdot (-1) = 1.$$

Allgemein hat eine Permutation σ demzufolge genau dann Signum -1, wenn die Anzahl der Zykel *gerader* Länge in ihrer Zykelzerlegung *ungerade* ist.

Aufgabe 2.16. Wir betrachten die Permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix} \in S_6$.

(a) Berechne σ^2 und σ^{-1}.

(b) Bestimme die Zykelzerlegung von σ.

(c) Man schreibe σ als Verkettung von Transpositionen. Was ist das Vorzeichen von σ?

Aufgabe 2.17. Beim im Bild (A) unten dargestellten „Schiebepuzzle“ sind mit den Zahlen 1 bis 15 beschriftete Würfel zufällig so in einem 4×4-Quadrat angeordnet, dass das Feld rechts unten frei bleibt.

Man kann nun nacheinander Würfel von links, rechts, oben oder unten in den jeweils freien Platz schieben und so z. B. von (A) aus die Position (B) erreichen, indem man den Würfel 2 nach unten schiebt. Ziel des Spiels ist es, durch solche Züge letztlich die vollständig geordnete Position (C) zu erreichen.

14	10	15	1
6	7	8	9
5	4	3	2
13	12	11	

(A)

14	10	15	1
6	7	8	9
5	4	3	
13	12	11	2

(B)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(C)

Wir wollen die möglichen Positionen des Puzzles im Folgenden als Permutationen in S_{16} auffassen, indem wir die Zahlen von links oben nach rechts unten lesen und den freien Platz dabei mit 16 bezeichnen. Die Zielposition (C) ist also z. B. gerade die Identität in S_{16}.

(a) Berechne das Signum der Ausgangsposition (A).

(b) Zeige, dass jeder mögliche Spielzug das Signum der Spielposition ändert.

(c) Beweise, dass es nicht möglich ist, von Position (A) aus das Ziel (C) zu erreichen.

3. Untergruppen

Nachdem wir nun einige grundlegende Gruppen kennengelernt haben, wollen wir in diesem Kapitel eine einfache Möglichkeit untersuchen, mit der man aus bereits bekannten Gruppen viele weitere gewinnen kann: Beginnend mit einer Gruppe G wollen wir versuchen, durch einfaches Einschränken der gegebenen Verknüpfung auf eine Teilmenge $U \subset G$ neue Gruppen zu erzeugen. Gruppen, die auf diese Art als Teilmengen von anderen entstehen, werden als Untergruppen bezeichnet.

Definition 3.1 (Untergruppen)**.** Es sei $(G, \cdot)$ eine Gruppe und U eine Teilmenge von G. Man nennt U eine **Untergruppe** von G, wenn „U mit der gegebenen Verknüpfung selbst wieder eine Gruppe ist“, d. h. wenn gilt:

(a) Für alle $a, b \in U$ ist $a \cdot b \in U$, d. h. die Verknüpfung $\cdot : G \times G \to G$ lässt sich auf eine Verknüpfung $\cdot : U \times U \to U$ einschränken (man sagt auch, U ist **abgeschlossen** bezüglich der Gruppenverknüpfung).

(b) $(U, \cdot)$ ist eine Gruppe.

Ist U eine Untergruppe von G, so schreibt man dies oft als $(U, \cdot) \leq (G, \cdot)$ oder auch kurz als $U \leq G$.

Beispiel 3.2.

(a) Nach Beispiel 1.2 (a) ist $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

(b) Es sei G eine beliebige Gruppe. Dann sind offensichtlich sowohl $\{e\}$ als auch G selbst Untergruppen von G. Aus naheliegenden Gründen werden sie die **trivialen Untergruppen** von G genannt.

Bevor wir zu interessanteren Beispielen von Untergruppen kommen, wollen wir zunächst ein Kriterium beweisen, mit dem man in der Praxis einfach überprüfen kann, ob eine gegebene Teilmenge einer Gruppe eine Untergruppe ist oder nicht.

Satz 3.3 (**Untergruppenkriterium**)**.** *Es sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $U \subset G$ ist genau dann eine Untergruppe von G, wenn die folgenden drei Bedingungen erfüllt sind:*

(U1) *Für alle $a, b \in U$ gilt $a \cdot b \in U$;*

(U2) *das neutrale Element e von G liegt in U;*

(U3) *zu jedem $a \in U$ liegt auch das inverse Element a^{-1} in U.*

03

Beweis. Wir müssen zwei Richtungen zeigen:

„⇒“: Es sei $U \leq G$. Wir müssen zeigen, dass die Eigenschaften (U1), (U2) und (U3) gelten.

(U1) Dies gilt natürlich nach Definition 3.1 (a).

(U2) Nach Voraussetzung ist $(U, \cdot)$ eine Gruppe, hat also insbesondere ein neutrales Element $\tilde{e}$, d. h. ein $\tilde{e} \in U$ mit $\tilde{e} \cdot a = a$ für alle $a \in U$. Beachte aber, dass wir noch nicht wissen, dass dieses neutrale Element $\tilde{e}$ von U wirklich gleich dem neutralen Element e von G sein muss — denn die Gleichung $\tilde{e} \cdot a = a$ gilt ja zunächst einmal nur für alle $a \in U$, und nicht für alle $a \in G$. Allerdings zeigt dies die folgende einfache Rechnung: Es ist

$$\begin{aligned} \tilde{e} \cdot \tilde{e} &= \tilde{e} && (\tilde{e} \text{ ist neutral in } U) \\ &= e \cdot \tilde{e}, && (e \text{ ist neutral in } G) \end{aligned}$$

und damit folgt nach der Kürzungsregel aus Lemma 1.10 (c), dass $e = \tilde{e} \in U$.

(U3) Es sei $a \in U$ beliebig. Da U eine Gruppe ist, gibt es in U ein inverses Element $a' \in U$ mit $a' \cdot a = \tilde{e}$, wobei $\tilde{e}$ wie in (U2) das neutrale Element von U bezeichnet. Dieses ist nach (U2) ist aber gleich e, d. h. es ist $a' \cdot a = e$. Also ist a' auch das inverse Element zu a in G. Damit folgt $a^{-1} = a' \in U$.

„$\Leftarrow$“: Nun setzen wir die Eigenschaften (U1), (U2) und (U3) voraus und müssen $U \leq G$ zeigen, d. h. die Bedingungen aus Definition 3.1 nachprüfen.

(a) ist genau die Eigenschaft (U1).

(b) Wir müssen die Gruppenaxiome aus Definition 1.1 (a) für U nachprüfen. Diese sind aber offensichtlich: Die Assoziativität (G1) gilt für alle Elemente von G und damit erst recht für alle Elemente von U, und die Existenz von neutralen und inversen Elementen (G2) bzw. (G3) ergibt sich sofort aus (U2) bzw. (U3). □

Bemerkung 3.4. Satz 3.3 bzw. sein Beweis besagt also insbesondere, dass die neutralen und inversen Elemente einer Untergruppe $U \leq G$ stets dieselben wie von G sind — obwohl wir dies in Definition 3.1 nicht vorausgesetzt haben.

Beispiel 3.5.

(a) In der symmetrischen Gruppe S_n (für ein $n \in \mathbb{N}_{>0}$) ist die Teilmenge

$$U = \{\sigma \in S_n : \sigma(1) = 1\}.$$

nach Satz 3.3 eine Untergruppe, da sie die Untergruppenkriterien erfüllt:

(U1) Sind $\sigma, \tau \in U$, also $\sigma(1) = \tau(1) = 1$, so ist auch $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(1) = 1$ und damit $\sigma \circ \tau \in U$.

(U2) Natürlich ist $\mathrm{id}(1) = 1$.

(U3) Ist $\sigma \in U$, also $\sigma(1) = 1$, so gilt auch für die Umkehrabbildung $\sigma^{-1}(1) = 1$ und damit $\sigma^{-1} \in U$.

(b) Es sei G eine beliebige Gruppe und $a \in G$. Dann ist die Menge

$$U = \{a^k : k \in \mathbb{Z}\} \subset G$$

aller (positiven und negativen) Potenzen von a eine Untergruppe von G, wie man wieder leicht durch Nachprüfen der Untergruppenkriterien sieht:

(U1) Sind a^k und a^l (für $k, l \in \mathbb{Z}$) zwei Elemente aus U, so ist ihre Verknüpfung $a^k \cdot a^l = a^{k+l}$ (siehe Lemma 1.12 (a)) wieder eine Potenz von a, also ein Element von U.

(U2) Es ist $e = a^0 \in U$.

(U3) Mit $a^k \in U$ ist auch das Inverse $(a^k)^{-1} = a^{-k}$ dieses Elements (siehe Lemma 1.12 (b)) eine Potenz von a, also ein Element von U.

Als konkretes Beispiel ist also für $n \in \mathbb{Z}$ z. B.

$$n\mathbb{Z} := \{k \cdot n : k \in \mathbb{Z}\},$$

d. h. die Menge aller ganzzahligen Vielfachen von n, eine Untergruppe von $(\mathbb{Z}, +)$ (da wir diese Gruppe additiv schreiben, bezeichnen wir die „Potenzen“ von n natürlich als $k \cdot n$ — siehe Definition 1.11). Beachte auch, dass die Elemente a^k nicht alle verschieden sein müssen: Für die Transposition $(1\ 2) \in S_3$ ist $(1\ 2)^k$ gleich id für gerade und $(1\ 2)$ für ungerade k, und damit ist auch

$$\{\mathrm{id}, (1\ 2)\} = \{(1\ 2)^k : k \in \mathbb{Z}\}$$

eine Untergruppe von S_3.

(c) Die Teilmenge $\{0, 2, 4\}$ ist keine Untergruppe von $(\mathbb{Z}, +)$, da sie die Elemente 2 und 4, aber nicht $2 + 4 = 6$ enthält, und damit das Untergruppenkriterium (U1) nicht erfüllt ist.

Aufgabe 3.6. Überprüfe, ob die folgenden Teilmengen U Untergruppen der gegebenen Gruppe G sind:

(a) $G = (\mathbb{Z},+)\times(\mathbb{Q}\backslash\{0\},\cdot)$, $U = \{(a,b)\in G : b = 2^a\}$;

(b) $G = S_4$, $U = \{\sigma \in S_4 : \sigma^2 = \mathrm{id}\}$;

(c) $G = S(\mathbb{R})$, $U = \{f\colon \mathbb{R}\to\mathbb{R}$ bijektiv mit $f(x) = x$ für alle $x \geq 0\}$;

(d) $G = (\mathbb{R},+)\times(\mathbb{R},+)$, $U = \{(x,y) : y = ax^2+bx+c\}$ für gegebene $a,b,c\in\mathbb{R}$;

(e) G eine beliebige Gruppe, $U = \{a\in G : a\cdot b = b\cdot a$ für alle $b\in G\}$.

Aufgabe 3.7. Es sei U eine Untergruppe einer Gruppe G. Untersuche, welche der folgenden Teilmengen von G in jedem Fall wieder Untergruppen von G sind:

(a) $V = \{aua^{-1} : u\in U\}$ für ein festes $a\in G$;

(b) $V = \{a\in G : aua^{-1}\in U$ für alle $u\in U\}$.

Aufgabe 3.8. Es sei G eine Gruppe und $U\subset G$ eine nicht-leere Teilmenge. Man beweise die folgenden vereinfachten Untergruppenkriterien:

(a) U ist eine Untergruppe von G genau dann, wenn $ab^{-1}\in U$ für alle $a,b\in U$ gilt.

(b) Hat U nur endlich viele Elemente, so ist U eine Untergruppe von G genau dann, wenn $ab\in U$ für alle $a,b\in U$ gilt, also wenn das Untergruppenkriterium (U1) aus Satz 3.3 gilt.

Bemerkung 3.9 (Vereinigungen und Durchschnitte von Untergruppen)**.**

(a) Sind U und V Untergruppen von G, so ist die Vereinigung $U\cup V$ in der Regel *keine* Untergruppe von G: Betrachten wir z. B. wie in Beispiel 3.5 (b) die Untergruppen $U = 2\mathbb{Z}$ und $V = 3\mathbb{Z}$ von $(\mathbb{Z},+)$, so liegen in der Vereinigung $2\mathbb{Z}\cup 3\mathbb{Z}$ zwar die Zahlen 2 und 3, nicht aber deren Summe $2+3=5$ — das Untergruppenkriterium (U1) aus Satz 3.3 ist also verletzt.

(b) Im Gegensatz zu (a) sind Durchschnitte von Untergruppen jedoch stets wieder Untergruppen — und zwar nicht nur Durchschnitte von *zwei* Untergruppen, sondern sogar von *beliebig vielen* (also evtl. sogar von unendlich vielen). Die korrekte mathematische Notation hierfür lautet wie folgt: Es sei I eine beliebige Menge (die sogenannte *Indexmenge*) und $U_i \leq G$ für alle $i\in I$. Wir haben also für jedes Element i von I eine Untergruppe U_i von G — hätten wir z. B. nur zwei Untergruppen, die wir miteinander schneiden wollen, so könnten wir als Indexmenge $I = \{1,2\}$ wählen und hätten demzufolge die Untergruppen $U_1, U_2 \leq G$. Wir behaupten nun, dass der Durchschnitt aller dieser Untergruppen U_i, geschrieben als

$$U = \bigcap_{i\in I} U_i := \{a\in G : a\in U_i \text{ für alle } i\in I\},$$

wieder eine Untergruppe von G ist. In der Tat prüft man die Untergruppenkriterien aus Satz 3.3 schnell nach:

(U1) Es seien $a,b\in U$, also $a,b\in U_i$ für alle $i\in I$. Da jedes U_i eine Untergruppe von G ist, gilt dann (nach dem Untergruppenkriterium angewendet auf die U_i) auch $ab\in U_i$ für alle $i\in I$. Also ist $ab\in U$.

(U2) Das neutrale Element e liegt in jedem U_i und damit auch im Durchschnitt U dieser Untergruppen.

(U3) ist ganz analog zu (U1): Ist $a\in U$, also $a\in U_i$ für alle $i\in I$, so ist auch $a^{-1}\in U_i$ für alle $i\in I$ (da jedes U_i eine Untergruppe von G ist) und somit $a^{-1}\in U$.

Die Untergruppenkriterien aus Satz 3.3 übertragen sich also direkt von den U_i auf ihren Durchschnitt U.

Aufgabe 3.10. Es seien U und V Untergruppen einer gegebenen Gruppe G. Zeige, dass man das Resultat aus Bemerkung 3.9 (a) wie folgt präzisieren kann: Die Vereinigung $U\cup V$ ist genau dann eine Untergruppe von G, wenn $U\subset V$ oder $V\subset U$ gilt (also wenn sozusagen „gar keine echte Vereinigung vorliegt“ und $U\cup V$ bereits eine der Untergruppen U oder V ist).

Mit Hilfe des Durchschnitts von Untergruppen können wir nun eine sehr wichtige und allgemeine Konstruktion durchführen, die es uns erlaubt, aus *jeder* Teilmenge M einer Gruppe G eine Untergruppe zu erzeugen. Wollen wir z. B. aus der Teilmenge $M = \{0,2,4\}$ der Gruppe $G = (\mathbb{Z},+)$ aus Beispiel 3.5 eine Untergruppe machen, so müssen wir zu ihr zunächst die Zahlen $2+2+2=6$, $2+2+2+2=8$ usw. hinzufügen, damit das Untergruppenkriterium (U1) erfüllt ist, und dann für (U3) auch die Inversen $-2,-4,-6,\ldots$ der Elemente $2,4,6,\ldots$. Wir erhalten so die Menge $2\mathbb{Z}$ aller geraden Zahlen, die wir in Beispiel 3.5 (b) schon als Untergruppe von G erkannt haben. Wir können sie uns also anschaulich als die kleinste Untergruppe von G vorstellen, die M enthält.

Diese Konstruktion der kleinsten Untergruppe, die eine gegebene Teilmenge enthält, wird formal wie folgt durchgeführt.

Definition 3.11 (Erzeugte Untergruppen)**.** Es sei M eine beliebige Teilmenge einer Gruppe G. Wir setzen

$$\langle M \rangle := \bigcap_{\substack{U \leq G \\ \text{mit } U \supset M}} U,$$

d. h. $\langle M \rangle$ ist der Durchschnitt aller Untergruppen von G, die M enthalten. Nach Bemerkung 3.9 (b) ist $\langle M \rangle$ als Durchschnitt von (in der Regel unendlich vielen) Untergruppen wieder eine Untergruppe von G. Man nennt sie die von M **erzeugte Untergruppe**. Ist $M = \{a_1,\ldots,a_n\}$ eine endliche Menge, so schreibt man statt $\langle M \rangle = \langle \{a_1,\ldots,a_n\} \rangle$ meistens abgekürzt $\langle a_1,\ldots,a_n \rangle$.

Diese Definition sieht auf den ersten Blick sicher sehr technisch und abschreckend aus. Ihre Grundidee ist aber sehr einfach: Wenn wir die *kleinste* Untergruppe von G haben wollen, die M enthält, dann schneiden wir einfach *alle* diese Untergruppen miteinander — wenn das dann wieder eine Untergruppe ist (was wir ja in Bemerkung 3.9 (b) gezeigt haben), dann muss das ja offensichtlich die kleinste sein. Allerdings habt ihr natürlich Recht, wenn ihr vermutet, dass man die von M erzeugte Untergruppe $\langle M \rangle$ ganz sicher nicht dadurch ausrechnen will, dass man wirklich konkret alle Untergruppen U mit $U \supset M$ bestimmt und dann deren Durchschnitt berechnet. Stattdessen ist für die konkrete Bestimmung von $\langle M \rangle$ das folgende Lemma viel handlicher.

Lemma 3.12. *Es sei M eine Teilmenge einer Gruppe G. Dann ist eine Teilmenge $V \subset G$ genau dann die von M erzeugte Untergruppe $\langle M \rangle$, wenn gilt:*

(1) *V ist eine Untergruppe von G, die M enthält; und*

(2) *ist U eine beliebige Untergruppe von G, die M enthält, so ist bereits $V \subset U$.*

Anschaulich ist $\langle M \rangle$ also „die kleinste Untergruppe von G, die M enthält“.

Beweis.

„⇒“: Es sei $V = \langle M \rangle$ wie in Definition 3.11. Wir müssen also die Eigenschaften (1) und (2) für $\langle M \rangle$ zeigen.

(1) Nach Bemerkung 3.9 (b) ist $\langle M \rangle \leq G$. Außerdem schneiden wir in Definition 3.11 nur Mengen miteinander, die M enthalten. Ihr Durchschnitt $\langle M \rangle$ enthält damit natürlich ebenfalls M.

(2) Ist $U \leq G$ mit $U \supset M$, so ist U natürlich eine der Untergruppen, über die wir in Definition 3.11 den Durchschnitt bilden. Dieser Durchschnitt kann daher höchstens kleiner als U sein, d. h. es ist $\langle M \rangle \subset U$.

„⇐“: Wir setzen jetzt voraus, dass V die Bedingungen (1) und (2) des Lemmas erfüllt. Außerdem wissen wir nach dem obigen Teil „⇒“, dass auch $\langle M \rangle$ diese Eigenschaften hat, d. h. dass gilt:

(3) $\langle M \rangle$ ist eine Untergruppe von G, die M enthält; und

(4) ist U eine beliebige Untergruppe von G, die M enthält, so ist bereits $\langle M \rangle \subset U$.

Wir kombinieren nun (1) mit (4): Nach (1) ist V eine Untergruppe, die M enthält. Also können wir (4) auf den Fall $U = V$ anwenden und erhalten $\langle M \rangle \subset V$. Analog können wir (3) mit (2) kombinieren, also (2) auf den Fall $U = \langle M \rangle$ anwenden und erhalten $V \subset \langle M \rangle$. Insgesamt gilt damit also wie behauptet $V = \langle M \rangle$. □

Beispiel 3.13.

(a) Es sei G eine Gruppe und $a \in G$. Wir behaupten, dass dann

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

genau die Untergruppe ist, die wir bereits in Beispiel 3.5 (b) gesehen haben. In der Tat ist dies mit dem Kriterium aus Lemma 3.12 sehr schnell überprüft:

(1) Nach Beispiel 3.5 (b) ist $\{a^k : k \in \mathbb{Z}\}$ eine Untergruppe von G, und natürlich enthält sie das Element a.

(2) Ist U eine beliebige Untergruppe von G, die a enthält, so muss sie wegen des Untergruppenkriteriums aus Satz 3.3 auch alle Verknüpfungen von a und a^{-1}, also alle Potenzen a^k mit $k \in \mathbb{Z}$ enthalten.

Konkret ist z. B. nach Beispiel 3.5 (b)

$$\langle n \rangle = n\mathbb{Z} \text{ in } \mathbb{Z} \text{ für alle } n \in \mathbb{Z}, \text{ und}$$
$$\langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\} \text{ in } S_3.$$

(b) Mit der gleichen Begründung wie in (a) ist die in $(\mathbb{R}, +)$ von zwei Zahlen $a, b \in \mathbb{R}$ erzeugte Untergruppe gleich

$$\langle a, b \rangle = \{ka + lb : k, l \in \mathbb{Z}\}.$$

(c) In Lemma 2.11 (b) haben wir gesehen, dass jede Permutation eine Verkettung von Transpositionen ist. Nach dem Untergruppenkriterium aus Satz 3.3 bedeutet dies, dass jede Untergruppe von S_n, die alle Transpositionen enthält, bereits die gesamte symmetrische Gruppe S_n ist. Ist $M \subset S_n$ die Menge aller Transpositionen, so gilt also $\langle M \rangle = S_n$.

In manchen Fällen ist für die von einer Menge M erzeugte Untergruppe $\langle M \rangle$ auch die folgende explizite „Formel“ nützlich:

Aufgabe 3.14. Es sei M eine Teilmenge einer Gruppe G. Zeige, dass dann

$$\langle M \rangle = \{a_1 \cdot \cdots \cdot a_n : n \in \mathbb{N},\ a_i \in M \text{ oder } a_i^{-1} \in M \text{ für alle } i = 1, \ldots, n\}$$

gilt, d. h. dass $\langle M \rangle$ aus allen Verknüpfungen besteht, die man aus den Elementen von M und ihren Inversen bilden kann.

Aufgabe 3.15. Es sei $n \in \mathbb{N}$ mit $n \geq 3$. Zeige, dass

$$\langle (1\ 3), (1\ 2\ 3) \rangle = \{\sigma \in S_n : \sigma(i) = i \text{ für alle } i \geq 4\}$$

in S_n gilt.

Aufgabe 3.16 (Diedergruppen)**.** Für eine gegebene Zahl $n \in \mathbb{N}_{\geq 3}$ betrachten wir die Permutationen

$$\sigma = (1\ 2\ 3\ \cdots\ n) \quad \text{und} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ n & n-1 & n-2 & \cdots & 1 \end{pmatrix}$$

in S_n. Man zeige:

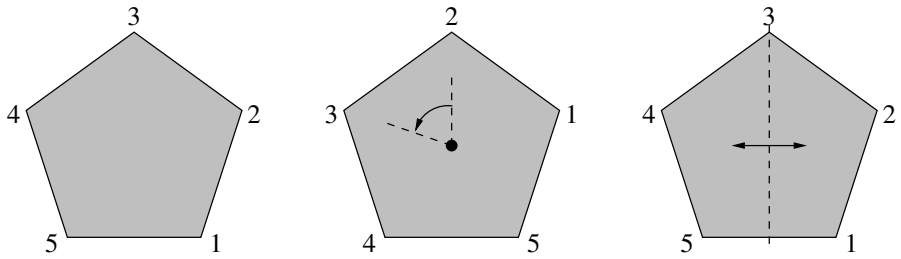
(a) $\sigma^n = \tau^2 = \mathrm{id}$ und $\tau\sigma = \sigma^{-1}\tau$.

(b) Es ist

$$\langle \sigma, \tau \rangle = \{\sigma^k \tau^l : k = 0, \ldots, n-1 \text{ und } l = 0, 1\} \quad \leq S_n,$$

und diese Untergruppe von S_n hat genau $2n$ Elemente. Wir bezeichnen sie im Folgenden mit D_n.

Die Gruppe D_n hat eine einfache geometrische Interpretation: Betrachten wir (wie im Bild unten links für $n = 5$ dargestellt) ein regelmäßiges n-Eck in der Ebene, dessen Eckpunkte der Reihe nach mit den Zahlen $1, \dots, n$ bezeichnet sind, so entspricht die Permutation σ genau einer Drehung um den Winkel $\frac{2\pi}{n}$, die Permutation τ einer Spiegelung.



σ: Drehung τ: Spiegelung

Lassen wir in $D_n = \langle \sigma, \tau \rangle$ nun alle möglichen Verknüpfungen dieser beiden Transformationen zu, so erhalten wir insgesamt *alle* möglichen Drehungen und Spiegelungen der Ebene, die das n-Eck auf sich selbst abbilden. Wir können uns D_n also als die *Gruppe aller Symmetrieoperationen bzw. Kongruenzabbildungen eines regelmäßigen n-Ecks* vorstellen.

Man nennt diese Gruppe D_n die **Diedergruppe** (gesprochen: Di-eder) der Ordnung $2n$. Der Name kommt aus dem Griechischen: Ein Dieder ist wörtlich genommen ein „Körper mit zwei Seiten“ — ihr kennt analog dazu wahrscheinlich alle ein Tetraeder als eine Figur im Raum, die von vier Seiten begrenzt wird (also eine „Pyramide mit dreieckiger Grundfläche“). Man kann sich nun ein n-Eck wie oben als „degenerierten“ Körper mit Volumen 0 im Raum vorstellen, der von zwei Seiten (der Vorderseite und Rückseite) begrenzt wird. Die Symmetriegruppen dieser „Körper“ werden daher Diedergruppen genannt.

Im Allgemeinen ist es sehr schwierig, zu einer gegebenen Gruppe alle Untergruppen konkret anzugeben oder auch nur die Anzahl der möglichen Untergruppen zu bestimmen. Im speziellen (und auch wichtigen) Fall der Gruppe $\mathbb{Z}$ hingegen wollen wir nun zeigen, dass es außer den Untergruppen $n\mathbb{Z}$, die wir in Beispiel 3.5 (b) gefunden haben, keine weiteren mehr gibt:

Satz 3.17 (Untergruppen von $\mathbb{Z}$)**.** *Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Mengen $\langle n \rangle = n\mathbb{Z}$ mit $n \in \mathbb{N}$ aus Beispiel 3.5 (b) bzw. 3.13 (a).*

Beweis. Wir wissen aus Beispiel 3.5 (b) bereits, dass $n\mathbb{Z} \leq \mathbb{Z}$ gilt. Wir müssen also nur noch zeigen, dass es zu einer beliebigen Untergruppe $U \leq \mathbb{Z}$ ein $n \in \mathbb{N}$ gibt mit $U = n\mathbb{Z}$.

Nach dem Untergruppenkriterium (U2) muss U die Zahl 0 enthalten. Ist $U = \{0\}$, so ist natürlich $U = 0\mathbb{Z}$ und wir sind fertig. Andernfalls gibt es ein Element $a \in U$ mit $a \neq 0$. Da nach (U3) mit a auch $-a$ in U liegen muss, gibt es dann also sogar eine positive Zahl in U. Es sei nun n die *kleinste* positive Zahl in U. Wir behaupten, dass dann $U = n\mathbb{Z}$ gilt und zeigen diese Gleichheit, indem wir die beiden Inklusionen „$\supset$“ und „$\subset$“ separat beweisen.

„$\supset$“: Natürlich ist U eine Untergruppe von $\mathbb{Z}$, die das Element n enthält. Nach Lemma 3.12 (2) muss U dann auch die von n erzeugte Untergruppe $\langle n \rangle = n\mathbb{Z}$ enthalten. Es gilt also $U \supset n\mathbb{Z}$.

„$\subset$“: Es sei $a \in U$ beliebig. Indem wir die ganze Zahl a mit Rest durch n dividieren, können wir a schreiben als

$$a = qn + r,$$

wobei $q \in \mathbb{Z}$ gilt und $r \in \{0, \dots, n-1\}$ der Rest der Division ist. Wir schreiben dies um als

$$r = a - qn.$$

Nun ist $a \in U$ nach Wahl von a, und außerdem auch $-qn \in n\mathbb{Z} \subset U$ nach dem Teil „$\supset$“, den wir bereits gezeigt haben. Wegen der Abgeschlossenheit (U1) von U liegt damit auch die Summe $r = a - qn$ dieser beiden Zahlen in U. Aber r war als Rest der obigen Division

kleiner als n, und n war schon als die kleinste positive Zahl in U gewählt! Dies ist natürlich nur dann möglich, wenn r gar nicht positiv ist, also $r = 0$ gilt. Setzen wir dies nun aber oben ein, so sehen wir, dass dann $a = qn + 0 \in n\mathbb{Z}$ folgt. Dies zeigt auch die Inklusion $U \subset n\mathbb{Z}$. $\square$

4. Morphismen

Wir haben nun viele Beispiele und Konstruktionen von Gruppen gesehen. Natürlich wollen wir diese vielen verschiedenen Gruppen jetzt auch irgendwie miteinander in Beziehung setzen. In der Sprache der Mathematik bedeutet dies einfach, dass wir *Abbildungen* zwischen Gruppen betrachten müssen.

Dabei helfen uns allerdings *beliebige* Abbildungen zwischen Gruppen nicht weiter — weil sie, wenn sie nur die zugrunde liegenden Mengen aufeinander abbilden und mit den Gruppenverknüpfungen nichts weiter zu tun haben, die Gruppen eben *nicht* wirklich miteinander in Beziehung setzen. Wir benötigen also Abbildungen, die mit den Gruppenoperationen in gewissem Sinne „verträglich" sind. Dies sind die sogenannten Morphismen, die wir jetzt einführen werden.

Definition 4.1 (Morphismen von Gruppen)**.** Es seien $(G,*)$ und $(H,\circ)$ zwei Gruppen. Eine Abbildung $f\colon G \to H$ heißt ein **Morphismus** (oder **Homomorphismus** oder noch ausführlicher **Gruppenhomomorphismus**), wenn für alle $a,b \in G$

$$f(a*b) = f(a) \circ f(b)$$

gilt (man sagt auch, f ist „mit den Gruppenverknüpfungen verträglich" bzw. „vertauscht mit den Gruppenverknüpfungen").

Bemerkung 4.2. Oft werden wir die beiden Gruppenverknüpfungen zur Vereinfachung der Schreibweise nicht mit unterschiedlichen Symbolen bezeichnen und die Bedingung aus Definition 4.1 einfach als $f(a \cdot b) = f(a) \cdot f(b)$ schreiben. Dies kann normalerweise nicht zu Verwechslungen führen, da ja schon aufgrund der jeweiligen Elemente klar ist, welche Verknüpfung gemeint sein muss: a und b sind Elemente von G, $f(a)$ und $f(b)$ dagegen Elemente von H.

Beispiel 4.3.

(a) Die Abbildung $f\colon (\mathbb{Z},+) \to (\mathbb{Z},+)$, $f(n) = 2n$ ist ein Morphismus, denn für alle $m,n \in \mathbb{Z}$ gilt
$$f(m+n) = 2(m+n) = 2m+2n = f(m)+f(n).$$

(b) Die Abbildung $f\colon (\mathbb{R},+) \to (\mathbb{R},+)$, $f(x) = x+1$ ist kein Morphismus, denn es ist z. B. $f(0+0) = f(0) = 1$, aber $f(0)+f(0) = 1+1 = 2$.

(c) Für jede Gruppe G und ein festes $a \in G$ ist die Abbildung $f\colon (\mathbb{Z},+) \to G$, $f(n) = a^n$ ein Morphismus, denn für alle $m,n \in \mathbb{Z}$ gilt nach den Rechenregeln für Potenzen aus Lemma 1.12 (a)
$$f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$$
(man beachte hier die unterschiedlichen Verknüpfungen in der Start- und Zielgruppe).

(d) Die Signumsabbildung $\operatorname{sign}\colon S_n \to (\mathbb{R}\backslash\{0\},\cdot)$ ist ein Morphismus, denn nach Satz 2.14 gilt $\operatorname{sign}(\sigma\tau) = \operatorname{sign}\sigma \cdot \operatorname{sign}\tau$ für alle $\sigma,\tau \in S_n$.

04

Wir haben oben schon gesagt, dass wir uns Morphismen als Abbildungen vorstellen sollten, die mit den Gruppenstrukturen verträglich sind. Nun hat eine Gruppe natürlich noch mehr „Struktur" als die Verknüpfung, nämlich ein neutrales sowie inverse Elemente. Wir würden erwarten, dass auch diese bei der Abbildung mit einem Morphismus erhalten bleiben. Dies ist in der Tat der Fall, wie wir im folgenden Lemma u. a. zeigen wollen.

Lemma 4.4 (Eigenschaften von Morphismen)**.** *Es sei $f\colon G \to H$ ein Morphismus von Gruppen. Dann gilt:*

(a) *$f(e) = e$ (beachte, dass der Buchstabe e hier auf der linken Seite das neutrale Element von G, auf der rechten Seite das von H bezeichnet).*

(b) *Für alle $a \in G$ gilt $f(a^{-1}) = f(a)^{-1}$ (beachte, dass das Inverse auf der linken Seite das in G und auf der rechten das in H ist).*

(c) *Ist f bijektiv, so ist auch die Umkehrabbildung $f^{-1}\colon H \to G$ ein Morphismus.*

(d) *Ist $g\colon H \to K$ ein weiterer Morphismus, so ist auch die Verkettung $g \circ f\colon G \to K$ ein Morphismus.*

Beweis. Zur besseren Verständlichkeit des Beweises bezeichnen wir das neutrale Element in G mit e_G und das in H mit e_H.

(a) Da f ein Morphismus ist, gilt zunächst

$$e_H \cdot f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$$

in H. Nach der Kürzungsregel aus Lemma 1.10 (c) können wir aus dieser Gleichung nun das Element $f(e_G)$ herauskürzen und erhalten wie behauptet $e_H = f(e_G)$.

(b) Für alle $a \in G$ gilt

$$\begin{aligned} f(a^{-1}) \cdot f(a) &= f(a^{-1} \cdot a) && (f \text{ ist Morphismus}) \\ &= f(e_G) \\ &= e_H && (\text{nach (a)}). \end{aligned}$$

Also ist $f(a^{-1})$ das inverse Element zu $f(a)$, d. h. es ist $f(a^{-1}) = f(a)^{-1}$.

(c) Ist f bijektiv, so wissen wir bereits, dass die Umkehrabbildung f^{-1} existiert. Es seien nun $a, b \in H$. Wir setzen $a' = f^{-1}(a)$ und $b' = f^{-1}(b)$, also $a = f(a')$ und $b = f(b')$. Dann gilt

$$\begin{aligned} f^{-1}(a \cdot b) &= f^{-1}(f(a') \cdot f(b')) \\ &= f^{-1}(f(a' \cdot b')) && (f \text{ ist Morphismus}) \\ &= a' \cdot b' && (f^{-1} \text{ ist Umkehrabbildung zu } f) \\ &= f^{-1}(a) \cdot f^{-1}(b). \end{aligned}$$

Also ist auch f^{-1} ein Morphismus.

(d) Für alle $a, b \in G$ gilt

$$\begin{aligned} (g \circ f)(a \cdot b) &= g(f(a \cdot b)) \\ &= g(f(a) \cdot f(b)) && (f \text{ ist Morphismus}) \\ &= g(f(a)) \cdot g(f(b)) && (g \text{ ist Morphismus}) \\ &= (g \circ f)(a) \cdot (g \circ f)(b), \end{aligned}$$

also ist $g \circ f$ ein Morphismus. □

Aufgabe 4.5. Welche der folgenden Abbildungen sind Morphismen?

(a) $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{R},\ f(m,n) = 2m + 3n$;

(b) $f\colon \mathbb{Q}\backslash\{0\} \to \mathbb{Q},\ f(x) = x$;

(c) $f\colon G \to G,\ f(a) = gah$ für eine beliebige Gruppe G und gegebene $g, h \in G$.

(Die Gruppen in (a) und (b) seien dabei mit den üblichen Verknüpfungen versehen.)

Aufgabe 4.6. Es seien $f, g\colon G \to H$ zwei Gruppenhomomorphismen. Man zeige:

(a) Die Menge $U = \{a \in G : f(a) = g(a)\}$ ist eine Untergruppe von G.

(b) Ist $M \subset G$ eine Teilmenge mit $\langle M \rangle = G$ und gilt $f|_M = g|_M$, so ist bereits $f = g$. Ein Morphismus ist durch seine Werte auf einer erzeugenden Menge also bereits eindeutig bestimmt.

Aufgabe 4.7. Bestimme *alle* Morphismen

(a) von $(\mathbb{Z}, +)$ nach $(\mathbb{Q}, +)$;

(b) von $(\mathbb{Q},+)$ nach $(\mathbb{Z},+)$;

(c) von S_n nach $(\mathbb{R},+)$ für $n \in \mathbb{N}_{>0}$.

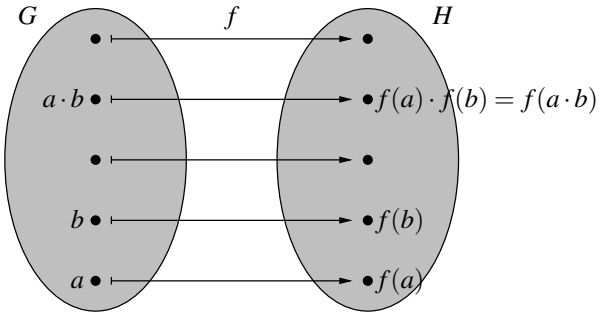
Wir wollen im Folgenden noch etwas genauer auf die bijektiven Morphismen aus Lemma 4.4 (c) eingehen. Sie haben einen besonderen Namen, und in der Tat auch eine besondere mathematische Bedeutung.

Definition 4.8 (Isomorphismen)**.** Es seien G und H zwei Gruppen.

(a) Einen bijektiven Morphismus $f\colon G \to H$ (der nach Lemma 4.4 (c) also einen Umkehrmorphismus besitzt) bezeichnet man als **Isomorphismus** (bzw. **Gruppenisomorphismus**).

(b) G und H heißen **isomorph** (in Zeichen: $G \cong H$), wenn es einen Isomorphismus $f\colon G \to H$ zwischen ihnen gibt.

Bemerkung 4.9. Sind G und H isomorph, gibt es also einen Isomorphismus $f\colon G \to H$, so bedeutet dies anschaulich, dass G und H „als Gruppen ununterscheidbar“ sind: Wir haben eine bijektive Abbildung f, mit der wir die Elemente von G mit denen von H identifizieren können, und bei Gruppenverknüpfungen, neutralen und inversen Elementen spielt es mit dieser Identifikation (nach Definition 4.1 bzw. Lemma 4.4 (a) und (b)) keine Rolle, ob wir sie in G oder H betrachten. Das folgende Bild veranschaulicht dies: Dort ist sowohl in G als auch in H z. B. die Verknüpfung der beiden unten eingezeichneten Elemente gleich dem Element, das als zweites von oben eingezeichnet ist. Wir können diese Berechnung in G durchführen und dann mit f nach H wechseln, oder erst die Elemente nach H umrechnen und sie dort verknüpfen — es kommt in jedem Fall dasselbe dabei heraus.



Wir können also sagen, dass isomorphe Gruppen „bis auf Umbenennung der Elemente gleich“ sind. In der Tat sagt man im mathematischen Sprachgebrauch auch oft, dass zwei Gruppen gleich sind, wenn sie in Wirklichkeit nur isomorph sind. Im folgenden Beispiel 4.10 (a) wird dies besonders deutlich.

Beispiel 4.10.

(a) Es seien $G = \mathbb{R}$ und

$$H = \{(x,0) : x \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R}$$

„die Menge aller Punkte auf der x-Achse in $\mathbb{R}^2$“. Wie üblich betrachten wir $\mathbb{R}$ und $\mathbb{R} \times \mathbb{R}$ dabei als Gruppen mit der Addition — wir werden im Folgenden zur Vereinfachung der Schreibweise die Verknüpfungen in derartigen „offensichtlichen Fällen“ nicht mehr jedesmal explizit hinschreiben. Man prüft mit dem Untergruppenkriterium aus Satz 3.3 sofort nach, dass H eine Untergruppe von $\mathbb{R} \times \mathbb{R}$, also selbst eine Gruppe ist.

Wir behaupten nun, dass $G \cong H$ gilt. In der Tat ist die Abbildung

$$f\colon G \to H,\ f(x) = (x,0)$$

ein Isomorphismus: Es ist offensichtlich, dass f bijektiv ist, und wegen

$$f(x+y) = (x+y,0) = (x,0)+(y,0) = f(x)+f(y) \qquad \text{für alle } x,y \in \mathbb{R}$$

ist f auch ein Morphismus.

Nach der Interpretation aus Bemerkung 4.9 sind G und H also „bis auf Umbenennung der Elemente gleich“. Das ist hier natürlich auch sofort anschaulich klar: Wir haben uns in H lediglich entschlossen, jede reelle Zahl x etwas komplizierter als $(x,0)$ zu schreiben — aber letztlich ändert das außer der Schreibweise der Elemente natürlich überhaupt nichts.

(b) Die Abbildung
$$f\colon \mathbb{Z} \to 2\mathbb{Z},\ f(n) = 2n$$
ist nach Beispiel 4.3 (a) ein Morphismus. Sie ist auch injektiv (denn aus $2n = 2m$ folgt $n = m$) und nach Definition von $2\mathbb{Z}$ surjektiv, also ein Isomorphismus. Wir sehen also, dass eine Gruppe (hier $\mathbb{Z}$) durchaus auch zu einer nicht-trivialen Untergruppe von sich selbst (hier $2\mathbb{Z}$) isomorph sein kann. Dies ist aber natürlich nur bei Gruppen mit unendlich vielen Elementen möglich, denn zwischen einer endlichen Gruppe und einer nicht-trivialen Teilmenge davon gibt es ja nicht einmal eine bijektive Abbildung — also erst recht keinen Isomorphismus.

(c) Wie ihr aus der Schule schon wisst (und auch in den Grundlagen der Mathematik noch exakt beweisen werdet) bildet die Exponentialfunktion $f(x) = \mathrm{e}^x$ die Menge $\mathbb{R}$ bijektiv auf $\mathbb{R}_{>0}$ ab und erfüllt die Gleichung $\mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y$ für alle $x, y \in \mathbb{R}$. Damit ist $f\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ ein Isomorphismus. Es können also durchaus auch Gruppen isomorph, also „praktisch ununterscheidbar“ sein, wenn ihre zugrunde liegenden Mengen und Verknüpfungen zunächst einmal recht unterschiedlich aussehen.

Bemerkung 4.11. Da isomorphe Gruppen als „praktisch gleich“ anzusehen sind, möchte man für zwei gegebene Gruppen G und H natürlich immer gerne wissen, ob sie isomorph sind oder nicht. Eine Richtung dabei ist einfach: Wenn man wie in Beispiel 4.10 einen Isomorphismus $f\colon G \to H$ konkret angeben kann, dann sind G und H natürlich isomorph. Wie aber können wir beweisen, dass zwei gegebene Gruppen *nicht* isomorph sind? Dass uns gerade kein Isomorphismus zwischen ihnen einfällt, oder dass eine konkret gegebene Abbildung kein Isomorphismus ist, ist natürlich kein Beweis — wir müssen ja zeigen, dass es *überhaupt keinen* bijektiven Morphismus zwischen G und H geben kann.

Die Strategie besteht hierbei darin, eine Eigenschaft zu suchen, die die eine Gruppe besitzt und die andere nicht (und die man in der Sprache der Gruppentheorie formulieren kann): Wenn es so etwas gibt, dann können die beiden Gruppen ja offensichtlich nicht ununterscheidbar sein.

Betrachten wir konkret einmal die beiden gegenüber Beispiel 4.10 (c) leicht abgeänderten Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}\backslash\{0\}, \cdot)$. Schauen wir uns in diesen Gruppen die Gleichung $x * x = e$ an, wobei $*$ die jeweilige Gruppenverknüpfung und e das jeweilige neutrale Element bezeichnen, so sehen wir:

- In $(\mathbb{R}, +)$ ist dies die Gleichung $x + x = 0$. Sie hat dort genau *eine* Lösung, nämlich $x = 0$.
- In $(\mathbb{R}\backslash\{0\}, \cdot)$ ist dies die Gleichung $x \cdot x = 1$. Sie hat dort *zwei* Lösungen, nämlich $x = \pm 1$.

Die beiden Gruppen verhalten sich bezüglich der Lösbarkeit der Gleichung $x * x = e$ also unterschiedlich und sind damit durchaus unterscheidbar, sollten also nach unserer Interpretation eigentlich nicht isomorph sein können.

In der Tat ist es einfach, diese Idee zu einem exakten Beweis zu machen: Angenommen, wir hätten einen Isomorphismus $f\colon (\mathbb{R}\backslash\{0\}, \cdot) \to (\mathbb{R}, +)$. Nach Lemma 4.4 (a) ist dann zunächst $f(1) = 0$. Da f ein Morphismus ist, gilt für den Wert $f(-1)$ ebenfalls
$$f(-1) + f(-1) = f((-1) \cdot (-1)) = f(1) = 0.$$
Diese Gleichung hat in $\mathbb{R}$ aber nur die Lösung $f(-1) = 0$. Damit ist also $f(1) = f(-1) = 0$, im Widerspruch zur Injektivität von f. Es kann also keinen Isomorphismus zwischen $(\mathbb{R}\backslash\{0\}, \cdot)$ und $(\mathbb{R}, +)$ geben, d. h. die beiden Gruppen sind nicht isomorph.

Ihr werdet euch jetzt vielleicht fragen, wie man darauf kommt, in diesem Fall gerade die Gleichung $x * x = e$ zu betrachten. Dafür gibt es in der Tat kein allgemein funktionierendes Rezept. So kann es also auch durchaus vorkommen, dass man von zwei Gruppen auch nach langem Nachdenken nicht entscheiden kann, ob sie isomorph sind oder nicht — einfach weil man weder einen Isomorphismus noch eine passende unterschiedliche Eigenschaft findet. Wer Lust hat, kann sich ja z. B. mal daran

versuchen zu entscheiden, ob die Gruppen $(\mathbb{R},+)$ und $(\mathbb{R},+)\times(\mathbb{R},+)$ isomorph sind oder nicht. Ich kann euch praktisch garantieren, dass ihr scheitern werdet.

Aufgabe 4.12. Sind die folgenden Gruppen isomorph?

(a) S_{n-1} und die Untergruppe $\{\sigma \in S_n : \sigma(n) = n\}$ von S_n (für ein gegebenes $n \in \mathbb{N}_{\geq 2}$);

(b) $S_2 \times S_2$ und $\langle (1\ 2\ 3\ 4) \rangle \leq S_4$;

(c) $(\mathbb{Q},+)$ und $(\mathbb{Q}_{>0},\cdot)$.

Nach unserer Untersuchung von Morphismen wollen wir diese jetzt als Nächstes mit den in Kapitel 3 betrachteten Untergruppen in Verbindung bringen. Die Situation ist hier eigentlich die bestmögliche: Wenn wir von Untergruppen das Bild oder Urbild unter einem Morphismus bilden, kommt stets wieder eine Untergruppe dabei heraus. Wie üblich bezeichnen wir hierbei für eine beliebige Abbildung $f\colon G \to H$

- für $U \subset G$ mit $f(U) := \{f(a) : a \in U\} \subset H$ das **Bild** von U unter f;
- für $U \subset H$ mit $f^{-1}(U) := \{a \in G : f(a) \in U\} \subset G$ das **Urbild** von U unter f.

Beachte, dass das Urbild trotz der Notation $f^{-1}(U)$ für *beliebige* (und nicht nur für bijektive) Abbildungen definiert ist: Es ist einfach die Menge aller Elemente von G, die durch f nach U abgebildet werden. Die Schreibweise soll also nicht bedeuten, dass auch wirklich eine Umkehrabbildung f^{-1} existiert.

Lemma 4.13. *Es sei $f\colon G \to H$ ein Morphismus von Gruppen. Dann gilt:*

(a) *Ist $U \leq G$, so ist $f(U) \leq H$.*

(b) *Ist $U \leq H$, so ist $f^{-1}(U) \leq G$.*

Beweis. Wir überprüfen die Untergruppenkriterien von Satz 3.3 für $f(U)$ bzw. $f^{-1}(U)$ — wir werden dabei sehen, dass sie sich in beiden Fällen direkt aus den entsprechenden Kriterien für U ergeben. Zur Verdeutlichung schreiben wir wieder das neutrale Element in G als e_G und das in H als e_H.

(a) Es sei $U \leq G$.

(U1) Es seien $a,b \in f(U)$, also $a = f(u)$, $b = f(v)$ für gewisse $u,v \in U$. Wegen (U1) für U ist dann $u \cdot v \in U$ und damit $a \cdot b = f(u) \cdot f(v) = f(u \cdot v) \in f(U)$.

(U2) Nach (U2) für U ist $e_G \in U$, also auch $e_H = f(e_G) \in f(U)$ nach Lemma 4.4 (a).

(U3) Es sei $a \in f(U)$, also $a = f(u)$ für ein $u \in U$. Dann ist $u^{-1} \in U$ nach (U3) für U, und somit auch $a^{-1} = (f(u))^{-1} = f(u^{-1}) \in f(U)$ nach Lemma 4.4 (b).

(b) Es sei nun $U \leq H$.

(U1) Es seien $a,b \in f^{-1}(U)$, also $f(a), f(b) \in U$. Dann ist auch $f(a \cdot b) = f(a) \cdot f(b) \in U$ nach (U1) für U, also $a \cdot b \in f^{-1}(U)$.

(U2) Nach (U2) für U und Lemma 4.4 (a) ist $f(e_G) = e_H \in U$. Also ist $e_G \in f^{-1}(U)$.

(U3) Es sei $a \in f^{-1}(U)$, also $f(a) \in U$. Dann ist auch $f(a^{-1}) = f(a)^{-1} \in U$ nach (U3) für U und Lemma 4.4 (b), also $a^{-1} \in f^{-1}(U)$. □

Besonders wichtig sind hierbei in der Praxis die Fälle, wenn wir für U die trivialen Untergruppen aus Beispiel 3.2 (b) einsetzen. Es ergeben sich dann die folgenden Untergruppen, die auch einen besonderen Namen haben.

Definition 4.14 (Bild und Kern eines Morphismus)**.** Es sei $f\colon G \to H$ ein Morphismus von Gruppen. Wir nennen

(a) $\operatorname{Im} f := f(G) = \{f(a) : a \in G\}$ das **Bild** von f;

(b) $\operatorname{Ker} f := f^{-1}(\{e\}) = \{a \in G : f(a) = e\}$ den **Kern** von f.

Nach Lemma 4.13 ist $\operatorname{Im} f \leq H$ und $\operatorname{Ker} f \leq G$. Die Bezeichnungen $\operatorname{Im} f$ und $\operatorname{Ker} f$ kommen übrigens von den englischen Worten *image* und *kernel*.

Aufgabe 4.15. Bestimme Bild und Kern derjenigen Abbildungen aus Aufgabe 4.5, die Morphismen sind.

Ein oft vorkommendes Beispiel für den Kern eines Morphismus ist der der Signumsabbildung $\operatorname{sign}\colon S_n \to \mathbb{R}\backslash\{0\}$ aus Beispiel 4.3 (d). Er ist die vermutlich wichtigste Untergruppe von S_n und hat deswegen eine besondere Bezeichnung:

Definition 4.16 (Alternierende Gruppen)**.** Für $n \in \mathbb{N}_{>0}$ heißt der Kern der Signumsabbildung $\operatorname{sign}\colon S_n \to \mathbb{R}\backslash\{0\}$

$$A_n := \{\sigma \in S_n : \operatorname{sign}\sigma = 1\} \quad \leq S_n$$

die **alternierende Gruppe** der Stufe n.

Beispiel 4.17. Für $n = 3$ ist nach Beispiel 2.5 (c) und Umschreiben in die Zykelschreibweise aus Konstruktion 2.10

$$\begin{aligned} S_3 &= \left\{ \left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right) \right\} \\ &= \{\mathrm{id}, (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 3)\}. \end{aligned}$$

Die drei Transpositionen haben dabei nach Beispiel 2.15 (a) Signum -1, die Identität und die beiden 3-Zykel Signum 1. Die zugehörige alternierende Gruppe ist also

$$A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 2\ 3) \rangle \quad \leq S_3.$$

Wir werden übrigens in Beispiel 6.19 (a) sehen, dass A_n für alle $n \geq 2$ genau halb so viele Elemente wie S_n (also $\frac{n!}{2}$) hat, d. h. dass es stets gleich viele Permutationen mit Vorzeichen 1 und -1 gibt.

Mit Hilfe des Kerns können wir auch ein einfaches Kriterium dafür angeben, ob ein Morphismus injektiv ist. Haben wir eine beliebige Abbildung $f\colon G \to H$ zwischen Mengen, so müssen wir für die Injektivität ja bekanntlich nachprüfen, ob das Urbild *jedes* Punktes in H höchstens ein Element besitzt. Ist f hingegen ein Gruppenhomomorphismus, so genügt es nachzuschauen, ob das Urbild *des neutralen Elements* einelementig ist — was in der Regel natürlich einfacher nachzuprüfen ist.

Lemma 4.18 (Kriterium für Injektivität)**.** *Ein Morphismus $f\colon G \to H$ von Gruppen ist genau dann injektiv, wenn* $\operatorname{Ker} f = \{e\}$.

Beweis. Wir haben zwei Richtungen zu zeigen:

„⇒“: Es sei f injektiv. Nach Lemma 4.4 (a) ist $f(e) = e$, also $e \in \operatorname{Ker} f$. Da nun wegen der Injektivität von f kein anderes Element von G auch noch auf e abgebildet werden kann, folgt sofort $\operatorname{Ker} f = \{e\}$.

„⇐“: Es gelte nun $\operatorname{Ker} f = \{e\}$; wir müssen zeigen, dass f injektiv ist. Es seien also $a, b \in G$ mit $f(a) = f(b)$. Dann ist $f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1} = e$, d. h. es ist $a \cdot b^{-1} \in \operatorname{Ker} f$. Nach Voraussetzung folgt also $a \cdot b^{-1} = e$ und damit $a = b$. □

Aufgabe 4.19.

(a) Es sei G eine Gruppe. Für $a \in G$ definieren wir die Abbildung

$$\sigma_a\colon G \to G,\ \sigma_a(b) = a \cdot b.$$

Zeige, dass σ_a ein Element der symmetrischen Gruppe $S(G)$ ist, und dass die Abbildung

$$f\colon G \to S(G),\ f(a) = \sigma_a$$

ein injektiver Morphismus ist.

(b) Beweise, dass jede Gruppe zu einer Untergruppe einer symmetrischen Gruppe isomorph ist.

Aufgabe 4.20 (A_n wird erzeugt von 3-Zykeln)**.** Es sei $n \in \mathbb{N}_{\geq 3}$. Man zeige:

(a) Für $n > 3$ gibt es zu jedem $\sigma \in A_n$ einen 3-Zykel α und ein $\beta \in A_n$ mit $\beta(n) = n$ und $\sigma = \alpha\beta$.

(b) Ist $M \subset S_n$ die Menge aller 3-Zykel, so gilt $\langle M \rangle = A_n$.

5. Äquivalenzrelationen

Wenn man eine große und komplizierte Menge (bzw. Gruppe) untersuchen will, so kann es sinnvoll sein, zunächst kleinere, einfachere Mengen (bzw. Gruppen) zu betrachten, die mit dieser zusammenhängen. Eine solche Möglichkeit ist natürlich, Teilmengen (bzw. Untergruppen) zu betrachten, also einfach einige Elemente wegzulassen. Es gibt aber noch eine andere Möglichkeit, bei der man keine Elemente weglassen muss: Man kann Elemente, die in gewissem Sinne „ähnlich sind“ (also für die betrachtete Anwendung gleiche Eigenschaften haben) miteinander identifizieren, also quasi gleich setzen. Formal heißt das, dass man solche „ähnlichen Elemente“ zu einer sogenannten Äquivalenzklasse zusammenfasst und statt mit den ursprünglichen Elementen dann mit diesen Klassen weiter rechnet.

Ein einfaches und sehr anschauliches Beispiel hierfür ist eine (analoge) Uhr, bei der wir der Einfachheit halber annehmen, dass wir nur ganze Stunden ablesen wollen. Eine solche Uhr kann z. B. zwischen 9 Uhr und 21 Uhr nicht unterscheiden, sie betrachtet also diese Zeiten — oder allgemeiner alle Zeiten, die sich nur um ein Vielfaches von 12 unterscheiden — als äquivalent, bzw. fasst sie zu einer Äquivalenzklasse zusammen.

Um diese Idee in ein mathematisch exaktes Konzept umzuwandeln, benötigen wir den Begriff der Äquivalenzrelation.

Definition 5.1 (Äquivalenzrelationen)**.** Es sei M eine Menge.

(a) Eine **Relation** auf M ist eine Teilmenge R des Produkts $M \times M$. Für $(a,b) \in M \times M$ schreibt man statt $(a,b) \in R$ in der Regel $a \sim_R b$ (oder einfach $a \sim b$, wenn klar ist, um welche Relation es geht) und sagt, „a steht in Relation zu b“. Man kann eine Relation also einfach dadurch angeben, dass man festlegt, für welche $a, b \in M$ gelten soll, dass $a \sim b$ ist.

(b) Eine Relation R heißt **Äquivalenzrelation**, wenn die folgenden Eigenschaften gelten:

(A1) Für alle $a \in M$ gilt $a \sim a$ (**Reflexivität**).

(A2) Sind $a, b \in M$ mit $a \sim b$, so gilt auch $b \sim a$ (**Symmetrie**).

(A3) Sind $a, b, c \in M$ mit $a \sim b$ und $b \sim c$, so gilt auch $a \sim c$ (**Transitivität**).

(c) Ist R eine Äquivalenzrelation, so sagt man statt $a \sim b$ auch, dass a (bezüglich dieser Relation) zu b **äquivalent** ist. Zu $a \in M$ heißt dann die Menge

$$\overline{a} := \{b \in M : b \sim a\}$$

aller Elemente, die zu a äquivalent sind, die **Äquivalenzklasse** von a; jedes Element dieser Menge nennt man einen **Repräsentanten** dieser Klasse. Die Menge aller Äquivalenzklassen bezeichnen wir mit

$$M/\sim \; := \; \{\overline{a} : a \in M\}.$$

Beachte, dass sich die Notation $\overline{a}$ einer Äquivalenzklasse immer auf eine gegebene Äquivalenzrelation bezieht, die aus dieser Schreibweise nicht ersichtlich ist und aus dem Zusammenhang klar sein muss.

Beispiel 5.2.

(a) Die einfachste Äquivalenzrelation ist die *Gleichheitsrelation* auf einer beliebigen Menge M, für die genau dann $a \sim b$ gilt, wenn $a = b$ ist. Die Bedingungen aus Definition 5.1 (b) sind hierfür offensichtlich erfüllt. Für alle $a \in M$ ist in diesem Fall $\overline{a} = \{a\}$: Jedes Element a ist nur zu sich selbst äquivalent; es werden keinerlei verschiedene Elemente miteinander identifiziert.

(b) Um das Uhrenbeispiel aus der Einleitung zu diesem Kapitel in unserer neuen Sprache zu formulieren, definieren wir auf $M = \mathbb{Z}$ die Relation

$$a \sim b \quad :\Leftrightarrow \quad b - a = 12k \text{ für ein } k \in \mathbb{Z} \quad \Leftrightarrow \quad b - a \in 12\mathbb{Z},$$

d. h. es gilt genau dann $a \sim b$, wenn eine Uhr a und b Stunden nicht unterscheiden kann. Man sieht sofort, dass dies eine Äquivalenzrelation ist, also die Eigenschaften aus Definition 5.1 (b) erfüllt:

(A1) Für alle $a \in \mathbb{Z}$ ist $a - a = 0 \in 12\mathbb{Z}$ und damit $a \sim a$.

(A2) Sind $a, b \in \mathbb{Z}$ mit $a \sim b$, also $b - a = 12k$ für ein $k \in \mathbb{Z}$, so folgt $a - b = 12 \cdot (-k) \in 12\mathbb{Z}$ und damit auch $b \sim a$.

(A3) Sind $a, b, c \in \mathbb{Z}$ mit $a \sim b$ und $b \sim c$, also $b - a = 12k$ und $c - b = 12l$ für gewisse $k, l \in \mathbb{Z}$, so ist auch $c - a = 12(k + l) \in 12\mathbb{Z}$ und damit $a \sim c$.

Bezüglich dieser Relation ist z. B.

$$\overline{9} = \{b \in \mathbb{Z} : b - 9 \in 12\mathbb{Z}\} = \{\ldots, -15, -3, 9, 21, \ldots\}$$

die Menge aller Zeiten, die von der Uhr als zu 9 Uhr äquivalent angesehen werden. Die Menge aller Äquivalenzklassen ist

$$\mathbb{Z}/\sim \; = \{\overline{0}, \overline{1}, \ldots, \overline{11}\}$$

und entspricht den möglichen Ständen der Uhr.

Wir sehen in diesem Beispiel, dass jede ganze Zahl in *genau einer* Äquivalenzklasse enthalten ist — nämlich in der, die dem zugehörigen Stand der Uhr entspricht. Die Vereinigung aller Äquivalenzklassen ist also die gesamte Menge $\mathbb{Z}$, und zwei verschiedene Äquivalenzklassen sind immer disjunkt, d. h. haben einen leeren Durchschnitt. Man sagt auch, dass die Äquivalenzklassen eine *Partition* der Menge $\mathbb{Z}$ bilden.

Wir wollen jetzt sehen, dass dies bei jeder Äquivalenzrelation so ist.

05

Lemma 5.3. *Für jede Äquivalenzrelation auf einer Menge M gilt:*

(a) *Für $a, b \in M$ gilt $a \sim b$ genau dann, wenn $\overline{a} = \overline{b}$.*

(b) *Jedes Element $a \in M$ liegt in genau einer Äquivalenzklasse. Insbesondere ist M also die disjunkte Vereinigung aller Äquivalenzklassen.*

Beweis.

(a) Es seien $a, b \in M$.

„⇒“: Es sei $a \sim b$ und damit nach (A2) auch $b \sim a$; wir müssen die Gleichheit $\overline{a} = \overline{b}$ zeigen. Wir tun dies, indem wir beweisen, dass die linke Menge in der rechten enthalten ist und umgekehrt.

„⊂“: Sei $c \in \overline{a}$, also $c \sim a$. Wegen $a \sim b$ ist nach (A3) dann auch $c \sim b$, also $c \in \overline{b}$. Damit gilt $\overline{a} \subset \overline{b}$.

„⊃“: Die umgekehrte Inklusion zeigt man analog durch Vertauschen der Rollen von a und b.

„⇐“: Es sei nun $\overline{a} = \overline{b}$. Nach (A1) ist $a \in \overline{a}$, also auch $a \in \overline{b}$. Damit folgt sofort $a \sim b$ nach Definition 5.1 (c).

(b) Wegen der Reflexivität liegt natürlich jedes $a \in M$ in seiner eigenen Äquivalenzklasse $\overline{a}$. Ist nun auch $a \in \overline{b}$ für ein $b \in M$, also $a \sim b$ nach Definition 5.1 (c), so gilt nach (a) bereits $\overline{a} = \overline{b}$. Also liegt a in genau einer Äquivalenzklasse von $\sim$, nämlich in $\overline{a}$. □

Aufgabe 5.4. Zwei Permutationen $\sigma, \tau \in S_n$ heißen *konjugiert* zueinander, in Zeichen $\sigma \sim \tau$, wenn es ein $\alpha \in S_n$ gibt mit $\sigma = \alpha\tau\alpha^{-1}$. Man beweise:

(a) Die Relation $\sim$ ist eine Äquivalenzrelation auf S_n.

(b) Alle Transpositionen in S_n sind zueinander konjugiert.

(c) Die konstante Abbildung 1 und das Signum sind die einzigen Gruppenhomomorphismen von S_n nach $\mathbb{R}\backslash\{0\}$.

Aufgabe 5.5. Es seien U und V zwei Untergruppen einer endlichen Gruppe G. Man zeige:

(a) Durch
$$(u,v) \sim (u',v') \quad :\Leftrightarrow \quad uv = u'v'$$
wird eine Äquivalenzrelation auf $U \times V$ definiert.

(b) Die Äquivalenzklasse von $(u,v) \in U \times V$ ist $\overline{(u,v)} = \{(ua, a^{-1}v) : a \in U \cap V\}$ und besitzt genau $|U \cap V|$ Elemente.

(c) Es gilt die **Produktformel** für Untergruppen
$$|UV| = \frac{|U| \cdot |V|}{|U \cap V|},$$
wobei $UV = \{uv : u \in U, v \in V\}$.

Auch wenn Äquivalenzrelationen verschiedenster Arten an vielen Stellen in der Mathematik auftreten, werden wir in dieser Vorlesung im Wesentlichen nur eine ganz spezielle benötigen. Diese Äquivalenzrelation, die man immer definieren kann, wenn man eine Gruppe und eine darin liegende Untergruppe hat, wollen wir jetzt einführen.

Lemma und Definition 5.6 (Linksnebenklassen)**.** *Es sei G eine Gruppe und $U \leq G$.*

(a) *Die Relation*
$$a \sim b \quad :\Leftrightarrow \quad a^{-1}b \in U$$
(für $a,b \in G$) ist eine Äquivalenzrelation auf G.

(b) *Für die Äquivalenzklasse $\overline{a}$ eines Elements $a \in G$ bezüglich dieser Relation gilt*
$$\overline{a} = aU := \{au : u \in U\}.$$
*Man nennt diese Klassen die **Linksnebenklassen** von U (weil man das Element $a \in G$ links neben alle Elemente von U schreibt). Die Menge aller Äquivalenzklassen dieser Relation, also die Menge aller Linksnebenklassen, wird mit*
$$G/U := G/\sim = \{aU : a \in G\}$$
*bezeichnet. Man liest G/U oft als „G **modulo** U“ und sagt, dass man G/U aus G erhält, indem man U „herausteilt“. Dementsprechend schreibt man für $a,b \in G$ statt $\overline{a} = \overline{b} \in G/U$ auch „$a = b \mod U$“ (gesprochen: $a = b$ modulo U).*

Beweis.

(a) Wir müssen die drei Eigenschaften aus Definition 5.1 (b) zeigen. In der Tat entsprechen diese Eigenschaften in gewissem Sinne genau den drei Eigenschaften des Untergruppenkriteriums aus Satz 3.3:

(A1): Für alle $a \in G$ gilt $a^{-1}a = e \in U$ nach (U2), und damit $a \sim a$ nach Definition von $\sim$.

(A2): Sind $a,b \in G$ mit $a \sim b$, also $a^{-1}b \in U$, so ist nach Lemma 1.10 (b) und (U3) auch $b^{-1}a = (a^{-1}b)^{-1} \in U$ und damit $b \sim a$.

(A3): Sind $a,b,c \in G$ mit $a \sim b$ und $b \sim c$, also $a^{-1}b \in U$ und $b^{-1}c \in U$, so ist nach (U1) auch $a^{-1}c = (a^{-1}b)(b^{-1}c) \in U$ und damit $a \sim c$.

(b) Für $a \in G$ ist

$$\begin{aligned}
\overline{a} &= \{b \in G : b \sim a\} && \text{(Definition von } \overline{a}\text{)} \\
&= \{b \in G : a \sim b\} && \text{(A2)} \\
&= \{b \in G : a^{-1}b = u \text{ für ein } u \in U\} && \text{(Definition von } \sim\text{)} \\
&= \{b \in G : b = au \text{ für ein } u \in U\} \\
&= aU
\end{aligned}$$

genau die Linksnebenklasse von a. □

Bemerkung 5.7. Es sei G eine Gruppe und $U \leq G$.

(a) Nach Lemma 5.3 (a) und Definition 5.6 gilt also für $a, b \in G$ und die dort betrachtete Äquivalenzrelation

$$\overline{a} = \overline{b} \quad \Leftrightarrow \quad a^{-1}b \in U.$$

Wenn wir im Folgenden mit dieser Äquivalenzrelation arbeiten, ist dies vermutlich das Einzige, was wir dafür benötigen werden, da es uns ermöglicht, jede Gleichung zwischen Äquivalenzklassen auf Relationen in der ursprünglichen Gruppe zurückzuführen.

Insbesondere ist also $\overline{b} = \overline{e}$ genau dann, wenn $b \in U$: Es werden genau die Elemente von G mit dem neutralen Element identifiziert, die in U liegen — was noch einmal anschaulich die Sprechweise des „Herausteilens“ von U erklärt.

(b) Es war in Definition 5.6 etwas willkürlich, dass wir $a \sim b$ durch $a^{-1}b \in U$ und nicht umgekehrt durch $ba^{-1} \in U$ definiert haben. In der Tat könnten wir genauso auch für diese „umgekehrte“ Relation eine zu Lemma 5.6 analoge Aussage beweisen, indem wir dort die Reihenfolge aller Verknüpfungen umdrehen. Wir würden dann demzufolge als Äquivalenzklassen also auch nicht die Linksnebenklassen, sondern die sogenannten **Rechtsnebenklassen**

$$Ua = \{ua : u \in U\}$$

erhalten. Ist G abelsch, so sind Links- und Rechtsnebenklassen natürlich dasselbe. Im nichtabelschen Fall werden sie im Allgemeinen verschieden sein, wie wir im folgenden Beispiel 5.8 (b) sehen werden — allerdings wird auch hier später (siehe Lemma 6.5) der Fall, in dem Links- und Rechtsnebenklassen übereinstimmen, eine besonders große Rolle spielen.

Wir vereinbaren im Folgenden, dass wie in Definition 5.6 die Notationen $\overline{a}$ bzw. G/U stets für die *Links*nebenklasse aU bzw. die Menge dieser *Links*nebenklassen stehen. Wollen wir zwischen Links- und Rechtsnebenklassen unterscheiden, müssen wir sie explizit als aU bzw. Ua schreiben.

Beispiel 5.8.

(a) Ist $G = \mathbb{Z}$, $n \in \mathbb{N}_{>0}$ und $U = n\mathbb{Z}$, so erhalten wir die Situation wie in Beispiel 5.2 (b): Für $a, b \in \mathbb{Z}$ ist $a \sim b$ nach Definition 5.6 genau dann, wenn $b - a \in n\mathbb{Z}$ (beachte, dass wir die Gruppenverknüpfung hier additiv schreiben), und die Äquivalenzklassen (also die Linksnebenklassen) sind

$$\overline{a} = a + n\mathbb{Z} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\},$$

also für $a \in \{0, \ldots, n-1\}$ alle ganzen Zahlen, die bei Division durch n den Rest a lassen. Demzufolge ist die Menge aller Linksnebenklassen die n-elementige Menge

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},$$

also die „Menge aller möglichen Reste bei Division durch n“. Da dieses Beispiel besonders wichtig ist, hat die Menge $\mathbb{Z}/n\mathbb{Z}$ eine besondere Bezeichnung: Wir setzen

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z},$$

und schreiben statt $a = b \bmod n\mathbb{Z}$ (also $\overline{a} = \overline{b}$ in $\mathbb{Z}_n$) oft auch kurz $a = b \bmod n$.

Wir können die Stände einer analogen Uhr also mit der Menge $\mathbb{Z}_{12}$ identifizieren.

(b) Wir betrachten die Gruppe $G = S_3$ und darin die Untergruppe

$$U = \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\}.$$

Ist nun $\sigma_1 = (1\ 2\ 3)$ und $\sigma_2 = (1\ 3\ 2)$, so bilden die drei Linksnebenklassen

$$\begin{aligned}
\overline{\mathrm{id}} &= \mathrm{id} \circ U &&= \{\mathrm{id}, (1\ 2)\}, \\
\overline{\sigma_1} &= \sigma_1 \circ U &&= \{(1\ 2\ 3), (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\}, \\
\overline{\sigma_2} &= \sigma_2 \circ U &&= \{(1\ 3\ 2), (1\ 3\ 2)(1\ 2)\} = \{(1\ 3\ 2), (2\ 3)\}
\end{aligned}$$

offensichtlich eine disjunkte Zerlegung von S_3. Also sind dies nach Lemma 5.3 (b) bereits alle Linksnebenklassen, und wir erhalten

$$S_3/U = \{\overline{\mathrm{id}}, \overline{\sigma_1}, \overline{\sigma_2}\}.$$

Berechnen wir außerdem noch die Rechtsnebenklasse von σ_1, so sehen wir weiterhin, dass

$$U \circ \sigma_1 = \{(1\ 2\ 3), (1\ 2)(1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 3)\} \neq \sigma_1 \circ U.$$

Links- und Rechtsnebenklassen sind hier also verschieden.

An Beispiel 5.8 (b) fällt auf, dass dort alle Linksnebenklassen gleich viele Elemente haben. Dies ist in der Tat allgemein so, wie das folgende Lemma zeigt.

Lemma 5.9. *Es sei G eine Gruppe und $U \leq G$ eine endliche Untergruppe. Dann hat jede Links- und jede Rechtsnebenklasse von U genauso viele Elemente wie U.*

Beweis. Für $a \in G$ betrachten wir die Abbildung

$$f \colon U \to aU,\ f(u) = au.$$

Nach Definition von aU ist f surjektiv. Die Abbildung f ist aber auch injektiv, denn aus $f(u) = f(v)$, also $au = av$, folgt mit der Kürzungsregel in Lemma 1.10 (c) natürlich sofort $u = v$. Also ist f bijektiv, und damit müssen die Startmenge U und die Zielmenge aU gleich viele Elemente haben. Die Aussage für Ua ergibt sich analog. □

Eine sehr einfache, aber dennoch mächtige Folgerung aus diesem Lemma ist der folgende Satz, der oft beim Auffinden aller Untergruppen einer gegebenen (endlichen) Gruppe nützlich ist.

Satz 5.10 (Satz von Lagrange). *Für jede Untergruppe U einer endlichen Gruppe G gilt*

$$|G| = |U| \cdot |G/U|.$$

Insbesondere ist die Ordnung jeder Untergruppe von G also ein Teiler der Ordnung von G.

Beweis. Nach Lemma 5.3 (b) ist G die disjunkte Vereinigung aller Linksnebenklassen. Die Behauptung des Satzes folgt nun sofort daraus, dass es $|G/U|$ Linksnebenklassen gibt und nach Lemma 5.9 jede von ihnen $|U|$ Elemente hat. □

Wir wollen nun noch ein paar nützliche Folgerungen aus dem Satz von Lagrange ziehen. Dazu benötigen wir die folgende Definition.

Definition 5.11 (Ordnung eines Gruppenelements)**.** Es sei G eine Gruppe und $a \in G$. Gibt es ein $n \in \mathbb{N}_{>0}$ mit $a^n = e$, so heißt das kleinste solche n die **Ordnung** $\operatorname{ord} a$ von a. Existiert kein solches n, so schreibt man oft formal $\operatorname{ord} a = \infty$.

Beispiel 5.12.

(a) Es sei $G = S_n$ und $\sigma = (a_1\ a_2\ \cdots\ a_k)$ ein k-Zykel wie in Notation 2.8 (a). Dann ist $\sigma^k = \mathrm{id}$, denn jedes a_i für $i = 1, \ldots, k$ wird durch k-maliges zyklisches Vorwärtsschieben in der Liste $a_1, \ldots, a_k$ natürlich wieder auf sich selbst abgebildet. Weiterhin ist $\sigma^i \neq \mathrm{id}$ für $1 \leq i < k$, denn in diesem Fall ist z. B. $\sigma^i(a_1) = a_{i+1} \neq a_1$. Also ist $\operatorname{ord} \sigma = k$: Jeder k-Zykel hat die Ordnung k.

(b) In $G = \mathbb{Z}$ ist $\operatorname{ord} 1 = \infty$, denn $n \cdot 1 \neq 0$ für alle $n \in \mathbb{N}_{>0}$.

Aufgabe 5.13. Zeige, dass in jeder Gruppe G für beliebige Elemente $a, b \in G$ gilt:

(a) $\operatorname{ord}(a^{-1}) = \operatorname{ord} a$.

(b) $\operatorname{ord}(ab) = \operatorname{ord}(ba)$.

(c) Ist $\operatorname{ord} a < \infty$ und $f\colon G \to H$ ein Morphismus, so ist $\operatorname{ord} f(a)$ ein Teiler von $\operatorname{ord} a$.

Beachte, dass wir den Begriff „Ordnung“ in den Definitionen 1.1 (c) und 5.11 für zwei zunächst erst einmal verschiedene Konzepte verwendet haben. Der Zusammenhang zwischen ihnen wird aus dem folgenden Lemma deutlich, das zeigt, dass die Ordnung $\operatorname{ord} a$ eines Elements a auch als die Ordnung der von a erzeugten Untergruppe interpretiert werden kann.

Lemma 5.14 (Ordnungen von Elementen und Untergruppen)**.** *Es seien G eine Gruppe und $a \in G$.*

(a) *Ist $\operatorname{ord} a =: n < \infty$, so gilt $\langle a \rangle = \{a^0, \dots, a^{n-1}\}$, und diese n Elemente sind alle verschieden.*

(b) *Ist $\operatorname{ord} a = \infty$, so gilt $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$, und alle a^k für $k \in \mathbb{Z}$ sind verschieden.*

Insbesondere ist in beiden Fällen also $\operatorname{ord} a = |\langle a \rangle| \in \mathbb{N}_{>0} \cup \{\infty\}$.

Beweis. Nach Beispiel 3.13 (a) ist in jedem Fall zunächst einmal $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

(a) Mit Division durch n mit Rest lässt sich jedes $k \in \mathbb{Z}$ schreiben als $k = qn + r$ mit $q \in \mathbb{Z}$ und $0 \le r \le n-1$. Wegen $a^n = e$ ist damit

$$\begin{aligned}\langle a \rangle &= \{a^{qn+r} : q \in \mathbb{Z} \text{ und } 0 \le r \le n-1\} = \{(a^n)^q \cdot a^r : q \in \mathbb{Z} \text{ und } 0 \le r \le n-1\} \\ &= \{a^r : 0 \le r \le n-1\}.\end{aligned}$$

Weiterhin sind diese n Elemente alle verschieden: Wäre $a^i = a^j$ für gewisse $0 \le i < j \le n-1$, so hätten wir $a^{j-i} = e$, was wegen $0 < j - i < n$ ein Widerspruch dazu ist, dass n nach Definition 5.11 die *kleinste* positive Zahl ist mit $a^n = e$.

(b) Wäre $a^i = a^j$ für gewisse $i, j \in \mathbb{Z}$ mit $i < j$, so wäre wie eben $a^{j-i} = e$ mit $j - i > 0$, im Widerspruch zu $\operatorname{ord} a = \infty$. □

Aus diesem Lemma ergibt sich wieder eine interessante und nützliche Folgerung.

Folgerung 5.15. *Es sei G eine endliche Gruppe und $a \in G$. Dann gilt:*

(a) *$\operatorname{ord} a$ ist ein Teiler von $|G|$.*

(b) ***(Kleiner Satz von Fermat)*** *$a^{|G|} = e$.*

Beweis. Nach Lemma 5.14 hat die von a erzeugte Untergruppe $\langle a \rangle$ die Ordnung $\operatorname{ord} a$. Da diese Ordnung nach dem Satz 5.10 von Lagrange ein Teiler von $|G|$ sein muss, ergibt sich sofort Teil (a). Weiterhin ist (wiederum nach dem Satz von Lagrange)

$$a^{|G|} = a^{|\langle a \rangle| \cdot |G/\langle a \rangle|} = \left(a^{|\langle a \rangle|}\right)^{|G/\langle a \rangle|} = \underbrace{\left(a^{\operatorname{ord} a}\right)}_{=e}^{|G/\langle a \rangle|} = e,$$

und damit folgt auch Teil (b). □

Beispiel 5.16 (Untergruppen von S_3)**.** Mit unseren Ergebnissen können wir nun sehr schnell eine vollständige Liste aller Untergruppen der symmetrischen Gruppe S_3 angeben: Natürlich gibt es zunächst die trivialen Untergruppen $\{\mathrm{id}\}$ und S_3. Ist U eine andere Untergruppe von S_3, muss U sicher ein Element $\sigma \neq \mathrm{id}$ enthalten. Da alle diese Elemente 2-Zykel oder 3-Zykel sind und damit nach Beispiel 5.12 (a) die Ordnung 2 oder 3 haben, können wir die folgenden Fälle unterscheiden:

(a) $\operatorname{ord} \sigma = 2$, d. h. σ ist eine Transposition: Dann ist 2 ein Teiler von $|U|$ nach Folgerung 5.15 (a) und $|U|$ ein Teiler von 6 nach Satz 5.10. Wegen $U \neq G$ ist also $|U| = 2$ und damit $U = \langle \sigma \rangle$. Wir erhalten so die drei Untergruppen

$$\langle (1\ 2) \rangle, \langle (1\ 3) \rangle \quad \text{und} \quad \langle (2\ 3) \rangle.$$

(b) $\operatorname{ord}\sigma = 3$, d. h. σ ist ein Dreierzykel: Wie oben ist dann 3 ein Teiler von $|U|$ und $|U|$ ein Teiler von 6, also $|U| = 3$ und damit wieder $U = \langle\sigma\rangle$. In diesem Fall gibt es nur eine solche Untergruppe, die beide Dreierzykel von S_3 enthält, nämlich

$$\langle(1\ 2\ 3)\rangle = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} = A_3$$

wie in Beispiel 4.17.

Insgesamt hat S_3 also die sechs Untergruppen $\{\mathrm{id}\}, \langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle, \langle(1\ 2\ 3)\rangle$ und S_3.

Aufgabe 5.17. Es seien $\sigma, \tau \in S_4$ mit $\operatorname{ord}\sigma = 3$ und $\operatorname{ord}\tau = 2$. Welche Ordnung kann dann die von diesen beiden Elementen erzeugte Untergruppe $\langle\sigma, \tau\rangle$ haben? Man gebe für jede solche mögliche Ordnung ein Beispiel an.

Aufgabe 5.18. Bestimme alle Untergruppen der Diedergruppe D_5 aus Aufgabe 3.16.

06

6. Faktorgruppen

Im vorangegangenen Kapitel haben wir zu einer Untergruppe U einer gegebenen Gruppe G die Menge der Linksnebenklassen $G/U = \{aU : a \in G\}$ untersucht und damit bereits einige interessante Resultate wie z. B. den Satz 5.10 von Lagrange erhalten.

Eine Menge ist für sich genommen aber noch keine besonders interessante Struktur. Wünschenswert wäre es natürlich, wenn wir G/U nicht nur als *Menge*, sondern ebenfalls wieder als *Gruppe* auffassen könnten, also wenn wir aus der gegebenen Verknüpfung in G auch eine Verknüpfung in G/U konstruieren könnten. Wir wollen daher in diesem Kapitel untersuchen, wann und wie dies möglich ist.

Als Erstes benötigen wir dazu eine wichtige Vorbemerkung, die immer dann relevant ist, wenn wir auf einer Menge von Äquivalenzklassen eine Funktion (oder Verknüpfung) definieren wollen.

Bemerkung 6.1 (Wohldefiniertheit)**.** Erinnern wir uns noch einmal an die Konstruktion des Signums einer Permutation $\sigma \in S_n$ aus Definition 2.13: Wir mussten hierfür eine Darstellung $\sigma = \tau_1 \cdots \tau_r$ von σ als Verkettung von Transpositionen $\tau_1, \ldots, \tau_r$ wählen, und haben dann $\operatorname{sign}\sigma := (-1)^r$ gesetzt. Damit dies die Zahl $\operatorname{sign}\sigma$ auch wirklich widerspruchsfrei definiert, mussten wir dabei natürlich überprüfen, dass das Gesamtresultat dieser Vorschrift von der zwischendurch nötigen Wahl der Verkettung von Transpositionen unabhängig ist: Lemma 2.12 (b) hat uns gesagt, dass bei einer anderen solchen Darstellung $\sigma = \tilde{\tau}_1 \cdots \tilde{\tau}_s$ in jedem Fall r und s beide gerade oder beide ungerade sind, so dass das Endergebnis $(-1)^r = (-1)^s$ immer dasselbe ist.

Abstrakt formuliert passiert es bei der Definition mathematischer Funktionen manchmal, dass die Abbildungsvorschrift an irgendeiner Stelle eine nicht eindeutig bestimmte Wahl erfordert. Wenn dies wie im Beispiel des Signums oben der Fall ist, ist es klar, dass wir am Ende überprüfen müssen, dass das Endresultat der Vorschrift nicht von dieser Wahl abhängt. Die mathematische Sprechweise hierfür ist, dass wir überprüfen müssen, ob die Funktion durch die gegebene Vorschrift **wohldefiniert** ist.

Besonders oft tritt dies bei der Untersuchung von Äquivalenzrelationen wie in Kapitel 5 auf. Ist $\sim$ eine Äquivalenzrelation auf einer Menge M und will man eine Abbildung $f\colon M/\sim \to N$ von der Menge der zugehörigen Äquivalenzklassen in eine weitere Menge N definieren, so ist die Idee hierfür in der Regel, dass man eine Abbildung $g\colon M \to N$ wählt und dann

$$f\colon M/\sim \to N,\ f(\overline{a}) := g(a)$$

setzt. Man möchte das Bild einer Äquivalenzklasse unter f also dadurch definieren, dass man einen Repräsentanten dieser Klasse wählt und diesen Repräsentanten dann mit g abbildet. Damit diese Vorschrift wohldefiniert ist, brauchen wir also offensichtlich, dass verschiedene Repräsentanten derselben Klasse das gleiche Endergebnis liefern, also dass gilt:

$$\text{Für alle } a,b \in M \text{ mit } \overline{a} = \overline{b} \text{ ist } g(a) = g(b).$$

Beispiel 6.2 (Verknüpfungen auf G/U)**.** Wir wollen nun wieder unsere ursprüngliche Situation betrachten, nämlich eine Menge G/U von Linksnebenklassen zu einer Untergruppe U einer gegebenen Gruppe G. Es ist natürlich sehr naheliegend, auf G/U eine Verknüpfung durch

$$\overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

definieren zu wollen: Um zwei Äquivalenzklassen in G/U miteinander zu verknüpfen, verknüpfen wir einfach zwei zugehörige Repräsentanten in G und nehmen dann vom Ergebnis wieder die Äquivalenzklasse.

(a) Als konkretes Beispiel betrachten wir noch einmal die Menge $\mathbb{Z}_{12} = \{\overline{0}, \dots, \overline{11}\}$ der Stände einer Uhr aus Beispiel 5.2 (b) bzw. Beispiel 5.8 (a). Wir würden also die Addition von $\mathbb{Z}$ auf $\mathbb{Z}_{12}$ übertragen wollen, indem wir z. B.

$$\overline{6} + \overline{8} = \overline{6+8} = \overline{14} = \overline{2}$$

rechnen: Wenn seit Mitternacht zuerst 6 und dann nochmal 8 Stunden vergehen, zeigt die Uhr anschließend auf die 2. Nach Bemerkung 6.1 müssen wir allerdings noch überprüfen, ob diese neue Verknüpfung auf $\mathbb{Z}_{12}$ wirklich wohldefiniert ist: Im Beispiel hätten wir statt der Repräsentanten 6 und 8 von $\overline{6}$ und $\overline{8}$ ja z. B. auch 18 bzw. 20 wählen können. In der Tat hätten wir dann allerdings ebenfalls wieder dasselbe Endergebnis

$$\overline{6} + \overline{8} = \overline{18+20} = \overline{38} = \overline{2}$$

erhalten: Auch wenn zuerst 18 und dann nochmal 20 Stunden vergehen, zeigt die Uhr danach auf die 2. In diesem Beispiel scheint die Situation also erst einmal in Ordnung zu sein. In der Tat ist die Verknüpfung in diesem Fall wohldefiniert, wie wir gleich in Beispiel 6.15 noch allgemein sehen werden. Leider ist dies jedoch nicht immer der Fall, wie das folgende Beispiel zeigt.

(b) Wir betrachten noch einmal das Beispiel 5.8 (b) der Untergruppe

$$U = \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\}$$

von S_3 mit den drei Linksnebenklassen

$$\overline{\mathrm{id}} = \{\mathrm{id}, (1\ 2)\}, \quad \overline{\sigma_1} = \{(1\ 2\ 3), (1\ 3)\}, \quad \overline{\sigma_2} = \{(1\ 3\ 2), (2\ 3)\},$$

wobei $\sigma_1 = (1\ 2\ 3)$ und $\sigma_2 = (1\ 3\ 2)$. Angenommen, wir könnten auch hier die Nebenklassen dadurch miteinander verknüpfen, dass wir einfach Repräsentanten der beiden Klassen miteinander verknüpfen und vom Ergebnis wieder die Nebenklasse nehmen. Um z. B. $\overline{\mathrm{id}} \circ \overline{\sigma_1}$ zu berechnen, könnten wir also den jeweils ersten oben aufgeführten Repräsentanten wählen und

$$\overline{\mathrm{id}} \circ \overline{\sigma_1} = \overline{\mathrm{id} \circ (1\ 2\ 3)} = \overline{(1\ 2\ 3)} = \overline{\sigma_1}$$

rechnen. Hätten wir für die erste Nebenklasse $\overline{\mathrm{id}}$ jedoch den zweiten Repräsentanten gewählt, so hätten wir als Ergebnis

$$\overline{\mathrm{id}} \circ \overline{\sigma_1} = \overline{(1\ 2) \circ (1\ 2\ 3)} = \overline{(2\ 3)} = \overline{\sigma_2}$$

erhalten, also nicht das gleiche wie vorher! Die Verknüpfung auf der Menge der Nebenklassen ist hier also nicht wohldefiniert.

Wir wollen diese Situation nun klären und herausfinden, in welchen Fällen die Gruppenverknüpfung in G auf eine in G/U übertragen werden kann. Die Eigenschaft von U, die wir hierfür benötigen, ist die folgende.

Definition 6.3 (Normalteiler)**.** Eine Teilmenge U einer Gruppe G heißt ein **Normalteiler**, in Zeichen $U \trianglelefteq G$, wenn gilt:

(a) U ist eine Untergruppe von G;

(b) für alle $a \in G$ und $u \in U$ ist $aua^{-1} \in U$.

Bemerkung 6.4. Da die Bedingung (b) in Definition 6.3 für alle $a \in G$ gelten muss, können wir dort auch genauso gut a durch a^{-1} ersetzen und erhalten die äquivalente Bedingung $a^{-1}ua \in U$.

Lemma 6.5. *Eine Untergruppe U einer Gruppe G ist genau dann ein Normalteiler, wenn $aU = Ua$ für alle $a \in G$ gilt, also wenn die Links- und Rechtsnebenklassen von U übereinstimmen.*

Beweis.

„⇒“ Ist $U \trianglelefteq G$, so gilt für alle $a \in G$ und $u \in U$ nach Bemerkung 6.4

$$aua^{-1} \in U \overset{\cdot a}{\Rightarrow} au \in Ua \Rightarrow aU \subset Ua$$
$$\text{und} \quad a^{-1}ua \in U \overset{a\cdot}{\Rightarrow} ua \in aU \Rightarrow Ua \subset aU,$$

und damit insgesamt $Ua = aU$.

„⇐“ Gilt $aU = Ua$ für alle $a \in G$, so ist $au \in aU = Ua$ und damit $aua^{-1} \in Uaa^{-1} = U$ für alle $u \in U$. □

Beispiel 6.6.

(a) Ist G abelsch, so ist jede Untergruppe U von G ein Normalteiler: Die Eigenschaft (b) aus Definition 6.3 ist hier natürlich stets erfüllt, denn es ist ja $aua^{-1} = aa^{-1}u = u \in U$ für alle $a \in G$ und $u \in U$.

(b) Die trivialen Untergruppen $\{e\}$ und G sind immer Normalteiler von G: In beiden Fällen sind die Eigenschaften aus Definition 6.3 offensichtlich.

(c) Die in Beispiel 6.2 (b) betrachtete Untergruppe $U = \langle (1\ 2) \rangle$ von S_3 ist kein Normalteiler: In der Tat haben wir in Beispiel 5.8 (b) konkret nachgeprüft, dass die äquivalente Normalteilerbedingung aus Lemma 6.5 in diesem Fall nicht erfüllt ist.

Ein weiteres, sehr wichtiges Beispiel von Normalteilern ist das folgende:

Lemma 6.7. *Ist $f\colon G \to H$ ein Gruppenhomomorphismus, so ist* $\operatorname{Ker} f$ *ein Normalteiler von G.*

Beweis. Wir wissen bereits (siehe Definition 4.14), dass $\operatorname{Ker} f$ eine Untergruppe von G ist. Weiterhin gilt für alle $a \in G$ und $u \in \operatorname{Ker} f$ nach Lemma 4.4

$$f(aua^{-1}) = f(a)\underbrace{f(u)}_{=e}f(a^{-1}) = f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e,$$

also $aua^{-1} \in \operatorname{Ker} f$. Damit ist $\operatorname{Ker} f$ ein Normalteiler von G. □

Beispiel 6.8. Die alternierende Gruppe (siehe Definition 4.16)

$$A_n = \{\sigma \in S_n : \operatorname{sign}\sigma = 1\}$$

ist als Kern der Signumsabbildung ein Normalteiler von S_n.

Aufgabe 6.9. Es sei U eine Untergruppe einer endlichen Gruppe G. Man zeige:

(a) Gibt es keine weitere Untergruppe von G, die genauso viele Elemente wie U hat, so ist U ein Normalteiler von G.

(b) Ist $|U| = \frac{1}{2}|G|$, so ist U ein Normalteiler von G.

Aufgabe 6.10. Welche der folgenden Teilmengen $U \subset G$ sind Normalteiler?

(a) $G = \mathbb{Z}$, $U = \{1, -1\}$;

(b) $G = S_n$, $U = \{\sigma \in S_n : \sigma(1) = 1\}$ für ein $n \in \mathbb{N}_{\geq 2}$;

(c) G eine beliebige Gruppe, $U = f^{-1}(N)$ für einen Gruppenhomomorphismus $f\colon G \to H$ und $N \trianglelefteq H$;

(d) G eine Gruppe mit $|G| = 24$, $U = \langle a, b \rangle$ für gewisse $a, b \in G$ mit $\operatorname{ord}(a) = 4$ und $\operatorname{ord}(b) = 3$.

Aufgabe 6.11. In einer Gruppe G seien U eine Untergruppe und N ein Normalteiler. Zeige, dass $UN := \{un : u \in U, n \in N\}$ dann eine Untergruppe von G ist.

Aufgabe 6.12. Es sei U eine Untergruppe einer Gruppe G.

Zeige, dass

$$V := \{(a, ua) : a \in G, u \in U\} \quad \subset G \times G$$

genau dann eine Untergruppe von $G \times G$ ist, wenn U ein Normalteiler von G ist.

Wie bereits angekündigt wollen wir nun sehen, dass sich die Gruppenverknüpfung von G auf eine in G/U überträgt, wenn U ein Normalteiler ist.

Satz und Definition 6.13 (Faktorgruppen)**.** *Es sei G eine Gruppe und $U \trianglelefteq G$. Dann gilt:*

(a) *Die Verknüpfung $\overline{a} \cdot \overline{b} := \overline{ab}$ ist wohldefiniert auf G/U und macht G/U zu einer Gruppe. Das neutrale Element dieser Gruppe ist $\overline{e}$, das zu $\overline{a}$ inverse Element ist $\overline{a^{-1}}$. Die Gruppe G/U wird als eine **Faktorgruppe** von G bezeichnet.*

(b) *Die Abbildung $\pi \colon G \to G/U$, $\pi(a) = \overline{a}$ ist ein surjektiver Morphismus mit Kern U. Man nennt sie die **Restklassenabbildung** von G/U.*

Beweis.

(a) Die Verknüpfung ist wohldefiniert: Sind $a, a', b, b' \in G$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, gilt also $a^{-1}a' =: u \in U$ und $b^{-1}b' =: v \in U$, so ist

$$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = b^{-1}ub' = b^{-1}ubb^{-1}b' = \underbrace{b^{-1}ub}_{\in U}v \in U,$$

wobei $b^{-1}ub \in U$ aus der Normalteilereigenschaft folgt. Also ist $\overline{ab} = \overline{a'b'}$ und die Verknüpfung damit wohldefiniert. Die Gruppenaxiome für G/U rechnet man nun ganz einfach nach:

(G1) Für alle $a, b, c \in G$ gilt

$$\left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} \overset{(*)}{=} \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right),$$

wobei $(*)$ die Assoziativität in G ist und alle anderen Gleichungen einfach nur die Definition der Verknüpfung auf G/U sind.

(G2) Für alle $a \in G$ ist $\overline{e} \cdot \overline{a} = \overline{ea} = \overline{a}$.

(G3) Für alle $a \in G$ ist $\overline{a^{-1}} \cdot \overline{a} = \overline{a^{-1}a} = \overline{e}$.

(b) Die Abbildung π ist nach Definition der Verknüpfung auf G/U ein Morphismus: Für alle $a, b \in G$ gilt nämlich

$$\pi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \pi(a) \cdot \pi(b).$$

Nach Definition von G/U ist π surjektiv. Der Kern von π ist

$$\operatorname{Ker} \pi = \{a \in G : \overline{a} = \overline{e}\} = \overline{e} = U. \qquad \square$$

Bemerkung 6.14.

(a) Die Normalteilereigenschaft von U ist für Satz 6.13 wirklich notwendig: Ist die Verknüpfung auf G/U wohldefiniert, so muss wegen $\overline{au} = \overline{a}$ für alle $a \in G$ und $u \in U$ insbesondere $\overline{au \cdot a^{-1}} = \overline{a \cdot a^{-1}} = \overline{e}$, also $aua^{-1} \in U$ gelten, und damit U ein Normalteiler sein.

(b) Ist G eine abelsche Gruppe, so auch jede Faktorgruppe G/U: Für alle $a, b \in G$ ist dann nämlich $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$.

(c) Wir hatten in Lemma 6.7 gesehen, dass jeder Kern eines Morphismus ein Normalteiler ist. Nach Satz 6.13 (b) gilt hier auch die Umkehrung: Jeder Normalteiler kann als Kern eines Morphismus geschrieben werden (nämlich als Kern der Restklassenabbildung).

Beispiel 6.15 ($\mathbb{Z}_n$ als Gruppe)**.** Es sei $n \in \mathbb{N}_{>0}$. Die Untergruppe $n\mathbb{Z}$ von $\mathbb{Z}$ ist natürlich ein Normalteiler, da $\mathbb{Z}$ abelsch ist (siehe Beispiel 6.6 (a)). Also ist die Menge $\mathbb{Z}_n$ mit der Verknüpfung $\overline{k} + \overline{l} := \overline{k+l}$, wie wir sie schon in Beispiel 6.2 (a) untersucht haben, nach Satz 6.13 und Bemerkung 6.14 (b) eine abelsche Gruppe. Wir können uns die Verknüpfung dort vorstellen als die gewöhnliche Addition in $\mathbb{Z}$, wobei wir uns bei der Summe aber immer nur den Rest bei Division durch n merken. Die Tabelle rechts zeigt die Verknüpfung dieser Gruppe im Beispiel $n = 3$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Diese Gruppen $(\mathbb{Z}_n, +)$ sind sicher die wichtigsten Beispiele von Faktorgruppen.

Bemerkung 6.16. Eine interessante Anwendung von Faktorgruppen besteht darin, dass man mit ihnen „aus jedem Morphismus einen Isomorphismus machen kann“. Um zu sehen, was damit gemeint ist, betrachten wir einmal einen beliebigen Morphismus $f\colon G \to H$ von Gruppen. Wir haben in Bemerkung 4.9 bereits gesehen, dass Isomorphismen, also bijektive Morphismen, besonders schön sind, da sie bedeuten, dass Start- und Zielraum „als Gruppen ununterscheidbar“ sind und daher miteinander identifiziert werden können.

Nun muss ein Morphismus f im Allgemeinen natürlich weder surjektiv noch injektiv sein. Dies lässt sich aber beheben: Klar ist zunächst einmal, dass man f natürlich immer zu einem surjektiven Morphismus machen kann, indem man den Zielraum H einfach durch die Untergruppe $\operatorname{Im} f$ ersetzt. Wie kann man f nun auch noch injektiv machen, d. h. (nach Lemma 4.18) den Kern von f zur trivialen Untergruppe machen, die nur aus einem (nämlich dem neutralen) Element besteht? Die Idee hierfür besteht darin, alle Elemente in $\operatorname{Ker} f$ miteinander zu identifizieren, so dass sie zu einem einzigen Element werden — mit anderen Worten also, beim Startraum von G zur Faktorgruppe $G/\operatorname{Ker} f$ überzugehen.

Kombinieren wir diese Ideen miteinander, so erhalten wir den folgenden wichtigen Satz:

Satz 6.17 (**Homomorphiesatz** für Gruppen)**.** *Es sei $f\colon G \to H$ ein Morphismus von Gruppen. Dann ist die Abbildung*

$$\begin{aligned} g\colon G/\operatorname{Ker} f &\to \operatorname{Im} f \\ \overline{a} &\mapsto f(a) \end{aligned}$$

zwischen der Faktorgruppe $G/\operatorname{Ker} f$ von G und der Untergruppe $\operatorname{Im} f$ von H ein Isomorphismus.

Beweis. Zunächst einmal ist $\operatorname{Ker} f$ nach Lemma 6.7 ein Normalteiler von G, so dass $G/\operatorname{Ker} f$ nach Satz 6.13 also wirklich eine Gruppe ist. Die im Satz angegebene Abbildung g ist außerdem wohldefiniert, denn für $a, b \in G$ mit $\overline{a} = \overline{b}$, also $a^{-1}b \in \operatorname{Ker} f$, gilt

$$e = f(a^{-1}b) = f(a)^{-1} f(b)$$

und damit $f(a) = f(b)$. Weiterhin ist g ein Morphismus, denn für $a, b \in G$ gilt

$$\begin{aligned} g\big(\overline{a} \cdot \overline{b}\big) &= g\big(\overline{ab}\big) && \text{(Definition der Verknüpfung in } G/\operatorname{Ker} f) \\ &= f(ab) && \text{(Definition von } g) \\ &= f(a) \cdot f(b) && (f \text{ ist Morphismus}) \\ &= g\big(\overline{a}\big) \cdot g\big(\overline{b}\big). && \text{(Definition von } g) \end{aligned}$$

Wir müssen also nur noch zeigen, dass g surjektiv und injektiv ist. Beides folgt im Prinzip unmittelbar aus der Konstruktion von g bzw. der Idee aus Bemerkung 6.16:

- g ist surjektiv: Ist b ein Element in der Zielgruppe $\operatorname{Im} f$, so gibt es also ein $a \in G$ mit $f(a) = b$, d. h. mit $g\big(\overline{a}\big) = b$.
- g ist injektiv: Ist $a \in G$ mit $g\big(\overline{a}\big) = f(a) = e$, so ist also $a \in \operatorname{Ker} f$ und damit $\overline{a} = \overline{e}$ nach Bemerkung 5.7 (a). Also ist $\operatorname{Ker} g = \{\overline{e}\}$ und g damit nach Lemma 4.18 injektiv. □

Folgerung 6.18. *Für jeden Morphismus $f\colon G \to H$ mit endlicher Startgruppe G gilt*

$$|G| = |\operatorname{Im} f| \cdot |\operatorname{Ker} f|.$$

Beweis. Nach dem Homomorphiesatz 6.17 ist $G/\operatorname{Ker} f$ isomorph zu $\operatorname{Im} f$. Insbesondere gilt also $|G/\operatorname{Ker} f| = |\operatorname{Im} f|$. Mit dem Satz 5.10 von Lagrange bedeutet dies aber sofort

$$\frac{|G|}{|\operatorname{Ker} f|} = |\operatorname{Im} f|, \quad \text{also} \quad |G| = |\operatorname{Im} f| \cdot |\operatorname{Ker} f|. \qquad \square$$

Beispiel 6.19.

(a) Wir betrachten für $n \in \mathbb{N}_{\geq 2}$ noch einmal den Morphismus $\operatorname{sign}\colon S_n \to \mathbb{R}\backslash\{0\}$ aus Beispiel 4.3 (d). Der Kern dieser Abbildung ist nach Definition 4.16 die alternierende Gruppe A_n, das Bild ist $\{\pm 1\}$ und hat damit Ordnung 2. Mit Folgerung 6.18 erhalten wir demnach

$$|S_n| = 2 \cdot |A_n|, \quad \text{also} \quad |A_n| = \frac{1}{2}|S_n| \overset{2.6}{=} \frac{n!}{2}.$$

(b) Ist G eine beliebige Gruppe und $f = \mathrm{id}\colon G \to G$ die Identität, so ist natürlich $\operatorname{Ker} f = \{e\}$ und $\operatorname{Im} f = G$. Nach dem Homomorphiesatz ist also $G/\{e\} \cong G$ (mit der Abbildung $\overline{a} \mapsto a$). Dies ist auch anschaulich klar: wenn man aus G „nichts herausteilt“, also keine nicht-trivialen Identifizierungen von Elementen aus G vornimmt, so ist die resultierende Gruppe immer noch G.

(c) Im anderen Extremfall, dem konstanten Morphismus $f\colon G \to G$, $a \mapsto e$, ist umgekehrt $\operatorname{Ker} f = G$ und $\operatorname{Im} f = \{e\}$. Hier besagt der Homomorphiesatz also $G/G \cong \{e\}$ (mit Isomorphismus $\overline{a} \mapsto e$): Wenn man aus G „alles herausteilt“, so bleibt nur noch die triviale Gruppe $\{e\}$ übrig.

07

Eine sehr schöne Anwendung des Homomorphiesatzes findet sich im Bereich der sogenannten Gruppenklassifikation. Natürlich wäre es wünschenswert, eine „vollständige Liste aller Gruppen“ hinschreiben zu können — also konkrete Beispiele von Gruppen so anzugeben, dass *jede beliebige* Gruppe zu (genau) einer dieser angegebenen Gruppen isomorph ist. Da isomorphe Gruppen ja ununterscheidbar sind, würde das nämlich bedeuten, dass wir dann eigentlich gar keine allgemeinen Gruppen mehr studieren müssten, sondern dass es reichen würde, stattdessen einfach nur alle Beispiele dieser Liste zu untersuchen. Falls ihr aus den Grundlagen der Mathematik schon Vektorräume kennt, werdet ihr vielleicht gemerkt haben, dass ihr dort auf genau diese Art vorgegangen seid: Ihr habt gezeigt, dass jeder (endlich-dimensionale) Vektorraum über $\mathbb{R}$ isomorph ist zu $\mathbb{R}^n$ für ein $n \in \mathbb{N}$ — und aus diesem Grund dann oft nur noch diese speziellen Vektorräume $\mathbb{R}^n$ untersucht (z. B. wenn man lineare Abbildungen durch Matrizen beschreibt).

Da wir uns dennoch schon seit Beginn dieser Vorlesung mit allgemeinen Gruppen beschäftigen, werdet ihr euch schon denken können, dass die Situation bei Gruppen hier nicht ganz so einfach ist. In der Tat wäre eine solche „Liste aller Gruppen“ so lang und kompliziert, dass man mit ihr eigentlich kaum noch etwas anfangen könnte. Wir können aber mit Hilfe des Homomorphiesatzes ein einfaches, aber dennoch verblüffendes Resultat in dieser Richtung zeigen: Wenn wir eine endliche Gruppe G haben, deren Ordnung eine *Primzahl* p ist (d. h. so dass $p \geq 2$ keine natürliche Zahl außer 1 und p als Teiler hat — ein Konzept, das wir in Kapitel 11 noch genauer untersuchen werden), so muss G bereits isomorph zu $\mathbb{Z}_p$ sein. Im Gegensatz zur Liste *aller* Gruppen ist die Liste aller Gruppen mit Primzahlordnung also wieder sehr einfach.

Um diese Aussage zeigen zu können, benötigen wir zuerst noch eine Definition.

Definition 6.20 (Zyklische Gruppen)**.** Eine Gruppe G heißt **zyklisch**, wenn sie von einem Element erzeugt werden kann, also wenn es ein $a \in G$ gibt mit $G = \langle a \rangle$.

Satz 6.21 (Klassifikation zyklischer Gruppen)**.** *Es sei G eine Gruppe.*

(a) *Ist G zyklisch, so ist G isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}_n$ für ein $n \in \mathbb{N}_{>0}$.*

(b) *Ist G endlich und $p := |G|$ eine Primzahl, so ist G isomorph zu $\mathbb{Z}_p$.*

Beweis.

(a) Es sei $a \in G$ mit $G = \langle a \rangle$. Wir betrachten die Abbildung

$$f\colon \mathbb{Z} \to G,\ k \mapsto a^k,$$

die aufgrund der Rechenregeln für Potenzen aus Lemma 1.12 ein Morphismus ist. Nach Beispiel 3.13 (a) ist dann

$$\operatorname{Im} f = \{a^k : k \in \mathbb{Z}\} = \langle a \rangle = G,$$

d. h. f ist surjektiv. Es ergeben sich nun zwei Fälle:

- Die Abbildung f ist auch injektiv. Dann ist $f\colon \mathbb{Z} \to G$ ein Isomorphismus, also $\mathbb{Z} \cong G$.
- Die Abbildung f ist nicht injektiv, nach Lemma 4.18 also $\operatorname{Ker} f \neq \{0\}$. Als Untergruppe von $\mathbb{Z}$ muss $\operatorname{Ker} f$ nach Satz 3.17 dann die Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}_{>0}$ haben. Aus dem Homomorphiesatz folgt damit $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong G$ (mit Isomorphismus $\overline{k} \mapsto a^k$).

(b) Es sei $a \in G$ ein beliebiges Element mit $a \neq e$. Nach dem Satz 5.10 von Lagrange muss die Ordnung der Untergruppe $\langle a \rangle$ von G ein Teiler der Gruppenordnung p sein. Da p eine Primzahl ist, kommt hier also nur $|\langle a \rangle| = 1$ oder $|\langle a \rangle| = p$ in Frage. Weil aber bereits die beiden Elemente e und a in $\langle a \rangle$ liegen, ist $|\langle a \rangle| = 1$ ausgeschlossen. Damit ist $|\langle a \rangle| = p$, d. h. es ist bereits $\langle a \rangle = G$. Also ist G zyklisch. Die Behauptung folgt damit aus Teil (a). □

Bemerkung 6.22 (S_3 als kleinste nicht-abelsche Gruppe)**.** Wir hatten in Aufgabe 1.15 bereits gesehen, dass jede nicht-abelsche Gruppe mindestens 5 Elemente haben muss. Dieses Ergebnis können wir jetzt verbessern: Da jede Gruppe der Ordnung 5 nach Satz 6.21 (b) isomorph zu $\mathbb{Z}_5$ und damit abelsch ist, muss jede nicht-abelsche Gruppe also sogar mindestens 6 Elemente haben.

In der Tat gibt es natürlich auch eine nicht-abelsche Gruppe der Ordnung 6, nämlich die symmetrische Gruppe S_3. Man kann zeigen, dass S_3 und $\mathbb{Z}_6$ bis auf Isomorphie die einzigen Gruppen der Ordnung 6 sind.

Aufgabe 6.23. Es sei $G = \mathbb{R}/\mathbb{Z}$.

(a) Für welche $a, b \in \mathbb{R}$ ist $f\colon G \to G$, $\overline{x} \mapsto \overline{ax+b}$ eine wohldefinierte Abbildung?

(b) Zeige, dass für jedes $n \in \mathbb{N}_{>0}$ die von $\overline{\frac{1}{n}}$ erzeugte Untergruppe von G isomorph zu $\mathbb{Z}_n$ ist.

Aufgabe 6.24.

(a) Es seien G und H zwei endliche Gruppen, deren Ordnungen $|G|$ und $|H|$ keinen gemeinsamen Teiler (größer als 1) besitzen. Zeige, dass es dann nur einen Morphismus von G nach H gibt.

(b) Bestimme alle Morphismen von $\mathbb{Z}_9$ nach $\mathbb{Z}_{11}$ sowie von $\mathbb{Z}_9$ nach $\mathbb{Z}_{12}$.

Aufgabe 6.25. Es sei G eine Gruppe mit $|G| = 10$. Zeige, dass G entweder kein Element der Ordnung 10 oder genau vier Elemente der Ordnung 10 besitzt, und gib für jeden dieser beiden Fälle ein Beispiel an.

Aufgabe 6.26. Es sei N ein Normalteiler einer Gruppe G. Zeige, dass die Abbildung

$$\begin{aligned} \{U\colon U \text{ ist Untergruppe von } G \text{ mit } U \supset N\} &\to \{V\colon V \text{ ist Untergruppe von } G/N\} \\ U &\mapsto U/N \end{aligned}$$

bijektiv ist. (Die Untergruppen einer Faktorgruppe G/N entsprechen in diesem Sinne also genau den Untergruppen von G, die N enthalten.)

Aufgabe 6.27. Der Satz 5.10 von Lagrange besagt bekanntlich, dass die Ordnung jeder Untergruppe einer endlichen Gruppe G ein Teiler von $|G|$ sein muss. Wir wollen nun in zwei einfachen Fällen die umgekehrte Fragestellung untersuchen, ob es zu jedem Teiler von $|G|$ auch eine Untergruppe dieser Ordnung geben muss. Zeige dazu für eine endliche Gruppe G:

(a) Ist 2 ein Teiler von $|G|$, so besitzt G ein Element der Ordnung 2 (und damit auch eine Untergruppe der Ordnung 2).

(b) Ist G abelsch und 2^n ein Teiler von $|G|$ für ein $n \in \mathbb{N}$, so hat G eine Untergruppe der Ordnung 2^n.

Hinweis: Für (a) zeige man, dass G außer dem neutralen Element noch mindestens ein weiteres Element a mit $a^{-1} = a$ besitzen muss. Für (b) empfiehlt sich Induktion über n und die Untersuchung einer geeigneten Faktorgruppe von G.

Aufgabe 6.28.

(a) Bestimme mit Hilfe von Aufgabe 6.26 alle Untergruppen von $\mathbb{Z}_n$ für $n > 0$.

(b) Man zeige: Ist G eine endliche zyklische Gruppe und n ein Teiler der Ordnung von G, so gibt es genau eine Untergruppe von G der Ordnung n, und diese ist ebenfalls zyklisch.

Aufgabe 6.29. Es sei G eine Gruppe. Man zeige:

(a) Sind $a, b \in G$ und ist $\operatorname{ord} a = \operatorname{ord} b$ eine Primzahl, so gilt $\langle a \rangle = \langle b \rangle$ oder $\langle a \rangle \cap \langle b \rangle = \{e\}$.

(b) Ist $|G| = 35$, so gibt es $a, b \in G$ mit $\operatorname{ord} a = 5$ und $\operatorname{ord} b = 7$.

(c) Ist $|G| = 35$ und G abelsch, so ist $G \cong \mathbb{Z}_{35}$.

Aufgabe 6.30. Man zeige: Ist G eine Gruppe, die genau drei Untergruppen besitzt, so ist $G \cong \mathbb{Z}_{p^2}$ für eine Primzahl p.

Aufgabe 6.31. Es seien $n \in \mathbb{N}_{>1}$ und U eine Untergruppe einer endlichen Gruppe G mit $|U| = \frac{1}{n}|G|$. Man zeige für alle $a \in G$:

(a) Ist U ein Normalteiler von G, so gilt $a^n \in U$.

(b) Im Allgemeinen liegt zwar mindestens eines der Elemente $a^1, a^2, \ldots, a^n$ in U, aber nicht notwendig a^n.

Aufgabe 6.32. Man zeige:

(a) Eine Gruppe der Ordnung 60 hat höchstens einen Normalteiler der Ordnung 12.

(b) Eine Gruppe der Ordnung 60 kann mehrere Untergruppen der Ordnung 12 haben.

7. Ringe und Körper

In den bisherigen Kapiteln haben wir nur Gruppen, also insbesondere nur Mengen mit lediglich *einer* Verknüpfung, untersucht. In der Praxis gibt es aber natürlich auch viele Mengen, auf denen *zwei* Verknüpfungen gegeben sind, die man sich dann in der Regel als Addition und Multiplikation vorstellen kann: z. B. die Mengen der ganzen Zahlen, reellen Zahlen, reellwertigen Funktionen oder Matrizen. Da Addition und Multiplikation hierbei nicht einfach unabhängige Verknüpfungen sind, sondern in der Regel über ein „Distributivgesetz“ $(a+b)c = ac+bc$ miteinander zusammen hängen, reicht es in diesen Fällen nicht aus, einfach zwei Gruppenstrukturen auf derselben Menge zu betrachten. Stattdessen bilden derartige Mengen eine neue Struktur, die man einen *Ring* nennt und die wir jetzt einführen wollen.

Definition 7.1 (Ringe)**.**

(a) Ein **Ring** ist eine Menge R mit zwei Verknüpfungen $+\colon R\times R\to R$ und $\cdot\colon R\times R\to R$ (genannt „Addition“ und „Multiplikation“ und immer geschrieben als „$+$“ bzw. „$\cdot$“), so dass die folgenden Eigenschaften gelten:

(R1) $(R,+)$ ist eine abelsche Gruppe. (Wie üblich bezeichnen wir das neutrale Element dieser Verknüpfung mit 0 und das zu $a\in R$ inverse Element mit $-a$.)

(R2) Für alle $a,b,c\in R$ gilt $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ (**Assoziativität** der Multiplikation).

(R3) Für alle $a,b,c\in R$ gilt die **Distributivität**

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

Wir schreiben einen solchen Ring als $(R,+,\cdot)$, oder in der Regel auch einfach nur als R, wenn die Verknüpfungen aus dem Zusammenhang klar sind.

(b) Gilt zusätzlich zu (R1), (R2) und (R3) noch

(R4) Es gibt ein $e\in R$ mit $e\cdot a = a\cdot e = a$ für alle $a\in R$ (Existenz eines **neutralen Elements** der Multiplikation),

so heißt R ein **Ring mit Eins**.

(c) Gilt zusätzlich zu (R1), (R2) und (R3)

(R5) Für alle $a,b\in R$ gilt $a\cdot b = b\cdot a$ (**Kommutativität** der Multiplikation),

dann heißt R ein **kommutativer Ring**.

Konvention 7.2. Um unsere Untersuchung von Ringen nicht zu kompliziert werden zu lassen, wollen wir uns in dieser Vorlesung auf den in der Praxis wichtigsten Fall beschränken, in dem alle Eigenschaften (R1), …, (R5) aus Definition 7.1 gelten. Wir vereinbaren daher:

Im Folgenden sei ein Ring stets kommutativ mit Eins.

Fasst man die Eigenschaften (R1), …, (R5) zusammen, so ist ein Ring für uns also eine Menge mit zwei Verknüpfungen „$+$“ und „$\cdot$“, von denen die Addition eine abelsche Gruppe bildet, die Multiplikation alle Eigenschaften einer abelschen Gruppe mit Ausnahme der Existenz inverser Elemente besitzt, und die das Distributivgesetz erfüllen.

Wenn ihr in die Literatur schaut, werdet ihr feststellen, dass einige Autoren ebenfalls diese Konvention verwenden, während andere unter einem Ring wirklich nur eine Struktur mit den drei Eigenschaften (R1), (R2) und (R3) verstehen. Es bleibt einem also nichts anderes übrig, als bei jedem Buch, in dem man etwas über Ringe liest, erst einmal zu überprüfen, welche Konvention der Autor verwendet.

Bemerkung 7.3. Eine Eins wie in Eigenschaft (R4) von Definition 7.1 ist stets eindeutig: Sind e und e' zwei solche Einselemente, so folgt natürlich sofort $e = e \cdot e' = e'$. Wir schreiben das (eindeutig bestimmte) Einselement eines Ringes daher in der Regel einfach als 1, wenn dadurch keine Verwirrung entstehen kann.

Beispiel 7.4.

(a) $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ (mit der üblichen Addition und Multiplikation) sind natürlich Ringe. Ebenso gilt dies für die Menge $\mathbb{C}$ der komplexen Zahlen, die ihr inzwischen sicher aus den Grundlagen der Mathematik kennt.

(b) Es sei $n \in \mathbb{N}_{>0}$. Wir haben in Beispiel 6.15 bereits gesehen, dass sich die additive Gruppenstruktur der ganzen Zahlen wohldefiniert auf $\mathbb{Z}_n$ übertragen lässt, wenn man $\overline{a} + \overline{b} := \overline{a+b}$ setzt. Wir wollen nun zeigen, dass sich genauso auch die Multiplikation durch $\overline{a} \cdot \overline{b} := \overline{ab}$ auf $\mathbb{Z}_n$ übertragen lässt und $\mathbb{Z}_n$ damit zusammen mit der Addition zu einem Ring macht. Dazu rechnen wir zunächst analog zu Satz 6.13 (a) nach, dass diese Verknüpfung wohldefiniert ist: Sind $a, b, a', b' \in \mathbb{Z}$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$ in $\mathbb{Z}_n$, also $a' = a + kn$ und $b' = b + ln$ für gewisse $k, l \in \mathbb{Z}$, so ist auch

$$a'b' = (a+kn)(b+ln) = ab + aln + bkn + kln^2 = ab + n(al + bk + kln) \quad \in ab + n\mathbb{Z}$$

und damit $\overline{ab} = \overline{a'b'}$. Von den Ringeigenschaften aus Definition 7.1 hatten wir (R1) schon gezeigt. Die anderen Eigenschaften übertragen sich nun genau wie in Satz 6.13 (a) von $\mathbb{Z}$ auf $\mathbb{Z}_n$; wir zeigen hier exemplarisch (R2): Für alle $a, b, c \in \mathbb{Z}$ gilt

$$\left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right)$$

in $\mathbb{Z}_n$. Also ist $\mathbb{Z}_n$ ein Ring.

Wir werden in Kapitel 8 noch genauer untersuchen, in welchen Fällen sich Ringe durch Herausteilen einer additiven Untergruppe wieder zu neuen Ringen machen lassen.

(c) Sind R und S Ringe, so ist auch ihr Produkt $R \times S$ mit der komponentenweise definierten Addition und Multiplikation

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2) \quad \text{und} \quad (a_1, a_2) \cdot (b_1, b_2) := (a_1 \cdot b_1, a_2 \cdot b_2)$$

ein Ring (mit Nullelement $(0,0)$ und Einselement $(1,1)$). Der Beweis dieser Aussage verläuft natürlich völlig analog zum Fall von Gruppen in Konstruktion 1.5.

(d) Ist M eine beliebige Menge und R ein Ring, so rechnet man sofort nach, dass auch die Menge

$$S = \{f \colon M \to R \text{ Abbildung}\}$$

aller Abbildungen von M nach R mit der punktweise definierten Addition und Multiplikation

$$(f+g)(x) := f(x) + g(x) \qquad \text{und} \quad (f \cdot g)(x) := f(x) \cdot g(x)$$

ein Ring ist. Das Nullelement 0 in S ist dabei die konstante Funktion mit Wert $0 \in R$, das Einselement 1 die konstante Funktion mit Wert $1 \in R$.

(e) Die einelementige Menge $R = \{0\}$ (mit den trivialen Verknüpfungen) ist ein Ring, wenn man $e = 0$ setzt (d. h. es gilt hier $1 = 0$ im Sinne von Bemerkung 7.3). Man bezeichnet diesen (eher uninteressanten) Ring als den **Nullring**. Wir werden gleich in Lemma 7.5 (c) sehen, dass dies der einzige Ring ist, in dem $1 = 0$ gilt — wir müssen uns also über diese etwas merkwürdig aussehende Gleichung nicht allzu viele Gedanken machen.

Wie im Fall von Gruppen sollten wir als Erstes die wichtigsten Rechenregeln in Ringen auflisten. Einige davon ergeben sich sofort daraus, dass ein Ring R mit der Addition eine abelsche Gruppe ist — so ist z. B. $-(-a) = a$ für alle $a \in R$, und aus $x + a = x + b$ (für $x, a, b \in R$) folgt $a = b$ (siehe Lemma 1.10). Derartige Regeln brauchen wir natürlich hier nicht noch einmal zu beweisen. Neu sind hingegen die Rechenregeln, die die additive Struktur eines Ringes mit der multiplikativen verknüpfen:

Lemma 7.5 (Rechenregeln in Ringen)**.** *In jedem Ring R gilt:*

(a) *Für alle $a \in R$ ist $0 \cdot a = 0$.*

(b) *Für alle $a, b \in R$ ist $(-a) \cdot b = -(a \cdot b)$.*

(c) *Ist R nicht der Nullring, so ist $1 \neq 0$.*

Beweis.

(a) Für alle $a \in R$ gilt zunächst $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Subtrahieren wir nun $0 \cdot a$ von beiden Seiten dieser Gleichung, so erhalten wir wie behauptet $0 = 0 \cdot a$.

(b) Für alle $a, b \in R$ ist $(-a) \cdot b + a \cdot b = (-a+a) \cdot b = 0 \cdot b \overset{\text{(a)}}{=} 0$. Also ist $(-a) \cdot b$ das additive Inverse zu $a \cdot b$, d. h. es ist $(-a) \cdot b = -(a \cdot b)$.

(c) Angenommen, es wäre $1 = 0$. Dann wäre für alle $a \in R$

$$a = 1 \cdot a = 0 \cdot a \overset{\text{(a)}}{=} 0.$$

Also wäre R dann der Nullring, im Widerspruch zur Voraussetzung. □

Wir hatten schon bemerkt, dass die Eigenschaften (R1), ..., (R5) aus Definition 7.1 über die Multiplikation in einem Ring besagen, dass sie alle Eigenschaften einer abelschen Gruppe bis auf evtl. die Existenz von Inversen erfüllt. Diese Existenz von multiplikativen Inversen, die also für manche Ringelemente gegeben sein wird und für manche nicht, müssen wir daher jetzt genauer untersuchen.

Definition 7.6 (Einheiten und Nullteiler)**.** Es sei $R \neq \{0\}$ ein Ring.

(a) Ein Element $a \in R$ heißt **invertierbar** bzw. eine **Einheit**, wenn es ein $a' \in R$ gibt mit $a' \cdot a = 1$. Die Menge aller Einheiten von R wird mit R^* bezeichnet.

(b) R heißt ein **Körper**, wenn alle Elemente außer 0 Einheiten sind, also wenn $R^* = R \setminus \{0\}$ gilt.

(c) Ein Element $a \in R$ heißt **Nullteiler**, wenn es ein $b \in R$ mit $b \neq 0$ gibt, so dass $ab = 0$.

(d) R heißt ein **Integritätsring**, wenn kein Element außer 0 ein Nullteiler ist, also wenn für alle $a, b \in R$ aus der Gleichung $ab = 0$ bereits folgt, dass $a = 0$ oder $b = 0$.

Bemerkung 7.7.

(a) Mit exakt derselben Rechnung wie in Satz 1.7 (c) zeigt man, dass ein multiplikatives inverses Element a' zu einer Einheit $a \in R^*$ wie in Definition 7.6 (a) eindeutig ist. Wir bezeichnen es daher wie bei multiplikativ geschriebenen Gruppen mit a^{-1}. Da die Multiplikation in einem Ring kommutativ ist, können wir hier für eine Einheit $a \in R^*$ auch problemlos die Schreibweise $\frac{b}{a}$ für ba^{-1} bzw. $a^{-1}b$ verwenden (siehe Notation 1.9 (b)).

(b) Fassen wir die Definitionen 7.1 (mit Konvention 7.2) und 7.6 (b) zusammen, so sehen wir, dass eine Menge K mit zwei Verknüpfungen „$+$“ und „$\cdot$“ genau dann ein Körper ist, wenn gilt:

(K1) $(K, +)$ ist eine abelsche Gruppe (deren neutrales Element wir mit 0 bezeichnen);

(K2) $(K \setminus \{0\}, \cdot)$ ist ebenfalls eine abelsche Gruppe (deren neutrales Element wir mit 1 bezeichnen);

(K3) für alle $a, b, c \in K$ gilt die Distributivität $(a+b)c = ac + bc$.

(c) In einem Ring $R \neq \{0\}$ ist 0 nach Lemma 7.5 immer ein Nullteiler und nie eine Einheit. Umgekehrt ist 1 immer eine Einheit und nie ein Nullteiler.

Das folgende Lemma fasst die wichtigsten Eigenschaften von Einheiten und Nullteilern zusammen.

Lemma 7.8. *Es sei $R \neq \{0\}$ ein Ring.*

(a) *Die Menge R^* aller Einheiten von R bildet mit der Multiplikation eine Gruppe. Sie wird daher auch die **Einheitengruppe** von R genannt.*

(b) *Ist $a \in R$ eine Einheit, so ist a kein Nullteiler. Insbesondere ist also jeder Körper ein Integritätsring.*

(c) ***(Kürzungsregel)*** *Es seien $a,b,c \in R$ und c kein Nullteiler. Dann gilt*

$$ac = bc \quad \text{genau dann wenn} \quad a = b.$$

Insbesondere gilt diese Kürzungsregel in einem Integritätsring also für alle $c \neq 0$.

Beweis.

(a) Zunächst einmal ist die Multiplikation wirklich eine Verknüpfung auf R^*, denn ist a invertierbar mit Inversem a^{-1} und b invertierbar mit Inversem b^{-1}, so ist auch ab invertierbar mit Inversem $a^{-1}b^{-1}$. Weiterhin erfüllt $(R^*, \cdot)$ die Gruppenaxiome aus Definition 1.1 (a):

(G1) Dies folgt aus Teil (R2) der Definition 7.1 (a).

(G2) Das Element 1 ist natürlich immer eine Einheit und damit das neutrale Element in R^*.

(G3) Ist $a \in R^*$ und damit $a^{-1} \cdot a = 1$, so besagt dieselbe Gleichung, dass auch $a^{-1} \in R^*$ gilt.

(b) Es sei a eine Einheit, d. h. es existiert ein multiplikatives Inverses $a^{-1} \in R$. Ist nun $b \in R$ mit $ab = 0$, so ergibt sich durch Multiplikation mit a^{-1} sofort $b = 0$. Also kann a kein Nullteiler sein.

Ist R ein Körper, sind also alle Elemente außer 0 Einheiten, so kann damit keines dieser Elemente ein Nullteiler sein. Also ist R dann ein Integritätsring.

(c) Die Richtung „$\Leftarrow$“ ist offensichtlich. Für die andere Richtung „$\Rightarrow$“ gelte nun $ac = bc$. Dann ist aber $(a-b)c = 0$, und da c kein Nullteiler ist, folgt daraus sofort $a - b = 0$, also $a = b$. □

Beispiel 7.9.

(a) Offensichtlich ist $\mathbb{Z}^* = \{1, -1\}$, der Ring $\mathbb{Z}$ ist also kein Körper. Die 0 ist aber der einzige Nullteiler in $\mathbb{Z}$, d. h. $\mathbb{Z}$ ist ein Integritätsring.

(b) $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper, da alle Elemente $a \neq 0$ ein multiplikatives Inverses $\frac{1}{a}$ besitzen. Wie in Lemma 7.8 (b) sind sie damit auch Integritätsringe.

(c) Im $\mathbb{Z}_6$ (wie in Beispiel 7.4 (b)) ist $\overline{2}$ ein Nullteiler, denn es ist $\overline{3} \neq \overline{0}$, aber $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$. Also ist $\mathbb{Z}_6$ kein Integritätsring, und damit nach Lemma 7.8 (b) auch kein Körper. In der Tat sieht man auch schnell direkt, dass es kein $\overline{n} \in \mathbb{Z}_6$ mit $\overline{2} \cdot \overline{n} = \overline{1}$ gibt, und $\overline{2}$ somit keine Einheit in $\mathbb{Z}_6$ ist.

Die Gleichung $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0} = \overline{2} \cdot \overline{0}$ zeigt auch, dass die Kürzungsregel für den Nullteiler $\overline{2}$ hier nicht gilt, denn es ist ja $\overline{3} \neq \overline{0}$.

08

Wie man an diesem Beispiel vielleicht schon erahnen kann, können wir sogar exakt angeben, für welche n der Ring $\mathbb{Z}_n$ ein Integritätsring bzw. ein Körper ist:

Satz 7.10. *Es sei $n \in \mathbb{N}_{>1}$. Dann sind die folgenden Aussagen äquivalent:*

(a) *$\mathbb{Z}_n$ ist ein Körper.*

(b) *$\mathbb{Z}_n$ ist ein Integritätsring.*

(c) *n ist eine Primzahl.*

Beweis.

(a) $\Rightarrow$ (b): Dies folgt sofort aus Lemma 7.8 (b).

(b) $\Rightarrow$ (c): Angenommen, n wäre keine Primzahl. Dann gäbe es eine Faktorisierung $n = p \cdot q$ für gewisse $1 < p, q < n$, und es wäre in $\mathbb{Z}_n$

$$\overline{p} \cdot \overline{q} = \overline{n} = \overline{0},$$

obwohl $\overline{p}$ und $\overline{q}$ nicht gleich $\overline{0}$ sind. Dies ist ein Widerspruch zur Annahme, dass $\mathbb{Z}_n$ ein Integritätsring ist.

(c) $\Rightarrow$ (a): Es sei n eine Primzahl und $a \in \{1,\dots,n-1\}$; wir müssen zeigen, dass $\overline{a}$ eine Einheit in $\mathbb{Z}_n$ ist. Die Ordnung der vom Element $\overline{a}$ erzeugten additive Untergruppe

$$\langle \overline{a} \rangle = \{k \cdot \overline{a} : k \in \mathbb{Z}\} = \{\overline{k} \cdot \overline{a} : k \in \mathbb{Z}\}$$

von $\mathbb{Z}_n$ muss dann nach dem Satz 5.10 von Lagrange als Teiler von n gleich 1 oder n sein. Da aber bereits die beiden verschiedenen Elemente $\overline{0}$ und $\overline{a}$ in dieser Untergruppe liegen, ist $|\langle \overline{a} \rangle| = 1$ ausgeschlossen, d. h. es ist $|\langle \overline{a} \rangle| = n$ und damit $\langle \overline{a} \rangle = \mathbb{Z}_n$ schon der gesamte Ring. Insbesondere ist also $\overline{1} \in \langle \overline{a} \rangle$, d. h. es gibt ein $k \in \mathbb{Z}$ mit $\overline{k} \cdot \overline{a} = \overline{1}$. Also ist $\overline{a}$ eine Einheit in $\mathbb{Z}_n$. □

Notation 7.11. Ist p eine Primzahl, so ist für den Körper $\mathbb{Z}_p$ in der Literatur auch die Bezeichnung $\mathbb{F}_p$ üblich — die Bezeichnung kommt vom englischen Wort „field", das in der Mathematik „Körper" bedeutet. Wir werden in diesem Skript jedoch weiterhin die Bezeichnung $\mathbb{Z}_p$ verwenden.

Beispiel 7.12. Im Körper $\mathbb{Z}_7$ ist $\overline{5}$ das multiplikative Inverse zu $\overline{3}$, also $\overline{3}^{-1} = \overline{5}$, denn $\overline{5} \cdot \overline{3} = \overline{15} = \overline{1}$. Man kann also leicht nachprüfen, dass ein gegebenes Element von $\mathbb{Z}_n$ das multiplikative Inverse eines anderen ist. Beachte aber, dass der Beweis von Satz 7.10 *nicht konstruktiv* ist, d. h. er sichert nur die Existenz von multiplikativ inversen Elementen im Körper $\mathbb{Z}_n$ für eine Primzahl n, sagt aber nicht, wie man dieses Inverse konkret bestimmen kann, wenn man nicht alle möglichen Elemente von $\mathbb{Z}_n$ durchprobieren möchte. Wir werden in Folgerung 10.31 noch ein explizites Verfahren kennenlernen, mit dem man Inverse in $\mathbb{Z}_n$ ohne Ausprobieren berechnen kann.

Bemerkung 7.13. Ist p eine Primzahl und $\mathbb{Z}_p$ damit nach Satz 7.10 ein Körper, so ist die Einheitengruppe dieses Körpers natürlich $(\mathbb{Z}_p^*, \cdot) = (\mathbb{Z}_p \backslash \{0\}, \cdot)$. Man kann nun zeigen, dass diese Gruppe zyklisch ist — und damit, da sie ja $p-1$ Elemente besitzt, nach Satz 6.21 (a) isomorph zu $(\mathbb{Z}_{p-1}, +)$ sein muss. Der Beweis dieser Aussage ist mit unseren momentanen Mitteln noch nicht möglich; er wird typischerweise in der Vorlesung „Elementare Zahlentheorie" behandelt.

Es gibt also ein $a \in \mathbb{Z}$, so dass

$$\mathbb{Z}_p^* = \langle \overline{a} \rangle = \{\overline{a}^k : k \in \mathbb{Z}\} = \{\overline{a}^k : k = 0,\dots,p-2\},$$

und damit dann zu jedem $\overline{b} \in \mathbb{Z}_p^*$ ein eindeutiges $k \in \{0,\dots,p-2\}$ mit $\overline{b} = \overline{a}^k$. Die folgende Tabelle zeigt ein konkretes Beispiel: In $\mathbb{Z}_7$ können wir z. B. $\overline{a} = \overline{3}$ wählen und erhalten dann jedes Element von $\mathbb{Z}_7 \backslash \{0\}$ auf eindeutige Art als ein $\overline{3}^k$ für ein $k \in \{0,\dots,5\}$.

k	0	1	2	3	4	5
$\overline{3}^k$	$\overline{1}$	$\overline{3}$	$\overline{2}$	$\overline{6}$	$\overline{4}$	$\overline{5}$

Im Gegensatz zur Inversenbildung in $\mathbb{Z}_p$ (siehe Beispiel 7.12) gibt es allerdings sowohl zur Bestimmung eines solchen a als auch zur anschließenden Berechnung von k aus $\overline{b} = \overline{a}^k$ in der Regel kein anderes Verfahren als das Ausprobieren aller Möglichkeiten. Wir hatten in Beispiel 0.2 der Einleitung schon gesehen, wie sich diese Tatsache für kryptographische Zwecke ausnutzen lässt.

Aufgabe 7.14.

(a) Zeige, dass $\overline{n-1}$ in $\mathbb{Z}_n$ für alle $n \in \mathbb{N}_{\geq 2}$ eine Einheit ist.

(b) Berechne $\overline{5^{12345}}$ in $\mathbb{Z}_7$.

(c) Es sei $a \in \mathbb{Z}_{11}$. Bestimme (in Abhängigkeit von a) alle $x, y \in \mathbb{Z}_{11}$, die das Gleichungssystem

$$\begin{aligned} \overline{5}x + \overline{6}y &= \overline{4} \\ \text{und} \qquad \overline{8}x + \overline{9}y &= a \end{aligned}$$

in $\mathbb{Z}_{11}$ erfüllen.

Aufgabe 7.15. Es seien R und S zwei Ringe. Zeige, dass $(R \times S)^* \cong R^* \times S^*$.

Aufgabe 7.16. Zeige, dass in einem endlichen Ring $R \neq \{0\}$ jedes Element eine Einheit oder ein Nullteiler ist.

Insbesondere ist jeder endliche Integritätsring $R \neq \{0\}$ also bereits ein Körper, so dass zusammen mit Lemma 7.8 (b) für endliche Ringe (ungleich dem Nullring) die Begriffe „Integritätsring“ und „Körper“ übereinstimmen — was wir für den speziellen Fall der Ringe $\mathbb{Z}_n$ ja auch schon in Satz 7.10 gesehen hatten.

Aufgabe 7.17 (Satz von Wilson). Zeige, dass $(p-1)! := \overline{1} \cdot \ldots \cdot \overline{p-1} = \overline{-1}$ in $\mathbb{Z}_p$ für jede Primzahl $p > 2$.

Aufgabe 7.18. Es sei K ein Körper. Zeige, dass $(K,+)$ als Gruppe dann niemals isomorph zu $(K\backslash\{0\},\cdot)$ sein kann.

Aufgabe 7.19. Es sei R ein Ring mit genau 5 Einheiten. Man zeige:

(a) In R gilt $-1 = 1$.

(b) Für jedes $a \in R^*$ gilt $(1+a+a^2)^3 = a^3$.

(c) Für jedes $a \in R^*$ gilt $1+a+a^2 = a$.

(d) Es gibt R gar nicht.

Hinweis: R^* ist bekanntlich eine Gruppe.

Nachdem wir nun Ringe (und Körper) eingeführt haben, wollen wir für diese Strukturen kurz die gleichen Konstruktionen einführen, wie wir sie für Gruppen in den vorangegangenen Kapiteln betrachtet haben: zuerst die Unterstrukturen (also Teilmengen von Ringen, die selbst wieder Ringe sind), dann die Morphismen (als Abbildungen, die die Ringstruktur erhalten), und schließlich im nächsten Kapitel die Faktorstrukturen (also das „Herausteilen“ von Äquivalenzrelationen). Alle diese Konstruktionen verlaufen mehr oder weniger parallel zu denen von Gruppen und sollten euch daher auch helfen, die generelle Vorgehensweise dabei besser zu verstehen.

Beginnen wir also mit den Unterstrukturen. Die Definition eines Unterrings verläuft ganz analog zu der einer Untergruppe in Definition 3.1:

Definition 7.20 (Unterringe)**.** Eine Teilmenge S eines Ringes R heißt **Unterring** von R, wenn S „mit der gleichen 0 und 1 wie in R und denselben Verknüpfungen selbst wieder ein Ring ist“, d. h. wenn gilt:

(a) $1 \in S$;

(b) für alle $a,b \in S$ ist $a+b \in S$ und $ab \in S$ (d. h. die Verknüpfungen „$+$“ und „$\cdot$“ in R lassen sich auf Verknüpfungen in S einschränken);

(c) $(S,+,\cdot)$ ist ein Ring.

Man verwendet hierfür genau wie bei Untergruppen oft die Schreibweise $S \leq R$, muss dabei aber natürlich darauf achten, dass aus dem Zusammenhang klar wird, ob Untergruppen oder Unterringe gemeint sind.

Bemerkung 7.21. Ein Unterring S eines Ringes R ist nach Definition natürlich insbesondere auch eine additive Untergruppe von R. Nach dem Untergruppenkriterium (U2) aus Satz 3.3 muss S dann also automatisch das additive neutrale Element $0 \in R$ enthalten. Wir mussten in Definition 7.20 also nicht explizit auch $0 \in S$ fordern, da dies schon aus den anderen Eigenschaften folgt.

Für das Element $1 \in S$ gilt dies jedoch nicht: Hätten wir in Definition 7.20 nicht explizit $1 \in S$ gefordert, so wäre z. B. der Nullring ein Unterring von $\mathbb{Z}$. Der Nullring besäße dann zwar auch ein Einselement (nämlich 0), dies wäre aber nicht das gleiche wie im Gesamtring $\mathbb{Z}$. Die Forderung (a) in Definition 7.20 schließt solche merkwürdigen Fälle aus.

Beispiel 7.22.

(a) Natürlich ist $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

(b) Es sei S ein Unterring von $\mathbb{Z}$. Dann muss S zunächst auch eine additive Untergruppe von $\mathbb{Z}$, also nach Satz 3.17 von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}$ sein. Weiterhin muss S nach Definition 7.20 (a) aber auch das Element 1 enthalten, was nur für $n = 1$ (und somit $S = \mathbb{Z}$) der Fall ist. Also ist der triviale Unterring $\mathbb{Z}$ der einzige Unterring von $\mathbb{Z}$.

Analog zum Untergruppenkriterium aus Satz 3.3 gibt es auch ein Unterringkriterium, an dem man sieht, dass in Definition 7.20 (c) die Überprüfung der meisten Ringaxiome überflüssig ist:

Lemma 7.23 (Unterringkriterium). *Eine Teilmenge S eines Ringes R ist genau dann ein Unterring, wenn gilt:*

(1) $1 \in S$;

(2) *für alle $a, b \in S$ ist $a + b \in S$ und $ab \in S$;*

(3) *für alle $a \in S$ ist $-a \in S$.*

Beweis.

„⇒“: Ist S ein Unterring von R, so gelten nach Definition natürlich (1) und (2). Außerdem ist S dann eine additive Untergruppe, also gilt (3) nach dem Untergruppenkriterium (U3).

„⇐“: Erfüllt umgekehrt S die Bedingungen (1), (2) und (3) des Unterringkriteriums, so gelten natürlich auch die Eigenschaften (a) und (b) der Definition 7.20. Weiterhin ist $-1 \in S$ nach (1) und (3), und damit auch $0 = 1 + (-1) \in S$ nach (2). Also erfüllt S bezüglich der Addition alle Bedingungen des Untergruppenkriteriums und ist somit eine Untergruppe von R, erfüllt also (R1). Weiterhin gilt (R4) für S nach (1). Die anderen drei Bedingungen (R2), (R3) und (R5) gelten natürlich in S, weil sie auch in R gelten. Damit ist $(S, +, \cdot)$ ein Ring, nach Definition 7.20 also auch ein Unterring von $(R, +, \cdot)$. □

Aufgabe 7.24. Es sei $a \in \mathbb{C}$ mit $a^2 \in \mathbb{Z}$. Wir definieren

$$\mathbb{Z}[a] := \{m + na : m, n \in \mathbb{Z}\} \subset \mathbb{C}.$$

(a) Zeige, dass $\mathbb{Z}[a]$ ein Ring ist.

(b) Bestimme die Einheiten von $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$.

(Hinweis zu (b): Für eine komplexe Zahl $z \in \mathbb{Z}[a]$ betrachte man das Betragsquadrat $|z|^2$. Aus den Grundlagen der Mathematik dürft ihr verwenden, dass $|zw|^2 = |z|^2\,|w|^2$ für alle $z, w \in \mathbb{C}$ gilt.)

Nach den Unterstrukturen wollen wir — wie bei Gruppen — als Nächstes die Morphismen betrachten. Wie erwartet sollen dies einfach die Abbildungen zwischen Ringen sein, die alle Strukturen (also die 0, die 1, die Addition und die Multiplikation) erhalten. Wir definieren die Konzepte von Kern und Bild eines solchen Morphismus sowie von Isomorphismen gleich mit — die Definitionen sind hier völlig analog zu denen von Gruppen.

Definition 7.25 (Morphismen von Ringen)**.**

(a) Eine Abbildung $f\colon R \to S$ zwischen zwei Ringen heißt ein **Morphismus** (oder **Homomorphismus** oder **Ringhomomorphismus**), wenn $f(1) = 1$ ist und für alle $a, b \in R$

$$f(a+b) = f(a) + f(b) \quad \text{und} \quad f(a \cdot b) = f(a) \cdot f(b)$$

gilt. Sind R und S Körper, so heißt ein solches f auch **Körperhomomorphismus**.

(b) Ein bijektiver Morphismus heißt **Isomorphismus** (bzw. auch **Ringisomorphismus** oder **Körperisomorphismus**). Zwei Ringe (bzw. Körper) heißen **isomorph**, wenn es einen Isomorphismus zwischen ihnen gibt.

(c) Ist $f\colon R \to S$ ein Ringhomomorphismus, so heißt

$$\operatorname{Im} f = f(R) = \{f(a) : a \in R\} \subset S \quad \text{das } \textbf{Bild} \text{ von } f$$

$$\text{und} \quad \operatorname{Ker} f = f^{-1}(\{0\}) = \{a \in R : f(a) = 0\} \subset R \quad \text{der } \textbf{Kern} \text{ von } f$$

(die Definitionen sind also exakt dieselben wie bei Gruppen, wenn man f als Gruppenhomomorphismus bezüglich der Addition auffasst).

Bemerkung 7.26. Jeder Ringhomomorphismus ist nach Definition auch ein Gruppenhomomorphismus bezüglich der Addition. Aus Lemma 4.4 (a) folgt also sofort, dass ein Ringhomomorphismus $f\colon R \to S$ stets $f(0) = 0$ erfüllen muss.

Im Gegensatz dazu gibt es bei der Bedingung $f(1) = 1$ wie schon bei der Definition von Ringen und Unterringen in der Literatur zwei Varianten: In manchen Büchern wird diese Bedingung unserer Definition 7.25 (a) weggelassen. Die Nullabbildung $f\colon R \to S$, $a \mapsto 0$ wäre dann ein Morphismus; nach unserer Definition ist sie keiner.

Beispiel 7.27. Die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $f(n) = (n,n)$ ist offensichtlich ein Ringhomomorphismus. In der Tat ist dies sogar der einzige Ringhomomorphismus von $\mathbb{Z}$ nach $\mathbb{Z} \times \mathbb{Z}$: Genau wie in Aufgabe 4.7 (a) sieht man, dass die einzigen *Gruppenhomomorphismen* bezüglich der Addition die Abbildungen $f(n) = (an, bn)$ für gewisse $a, b \in \mathbb{Z}$ sind — und für einen *Ringhomomorphismus* muss dann wegen $f(1) = (1,1)$ natürlich $a = b = 1$ gelten.

Bemerkung 7.28 (Eigenschaften von Ringhomomorphismen)**.** Genau wie im Fall von Gruppen zeigt man die folgenden beiden einfachen Eigenschaften von Ringhomomorphismen:

(a) Ist $f\colon R \to S$ ein Ringisomorphismus, so ist auch die Umkehrabbildung $f^{-1}\colon S \to R$ ein Ringisomorphismus (vgl. Lemma 4.4 (c)). Isomorphismen spielen in der Theorie der Ringe dieselbe anschauliche Bedeutung wie bei den Gruppen: Ringe, zwischen denen ein Isomorphismus existiert, können als „gleichwertig“ angesehen und miteinander identifiziert werden.

(b) Sind $f\colon R \to S$ und $g\colon S \to T$ Ringhomomorphismen, so ist auch die Verkettung $g \circ f\colon R \to T$ ein Ringhomomorphismus (vgl. Lemma 4.4 (d)).

Aufgabe 7.29. Beweise explizit die Aussagen von Bemerkung 7.28.

Bemerkung 7.30 (Bilder und Kerne von Ringhomomorphismen)**.** Für einen Gruppenhomomorphismus $f\colon G \to H$ hatten wir in Definition 4.14 gesehen, dass $\operatorname{Ker} f$ und $\operatorname{Im} f$ Untergruppen von G bzw. H sind. Für einen Ringhomomorphismus $f\colon R \to S$ ist die Situation etwas anders:

(a) Das Bild $\operatorname{Im} f$ ist ein Unterring von S, wie wir einfach anhand der Unterringkriterien aus Lemma 7.23 nachprüfen können:

(1) nach Definition 7.25 (a) ist $f(1) = 1$ und damit $1 \in \operatorname{Im} f$;

(2) für $a, b \in \operatorname{Im} f$, also $a = f(u)$ und $b = f(v)$ für gewisse $u, v \in R$, gilt sowohl $a + b = f(u) + f(v) = f(u+v) \in \operatorname{Im} f$ als auch $ab = f(u)f(v) = f(uv) \in \operatorname{Im} f$;

(3) für $a \in \operatorname{Im} f$, also $a = f(u)$ für ein $u \in R$, gilt $-a = -f(u) = f(-u) \in \operatorname{Im} f$.

(b) Der Kern $\operatorname{Ker} f$ ist hingegen (falls S nicht der Nullring ist) *nie* ein Unterring von R, denn es gilt ja $f(1) = 1$ nach Definition 7.25 (a) und damit $1 \notin \operatorname{Ker} f$. In der Tat bildet der Kern eines Ringhomomorphismus eine andere Art von Unterstruktur — ein sogenanntes *Ideal*. Diesen Begriff werden wir im nächsten Kapitel kennenlernen (siehe Definition 8.1 und Lemma 8.4).

Aufgabe 7.31. Man zeige:

(a) Ist $f\colon K \to R$ ein Ringhomomorphismus von einem Körper K in einen Ring $R \neq \{0\}$, so ist f injektiv.

(b) Von den drei Ringen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind keine zwei isomorph zueinander.

Aufgabe 7.32. Bestimme alle Ringhomomorphismen von $\mathbb{Z}_{12}$ nach $\mathbb{Z}_8$ und von $\mathbb{Z}_{12}$ nach $\mathbb{Z}_6$.

8. Ideale und Faktorringe

Im letzten Kapitel haben wir Ringe eingeführt und (analog zur Theorie von Gruppen) Unterringe und Ringhomomorphismen untersucht. Es fehlen uns allerdings noch die Faktorstrukturen — d. h. wir müssen noch sehen, wie man aus einem Ring analog zu den Faktorgruppen in Kapitel 6 geeignete Unterstrukturen herausteilen kann. Ein Beispiel dafür haben wir bereits gesehen: In Beispiel 7.4 (b) hatten wir gezeigt, dass $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ein Ring ist. In diesem Fall hatten wir also durch Herausteilen der Untergruppe (bzw. des Normalteilers) $n\mathbb{Z}$ bereits eine Ringstruktur erhalten — insbesondere war also neben der Addition $\overline{a}+\overline{b} := \overline{a+b}$ auch die Multiplikation $\overline{a}\cdot\overline{b} := \overline{ab}$ wohldefiniert.

Wir wollen nun untersuchen, ob dies immer der Fall ist: Es sei R ein Ring und S eine additive Untergruppe von R. Da $(R,+)$ nach der Ringeigenschaft (R1) eine abelsche Gruppe ist, ist $(S,+)$ dann nach Beispiel 6.6 (a) sogar ein Normalteiler von $(R,+)$. Wir können nach Satz 6.13 also in jedem Fall schon einmal die Faktor*gruppe* $(R/S,+)$ bilden, d. h. wir haben auf R/S bereits eine wohldefinierte (und kommutative) Addition.

Leider bedeutet dies jedoch im Allgemeinen nicht, dass wir mit der Vorschrift $\overline{a}\cdot\overline{b} := \overline{ab}$ dann auch eine wohldefinierte Multiplikation auf R/S erhalten: Für $R = \mathbb{R}$ und $S = \mathbb{Z}$ ist z. B. $\overline{1} = \overline{2}$ in $\mathbb{R}/\mathbb{Z}$ wegen $2-1 \in \mathbb{Z}$, aber $\overline{\frac{1}{2}\cdot 1} = \overline{\frac{1}{2}} \neq \overline{1} = \overline{\frac{1}{2}\cdot 2}$ wegen $1-\frac{1}{2} \notin \mathbb{Z}$, so dass die Multiplikation von $\overline{\frac{1}{2}}$ mit $\overline{1} = \overline{2}$ also nicht wohldefiniert ist. Da $\mathbb{Z}$ sogar ein Unterring von $\mathbb{R}$ ist, sehen wir an diesem Beispiel auch schon, dass wir Unterringe auch nicht herausteilen können.

Wir müssen an unsere herausgeteilte Menge S also andere Bedingungen stellen. Wie im Fall von Faktorgruppen geben wir auch hier die nötigen Bedingungen zunächst in Form einer Definition an und zeigen später, dass wir damit wirklich das Gewünschte erreichen.

Definition 8.1 (Ideale)**.** Eine Teilmenge I eines Ringes R heißt ein **Ideal**, wenn gilt:

(I1) $0 \in I$;

(I2) für alle $a,b \in I$ ist $a+b \in I$;

(I3) für alle $a \in I$ und $x \in R$ ist $a\cdot x \in I$.

Ist I ein Ideal von R, so schreiben wir dies als $I \trianglelefteq R$, sofern keine Verwechslungsgefahr mit dem Begriff des Normalteilers aus Definition 6.3 besteht. (Die gleiche Bezeichnung kommt daher, dass sich Ideale in Ringen analog zu Normalteilern in Untergruppen als diejenigen Teilmengen herausstellen werden, mit denen eine Faktorstruktur definiert werden kann.)

Bemerkung 8.2.

(a) Jedes Ideal I eines Ringes R ist eine additive Untergruppe von R: Die Eigenschaften (U1) und (U2) des Untergruppenkriteriums aus Satz 3.3 sind genau die Bedingungen (I2) und (I1) in Definition 8.1, und die Eigenschaft (U3) folgt aus (I3) mit $x = -1$. Da $(R,+)$ außerdem nach Definition eines Ringes abelsch ist, ist jedes Ideal von R nach Beispiel 6.6 (a) sogar ein Normalteiler bezüglich der Addition in R.

(b) Ist I ein Ideal in einem Ring R mit $1 \in I$, so folgt aus Eigenschaft (I3) von Definition 8.1 mit $a = 1$ sofort $x \in I$ für alle $x \in R$, d. h. es ist dann bereits $I = R$. Da jeder Unterring die 1 enthalten muss, schließen sich Unterringe und Ideale also fast vollständig aus: Die einzige Teilmenge von R, die gleichzeitig ein Unterring und ein Ideal von R ist, ist R selbst. Unterringe und Ideale sind in diesem Sinne also „sehr unterschiedliche“ Objekte.

Beispiel 8.3.

(a) Im Ring $R = \mathbb{Z}$ ist $I = n\mathbb{Z}$ für $n \in \mathbb{N}$ ein Ideal:

(I1) ist offensichtlich;

(I2) für zwei Zahlen $kn, ln \in n\mathbb{Z}$ (mit $k,l \in \mathbb{Z}$) ist auch $kn+ln = (k+l)n \in n\mathbb{Z}$;

(I3) für $kn \in n\mathbb{Z}$ und $x \in \mathbb{Z}$ (mit $k,x \in \mathbb{Z}$) ist auch $kn \cdot x = (kx) \cdot n \in n\mathbb{Z}$.

Da jedes Ideal eines Ringes nach Bemerkung 8.2 (a) auch eine additive Untergruppe sein muss und diese im Ring $\mathbb{Z}$ nach Satz 3.17 alle von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}$ sind, sind dies auch bereits alle Ideale von $\mathbb{Z}$. Insbesondere stimmen Untergruppen und Ideale im Ring $\mathbb{Z}$ also überein. Dies ist aber nicht in jedem Ring so: So ist z. B. $\mathbb{Z}$ eine additive Untergruppe von $\mathbb{Q}$, aber nach Bemerkung 8.2 (b) kein Ideal (denn es ist ja $1 \in \mathbb{Z}$, aber $\mathbb{Z} \neq \mathbb{Q}$).

(b) In einem Ring R sind $\{0\}$ und R offensichtlich stets Ideale von R. Sie werden die **trivialen Ideale** von R genannt.

(c) Ist K ein Körper, so sind die trivialen Ideale $\{0\}$ und K aus (b) bereits die einzigen Ideale von K: Enthält ein Ideal $I \trianglelefteq K$ nämlich ein beliebiges Element $a \neq 0$, so enthält es nach Eigenschaft (I3) auch $1 = a \cdot a^{-1}$ und ist nach Bemerkung 8.2 (b) damit gleich K.

09

Wir hatten schon erwähnt, dass Ideale in Ringen in gewissem Sinne analog zu Normalteilern in Gruppen sind. Da Kerne von Gruppenhomomorphismen nach Lemma 6.7 Normalteiler sind, ist es daher nicht weiter erstaunlich, dass Kerne von Ringhomomorphismen Ideale sind:

Lemma 8.4. *Ist $f\colon R \to S$ ein Ringhomomorphismus, so ist* $\operatorname{Ker} f$ *ein Ideal von R.*

Beweis. Wir prüfen die Idealeigenschaften nach:

(I1) Es ist $f(0) = 0$ nach Bemerkung 7.26 und damit $0 \in \operatorname{Ker} f$.

(I2) Für $a,b \in \operatorname{Ker} f$ ist $f(a+b) = f(a)+f(b) = 0+0 = 0$ und damit $a+b \in \operatorname{Ker} f$.

(I3) Für $a \in \operatorname{Ker} f$ und $x \in R$ ist $f(ax) = f(a)f(x) = 0 \cdot f(x) = 0$ und damit $ax \in \operatorname{Ker} f$. □

Als wir Untergruppen in Kapitel 3 untersucht haben, haben wir gesehen, dass man zu jeder Teilmenge M einer Gruppe G eine davon erzeugte Untergruppe $\langle M \rangle$ konstruieren kann, die man sich vorstellen kann als die „kleinste Untergruppe von G, die M enthält“. Wir hatten diese von M erzeugte Untergruppe zwar elegant, aber recht abstrakt definiert als Durchschnitt aller Untergruppen, die M enthalten (siehe Definition 3.11). Später hatten wir in Aufgabe 3.14 dann eine Darstellung für $\langle M \rangle$ gesehen, die zwar explizit war, aber dennoch so kompliziert, dass sie insbesondere für nicht-abelsche Gruppen meistens nicht wirklich zur Berechnung von $\langle M \rangle$ geeignet ist.

Auch für Ideale gibt es eine ähnliche Konstruktion, mit der man einer Teilmenge M eines Ringes R ein „kleinstes Ideal, das M enthält“ zuordnen kann. Man könnte dies analog zum Fall von Untergruppen als Schnitt über alle Ideale definieren, die M enthalten (siehe Aufgabe 8.7) — im Fall von Idealen ist jedoch die zu Aufgabe 3.14 analoge explizite Formel so einfach und nützlich, dass wir sie hier als Definition verwenden wollen.

Definition 8.5 (Erzeugte Ideale)**.** Es sei M eine beliebige Teilmenge eines Ringes R. Dann heißt

$$\langle M \rangle := \{a_1x_1 + \cdots + a_nx_n : n \in \mathbb{N}; a_1, \ldots, a_n \in M; x_1, \ldots, x_n \in R\},$$

das von M **erzeugte Ideal**. Man sagt auch, dass $\langle M \rangle$ aus den endlichen *Linearkombinationen* von Elementen aus M mit Koeffizienten in R besteht.

Ist $M = \{a_1, \ldots, a_n\}$ eine endliche Menge, so schreibt man statt $\langle M \rangle = \langle \{a_1, \ldots, a_n\} \rangle$ in der Regel auch $\langle a_1, \ldots, a_n \rangle$.

Beachte, dass wir wegen der Analogie der Konstruktion hier die gleiche Bezeichnung wie für die von M erzeugte Untergruppe in Definition 3.11 verwendet haben — genauso wie wir das Symbol „$\leq$“ sowohl für Untergruppen als auch Unterringe benutzt haben. Falls eine Verwechslungsgefahr besteht, ist für das von M erzeugte Ideal in der Literatur statt $\langle M \rangle$ oft auch die Bezeichnung (M) oder $\langle M \rangle_R$ üblich.

Bevor wir Beispiele dieser Konstruktion betrachten, sollten wir uns zunächst davon überzeugen, dass $\langle M \rangle$ wirklich ein Ideal ist, und in der Tat auch interpretiert werden kann als das kleinste Ideal, das M enthält. Wir zeigen dazu für $\langle M \rangle$ die zu Lemma 3.12 analogen Eigenschaften.

Lemma 8.6. *Für jede Teilmenge M eines Ringes R gilt:*

(a) $\langle M \rangle$ *ist ein Ideal, das M enthält.*

(b) *Ist I ein beliebiges Ideal, das M enthält, so gilt bereits $\langle M \rangle \subset I$.*

$\langle M \rangle$ *ist damit also das kleinste Ideal, das M enthält.*

Beweis.

(a) $\langle M \rangle$ erfüllt (I1), da in Definition 8.5 auch $n = 0$ erlaubt ist und damit die leere Summe, also 0, in $\langle M \rangle$ enthalten ist. Die Eigenschaft (I2) ist offensichtlich. Für (I3) seien $a \in \langle M \rangle$ und $x \in R$, also $a = a_1x_1 + \cdots + a_nx_n$ für gewisse $n \in \mathbb{N}$, $a_1, \ldots, a_n \in M$ und $x_1, \ldots, x_n \in R$. Dann ist auch $ax = a_1(xx_1) + \cdots + a_n(xx_n) \in \langle M \rangle$. Also ist $\langle M \rangle$ ein Ideal. Weiterhin ist M natürlich in $\langle M \rangle$ enthalten, denn für $a \in M$ ist $a = a \cdot 1 \in \langle M \rangle$.

(b) Es seien $n \in \mathbb{N}$, $a_1, \ldots, a_n \in M$ und $x_1, \ldots, x_n \in R$. Ist I ein beliebiges Ideal mit $M \subset I$, so enthält I also $a_1x_1, \ldots, a_nx_n$ nach Eigenschaft (I3), und damit auch $a_1x_1 + \cdots + a_nx_n$ nach (I2) (bzw. nach (I1) im Fall $n = 0$). Also gilt $\langle M \rangle \subset I$. □

Aufgabe 8.7. Es sei M eine Teilmenge eines Ringes R. Zeige, dass für das von M erzeugte Ideal $\langle M \rangle$ die Formel

$$\langle M \rangle = \bigcap_{\substack{I \trianglelefteq R \\ \text{mit } I \supset M}} I$$

gilt, also die analoge Formel zu unserer Definition 3.11 für die von einer Teilmenge einer Gruppe erzeugte Untergruppe.

Beispiel 8.8.

(a) Besteht die Menge M in Definition 8.5 nur aus einem Element a, so ist offensichtlich

$$\langle a \rangle = \{ax : x \in R\}$$

die „Menge aller Vielfachen von a“. Insbesondere gilt in $R = \mathbb{Z}$ also für $n \in \mathbb{N}$

$$\langle n \rangle = \{nx : x \in \mathbb{Z}\} = n\mathbb{Z},$$

d. h. hier stimmt das von einem Element erzeugte Ideal mit der von ihm erzeugten Untergruppe in Beispiel 3.13 (a) überein.

(b) Im Ring $R = \mathbb{Z} \times \mathbb{Z}$ ist das vom Element $(2,2)$ erzeugte Ideal

$$\langle (2,2) \rangle = \{(2,2) \cdot (m,n) : m,n \in \mathbb{Z}\} = \{(2m,2n) : m,n \in \mathbb{Z}\},$$

während die von diesem Element erzeugte (additive) Untergruppe nach Beispiel 3.13 (a) gleich

$$\{n \cdot (2,2) : n \in \mathbb{Z}\} = \{(2n,2n) : n \in \mathbb{Z}\}$$

ist.

(c) Wir wissen aus Beispiel 8.3 (c) bereits, dass ein Körper nur die beiden trivialen Ideale besitzt. In der Tat gilt hiervon auch die Umkehrung: Ist $R \neq \{0\}$ ein Ring, in dem $\{0\}$ und R die einzigen Ideale sind, so muss von jedem Element $a \neq 0$ das erzeugte Ideal $\langle a \rangle$ bereits gleich R sein und damit insbesondere die Eins enthalten. Nach (a) ist dann aber $ax = 1$ für ein $x \in R$, d. h. a ist invertierbar. Also ist R dann ein Körper.

Aufgabe 8.9. Ist I ein Ideal in einem Ring R, so heißt

$$\sqrt{I} := \{a \in R : a^n \in I \text{ für ein } n \in \mathbb{N}\} \quad \subset R$$

das **Radikal** von I.

(a) Zeige, dass $\sqrt{I}$ wieder ein Ideal von R ist.

(b) Man zeige: Ist $a \in \sqrt{\langle 0 \rangle}$, so ist $1 + a$ eine Einheit in R.

(c) Berechne das Ideal $\sqrt{180\mathbb{Z}}$ in $\mathbb{Z}$.

Wie bereits angekündigt sind Ideale in Ringen besonders deswegen interessant, weil man mit ihnen analog zu Satz 6.13 Faktorstrukturen definieren kann. Dies wollen wir jetzt zeigen. Ist dazu zunächst einmal I eine additive Untergruppe in einem Ring R, so können wir in jedem Fall die zugehörige Faktorgruppe R/I bilden, d. h. es ist $\overline{x} = x + I$ für $x \in R$ (siehe Lemma 5.6 (b)) und $\overline{x} = \overline{y}$ in R/I genau dann, wenn $y - x \in I$ (siehe Bemerkung 5.7 (a)). Ist I zusätzlich ein Ideal, so lässt sich auch die Multiplikation wohldefiniert von R auf R/I übertragen:

Satz 8.10 (Faktorringe). *Es sei $I \trianglelefteq R$ ein Ideal in einem Ring R. Dann gilt:*

(a) *Auf der Menge R/I ist neben der Addition auch die Multiplikation $\overline{x} \cdot \overline{y} := \overline{x \cdot y}$ wohldefiniert und macht R/I zu einem Ring.*

(b) *Die Restklassenabbildung $\pi \colon R \to R/I$, $x \mapsto \overline{x}$ ist ein surjektiver Ringhomomorphismus mit Kern I.*

*Analog zum Fall von Gruppen wird R/I als ein **Faktorring** von R bezeichnet.*

Beweis.

(a) Die Multiplikation ist wohldefiniert: Es seien $x, x', y, y' \in R$ mit $\overline{x} = \overline{x'}$ und $\overline{y} = \overline{y'}$, d. h. es ist $x' = x + a$ und $y' = y + b$ für gewisse $a, b \in I$. Dann gilt

$$x'y' = (x+a)(y+b) = xy + \underbrace{ay + bx + ab}_{\in I},$$

wobei die Summe der letzten drei Terme in I liegt, weil jeder einen Faktor aus I (nämlich a oder b) enthält und Ideale bezüglich Summen sowie Produkten mit beliebigen Ringelementen abgeschlossen sind. Also ist $\overline{xy} = \overline{x'y'}$ in R/I.

Analog zu Satz 6.13 (a) übertragen sich nun die Ringeigenschaften aus Definition 7.1 sofort von R auf R/I. Wir zeigen exemplarisch die Distributivität (R3): Für alle $x, y, z \in R$ gilt

$$\left(\overline{x} + \overline{y}\right) \cdot \overline{z} = \overline{x+y} \cdot \overline{z} = \overline{(x+y)z} \overset{(*)}{=} \overline{xz + yz} = \overline{xz} + \overline{yz} = \overline{x} \cdot \overline{z} + \overline{y} \cdot \overline{z},$$

wobei $(*)$ die Distributivität in R ist und alle anderen Gleichungen einfach nur die Definitionen der Verknüpfungen auf R/I sind.

(b) Wir wissen aus Satz 6.13 (b) bereits, dass die Restklassenabbildung π ein surjektiver additiver Gruppenhomomorphismus mit Kern I ist. Weiterhin ist $\pi(1) = \overline{1}$ das multiplikative neutrale Element des Faktorringes, und es gilt

$$\pi(x \cdot y) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = \pi(x) \cdot \pi(y)$$

für alle $x, y \in R$. Also ist π sogar ein Ringhomomorphismus. □

Beispiel 8.11. Da $n\mathbb{Z}$ nach Beispiel 8.3 (a) ein Ideal in $\mathbb{Z}$ ist, ist $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ nach Satz 8.10 ein Ring — wie wir vorher schon in Beispiel 7.4 (b) gesehen hatten.

Zum Abschluss dieses Kapitels wollen wir schließlich noch den Homomorphiesatz, den wir in Satz 6.17 für Gruppen gesehen hatten, auf den Fall von Ringen übertragen. Mit unseren Vorbereitungen verläuft diese Übertragung nun genau wie erwartet:

Satz 8.12 (**Homomorphiesatz** für Ringe). *Es sei $f \colon R \to S$ ein Ringhomomorphismus. Dann ist die Abbildung*

$$\begin{aligned} g \colon R/\operatorname{Ker} f &\to \operatorname{Im} f \\ \overline{x} &\mapsto f(x) \end{aligned}$$

zwischen dem Faktorring $R/\operatorname{Ker} f$ von R und dem Unterring $\operatorname{Im} f$ von S ein Ringisomorphismus.

Beweis. Da $\operatorname{Ker} f$ nach Lemma 8.4 ein Ideal von R ist, können wir den Faktorring $R/\operatorname{Ker} f$ bilden. Wenden wir weiterhin den Homomorphiesatz 6.17 für Gruppen auf den zugehörigen Gruppenhomomorphismus $f\colon (R,+) \to (S,+)$ an, so sehen wir, dass g wohldefiniert, mit der Addition verträglich und bijektiv ist. Außerdem ist g auch mit der Multiplikation verträglich: Für alle $x, y \in R/\operatorname{Ker} f$ ist

$$g(\overline{x} \cdot \overline{y}) = g(\overline{xy}) = f(xy) = f(x)\,f(y) = g(\overline{x}) \cdot g(\overline{y}).$$

Wegen $f(1) = 1$ gilt schließlich auch $g(\overline{1}) = f(1) = 1$, und damit ist g ein Ringisomorphismus. □

Aufgabe 8.13. Es seien R ein Integritätsring und $a, b \in R \setminus \{0\}$ keine Einheiten.

Man zeige: Ist $\overline{a}$ ein Nullteiler in $R/\langle b \rangle$, so ist $\overline{b}$ ein Nullteiler in $R/\langle a \rangle$.

Aufgabe 8.14. In einem Ring R heißt ein Element $e \in R$ *idempotent*, wenn $e^2 = e$.

Offensichtlich sind 0 und 1 stets idempotent. Man zeige nun:

(a) Ist $R = S \times T$ ein nicht-triviales Produkt von zwei Ringen (d. h. S und T sind beide nicht der Nullring), so besitzt R ein idempotentes Element $e \notin \{0, 1\}$.

(b) Besitzt umgekehrt R ein idempotentes Element $e \notin \{0, 1\}$, so ist $R \cong R/\langle e \rangle \times R/\langle 1 - e \rangle$ isomorph zu einem nicht-trivialen Produkt von zwei Ringen.

Ist $\mathbb{Z}_8$ bzw. $\mathbb{Z}_{12}$ isomorph zu einem nicht-trivialen Produkt von zwei Ringen?

9. Polynom- und Potenzreihenringe

Bevor wir mit der allgemeinen Untersuchung von Ringen fortfahren, wollen wir in diesem Kapitel kurz zwei sehr wichtige weitere Beispiele von Ringen einführen, deren Objekte ihr sicher in der einen oder anderen Form schon in den Grundlagen der Mathematik oder auch schon in der Schule gesehen habt: die *Polynome*, also Ausdrücke der Form

$$a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \tag{1}$$

(mit $n \in \mathbb{N}$ und gegebenen Koeffizienten a_n in einem Ring R, z. B. im Ring $\mathbb{R}$ der reellen Zahlen), und als „unendliche Variante" davon die *Potenzreihen*, also nicht notwendig abbrechende Summen der Form

$$a_0 + a_1 t + a_2 t^2 + \cdots . \tag{2}$$

Vermutlich werdet ihr diese Ausdrücke dabei bisher stets als Funktionen aufgefasst haben, die einer (z. B. reellen) Zahl t die Zahl zuordnen, die eben durch die Formel (1) bzw. (2) gegeben ist. Bei den Potenzreihen muss man dazu natürlich vorher noch überprüfen, dass die Reihe für die eingesetzten Werte von t auch konvergiert.

In der Algebra ist die Herangehensweise an Polynome und Potenzreihen etwas anders. Das muss auch so sein, denn in einem allgemeinen Ring R haben wir ja überhaupt keinen Konvergenzbegriff und damit keinerlei Möglichkeit, eine unendliche Summe wie in (2) als Funktion aufzufassen: Wenn wir dort für t ein Ringelement einsetzen würden, ergäbe sich lediglich eine (undefinierte) Summe unendlich vieler Elemente aus R.

Wir wollen eine Potenzreihe wie in (2) daher in einem beliebigen Ring R als rein *formale Summe* auffassen, in die wir zunächst einmal keine Werte für t einsetzen können. Der entscheidende Punkt hierbei ist, dass wir solche Potenzreihen trotzdem addieren und multiplizieren können: Betrachten wir z. B. die formalen Potenzreihen

$$f = 1 + t + t^2 + t^3 + t^4 + t^5 + \cdots \quad \text{und} \quad g = 1 - t + t^2 - t^3 + t^4 - t^5 \pm \cdots ,$$

so erscheint es sicher in einem beliebigen Ring sinnvoll, die Summe dieser beiden Reihen einfach formal koeffizientenweise als

$$f + g = 2 + 2t^2 + 2t^4 + \cdots$$

zu *definieren*, selbst wenn man für t eigentlich keine Werte einsetzen und f und g damit nicht als Funktionen ansehen kann. Analog werden wir auch eine Multiplikation von Potenzreihen durch „formales Ausmultiplizieren" definieren und die Menge dieser formalen Potenzreihen damit zu einem Ring machen.

Bei Polynomen scheint die Situation zunächst etwas anders zu sein, denn in der *endlichen* Summe (1) könnten wir natürlich in einem beliebigen Ring R Werte für t einsetzen und das Polynom somit tatsächlich als Funktion von R nach R auffassen. Wir werden jedoch z. B. in Bemerkung 9.16 (b) sehen, dass es algebraisch viel schöner ist, Polynome dennoch *nicht* als solche Funktionen, sondern (wie schon bei den Potenzreihen) als formale Ausdrücke der Form (1) zu definieren. In der Tat macht dies in manchen Ringen einen Unterschied: Betrachten wir z. B. das Polynom $t^2 + t$ über dem Ring $\mathbb{Z}_2$, so stellt dieses zwar die Nullfunktion dar (denn es ist $\overline{0}^2 + \overline{0} = \overline{1}^2 + \overline{1} = \overline{0}$, d. h. jedes Element von $\mathbb{Z}_2$ wird unter der Funktion $t \mapsto t^2 + t$ auf die Null abgebildet), es ist aber als formaler Ausdruck trotzdem nicht das Nullpolynom. Wir wollen die Polynome $t^2 + t$ und $\overline{0}$ über $\mathbb{Z}_2$ daher als *verschieden* ansehen, auch wenn sie beim Einsetzen von Werten dieselbe Funktion beschreiben.

Nach diesen Vorbemerkungen können wir nun damit beginnen, Potenzreihen über einem beliebigen Ring exakt zu definieren. Wie gerade erläutert ist eine solche formale Potenzreihe der Form (2) einfach dadurch gegeben, dass man ihre Koeffizienten $a_0, a_1, a_2, \ldots$ angibt. Dabei gibt es für die

Wahl dieser Koeffizienten keinerlei Einschränkungen. Eine Potenzreihe „ist“ also letztlich einfach diese Folge $a_0, a_1, a_2, \dots$ in R, d. h. eine Abbildung von $\mathbb{N}$ nach R.

Definition 9.1 (Potenzreihen)**.** Es sei R ein Ring.

(a) Eine **(formale) Potenzreihe** über R ist eine Abbildung $\mathbb{N} \to R$, $n \mapsto a_n$. Wir werden eine solche Potenzreihe jedoch *nie* als derartige Abbildung, sondern *immer* in der Form

$$\sum_{k=0}^{\infty} a_k t^k \quad \text{oder} \quad a_0 + a_1 t + a_2 t^2 + \cdots$$

schreiben (wobei wir für k natürlich auch einen anderen Buchstaben wählen können). Beachte, dass es sich dabei aber nur um eine *formale Schreibweise* für die obige Abbildung $\mathbb{N} \to R$ und *nicht* um eine wirkliche „unendliche Summe“ in R handelt!

Die Menge aller Potenzreihen über R wird mit $R[\![t]\!]$ bezeichnet.

(b) Sind $f = \sum_{k=0}^{\infty} a_k t^k$ und $g = \sum_{k=0}^{\infty} b_k t^k$ zwei Potenzreihen über R, so definieren wir ihre Summe $f+g$ und ihr Produkt $f \cdot g$ als die Potenzreihen

$$f + g := \sum_{k=0}^{\infty} (a_k + b_k) t^k$$

$$\text{und} \qquad f \cdot g := \sum_{n=0}^{\infty} \Bigg(\underbrace{\sum_{k+l=n} a_k b_l}_{(*)} \Bigg) t^n.$$

Beachte dabei, dass die Summe $(*)$ eine „echte“ (endliche) Summe in R ist, während die beiden anderen Summenzeichen die „formalen unendlichen Summen“ aus (a) sind.

Bemerkung 9.2.

(a) In der Schreibweise von Definition 9.1 können wir t als *formale Variable* auffassen. Natürlich könnte man auch hier einen anderen Buchstaben als formale Variable wählen und die Notation $R[\![t]\!]$ entsprechend abändern. Wir werden die formale Variable einer Potenzreihe in diesem Skript jedoch immer mit dem Buchstaben t bezeichnen.

(b) Beachte, dass die Multiplikation von Potenzreihen in Definition 9.1 (b) genau so eingeführt wurde, wie man es erwarten würde, wenn man diese formalen unendlichen Summen naiv ausmultiplizieren könnte: Dann wäre nämlich

$$\begin{aligned} \Bigg(\sum_{k=0}^{\infty} a_k t^k \Bigg) \cdot \Bigg(\sum_{l=0}^{\infty} b_l t^l \Bigg) &= (a_0 + a_1 t + a_2 t^2 + \cdots) \cdot (b_0 + b_1 t + b_2 t^2 + \cdots) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0) t + (a_0 b_2 + a_1 b_1 + a_2 b_0) t^2 + \cdots \\ &= \sum_{n=0}^{\infty} \Bigg(\sum_{k+l=n} a_k b_l \Bigg) t^n, \end{aligned}$$

und das ist ja gerade unsere Definition. In der Analysis ist es ein *Satz* (den ihr in den Grundlagen der Mathematik vielleicht schon bewiesen habt), dass dieses „unendliche Ausmultiplizieren“ — das sogenannte *Cauchy-Produkt von Reihen* — bei bestimmten konvergenten reellen oder komplexen Reihen erlaubt ist [G, Satz 7.33]. Bei uns in der Algebra dagegen ist dies einfach nur die *Definition* der Multiplikation von formalen Potenzreihen.

Beispiel 9.3. In einem Ring R betrachten wir die Potenzreihe

$$f = 1 + t + t^2 + t^3 + \cdots = \sum_{k=0}^{\infty} t^k \ \in R[\![t]\!].$$

Dann ist das Produkt von f mit sich selbst nach Definition 9.1 (b)

$$f^2 = \sum_{n=0}^{\infty} \Bigg(\sum_{k+l=n} 1 \cdot 1 \Bigg) t^n = \sum_{n=0}^{\infty} (n+1) t^n,$$

da die Summe über k und l aus $n+1$ Summanden (nämlich $(k,l) = (0,n),(1,n-1),\dots,(n,0)$) besteht.

Lemma 9.4. *Für jeden Ring R ist die Menge $R[\![t]\!]$ aller Potenzreihen über R mit den Verknüpfungen aus Definition 9.1 (b) ein Ring. Er wird der **(formale) Potenzreihenring** über R genannt.*

Beweis. Die Überprüfung der Ringaxiome aus Definition 7.1 ergibt sich durch einfaches Nachrechnen. Wir zeigen hier exemplarisch den Beweis der Distributivität (R3): Für

$$f = \sum_{k=0}^{\infty} a_k t^k, \quad g = \sum_{k=0}^{\infty} b_k t^k \quad \text{und} \quad h = \sum_{l=0}^{\infty} c_l t^l$$

ist

$$\begin{aligned}
(f+g)\cdot h &= \left(\sum_{k=0}^{\infty} (a_k + b_k) t^k\right) \cdot \left(\sum_{l=0}^{\infty} c_l t^l\right) \\
&= \sum_{n=0}^{\infty} \left(\sum_{k+l=n} (a_k + b_k) c_l\right) t^n \\
&\overset{(*)}{=} \sum_{n=0}^{\infty} \left(\sum_{k+l=n} a_k c_l + \sum_{k+l=n} b_k c_l\right) t^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{k+l=n} a_k c_l\right) t^n + \sum_{n=0}^{\infty} \left(\sum_{k+l=n} b_k c_l\right) t^n \\
&= f\cdot h + g \cdot h,
\end{aligned}$$

wobei $(*)$ die Distributivität in R ist (beachte, dass die Summen über k und l „echte“ endliche Summen in R sind) und alle anderen Gleichungen aus der Definition 9.1 (b) der Addition und Multiplikation in $R[\![t]\!]$ folgen.

Die Null in $R[\![t]\!]$ ist natürlich die Potenzreihe, bei der alle Koeffizienten gleich 0 sind; die Eins diejenige, bei der nur der konstante Koeffizient gleich 1 und alle anderen gleich 0 sind. □

Notation 9.5. Aus naheliegenden Gründen schreibt man die Potenzreihe

$$a_0 + 0\cdot t + 0\cdot t^2 + 0\cdot t^3 + \cdots \quad \in R[\![t]\!]$$

über einem Ring R einfach kurz als a_0, und die Potenzreihe

$$0 + 1\cdot t + 0\cdot t^2 + 0\cdot t^3 + \cdots \quad \in R[\![t]\!]$$

einfach als t. Da die Addition und Multiplikation in $R[\![t]\!]$ ja gerade so definiert sind, wie man es durch formales Addieren und Ausmultiplizieren von Potenzreihen erwarten würde, können wir dann jede „abbrechende Potenzreihe“

$$a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + 0\cdot t^{n+1} + 0\cdot t^{n+2} + \cdots,$$

also jede Potenzreihe $\sum_{k=0}^{\infty} a_k t^k$, für die es ein $n \in \mathbb{N}$ gibt mit $a_k = 0$ für alle $k > n$, offensichtlich einfach als

$$a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n,$$

schreiben, wobei dies nun *keine* formale Summe mehr ist, sondern eine „echte“ Verknüpfung der Potenzreihen $a_0,\dots,a_n,t \in R[\![t]\!]$ mit der Addition und Multiplikation wie in Definition 9.1 (b). Diese „abbrechenden Potenzreihen“ sind jetzt genau die Polynome, die wir bereits am Anfang dieses Kapitels erwähnt hatten.

Definition 9.6 (Polynome)**.** Es sei R ein Ring.

(a) Ein **Polynom** über R ist eine Potenzreihe der Form $a_0 + a_1 t + \cdots a_n t^n$, also eine Potenzreihe, bei der nur endlich viele Koeffizienten ungleich Null sind. Die Menge aller Polynome über R wird mit $R[t]$ bezeichnet.

(b) Ist $f \in R[t]$ ein Polynom mit $f \neq 0$, so können wir f offensichtlich eindeutig als

$$f = a_0 + a_1 t + \cdots a_n t^n$$

mit $n \in \mathbb{N}$ und $a_n \neq 0$ schreiben. Die Zahl n, also der höchste in f auftretende Exponent von t, wird der **Grad** von f genannt und als $\deg f$ geschrieben (die Bezeichnung kommt vom englischen Wort „degree“). Der höchste Koeffizient $a_n \in R$ heißt **Leitkoeffizient** von f. Man nennt f **normiert**, wenn dieser Leitkoeffizient gleich 1 ist.

Den Grad des Nullpolynoms definiert man formal als $\deg 0 = -\infty$ (auf diese Art bleiben z. B. die Formeln aus Lemma 9.7 (a) und 9.9 (a) auch in diesem Fall richtig).

(c) Ein Polynom vom Grad $-\infty$ oder 0 heißt **konstantes Polynom**, eines vom Grad 1 **lineares Polynom**.

Lemma 9.7. *Es sei wieder R ein Ring.*

(a) *Sind $f, g \in R[t]$ Polynome über R, so sind auch $f+g$ und $f \cdot g$ Polynome über R, und es gilt*

$$\deg(f+g) \leq \max\{\deg f, \deg g\} \quad \textit{und} \quad \deg(f \cdot g) \leq \deg f + \deg g.$$

(b) *Es gilt $R \leq R[t] \leq R[\![t]\!]$, wobei R wie in Notation 9.5 als Teilmenge von $R[t]$ bzw. $R[\![t]\!]$ angesehen wird, indem man ein $a_0 \in R$ als konstantes Polynom auffasst.*

*Insbesondere ist $R[t]$ also ein Ring; er wird der **Polynomring** über R genannt.*

Beweis.

(a) Für $f = 0$ oder $g = 0$ sind die Aussagen aufgrund der Definition $\deg 0 = -\infty$ richtig. Da f und g ansonsten nur Terme t^k mit $k \leq \deg f$ bzw. $k \leq \deg g$ enthält, ist natürlich aufgrund von Definition 9.1 (b) klar, dass $f+g$ und $f \cdot g$ nur Terme t^k mit $k \leq \max\{\deg f, \deg g\}$ bzw. $k \leq \deg f + \deg g$ enthalten kann.

(b) Beide Aussagen folgen mit (a) direkt aus dem Unterringkriterium von Lemma 7.23. □

10

Beispiel 9.8. Sowohl für den Grad von $f+g$ als auch für den von $f \cdot g$ kann in Lemma 9.7 (a) eine echte Ungleichung stehen: Für $R = \mathbb{Z}_4$ und das Polynom $f = g = \overline{2}t + \overline{1}$ vom Grad 1 ist

$$\deg(f+g) = \deg(\overline{4}t + \overline{2}) = \deg(\overline{2}) = 0 < 1 = \max\{\deg f, \deg g\}$$

und

$$\deg(f \cdot g) = \deg((\overline{2}t + \overline{1})^2) = \deg(\overline{4}t^2 + \overline{4}t + \overline{1}) = \deg(\overline{1}) = 0 < 2 = \deg f + \deg g.$$

Ist R ein Integritätsring, so steht bei der Formel für $\deg(f \cdot g)$ jedoch immer die Gleichheit:

Lemma 9.9. *Für jeden Integritätsring R gilt:*

(a) ***(Gradformel)** Für alle $f, g \in R[t]$ gilt $\deg(f \cdot g) = \deg f + \deg g$.*

(b) *$R[t]$ ist ein Integritätsring.*

(c) *Die Einheitengruppe des Polynomrings über R ist $R[t]^* = R^*$, besteht also genau aus den konstanten Polynomen mit Wert in R^*.*

Beweis.

(a) Für $f = 0$ oder $g = 0$ ist die Formel wegen $\deg 0 = -\infty$ trivialerweise richtig. Ist ansonsten $n = \deg f$ und $m = \deg g$, so können wir f und g als

$$f = a_n t^n + \cdots + a_1 t + a_0 \quad \text{und} \quad g = b_m t^m + \cdots + b_1 t + b_0$$

mit $a_n, b_m \neq 0$ schreiben. Damit ist

$$f \cdot g = a_n b_m t^{n+m} + (\text{Terme mit niedrigeren Potenzen von } t).$$

Da R ein Integritätsring ist, folgt nun $a_n b_m \neq 0$ und damit $\deg(f \cdot g) = n + m = \deg f + \deg g$.

(b) Sind $f, g \neq 0$, also $\deg f, \deg g \geq 0$, so ist nach (a) auch $\deg(f \cdot g) \geq 0$ und damit $f \cdot g \neq 0$.

(c) Offensichtlich ist jede Einheit von R auch eine von $R[t]$. Ist umgekehrt $f \in R[t]^*$, so gibt es ein $g \in R[t]$ mit $f \cdot g = 1$. Aus der Gradformel (a) folgt daraus $\deg f + \deg g = 0$, also $\deg f = \deg g = 0$. Damit liegen $f = a_0$ und $g = b_0$ in R, und wegen $f \cdot g = a_0 \cdot b_0 = 1$ muss sogar $f = a_0 \in R^*$ gelten. □

Aufgabe 9.10. Für eine Potenzreihe $f = \sum_{n=0}^{\infty} a_n t^n$ über einem Ring R definieren wir die *(formale) Ableitung* als $f' := \sum_{n=1}^{\infty} n a_n t^{n-1}$.

(a) Man zeige: Für alle $f, g \in R[\![t]\!]$ gilt $(f+g)' = f' + g'$ und $(fg)' = f'g + fg'$.

(b) Bestimme in den beiden Fällen $R = \mathbb{R}$ und $R = \mathbb{Z}_7$ alle Potenzreihen mit Ableitung $0 \in R[\![t]\!]$.

Aufgabe 9.11. Es seien R ein Ring und $a \in R$. Zeige, dass die Potenzreihe $1 - at \in R[\![t]\!]$ invertierbar ist, und berechne $(1-at)^{-1} \in R[\![t]\!]$.

Aufgabe 9.12. Zeige, dass eine Potenzreihe $\sum_{n=0}^{\infty} a_n t^n$ über einem Ring R genau dann in $R[\![t]\!]$ invertierbar ist, wenn $a_0 \in R^*$.

Aufgabe 9.13. In dieser Aufgabe wollen wir mit Hilfe von Potenzreihen eine explizite Formel für die durch

$$a_0 = a_1 = 1 \quad \text{und} \quad a_{n+2} = a_{n+1} + a_n \text{ für } n \in \mathbb{N}$$

rekursiv definierte *Fibonacci-Folge* $1, 1, 2, 3, 5, 8, 13, \ldots$ herleiten.

(a) Nach Aufgabe 9.12 ist $1 - t - t^2$ in $\mathbb{R}[\![t]\!]$ invertierbar. Zeige, dass sich das Inverse dieser Potenzreihe als $\frac{1}{1-t-t^2} = \frac{b_1}{1-c_1 t} + \frac{b_2}{1-c_2 t}$ für gewisse $b_1, b_2, c_1, c_2 \in \mathbb{R}$ schreiben lässt, und bestimme diese Koeffizienten.

(b) Zeige, dass die Fibonacci-Zahlen genau die Koeffizienten der Potenzreihe $\frac{1}{1-t-t^2}$ sind, d. h. dass

$$\frac{1}{1-t-t^2} = \sum_{n=0}^{\infty} a_n t^n$$

gilt, und folgere daraus für $n \in \mathbb{N}$ die nicht-rekursive Formel

$$a_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right).$$

Aufgabe 9.14. Ist der Potenzreihenring $R[\![t]\!]$ über einem Integritätsring R ebenfalls wieder ein Integritätsring?

Wie schon am Anfang dieses Kapitels erwähnt bestimmt ein Polynom über R eine Funktion von R nach R:

Definition 9.15 (Polynomfunktionen)**.** Ist $f = a_0 + a_1 t + \cdots + a_n t^n$ ein Polynom über einem Ring R und $x \in R$, so heißt das Ringelement

$$f(x) := a_0 + a_1 x + \cdots + a_n x^n \quad \in R$$

der **Wert** von f in x. Die zugehörige Funktion $R \to R$, $x \mapsto f(x)$ wird eine **Polynomfunktion** genannt. Ist $f(x) = 0 \in R$, so heißt x eine **Nullstelle** von f.

Bemerkung 9.16.

(a) Beachte, dass wir für Potenzreihen $f \in R[\![t]\!]$ keinen Wert $f(x)$ in einem Punkt $x \in R$ definieren können, da wir in der Algebra (also ohne Konvergenzbegriff) keine unendlichen Summen in R bilden können.

(b) Nach Definition 9.15 bestimmt jedes Polynom f über einem Ring R eine Polynomfunktion $R \to R$, $x \mapsto f(x)$. Wie wir schon in der Einleitung dieses Kapitels gesehen haben, können aber zwei verschiedene Polynome dieselbe Polynomfunktion bestimmen: Das Polynom $t^2 + t$ über $\mathbb{Z}_2$ hat z. B. in jedem Element von $\mathbb{Z}_2$ den Wert Null. Während die beiden *Polynome* $t^2 + t$ und $\overline{0}$ verschieden sind, sind die beiden zugehörigen *Polynomfunktionen* $t \mapsto t^2 + t$

und $t \mapsto \overline{0}$ hier also gleich. Beachte, dass dies u. a. auch bedeutet, dass man einer *Polynomfunktion* in der Regel keinen wohldefinierten Grad zuordnen kann — hier verhalten sich Polynome aus algebraischer Sicht also deutlich schöner als Polynomfunktionen.

Wir werden in Folgerung 11.16 allerdings noch sehen, dass Polynome und Polynomfunktionen über Körpern mit unendlich vielen Elementen (also z. B. $\mathbb{R}$ oder $\mathbb{C}$) übereinstimmen, so dass es in diesem wohl wichtigsten Fall keinen Unterschied macht, ob wir bei Polynomen an Funktionen oder an die formalen Ausdrücke aus Definition 9.6 denken.

Aufgabe 9.17. Man zeige:

(a) Sind $R \leq S$ Ringe und $x \in S$, so ist die „Auswerteabbildung“

$$\varphi\colon R[t] \to S,\ f = \sum_{k=0}^{n} a_k t^k \ \mapsto\ f(x) := \sum_{k=0}^{n} a_k x^k$$

ein Ringhomomorphismus.

(b) Jedes Element des Ringes $\mathbb{R}[t]/\langle t^2+1\rangle$ lässt sich in der Form $\overline{x+yt}$ mit $x, y \in \mathbb{R}$ schreiben.

(c) Die Abbildung $\mathbb{R}[t]/\langle t^2+1\rangle \to \mathbb{C},\ \overline{f} \mapsto f(\mathrm{i})$ ist ein Ringisomorphismus.

(Man kann $\mathbb{C}$ also algebraisch sehr elegant als $\mathbb{R}[t]/\langle t^2+1\rangle$ definieren — dies definiert dann gleichzeitig schon die Addition und Multiplikation auf $\mathbb{C}$ und zeigt dafür ohne weitere Rechnung alle Ringaxiome. In der Tat werden wir in Beispiel 11.21 (b) noch sehen, dass sich sogar alle Körperaxiome schon automatisch ergeben.)

Bemerkung 9.18 (Die Notation $R[\cdot]$)**.** Um Verwirrungen zu vermeiden, ist es wichtig zu verstehen, dass die Notation $R[\,\cdot\,]$ für einen Ring R zwei verschiedene Dinge bedeuten kann:

(a) Steht in den Klammern eine (vorher unbekannte) formale Variable, so wie in $R[t]$ in Definition 9.6, so ist der dort eingeführte Polynomring gemeint.

(b) Steht in den Klammern ein Element a eines größeren bereits bekannten Ringes $S \geq R$, so wie z. B. in $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ mit $a = \sqrt{5}\,\mathrm{i} \in \mathbb{C}$ in Aufgabe 7.24, so ist der *Ring aller Werte von Polynomausdrücken* in diesem Element mit Koeffizienten in R gemeint, also der Unterring

$$R[a] := \{c_0 + c_1 a + \cdots c_n a^n : n \in \mathbb{N}; c_0, \ldots, c_n \in R\}$$

von S. Liegt a^2 bereits wieder in R, so können wir uns dabei natürlich auf lineare Polynomausdrücke beschränken und erhalten z. B.

$$\mathbb{Z}[\sqrt{5}\,\mathrm{i}] = \{c_0 + c_1\sqrt{5}\,\mathrm{i} : c_0, c_1 \in \mathbb{Z}\} \quad \leq \mathbb{C}$$

wie in Aufgabe 7.24.

Die in der Literatur übliche gleiche Notation für diese beiden Konzepte kommt daher, dass in beiden Fällen Polynomausdrücke in dem in Klammern genannten Element betrachtet werden. Auch die Sprechweise ist daher oft in beiden Fällen gleich: Man sagt, dass $R[\,\cdot\,]$ aus R durch *Adjunktion* des in Klammern stehenden Elements entsteht und spricht die Fälle (a) und (b) oben demzufolge auch als „R adjungiert t“ bzw. „R adjungiert a“. Die formale Konstruktion dieser Ringe ist in (a) und (b) jedoch unterschiedlich.

10. Teilbarkeit in Ringen

Ein wichtiges Konzept in Ringen, das ihr für den Fall des Ringes $\mathbb{Z}$ bereits aus der Schule kennt, ist das von *Teilern* — also der Frage, wann und wie man ein Ringelement als Produkt von zwei anderen schreiben kann. Dies wollen wir jetzt in allgemeinen Ringen untersuchen, wobei die Polynomringe über Körpern letztlich neben $\mathbb{Z}$ die wichtigsten Anwendungsbeispiele sein werden. Um die Theorie dazu nicht zu kompliziert werden zu lassen, wollen wir uns dabei auf den Fall von Integritätsringen beschränken, also die Existenz von Nullteilern außer der 0 ausschließen.

Definition 10.1 (Teiler)**.** Es seien R ein Integritätsring und $a, b \in R$. Man sagt, dass b ein **Teiler** von a ist (in Zeichen: $b \mid a$), wenn es ein $c \in R$ gibt mit $a = b \cdot c$. In diesem Fall heißt a dann auch ein **Vielfaches** von b.

Beispiel 10.2.

(a) Die Teiler von 4 im Ring $\mathbb{Z}$ sind -4, -2, -1, 1, 2 und 4.

(b) Das Polynom $2t$ ist im Integritätsring $\mathbb{Q}[t]$ ein Teiler von t^2 (denn $t^2 = 2t \cdot \frac{1}{2} t$), nicht jedoch in $\mathbb{Z}[t]$.

Wie üblich wollen wir zuerst die wichtigsten Eigenschaften von Teilern untersuchen. Besonders wichtig ist dabei, dass sich die Teilbarkeitseigenschaft auch mit Hilfe von Idealen formulieren lässt.

Lemma 10.3 (Eigenschaften der Teilbarkeit)**.** *Es seien a, b, c Elemente in einem Integritätsring R.*

(a) *Gilt $c \mid b$ und $b \mid a$, so auch $c \mid a$ (Transitivität).*

(b) *Es ist $b \mid a$ genau dann, wenn $a \in \langle b \rangle$.*

(c) *Es gilt*

$$b \mid a \text{ und } a \mid b \quad \Leftrightarrow \quad \text{es gibt ein } d \in R^* \text{ mit } a = bd \quad \Leftrightarrow \quad \langle a \rangle = \langle b \rangle.$$

*Man sagt in diesem Fall auch, dass a und b zueinander **assoziiert** sind.*

Beweis.

(a) Gilt $c \mid b$ und $b \mid a$, also $b = cd$ und $a = be$ für gewisse $d, e \in R$, so ist auch $a = cde$, also $c \mid a$.

(b) Es gilt

$$b \mid a \quad \Leftrightarrow \quad \text{es gibt ein } c \in R \text{ mit } a = bc \quad \Leftrightarrow \quad a \in \{bc : c \in R\} \overset{8.8(a)}{=} \langle b \rangle.$$

(c) Wir zeigen die Äquivalenzen durch einen Ringschluss.

Es gelte zunächst $b \mid a$ und $a \mid b$, d. h. es gibt $d, e \in R$ mit $a = bd$ und $b = ae$. Setzt man dies ineinander ein, so ergibt sich $a = ade$ und $b = bde$. Sind nun a oder b ungleich 0, so folgt daraus mit der Kürzungsregel aus Lemma 7.8 (c) sofort $de = 1$, also $a = bd$ mit $d \in R^*$. Andernfalls ist $a = b = 0$, und damit natürlich auch $a = b \cdot 1$ mit $1 \in R^*$.

Nun sei $a = bd$ für ein $d \in R^*$. Dann ist auch $b = ad^{-1}$, nach Beispiel 8.8 (a) also $a \in \langle b \rangle$ und $b \in \langle a \rangle$. Nach Lemma 8.6 (b) bedeutet dies aber gerade $\langle a \rangle \subset \langle b \rangle$ und $\langle b \rangle \subset \langle a \rangle$, also $\langle a \rangle = \langle b \rangle$.

Ist schließlich $\langle a \rangle = \langle b \rangle$, also $a \in \langle b \rangle$ und $b \in \langle a \rangle$, so gilt $b \mid a$ und $a \mid b$ nach (b). □

Aufgabe 10.4. Man zeige:

(a) Eine natürliche Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme (also die Summe aller ihrer Ziffern) durch 3 teilbar ist.

(b) Für $a, b \in \mathbb{Z}$ gilt $17 \mid a + 3b$ genau dann, wenn $17 \mid b + 6a$.

Wie ihr vom Fall der ganzen Zahlen $\mathbb{Z}$ wisst, spielt bei der Untersuchung der Teilbarkeit vor allem der größte gemeinsame Teiler (und das kleinste gemeinsame Vielfache) von zwei gegebenen Zahlen eine große Rolle. Wir wollen ein derartiges Konzept daher auch in allgemeinen Integritätsringen einführen. Dabei haben wir jedoch zunächst das Problem, dass wir auf einem allgemeinen Integritätsring R keine „Ordnung“ haben, mit deren Hilfe wir sagen könnten, welchen gemeinsamen Teiler zweier Elemente von R wir als den *größten* ansehen wollen. Das folgende Beispiel zeigt, wie wir dieses Problem lösen können.

Beispiel 10.5. Betrachten wir die beiden ganzen Zahlen 12 und 30, so sind die gemeinsamen Teiler von ihnen -6, -3, -2, -1, 1, 2, 3 und 6. Von diesen ist 6 natürlich die größte Zahl — aber die 6 ist auch in dem Sinne „am größten“, dass jedes andere Element dieser Liste ein Teiler davon ist.

Es ist diese zweite Eigenschaft, die wir zur Definition eines größten gemeinsamen Teilers verwenden wollen und die so auch in jedem Integritätsring anwendbar ist. Wie in der folgenden Definition messen wir die Größe eines Teilers also ebenfalls wieder mit Hilfe der Teilbarkeit.

Definition 10.6 (ggT und kgV)**.** Es seien a,b zwei Elemente in einem Integritätsring R.

(a) Ein Element $g \in R$ heißt **größter gemeinsamer Teiler** von a und b, wenn gilt:

(1) $g \mid a$ und $g \mid b$ („g ist ein gemeinsamer Teiler“);

(2) ist $c \in R$ mit $c \mid a$ und $c \mid b$, so gilt auch $c \mid g$ („g ist der *größte* gemeinsame Teiler“).

Wir bezeichnen die Menge aller größten gemeinsamen Teiler von a und b mit $\operatorname{ggT}(a,b)$. Ist $1 \in \operatorname{ggT}(a,b)$, so heißen a und b **teilerfremd**.

(b) Ein Element $k \in R$ heißt **kleinstes gemeinsames Vielfaches** von a und b, wenn gilt:

(1) $a \mid k$ und $b \mid k$ („k ist ein gemeinsames Vielfaches“);

(2) ist $c \in R$ mit $a \mid c$ und $b \mid c$, so gilt auch $k \mid c$ („k ist das *kleinste* gemeinsame Vielfache“).

Wir bezeichnen die Menge aller kleinsten gemeinsamen Vielfachen von a und b mit $\operatorname{kgV}(a,b)$.

Beachte, dass durch unsere vielleicht etwas eigenwillig erscheinende Definition der „Größe“ eines Teilers bzw. Vielfachen zunächst einmal überhaupt nicht klar ist, ob größte gemeinsame Teiler und kleinste gemeinsame Vielfache überhaupt existieren, und ob sie im Fall der Existenz eindeutig sind. Wir haben $\operatorname{ggT}(a,b)$ und $\operatorname{kgV}(a,b)$ daher vorsichtshalber erst einmal als *Mengen* definiert (die auch leer sein oder mehr als ein Element enthalten können).

In der Tat wollen wir uns nun mit der Frage nach dieser Existenz und Eindeutigkeit von größten gemeinsamen Teilern beschäftigen (der Fall der kleinsten gemeinsamen Vielfachen wird sich in Folgerung 11.12 (c) dann relativ einfach daraus ergeben). Wir beginnen dabei mit der Eindeutigkeit, da deren Untersuchung deutlich einfacher ist als die der Existenz.

Beispiel 10.7 ((Nicht-)Eindeutigkeit des größten gemeinsamen Teilers)**.** Wir haben in Beispiel 10.5 schon festgestellt, dass -6, -3, -2, -1, 1, 2, 3 und 6 die gemeinsamen Teiler von 12 und 30 sind. Von diesen ist 6, aber auch -6 nach Definition 10.6 (a) ein größter gemeinsamer Teiler, denn alle diese acht Teiler von 12 und 30 sind auch Teiler von -6 und 6. Also ist

$$\operatorname{ggT}(12,30) = \{-6,6\}.$$

Insbesondere ist der größte gemeinsame Teiler also *nicht eindeutig*. Diese Nichteindeutigkeit besteht hier aber nur im Vorzeichen, also in der Möglichkeit, einen größten gemeinsamen Teiler noch mit der Einheit -1 von $\mathbb{Z}$ zu multiplizieren. Dies ist in der Tat ein allgemeines Phänomen, wie der folgende Satz zeigt.

Satz 10.8 ((Nicht-)Eindeutigkeit des größten gemeinsamen Teilers)**.** *Es sei g ein größter gemeinsamer Teiler zweier Elemente a,b in einem Integritätsring R. Dann ist $\operatorname{ggT}(a,b) = R^* g = \{cg : c \in R^*\}$ genau die Menge aller zu g assoziierten Elemente.*

Ein größter gemeinsamer Teiler zweier Elemente in einem Integritätsring ist also stets eindeutig bis auf Multiplikation mit Einheiten.

Beweis.

„$\subset$“: Es sei $g' \in \mathrm{ggT}(a,b)$. Damit sind g und g' größte gemeinsame Teiler von a und b. Wenden wir Teil (1) von Definition 10.6 (a) auf g' an, so sehen wir also, dass $g' \mid a$ und $g' \mid b$. Damit können wir dann Teil (2) mit $c = g'$ anwenden und erhalten $g' \mid g$. Durch Vertauschen der Rollen von g und g' ergibt sich genauso $g \mid g'$. Nach Lemma 10.3 (c) folgt damit $g' = cg$ für ein $c \in R^*$.

„$\supset$“: Es sei $g' = cg$ für ein $c \in R^*$. Dann folgt $g \mid g'$ und $g' \mid g$ nach Lemma 10.3 (c). Unter Benutzung der Transitivität der Teilbarkeitsrelation aus Lemma 10.3 (a) erfüllt daher mit g auch g' die beiden Eigenschaften aus Definition 10.6 (a):

(1) es gilt $g' \mid g \mid a$ und $g' \mid g \mid b$;

(2) ist $d \in R$ mit $d \mid a$ und $d \mid b$, so folgt $d \mid g \mid g'$.

Also ist auch g' ein größter gemeinsamer Teiler von a und b. □

Bemerkung 10.9. Der Beweis von Satz 10.8 lässt sich durch „Umkehren der Teilbarkeitsrelationen“ ganz analog auch für den Fall des kleinsten gemeinsamen Vielfachen führen.

Nach der Eindeutigkeit kommen wir nun zur Existenz eines größten gemeinsamen Teilers. Mit der Vorstellung des Ringes $\mathbb{Z}$ im Hintergrund würden wir wahrscheinlich erwarten, dass zwei Elemente a und b eines Integritätsringes R stets einen größten gemeinsamen Teiler besitzen. Allerdings haben wir die „Größe“ der gemeinsamen Teiler in Definition 10.6 (a) ja wieder über die Teilbarkeit definiert, und es ist ja bereits im Ring $\mathbb{Z}$ so, dass zwei beliebige Zahlen bezüglich Teilbarkeit nicht unbedingt miteinander vergleichbar sein müssen: Für z. B. die ganzen Zahlen 2 und 3 gilt weder $2 \mid 3$ noch $3 \mid 2$. Daher könnte es natürlich passieren, dass zu a und b kein größter gemeinsamer Teiler existiert, weil es zwei gemeinsame Teiler gibt, zu denen kein größerer existiert, und die nicht miteinander vergleichbar sind. Im folgenden Beispiel ist dies der Fall:

Aufgabe 10.10 ((Nicht-)Existenz eines größten gemeinsamen Teilers)**.** Bestimme alle gemeinsamen Teiler von $2+2\sqrt{5}\mathrm{i}$ und 6 im Ring $\mathbb{Z}[\sqrt{5}\mathrm{i}]$ aus Aufgabe 7.24 und zeige so, dass es keinen größten gemeinsamen Teiler gibt.

Die Frage nach der Existenz eines größten gemeinsamen Teilers gestaltet sich also etwas schwieriger als erwartet. Zu ihrer Untersuchung ist es nützlich, die Idealschreibweise aus Lemma 10.3 zu verwenden und eine weitere Bedingung an die betrachteten Ringe zu stellen.

Definition 10.11 (Hauptidealringe)**.** Es sei R ein Integritätsring.

(a) Ein Ideal der Form $\langle a \rangle$ für ein $a \in R$ (also eines, das von nur einem Element erzeugt werden kann) nennt man ein **Hauptideal**.

(b) Man bezeichnet R als einen **Hauptidealring**, wenn jedes Ideal in R ein Hauptideal ist.

Beispiel 10.12. $\mathbb{Z}$ ist ein Hauptidealring, da alle Ideale in diesem Ring nach Beispiel 8.3 (a) von der Form $\langle n \rangle$ für ein $n \in \mathbb{N}$, also Hauptideale sind.

Satz 10.13 (Größte gemeinsame Teiler in Hauptidealringen)**.** *Es seien a und b zwei Elemente in einem Integritätsring R.*

(a) *Ist $g \in R$ mit $\langle a,b \rangle = \langle g \rangle$, so ist $g \in \mathrm{ggT}(a,b)$.*

Insbesondere existiert in einem Hauptidealring also stets ein größter gemeinsamer Teiler von a und b.

(b) *Ist R ein Hauptidealring, so gilt auch die Umkehrung: Ist $g \in \mathrm{ggT}(a,b)$, so ist $\langle a,b \rangle = \langle g \rangle$.*

*Insbesondere gibt es also in einem Hauptidealring zu jedem $g \in \mathrm{ggT}(a,b)$ Elemente $d,e \in R$ mit $g = da + eb$. Diese Aussage wird oft auch als **Lemma von Bézout** bezeichnet.*

Beweis.

(a) Wir überprüfen die beiden Bedingungen aus Definition 10.6:

(1) Nach Voraussetzung gilt $a \in \langle g \rangle$ und $b \in \langle g \rangle$, mit Lemma 10.3 (b) also $g \mid a$ und $g \mid b$.

(2) Es sei c ein gemeinsamer Teiler von a und b, also $c \mid a$ und $c \mid b$ bzw. $a \in \langle c \rangle$ und $b \in \langle c \rangle$. Nach Lemma 8.6 (b) ist dann auch $\langle g \rangle = \langle a,b \rangle \subset \langle c \rangle$, also $g \in \langle c \rangle$ und damit $c \mid g$.

11

(b) Da R ein Hauptidealring ist, gibt es ein $c \in R$ mit $\langle a,b \rangle = \langle c \rangle$. Dieses c ist nach (a) ebenfalls ein größter gemeinsamer Teiler von a und b. Nach Satz 10.8 sind c und g also assoziiert, und damit gilt $\langle a,b \rangle = \langle c \rangle = \langle g \rangle$ nach Lemma 10.3 (c).

Das Lemma von Bézout ergibt sich nun unmittelbar aus $g \in \langle a,b \rangle = \{da + eb : d,e \in R\}$ (siehe Definition 8.5). □

Beispiel 10.14.

(a) Wir haben in Beispiel 10.7 bereits gesehen, dass $6 \in \mathrm{ggT}(12,30)$ in $\mathbb{Z}$ gilt. Da $\mathbb{Z}$ nach Beispiel 10.12 ein Hauptidealring ist, muss sich 6 nach Satz 10.13 (b) also als Linearkombination von 12 und 30 schreiben lassen, was wir wegen $6 = -2 \cdot 12 + 1 \cdot 30$ hier natürlich auch direkt sehen können. Außerdem besagt der Satz auch, dass $\langle 12,30 \rangle = \langle 6 \rangle$ (was man ebenfalls auch direkt überprüfen könnte).

(b) Da in $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ nach Aufgabe 10.10 im Allgemeinen kein größter gemeinsamer Teiler existiert, kann dieser Ring nach Satz 10.13 (a) kein Hauptidealring sein.

(c) Wir betrachten die beiden Elemente 2 und t im Polynomring $\mathbb{Z}[t]$: Nach der Gradformel aus Lemma 9.9 (a) sind Teiler von 2 nur konstante Polynome, also ± 1 und ± 2. Aber ± 2 ist wie in Beispiel 10.2 (b) kein Teiler von t. Damit sind ± 1 die einzigen gemeinsamen Teiler von 2 und t, und es folgt $\mathrm{ggT}(2,t) = \{1,-1\}$.

Beachte aber, dass es keine Linearkombination $f \cdot 2 + g \cdot t = 1$ mit $f,g \in \mathbb{Z}[t]$ geben kann, da der konstante Term des Polynoms auf der linken Seite dieser Gleichung in jedem Fall gerade, auf der rechten aber gleich 1 ist. Satz 10.13 (b) zeigt also, dass $\mathbb{Z}[t]$ kein Hauptidealring sein kann, bzw. dass das Ideal $\langle 2,t \rangle \trianglelefteq \mathbb{Z}[t]$ kein Hauptideal ist.

Um die Situation zu vereinfachen, wollen wir im Rest dieses Kapitels nun nur noch Hauptidealringe betrachten, so dass ein größter gemeinsamer Teiler g von zwei Elementen a und b nach Satz 10.13 also stets existiert und durch die Idealgleichung $\langle a,b \rangle = \langle g \rangle$ charakterisiert ist. Es bleiben dann noch zwei Fragen:

- Wie kann man erkennen, ob ein gegebener Integritätsring ein Hauptidealring ist?
- Wie kann man in einem Hauptidealring zu zwei gegebenen Elementen a und b konkret ein $g \in \mathrm{ggT}(a,b)$ finden, also ein g mit $\langle a,b \rangle = \langle g \rangle$?

In der Tat lassen sich beide Fragen gleichzeitig beantworten, indem man die folgende einfache Umformungsregel für Erzeuger von Idealen geschickt mehrfach anwendet.

Lemma 10.15. *Für alle a,b,q in einem Ring R gilt $\langle a,b \rangle = \langle a,b+qa \rangle$.*

Beweis. Es gilt $a \in \langle a,b+qa \rangle$ und $b = a \cdot (-q) + (b+qa) \in \langle a,b+qa \rangle$, und damit nach Lemma 8.6 (b) auch $\langle a,b \rangle \subset \langle a,b+qa \rangle$.

Analog ist $a \in \langle a,b \rangle$ und $b+qa = a \cdot q + b \in \langle a,b \rangle$ und damit auch $\langle a,b+qa \rangle \subset \langle a,b \rangle$. □

Beispiel 10.16. In $\mathbb{Z}$ können wir das Ideal $\langle 44,10 \rangle$ umformen als

$$\begin{aligned} \langle 44,10 \rangle &\overset{10.15}{=} \langle 44 - 4 \cdot 10, 10 \rangle = \langle 4,10 \rangle \\ &\overset{10.15}{=} \langle 4, 10 - 2 \cdot 4 \rangle = \langle 4,2 \rangle \\ &\overset{10.15}{=} \langle 4 - 2 \cdot 2, 2 \rangle = \langle 0,2 \rangle = \langle 2 \rangle. \end{aligned}$$

Damit haben wir $\langle 44,10 \rangle = \langle 2 \rangle$ als Hauptideal geschrieben; nach Satz 10.13 ist also insbesondere $2 \in \mathrm{ggT}(44,10)$.

Natürlich ist klar, welche Strategie wir hier angewendet haben: Wir haben die jeweils größere Zahl mit Rest durch die kleinere geteilt und konnten sie mit Hilfe von Lemma 10.15 dann durch den Rest dieser Division ersetzen. Da die beteiligten Zahlen bei dieser Vorgehensweise in $\mathbb{N}$ bleiben und immer kleiner werden, ist klar, dass letztlich einmal eine der Zahlen gleich Null werden und das Verfahren somit funktionieren muss.

Die entscheidende Idee bei diesem Verfahren ist also eine Division mit Rest. Eine solche existiert zwar nicht in jedem Integritätsring, aber doch in deutlich mehr Ringen als nur in $\mathbb{Z}$. Wir wollen die Existenz einer solchen Division mit Rest daher jetzt als Eigenschaft eines Ringes definieren. Wie wir sehen werden, wird sie uns sowohl sicherstellen, dass wir einen Hauptidealring haben, als auch ein konkretes Verfahren zur Bestimmung eines größten gemeinsamen Teilers liefern.

Definition 10.17 (Euklidische Ringe)**.** Ein Integritätsring R heißt **euklidischer Ring**, wenn es eine Abbildung $\delta\colon R\backslash\{0\} \to \mathbb{N}$ mit der folgenden Eigenschaft gibt: Für alle $a,b \in R$ mit $b \neq 0$ gibt es $q,r \in R$ mit $a = qb + r$, so dass $r = 0$ oder $\delta(r) < \delta(b)$ ist. (Es muss also eine Division mit Rest geben, wobei der Rest r — sofern er nicht Null ist — „gemessen mit der Funktion δ“ stets kleiner ist als das Element, durch das man geteilt hat.)

Eine Funktion δ mit dieser Eigenschaft wird als **euklidische Funktion** bezeichnet.

Beispiel 10.18. Der Ring $\mathbb{Z}$ ist mit der Funktion $\delta(n) := |n|$ ein euklidischer Ring.

Beachte, dass die Division mit Rest im Sinne von Definition 10.17 in diesem Fall nicht eindeutig ist: Wollen wir z. B. $a = -5$ mit Rest durch $b = 2$ teilen, so wären sowohl $-5 = (-3)\cdot 2 + 1$ als auch $-5 = (-2)\cdot 2 - 1$ wegen $|1| = |-1| < |2|$ erlaubte Ergebnisse. Dies ist jedoch nicht weiter schlimm, denn eine Eindeutigkeit der Division mit Rest wird im Folgenden nicht benötigt (und wurde in Definition 10.17 ja auch nicht verlangt).

Ein zweites und sehr wichtiges Beispiel ist der Polynomring über einem beliebigen Körper, in dem mit der sogenannten Polynomdivision ebenfalls eine Division mit Rest existiert.

Satz 10.19 (**Polynomdivision**)**.** *Es sei K ein Körper. Dann ist der Polynomring $K[t]$ mit der Gradfunktion $\delta(f) := \deg f$ ein euklidischer Ring.*

Mit anderen Worten gibt es also zu je zwei Polynomen $f,g \in K[t]$ mit $g \neq 0$ stets Polynome $q,r \in K[t]$ mit $f = qg + r$ und $\deg r < \deg g$.

Beweis. Es seien $n = \deg f \in \mathbb{N} \cup \{-\infty\}$ und $m = \deg g \in \mathbb{N}$. Wir zeigen den Satz mit Induktion über n. Der Induktionsanfang ist dabei trivial, denn für $n < m$ können wir einfach $q = 0$ und $r = f$ setzen.

Es sei nun also $n \geq m$. Man kann f und g dann schreiben als

$$f = a_n t^n + \cdots + a_1 t + a_0 \quad \text{und} \quad g = b_m t^m + \cdots + b_1 t + b_0$$

mit $a_n, b_m \neq 0$. Wir dividieren nun die jeweils höchsten Terme von f und g durcheinander und erhalten

$$q' := \frac{a_n}{b_m} t^{n-m} \quad \in K[t]$$

(beachte, dass wir $\frac{a_n}{b_m}$ bilden können, weil K ein Körper ist, und t^{n-m}, weil wir $n \geq m$ vorausgesetzt haben). Dies wird unser erster Term im Ergebnis der Division. Subtrahieren wir nun $q'g$ von f, so erhalten wir

$$f - q'g = a_n t^n + \cdots + a_1 t + a_0 - \frac{a_n}{b_m} t^{n-m} \cdot (b_m t^m + \cdots + b_1 t + b_0).$$

Da sich der Term $a_n t^n$ in diesem Ausdruck weghebt, ist $\deg(f - q'g) < n$. Wir können also die Induktionsvoraussetzung auf $f - q'g$ anwenden und erhalten Polynome $q'', r \in K[t]$ mit $\deg r < \deg g$ und

$$f - q'g = q''g + r, \quad \text{also} \quad f = (q' + q'')g + r.$$

Setzen wir nun $q = q' + q''$, so erhalten wir offensichtlich genau den gewünschten Ausdruck. □

Beispiel 10.20. Der Beweis von Satz 10.19 ist konstruktiv, d. h. er gibt auch ein Verfahren an, mit dem man die Division von $f \in K[t]$ durch $g \in K[t]\backslash\{0\}$ konkret durchführen kann: Man muss einfach den höchsten Term von f durch den höchsten Term von g teilen, dies als ersten Teil q' des Ergebnisses hinschreiben, und das Verfahren dann mit $f - q'g$ fortsetzen — so lange, bis der Grad dieses Polynoms kleiner ist als der von g. Wollen wir z. B. in $\mathbb{R}[t]$ das Polynom $f = 2t^2 + 1$ durch $g = t - 2$ dividieren, so können wir dies wie folgt aufschreiben (wobei wir im ersten Schritt zur Verdeutlichung die Notationen von oben noch mit an die Rechnung geschrieben haben):

$$\begin{array}{rl} & (2t^2+1) \,:\, (t-2) \;=\; 2t+4 \\ q'g \longrightarrow & -\,\underline{(2t^2-4t)} \qquad\qquad \uparrow \\ & \qquad 4t+1 \qquad\qquad = \frac{2t^2}{t} =: q' \\ f - q'g \longrightarrow & -\,\underline{(4t-8)} \\ & \qquad\; 9 \end{array}$$

Das Ergebnis ist also $2t^2 + 1 = (2t+4)\cdot(t-2) + 9$ (d. h. $q = 2t+4$ und $r = 9$). Zur Kontrolle der Rechnung kann man diese Gleichheit durch Ausmultiplizieren natürlich auch direkt überprüfen.

Wie bereits angekündigt wollen wir nun sehen, dass euklidische Ringe stets Hauptidealringe sind.

Satz 10.21. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Es sei I ein Ideal in einem euklidischen Ring R. Ist $I = \{0\}$, so sind wir offensichtlich fertig, denn dann ist ja $I = \langle 0 \rangle$. Andernfalls wählen wir ein Element $g \in I\backslash\{0\}$, für das die euklidische Funktion δ minimal ist — ein solches Element existiert in jedem Fall, da δ ja nur natürliche Zahlen als Werte annimmt und jede nicht-leere Menge natürlicher Zahlen ein Minimum besitzt.

Wir behaupten nun, dass $I = \langle g \rangle$ gilt und I somit ein Hauptideal ist. Die Inklusion $I \supset \langle g \rangle$ ist dabei wegen $g \in I$ klar nach Lemma 8.6 (b). Für die umgekehrte Inklusion $I \subset \langle g \rangle$ sei $a \in I$ beliebig. Wir dividieren a gemäß Definition 10.17 mit Rest durch g und erhalten

$$a = qg + r \qquad (*)$$

für gewisse $q, r \in R$ mit $r = 0$ oder $\delta(r) < \delta(g)$. Wegen $a \in I$ und $g \in I$ ist nun aber auch $r = a - qg \in I$ nach Definition 8.1. Da g ein Element mit minimaler euklidischer Funktion in I war, kann also nicht $\delta(r) < \delta(g)$ gelten. Damit ist notwendigerweise $r = 0$, und mit $(*)$ folgt $a = qg \in \langle g \rangle$. □

Beispiel 10.22. Neben $\mathbb{Z}$ ist nach Satz 10.19 also auch der Polynomring über einem Körper ein Hauptidealring. Dies sind sicher die beiden wichtigsten Beispiele für Hauptidealringe. Zwei weitere ergeben sich aus den folgenden beiden Aufgaben.

Aufgabe 10.23. Zeige, dass der Ring $\mathbb{Z}[\mathrm{i}] = \{a + b\,\mathrm{i} : a, b \in \mathbb{Z}\}$ (siehe Aufgabe 7.24 (a)) mit der Funktion $\delta(z) := |z|^2$ ein euklidischer Ring (und damit ein Hauptidealring) ist.

Aufgabe 10.24. Es sei K ein Körper. Zeige, dass jedes Ideal $I \trianglelefteq K[\![t]\!]$ mit $I \neq \langle 0 \rangle$ von der Form $\langle t^n \rangle$ für ein $n \in \mathbb{N}$ ist. Insbesondere ist $K[\![t]\!]$ also ein Hauptidealring.

Bemerkung 10.25. Man kann zeigen, dass es Hauptidealringe gibt, die nicht euklidisch sind. Eines der einfachsten Beispiele hierfür ist der Ring $\mathbb{Z}\left[\frac{1+\sqrt{19}\,\mathrm{i}}{2}\right]$ in der Notation aus Bemerkung 9.18 (b). Der Beweis dieser Tatsache ist jedoch recht aufwändig und soll hier nicht gegeben werden.

Ist I ein Ideal in einem Hauptidealring R, so besagt der Beweis von Satz 10.21 bereits, wie wir ein Element $g \in R$ mit $I = \langle g \rangle$ finden können: Wir können in $I\backslash\{0\}$ ein Element mit minimaler euklidischer Funktion suchen. Dies ist oftmals aber nur schwer durchführbar. Für Ideale der Form $I = \langle a, b \rangle$, die für die Bestimmung von $\mathrm{ggT}(a, b)$ benötigt werden, ist das folgende an Beispiel 10.16 angelehnte Verfahren deutlich einfacher.

Satz 10.26 (Euklidischer Algorithmus). *Es seien R ein euklidischer Ring und $a_1, a_2 \in R$.*

Wir konstruieren daraus nun wie folgt rekursiv eine (abbrechende) Folge $a_1, a_2, \dots, a_N$ in R: Sind $a_1, \dots, a_{n-1} \in R$ für ein $n \geq 3$ bereits bestimmt und ist $a_{n-1} \neq 0$, so teilen wir a_{n-2} wie in Definition 10.17 mit Rest durch a_{n-1} und erhalten so eine Darstellung

$$a_{n-2} = q_n a_{n-1} + r_n$$

für gewisse $q_n, r_n \in R$. Wir setzen dann $a_n := r_n = a_{n-2} - q_n a_{n-1}$.

Die so konstruierte Folge bricht nach endlich vielen Schritten ab, d. h. es ist $a_N = 0$ für ein $N \in \mathbb{N}$, und es gilt dann $\langle a_1, a_2 \rangle = \langle a_{N-1} \rangle$. Insbesondere ist das letzte Folgenglied a_{N-1}, das nicht Null ist, nach Satz 10.13 (a) also ein größter gemeinsamer Teiler von a_1 und a_2.

Beweis. Angenommen, die Folge $a_1, a_2, \dots$ würde nicht abbrechen, d. h. es wäre $a_n \neq 0$ für alle $n \in \mathbb{N}$. Nach der Definition eines euklidischen Ringes wäre dann $\delta(a_n) = \delta(r_n) < \delta(a_{n-1})$ für alle $n \geq 3$. Die Zahlen $\delta(a_n)$ müssten für $n \geq 2$ also eine unendliche, streng monoton fallende Folge natürlicher Zahlen bilden, was offensichtlich nicht möglich ist.

Nun gilt für alle $n \geq 3$

$$\langle a_{n-1}, a_n \rangle = \langle a_{n-1}, r_n \rangle = \langle a_{n-1}, a_{n-2} - q_n a_{n-1} \rangle \overset{10.15}{=} \langle a_{n-2}, a_{n-1} \rangle,$$

und daher mit Induktion über n

$$\langle a_1, a_2 \rangle = \langle a_2, a_3 \rangle = \dots = \langle a_{N-1}, a_N \rangle = \langle a_{N-1}, 0 \rangle = \langle a_{N-1} \rangle. \qquad \square$$

Algorithmus 10.27 (Erweiterter euklidischer Algorithmus). Satz 10.26 bestimmt zu zwei Elementen a_1, a_2 eines euklidischen Ringes R ein Element a_{N-1} mit $\langle a_1, a_2 \rangle = \langle a_{N-1} \rangle$. Wegen $a_{N-1} \in \langle a_1, a_2 \rangle$ lässt sich a_{N-1} dann also insbesondere als Linearkombination $a_{N-1} = d a_1 + e a_2$ der Ausgangselemente a_1 und a_2 mit geeigneten $d, e \in R$ schreiben.

Oft möchte man auch diese Elemente d und e konkret berechnen. Dies ist durch eine kleine Erweiterung des Algorithmus aus Satz 10.26 möglich: Statt nur der Elemente a_n berechnen wir zeilenweise eine Tabelle mit Zeilen (a_n, d_n, e_n) für $n = 1, 2, \dots, N-1$, so dass in jeder Zeile $a_n = d_n a_1 + e_n a_2$ gilt. Dies ist sehr einfach: In die ersten beiden Zeilen können wir $(a_1, 1, 0)$ und $(a_2, 0, 1)$ schreiben, denn es ist ja $a_1 = 1 \cdot a_1 + 0 \cdot a_2$ und $a_2 = 0 \cdot a_1 + 1 \cdot a_2$. Berechnen wir nun a_n aus a_{n-2} und a_{n-1} als $a_n = a_{n-2} - q_n a_{n-1}$ wie in Satz 10.26, so führen wir die gleiche Rechnung in allen drei Spalten der Tabelle durch, setzen also auch $d_n = d_{n-2} - q_n d_{n-1}$ und $e_n = e_{n-2} - q_n e_{n-1}$. Dann folgt mit Induktion für alle n

$$a_n = a_{n-2} - q_n a_{n-1} = (d_{n-2} a_1 + e_{n-2} a_2) - q_n (d_{n-1} a_1 + e_{n-1} a_2) = d_n a_1 + e_n a_2,$$

und damit steht dann in der letzten Zeile $(a_{N-1}, d_{N-1}, e_{N-1})$ das gewünschte Ergebnis, so dass $a_{N-1} = d_{N-1} a_1 + e_{N-1} a_2$ gilt.

Die Tabelle unten zeigt dies konkret im Fall der beiden gegebenen Zahlen $a_1 = 11$ und $a_2 = 9$ in $\mathbb{Z}$. Für $n \geq 3$ entsteht der Eintrag a_n der ersten Spalte jeweils dadurch, dass man von a_{n-2} so oft wie möglich a_{n-1} abzieht, also den Rest der Division von a_{n-2} durch a_{n-1} hinschreibt. Dies ist durch die Pfeile auf der linken Seite der Tabelle angedeutet. In den anderen beiden Spalten machen wir (wie durch die Pfeile auf der rechten Seite angedeutet) exakt die gleichen Umformungen. Das gesuchte Ergebnis steht am Ende in der letzten Zeile, die nicht mit 0 beginnt: Im Beispiel unten ist dies $(1, -4, 5)$, und es besagt, dass $\langle 11, 9 \rangle = \langle 1 \rangle$ bzw. $1 \in \mathrm{ggT}(11, 9)$ gilt, und dass $1 = -4 \cdot 11 + 5 \cdot 9$ ist.

$11 - 1 \cdot 9 = 2$
$9 - 4 \cdot 2 = 1$
$2 - 2 \cdot 1 = 0$

a_n	d_n	e_n
11	1	0
9	0	1
2	1	-1
1	-4	5
0		

$(1,0) - 1 \cdot (0,1) = (1,-1)$
$(0,1) - 4 \cdot (1,-1) = (-4,5)$

12

Bemerkung 10.28. Das Verfahren aus Satz 10.26 lässt sich leicht auf mehr als zwei Elemente verallgemeinern: Sind $a_1,\dots,a_n$ Elemente in einem euklidischen Ring R und bestimmen wir mit Satz 10.26 ein $g \in \mathrm{ggT}(a_1,a_2)$, also mit $\langle a_1,a_2\rangle = \langle g\rangle$, so ist

$$\langle a_1,a_2,a_3,\dots,a_n\rangle = \langle g,a_3,\dots,a_n\rangle.$$

Auf diese Art können wir dann also rekursiv auch jedes Ideal, das von endlich vielen Elementen erzeugt wird, als Hauptideal schreiben: Man muss nur fortlaufend zwei Erzeuger durch einen größten gemeinsamen Teiler von ihnen ersetzen.

Bemerkung 10.29. Fassen wir die wichtigsten Ergebnisse dieses Kapitels zur Existenz und Eindeutigkeit von größten gemeinsamen Teilern zusammen, so sehen wir also:

> In einem Hauptidealring R existiert zu je zwei Elementen a und b stets ein größter gemeinsamer Teiler g, der bis auf Multiplikation mit Einheiten eindeutig bestimmt ist und sich als $g = da+eb$ mit $d,e \in R$ darstellen lässt.
>
> In euklidischen Ringen wie z. B. $\mathbb{Z}$ und Polynomringen über einem Körper können g sowie d und e mit dem (erweiterten) euklidischen Algorithmus berechnet werden.

Notation 10.30 (ggT und ggt)**.** In $\mathbb{Z}$ und $K[t]$ für einen Körper K können wir die Nichteindeutigkeit des größten gemeinsamen Teilers in Bemerkung 10.29 leicht durch eine Konvention beseitigen:

(a) Im Ring $R=\mathbb{Z}$ ist die Einheitengruppe $\mathbb{Z}^* = \{1,-1\}$. In diesem Fall besitzen zwei beliebige ganze Zahlen $m,n \in \mathbb{Z}$ also stets einen *eindeutigen nicht-negativen* größten gemeinsamen Teiler, den wir im Folgenden mit $\mathrm{ggt}(m,n) \in \mathbb{Z}$ bezeichnen werden — im Unterschied zur *Menge* $\mathrm{ggT}(m,n) = \{\mathrm{ggt}(m,n), -\mathrm{ggt}(m,n)\} \subset \mathbb{Z}$.

(b) Im Polynomring $R=K[t]$ über einem Körper K ist $K[t]^* = K^* = K\backslash\{0\}$ nach Lemma 9.9 (c), d. h. der größte gemeinsame Teiler zweier Polynome ist eindeutig bis auf Multiplikation mit einer Konstanten ungleich 0. In diesem Fall existiert zu zwei Polynomen $f,g \in K[t]$, die nicht beide gleich Null sind, also stets ein *eindeutiger normierter* größter gemeinsamer Teiler, den wir wieder mit $\mathrm{ggt}(f,g) \in K[t]$ bezeichnen.

Eine sehr wichtige Anwendung des erweiterten euklidischen Algorithmus ist, dass wir mit seiner Hilfe multiplikative Inverse in Faktorringen wie z. B. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ konkret berechnen können. Bisher hatten wir hierzu ja nur in Satz 7.10 gesehen, dass in $\mathbb{Z}_n$ für eine Primzahl n *jedes* Element ungleich 0 ein multiplikatives Inverses besitzt — wir wussten aber noch nicht, wie wir dieses ohne Ausprobieren bestimmen können.

Folgerung 10.31 (Inversenberechnung in Faktorringen)**.** *Es seien a und b Elemente eines Hauptidealringes R und $b \notin R^*$ (so dass also $R/\langle b\rangle$ nicht der Nullring ist). Dann gilt*

$$\overline{a} \text{ ist eine Einheit in } R/\langle b\rangle \quad\Leftrightarrow\quad a \text{ und } b \text{ sind teilerfremd.}$$

Schreiben wir dann $da+eb=1$ für gewisse $d,e \in R$ wie in Satz 10.13 (b), so ist $\overline{a}^{-1} = \overline{d}$ in $R/\langle b\rangle$.

Beweis. Es gilt

$$\begin{aligned}
&\overline{a} \text{ ist eine Einheit in } R/\langle b\rangle \\
\Leftrightarrow\ &\text{es gibt ein } d \in R \text{ mit } \overline{d}\,\overline{a} = \overline{1} \text{ in } R/\langle b\rangle \\
\Leftrightarrow\ &\text{es gibt ein } d \in R \text{ mit } 1-da \in \langle b\rangle \\
\Leftrightarrow\ &\text{es gibt } d,e \in R \text{ mit } da+eb=1 && \text{(Beispiel 8.8 (a))} \\
\Leftrightarrow\ &\langle a,b\rangle = \langle 1\rangle = R \\
\Leftrightarrow\ &1 \in \mathrm{ggT}(a,b) && \text{(Satz 10.13),}
\end{aligned}$$

und in diesem Fall ist dann offensichtlich $\overline{a}^{-1} = \overline{d}$. □

Beispiel 10.32.

(a) Die Einheiten von $\mathbb{Z}_{10}$ sind nach Folgerung 10.31 die Klassen aller zu 10 teilerfremden Zahlen, also $\mathbb{Z}_{10}^* = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$.

(b) Aus der Gleichung $1 = -4 \cdot 11 + 5 \cdot 9$ im Beispiel von Algorithmus 10.27 erhalten wir sofort $\overline{5}^{-1} = \overline{9}$ in $\mathbb{Z}_{11}$.

Aufgabe 10.33. Bestimme $\operatorname{Im} f$ für den Gruppenhomomorphismus

$$f \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ (m,n) \mapsto 693m + 483n,$$

und gib für jedes $a \in \operatorname{Im} f$ explizit ein Urbild in $f^{-1}(\{a\})$ an.

Aufgabe 10.34. Es seien $f = t^5 + \overline{2}t^3 - t$ und $g = \overline{2}t^3 + t^2 + \overline{1}$ in $\mathbb{Z}_5[t]$.

(a) Berechne alle größten gemeinsamen Teiler von f und g und stelle einen von ihnen in der Form $df + eg$ mit $d, e \in \mathbb{Z}_5[t]$ dar.

(b) Liegt das Polynom $t^3 + t^2 + \overline{1}$ im Ideal $\langle f, g \rangle$?

(c) Ist $\overline{t^{1000}}$ eine Einheit in $\mathbb{Z}_5[t]/\langle f, g \rangle$?

Aufgabe 10.35. Zeige, dass für alle $q, m, n \in \mathbb{N}_{>0}$ mit $q \neq 1$ gilt, dass

$$\operatorname{ggt}(q^m - 1, q^n - 1) = q^{\operatorname{ggt}(m,n)} - 1.$$

Aufgabe 10.36. Es sei $I_0 \subset I_1 \subset I_2 \subset \cdots$ eine Folge von Idealen in einem Ring R, von denen jedes im nächsten enthalten ist (man spricht in diesem Fall auch von einer aufsteigenden Kette von Idealen).

(a) Zeige, dass die Vereinigung $\bigcup_{n \in \mathbb{N}} I_n$ aller dieser Ideale wieder ein Ideal in R ist.

(b) Ist R ein Hauptidealring, so zeige man, dass die Kette von Idealen ab einem gewissen Glied konstant ist, d. h. dass es ein $n_0 \in \mathbb{N}$ gibt mit $I_n = I_{n_0}$ für alle $n \geq n_0$.

(c) Gib ein Beispiel für einen Ring R und eine aufsteigende Idealkette in R an, die nicht ab einem gewissen Glied konstant ist.

Aufgabe 10.37. Es sei $I_0 \supsetneq I_1 \supsetneq I_2 \supsetneq \cdots$ eine unendliche Folge von Idealen in $\mathbb{R}[t]$. Zeige, dass $\bigcap_{n=0}^{\infty} I_n = \{0\}$.

11. Primfaktorzerlegungen

Euch ist sicher aus der Schule bekannt, dass sich jede positive ganze Zahl a als ein Produkt $a = p_1 \cdot \cdots \cdot p_n$ von Primzahlen schreiben lässt, und dass diese Darstellung bis auf die Reihenfolge der Faktoren eindeutig ist. Bei der Betrachtung von Teilern spielt diese sogenannte Primfaktorzerlegung eine große Rolle: Kennt man die Primfaktorzerlegung von a, so kann man daraus sofort alle Teiler von a ablesen, da dies genau die Zahlen sind, die sich als Produkte von einigen der Faktoren $p_1, \ldots, p_n$ schreiben lassen. Der größte gemeinsame Teiler zweier Zahlen a und b (im Sinne von Notation 10.30 (a)) ist dann also genau das Produkt aller Primfaktoren (mit entsprechenden Potenzen), die in beiden Zahlen auftreten.

Wir wollen nun untersuchen, in wie weit etwas Analoges auch in beliebigen Integritätsringen existiert. Es ist klar, dass wir dafür zunächst erst einmal definieren müssen, was wir unter einem „Primelement“ in einem beliebigen Integritätsring überhaupt verstehen wollen. Denken wir hierfür noch einmal an den uns bekannten Fall des Ringes $\mathbb{Z}$: Was genau ist eigentlich eine Primzahl? Die meisten von euch würden hierauf wahrscheinlich antworten, dass eine Zahl p (positiv und größer als 1) eine Primzahl heißt, wenn sie außer 1 und p keine weiteren (positiven) Teiler besitzt. Diese Antwort ist natürlich letztlich auch richtig — allerdings ist dies *nicht* die Eigenschaft, durch die man in allgemeinen Integritätsringen Primelemente definiert. Stattdessen wird ein Element mit dieser Eigenschaft *irreduzibel* genannt und die Primeigenschaft zunächst einmal anders definiert:

Definition 11.1 (Primelemente und irreduzible Elemente)**.** Es seien R ein Integritätsring und $p \in R$ mit $p \neq 0$ und $p \notin R^*$.

(a) p heißt **irreduzibel**, wenn für alle $a, b \in R$ mit $p = a \cdot b$ gilt, dass $a \in R^*$ oder $b \in R^*$ ist.

(b) p heißt **prim**, wenn für alle $a, b \in R$ mit $p \mid a \cdot b$ gilt, dass $p \mid a$ oder $p \mid b$ ist.

Bemerkung 11.2.

(a) Nach Definition 11.1 (a) ist p genau dann irreduzibel, wenn jeder Teiler von p (also a in der Gleichung $p = a \cdot b$) entweder eine Einheit oder zu p assoziiert ist, d. h. wenn 1 und p bis auf Multiplikation mit Einheiten die einzigen Teiler von p sind. Dies ist also genau die Eigenschaft, über die normalerweise Primzahlen definiert werden.

(b) Denken wir wieder an die Primfaktorzerlegung in $\mathbb{Z}$, so ist es dort einleuchtend, dass auch die Eigenschaft (b) aus Definition 11.1 (für positive Zahlen) genau die Primzahlen charakterisiert: Wenn eine Primzahl p als Faktor im Produkt $a \cdot b$ enthalten ist, muss sie natürlich in der Primfaktorzerlegung von a oder b enthalten sein. Ist p hingegen keine Primzahl und kann auf nicht-triviale Art als Produkt $k \cdot l$ geschrieben werden, so könnte hingegen z. B. der Faktor k in a und l in b enthalten sein, so dass $p = k \cdot l$ zwar ein Teiler von $a \cdot b$, aber nicht von a oder b ist.

In $\mathbb{Z}$ scheinen die beiden in Definition 11.1 eingeführten Begriffe also übereinzustimmen. In der Tat werden wir dies in Bemerkung 11.6 auch noch beweisen. Gilt dies auch in allgemeinen Integritätsringen? Eine der beiden Implikationen ist einfach:

Lemma 11.3 („prim $\Rightarrow$ irreduzibel“)**.** *In einem Integritätsring ist jedes Primelement irreduzibel.*

Beweis. Es seien R ein Integritätsring und $p \in R$ prim. Ferner seien $a, b \in R$ mit $p = a \cdot b$. Dann gilt natürlich auch $p \mid a \cdot b$, und daher muss p als Primelement ein Teiler von a oder b sein. Nach evtl. Umbenennen der Elemente können wir $p \mid a$ annehmen, also $a = pc$ für ein $c \in R$. Einsetzen in $p = a \cdot b$ liefert dann $p = pcb$, nach der Kürzungsregel aus Lemma 7.8 (c) also $1 = cb$. Also ist $b \in R^*$ und p somit irreduzibel. □

Leider gilt die Umkehrung dieses Lemmas jedoch nicht — wie ihr wohl schon vermuten werdet, wenn es zwei unterschiedliche Namen für diese beiden Eigenschaften gibt.

Beispiel 11.4 („irreduzibel $\not\Rightarrow$ prim“)**.** Es sei $R = \mathbb{Z}[\sqrt{5}\mathrm{i}]$ wieder der Ring aus Aufgabe 7.24 (a). Wie in Aufgabe 10.10 zeigt man schnell, dass die Zahl 2 bis auf Einheiten nur die Teiler 1 und 2 in R besitzt und damit irreduzibel in R ist. Allerdings gilt in R auch

$$(1+\sqrt{5}\mathrm{i})(1-\sqrt{5}\mathrm{i}) = 6 = 2\cdot 3 \quad \text{und damit} \quad 2 \,|\, (1+\sqrt{5}\mathrm{i})(1-\sqrt{5}\mathrm{i}),$$

und da 2 wegen $\frac{1\pm\sqrt{5}\mathrm{i}}{2} \notin R$ kein Teiler von $1\pm\sqrt{5}\mathrm{i}$ ist, ist 2 nicht prim in R.

In diesem Ring R ist also nicht jedes irreduzible Element prim. Das Gegenbeispiel, das wir hier für die Umkehrung von Lemma 11.3 gefunden haben, ist damit effektiv wieder das gleiche wie das, mit dem wir in Kapitel 10 gesehen haben, dass in beliebigen Integritätsringen nicht notwendig ein größter gemeinsamer Teiler zweier Elemente existieren muss.

Wir wollen nun aber sehen, dass die Umkehrung von Lemma 11.3 zumindest in Hauptidealringen gilt.

Satz 11.5. *In einem Hauptidealring ist jedes irreduzible Element prim.*

Beweis. Es sei p ein irreduzibles Element in einem Hauptidealring R. Ferner seien $a,b \in R$ mit $p \,|\, a\cdot b$. Wir müssen zeigen, dass $p \,|\, a$ oder $p \,|\, b$ gilt.

Da R ein Hauptidealring ist, existiert nach Satz 10.13 (a) ein größter gemeinsamer Teiler von a und p. Allerdings ist p nach Voraussetzung irreduzibel und hat daher nach Bemerkung 11.2 (a) bis auf Multiplikation mit Einheiten überhaupt nur die Teiler 1 und p. Der größte gemeinsame Teiler von a und p muss also einer von diesen beiden sein:

- Ist $p \in \mathrm{ggT}(a,p)$, so gilt natürlich $p \,|\, a$ und wir sind fertig.
- Ist $1 \in \mathrm{ggT}(a,p)$, so haben wir nach Lemma 10.13 (b) eine Darstellung $1 = da + ep$ für gewisse $d,e \in R$. Multiplizieren wir diese Gleichung mit b, so erhalten wir wegen $p \,|\, ab$, also $ab \in \langle p \rangle$, auch

$$b = dab + epb \in \langle p \rangle \quad \text{und damit} \quad p \,|\, b. \qquad \square$$

Bemerkung 11.6. Für Hauptidealringe, nach Beispiel 10.22 also z. B. für $\mathbb{Z}$ oder Polynomringe über einem Körper, stimmen die Begriffe „irreduzibel“ und „prim“ nach Lemma 11.3 und Satz 11.5 also überein. Im Ring $\mathbb{Z}$ sind die positiven Elemente mit dieser Eigenschaft nach Definition genau die Primzahlen.

Aufgabe 11.7. Es seien R ein Integritätsring und $p \in R$ mit $p \neq 0$ und $p \notin R^*$. Ferner sei $c \in R^*$ eine Einheit. Man zeige:

(a) p ist genau dann irreduzibel, wenn $c \cdot p$ es ist.

(b) p ist genau dann prim, wenn $c \cdot p$ es ist.

Aufgabe 11.8.

(a) Zeige, dass das Polynom $t^4+t^3+t^2+t+1$ prim in $\mathbb{Z}_2[t]$ ist.

(b) Ist das Polynom $t^4 - 13t^3 + 37t^2 + 3t - 99$ irreduzibel in $\mathbb{Z}[t]$?

Mit diesen Vorbereitungen wollen wir nun Primfaktorzerlegungen untersuchen. Da wir hierfür *beide* Eigenschaften aus Definition 11.1 benötigen werden, können wir dies nur in Hauptidealringen durchführen.

Satz 11.9 (Primfaktorzerlegung in Hauptidealringen)**.** *Es seien R ein Hauptidealring und $a \in R$ mit $a \neq 0$ und $a \notin R^*$. Dann gilt:*

(a) *Es gibt ein $n \in \mathbb{N}_{>0}$ und Primelemente $p_1,\dots,p_n \in R$, so dass $a = p_1 \cdot \dots \cdot p_n$. Man nennt eine solche Darstellung eine **Primfaktorzerlegung** von a.*

(b) *Die Darstellung aus (a) ist „bis auf die Reihenfolge und bis auf Multiplikation mit Einheiten eindeutig“, d. h. sind $a = p_1 \cdot \dots \cdot p_n$ und $a = q_1 \cdot \dots \cdot q_m$ zwei Primfaktorzerlegungen wie in (a), so gilt $n = m$, und nach evtl. Umbenennen der $q_1, \dots, q_m$ ist $q_i = c_i\, p_i$ für gewisse $c_i \in R^*$ und alle $i = 1, \dots, n$.*

Beweis.

(a) Angenommen, a hätte keine solche Primfaktorzerlegung. Wir konstruieren dann wie folgt rekursiv eine Folge $a_0, a_1, a_2, \dots$ von Elementen aus $R \backslash R^* \backslash \{0\}$, die ebenfalls allesamt keine Primfaktorzerlegung besitzen: Als Startwert wählen wir $a_0 := a$. Ist nun a_n für ein $n \in \mathbb{N}$ bereits konstruiert und besitzt keine Primfaktorzerlegung, so ist a_n natürlich insbesondere nicht selbst prim, nach Satz 11.5 also auch nicht irreduzibel, und kann damit in der Form $a_n = a_{n+1} \cdot b_{n+1}$ geschrieben werden, wobei weder a_{n+1} noch b_{n+1} eine Einheit ist. Von diesen beiden Elementen kann mindestens eines keine Primfaktorzerlegung besitzen, da sonst $a_n = a_{n+1} b_{n+1}$ auch eine hätte. Nach evtl. Vertauschen von a_{n+1} mit b_{n+1} können wir also annehmen, dass a_{n+1} keine Primfaktorzerlegung besitzt, und das Verfahren so rekursiv fortsetzen.

Nach Konstruktion gilt nun $a_n \in \langle a_{n+1} \rangle$ und damit $\langle a_n \rangle \subset \langle a_{n+1} \rangle$ für alle n. Dabei ist die Gleichheit $\langle a_n \rangle = \langle a_{n+1} \rangle$ ausgeschlossen, denn sonst wäre $a_{n+1} = a_n c_n$ für ein $c_n \in R$, woraus aber $a_n = a_{n+1} b_{n+1} = a_n c_n b_{n+1}$ und damit nach der Kürzungsregel $1 = c_n b_{n+1}$ folgen würde — was ein Widerspruch dazu wäre, dass b_{n+1} keine Einheit ist. Wir erhalten also eine unendliche aufsteigende Kette von Idealen

$$\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$$

in R, die nach Aufgabe 10.36 (b) aber in einem Hauptidealring nicht existieren kann.

(b) Es seien nun $p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$ zwei Primfaktorzerlegungen von a. Wir können ohne Einschränkung $n \leq m$ annehmen und zeigen nun die behauptete Gleichheit der Zerlegungen mit Induktion über n.

Da p_1 prim und ein Teiler von $q_1 \cdot \dots \cdot q_m$ ist, muss p_1 nach Definition 11.1 (b) einen der Faktoren $q_1, \dots, q_m$ teilen. Nach evtl. Umnummerieren können wir also $p_1 \,|\, q_1$ annehmen, d. h. es ist $q_1 = c_1\, p_1$ für ein $c_1 \in R$. Da aber auch q_1 prim und somit nach Lemma 11.3 auch irreduzibel ist, muss $c_1 \in R^*$ gelten. Teilen wir aus dem Ausdruck für a nun mit Hilfe der Kürzungsregel aus Lemma 7.8 (c) den Faktor p_1 heraus, so erhalten wir

$$p_2 \cdot \dots \cdot p_n = (c_1 q_2) \cdot q_3 \cdot \dots \cdot q_m. \qquad (*)$$

Wir können nun die bereits angekündigte Induktion über n durchführen:

- $n = 1$: In diesem Fall besagt $(*)$ gerade $1 = c_1 q_2 \cdot q_3 \cdot \dots \cdot q_m$, d. h. $q_2, \dots, q_m$ sind Einheiten. Da Primelemente aber nach Definition 11.1 keine Einheiten sein können, muss $m = 1$ gelten, und der Beweis ist in diesem Fall fertig.
- $n - 1 \to n$: Beachte, dass in $(*)$ nach Aufgabe 11.7 mit q_2 auch $c_1 q_2$ prim ist. Anwenden der Induktionsannahme auf $(*)$ liefert also sofort die Behauptung. □

Bemerkung 11.10. In den wichtigsten Hauptidealringen $\mathbb{Z}$ und $K[t]$ für einen Körper K können wir die Eindeutigkeit bis auf Einheiten in Satz 11.9 noch auf einfache Art durch eine „echte Eindeutigkeit“ ersetzen:

(a) In $\mathbb{Z}$ sind die Einheiten genau ± 1. Beschränken wir uns hier also auf positive Zahlen und Zerlegungen in positive Primfaktoren, so besagt Satz 11.9 gerade, dass sich jedes $n \in \mathbb{N}_{>1}$ (bis auf die Reihenfolge) eindeutig als Produkt von (positiven) Primzahlen schreiben lässt. Diese Aussage, die ihr ja sicher schon aus der Schule kennt, wird oft als **Hauptsatz der elementaren Zahlentheorie** bezeichnet.

(b) Im Polynomring $K[t]$ über einem Körper K ist $K[t]^* = K^* = K \backslash \{0\}$ nach Lemma 9.9 (c) und Definition 7.6 (b), d. h. die Einheiten in $K[t]$ sind genau die konstanten Polynome ungleich Null. Es gibt also offensichtlich zu jedem Polynom $f = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$ (mit

$n = \deg f \in \mathbb{N}$, also $a_n \neq 0$) genau ein *normiertes* Polynom, das sich von f nur durch Multiplikation mit einer Einheit unterscheidet, nämlich $\frac{1}{a_n} \cdot f$. Aus Satz 11.9 erhalten wir damit die Aussage, dass sich jedes normierte Polynom in $K[t]$ bis auf die Reihenfolge eindeutig als Produkt von normierten irreduziblen Polynomen schreiben lässt.

Aufgabe 11.11. Zerlege die Zahl 15 im Ring $\mathbb{Z}[\mathrm{i}]$ (der nach Aufgabe 10.23 ein Hauptidealring ist) in Primfaktoren.

Kennt man die Primfaktorzerlegung von Elementen, so lassen sich damit wie folgt sehr einfach größte gemeinsame Teiler (und auch kleinste gemeinsame Vielfache) bestimmen.

Folgerung 11.12 (Größte gemeinsame Teiler und kleinste gemeinsame Vielfache aus Primfaktorzerlegungen)**.** *Es seien $a, b \in R \backslash R^* \backslash \{0\}$ zwei Elemente in einem Hauptidealring R, die wir bis auf Multiplikation mit Einheiten als Primfaktorzerlegungen $a = a_0 p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ und $b = b_0 p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ schreiben, wobei $a_0, b_0 \in R^*$ und $k_1, \ldots, k_n, l_1, \ldots, l_n \in \mathbb{N}$ gilt und die $p_1, \ldots, p_n$ paarweise nicht assoziierte Primelemente sind.*

(a) *Es gilt $b \mid a$ genau dann wenn $l_i \leq k_i$ für alle i.*

(b) *Ein größter gemeinsamer Teiler von a und b ist $p_1^{\min(k_1,l_1)} \cdot \ldots \cdot p_n^{\min(k_n,l_n)}$.*

(c) *Ein kleinstes gemeinsames Vielfaches von a und b ist $p_1^{\max(k_1,l_1)} \cdot \ldots \cdot p_n^{\max(k_n,l_n)}$.*

Insbesondere existiert zu a und b also immer ein kleinstes gemeinsames Vielfaches (und ist dann nach Bemerkung 10.9 eindeutig bestimmt).

Beweis.

(a) „$\Rightarrow$“: Es gelte $b \mid a$, also $a = bc$ für ein $c \in R$. Schreiben wir auch c in seiner Primfaktorzerlegung $c = c_0 p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$ mit $c_0 \in R^*$ (wobei wir die vorkommenden Primfaktoren bei Bedarf ergänzen und die zugehörigen Exponenten für a und b gleich 0 setzen), so bedeutet die Gleichung $a = bc$ gerade

$$a_0 p_1^{k_1} \cdot \ldots \cdot p_n^{k_n} = b_0 c_0 p_1^{l_1+m_1} \cdot \ldots \cdot p_n^{l_n+m_n}.$$

Wegen der Eindeutigkeit der Primfaktorzerlegung folgt hieraus nun sofort $k_i = l_i + m_i$ (und $a_0 = b_0 c_0$), und damit $l_i \leq k_i$ für alle i.

„$\Leftarrow$“: Ist $l_i \leq k_i$ für alle i, so gilt natürlich $a = bc$ mit $c = \frac{a_0}{b_0} p_1^{k_1-l_1} \cdot \ldots \cdot p_n^{k_n-l_n}$, und damit $b \mid a$.

(b) Dies ergibt sich unmittelbar daraus, dass ein Element $p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$ von R nach (a) genau dann ein gemeinsamer Teiler von a und b ist, wenn $m_i \leq k_i$ und $m_i \leq l_i$, also $m_i \leq \min(k_i, l_i)$ gilt.

(c) Analog zu (b) folgt dies daraus, dass ein Element $p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$ von R nach (a) genau dann ein gemeinsames Vielfaches von a und b ist, wenn $m_i \geq k_i$ und $m_i \geq l_i$ gilt, also $m_i \geq \max(k_i, l_i)$ gilt. □

13

Aufgabe 11.13. Es seien $m, n \in \mathbb{Z}$ mit $m, n \neq 0$. Nach Folgerung 11.12 (c) gibt es dann zu m und n ein kleinstes gemeinsames Vielfaches, das nach Bemerkung 10.9 bis auf das Vorzeichen eindeutig bestimmt ist. Analog zu Notation 10.30 (a) bezeichnen wir das eindeutig bestimmte *positive* kleinste gemeinsame Vielfache von m und n mit $\mathrm{kgv}(m, n)$.

Zeige, dass $\mathrm{ggt}(m, n) \cdot \mathrm{kgv}(m, n) = m \cdot n$. Lässt sich dieses Ergebnis auf andere Hauptidealringe verallgemeinern?

Bemerkung 11.14.

(a) Ein Integritätsring R, in dem jedes Element $a \in R$ mit $a \neq 0$ und $a \notin R^*$ eine bis auf Einheiten eindeutige Primfaktorzerlegung wie in Satz 11.9 besitzt, wird als ein **faktorieller Ring** oder **ZPE-Ring** (von „**Z**erlegung in **P**rimfaktoren, **e**indeutig“) bezeichnet. Satz 11.9 besagt damit also, dass jeder Hauptidealring faktoriell ist. Es gibt jedoch noch weitaus mehr faktorielle

Ringe. So kann man z. B. zeigen, dass jeder Polynomring $R[t]$ über einem faktoriellen Ring R, also z. B. $\mathbb{Z}[t]$, selbst wieder faktoriell ist — momentan wissen wir dies nur, wenn R ein Körper und $R[t]$ damit ein Hauptidealring ist.

Der Ring $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ hingegen ist nicht faktoriell, denn nach Beispiel 11.4 ist in ihm 2 nicht prim, allerdings irreduzibel und damit nicht weiter zerlegbar, und besitzt damit also insbesondere keine Primfaktorzerlegung.

(b) Der Beweis der Existenz einer Primfaktorzerlegung in Satz 11.9 ist nicht konstruktiv. In der Tat gibt es für die konkrete Berechnung einer Primfaktorzerlegung (und sogar schon für die Untersuchung, ob ein gegebenes Element prim ist) selbst im einfachsten Hauptidealring $\mathbb{Z}$ keine brauchbare Methode — also keine Methode, die wesentlich besser ist als einfach der Reihe nach von allen von der Größe her in Frage kommenden Zahlen nachzuprüfen, ob sie ein Teiler der gegebenen Zahl sind. In der Regel wird man größte gemeinsame Teiler daher nicht mit Folgerung 11.12, sondern mit dem euklidischen Algorithmus aus Satz 10.26 berechnen.

Im Polynomring über einem Körper gibt es allerdings noch ein wichtiges Hilfsmittel, das bei der Untersuchung der Irreduzibilität bzw. der Bestimmung der Primfaktorzerlegung nützlich ist:

Lemma 11.15 (Abspalten von Nullstellen in Polynomen)**.** *Es seien K ein Körper und $f \in K[t]$ ein Polynom vom Grad $n \in \mathbb{N}_{\geq 0}$. Dann gilt:*

(a) *Ist $a \in K$ mit $f(a) = 0$, so gilt $t - a \mid f$.*

(b) *f hat höchstens n Nullstellen.*

Beweis.

(a) Wir können f mit Rest durch $t - a$ dividieren und erhalten $f = q(t-a) + r$ für gewisse $q, r \in K[t]$ mit $\deg r < \deg(t-a) = 1$. Insbesondere ist r also ein konstantes Polynom. Setzen wir in diese Gleichung nun den Wert a ein, so erhalten wir

$$0 = f(a) = q(a)\,(a-a) + r(a) = r(a) \quad \in K.$$

Da r ein konstantes Polynom ist, dessen Wert an einer Stelle a gleich Null ist, muss r bereits das Nullpolynom sein. Also ist $f = q\,(t-a)$, d. h. $t - a \mid f$.

(b) Wir zeigen die Aussage mit Induktion über n.

- $n = 0$: In diesem Fall ist die Aussage trivial, da ein konstantes Polynom $f \neq 0$ natürlich keine Nullstellen besitzt.
- $n - 1 \to n$: Hat f keine Nullstellen, so sind wir fertig. Ist andernfalls $a \in K$ eine Nullstelle von f, so können wir dieses Polynom nach (a) als $(t-a) \cdot g$ für ein $g \in K[t]$ schreiben, das nach Lemma 9.9 (a) Grad $n-1$ haben muss und nach Induktionsvoraussetzung daher höchstens $n-1$ Nullstellen besitzt. Damit hat $f = (t-a)\,g$ höchstens n Nullstellen, nämlich a und die Nullstellen von g. □

Eine wesentliche Folgerung aus diesem Lemma ist, dass der Unterschied zwischen Polynomen und Polynomfunktionen, den wir in Bemerkung 9.16 (b) gesehen hatten, nur in Körpern mit endlich vielen Elementen auftritt.

Folgerung 11.16. *Es sei K ein Körper mit unendlich vielen Elementen. Sind dann $f, g \in K[t]$ zwei Polynome mit $f(a) = g(a)$ für alle $a \in K$, so gilt bereits $f = g \in K[t]$ (d. h. „in unendlichen Körpern sind Polynome und Polynomfunktionen dasselbe“).*

Beweis. Das Polynom $f - g$ hat nach Voraussetzung unendlich viele Nullstellen — nämlich alle Elemente von K. Also muss $f - g$ nach Lemma 11.15 (b) das Nullpolynom sein, d. h. es ist $f = g$. □

Bemerkung 11.17. Für Polynome von kleinem Grad ist es nun in der Regel einfach, eine Primfaktorzerlegung zu finden bzw. zu untersuchen, ob sie irreduzibel sind. Es seien dazu K ein Körper und $f \in K[t]$.

(a) Ist $\deg f = 1$, so ist f immer irreduzibel, denn in einer möglichen Zerlegung $f = gh$ mit $g,h \in K[t]$ muss eines der Polynome g und h nach der Gradformel aus Lemma 9.9 (a) Grad 0 haben und damit konstant, also eine Einheit sein.

(b) Analog ist das Polynom f irreduzibel, wenn es keine Nullstellen hat und sein Grad gleich 2 oder 3 ist: In einer Zerlegung $f = gh$ in nicht-konstante Polynome müsste dann nämlich mindestens einer der Faktoren Grad 1 haben, so dass dieser Faktor und damit auch f eine Nullstelle haben müsste. So sind z. B. die Polynome $t^2+1 \in \mathbb{R}[t]$ und $t^2+t+\overline{1} \in \mathbb{Z}_2[t]$ irreduzibel, da sie vom Grad 2 sind und in dem jeweils betrachteten Grundkörper keine Nullstellen haben.

(c) Hat umgekehrt f eine Nullstelle und ist $\deg f > 1$, so ist f sicher nicht irreduzibel, da wir die Nullstelle dann nach Lemma 11.15 abspalten können und so eine Zerlegung in Nichteinheiten erhalten.

(d) Der sogenannte *Fundamentalsatz der Algebra* besagt, dass jedes nicht-konstante Polynom über dem Körper $\mathbb{C}$ der komplexen Zahlen eine Nullstelle in $\mathbb{C}$ besitzt. Einen Beweis dieser Aussage werdet ihr erst in späteren Vorlesungen sehen (z. B. in der „Einführung in die Algebra“ oder der „Einführung in die Funktionentheorie“), da er Methoden benutzt, die deutlich über den Inhalt dieses Skripts hinaus gehen. Mit (a) und (c) können wir hier aber schon einmal festhalten, dass ein Polynom über $\mathbb{C}$ nach diesem Fundamentalsatz der Algebra genau dann irreduzibel ist, wenn es Grad 1 hat. Dementsprechend besteht die Primfaktorzerlegung eines komplexen Polynoms also ausschließlich aus linearen Faktoren.

Aufgabe 11.18 (Irreduzibilität für reelle Polynome)**.** Es sei $f \in \mathbb{R}[t]$ ein reelles Polynom. Man beweise:

(a) Ist $a \in \mathbb{C}$ eine Nullstelle von f, so ist auch die komplex konjugierte Zahl $\overline{a}$ eine Nullstelle von f.

(b) Das Polynom f ist genau dann irreduzibel in $\mathbb{R}[t]$, wenn
- $\deg f = 1$, oder
- $\deg f = 2$ und f keine reellen Nullstellen besitzt.

(Hinweis: Für Teil (b) könnt (und müsst) ihr den Fundamentalsatz der Algebra aus Bemerkung 11.17 (d) verwenden.)

Aufgabe 11.19. Es sei $f = t^{1000} + 5t^{100} + t^2 - 1 \in \mathbb{R}[t]$.

(a) Ist $t-1$ ein Teiler von f in $\mathbb{R}[t]$?

(b) Ist $\overline{t-1}$ invertierbar in $\mathbb{R}[t]/\langle f \rangle$?

Da wir nun in einfachen Fällen bestimmen können, ob ein gegebenes Polynom über einem Körper irreduzibel (und damit prim) ist, ist es nützlich, die Aussage aus Satz 7.10, dass $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$ genau dann ein Körper ist, wenn p eine Primzahl ist, auf allgemeine Hauptidealringe zu erweitern.

Satz 11.20 (Faktorringe als Körper)**.** *Es sei p ein Element in einem Hauptidealring R. Dann sind äquivalent:*

(a) *$R/\langle p \rangle$ ist ein Körper.*

(b) *$R/\langle p \rangle$ ist ein Integritätsring.*

(c) *p ist prim.*

Beweis.

(a) $\Rightarrow$ (b): Dies ergibt sich sofort aus Lemma 7.8 (b).

(b) $\Rightarrow$ (c): Es seien $a,b \in R$ mit $p \mid ab$, also $ab \in \langle p \rangle$. Dann gilt $\overline{ab} = \overline{0}$ in $R/\langle p \rangle$. Da $R/\langle p \rangle$ ein Integritätsring ist, bedeutet dies aber gerade $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$, und damit $p \mid a$ oder $p \mid b$.

(c) $\Rightarrow$ (a): Es sei p prim, und damit nach Lemma 11.3 auch irreduzibel. Bis auf Multiplikation mit Einheiten sind 1 und p also die einzigen Teiler von p. Ist nun $\overline{a} \in R/\langle p \rangle$ nicht gleich $\overline{0}$, also $p \nmid a$, so ist 1 damit der einzige gemeinsame Teiler von p und a, und daher ist $\overline{a}$ nach Folgerung 10.31 eine Einheit in $R/\langle p \rangle$. Also ist $R/\langle p \rangle$ ein Körper. □

Beispiel 11.21.

(a) Für den Hauptidealring $R = \mathbb{Z}$ erhalten wir aus Satz 11.20 wieder exakt die Aussage aus Satz 7.10 zurück.

(b) Da das Polynom $t^2+1 \in \mathbb{R}[t]$ nach Bemerkung 11.17 (b) irreduzibel ist, ist $\mathbb{R}[t]/\langle t^2+1 \rangle$ nach Satz 11.20 ein Körper — und zwar gerade $\mathbb{C}$, wie wir in Aufgabe 9.17 bereits gesehen hatten. In der Tat ist es algebraisch die eleganteste Art, die komplexen Zahlen als Körper zu konstruieren, indem man sie einfach als $\mathbb{C} := \mathbb{R}[t]/\langle t^2+1 \rangle$ *definiert*.

(c) Auch das Polynom $f := t^2+t+\overline{1} \in \mathbb{Z}_2[t]$ ist nach Bemerkung 11.17 (b) irreduzibel, und damit ist auch $R := \mathbb{Z}_2[t]/\langle f \rangle$ ein Körper. Da jede Klasse in R durch Betrachtung des Rests bei der Polynomdivision durch f (siehe Satz 10.19) einen eindeutigen Repräsentanten modulo f der Form $a_1 t + a_0$ mit $a_0, a_1 \in \mathbb{Z}_2$ hat, ist R ein Körper mit genau 4 Elementen. Er wird in der Literatur aufgrund des englischen Worts „field“ für „Körper“ mit $\mathbb{F}_4$ bezeichnet.

Beachte, dass $\mathbb{F}_4$ natürlich nicht isomorph zu $\mathbb{Z}_4$ ist, weil $\mathbb{Z}_4$ ja kein Körper ist.

Zum Abschluss wollen wir nun als Anwendung der Primfaktorzerlegung und unserer Ergebnisse zur Teilbarkeit in Ringen noch einen häufig vorkommenden Typ von Gleichungssystemen betrachten: Angenommen, wir suchen alle ganzen Zahlen $x \in \mathbb{Z}$, die modulo bestimmter Zahlen vorgegebene Restklassen darstellen, d. h. alle Zahlen, die ein Gleichungssystem der Form

$$\begin{array}{lll} x = a_1 \mod n_1 & & \overline{x} = \overline{a_1} \in \mathbb{Z}_{n_1} \\ \vdots & \text{bzw.} & \vdots \\ x = a_k \mod n_k & & \overline{x} = \overline{a_k} \in \mathbb{Z}_{n_k} \end{array}$$

erfüllen (beachte, dass wir die Notation $\overline{x}$ hierbei für die Restklassen von x in *verschiedenen* Faktorringen $\mathbb{Z}_{n_1}, \ldots, \mathbb{Z}_{n_k}$ verwendet haben). Das entscheidende Hilfsmittel bei der Lösung derartiger Gleichungssysteme ist der sogenannte chinesische Restsatz (der so genannt wird, da er in China bereits im 3. Jahrhundert bekannt war). In der Tat liefert der Beweis dieses Satzes bereits einen Algorithmus zur Lösung des obigen Gleichungssystems.

Satz 11.22 (Chinesischer Restsatz). *Es seien $n_1, \ldots, n_k \in \mathbb{N}_{>1}$ paarweise teilerfremde Zahlen, d. h. es gelte $\operatorname{ggt}(n_i, n_j) = 1$ für alle $i, j = 1, \ldots, k$ mit $i \neq j$. Dann ist die Abbildung*

$$\begin{array}{rcl} f\colon \mathbb{Z}_N & \to & \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ \overline{a} & \mapsto & (\overline{a}, \ldots, \overline{a}) \end{array}$$

mit $N := n_1 \cdot \cdots \cdot n_k$ ein Ringisomorphismus. (Beachte, dass auch hierbei wieder die Notation $\overline{a}$ für die Restklassen von a in verschiedenen Faktorringen $\mathbb{Z}_N, \mathbb{Z}_{n_1}, \ldots, \mathbb{Z}_{n_k}$ verwendet wurde.)

Beweis. Als Erstes müssen wir die Wohldefiniertheit von f überprüfen (siehe Bemerkung 6.1): Sind $a,b \in \mathbb{Z}$ mit $\overline{a} = \overline{b} \in \mathbb{Z}_N$, also $b - a \in N\mathbb{Z}$, so ist wegen $N\mathbb{Z} \subset n_i\mathbb{Z}$ für alle $i = 1, \ldots, k$ natürlich auch $b - a \in n_i\mathbb{Z}$ und damit $\overline{a} = \overline{b} \in \mathbb{Z}_{n_i}$. Also ist dann auch $(\overline{a}, \ldots, \overline{a}) = (\overline{b}, \ldots, \overline{b}) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, d. h. f ist wohldefiniert.

Als Nächstes stellen wir fest, dass f in der Tat ein Ringhomomorphismus ist: Es ist $f(\overline{1}) = (\overline{1}, \ldots, \overline{1})$, für alle $a,b \in \mathbb{Z}$ ist

$$f(\overline{a}+\overline{b}) = (\overline{a}+\overline{b}, \ldots, \overline{a}+\overline{b}) = (\overline{a}, \ldots, \overline{a}) + (\overline{b}, \ldots, \overline{b}) = f(\overline{a}) + f(\overline{b}),$$

und eine analoge Aussage gilt natürlich genauso für die Multiplikation.

Es bleibt also nur noch die Bijektivität von f zu zeigen. Da der Start- und Zielraum von f die gleiche (endliche) Anzahl N von Elementen haben, genügt es hierfür zu zeigen, dass f surjektiv ist. Es seien dazu $a_1,\dots,a_k \in \mathbb{Z}$ beliebig. Wir müssen zeigen, dass es ein $a \in \mathbb{Z}$ gibt, das $f(\overline{a}) = (\overline{a_1},\dots,\overline{a_k})$ erfüllt und damit das oben betrachtete Gleichungssystem $\overline{x} = \overline{a_i} \in \mathbb{Z}_{n_i}$ für alle $i = 1,\dots,k$ löst. Der Beweis hierfür ist konstruktiv und ermöglicht damit auch eine explizite Lösung dieses Gleichungssystems:

(1) Für $i = 1,\dots,k$ setzen wir
$$N_i := \frac{N}{n_i} = n_1 \cdot \dots \cdot n_{i-1} \cdot n_{i+1} \cdot \dots \cdot n_k.$$

(2) Nach Voraussetzung ist $\operatorname{ggt}(n_i, n_j) = 1$ für $i \neq j$, d. h. jede Primzahl tritt in der Primfaktorzerlegung von höchstens einer der Zahlen $n_1,\dots,n_k$ auf. Damit gilt dann natürlich auch $\operatorname{ggt}(n_i, N_i) = 1$ für alle $i = 1,\dots,k$. Nach Folgerung 10.31 ist $\overline{N_i}$ also eine Einheit in $\mathbb{Z}_{n_i}$, und wir können mit dem erweiterten euklidischen Algorithmus 10.27 ihr multiplikatives Inverses $\overline{M_i}$ in $\mathbb{Z}_{n_i}$, also ein $M_i \in \mathbb{Z}$ mit
$$\overline{M_i} \cdot \overline{N_i} = \overline{1} \quad \in \mathbb{Z}_{n_i} \qquad (*)$$
berechnen.

(3) Wir setzen nun
$$a := \sum_{i=1}^{k} a_i M_i N_i \quad \in \mathbb{Z}.$$

Dann ist a eine (und damit, wie wir schon gesehen haben, modulo N die einzige) Lösung des Gleichungssystems $\overline{x} = \overline{a_i} \in \mathbb{Z}_{n_i}$ für alle i, denn für alle i gilt in $\mathbb{Z}_{n_i}$
$$\begin{aligned}\overline{a} &= \sum_{j=1}^{k} \overline{a_j}\,\overline{M_j}\,\overline{N_j} \\ &= \overline{a_i}\,\overline{M_i}\,\overline{N_i} \qquad (N_j \text{ enthält für } j \neq i \text{ den Faktor } n_i, \text{ also ist dann } \overline{N_j} = \overline{0} \in \mathbb{Z}_{n_i}) \\ &\overset{(*)}{=} \overline{a_i}.\end{aligned}$$

Mit anderen Worten ist die Restklasse $\overline{a} \in \mathbb{Z}_N$ ein (und damit das einzige) Urbild von $(\overline{a_1},\dots,\overline{a_k})$ unter f, d. h. f ist surjektiv. □

Beispiel 11.23. Mit Hilfe des chinesischen Restsatzes können wir nun Gleichungssysteme von Restklassen, wie wir sie oben betrachtet haben, leicht umformen. Dabei können wir den Isomorphismus aus Satz 11.22 „sowohl von links nach rechts als auch von rechts nach links lesen“:

(a) Betrachten wir für ein gegebenes $a \in \mathbb{Z}$ die Gleichung $\overline{x} = \overline{a}$ in einem Restklassenring $\mathbb{Z}_N$ und können wir dieses N als Produkt $N = n_1 \cdot \dots \cdot n_k$ von Zahlen mit $\operatorname{ggt}(n_i, n_j) = 1$ für $i \neq j$ schreiben, so lässt sich die betrachtete Gleichung durch Anwenden des Isomorphismus aus dem chinesischen Restsatz 11.22 vom Ring $\mathbb{Z}_N$ nach $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ übertragen, d. h. wir erhalten die Äquivalenz von Gleichungssystemen
$$\overline{x} = \overline{a} \ \in \mathbb{Z}_N \quad \Leftrightarrow \quad \begin{cases} \overline{x} = \overline{a} \ \in \mathbb{Z}_{n_1} \\ \quad \vdots \\ \overline{x} = \overline{a} \ \in \mathbb{Z}_{n_k}. \end{cases}$$
Konkret sind z. B. die folgenden Gleichungssysteme äquivalent:
$$x = 5 \mod 6 \quad \Leftrightarrow \quad \begin{matrix} x = 5 \mod 2 \\ x = 5 \mod 3 \end{matrix} \quad \Leftrightarrow \quad \begin{matrix} x = 1 \mod 2 \\ x = 2 \mod 3, \end{matrix}$$
wobei sich die zweite Äquivalenz natürlich einfach durch Reduktion der rechten Seiten modulo 2 bzw. 3 ergibt.

(b) Deutlich nützlicher ist die Anwendung des Isomorphismus aus Satz 11.22 „in der umgekehrten Richtung“: Indem wir die explizite Konstruktion des Umkehrisomorphismus aus dem Beweis des Satzes verwenden, können wir mehrere Gleichungen zu einer zusammenfassen. Als konkretes Beispiel hierfür wollen wir alle $x \in \mathbb{Z}$ finden, die das Gleichungssystem

$$\begin{aligned} x &= 1 \mod 2 \\ x &= 1 \mod 5 \\ x &= 2 \mod 7 \end{aligned}$$

erfüllen. Dazu gehen wir die drei Schritte aus dem Beweis des chinesischen Restsatzes durch:

(1) Es ist zunächst einmal $n_1 = 2$, $n_2 = 5$ und $n_3 = 7$, wir haben damit also $N = 2 \cdot 5 \cdot 7 = 70$ und setzen $N_1 = 5 \cdot 7 = 35$, $N_2 = 2 \cdot 7 = 14$ und $N_3 = 2 \cdot 5 = 10$.

(2) Die Inversen von N_i modulo n_i für alle i sehen wir in diesem Fall auch ohne den erweiterten euklidischen Algorithmus sofort:

- In $\mathbb{Z}_{n_1} = \mathbb{Z}_2$ ist das Inverse von $\overline{N_1} = \overline{35} = \overline{1}$ gleich $\overline{1}$, also setzen wir $M_1 = 1$.
- In $\mathbb{Z}_{n_2} = \mathbb{Z}_5$ ist das Inverse von $\overline{N_2} = \overline{14} = \overline{4}$ gleich $\overline{4}$, also setzen wir $M_2 = 4$.
- In $\mathbb{Z}_{n_3} = \mathbb{Z}_7$ ist das Inverse von $\overline{N_3} = \overline{10} = \overline{3}$ gleich $\overline{5}$, also setzen wir $M_3 = 5$.

(3) Mit den rechten Seiten $a_1 = 1$, $a_2 = 1$ und $a_3 = 2$ des Gleichungssystems bilden wir nun die Zahl

$$a = a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 = 1 \cdot 1 \cdot 35 + 1 \cdot 4 \cdot 14 + 2 \cdot 5 \cdot 10 = 191.$$

Die Lösung des gegebenen Gleichungssystems sind also alle $x \in \mathbb{Z}$ mit $\overline{x} = \overline{191} = \overline{51} \in \mathbb{Z}_{70}$, d. h. alle $x \in 51 + 70\mathbb{Z}$.

Eine Kontrolle dieses Ergebnisses ist natürlich sehr einfach möglich, da man ja schnell nachprüfen kann, dass die Zahl 51 wirklich das gegebene Gleichungssystem erfüllt.

Aufgabe 11.24. Bestimme alle $x \in \mathbb{Z}$, für die die folgenden Gleichungssysteme erfüllt sind:

(a) $\begin{aligned} x &= 2 \mod 4 \\ x &= 6 \mod 7 \\ x &= 3 \mod 9 \end{aligned}$ (b) $\begin{aligned} x &= 5 \mod 6 \\ 3x &= -1 \mod 14 \end{aligned}$ (c) $x = 1 \mod n$ für alle $n = 2, \ldots, 10$

Aufgabe 11.25. Zeige die folgende Umkehrung des chinesischen Restsatzes: Sind $n, m \in \mathbb{N}_{>0}$ nicht teilerfremd, so ist $\mathbb{Z}_{nm}$ nicht isomorph zu $\mathbb{Z}_n \times \mathbb{Z}_m$.

Der chinesische Restsatz lässt sich schließlich noch einfach auf die Einheitengruppen übertragen:

Folgerung 11.26. *Es seien $n_1, \ldots, n_k \in \mathbb{N}_{>1}$ paarweise teilerfremde Zahlen. Dann ist die Abbildung*

$$\begin{aligned} f\colon \mathbb{Z}_N^* &\to \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^* \\ \overline{a} &\mapsto (\overline{a}, \ldots, \overline{a}) \end{aligned}$$

mit $N := n_1 \cdot \cdots \cdot n_k$ ein Gruppenisomorphismus.

Beweis. Die Abbildung f aus dem chinesischen Restsatz 11.22 ist ein Ringisomorphismus und bildet damit die Einheiten von $\mathbb{Z}_N$ genau auf die Einheiten von $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ ab. Letztere sind nach Aufgabe 7.15 aber genau die Elemente von $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$, woraus die Behauptung folgt. □

Aufgabe 11.27. Man beweise oder widerlege:

(a) $\mathbb{Z}_{25}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_5^*$;

(b) $\mathbb{Z}_{15}^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Aufgabe 11.28. Es sei $k \in \mathbb{N}$, so dass die drei Zahlen $6k+1$, $12k+1$ und $18k+1$ prim sind.

Man zeige: Für $n := (6k+1)(12k+1)(18k+1)$ und alle $a \in \mathbb{Z}$ mit $\operatorname{ggt}(a,n) = 1$ gilt $a^{n-1} = 1 \mod n$.

14

Literatur

[B] S. Bosch, *Algebra*, Springer (2006)
[E] H.-D. Ebbinghaus et al., *Zahlen*, Springer (1988)
[G] A. Gathmann, *Grundlagen der Mathematik*, Vorlesungsskript TU Kaiserslautern (2018/19), https://www.mathematik.uni-kl.de/~gathmann/gdm
[L] S. Lang, *Algebraische Strukturen*, Vandenhoeck & Ruprecht (1979)
[M] T. Markwig, *Algebraische Strukturen*, Vorlesungsskript TU Kaiserslautern (2008/09), https://www.math.uni-tuebingen.de/~keilen/download/Lehre/AGSWS08/skript.pdf

Index