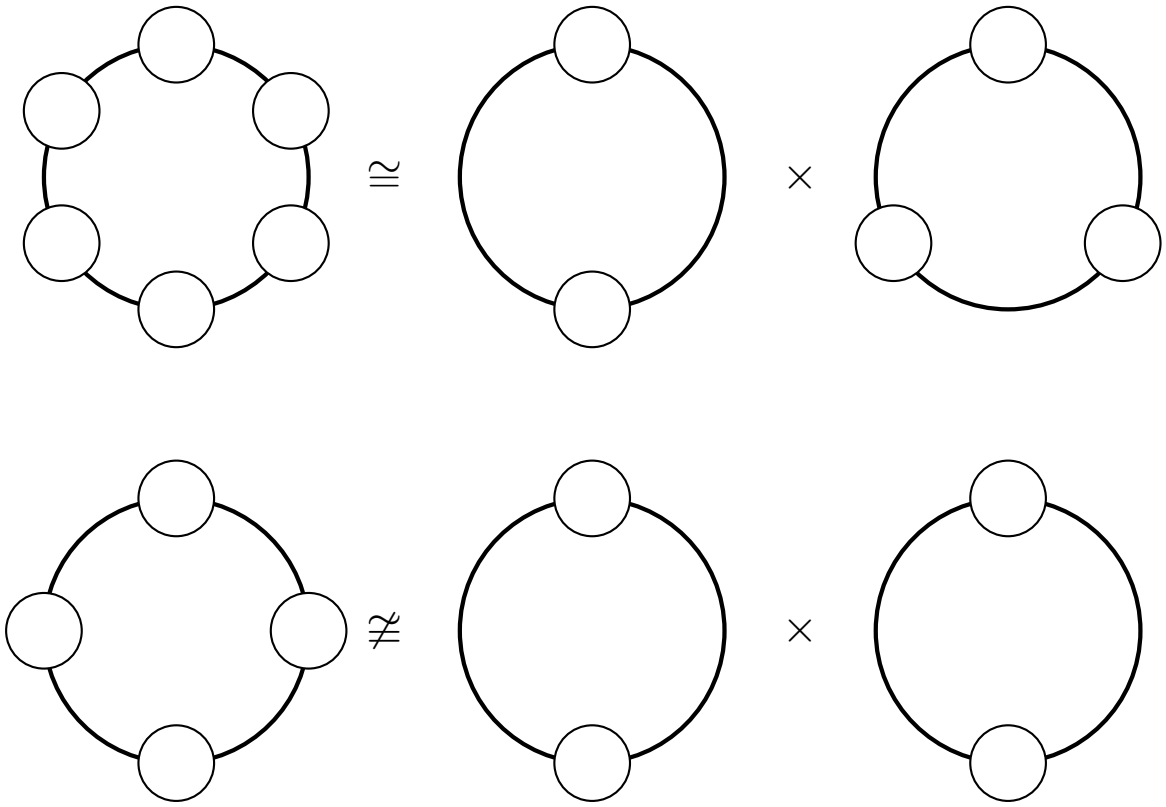


Algebra

Eine grundlagenorientierte Einführungsvorlesung

Martin Goldstern Clemens Schindler Reinhard Winkler

Vorwort

Dieser Text dient als Einführung in das Gebiet der Algebra. Klassischerweise geht es dabei um Mengen, die „Rechenoperationen“ tragen, sodass gewisse „Rechenregeln“ erfüllt sind, beispielsweise Gruppen oder auch Körper. Oft handelt es sich um Abstraktionen von „konkreten“ Objekten mit dem Ziel, den wesentlichen strukturellen Kern von Eigenschaften, die diese Objekte haben, freizulegen. Als Beispiel können hier die ganzen Zahlen dienen, die man als Gruppe oder auch als Ring auffassen kann. Die interessanten Fragen kreisen somit zumeist darum, die Struktur dieser Objekte zu verstehen. Eine Möglichkeit dazu sind Klassifikationen. Das bedeutet, dass man zu einer (beispielsweise durch das Erfülltsein bestimmer Rechenregeln gegebenen) Klasse von Strukturen eine Liste „konkreter“ Objekte derart findet, dass man zu jeder Struktur aus der Klasse auf möglichst kanonische Weise einen eindeutigen Vertreter auf der Liste findet, der dazu strukturgleich („isomorph“) ist. Ein anderer wichtiger Typus von Einsichten beschäftigt sich mit Verbindungen zwischen Strukturen aus verschiedenen Klassen, beispielsweise Körpern und (Mengen von) Polynomen, insbesondere deren Nullstellen.
Im letzten Jahrhundert entstand noch ein weiteres Feld innerhalb der Mathematik, nämlich die sogenannte *allgemeine* oder *universelle* Algebra. In einem zusätzlichen Abstraktionsschritt treten hier die konkreten, in der *klassischen* Algebra studierten Klassen wie Gruppen in den Hintergrund. Stattdessen rücken die Rechenoperationen und Rechengesetze an sich in den Fokus, mit dem Ziel, das Wechselspiel zwischen Strukturen und allen auf ihnen geltenden Gesetze zu verstehen.
Mathematik lebt zu einem guten Teil von ihren reichhaltigen inneren Querverbindungen. Für die Algebra als stark strukturtheoretisch geprägter Disziplin gilt das ganz besonders. Aus diesem Grund hängt die Qualität eines Buchs über dieses Thema nicht zuletzt von einem ökonomischen Aufbau ab, in dem gleichzeitig die keineswegs nur linear verlaufenden Verbindungen sichtbar werden. In der Algebra noch mehr als in manch anderen Teilgebieten der Mathematik spielt dabei ein sorgfältiger begrifflicher Aufbau eine wesentliche Rolle. Ein profundes Verständnis für diesen Aufbau ist daher ein wichtiger Schlüssel zur Bewältigung des Großteils des Stoffes. In vielen Fällen ist es dabei möglich, ausufernde technische Komplikationen zu vermeiden, die stets die Gefahr bergen, dass Details den Blick auf die wesentlichen Ideen verdecken. Die Grobstruktur ist vorwiegend diesem Anliegen geschuldet, insbesondere stecken wir uns zu Beginn einen begrifflichen Rahmen, der nicht nur die klassische sondern auch die allgemeine Algebra aufnimmt. Dies bietet zwei Vorteile: einerseits den offensichtlichen, dass wir Inhalte aus der allgemeinen Algebra besprechen können; andererseits den etwas versteckteren, dass wir beispielsweise die grundlegenden algebraischen Begriffsbildungen wie Unteralgebra oder Homomorphismus in allgemeiner Terminologie einführen können und erst später auf klassische Algebren wie Gruppen oder Ringe spezialisieren. Auf diese Weise wird sichtbar, welche Eigenschaften aus allgemeinen Prinzipien folgen (und sich dort oftmals mit weniger technischen Details darstellen lassen) und welche von spezielleren Situationen abhängig sind. Viele einführende Bücher über Algebra befassen sich ausschließlich mit klassischer Algebra; wir hingegen sind überzeugt, dass die allgemeinere Sichtweise ein klareres Bild ergeben kann, auch wenn man nur an klassischer Algebra interessiert sein sollte.

In Kapitel 1 beginnen wir mit einem Einstieg in die Welt der Algebra, indem wir wesentliche Ideen und Begriffe anhand von bereits bekannten Beispielen motivieren. Mit Kapitel 2 schaffen wir einen begrifflichen Rahmen für alles Folgende und führen außerdem die grundlegenden algebraischen Konstruktionen ein. In Kapitel 3 spezialisieren wir auf wichtige Klassen algebraischer Strukturen aus der klassischen Algebra, insbesondere Gruppen und noch spezifischer abelsche Gruppen, Ringe und Boolesche Algebren. Ein Einblick in die allgemeine Algebra in Gestalt zweier grundlegender Konstruktionen folgt in Kapitel 4. Mit Kapitel 5 analysieren wir vom klassischen Satz von der Primfaktorzerlegung ausgehend das Konzept der Teilbarkeit und zugehörige Begriffsbildungen. In Kapitel 6 betrachten wir schließlich die Klasse der Körper, die in vielerlei Hinsicht die reichhaltigste Struktur unter den klassischen algebraischen Objekten tragen. Den Kapiteln und Abschnitten (erste und zweite Gliederungsebene) und auch jedem der Unterabschnitte (dritte Gliederungsebene) des Haupttexts ist stets eine Einleitung mit dem jeweiligen „Inhalt in Kurzfassung“ vorangestellt. Dies soll helfen, das Wichtige mit einem kurzen Blick im Auge zu behalten und vom Beiläufigen zu unterscheiden. Kapitel A bildet einen Anhang, der mengentheoretische Grundlagen bereitstellt, auf die in der Algebra gelegentlich zurückgegriffen wird. Eine systematische Behandlung der Inhalte des Anhangs muss Büchern speziell über Logik, Mengenlehre und Grundlagen der Mathematik vorbehalten bleiben. Insgesamt halten Sie mehr Material in Händen als in einem Semester durchgearbeitet werden kann, sodass hier stets eine Auswahl getroffen werden muss. Bei entsprechendem Interesse Ihrerseits, liebe Leser:innen, können viele Abschnitte aber als Ausgangspunkt zu weitergehender Beschäftigung mit dem weiten Feld der Algebra dienen. Schließlich verweisen wir auf unser vertiefendes Buch *Algebra II – eine vertiefende Vorlesung*, das eine Fortsetzung der hier versammelten Inhalte darstellt und (gemeinsam mit dem vorliegenden Text) unter `https://algebrabuch.github.io` zum Download verfügbar ist. An einzelnen Stellen beziehen wir uns zwecks Ausblicks auf besagte Fortsetzung; diese Referenzen sind an Kapitelnummern von 7 bis 10 zu erkennen.

Dieses Buch ist entstanden aus einem über die Jahre kontinuierlich verbesserten Skriptum von zweien von uns (Martin Goldstern und Reinhard Winkler) zu der regelmäßig angebotenen (Pflicht-)Lehrveranstaltung *Algebra* an der Technischen Universität Wien. Auf Reinhard Winklers Wunsch vor seinem Tod im Herbst 2021 nach kurzer schwerer Krankheit kam Clemens Schindler dazu und wir haben das Unterfangen, das Skriptum qualitativ auf Buchniveau zu bringen, vollendet. Vereinzelte Fragmente stammen noch von anderen Autor:innen, die für uns nicht mehr alle identifizierbar sind, denen aber durchwegs unser Dank gilt. Insbesondere bedanken wir uns bei Thomas Baumhauer, Sophie Hotz, Christiane Schütz, Friedrich Urbanek und Sebastian Zivota sowie den unzähligen Studierenden, die uns auf Fehler, Ungereimtheiten und Verbesserungsmöglichkeiten aufmerksam gemacht haben und so zu einem wesentlich runderen Text beigetragen haben. Außerdem gilt ein großer Dank unserem Kollegen Michael Pinsker, der zahlreiche Verbesserungsvorschläge gemacht und Ungereimtheiten aufgezeigt hat. Wenn auch Sie Falsches oder Irreführendes entdecken, bitten wir um eine Nachricht an `algebrabuch@gmail.com` – herzlichen Dank!

Martin Goldstern, Clemens Schindler, Reinhard Winkler † September 2023

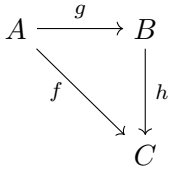
Notationelle Bemerkungen

Durch den gesamten Text hindurch verwenden wir einige notationelle Konventionen, die wir zum einfacheren Nachschlagen an dieser Stelle sammeln.

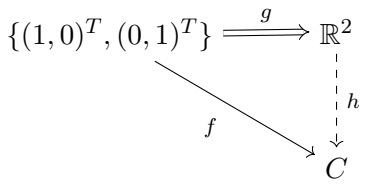
Die Verknüpfung von Funktionen schreiben wir „von rechts nach links“, also explizit $f \circ g(x) := f(g(x))$. Für Äquivalenzrelationen schreiben wir $\sim$, $\equiv$ etc. Für Ordnungsrelationen schreiben wir $\leq$, $\sqsubseteq$ etc., für die entsprechende strikte Ordnung $<$, $\sqsubset$ etc. Einzige Ausnahme davon bildet die Teilmengenrelation: In einigen Büchern wird das Symbol $\subset$ verwendet, wobei damit manchmal die strikte und manchmal die nicht-strikte Teilmenge gemeint ist. Um hier keine Missverständnisse aufkommen zu lassen, schreiben wir $\subseteq$ für die nicht-strikte Teilmenge und $\subsetneq$ für die strikte Teilmenge.

Eines der zentralen Objekte, mit denen wir uns in diesem Text beschäftigen, ist die sogenannte algebraische Struktur. Das ist eine Trägermenge, sagen wir A, versehen mit gewissen Operationen, der Einfachheit halber betrachten wir exemplarisch Addition $+ : A \times A \to A$, $(a, b) \mapsto a + b$ und additive Inverse $- : A \to A$, $a \mapsto -a$. Die entstehende Struktur bezeichnen wir in diesem Beispiel mit $\mathfrak{A} = (A, +, -)$. Diese Namensgebung verfolgen wir durch den ganzen Text hindurch: Wenn die Trägermenge A, B, C, D etc. heißt, so heißt die entsprechende algebraische Struktur $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ etc. Im Kontext der klassischen algebraischen Strukturen, also Gruppen, Ringen, Körpern, Vektorräumen etc., und wenn aus dem Zusammenhang klar ist, von welchem Typus von Struktur gerade die Rede ist, werden wir auf die Unterscheidung zwischen A und $\mathfrak{A}$ zur einfacheren Notation verzichten. Beispielsweise werden wir zumeist von der Gruppe G sprechen, und nicht von der Gruppe $\mathfrak{G}$ auf der Trägermenge G.

An vielen Stellen werden sogenannte kommutative Diagramme eine wichtige Rolle spielen, wie zum Beispiel



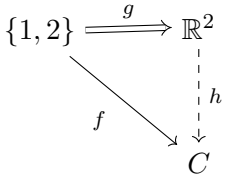
Das bedeutet, dass Abbildungen $f : A \to C$, $g : A \to B$ und $h : B \to C$ vorliegen, sodass $f = h \circ g$ gilt. Eine Erweiterung dieser Notation verdient eine spezielle Situation, auf die wir wiederholt stoßen werden und die sich am besten anhand eines Beispiels illustrieren lässt: Sei $\mathbb{R}^2$ der kanonische zweidimensionale Vektorraum über $\mathbb{R}$, sei $\{(1,0)^T, (0,1)^T\}$ die kanonische Basis und sei C irgendein Vektorraum über $\mathbb{R}$. Dann ist $\{(1,0)^T, (0,1)^T\}$ in $\mathbb{R}^2$ enthalten, also $g : \{(1,0)^T, (0,1)^T\} \to \mathbb{R}^2$ für die Inklusionsabbildung. Ist eine *beliebige* Abbildung $f : \{(1,0)^T, (0,1)^T\} \to C$ gegeben, so *existiert* eine *eindeutige* lineare Abbildung $h : \mathbb{R}^2 \to C$, sodass $f = h \circ g$, nämlich $h((x,y)^T) := xf((1,0)^T) + yf((0,1)^T)$ – dies ist eine Anwendung des Fortsetzungssatzes, den wir in Satz 1.3.1.2 wiederholen werden. Wir werden dafür



schreiben. Die unterschiedlichen Pfeiltypen sind also folgendermaßen zu verstehen: Die doppelt gezeichnete Inklusionsabbildung g ist fest mit dem betrachteten Objekt verbunden, hier mit der kanonischen Basis $\{(1,0)^T,(0,1)^T\}$ als Teilmenge von $\mathbb{R}^2$; vor der durchgezogenen Abbildung f sowie vor dem Objekt C ist ein Allquantor zu denken; und vor der strichliert gezeichneten Abbildung h ist ein Quantor der eindeutigen Existenz zu denken; kurz:

$$g \text{ fest} \rightsquigarrow \forall f, C\ \exists! h$$

Wenn wir uns später mit dieser Situation beschäftigen werden, wird g nicht notwendigerweise die Inklusionsabbildung sein. In unserem aktuellen Beispiel können wir zur Illustration die kanonische Basis $\{(1,0)^T,(0,1)^T\}$ durch $\{1,2\}$ ersetzen und die Abbildung $g : \{1,2\} \to \mathbb{R}^2$ betrachten, die durch $g(1) := (1,0)^T$ und $g(2) := (0,1)^T$ definiert ist[1]. Dann gilt



Explizit: Wenn g so wie eben beschrieben definiert ist (und damit fest gegeben ist), dann gibt es für jeden Vektorraum C und jede Funktion $f : \{1,2\} \to C$ eine eindeutige lineare Abbildung $h : \mathbb{R}^2 \to C$, die das Diagramm schließt (nämlich $h((x,y)^T) := xf(1)+yf(2)$).

[1] Dies ist die formale Entsprechung des üblichen Vorgehens, die kanonischen Basisvektoren mit Indizes zu definieren, also $e_1 := (1,0)^T$ und $e_2 := (0,1)^T$.

Klassifikation der UE-Aufgaben

Jede Übungsaufgabe wird zu einem von mehreren Typen (gelegentlich auch zu mehr als einem) durch jeweils einen der Buchstaben A, B, D, E, F, V, W zugeordnet. Dies soll Ihnen im Vorhinein darüber Information geben, welche Arbeit und welche Einsicht Sie erwartet:

(A) (Alternative Sichtweise): Für einen bereits bekannten Inhalt soll durch einen alternativen Zugang das Verständnis erweitert werden.

(B) (Beispiel): Damit wird ein explizites Beispiel behandelt, das charakteristisch ist für einen Begriff oder Sachverhalt aus der allgemeinen Theorie. Oder ein Gegenbeispiel, welches belegt, dass eine scheinbar harmlose Variante oder Umformulierung den Sinn einer Definition deutlich verändert, oder aus einem wahren und interessanten Satz einen falschen oder trivial gültigen Satz erzeugt.

(D) (Diskussion): Damit werden offene und möglicherweise vage Aufgabenstellungen markiert, die eher zur Diskussion anregen sollen als ein ganz bestimmtes Ergebnis einzufordern.

(E) (Erweiterung): Damit wird der eigentliche Inhalt des Textes verlassen. Der Lohn für den Aufwand, sich trotzdem mit der Aufgabe zu beschäftigen, besteht in einer Erweiterung des Horizonts und/oder Vertiefung des Verständnisses. Über diesen Umweg kann man davon eventuell auch in Hinblick auf den Kernstoff profitieren. Oft ergibt sich dieser Effekt schon allein dadurch, dass man sich die Aufgabenstellung klar macht.

(F) (Fingerübung): Solche Aufgaben dienen vor allem der Kontrolle des Verständnisses der wesentlichen Konzepte, sind abgesehen davon aber in der Regel für sich genommen von geringerem Interesse. Diese Aufgaben können sehr kurz oder auch länger sein. Substanzielle, d. h. für die Theorie wichtige, neue Ideen sind für die Bearbeitung nicht erforderlich. Fingerübungen, die dennoch irgendwelche Einsichten von allgemeinerem Interesse zeitigen, sind mit (F+) gekennzeichnet.

(V) (Vervollständigung): Hier steht das Anliegen im Vordergrund, Beweislücken im Haupttext zu schließen. Häufig handelt es sich um kleine, eher technische Ergänzungen, die zunächst ausgespart wurden, damit in einem Beweis die wesentlichen Gedanken nicht durch ausufernde technische Details verschleiert werden. Außerdem werden gewisse Beweise, die aber weder sehr schwierig sind noch besondere Ideen beinhalten, in Übungsaufgaben von diesem Typ ausgelagert.

(W) (Wichtig, Wesentlich): In solchen Übungsaufgaben werden Aussagen bewiesen, die eine wichtige Rolle für das Verständnis der Hauptinhalte des Textes spielen.

Selbstverständlich sind die Grenzen zwischen diesen Typen nicht scharf, und die meisten Übungsaufgaben tragen viele Aspekte in sich. Wir haben den- oder diejenigen davon ausgewählt, den oder die wir im Vordergrund sehen.

Inhaltsverzeichnis

1. Einführung in die algebraische Denkweise

Auf Kapitel 1 wird zwar später gelegentlich zurückgegriffen werden, doch folgt es selbst noch keinem strengen systematischen Aufbau. Dieser beginnt erst mit Kapitel 2. Vorerst sollen anhand bereits bekannter Beispiele fundamentale und einfache, teilweise aber relativ abstrakte Begriffe, welche die Algebra nach modernem Verständnis durchziehen, vertraut gemacht werden. In Abschnitt 1.1 stehen mengentheoretische Grundlegungen von dem System $\mathbb{N}$ der natürlichen Zahlen im Mittelpunkt, wobei wir uns besonders auf zwei zentrale Aufgaben der Algebra konzentrieren, nämlich Axiomatisierung und Klassifikation. Anhand der klassischen Erweiterungen der Zahlenbereiche, ausgehend von $\mathbb{N}$ über $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ bis $\mathbb{C}$ wird in Abschnitt 1.2 ein weiteres sehr typisches Anliegen der Algebra vorgestellt: die Konstruktion von Strukturen mit gewissen gewünschten Eigenschaften. Dabei treten Homo- und Isomorphismen (strukturverträgliche Abbildungen) deutlich in den Vordergrund. Für den Fall von Vektorräumen ist vieles davon schon aus der Linearen Algebra bekannt und wird in Abschnitt 1.3 nochmals in neuem Lichte rekapituliert.

1.1. Die natürlichen Zahlen

Leopold Kronecker (1823–1891) meinte bekanntlich über die Herkunft mathematischer Begriffe, die ganzen Zahlen habe der liebe Gott gemacht, alles andere sei Menschenwerk. Doch gibt es gute Gründe, auch die ganzen und sogar die natürlichen Zahlen (welche Kronecker wohl meinte) genauer zu hinterfragen. Die moderne, stark von der Mengenlehre Georg Cantors (1845–1918) geprägte Mathematik gibt uns einen großzügigen Rahmen dafür. Interpretiert man Kronecker historisch und didaktisch, so kann man seinem berühmten Diktum durchaus Sinnvolles abgewinnen: In der Geschichte der Menschen – sowohl kollektiv als Jahrtausende alte Entwicklung unserer Zivilisation wie auch individuell als psychologisch-intellektuelle Entfaltung des heranwachsenden Menschen – erscheinen, wenn man die Stränge zurück verfolgt, immer wieder die natürlichen Zahlen zusammen mit den elementaren Operationen (Addition, Multiplikation etc.) als die erste und entscheidende Abstraktion und somit als Ausgangspunkt der Mathematik. Gleichzeitig ermöglichen sie einen reizvollen Einstieg in die Welt der Algebra. Ein solcher, selbst noch nicht der Algebra im engeren Sinne zuzuordnen, soll in diesem Abschnitt geboten werden.

In 1.1.1 stellen wir einen mengentheoretisch basierten Zugang zum System $\mathbb{N}$ der natürlichen Zahlen vor. Dabei orientieren wir uns möglichst eng an der Bedeutung natürlicher Zahlen als Kardinalitäten endlicher Mengen, d. h. als Invarianten bezüglich Bijektionen. Die Axiomatisierung von $\mathbb{N}$ durch Giuseppe Peano (1858–1932) ist Gegenstand von 1.1.2. In 1.1.3 behandeln wir das in der axiomatischen Mengenlehre zum Standard gewordene Modell von $\mathbb{N}$ nach John von Neumann. In 1.1.4 führen wir die Arithmetik auf $\mathbb{N}$

– ihrer ursprünglichen Bedeutung entsprechend – auf mengentheoretische Operationen zurück. Damit wird auch der Beweis der grundlegenden Rechenregeln wie dem Assoziativgesetz sehr einfach. Unterabschnitt 1.1.5 bringt einige Bemerkungen zur Induktion als Beweismethode. Den Abschnitt beschließen in 1.1.6 einige Bemerkungen zur Darstellung mathematischer Objekte, insbesondere zur Zifferndarstellung natürlicher Zahlen.

1.1.1. Natürliche Zahlen als endliche Kardinalitäten

Inhalt in Kurzfassung: Jede natürliche Zahl entspricht einer Klasse untereinander gleichmächtiger endlicher Mengen. Dieser Grundgedanke wird nun mathematisch streng entwickelt, wobei wir uns besonders auf die dazu notwendigen Begriffe und Definitionen konzentrieren und für Beweise größtenteils auf den Anhang verweisen.

Es gibt verschiedene Möglichkeiten, die natürlichen Zahlen zu beschreiben; wir beginnen hier mit einem Zugang, der die natürlichen Zahlen als „Größen“ von *endlichen* Mengen beschreibt.
Wir verstehen diese Beschreibung der natürlichen Zahlen als „grundlagenorientiert“. Das Ziel ist es nicht, neue Fakten über die natürlichen Zahlen zu entdecken oder zu beweisen; im Gegenteil, wir beschäftigen uns hier mit Tatsachen, die wir eigentlich schon wissen. Ziel dabei ist es, die Rolle der Definitionen (und Beweise) besser zu verstehen.
Die folgende Definition ist für endliche wie auch für unendliche Mengen sinnvoll:

Definition 1.1.1.1. Wenn A und B beliebige Mengen sind, dann schreiben wir $A \approx B$ („A und B sind gleichmächtig“) als Abkürzung für „Es gibt eine bijektive Abbildung zwischen A und B.“:

$$A \approx B \;:\Leftrightarrow\; \exists f\colon A \to B,\ f \text{ bijektiv}$$

Die Relation $\approx$ ist reflexiv, weil die identische Abildung auf jeder Menge bijektiv ist; symmetrisch, weil die Umkehrabbildung einer bijektiven Abbildung wieder bijektiv ist; und transitiv, weil die Verkettung bijektiver Abbildungen ebenfalls bijektiv ist. Also gilt:

Proposition 1.1.1.2. *Auf jeder Menge von Mengen ist die Relation $\approx$ eine Äquivalenzrelation*[1]*.*

Wir konzentrieren uns nun auf die Teilmengen einer beliebigen festen Menge.

[1] Zur Erinnerung: Eine binäre Relation R (d. h. eine Teilmenge R von $M \times M$) auf M heißt Äquivalenzrelation, wenn sie – wie Halbordnungen – reflexiv und transitiv, darüber hinaus aber symmetrisch ist statt antisymmetrisch. Symmetrisch bedeutet, dass $(a, b) \in R$ genau dann, wenn $(b, a) \in R$. Zwischen den Äquivalenzrelationen und den Partitionen auf M herrscht eine wohlbekannte bijektive Beziehung, auf die wir uns sehr häufig beziehen werden. Dabei wird einer Äquivalenzrelation als Partition die Menge aller Äquivalenzklassen zugeordnet.
Statt $(a, b) \in R$ verwendet man oft die Infixnotation $a\ R\ b$ – insbesondere dann, wenn man die Äquivalenzrelation nicht mit einem Buchstaben sondern mit einem Symbol wie $\sim$, $\equiv$, $\cong$ etc bezeichnet.
Die *Äquivalenzklasse* von $a \in M$ wird mit $[a]$, $[a]_R$ oder a/R bezeichnet. Diese Grundbegriffe werden wir in Unterabschnitt 2.1.1 systematisch zusammenstellen.

Definition 1.1.1.3. Sei M eine beliebige Menge. Mit $\mathfrak{P}(M)$ bezeichnen wir die Potenzmenge von M, also die Menge aller[2] Teilmengen. Mit $\mathfrak{P}_{\text{fin}}(M)$ bezeichnen wir die Menge aller endlichen Teilmengen von M.

Wenn wir den Begriff „endlich“ auch formal (und nicht nur intuitiv und informell) behandeln wollen, müssen wir eine abstrakte Eigenschaft finden, die wir den endlichen Mengen im intuitiven Sinne zuschreiben. Wir beginnen mit den endlichen *Teilmengen* einer beliebigen Menge und gehen von dem Umstand aus, dass die endlichen Teilmengen genau jene sind, die wir von der leeren Menge durch schrittweises Hinzufügen einzelner Elemente zwangsläufig erreichen. Schließlich nennen wir eine Menge endlich, wenn alle ihre Teilmengen (im obigen Sinne) endlich ist. Im Detail:

Definition 1.1.1.4. Sei M eine Menge.

- Wir nennen eine Familie $\mathscr{A} \subseteq \mathfrak{P}(M)$ *induktiv*, wenn erstens $\emptyset \in \mathscr{A}$ gilt und zweitens für alle $B \in \mathscr{A}$ und alle $x \in M$ auch die Vereinigung $B \cup \{x\}$ in $\mathscr{A}$ liegt.
- Dann ist $\mathfrak{P}(M)$ eine induktive Menge (insbesondere gibt es induktive Mengen), und $\mathfrak{P}_{\text{fin}}$ ist als Durchschnitt aller induktiven Mengen definiert:

  $$\mathfrak{P}_{\text{fin}}(M) := \bigcap \{\mathscr{A} \subseteq \mathfrak{P}(M) \mid \mathscr{A} \text{ induktiv}\}$$

  Anders formuliert gilt

  $$X \in \mathfrak{P}_{\text{fin}}(M) \;\Leftrightarrow\; \forall \mathscr{A} \subseteq \mathfrak{P}(M) : (\mathscr{A} \text{ induktiv } \Rightarrow X \in \mathscr{A}).$$

- Die Menge M heißt *endlich*, wenn $\mathfrak{P}(M) = \mathfrak{P}_{\text{fin}}(M)$ gilt, und *unendlich* sonst.

Der Grundgedanke hinter dieser Definition, insbesondere hinter dem Begriff der induktiven Familien, wird uns in späteren Unterabschnitten wieder begegnen, nämlich in Form des *Induktionsprinzips*[3].
Die folgenden Tatsachen sind mit dem intuitiven Begriff von Endlichkeit klar. Insofern ist es bemerkenswert, dass man sie mit der abstrakten Definition formal beweisen kann. Da sich diese Beweise außerhalb des Kerninteresses der Algebra befinden sondern der Mengenlehre und den Grundlagen der Mathematik zugeordnet werden können, belassen wir es im Haupttext bei der Auflistung und verweisen einschlägig Interessierte auf den Anhang. Dort haben wir Beweisskizzen zusammengestellt.

Proposition 1.1.1.5 (Siehe Proposition A.3.1.1)**.**

(1) *Sei M eine beliebige Menge und $(\mathscr{A}_i : i \in I)$ eine Familie von induktiven Teilmengen von $\mathfrak{P}(M)$. Dann ist auch $\bigcap_i \mathscr{A}_i$ induktiv. Insbesondere ist $\mathfrak{P}_{\text{fin}}(M)$ induktiv.*

(2) *Wenn $A \subseteq M$, dann gilt $\mathfrak{P}_{\text{fin}}(A) = \mathfrak{P}_{\text{fin}}(M) \cap \mathfrak{P}(A)$.*

(3) *Wenn $A \in \mathfrak{P}_{\text{fin}}(M)$, dann gilt $\mathfrak{P}(A) \subseteq \mathfrak{P}_{\text{fin}}(M)$.*

(4) *Die Menge $\mathfrak{P}_{\text{fin}}(M)$ besteht genau aus allen endlichen Teilmengen von M.*

[2] Insbesondere ist die leere Menge, die wir mit $\emptyset$ bezeichnen, jedenfalls ein Element von $\mathfrak{P}(M)$, ebenso wie die Menge M selbst.

[3] Das ähnliche Wort lässt bereits eine Verwandtschaft vermuten.

(5) *Hat die leere Menge $\emptyset$ eine gewisse Eigenschaft, die sich von jeder Menge M auf jede Menge der Form $M \cup \{x\}$ (x beliebig) vererbt, so hat jede endliche Menge diese Eigenschaft.*

(6) *Sei M eine beliebige Menge. Dann sind die folgenden Aussagen äquivalent:*
   (a) $\mathfrak{P}(M) = \mathfrak{P}_{\text{fin}}(M)$.
   (b) $M \in \mathfrak{P}_{\text{fin}}(M)$.
   (c) Es gibt ein maximales Element in $\mathfrak{P}_{\text{fin}}(M)$, das heißt: Es gibt $A \in \mathfrak{P}_{\text{fin}}(M)$, sodass es keine echte Obermenge $B \supsetneq A$ in $\mathfrak{P}_{\text{fin}}(M)$ gibt.
   (d) Jede nichtleere Teilmenge $\mathcal{E} \subseteq \mathfrak{P}(M)$ hat ein maximales Element.

(5) *Wenn $A \subseteq B$ gilt und B endlich ist, dann auch A.*

(6) *Wenn $M \approx N$ durch eine Bijektion $f\colon M \to N$ bezeugt wird, dann induziert f eine natürliche Bijektion zwischen $\mathfrak{P}(M)$ und $\mathfrak{P}(N)$; die Einschränkung dieser Bijektion auf $\mathfrak{P}_{\text{fin}}(M)$ liefert eine Bijektion $g : \mathfrak{P}_{\text{fin}}(M) \to \mathfrak{P}_{\text{fin}}(N)$, die überdies mit der Relation $\approx$ verträglich ist (das heißt: $A_1 \approx A_2$ impliziert $g(A_1) \approx g(A_2)$).*

(7) *Wenn M endlich ist und $M \approx N$, dann ist auch N endlich.*

(8) *Wenn A endlich ist, dann ist auch $A \cup \{a\}$ endlich. (Wenn $a \in A$ gilt, dann ist das trivial, also ist diese Aussage nur für $a \notin A$ interessant.)*

(9) *Wenn A und B endliche Mengen sind, dann ist auch die Vereinigungsmenge $A \cup B$ endlich.*

(10) *Wenn A und B endliche Mengen sind, dann ist auch die Produktmenge $A \times B$ endlich.*

(11) *Wenn A und B endliche Mengen sind, dann ist auch die Menge B^A endlich. (Wir schreiben[4] B^A für die Menge aller Funktionen von A nach B.)*

Damit können wir die natürlichen Zahlen formal definieren:

Definition 1.1.1.6. Sei I eine beliebige unendliche Menge (in der axiomatischen Mengenlehre wird durch ein Axiom festgelegt, dass es eine solche gibt). Nach Proposition 1.1.1.2 induziert die Relation $\approx$ auf der Menge $\mathfrak{P}_{\text{fin}}(I)$ eine Äquivalenzrelation. Dadurch wird $\mathfrak{P}_{\text{fin}}(I)$ in Klassen gleichmächtiger Mengen partitioniert; die Äquivalenzklasse einer Menge $E \in \mathfrak{P}_{\text{fin}}(I)$ bezeichnen wir mit $[E]_{\approx} = [E]_{\approx,I} := \{D \in \mathfrak{P}_{\text{fin}}(I) : D \approx E\}$. Die Menge aller dieser Äquivalenzklassen bezeichnen wir mit

$$\mathbb{N}_I := \{[E]_{\approx,I} \mid E \in \mathfrak{P}_{\text{fin}}(I)\}.$$

Lemma 1.1.1.7 (*Induktionsprinzip* für $\mathbb{N}_I$)**.** *Sei $A \subseteq \mathbb{N}_I$ mit*

- *$[\emptyset]_{\approx} \in A$;*
- *für alle $[B] \in A$ und alle $x \in I$ gilt auch $[B \cup \{x\}]_{\approx} \in A$.*

[4] Wir identifizieren Funktionen formal mit ihren Graphen; eine Funktion von A nach B ist also eine Menge f, die erstens eine Teilmenge von $A \times B$ ist, und die zweitens die Eigenschaft hat, dass es für jedes $x \in A$ genau ein $y \in B$ gibt, welches $(x, y) \in f$ erfüllt. In Unterabschnitt 2.1.1 werden auch diese Grundlagenbegriffe systematisch zusammengestellt werden.

Dann ist $A = \mathbb{N}_I$.

Beweis. Die Menge $\mathscr{A} := \{B : [B] \in A\}$ ist eine induktive Teilmenge von $\mathfrak{P}_{\text{fin}}(I)$, daher muss $A = \mathbb{N}_I$ gelten. □

Unsere Definition der natürlichen Zahlen hängt von der gewählten Menge I ab. Tatsächlich ist es für die entstehende Menge $\mathbb{N}_I$ aber ziemlich unerheblich, welche Menge I man verwendet. Dies wollen wir als Nächstes exakt formulieren.

Definition 1.1.1.8. Seien I und I' beliebige unendliche Mengen, $n \in \mathbb{N}_I$, $n' \in \mathbb{N}_{I'}$. Wir schreiben $n \sim n'$, wenn es $E \in n$, $E' \in n'$ mit $E \approx E'$ gibt. (Äquivalent: Wenn für alle $E \in n$ und alle $E' \in n'$ gilt: $E \approx E'$.)

Lemma 1.1.1.9 (Siehe Lemma A.3.4.1)**.** *Wenn I und I' unendlich sind, dann gibt es (genau) eine Bijektion $\iota\colon \mathbb{N}_I \to \mathbb{N}_{I'}$, die*

$$\forall n \in \mathbb{N}_I : \ \iota(n) \sim n$$

erfüllt.

Die Abbildung ι ordnet also jeder Äquivalenzklasse n gleichmächtiger Teilmengen von I die Äquivalenzklasse jener Teilmengen von I' zu, die gleichmächtig zu den Elementen von n sind. Zum Beispiel wird der Klasse aller 1-elementigen Teilmengen von I die Klasse alle 1-elementigen Teilmengen von I' zugeordnet. Aussagen über $\mathbb{N}_I$ kann man somit leicht in Aussagen über $\mathbb{N}_{I'}$ übersetzen. Daher lassen wir in vielen Fällen den Index I weg und schreiben nur $\mathbb{N}$ – so wie wir es gewöhnt sind.

1.1.2. Axiomatisierung nach Peano

Inhalt in Kurzfassung: Die essentiellen Eigenschaften des (unendlichen) Systems $\mathbb{N}$ der natürlichen Zahlen lassen sich durch einige wenige Forderungen erfassen. Hier wird dazu im Wesentlichen (nicht in der Formalisierung) der berühmte Zugang von Peano gewählt. Dass er das Gewünschte leistet, wird durch einen Eindeutigkeitssatz illustriert.

Wir nehmen im Folgenden an, dass es eine unendliche Menge I gibt, und wir schreiben $\mathbb{N}_I$ bzw. nur $\mathbb{N}$ für die Menge aller $\approx$-Äquivalenzklassen von $\mathfrak{P}_{\text{fin}}(I)$. Anhand der natürlichen Zahlen wollen wir in diesem Unterabschnitt ein zentrales Anliegen der Algebra illustrieren, nämlich den Wunsch nach Axiomatisierungen gewisser Objekte. Dazu greift man Charakteristika des konkreten Objekts heraus, formuliert sie als Axiome und untersucht, welche Eigenschaften andere Objekte haben, die nur diese Axiome erfüllen. In vielen Fällen stellt sich dann die Frage, wie „ähnlich“ diese Objekte zum ursprünglichen Objekt sind. In der Algebra geht es in den Axiomen zumeist um Eigenschaften gewisser Operationen sowie das Zusammenspiel zwischen Operationen und (bestimmten Elementen) der Grundmenge.
Wir schreiben 0 oder 0_I für die Äquivalenzklasse der leeren Menge, und 1 oder 1_I für die Äquivalenzklasse aller einelementigen Mengen $\{x\} \subseteq I$. Im Sinne der natürlichen

Ordnung auf $\mathbb{N}_I$ (die wir in Definition 1.1.4.10 einführen werden) ist 1 der Nachfolger von 0.
Allgemeiner kann man jeder Äquivalenzklasse $n = [C]_\approx$ ihren „Nachfolger“ $\nu(n)$ zuordnen, nämlich die Äquivalenzklasse

$$\nu([C]) := [C \cup \{d\}]_\approx$$

für beliebiges $d \in I \setminus C$. (Man sieht leicht, dass diese Definition nicht von der Wahl des Repräsentanten C abhängt, also dass ν wohldefiniert ist.)
Es gelten die folgenden Aussagen, die uns zu den gesuchten Axiomen führen (wobei wir den Index I unterdrücken):

Lemma 1.1.2.1.

(1) $0 \in \mathbb{N}$.

(2) *Für alle* $n \in \mathbb{N}$ *ist auch* $\nu(n) \in \mathbb{N}$.

(3) *Die Abbildung* $\nu\colon \mathbb{N} \to \mathbb{N}$ *ist injektiv: Aus* $\nu(n) = \nu(k)$ *folgt* $n = k$.

(4) *Für alle* $n \in \mathbb{N}$ *gilt:* $\nu(n) \neq 0$.

(5) *Für jede Teilmenge* $T \subseteq \mathbb{N}$ *gilt:*

Wenn $0 \in T$,
und für alle $n \in \mathbb{N}$ *die Implikation* $(n \in T \Rightarrow \nu(n) \in T)$ *gilt,*
dann ist $T = \mathbb{N}$.

Beweis. Die Punkte (1), (2) und (4) sind klar.

(3) Aus der Existenz einer Bijektion $f\colon C \cup \{c\} \to D \cup \{d\}$ (mit $c \notin C$, $d \notin D$) ist auf die Existenz einer Bijektion $g\colon C \to D$ zu schließen.
Wenn $f(c) = d$ gilt, dann ist die Einschränkung[5] $g := f|_C$ bereits die gewünschte Bijektion; andernfalls sei $d' = f(c)$ und $c' := f^{-1}(d)$. Dann gilt sicher $d' \neq d$, also $d' \in D$, analog $c' \in C$. Wir definieren $g(c') := d'$ sowie $g|_{C\setminus\{c'\}} := f|_{C\setminus\{c'\}}$ und erhalten eine Bijektion $g\colon C \to D$.

(5) Dies ist eine Umformulierung von Lemma 1.1.1.7. □

Definition 1.1.2.2. Sei M eine Menge, 0_M ein Element und ν_M eine Funktion mit Definitionsbereich M. Wir nennen $(M, 0_M, \nu_M)$ eine *Peano-Struktur*, wenn die sogenannten *Peano-Axiome*[6], das sind die (entsprechend umformulierten) Eigenschaften aus Lemma 1.1.2.1, erfüllt sind:

[5] Wir verwenden die Schreibweise $f|_T$ für die Einschränkung $f \cap (T \times B)$ einer Funktion $f : A \to B$ auf die Teilmenge $T \subseteq A$.

[6] Giuseppe Peano formulierte diese Axiome 1889. In Peanos Version beginnen die natürlichen Zahlen allerdings mit 1, nicht mit 0. Dieser Unterschied ist für unsere Überlegungen aber nicht relevant.

Die Frage, ob 0 eine „natürliche“ Zahl ist, ist keine mathematische. Es ist offensichtlich, dass sowohl die Menge $\{0, 1, 2, \ldots\}$ der endlichen Kardinalzahlen also auch die Menge $\{1, 2, \ldots\}$ der beim Zählen verwendeten Zahlen in der Mathematik eine wichtige Rolle spielen; welche dieser Mengen das Prädikat „natürlich“ erhält, ist aus mathematischer Sicht egal. Dass wir 0 zu den natürlichen Zahlen rechnen, erweist sich erstens in der Algebra oft als zweckmäßig und stimmt zweitens mit internationalen und österreichischen Normen überein, siehe ÖNORM EN ISO 80000-2.

(1) $0_M \in M$.

(2) $\nu_M \colon M \to M$, d. h.: für alle $n \in M$ ist auch $\nu_M(n) \in M$.

(3) Die Abbildung ν_M ist injektiv: Aus $\nu_M(n) = \nu_M(k)$ folgt $n = k$.

(4) Für alle $n \in M$ gilt: $\nu_M(n) \neq 0_M$.

(5) Für jede Teilmenge[7] $T \subseteq M$ gilt:

Wenn $0_M \in T$,
und für alle $n \in M$ die Implikation $(n \in T \Rightarrow \nu_M(n) \in T)$ gilt,
dann ist $T = M$.

Lemma 1.1.2.1 besagt, dass die Struktur $(\mathbb{N}_I, \nu_I, 0_I)$ eine Peano-Struktur ist. Tatsächlich aber enthalten die fünf Peano-Axiome in einem gewissen Sinn alle wesentliche Information über die natürlichen Zahlen. Diese noch etwas vage Behauptung wollen wir nun präzisieren.
In den Peano-Axiomen steckt sicherlich dann die wesentliche Information über die natürlichen Zahlen, wenn jede Peano-Struktur $(M, 0_M, \nu_M)$ im Sinne von Definition 1.1.2.2 zu $(\mathbb{N}, 0, \nu)$ strukturgleich ist. Dies wiederum bedeutet, dass die Elemente von M in bijektiver Weise den natürlichen Zahlen *entsprechen*, in mathematischer Terminologie: Es gibt einen *Isomorphismus* zwischen $\mathbb{N}$ und M, d. h. genauer eine bijektive Abbildung $\varphi \colon \mathbb{N} \to M$ mit

- $\varphi(0) = 0_M$ und
- $\varphi(\nu(n)) = \nu_M(\varphi(n))$ für alle $n \in \mathbb{N}$, also $\varphi \circ \nu = \nu_M \circ \varphi$.

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\nu} & \mathbb{N} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ M & \xrightarrow{\nu_M} & M \end{array}$$

In diesem Fall heißen $(\mathbb{N}, 0, \nu)$ und $(M, 0_M, \nu_M)$ *isomorph*, symbolisch

$$(\mathbb{N}, 0, \nu) \cong (M, 0_M, \nu_M).$$

Der Begriff des Isomorphismus ist zentral in der Algebra, muss aber natürlich an die jeweilige Situation angepasst werden. Im vorliegenden Fall geht es nur um die sogenannte *Verträglichkeit* mit Nullelement 0 und Nachfolgerfunktion ν. Schon im vorliegenden

[7] Man beachte, dass diese letzte Forderung nicht über *Elemente* der betrachteten Struktur (also: über natürliche Zahlen) quantifiziert, sondern über *Teilmengen* der betrachteten Struktur (also: über Mengen von natürlichen Zahlen). Die Sprache, in der dieses Axiom formuliert ist, nennt man daher „Logik zweiter Stufe“; in „Logik erster Stufe“ beziehen sich die Quantoren $\forall$ und $\exists$ immer nur auf Elemente einer Struktur.

Es gibt eine schwächere, erststufige Variante der Peano-Axiome, mit der wir uns hier aber nicht beschäftigen werden. Solche Axiome ließen Spielraum für sogenannte *Nonstandardmodelle* der natürlichen Zahlen, die zu $\mathbb{N}$ nicht isomorph sind. Diesbezüglich Interessierte seien auf die mathematische Logik verwiesen.

einführenden Kapitel werden wir Isomorphismen in vielen anderen Varianten verwenden und davon ausgehen, dass aus dem Kontext klar ist, was genau jeweils damit gemeint ist. Sogar im vergangenen Unterabschnitt sind wir implizit auf die entsprechende Idee gestoßen: Lemma 1.1.1.9 besagt genau, dass $\mathbb{N}_I$ und $\mathbb{N}_{I'}$ isomorph sind. Systematisch werden wir in Unterabschnitt 2.1.5 darauf zurückkommen.
Tatsächlich gilt die folgende Eindeutigkeitsaussage modulo Isomorphie, die uns zeigt, dass wir $\mathbb{N}$ auch als beliebige Peano-Struktur definieren könnten. Außerdem berechtigt sie uns nochmals, irgendeine der in Unterabschnitt 1.1.1 konstruierten Mengen $\mathbb{N}_I$ zur Definition der natürlichen Zahlen heranzuziehen – sie ist stärker als Lemma 1.1.1.9, da wir nun sehen, dass es wirklich nur auf die Peano-Axiome ankommt und nicht auf hypothetische weitere, noch nicht identifizierte Eigenschaften der $\mathbb{N}_I$.

Satz 1.1.2.3 (Siehe Satz A.3.4.2)**.** *Ist $(M, 0_M, \nu_M)$ eine beliebige Peano-Struktur, so gilt*

$$(\mathbb{N}, 0, \nu) \cong (M, 0_M, \nu_M).$$

Der zugehörige Isomorphismus $\varphi\colon \mathbb{N} \to M$ ist eindeutig bestimmt.

Einsichtig ist dies sofort, weil die Rekursion $\varphi(0) := 0_M$, $\varphi(\nu(n)) := \nu_M(\varphi(n))$ tatsächlich einen eindeutigen Isomorphismus φ definiert. Streng genommen beruht dies (wie auch schon Lemma 1.1.1.9) auf dem Rekursionssatz. Für eine genaue Behandlung verweisen wir wieder auf den Anhang.
Stattdessen betrachten wir eine Übungsaufgabe, die auf andere Art die Rolle der verschiedenen Peano-Axiome klarmacht.

UE 1 ► Übungsaufgabe 1.1.2.4. (B) Illustrieren Sie für die Peano-Axiome[8] (3)-(5), dass nicht darauf verzichtet werden kann, ohne dadurch die Eindeutigkeit der beschriebenen Struktur zu verlieren. Finden Sie dazu für $j = 3, 4, 5$ eine Menge $M^{(j)}$, ein Element $0_{M^{(j)}}$ und eine Funktion $\nu_{M^{(j)}}$, sodass $(M^{(j)}, 0_{M^{(j)}}, \nu_{M^{(j)}})$ alle Peano-Axiome erfüllt außer (j). **◄ UE 1**

UE 2 ► Übungsaufgabe 1.1.2.5. (F+) Begründen Sie: Ist jedes Modell der Peano-Axiome isomorph zu $(\mathbb{N}, 0, \nu)$, so sind auch je zwei beliebige Modelle der Peano-Axiome zueinander isomorph. **◄ UE 2**

Ein alternativer, stärker mengentheoretisch orientierter Zugang zu den natürlichen Zahlen stammt von Richard Dedekind (1831-1916): Sei M eine Menge und $f : M \to M$ injektiv aber nicht surjektiv. Dann erhält man eine Peano-Struktur wie folgt: Weil f nicht surjektiv ist, gibt es ein $m_0 \in M \setminus f(M)$. Wir setzen $0_M := m_0$ und nennen eine Teilmenge $T \subseteq M$ Dedekind-induktiv, wenn $m_0 \in T$ und aus $m \in T$ stets $f(m) \in T$ folgt. Sei $\mathbb{N}_M$ der Schnitt aller Dedekind-induktiven Teilmengen von M, außerdem $\nu_M := f|_{\mathbb{N}_M}$ die Einschränkung von f auf $\mathbb{N}_M$. Dann erweist sich $(\mathbb{N}_M, 0_M, \nu_M)$ als Peano-Struktur.

UE 3 ► Übungsaufgabe 1.1.2.6. (V,E) Führen Sie alle zugehörigen Überlegungen zum gerade beschriebenen Dedekindschen Zugang im Detail durch. **◄ UE 3**

[8] Die Axiome (1) und (2) besagen genau, dass eine Peano-Struktur stets eine Algebra im Sinne von Definition 2.1.3.2 ist, was wir auch in dieser Aufgabe jedenfalls fordern wollen.

1.1.3. Das von Neumannsche Modell

Inhalt in Kurzfassung: Ein mengentheoretisches Modell für die Peano-Axiome (siehe vorangegangener Unterabschnitt) wurde von John von Neumann angegeben. Es hat für sich reizvolle Eigenschaften, zeigt aber vor allem, dass die Mengenlehre mindestens so stark ist wie die Peano-Arithmetik (in Wahrheit sogar stärker).

Die scheinbare Abhängigkeit der natürlichen Zahlen $\mathbb{N}_I$ von einem willkürlichen Parameter I mag als ein ästhetischer Mangel unserer Definition erscheinen. Dies führt uns zu einem weiteren zentralen Anliegen der Algebra (und der Mathematik insgesamt), nämlich der Klassifikation von Objekten. Wenn wir (dank Satz 1.1.2.3 und Übungsaufgabe 1.1.2.5) schon wissen, dass je zwei Peano-Strukturen isomorph sind, so stellt sich die Frage nach einem „kanonischen“ Vertreter, also in diesem Fall nach einer „natürlichen“ Penao-Struktur. In Unterabschnitt 2.1.7 werden wir auf Überlegungen zur Klassifikation zurückkommen.
Warum beschränken wir uns etwa in der Definition der Zahl 1 auf jene Mengen $\{a\}$, für die $a \in I$ (mit festem I) gilt, bei der Definition der Zahl 2 auf jene Mengen $\{a, b\}$, die (neben $a \neq b$) auch $a, b \in I$ erfüllen, etc? Könnten wir nicht eine Menge M als „induktiv“ definieren, wenn erstens $\emptyset \in M$ gilt, und zweitens für alle $C \in M$ und beliebiges $x \notin C$ auch $C \cup \{x\} \in M$? Der Durchschnitt aller induktiven Mengen wäre dann immer noch induktiv und würde (modulo der Relation $\approx$) auch ein Modell der natürlichen Zahlen liefern, wäre also insbesondere isomorph zu $\mathbb{N}_I$ und würde die Peano-Axiome erfüllen. Dabei würde die Zahl 1 aus *allen* einelementigen Mengen $\{a\}$ bestehen.
So eine Konstruktion lässt sich (auf Basis der mengentheoretischen Axiome ZFC, siehe Abschnitt A.6 im Anhang) aber nicht durchführen, da so eine Menge M insbesondere alle Singletons $\{a\}$ enthalten müsste, und damit, vereinfacht gesprochen, zu groß wäre. Man kann (aus den ZFC-Axiomen) sogar beweisen, dass es so eine Menge nicht geben kann.
Da wir aber ohnehin nach der Relation $\approx$ ausfaktorisieren, d. h. zur Menge der Äquivalenzklassen übergehen wollen, erweist es sich als gar nicht nötig, *alle* Repräsentanten einer Äquivalenzklasse (z. B. alle Singletons) in unserer gesuchten Menge unterzubringen. Die folgende Konstruktion, die auf John von Neumann (1903–1957) zurückgeht, strebt das andere Extrem an und sucht in jeder Äquivalenzklasse (bezüglich $\approx$) einen *einzigen* Repräsentanten. In diesem System wird die Rolle der Zahl 0 von der leeren Menge übernommen:

$$0_{\text{vN}} := \emptyset$$

Die Zahl 1 wird durch eine einzige Menge der Form $\{a\}$ repräsentiert; eine kanonische Wahl von a ergibt sich durch[9] die Definition $a := 0_{\text{vN}}$:

$$1_{\text{vN}} := \{0_{\text{vN}}\}$$

Ein Repräsentant der Zahl 2 ist eine Menge der Form $\{x, y\}$, wobei wir garantieren

[9] Man beachte, dass die Menge $\emptyset$ zwar leer ist, die Menge $\{\emptyset\}$ aber nicht, weil sie definitionsgemäß ein Element enthält. Daraus folgt auch, dass die Mengen $\emptyset$ und $\{\emptyset\}$ verschieden sind.

müssen, dass $x \neq y$ gilt; es bietet sich an, $x := 0_{\mathrm{vN}}$ und $y := 1_{\mathrm{vN}}$ zu wählen, etc.

$$2_{\mathrm{vN}} := \{0_{\mathrm{vN}}, 1_{\mathrm{vN}}\},\ 3_{\mathrm{vN}} := \{0_{\mathrm{vN}}, 1_{\mathrm{vN}}, 2_{\mathrm{vN}}\},\ \ldots$$

Um klarzustellen, was „. . . “ hier bedeutet, gehen wir so vor:

Definition 1.1.3.1. Eine Menge S von Mengen heißt vN-induktiv, falls $\emptyset \in S$ und zu jedem $s \in S$ auch $s' := s \cup \{s\}$ in S liegt.

Man sieht leicht, dass eine vN-induktive Menge S jedenfalls die Elemente $0_{\mathrm{vN}}, 1_{\mathrm{vN}}, 2_{\mathrm{vN}}, \ldots$ enthalten muss.
Das Unendlichkeitsaxiom der Mengenlehre (siehe Unterabschnitt A.6.2) garantiert die Existenz vN-induktiver Mengen. Die Menge $\mathbb{N}_{\mathrm{vN}}$ der natürlichen Zahlen (im Sinne der von Neumannschen Konstruktion) ist definiert wie folgt:

$$n \in \mathbb{N}_{\mathrm{vN}} \quad :\Leftrightarrow \quad \forall S : (S \text{ vN-induktiv} \Rightarrow n \in S).$$

Diese Definition kann man sich als

$$\mathbb{N}_{\mathrm{vN}} := \bigcap \{S :\ S \text{ ist vN-induktiv}\} = \bigcap_{S \text{ ist vN-induktiv}} S$$

vorstellen, hier muss man aber etwas Vorsicht walten lassen: es gibt nämlich (sobald wir uns darauf geeinigt haben, dass es überhaupt vN-induktive Mengen gibt) „sehr viele“ vN-induktive Mengen; daraus kann man auf Basis der ZFC-Axiome folgern, dass es keine *Menge* $\mathfrak{S}$ gibt, die alle vN-induktiven Mengen enthält. Die obige Notation $\{S :\ S \text{ ist vN-induktiv}\}$ ist also nicht so zu verstehen, dass hier eine Menge definiert wird, sondern eher eine *Unmenge*; der in der Mengenlehre übliche Terminus technicus ist hier *Klasse*.
Auch wenn es die Menge $\mathfrak{S}$, die alle vN-induktiven Mengen enthält, nicht gibt, so kann man aus den ZFC-Axiomen dennoch die Existenz des gerade betrachteten Durchschnitts folgern. Diese Feinheit wird uns im Folgenden aber nicht mehr beschäftigen.

UE 4 ► Übungsaufgabe 1.1.3.2. (F+) Zeigen Sie, dass der Schnitt vN-induktiver Mengen (insbesondere also die Menge $\mathbb{N}_{\mathrm{vN}}$) vN-induktiv ist. **◄ UE 4**

Aus der Definition von $\mathbb{N}_{\mathrm{vN}}$ lässt sich leicht das *Induktionsprinzip* (oder auch *Prinzip der vollständigen Induktion*) gewinnen. Setzen wir $0_{\mathrm{vN}} := \emptyset$ und $\nu_{\mathrm{vN}} : \mathbb{N}_{\mathrm{vN}} \to \mathbb{N}_{\mathrm{vN}}$, $\nu_{\mathrm{vN}}(n) := n \cup \{n\}$, so gilt für jede Teilmenge $T \subseteq \mathbb{N}_{\mathrm{vN}}$:

> Wenn $0_{\mathrm{vN}} \in T$,
> und für alle $n \in \mathbb{N}_{\mathrm{vN}}$ die Implikation $(n \in T \Rightarrow \nu_{\mathrm{vN}}(n) \in T)$ gilt,
> dann ist $T = \mathbb{N}_{\mathrm{vN}}$.

Zum Beweis reicht es, Folgendes zu beobachten: Die Voraussetzung besagt genau, dass T eine vN-induktive Teilmenge von $\mathbb{N}_{\mathrm{vN}}$ ist. Da $\mathbb{N}_{\mathrm{vN}}$ umgekehrt in allen vN-induktiven Mengen enthalten ist, folgt $T = \mathbb{N}_{\mathrm{vN}}$. Mit anderen Worten haben wir das fünfte Peano-Axiom für $(\mathbb{N}_{\mathrm{vN}}, 0_{\mathrm{vN}}, \nu_{\mathrm{vN}})$ nachgewiesen. Tatsächlich gelten auch die anderen Peano-Axiome:

Satz 1.1.3.3 (Siehe Satz A.3.2.1.)**.** *Die Struktur* $(\mathbb{N}_{vN}, 0_{vN}, \nu_{vN})$ *(genannt das* Modell von John von Neumann*) mit* $\nu_{vN}\colon \mathbb{N}_{vN} \to \mathbb{N}_{vN}$, $n \mapsto n \cup \{n\}$, *ist ein Modell der Peano-Axiome (und daher isomorph zu* $(\mathbb{N}_I, 0_I, \nu_I)$ *für jede unendliche Menge* I*).*

Zwar haben wir nicht über Axiomatisierungen der Mengenlehre, etwa durch das Axiomensystem ZFC (siehe Abschnitt A.6 im Anhang) gesprochen, doch sei an dieser Stelle auf folgende Konsequenz von Satz 1.1.3.3 hingewiesen: Ist eine Mengenlehre, in der das Modell der natürlichen Zahlen von John von Neumann konstruiert werden kann, widerspruchsfrei, so sind auch die Peano-Axiome widerspruchsfrei. Analoges gilt auch für die nun folgende Ausweitung um die arithmetischen Operationen zur Peano-Arithmetik.

1.1.4. Arithmetik und Ordnung der natürlichen Zahlen

Inhalt in Kurzfassung: In den bisher behandelten Peano-Axiomen war von einer Nachfolgerfunktion die Rede, nicht jedoch von Addition, Multiplikation und Ordnung auf $\mathbb{N}$. Diese Anreicherungen der Struktur sollen nun wieder auf mengentheoretischer Grundlage erfolgen. Außerdem werden die wichtigsten Rechenregeln für natürliche Zahlen hergeleitet.

Wir rekapitulieren Proposition 1.1.1.5 und bauen aus:

Satz 1.1.4.1 (Siehe Satz A.3.3.1)**.** *Sei* I *eine unendliche Menge und seien* $n, k \in \mathbb{N}_I$*. Dann gibt es disjunkte Mengen* $A, B \in \mathfrak{P}_{\text{fin}}(I)$ *mit* $n = [A]_\approx$, $k = [B]_\approx$*; für jede solche Wahl von* A *und* B *gilt dann auch* $A \cup B \in \mathfrak{P}_{\text{fin}}(I)$*. Weiters gibt es*

- *eine Menge* $C \in \mathfrak{P}_{\text{fin}}(I)$ *mit* $C \approx A \times B$*.*
- *eine Menge* $D \in \mathfrak{P}_{\text{fin}}(I)$ *mit* $D \approx B^A$*.*

Dieser Satz erlaubt uns, arithmetische Operationen auf der Menge $\mathbb{N}_I$ zu definieren:

Definition 1.1.4.2. Sei I eine unendliche Menge, $A, B \in \mathfrak{P}_{\text{fin}}(I)$.
Wir definieren

$$\begin{aligned} [A]_\approx + [B]_\approx &:= [A \cup B]_\approx \quad \text{(sofern } A \text{ und } B \text{ disjunkt sind)} \\ [A]_\approx \cdot [B]_\approx &:= [A \times B]_\approx \\ [B]_\approx^{[A]_\approx} &:= [B^A]_\approx \end{aligned}$$

Bei diesen Definitionen ist ein Aspekt, nämlich *Wohldefiniertheit*, entscheidend in einer Weise, die uns durch die ganze Algebra begleiten wird. Und zwar werden Operationen (oder allgemeiner Funktionen; hier sind es Addition, Multiplikation und Exponentiation) auf einer Menge von Äquivalenzklassen definiert, indem man auf ihre Repräsentanten bereits bekannte Operationen (hier: die Konstruktion von Vereinigungen, kartesischen Produkte und Mengen von Funktionen) anwendet. A priori wäre es denkbar, dass verschiedene Elemente der Klassen (also verschiedene Repräsentanten) zu verschiedenen Ergebnissen führen. Wohldefiniertheit bedeutet hier, dass genau das nicht eintreten kann,

dass also – formuliert am Beispiel von $\cdot$, die anderen Operationen sind analog zu behandeln – Folgendes gilt: Wenn $A \approx A'$ und $B \approx B'$, dann auch $A \times A' \approx B \times B'$. Beim in der Algebra besonders wichtigen Begriff der *Kongruenzrelation* (siehe Definition 2.2.3.2) wird ebenfalls diese Art von Wohldefiniertheit die zentrale Rolle spielen.

UE 5 ► **Übungsaufgabe 1.1.4.3.** (V) Zeigen Sie, dass $n + k$, $n \cdot k$ und n^k wohldefiniert sind. ◄ **UE 5**
(Bevor Sie den Beweis beginnen, geben Sie jeweils ausführlicher an, was überhaupt zu zeigen ist.)

Man kann leicht zeigen, dass die üblichen Rechengesetze für die Elemente von $\mathbb{N}_I$ gelten, zum Beispiel:

Lemma 1.1.4.4. *Die Addition ist eine kommutative Operation auf den natürlichen Zahlen.*

Beweis. Sei $k + l = j$. Das heißt, dass es disjunkte Mengen K und L gibt mit $[K]_\approx = k$, $[L]_\approx = l$, und mit $[K \cup L]_\approx = j$.
Dann ist aber $l+k$ definitionsgemäß die $\approx$-Äquivalenzklasse der Menge $L \cup K$, in Zeichen $[L \cup K]_\approx = l+k$. Wegen $L \cup K = K \cup L$ erhalten wir $l+k = [L \cup K]_\approx = [K \cup L]_\approx = k+l$. □

UE 6 ► **Übungsaufgabe 1.1.4.5.** (F) Beweisen Sie (auf Grundlage der obigen Definition 1.1.4.2), ◄ **UE 6**
dass für alle natürlichen Zahlen k, k', l, j die folgenden Gleichungen bzw. Implikationen gelten (dabei schreiben wir $1 := \nu(0)$):

(1) $k + l = l + k$. (Haben wir schon gezeigt.)
(2) $k \cdot l = l \cdot k$.
(3) $(k + l) + j = k + (l + j)$ (Assoziativgesetz für Addition und Multiplikation)
(4) $k \cdot (l + j) = k \cdot l + k \cdot j$ (Distributivgesetz)
(5) $k + 0 = k$, $k + 1 = \nu(k)$.
(6) $k \cdot 0 = 0$, $k \cdot 1 = k$.
(7) Wenn $k \neq 0$, dann gibt es j mit $k = j + 1$.
(8) Aus $k + l = k' + l$ folgt $k = k'$. (Kürzungsregel für $+$)
(9) Aus $k \cdot l = k' \cdot l$ und $l \neq 0$ folgt $k = k'$. (Kürzungsregel für $\cdot$)

Hinweis: In den meisten Unterpunkten ist eine geeignete Bijektion zu finden. In (8) und (9) bietet sich Induktion an (siehe Lemma 1.1.1.7) – formal gesprochen also beispielsweise für (8) der Beweis, dass die Menge $\{l \in \mathbb{N}_I \mid \forall k, k' \in \mathbb{N}_I : k + l = k' + l \Rightarrow k = k'\}$ das Element $0 = [\emptyset]_\approx$ enthält und unter Nachfolgern abgeschlossen ist (was heißt das genau?). Dabei kann es nützlich sein, zuerst nachzuweisen, dass 1 in dieser Menge enthalten ist (Bijektion!). In (9) erweist sich Induktion „nach k“ als zielführend (was heißt das genau?).

UE 7 ► Übungsaufgabe 1.1.4.6. (F) Beweisen Sie (auf Grundlage der obigen Definition 1.1.4.2), dass für alle natürlichen Zahlen k, l, j die folgenden Gleichungen gelten: **◄ UE 7**

(1) $(k^j)^l = k^{j \cdot l}$.

(2) $(k^j) \cdot (k^l) = k^{j+l}$.

Hinweis: Wieder sind geeignete Bijektionen zu finden, für den ersten Beweis ist eine Bijektion b zwischen den Mengen $(K^J)^L$ und $K^{J \times L}$ gesucht. Beachten Sie, dass die Elemente der Definitions- wie auch der Wertemenge der Funktion b selbst wiederum Funktionen sind.

Wir betrachten die Aussagen (3) und (5) aus Übungsaufgabe 1.1.4.5 nochmals unter einem etwas anderen Blickwinkel:

Satz 1.1.4.7.

(1) *Für alle $x, y \in \mathbb{N}_I$ gilt*

$$((+)) \qquad x + 0 = x \quad \textit{und} \quad x + \nu(y) = \nu(x + y).$$

(2) *Umgekehrt: Sei $f \colon \mathbb{N}_I \times \mathbb{N}_I \to \mathbb{N}_I$ eine beliebige Funktion, die $f(x, 0) = x$ und $f(x, \nu(y)) = \nu(f(x, y))$ für alle $x, y \in \mathbb{N}_I$ erfüllt. Dann muss $f(x, y) = x + y$ für alle $x, y \in \mathbb{N}_I$ gelten.*

Kurz gesagt: Die Gleichungen $((+))$ charakterisieren die Additionsfunktion.

Beweis. Wir skizzieren einen Beweis von (2): Für beliebiges $x \in \mathbb{N}_I$ betrachten wir die Menge $T_x := \{y \in \mathbb{N}_I : f(x, y) = x + y\}$. Man sieht leicht, dass T_x das Element 0 enthält und unter Nachfolgern abgeschlossen ist; daraus folgt die Behauptung. □

UE 8 ► Übungsaufgabe 1.1.4.8. (F) Zeigen Sie, dass die Gleichungen **◄ UE 8**

$$((\cdot)) \qquad \forall x, y : \ x \cdot 0 = 0 \ \text{ und } \ x \cdot \nu(y) = (x \cdot y) + x$$

die Multiplikationsfunktion charakterisieren.

UE 9 ► Übungsaufgabe 1.1.4.9. (F) Zeigen Sie, dass die Gleichungen **◄ UE 9**

$$((\uparrow)) \qquad \forall x, y : \ x^0 = 1 \ \text{ und } \ x^{\nu(y)} = (x^y) \cdot x$$

die Exponentiation charakterisieren.

Definition 1.1.4.10. Sei I eine unendliche Menge. Auf der Menge $\mathbb{N}_I$ definieren wir die folgende Relation $\leq$:

$$[E]_{\approx} \leq [F]_{\approx} \ :\Leftrightarrow \ \exists E' : E \approx E' \subseteq F$$

Auch hier ist wieder die Wohldefiniertheit zu beachten:

Lemma 1.1.4.11. *Seien $C, D, E, F \in \mathfrak{P}_{\text{fin}}(I)$ und sei $C \approx E$ sowie $D \approx F$. Weiters gebe es E' mit $E \approx E' \subseteq F$. Dann gibt es C' mit $C \approx C' \subseteq D$.*

Beweis. Seien $f : C \to E$, $g : D \to F$ und $h : E \to E'$ Bijektionen. Wir setzen $C' := g^{-1}(E') \subseteq D$ und bemerken, dass $g^{-1}|_{E'} \circ h \circ f$ eine Bijektion $C \to C'$ ist, womit wir $C \approx C'$ erhalten. □

Unmittelbar aus der Definition folgt $n \leq \nu(n)$ für alle $n \in \mathbb{N}_I$. Wir sammeln einige weitere wichtige (und intuitiv klare) Tatsachen über $\leq$ und über das Zusammenspiel zwischen $\leq$ und den Rechenoperationen $+$ sowie $\cdot$ im folgenden Satz:

Satz 1.1.4.12 (Siehe Satz A.3.3.2)**.** *Sei $\leq$ die durch Definition 1.1.4.10 gegebene Relation. Für alle natürlichen Zahlen k, k', n, n' gelten folgende Eigenschaften:*

(1) $\nu(n) \not\leq n$.

(2) *Wenn $k \leq n$ und $k \neq n$, dann gilt $\nu(k) \leq n$.*

(3) *$\leq$ ist reflexiv, transitiv und antisymmetrisch, d. h. eine Ordnungsrelation.*

(4) *Es gilt entweder $n \leq k$ oder $k \leq n$, d. h. $\leq$ ist eine lineare Ordnung.*

(5) *Es gilt*

$$((\leq)) \qquad \forall x, y: \ (x \leq 0 \Leftrightarrow x = 0) \text{ und } (x \leq \nu(y) \Leftrightarrow x \leq y \text{ oder } x = \nu(y))$$

(6) *Die Bedingung $((\leq))$ charakterisiert bereits die Relation $\leq$, das heißt:*
Jede Relation $R \subseteq \mathbb{N} \times \mathbb{N}$, die $x \ R \ 0 \Leftrightarrow x = 0$ und $x \ R \ \nu(y) \ \Leftrightarrow \ x \ R \ y$ oder $x = \nu(y)$ für alle x, y erfüllt, muss die Relation $\leq$ sein.

(7) *Aus $k \leq k'$ und $n \leq n'$ folgt $k + n \leq k' + n'$. (Monotoniegesetz für $+$)*

(8) *Aus $k \leq k'$ und $n \leq n'$ folgt $k \cdot n \leq k' \cdot n'$. (Monotoniegesetz für $\cdot$)*

Aussage (6) liefert also eine Charakterisierung der Relation $\leq$, in Analogie zu den oben genannten Bedingungen $((+))$, $((*))$ und $((\uparrow))$, die Addition, Multiplikation und Exponentiation durch jeweils zwei Bedingungen charakterisieren – eine für die Zahl 0, die andere für Nachfolger.
Die in diesem Unterabschnitt besprochenen Sachverhalte, insbesondere die Eigenschaften $((+))$ und $((\cdot))$ sowie $((\leq))$ können wir auch aus Sicht der Peano-Axiome betrachten.

Definition 1.1.4.13. Unter der *Peano-Arithmetik* verstehen wir die Peano-Axiome erweitert um die Axiome $((+))$, $((\cdot))$ und $((\leq))$. Explizit:

(1) $0_M \in M$.

(2) $\nu_M \colon M \to M$, d. h.: für alle $n \in M$ ist auch $\nu_M(n) \in M$.

(3) Die Abbildung ν_M ist injektiv: Aus $\nu_M(n) = \nu_M(k)$ folgt $n = k$.

(4) Für alle $n \in M$ gilt: $\nu_M(n) \neq 0_M$.

(5) Für jede Teilmenge $T \subseteq M$ gilt:

Wenn $0_M \in T$,
und für alle $n \in M$ die Implikation $(n \in T \Rightarrow \nu_M(n) \in T)$ gilt,
dann ist $T = M$.

((+)) Für alle $x, y \in M$ gilt: $x +_M 0_M = x$ und $x +_M \nu_M(y) = \nu_M(x +_M y)$.

((·)) Für alle $x, y \in M$ gilt: $x \cdot_M 0_M = 0_M$ und $x \cdot_M \nu_M(y) = (x \cdot_M y) +_M x$.

((≤)) Für alle $x, y \in M$ gilt: $(x \leq_M 0_M \Leftrightarrow x = 0_M)$ und
$(x \leq_M \nu_M(y) \Leftrightarrow x \leq_M y$ oder $x = \nu_M(y))$.

Wir nennen $(M, 0_M, \nu_M, +_M, \cdot_M, \leq_M)$ ein *Modell der Peano-Arithmetik*, wenn die Axiome der Peano-Arithmetik erfüllt sind.

Die Eindeutigkeitsaussage bis auf Isomorphie für Peano-Strukturen vererbt sich in sehr starker Form auf Modelle der Peano-Arithmetik:

Satz 1.1.4.14. *Sind $(M, 0_M, \nu_M, +_M, \cdot_M, \leq_M)$ und $(N, 0_N, \nu_N, +_N, \cdot_N, \leq_N)$ zwei Modelle der Peano-Arithmetik, so gibt es einen Isomorphismus zwischen diesen beiden Strukturen, d. h. eine bijektive Abbildung $\varphi : M \to N$ mit*

- *$\varphi(0_M) = 0_N$.*
- *Für alle $x \in M$ gilt: $\nu_N(\varphi(x)) = \varphi(\nu_M(x))$.*
- *Für alle $x, y \in M$ gilt: $\varphi(x +_M y) = \varphi(x) +_N \varphi(y)$.*
- *Für alle $x, y \in M$ gilt: $\varphi(x \cdot_M y) = \varphi(x) \cdot_N \varphi(y)$.*
- *Für alle $x, y \in M$ gilt: $x \leq_M y \Leftrightarrow \varphi(x) \leq_N \varphi(y)$.*

Dabei ist der Isomorphismus φ eindeutig bestimmt.
Tatsächlich gilt sogar: Ein Isomorphismus $\varphi : (M, 0_M, \nu_M) \cong (N, 0_N, \nu_N)$ im Sinne von Satz 1.1.2.3 ist automatisch ein Isomorphismus $(M, 0_M, \nu_M, +_M, \cdot_M, \leq_M) \cong (N, 0_N, \nu_N, +_N, \cdot_N, \leq_N)$.

UE 10 ► **Übungsaufgabe 1.1.4.15.** (V) Zeigen Sie Satz 1.1.4.14. ◄ **UE 10**
Hinweis: Um die Verträglichkeit von φ mit beispielsweise $+$ nachzuweisen, betrachten Sie die Abbildung $\oplus : N \times N \to N$, $z \oplus w := \varphi(\varphi^{-1}(z) +_M \varphi^{-1}(w))$ und wiederholen den Beweis von Satz 1.1.4.7.

Nach Satz 1.1.4.14 gelten alle Eigenschaften aus Übungsaufgabe 1.1.4.5 und Satz 1.1.4.12 automatisch in jedem Modell der Peano-Arithmetik. Alternativ kann man diese Eigenschaften auch direkt aus den Axiomen ableiten, typischerweise unter Verwendung von (gegebenfalls verschachtelter) Induktion. Für eine Kostprobe verweisen wir auf Übungsaufgabe 1.1.5.4 im nächsten Unterabschnitt.

1.1.5. Bemerkungen zu Induktionsbeweisen

Inhalt in Kurzfassung: Wir erläutern hier verschiedene Möglichkeiten, wie man das Induktionsprinzip in Beweisen einsetzen kann.

Anmerkung 1.1.5.1. Um eine Aussage $\forall x \in \mathbb{N} : \psi(x)$ zu beweisen, genügt es zu zeigen, dass die Menge $M := \{n \in \mathbb{N} \mid \psi(n)\}$ erstens die Zahl 0 enthält und zweitens unter der Nachfolgeroperation $x \mapsto x + 1$ abgeschlossen ist.

Wenn eine Aussage $\forall x \in \mathbb{N}\ \forall y \in \mathbb{N} : \varphi(x, y)$ (wie etwa das Kommutativgesetz der Addition) mit Induktion zu beweisen ist, dann bieten sich verschiedene Möglichkeiten an:

- „Induktion mit Parameter“: Wir halten einen (beliebigen) Wert $b \in \mathbb{N}$ fest, und beweisen dann die Aussage $\forall x \in \mathbb{N} : \varphi(x, b)$ mit Induktion „nach x“. Das heißt, wir zeigen, dass für jedes $b \in \mathbb{N}$ die Menge

  $$M_b := \{x \in \mathbb{N} \mid \varphi(x, b)\}$$

  sowohl die Zahl 0 enthält als auch unter Nachfolgern abgeschlossen ist.
- „Simultane Induktion“: Wir setzen $\psi(x) := \forall y : \varphi(x, y)$, und beweisen die Formel $\forall x : \psi(x)$ mit Induktion „nach x“. Das heißt, wir zeigen, dass die Menge

  $$M := \{x \in \mathbb{N} \mid \forall y : \varphi(x, y)\}$$

  sowohl die Zahl 0 enthält als auch unter Nachfolgern abgeschlossen ist.
- „Induktion nach dem Maximum“: Wir setzen $\psi(z) := \forall x \leq z\ \forall y \leq z : \varphi(x, y)$, und beweisen die Formel $\forall z : \psi(z)$ mit Induktion „nach z“. Das heißt, wir zeigen, dass die Menge

  $$M := \{z \in \mathbb{N} \mid \forall x \leq z\ \forall y \leq z : \varphi(x, y)\}$$

  sowohl die Zahl 0 enthält als auch unter Nachfolgern abgeschlossen ist.

Diese Liste ist nicht vollständig. Man könnte zum Beispiel auch „Induktion nach der Summe“ betrachten.
Man beachte, dass man bei Parameter-Induktion im Induktionsschritt

$$\varphi(n, b) \Rightarrow \varphi(n + 1, b)$$

nur die Voraussetzung $\varphi(n, b)$ verwenden darf; bei simultaner Induktion kann man hingegen für den Beweis von $\varphi(n + 1, y)$ bereits $\forall z\ \varphi(n, z)$ verwenden.

Es kommt gelegentlich vor, dass man sich den Induktionsschritt $\varphi(x) \Rightarrow \varphi(x+1)$ dadurch erleichtern kann, dass man φ durch eine stärkere Aussage φ' ersetzt. Die Implikation $\varphi'(x) \to \varphi'(x+1)$ könnte nämlich wegen der stärkeren Voraussetzung leichter zu beweisen sein. Ein Spezialfall dieser Variante ist die „Verlaufsinduktion“, deren Korrektheit sehr einfach nachzuweisen ist:

Lemma 1.1.5.2. *Sei $\varphi(x)$ eine Formel. Wir setzen $\varphi_{\leq}(x) := \forall y \in \mathbb{N} : (y \leq x \Rightarrow \varphi(y))$ und $\varphi_{<}(x) := \forall y \in \mathbb{N} : (y < x \Rightarrow \varphi(y))$. Dann sind die folgenden Aussagen äquivalent:*

(1) $\forall x \in \mathbb{N} : \varphi(x)$.

(2) $\forall x \in \mathbb{N} : \varphi_{\leq}(x)$.

(3) $\forall x \in \mathbb{N} : \varphi_{<}(x)$.

Anmerkung 1.1.5.3.

(1) Für einen Induktionsbeweis von $\forall x \in \mathbb{N} : \varphi_{<}(x)$ ist kein „Induktionsanfang“ notwendig, denn $\varphi_{<}(0)$ gilt trivialerweise.

(2) Im Induktionsschritt für die erste Aussage muss man

$$(*)_1 \qquad \varphi(x) \Rightarrow \varphi(x+1)$$

beweisen. Für die zweite Aussage hingegen muss man

$$(*)_2 \qquad \varphi_{\leq}(x) \Rightarrow \varphi_{\leq}(x+1)$$

beweisen, was zu

$$(*)_2' \qquad \varphi_{\leq}(x) \Rightarrow \varphi(x+1)$$

äquivalent ist. Da die Voraussetzung in $(*)_2'$ stärker als die in $(*)_1$ ist, ist $(*)_2'$ oft leichter beweisbar als $(*)_1$.

(3) Ein Beweis mittels Verlaufsinduktion lässt sich auch als Widerspruchsbeweis umsetzen: Um $(*)_2'$ zu zeigen, kann man die Annahme auf einen Widerspruch führen, dass $\varphi_{\leq}(x)$, d. h. $\forall y \leq x : \varphi(y)$, gilt, $\varphi(x+1)$ aber nicht. Mit anderen Worten geht man hier davon aus, dass $x+1$ minimal ist mit der Eigenschaft, φ *nicht* zu erfüllen, und leitet einen Widerspruch her. Somit können Induktionsbeweise auch wie folgt strukturiert sein: „Sei z minimal mit $\neg\varphi(z)$ … Also war z nicht minimal, Widerspruch."

Eine andere Möglichkeit, diese häufig verwendete Art des Induktionsbeweises herzuleiten, verwendet die (mit „gewöhnlicher" Induktion zu beweisende) Tatsache, dass jede nichtleere Teilmenge von $\mathbb{N}$ ein kleinstes[10] Element hat, siehe Satz A.1.1.2. Wäre daher $\forall x \in \mathbb{N} : \varphi(x)$ falsch, so hätte $\{x \in \mathbb{N} \mid \neg\varphi(x)\}$ ein kleinstes Element z, mit dem man dann arbeiten kann.

Als Anwendung dieser Ideen wollen wir die Assoziativität und Kommutativität von $+$ in der Peano-Arithmetik betrachten.

UE 11 ► Übungsaufgabe 1.1.5.4. Für die Addition auf $\mathbb{N}$ gilt **◄ UE 11**

(1) $\forall x \in \mathbb{N} : x + 0 = x$.

(2) $\forall x, y \in \mathbb{N} : (x + y) + 1 = x + (y + 1)$.

Zeigen Sie (nur unter Verwendung dieser Axiome, plus Induktion):

(a) $\forall x, y, z \in \mathbb{N} : (x + y) + z = x + (y + z)$.

(b) $\forall y \in \mathbb{N} : 0 + y = y$ (insbesondere gilt also $0 + 1 = 1$).

(c) $\forall x, y \in \mathbb{N} : x + y = y + x$.

Geben Sie bei jedem Induktionsbeweis an, von welcher Menge Sie zeigen, dass sie 0 enthält und unter Nachfolgern abgeschlossen ist.

[10] Die Unterscheidung zwischen „minimales" und „kleinstes" Element führen wir in Definition 2.1.2.3 ein. An dieser Stelle genügt der Hinweis, dass in der aktuellen Situation diese Begriffe zusammenfallen, weil $\mathbb{N}$ totalgeordnet ist.

1.1.6. Zifferndarstellung und Normalform

Inhalt in Kurzfassung: Für das Operieren mit konkreten Zahlen sind geeignete Formen der Repräsentation wie die übliche Zahlendarstellung zur Basis 10 unabdingbar. Es folgen dazu einige grundsätzliche Überlegungen.

Wegen der großen Bedeutung der Symbolsprache in der Mathematik ist die Unterscheidung zwischen einem mathematischen Objekt und seiner symbolischen Darstellung von großer Wichtigkeit. So bezeichnen etwa die Symbolketten *zwei*, *two*, 2 und $1 + 1$ dasselbe mathematische Objekt. Von Interesse sind daher Bezeichnungssysteme, die einer Bijektion zwischen der Menge der zu beschreibenden Objekte und ihren symbolischen Repräsentationen entsprechen. Man spricht dann von einer *Normalform*. In der Mathematik spielen überdies Operationen wie etwa Addition und Multiplikation eine so wichtige Rolle, dass man Normalformen bevorzugt, bei denen diese Operationen einfach handhabbare Entsprechungen auf symbolischer Ebene haben.
Der Begriff des Algorithmus und erst recht seine systematische Analyse kommen ohne eine sorgfältige Behandlung all dieser Aspekte nicht aus. Das ist zwar nicht Hauptthema der Algebra. Wir wollen aber an geeigneten Stellen auf damit verbundene Aspekte und auch Schwierigkeiten hinweisen.
Bei den natürlichen Zahlen liegen die Dinge denkbar einfach. Denn die übliche Zifferndarstellung in einem Positionssystem zu einer Basis $b \in \mathbb{N}$ mit $b \geq 2$ (im dekadischen Fall ist $b = 10$) erfüllt alle Desiderata in geradezu idealtypischer Weise. Beruhend auf der Darstellung $n = \sum_{i \geq 0} a_i b^i$ mit $a_i \in \{0, 1 \ldots, b-1\}$ wird jedem $n \in \mathbb{N}$ eine eindeutige[11] endliche Folge von Ziffern a_i zugeordnet, womit einfache Algorithmen für die Grundrechnungsarten formuliert werden können.

UE 12 ▶ Übungsaufgabe 1.1.6.1. (V,E) Führen Sie dies genauer aus, indem Sie folgende Aufgaben behandeln. Als Basis dürfen Sie der Einfachheit halber $b = 2$ setzen (binäre Darstellung). **◀ UE 12**

1. Beschreiben Sie präzise (etwa durch eine rekursive Definition) eine Bijektion, welche jeder natürlichen Zahl n ihre symbolische Darstellung zuordnet.
2. Beweisen Sie, dass es sich tatsächlich um eine Bijektion handelt. (Geben Sie Definitions- und Wertemenge explizit an.)
3. Beschreiben Sie den Algorithmus für die Bildung des Nachfolgers einer natürlichen Zahl. (Wie berechnet man aus der symbolischen Darstellung einer Zahl n die symbolische Darstellung von $\nu(n)$?)
4. Beschreiben Sie den Algorithmus für die Addition zweier natürlicher Zahlen.
5. Beweisen Sie, dass Ihr Additionsalgorithmus tatsächlich das Gewünschte leistet.

[11] Für die Eindeutigkeit muss man noch verlangen, dass die führende Ziffer ungleich 0 ist – ausgenommen bei der Darstellung der Zahl 0, wo man die Darstellung durch die Ziffer 0 der Darstellung durch eine leere Summe bzw. durch die leere Folge vorzieht.

6. Beschreiben Sie den Algorithmus für die Multiplikation zweier natürlicher Zahlen.

7. Beweisen Sie, dass Ihr Multiplikationsalgorithmus tatsächlich das Gewünschte leistet.

8. Beschreiben Sie einen Algorithmus, der von zwei natürlichen Zahlen die größere bestimmt.

Etwas komplizierter als bei der Arithmetik natürlicher Zahlen können die Dinge liegen, wenn aus verschiedenen a priori in Frage kommenden Darstellungen für ein und dasselbe Objekt erst eine als Normalform ausgezeichnet werden muss. Beispiele: Zu jedem Bruch ganzer Zahlen kann eindeutig eine gekürzte Darstellung mit positivem Nenner als Normalform ausgewählt werden (warum?). Jede gebrochen rationale Funktion besitzt Darstellungen als Bruch von Polynomen, aus denen mit Hilfe einer Normierung (z. B. gekürzte Darstellung und höchster Koeffizient im Nenner gleich 1, siehe Unterabschnitt 5.3.1) eine als Normalform ausgewählt werden kann. Die Partialbruchzerlegung (siehe Unterabschnitt 5.3.5) gibt Anlass zu einer anderen Normalform. In Booleschen Algebren gibt es konjunktive und disjunktive Normalformen etc. Es gibt auch Beispiele, in denen Normalformen nicht in algorithmisch befriedigender Weise ermittelt werden können (Schlagwort Wortproblem in Gruppen).

1.2. Zahlenbereichserweiterungen als Beispielgeber

In Abschnitt 1.1 über das System der natürlichen Zahlen war das Anliegen, sehr elementare mathematische Objekte nicht naiv, sondern begrifflich klar zu fassen. Nun wenden wir uns Systemen zu, die zwar immer noch wohlbekannt sind, deren Komplexität aber zunimmt. Dies geschieht im Zuge von Konstruktionen, die für die Algebra typisch und anhand der bekanntesten Beispiele besonders leicht zu fassen sind. Das sind vor allem die schrittweisen Zahlenbereichserweiterungen von $\mathbb{N}$ zu $\mathbb{Z}$ (1.2.1), von $\mathbb{Z}$ zu $\mathbb{Q}$ (1.2.2), von $\mathbb{Q}$ zu $\mathbb{R}$ (1.2.3) und von $\mathbb{R}$ zu $\mathbb{C}$ (1.2.4).
Aus didaktischen Gründen soll in diesem Abschnitt der Herausarbeitung des Exemplarischen der Vorzug gegeben werden gegenüber systematischer Vollständigkeit, die an späteren Stellen, vor allem in Kapitel 3, nachgeholt wird.

1.2.1. Die ganzen Zahlen

Inhalt in Kurzfassung: Die Konstruktion des Systems $\mathbb{Z}$ der ganzen Zahlen kann ausgehend von $\mathbb{N}$ mit rein mengentheoretischen Mitteln erfolgen. Diese Konstruktion ist typisch für die Denkweise in der Algebra und wird sich, bezogen auf die additive Struktur, später (z. B. in der Theorie der Halbgruppen) auch für Verallgemeinerungen eignen.

Die Kürzungsregel für die Addition natürlicher Zahlen (aus $b + c = b + d$ folgt $c = d$, siehe Übungsaufgabe 1.1.4.5(8), umformuliert mithilfe der Kommutativität) lässt sich in die Sprache der Gleichungen übersetzen: Eine Gleichung der Form $b + x = a$ besitzt in $\mathbb{N}$ höchstens eine Lösung für x, für die wir $x = a - b$ schreiben. Ist $a < b$, gibt es aber

keine Lösung in $\mathbb{N}$. Dies führt zur Erweiterung der Menge $\mathbb{N}$ zu einer Menge $\mathbb{Z}$, die also mindestens alle Elemente $a - b$ mit $a, b \in \mathbb{N}$ enthalten soll. (In diesem Fall erweist sich das auch als ausreichend.) Um auf mengentheoretisch festem Boden zu stehen, schreiben wir anstatt des noch in der Luft hängenden formalen Ausdrucks $a - b$ das geordnete Paar[12] (a, b) an[13]. Hier ergibt sich aber die Notwendigkeit, verschiedene Paare als ein und dasselbe Objekt zu definieren, weil beispielsweise $(2, 3)$ und $(3, 4)$ dieselbe ganze Zahl $2 - 3 = 3 - 4 = -1$ repräsentieren. Das allgemeine Problem behebt man, indem man eine geeignete Äquivalenzrelation $\sim$ auf der Menge $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N} = \{(a, b) : \ a, b \in \mathbb{N}\}$ definiert derart, dass $(a, b) \sim (c, d)$ genau dann gilt, wenn die Paare (a, b) und (c, d) im zu konstruierenden neuen Bereich demselben Objekt entsprechen sollen. In vorliegenden Fall soll das $a - b = c - d$ bedeuten, was sich zu $a + d = c + b$ umschreiben lässt, einer innerhalb $\mathbb{N}$ sinnvollen Beziehung, die wir als Definition für $(a, b) \sim (c, d)$ verwenden. Die Menge $\mathbb{Z}$ definieren wir daher als sogenannte Faktormenge

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/_\sim = \{[(a, b)]_\sim : \ a, b \in \mathbb{N}\},$$

d. h. als Menge aller Äquivalenzklassen

$$[(a, b)]_\sim := \{(c, d) \in \mathbb{N} \times \mathbb{N} : (c, d) \sim (a, b)\}$$

bezüglich $\sim$.
Für die Algebra ist diese Menge $\mathbb{Z}$ deshalb so interessant, weil auf ihr in natürlicher Weise wieder eine Addition definiert werden kann. Zunächst kann man für Paare definieren:

$$(a, b) + (c, d) := (a + c, b + d).$$

Weil also auf dem kartesischen Produkt $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ die neue Operation durch *komponentenweise* Festsetzung entsteht, spricht man von einem *direkten Produkt* von zwei Kopien des kommutativen additiven Monoids $\mathbb{N}$. Klarerweise übertragen sich Assoziativität, Kommutativität und ähnliche Gesetze von $\mathbb{N}$ auf $\mathbb{N} \times \mathbb{N}$.
Noch interessanter aber ist, dass diese Definition der Addition *verträglich* ist mit $\sim$, genauer: Sind $p_1, p_2, q_1, q_2 \in \mathbb{N}^2$ Paare mit $p_1 \sim p_2$ und $q_1 \sim q_2$, so folgt auch $p_1 + q_1 \sim p_2 + q_2$. Man sagt, dass $\sim$ eine *Kongruenzrelation* bezüglich $+$ ist.
Ganz ähnliche Situationen werden uns noch häufig begegenen, und wir werden später eine Definition in allgemeinerem Kontext geben. Vorläufig ist es wichtig, sich klar zu machen, dass das Ergebnis der Definition

$$[p]_\sim + [q]_\sim := [p + q]_\sim$$

gerade wegen der Verträglichkeit mit $+$ (also wegen der Kongruenzeigenschaft von $\sim$ bezüglich $+$) nicht von den speziellen Vertretern p und q der Äquivalenzklassen abhängt.

[12] Das geordnete Paar, bestehend aus zwei beliebig vorgegebenen Komponenten a, b, wird nach Kuratowski meist als Menge $(a, b) := \{\{a\}, \{a, b\}\}$ definiert. Damit sind die gewünschten Eigenschaften erfüllt, insbesondere ist $(a, b) = (c, d)$ dann und nur dann, wenn sowohl $a = c$ als auch $b = d$.

[13] A posteriori stellt sich das Paar (a, b) zwar tatsächlich als Differenz der natürlichen Zahlen a und b heraus (genauer: als ein Repräsentant dieser Differenz, die selbst eine Äquivalenzklasse ist); diese Differenz kann man aber erst bilden, wenn die Grundmenge feststeht.

Wie schon im Zusammenhang mit den entsprechenden Definitionen auf $\mathbb{N}$ spricht man von *Wohldefiniertheit* und sagt, die Operation auf der Menge der Äquivalenzklassen werde durch jene auf den Elementen *induziert*. Man kann den Übergang von einem Element $p = (a, b) \in \mathbb{N}^2$ zu seiner Äquivalenzklasse $[p]_\sim$ als eine Abbildung $\kappa : \mathbb{N}^2 \to \mathbb{Z}$, die sogenannte *kanonische Abbildung*, auffassen, die wegen Wohldefiniertheit und Verträglichkeit mit + die sogenannte *Homomorphiebedingung*

$$\kappa(p + q) = \kappa(p) + \kappa(q)$$

erfüllt. Deshalb heißt κ auch der *kanonische Homomorphismus*. Beim Übergang von Paaren zu Äquivalenzklassen bleiben überdies Assoziativität, Kommutativität etc. erhalten. (Siehe auch die Fußnote auf Seite 98.)

Ein weiterer entscheidender Punkt bei der Zahlenbereichserweiterung von $\mathbb{N}$ auf $\mathbb{Z}$ liegt darin, dass $\mathbb{N}$ mit einer Teilmenge von $\mathbb{Z}$ identifiziert[14] werden kann. Damit ist gemeint, dass sich die Zuordnung $\iota\colon \mathbb{N} \to \mathbb{Z}$, $n \mapsto [(n, 0)]_\sim$ als *isomorphe Einbettung* (genannt die kanonische Einbettung) erweist, d. h. als injektiver Homomorphismus: Unmittelbar sieht man $\iota(m + n) = \iota(m) + \iota(n)$. Außerdem ist ι injektiv, weil aus $[(m, 0)]_\sim = \iota(m) = \iota(n) = [(n, 0)]_\sim$ die Äquivalenz $(m, 0) \sim (n, 0)$, also $m = m + 0 = n + 0 = n$ folgt.

Diese Konstruktion liefert allerdings nicht die gewünschte Beziehung $\mathbb{N} \subseteq \mathbb{Z}$; um diese zu garantieren, modifizieren wir die eben konstruierte Menge zu einer Menge $\mathbb{Z}'$, indem wir sämtliche Elemente in $\mathbb{Z}$, die die Form $\iota(n) = [(n, 0)]_\sim$ haben, durch ihre ι-Urbilder n ersetzen. Schließlich vergessen wir die ursprünglich konstruierte Menge $\mathbb{Z}$ und benennen die neue Menge von $\mathbb{Z}'$ auf $\mathbb{Z}$ um.

So wie die bisherigen Konstruktionsschritte wird uns auch dieses sogenannte *Prinzip der isomorphen Einbettung* noch oft begegnen.

Was wir in $\mathbb{N}$ vermisst und weshalb wir die Erweiterung zu $\mathbb{Z}$ überhaupt durchgeführt haben, nämlich die uneingeschränkte Ausführbarkeit der Subtraktion, funktioniert tatsächlich in ganz $\mathbb{Z}$: Zunächst ist $\iota(0) = [(0, 0)]_\sim$ neutrales Element bezüglich + in $\mathbb{Z}$. Für jedes Paar $(m, n) \in \mathbb{N}^2$ spielt deshalb das Paar (n, m) wegen[15]

$$(m, n) + (n, m) = (n, m) + (m, n) = (m + n, n + m) \sim (0, 0) = \iota(0)$$

in $\mathbb{Z}$ die Rolle des inversen Elementes, also $-[(m, n)]_\sim = [(n, m)]_\sim$. Deshalb haben beliebige Gleichungen der Form $k + x = l$ in $\mathbb{Z}$ die Lösung $x = l - k = l + (-k)$. Kurz formuliert: $\mathbb{Z}$ ist eine Gruppe.

Schließlich beachte man, dass wir für unsere Zwecke auf kein Element von $\mathbb{Z}$ verzichten können, also dass $\mathbb{Z}$ in der obigen Konstruktion so sparsam wie möglich gewählt wurde. Das kommt zum Ausdruck in der dritten Aussage des folgenden Satzes.

Satz 1.2.1.1.

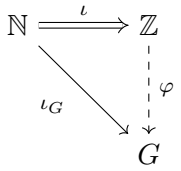
[14] Wenn wir sagen, dass wir X und Y „identifizieren“, dann bedeutet dies Folgendes: X und Y haben gewisse gemeinsame Eigenschaften; solange es nur um diese Eigenschaften geht, ist es egal, ob wir von X oder von Y sprechen. Wir lassen es sogar zu, dass wir von X sprechen, aus formalen Gründen aber tatsächlich Y meinen.

[15] Man beachte die Verwendung der Kommutativität $m + n = n + m$.

(1) *$\mathbb{Z}$ ist bezüglich der Addition eine (*abelsche*, d. h. kommutative) Gruppe (mit obigen neutralen und inversen Elementen).*

(2) *Die oben beschriebene Abbildung $\iota\colon \mathbb{N} \to \mathbb{Z}$ ist eine isomorphe Einbettung der additiven Halbgruppe $\mathbb{N}$.*

(3) *Ist G irgendeine Gruppe und $\iota_G\colon \mathbb{N} \to G$ eine isomorphe Einbettung der additiven Halbgruppe $\mathbb{N}$, so gibt es eine isomorphe Einbettung $\varphi\colon \mathbb{Z} \to G$ mit $\iota_G = \varphi \circ \iota$, die sogar eindeutig bestimmt ist.*



(Zur Bedeutung der verschieden gestalteten Pfeile in diesem Diagramm sei auf die einführenden „Notationellen Bemerkungen“ verwiesen.)

UE 13 ► **Übungsaufgabe 1.2.1.2.** (V,W) Beweisen Sie Satz 1.2.1.1, indem Sie die folgenden noch ausständigen Schritte vollständig durchführen. Es gelten die Notationen des gesamten Unterabschnitts. ◄ **UE 13**

1. Die Relation $\sim$ ist eine Äquivalenzrelation auf $\mathbb{N}^2$. (Wo geht dabei die Kürzbarkeit der Addition in $\mathbb{N}$ ein?)

2. Es handelt sich bei $\sim$ sogar um eine Kongruenzrelation.

3. Geben Sie die Abbildung φ an, prüfen Sie die behaupteten Eigenschaften nach und begründen Sie die Eindeutigkeit.

Die Eigenschaften in Satz 1.2.1.1 zeichnen die ganzen Zahlen als (additive) Differenzengruppe von $\mathbb{N}$ aus. In Unterabschnitt 3.1.4 werden wir diese Konstruktion statt auf $\mathbb{N}$ auf beliebige *kommutative kürzbare Monoide* anwenden.
Wir kehren zurück zum System der ganzen Zahlen $\mathbb{Z}$. Bisher haben wir uns nur um die additive Struktur gekümmert. Doch die Multiplikation auf $\mathbb{N}$ lässt sich ebenfalls fortsetzen. Denn auch die Definition

$$[(a,b)]_\sim \cdot [(c,d)]_\sim := [(ac+bd, ad+bc)]_\sim$$

erweist sich als unabhängig von den Vertretern der Klassen, d. h., $\sim$ ist auch bezüglich $\cdot$ eine Kongruenzrelation. Daraus folgt:

Proposition 1.2.1.3. *$\mathbb{Z}$ ist bezüglich der Multiplikation ein kommutatives Monoid mit neutralem Element $\iota(1)$.*

UE 14 ▶ **Übungsaufgabe 1.2.1.4.** (V) Beweisen Sie Proposition 1.2.1.3 in allen Einzelheiten. (Zeigen Sie insbesondere, dass $\sim$ eine Kongruenzrelation ist.) ◀ **UE 14**

Nun zur Ordnungsstruktur auf $\mathbb{Z}$: Sei $\iota\colon \mathbb{N} \to \mathbb{Z}$ die kanonische Einbettung. Wir nennen ein Element $\iota(n) \in \mathbb{Z}$ positiv, falls $n \in \mathbb{N} \setminus \{0\}$ (wohldefiniert wegen der Injektivität von ι), und negativ, falls $-\iota(n)$ positiv ist. Es bezeichne $\mathbb{Z}^+$ die Menge der positiven, $\mathbb{Z}^-$ die der negativen Elemente. Dann bilden die drei Mengen $\mathbb{Z}^+, \mathbb{Z}^-, \{0\}$ eine disjunkte Zerlegung von $\mathbb{Z}$.

UE 15 ▶ **Übungsaufgabe 1.2.1.5.** (F) Beweisen Sie, dass es sich tatsächlich um eine Partition der Menge $\mathbb{Z}$ handelt. ◀ **UE 15**

Außerdem setzen wir $a \leq b$, sofern $b - a$ positiv oder $a = b$ ist. Damit gilt:

Satz 1.2.1.6. *Die bisher auf $\mathbb{Z}$ definierten Strukturen haben folgende weitere Eigenschaften:*

(1) $\mathbb{Z}$ zusammen mit Addition und Multiplikation ist ein Integritätsbereich*, das ist definitionsgemäß ein nullteilerfreier kommutativer Ring mit Einselement. (Ein Ring heißt* nullteilerfrei*, wenn aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt.)*

(2) Zieht man auch noch die Ordungsrelation heran, erhält man sogar einen angeordneten Ring. Damit ist gemeint, dass eine Totalordnung $\leq$ auf $\mathbb{Z}$ vorliegt, die folgende Monotoniegesetze erfüllt: Für $a, b, c \in \mathbb{Z}$ folgt aus $a \leq b$ stets $a + c \leq b + c$ und, sofern zusätzlich $c \geq 0$ gilt, $ac \leq bc$.

UE 16 ▶ **Übungsaufgabe 1.2.1.7.** (V) Beweisen Sie Satz 1.2.1.6. Verwenden Sie hier nur die als bekannt vorausgesetzten Rechenregeln in $\mathbb{N}$; die Rechenregeln für $\mathbb{Z}$ dürfen Sie nicht voraussetzen. ◀ **UE 16**

UE 17 ▶ **Übungsaufgabe 1.2.1.8.** (B) ◀ **UE 17**

(1) Finden Sie alle Halbgruppenhomomorphismen $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, d. h. alle Abbildungen $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x + y) = f(x) + f(y)$ für alle $x, y \in \mathbb{Z}$.

(2) Finden Sie alle Gruppenhomomorphismen $f : (\mathbb{Z}, +, 0, -) \to (\mathbb{Z}, +, 0, -)$, d. h. alle Abbildungen $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x + y) = f(x) + f(y)$ für alle $x, y \in \mathbb{Z}$ und $f(0) = 0$ und $f(-x) = -f(x)$ für alle $x \in \mathbb{Z}$.

(3) Finden Sie alle Ring-Homomorphismen $f : (\mathbb{Z}, +, 0, -, \cdot) \to (\mathbb{Z}, +, 0, -, \cdot)$, d. h. alle Abbildungen $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x + y) = f(x) + f(y)$ für alle $x, y \in \mathbb{Z}$ und $f(0) = 0$ und $f(-x) = -f(x)$ für alle $x \in \mathbb{Z}$ und $f(x \cdot y) = f(x) \cdot f(y)$ für alle $x, y \in \mathbb{Z}$.

(4) Finden Sie alle Ring_1-Homomorphismen $f : (\mathbb{Z}, +, 0, -, \cdot, 1) \to (\mathbb{Z}, +, 0, -, \cdot, 1)$, d. h. alle Abbildungen $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x + y) = f(x) + f(y)$ für alle $x, y \in \mathbb{Z}$ und $f(0) = 0$ und $f(-x) = -f(x)$ für alle $x \in \mathbb{Z}$ und $f(x \cdot y) = f(x) \cdot f(y)$ für alle $x, y \in \mathbb{Z}$ und $f(1) = 1$.

Hinweis: Die Reihenfolge ist so gewählt, dass die erste zu beschreibende Mengen von Homomorphismen die nachfolgenden (nicht notwendigerweise strikt) umfasst etc. Wenn es Ihnen sympathischer ist, können Sie auch in anderer Reihenfolge vorgehen.

1.2.2. Die rationalen Zahlen

Inhalt in Kurzfassung: Die Konstruktion des Systems $\mathbb{Q}$ der rationalen Zahlen aus $\mathbb{Z}$ folgt jener von $\mathbb{Z}$ aus $\mathbb{N}$ aus dem vorangegangenen Abschnitt.

Der Übergang von $\mathbb{Z}$, dem System der ganzen Zahlen, zu $\mathbb{Q}$, dem der rationalen, erfolgt in weitgehender Analogie zu jenem von $\mathbb{N}$ zu $\mathbb{Z}$. Wir können uns entsprechend kurz fassen. Wegen der multiplikativen Kürzungsregel haben Gleichungen der Gestalt $bx = a$ für $b \neq 0$ in $\mathbb{Z}$ höchstens eine Lösung. Eine solche existiert genau dann, wenn b ein Teiler von a ist. Dies motiviert einerseits zur Untersuchung von Teilbarkeitseigenschaften in $\mathbb{Z}$ und verwandten Strukturen (siehe Kapitel 5), andererseits zur Erweiterung des Zahlenbereichs um Lösungen, die wir als Brüche $\frac{a}{b}$ anschreiben, zu einem Körper.
Eine ganz analoge Konstruktion wie in 1.2.1 auf $\mathbb{N} \times \mathbb{N}$ können wir auf die multiplikative Halbgruppe $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ anwenden und erhalten die Menge $\mathbb{Q}$ aller Äquivalenzklassen von Paaren (a, b) mit $b \neq 0$. Wie gewohnt schreiben wir die Elemente von $\mathbb{Q}$ als Brüche an. Die Schreibweise $\frac{a}{b}$ steht also für die Äquivalenzklasse des Paares (a, b). In Übereinstimmung mit den Rechenregeln für das Erweitern bzw. Kürzen von Brüchen ist $\frac{a}{b} = \frac{c}{d}$ genau dann, wenn $ad = cb$ in $\mathbb{Z}$ gilt. Neutrales Element ist $1 := [(1, 1)]_\sim$. Doch auch die additive Struktur von $\mathbb{Z}$ kann in bekannter Weise durch $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ auf $\mathbb{Q}$ fortgesetzt werden. Wir fassen zusammen:

Satz 1.2.2.1. *Auf der Menge $M := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ seien die Operationen $(a, b) + (c, d) := (ad + cb, bd)$ und $(a, b) \cdot (c, d) := (ac, bd)$ definiert. Außerdem definieren wir $(a, b) \sim (c, d)$ durch $ad = cb$ und setzen $\mathbb{Q} := M/\sim$ sowie $0 := [(0, 1)]_\sim$ und $1 := [(1, 1)]_\sim$. Dann gilt:*

(1) *$(M, \cdot, (1, 1))$ ist ein kommutatives Monoid.*

(2) *Die Relation $\sim$ ist eine Kongruenzrelation auf M bezüglich $\cdot$. Also ist die Multiplikation $[(a, b)]_\sim \cdot [(c, d)]_\sim := [(ac, bd)]_\sim$ auf $\mathbb{Q}$ wohldefiniert.*

(3) *Die Menge $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ bildet bezüglich der induzierten Operation $\cdot$ (siehe (2)) und dem neutralen Element 1 nicht nur ein kommutatives Monoid, sondern (mit den Inversen $[(a, b)]_\sim^{-1} := [(b, a)]_\sim$) sogar eine (abelsche) Gruppe.*

(Dies ist weitgehend parallel zur Situation bei der Erweiterung von $\mathbb{N}$ zu $\mathbb{Z}$.)

(4) *$(M, +, (0, 1))$ ist ein kommutatives Monoid.*

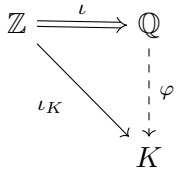
(5) *Die Relation $\sim$ ist eine Kongruenzrelation auf M auch bezüglich $+$. Also ist die Addition $[(a, b)]_\sim + [(c, d)]_\sim := [(ad + cb, bd)]_\sim$ auf $\mathbb{Q}$ wohldefiniert.*

(6) *Die Menge $\mathbb{Q}$ bildet bezüglich der induzierten Operation $+$ (siehe (5)) und dem neutralen Element 0 nicht nur ein kommutatives Monoid, sondern (mit den Inversen $-[(a, b)]_\sim := [(-a, b)]_\sim$) sogar eine (abelsche) Gruppe.*

(7) *$(\mathbb{Q}, +, 0, -, \cdot, 1)$ ist sogar ein Körper.*

(8) *Die Abbildung* $\iota\colon \mathbb{Z} \to \mathbb{Q}$, $k \mapsto [(k,1)]_\sim$ *ist eine isomorphe Einbettung des Integritätsbereichs* $\mathbb{Z}$ *in* $\mathbb{Q}$.

(9) *Jeder Körper* K*, der vermittels einer Einbettung* $\iota_K\colon \mathbb{Z} \to K$ *eine isomorphe Kopie des Integritätsbereichs* $\mathbb{Z}$ *enthält, enthält auch eine isomorphe Kopie des Körpers* $\mathbb{Q}$ *vermittels einer durch die Bedingung* $\iota_K = \varphi \circ \iota$ *eindeutig bestimmten Einbettung* $\varphi\colon \mathbb{Q} \to K$*. (In diesem Sinne ist* $\mathbb{Q}$ *der kleinste Körper, der* $\mathbb{Z}$ *enthält.)*



(10) *Die Ordungsrelation auf* $\mathbb{Z}$ *kann in eindeutiger Weise so auf* $\mathbb{Q}$ *fortgesetzt werden, dass gilt:*

1. *Die Ungleichung* $[(a,b)]_\sim > 0$ *gilt genau dann, wenn* $ab > 0$ *in* $\mathbb{Z}$*.*
2. *In* $(\mathbb{Q}, +, \cdot, \leq)$ *gelten die* Monotoniegesetze*: Aus* $q_1 \leq q_2$ *folgt stets* $q_1 + q_3 \leq q_2 + q_3$*, im Falle* $q_3 > 0$ *auch* $q_1 q_3 \leq q_2 q_3$*.*

UE 18 ► **Übungsaufgabe 1.2.2.2.** (V,W) Beweisen Sie Satz 1.2.2.1. Verwenden Sie dabei nur die als bekannt vorausgesetzten Rechenregeln in $\mathbb{Z}$; die Rechenregeln für $\mathbb{Q}$ dürfen Sie nicht voraussetzen. ◄ **UE 18**

Die letzte Aussage in Satz 1.2.2.1 weist $\mathbb{Q}$ als einen *angeordneten Körper* aus, die anderen als *Quotientenkörper* von $\mathbb{Z}$. Auf die allgemeine Konstruktion des Quotientenkörpers eines Integritätsbereichs (und noch allgemeiner: eines Bruchrings) werden wir in Unterabschnitt 3.4.5 zurückkommen.

1.2.3. Die reellen Zahlen

Inhalt in Kurzfassung: Für die dritte große Zahlenbereichserweiterung, nämlich von $\mathbb{Q}$ zu $\mathbb{R}$, sind mehrere Zugänge möglich. In jedem Fall sind aber neue Ideen erforderlich. Hier beschreiten wir den Weg mittels Cauchyfolgen. (Eine alternative Konstruktion mittels Dedekindscher Schnitte wird in Unterabschnitt 3.5.3 zur Sprache kommen.) Trotz der nun stärker analytischen Aura treten im Zusammenhang mit den Cauchyfolgen aber wieder Aspekte von großem algebraischen Interesse auf (Idealeigenschaft).

Der Übergang von $\mathbb{Q}$ zu $\mathbb{R}$ unterscheidet sich stark von den bisherigen Zahlenbereichserweiterungen. Der Grund liegt darin, dass man sich diesmal keine algebraische Eigenschaft von der Erweiterung wünscht, sondern eine ordnungstheoretische bzw. eine topologisch-analytische. Das wird oft verschleiert, wenn an dieser Stelle der berühmte Beweis für die Irrationalität von $\sqrt{2}$ geführt wird, weil dadurch der Eindruck erweckt wird, dass es nur um die Ergänzung von Wurzeln gehe. Doch zeigt die imaginäre Wurzel $\sqrt{-1}$, dass es

nicht primär darum geht. Der Unterschied besteht darin, dass $\sqrt{2}$ gewissermaßen einer Lücke in $\mathbb{Q}$ entspricht, und zwar irgendwo zwischen $\frac{14}{10}$ und $\frac{15}{10}$. Das ist bei $\sqrt{-1}$ nicht der Fall. Deshalb lohnt eine Übungsaufgabe, in der einige Lücken in $\mathbb{Q}$ auszumachen sind, auch solche, die keinen Wurzeln entsprechen, sondern anders motiviert sind.

UE 19 ► Übungsaufgabe 1.2.3.1. (B,E) In dieser Aufgabe dürfen Sie wichtige Eigenschaften natürlicher Zahlen ohne Beweis verwenden, sofern Sie diese sorgfältig formulieren. **◄ UE 19**

1. Zeigen Sie, dass es kein $\alpha \in \mathbb{Q}$ mit $\alpha^2 = 2$ gibt.
2. Wie in Teil 1 mit $\alpha^2 = 3$ statt $\alpha^2 = 2$.
3. Für welche $m, n \in \mathbb{N}$ gibt es ein $\alpha \in \mathbb{Q}$ mit $\alpha^m = n$? (Begründung)
4. Zeigen Sie, dass die Eulersche Zahl $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ irrational ist. (Anleitung: Jede Partialsumme s_n ist eine rationale Zahl der Form $\frac{p_n}{n!}$ mit $p_n \in \mathbb{N}$. Wäre $e = \frac{p}{q}$ rational mit $p, q \in \mathbb{N}$, so ließe sich die Differenz $d := e - s_q > 0$ auf gemeinsamen Nenner $q!$ bringen, erfüllte also $d \geq \frac{1}{q!}$. Daraus lässt sich ein Widerspruch ableiten. In dieser Aufgabe dürfen Sie die Theorie unendlicher Reihen aus der Analysis verwenden, insbesondere die Formel für die geometrische Reihe.)
5. Die Kreiszahl π ist definiert als das Doppelte der kleinsten positiven Nullstelle des Cosinusfunktion $\cos x := \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}$. Was aus der reellen Analysis fließt bei der Wohldefiniertheit von π ein?
6. Zeigen Sie $\pi \notin \mathbb{Q}$. (Sehr schwierig.)

Die Vertiefung der Theorie der reellen Zahlen im Sinne der reellen Analysis ist natürlich dort besser aufgehoben. Dennoch gibt es auch aus algebraischer Sicht manch Interessantes, das wir aus der Analysis rekapitulieren oder uns in einem neuen Licht vor Augen führen wollen. Auf die stark ordnungstheoretisch orientierte Konstruktion von $\mathbb{R}$ mittels Dedekindscher Schnitte werden wir noch an geeigneter Stelle (Unterabschnitt 3.5.3) zu sprechen kommen. Um typisch algebraische Konzepte exemplarisch vorzustellen, hat die folgende alternative Konstruktion von $\mathbb{R}$, die auf Cantor zurückgeht, manche Vorzüge: Wir betrachten die Menge CF aller Cauchyfolgen in $\mathbb{Q}$. Zur Erinnerung: Eine Folge $x = (x_n)_{n\in\mathbb{N}}$ (zunächst) rationaler Zahlen x_n heißt *Cauchyfolge*, wenn es zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ gibt derart, dass $|x_{n_1} - x_{n_2}| < \varepsilon$ für alle $n_1, n_2 \geq n_0$ gilt. Auf CF sind in natürlicher Weise Addition und Multiplikation definiert, nämlich durch

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} := (x_n + y_n)_{n\in\mathbb{N}}$$

und

$$(x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} := (x_n \cdot y_n)_{n\in\mathbb{N}}.$$

UE 20 ► Übungsaufgabe 1.2.3.2. (V) Beweisen Sie, dass $(x_n + y_n)_{n\in\mathbb{N}}$ und $(x_n \cdot y_n)_{n\in\mathbb{N}}$ wieder Cauchyfolgen sind. **◄ UE 20**

Diese Definitionen sind wieder Beispiele eines direkten Produktes, hier nicht nur von zwei Strukturen, sondern von abzählbar vielen Kopien des Ringes $\mathbb{Q}$ der rationalen Zahlen, für jedes $n \in \mathbb{N}$ eine Kopie.
Klarerweise erfüllen die Operationen + und · auf CF alle Gesetze eines kommutativen Ringes, wobei die konstanten Folgen mit Wert 0 bzw. 1 Null- bzw. Einselement sind (für die wir wieder 0 und 1 schreiben). Allerdings können verschiedene rationale Folgen gegen dieselbe reelle Zahl konvergieren. Also identifizieren wir gemäß einer geeigneten Äquivalenzrelation $\sim$, nämlich:

$$x = (x_n)_{n\in\mathbb{N}} \quad \sim \quad y = (y_n)_{n\in\mathbb{N}}$$

genau dann, wenn $(x_n - y_n)_{n\in\mathbb{N}}$ eine Nullfolge ist. Nützlich ist auch eine Formulierung mit Hilfe der Menge

$$I := \{(z_n)_{n\in\mathbb{N}} \mid z_n \in \mathbb{Q},\ \forall \varepsilon > 0\, \exists n_0 \in \mathbb{N}\, \forall n \geq n_0 :\ |z_n| < \varepsilon\}$$

aller rationalen Nullfolgen[16]. Dann gilt $x = (x_n)_{n\in\mathbb{N}} \sim y = (y_n)_{n\in\mathbb{N}}$ genau dann, wenn $(x_n - y_n)_{n\in\mathbb{N}} \in I$.
Die Menge I aller Nullfolgen in $\mathbb{Q}$ spielt nun eine zentrale Rolle. Weil $\sim$ vermittels I definiert wurde, schreiben wir für die Menge CF $/_\sim$ aller $\sim$-Äquivalenzklassen auch CF $/I$.
Als entscheidend dafür, dass die nun folgende Konstruktion möglich ist, erweist sich, dass I ein sogenanntes *Ideal* in CF ist. Das ist allgemein eine nichtleere Teilmenge $I \subseteq R$ eines Ringes R mit folgenden beiden Eigenschaften:

1. Aus $a, b \in I$ folgt $a + b \in I$ und aus $a \in I$ folgt $-a \in I$. (I ist also eine additive Untergruppe von R.)

2. Aus $a \in I$ folgt $ab, ba \in I$ für beliebige $b \in R$. (Idealeigenschaft)

UE 21 ► **Übungsaufgabe 1.2.3.3.** (V) Prüfen Sie nach: Die Menge I aller Nullfolgen in $\mathbb{Q}$ bildet ein Ideal im Ring $R :=$ CF. ◄ **UE 21**

Von sehr allgemeiner Bedeutung ist der folgende Zusammenhang:

Proposition 1.2.3.4. *Sei R ein Ring.*

(1) *Sei $I \subseteq R$ ein Ideal und die Relation $\sim_I$ auf R definiert durch: $a \sim_I b$ genau dann, wenn $a - b \in I$. Dann ist $\sim_I$ eine Kongruenzrelation auf R, d. h., aus $a \sim b$ und $c \sim d$ folgt $a + c \sim b + d$, $ac \sim bd$ und $-a \sim -b$.*

(2) *Ist umgekehrt $\sim$ eine Kongruenzrelation auf einem Ring R, so bildet die Nullklasse $I_\sim := [0]_\sim$ ein Ideal.*

(3) *Die Konstruktionen aus 1. und 2. sind invers zueinander, d. h. $I_{\sim_I} = I$ und $\sim_{I_\sim} = \sim$.*

[16] Die Variable $\varepsilon > 0$ wird meist für reelle Größen verwendet, die an dieser Stelle allerdings noch nicht zur Verfügung stehen. Doch auch wenn man nur rationale ε zulässt – und so ist die Formel hier zu verstehen –, ändert das nichts an der Menge I.

UE 22 ► Übungsaufgabe 1.2.3.5. (W) Beweisen Sie Proposition 1.2.3.4. **◄ UE 22**

Deshalb sind auf $\mathbb{R} := \mathrm{CF}/I$ die Operationen

$$[(x_n)_{n\in\mathbb{N}}]_\sim + [(y_n)_{n\in\mathbb{N}}]_\sim := [(x_n + y_n)_{n\in\mathbb{N}}]_\sim, \quad -[(x_n)_{n\in\mathbb{N}}]_\sim := [(-x_n)_{n\in\mathbb{N}}]_\sim$$

und

$$[(x_n)_{n\in\mathbb{N}}]_\sim \cdot [(y_n)_{n\in\mathbb{N}}]_\sim := [(x_n y_n)_{n\in\mathbb{N}}]_\sim$$

wohldefiniert. Sie machen $\mathbb{R}$ zu einem Ring mit Nullelement $0 := [(0)_{n\in\mathbb{N}}]_\sim$ und Einselement $1 := [(1)_{n\in\mathbb{N}}]_\sim$. (Dies folgt im Wesentlichen unmittelbar aus dem Bisherigen.) Folglich besitzt $\mathbb{R}$ eine natürliche Ringstruktur. Auch die Ordungsstruktur kann in natürlicher Weise definiert werden. Zwar lässt sie sich als Totalordnung nicht direkt von $\mathbb{Q}$ auf das direkte Produkt fortsetzen, sehr wohl aber auf die Menge der $\sim$-Äquivalenzklassen:

$$x = [(x_n)_{n\in\mathbb{N}}]_\sim \leq y = [(y_n)_{n\in\mathbb{N}}]_\sim :\Leftrightarrow x \sim y \text{ oder } \exists n_0 \in \mathbb{N}\, \forall n \geq n_0 : x_n < y_n.$$

UE 23 ► Übungsaufgabe 1.2.3.6. (V) Zeigen Sie, dass die Relation $\leq$ auf $\mathbb{R}$ wohldefiniert und eine Totalordnung ist. **◄ UE 23**

Auf diese Weise wird $\mathbb{R}$ ein angeordneter Körper, wie auch schon $\mathbb{Q}$. Darüber hinaus – und das ist die für die Analysis entscheidende Eigenschaft – ist $\mathbb{R}$ als solcher sogar *vollständig*. Das bedeutet explizit: Ist $T \subseteq \mathbb{R}$ nicht leer und nach oben beschränkt (es gibt eine obere Schranke von T, das ist ein $s \in \mathbb{R}$ mit $t \leq s$ für alle $t \in T$), so hat T sogar ein sogenanntes *Supremum* (eine kleinste obere Schranke) $s_0 = \sup T$ in $\mathbb{R}$ (nicht notwendig in T selbst), das also $s_0 \leq s$ für alle oberen Schranken s von T erfüllt. Wir können also sehr kurz zusammenfassen:

Satz 1.2.3.7. $\mathbb{R}$ *mit den Operationen und der Relation aus Aufgabe 1.2.3.6 ist ein vollständig angeordneter Körper.*

UE 24 ► Übungsaufgabe 1.2.3.8. (V) Beweisen Sie Satz 1.2.3.7. Gehen Sie dabei wie folgt vor: **◄ UE 24**

1. Listen Sie (möglichst übersichtlich gegliedert) alle Eigenschaften auf, die im Begriff des vollständig angeordneten Körper enthalten sind.
2. Markieren Sie, welche dieser Eigenschaften aus dem bisher Gesagten bereits unmittelbar abzulesen sind.
3. Formulieren Sie, was für die verbleibenden Eigenschaften zu zeigen ist.
4. Beweisen Sie die Vollständigkeit von $\mathbb{R}$.

In Unterabschnitt 3.5.3 werden wir nochmals auf die reellen Zahlen zu sprechen kommen, indem wir eine alternative Konstruktion zur Vervollständigung von Halbordnungen, nämlich mittels Dedekindscher Schnitte, auf $\mathbb{Q}$ anwenden werden. Die folgenden Übungsaufgabe weist bereits in diese Richtung. Außerdem werden wir in Unterabschnitt 3.5.3 einen Blick auf die Struktur beliebiger (archimedisch) angeordneter Körper werfen und einen Eindeutigkeitssatz für $\mathbb{R}$ beweisen.

UE 25 ► **Übungsaufgabe 1.2.3.9.** (A) (In dieser Aufgabe gehen wir davon aus, dass wir die rationalen Zahlen gut verstehen, ebenso wie die Grundrechnungsarten und die Ordnung auf den rationalen Zahlen. Fakten über die reellen Zahlen dürfen wir noch nicht ohne Beweis verwenden.) ◄ **UE 25**

Wir betrachten die oben definierte Äquivalenzrelation $\sim$ auf der Menge CF aller Cauchyfolgen in $\mathbb{Q}$. Für zwei verschiedene Äquivalenzklassen $[x]_\sim$, $[y]_\sim$ definieren wir

$$[x]_\sim < [y]_\sim \qquad \Leftrightarrow \qquad \exists n_0 \, \forall n > n_0 \; (x_n < y_n).$$

Es sei D die Menge aller $A \subseteq \mathbb{Q}$ mit folgenden Eigenschaften:
$A \neq \emptyset$, $A \neq \mathbb{Q}$, $\forall a \in A \, \forall q \in \mathbb{Q} : (q < a \Rightarrow q \in A)$, und A hat kein größtes Element.
Geben Sie eine (natürliche) Bijektion $f : \mathrm{CF}/\!\sim \to D$ an, die $[x]_\sim < [y]_\sim \Leftrightarrow f([x]_\sim) \subsetneq f([y]_\sim)$ erfüllt. In Ihrer Definition dürfen aber nur rationale Zahlen (Folgen/Mengen von rationalen Zahlen etc.) vorkommen, nicht beliebige reelle Zahlen. Die Definition $f([x]_\sim) := \{q \in \mathbb{Q} : q < \lim_{n\to\infty} x_n\}$ ist also nicht erlaubt.
Zeigen Sie, dass D bzw. CF $/\!\sim$ durch $\subseteq$ bzw. durch die oben definierte Relation $\leq$ linear geordnet wird. (Hinweis zur Notation: Wie generell im Zusammenhang mit Halbordnungen steht $x \leq y$ für $x < y$ oder $x = y$ und $x < y$ für $x \leq y$ und $x \neq y$.)

1.2.4. Die komplexen Zahlen

Inhalt in Kurzfassung: Komplexe Zahlen können in vertrauter Weise als Paare mit Real- und Imaginärteil als Komponenten aufgefasst werden. Sie bilden einen Körper $\mathbb{C}$, für den ein Eindeutigkeitssatz gilt, außerdem der Fundamentalsatz der Algebra. Der hier skizzierte Beweis verlangt keine höheren Hilfsmittel, lediglich den Satz vom Maximum aus der reellen Analysis. Abschließend werden auch noch kurz die Hamiltonschen Quaternionen besprochen.

Bekanntlich entsteht das System $\mathbb{C}$ der komplexen Zahlen aus dem Bedürfnis, auch Gleichungen wie (als einfachsten Fall) $p(x) = x^2 + 1 = 0$, die keine reellen Lösungen besitzen, zu lösen. Ist K irgendein Körper, der den Körper $\mathbb{R}$ enthält und $i \in K$ (imaginäre Einheit) so eine Lösung (d. h., es gelte $i^2 + 1 = 0$), so ist auch $-i$ eine Lösung. Offenbar können wir schreiben $p(x) = x^2 + 1 = (x - i)(x + i)$, woraus ersichtlich ist, dass i und $-i$ die einzigen Lösungen von $p(x) = 0$ sind. Klarerweise muss K als Körper auch alle Elemente der Form $a + ib$ mit $a, b \in \mathbb{R}$ enthalten. Wir fassen so ein Element als Paar

(a, b) auf und entsprechend den Körper $\mathbb{C}$ der komplexen Zahlen[17] in üblicher Weise als Menge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ mit den Operationen $(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2)$ sowie $-(a, b) := (-a, -b)$ (direktes Produkt der additiven Gruppe $\mathbb{R}$ mit sich selbst) und $(a_1, b_1) \cdot (a_2, b_2) := (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$.

UE 26 ► Übungsaufgabe 1.2.4.1. (W) Zeigen Sie, dass $\mathbb{C}$ mit diesen Operationen wirklich einen Körper und dass die Menge $\{(a, 0) : a \in \mathbb{R}\}$ einen zu $\mathbb{R}$ isomorphen Unterkörper bildet. **◄ UE 26**

Wir werden in Zukunft die Menge $\{(a, 0) : a \in \mathbb{R}\}$ vermittels des Prinzips der isomorphen Einbettung mit $\mathbb{R}$ identifizieren, also die Menge $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auffassen. Weiters definieren wir $i := (0, 1)$. Für dieses Element gilt $i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1$. Jedes Element $z \in \mathbb{C}$ lässt sich somit tatsächlich eindeutig in der Form $z = (a, b) = (a, 0) + (0, b) = (a, 0) + (0, 1)(b, 0) = a + ib$ schreiben.

UE 27 ► Übungsaufgabe 1.2.4.2. (F) **◄ UE 27**

(1) Finden Sie alle komplexen Zahlen $z = a + bi$, die $z^2 = i$ erfüllen.

(2) Finden Sie alle komplexen Zahlen $z = a + bi$, die $z^5 + 2 = 0$ erfüllen.

Hinweis: Polarkoordinaten

Leicht identifiziert man auch eine isomorphe Kopie von $\mathbb{C}$ innerhalb eines beliebigen Körpers, wenn dieser sowohl $\mathbb{R}$ als auch eine Entsprechung von i enthält. Genauer gilt:

Satz 1.2.4.3. *Sei K ein Körper, $\varphi\colon \mathbb{R} \to K$ eine isomorphe Einbettung von $\mathbb{R}$ als Körper und i_K ein Element von K mit $i_K^2 = -1 \in K$. Dann gibt es genau zwei isomorphe Einbettungen $\psi\colon \mathbb{C} \to K$, die $\psi(a, 0) = \varphi(a)$ für alle $a \in \mathbb{R}$ erfüllen. Diese sind gegeben durch $\psi_1(a, b) := \varphi(a) + i_K\varphi(b)$ und $\psi_2(a, b) := \varphi(a) - i_K\varphi(b)$. Insbesondere (wenn*

[17] Die geometrische Interpretation als komplexe Zahlenebene sowie die Darstellung in Polarkoordinaten dürfte aus der Analysis bekannt sein. Die wichtigsten Fakten:

- Die Zahl $a - ib$ bzw. $(a, -b)$ nennen wir zu $a + ib = (a, b)$ *konjugiert*. Die zu $z = a + ib$ konjugierte Zahl $a - ib$ wird meist mit $\bar{z}$ bezeichnet. Die Zahl $z\bar{z} = (a + ib)(a - ib) = a^2 + b^2$ ist reell und nichtnegativ.
- Der *Absolutbetrag* der Zahl $a + ib$ $(a, b \in \mathbb{R})$ ist die reelle Zahl $|a + ib| := \sqrt{a^2 + b^2}$. Für reelle Zahlen stimmt dies mit dem üblichen Betrag überein.
- Die Gleichung $|z_1 \cdot z_2|^2 = |z_1|^2 \cdot |z_2|^2$ lässt sich leicht nachrechnen; daraus erhält man $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.
- Jede Zahl $a + ib$ mit $|a + ib| = 1$ lässt sich eindeutig in der Form $\cos\varphi + i\sin\varphi = \exp(i\varphi) = e^{i\varphi}$ mit $\varphi \in (-\pi, \pi]$ schreiben (oder, je nach Geschmack, $\varphi \in [0, 2\pi)$).
- Damit ist jede Zahl $z \in \mathbb{C}\setminus\{0\}$ eindeutig als $z = r \cdot e^{i\varphi}$ darstellbar (mit $r = |z| > 0$, $\varphi \in [0, 2\pi)$).
- Multiplikation und Division lassen sich in dieser Darstellung besonders leicht ausführen: $re^{i\varphi} \cdot se^{i\psi} = rs \cdot e^{i(\varphi+\psi)}$ und $\frac{re^{i\varphi}}{se^{i\psi}} = \frac{r}{s} \cdot e^{i(\varphi-\psi)}$.

Um interessante Beispiele zu gewinnen, werden wir gelegentlich die Darstellung komplexer Zahlen mittels Polarkoordinaten verwenden. Für den systematischen Aufbau einer in sich geschlossenen algebraischen Theorie wäre das nicht nötig.

man nämlich $K = \mathbb{C}$ setzt) hat $\mathbb{C}$ genau zwei Körperautomorphismen, die $\mathbb{R}$, genauer: die Menge aller Paare $(a, 0)$ mit $a \in \mathbb{R}$, punktweise fest lassen. Einer davon ist die Identität, der andere die Konjugation $(a, b) \mapsto (a, -b)$.

UE 28 ▶ Übungsaufgabe 1.2.4.4. (W) Beweisen Sie Satz 1.2.4.3. Hinweis: Zeigen Sie, dass ψ durch $\psi(0, 1)$ eindeutig festgelegt ist und für diesen Wert nur i_K und $-i_K$ in Frage kommen. **◀ UE 28**

Wie aus Satz 1.2.4.3 hervorgeht, muss man gewisse Eindeutigkeiten innerhalb der Bereiche $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ im Falle von $\mathbb{C}$ zu einer Zweideutigkeit abschwächen. Dennoch spricht man beispielsweise von *der* komplexen Zahl $2 + 3i$ (gemeint ist das Paar $(2, 3)$), ohne auf die Problematik[18] einzugehen, dass durch die Forderung $i^2 = -1$ noch nicht ausgeschlossen ist, dass damit genauso $2 - 3i$ gemeint sein könnte (also das Paar $(2, -3)$). Selbstverständlich werden auch wir uns dieser etwas ungenauen aber praktischen und deshalb gebräuchlichen Ausdrucksweise bedienen.
Man beachte, dass im Zusammenhang mit $\mathbb{C}$ nur algebraische Gesichtspunkte im Spiel waren, keine ordnungstheoretischen. Der Grund:

Satz 1.2.4.5. *Es gibt keine Ordnungsrelation, die $\mathbb{C}$ zu einem angeordneten Körper macht.*

UE 29 ▶ Übungsaufgabe 1.2.4.6. (V) Beweisen Sie Satz 1.2.4.5. **◀ UE 29**

Es sei hervorgehoben, dass in Satz 1.2.4.3 auf die Forderung $\psi(a, 0) = \varphi(a)$ nicht verzichtet werden kann. Auf den ersten Blick und angesichts von Übungsaufgabe 3.5.3.13 mag das erstaunen. Der Körper $\mathbb{C}$ besitzt aber unüberschaubar viele Automorphismen, wie wir später sehen werden (eine explizite Konstruktion ohne Verwendung des Auswahlaxioms bzw. des Zornschen Lemmas ist übrigens gar nicht möglich); siehe Anmerkung 6.2.3.6 und Übungsaufgabe 6.2.3.7.
Die enorme Bedeutung der komplexen Zahlen für große Teile der Mathematik (insbesondere auch für die Analysis) liegt nicht nur, aber zu einem guten Teil daran, dass der Körper der komplexen Zahlen *algebraisch abgeschlossen* ist.

Definition 1.2.4.7. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes Polynom

$$p(x) = \sum_{k=0}^{n} a_k x^k$$

mit $a_k \in K$, $n \geq 1$ und $a_n \neq 0$ mindestens eine Nullstelle in K hat.

Dass der Körper $\mathbb{C}$ diese Eigenschaft hat, ist einer der großen Sätze der Mathematik:

[18] Um weitere potentielle Unklarheiten zu vermeiden, verwenden wir das Symbol $\sqrt{t}$ ausschließlich dann, wenn t eine nichtnegative reelle Zahl ist; in diesem Fall bezeichnet $\sqrt{t}$ jene eindeutig bestimmte nichtnegative reelle Zahl r mit $r^2 = t$.

Satz 1.2.4.8 (Fundamentalsatz der Algebra, Fassung 1)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Trotz seines Namens ist der analytische Charakter des Fundamentalsatzes mindestens ebenso stark ausgeprägt wie der algebraische. Denn in der einen oder anderen Weise muss die Vollständigkeit der reellen Zahlen eingesetzt werden. Die ersten Beweise, die modernen Ansprüchen genügen, wurden von Carl Friedrich Gauß (1777–1855) erbracht. Mittlerweile gibt es zahlreiche Beweise. Wir werden in Unterabschnitt 9.3.5 einen mit sehr starkem algebraischen Anteil kennenlernen. Andere Beweise betonen den topologischen Aspekt oder verwenden vergleichsweise starke Geschütze aus der komplexen Analysis. Ein relativ leicht zugänglicher ist vermutlich bereits aus der Analysis-Grundvorlesung bekannt: Man zeigt erstens, dass für ein Polynom p die Funktion $|p|$, die jedem $z \in \mathbb{C}$ den Wert $|p(z)| \in \mathbb{R}$, $|p(z)| \geq 0$ zuordnet, ein (globales) Minimum haben muss, und zweitens, dass der Wert dieses Minimums nicht > 0 sein kann:

1. Sei also das komplexe Polynom $p(z) = \sum_{k=0}^{n} a_k z^k$ mit $a_k \in \mathbb{C}$, $n \geq 1$ und $a_n \neq 0$ vorgegeben. Für eine genügend große reelle Zahl R gilt

   $$\forall z \in \mathbb{C} : |z| \geq R \Rightarrow |p(z)| > |a_0| = |p(0)| \quad \text{(warum?)}$$

   Auf der kompakten Kreisscheibe D um 0 mit Radius R nimmt $|p|$ als stetige Funktion an einem Punkt $z_0 \in D$ einen minimalen Wert an, der dann ein globales Minimum von $|p|$ auf ganz $\mathbb{C}$ sein muss (warum?).

2. Ohne Beschränkung der Allgemeinheit ist $z_0 = 0$ (warum? $q(z) := p(z + z_0)$) Wenn nun z_0 keine Nullstelle von p wäre, dann hätte $p(z)$ ohne Beschränkung der Allgemeinheit die Form $p(z) = 1 + a_k z^k + \cdots + a_n z^n$ mit $k \geq 1$, $a_k \neq 0$ (warum?). Wähle $c \in \mathbb{C}$ so, dass $c^k = -1/a_k$ gilt, und betrachte $p(c\varepsilon)$ für kleines $\varepsilon > 0$, um einen Widerspruch herzuleiten.

UE 30 ► **Übungsaufgabe 1.2.4.9.** (V) Führen Sie den oben skizzierten Beweis des Fundamentalsatzes genauer aus. ◄ **UE 30**

Der Fundamentalsatz lässt sich auch so lesen: Es gibt keine Erweiterungen von $\mathbb{C}$ mehr, die durch das Lösen polynomieller Gleichungen entstehen. Genausowenig führt uns nach Satz 1.2.4.5 die Idee weiter, die hinter der Erweiterung von $\mathbb{Q}$ auf $\mathbb{R}$ steht, da dazu eine Ordnung notwendig ist. Mit den komplexen Zahlen ist somit ein Abschluss der Zahlenbereichserweiterungen erreicht. Trotzdem sind Erweiterungen möglich: entweder sogenannte transzendente (mehr hierüber insbesondere in Unterabschnitt 6.1.5) oder solche Erweiterungen, bei denen gewisse Eigenschaften eines Körpers verloren gehen.
Verzichtet man lediglich auf die Kommutativität der Multiplikation, so gibt es den *Schiefkörper* $\mathbb{H}$ der sogenannten Hamiltonschen *Quaternionen*. Als Vektorraum über $\mathbb{R}$ ist er 4-dimensional. Eine Basis ist gegeben durch Elemente, die man traditionell mit $1, i, j, k$ bezeichnet. Dabei fasst man 1 und i als die entsprechenden komplexen Zahlen auf, j und k als zusätzliche sogenannte imaginäre Einheiten, von denen jede dieselbe Rolle spielt

wie i, d. h. $i^2 = j^2 = k^2 = -1$. Insbesondere hat jedes $z \in \mathbb{H}$ eine eindeutige Darstellung $z = r_1 1 + r_2 i + r_3 j + r_4 k$ mit $r_1, r_2, r_3, r_4 \in \mathbb{R}$. Weiterhin ist 1 neutrales Element bezüglich der Multiplikation. Außerdem gilt $ij = k = -ji$, $jk = i = -kj$ und $ki = j = -ik$, sowie $rz = zr$ für alle $z \in \mathbb{H}$ und alle $r \in \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$.

UE 31 ► **Übungsaufgabe 1.2.4.10.** (B,E) Zeigen Sie: Es gibt tatsächlich einen sogar (bis auf Isomorphie) eindeutig bestimmten Schiefkörper $\mathbb{H}$ mit den angegebenen Eigenschaften. Anleitung für die Existenz eines solchen Schiefkörpers: Realisieren Sie $\mathbb{H}$ als eine vierparametrige Menge reeller 4×4-Matrizen $A(r_1, r_2, r_3, r_4)$, $r_1, r_2, r_3, r_4 \in \mathbb{R}$. Gehen Sie dabei davon aus, dass die Multiplikation mit einer Quaternion $z = r_1 1 + r_2 i + r_3 j + r_4 k$ einer linearen Transformation des Raumes $\mathbb{R}^4$ entspricht, und ordnen Sie diesem z die entsprechende Matrix zu. Überzeugen Sie sich, dass diese Zuordnung $z \mapsto A(r_1, r_2, r_3, r_4)$ eine isomorphe Einbettung ist. Überprüfen Sie, dass die Spaltenvektoren von $A(r_1, r_2, r_3, r_4)$ orthogonal (nicht notwendig normiert!) sind und dass $A(r_1, r_2, r_3, r_4)$ die Determinante $\sqrt{r_1^2 + r_2^2 + r_3^2 + r_4^2}$ hat. Hieraus folgt leicht, dass es sich bei $\mathbb{H}$ nicht nur um einen Ring mit 1, sondern um einen Schiefkörper handelt. ◄ **UE 31**

Schwächt man die Forderungen an einen Körper noch weiter ab, so finden sich auch noch weitere Strukturen höherer Dimension, z. B. die Oktonionen, bei denen auch die Assoziativität der Multiplikation verloren geht.

1.3. Paradigmen aus der Linearen Algebra

In diesem Abschnitt rekapitulieren wir wichtige Begriffe und Resultate aus der Linearen Algebra, um erste Beispiele von Klassifikationssätzen zu erhalten: Mit Hilfe des Begriffs der Linearen (Un-)Abhängigkeit (1.3.1) lässt sich das Austauschlemma formulieren und beweisen (1.3.2). Darauf fußt (wenigstens für endlich erzeugte Vektorräume) der Dimensionsbegriff, der eine vollständige Klassifikation aller Vektorräume über einem festen Körper ermöglicht (1.3.3).

1.3.1. Lineare (Un-)Abhängigkeit

Inhalt in Kurzfassung: Der Vollständigkeit halber werden einige Grundlagen aus der Linearen Algebra wiederholt. Besonders interessant in Hinblick auf spätere Verallgemeinerungen sind der Fortsetzungssatz für lineare Abbildungen und die Existenz von Basen.

Aus der Linearen Algebra sind die folgenden Begriffe bekannt:

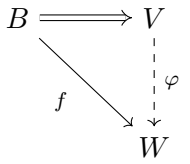
Definition 1.3.1.1. Sei V ein Vektorraum über dem Körper (oder auch Schiefkörper) K. Für jede Teilmenge $T \subseteq V$ schreiben wir $[T]$ für die *lineare Hülle* von T, also für den Durchschnitt aller Untervektorräume $U \leq V$, die $T \subseteq U$ erfüllen. Eine Menge T heißt *linear abhängig*, wenn es ein $t \in T$ gibt mit $t \in [T \setminus \{t\}]$. (Das heißt: t lässt sich als K-Linearkombination von Vektoren in $T \setminus \{t\}$, genauer: von einer endlichen Teilmenge von $T \setminus \{t\}$, schreiben.) Äquivalent: der Nullvektor lässt sich als nichttriviale Linearkombination (von endlich vielen Vektoren in T) darstellen.

Eine Menge S von Vektoren heißt *linear unabhängig*, wenn sie nicht linear abhängig ist; äquivalent: wenn sich jeder Vektor in $[S]$ auf genau eine Weise als Linearkombination von Vektoren in S schreiben lässt.
Ein *Erzeugendensystem* von V ist eine Teilmenge E mit $[E] = V$.
Eine Teilmenge B von V heißt *Basis* von V, wenn die folgenden (äquivalenten) Bedingungen erfüllt sind:

- B ist minimales[19] Erzeugendensystem, das heißt: $[B] = V$ aber $[B'] \neq V$ für alle echten Teilmengen $B' \subsetneq B$.
- B ist linear unabhängiges Erzeugendensystem.
- B ist maximale[20] linear unabhängige Menge, das heißt: B ist linear unabhängig, aber es gibt keine linear unabhängige echte Obermenge $B' \supsetneq B$.

Man beachte, dass die leere Menge $\emptyset$ stets linear unabhängig ist, während eine Menge, die den Nullvektor 0 enthält, immer linear abhängig ist.
Aus der Definition ergibt sich leicht:

Satz 1.3.1.2 (Fortsetzungssatz)**.** *Sei B Basis von V, und sei W ein beliebiger Vektorraum über dem Körper oder Schiefkörper K. Dann gibt es für jede Funktion $f\colon B \to W$ genau eine lineare Abbildung $\varphi\colon V \to W$, die f fortsetzt.*



Aus der linearen Unabhängigkeit von B folgt nämlich, dass die durch

$$\varphi\left(\sum_{b\in B} x_b b\right) := \sum_{b\in B} x_b f(b)$$

definierte Abbildung wohldefiniert ist. Weil B Erzeugendensystem ist, ist φ auf ganz V definiert; die Linearität von φ ergibt sich aus der Definition. Klarerweise ist φ die einzige lineare Fortsetzung von f.
Mit Hilfe des Auswahlaxioms kann man zeigen, dass jeder Vektorraum eine Basis hat. Man kann sogar den folgenden stärkeren Satz zeigen:

Satz 1.3.1.3. *Sei V Vektorraum, und sei $L \subseteq V$ eine linear unabhängige Menge. Dann gibt es eine Basis B von V mit $L \subseteq B$.*

[19] Man beachtet, dass hier Minimalität in Bezug auf die partielle Ordnung $\subseteq$ gemeint ist, nicht Minimalität in Bezug auf „Größe“ im Sinne von Kardinalität.
[20] Auch hier geht es nicht um Maximalität im Sinne der Kardinalität, sondern in Bezug auf $\subseteq$.

1.3.2. Das Austauschlemma und seine Konsequenzen

Inhalt in Kurzfassung: Für endlich erzeugte Vektorräume hat das Austauschlemma zur Folge, dass je zwei Basen gleich viele Elemente haben. Auch dieses Motiv wird später Verallgemeinerungen ermöglichen (Schlagwort Transzendenzbasen; siehe Definition 6.1.5.1).

Die Sätze aus diesem Abschnitt sind aus der Linearen Algebra bereits bekannt. Wir führen sie deshalb nochmals explizit an, weil wir später (in Unterabschnitt 6.1.5) mit ganz ähnlichen Konzepten/Beweisen algebraische Unabhängigkeit statt linearer Unabhängigkeit untersuchen können.

Lemma 1.3.2.1 (Austauschlemma)**.** *Sei V ein K-Vektorraum, $A \subseteq V$ und $b, c \in V$. Wenn $c \in [A \cup \{b\}]$ aber $c \notin [A]$ gilt, dann ist $b \in [A \cup \{c\}]$.*

Beweis. Der Vektor c lässt sich als Linearkombination $c = \lambda b + \sum_{i \in I} \lambda_i a_i$ schreiben, mit I endlich, $\lambda, \lambda_i \in K$ und $a_i \in V$. Es muss $\lambda \neq 0$ gelten, sonst wäre c in $[A]$. Daher lässt sich b als $\frac{1}{\lambda}(c - \sum_i \lambda_i a_a)$ schreiben, also $b \in [A \cup \{c\}]$. □

Folgerung 1.3.2.2. *Wenn V, A, b, c die Voraussetzungen des Austauschlemmas erfüllen, dann gilt $[A \cup \{b\}] = [A \cup \{c\}]$.*
Wenn A überdies linear unabhängig war, dann sind auch $A \cup \{b\}$ und $A \cup \{c\}$ linear unabhängig.

Folgerung 1.3.2.3 (Austauschsatz von Steinitz[21])**.** *Wenn B und C Basen des K-Vektorraums V sind, dann gibt es für jedes $b \in B$ ein $c \in C$, sodass $(B \setminus \{b\}) \cup \{c\}$ wiederum eine Basis ist.*

Beweis. Sei $b \in B$. Die Annahme $C \subseteq [B \setminus \{b\}]$ führt via $V = [C] \subseteq [[B \setminus \{b\}]] = [B \setminus \{b\}] \subsetneq V$ zu einem Widerspruch, daher gibt es ein c mit $c \notin [B \setminus \{b\}]$. Nach dem Austauschlemma gilt $b \in [(B \setminus \{b\}) \cup \{c\}]$. Daher ist $(B \setminus \{b\}) \cup \{c\}$ ein Erzeugendensystem, und nach Folgerung 1.3.2.2 sogar eine Basis. □

Lemma 1.3.2.4. *Sei V Vektorraum mit einer endlichen Basis B. Dann gilt: Für jede Basis C von V gilt $|B| = |C|$, also: alle Basen von V haben die gleiche (endliche) Kardinalität.*

Beweis. Sei $C_0 := C$. Wenn $B \neq C_0$ ist, sei $c \in C_0 \setminus B$ beliebig. (So ein c gibt es, sonst wäre $C_0 \subsetneq B$, was für Basen unmöglich ist.)
Wir finden mit dem Austauschsatz von Steinitz (mit vertauschten Rollen von B und C) ein $b \in B$, sodass $C_1 := (C_0 \setminus \{c\}) \cup \{b\}$ noch immer eine Basis ist. Wir wissen $b \notin C_0$, denn sonst wäre ja $C_0 \setminus \{c\}$ eine Basis; somit gilt $|C_0| = |C_1|$. Weil b ein neues Element von $B \cap C_1$ ist, gilt $|B \cap C_1| = |B \cap C_0| + 1$. Mit Induktion finden wir weitere Basen C_2, C_3, ... die alle gleich groß sind, aber immer größeren Schnitt mit B haben. Nach höchstens $|B|$ Schritten müssen wir eine Basis C_k erhalten, für die $C_k = B$ gilt. Wegen $|C_0| = |C_1| = \cdots = |C_k|$ erhalten wir $|C| = |B|$. □

[21] Ernst Steinitz (1871-1928)

1.3.3. Die Klassifikation beliebiger Vektorräume durch ihre Dimension

Inhalt in Kurzfassung: Da je zwei Basen eines Vektorraums gleich viele Elemente enthalten, kann deren Anzahl als Definition der Dimension dieses Vektorraums dienen. Es zeigt sich, dass die Vektorräume über einem gegebenen Körper mit dieser Zahl in folgendem Sinne klassifiziert werden können: Zwei Vektorräume sind genau dann isomorph, wenn sie dieselbe Dimension haben.

Die Eindeutigkeit der Kardinalität einer Basis (somit auch die Sinnhaftigkeit der Definition der Dimension) lässt sich für beliebige Vektorräume beweisen, unabhängig von der Größe ihrer Erzeugendensysteme.

Lemma 1.3.3.1. *Sei V Vektorraum über K, sei $B \subseteq V$ Basis, und sei $C \subseteq V$, $|C| < |B|$. Dann ist C kein Erzeugendensystem: $[C] \subsetneq V$.*

Folgerung 1.3.3.2. *Seien B_1, B_2 Basen von V. Dann gilt $|B_1| = |B_2|$.*

Beweis von Lemma 1.3.3.1. Ist V endlichdimensional, so folgt die Behauptung aus Lemma 1.3.2.4.
Sei also V nicht endlichdimensional. Dann müssen B und C unendlich sein.
Für jedes $c \in C$ gibt es eine endliche Menge $S_c \subseteq B$ mit $c \in [S_c]$. Da die Mengen S_c alle endlich sind, kann die Menge $\bigcup_{c\in C} S_c$ höchstens die Kardinalität $|C| < |B|$ haben (siehe Unterabschnitt A.5.6 im Anhang), also ist die Menge $S := \bigcup_{c\in C} S_c$ eine echte Teilmenge von B. Nun war aber B eine minimales Erzeugendensystem, daher gilt $[S] \subsetneq [B] = V$. Andererseits gilt $\forall c \in C : c \in [S_c] \subseteq [S]$, daher $C \subseteq [S]$ und somit $[C] \subseteq [S]$. Also ist C kein Erzeugendensystem von V. □

Zusammen mit Satz 1.3.1.3, wonach jeder Vektorraum eine Basis besitzt ($L = \emptyset$ setzen), können wir nun die Dimension eines Vektorraumes definieren.

Definition 1.3.3.3. Die *Dimension* $\dim_K V$ eines Vektoraumes V über dem Körper K ist definiert als die Kardinalität einer (und somit jeder beliebigen) Basis von V.

Damit erhalten wir:

Satz 1.3.3.4 (Klassifikation der K-Vektorräume)**.** *Für zwei Vektorräume V_1 und V_2 über demselben Körper K sind die folgenden beiden Aussagen äquivalent:*

(1) *$V_1 \cong V_2$. (V_1 und V_2 sind isomorph, d. h. definitionsgemäß: Es gibt eine K-lineare Bijektion $f\colon V_1 \to V_2$, und die inverse Abbildung ist auch K-linear.)*

(2) *$\dim_K V_1 = \dim_K V_2$. (Je zwei Basen B_1 von V_1 und B_2 von V_2 sind gleichmächtig, d. h. definitionsgemäß: es gibt eine Bijektion $g\colon B_1 \to B_2$. Äquivalent: es* gibt *Basen B_1 von V_1 und B_2 von V_2, die gleichmächtig sind.)*

Kurz gesagt: K-Vektorräume sind durch ihre Dimension eindeutig (bis auf K-Isomorphie) bestimmt.

Beweis. Sei zunächst $V_1 \cong V_2$, mit Isomorphismus $f : V_1 \to V_2$. Wenn B_1 eine Basis ist, dann ist $f(B_1)$ eine dazu gleichmächtige Basis von V_2, also folgt $\dim_K V_1 = \dim_K V_2$.

Sei jetzt $\dim_K V_1 = \dim_K V_2$, bezeugt durch Basen B_1 von V_1 und B_2 von V_2 sowie eine Bijektion $g : B_1 \to B_2$. Wenden wir den Fortsetzungssatz 1.3.1.2 auf $g : B_1 \to V_2$ sowie auf $g^{-1} : B_2 \to V_1$ an, so erhalten wir eindeutige Fortsetzungen zu linearen Abbildungen $\varphi_1 : V_1 \to V_2$ und $\varphi_2 : V_2 \to V_1$. Die Verkettungen $\varphi_2 \circ \varphi_1$ bzw. $\varphi_1 \circ \varphi_2$ stimmen auf B_1 bzw. B_2 mit der Identität auf V_1 bzw. V_2 überein. Je eine Anwendung der Eindeutigkeitsaussage des Fortsetzungssatzes liefert $\varphi_2 \circ \varphi_1 = \mathrm{id}_{V_1}$ bzw. $\varphi_1 \circ \varphi_2 = \mathrm{id}_{V_2}$. Somit ist $f := \varphi_1$ ein Isomorphismus $V_1 \to V_2$ mit Inverser $f^{-1} = \varphi_2$ und wir erhalten $V_1 \cong V_2$. □

UE 32 ► Übungsaufgabe 1.3.3.5. (F+) Wir nennen Unterräume U_1, U_2 eines Vektorraums V äquivalent ($U_1 \sim U_2$), wenn es einen Automorphismus $f : V \to V$ gibt, der $f(U_1) = U_2$ erfüllt. **◄ UE 32**

(1) Zeigen Sie, dass zwei Unterräume eines endlichdimensionalen Vektorraums genau dann äquivalent sind, wenn sie die gleiche Dimension haben.

(2) Zeigen Sie anhand eines Beispiels, dass dies für unendlichdimensionale Vektorräume nicht immer gilt.

(3) Finden Sie eine Charakterisierung der Relation $\sim$, die auch für unendlichdimensionale Vektorräume funktioniert. (Hinweis: Kodimension.)

2. Grundbegriffe

Hier beginnt der systematisch aufbauende Teil der Vorlesung. In den bisherigen Abschnitten wurden unter anderem die (überwiegend bereits vertrauten) Zahlenbereichskonstruktionen unter algebraischen Gesichtspunkten rekapituliert. Nun geht es um einen gemeinsamen begrifflichen Rahmen für die Untersuchung der behandelten Strukturen und für natürliche Verallgemeinerungen. Ein erster solcher Rahmen, der auch dem Zugang in der mathematischen Logik, insbesondere der Modelltheorie entspricht, wird in Abschnitt 2.1 entwickelt. Dabei handelt es sich im Wesentlichen um die Sichtweise der sogenannten *Allgemeinen* oder auch *Universellen Algebra*. In Abschnitt 2.2 betrachten wir einige wichtige algebraische Konstruktionen (insbesondere Unteralgebren, direkte Produkte und homomorphe Bilder) und deren Beziehungen untereinander in Gestalt der Isomorphiesätze. Abstrakter und in mancherlei Hinsicht dem strukturtheoretischen Denken der Algebra besser angepasst ist die Kategorientheorie, deren allererste Anfänge Inhalt von Abschnitt 2.3 sind.

2.1. Der logisch-modelltheoretische Rahmen der allgemeinen Algebra

In diesem Abschnitt wird ein recht weiter begrifflicher Rahmen gesteckt, innerhalb dessen die meisten strukturtheoretischen Anliegen, die uns in weiterer Folge beschäftigen werden, einheitlich abgehandelt werden können. Entsprechend beginnen wir mit der Rekapitulation notationeller und terminologischer Konventionen (2.1.1) und Grundbegriffen der Ordnungstheorie (2.1.2), in der eine Menge durch gewisse Relationen Struktur erhält. Sind es statt Relationen Operationen, so liegt eine universelle Algebra vor (2.1.3). Die Synthese beider Strukturelemente nennt man auch relationale Strukturen (2.1.4). Verbindendes Element von Strukturen sind Homomorphismen zwischen Algebren (2.1.5) bzw. strukturverträgliche Abbildungen zwischen relationalen Strukturen (2.1.6). In beiden Fällen kann die Klassifikation modulo Isomorphie als generelles Paradigma der Algebra verstanden werden (2.1.7). Weitere Themen, die in diesem Abschnitt angeschnitten werden, sind Terme, Termalgebra, Gesetze und Varietäten (2.1.8), die mathematische Logik in Form eines kurzen Exkurses (2.1.9) und Strukturen innerhalb derer Funktionen unterschiedlicher Stelligkeit eingesetzt werden können, sogenannte Klone (2.1.10).

2.1.1. Notation und Terminologie

Inhalt in Kurzfassung: Weitgehend bereits aus dem ersten Semester bekannte Grundbegriffe werden der Vollständigkeit halber zusammengestellt und in der Algebra wichtige Eigenschaften und Gesichtspunkte hervorgehoben. Beispiele solcher Grundbegriffe sind:

kartesisches Produkt, geordnetes Paar, Relation, Funktion/Abbildung, injektiv, surjektiv, bijektiv, Relationenprodukt mit der Verkettung von Abbildungen als Spezialfall, inverse Relation/Abbildung, (Halb-)Ordnungsrelation, Äquivalenzrelation und Quasiordnung.

Jahrtausendelang kam die Logik kaum über jene sogenannten *Syllogismen* hinaus, die Aristoteles schon im vierten Jahrhundert vor unserer Zeitrechnung formuliert hat. Dabei handelt es sich um Schlussfiguren wie jene nach dem berühmten Beispiel:

Alle Menschen sind sterblich. Sokrates ist ein Mensch. Also ist Sokrates sterblich.

Heute können wir dafür auch formal schreiben:

$$((\forall x : (m(x) \to s(x))) \wedge m(S)) \to s(S).$$

Dabei stehen die Symbole m und s für die Prädikate „ist Mensch“ bzw. „ist sterblich“, S für Sokrates. Denkt man in diesem Zusammenhang an wichtige mathematische Konzepte wie etwa die Definition

$$\forall \varepsilon > 0 \; \exists n_0 = n_0(\varepsilon) \; \forall n \geq n_0 : \; |x_n - \alpha| < \varepsilon$$

für die Grenzwertbeziehung $\lim_{n\to\infty} x_n = \alpha$ einer Folge $(x_n)_{n\in\mathbb{N}}$, so beobachten wir: In den Formeln können Teilaussagen (im Beispiel: $|x_n - \alpha| < \varepsilon$) vorkommen, die nicht nur von einem Objekt abhängen (wie die Prädikate bei Aristoteles), sondern von mehreren (im Beispiel: vom Folgenindex n, der reellen Zahl α und der positiven reellen Zahl ε). Zur formalen Beschreibung sind also mehrstellige Prädikate erforderlich. In mengentheoretischer Terminologie entsprechen dem Teilmengen n-facher kartesischer Produkte, also Mengen von n-Tupeln. Kazimierz Kuratowski (1896–1980) folgend definieren wir daher:

Definition 2.1.1.1. Für beliebige Objekte (Mengen) a, b ist das *geordnete Paar*[1] (a, b) die Menge $\{\{a\}, \{a, b\}\}$. Das *kartesische Produkt* zweier beliebiger Mengen A, B definieren wir durch $A \times B := \{(a, b) : \; a \in A, b \in B\}$. Rekursiv definieren wir für $n = 1, 2, \ldots$ und für Mengen $A_1, \ldots, A_n$ außerdem $A_1 \times \cdots \times A_n \times A_{n+1} := (A_1 \times A_2 \times \cdots \times A_n) \times A_{n+1}$, im Falle $A_1 = A_2 = \cdots = A$ entsprechend $A^1 := A$, $A^{n+1} := A^n \times A$. Wir schreiben für $a \in A = A^1$ gelegentlich auch (a), für $((a_1, a_2), a_3) \in (A_1 \times A_2) \times A_3 = A_1 \times A_2 \times A_3$ meist (a_1, a_2, a_3) etc. Schließlich vereinbaren wir $A^0 := \{\emptyset\}$.
Teilmengen ρ von $A_1 \times \ldots \times A_n$ heißen auch *n-stellige Relationen* zwischen den Mengen $A_1, \ldots, A_n$. Im Fall $n = 2$, $A_1 = A_2 = A$ heißt ρ auch eine *binäre Relation*[2] auf A. Für $(a, b) \in \rho$ schreiben wir auch $a \; \rho \; b$.

[1] Die wesentliche Eigenschaft dieses Paarbegriffs: $(a_1, b_1) = (a_2, b_2)$ genau dann, wenn $a_1 = a_2$ und $b_1 = b_2$. Es gibt auch andere formale Definitionen des geordneten Paares, welche unsere Zwecke gleich gut erfüllen wie die hier gewählte. Es soll nur verdeutlicht werden, dass der Begriff des geordneten Paares im Rahmen der Mengenlehre definiert werden kann und dafür neben den Mengen keine weitere Sorte von Ausgangsobjekten vonnöten ist.

[2] Man beachte, dass wir Relationen nicht nur als Aussagen oder Prädikate betrachten, sondern als *Objekte*. Die Formeln $3 < 4$ ist eine Aussage über die Zahlen 3 und 4, aber die Relation $<$ (auf den natürlichen Zahlen) ist ein Objekt, konkreter: eine Menge, nämlich eine Mengen von Paaren. Man kann also mit Relationen mengentheoretische Operationen ausführen (zum Beispiel den Durchschnitt zweier Relationen bilden).

Gibt es für eine Relation ρ zwischen A und B zu jedem $a \in A$ genau ein $b \in B$ mit $(a, b) \in \rho$, so heißt ρ auch *Funktion*[3] oder *Abbildung* von A nach B, symbolisch

$$\rho\colon A \to B.$$

In diesem Fall schreiben wir $\rho(a)$ für jenes $b \in B$ mit $a\ \rho\ b$ oder auch $\rho : a \mapsto b$. Eine Abbildung $\rho\colon A \to B$ heißt *injektiv*[4] */surjektiv*[5]*/bijektiv*[6], falls es zu jedem $b \in B$ höchstens/mindestens/genau ein $a \in A$ gibt mit $f(a) = b$.[7]
Für eine Abbildung $f\colon A \to B$ sowie Teilmengen $A_0 \subseteq A$ und $B_0 \subseteq B$ sind die Schreibweisen $f(A_0) := \{f(a) :\ a \in A_0\}$ für das soganannte *Bild* der Menge A_0 und $f^{-1}(B_0) := \{a \in A :\ f(a) \in B_0\}$ für das *Urbild* der Menge B_0 unter f gebräuchlich. Unter der *Einschränkung* $f|_{A_0}$ von f auf A_0 versteht man die Menge $f \cap (A_0 \times B)$, die offensichtlich selbst eine Abbildung $f|_{A_0}\colon A_0 \to B$ ist.
Wir wenden uns auch der Komposition von Abbildungen und – allgemeiner – Relationen zu.

Definition 2.1.1.2. Seien $\rho_1 \subseteq A \times B$ und $\rho_2 \subseteq B \times C$ Relationen. Dann ist das *Relationenprodukt* (genannt auch Verkettung, Komposition, Verknüpfung oder Hintereinanderausführung von Relationen oder, gegebenenfalls, Funktionen) als die Menge

$$\{\, (a, c) \in A \times C \mid \exists b \in B : (a, b) \in \rho_1 \text{ und } (b, c) \in \rho_2 \,\}$$

definiert.
Für diese Operation auf Relationen gibt es zwei einander widersprechende Schreibweisen: Einerseits könnte man dieses Produkt $\rho_1 \circ \rho_2$ nennen, weil dann

$$a(\rho_1 \circ \rho_2)c \ \Leftrightarrow\ \exists b \in B : a\ \rho_1\ b\ \rho_2\ c$$

gilt, andererseits ist im Spezialfall, dass ρ_1 und ρ_2 Funktionen sind, die Schreibweise $\rho_2 \circ \rho_1$ üblich[8], weil dann

$$\rho_2(\rho_1(a)) = (\rho_2 \circ \rho_1)(a)$$

[3] Manche Lehrbücher verlangen, dass eine Funktion F durch eine Relation ρ, eine Definitionsmenge A und eine Zielmenge B festgelegt wird, also etwa $F = (A, \rho, B)$, und bezeichnen ρ als den „Graphen der Funktion F“. Wir identifizieren eine Funktion mit ihrem Graphen ρ; die Definitionsmenge ist durch ρ eindeutig bestimmt als die Menge $\{a \mid \exists b : (a, b) \in \rho\}$; die Zielmenge kann irgendeine Menge sein, die $\{b \mid \exists a : (a, b) \in \rho\}$ enthält, und ergibt sich meist aus dem Kontext.
Beachten Sie, dass man die Injektivität einer Funktion aus ihrem Graphen ablesen kann; Surjektivität ist hingegen keine Eigenschaft der Funktion selbst, sondern eine Beziehung zwischen einer Funktion und einer Zielmenge. So ist zum Beispiel die Funktion $\{(x, x^2) : x \in \mathbb{R}\}$ surjektiv von $\mathbb{R}$ auf $\mathbb{R}_{\geq 0}$, aber nicht surjektiv von $\mathbb{R}$ auf $\mathbb{R}$.

[4] englisch: *injective* oder *one-to-one, 1-1*

[5] englisch: *surjective* oder *onto*

[6] englisch: *bijective*

[7] Anmerkung zur Injektivität: Eine Abbildung $f\colon A \to B$ ist injektiv, wenn für alle $x_1, x_2 \in A$ die Implikation $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ gilt. Äquivalent dazu ist die Implikation $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$; letztere Implikation ist oft leichter nachzuprüfen, weil wir mit Gleichungen besser umgehen können als mit Ungleichungen.

[8] Die Notation $f(x)$ für Funktionsanwendung geht auf Leonhard Euler (1707–1783) zurück. Grundsätzlich spräche aber nichts dagegen und manches dafür, das Objekt $g(f(x))$ in umgekehrter Reihenfolge zu notieren als $(x)(f \circ g) = ((x)f)g$ oder, noch einfacher, als xfg oder x_{fg}. Tatsächlich findet sich diese Schreibweise in der Fachliteratur vereinzelt, besonders in der Gruppentheorie, wo sie mit der lateinischen Schrift, weil sie von links nach rechts verläuft, eindeutig besser harmoniert.

gilt. Bei Bedarf könnte man zwei Symbole $\rho_1 \underset{\rightarrow}{\circ} \rho_2$ und $\rho_2 \underset{\leftarrow}{\circ} \rho_1$ parallel für Relationsprodukte verwenden; wir entscheiden uns für die zweite Variante und nennen das oben beschriebene Produkt $\rho_2 \circ \rho_1$.

Definition 2.1.1.3. Die *inverse Relation* (auch *duale Relation*) $\rho^{-1} \subseteq B \times A$ einer Relation $\rho \subseteq A \times B$ ist definiert als die Menge aller $(b, a) \in B \times A$ mit $(a, b) \in \rho$.

Folgende Eigenschaften sind leicht nachzuprüfen:

Proposition 2.1.1.4. *Für Relationen $\rho = \rho_1 \subseteq A \times B$, $\rho_2 \subseteq B \times C$ und $\rho_3 \subseteq C \times D$ gilt:*

1. *Das Relationenprodukt ist assoziativ:* $(\rho_3 \circ \rho_2) \circ \rho_1 = \rho_3 \circ (\rho_2 \circ \rho_1)$
2. *Für die identische Relation (Abbildung)* $\mathrm{id}_B := \{(b, b) \mid b \in B\}$ *auf B gilt* $\rho_2 \circ \mathrm{id}_B = \rho_2$ *und* $\mathrm{id}_B \circ \rho_1 = \rho_1$.
3. *Sind ρ_1 und ρ_2 Funktionen, so auch $\rho_2 \circ \rho_1$.*
4. *Sind ρ_1 und ρ_2 injektive Funktionen, so auch $\rho_2 \circ \rho_1$.*
5. *Sind ρ_1 und ρ_2 surjektive Funktionen, so auch $\rho_2 \circ \rho_1$.*
6. *Sind ρ_1 und ρ_2 bijektive Funktionen, so auch $\rho_2 \circ \rho_1$.*
7. *Sei $\rho : A \to B$ eine Funktion. Die inverse Relation ρ^{-1} ist genau dann eine Funktion, wenn ρ eine injektive Funktion ist. In diesem Fall ist $\rho^{-1} \colon \rho(A) \to A$.*
8. *Genau dann ist sogar $\rho^{-1} \colon B \to A$, wenn $\rho \colon A \to B$ eine bijektive Funktion ist.*

UE 33 ▶ Übungsaufgabe 2.1.1.5. (V) Beweisen Sie Proposition 2.1.1.4. **◀ UE 33**

Definition 2.1.1.6. Eine binäre Relation ρ auf A heißt

- *reflexiv (auf A)*, falls $a \rho a$ für alle $a \in A$.
- *antireflexiv (auch areflexiv oder irreflexiv)*, falls $(a, a) \notin \rho$ für alle $a \in A$.
- *transitiv*, falls $a \rho b$ und $b \rho c$ stets (also für alle $a, b, c \in A$) $a \rho c$ impliziert.
- *symmetrisch*, falls $a \rho b$ stets $b \rho a$ impliziert.
- *antisymmetrisch*, falls $a \rho b$ und $b \rho a$ stets $a = b$ impliziert.

Die Elemente $a, b \in A$ heißen *vergleichbar* (bezüglich ρ), falls $a \rho b$ oder $b \rho a$ gilt. Die binäre Relation ρ auf A heißt

- *Halbordnung(srelation)*[9] auf A und (A, ρ) heißt *Halbordnung*[10] (oder *partielle Ordnung*), wenn ρ reflexiv, transitiv und antisymmetrisch ist. Eine antireflexive transitive Relation ρ heißt *strikte Halbordnung(srelation)*, und (A, ρ) heißt entsprechend

[9] englisch: *partial order*

[10] Achtung: in manchen Büchern wird *Halbordnung* durch *Ordnung* abgekürzt, in anderen ist eine *Ordnung* immer eine Totalordnung.

strikte Halbordnung. Jeder Halbordnung (M, R) kann man die strikte Halbordnung (M, R') mit $R' = R \setminus \{(x, x) \mid x \in M\}$ zuordnen und umgekehrt. Offensichtlich ist dieser Zusammenhang zwischen Halbordnungen und strikten Halbordnungen ein bijektiver.[11]

- (*strikte*) *Totalordnung*[12] (alternativ auch *Kette*[13] oder *lineare Ordnung*[14]) auf A, wenn ρ eine (strikte) Halbordnung auf A ist, in der je zwei Elemente $a \neq b \in A$ vergleichbar sind.
- (*strikte*) *Wohlordnung*[15], wenn ρ eine (strikte) Totalordnung ist mit: Jede nichtleere Teilmenge $T \subseteq A$ hat ein kleinstes Element, d. h., es gibt ein $t_0 \in T$ mit $t_0 \, \rho \, t$ für alle $t \in T \setminus \{t_0\}$.
- *Äquivalenzrelation*, wenn ρ reflexiv, transitiv und symmetrisch ist.

UE 34 ► **Übungsaufgabe 2.1.1.7.** (F) Sei M eine beliebige Menge. Ist jede symmetrische transitive Relation $\rho \subseteq M \times M$ auch reflexiv? ◄ **UE 34**

Bekanntlich stehen die Äquivalenzrelationen auf einer Menge A in einem bijektiven Zusammenhang mit den *Partitionen* $\mathcal{P}$ von A. Das sind jene Teilmengen $\mathcal{P} \subseteq \mathfrak{P}(\mathcal{A})$ Potenzmenge, für die gilt: Alle $K \in \mathcal{P}$ sind nicht leer, paarweise *disjunkt* (d. h., je zwei $K_1 \neq K_2 \in \mathcal{P}$ haben leeren Schnitt) und ihre Vereinigung ist ganz A. Es gilt nämlich:

Proposition 2.1.1.8. *Sei A eine Menge.*
Für jede Äquivalenzrelation $\sim$ auf A und für jedes $a \in A$ sei $[a]_\sim := \{b \in A \mid a \sim b\}$, genannt die Äquivalenzklasse *von a. Außerdem bezeichne $\mathcal{P}_\sim$ die Menge aller Äquivalenzklassen $[a]_\sim$ mit $a \in A$.*
Umgekehrt sei für jede Partition $\mathcal{P}$ von A die Relation $\sim_\mathcal{P}$ auf A definiert durch: $a \sim_\mathcal{P} b$ genau dann, wenn es ein $K \in \mathcal{P}$ gibt mit $a, b \in K$.
Dann gilt:

1. *Für jede Äquivalenzrelation $\sim$ auf A ist $\mathcal{P}_\sim$ eine Partition von A.*
2. *Für jede Partition $\mathcal{P}$ von A ist $\sim_\mathcal{P}$ eine Äquivalenzrelation auf A.*
3. *Die Zuordnungen $\sim \mapsto \mathcal{P}_\sim$ und $\mathcal{P} \mapsto \sim_\mathcal{P}$ sind zueinander inverse Bijektionen zwischen der Menge aller Äquivalenzrelationen auf A und der Menge aller Partitionen von A, d. h. explizit: Für jede Äquivalenzrelation $\sim$ auf A stimmt die Äquivalenzrelation $\sim_{\mathcal{P}_\sim}$ wieder mit $\sim$ überein, und für jede Partition $\mathcal{P}$ von A stimmt die Partition $\mathcal{P}_{\sim_\mathcal{P}}$ wieder mit $\mathcal{P}$ überein.*

[11] Aus diesem Grund ist mit dem Wort „Ordnung“ oder „Halbordnung“ gelegentlich auch eine strikte Halbordnung gemeint. Ob es sich tatsächlich um eine Halbordnung in unserem Sinn oder um eine strikte Halbordnung handelt, lässt sich meist aus dem Kontext oder aus der Notation erschließen: Für Halbordnungen werden meist Symbole wie $\leq$, $\leqq$, $\preceq$, $\sqsubseteq$ etc verwendet, für strikte Halbordnungen $<$, $\prec$, $\sqsubset$, etc.
[12] englisch: *total order*
[13] englisch: *chain*
[14] englisch: *linear order*
[15] englisch: *well-order*

UE 35 ► **Übungsaufgabe 2.1.1.9.** (V,W) Beweisen Sie Proposition 2.1.1.8. ◄ **UE 35**

Definition 2.1.1.10. Sei A eine Menge und $\sim$ eine Äquivalenzrelation auf A. Dann schreibt man $A/_\sim$ für die der Relation $\sim$ gemäß Proposition 2.1.1.8 zugeordnete Partition $\mathcal{P}_\sim$, d. h. explizit: $A/_\sim = \{[a]_\sim \mid a \in A\}$.

Eine Verbindung zwischen Äquivalenzrelationen und Halbordnungen stellen die Quasiordnungen dar.

Definition 2.1.1.11. Eine binäre Relation auf A heißt *Quasiordnung* oder auch *Präordnung*, wenn sie reflexiv und transitiv ist.

Im Gegensatz zu Halbordnungen wird also bei einer Quasiordnung keine Antisymmetrie vorausgesetzt. Das elementarste und gleichzeitig eines der wichtigsten Beispiele ist die Teilerrelation auf $\mathbb{Z}$ (oder, allgemeiner, auf einem Ring mit Eins). Sinnvollerweise identifiziert man in diesem Kontext die Zahlen k und $-k$. Diesem naheliegenden Schritt entspricht der folgende allgemeine Sachverhalt.

Satz 2.1.1.12. *Sei $\leq_M$ eine Quasiordnung auf einer Menge M. Definiert man für $a, b \in M$ die Relation $a \sim b$ durch $a \sim b :\Leftrightarrow a \leq_M b$ und $b \leq_M a$, so erhält man eine Äquivalenzrelation $\sim$ auf M. Auf der Faktormenge $M/\sim$ (der Menge aller Äquivalenzklassen auf M) lässt sich durch $[a]_\sim \leq [b]_\sim :\Leftrightarrow a \leq_M b$ eine Halbordnungsrelation definieren.*

UE 36 ► **Übungsaufgabe 2.1.1.13.** (V,W) Beweisen Sie Satz 2.1.1.12. Vergessen Sie insbesondere nicht, auf die Wohldefiniertheit einzugehen. ◄ **UE 36**

Definition 2.1.1.14. Mit den Bezeichnungen aus Satz 2.1.1.12 heißt $(M/\sim, \leq)$ die *der Quasiordnung $(M, \leq_M)$ zugehörige Halbordnung.*

Anmerkung 2.1.1.15. Der einfacheren Terminologie halber wollen wir auch dann von Äquivalenzrelationen etc. sprechen, wenn A und ρ keine Mengen sind, sondern *Klassen*. Intuitiv sind das mengenähnliche Objekte (insofern sie durch ihre Elemente eindeutig bestimmt sind), die aber so groß sind, dass man Widersprüche in Kauf nehmen müsste, wenn man alle Operationen, die für Mengen erlaubt sind, auch mit Klassen uneingeschränkt ausführte. Der wichtigste formale Unterschied besteht darin, dass nur Mengen selbst wieder als Elemente von Mengen oder auch Klassen auftreten können. Wichtige Beispiele echter Klassen: Klassen von Algebren wie etwa die Klasse aller Gruppen oder auch die Klasse aller zu einer gegebenen Menge gleichmächtigen Mengen.

2.1.2. Grundbegriffe der Ordnungstheorie

Inhalt in Kurzfassung: Von den zahlreichen Begriffen aus der Theorie der Halbordnungen, die im Folgenden eingeführt werden, werden später vor allem vollständige Verbände und die mit ihnen zusammenhängenden Aussagen immer wieder eine wichtige Rolle spielen.

Nützlich für die Veranschaulichung von (endlichen) Halbordnungen sind Hassediagramme.

Wir erinnern daran, dass eine Halbordnung auf einer Menge M eine zweistellige Relation R ist, die antisymmetrisch, transitiv und auf M reflexiv ist. (Siehe Definition 2.1.1.6.) Statt „$a \leq x$ und $b \leq x$“ schreiben wir meist abgekürzt $a, b \leq x$; analog ist $x \leq a, b$ zu verstehen. Statt „$a \leq b$ und $b \leq c$“ schreiben wir oft $a \leq b \leq c$.

Beispiele 2.1.2.1.

(1) $(\mathbb{R}, \leq)$ ist eine Kette.

(2) $(\mathbb{N}, |)$ ist eine halbgeordnete Menge, aber keine Kette.

(3) $(\mathfrak{P}(M), \subseteq)$ ist eine halbgeordnete Menge, aber für $|M| \geq 2$ keine Kette.

(4) Ist $(M, \leq)$ eine halbgeordnete Menge und $N \subseteq M$, dann ist $(N, \leq_N)$ ebenfalls eine halbgeordnete Menge. Ist $(M, \leq)$ eine Kette, dann auch $(N, \leq_N)$. Dabei steht $\leq_N$ für die Menge aller Paare (x, y) die sowohl $x \leq y$ als auch $x, y \in N$ erfüllen, also für $\leq \cap (N \times N)$.

Definition 2.1.2.2. Seien $(P, \leq)$ und $(Q, \sqsubseteq)$ partielle Ordnungen (und $<$ bzw. $\sqsubset$ die zugehörigen strikten Ordnungsrelationen). Eine Funktion $f : P \to Q$ heißt

- *(schwach) monoton*, wenn für alle $x, x' \in P$ die Implikation $x \leq x' \Rightarrow f(x) \sqsubseteq f(x')$ gilt;
- *streng monoton*, wenn für alle $x, x' \in P$ die Implikation $x < x' \Rightarrow f(x) \sqsubset f(x')$ gilt.

Definition 2.1.2.3. Sei $(P, \leq)$ eine partielle Ordnung (und $(P, <)$ die zugehörige strikte partielle Ordnung), $A \subseteq P$, $p_0 \in P$. Dann heißt

- p_0 *untere Schranke* von A, wenn $p_0 \leq a$ für alle $a \in A$ gilt.
- p_0 *kleinstes Element* von A, wenn $p_0 \in A$ und $p_0 \leq a$ für alle $a \in A$ gilt; wir schreiben dann $p_0 = \min(A)$.
- p_0 *minimal*[16] in A, wenn $p_0 \in A$ und es kein $a \in A$ mit $a < p_0$ gibt (sehr wohl aber ist erlaubt, dass a und p_0 unvergleichbar sind).
- p_0 *Infimum* von A, wenn p_0 die größte untere Schranke von A ist; wir schreiben dann $p_0 = \inf A$.
  (Wenn A ein kleinstes Element m hat, dann gilt $m = \inf A$. Wenn A kein kleinstes Element hat, dann kann es dennoch ein Infimum geben; dieses liegt dann aber nicht in A.)
- Eine Teilmenge $A \subseteq P$ heißt *nach unten beschränkt*, wenn es in P eine untere Schranke von A gibt.
- Eine Teilmenge $A \subseteq P$ heißt *Antikette*, wenn je zwei verschiedene Elemente $a, b \in A$ unvergleichbar sind, also wenn weder $a \leq b$ noch $b \leq a$ gilt.

[16] Man beachte den Unterschied zwischen einem minimalen und einem (=**dem**) kleinsten Element. Die Aussage „x ist minimal in A“ ist im Allgemeinen nicht äquivalent zu „$x = \min(A)$“!

Analog sind die Begriffe *obere Schranke*, *größtes Element*, *maximal*, *Supremum* und *nach oben beschränkt* definiert. Eine Teilmenge $A \subseteq P$ heißt (schlechthin) *beschränkt*, wenn A sowohl nach unten als auch nach oben beschränkt ist.

Der Paarigkeit, mit der die meisten dieser Begriffe auftreten, liegt ein ziemlich offensichtliches *Dualitätsprinzip* für halbgeordnete Mengen zugrunde: Ist $(M, \leq)$ eine halbgeordnete Menge, dann auch $(M, \geq)$. Daraus ergeben sich die folgenden dualen Begriffe:

$\leq$	$\geq$
kleinstes Element	größtes Element
minimales Element	maximales Element
Infimum	Supremum

So gilt etwa: m ist minimal in $(M, \leq) \Leftrightarrow m$ ist maximal in $(M, \geq)$.

Beispiele 2.1.2.4.

(1) In $(\mathbb{R}, \leq)$ entsprechen die eben definierten Begriffe den in der Analysis üblichen.

(2) In $(\mathbb{N}, |)$ gilt für $T \subseteq \mathbb{N}$ mit $T \neq \emptyset$ Folgendes: $\inf T = \mathrm{ggT}(T)$ und $\sup T = \mathrm{kgV}(T)$. Weiters ist $\inf \emptyset = 0$ und $\sup \emptyset = 1$.

(3) In $(\mathfrak{P}(M), \subseteq)$ gilt für $\mathfrak{S} \subseteq \mathfrak{P}(M)$: $\inf \mathfrak{S} = \bigcap \mathfrak{S} := \bigcap_{A \in \mathfrak{S}} A$ und $\sup \mathfrak{S} = \bigcup \mathfrak{S} := \bigcup_{A \in \mathfrak{S}} A$.

Anmerkung 2.1.2.5.

- Man beachte, dass die leere Menge zwar kein kleinstes oder minimales Element enthalten kann, dass aber jedes Element von P sowohl obere wie auch untere Schranke der leeren Menge ist.
- Um zu zeigen, dass p kleinstes Element der Menge A ist, genügt es im Allgemeinen *nicht*, die Annahme $\exists a \in A : a < p$ auf einen Widerspruch zu führen. Damit zeigt man nämlich nur, dass p *minimal* in A ist.
- Man sieht leicht, dass eine partielle Ordnung höchstens ein kleinstes Element enthalten kann (möglicherweise aber mehrere minimale Elemente).
- Eine Halbordnung $(P, \leq)$ (aufgefasst als Teilmenge ihrer selbst) ist folglich genau dann nach unten/oben beschränkt, wenn sie ein kleinstes/größtes Element enthält. Insbesondere ist die einelementige Halbordnung beschränkt, nicht aber die leere Halbordnung.

Definition 2.1.2.6. Eine Halbordnung $(M, \leq)$ heißt eine *Noethersche Halbordnung*, wenn sie die *aufsteigende Kettenbedingung* (ACC = ascending chain condition) erfüllt: Es gibt keine unendlich aufsteigenden Ketten, das heißt: keine streng monotone Abbildung $f\colon (\mathbb{N}, \leq) \to (M, \leq)$. Dual heißt $(M, \leq)$ eine *Artinsche Halbordnung*, wenn sie die *absteigende Kettenbedingung* (DCC = descending chain condition) erfüllt: Es gibt keine unendlich absteigenden Ketten, das heißt: keine streng monotone Abbildung $f\colon (\mathbb{N}, \leq) \to (M, \geq)$.

UE 37 ▶ **Übungsaufgabe 2.1.2.7.** (B) Man gebe Beispiele von Halbordnungen (oder sogar linearen Ordnungen), die zeigen, dass die Kettenbedingungen ACC und DCC unabhängig voneinander sind (also dass keine die andere impliziert). ◀ **UE 37**

UE 38 ▶ **Übungsaufgabe 2.1.2.8.** (E) Man zeige, dass eine Kette mit ACC und DCC endlich ist. ◀ **UE 38**

UE 39 ▶ **Übungsaufgabe 2.1.2.9.** (B,E) Gilt die Aussage aus Übungsaufgabe 2.1.2.8 für beliebige Halbordnungen, wenn man zusätzlich voraussetzt, dass es keine unendliche Antikette gibt? ◀ **UE 39**

UE 40 ▶ **Übungsaufgabe 2.1.2.10.** (F,B) Geben Sie eine nichtleere partielle Ordnung an, die kein kleinstes Element hat. (Wenn möglich, finden Sie eine endliche partielle Ordnung mit dieser Eigenschaft.)
Geben Sie eine nichtleere partielle Ordnung an, die kein minimales Element hat. (Wenn möglich, finden Sie eine endliche partielle Ordnung mit dieser Eigenschaft.) ◀ **UE 40**

UE 41 ▶ **Übungsaufgabe 2.1.2.11.** (F,B) Geben Sie eine nichtleere partielle Ordnung an, die genau ein minimales Element hat, aber kein kleinstes Element hat. (Wenn möglich, finden Sie eine endliche partielle Ordnung mit dieser Eigenschaft.) ◀ **UE 41**

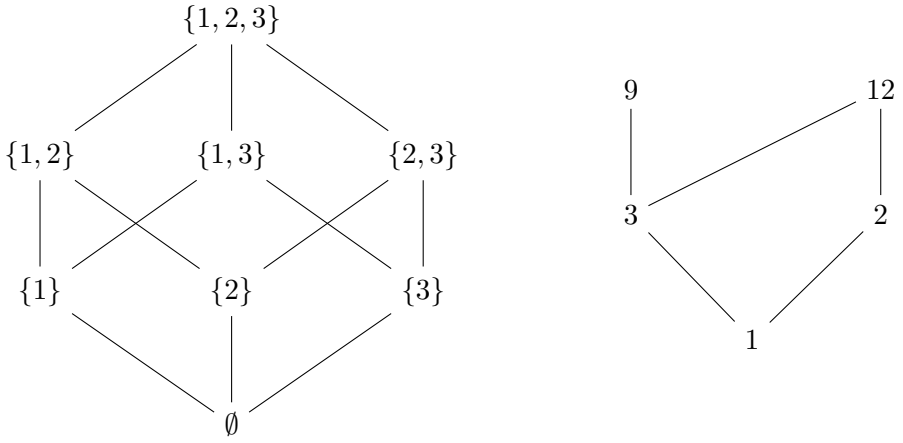
Oft sind die folgenden einfachen Charakterisierungen Noetherscher bzw. Artinscher Halbordnungen nützlich:

Proposition 2.1.2.12. *Eine Halbordnung $(M, \leq)$ ist genau dann Noethersch, wenn sie die sogenannte* Maximalbedingung *erfüllt: Jede nichtleere Teilmenge $T \subseteq M$ enthält ein maximales Element.*
Eine Halbordnung $(M, \leq)$ ist genau dann Artinsch, wenn sie die sogenannte Minimalbedingung *erfüllt: Jede nichtleere Teilmenge $T \subseteq M$ enthält ein minimales Element.*

Beweis. Wegen der Dualität genügt es, die erste der beiden Aussagen zu beweisen.
Sei also $(M, \leq)$ eine Noethersche Halbordnung und $T \subseteq M$ nicht leer. Wir nehmen indirekt an, dass T kein maximales Element enthalte. Dann ist für jedes $t \in T$ die Menge $S_t := \{t' \in T \mid t' > t\}$ nicht leer. Laut Auswahlaxiom gibt es somit eine Funktion $f : T \to T$ mit $f(t) \in S_t$ für alle $t \in T$. Wir wählen irgendein $t_0 \in T$. Nach dem Rekursionssatz (siehe Satz A.2.2.1) gibt es eine (eindeutige) Folge $(t_n)_{n\in\mathbb{N}}$ mit $t_{n+1} = f(t_n)$ für alle $n \in \mathbb{N}$. Nach Konstruktion ist $t_0 < t_1 < t_2 \ldots \in T \subseteq M$ eine unendlich echt aufsteigende Folge, im Widerspruch zur Voraussetzung, dass $(M, \leq)$ Noethersch ist, d. h. ACC erfüllt.
Zum Beweis der Umkehrung sei die Maximalbedingung an $(M, \leq)$ vorausgesetzt. Wäre $(M, \leq)$ nicht Noethersch, so gäbe es eine unendlich echt aufsteigende Folge von Elementen $t_0 < t_1 < \ldots \in M$. Dann hätte die Menge $T := \{t_n \mid n \in \mathbb{N}\} \subseteq M$ kein maximales Element, Widerspruch zur Voraussetzung. □

Definition 2.1.2.13. Sei $(P, \leq)$ eine Halbordnung und $(P, <)$ die zugehörige strikte Halbordnung. Für $p, q \in P$ sagen wir, dass q ein (direkter) *Nachfolger* von p ist, wenn $p < q$ gilt, es aber kein r mit $p < r < q$ gibt. Gelegentlich schreibt man dies als $p \lessdot q$. Das *Hasse-Diagramm* von P ist ein gerichteter Graph, dessen Knotenmenge die Menge P ist, und dessen Kanten die Paare (p, q) mit $p \lessdot q$ sind. In graphischen Darstellungen eines Hassediagramms stellt man den Graphen üblicherweise so dar, dass die Kanten alle hinauf gerichtet sind und erspart sich damit das Einzeichnen von Pfeilen.

Beispiel 2.1.2.14. Die Potenzmenge $\mathfrak{P}(\{1, 2, 3\})$ der 3-elementigen Menge $\{1, 2, 3\}$ wird durch die Relation $\subseteq$ halbgeordnet, ebenso die Menge $\{1, 2, 3, 9, 12\}$ durch die Relation $x|y$ (x teilt y). Die Hassediagramme dieser Relationen sehen so aus:



UE 42 ► **Übungsaufgabe 2.1.2.15.** (F) Sei $(P, <)$ eine endliche partielle Ordnung. Dann ist $<$ die *transitive Hülle* der Relation $\lessdot$, d. h.: die kleinste transitive Relation, die $\lessdot$ als Teilmenge enthält. ◄ **UE 42**

UE 43 ► **Übungsaufgabe 2.1.2.16.** (F,E) Geben Sie zwei verschiedene partielle Ordnungen $(P, <_1)$, $(P, <_2)$ auf derselben Grundmenge an, die die gleichen Hassediagramme (was genau bedeutet das?) haben.[17] ◄ **UE 43**

Proposition 2.1.2.17. *Sei $(P, \leq)$ eine Halbordnung, in der jede Teilmenge ein Infimum hat. Dann hat auch jede Teilmenge von P ein Supremum. Insbesondere liegt ein* vollständiger Verband *vor (siehe auch Definition 2.1.4.3).*

[17] Aus der vorigen Übungsaufgabe ergibt sich, dass jede endliche partielle Ordnung durch ihre Grundmenge und ihr Hassediagramm eindeutig bestimmt ist. Da das Hassediagram übersichtlicher als die Ordnung selbst ist, werden kleine endliche partielle Ordnungen meist durch ihr Hassediagramm beschrieben. Für unendliche partielle Ordnungen ist das Hassediagramm aber im Allgemeinen wenig aussagekräftig; daher wird der Begriff „Hassediagramm“ oft überhaupt nur für endliche partielle Ordnungen definiert.

UE 44 ► **Übungsaufgabe 2.1.2.18.** (V,W) Beweisen Sie Proposition 2.1.2.17 und erläutern Sie, warum die Halbordnung $(\mathbb{N}, \leq)$ kein Gegenbeispiel ist. ◄ **UE 44**

Die häufigste Anwendung von Proposition 2.1.2.17 ist die folgende.

Folgerung 2.1.2.19. *Sei X eine Menge und $\mathfrak{S}$ eine durchschnittsstabile Menge von Teilmengen von X. (Explizit bedeutet das: Für jedes $\mathfrak{T} \subseteq \mathfrak{S}$ liegt auch der Durchschnitt $\bigcap \mathfrak{T} = \bigcap_{T \in \mathfrak{T}} T$, also das Infimum von $\mathfrak{T}$ bezüglich $\subseteq$, wieder in $\mathfrak{S}$. Weil der Durchschnitt über die leere Menge vereinbarungsgemäß die gesamte Menge X ist, heißt das für $\mathfrak{T} = \emptyset$ insbesondere $X \in \mathfrak{S}$.) Dann ist $\mathfrak{S}$ bezüglich der Inklusion $\subseteq$ sogar ein vollständiger Verband.*

Für uns sehr wichtige Beispiele von solch durchschnittsstabilen Systemen $\mathfrak{S}$ werden sein: Die Menge $\mathrm{Sub}(\mathfrak{A})$ aller Unteralgebren und die Menge $\mathrm{Con}(\mathfrak{A})$ aller Kongruenzrelationen einer Algebra $\mathfrak{A}$ (und somit als Spezialfall auch die Menge aller Normalteiler einer Gruppe und die Menge aller Ideale eines Rings). Interessant ist meist die Frage, ob das Supremum in solchen Verbänden konkret beschrieben werden kann. Im Kontrast zum Infimum, das als mengentheoretischer Schnitt eine sehr einfache Interpretation hat, kann nämlich, wenn $\mathfrak{S}$ nicht die gesamte Potenzmenge von X ist, als Supremum nicht einfach die Vereinigung genommen werden, sondern es muss im Allgemeinen ein mehr oder weniger komplizierter Erzeugungsprozess beschrieben werden, siehe zum Beispiel Unterabschnitt 2.2.1.

2.1.3. Operationen und universelle Algebren

Inhalt in Kurzfassung: Im Zentrum der Algebra stehen algebraische Strukturen, die nun eingeführt werden sollen. Dabei handelt es sich um Mengen zusammen mit Operationen unterschiedlicher Stelligkeit. Interessante Eigenschaften solcher Operationen sind z. B. Gesetze (wie etwa Assoziativ-, Kommutativ- oder Distributivgesetz), die Anlass geben zur Definition interessanter Klassen algebraischer Strukturen (wie etwa Gruppen, Ringe oder Körper). Dieser Unterabschnitt bringt einen systematischen Aufbau zahlreicher derartiger Begriffsbildungen.

Wir beschäftigen uns nun mit speziellen Funktionen, nämlich solchen, deren Definitionsbereich ein n-faches kartesisches Produkt des Zielbereichs ist, also mit der Situation $f : A^n \to A$ – sogenannte n-stellige Operationen auf A.

Definition 2.1.3.1. Sind A, B Mengen, so bezeichnet A^B die Menge aller Abbildungen $f\colon B \to A$.

Im Fall $n = 0 = \emptyset$ steht $A^n = A^0$ also für die Menge aller Abbildungen $f\colon \emptyset \to A$, d. h. für die Menge aller Mengen von geordneten Paaren (a, b) mit $a \in \emptyset$, $b \in A$. Da es keine solchen Paare gibt, die Elemente von f sein könnten, ist die leere Menge das einzige derartige f, d. h. $A^0 = \{\emptyset\}$. Eine 0-stellige Operation $\omega\colon A^0 \to A$ ist also eindeutig bestimmt durch $c := \omega(\emptyset) \in A$. Somit entsprechen die 0-stelligen Operationen auf A

genau den Elementen von A, die wir demnach als die Werte (notgedrungen konstanter) Funktionen $\omega\colon A^0 \to A$ auffassen können. Oft schreiben wir $c \in A$ für die 0-stellige Operation ω mit $\omega(\emptyset) = c$.
Diese Haarspalterei wirkt müßig, hat aber praktischen Nutzen. Denn auf diese Weise lässt sich beispielsweise das neutrale Element einer Gruppe als 0-stellige Operation auffassen, was zur Vereinheitlichung nicht nur der Notation, sondern auch der Konzepte beiträgt.
Eine weitere Besonderheit besteht darin, dass auf der leeren Menge $A = \emptyset$ keine 0-stellige Operation existiert, sehr wohl aber zu jedem $n \geq 1$ genau eine n-stellige Operation ω, nämlich die leere Menge $\emptyset\colon \emptyset^n \to \emptyset$ selbst.
Weniger pathologisch sind Operationen höherer Stelligkeit. Dennoch erscheint eine formale Bemerkung angebracht: Die Notation A^n kann man nämlich auf zwei Arten verstehen, entweder über die (rekursive) Definition $A^1 := A$, $A^{n+1} := A^n \times A$ aus Definition 2.1.1.1 oder gemäß Definition 2.1.3.1 als Menge von Abbildungen $n \to A$. Besonders klar wird die Identifikation dieser formal verschiedenen Objekte, wenn wir das von Neumannsche Modell der natürlichen Zahlen zugrundelegen, also n als Menge $\{0, 1, \ldots, n-1\}$ auffassen. Betrachten wir exemplarisch $n = 2$, so haben wir es also entweder mit der Menge von Paaren (a, a') für $a, a' \in A$ oder mit der Menge von Abbildungen $2 = \{0, 1\} \to A$ zu tun. Identifizieren wir (a, a') mit der Funktion $0 \mapsto a$, $1 \mapsto a'$, so wird klar, dass es egal ist, auf welche Art wir A^2 interpretieren.
Typische Beispiele für 1-stellige Operationen $\omega : A \to A$ sind die Inversenbildung, etwa $\omega : a \mapsto -a$ in einer abelschen Gruppe A, oder die Komplementbildung $\omega : b \mapsto b'$ in einer Booleschen Algebra B. In diesen beiden Fällen schreiben wir auch $-$ bzw. $'$ für ω.
Die klassischen Beispiele n-ärer Operationen liegen im Fall $n = 2$ vor: Addition und Multiplikation, außerdem Schnitt und Vereinigung in Verbänden etc. Meist verwendet man für das Bild des Paares (a, b), $a, b \in A$, unter einer binären Operation ω die Schreibweise $a\,\omega\,b$ statt $\omega(a, b)$ und ersetzt ω durch vertraute Operationssymbole wie $+, \cdot, \cup, \cap, \circ$ etc., also $a + b$ etc. oder, wenn über ω kein Zweifel herrscht, manchmal auch schlicht ab, wie bei der gewöhnlichen Multiplikation. Die Schreibweise A_1A_2 (wobei A_1 und A_2 Teilmengen von A sind) steht dann für das sogenannte *Komplexprodukt* der Mengen A_1 und A_2, bestehend aus allen Elementen a_1a_2 mit $a_1 \in A_1$ und $a_2 \in A_2$.
Für $n \geq 3$ spielen n-stellige Operationen vor allem in der allgemeinen Algebra und, damit eng verwandt, in der Theorie der Klone eine wichtige Rolle. (Unendlichstellige Operationen sind zwar auch denkbar, werden aber hier nicht behandelt.)
Zwecks Zusammenfassung und Weiterentwicklung fassen wir die nächste, entscheidende Definition:

Definition 2.1.3.2. Sei A eine Menge[18] und $n \in \mathbb{N}$. Dann verstehen wir unter einer *n-stelligen* (auch *n-ären*) *Operation* auf A eine Abbildung $\omega\colon A^n \to A$. Im Fall $n = 2$ heißt ω auch eine *binäre Operation*, im Fall $n = 1$ eine *unäre Operation*. Im Fall $n = 0$ spricht man auch von einer *Konstanten* oder einem (durch ω) *ausgezeichneten Element* von A. Ist ω nur auf einer Teilmenge von A^n definiert, spricht man von einer *partiellen*

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

Operation.
Ist I eine Indexmenge und für jedes $i \in I$ eine n_i-stellige Operation $\omega_i \colon A^{n_i} \to A$ auf der Menge A gegeben, so heißt $\mathfrak{A} = (A, \Omega)$ mit $\Omega = (\omega_i)_{i \in I}$ eine *universelle* oder *allgemeine Algebra*. Dabei heißen A die *Trägermenge*, $\tau = (n_i)_{i \in I}$ der *Typ* (oder auch die *Signatur*) und ω_i die *(fundamentalen) Operationen* von $\mathfrak{A}$. Ist $I = \{1, 2, \ldots, k\}$ endlich, so identifizieren wir $\mathfrak{A} = (A, \Omega)$ oft auch mit $(A, \omega_1, \ldots, \omega_k)$ und schreiben für den Typ $\tau = (n_1, \ldots, n_k)$.

Interessante, häufig auftretende Eigenschaften von Operationen und Elementen sind die folgenden.

Definition 2.1.3.3. Auf der Menge A seien 2-stellige Operationen $\circ, +, \cdot, \vee$ und $\wedge$, 1-stellige Operationen $-, ^{-1}$ und $'$ und 0-stellige Operationen (Konstante) $0, 1, e \in A$ gegeben.

1. Die Operation $\circ$ heißt *assoziativ*, wenn alle $a, b, c \in A$ das sogenannte *Assoziativgesetz* erfüllen: $(a \circ b) \circ c = a \circ (b \circ c)$

2. Die Operation $\circ$ heißt *kommutativ*, wenn alle $a, b \in A$ das sogenannte *Kommutativgesetz* erfüllen: $a \circ b = b \circ a$

3. Die Operation $\cdot$ heißt *distributiv* bezüglich $+$, wenn alle $a, b, c \in A$ die sogenannten *Distributivgesetze* erfüllen: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (*Linksdistributivität*) und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ (*Rechtsdistributivität*). Wie üblich werden wir die Konvention *Punkt geht vor Strich* verwenden sowie die Multiplikation nicht immer eigens notieren. Entsprechend vereinfacht sich oben z. B. der Ausdruck $(b \cdot a) + (c \cdot a)$ zu $ba + ca$.

4. Das Element $e \in A$ heißt *linksneutrales Element* bezüglich $\circ$, wenn es $e \circ a = a$ für alle $a \in A$ erfüllt. Entsprechend heißt $e \in A$ *rechtsneutrales Element* bezüglich $\circ$, wenn es $a \circ e = a$ für alle $a \in A$ erfüllt. Ist e sowohl links- als auch rechtsneutrales Element, so heißt e *neutrales Element* bezüglich $\circ$. Ein neutrales Element bezüglich einer additiv notierten Operation $+$ nennt man meistens *Nullelement* (oder schlicht Null) und schreibt dafür 0_A oder schlicht 0, analog *Einselement* 1_A oder 1 für eine multiplikativ notierte Operation $\cdot$.

5. Sei e ein neutrales Element bezüglich $\circ$, und $a \in A$. Wenn es $a^* \in A$ gibt mit $a^* \circ a = e$, dann heißt a *linksinvertierbar*; analog heißt es *rechtsinvertierbar*, wenn es $a^* \in A$ gibt mit $a \circ a^* = e$. In diesen Fällen heißt $a^* \in A$ *Linksinverses* von a bzw. *Rechtsinverses* von a. Wenn a sowohl links- als auch rechtsinvertierbar ist, dann heißt a *invertierbar*. Ein Element, das sowohl Links- als auch Rechtsinverses von a ist, heißt schlicht *Inverses* oder *inverses Element* von a und wird meist als a^{-1} angeschrieben[19]. Wenn für jedes $a \in B \subseteq A$ (oft ist $B = A$, aber nicht

[19] Man beachte, dass nach dieser Definition ein invertierbares Element nicht unbedingt ein Inverses haben muss, weil das Links- und Rechtsinverse verschieden sein können! Für eine (äußerst prominente und wichtige) Situation, in der invertierbare Elemente stets ein Inverses haben, sei auf Proposition 2.1.3.9 verwiesen.

immer) ein Inverses a^{-1} existiert, so heißt die Abbildung $.^{-1} : B \to A$, $a \mapsto a^{-1}$ *Inversenbildung* (bezüglich $\circ$ und e) auf $B \subseteq A$. Für die Inversenbildung bezüglich einer additiv notierten Operation $+$ schreibt man meist $-$, also $-a$ für das inverse Element von a (welches dann durch $a + (-a) = (-a) + a = 0$ charakterisiert ist).

6. Man sagt, $\vee$ und $\wedge$ erfüllen die *Verschmelzungsgesetze*[20], wenn für alle $a, b \in A$ die Gleichungen $a \wedge (a \vee b) = a$ und $a \vee (a \wedge b) = a$ gelten. (De facto treten diese nur für kommutative und assoziative Operationen $\vee$ und $\wedge$ auf.)

7. Ein Element 1 heißt *absorbierend* bezüglich $\vee$, wenn für alle $a \in A$ die Gleichung $a \vee 1 = 1 \vee a = 1$ gilt.

8. Sei 1 absorbierend bezüglich $\vee$ und neutral bezüglich $\wedge$, dual dazu 0 absorbierend bezüglich $\wedge$ und neutral bezüglich $\vee$. Dann heißen a und b *komplementär*, wenn $a \vee b = b \vee a = 1$ und $a \wedge b = b \wedge a = 0$ gilt. Wir sagen auch, dass a ein *Komplement* von b ist und schreiben $b = a'$ sowie $a = b'$.

9. Bezüglich der Operation $\circ$ heißt $a \in A$ *linkskürzbar* (manchmal auch *linksregulär*) bzw. *rechtskürzbar* (*rechtsregulär*), wenn es zu jedem $b \in A$ höchstens ein $c \in A$ gibt mit $a \circ c = b$ oder, äquivalent, wenn $a \circ c_1 = a \circ c_2$ stets $c_1 = c_2$ impliziert (bzw. wenn $c_1 \circ a = c_2 \circ a$ stets $c_1 = c_2$ impliziert). Man sagt, die Operation $\circ$ habe eine der genannten Eigenschaften, wenn alle $a \in A$ sie haben. Liegen sowohl Links- als auch Rechtskürzbarkeit vor, so spricht man von *Kürzbarkeit* schlechthin.

10. Ein Element a heißt *idempotent* bezüglich einer binären Operation $\circ$ auf einer Menge A, wenn $a \circ a = a$. Die Operation $\circ$ heißt idempotent, wenn alle $a \in A$ idempotent bezüglich $\circ$ sind.

UE 45 ► **Übungsaufgabe 2.1.3.4.** (F) Geben Sie eine zusätzlich Voraussetzung an, unter der aus der Existenz eines (Links-, Rechts-) Inversen von a auf die (Links-,Rechts-) Kürzbarkeit von a geschlossen werden kann. ◄ **UE 45**

UE 46 ► **Übungsaufgabe 2.1.3.5.** (V) Man zeige: Ist $\cdot$ eine assoziative Operation auf H, dann gilt für $a_1, \ldots, a_n \in H$, $n \geq 3$, und $r, s \in \mathbb{N}$, $0 \leq r < s \leq n$: ◄ **UE 46**

$$a_1 \cdots a_n = a_1 \cdots a_r (a_{r+1} \cdots a_s) a_{s+1} \cdots a_n.$$

Wo Klammern fehlen, sind die Operationen von links nach rechts auszuführen. Zum Beispiel ist $a_1a_2a_3(a_4a_5a_6)a_7a_8$ Abkürzung für den Ausdruck

$$\big[\big[((a_1a_2)a_3) \cdot \big((a_4a_5)a_6\big)\big] \cdot a_7\big] \cdot a_8 \ .$$

Formulieren Sie Ihren Beweis als Induktionsbeweis, und erklären Sie insbesondere, was die Induktionsvoraussetzung ist. Hinweis: Zeigen Sie zunächst $b \cdot (c_1 \cdots c_n) = bc_1 \cdots c_n$ mit Induktion nach n, dann $a_1 \cdots a_s = a_1 \cdots a_r (a_{r+1} \cdots a_s)$.

[20] englisch: *absorption laws*

Obwohl das Kommutativgesetz insofern einfacher anmutet als das Assoziativgesetz, als es nur zwei Variable involviert, ist Assoziativität jene Eigenschaft, auf die am seltensten verzichtet werden kann. Erstmals ist sie im Zusammenhang mit der mengentheoretischen Vereinigung $\cup$ aufgetreten. Von dort hat sie sich auf die Addition $+$ auf den Zahlenbereichen $\mathbb{N}$ und in weiterer Folge auf $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ übertragen. Ähnliches gilt für das kartesische Produkt $\times$ und die ebenfalls assoziative Multiplikation. Die Wichtigkeit der Assoziativität auch ohne Kommutativität ergibt sich vor allem daraus, dass die Komposition (die Verknüpfung, die Hintereinanderausführung, das Produkt) $\circ$ von Relationen und vor allem Funktionen assoziativ ist. Das wurde in Proposition 2.1.1.4 festgehalten und inspiriert die folgende Definition:

Definition 2.1.3.6. Sei A eine Menge. Es bestehe R_A aus allen binären Relationen auf A, es bestehe M_A aus allen Funktionen $f\colon A \to A$ und es bestehe S_A aus allen bijektiven $f \in M_A$ – insbesondere ist das bezüglich $\circ$ neutrale Element id_A in allen diesen Mengen enthalten. Man nennt $(R_A, \circ, \mathrm{id}_A)$ das *Relationenmonoid* auf A und $(M_A, \circ, \mathrm{id}_A)$ das *symmetrische Monoid* (manchmal auch die *symmetrische Halbgruppe*) auf A. In S_A gibt es sogar zu jedem Element f ein Inverses, nämlich die Umkehrfunktion f^{-1}. Man nennt $(S_A, \circ, \mathrm{id}_A, {}^{-1})$ die *symmetrische Gruppe* auf A. Im Fall $A = \{1, 2, \ldots, n\}$ (oder allgemeiner $|A| = n$) mit $n \in \mathbb{N}$ schreibt man S_n für S_A.

Tatsächlich handelt es sich dabei um Monoide bzw. um eine Gruppe, wie aus der folgenden Definition auch von einigen weiteren wichtigen Klassen von Algebren ersichtlich ist:

Definition 2.1.3.7. Sei $\mathfrak{A} = (A, \Omega)$, $\Omega = (\omega_i)_{i \in I}$, eine universelle Algebra vom Typ $\tau = (n_i)_{i \in I}$ (meist ist I endlich und entsprechend $\tau = (n_1, \ldots, n_k)$).

1. Eine Algebra $\mathfrak{A} = (A, \circ)$ vom Typ (2) heißt *Halbgruppe*, wenn $\circ$ assoziativ ist. Die Halbgruppe heißt *kommutativ*, wenn $\circ$ kommutativ ist.

2. Eine Algebra $\mathfrak{A} = (A, \circ, e)$ vom Typ $(2, 0)$ heißt *Monoid*, wenn $(A, \circ)$ eine Halbgruppe und e neutrales Element bezüglich $\circ$ ist. Das Monoid heißt *kommutativ*, wenn $\circ$ kommutativ ist.

3. Eine Algebra $\mathfrak{A} = (A, \circ, e, {}^{-1})$ vom Typ $(2, 0, 1)$ heißt *Gruppe*, wenn $(A, \circ, e)$ ein Monoid und ${}^{-1}$ eine Inversenbildung bezüglich $\circ$ und e ist. Wenn $\circ$ kommutativ ist, heißt $\mathfrak{A}$ eine *abelsche Gruppe* oder seltener auch *kommutative Gruppe*.

4. Eine Algebra $\mathfrak{A} = (A, +, 0, \cdot)$ vom Typ $(2, 0, 2)$ heißt *Halbring*, wenn $(A, +, 0)$ ein kommutatives Monoid ist, $(A, \cdot)$ eine Halbgruppe und $\cdot$ distributiv bezüglich $+$. Der Halbring heißt *kommutativ*, wenn $\cdot$ kommutativ ist. Gibt es ein Einselement 1 bezüglich $\cdot$, so heißt die Algebra $(A, +, 0, \cdot, 1)$ vom Typ $(2, 0, 2, 1)$ *Halbring mit Einselement*.

5. Eine Algebra $\mathfrak{A} = (A, +, 0, -, \cdot)$ vom Typ $(2, 0, 1, 2)$ heißt *Ring*, wenn $(A, +, 0, \cdot)$ ein Halbring ist und $(A, +, 0, -)$ eine abelsche Gruppe. Ist 1 ein Einselement bezüglich $\cdot$, so heißt die Algebra $(A, +, 0, -, \cdot, 1)$ vom Typ $(2, 0, 1, 2, 0)$ ein *Ring mit*

Einselement, kurz *Ring mit* 1. Ein Ring (mit oder ohne 1) heißt *kommutativ*, wenn er als Halbring kommutativ ist, d. h., wenn die Multiplikation kommutativ ist.

6. Ist $(A, +, 0, -, \cdot, 1)$ ein Ring, so heißt ein Element $a \in A$ *Linksnullteiler* (*Rechtsnullteiler*), wenn es ein $b \in A \setminus \{0\}$ gibt mit $ab = 0$ ($ba = 0$). In jedem der beiden Fälle heißt a ein *Nullteiler*. Der Ring heißt *nullteilerfrei*, wenn 0 der einzige Nullteiler in A ist.

7. Ist die Algebra $\mathfrak{A} = (A, +, 0, -, \cdot, 1)$ vom Typ $(2, 0, 1, 2, 0)$ ein kommutativer Ring mit Einselement, der überdies $1 \neq 0$ erfüllt und nullteilerfrei ist, so heißt $\mathfrak{A}$ *Integritätsbereich*[21]. Besitzen alle $a \in A \setminus \{0\}$ sogar ein multiplikatives Inverses a^{-1}, so heißt $\mathfrak{A}$ ein *Körper*.[22] Ist $\mathfrak{A}$ hingegen ein (nicht notwendigerweise kommutativer) Ring mit $1 \neq 0$, in dem alle Elemente $\neq 0$ ein multiplikatives Inverses haben, spricht man von einem *Schiefkörper* oder *Divisionsring*.[23] Da 0 kein multiplikatives Inverses haben kann, können wir $^{-1}$ nicht als weitere Operation zum Typ hinzufügen – diese Tatsache wird uns noch wiederholt beschäftigen.

8. Sei $\mathfrak{R} = (R, +_R, 0_R, -_R, \cdot_R)$ ein Ring und $\mathfrak{A} = (A, +_A, 0_A, -_A)$ eine abelsche Gruppe. Weiters sei $\Omega = (\omega_r)_{r \in R}$ mit 1-stelligen Operationen ω_r auf A, wobei wir $ra := \omega_r(a)$ für $r \in R$ und $a \in A$ schreiben. Gelten für alle $r, s \in R$ und $a, b \in A$ das Assoziativgesetz $(rs)a = r(sa)$ und beide Distributivgesetze $r(a+b) = ra+rb$ und $(r+s)a = ra+sa$, so heißt die Algebra $\mathfrak{M} = (A, +_A, \Omega)$ vom Typ $(2, (1)_{r \in R})$ ein $\mathfrak{R}$-*Modul* (oder Modul über $\mathfrak{R}$). (Manchmal spricht man auch von einem *Links-Modul*, wobei entsprechend ein *Rechts-Modul* vorliegt, wenn man ar statt ra für $\omega_r(a)$ schreibt und die entsprechenden Gesetze fordert.) Gibt es überdies ein 1_R, welches $\mathfrak{R}_1 = (R, +_R, 0_R, -_R, \cdot_R, 1_R)$ zu einem Ring mit Einselement macht, und gilt $1_R a = a$ für alle $a \in A$, so nennt man $\mathfrak{M}$ einen *unitären* $\mathfrak{R}$-*Modul*.

   Wir werden – obwohl formal nicht ganz korrekt – die Operationen ω_r, $r \in R$, auch oft in einer einzigen Funktion $R \times A \to A$ zusammenfassen, um die Notation zu vereinfachen[24].

   Ist $\mathfrak{K} = \mathfrak{R}_1$ sogar ein Schiefkörper oder Körper, so heißt $\mathfrak{M}$ ein *Vektorraum*[25] über $\mathfrak{K}$ oder kurz ein $\mathfrak{K}$-*Vektorraum*.

9. Eine kommutative Halbgruppe $(A, \wedge)$ heißt *Halbverband*[26], wenn $\wedge$ idempotent ist.

10. Eine Algebra $\mathfrak{A} = (A, \vee, \wedge)$ vom Typ $(2, 2)$ heißt *Verband*[27] (*im algebraischen Sinn*), wenn $(A, \vee)$ und $(A, \wedge)$ kommutative Halbgruppen sind und $\vee$ und $\wedge$ beide Verschmelzungsgesetze erfüllen. (Wir werden uns in Proposition 2.1.4.7 davon

[21] englisch: *integral domain*
[22] englisch: *field*
[23] englisch: *skew field* oder *division ring*
[24] Als formale Definition („Ein R-Modul ist eine abelsche Gruppe A zusammen mit einer Operation $R \times A \to A$ mit den Eigenschaften...“) ist dieser Ansatz unpraktisch, da er nicht in unseren begrifflichen Rahmen passt, in dem die Operationen stets Funktionen $A^n \to A$ sind.
[25] englisch: *vector space*
[26] englisch: *semilattice*
[27] englisch: *lattice*

überzeugen, dass dann sowohl $(A, \vee)$ als auch $(A, \wedge)$ Halbverbände sind.) Gibt es überdies neutrale Elemente $0 \in A$ bezüglich $\vee$ und $1 \in A$ bezüglich $\wedge$, so heißt die Algebra $(A, \vee, \wedge, 0, 1)$ vom Typ $(2, 2, 0, 0)$ ein *beschränkter Verband*. Ein Verband heißt *distributiv*, wenn sowohl $\vee$ distributiv ist bezüglich $\wedge$ als auch $\wedge$ bezüglich $\vee$.

11. Eine *Boolesche Algebra* ist eine Algebra $\mathfrak{A} = (A, \vee, \wedge, 0, 1, ')$ vom Typ $(2, 2, 0, 0, 1)$ mit folgenden Eigenschaften: $(A, \vee, \wedge, 0, 1)$ ist beschränkter distributiver Verband, und für alle $a \in A$ sind a und a' komplementär zueinander.

UE 47 ► **Übungsaufgabe 2.1.3.8.** (F) Sei R ein beliebiger Ring und $r \in R$. Zeigen Sie, dass r genau dann linkskürzbar (rechtskürzbar) ist, wenn r kein Linksnullteiler (Rechtsnullteiler) ist. ◄ **UE 47**

Vor allem in späteren Kapiteln werden wir in der Notation zunehmend schlampig sein, nicht alle Operationen einzeln auflisten und eventuell nicht einmal zwischen Algebra und Trägermenge unterscheiden. Diese Lockerheit im Umgang entspricht den globalen Gepflogenheiten in den meisten Teilen der Mathematik inklusive Algebra und hat unterschiedliche Rechtfertigungen. Zum Beispiel sind das neutrale Element e sowie Inverse bezüglich einer assoziativen binären Operation $\circ$ eindeutig bestimmt, bedürfen daher nicht unbedingt einer expliziten Hervorhebung als 0- bzw. 1-stellige Operationen. Genauer:

Proposition 2.1.3.9. *Sei $\circ$ eine binäre Operation auf der Menge A. Ist von (Links-, Rechts-) Inversen die Rede, so gebe es auch ein neutrales Element $e \in A$ bezüglich $\circ$. Die Begriffe neutral bzw. invers sind stets bezüglich $\circ$ zu verstehen.*

1. *Ist e_l ein linksneutrales Element und e_r ein rechtsneutrales Element, so gilt $e_l = e_r$.*
2. *Es gibt höchstens ein neutrales Element.*
3. *Ist $\circ$ assoziativ und sind a_l und a_r links- bzw. rechtsinvers zu a, so gilt $a_l = a_r$.*
4. *Ist $\circ$ assoziativ, dann sind Inverse (sofern sie existieren) eindeutig bestimmt.*
5. *Ist a_l ein Linksinverses zu a, so ist umgekehrt a ein Rechtsinverses zu a_l. Analog gilt: Ist a_r ein Rechtsinverses zu a, so ist umgekehrt a ein Linksinverses zu a_r. Ist a^{-1} ein Inverses von a, dann ist a ein Inverses von a^{-1}.*
6. *Sei $\circ$ assoziativ. Hat $a \circ b$ ein Linksinverses, so hat b ein Linksinverses. Analog gilt: Hat $a \circ b$ ein Rechtsinverses, so hat a ein Rechtsinverses.*
7. *Sei $\circ$ assoziativ. Haben a und b Linksinverse a_l bzw. b_l, so hat $a \circ b$ das Linksinverse $b_l \circ a_l$. Analog gilt: Haben a und b Rechtsinverse a_r bzw. b_r, so hat $a \circ b$ das Rechtsinverse $b_r \circ a_r$.*
8. *Sei $\circ$ assoziativ und e ein neutrales Element. Außerdem gebe zu jedem $a \in A$ (mindestens) ein linksinverses Element a_l. Dann ist $a_l = a^{-1}$ für alle $a \in A$ sogar ein inverses Element und $(A, \circ, e, .^{-1})$ eine Gruppe.*

Beweis.

1. In $e_l = e_l \circ e_r = e_r$ gilt die erste Gleichheit, weil e_l linksneutral, die zweite, weil e_r rechtsneutral ist.

2. Sind e und e' neutrale Elemente, so ist e linksneutral und e' rechtsneutral, nach Aussage 1 also $e = e'$.

3. Es gilt $a_l = a_l \circ e = a_l \circ (a \circ a_r) = (a_l \circ a) \circ a_r = e \circ a_r = a_r$.

4. Je zwei Inverse sind sowohl links- als auch rechtsinvers, müssen nach der dritten Aussage also übereinstimmen.

5. Die erste Behauptung ist aus $a_l \circ a = e$ unmittelbar ersichtlich, die zweite aus $a \circ a_r = e$, die dritte aus $a \circ a^{-1} = a^{-1} \circ a = e$.

6. Ist c_l ein Linksinverses von $a \circ b$, so folgt $(c_l \circ a) \circ b = c_l \circ (a \circ b) = e$, also ist $c_l \circ a$ ein Linksinverses von b. Analog beweist man die zweite Aussage.

7. Die Rechnung $(b_l \circ a_l) \circ (a \circ b) = b_l \circ (a_l \circ a) \circ b = b_l \circ e \circ b = b_l \circ b = e$ zeigt die erste Behauptung, analog $(a \circ b) \circ (b_r \circ a_r) = e$ die zweite.

8. Nach Voraussetzung gibt es sowohl ein Linksinverses a_l für a als auch ein Linksinverses $(a_l)_l$ für a_l. Damit gilt $a = e \circ a = ((a_l)_l \circ a_l) \circ a = (a_l)_l \circ (a_l \circ a) = (a_l)_l \circ e = (a_l)_l$, folglich $a \circ a_l = (a_l)_l \circ a_l = e$. Also ist a_l auch rechtsinvers für a.

□

Man könnte Gruppen alternativ beispielsweise auch definieren als Algebren $(G, \circ)$ vom Typ (2), mit einer assoziativen Operation $\circ$, zu der es ein neutrales Element e gibt und sodass zu allen $g \in G$ Linksinverse existieren. Wegen Proposition 2.1.3.9 sind sowohl e als auch sämtliche Inverse eindeutig bestimmt. Somit gibt es eine und nur eine Möglichkeit, was in der entsprechenden Gruppe $(G, \circ, e, ^{-1})$ im Sinn von Definition 2.1.3.7 die 0-stellige Operation e und die 1-stellige Operation $^{-1}$ sein müssen. Wir werden Gruppen in den meisten Fällen als Algebren vom Typ $(2, 0, 1)$ auffassen und nicht als Algebren vom Typ (2).

2.1.4. Relationale Strukturen

Inhalt in Kurzfassung: Erlaubt man auf (Trägermengen von) Algebren, wie sie im vorangegangenen Unterabschnitt definiert wurden, zusätzlich Relationen, so erhält man relationale Strukturen. Wichtige Beispiele sind (halb)geordnete (Halb-)Gruppen oder auch Verbände, die man sowohl in einem algebraischen als auch in einem ordnungstheoretischen Sinn auffassen kann.

Nicht alle wichtigen Strukturelemente aus den Zahlenbereichserweiterungen können innerhalb des bisherigen Rahmens für universelle Algebren wiedergegeben werden. Vor

allem gilt das für die Ordnungsrelation. Um ähnliche Flexibilität wie bei den Operationen zu haben, ziehen wir Relationen beliebiger endlicher Stelligkeit in Betracht. (Die meisten betrachteten Relationen werden aber zweistellig sein.)
Relationale Strukturen ergeben sich nun als natürliche Verallgemeinerung universeller Algebren, indem wir zusätzlich zu den Operationen auch noch Relationen zulassen.

Definition 2.1.4.1. Seien ω_i, $i \in I$, n_i-stellige Operationen auf A und ρ_j, $j \in J$, m_j-stellige Relationen auf A. Zur Abkürzung schreiben wir $\Omega = (\omega_i)_{i\in I}$ und $R = (\rho_j)_{j\in J}$. Dann heißt $\mathfrak{A} = (A, \Omega, R)$ eine *relationale Struktur* vom *Typ* (oder auch von der *Signatur*) (τ, σ) mit *Trägermenge* A, wobei $\tau = (n_i)_{i\in I}$ und $\sigma = (m_j)_{j\in J}$. Ist $J = \emptyset$, so fassen wir $\mathfrak{A}$ als universelle Algebra (A, Ω) auf und nennen $\mathfrak{A}$ auch *rein algebraisch*. Ist $I = \emptyset$, so nennen wir $\mathfrak{A} = (A, R)$ auch *rein relational*.
Fassen wir in einer relationalen Struktur (A, Ω, R) jedes $\omega_i \colon A^{n_i} \to A$ als Teilmenge $\omega_i \subseteq A^{n_i} \times A = A^{n_i+1}$ auf, also als $(n_i + 1)$-stellige Relation auf A, so nennen wir die resultierende Struktur $(A, \Omega \cup R)$ die *zugehörige rein relationale Struktur*.

Wie schon bei universellen Algebren schreiben wir bei endlichen Indexmengen I und J alle ω_i und ρ_j meist einzeln an, etwa $\mathfrak{A} = (\mathbb{R}, +, 0, -, \cdot, 1, \leq)$ im Fall des angeordneten Körpers der reellen Zahlen. Hier ist also $|I| = 5$ und $|J| = 1$. Die wichtigsten Typen relationaler Strukturen, die nicht rein algebraisch sind, sind tatsächlich von ähnlicher Art, bei denen sich nämlich eine oder mehrere algebraische Operationen mit einer (Halb-)Ordnungsrelation verbinden: (halb)geordnete Gruppen und, darauf aufbauend, geordnete Ringe und Körper. In Abschnitt 3.5 werden wir noch interessante Beispiele dazu betrachten. Hier begnügen wir uns mit der folgenden Definition.

Definition 2.1.4.2. Unter einer *halbgeordneten Halbgruppe* verstehen wir eine relationale Struktur $\mathcal{H} = (H, \circ, \leq)$, wobei $(H, \circ)$ eine Halbgruppe ist, $(H, \leq)$ eine Halbordnung ist und zusätzlich das *Monotoniegesetz* gilt: Für $a, b, c \in H$ folgt aus $a \leq b$ stets $c \circ a \leq c \circ b$ und $a \circ c \leq b \circ c$. Ist $(H, \leq)$ zusätzlich eine Totalordnung, heißt $\mathcal{H}$ eine *geordnete Halbgruppe*.
$\mathcal{G} = (G, \circ, e, ^{-1}, \leq)$ heißt eine *(halb)geordnete Gruppe*, wenn $(G, \circ, e, ^{-1})$ eine Gruppe ist und $(G, \circ, \leq)$ eine (halb)geordnete Halbgruppe.
$\mathcal{K} = (K, +, 0, -, \cdot, 1, \leq)$ heißt ein *(an)geordneter Körper*, wenn $(K, +, 0, -, \cdot, 1)$ ein Körper ist, $(K, +, 0, -, \leq)$ eine geordnete Gruppe und wenn überdies auch das Monotoniegesetz für die Multiplikation gilt: Für alle $a, b, c \in K$ folgt aus $a \leq b$ und $c \geq 0$ auch $a \cdot c \leq b \cdot c$ und[28] $c \cdot a \leq c \cdot b$.

Einen wichtigen Sonderfall stellen Halbverbände $(H, \vee)$ oder $(H, \wedge)$ und Verbände $(V, \vee, \wedge)$ dar. Sie tragen bereits per se eine Halbordnungsstruktur. Und umgekehrt lassen sich (Halb-)Verbände im ordnungstheoretischen Sinn auch algebraisch umdeuten.

Definition 2.1.4.3. Sei $(P, \leq)$ eine partielle Ordnung.

[28] Das zweite Monotoniegesetz folgt wegen der Kommutativität der Multiplikation aus dem ersten; der Vollständigkeit halber listen wir beide auf.

(1) P (genauer: $(P, \leq)$) heißt *Vereinigungs-Halbverband im ordnungstheoretischen Sinn*, wenn jede 2-elementige Teilmenge $\{a, b\}$ eine kleinste obere Schranke $\sup\{a, b\}$ hat. Statt $\sup\{a, b\}$ schreibt man auch oft $a \vee b$ und bezeichnet dies als Vereinigung[29] von a und b.

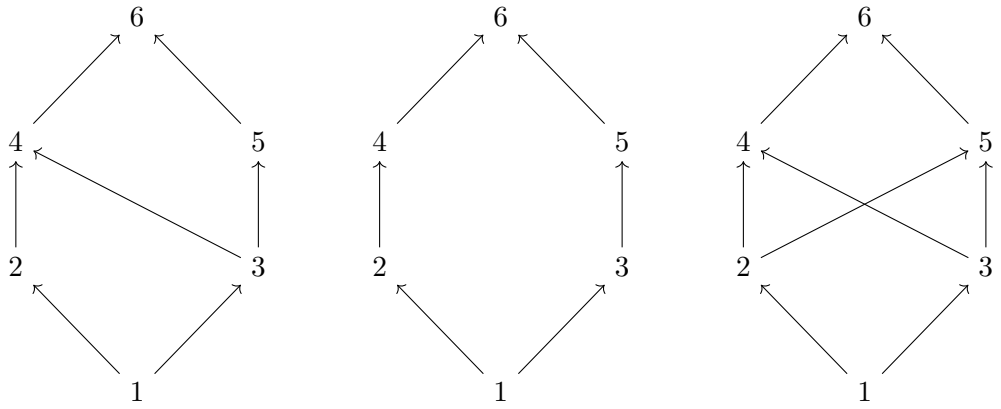
(2) *Schnitt-Halbverbände im ordnungstheoretischen Sinn* sind analog definiert. Statt $\inf\{a, b\}$ schreibt man oft $a \wedge b$ und bezeichnet dies als Schnitt[30] von a und b.

(3) P heißt *Verband* oder *verbandsgeordnete Menge*, wenn P sowohl Schnitt- als auch Vereinigungs-Halbverband ist.

(4) P heißt *vollständig*, wenn jede Teilmenge von P sowohl eine kleinste obere als auch eine größte untere Schranke hat. (Siehe dazu auch Proposition 2.1.2.17.)

(5) P heißt *bedingt vollständig*[31], wenn jede nichtleere *beschränkte* Teilmenge (jede nichtleere Teilmenge, die sowohl eine obere als auch eine untere Schranke hat) auch eine kleinste obere Schranke (also ein Supremum) und eine größte untere Schranke (also ein Infimum) hat.

Beispiel 2.1.4.4. Auf $M = \{1, 2, 3, 4, 5, 6\}$ seien drei Halbordnungsrelationen $\leq_a$, $\leq_b$ und $\leq_c$ durch die folgenden Hasse-Diagramme definiert:



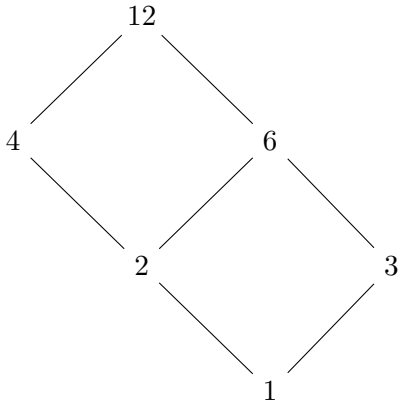
Die ersten beiden sind verbandsgeordnet, $(M, \leq_c)$ aber nicht. Zum Beispiel ist $\inf_a\{2, 3\} = 1$ und $\sup_a\{2, 3\} = 4$, und $\sup_b\{2, 3\} = 6$. Hingegen ist $(M, \leq_c)$ *nicht* verbandsgeordnet: $\sup_c\{2, 3\}$ existiert nicht, da die Menge $\{2, 3\}$ die oberen Schranken 4, 5 und 6 und damit keine kleinste obere Schranke besitzt.

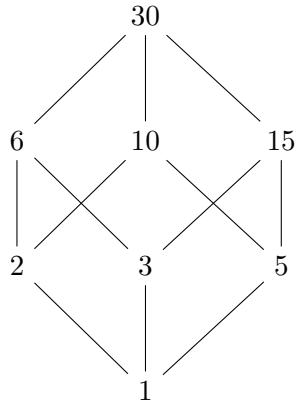
Beispiel 2.1.4.5. Teilerverbände $(T_n, \mathrm{ggT}, \mathrm{kgV})$ mit $T_n := \{t \in \mathbb{N}^+ \mid t \text{ teilt } n\}$, $n \in \mathbb{N}^+$. Hassediagramm von T_{12} und von T_{30}:

[29] englisch: *join*

[30] englisch: *meet*

[31] Um schleppende Formulierungen zu vermeiden, werden bedingt vollständige lineare Ordnungen, die offensichtlich nicht beschränkt sind, oft einfach als vollständig bezeichnet, wie wir dies etwa bei vollständig angeordneten Körpern getan haben.





UE 48 ▶ **Übungsaufgabe 2.1.4.6.** (F) $(P, \leq)$ ist genau dann ein Verband, wenn jede nichtleere endliche Teilmenge eine kleinste obere und eine größte untere Schranke hat. ◀ **UE 48**

(Halb-)Verbände im ordnungstheoretischen Sinn können in solche im algebraischen Sinn übersetzt werden, weshalb man meist nur von (Halb-)Verbänden spricht. Das beruht auf folgenden Aussagen.

Proposition 2.1.4.7.

(1) *Sei $(P, \leq)$ ein Vereinigungs-Halbverband im ordnungstheoretischen Sinn, d. h. eine Halbordnung, in der zu je zwei Elementen $a, b \in P$ das Supremum $a \vee_{\leq} b := \sup\{a, b\}$ existiert. Dann ist $(P, \vee_{\leq})$ ein Vereinigungs-Halbverband im algebraischen Sinn (siehe Definition 2.1.3.7).*

(2) *Sei umgekehrt $(P, \vee)$ ein Halbverband im algebraischen Sinn (d. h. eine idempotente kommutative Halbgruppe). Dann wird $(P, \leq_{\vee})$ zu einem Vereinigungshalbverband in ordnungstheoretischen Sinn, wenn man $a \leq_{\vee} b :\Leftrightarrow a \vee b = b$ definiert.*

(3) *Für (Vereinigungs-)Halbverbände sind die beiden Zuordnungen $\leq \mapsto \vee_{\leq}$ und $\vee \mapsto \leq_{\vee}$ zueinander invers. (Halbverbände im algebraischen und ordnungstheoretischen Sinn sind also im Wesentlichen dieselben Objekte.)*

(4) *Sei $(P, \leq)$ ein Verband im ordnungstheoretischen Sinn. Dann ist $(P, \vee_{\leq}, \wedge_{\leq})$ ein Verband im algebraischen Sinn, wenn $\vee_{\leq}$ wie in Teil 1 als Supremum definiert ist und $\wedge_{\leq}$ analog als Infimum: $a \wedge_{\leq} b := \inf\{a, b\}$.*

(5) *Ist $(P, \vee, \wedge)$ ein Verband im algebraischen Sinn, dann sind $(P, \vee)$ und $(P, \wedge)$ Halbverbände im algebraischen Sinn.*

(6) *Sei $(P, \vee, \wedge)$ ein Verband im algebraischen Sinn. Dann ist $a \vee b = b$ äquivalent zu $a \wedge b = a$, und $(P, \leq_{\vee})$ ist ein Verband im ordnungstheoretischen Sinn.*

(7) *Ist $(P, \vee, \wedge)$ ein Verband, so ist $\wedge$ durch $\vee$ eindeutig bestimmt und umgekehrt.*

(8) *Für Verbände sind die beiden Zuordnungen $\leq \mapsto (\vee_{\leq}, \wedge_{\leq})$ und $(\vee, \wedge) \mapsto \leq_{\vee}$ aus Teil 4 bzw. Teil 6 zueinander invers. (Verbände im algebraischen und ordnungstheoretischen Sinn sind also im Wesentlichen dieselben Objekte.)*

UE 49 ► Übungsaufgabe 2.1.4.8. (V) Beweisen Sie Proposition 2.1.4.7. **◄ UE 49**

In den allermeisten Fällen werden wir Proposition 2.1.4.7 in der folgenden wesentlich kürzeren Fassung verwenden:

Folgerung 2.1.4.9. *Auf einer Menge V entsprechen Verbandsstrukturen im ordnungstheoretischen Sinn jenen im algebraischen Sinn auf kanonische bijektive Weise, indem $(V, \leq)$ auf $(V, \vee_\leq, \wedge_\leq)$ und umgekehrt $(V, \vee, \wedge)$ auf $(V, \leq_{\vee,\wedge})$ abgebildet wird. Dabei ist $a \leq_{\vee,\wedge} b$ genau dann, wenn $a \vee b = b$ oder, äquivalent, $a \wedge b = a$ gilt.*

Beweis. Umformulierung der letzten Aussage in Proposition 2.1.4.7. □

Bei Anwendungen von Folgerung 2.1.4.9 werden wir statt $\leq_{\vee,\wedge}$ meist nur $\leq$ und statt $\vee_\leq$ und $\wedge_\leq$ meist $\vee$ bzw. $\wedge$ schreiben.

UE 50 ► Übungsaufgabe 2.1.4.10. (B) Für jeden Verband $(V, \wedge, \vee)$ sind $(V, \wedge)$ und $(V, \vee)$ Halbverbände (vgl. Proposition 2.1.4.7, Aussage 5). Geben Sie ein Beispiel einer Struktur $(V, \wedge, \vee)$ an, die kein Verband ist, wo aber $(V, \wedge)$ und $(V, \vee)$ Halbverbände sind. (Hinweis: Es gibt eine endliche Struktur mit sehr wenigen Elementen, die diese Bedingungen erfüllt.) **◄ UE 50**

UE 51 ► Übungsaufgabe 2.1.4.11. (F) Sei $(V, \vee, \wedge)$ ein Verband, der $\forall x, y, z : (x \wedge z) \vee (y \wedge z) = (x \vee y) \wedge z$ erfüllt. Zeigen Sie, dass dann auch $\forall x, y, z : (x \vee z) \wedge (y \vee z) = (x \wedge y) \vee z$ gilt, also dass V distributiv ist. (Hinweis: Schreiben Sie $+$ für $\vee$ und $\cdot$ für $\wedge$.) **◄ UE 51**

UE 52 ► Übungsaufgabe 2.1.4.12. (F,B) Man bestimme die Hasse-Diagramme aller Verbände mit höchstens 6 Elementen (bis auf Isomorphie). (Es genügt nicht, alle solchen Verbände zu finden; Sie müssen auch beweisen, dass Ihre Liste vollständig ist, und dass keine zwei Verbände auf Ihrer Liste zueinander isomorph sind.)
Hinweis: Wenn Sie aus einem 6-elementigen Verband ein Element entfernen, ist die verbleibende Ordnung im Allgemeinen kein Verband.
Hinweis: Gehen Sie systematisch vor. Schaffen Sie Übersichtlichkeit, indem Sie Verbände nach irgendeinem unter Isomorphie invarianten Merkmal klassifizieren, zum Beispiel: Länge der längsten Kette. Größe der größten Antikette. Anzahl der oberen Nachbarn des kleinsten Elements. Etc. Wenn es zu viele Strukturen mit einem gemeinsamen Merkmal gibt, verwenden Sie ein weiteres Merkmal. **◄ UE 52**

2.1.5. Homomorphismen zwischen Algebren

Inhalt in Kurzfassung: Verallgemeinert man den Begriff der linearen Abbildung zwischen Vektorräumen auf beliebige (universelle) Algebren, so stößt man auf jenen der Homomorphismen. Bei den meisten Abbildungen, die in der Algebra von Interesse sind,

handelt es sich um solche.

Im Zuge der Zahlenbereichserweiterungen, vor allem der Eindeutigkeitssätze, haben wir exzessiv vom Begriff des Isomorphismus, der stärksten Form strukturverträglicher Abbildungen, Gebrauch gemacht. Nun sollen einige wichtige Varianten davon systematisch zusammengestellt werden. Wir beginnen mit jener Bedingung, die an die meisten in der Algebra vorkommenden Abbildungen gestellt wird, der Homomorphiebedingung.

Definition 2.1.5.1. Seien die Mengen A, B, die Abbildung $f\colon A \to B$ und zwei n-stellige Operationen ω^A und ω^B auf A bzw. B gegeben ($n \in \mathbb{N}$). Dann heißt f *verträglich* mit ω^A und ω^B (oder auch f, ω^A und ω^B *miteinander verträglich*), wenn für alle $a_1, \ldots, a_n \in A$ die sogenannte *Homomorphiebedingung*

$$f(\,\omega^A(a_1, \ldots, a_n)\,) = \omega^B(\,f(a_1), \ldots, f(a_n)\,)$$

erfüllt ist. In diesem Fall heißt f auch *Homomorphismus* bezüglich ω^A und ω^B. Schreibt man $f^{[n]}$ für die Abbildung $f^{[n]}\colon A^n \to B^n$, $(a_1, \ldots, a_n) \mapsto (f(a_1), \ldots, f(a_n))$, so lässt sich die Homomorphiebedingung auch kurz schreiben als $f \circ \omega^A = \omega^B \circ f^{[n]}$.

$$\begin{array}{ccc} A^n & \xrightarrow{\omega^A} & A \\ {\scriptstyle f^{[n]}}\downarrow & & \downarrow{\scriptstyle f} \\ B^n & \xrightarrow{\omega^B} & B \end{array}$$

Seien $\mathfrak{A} = (A, \Omega^{\mathfrak{A}})$ mit $\Omega^{\mathfrak{A}} = (\omega_i^{\mathfrak{A}})_{i\in I}$ und $\mathfrak{B} = (B, \Omega^{\mathfrak{B}})$ mit $\Omega^{\mathfrak{B}} = (\omega_i^{\mathfrak{B}})_{i\in I}$ universelle Algebren vom selben Typ $\tau = (n_i)_{i\in I}$. Die Abbildung $f\colon A \to B$ sei für alle $i \in I$ verträglich mit $\omega_i^{\mathfrak{A}}$ und $\omega_i^{\mathfrak{B}}$. Dann heißt f auch *Homomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$, symbolisch $f\colon \mathfrak{A} \to \mathfrak{B}$. So ein Homomorphismus f heißt überdies:

- *Monomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ (oder auch eine *isomorphe Einbettung*[32] von $\mathfrak{A}$ in $\mathfrak{B}$), wenn $f\colon A \to B$ injektiv ist.
- *Epimorphismus* von $\mathfrak{A}$ nach (auf) $\mathfrak{B}$, wenn $f\colon A \to B$ surjektiv ist.
- *Isomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ (oder auch zwischen $\mathfrak{A}$ und $\mathfrak{B}$), wenn $f\colon A \to B$ bijektiv ist. Gibt es einen Isomorphismus zwischen $\mathfrak{A}$ und $\mathfrak{B}$, so heißen $\mathfrak{A}$ und $\mathfrak{B}$ *isomorph*, und man schreibt $\mathfrak{A} \cong \mathfrak{B}$.
- *Endomorphismus* von $\mathfrak{A}$, wenn $\mathfrak{A} = \mathfrak{B}$ gilt.
- *Automorphismus* von $\mathfrak{A}$, wenn f ein Isomorphismus $\mathfrak{A} \to \mathfrak{A}$ ist.

Obwohl in der Bezeichnung *Isomorphismus* die Gleichheit der Struktur zum Ausdruck kommt, wurde in der Definition nicht eigens gefordert, dass die Umkehrabbildung f^{-1} eines Isomorphismus f auch ein Homomorphismus ist. Der Grund ist die dritte Behauptung in:

[32] Der Name kommt daher, dass – wie wir später sehen werden – das Bild $f(A)$ die Trägermenge einer sogenannten *Unteralgebra* $f(\mathfrak{A})$ von $\mathfrak{B}$ ist. Dabei ist f ein Isomorphismus von $\mathfrak{A}$ nach $f(\mathfrak{A})$. Somit haben wir eine „Kopie“ von $\mathfrak{A}$ gefunden, die in $\mathfrak{B}$ enthalten ist. Anders gesagt lässt sich $\mathfrak{A}$ auf strukturgleiche (also isomorphe) Art in $\mathfrak{B}$ einbetten.

Proposition 2.1.5.2.

(1) *Sind* $f\colon \mathfrak{A} \to \mathfrak{B}$ *und* $g\colon \mathfrak{B} \to \mathfrak{C}$ *Homomorphismen, so auch ihre Komposition* $h := g \circ f\colon \mathfrak{A} \to \mathfrak{C}$*, analog für Mono-, Epi-, Iso-, Endo- und Automorphismen.*

(2) *Die Identität* id_A *ist ein Automorphismus jeder Algebra* $\mathfrak{A}$ *mit Trägermenge* A*.*

(3) *Ist* $f\colon A \to B$ *bijektiv und strukturverträglich mit den* n*-stelligen Operationen* ω^A *auf* A *und* ω^B *auf* B*, so ist die Umkehrfunktion* $f^{-1}\colon B \to A$ *strukturverträglich mit* ω^B *und* ω^A*.*

(4) *Die Endomorphismen einer Algebra* $\mathfrak{A}$ *bilden (bezüglich der Komposition* $\circ$ *und dem neutralen Element* id_A*) ein Monoid, das sogenannte* Endomorphismenmonoid $\mathrm{End}(\mathfrak{A})$ *von* $\mathfrak{A}$*.*

(5) *Die Automorphismen einer Algebra* $\mathfrak{A}$ *bilden (bezüglich der Komposition* $\circ$*, dem neutralen Element* id_A *und der Inversenbildung von Funktionen) eine Gruppe, die sogenannte* Automorphismengruppe $\mathrm{Aut}(\mathfrak{A})$ *von* $\mathfrak{A}$*.*

UE 53 ▶ Übungsaufgabe 2.1.5.3. (V,W) Beweisen Sie Proposition 2.1.5.2. **◀ UE 53**

2.1.6. Homomorphismen zwischen relationalen Strukturen

Inhalt in Kurzfassung: Will man den Begriff des Homomorphismus von rein algebraischen auf relationale Strukturen verallgemeinern, so bieten sich eine schwächere und eine stärkere Variante an (entspricht Monotonie in eine oder in beide Richtungen), die nun kurz zu besprechen sind.

Wenn man das Konzept des Homomorphismus von rein algebraischen Strukturen auf relationale überträgt, wird eine zusätzliche Unterscheidung nötig, weil die Entsprechung der dritten Aussage in Proposition 2.1.5.2 nicht mehr gilt. Ein einfaches Beispiel: Betrachten wir auf der Potenzmenge $A := \mathfrak{P}(M)$ der Menge M einerseits die Relation $\subseteq$ und andererseits die Relation $\leq$, die durch $A \leq B$ für $|A| \leq |B|$ definiert sei. Dann ist die identische Abbildung id_A verträglich mit diesen Relationen in dem schwachen Sinn, dass aus $A \subseteq B$ stets $A \leq B$ folgt, nicht aber im starken Sinn, dass auch die Umkehrung gilt. Allgemein definiert man:

Definition 2.1.6.1. Seien zwei n-stellige Relationen ρ^A und ρ^B auf A bzw. B gegeben. Dann sagen wir, f sei *schwach* bzw. *stark (struktur-)verträglich* mit ρ^A und ρ^B, wenn für alle $a_1, \ldots, a_n \in A$ aus $(a_1, \ldots, a_n) \in \rho^A$ stets $(\, f(a_1), \ldots, f(a_n)\,) \in \rho^B$ folgt bzw. wenn diese beiden Aussagen sogar äquivalent sind.
Ist $n = 2$ und sind $\leq^A$ und $\leq^B$ Halbordnungsrelationen auf A bzw. auf B, so heißt eine Abbildung, die mit $\leq^A$ und $\leq^B$ schwach strukturverträglich ist, auch *monoton* oder *monoton wachsend*. Eine Abbildung, die mit $\leq^A$ und $\geq^B$ schwach strukturverträglich ist, heißt auch *antiton* oder *monoton fallend*. Eine Abbildung, die mit den strikten Halbordnungsrelationen $<^A$ und $<^B$ schwach strukturverträglich ist, heißt auch *streng monoton wachsend*. Eine Abbildung, die mit den strikten Halbordnungsrelationen $<^A$ und $>^B$ schwach strukturverträglich ist, heißt auch *streng monoton fallend*.

UE 54 ► **Übungsaufgabe 2.1.6.2.** (E) Interpretieren Sie für diese Aufgabe n-stellige Operationen ω^A, ω^B als $n+1$-stellige Relationen ρ^A, ρ^B. Zeigen Sie: Die Homomorphiebedingung $f(\,\omega^A(a_1,\ldots,a_n)\,) = \omega^B(\,f(a_1),\ldots,f(a_n)\,)$ lässt sich als schwache Strukturverträglichkeit bezüglich ρ^A und ρ^B deuten, nicht aber als starke. Lediglich für injektives f sind beide Aussagen äquivalent. ◄ **UE 54**

Offensichtlich gilt:

Proposition 2.1.6.3. *Ist $f\colon A \to B$ bijektiv und stark strukturverträglich mit den n-stelligen Relationen ρ^A auf A und ρ^B auf B, so ist die Umkehrfunktion $f^{-1}\colon B \to A$ stark strukturverträglich mit ρ^B und ρ^A.*

Im Hinblick auf Umkehrfunktionen ist bei Relationen also starke Strukturverträglichkeit das passende Konzept, während sich bei nicht notwendig bijektiven Homomorphismen von Algebren schwache Strukturverträglichkeit als angemessen erweist.

UE 55 ► **Übungsaufgabe 2.1.6.4.** (F) Prüfen Sie für Abbildungen $f\colon A \to B$, $g\colon B \to C$, n-stellige Operationen $\omega^A, \omega^B, \omega^C$ und für m-stellige Relationen ρ^A, ρ^B, ρ^C (jeweils auf A, B bzw. C) nach: ◄ **UE 55**

1. Sind f und g schwach strukturverträglich mit ρ^A und ρ^B bzw. ρ^B und ρ^C, so ist $g \circ f$ schwach strukturverträglich mit ρ^A und ρ^C.
2. Sind f und g stark strukturverträglich mit ρ^A und ρ^B bzw. ρ^B und ρ^C, so ist $g \circ f$ stark strukturverträglich mit ρ^A und ρ^C.

Wegen der Notwendigkeit der Unterscheidung zwischen schwacher und starker Strukturverträglichkeit sind verschiedene Definitionen eines Homomorphismus zwischen relationalen Strukturen möglich. Um keinen überflüssigen terminologischen Ballast anzusammeln, wollen wir uns damit begnügen, zwischen relationalen Strukturen (in unserem Fall zwischen geordneten Gruppen und Körpern) nur *Isomorphismen* und *isomorphe Einbettungen* (*Monomorphismen*) zu betrachten und dabei stets starke Strukturverträglichkeit zu verlangen. Wegen Aussage 3 in Proposition 2.1.5.2 führt diese Sprechweise zu keinen Mehrdeutigkeiten.

UE 56 ► **Übungsaufgabe 2.1.6.5.** (F) Prüfen Sie für Abbildungen $f\colon A \to B$, $g\colon B \to C$ und relationale Strukturen $\mathfrak{A} = (A, \Omega^{\mathfrak{A}}, R^{\mathfrak{A}})$, $\mathfrak{B} = (B, \Omega^{\mathfrak{B}}, R^{\mathfrak{B}})$ und $\mathfrak{C} = (C, \Omega^{\mathfrak{C}}, R^{\mathfrak{C}})$ nach: ◄ **UE 56**

1. Sind f und g beide injektiv und stark strukturverträglich, so auch $g \circ f\colon \mathfrak{A} \to \mathfrak{C}$.
2. Die Automorphismen von $\mathfrak{A}$ bilden (bezüglich der Komposition $\circ$, dem neutralen Element id_A und der Inversenbildung von Funktionen) eine Gruppe, genannt die Automorphismengruppe $\mathrm{Aut}(\mathfrak{A})$.

Bemerkung: Die Übungsaufgaben 2.1.5.3 und 2.1.6.4 sollen verwendet und nicht nochmals bewiesen werden.

UE 57 ► **Übungsaufgabe 2.1.6.6.** (B,E) Man zeige: Jede abzählbare dichte (zwischen je zwei Elementen liegen weitere) Kette ohne größtes und ohne kleinstes Element ist ordnungsisomorph zu den rationalen Zahlen mit der natürlichen Ordnung. ◄ **UE 57**
Hinweis: Verwenden Sie die Aufzählung $\mathbb{Q} = \{q_n \mid n \in \mathbb{N}\}$. Zeigen Sie zunächst, dass Sie jeden partiellen Isomorphismus p, das ist ein Isomorphismus $p : A \to B$ zwischen endlichen Teilmengen von $\mathbb{Q}$, zu einem partiellen Isomorphismus fortsetzen können, dessen Definitions- und Bildbereich echt größer ist.

2.1.7. Klassifikation modulo Isomorphie als Paradigma

Inhalt in Kurzfassung: Unter dem Gesichtspunkt der Algebra unterscheiden sich zwei isomorphe Strukturen nicht wesentlich. Dieser Gesichtspunkt lässt sogenannte Klassifikationssätze (schwächer: Darstellungssätze) besonders interessant erscheinen. Es geht nun darum, was genau darunter zu verstehen ist.

Eines der Hauptanliegen der Algebra besteht in der Klassifikation algebraischer oder sogar beliebiger relationaler Strukturen nach Isomorphie. In der Modelltheorie treten gewisse noch allgemeinere Aspekte in den Vordergrund, weshalb man die Modelltheorie sinnvollerweise als ein Teilgebiet der Logik ansieht und nicht mehr der Algebra. In Letzterer orientiert man sich an der aus der Linearen Algebra bekannten Klassifikation der Vektorräume mittels Dimension. Ausgangspunkt für uns ist die folgende einfache Beobachtung:

Proposition 2.1.7.1. *Auf jeder Klasse $\mathcal{K}$ von relationalen Strukturen desselben Typs ist $\cong$ eine Äquivalenzrelation.*

UE 58 ► **Übungsaufgabe 2.1.7.2.** (F) Folgern Sie Proposition 2.1.7.1 aus bereits Bekanntem. ◄ **UE 58**

Ein Klassifikationssatz bezieht sich auf eine bestimmte Klasse $\mathcal{K}$ von relationalen Strukturen (Algebren), die typischerweise alle denselben Typ haben, und gibt an, wie man aus jeder Äquivalenzklasse bezüglich $\cong$ auf $\mathcal{K}$ (siehe Proposition 2.1.7.1) einen (möglichst kanonischen) Vertreter erhält. Es folgen einige typische Beispiele für Klassen $\mathcal{K}$ mit Klassifikationssätzen. Manche davon sind bereits bekannt, manche werden wir erst in späteren Kapiteln oder gar nicht in dieser Vorlesung kennen lernen.

- Mengen: Die Isomorphismen sind die bijektiven Abbildungen. Zwei Mengen sind also genau dann isomorph, wenn sie die gleiche Kardinalität (Mächtigkeit) κ haben. Ein kanonisches Vertretersystem ist die Klasse der sogenannten Kardinalzahlen (siehe Unterabschnitt A.5.3.
- Vektorräume V über einem festen Körper K (siehe Satz 1.3.3.4): Die Isomorphismen sind die bijektiven linearen Abbildungen. Je zwei Vektorräume sind genau dann isomorph, wenn sie dieselbe Dimension haben. Also gibt es zu jeder Kardinalzahl κ bis auf Isomorphie genau einen Vektorraum V_κ über K mit der Dimension κ. Dabei kann V_κ als Menge aller κ-tupel mit Eintragungen aus K, von denen nur endlich viele $\neq 0$ sind, gewählt werden.

- zyklische Gruppen (siehe Satz 3.2.4.9): Die Isomorphismen sind Gruppenisomorphismen. Je zwei zyklische Gruppen sind genau dann isomorph, wenn sie die gleiche Mächtigkeit haben. Als Mächtigkeiten treten genau $\aleph_0$ (abzählbar unendlich) und die natürlichen Zahlen $n = 1, 2, \ldots$ auf. Kanonische Vertreter sind die Gruppen $\mathbb{Z}$ und die Restklassengruppen[33] $C_n = \mathbb{Z}/n\mathbb{Z}$.
- endliche abelsche Gruppen (siehe Satz 3.3.4.2): Bis auf Isomorphie treten genau die endlichen direkten Produkte von endlichen zyklischen Gruppen auf, wobei man Eindeutigkeit erzielt, wenn man nur jene von Primzahlpotenzordnung als Bausteine verwendet.
- endlich erzeugte abelsche Gruppen (siehe Satz 7.4.3.2): Jede endlich erzeugte abelsche Gruppe ist endliches Produkt von zyklischen Gruppen, genauer: lässt sich eindeutig in der Form $\mathbb{Z}^n \times G$ darstellen, wobei G endlich und zyklisch ist und $n \geq 0$. Auf G ist dann Satz 3.3.4.2 anwendbar.
- endliche einfache Gruppen: Der berühmte (und komplizierte) Klassifikationssatz sprengt den Rahmen der Vorlesung bei Weitem.
- Primkörper (siehe Satz 6.1.1.8): Alle Primkörper (das sind definitionsgemäß Körper, die nur sich selbst als Unterkörper enthalten) sind bis auf Isomorphie gegeben durch die Restklassenkörper $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ mit einer Primzahl p (Charakteristik p) und den Körper $\mathbb{Q}$ der rationalen Zahlen (Charakteristik 0).
- endliche Körper (siehe Satz 6.3.1.2): Zu jeder Primzahlpotenz p^n, $p \in \mathbb{P}$, $n = 1, 2, \ldots$, gibt es bis auf Isomorphie genau einen Körper mit p^n Elementen. Umgekehrt hat jeder endliche Körper als Kardinalität eine Primzahlpotenz $p^n > 1$. Wie genau all diese Körper erhalten werden können (nämlich als Zerfällungskörper des Polynoms $x^{p^n} - x$ über dem Primkörper mit p Elementen), ist eines der wichtigsten Resultate dieser Vorlesung.
- endliche Boolesche Algebren (siehe Satz 3.6.7.6): Bis auf Isomorphie gibt es zu jeder Zweierpotenz 2^n, $n \in \mathbb{N}$, genau eine Boolesche Algebra mit 2^n Elementen, z. B. die Potenzmengenalgebra einer n-elementigen Menge (kanonischer Vertreter: die Menge $n = \{0, 1, \ldots, n-1\}$). Umgekehrt hat jede endliche Boolesche Algebra als Kardinalität eine Zweierpotenz. Diesen Klassifikationssatz kann man als Spezialfall des Darstellungssatzes von Stone sehen, oder aus dem Hauptsatz über endliche abelsche Gruppen folgern.

Etwas schwächer sind sogenannte Darstellungssätze. Von ihnen verlangt man etwas weniger als von einem Klassifikationssatz. Und zwar genügt es, wenn für die Klasse $\mathfrak{K}$ von abstrakten Strukturen eine Teilklasse $\mathfrak{T}$ angegeben werden kann derart, dass es erstens zu jeder Struktur aus $\mathfrak{K}$ eine isomorphe aus $\mathfrak{T}$ gibt, und dass zweitens die Grundmengen, Operationen und Relationen der Strukturen in $\mathfrak{T}$ in konkreterer Weise als die in $\mathfrak{K}$ beschrieben werden können (statt abstrakten Gruppen in $\mathfrak{K}$ betrachtet man in $\mathfrak{T}$ z. B. nur Gruppen von linearen Abbildungen auf Vektorräumen, wobei die Multiplikation einfach die Verknüpfung von Abbildungen ist).

[33] Die Gruppe $\mathbb{Z}/n\mathbb{Z}$ wird oft auch mit $\mathbb{Z}_n$ bezeichnet; wir reservieren dieses Symbol aber für den Restklassen*ring* modulo n.

Wünschenswert ist auch die Angabe einer Strukturanalyse, mit Hilfe derer zu einer gegebenen Struktur aus $\mathfrak{K}$ eine isomorphe aus $\mathfrak{T}$ konstruiert werden kann. Im Gegensatz zu einem Klassifikationssatz ist es anhand eines Darstellungssatzes typischerweise jedoch nicht möglich, genau einen kanonischen Vertreter jedes Isomorphietyps anzugeben.
Wichtige Beispiele sind:

- Monoide und Gruppen: Der *Darstellungssatz von Cayley* für Monoide (siehe Satz 3.1.2.5) besagt, dass jedes Monoid isomorph ist zu einem Untermonoid des symmetrischen Monoids, analog für Gruppen (siehe Satz 3.2.5.1).
- Boolesche Algebren (siehe Satz 3.6.8.17): Nach dem (allgemeinen) Darstellungssatz von Stone ist jede Boolesche Algebra isomorph zu einer Mengenalgebra, also zu einer Unteralgebra einer Potenzmengenalgebra.

Der Beweis des Satzes von Cayley ist sehr leicht, der des Satzes von Stone deutlich anspruchsvoller. Sein Beweis zeigt zwar, wie man zu einer beliebig vorgegebenen Booleschen Algebra eine (in diesem Fall kanonische) isomorphe Mengenalgebra erhält. Isomorphe, aber verschiedene Boolesche Algebren können jedoch (anders wäre es bei einem echten Klassifikationssatz) zu nicht identischen (wenn auch natürlich isomorphen) Mengenalgebren führen.

2.1.8. Terme, Termalgebra, Gesetze und Varietäten

Inhalt in Kurzfassung: Ähnlich wie in der Logik ist es in der (universellen) Algebra unausweichlich, auch die formale Sprache zum Gegenstand zu machen. Dazu braucht es strenge Definitionen von scheinbar selbstverständlichen Begriffen wie Term etc. Von herausragendem Interesse ist in diesem Zusammenhang die Termalgebra (über gegebenen Mengen von Variablen und Operationssymbolen) sowie die Tatsache, dass beliebige Variablenbelegungen mit Elementen einer Algebra des entsprechenden Typs zu einem eindeutigen Homomorphismus auf der Termalgebra, dem sogenannten Einsetzungshomomorphismus, fortgesetzt werden können.

Bisher haben wir Ausdrücke der Gestalt $x + y$ ausschließlich als Bezeichnung für ein Objekt verwendet, in diesem Fall die Summe von x und y unter der Annahme, dass x und y ebenso bekannt sind wie die Operation $+$. Nun sollen die Ausdrücke (die schriftlichen Zeichenreihen oder, noch genauer, die ihnen entsprechenden abstrakten mathematischen Objekte) selbst zum Gegenstand gemacht werden. Vorgegeben denken wir uns dabei Mengen von Symbolen, aus denen die *Variablen* x und y sowie das *Operationssymbol* $+$ entnommen sind. Das führt wie folgt zum Begriff des Terms.

Definition 2.1.8.1. Sei (τ) mit $\tau = (n_i)_{i\in I}$ ein Typ allgemeiner Algebren und X eine Menge, deren Elemente wir *Variablen* nennen. Jedem $i \in I$ ordnen wir ein sogenanntes *Operationssymbol* ω_i zu.[34] (Alle Symbole $x \in X$ und ω_i, $i \in I$, seien paarweise verschieden und auch verschieden von allen später noch auftretenden syntaktischen Symbolen.)

[34] Wir könnten ω_i mit i identifizieren, den Index i also selbst als Operationssymbol verwenden. Weil dies aber zu sehr ungewohnten Schriftbildern führt, schreiben wir ω_i, wenn wir die Rolle als Operationssymbol betonen wollen.

Jene ω_i mit $n_i = 0$ heißen auch *Konstantensymbole*, für die wir gelegentlich c_i schreiben. Die Menge $T = T(X, \tau)$ der *Terme* der zugeordneten Sprache ist definiert als Vereinigung $T := \bigcup_{k\in\mathbb{N}} T_k$ der Mengen T_k, $k \in \mathbb{N}$, die rekursiv wie folgt definiert sind:

- $T_0 := X$.
- $T_{k+1} = T_k \cup S_k$, wobei S_k als die Menge aller Symbolketten $\omega_i(t_1, \ldots, t_{n_i})$ mit $n_i \geq 0$ und $t_1, \ldots, t_{n_i} \in T_k$ definiert ist:

$$T_{k+1} := T_k \cup \{\omega_i(t_1, \ldots, t_{n_i}) \mid i \in I, t_1, \ldots, t_{n_i} \in T_k\}.$$

  (Man beachte, dass insbesondere $\Omega_0 := \{\omega_i \in \Omega \mid n_i = 0\} \subseteq T_1$.)

Für $t \in T$ heißt $\min\{k \in \mathbb{N} \mid t \in T_k\}$ auch die *Stufe* von t.
Die n_i-stelligen Operationen $\omega_i^{\mathfrak{T}} : (t_1, \ldots, t_{n_i}) \mapsto \omega_i(t_1, \ldots, t_{n_i})$ auf T machen $\mathfrak{T} = \mathfrak{T}(X, \tau) = (T, (\omega_i^{\mathfrak{T}})_{i\in I})$ zu einer Algebra vom Typ τ, der sogenannten *Termalgebra*, die von Ω, τ und X induziert wird.

Die Stufen der Terme – und vor allem die Tatsache, dass für $t = \omega_i(t_1, \ldots, t_{n_i})$ die Terme t_i eine strikt niedrigere Stufe haben als t – machen es möglich, Induktionsbeweise nach der Stufe k eines Terms zu führen, wie wir das beispielsweise in Satz 2.1.8.4 tun werden. Eine einfachere Anwendung ist die rekursive Definition der Menge $v(t)$ von Variablen, die – wie man sagt – *im Term t vorkommen*: Ist $t = x \in X$ von der Stufe 0, so sei $v(t) := \{x\}$. Ist $t = \omega(t_1, \ldots, t_n)$ von der Stufe k mit Termen t_i der Stufen $k_i < k$, so sei $v(t) := v(t_1) \cup \ldots \cup v(t_n)$. Wir vereinbaren, dass die Schreibweise $t = t(x_1, \ldots, x_n)$ mit Variablen $x_1, \ldots, x_n \in X$ die Inklusion $v(t) \subseteq \{x_1, \ldots, x_n\}$ bedeute, dass also alle Variablen, die in t vorkommen, unter den x_i, $i = 1, \ldots, n$ zu finden sind.

Es folgen nun einige Bemerkungen zur Codierung von Termen, die weniger aus algebraischer als aus informatischer Sicht von Interesse sind.
Die Symbolketten aus Definition 2.1.8.1 sind so aufgebaut, dass das Operationssymbol ω_i den Termen $t_1, \ldots, t_{n_i}$, auf die es angewendet wird, vorangestellt wird. Man spricht deshalb von *Präfixnotation*.[35] Für zweistellige Operationen ist es meist üblich, stattdessen, d. h. statt $\omega(x, y)$, die sogenannte *Infixnotation* $x\ \omega\ y$ zu verwenden, bei der das Operationssymbol zwischen den Operanden steht; insbesondere dann, wenn das Operationssymbol ω nicht durch einen Buchstaben, sondern durch ein abstraktes Symbol wie $+, \circ, *$ etc. dargestellt wird. In *Postfixnotation*[36] (wie sie etwa in der Programmiersprache FORTH oder der Seitenbeschreibungssprache PostScript verwendet wird) stellt man das Operationssymbol hinter die Operanden.

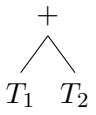
Beispiel 2.1.8.2. In der folgenden Tabelle stehen in jeder Zeile äquivalente Ausdrücke: zuerst in Präfixnotation, dann Infix, dann Postfix.

Präfix	Infix	Postfix
$\sin(+(a, b))$	$\sin(a + b)$	$a, b, +, \sin$
$+(\sin(a), b)$	$\sin(a)+b$	$a, \sin, b, +$
$*(+(a, b), -(c, d))$	$(a + b) * (c - d)$	$a, b, +, c, d, -, *$

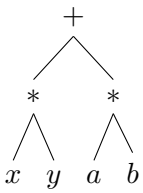
[35] auch: *polnische Notation*
[36] auch: umgekehrte polnische Notation, reverse Polish notation, RPN

Die Präfixnotation in der ersten Zeile lässt sich von links nach rechts so lesen: „Sinus der Summe von a und b.“ Die Postfixnotation kann man als Rezept oder Algorithmus von links nach rechts so lesen: „Man nehme a und b, addiere die beiden, und bilde von diesem Zwischenresultat den Sinus.“

In der Praxis wird meist eine gemischte Notation verwendet: Für einstellige Operationen wird meistens Präfixnotation verwendet ($\sin(x)$, $-x$), gelegentlich aber auch Postfixnotation (x^{-1}, $n!$). Die Komplementbildung von Mengen wird manchmal durch Präfixnotation ($-A$ oder $\sim A$) ausgedrückt, manchmal in Postfixnotation (A' oder A^c). Binäre Operationssymbole werden meist in Infixnotation geschrieben, und in Präfixform wenn sie durch Buchstaben oder Buchstabenketten beschrieben werden: $x \wedge y$, aber $\min(x, y)$. Die Unterscheidung zwischen Prä-, In- und Postfixnotation spielt beim praktischen Umgang mit formalen Sprachen eine Rolle, ist rein mathematisch aber von mäßigem Interesse. Bemerkenswert ist, dass bei ausschließlicher Verwendung der Postfixnotation (ebenso wie bei ausschließlicher Verwendung der Präfixnotation) keine Klammern notwendig sind: auch ohne Klammern lassen sich Terme eindeutig[37] decodieren. (Man spricht von *eindeutiger Lesbarkeit*.) Daher lässt man Klammern bei verschachtelten Funktionen gelegentlich weg, z. B. $fg(x)$ oder fgx statt $f(g(x))$.
Oft ist es sinnvoll, sich Terme nicht als lineare Zeichenkette vorzustellen, sondern in Form eines *Baumdiagramms*: Ein Term t, der eine Summe darstellt (also $t_1 + t_2$, bzw. $+(t_1, t_2)$ bzw. $t_1\, t_2\, +$), wird in einen Baum (genauer: einen *planaren Wurzelbaum*[38]) transformiert, dessen Wurzel (die traditionell oben geschrieben wird) mit dem Symbol + markiert ist; von der Wurzel führt ein Zweig nach links und einer nach rechts; an diesen beiden Zweigen hängen die Bäume T_1 und T_2, die t_1 und t_2 repräsentieren (wir lesen die Argumente von + also „von links nach rechts“):



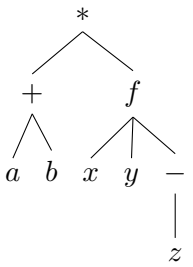
Der Term $(x * y) + (a * b)$ wird durch den Baum



[37] solange die Stelligkeit der Funktionssymbole bekannt ist. Wenn f einstellig und g zweistellig ist, dann ist mit $f\, g\, x\, y$ der Ausdruck $f(g(x, y))$ gemeint; wenn aber f zweistellig und g einstellig ist, dann ist $f(g(x), y)$ gemeint.

[38] Ein *Baum* ist ein zusammenhängender kreisfreier Graph. Ein *Wurzelbaum* ist ein Baum mit einem ausgezeichneten Knoten, der Wurzel. In einem Wurzelbaum hat jeder Knoten außer der Wurzel einen „Vorgänger“, nämlich den nächsten Knoten auf dem Weg zur Wurzel; die anderen Nachbarn des Knotens heißen Nachfolger. In einem planaren Baum sind die Nachfolger jedes Knotens linear geordnet.

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



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

UE 59 ► Übungsaufgabe 2.1.8.3. (F) Ergänzen Sie die folgende Tabelle. Dabei seien $*$ und $+$ zweistellige Operationen, cos und sin einstellig, i nullstellig und a, b, c Variablen. **◄ UE 59**

Präfix	Infix	Postfix
$+ \exp * a\, b\, c$		
	$\exp(-a * b)$	
	$\exp(-a) * b$	
		$a \cos i\, b \sin * +$

Geben Sie für jeden dieser Ausdrücke auch ein Baumdiagramm an.

Wir kehren nun wieder zurück zu algebraisch wesentlichen Gesichtspunkten. Die bereits erwähnte Decodierbarkeit (eindeutige Lesbarkeit) des Baumes ist für die folgende, auf Kapitel 4 abzielende *universelle Eigenschaft* der Termalgebra entscheidend. Sie bringt eine höchst vertraute Tatsache zum Ausdruck: Jeder Term kann eindeutig ausgewertet werden, wenn man jede der in ihm auftretenden Variablen mit einem Wert belegt. Will man streng axiomatisch auf Basis beispielsweise der mengentheoretischen ZFC-Axiome vorgehen, so sind gewisse Feinheiten zu beachten. Dazu ein kurzer Exkurs.
Versteht man Terme als Symbolketten, so könnte man beispielsweise mit einem 2-stelligen Operationssymbol ω_2 und zwei Variablen x, y den Term $t = \omega_2(x, y)$ bilden. Fasst man diesen Term im Sinne der Präfixnotation als Kette der Symbole ω_2, x und y auf und weiter eine Kette als 3-Tupel, so wäre nach der rekursiven Definition 2.1.1.1 unser Term gegeben durch $t = (\omega_2, x, y) = ((\omega_2, x), y)$. Auf Basis des durch ZFC garantierten mengentheoretischen Universums ist jedes Objekt selbst wieder eine Menge. So könnte es ein einstelliges Operationssymbol ω_1 geben, das zufällig jene Menge ist, die das geordnete Paar (ω_2, x) darstellt. Dann wäre $t = (\omega_2, x, y) = ((\omega_2, x), y) = (\omega_1, y)$. Somit hätte der Term t neben der Interpretation als $\omega_2(x, y)$ auch jene als $\omega_1(y)$, und die eindeutige Lesbarkeit wäre verletzt. In der streng axiomatischen Mengentheorie hat man also Sorge zu tragen, dass solche ungewollten Koinzidenzen nicht auftreten können, indem man die Symbole, aus denen sich Terme aufbauen lassen, mit entsprechendem Vorbedacht wählt.

Das ist möglich, wir wollen uns mit den technischen Details dazu aber nicht beschäftigen, sondern einfach darauf vertrauen, dass eindeutige Lesbarkeit garantiert ist. Damit lässt sich der folgende für die Termalgebra zentrale Satz beweisen.

Satz 2.1.8.4. *Sei X eine Variablenmenge, $\tau = (n_i)_{i\in I}$ ein Typ universeller Algebren, $\mathfrak{T} = \mathfrak{T}(X,\tau)$ die zugehörige Termalgebra und $\mathfrak{A}$ eine Algebra des Typs τ mit Trägermenge A und Operationen $(\omega_i^{\mathfrak{A}})_{i\in I}$.*
*Dann gibt es zu jeder Abbildung $\alpha\colon X \to A$ (*Variablenbelegung*) einen eindeutigen Homomorphismus $\bar{\alpha}\colon T \to A$, der α fortsetzt, den von α induzierten* Einsetzungshomomorphismus *von der Termalgebra $\mathfrak{T}$ nach $\mathfrak{A}$.*
(In der Sprechweise von Kapitel 4 lässt sich sagen: Die Termalgebra $\mathfrak{T}$ ist frei über der Variablenmenge X in der Klasse aller Algebren vom Typ τ.)

Beweis. Sei also $\alpha\colon X \to A$ vorgegeben. Wie in Definition 2.1.8.1 bezeichne T_k die Menge der Terme der Stufe k und T ihre Vereinigung. Wir konstruieren rekursiv Abbildungen $\alpha_k\colon T_k \to A$ derart, dass $\bar{\alpha} := \bigcup_{k\in\mathbb{N}} \alpha_k$ die behauptete Eigenschaft hat. Und zwar setzen wir $\alpha_0(x) := \alpha(x)$ für $x \in X$. Damit ist $\alpha_0\colon T_0 \to A$ definiert. Für $k \geq 0$ sei nun $\alpha_k\colon T_k \to A$ bereits definiert. Wir setzen $\alpha_{k+1}(t) := \alpha_k(t)$ sofern $t \in T_k$. Andernfalls ist $t \in T_{k+1} \setminus T_k$, also t von der Stufe $k+1$. Im Spezialfall $k = 0$ und $n_i = 0$ setzen wir $\alpha_1(\omega_i) := \omega_i^{\mathfrak{A}}$. Ansonsten hat t die Gestalt $t = \omega_i(t_1,\ldots,t_{n_i})$ mit $i \in I$ und $t_1,\ldots,t_{n_i} \in T_k$. Dann setzen wir $\alpha_{k+1}(t) := \omega_i^{\mathfrak{A}}(\alpha_k(t_1),\ldots,\alpha_k(t_{n_i}))$. Auf diese Weise wird α_{k+1} eine wohldefinierte[39] Abbildung $T_{k+1} \to A$, die $\alpha_k\colon T_k \to A$ fortsetzt. Somit ist auch die Vereinigung $\bar{\alpha} := \bigcup_{k\in\mathbb{N}} \alpha_k : T \to A$ eine wohldefinierte Abbildung. Zu zeigen bleibt, dass $\bar{\alpha}\colon \mathfrak{T} \to \mathfrak{A}$ ein Homomorphismus ist und als solcher, der α fortsetzen soll, eindeutig bestimmt.
Zur Homomorphiebedingung: Sei $i \in I$ beliebig und $t_1,\ldots,t_{n_i} \in T$. Wir betrachten den Term $t := \omega_i(t_1,\ldots,t_{n_i})$. Zu zeigen ist

$$\bar{\alpha}(t) = \bar{\alpha}(\omega_i(t_1,\ldots,t_{n_i})) = \omega_i^{\mathfrak{A}}(\bar{\alpha}(t_1),\ldots,\bar{\alpha}(t_{n_i})).$$

Ist $n_i = 0$, so gilt diese Beziehung aufgrund der speziellen Definition von $\alpha_1 \subseteq \bar{\alpha}$ für diesen Fall. Für $n_i > 0$ sei $k := \max\{k_1,\ldots,k_{n_i}\}$, wobei k_j die Stufe von t_j sei ($j = 1,\ldots,n_i$). Dann ist t von der Stufe $k+1$. Nach Konstruktion gilt daher tatsächlich

$$\bar{\alpha}(t) = \alpha_{k+1}(t) = \omega_i^{\mathfrak{A}}(\alpha_k(t_1),\ldots,\alpha_k(t_{n_i})) = \omega_i^{\mathfrak{A}}(\bar{\alpha}(t_1),\ldots,\bar{\alpha}(t_{n_i})).$$

Zur Eindeutigkeit: Sei $\bar{\beta} : \mathfrak{T} \to \mathfrak{A}$ ein weiterer Homomorphismus mit $\bar{\beta}(x) = \bar{\alpha}(x) = \alpha(x) = \beta(x)$ für alle $x \in X$. Diese Voraussetzung besagt gerade, dass $\bar{\alpha}$ und $\bar{\beta}$ auf T_0 übereinstimmen. Mit Induktion nach k folgt, dass dies auf allen T_k, $k \in \mathbb{N}$ gilt, woraus $\bar{\beta} = \bar{\alpha}$ folgt – denn der Induktionsschritt ist eine unmittelbare Anwendung der Homomorphiebedingung: Gilt die Behauptung für ein beliebiges $k \in \mathbb{N}$ und ist $t := \omega_i(t_1,\ldots,t_{n_i})$ ein Term der Stufe $k+1$, dann folgt aus der Homomorphiebedingung

$$\bar{\beta}(t) = \bar{\beta}(\omega_i(t_1,\ldots,t_{n_i})) = \omega_i^{\mathfrak{A}}(\bar{\beta}(t_1),\ldots,\bar{\beta}(t_{n_i})),$$

[39] An dieser Stelle fließt die eindeutige Lesbarkeit ein. Streng genommen geht man auch hier mit Induktion vor: Aus dem Term t sind sowohl ω_i (als erstes Symbol der Zeichenkette) als auch die t_j (z. B. als Eintragungen eines n_i-tupels) ablesbar, und die t_j sind nach Induktionsannahme eindeutig lesbar.

was nach Induktionsannahme tatsächlich mit

$$\omega_i^{\mathfrak{A}}(\bar{\alpha}_k(t_1),\ldots,\alpha_k(t_{n_i})) = \omega_i^{\mathfrak{A}}(\bar{\alpha}(t_1),\ldots,\bar{\alpha}(t_{n_i})) = \bar{\alpha}(t)$$

übereinstimmt. Man beachte, dass dies nach Konstruktion auch für $n_i = 0$ gilt, denn $\bar{\beta}(\omega_i) = \omega_i^{\mathfrak{A}} = \bar{\alpha}(\omega_i)$. □

Die obige rekursive Definition der Menge $v(t)$ aller Variablen, die im Term t vorkommen, führt zu den folgenden interessanten Tatsachen: Mit Induktion nach der Stufe von t zeigt man, dass $v(t)$ stets endlich ist. Bereits oben haben wir eingeführt, dass wir im Falle $v(t) \subseteq \{x_1,\ldots,x_n\}$ auch $t = t(x_1,\ldots,x_n)$ schreiben. Diese Notation ist gerechtfertigt, denn man sieht gleichfalls sehr leicht, dass für eine Variablenbelegung $\alpha\colon X \to A$ der Wert $\bar{\alpha}(t)$ nur von den $a_i := \alpha(x_i)$ für $i = 1,\ldots,n$ abhängt, d. h. von der Belegung nur für jene Variablen, die in t vorkommen. Man schreibt dafür deshalb $t(a_1,\ldots,a_n) := t^{\mathfrak{A}}(a_1,\ldots,a_n) := \bar{\alpha}(t)$ und nennt ihn den *Wert* des Terms t.

UE 60 ► Übungsaufgabe 2.1.8.5. (V) Beweisen Sie die hier behaupteten Aussagen: **◄ UE 60**

1. In jedem Term t kommen nur endlich viele Variablen vor.
2. Der Wert $\bar{\alpha}(t)$ eines Terms t für eine Variablenbelegung $\alpha\colon X \to A$ hängt nur von den $\alpha(x)$ für jene $x \in X$ mit $x \in v(t)$ ab, also für die Variablen, die in t vorkommen.

Mit Hilfe des Einsetzungshomomorphismus lässt sich zum Beispiel die Gültigkeit des Assoziativgesetzes $(xy)z = x(yz)$ in einer Algebra mit einer binären Operation so formulieren: Für jede Variablenbelegung $\alpha : X \to A$ mit $X = \{x,y,z\}$ liefert der α nach Satz 2.1.8.4 eindeutig fortsetzende Einsetzungshomomorphismus $\bar{\alpha}$ für die beiden Terme $t_1 = (xy)z$ und $t_2 = x(yz)$ denselben Wert $\bar{\alpha}(t_1) = \bar{\alpha}(t_2) \in A$. Dies in offensichtlicher Weise verallgemeinernd definieren wir:

Definition 2.1.8.6. Sei τ ein Typ von Algebren, X eine Variablenmenge und $\mathfrak{T} = \mathfrak{T}(X,\tau)$ die dadurch induzierte Termalgebra mit Trägermenge T.
Ein *Gesetz* (oder auch eine *Gleichung*) γ (für den Typ τ) ist ein Paar $(t_1,t_2) \in T^2$, für das wir auch[40] $t_1 \approx t_2$ schreiben.
Ist überdies $\mathfrak{A}$ eine Algebra vom Typ τ mit Trägermenge A, so sagen wir, dass in $\mathfrak{A}$ das Gesetz $\gamma = (t_1,t_2)$ *gilt*, wenn für alle $\alpha\colon X \to A$ der induzierte Einsetzungshomomorphismus $\bar{\alpha}\colon \mathfrak{T} \to \mathfrak{A}$ (siehe Satz 2.1.8.4) für t_1 und t_2 dasselbe Bild $\bar{\alpha}(t_1) = \bar{\alpha}(t_2) \in A$ liefert. Wir schreiben in diesem Fall $\mathfrak{A} \models t_1 \approx t_2$.
Ist $\Gamma \subseteq T^2$ eine Menge von Gesetzen, so heißt die Klasse $\mathcal{V}(\Gamma)$ aller Algebren vom Typ τ, in denen alle Gesetze $\gamma \in \Gamma$ gelten, die durch Γ bestimmte *Varietät*, und man nennt

[40] Wenn $x_1,\ldots,x_n$ eine Liste aller Variablen ist, die in t_1 und/oder t_2 vorkommen, dann könnte man das Gesetz $t_1 \approx t_2$ auch ausführlicher in der erststufigen Sprache der Prädikatenlogik in der Form $\forall x_1 \cdots \forall x_n : t_1 = t_2$ schreiben. Die Schreibweise mit dem Symbol $\approx$ soll darauf hinweisen, dass die Terme t_1 und t_2 nicht als formale Objekte gleich sind, sondern nur ihre Auswertungen an allen Elementen der betrachteten Algebra übereinstimmen.

τ auch den *Typ der Varietät*. Statt „Varietät“ sagt man auch[41,42,43] *gleichungsdefinierte Klasse*.

Beispiele 2.1.8.7. Direkt nach Definition sind die folgenden Klassen von Strukturen Varietäten: Halbgruppen, Monoide, Gruppen, (kommutative) Ringe (mit 1), (distributive) Verbände, Boolesche Algebren, Vektorräume über einem festen Körper K, (unitäre) Moduln über einem festen Ring R.
Keine Varietäten bilden die Klasse der Integritätsbereiche, die Klasse der Körper oder auch die Klasse der endlichen Gruppen. Intuitiv ist dies jeweils klar – bei Körpern müssten wir beispielsweise $\forall x \neq 0 : x \cdot x^{-1} = 1$ fordern, allerdings ist $^{-1}$ ja kein Operationensymbol. Außerdem müssten wir bei den Variablenbelegungen stets 0 ausnehmen. Und wie sollte man Nullteilerfreiheit oder Endlichkeit überhaupt als Gesetz formulieren? Natürlich ist das kein Beweis, dass *keine* Menge von Gesetze die entsprechende Klasse liefert. Dies werden wir erst in den Unterabschnitten 2.2.1 sowie 2.2.2 nachholen, siehe Beispiele 2.2.1.5, 2.2.2.10, 2.2.3.25, 2.2.5.2.

Wichtig insbesondere im Kontext der universellen Algebra ist die Tatsache, dass man einen Term über einem gegebenen Typ auch als Funktion auf einer beliebigen Algebra dieses Typs auffassen kann, als sogenannte *Termfunktion*. Beispielsweise induziert der Term $t = t(x_1, x_2, x_3) = (x_1x_2)x_3$ auf jeder Algebra $\mathfrak{A}$ vom Typ (2) die Funktion $t^{\mathfrak{A}} : (a_1, a_2, a_3) \mapsto (a_1a_2)a_3$, wobei das Rechnen mit Termfunktionen dem Rechnen mit Termen entspricht. Wenngleich dies intuitiv unmittelbar einsichtig ist, lohnt doch ein genauerer Blick im Rahmen einer Übungsaufgabe. In Übungsaufgabe 2.2.2.11, wenn wir Unteralgebren und direkte Produkte zur Verfügung haben, werden wir dieses Thema nochmals unter anderem Blickwinkel beleuchten.

UE 61 ► **Übungsaufgabe 2.1.8.8.** (F+) Sei $\tau = (n_i)_{i\in I}$ ein Typ von Algebren und sei $X = \{x_1, x_2, \dots\}$ eine Variablenmenge. Sei weiters $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I})$ eine Algebra vom Typ τ und $\mathfrak{T}^{(k)} := \mathfrak{T}(X^{(k)}, \tau)$ für $k \geq 1$ die von $X^{(k)} = \{x_1, \dots, x_k\}$ und τ induzierte Termalgebra. ◄ **UE 61**

(1) Geben Sie eine formale Definition (rekursiv nach der Stufe) der von einem Term $t \in T^{(k)}$ auf der Algebra $\mathfrak{A}$ induzierten Termfunktion $t^{\mathfrak{A}} : A^k \to A$ an.

(2) Seien $a_1, \dots, a_k \in A$ und sei $\alpha_{a_1,\dots,a_k} : X^{(k)} \to A$ die durch $x_i \mapsto a_i$ definierte Variablenbelegung. Zeigen Sie $t^{\mathfrak{A}}(a_1, \dots, a_n) = \bar{\alpha}_{a_1,\dots,a_n}(t)$ für den gemäß Satz 2.1.8.4 gegebenen Einsetzungshomomorphismus $\bar{\alpha}_{a_1,\dots,a_n}$. Schließen Sie, dass für Terme $t_1, t_2 \in T^{(k)}$ die Aussage $\mathfrak{A} \models t_1 \approx t_2$ äquivalent zu $t_1^{\mathfrak{A}} = t_2^{\mathfrak{A}}$ ist.

(3) Bezeichne $T^{(k),\mathfrak{A}} = \{t^{\mathfrak{A}} \mid t \in T^{(k)}\}$ die Menge der k-stelligen Termfunktionen. Wir definieren Operationen $\omega_i^{\mathfrak{T}^{(k)},\mathfrak{A}}$ der Stelligkeit n_i auf $T^{(k),\mathfrak{A}}$ wie folgt:

[41] Die Nomenklatur ist nicht immer eindeutig. Das Wort „Varietät“ wird manchmal für gleichungsdefinierte Klassen verwendet, manchmal für Klassen von Algebren, die unter H, S und P abgeschlossen sind, siehe Definition 4.1.1.1. Wegen des Satzes von Birkhoff 4.1.7.1 liefern diese Definitionen aber äquivalente Begriffe.

[42] Achtung! In der algebraischen Geometrie wird das Wort „Varietät“ für einen völlig anderen Begriff verwendet, nämlich für die Menge aller Lösungen eines polynomialen Gleichungssystems.

[43] englisch: *variety*

$\omega_i^{\mathfrak{T}^{(k)},\mathfrak{A}}(t_1^{\mathfrak{A}},\ldots,t_{n_i}^{\mathfrak{A}}) := \omega_i^{\mathfrak{A}} \circ (t_1^{\mathfrak{A}},\ldots,t_{n_i}^{\mathfrak{A}})$ für $t_1^{\mathfrak{A}},\ldots,t_{n_i}^{\mathfrak{A}} \in T^{(k),\mathfrak{A}}$, also explizit

$$\omega_i^{\mathfrak{T}^{(k)},\mathfrak{A}}(t_1^{\mathfrak{A}},\ldots,t_{n_i}^{\mathfrak{A}}) : (a_1,\ldots,a_k) \mapsto \omega_i^{\mathfrak{A}}\left(t_1^{\mathfrak{A}}(a_1,\ldots,a_k),\ldots,t_{n_i}^{\mathfrak{A}}(a_1,\ldots,a_k)\right).$$

Zeigen Sie $\omega_i^{\mathfrak{T}^{(k)},\mathfrak{A}}(t_1^{\mathfrak{A}},\ldots,t_{n_i}^{\mathfrak{A}}) \in T^{(k),\mathfrak{A}}$, also dass diese Funktion wieder eine Termfunktion ist. Zeigen Sie außerdem, dass für die τ-Algebra $\mathfrak{T}^{(k),\mathfrak{A}} = (T^{(k),\mathfrak{A}}, (\omega_i^{\mathfrak{T}^{(k)},\mathfrak{A}})_{i\in I})$ die Abbildung $\psi : \mathfrak{T}^{(k)} \to \mathfrak{T}^{(k),\mathfrak{A}}$, $t \mapsto t^{\mathfrak{A}}$ ein Homomorphismus ist.

2.1.9. Ein kurzer Exkurs in die mathematische Logik

Inhalt in Kurzfassung: Viele Begriffsbildungen der universellen Algebra werden im Lichte der mathematischen Logik noch besser verständlich. Der vorliegende Unterabschnitt dient dem Zweck, die relevanten Verbindungen herzustellen.

Im Titel dieses Abschnitts ist von einem logisch-modelltheoretischen Rahmen der allgemeinen Algebra die Rede. Das verlangt noch einige Erklärungen.
Algebra und (mathematische) Logik gelten als zwei verschiedene und wichtige Teilgebiete der Mathematik. In der (klassischen) Algebra stehen Strukturen wie Gruppen, Ringe, Körper, Vektorräume etc. im Mittelpunkt. Ein Charakteristikum der Logik ist die (im Vergleich zur klassischen Algebra und erst recht im Vergleich zu vielen anderen mathematischen Disziplinen wie etwa der Analysis) wichtige Rolle der formalen Sprache, in der über ihre Objekte gesprochen wird. Traditionell gelten Beweistheorie, Rekursionstheorie, Mengenlehre und Modelltheorie als die vier Säulen der Logik:

- Die *Beweistheorie* beschäftigt sich mit der Frage, wie sich mathematisches Beweisen formalisieren lässt; sie betrachtet Beweise als mathematische Objekte und analysiert ihre Struktur.
- Die *Berechenbarkeitstheorie* (früher auch *Rekursionstheorie*) untersucht Beziehungen zwischen berechenbaren und nicht berechenbaren Funktionen, bzw. zwischen entscheidbaren und nicht entscheidbaren Mengen; sie steht der Theoretischen Informatik sehr nahe.
- Die *Mengenlehre* beschäftigt sich mit „dem“ mathematischen Universum der Mengen, bzw. mit Modellen der Mengenaxiome (etwa der ZFC-Axiome, siehe auch Unterabschnitt A.6.2 im Anhang). Unendliche Kardinalitäten und Wohlordnungen sind sowohl wichtiges Hilfsmittel als auch Objekt der Untersuchungen.
- Die *Modelltheorie* schließlich steht anderen traditionsreichen Teilen der Mathematik, insbesondere der Algebra, am nächsten. Denn auch die Modelltheorie hat relationale Strukturen als zentralen Gegenstand, allerdings im stärkeren Wechselspiel mit der formalen Sprache, mit der sich diese beschreiben lassen.

Es folgen einige Bemerkungen zur Modelltheorie, insbesondere zur Modelltheorie der *Prädikatenlogik erster Stufe*.
Die Strenge und Präzision der mathematischen Methode beruht wesentlich auf der klaren logischen Struktur ihrer Aussagen. Diese Struktur ergibt sich dadurch, dass einfache

Aussagen mittels logischer Junktoren (und $\wedge$, oder $\vee$, Negation $\neg$, Implikation $\rightarrow$, Äquivalenz $\leftrightarrow$) und Quantoren (Allquantor $\forall$, Existenzquantor $\exists$) zu komplizierteren zusammengesetzt werden können. Quantoren sind nur in Verbindung mit Variablen sinnvoll, was spezielle Regeln für deren Verwendung erfordert, außerdem eventuell gewisse syntaktische Hilfszeichen wie Klammern, Punkte, Doppelpunkte etc. Es bleibt die Frage nach den elementarsten Aussagen, mit denen alles beginnt.
In jedem Fall fordert man ein Symbol für die Gleichheit, üblicherweise $=$. Zwischen welchen Objekten Gleichheit bzw. Ungleichheit behauptet werden kann, hängt nun von der Struktur ab, auf die wir uns beziehen wollen. Dargestellt werden ihre Elemente durch Terme, die sich aus Konstanten, Variablen und deren Verknüpfungen zusammensetzen. Die Verknüpfungen entsprechen den Operationen in universellen Algebren. Verbindet man zwei Terme t_1 und t_2, so wie wir das in Definition 2.1.8.6 getan haben, durch das Gleichheitssymbol $=$, so entsteht die elementare Aussage $t_1 = t_2$. Haben wir es mit einer relationalen Struktur zu tun, ist es überdies möglich, zusätzliche Relationen, die zwischen durch Terme dargestellten Objekten bestehen können, zum Ausdruck zu bringen, z. B. $t_1 \leq t_2$. Aus diesen Gründen ist es sinnvoll, gewissen Klassen relationaler Strukturen eine formale Sprache zuzuordnen. Das soll nun skizziert werden.

Sei (τ, σ) mit $\tau = (n_i)_{i\in I}$ und $\sigma = (m_j)_{j\in J}$ ein Typ relationaler Strukturen und X eine unendliche Variablenmenge. Wie schon bei den rein algebraischen Strukturen sei jedem $i \in I$ ein Operationensymbol ω_i zugeordnet. Die Menge $T = T(X, \tau)$ der Terme sei so definiert wie schon in Definition 2.1.8.1. Darauf aufbauend wollen wir nun die Menge der Formeln definieren. Dabei treten neue Symbole auf: für jedes $j \in J$ ein Relationssymbol, das wir mit j identifizieren dürften aber aus Gewohnheit als ρ_j anschreiben; außerdem Symbole für die logischen Junktoren und Quantoren. Genauer lautet die Definition wie folgt.

Definition 2.1.9.1. Unter den obigen Vereinbarungen bezeichnen wir Zeichenketten der Gestalt $t_1 = t_2$ (Gleichheit von Termen) und der Gestalt $\rho_j(t_1, \ldots, t_{m_j})$ mit Termen t_i als *elementare Formeln* oder *Atomformeln*. (Für $m_j = 2$ schreiben wir oft auch $t_1\ \rho_j\ t_2$.) Beliebige Formeln ergeben sich rekursiv, nämlich als Zeichenketten, die in der kleinsten Menge $F = F(\Omega, R, \tau, \sigma, X)$ mit folgenden Eigenschaften liegen:

1. Alle elementaren Formeln sind Elemente von F.
2. Sind f, f_1 und f_2 Formeln in F, so auch die Zeichenketten $\neg f$, $f_1 \wedge f_2$ (eigentlich $(f_1) \wedge (f_2)$ etc.), $f_1 \vee f_2$, $f_1 \rightarrow f_2$ und $f_1 \leftrightarrow f_2$.
3. Ist f eine Formel in F und x eine Variable, so sind auch die Formeln $\forall x\colon f$ (eigentlich $\forall x\colon (f)$) und $\exists x\colon f$ Formeln, also in F.

Damit ist die durch Ω, τ, R, σ und X induzierte *formale Sprache* gegeben.
Als *geschlossene Formeln* (oft auch *Aussagen*) bezeichnen wir Formeln ohne *freie*[44] *Variable*.

[44]Die Menge $Fr(\varphi)$ der freien Variablen einer Formel φ ist rekursiv definiert: Die freien Variablen einer elementaren Formel sind alle in dieser Formel vorkommenden Variablen. $Fr(\varphi_1 \wedge \varphi_2)$ ist

Gesetze im Sinn von Definition 2.1.8.6 lassen sich als elementare Formeln ohne Relationssymbole oder alternativ als spezielle geschlossene Formeln auffassen, nämlich solche, bei denen alle in einer Gleichung auftretenden Variablen durch einen Allquantor gebunden sind.
Hier wollen wir noch die *Interpretation von Formeln* besprechen. Bei gegebener Variablenbelegung $\alpha\colon X \to A$ steht ein Term t für das Element $\bar{\alpha}(t)$ in A. Die Entsprechung von Termen in einer natürlichen Sprache sind also Nomen (d. h. Substantive und Pronomen). Im Gegensatz dazu steht eine Formel für eine Aussage über die von den involvierten Termen repräsentierten Objekte. In der Grammatik natürlicher Sprachen entspricht dem das Prädikat eines Satzes. Aussagen können wahr oder falsch sein, sie nehmen als Werte also keine Elemente der zu beschreibenden Struktur an, sondern einen von zwei möglichen Wahrheitswerten 1 (für *wahr*) und 0 (für *falsch*). Ähnliches wie für die Termbelegung $\bar{\alpha}$, die durch eine Variablenbelegung α eindeutig bestimmt ist, gilt auch für die Wahrheitswertebelegung von Formeln. Genauer wird dies, in Analogie zu Satz 2.1.8.4, in Proposition 2.1.9.3 beschrieben.
Zunächst brauchen wir noch eine Notation, die uns erlaubt, über Modifikationen von Variablenbelegungen zu sprechen:

Definition 2.1.9.2. Sei $\alpha\colon X \to A$ eine Variablenbelegung; sei $y \in X$ eine Variable, und sei $b \in A$. Mit $\alpha_{y/b}$ bezeichnen wir jene Variablenbelegung $\beta\colon X \to A$, die $\beta(y) = b$ erfüllt, aber an allen anderen Stellen mit α übereinstimmt: $\forall x \neq y : \beta(x) = \alpha(x)$.

Proposition 2.1.9.3. *Mit den Notationen von oben sei wieder $\alpha\colon X \to A$ eine Variablenbelegung in der relationalen Struktur $\mathfrak{A} = (A, \Omega^{\mathfrak{A}}, R^{\mathfrak{A}})$ vom Typ (τ, σ) mit $\tau = (n_i)_{i\in I}$ und $\sigma = (m_j)_{j\in J}$, wobei $\Omega^{\mathfrak{A}} = (\omega_i^{\mathfrak{A}})_{i\in I}$ und $R^{\mathfrak{A}} = (\rho_j^{\mathfrak{A}})_{j\in J}$. Sei weiters, gemäß Proposition 2.1.8.4, $\bar{\alpha}$ die zugehörige Termbelegung. Dann gibt es genau eine Abbildung $\hat{\alpha}\colon F \to \{0, 1\}$ mit folgenden Eigenschaften:*

1. *Eine elementare Formel der Gestalt $t_1 = t_2$, $t_1, t_2 \in T$, erhält unter $\hat{\alpha}$ genau dann den Wahrheitswert 1, wenn $\bar{\alpha}(t_1) = \bar{\alpha}(t_2)$.*

2. *Eine elementare Formel der Gestalt $\rho_j(t_1, \ldots, t_{m_j})$ erhält genau dann den Wahrheitswert 1, wenn $(\bar{\alpha}(t_1), \ldots, \bar{\alpha}(t_{m_j}) \in \rho_{j,\mathfrak{A}}$.*

3. *Eine Formel der Gestalt $\neg f$ mit $f \in F$ erhält genau dann den Wahrheitswert 1, wenn f den Wahrheitswert 0 erhält.*

4. *Eine Formel der Gestalt $f_1 \wedge f_2$ mit $f_1, f_2 \in F$ erhält genau dann den Wahrheitswert 1, wenn sowohl f_1 als auch f_2 den Wahrheitswert 1 erhalten.*
   Kurz gesagt: $\hat{\alpha}(f_1 \wedge f_2) = \min(\hat{\alpha}(f_1), \hat{\alpha}(f_2))$.

5. *Eine Formel der Gestalt $f_1 \vee f_2$ mit $f_1, f_2 \in F$ erhält genau dann den Wahrheitswert 1, wenn wenigstens eine der Formeln f_1 oder f_2 den Wahrheitswert 1 erhält.*
   Kurz gesagt: $\hat{\alpha}(f_1 \vee f_2) = \max(\hat{\alpha}(f_1), \hat{\alpha}(f_2))$.

als die Vereinigung $Fr(\varphi_1) \cup Fr(\varphi_2)$ definiert, analog für die anderen Junktoren. Schließlich ist $Fr(\exists x\, \varphi) = Fr(\forall x\, \varphi) := Fr(\varphi) \setminus \{x\}$ definiert. Variable, die nicht frei sind, heißen (durch einen Quantor) gebunden.

6. *Eine Formel der Gestalt $f_1 \to f_2$ mit $f_1, f_2 \in F$ erhält genau dann den Wahrheitswert* 1*, wenn f_1 den Wahrheitswert* 0 *oder f_2 den Wahrheitswert* 1 *erhält. Anders ausgedrückt: $\hat{\alpha}(f_1 \to f_2) = 0$ gilt genau dann, wenn $\hat{\alpha}(f_1) = 1$ aber $\hat{\alpha}(f_2) = 0$ ist.*

7. *Eine Formel der Gestalt $\forall y\colon f_1$ erhält genau dann den Wahrheitswert 1 unter $\hat{\alpha}$, wenn für alle $b \in A$ die Gleichung $\widehat{\alpha_{y/b}}(f_1) = 1$ gilt.*
Kurz gesagt: $\hat{\alpha}(\forall y\colon f_1) = \min\{\widehat{\alpha_{y/b}}(f_1) : b \in A\}$.

8. *Eine Formel der Gestalt $\exists y\colon f_1$ erhält genau dann den Wahrheitswert 1 unter $\hat{\alpha}$, wenn es ein $b \in A$ gibt, sodass die Gleichung $\widehat{\alpha_{y/b}}(f_1) = 1$ gilt.*
Kurz gesagt: $\hat{\alpha}(\exists y\colon f_1) = \max\{\widehat{\alpha_{y/b}}(f_1) : b \in A\}$.

Erhält eine Formel $f \in F$ durch $\hat{\alpha}$ den Wahrheitswert 1*, so sagen wir, „f gilt für die Variablenbelegung α“. Gilt das für alle Variablenbelegungen $X \to A$, so sagen wir, „f gilt in $\mathfrak{A}$“.*

Damit ist die Bedeutung einer formalen Sprache skizziert, sofern man nur eine feste Struktur $\mathfrak{A}$ im Auge hat. Ist man dagegen an einer Theorie interessiert, die Gültigkeit für eine große Klasse von Strukturen hat, so stößt man auf *Axiomensysteme* und *axiomatische Theorien*. Dabei zeichnet man gewisse Formeln, die in allen betrachteten Strukturen gelten (sollen), als Axiome aus. Eine relationale Struktur $\mathfrak{A}$ vom der Sprache zugehörigen Typ (τ, σ) heißt *Modell* der Theorie (oder der Axiome), wenn jedes Axiom in $\mathfrak{A}$ gilt. Klarerweise zieht die Gültigkeit gewisser Formeln in einer Struktur die Gültigkeit vieler weiterer Formeln nach sich. Man sagt daher: Eine Formel f *folgt* aus einer Menge M anderer Formeln, wenn in jedem Modell für M auch f gilt. Das vielleicht wichtigste Ergebnis der mathematischen Logik, der *Vollständigkeitssatz* von Kurt Gödel (1906–1978), besagt, dass dieser Folgerungsbegriff auf der formalen Ebene der Zeichenketten, welche Formeln definitionsgemäß ja sind, nachvollzogen werden kann. Anders ausgedrückt: Logisches Schließen in diesem Sinne von Folgerung lässt sich automatisieren.
Wer meint, damit könne alle Mathematik den Computern überlassen werden, irrt allerdings in mehrfacher Hinsicht. Nur ein Aspekt sei hier hervorgehoben. Zur Illustration wählen wir etwa das Beispiel der angeordneten Körper $(K, +, 0, -, \cdot, 1, \leq)$. Man überlegt sich leicht, wie die zugehörige formale Sprache einer Theorie der angeordneten Körper und ihre Axiomatisierung aussehen kann.

UE 62 ▶ Übungsaufgabe 2.1.9.4. (F) **◀ UE 62**

(1) Verwenden Sie die Symbole $+, 0, -, \cdot, 1, \leq$ (mit den üblichen Stelligkeiten), sowie die üblichen logischen Symbole $(\vee, \wedge, \Rightarrow, \neg, \forall, \exists$ und Variable $x_1, x_2, \ldots)$, und formulieren Sie in der auf diesem Alphabet aufbauenden Sprache ein Axiomensystem, das genau die angeordneten Körper beschreibt.

(2) Noch einmal das Gleiche, aber nun mit einer Sprache, in der es statt dem 2-stelligen Relationssymbol $\leq$ ein einstelliges Relationssymbol P gibt, welches als „ist positiv“ interpretiert werden soll.

Es zeigt sich, dass die Menge der Formeln in einer solchen Sprache relativ klein ist, gemessen an dem, was uns beispielsweise schon in den reellen Zahlen interessiert. Versucht man etwa, die archimedische Eigenschaft (die Menge $\mathbb{N}_K = \{0_K, 1_K, 1_K + 1_K, \dots\}$ der natürlichen Zahlen innerhalb eines angeordneten Körpers, siehe Definition 3.5.3.7, ist in diesem unbeschränkt) mit den Mitteln dieser Sprache auszudrücken, wird man scheitern. Ein strenger Beweis, dass dies notgedrungen so sein muss, übersteigt zwar den Rahmen dieser Vorlesung.[45] Wer ein paar Minuten investiert, um der Frage nachzugehen, wird aber eine deutliche Intuition gewinnen, warum dies so ist – denn wie soll man ausdrücken, dass ein Element eine obere Schranke *aller* Elemente von $\mathbb{N}_K$ ist (ein solches gilt es zu verhindern)?
Versucht man die auftretenden Probleme zu überwinden, kann man beispielsweise auf den Gedanken kommen, die Sprache dahingehend zu erweitern, dass wir uns gestatten, in Bezug auf eine relationale Struktur $\mathfrak{A} = (A, \Omega, R)$ nicht nur über Elemente von A zu sprechen (sogenannte erststufige Theorien, genannt auch *Prädikatenlogik erster Stufe*), sondern auch über Teilmengen und allgemeiner Relationen auf A, also auch Teilmengen von A^2, A^3, etc. (*Prädikatenlogik zweiter Stufe*). Tatsächlich erweitert das die Ausdruckskraft der Sprache erheblich. Und zwar werden dadurch typischerweise viel mehr Aussagen formulierbar als innerhalb eines vernünftigen Axiomensystems beweisbar sind. Im Gegensatz zur Prädikatenlogik erster Stufe gilt nämlich auf der zweiten Stufe kein Vollständigkeitssatz.
Um keine Missverständnisse zu provozieren, noch eine Bemerkung zum berühmten *Unvollständigkeitssatz* von Gödel: Er besagt, dass es in der Theorie der Peano-Arithmetik (und auch in jeder umfassenderen Theorie, in der man über die natürlichen Zahlen sprechen kann, sofern nur eine sehr milde Bedingung an das Axiomensystem erfüllt ist) wahre Sätze gibt, die formulierbar aber nicht innerhalb des Axiomensystems beweisbar sind. Allerdings muss für diese Formulierung das Induktionsaxiom modifiziert werden. Indem es über beliebige Teilmengen von $\mathbb{N}$ spricht, gehört es in der Fassung von Definition 1.1.2.2 nämlich einer Logik zweiter Stufe an, wo sowieso Vollständigkeit außer Reichweite ist. Man ersetzt das Induktionsprinzip daher durch ein sogenanntes Axiomenschema der Form

$$(\varphi(0) \wedge \forall n : \ (\varphi(n) \to \varphi(n+1))) \to \forall n : \ \varphi(n).$$

Hierin darf man für φ jede Formel ersetzen, die von einer Variablen n abhängt und die der (erststufigen) Sprache der Peano-Arithmetik angehört. Der wesentliche Unterschied zum Induktionsprinzip in der mengentheoretischen Fassung wird deutlich, wenn man sich vor Augen hält, dass es überabzählbar viele Teilmengen T von $\mathbb{N}$ gibt, aber nur abzählbar viele zugelassene Formeln φ in einer Variablen (von denen jede eine Teilmenge von $\mathbb{N}$ beschreibt, nämlich $T_\varphi = \{n \mid \varphi(n)\}$).
Noch eine Bemerkung in Anschluss an Übungsaufgabe 2.1.9.4: Man kann die Axiome eines angeordneten Körpers noch um Bedingungen ergänzen, die für die reellen Zahlen (via Zwischenwertsatz für stetige Funktionen) aus der Vollständigkeit folgen, nämlich dass jedes Polynom ungeraden Grades eine Nullstelle hat und jedes positive Element eine

[45] Hinweis: Kompaktheitssatz der Prädikatenlogik erster Stufe.

Quadratwurzel. Diese Bedingungen lassen sich in (erststufige) Formeln in der Sprache der angeordneten Körper übersetzen. Übernimmt man diese Formeln als Axiome, erhält man die *Theorie der reell abgeschlossenen Körper*. Diese Theorie erweist sich nicht nur als vollständig, sondern sogar als entscheidbar: Es gibt einen Algorithmus, der jede Frage, die sich in der Sprache der angeordneten Körper formulieren lässt, entscheidet; genauer: es gibt einen Algorithmus, der für jede geschlossene Formel φ, die in der erststufigen Sprache der angeordneten Körper formuliert ist, entweder einen Beweis dafür findet, dass φ in allen reell abgeschlossenen Körpern (insbesondere auch in $\mathbb{R}$) gilt, oder einen Beweis dafür, dass φ in keinem reell abgeschlossenen Körper gilt (also insbesondere nicht in $\mathbb{R}$) .
Die Theorie der reell abgeschlossenen Körper liefert also in Bezug auf erststufige Formeln eine vollständige Beschreibung der reellen Zahlen $\mathbb{R}$. Trotzdem gibt es auch zu $\mathbb{R}$ nicht isomorphe Modelle dieser Theorie: Einerseits sogenannte *Nonstandardmodelle* von $\mathbb{R}$ (die allesamt nicht archimedisch angeordnet sind), weiters aber auch gewisse Unterkörper von $\mathbb{R}$, darunter sogar viele abzählbare, wie zum Beispiel die Menge aller algebraischen reellen Zahlen.

2.1.10. Klone

Inhalt in Kurzfassung: Klone entsprechen der Idee, dass nicht nur einstellige Operationen (Funktionen auf einer Menge) durch Verkettung zu Halbgruppen zusammengesetzt werden können, sondern auch mehrstellige Operationen (Funktionen in mehreren Variablen) ineinander eingesetzt werden können. Die bezüglich dieser Operation abgeschlossenen Systeme (die außerdem die sogenannten Projektionen enthalten) nennt man Klone. Der folgende Unterabschnitt soll einen ersten bescheidenen Eindruck von der Theorie der Klone geben.

Etwas weiter von formalen Sprachen und Logik entfernt ist ein weiterer Gesichtspunkt, der in der universellen Algebra eine wichtige Rolle spielt. Dabei geht es weniger darum, von welchen (fundamentalen) Operationen ω auf einer Menge A wir ausgehen, sondern welche Operationen mit ihnen erzeugt werden können. In diesem Sinne wäre es beispielsweise unerheblich, ob wir in einer abelschen Gruppe neben der binären Operation $+$ die Inversenbildung wie bisher über eine (fundamentale) einstellige Operation $\omega_1 : a \mapsto -a$ oder vermittels einer binären Operation (Subtraktion) $\omega_2 : (a, b) \mapsto a - b$ ins Spiel bringen. Zusammen[46] mit $+$ lassen sich nämlich beide wechselseitig ausdrücken: $\omega_1(a) = \omega_2(\omega_2(a, a), a)$ beziehungsweise $\omega_2(a, b) = a + \omega_1(b)$. Offenbar interessieren also Mengen von Operationen, die bezüglich eines geeigneten Begriffs einer Komposition abgeschlossen sein. Der genaue Begriff lautet wie folgt.

Definition 2.1.10.1. Sei A eine Menge. Für alle $n \in \mathbb{N} \setminus \{0\}$ seien die n-stelligen *Projektionen* $\pi_i^{(n)} \colon A^n \to A$ für $i = 1, \ldots, n$ definiert durch $\pi_i^{(n)}(a_1, \ldots, a_n) := a_i$. Weiters sei für n-stellige Operationen f_i, $i = 1, \ldots, k$, und eine k-stellige Operation g auf A die

[46] Überdies lässt sich auch die Operation $+$ durch die Operation ω_2 ausdrücken, denn $a + b = a - (-b) = a - (0 - b) = \omega_2(a, \omega_2(\omega_2(b, b), b))$.

Komposition $h = g \circ_{n,k} (f_1, \ldots, f_k)$ definiert als die n-stellige Operation

$$h(\vec{a}) := g(\, f_1(\vec{a}), \ldots, f_k(\vec{a})\,) \quad \text{für alle } \vec{a} = (a_1, \ldots, a_n) \in A^n.$$

Statt $g \circ_{n,k} (f_1, \ldots, f_k)$ schreibt man oft auch kürzer $g(f_1, \ldots, f_k)$ (oder noch kürzer $g \circ \vec{f}$).
Unter einem *Klon* auf A versteht man eine Menge Ω von Operationen auf A mit positiven Stelligkeiten mit folgenden Eigenschaften:

1. Ω enthält alle Projektionen $\pi_i^{(n)}$, $n = 1, 2, \ldots$, $1 \leq i \leq n$.
2. Ω ist abgeschlossen unter allen $\circ_{n,k}$, d. h.:

   Liegen die n-stelligen Operationen $f_1, \ldots, f_k$ und die k-stellige Operation g in Ω, so auch die Komposition $g \circ_{n,k} (f_1, \ldots, f_k)$.

Die Vereinigung aller $\circ_{n,k}$, $n, k \in \mathbb{N}$, bezeichnen wir mit $\circ$.

Definition 2.1.10.2. Ein „binärer (oder 2-stelliger) Klon“ auf einer Menge A ist eine Menge von zweistelligen Funktionen $f : A^2 \to A$, die erstens die beiden Projektionen enthält und die zweitens unter $\circ_{2,2}$ abgeschlossen ist.
Analog werden ternäre (3-stellige) und höherstellige Klone definiert, sowie auch unäre Klone. Unäre Klone sind dann einfach Untermonoide des Transformationsmonoids $(A^A, \circ)$.

Jeder Klon Ω auf A induziert in natürlicher Weise einen binären Klon $\Omega \cap (A^{A^2})$. Im Allgemeinen ist diese Abbildung $\Omega \mapsto \Omega \cap (A^{A^2})$ aber nicht injektiv.

UE 63 ► **Übungsaufgabe 2.1.10.3.** (B) Finden Sie eine Menge A und zwei Klone $C_1 \neq C_2$ auf A mit $C_1 \cap A^{A^2} = C_2 \cap A^{A^2}$. ◄ **UE 63**
(Hinweis: Zum Beispiel $A := \{0, 1\}$. Als C_1 wähle man einen trivialen Klon, als C_2 den kleinsten Klon, der die „Mehrheitsfunktion“ $m(x_1, x_2, x_3) = 1 \Leftrightarrow |\{i : x_i = 1\}| \geq 2$ enthält.)

UE 64 ► **Übungsaufgabe 2.1.10.4.** (B) Sei $k \geq 3$, $A := \{1, \ldots, k\}$. Mit A^A bezeichnen wir die Menge aller einstelligen Operationen auf A (also aller Funktionen von A nach A). Finden Sie mindestens 3 Klone C auf A, die $A^A \subseteq C$ erfüllen. ◄ **UE 64**
(Hinweis: Den kleinsten und den größten Klon mit der geforderten Eigenschaft findet man leicht. Um einen weiteren Klon zu finden, betrachten Sie die Menge aller nicht surjektiven Funktionen. Beachten Sie aber, dass jede Projektion surjektiv ist.)

UE 65 ► **Übungsaufgabe 2.1.10.5.** (F) Sei $1 \leq k < n$, und sei $f\colon A^k \to A$. Sei $g\colon A^n \to A$ durch ◄ **UE 65**

$$g(a_1, \ldots, a_n) := f(a_1, \ldots, a_k)$$

definiert. Sei Ω ein Klon auf A.
Zeigen Sie: Dann gilt $f \in \Omega \;\Leftrightarrow\; g \in \Omega$.

Anmerkung 2.1.10.6. Warum haben wir in der Definition eines Klons keine nullstelligen Funktionen zugelassen? Wenn wir den Begriff „$_0$Klon“ analog zum Begriff „Klon“ definieren, aber auch nullstellige Funktionen zulassen, dann könnte man die gerade bewiesene Eigenschaft auch für $k = 0$ formulieren, allerdings nicht beweisen. Mit anderen Worten: es gäbe dann einen $_0$Klon Ω, der zwar eine konstante einstellige Funktion g enthält (eine sogenannte „virtuelle Konstante“), nicht aber die zugehörige tatsächliche Konstante, die nullstellige Funktion f.

Ein wichtiges Beispiel erhalten wir mit den Termfunktionen aus Übungsaufgabe 2.1.8.8.

UE 66 ► Übungsaufgabe 2.1.10.7. (F) Sei $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I})$ eine Algebra vom Typ $\tau = (n_i)_{i\in I}$ und sei $T^{(k),\mathfrak{A}}$ die Menge der k-stelligen Termfunktionen, siehe Übungsaufgabe 2.1.8.8. **◄ UE 66**

(1) Seien $t^{\mathfrak{A}} \in T^{(k),\mathfrak{A}}$ und $s_1, \dots, s_k \in T^{(\ell),\mathfrak{A}}$. Zeigen Sie, dass die Komposition

$$t^{\mathfrak{A}} \circ (s_1^{\mathfrak{A}}, \dots, s_k^{\mathfrak{A}}) : (a_1, \dots, a_\ell) \mapsto t^{\mathfrak{A}} \left(s_1^{\mathfrak{A}}(a_1, \dots, a_\ell), \dots, s_k^{\mathfrak{A}}(a_1, \dots, a_\ell)\right)$$

wieder eine Termfunktion ist, also $t^{\mathfrak{A}} \circ (s_1^{\mathfrak{A}}, \dots, s_k^{\mathfrak{A}}) \in T^{(\ell),\mathfrak{A}}$.

(2) Zeigen Sie, dass die Projektionen $\pi_j^{(k)} : A^k \to A$, $(a_1, \dots, a_k) \mapsto a_j$ für $k \geq 1$ und $j = 1, \dots, k$ immer Termfunktionen sind, also $\pi_j^{(k)} \in T^{(k),\mathfrak{A}}$.

(Somit ist $\mathrm{Clo}(\mathfrak{A}) := \bigcup_{k\geq 1} T^{(k),\mathfrak{A}}$ ein Klon, der sogenannte *Termklon* von $\mathfrak{A}$.)

(3) Zeigen Sie mit Induktion nach der Stufe, dass jeder Klon auf A, der die fundamentalen Operationen $\omega_i^{\mathfrak{A}}$ von $\mathfrak{A}$ enthält, auch alle Termfunktionen enthält. Somit wird der Termklon von den fundamentalen Operationen *erzeugt*.

In der universellen Algebra spielt auch der von den fundamentalen Operationen zusammen mit allen Konstanten erzeugte Klon eine wichtige Rolle, der sogenannte Klon der *Polynomfunktionen*. Die Bezeichnung rührt daher, dass es sich dabei um genau jene Funktionen handelt, die durch Polynome auf der entsprechenden Algebra induziert werden (siehe Definition 4.2.3.1 für eine allgemeine Definition).
Umgekehrt kann jeder Klon auf einer Menge A als Menge der fundamentalen Operationen einer Algebra aufgefasst werden, was die Bedeutung von Klonen in der Algebra erklärt – tatsächlich kann man (universelle) Algebra auch als Studium von Klonen auffassen. Ist $|A| \in \{0, 1\}$, so gibt es trivialerweise nur einen Klon auf A. Für $|A| = 2$ sind es immerhin (abzählbar) unendlich viele, für $|A| = 3$ schon überabzählbar viele. Noch viel komplizierter ist die Situation bei unendlichem A. Die interessanten Fragen hängen stark mit unendlicher Kombinatorik zusammen.
Erwähnenswert im Zusammenhang mit Klonen ist folgender Satz:

Satz 2.1.10.8. *Sei Ω ein Klon auf der Menge A, der alle binären Operationen auf A enthält. Dann ist Ω bereits der Klon aller Operationen (beliebiger Stelligkeit) auf A.*

UE 67 ► Übungsaufgabe 2.1.10.9. (V) Man beweise Satz 2.1.10.8 für: **◄ UE 67**

1. endliches A. Anleitung: Orientieren Sie sich an der Lagrangeinterpolation über Körpern, siehe Unterabschnitt 5.3.6.

2. unendliches A. Anleitung: Verwenden Sie, dass jede unendliche Menge A gleichmächtig zu $A \times A$ ist (siehe Satz A.5.6.5 im Anhang). Sei $p\colon A \times A \to A$ bijektiv. Finden Sie zunächst bijektive Abbildungen $p_n\colon A^n \to A$ in dem von p erzeugten Klon und zeigen Sie dann, dass die Menge aller unären Operationen zusammen mit den p_n alle Operationen erzeugt.

Dieses Ergebnis kann man als Erklärung dafür ansehen, dass in der klassischen Algebra explizit kaum Operationen mit einer Stelligkeit $n > 2$ auftreten.

UE 68 ▶ **Übungsaufgabe 2.1.10.10.** (F) Sei $(P, \leq)$ eine Halbordnung. Auf P^k definieren wir eine Halbordnung $\leq_k$ „punktweise“: $(x_1, \ldots, x_k) \leq_k (y_1, \ldots, y_k)$ genau dann, wenn $x_1 \leq y_1, \ldots, x_k \leq y_k$. Eine Funktion $f\colon P^k \to P$ heißt monoton, wenn $\vec{x} \leq_k \vec{y} \Rightarrow f(\vec{x}) \leq f(\vec{y})$ für alle $\vec{x}, \vec{y} \in P^k$ gilt. Zeigen Sie, dass die Menge ◀ **UE 68**

$$C_{\leq} := \bigcup_{n=1}^{\infty} \{f\colon P^n \to P \mid f \text{ monoton}\}$$

einen Klon bildet. Beschreiben Sie für jede mögliche Halbordnung R auf der Menge $\{0, 1\}$ den Klon C_R. (Überlegen Sie insbesondere, ob $R \neq S \Rightarrow C_R \neq C_S$ gilt.)

UE 69 ▶ **Übungsaufgabe 2.1.10.11.** (B) Sei $(P, \leq)$ eine Halbordnung. Auf P^k definieren wir die „lexikographische“ Halbordnung $\leq_{k,\text{lex}}$ wie folgt: Für $\vec{x} := (x_1, \ldots, x_k) \neq \vec{y} := (y_1, \ldots, y_k)$ sei $i := i_{\vec{x},\vec{y}}$ minimal mit $x_i \neq y_i$. Wir setzen $\vec{x} <_{k,\text{lex}} \vec{y}$ genau dann, wenn $x_{i_{\vec{x},\vec{y}}} < y_{i_{\vec{x},\vec{y}}}$. Weiters sei $\vec{x} \leq_{k,\text{lex}} \vec{y}$ genau dann, wenn $\vec{x} <_{k,\text{lex}} \vec{y}$ oder $\vec{x} = \vec{y}$. ◀ **UE 69**
(Anmerkung: Wenn $(P, \leq)$ eine lineare Ordnung ist, dann auch $\leq_{k,\text{lex}}$.)
Wir nennen eine Funktion $f\colon P^k \to P$ lex-monoton, wenn $\vec{x} \leq_{k,\text{lex}} \vec{y} \Rightarrow f(\vec{x}) \leq f(\vec{y})$ für alle $\vec{x}, \vec{y} \in P^k$ gilt. Ist die Menge aller lex-monotonen Funktionen ein Klon?

UE 70 ▶ **Übungsaufgabe 2.1.10.12.** (F) Zeigen Sie, dass die Menge $\mathcal{O}_A$ aller Klone auf einer Menge A (geordnet durch die Relation $\subseteq$) einen vollständigen Verband bildet. ◀ **UE 70**

2.2. Elemente algebraischer Strukturanalyse

Für eine, mehrere oder gar viele gegebene Algebren gibt es mehrere Methoden, um zu weiteren zu kommen. In diesem Abschnitt sollen die wichtigsten besprochen werden: Unteralgebren (Teilmengen, die selbst wieder Algebren bilden, 2.2.1), direkte Produkte (kartesische Produkte, die komponentenweise die gegebenen Strukturen erben, 2.2.2), Faktoralgebren (Partitionen, also Vergröberungen der ursprünglichen Algebra nach Äquivalenzrelationen, auf die sich die ursprüngliche algebraische Struktur übertragen lässt;

über den Homomorphiesatz gibt dies auch einen Überblick über die auf der gegebenen Algebra definierten Homomorphismen, 2.2.3), und direkte Limiten (2.2.4). Der kurze Unterabschnitt 2.2.5 beschäftigt sich mit der Frage der Kardinalitäten von Algebren in einer Varietät. Vermittels der sogenannten Isomorphiesätze (2.2.6) versteht man auch gewisse Kombinationen der in diesem Abschnitt eingeführten Konstruktionen sehr gut.

2.2.1. Unteralgebren und Erzeugnisse

Inhalt in Kurzfassung: In Verallgemeinerung des Begriffs des Unterraums eines Vektorraums sind Unteralgebren einer Algebra genau das, was man sich erwartet: Teilmengen, auf denen wieder eine Algebra desselben Typs vorliegt. Sehr schnell überzeugt man sich: Der Durchschnitt von Unteralgebren ist wieder eine Unteralgebra. Daraus folgt, dass sämtliche Unteralgebren einer gegebenen Algebra bezüglich der Inklusion einen vollständigen Verband bilden. Insbesondere gibt es zu jeder Teilmenge eine kleinste umfassende Unteralgebra, das sogenannte Erzeugnis dieser Teilmenge. Ein häufig verwendetes Ergebnis besagt, dass zwei Homomorphismen, die auf einer Teilmenge übereinstimmen, auch auf deren Erzeugnis übereinstimmen.

Aus der linearen Algebra kennen wir bereits die Begriffe der Untergruppe und des Untervektorraums; es handelt sich hier immer um Untermengen einer vorgegebenen Struktur (einer Gruppe, eines Vektorraums), die unter gewissen Operationen abgeschlossen sind. Hier besprechen wir das zugrunde liegende allgemeinere Konzept.

Definition 2.2.1.1. Ist A eine Menge, $\omega : A^n \to A$ eine n-stellige Operation auf A ($n \in \mathbb{N}$) und $U \subseteq A$, dann heißt U *abgeschlossen* bezüglich ω, wenn $\omega(U^n) \subseteq U$ gilt (d. h., wenn aus $u_1, \ldots, u_n \in U$ stets $\omega(u_1, \ldots, u_n) \in U$ folgt; im Fall $n = 0$ bedeutet das $\omega \in U$).
Ist $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra vom Typ $(n_i)_{i\in I}$ und $U \subseteq A$, dann heißt U *abgeschlossen* bezüglich $(\omega_i)_{i\in I}$, wenn U abgeschlossen bezüglich ω_i für alle $i \in I$ ist. In diesem Fall wird durch $\omega_i^*(x_1, \ldots, x_{n_i}) := \omega_i(x_1, \ldots, x_{n_i})$, $(x_1, \ldots, x_{n_i}) \in U^{n_i}$, eine n_i-stellige Operation ω_i^* auf U definiert: $\omega_i^* = \omega_i|_{U^{n_i}}$. Die Algebra $\mathfrak{U} := (U, (\omega_i^*)_{i\in I})$ (oft ungenau U statt $\mathfrak{U}$) heißt dann eine *Unteralgebra* von $\mathfrak{A}$, symbolisch $U \leq \mathfrak{A}$ oder $\mathfrak{U} \leq \mathfrak{A}$. Meist schreiben wir ω_i für ω_i^*. Wir bezeichnen die Menge aller Unteralgebren von $\mathfrak{A}$ mit $\mathrm{Sub}(\mathfrak{A})$.

Anmerkung 2.2.1.2. Bei Algebren ohne nullstellige Operationen ist es sinnvoll, auch die leere Menge als Unteralgebra zuzulassen, vor allem aus folgendem Grunde. Der Durchschnitt aller Unteralgebren einer Algebra $(A, (\omega_i)_{i\in I})$ wird sich wiederum als Unteralgebra herausstellen und ist dann klarerweise die kleinste Unteralgebra von A. Wenn die Stelligkeit aller Operationen positiv ist, dann kann das auch die leere[47] Menge sein; wenn es allerdings nullstellige Operationen gibt, dann enthält jede Unteralgebra alle nullstelligen Operationen (bzw. genauer: deren Werte).

Unteralgebren von Gruppen sind wieder Gruppen, die man *Untergruppen* nennt, ähnlich Unteralgebren von Ringen, die man *Unterringe* nennt etc. Generell sind Varietäten abgeschlossen bezüglich der Bildung von Unteralgebren:

[47] Siehe Fußnote auf Seite 50.

Proposition 2.2.1.3. *Sei $\mathcal{V}$ eine Varietät (siehe 2.1.8.6), $\mathfrak{A} \in \mathcal{V}$ und $\mathfrak{U} \leq \mathfrak{A}$. Dann ist $\mathfrak{U} \in \mathcal{V}$.*

UE 71 ► Übungsaufgabe 2.2.1.4. (F) Beweisen Sie Proposition 2.2.1.3. **◄ UE 71**

Zur Illustration einige kunterbunte Beispiele:

Beispiele 2.2.1.5.

- Sei $(H, \cdot)$ eine Halbgruppe. Dann ist $U \subseteq H$ eine Unteralgebra von $(H, \cdot)$, wenn für $x, y \in U$ immer $xy \in U$ gilt. Es ist dann $\cdot = \cdot|_{U \times U}$ eine binäre Operation auf U, und $(U, \cdot)$ ist nach Proposition 2.2.1.3 eine Halbgruppe, explizit: das Assoziativgesetz gilt in H und damit erst recht in U. Man nennt $(U, \cdot)$ *Unterhalbgruppe* von $(H, \cdot)$.
- Ist $(G, \cdot)$ eine Gruppe vom Typ (2) und $(U, \cdot)$ Unterhalbgruppe von $(G, \cdot)$, so ist im allgemeinen $(U, \cdot)$ *keine* Gruppe. Beispiel: $(G, \cdot) = (\mathbb{Z}, +)$, $(U, \cdot) = (\mathbb{N}, +)$.
- Hingegen: Sei $(G, \cdot, e, {}^{-1})$ eine Gruppe vom Typ $(2, 0, 1)$. Dann ist $U \subseteq G$ eine Unteralgebra von $(G, \cdot, e, {}^{-1})$, wenn

$$\begin{aligned} \forall x, y \in U : xy &\in U \\ e &\in U \\ \forall x \in U : x^{-1} &\in U \end{aligned}$$

  gilt. Bekanntermaßen ist das äquivalent zu

$$\begin{aligned} U &\neq \emptyset \\ \forall x, y \in U : xy^{-1} &\in U \end{aligned}$$

  Nach Proposition 2.2.1.3 ist die Unteralgebra $(U, \cdot, e, {}^{-1})$ wieder eine Gruppe, genannt *Untergruppe* von $(G, \cdot, e, {}^{-1})$.
- Ist $(R, +, 0, -, \cdot)$ ein Ring vom Typ $(2, 0, 1, 2)$, dann ist jede Unteralgebra $(U, +, 0, -, \cdot)$ wieder ein Ring, genannt *Unterring* von $(R, +, 0, -, \cdot)$. Dies gilt nicht für Ringe vom Typ $(2, 2)$. Beispiel: $(\mathbb{N}, +, \cdot)$ ist Unter*algebra* von $(\mathbb{Z}, +, \cdot)$, aber nicht Unter*ring*.
- Ist der Ring $(R, +, 0, -, \cdot)$ aus dem letzten Punkt sogar ein Integritätsbereich, so ist jeder Unterring $(U, +, 0, -, \cdot)$ ebenfalls ein Integritätsbereich: Nach Proposition 2.2.1.3 ist U jedenfalls ein kommutativer Ring mit Einselement, und ein Nullteiler in U müsste insbesondere ein Nullteiler in R sein.
- Wichtig ist folgende abweichende Situation: Sei $(K, +, 0, -, \cdot, 1)$ ein Körper vom Typ $(2, 0, 1, 2, 0)$ und $(U, +, 0, -, \cdot, 1)$ eine Unteralgebra (d. h. ein Unterring mit demselben Einselement). Dann kann U ein Körper sein, muss aber nicht, zum Beispiel ist $(\mathbb{Z}, +, 0, -, \cdot, 1)$ eine Unteralgebra von $(\mathbb{C}, +, 0, -, \cdot, 1)$ aber kein Körper. Dies zeigt, dass – wie wir in Beispiel 2.1.8.7 schon behauptet haben – die Klasse der Körper keine Varietät bilden kann.

Ist $(U, +, 0, -, \cdot, 1)$ selbst ein Körper, so heißt dieser ein *Unterkörper* von $(K, +, 0, -, \cdot, 1)$. Es gilt: U ist ein Unterkörper genau dann, wenn

$$\begin{aligned} \forall x, y \in U : x + y \in U \\ 0 \in U \\ \forall x \in U : -x \in U \\ \forall x, y \in U : xy \in U \\ 1 \in U \\ \forall x \in U : (x \neq 0 \Rightarrow x^{-1} \in U). \end{aligned}$$

Das Konzept des Unterkörpers ist also kein Spezialfall unseres allgemeinen Begriffs der Unteralgebra.

- Ist () Andererseits
- Sei $(V, +, 0, -, (\omega_\lambda)_{\lambda \in K})$ ein Vektorraum über K und $(U, +, 0, -, (\omega_\lambda)_{\lambda \in K})$ eine Unteralgebra, d. h.,

$$\begin{aligned} \forall x, y \in U : x + y \in U \\ 0 \in U \\ \forall x \in U : -x \in U \\ \forall \lambda \in K, x \in U : \omega_\lambda(x) = \lambda x \in U. \end{aligned}$$

  Dann ist auch $(U, +, 0, -, (\omega_\lambda)_{\lambda \in K})$ ein Vektorraum über K, genannt ein *Unterraum.*

- Betrachten wir das Monoid $M = (\{0, 1\}, \cdot, 1)$. Jede Teilmenge von $\{0, 1\}$ (insbesondere also auch die leere Menge) ist eine Unterhalbgruppe der Halbgruppe $(\{0, 1\}, \cdot)$. Die Algebren $(\{0\}, \cdot, 0)$, $(\{1\}, \cdot, 1)$ und natürlich $(\{0, 1\}, \cdot, 1)$ sind überdies Monoide. Allerdings sind nur $(\{1\}, \cdot, 1)$ und $(\{0, 1\}, \cdot, 1)$ *Untermonoide*, weil nur diese das neutrale Element 1 von M haben – wir verstehen ein Monoid ja als Algebra vom Typ $(2, 0)$.

UE 72 ► **Übungsaufgabe 2.2.1.6.** (F) Man zeige: $S := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{R}$ (mit den Standardoperationen). ◄ **UE 72**
Hinweis für $^{-1}$: $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$

UE 73 ► **Übungsaufgabe 2.2.1.7.** (F) Sei $K = (K, +, 0, -, \cdot, 1)$ ein Körper mit Charakteristik 0. Zeigen Sie, dass es einen Unterkörper K_0 von K gibt, der zu $\mathbb{Q}$ isomorph ist. ◄ **UE 73**
(Anmerkung: durch $f(0_\mathbb{N}) := 0_K$, $f((n+1)_\mathbb{N}) := f(n) + 1_K$ wird eine Funktion $f : \mathbb{N} \to K$ definiert; statt $f(n)$ schreibt man meist $n * 1$. „Charakteristik 0“ bedeutet: Für alle $n > 0$ gilt $f(n) \neq 0_K$.)

Proposition 2.2.1.8. *Sei (A, Ω) eine Algebra und $(T_j)_{j\in J}$ eine Familie von Unteralgebren. Dann ist $T := \bigcap_{j\in J} T_j$ ebenfalls eine Unteralgebra. Ist (A, Ω) ein Körper, und sind die T_j Unterkörper, so auch T.*

Anmerkung 2.2.1.9. Für die leere Indexmenge $J = \emptyset$ ist der in Proposition 2.2.1.8 auftretende allgemeine Durchschnitt $\bigcap_{j\in J} T_j := \{ x \in A \mid \forall j \in J : x \in T_j \}$ als $\bigcap_{j\in J} T_j := A$ definiert.

Beweis (von Proposition 2.2.1.8). Der Fall $J = \emptyset$ ist klar, sodass wir im Folgenden $J \neq \emptyset$ annehmen. Ist $\omega \in \Omega$ eine n-stellige Operation und sind $a_1, \ldots, a_n \in T$ beliebig, so gilt $\omega(a_1, \ldots, a_n) \in T_j$ für alle $j \in J$, da T_j eine Unteralgebra ist. Also gilt $\omega(a_1, \ldots, a_n) \in T$. Den Körperfall beweist man analog. □

Zusammen mit Folgerung 2.1.2.19 folgt, wie bereits dort angekündigt:

Folgerung 2.2.1.10. *Ist $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra, so bildet $(\mathrm{Sub}(\mathfrak{A}), \subseteq)$ eine vollständig verbandsgeordnete Menge, wobei das Infimum der mengentheoretische Durchschnitt ist.*

Wir interessieren uns nicht nur für das Infimum (= mengentheoretischer Schnitt), sondern auch für das Supremum in $\mathrm{Sub}(\mathfrak{A})$. Man überzeugt sich sehr schnell, dass diese im Allgemeinen nicht die mengentheoretische Vereinigung ist:

UE 74 ► Übungsaufgabe 2.2.1.11. (B,F) **◄ UE 74**

(a) Zeigen Sie anhand eines Beispiels, dass für zwei Unteralgebren $\mathfrak{U}_1, \mathfrak{U}_2$ einer Algebra $\mathfrak{A}$ mit Trägermengen U_1, U_2 die Vereinigung $U := U_1 \cup U_2$ keine (Trägermenge einer) Unteralgebra von $\mathfrak{A}$ sein muss.

(b) Sei $(I, \leq)$ eine Totalordnung und seien $\mathfrak{U}_i$, $i \in I$, Unteralgebren von $\mathfrak{A}$ mit $U_i \subseteq U_j$ für alle $i \leq j$. Zeigen Sie, dass $\bigcup_{i\in I} U_i$ eine (Trägermenge einer) Unteralgebra von $\mathfrak{A}$ ist.

Für $S \subseteq A$ ist

$$\bigcap \{T \mid T \supseteq S \text{ und } T \leq \mathfrak{A}\}$$

die *kleinste* Unteralgebra von $\mathfrak{A}$, die S enthält. Entsprechend definiert man:

Definition 2.2.1.12. $\langle S \rangle := \bigcap \{T \mid T \supseteq S \text{ und } T \leq \mathfrak{A}\}$ heißt die *von S erzeugte Unteralgebra* von $\mathfrak{A}$, und S heißt ein *Erzeugendensystem* von $\langle S \rangle$. Wenn S endlich ist, sagen wir $S = \{s_1, \ldots, s_n\}$, dann schreiben wir statt $\langle \{s_1, \ldots, s_n\} \rangle$ abkürzend $\langle s_1, \ldots, s_n \rangle$.

Anmerkung 2.2.1.13. Nach Definition ist das Supremum in $\mathrm{Sub}(\mathfrak{A})$ von zwei Unteralgebren $\mathfrak{U}_1, \mathfrak{U}_2 \in \mathrm{Sub}(\mathfrak{A})$ gegeben durch die kleinste Unteralgebra, die die Trägermengen U_1, U_2 umfasst. Dies ist genau die von $U_1 \cup U_2$ erzeugte Unteralgebra, d. h. $U_1 \vee U_2 = \langle U_1 \cup U_2 \rangle \leq \mathfrak{A}$.

Die von S erzeugte Algebra $\langle S\rangle$ kann auch so konstruiert werden: Sei $S_0 := S$. Induktiv definieren wir nun eine aufsteigende Folge von Mengen gemäß

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

und setzen $S_\infty := \bigcup_{k=0}^{\infty} S_k$. Insbesondere sind alle (Werte von) nullstelligen Operationen in S_1 enthalten. Wir zeigen als Nächstes, dass $S_\infty = \langle S\rangle$ gilt, und stellen eine Verbindung zu Termen her:

Proposition 2.2.1.14. *Seien $\mathfrak{A} = (A, \Omega)$ eine Algebra, $S \subseteq A$ und S_k, $k \in \mathbb{N}$, sowie S_∞ definiert wie oben. Sei außerdem T die Menge der Terme (siehe Definition 2.1.8.1) über der Variablenmenge S und den Operationen[48] Ω. Dann gilt:*

(1) $S_\infty = \langle S\rangle$.

(2) *$\langle S\rangle$ ist genau die Menge aller Werte von Termen, wenn wir für die Variablen aus S ihren „Wert“ in A einsetzen. Formal: Sei $\alpha : S \to A$ die identische Abbildung $s \mapsto s$. Für den von α induzierten Einsetzungshomomorphismus $\bar\alpha : T \to A$ gilt $\langle S\rangle = \bar\alpha(T)$. Insbesondere kann man die Kardinalität von $\langle S\rangle$ abschätzen durch $|\langle S\rangle| \leq \max\{|\mathbb{N}|, |S|, |\Omega|\}$.*

Beweis.

(1) Mit Induktion nach k zeigt man unmittelbar, dass für alle $k \in \mathbb{N}$ die Inklusion $S_k \subseteq \langle S\rangle$ gilt. Da jedenfalls $S = S_0 \subseteq S_\infty$ gilt, genügt es für die Inklusion $\langle S\rangle \subseteq S_\infty$ nachzuweisen, dass S_∞ unter den Operationen aus Ω abgeschlossen ist. Sei dazu $\omega \in \Omega$ eine n-stellige Operation und seien $b_1, \ldots, b_n \in S_\infty$. Für jedes $i = 1, \ldots, n$ gibt es $k_i \in \mathbb{N}$ mit $b_i \in S_{k_i}$. Setzen wir $k := \max(k_1, \ldots, k_n)$, so gilt also $b_1, \ldots, b_n \in S_k$. Nach Definition von S_{k+1} folgt $\omega(b_1, \ldots, b_n) \in S_{k+1} \subseteq S_\infty$.

(2) Wir beweisen zunächst mit Induktion nach k, dass S_k genau die Menge aller Werte von höchstens k-stufigen Termen ist, formal $S_k = \bar\alpha(T_k)$, wobei T_k die Menge der höchstens k-stufigen Terme bezeichnet. (Noch formaler: Wir beweisen, dass die Menge $\{k \in \mathbb{N} \mid S_k = \bar\alpha(T_k)\}$ induktiv ist.)

Der Induktionsanfang $k = 0$ folgt direkt aus den Definitionen: $S_0 = S$ (als Werte), $T_0 = S$ (als Variablen) und $\bar\alpha(S) = S$. Unter der Annahme $S_k = \bar\alpha(T_k)$ gilt

$$\begin{aligned} b \in S_{k+1} &\Leftrightarrow b \in \underbrace{S_k}_{=\bar\alpha(T_k)} \text{ oder } \exists \omega \in \Omega\, \exists b_1, \ldots, b_n \in \underbrace{S_k}_{=\bar\alpha(T_k)} : b = \omega(b_1, \ldots, b_n) \\ &\Leftrightarrow b \in \bar\alpha(T_k) \text{ oder } \exists \omega \in \Omega\, \exists p_1, \ldots, p_n \in T_k : b = \underbrace{\omega(\bar\alpha(p_1), \ldots, \bar\alpha(p_n))}_{=\bar\alpha(\omega(p_1, \ldots, p_n))} \\ &\Leftrightarrow b \in \bar\alpha(T_{k+1}), \end{aligned}$$

also $S_{k+1} = \bar\alpha(T_{k+1})$ wie gewünscht.

Unter Berücksichtigung von $S_\infty = \bigcup_{k=0}^{\infty} S_k$ und 1. sowie $T = \bigcup_{k=0}^{\infty} T_k$ ergibt sich daraus unmittelbar die Aussage.

[48] Genauer: der Sprache, die wir der Operationenmenge Ω zuordnen

Für die Kardinalitätsabschätzung verwenden wir Unterabschnitt A.5.6 aus dem Anhang und bemerken zunächst $|T_k^n \times \Omega| \leq \max(|\mathbb{N}|, |T_k|, |\Omega|)$ für feste n und k. Daraus folgt $|\bigcup_{n\in\mathbb{N}} T_k^n \times \Omega| \leq \max(|\mathbb{N}|, |T_k|, |\Omega|)$ für festes k. Mit Induktion nach k schließt man auf $|T_k| \leq \max(|\mathbb{N}|, |S|, |\Omega|)$ für alle k und erhält folglich $|\bar{\alpha}(T)| = |\bigcup_{k\in\mathbb{N}} \bar{\alpha}(T_k)| \leq \max(|\mathbb{N}|, |S|, |\Omega|)$.

□

Obwohl Unterkörper kein Spezialfall von Unteralgebren sind, lassen sich die meisten Konzepte und Sachverhalte, die Algebren und Unteralgebren betreffen, in offensichtlicher Weise auf Körper und Unterkörper übertragen, wenn man die Bildung multiplikativer Inverse sinngemäß mit einbezieht. Wenn wir eine Teilmenge S eines Körpers K betrachten, ist mit $\langle S\rangle$ also nicht der Durchschnitt aller Unteralgebren von K gemeint, die S enthalten, sondern der Durchschnitt aller Unter*körper*, die S enthalten.

UE 75 ► **Übungsaufgabe 2.2.1.15.** (F+) Formulieren und beweisen Sie eine Variante von Proposition 2.2.1.14 sowie von der zweiten Aussage in Übungsaufgabe 2.2.1.11 für Körper. ◄ **UE 75**

Anmerkung 2.2.1.16. Die Beschreibung der erzeugten Algebra $\langle S\rangle$ „von unten“ als Vereinigung der Mengen S_k ist für viele leichter zu verstehen, weil sie algorithmischen Charakter hat und die Elemente des Abschlusses explizit beschreibt. Sind S und Ω höchstens abzählbar, so kann man auch $\langle S\rangle$ explizit abzählen.
Die Beschreibung des Abschlusses „von oben“ als Durchschnitt aller abgeschlossenen Mengen ist abstrakter und scheint auch komplizierter zu sein, weil es typischerweise sehr viele (oft überabzählbar viele) abgeschlossene Mengen gibt, deren Durchschnitt man bilden muss. Oft ist diese Charakterisierung aber leichter anwendbar, weil man sich dadurch ein mühsames Induktionsargument („Nach Induktion über k zeigen wir, dass für alle S_k gilt: ...“) ersparen kann.

Als Anwendung dazu lässt sich die wichtige Tatsache deuten, dass Homomorphismen durch ihre Werte auf einem Erzeugendensystem eindeutig bestimmt sind:

Proposition 2.2.1.17. *Seien $\mathfrak{A}$, $\mathfrak{B}$ Algebren, $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ und $\varphi'\colon \mathfrak{A} \to \mathfrak{B}$ Homomorphismen. Sei $A_0 \subseteq A$. Wenn $\mathfrak{A} = \langle A_0\rangle$ und $\varphi(a) = \varphi'(a)$ für alle $a \in A_0$, dann ist $\varphi = \varphi'$.*

UE 76 ► **Übungsaufgabe 2.2.1.18.** (V,W) Zeigen Sie Proposition 2.2.1.17. (Anmerkung: Es gibt zwei Möglichkeiten, dies zu beweisen: „von oben“ und „von unten“.) Diskutieren Sie auch die entsprechende Modifikation dieser Aussage für Körper. ◄ **UE 76**

Mit derselben Idee wie die erste Aussage von Proposition 2.2.1.14 beweist man:

Proposition 2.2.1.19. *Sei $\mathfrak{A} = (A, \Omega)$ eine Algebra oder ein Körper und sei $S \subseteq A$. Dann gilt*

$$\langle S\rangle = \bigcup_{S'\subseteq S \text{ endlich}} \langle S'\rangle.$$

UE 77 ► Übungsaufgabe 2.2.1.20. (V) Zeigen Sie Proposition 2.2.1.19. **◄ UE 77**

UE 78 ► Übungsaufgabe 2.2.1.21. (F) Zeigen Sie: **◄ UE 78**

(1) In Vektorräumen gilt[49]:

$$\langle\{x_1,\dots,x_n\}\rangle = \left\{ \sum_{1\le i\le n} \lambda_i x_i \mid \lambda_1,\dots,\lambda_n \in K \right\}.$$

(2) Ist $(G,\cdot,e,^{-1})$ eine *abelsche* Gruppe, dann gilt:

$$\langle\{x_1,\dots,x_n\}\rangle = \{\, x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} \mid k_1,\dots,k_n \in \mathbb{Z}\,\}.$$

Schreibt man die abelsche Gruppe in der Form $(G,+,0,-)$, dann gilt:

$$\langle\{x_1,\dots,x_n\}\rangle = \{k_1x_1 + k_2x_2 + \cdots + k_nx_n \mid k_1,\dots,k_n \in \mathbb{Z}\}.$$

(Man beachte aber, dass diese Darstellung im Allgemeinen nicht eindeutig ist; im Allgemeinen kann man nicht einmal aus der Gleichung $k_1x_1 = k_1'x_1$ (in G) die Gleichheit $k_1 = k_1'$ (in $\mathbb{Z}$) folgern.)

In diesem Unterpunkt (und allen folgenden) dürfen (und sollen) Sie einerseits die Tatsache, dass in Produkten beliebig umgeklammert werden kann (siehe Übungsaufgabe 2.1.3.5), und andererseits die – wohlvertraute – Rechenregel $a^{m+n} = a^m a^n$ für Potenzen ohne Beweis verwenden (siehe Proposition 3.1.1.10 und Übungsaufgabe 3.1.1.11); für eine präzise Formulierung der Potenzen sei ebenfalls auf Abschnitt 3.1.1 verwiesen.

(3) In beliebigen (nichtabelschen) Gruppen gilt:

$$\langle\{x_1,x_2\}\rangle = \{x_1^{k_{11}}x_2^{k_{12}}x_1^{k_{21}}x_2^{k_{22}}\cdots x_1^{k_{n1}}x_2^{k_{n2}} \mid n\in\mathbb{N},\, k_{ij}\in\mathbb{Z}\}.$$

(4) Ist R ein kommutativer Unterring mit 1 von S und $\alpha \in S$, so gilt:

$$\langle R\cup\{\alpha\}\rangle = \{p(\alpha) \mid p\in R[x]\}.$$

Dabei bezeichnet $R[x]$ die Menge aller Polynome $\sum_{k=0}^{n} a_k x^k$ mit $n\in\mathbb{N}$ und $a_i \in R$, $p(\alpha)$ den Wert des Polynoms p, wenn man für die „Unbestimmte“ x das Element α einsetzt.

(5) Ist K ein Unterkörper von E und $\alpha\in E$, so gilt:

$$\langle K\cup\{\alpha\}\rangle = \left\{ \frac{p(\alpha)}{q(\alpha)} \mid p,q\in K[x], q(\alpha)\neq 0 \right\}.$$

[49] Die leere Summe $\sum_{i\in\emptyset} x_i$ definieren wir als 0. Dadurch gilt erstens die Gleichung $\sum_{i\in A\cup B} x_i = \sum_{i\in A} x_i + \sum_{j\in B} x_j$ für alle disjunkten Mengen A, B, und zweitens passt dann die angeführte Formel zur Tatsache, dass der von der leeren Menge erzeugte Vektorraum genau aus dem Nullvektor besteht: $\langle\emptyset\rangle = \{0\}$.

UE 79 ► Übungsaufgabe 2.2.1.22. (W) Sei K_1 der Durchschnitt aller Unterkörper von $\mathbb{R}$, die $\sqrt{5}$ enthalten, und sei K_2 der Durchschnitt aller Unterkörper von $\mathbb{R}$, die π enthalten. **◄ UE 79**

(1) Beschreiben Sie K_1, und geben Sie einen Gruppenisomorphismus zwischen $(K_1, +, 0, -)$ und der additiven Gruppe $\mathbb{Q} \times \mathbb{Q}$ an.
(Hinweis: Siehe Übungsaufgabe 2.2.1.6.)

(2) Beschreiben Sie K_2, und geben Sie eine möglichst explizite surjektive Abbildung von $\mathbb{Q}^{<\infty} \times \mathbb{Q}^{<\infty}$ auf K_2 an. (Mit $X^{<\infty}$ bezeichnen wir die Menge $\bigcup_{n\in\mathbb{N}} X^n$ aller endlichen Folgen mit Elementen aus X.)
(Hinweis: Siehe Übungsaufgabe 2.2.1.21. Verwenden Sie ohne Beweis, dass der Ausdruck $\sum_{i=0}^{n} a_i\pi^i \neq 0$ ist, solange nicht alle $a_i = 0$ sind. Später werden wir sagen, dass π *transzendent* ist.)

In beiden Unteraufgaben ist zu beweisen, dass die von Ihnen beschriebene Menge tatsächlich ein Körper ist, und dass die von Ihnen beschriebene Abbildung ein Isomorphismus bzw. surjektiv ist.

UE 80 ► Übungsaufgabe 2.2.1.23. (F) **◄ UE 80**

(1) Gegeben sei folgende Menge $\mathcal{S}$ von Teilmengen der Menge $\{0, 1, 2, 3\}$:

$$\mathcal{S} := \{\, \{0\},\, \{0,1\},\, \{0,2\},\, \{0,2,3\},\, \{0,1,2,3\} \,\}$$

Geben Sie eine Algebra $\mathfrak{A}$ auf der Menge $A = \{0, 1, 2, 3\}$ an, deren Unteralgebren genau die Elemente von $\mathcal{S}$ sind.

(2) Ist Teil (1) für beliebige Mengen $\mathcal{S} \subseteq \mathfrak{P}(A)$ lösbar?

UE 81 ► Übungsaufgabe 2.2.1.24. (E,D) (Fortsetzung der vorigen Aufgabe.) **◄ UE 81**

(1) Sei A eine endliche Menge. Geben Sie ein Kriterium an, das Ihnen für eine vorgelegte Menge $\mathcal{S} \subseteq \mathfrak{P}(A)$ erlaubt zu entscheiden, ob es eine Algebra $\mathfrak{A}$ auf der Grundmenge A gibt, sodass $\mathrm{Sub}(\mathfrak{A}) = \mathcal{S}$.

Hinweis: Finden Sie für $B \in \mathfrak{P}(A) \setminus \mathcal{S}$ eine Operation f_B (mit einer möglicherweise hohen Stelligkeit), die verhindert, dass B eine (Trägermenge einer) Unteralgebra von $\mathfrak{A}$ ist. Dabei müssen Sie darauf achten, dass alle $C \in \mathcal{S}$ abgeschlossen bezüglich f_B sind.

(2) Inwiefern kann Ihr Kriterium auf unendliche Mengen verallgemeinert werden?

So wie in der Linearen Algebra endlichdimensionale Vektorräume viele interessante Eigenschaften haben, die nicht für beliebige Vektorräume gelten, spielt die entsprechende Verallgemeinerung dieses Konzeptes in sehr vielen einzelnen Strukturtheorien eine entscheidende Rolle.

Definition 2.2.1.25. Eine Algebra $\mathfrak{A}$ mit Trägermenge A heißt *endlich erzeugt* beziehungsweise *abzählbar erzeugt*, wenn es eine endliche bzw. höchstens abzählbar unendliche Menge $E \subseteq A$ gibt mit $A = \langle E \rangle_{\mathfrak{A}}$.

Es besteht der folgende Zusammenhang zu Noetherschen Halbordungen:

Proposition 2.2.1.26. *Der Unteralgebrenverband* $(\mathrm{Sub}(\mathfrak{A}), \subseteq)$ *einer Algebra* $\mathfrak{A}$ *ist genau dann Noethersch, wenn jede Unteralgebra von* $\mathfrak{A}$ *endlich erzeugt ist.*

Beweis. Sei $(\mathrm{Sub}(\mathfrak{A}), \subseteq)$ Noethersch. Wir nehmen indirekt an, dass es eine Unteralgebra $\mathfrak{U} \leq \mathfrak{A}$ mit Trägermenge U gebe, die nicht endlich erzeugt ist. Dann ist zu jeder endlichen Teilmenge $E \subseteq U$ die Menge $C_E := U \setminus \langle E \rangle_{\mathfrak{A}}$ nicht leer. Laut Auswahlaxiom gibt es eine Abbildung $f : \mathcal{E} \to U$ von der Menge $\mathcal{E}$ aller endlichen $E \subseteq U$ nach U mit $f(E) \in C_E$ für alle $E \in \mathcal{E}$. Nach dem Rekursionssatz A.2.2.1 gibt es eine eindeutige Folge von $u_n \in U$ mit $u_0 = f(\emptyset)$ und $u_{n+1} := f(\{u_0, \ldots, u_n\})$ für alle $n \in \mathbb{N}$. Nach Konstruktion bilden dann die $\mathfrak{U}_n := \langle \{u_0, \ldots, u_n\} \rangle_{\mathfrak{A}} \leq \mathfrak{A}$, $n \in \mathbb{N}$, eine unendliche echt aufsteigende Folge in $\mathrm{Sub}(\mathfrak{A})$, Widerspruch zu Noethersch.
Sei nun umgekehrt jede Unteralgebra $\mathfrak{U} \leq \mathfrak{A}$ endlich erzeugt. Der Beweis ist erbracht, wenn wir zu einer beliebig vorgegebenen unendlichen (nicht notwendig echt) aufsteigenden Folge von Unteralgebren $\mathfrak{U}_0 \leq \mathfrak{U}_1 \leq \ldots \leq \mathfrak{A}$ ein $n_0 \in \mathbb{N}$ finden, sodass $\mathfrak{U}_n = \mathfrak{U}_{n_0}$ für alle $n \geq n_0$ gilt. Für $n \in \mathbb{N}$ bezeichne dazu U_n die Trägermengen von $\mathfrak{U}_n$. Die Vereinigung $U := \bigcup_{n \in \mathbb{N}} U_n$ ist laut Übungsaufgabe 2.2.1.11 die Trägermenge einer Unteralgebra $\mathfrak{U}$. Nach Voraussetzung wird $\mathfrak{U}$ von endlich vielen Elementen $u_1, \ldots, u_m \in U$ erzeugt. Zu jedem $i = 1, \ldots, m$ gibt es einen Index $k_i \in \mathbb{N}$ mit $u_i \in U_{k_i}$. Weil die U_n eine Kette bezüglich $\subseteq$ bilden, gilt $u_i \in U_{n_0}$ für $i = 1, \ldots, m$, wenn wir $n_0 := \max\{k_1, \ldots, k_m\}$ setzen. Folglich gilt

$$\mathfrak{U} = \langle \{u_1, \ldots, u_m\} \rangle_{\mathfrak{A}} \leq \mathfrak{U}_{n_0} \leq \mathfrak{U}_n \leq \mathfrak{U},$$

also $\mathfrak{U}_n = \mathfrak{U}_{n_0}$ für alle $n \geq n_0$, womit der Satz bewiesen ist. □

UE 82 ► **Übungsaufgabe 2.2.1.27.** (A) Geben Sie unter Verwendung von Proposition 2.1.2.12 ◄ **UE 82** einen alternativen Beweis der Implikation „Noethersch ⇒ endlich erzeugt“ in Satz 2.2.1.26:

> Sei $\mathfrak{A}$ Noethersch, und sei $\mathfrak{U}$ eine Unteralgebra mit Trägermenge U. Um zu zeigen, dass $\mathfrak{U}$ endlich erzeugt ist, betrachten wir die Familie aller endlich erzeugten Unteralgebren von $\mathfrak{U}$; diese hat ein maximales Element...

Als Abschluss des Unterabschnitts über Unteralgebren heben wir noch ihre Verträglichkeit mit Homomorphismen hervor, sowohl Bilder als auch Urbilder betreffend. Sei dazu $f\colon \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus zwischen zwei Algebren desselben Typs $(n_i)_{i \in I}$ mit entsprechenden Operationen $\omega_i^{\mathfrak{A}}$ und $\omega_i^{\mathfrak{B}}$. Dann ist die Menge $f(A)$ der Bilder $f(a)$, $a \in A$, eine Unteralgebra von $\mathfrak{B}$. Sind nämlich $a_1, \ldots, a_{n_i}$ für irgendein $i \in I$ beliebige Elemente aus A, so ist wegen der Homomorphiebedingung

$$\omega_i^{\mathfrak{B}}(f(a_1), \ldots, f(a_{n_i})) = f(\omega_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i}))$$

die Menge $f(A)$ abgeschlossen bezüglich $\omega_i^{\mathfrak{B}}$. Dasselbe Argument lässt sich auf Unteralgebren von $\mathfrak{A}$ statt auf $\mathfrak{A}$ selbst anwenden: Ist U eine Unteralgebra von $\mathfrak{A}$, so ist $f(U)$ eine Unteralgebra von $\mathfrak{B}$. Außerdem zeigt ein sehr ähnliches Argument die analoge Aussage für Urbilder statt Bilder unter Homomorphismen.

Proposition 2.2.1.28. *Bilder wie auch Urbilder von Unteralgebren unter Homomorphismen sind wieder Unteralgebren.*

UE 83 ► **Übungsaufgabe 2.2.1.29.** (V) Beweisen Sie die Aussage über Urbilder aus Proposition 2.2.1.28. ◄ **UE 83**

2.2.2. Direkte Produkte

Inhalt in Kurzfassung: Liegt eine Familie von Algebren des gleichen Typs vor, so trägt das kartesische Produkt ihrer Trägermengen eine natürliche algebraische Struktur desselben Typs. Man spricht vom direkten Produkt der Algebren. Direkte Produkte zeichnen sich durch eine universelle Eigenschaft aus, in der die sogenannten Projektionen vom direkten Produkt in die einzelnen Komponenten eine zentrale Rolle spielen.

Wir erinnern uns an die Konstruktion ganzer Zahlen $k = [(n_1, n_2)]_\sim$ als Äquivalenzklassen von Paaren natürlicher Zahlen n_1, n_2 oder die Konstruktion reeller Zahlen $r = [(a_n)_{n\in\mathbb{N}}]_\sim$ als Äquivalenzklassen von Cauchyfolgen rationaler Zahlen a_n. In beiden Fällen trägt die Menge der Paare bzw. Folgen selbst eine algebraische Struktur, die sich aus der komponentenweisen Anwendung von Operationen ergibt, z. B.: $(m_1, m_2)+(n_1, n_2) = (m_1+n_1, m_2+n_2)$ bzw. $(a_n)_{n\in\mathbb{N}}+(b_n)_{n\in\mathbb{N}} = (a_n+b_n)_{n\in\mathbb{N}}$. Das ist charakteristisch für die allgemeine Konstruktion *direkter Produkte* aus zwei oder mehreren (eventuell auch unendlich vielen) Strukturen gleicher Art zu einer weiteren, „größeren“ Struktur dieser Art. In unseren Beispielen sind es zwei bzw. abzählbar unendlich viele Kopien der additiven Strukturen auf $\mathbb{N}$ bzw. $\mathbb{Q}$. Darüber hinaus gibt es natürliche Epimorphismen vom direkten Produkt auf jede der Komponenten, nämlich die Projektionen, z. B. $(n_1, n_2) \mapsto n_1$. Diese Beobachtung lässt sich zur Definition 2.2.2.3 präzisieren, die wir vorbereiten, indem wir in Verallgemeinerung von Definition 2.1.1.1 zunächst lediglich die Trägermengen behandeln:

Definition 2.2.2.1. Sei K eine Indexmenge und seien A_k, $k \in K$, Mengen. Das *kartesische Produkt* $\prod_{k\in K} A_k$ ist die Menge aller Funktionen f mit Definitionsbereich K, die

$$\forall k \in K : f(k) \in A_k$$

erfüllen (die Funktionen f gehen also von K in die Menge $\bigcup_{k\in K} A_k$).
Die Elemente von $A := \prod_{k\in K} A_k$ heißen *K-Tupel*; wir bezeichnen Elemente von A auch manchmal als Vektoren $\vec{a} = (a_k \mid k \in K)$. Statt $(a_k \mid k \in K)$ ist auch die Schreibweise $(a_k)_{k\in K}$ üblich.
Für $j \in K$ heißt die Abbildung $\pi_j \colon \prod_k A_k \to A_j$, die durch $\pi_j(f) = f(j)$ definiert ist, die j-te *Projektion*.

Wir erwähnen, dass man für die Existenz von Abbildungen f wie oben (also von Elementen von $\prod_{k\in K} A_k$) das Auswahlaxiom benötigt – tatsächlich ist „für alle K und A_k ist $\prod_{k\in K} A_k$ nichtleer“ eine äquivalente Formulierung des Auswahlaxioms, siehe Unterabschnitt A.4.2 im Anhang.

Eine Bemerkung zum Fall $K = \{1, 2\}$ ist am Platze. In diesem Fall besteht das kartesische Produkt aus allen Abbildungen $1 \mapsto a_1 \in A_1, 2 \mapsto a_2 \in A_2$. Notiert man so eine Abbildung als $(a_k)_{k\in K} = (a_k)_{k=1,2}$, so liegt es nahe, sie mit dem geordneten Paar (a_1, a_2) zu identifizieren. Dann wäre die Menge $\prod_{k\in K} A_k = \prod_{k=1,2} A_k$ als Menge aller Paare (a_1, a_2) mit $a_1 \in A_1$ und $a_2 \in A_2$ schlicht das gewöhnliche kartesische Produkt zweier Mengen gemäß Definition 2.1.1.1, daher die Bezeichnungsweise. Ein typisches Element von $\prod_{k=1,2} A_k$ hat präzise gesprochen jedoch die Form $\{(1, a_1), (2, a_2)\}$ und nicht (a_1, a_2). Obwohl die beiden Mengen rein formal also verschieden sind, bezeichnet man beide als „kartesische Produkte“ $A_1 \times A_2$ und identifiziert sie oft in der beschriebenen Weise (siehe auch die Bemerkungen nach Definition 2.1.3.1).
Ein Sonderfall, der aus anderen Gründen gesonderte Erwähnung verdient, ist $K = \emptyset$. Dann gibt es genau eine Familie $(A_k \mid k \in K)$ von Mengen, und das Produkt dieser „leeren“ Familie enthält ein einziges Tupel, nämlich die leere Menge, symbolisch: $\prod_{k\in\emptyset} A_k = \{\emptyset\}$.

UE 84 ► **Übungsaufgabe 2.2.2.2.** (F+) Seien A_k, $k \in K$, Mengen, $A := \prod_{k\in K} A_k$ deren Produkt, und für alle $j \in K$ sei $\pi_j \colon A \to A_j$ die j-te Projektion. Sei B eine beliebige Menge, und seien $q_j \colon B \to A_j$ beliebige Abbildungen.
Dann gibt es genau eine Abbildung $h \colon B \to A$, die $\pi_j \circ h = q_j$ für alle $j \in K$ erfüllt. ◄ **UE 84**

Analoges gilt für algebraische Strukturen. Die Präzisierung gelingt mit folgender Definition, die Definition 2.2.2.1 als Spezialfall (mit $I = \emptyset$) enthält.

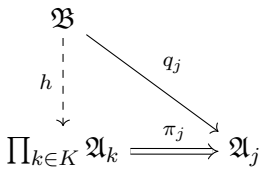
Definition 2.2.2.3. Seien $\mathfrak{A}_k = (A_k, (\omega_{i,k})_{i\in I})$, $k \in K$, Algebren vom selben Typ $(n_i)_{i\in I}$ und sei $A := \prod_{k\in K} A_k$ das Produkt aller Trägermengen A_k. Für alle $i \in I$ sei die Operation ω_i auf A komponentenweise definiert:

$$\omega_i((a_{k,1})_{k\in K}, \ldots, (a_{k,n_i})_{k\in K}) := (\omega_{i,k}(a_{k,1}, \ldots, a_{k,n_i}))_{k\in K}$$

Die Algebra $\mathfrak{A} := (A, (\omega_i)_{i\in I})$ heißt das *direkte Produkt* der Algebren $\mathfrak{A}_k$ und wird mit $\prod_{k\in K} \mathfrak{A}_k$ bezeichnet. Ist K endlich mit m Elementen, so schreibt man für das direkte Produkt $\mathfrak{A}$ häufig auch $\mathfrak{A}_1 \times \ldots \times \mathfrak{A}_m$.

In unmittelbarer Verallgemeinerung von Übungsaufgabe 2.2.2.2 ergibt sich:

Proposition 2.2.2.4. *Seien $\mathfrak{A}_k$, $k \in K$, Algebren desselben Typs, und sei $\mathfrak{A} := \prod_k \mathfrak{A}_k$ deren Produkt. Für alle $j \in K$ sei $\pi_j \colon \mathfrak{A} \to \mathfrak{A}_j$ die j-te Projektion. Sei $\mathfrak{B}$ eine beliebige Algebra vom selben Typ wie die $\mathfrak{A}_k$, und seien $q_j \colon \mathfrak{B} \to \mathfrak{A}_j$ beliebige Homomorphismen. Dann sind die Abbildungen p_j Homomorphismen, und es gibt genau einen Homomorphismus $h : \mathfrak{B} \to \mathfrak{A}$, der $\pi_j \circ h = q_j$ für alle j erfüllt.*



(Zur Bedeutung der verschieden gestalteten Pfeile in diesem Diagramm sei auf die einführenden „Notationellen Bemerkungen“ verwiesen.)

UE 85 ► Übungsaufgabe 2.2.2.5. (W) Beweisen Sie Proposition 2.2.2.4. **◄ UE 85**

UE 86 ► Übungsaufgabe 2.2.2.6. (F) Man kann Produkte „zusammenfassen“. Wenn die Indexmenge I eine disjunkte Vereinigung $I = \bigcup_{k\in K} J_k$ ist, dann ist das Produkt über I kanonisch isomorph zu einem Produkt (über der Indexmenge K) von Produkten: **◄ UE 86**

$$\prod_{i\in I} \mathfrak{A}_i \cong \prod_{k\in K} \mathfrak{B}_k \quad \text{mit } \mathfrak{B}_k := \prod_{j\in J_k} \mathfrak{A}_j.$$

(Geben Sie den Isomorphismus explizit an.)

Unmittelbar einsichtig ist:

Proposition 2.2.2.7. *Seien $\mathfrak{A}_k$, $k \in K$, Algebren desselben Typs τ mit Trägermengen A_k, und sei $t = t(x_1, \ldots, x_n)$, $x_i \in X$, ein Term aus der Termalgebra $\mathfrak{T}(X, \tau)$. Weiters seien für alle $k \in K$ Elemente $a_{1,k}, \ldots, a_{n,k} \in A_k$ gegeben. Dann gilt in der Produktalgebra $\mathfrak{A} := \prod_{k\in K} \mathfrak{A}_k$:*

1. $t^{\mathfrak{A}}\left((a_{1,k})_{k\in K}, \ldots, (a_{n,k})_{k\in K}\right) = \left(t^{\mathfrak{A}_k}(a_{1,k}, \ldots, a_{n,k})\right)_{k\in K}$
2. *Gilt in allen $\mathfrak{A}_k$, $k \in K$, ein Gesetz der Form $t_1 \approx t_2$ mit $t_1, t_2 \in \mathfrak{T}(X, \tau)$, so auch in $\mathfrak{A}$.*

UE 87 ► Übungsaufgabe 2.2.2.8. (V) Beweisen Sie Proposition 2.2.2.7. Anleitung für den ersten Teil: Induktion nach der Stufe des Terms t. **◄ UE 87**

Daraus folgt unmittelbar:

Folgerung 2.2.2.9. *Ist $\mathcal{V}$ eine Varietät mit $\mathfrak{A}_k \in \mathcal{V}$ für alle $k \in K$, so liegt auch das direkte Produkt $\prod_{k\in K} \mathfrak{A}_k$ in $\mathcal{V}$.*

Beispiele 2.2.2.10. Insbesondere gilt also: Direkte Produkte von Halbgruppen (bzw. Gruppen, Vektorräumen über dem selben Körper K, Ringen, Booleschen Algebren) sind wieder Halbgruppen (bzw. Gruppen, Vektorräume über K, Ringe, Boolesche Algebren). Nun können wir auch argumentieren, dass die Klasse der Integritätsbereiche keine Varietät bildet. Das direkte Produkt von zwei Integritätsbereichen $(R, +_R, 0_R, -_R, \cdot_R, 1_R)$ und $(S, +_S, 0_S, -_S, \cdot_S, 1_S)$ ist *niemals* ein Integritätsbereich, denn $(0_R, 1_S) \neq 0_{R\times S}$ ist ein Nullteiler: $(0_R, 1_S) \cdot (1_R, 0_S) = (0_R, 0_S)$.

Die rekursive Definition der von einem k-stelligen Term $t \in \mathfrak{T}^{(k)}$ induzierten Termfunktion $t^{\mathfrak{A}} : A^k \to A$ in Übungsaufgabe 2.1.8.8 verläuft weitgehend parallel zum Beweis des Satzes 2.1.8.4 über den Auswertungshomomorphismus. Dies ist kein Wunder, wie die folgende Übungsaufgabe zeigt.

UE 88 ► **Übungsaufgabe 2.2.2.11.** (A) Ein alternativer Beweis für Übungsaufgabe 2.1.8.8: ◄ **UE 88**
Sei $\tau = (n_i)_{i\in I}$ ein Typ von Algebren und sei $X = \{x_1, x_2, \dots\}$ eine Variablenmenge. Sei weiters $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I})$ eine Algebra vom Typ τ und $\mathfrak{T}^{(k)} := \mathfrak{T}(X^{(k)}, \tau)$ für $k \geq 1$ die von $X^{(k)} = \{x_1, \dots, x_k\}$ und τ induzierte Termalgebra.
Finden Sie eine Algebra $\mathfrak{B} = (B, (\omega_i^{\mathfrak{B}})_{i\in I})$ vom Typ τ und eine Variablenbelegung $\beta : X \to B$, sodass $t^{\mathfrak{A}} = \bar{\beta}(t)$ für alle $t \in \mathfrak{T}^{(k)}$ gilt, wobei $\bar{\beta} : \mathfrak{T}^{(k)} = \mathfrak{T}(X^{(k)}, \tau) \to \mathfrak{B}$ der gemäß Satz 2.1.8.4 gegebene Einsetzungshomomorphismus ist. Außerdem sollen die in Übungsaufgabe 2.1.8.8 gefundenen Operationen $\omega_i^{\mathfrak{T}^{(k)},\mathfrak{A}}$ auf $\mathfrak{T}^{(k),\mathfrak{A}}$ genau die Einschränkungen von $\omega_i^{\mathfrak{B}}$ auf $\mathfrak{T}^{(k),\mathfrak{A}} = \bar{\beta}(\mathfrak{T}^{(k)})$ sein, also $\mathfrak{T}^{(k),\mathfrak{A}} \leq \mathfrak{B}$.
(Die Ergebnisse aus Übungsaufgabe 2.1.8.8 dürfen Sie dabei nicht verwenden, um $\mathfrak{B}$ zu finden, $\mathfrak{B} = \mathfrak{T}^{(k),\mathfrak{A}}$ ist also nicht erlaubt.)

In direkten Produkten von Monoiden, Gruppen, Ringen etc. haben die ursprünglichen Komponenten isomorphe Kopien in den ihnen entsprechenden Komponenten des Produktes; für Gruppen G, H gilt nämlich $G \cong G \times \{e_H\} \leq G \times H$. Man beachte aber, dass dies allgemein *nicht* gilt. Ein einfaches Beispiel, das diese Situation illustriert, erhält man in der Klasse aller Algebren vom Typ (1), d. h. mit einer einzigen einstelligen Operation. Dazu betrachten wir je eine zwei- und dreielementige Trägermenge $A = \{a_1, a_2\}$ und $B = \{b_1, b_2, b_3\}$ zusammen mit den zyklischen Permutationen $f_A : a_1 \mapsto a_2 \mapsto a_1$ und $f_B : b_1 \mapsto b_2 \mapsto b_3 \mapsto b_1$. Die Operation f_C auf dem direkten Produkt auf $C := A \times B$ ist dann ebenfalls eine zyklische Permutation, diemals auf einer sechselementigen Menge. Dann hat (C, f_C) nur die trivialen Unteralgebren, insbesondere also keine isomorphen Kopien von (A, f_A) und (B, f_B).

UE 89 ► **Übungsaufgabe 2.2.2.12.** (B) Führen Sie diese Überlegung in allen Details aus. ◄ **UE 89**

2.2.3. Homomorphe Bilder, Kongruenzrelationen und Faktoralgebren

Inhalt in Kurzfassung: So wie dem Konzept der Teilmenge einer Menge in der Algebra das Konzept der Unteralgebra entspricht und dem des kartesischen Produktes das direkte Produkt, so entsprechen den Konzepten Äquivalenzrelation und Partition in der Algebra jene von Kongruenzrelation bzw. Faktoralgebra. Eine wichtige Rolle spielen dabei auch Homomorphismen, insbesondere der kanonische Homomorphismus. Dies kommt im Homomorphiesatz zum Ausdruck. Sämtliche Kongruenzrelationen einer gegebenen Algebra bilden einen vollständigen Verband (sehr ähnlich wie auch die Unteralgebren). Die klassischen Beispiele sind die Kongruenzen ganzer Zahlen modulo einer natürlichen Zahl mit den Restklassenringen als Faktoralgebren. Auf jeder Algebra gibt es zwei Partitionen, die immer auch Faktoralgebren induzieren: die einelementige Partition und jene aus ausschließlich einelementigen Klassen. Entsprechend sind die zugehörigen Äquivalenzrelationen stets auch Kongruenzrelationen, die sogenannten trivialen. Eine Algebra, die

außer den trivialen Kongruenzrelationen keine weiteren besitzt, heißt einfach.

In diesem Unterabschnitt geht es um drei Konzepte, die sich ineinander übersetzen lassen. Als Ausgangspunkt wählen wir strukturerhaltende Abbildungen zwischen Algebren, also Homomorphismen. Jede Abbildung induziert eine Äquivalenzrelation bzw. Partition auf ihrem Definitionsbereich, indem man Elemente mit demselben Bild als äquivalent auffasst. Handelt es sich zusätzlich um einen Homomorphismus, ist die Äquivalenzrelation automatisch verträglich mit den Operationen, was sie zu einer sogenannten Kongruenzrelation macht. Dadurch wird auf der Partition eine natürliche Definition von Operationen möglich, wodurch eine sogenannte Faktoralgebra entsteht. Die Situation wird durch den Homomorphiesatz beschrieben. Nun zur Ausführung dieses Programms im Detail.
Wie jede Abbildung induziert auch ein Homomorphismus zwischen Gruppen oder auch irgendwelchen Algebrendesselben Typs in natürlicher Weise eine Äquivalenzrelation:

Definition 2.2.3.1. Seien $\mathfrak{A}$ und $\mathfrak{B}$ Algebren desselben Typs, und sei $f : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus. Dann nennt man die die durch

$$x \sim y \ :\Leftrightarrow \ f(x) = f(y)$$

definierte Äquivalenzrelation $\sim$ auf A den *Kern* von f, symbolisch $\ker f$.

In manchen Fällen, die später eine wichtige Rolle spielen werden – nämlich wenn es sich bei den beiden Algebren z. B. um Gruppen, Ringe, Moduln, Vektorräume oder Boolesche Algebren handelt – ist $\ker f$ durch eine einzige Klasse, nämlich das Urbild der 0, eindeutig bestimmt, weshalb man auch diese Klasse als Kern bezeichnet. Die Äquivalenzrelation $\ker f$ hat die besondere Eigenschaft, mit allen Operationen von G in folgendem Sinn *verträglich* zu sein: wenn etwa $+$ eine zweistellige Operation ist, dann gilt

$$\begin{aligned} g_1 \sim \tilde{g}_1 \text{ und } g_2 \sim \tilde{g}_2 &\Rightarrow f(g_1) = f(\tilde{g}_1) \text{ und } f(g_2) = f(\tilde{g}_2) \\ &\Rightarrow f(g_1 + g_2) = f(g_1) + f(g_2) = f(\tilde{g}_1) + f(\tilde{g}_2) = f(\tilde{g}_1 + \tilde{g}_2) \\ &\Rightarrow g_1 + g_2 \sim \tilde{g}_1 + \tilde{g}_2. \end{aligned}$$

(Analoges gilt für alle Stelligkeiten.)
Im Homomorphiesatz 2.2.3.17 wird diese Überlegung noch mit Faktoralgebren in Verbindung gebracht. Dazu heben wir Relationen, die in der oben beschriebenen Weise mit Operationen verträglich sind, durch folgende Definition hervor.

Definition 2.2.3.2. Ist $f : A^n \to C$ eine Abbildung und $\sim$ eine Äquivalenzrelation auf A, so heißen f und $\sim$ verträglich, wenn gilt: Für alle $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ mit $a_k \sim b_k$ für $k = 1, \ldots, n$ gilt $f(a_1, \ldots, a_n) \sim f(b_1, \ldots, b_n)$.
Sei nun $\mathfrak{A} = (A, (\omega_i)_{i \in I})$ eine Algebra vom Typ $(n_i)_{i \in I}$ und $\sim$ eine Äquivalenzrelation auf A. Dann heißt $\sim$ *Kongruenz(relation)* auf $\mathfrak{A}$, wenn $\sim$ mit allen ω_i *verträglich* ist, wenn also für alle $i \in I$ und $a_1, \ldots, a_{n_i}, b_1, \ldots, b_{n_i} \in A$ gilt:

$$a_1 \sim b_1, \ldots, a_{n_i} \sim b_{n_i} \Rightarrow \omega_i(a_1 \ldots a_{n_i}) \sim \omega_i(b_1 \ldots b_{n_i}).$$

Wir bezeichnen die Menge aller Kongruenzrelationen auf $\mathfrak{A}$ mit $\mathrm{Con}(\mathfrak{A})$.

Man beachte, dass für $n_i = 0$ die Verträglichkeitsbedingung in Definition 2.2.3.2 von jeder Äquivalenzrelation erfüllt wird (Reflexivität von $\sim$).

UE 90 ► Übungsaufgabe 2.2.3.3. (B,F) Sei $A = \{1, 2, 3, 4, 5, 6, 7\}$ eine 7-elementige Menge und $\sim$ die durch die Partition $\{\{1, 2\}, \{3, 4, 5\}, \{6, 7\}\}$ induzierte Äquivalenzrelation. **◄ UE 90**

(1) Geben Sie eine Algebra $\mathfrak{A} = (A, \omega_1, \ldots, \omega_k)$ an, sodass $\sim$ die einzige nichttriviale Kongruenzrelation (siehe Definition 2.2.3.14) dieser Algebra ist. (Hinweis: Man kommt mit unären Funktionen aus.)

(2) Sei $\mathfrak{B}$ eine beliebige Algebra gleichen Typs, und sei $\varphi : \mathfrak{A}/_\sim \to \mathfrak{B}$ ein beliebiger Homomorphismus. Zeigen Sie, dass φ entweder konstant oder injektiv sein muss.

UE 91 ► Übungsaufgabe 2.2.3.4. (E) (Fortsetzung von Punkt (1) der vorigen Aufgabe.) Kommt man ganz allgemein immer mit unären Operationen aus? Genauer lautet die Frage: Angenommen, zu einer Familie F von Äquivalenzrelationen auf einer Menge A gibt es eine Menge von Operationen ω_i auf A derart, dass die Elemente von F genau die Kongruenzrelationen von $(A, (\omega_i)_{i\in I})$ sind. Gibt es dann immer eine Familie von einstelligen Operationen mit derselben Eigenschaft? **◄ UE 91**

Das System $\mathrm{Con}(\mathfrak{A})$ aller Kongruenzrelationen einer Algebra $\mathfrak{A}$ verhält sich sehr ähnlich wie $\mathrm{Sub}(\mathfrak{A})$, jenes aller Unteralgebren. Entsprechend gehen wir analog vor wie in Proposition 2.2.1.8 und Folgerung 2.2.1.10:

Proposition 2.2.3.5. *Seien $\mathfrak{A} = (A, \Omega)$ eine Algebra und $\sim_j$ für $j \in J$ Kongruenzrelationen. Dann ist auch der mengentheoretische Schnitt $\sim$ aller $\sim_j$, $j \in J$, (für $J = \emptyset$ ist für $\sim$ die Allrelation $\nabla_A = A \times A$ zu setzen) eine Kongruenzrelation auf $\mathfrak{A}$.*

Zusammen mit Folgerung 2.1.2.19 folgt, wie bereits dort angekündigt:

Folgerung 2.2.3.6. *Ist $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra, so ist $(\mathrm{Con}(\mathfrak{A}), \subseteq)$ ein vollständiger Verband (im ordnungstheoretischen Sinn) mit dem mengentheoretischen Durchschnitt als Infimum.*

UE 92 ► Übungsaufgabe 2.2.3.7. (V) Beweisen Sie Proposition 2.2.3.5 und Folgerung 2.2.3.6. **◄ UE 92**

UE 93 ► Übungsaufgabe 2.2.3.8. (A) Sei $\mathfrak{A}$ eine Algebra mit Trägermenge A. **◄ UE 93**

(1) Zeigen Sie $\mathrm{Con}(\mathfrak{A}) = \mathrm{Sub}(\mathfrak{A} \times \mathfrak{A}) \cap \mathrm{Eq}(A)$, wobei $\mathrm{Eq}(A)$ die Menge der Äquivalenzrelationen auf A bezeichne.

(2) Finden Sie eine Algebra $\mathfrak{B}$ auf der Menge $B := A \times A$, sodass $\mathrm{Con}(\mathfrak{A}) = \mathrm{Sub}(\mathfrak{B})$.

Auch das Supremum in $\mathrm{Con}(\mathfrak{A})$ lässt sich ähnlich beschreiben wie in $\mathrm{Sub}(\mathfrak{A})$: Ist $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra und $M \subseteq A \times A$, so ist der Schnitt $\sim$ aller Kongruenzrelationen auf $\mathfrak{A}$, die M als Teilmenge enthalten, die von M erzeugte Kongruenzrelation auf $\mathfrak{A}$. Insbesondere gilt das, wenn M die Vereinigung einer Familie von Kongruenzrelationen $\sim_j$, $j \in J$, auf $\mathfrak{A}$ ist. Das ist die Beschreibung des Supremums im vollständigen Verband $(\mathrm{Con}(\mathfrak{A}), \subseteq)$ *von oben*. So wie bei Unteralgebren lässt sich $\sim$ auch durch einen Erzeugungsprozess *von unten* beschreiben:

UE 94 ► **Übungsaufgabe 2.2.3.9.** (E) Sei $\mathfrak{A}$ eine Algebra, $\theta_1, \theta_2 \in \mathrm{Con}(\mathfrak{A})$. Wir definieren ψ als die Menge aller Paare $(a, b) \in A \times A$, für die es ein $n \geq 0$ und eine Folge $(a_0, \ldots, a_n)$ gibt, sodass $a_0 = a$, $a_n = b$ gilt, sowie für alle $i \in \{0, \ldots, n-1\} : (a_i, a_{i+1}) \in \theta_1 \cup \theta_2$.
Zeigen Sie, dass ψ eine Kongruenzrelation ist, und weiters, dass ψ in $(\mathrm{Con}(\mathfrak{A}), \subseteq)$ die kleinste obere Schranke von θ_1 und θ_2 ist.
(Wenn es Ihnen die Notation erleichtert, nehmen Sie an, dass $\mathfrak{A}$ eine Algebra vom Typ $(2, 2, 0)$ ist.) ◄ **UE 94**

UE 95 ► **Übungsaufgabe 2.2.3.10.** (E) Sei $\mathfrak{M}$ eine Algebra, sei $(\sim_j | \ j \in J)$ eine Familie von Kongruenzrelationen, und sei $M \subseteq A \times A$ die Vereinigung der Relationen $\sim_j$.
Beschreiben Sie das Supremum der Relationen $\sim_j$ (äquivalent die von M erzeugte Kongruenzrelation) im Kongruenzverband durch einen Erzeugungsprozess von unten, indem Sie definieren, wie man M_{n+1} aus M_n erhält derart, dass gilt: Setzt man $M_0 := M$ und nimmt man als $\sim$ die Vereinigung $\bigcup_{n\in\mathbb{N}} M_n$, so ist $\sim$ die von M erzeugte Kongruenzrelation. ◄ **UE 95**

Die große Bedeutung von Kongruenzrelationen ergibt sich daraus, dass genau sie die Konstruktion von Faktoralgebren ermöglichen:

Proposition 2.2.3.11. *Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra vom Typ $\tau = (n_i)_{i\in I}$ und $\sim$ eine Äquivalenzrelation auf $\mathfrak{A}$. Dann sind folgende beiden Aussagen äquivalent:*

1. *Die Relation $\sim$ ist sogar eine Kongruenzrelation auf $\mathfrak{A}$.*
2. *Auf der Menge $A/_\sim$ aller Äquivalenzklassen bezüglich $\sim$ gibt es eine Familie von n_i-stelligen Operationen ω_i^* mit*

$$\omega_i^*([a_1]_\sim, \ldots, [a_{n_i}]_\sim) = [\omega_i(a_1, \ldots, a_{n_i})]_\sim$$

für alle $i \in I$ und $a_1, \ldots, a_{n_i} \in A$.

Definition 2.2.3.12. Sind die beiden äquivalenten Bedingungen aus Proposition 2.2.3.11 erfüllt, so heißt die Algebra $\mathfrak{A}/_\sim := (A/_\sim, (\omega_i^*)_{i\in I})$ die *Faktoralgebra* von $\mathfrak{A}$ nach (oder bezüglich) der Kongruenzrelation $\sim$. (Oft schreiben wir nur ω_i statt ω_i^*.)

UE 96 ▶ **Übungsaufgabe 2.2.3.13.** (V,W) Beweisen Sie Proposition 2.2.3.11. Hinweis: Fasst man die zweite Bedingung als Definition der Operationen ω_i^* auf, so ist vor allem Wohldefiniertheit[50] zu zeigen. ◀ **UE 96**

Definition 2.2.3.14. Auf einer beliebigen Algebra $\mathfrak{A}$ mit Trägermenge A sind die *Gleichheitsrelation*[51] $\Delta_A = \Delta = \{(x, x) \mid x \in A\}$, genannt auch *Identität*, und die *Allrelation* $\nabla_A = \nabla = A \times A$ stets Kongruenzen, genannt die *trivialen Kongruenzen* auf $\mathfrak{A}$. $\mathfrak{A}/\Delta$ und $\mathfrak{A}/\nabla$ sind die *trivialen Faktoralgebren*. Eine Algebra, auf der es außer den trivialen Kongruenzen keine weiteren gibt, heißt *einfach*.

Es gilt $\mathfrak{A}/\Delta \cong \mathfrak{A}$ und $|\mathfrak{A}/\nabla| \leq 1$. Aus dem Homomorphiesatz 2.2.3.17 wird folgen, dass eine Algebra $\mathfrak{A}$ genau dann einfach ist, wenn sie nur *triviale* homomorphe Bilder hat (d. h., jeder Homomorphismus $h\colon A \to B$ ist entweder konstant oder injektiv).

UE 97 ▶ **Übungsaufgabe 2.2.3.15.** (B) Wie viele triviale Äquivalenzrelationen und wie viele nichttriviale Äquivalenzrelationen gibt es ◀ **UE 97**

1. auf einer 3-elementigen Menge?
2. auf einer 2-elementigen Menge?

[50] Was heißt es, dass eine Funktion wohldefiniert ist? Wenn wir eine Funktion f auf einer Menge X durch eine Rechenvorschrift (etwa einen Term) t definieren, also $f(x) := t(x)$ setzen, dann bedeutet das Wort „wohldefiniert“ nur soviel, dass die Rechenvorschrift t für jede Eingabe x im gewünschten Definitionbereich der Funktion tatsächlich ein Resultat $t(x)$ ausgibt. (Man muss etwa darauf achten, dass nicht durch 0 dividiert wird, dass eventuell auftretende Wurzeln wirklich definiert sind, etc.)
Wenn wir aber f durch eine Formel

$$(*) \qquad f(H(s)) := t(s) \text{ für alle } s \in S$$

definieren, wobei H eine bereits definierte Funktion ist, die S surjektiv auf X abbildet (zum Beispiel könnte $H(s) := [s]_\sim$ für eine vorgegebene Äquivalenzrelation $\sim$ sein), dann enthält diese „Definition“ implizit die Behauptung, dass es tatsächlich eine Funktion gibt, die jedem Element der Form $H(s)$ das Element $t(s)$ zuordnet. Wenn es nämlich Objekte s_1, s_2 gibt, die zwar $H(s_1) = H(s_2)$ aber $t(s_1) \neq t(s_2)$ erfüllen, dann ist die „Definition“ $(*)$ nicht sinnvoll, da sie nicht erklärt, ob der Wert f an der Stelle $H(s_1)$ nun $t(s_1)$ oder $t(s_2)$ sein soll.

Mit anderen Worten: Durch die Definition $(*)$ wird zunächst nur die Relation $\{(H(s), t(s)) : s \in S\}$ definiert; zu überprüfen ist noch, ob diese Relation tatsächlich eine Funktion ist.

Notwendig und hinreichend für die Gültigkeit der genannten Behauptung ist die Implikation

$$(**) \qquad \forall s, s' \; (H(s) = H(s') \Rightarrow t(s) = t(s')).$$

Wenn wir also eine Funktion f durch eine Vorschrift $(*)$ definieren, müssen wir uns immer erst vergewissern, dass $(**)$ erfüllt ist.

Bevor man überprüft hat, ob f tatsächlich wohldefiniert ist, empfiehlt es sich, den Ausdruck $f(\cdots)$ nicht zu verwenden, da ja noch nicht klar ist, was damit überhaupt gemeint ist.

Ein Spezialfall liegt vor, wenn H injektiv ist. Dann ist Wohldefiniertheit kein Problem, weil die Vorschrift $(*)$ in diesem Fall äquivalent zu folgender Forderung ist: $f(x) = t(H^{-1}(x))$ für alle y.

[51] Auch andere Notationen sind üblich. Statt Δ_A schreibt man auch id_A oder $=_A$ oder ι_A, statt ∇_A auch ω_A oder einfach A^2.

3. auf einer 1-elementigen Menge?

4. auf der leeren Menge?

Nachdem wir den Zusammenhang zwischen Kongruenzrelationen und Faktoralgebren geklärt haben, sei auch noch hervorgehoben, wie diese einen Homomorphismus induzieren:

Proposition 2.2.3.16. *Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra und $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$. Dann ist die Abbildung*

$$\nu : \begin{cases} A \to A/_\sim \\ a \mapsto [a]_\sim \end{cases}$$

ein surjektiver Homomorphismus von $\mathfrak{A}$ auf die Faktoralgebra $\mathfrak{A}/_\sim$, der sogenannte natürliche *oder auch* kanonische Homomorphismus.

Beweis. Ist $\tau = (n_i)_{i\in I}$ der Typ von $\mathfrak{A}$, so folgt die Behauptung aus (Notation wie in Proposition 2.2.3.11)

$$\nu(\omega_i(a_1, \ldots, a_{n_i})) = [\omega_i(a_1, \ldots, a_{n_i})]_\sim = \omega_i^*([a_1]_\sim, \ldots, [a_{n_i}]_\sim) = \omega_i^*(\nu(a_1), \ldots, \nu(a_{n_i})).$$

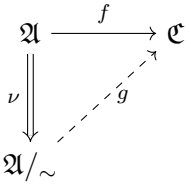
Die Surjektivität folgt daraus, dass jedes Element γ von $\mathfrak{A}/_\sim$ per definitionem die Gestalt $\gamma = [a]_\sim = \nu(a)$ für ein $a \in A$ hat. □

Gewissermaßen als Umkehrung kommen wir nun zum bereits angekündigten Homomorphiesatz, der die Beziehung zwischen Homomorphismen, Kongruenzrelationen und Faktoralgebren zusammenfasst:

Satz 2.2.3.17 (Homomorphiesatz)**.** *Seien $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I})$ und $\mathfrak{C} = (C, (\omega_i^{\mathfrak{C}})_{i\in I})$ Algebren vom selben Typ $(n_i)_{i\in I}$ und $f\colon \mathfrak{A} \to \mathfrak{C}$ ein Homomorphismus. Dann ist der sogenannte* Kern

$$\sim := \{(x, y) \mid f(x) = f(y)\}$$

von f eine Kongruenz auf $\mathfrak{A}$, und es gibt genau eine Abbildung g von $\mathfrak{A}/_\sim$ nach $\mathfrak{C}$ mit $f = g \circ \nu$ (ν ist die natürliche Abbildung $a \mapsto [a]_\sim$). Dieses g ist ein injektiver Homomorphismus $g\colon \mathfrak{A}/_\sim \to \mathfrak{C}$ und genau dann sogar ein Isomorphismus, wenn f surjektiv ist.



Beweis. Wir beweisen zunächst jene Behauptungen, die für beliebige Abbildungen unabhängig von einer zugrunde liegenden algebraischen Struktur gelten: Dass die Relation $\sim$ eine Äquivalenzrelation ist, gilt für beliebige Abbildungen und überträgt sich unmittelbar von den entsprechenden Eigenschaften der Gleichheitsrelation (Reflexivität,

Symmetrie und Transitivität). Wegen der Bedingung $f = g \circ \nu$ ist $g([a]_\sim) := f(a)$ die einzig mögliche Definition von g mit den geforderten Eigenschaften. Aus $[a]_\sim = [b]_\sim$ folgt nach Definition von $\sim$ die Gleichheit $f(a) = f(b)$, weshalb g durch diese Festlegung tatsächlich wohldefiniert ist. Weil die kanonische Abbildung $\nu : A \to A/_\sim$ surjektiv ist, stimmen die Bilder von g und $g \circ \nu = f$ überein. Somit ist g surjektiv genau dann, wenn f surjektiv ist.
Es verbleibt der Beweis der algebraischen Aussagen des Homomorphiesatzes, nämlich dass $\sim$ mit den Operationen verträglich (also eine Kongruenzrelation) ist und dass g ein Homomorphismus ist. Für $n_i = 0$ ist die Verträglichkeit von ω_i mit $\sim$ trivial und jene mit g aus der Beziehung $g(\omega_i^{\mathfrak{A}/\sim}) = g([\omega_i^{\mathfrak{A}}]_\sim) = f(\omega_i^{\mathfrak{A}}) = \omega_i^{\mathfrak{C}}$ ersichtlich. Sei daher ab nun $n_i > 0$. Wir haben:

$$\left.\begin{array}{c} a_1 \sim b_1 \\ \vdots \\ a_{n_i} \sim b_{n_i} \end{array}\right\} \Rightarrow \left\{\begin{array}{c} f(a_1) = f(b_1) \\ \vdots \\ f(a_{n_i}) = f(b_{n_i}) \end{array}\right\} \Rightarrow \omega_i^{\mathfrak{C}}(f(a_1), \ldots, f(a_{n_i})) = \omega_i^{\mathfrak{C}}(f(b_1), \ldots, f(b_{n_i}))$$

Weil f ein Homomorphismus ist, folgt daraus $f(\omega_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})) = f(\omega_i^{\mathfrak{A}}(b_1, \ldots, b_{n_i}))$ und somit

$$\omega_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i}) \sim \omega_i^{\mathfrak{A}}(b_1, \ldots, b_{n_i}),$$

d. h. die Verträglichkeit von $\sim$ mit ω_i. Die Verträglichkeit von $\sim$ mit g (Homomorphieeigenschaft von g) liest man aus

$$\begin{aligned} g(\,\omega_i^{\mathfrak{A}/\sim}([a_1]_\sim, \ldots, [a_{n_i}]_\sim)\,) &= g(\,[\omega_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})]_\sim\,) = f(\omega_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})) \\ &= \omega_i^{\mathfrak{C}}(\,f(a_1), \ldots, f(a_{n_i})\,) = \omega_i^{\mathfrak{C}}(\,g([a_1]_\sim), \ldots, g([a_{n_i}]_\sim)\,) \end{aligned}$$

ab. □

Folgerung 2.2.3.18. *Seien $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I})$ und $\mathfrak{C} = (C, (\omega_i^{\mathfrak{C}})_{i\in I})$ Algebren vom selben Typ $(n_i)_{i\in I}$ und $f\colon \mathfrak{A} \to \mathfrak{C}$ ein Homomorphismus. Sei weiters $\sim$ der Kern von f. Für die Unteralgebra $f(\mathfrak{A}) := (f(A), (\omega_i^{\mathfrak{C}})_{i\in I})$ (im surjektiven Fall also $\mathfrak{C}$ selbst) von $\mathfrak{C}$ gilt $f(\mathfrak{A}) \cong \mathfrak{A}/_\sim$, also ist jedes homomorphe Bild einer Algebra isomorph zu einer Faktoralgebra.*

Anmerkung 2.2.3.19. Im Homomorphiesatz 2.2.3.17 beachte man insbesondere den Fall, dass $I = \emptyset$ leer ist, sodass die Aussage in den entsprechenden Sachverhalt betreffend beliebige Abbildungen übergeht. Diese einfachere Aussage war Gegenstand des ersten Teils im Beweis.

UE 98 ► **Übungsaufgabe 2.2.3.20.** (B) Mit C_2 bezeichnen wir die (bis auf Isomorphie einzige) 2-elementige Gruppe, also mit Trägermenge $\{0, 1\}$ und Operation „Addition modulo 2“. Finden Sie alle Kongruenzrelationen auf der 4-elementigen Gruppe Gruppe $C_2 \times C_2$; geben Sie für jede dieser Kongruenzrelationen θ einen surjektiven Homomorphismus $C_2 \times C_2 \to ??$ an, der θ induziert. ◄ **UE 98**

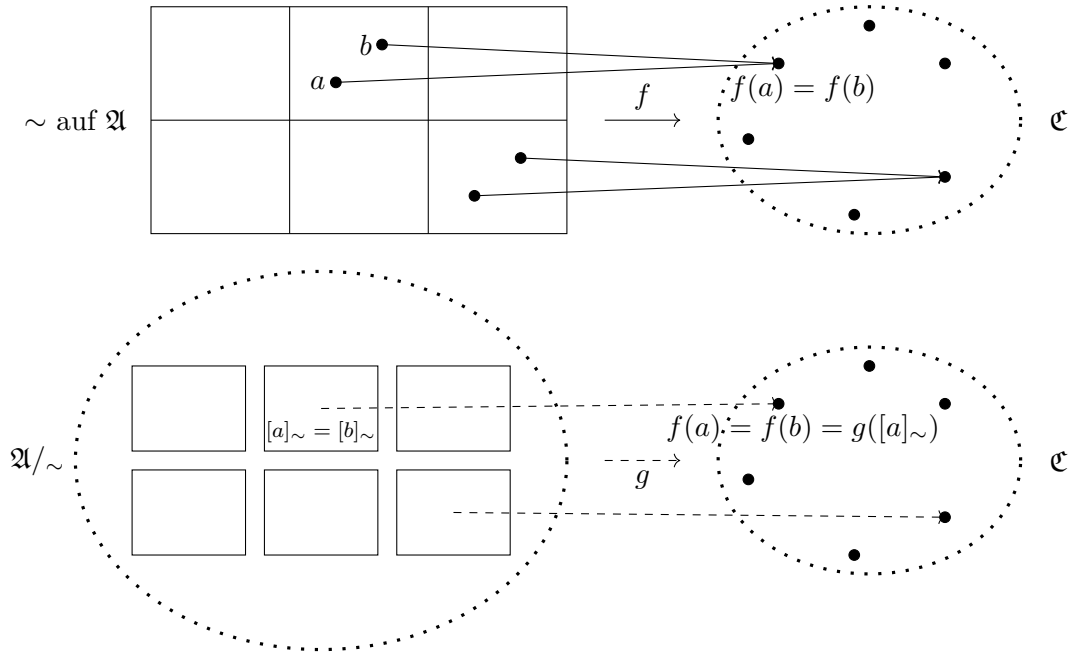


Abbildung 2.1.: Illustration des Homomorphiesatzes.

Beispiel 2.2.3.21. Das klassische Beispiel einer Kongruenzrelation ist Kongruenz modulo m, symbolisch $\equiv_m$, auf $\mathbb{Z}$, definiert durch: $a \equiv_m b$ genau dann, wenn m ein Teiler von $b-a$ ist, symbolisch $m|(b-a)$, wenn es also ein $d \in \mathbb{Z}$ mit $b-a = dm$ gibt. Diese Relation ist nicht nur eine Äquivalenzrelation, sondern auch verträglich mit Addition, Multiplikation und additiver Inversenbildung auf $\mathbb{Z}$ und folglich eine Kongruenzrelation auf dem (kommutativen) Ring $\mathbb{Z}$ (mit 1) – für die Verträglichkeit mit der Multiplikation nimmt man $a \equiv_m b$, $a' \equiv_m b'$ an, formt gemäß $bb'-aa' = bb'-ba'+ba'-aa' = b(b'-a')+(b-a)a'$ um und sieht, dass $aa' \equiv_m bb'$. Das ermöglicht die Konstruktion der Faktoralgebra $\mathbb{Z}_m := \mathbb{Z}/_{\equiv_m}$, des sogenannten *Restklassenrings* modulo m. In Abschnitt 3.4 über Ringe werden wir darauf zurückkommen.

Wie wir aus Proposition 2.2.1.3 und Folgerung 2.2.2.9 wissen, vererben sich Gesetze, wie sie für die Definition von Varietäten verwendet werden, auf Unteralgebren und auf direkte Produkte. Analoges gilt für homomorphe Bilder und Faktoralgebren. Im Wesentlichen liegt das an:

Proposition 2.2.3.22. *Seien $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I})$ und $\mathfrak{B} = (B, (\omega_i^{\mathfrak{B}})_{i\in I})$ Algebren desselben Typs $\tau = (n_i)_{i\in I}$ und $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus. Dann gilt für jeden Term $t = t(x_1, \ldots, x_n)$ und alle $a_1, \ldots, a_n \in A$ die Gleichung*

$$\varphi(t^{\mathfrak{A}}(a_1, \ldots, a_n)) = t^{\mathfrak{B}}(\varphi(a_1), \ldots, \varphi(a_n)).$$

Hieraus folgt fast unmittelbar:

Folgerung 2.2.3.23. *Sei $\mathcal{V}$ eine Varietät mit $\mathfrak{A} \in \mathcal{V}$.*

1. *Ist $\mathfrak{B}$ eine Algebra desselben Typs wie $\mathfrak{A}$ und $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ ein surjektiver Homomorphismus, dann folgt $\mathfrak{B} \in \mathcal{V}$.*
2. *Ist $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$, dann folgt $\mathfrak{A}/_\sim \in \mathcal{V}$.*

UE 99 ► **Übungsaufgabe 2.2.3.24.** (V,W) Beweisen Sie Proposition 2.2.3.22 (Induktion nach der Stufe von t) und folgern Sie daraus 2.2.3.23. ◄ **UE 99**

Beispiele 2.2.3.25. Insbesondere sind folgende Klassen abgeschlossen bezüglich homomorpher Bilder und der Bildung von Faktoralgebren: Halbgruppen, (abelsche) Gruppen, Vektorräume über einem festen Körper, (kommutative) Ringe (mit 1), Verbände und Boolesche Algebren.
Nicht gilt das jedoch für Integritätsbereiche und Körper: Jede Algebra hat, faktorisiert nach der Allrelation, eine einelementige Algebra als Faktoralgebra. Diese ist definitionsgemäß weder Körper noch Integritätsbereich, also gilt Folgerung 2.2.3.23 nicht, wenn man statt einer Varietät $\mathcal{V}$ die Klasse der Körper oder die Klasse der Integritätsbereiche nimmt. Ein nicht einelementiges Beispiel liefert der Integritätsbereich $\mathbb{Z}$ faktorisiert nach $\equiv_m$ für eine zusammengesetzte Zahl (d. h. Nicht-Primzahl) m. Denn auch dann ist, wie wir später noch ausführlicher besprechen werden, der Restklassenring $\mathbb{Z}_m = \mathbb{Z}/_{\equiv_m}$ kein Integritätsbereich.
Diese Überlegungen liefern somit ein weiteres Argument, wieso die Klasse der Körper und die Klasse der Integritätsbereiche keine Varietäten bilden.

2.2.4. Direkte Limiten

Inhalt in Kurzfassung: Zu jeder Familie von Mengen gibt es die Vereinigungsmenge. Hat man es jedoch mit algebraischen Strukturen zu tun, so bildet die Vereinigung in der Regel keine natürliche algebraische Struktur. Sehr wohl lässt sich eine solche aber unter zusätzlichen Voraussetzungen definieren, zum Beispiel in Varietäten, sofern die Algebren in einer verträglichen Weise ineinander eingebettet sind. Die resultierende Struktur zeichnet sich durch eine universelle Eigenschaft aus.

Beispiel 2.2.4.1. Sei $(\mathfrak{R}_n \mid n \in \mathbb{N})$ eine aufsteigende Familie von Ringen mit Einselement. Das heißt:

- Für alle $n \in \mathbb{N}$ ist $\mathfrak{R}_n = (R_n, +_n, 0_n, -_n, \cdot_n, 1_n)$ ein Ring.
- Für alle $n \in \mathbb{N}$ ist $\mathfrak{R}_n$ Unterring von $\mathfrak{R}_{n+1}$; es gilt also $R_n \subseteq R_{n+1}$, $0_n = 0_{n+1}$ sowie $1_n = 1_{n+1}$, und die Operationen $+_n$, $-_n$, $\cdot_n$ sind die Einschränkungen der Operationen $+_{n+1}$, $-_{n+1}$, $\cdot_{n+1}$ auf $\mathfrak{R}_n$ bzw. auf $\mathfrak{R}_n \times \mathfrak{R}_n$.

(Mit anderen Worten: Für alle $n \in \mathbb{N}$ ist die Identitätsabbildung $\mathrm{id}_n\colon R_n \to R_{n+1}$ ein Homomorphismus von Ringen mit 1.)
Dann gibt es genau einen Ring $\mathfrak{R}_\infty$ mit Eins mit folgenden Eigenschaften:

Alle $\mathfrak{R}_n$ sind Unterringe mit 1 von $\mathfrak{R}_\infty$, und für jeden Ring $\mathfrak{S}$ mit Eins und jede Familie von einander fortsetzenden Homomorphismen $\psi_n\colon \mathfrak{R}_n \to \mathfrak{S}$ von Ringen mit 1 gibt es genau einen Homomorphismus $\psi\colon \mathfrak{R}_\infty \to \mathfrak{S}$ von Ringen mit 1, der alle ψ_n fortsetzt.

Beweis. Auf der Menge $R_\infty := \bigcup_n R_n$ lassen sich in natürlicher Weise Ringoperationen definieren. Wenn etwa $x \in R_n$, $y \in R_m$ mit $k := \max(m,n)$ ist, können wir $x +_R y := x +_k y$ setzen, ähnlich für die anderen Operationen. Außerdem setzen wir $0_\infty := 0_n$, $1_\infty := 1_n$ für irgendein (und somit alle) $n \in \mathbb{N}$.
Man überprüft leicht, dass diese Operationen wohldefiniert sind und dass die Struktur $\mathfrak{R}_\infty = (R_\infty, +_\infty, 0_\infty, -_\infty, \cdot_\infty, 1_\infty)$ dadurch zu einen Ring mit Einselement wird. Sind ein Ring $\mathcal{S}$ mit 1 und einander fortsetzende Homomorphismen $\psi_n\colon \mathfrak{R}_n \to \mathcal{S}$ wie oben gegeben, so sieht man schnell, dass $\psi := \bigcup_{n\in\mathbb{N}} \psi_n$ (d. h. $\psi(r) = \psi_n(r)$, wenn $r \in \mathfrak{R}_n$) ein wohldefinierter Homomorphismus ist. Offensichtlich setzt er alle ψ_n fort. Die Eindeutigkeitsaussage folgt daraus, dass die Definitionsbereiche der ψ_n bereits ganz R_∞ ausschöpfen. □

Ein analoger Satz gilt auch für andere algebraische Strukturen:

Satz 2.2.4.2. *Sei $\mathcal{K}$ eine Varietät von Algebren oder die Klasse aller Körper. Seien $\mathfrak{A}_n$, $n \in \mathbb{N}$, Algebren in $\mathcal{K}$, wobei für alle n die Unteralgebrenbeziehung $\mathfrak{A}_n \leq \mathfrak{A}_{n+1}$ gilt. Dann gibt es eine Algebra $\mathfrak{A}_\infty \in \mathcal{K}$ mit folgenden Eigenschaften:*

- *Für alle n gilt: $\mathfrak{A}_n$ ist eine Unteralgebra von $\mathfrak{A}_\infty$.*
- *A_∞, die Trägermenge von $\mathfrak{A}_\infty$, ist die Vereinigung $A_\infty = \bigcup_n A_n$.*
- *(Daher:) Für jede Algebra $\mathfrak{B} \in \mathcal{K}$ und jede Familie $(\psi_n \mid n \in \mathbb{N})$ von einander fortsetzenden Homomorphismen $\psi_n\colon \mathfrak{A}_n \to \mathfrak{B}$ gibt es genau einen Homomorphismus $\psi\colon \mathfrak{A}_\infty \to \mathfrak{B}$, der alle ψ_n fortsetzt.*

UE 100 ► **Übungsaufgabe 2.2.4.3.** (V) Beweisen Sie Satz 2.2.4.2. Überlegen Sie insbesondere, warum die von Ihnen gefundenen Operationen wohldefiniert sind, und warum $\mathfrak{A}_\infty \in \mathcal{K}$ gilt. ◄ **UE 100**

Die folgende Darstellung von $\mathfrak{A}_\infty$ als homomorphes Bild einer Unteralgebra von $\prod_n \mathfrak{A}_n$ wird in Satz 2.2.4.6 zu einer Verallgemeinerung dieser Konstruktion führen.

Satz 2.2.4.4. *Seien $\mathfrak{A}_n$, $n \in \mathbb{N}$, aufsteigende nichtleere[52] Algebren in $\mathcal{K}$ wie in Satz 2.2.4.2, und sei $\mathfrak{A}_\infty$ deren Vereinigung. Dann ist $\mathfrak{A}_\infty$ homomorphes Bild einer geeigneten Unteralgebra von $\prod_{n\in\mathbb{N}} \mathfrak{A}_n$. (Insbesondere vererben sich alle Gesetze, die in allen $\mathfrak{A}_n$ gelten, auf $\mathfrak{A}_\infty$.)*

Beweis. Sei B als die Menge aller Tupel $\bar{a} = (a_i)_{i\in\mathbb{N}}$ definiert, die $\exists i_0 \in \mathbb{N}\ \forall i \geq i_0 : a_i = a_{i_0}$ erfüllen. Wir definieren $\lim \bar{a} = \lim(a_i)_{i\in\mathbb{N}} := a_{i_0}$. Wenn wir A als topologischen Raum mit der diskreten Topologie betrachten, dann ist $\lim \bar{a}$ tatsächlich der Grenzwert

[52] Der Fall $\forall n : A_n = \emptyset$ ist trivial, und im Fall $\exists j : A_j = \emptyset \ \wedge\ \exists j : A_j \neq \emptyset$ muss man beim Produkt der A_n die leeren Faktoren weglassen.

der Folge $\bar{a}$ in diesem Raum. Es ist klar, dass alle Operationen stetig sind; wenn etwa $+$ eine zweistellige Operation ist, dann gilt $\lim(\bar{a} + \bar{b}) = \lim \bar{a} + \lim \bar{b}$.
Auf B definieren wir eine Äquivalenzrelation $\sim$ durch: $(a_i)_{i\in\mathbb{N}} \sim (b_i)_{i\in\mathbb{N}}$ genau dann, wenn es ein $i_1 \in \mathbb{N}$ gibt mit $\forall i \geq i_1 : a_i = b_i$, wenn also die beiden Tupel „schließlich“ übereinstimmen. Anders formuliert gilt $(a_i)_{i\in\mathbb{N}} \sim (b_i)_{i\in\mathbb{N}}$ genau dann, wenn $\lim \bar{a} = \lim \bar{b}$.
Sei $C := B/_\sim$.
Dann ist B ist Trägermenge einer Unteralgebra $\mathfrak{B}$ von $\prod_{i\in\mathbb{N}} \mathfrak{A}_i$: Wenn ω eine k-stellige Operation ist, und $\bar{b}_1, \ldots, \bar{b}_k \in B$, dann wollen wir zeigen, dass auch $\bar{c} := \omega(\bar{b}_1, \ldots, \bar{b}_k)$ in B liegt. Für jedes $j = 1, \ldots, k$ finden wir $i_j \in \mathbb{N}$, sodass die Folge (oder das $\mathbb{N}$-Tupel) $\bar{b}_j$ ab dem i_j-ten Eintrag konstant mit Wert $b(j) = \lim \bar{b}_j$ ist. Wenn wir $i^* := \max(i_1, \ldots, i_k)$ setzen, dann gilt für $j = 1, \ldots, k$, dass alle Folgen $\bar{b}_1, \ldots, \bar{b}_k$ ab dem i^*-ten Eintrag gemeinsam konstant sind, d. h. $(b_j)_{i^*} = (b_j)_{i^*+1} = \cdots = b(j)$. Daher ist auch $\bar{c}$ ab dem i^*-ten Eintrag konstant, nämlich mit Wert $\omega(b(1), \ldots, b(k))$. Somit liegt $\bar{c}$ in B.
Außerdem ist $\sim$ wegen der bereits erwähnten Stetigkeit der Operationen bezüglich der diskreten Topologie auf A eine Kongruenzrelation auf B, also trägt auch C eine algebraische Struktur vom Typ τ. Somit wird C zu einer Faktoralgebra $\mathfrak{C}$.
Schließlich gilt $\mathfrak{C} \cong \mathfrak{A}_\infty$: Man prüft nach, dass die Abbildung $\lim\colon C \to A_\infty$ ein Isomorphismus ist. Um die Surjektivität zu zeigen, muss man für jedes $a \in A_\infty$ eine Folge $\bar{b} \in B$ mit Grenzwert a finden. Wenn $a \in A_i$ gilt, dann können wir eine Folge $\bar{b} = (b_0, b_1, \ldots)$ finden, deren Werte $b_0 \in A_0$, …, $b_{i-1} \in A_{i-1}$ beliebig sind, und die ab i den konstanten Wert $b_i = b_{i+1} = \cdots = a$ hat.
Insgesamt ist $\mathfrak{B}$ also eine Unteralgebra von $\prod_{n\in\mathbb{N}} \mathfrak{A}_n$; weiters ist $\mathfrak{A}_\infty$ isomorph zur Faktoralgebra (insbesondere homomorphes Bild) $\mathfrak{C}$ von $\mathfrak{B}$. Somit ist $\mathfrak{A}_\infty$ ein homomorphes Bild einer Unteralgebra des Produkts der $\mathfrak{A}_n$. □

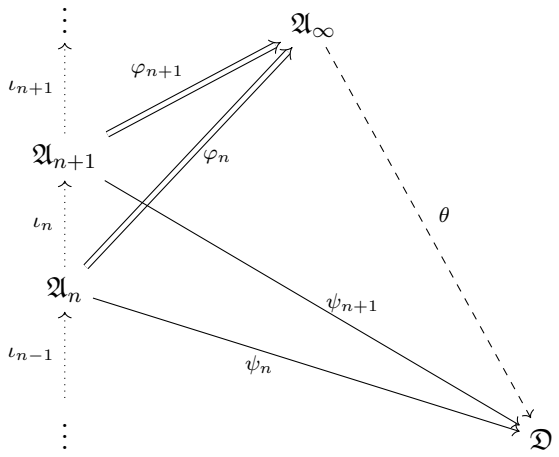
Anmerkung 2.2.4.5. Der Fall, dass $\mathcal{K}$ die Klasse aller Körper ist, verdient gesonderte Beachtung: Aus den Beispielen 2.2.2.10 und 2.2.3.25 wissen wir, dass direkte Produkte sowie Faktoren/homomorphe Bilder von Körpern niemals bzw. nicht unbedingt Körper sind, sondern im Allgemeinen nur kommutative Ringe mit Einselement. Dennoch ist $\mathfrak{A}_\infty$ nach Satz 2.2.4.2 wieder ein Körper, obwohl man in der Konstruktion aus Satz 2.2.4.4 die Klasse der Körper „zwischendurch“ verlässt.

In Satz 2.2.4.2 haben wir eine aufsteigende Familie von Algebren betrachtet; wenn man statt $\mathfrak{A}_n \leq \mathfrak{A}_{n+1}$ verlangt, dass es einen injektiven Homomorphismus $\iota_n : \mathfrak{A}_n \to \mathfrak{A}_{n+1}$ gibt, so erhält man eine ganz ähnliche Situation, die man durch Umbenennung (oder Identifikation von Elementen mit ihren ι-Bildern) auf Satz 2.2.4.2 zurückführen kann: man benennt für jedes $a_1 \in A_1$ das Element $\iota_1(a_1) \in A_2$ in $a_1 \in A_1$ um, danach für alle a_2 aus der (bereits teilweise umbenannten!) Menge A_2 das Element $\iota_2(a_2) \in A_3$ in $a_2 \in A_2$, und so weiter.
Die folgende Konstruktion ist eine interessante Verallgemeinerung, bei der man nicht mehr die Injektivität der Abbildungen ι_n verlangt. Im Spezialfall $\mathfrak{A}_n \leq \mathfrak{A}_{n+1}$ und $\iota_n = \mathrm{id}_{A_n}$ ergibt sich einfach Satz 2.2.4.2.

Satz 2.2.4.6. *Sei $\mathcal{K}$ eine Varietät von Algebren oder die Klasse aller Körper. Seien $\mathfrak{A}_n, n \in \mathbb{N}$, Algebren in $\mathcal{K}$, und seien $\iota_n\colon \mathfrak{A}_n \to \mathfrak{A}_{n+1}$ Homomorphismen.*
Dann gibt es eine Algebra $\mathfrak{A}_\infty \in \mathcal{K}$ sowie Abbildungen φ_n mit folgenden Eigenschaften:

- *Für alle n ist $\varphi_n \colon \mathfrak{A}_n \to \mathfrak{A}_\infty$ ein Homomorphismus.*
- *Für alle n ist $\varphi_n = \varphi_{n+1} \circ \iota_n$.*
- *Für jede Algebra $\mathfrak{D} \in \mathcal{K}$ und jede Familie $(\psi_n \mid n \in \mathbb{N})$ von Homomorphismen $\psi_n \colon \mathfrak{A}_n \to \mathfrak{D}$, die $\psi_n = \psi_{n+1} \circ \iota_n$ für alle $n \in \mathbb{N}$ erfüllen, gibt es genau einen Homomorphismus $\theta \colon \mathfrak{A}_\infty \to \mathfrak{D}$ mit $\theta \circ \varphi_n = \psi_n$ für alle $n \in \mathbb{N}$.*

Diese Algebra nennt man direkter Limes *des Systems $((\mathfrak{A}_n)_{n\in\mathbb{N}}, (\iota_n)_{n\in\mathbb{N}})$. Dabei kann man die Algebra $\mathfrak{A}_\infty$ als homomorphes Bild einer Unteralgebra von $\prod_{n\in\mathbb{N}} \mathfrak{A}_n$ erhalten.*



Beweis. Wir betrachten zunächst den Fall, dass $\mathcal{K}$ die Klasse aller Körper ist. Wie wir in Proposition 3.4.2.2 zeigen werden, sind Homomorphismen von einem Körper in einen nichttrivialen Ring (insbesondere Homomorphismen zwischen Körpern) immer injektiv. Somit können wir wie oben beschrieben durch Umbenennen der Elemente erreichen, dass eine aufsteigende Familie von Körpern vorliegt, und können Satz 2.2.4.2 kombiniert mit Satz 2.2.4.4 verwenden.
Sei jetzt $\mathcal{K}$ eine Varietät; in diesem Fall müssen die ι_n nicht zwingend injektiv sein. Der Beweis entsteht dennoch nur durch eine geringfügige Modifikation des Beweises von Satz 2.2.4.4.
Sei B als die Menge aller Tupel $\bar{a} = (a_i)_{i\in\mathbb{N}}$ definiert, die $\exists i_0 \in \mathbb{N}\ \forall i \geq i_0 : a_{i+1} = \iota_i(a_i)$ erfüllen. Auf B definieren wir wiederum eine Äquivalenzrelation $\sim$ durch $\bar{a} \sim \bar{b}$ genau dann, wenn es ein $i_1 \in \mathbb{N}$ gibt mit $\forall i \geq i_1 : a_i = b_i$, wenn also die beiden Tupel „schließlich“ übereinstimmen.
Sei $A_\infty := B/\!\sim$. Dann ist B Trägermenge einer Unteralgebra $\mathfrak{B}$ von $\prod_{i\in\mathbb{N}} \mathfrak{A}_i$, und $\sim$ ist eine Kongruenzrelation auf $\mathfrak{B}$. Somit trägt auch A_∞ eine algebraische Struktur, wird also zu einer Faktoralgebra $\mathfrak{A}_\infty$.
Wir definieren $\varphi_n : \mathfrak{A}_n \to \mathfrak{A}_\infty$ in natürlicher Weise: Für jedes $a \in \mathfrak{A}_n$ wählen wir eine Folge $\bar{b} = (b_i)_{i\in\mathbb{N}}$ in $\prod_{i\in\mathbb{N}} \mathfrak{A}_i$ mit den folgenden Eigenschaften:

- Für $i < n$ sei $b_i \in R_i$ beliebig.
- $b_n = a$.

- $b_{n+1} = \iota_n(b_n)$, und weiter $b_{m+1} = \iota_m(b_m)$ für alle $m \geq n$.

Dann ist $\bar{b}$ in der Algebra B. (Durch diese Eigenschaften ist zwar $\bar{b}$ nicht eindeutig bestimmt, wohl aber die $\sim$-Äquivalenzklasse von $\bar{b}$.)
Sei $\varphi_n(a)$ die $\sim$-Äquivalenzklasse von $\bar{b}$.
Wir beobachten, dass A_∞ die Vereinigung der Bilder $\varphi_n(A_n)$ ist: Für $[(b_i)_{i\in\mathbb{N}}] \in A_\infty$ gibt es $i_0 \in \mathbb{N}$ mit $\forall i \geq i_0 : b_{i+1} = \iota_i(b_i)$. Dann gilt $[(b_i)_{i\in\mathbb{N}}] = \varphi_{i_0}(b_{i_0})$ und wir erhalten tatsächlich $A_\infty = \bigcup_{n\in\mathbb{N}} \varphi_n(A_n)$.
Somit bleibt zu zeigen, dass es zu $\mathfrak{D} \in \mathcal{K}$ und einer Familie $(\psi_n \mid n \in \mathbb{N})$ von Homomorphismen $\psi_n \colon \mathfrak{A}_n \to \mathfrak{D}$, die $\forall n : \psi_n = \psi_{n+1} \circ \iota_n$ erfüllen, stets genau einen Homomorphismus $\theta \colon \mathfrak{A}_\infty \to \mathfrak{D}$ gibt, der $\forall n : \psi \circ \varphi_n = \psi_n$ erfüllt. Ist $[(b_i)_{i\in\mathbb{N}}]_\sim \in A_\infty$ gegeben, so gibt es $i_0 \in \mathbb{N}$ mit $\forall i \geq i_0 : b_{i+1} = \iota_i(b_i)$. Dann gilt für alle $i \geq i_0$, dass $\psi_i(b_i) = \psi_{i+1}(\iota_i(b_i)) = \psi_{i+1}(b_{i+1})$. Wir definieren $\theta([(b_i)_{i\in\mathbb{N}}]_\sim) := \psi_i(b_i)$ für irgendein $i \geq i_0$ (nach dem gerade Gezeigten stimmen diese Werte für alle $i \geq i_0$ überein) und bemerken, dass die θ wohldefiniert ist, d. h. nicht vom gewählten $\sim$-Repräsentanten abhängt. Man rechnet leicht nach, dass θ ein Homomorphismus ist, der $\forall n : \theta \circ \varphi_n = \psi_n$ erfüllt. Wegen $\forall n : \theta \circ \varphi_n = \psi_n$ ist die Einschränkung von θ auf $\varphi_n(A_n)$ bereits festgelegt; aus $A_\infty = \bigcup_{n\in\mathbb{N}} \varphi_n(A_n)$ folgt damit die Eindeutigkeit von θ auf ganz A_∞. □

2.2.5. Triviale und nichttriviale Varietäten

Inhalt in Kurzfassung: Für Varietäten gilt eine bemerkenswerte Dichotomie. Und zwar enthält eine Varietät entweder nur höchstens einelementige Algebren und eventuell die leere Algebra (trivialer Fall) oder Algebren beliebig großer Kardinalität.

Gilt in einer Varietät $\mathcal{V}$ eines Typs τ das Gesetz $x \approx y$, so müssen in jeder Algebra $\mathfrak{A} \in \mathcal{V}$ je zwei Elemente gleich sein. Folglich enthält $\mathcal{V}$ nur einelementige Algebren (von denen je zwei zueinander isomorph sind) und, wenn im Typ τ keine 0-stelligen Operationen vorkommen, die leere Algebra. In diesem Fall heißt $\mathcal{V}$ jeweils die *triviale Varietät* (oder: ausgeartete Varietät) zum Typ τ. Gilt das Gesetz $x \approx y$ in $\mathcal{V}$ hingegen nicht, so gibt es zumindest ein $\mathfrak{A} \in \mathcal{V}$ mit mehr als einem Element. Wegen Folgerung 2.2.2.9 liegen dann auch alle Potenzen $\mathfrak{A}^M = \prod_{m\in M} \mathfrak{A}_m$ (wobei für jedes $m \in M$ die Algebra $\mathfrak{A}_m$ gleich der Algebra $\mathfrak{A}$ ist) in $\mathcal{V}$, und somit Algebren von beliebig großer Kardinalität. Also:

Proposition 2.2.5.1. *Für eine Varietät $\mathcal{V}$ zum Typ $\tau = (n_i)_{i\in I}$ gilt genau einer der folgenden beiden Fälle:*

1. *$\mathcal{V}$ ist die triviale Varietät und enthält ausschließlich einelementige Algebren sowie, falls $n_i > 0$ für alle $i \in I$, die leere Algebra.*

2. *$\mathcal{V}$ ist nichttrivial und enthält zu jeder vorgegebenen Kardinalität κ eine Algebra mit einer Trägermenge A, die $|A| \geq \kappa$ erfüllt.*

Gelegentlich werden wir „ohne Beschränkung der Allgemeinheit“ triviale Varietäten von unseren Überlegungen ausschließen, oder genauer: nur nichttriviale Varietäten betrach-

ten, und den (meist uninteressanten) Fall der trivialen Varietäten dem Leser[53] überlassen.

Beispiel 2.2.5.2. Wegen Proposition 2.2.5.1 ist nun auch klar, dass die in Beispiel 2.1.8.7 erwähnte (und jedenfalls nichttriviale) Klasse aller endlichen Gruppen keine Varietät bilden kann.

2.2.6. Isomorphiesätze

Inhalt in Kurzfassung: In den beiden Isomorphiesätzen geht es vor allem darum, dass verschiedene Konstruktionen zu isomorphen Strukturen führen. Im ersten wird die Reihenfolge der Bildung einer Unter- und einer Faktoralgebra vertauscht; im zweiten werden zwei Faktorisierungen durch eine einzige ersetzt. Der zweite liefert darüber hinaus die Isomorphie des Kongruenzverbandes einer Faktoralgebra mit einem Teilintervall des Kongruenzverbandes der ursprünglichen Algebra.

Lemma 2.2.6.1. *Sei $\mathfrak{A}$ eine Algebra, θ eine Kongruenzrelation und $\mathfrak{B}$ eine Unteralgebra von $\mathfrak{A}$. Dann ist $[B]_\theta := \bigcup_{b\in B}[b]_\theta$ unter den Operationen von $\mathfrak{A}$ abgeschlossen, also die Trägermenge einer Unteralgebra $[\mathfrak{B}]_\theta$ von $\mathfrak{A}$.*

Beweis. Sei ω eine n-stellige Operation von $\mathfrak{A}$ und seien $a_1, \dots, a_n \in [B]_\theta$. Letzteres bedeutet gerade, dass es $b_1, \dots, b_n \in B$ gibt mit $a_i \ \theta \ b_i$. Es folgt $\omega(a_1, \dots, a_n) \ \theta \ \omega(b_1, \dots, b_n)$. Weil $\mathfrak{B}$ eine Unteralgebra ist, gilt $\omega(b_1, \dots, b_n) \in B$ und daher $\omega(a_1, \dots, a_n) \in [B]_\theta$. □

Notation 2.2.6.2. Sei θ eine Äquivalenzrelation auf einer Menge $A \supseteq B$. Dann ist $\theta|_B := \theta \cap (B \times B)$ eine Äquivalenzrelation auf B. Um die Notation zu vereinfachen, schreiben wir in so einem Fall oft auch B/θ statt $B/(\theta|_B)$.

Satz 2.2.6.3 (Erster Isomorphiesatz)**.** *(Saloppe Formulierung: Faktorisierung und Übergang zu einer Unteralgebra sind miteinander verträglich.) Sei $\mathfrak{A}$ eine Algebra, θ eine Kongruenzrelation auf $\mathfrak{A}$ und $\mathfrak{B}$ eine Unteralgebra von $\mathfrak{A}$. Sei außerdem $[B]_\theta := \bigcup_{b\in B}[b]_\theta$. Dann gilt*

$$\mathfrak{B}/\theta \cong [\mathfrak{B}]_\theta/\theta.$$

Ein Isomorphismus ist gegeben durch $[b]_{\theta|_B} \mapsto [b]_{\theta|_{[B]_\theta}}$.

Beweis. Sei $\varphi\colon \mathfrak{A} \to \mathfrak{A}/\theta$, $\varphi(a) := [a]_\theta$, der kanonische Homomorphismus. Bezeichne außerdem $\mathfrak{D}$ die Unteralgebra von $\mathfrak{A}/\theta$ auf $D := \varphi(B)$. Dann ist $\theta|_B = \ker(\varphi|_B)$, nach dem Homomorphiesatz 2.2.3.17 folgt also $\mathfrak{B}/\theta \cong \mathfrak{D}$ via $g_1 : [b]_{\theta|_B} \mapsto \varphi(b)$.
Weiters ist $[B]_\theta = \varphi^{-1}(D)$, und $\varphi([B]_\theta) = D$. Ähnlich wie vorhin ist $\theta|_{[B]_\theta} = \ker(\varphi|_{[B]_\theta})$, daher wiederum $[\mathfrak{B}]_\theta/\theta \cong \mathfrak{D}$ via $g_2 : [b]_{\theta|_{[B]_\theta}} \mapsto \varphi(b)$.
Insgesamt ergibt sich $\mathfrak{B}/\theta \cong [\mathfrak{B}]_\theta/\theta$ via $g_2^{-1} \circ g_1 : [b]_{\theta|_B} \mapsto [b]_{\theta|_{[B]_\theta}}$. □

[53] Selbstverständlich: allen, die diesen Text lesen – Lesern, Leserinnen, Leser:innen, und small furry creatures from Alpha Centauri.

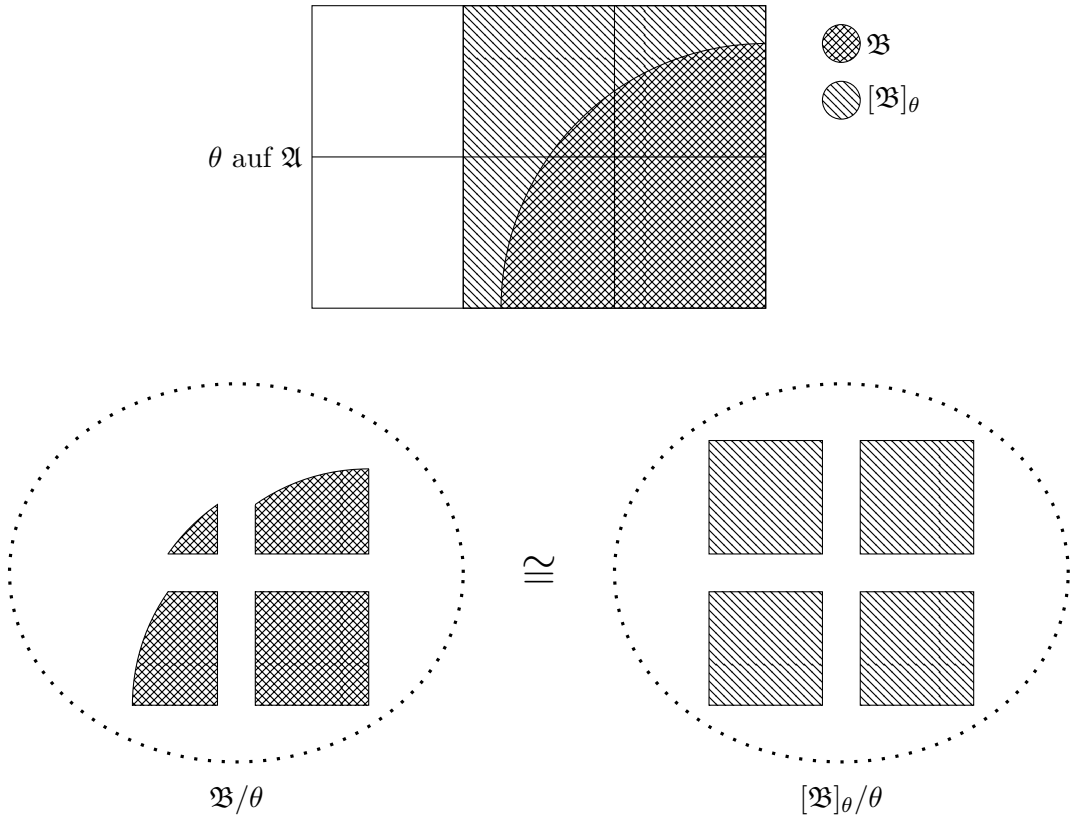


Abbildung 2.2.: Illustration des ersten Isomorphiesatzes.

UE 101 ► **Übungsaufgabe 2.2.6.4.** (F) Auf der Menge $M = \{1, 2, 3, 4, 5\}$ betrachten wir die Äquivalenzrelation θ, die durch die Partition $\{\{1, 2\}, \{3, 4\}, \{5\}\}$ gegeben ist, sowie die Untermenge $U := \{4, 5\}$. Definieren Sie auf der Menge M eine Algebra $\mathfrak{M}$, sodass θ eine Kongruenz ist und U eine Unteralgebra, und geben Sie explizit den Isomorphismus an, der im ersten Isomorphiesatz beschrieben wird. Um eine triviale Lösung zu vermeiden, verlangen wir zusätzlich, dass es neben der Allrelation keine Kongruenz $\sim$ mit $2 \sim 3$ gibt. ◄ **UE 101**

Mit der folgenden Aussage steuern wir auf den zweiten Isomorphiesatz zu:

Lemma 2.2.6.5. *Es seien θ_1 und θ_2 Kongruenzrelationen auf einer Algebra $\mathfrak{A}$ mit $\theta_1 \subseteq \theta_2$. Dann ist die Relation*

$$\theta_2/\theta_1 := \{([a]_{\theta_1}, [b]_{\theta_1}) \mid (a, b) \in \theta_2\}$$

eine Kongruenzrelation auf $\mathfrak{A}/\theta_1$.

Beweis. Die Reflexivität und Symmetrie von θ_2/θ_1 folgen unmittelbar aus den entsprechenden Eigenschaften von θ_2 (siehe auch Übungsaufgabe 2.2.6.6), womit θ_2/θ_1 eine Äquivalenzrelation ist. Außerdem gilt

$$\forall x, y \in A : ([x]_{\theta_1}, [y]_{\theta_2}) \in \theta_2/\theta_1 \Leftrightarrow (x, y) \in \theta_2$$

(und nicht nur die direkt aus der Definition folgende Richtung $\Leftarrow$). Daraus folgt dann auch die Transitivität von θ_2/θ_1. Den Beweis dieser Tatsachen überlassen wir der Leserin[54] in Übungsaufgabe 2.2.6.6.
Sei nun ω eine beliebige n-stellige Operation von $\mathfrak{A}$ (und damit auch von $\mathfrak{A}/\theta_1$) sowie $([a_1]_{\theta_1}, [b_1]_{\theta_1}), \ldots, ([a_n]_{\theta_1}, [b_n]_{\theta_1}) \in \theta_2/\theta_1$. Dies bedeutet, dass $(a_i, b_i) \in \theta_2$ für $1 \leq i \leq n$. Weil θ_2 eine Kongruenz ist, folgt daraus auch

$$(\omega(a_1, \ldots, a_n), \omega(b_1, \ldots, b_n)) \in \theta_2,$$

also $([\omega(a_1, \ldots, a_n)]_{\theta_1}, [\omega(b_1, \ldots, b_n)]_{\theta_1}) \in \theta_2/\theta_1$. Zusammen mit $\omega([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1}) = [\omega(a_1, \ldots, a_n)]_{\theta_1}$ und der entsprechenden Gleichheit für die b_i erhalten wir

$$(\omega([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1}), \omega([b_1]_{\theta_1}, \ldots, [b_n]_{\theta_1})) \in \theta_2/\theta_1.$$

Wir haben damit gezeigt, dass θ_2/θ_1 mit der Operation ω verträglich ist. Da ω beliebig war, ist θ_2/θ_1 somit eine Kongruenz. □

UE 102 ► **Übungsaufgabe 2.2.6.6.** (F,V) Seien A eine Menge, θ_1, θ_2 Äquivalenzrelationen auf A und θ_2/θ_1 wie in Lemma 2.2.6.5 definiert. ◄ **UE 102**

1. Zeigen Sie: Wenn zusätzlich $\theta_1 \subseteq \theta_2$, dann gilt für alle $x, y \in A$ die Äquivalenz $([x]_{\theta_1}, [y]_{\theta_1}) \in \theta_2/\theta_1 \Leftrightarrow (x, y) \in \theta_2$. Außerdem ist θ_2/θ_1 eine Äquivalenzrelation.
2. Geben Sie ein Beispiel von einer Menge A und Äquivalenzrelationen θ_1, θ_2 sowie von Elementen $x, y \in A$ an derart, dass die Aussagen $([x]_{\theta_1}, [y]_{\theta_1}) \in \theta_2/\theta_1$ und $(x, y) \in \theta_2$ nicht äquivalent sind.
3. Zeigen Sie: Wenn die Aussagen $([x]_{\theta_1}, [y]_{\theta_1}) \in \theta_2/\theta_1$ und $(x, y) \in \theta_2$ für alle $x, y \in A$ äquivalent sind, dann gilt schon $\theta_1 \subseteq \theta_2$.

Satz 2.2.6.7 (Zweiter Isomorphiesatz)**.** *(Saloppe verbale Formulierung: Iterierte Faktorisierung lässt sich durch eine einzige ersetzen.) Sei $\mathfrak{A}$ eine Algebra, seien $\theta_1 \subseteq \theta_2$ Kongruenzen auf $\mathfrak{A}$ und sei $\theta_2/\theta_1 := \{([a]_{\theta_1}, [b]_{\theta_1}) \mid (a, b) \in \theta_2\}$ die Kongruenz aus Lemma 2.2.6.5. Dann gilt*

$$(\mathfrak{A}/\theta_1)/(\theta_2/\theta_1) \cong \mathfrak{A}/\theta_2$$

vermittels des Isomorphismus

$$f\colon (\mathfrak{A}/\theta_1)/(\theta_2/\theta_1) \to \mathfrak{A}/\theta_2, \quad [[a]_{\theta_1}]_{\theta_2/\theta_1} \mapsto [a]_{\theta_2}.$$

[54] Siehe Fußnote auf Seite 107.

Überdies gilt für jede Kongruenzrelation $\theta \in \mathrm{Con}(\mathfrak{A})$: Das Intervall

$$[\theta, \nabla] := \{\psi \in \mathrm{Con}(\mathfrak{A}) \mid \theta \subseteq \psi\}$$

im Kongruenzverband $\mathrm{Con}(\mathfrak{A})$ *ist ein Unterverband von* $\mathrm{Con}(\mathfrak{A})$ *und isomorph zum Kongruenzverband* $\mathrm{Con}(\mathfrak{A}/\theta)$ *der Faktoralgebra. Ein Verbandsisomorphismus ist gegeben durch*

$$k\colon [\theta, \nabla] \to \mathrm{Con}(\mathfrak{A}/\theta) \quad k(\psi) := \psi/\theta.$$

Beweis. Wir betrachten zunächst die Abbildung $g : [a]_{\theta_1} \mapsto [a]_{\theta_2}$. Sie ist als Abbildung $g : A/\theta_1 \to A/\theta_2$ wohldefiniert, denn sind $a, b \in A$ mit $[a]_{\theta_1} = [b]_{\theta_1}$, so gilt wegen $\theta_1 \subseteq \theta_2$ auch $[a]_{\theta_2} = [b]_{\theta_2}$. Die Surjektivität von g ist offensichtlich. Die Homomorphiebedingung gilt, weil für eine beliebige n-stellige Operation ω von $\mathfrak{A}$ (und damit auch von beiden Faktoralgebren) sowie für $a_1, \ldots, a_n \in A$

$$\begin{aligned} g(\omega([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1})) &= g([\omega(a_1, \ldots, a_n)]_{\theta_1}) = [\omega(a_1, \ldots, a_n)]_{\theta_2} = \\ &= \omega([a_1]_{\theta_2}, \ldots, [a_n]_{\theta_2}) = \omega(g([a_1]_{\theta_1}), \ldots, g([a_n]_{\theta_1})) \end{aligned}$$

gilt. Insgesamt ist g also ein surjektiver Homomorphismus mit Kern $\ker g = \theta_2/\theta_1 \in \mathrm{Con}(\mathfrak{A}/\theta_1)$. Nach dem Homomorphiesatz 2.2.3.17 folgt daher, dass f wie in der Aussage des Satzes tatsächlich ein Isomorphismus für $(\mathfrak{A}/\theta_1)/(\theta_2/\theta_1) = (\mathfrak{A}/\theta_1)/(\ker g) \cong \mathfrak{A}/\theta_2$ ist.

Nun zur Abbildung k: Lemma 2.2.6.5 zeigt $k\colon [\theta, \nabla] \to \mathrm{Con}(\mathfrak{A}/\theta)$. Klarerweise ist k mit $\subseteq$ stark verträglich, denn für $\theta \subseteq \psi_1, \psi_2$ gilt $\psi_1 \subseteq \psi_2$ genau dann, wenn $\psi_1/\theta \subseteq \psi_2/\theta$. Schließlich gibt es zu jedem $\Psi \in \mathrm{Con}(\mathfrak{A}/\theta)$ genau ein $\psi \in [\theta, \nabla] \subseteq \mathrm{Con}(\mathfrak{A})$ mit $k(\psi) = \Psi$, nämlich $\psi = \{(a, b) \in A^2 : \ ([a]_\theta, [b]_\theta) \in \Psi\}$. Folglich ist k bijektiv, somit ein Isomorphismus zwischen den $\subseteq$-Halbordnungen $[\theta, \nabla] \subseteq \mathrm{Con}(\mathfrak{A})$ und $\mathrm{Con}(\mathfrak{A}/\theta)$. Da beides Verbände sind, handelt es sich bei k sogar um einen Verbandsisomorphismus. □

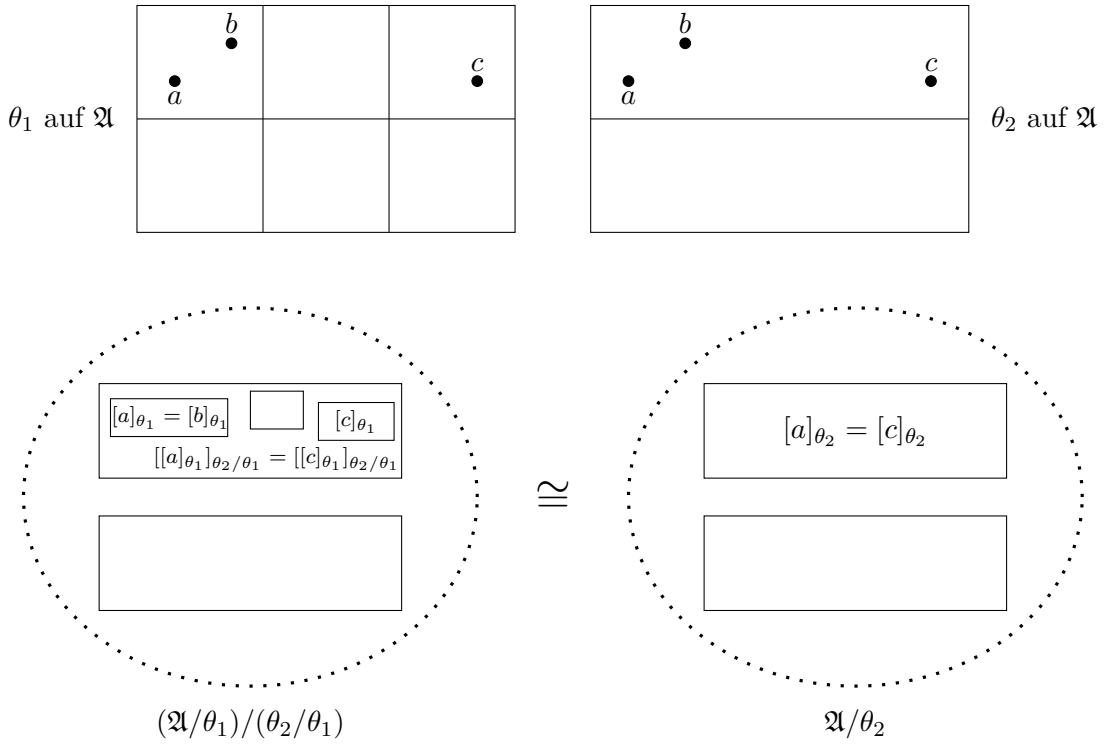
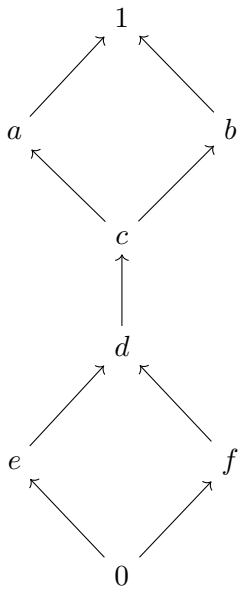


Abbildung 2.3.: Illustration des zweiten Isomorphiesatzes.

UE 103 ▶ Übungsaufgabe 2.2.6.8. (B) **◀ UE 103**

Sei V der durch das nebenstehende Hasse-Diagramm gegebene Verband.



(1) Begründen Sie, dass diese partielle Ordnung tatsächlich einen Verband definiert.

Ab nun betrachten wir V als Algebra.

(2) Finden Sie zwei nichttriviale Kongruenzrelationen θ_2 und θ_1 mit $\theta_1 \subsetneq \theta_2$.

(3) Geben Sie V/θ_2, V/θ_1, θ_2/θ_1 und $(V/\theta_1)/(\theta_2/\theta_1)$ an.

(4) Sei $\theta = \{(0,0),(e,e),(f,f)\} \cup (V \setminus \{0,e,f\})^2$. Finden Sie einen Verband V' und einen Homomorphismus $\varphi\colon V \to V'$ (im Sinne der Algebra), der die Kongruenzrelation θ induziert.

(5) Seien V und θ wie bisher und $B = \{0,1\}$. Geben Sie $\theta|_B$, $[B]_\theta$, $\theta|_{[B]_\theta}$, B/θ, und $[B]_\theta/\theta$ an.

UE 104 ► **Übungsaufgabe 2.2.6.9.** (B) Sei $M = \{1, 2, 3, 4, 5\}$. Auf M betrachten wir die Äquivalenzrelationen, die durch die Partitionen $\{\{1, 2\}, \{3\}, \{4\}, \{5\}\}$ und $\{\{1, 2\}, \{3, 4, 5\}\}$ gegeben sind. Definieren Sie auf der Menge M eine Algebra $\mathfrak{M}$, sodass diese beiden Relationen die einzigen nichttrivialen Kongruenzen von $\mathfrak{M}$ sind, und geben Sie explizit den Isomorphismus an, der im zweiten Isomorphiesatz beschrieben wird. ◄ **UE 104**

2.3. Der kategorientheoretische Rahmen

In mancherlei Hinsicht noch wesentlich weiter gefasst als die bisherigen Strukturen eines gewissen Typs ist der begriffliche Rahmen der *Kategorientheorie*. Er erlaubt es, neben algebraischen und relationalen Strukturen z. B. auch topologische, maßtheoretische und viele andere in geeignete Klassen zusammenzufassen. Dazu ist es deutlich mehr als bisher nötig, nicht nur Mengen in Betracht zu ziehen, sondern auch echte *Klassen*, d. h. Klassen, die keine Mengen sind.[55]
Unterabschnitt 2.3.1 bringt dazu die grundlegenden Definitionen, 2.3.2 einige typische Beispiele. In 2.3.3 findet sich jener (in wenigen Zeilen beweisbare) Satz, den wir an vielen Stellen gewinnbringend einsetzen werden: Universelle (d. h. initiale bzw. finale) Objekte sind bis auf Äquivalenz eindeutig bestimmt, was in unseren Anwendungsbeispielen insbesondere Isomorphie bedeutet. In vielen Situationen lohnt es auch das Konzept des Funktors (2.3.4) zu kennen. Es ist das kategorientheoretische Analogon zum Homomorphismus zwischen Algebren. Eine auf den ersten Blick überraschende, ebenfalls aber höchst praktische Anwendung dieses Begriffs sind kommutative Diagramme, der Gegenstand von 2.3.5. Einen etwas weiteren Ausblick eröffnen natürliche Transformationen (2.3.6).

2.3.1. Kategorien

Inhalt in Kurzfassung: Dem Begriff der Kategorie liegt die Idee zugrunde, dass es von Interesse ist, Strukturen gleicher Art (seien es algebraische, relationale, topologische etc.) als sogenannte Objekte zu einer Klasse zusammenzufassen und die strukturverträglichen Abbildungen (Morphismen) zwischen je zwei solchen Objekten zu betrachten. Die formale Definition einer Kategorie ist extrem allgemein und Gegenstand dieses Unterabschnitts.

Wir definieren den Begriff der „Kategorie“, sowie den der „konkreten Kategorie“.

[55] In der Mengenlehre, die durch die ZFC-Axiome (von Zermelo und Fraenkel) beschrieben wird, gibt es gar keine Klassen; wenn man aber doch von Klassen spricht, wie etwa der Klasse aller Gruppen, dann spricht man in Wirklichkeit über die *Eigenschaft*, eine Gruppe zu sein; man kann beweisen, dass es keine Menge gibt, die alle Gruppen als Elemente enthält. In anderen Formulierungen der Mengenlehre, etwa im System NBG, das auf von Neumann, Bernays und Gödel zurückgeht, gibt es neben den Mengen auch „echte Klassen“ oder „Unmengen“, die zwar (ebenso wie Mengen) dadurch bestimmt sind, welche Elemente sie enthalten, die aber selbst nicht als Elemente anderer Klassen oder Mengen auftreten können. Typischerweise kommt eine Klasse zustande durch Zusammenfassung aller Objekte mit einer bestimmen Eigenschaft, was ja ziemlich genau dem Inhalt der historisch ersten Mengendefinition von Cantor entspricht. Die Einschränkungen beim Umgang mit Klassen gegenüber dem mit Mengen sind nötig, um Paradoxien von der Art jener von Russell zu vermeiden.

Definition 2.3.1.1. Eine *Kategorie* $\mathcal{C}$ ist gegeben durch

(i) eine Klasse von *Objekten* $A, B, \ldots \in \mathrm{Ob}(\mathcal{C})$ zusammen

(ii) mit einer Klasse paarweise disjunkter Mengen[56] $\mathrm{Hom}(A,B) = \mathrm{Hom}_{\mathcal{C}}(A,B)$ von *Morphismen* f (für alle $A, B \in \mathrm{Ob}(\mathcal{C})$);

(iii) und einer Klasse von *Kompositionen*, geschrieben $(g,f) \mapsto g \circ f$,

$$\mathrm{Hom}(B,C) \times \mathrm{Hom}(A,B) \to \mathrm{Hom}(A,C)$$

für alle $A, B, C \in \mathrm{Ob}(\mathcal{C})$,

die die untenstehenden Eigenschaften (I) und (II) erfüllen.
Statt $A \in \mathrm{Ob}(\mathcal{C})$ schreiben wir oft nur $A \in \mathcal{C}$. Statt $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ schreiben wir auch $f\colon A \to B$ oder $f\colon A \to^{\mathcal{C}} B$; wir nennen A die *Quelle* und B das *Ziel* von f.

(I) *Assoziativgesetz*: $\forall A, B, C, D \in \mathrm{Ob}(\mathcal{C})\ \forall f\colon A \to B, g\colon B \to C, h\colon C \to D$:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

(II) *Identität*: Für jedes Objekt $B \in \mathrm{Ob}(\mathcal{C})$ gibt es einen ausgezeichneten Morphismus $1_B \in \mathrm{Hom}(B,B)$, genannt die Identität auf B, sodass für alle $A, C \in \mathrm{Ob}(\mathcal{C})$ und alle $f\colon A \to B$ sowie $g\colon B \to C$ gilt:

$$1_B \circ f = f$$
$$g \circ 1_B = g$$

Ein Morphismus $f\colon A \to B$ heißt *Äquivalenz*, falls es ein $g\colon B \to A$ gibt mit $g \circ f = 1_A$ und $f \circ g = 1_B$. In diesem Fall heißen A und B *äquivalent*, i.Z. $A \cong B$.
Bilden die Objekte einer Kategorie $\mathcal{C}$ eine Menge, so spricht man auch von einer *kleinen Kategorie*.

Wir werden noch zahlreiche Beispiele von Kategorien kennen lernen. Sehr typisch ist etwa die Kategorie der Gruppen mit den Gruppenhomomorphismen als Morphismen und der üblichen Verkettung von Abbildungen als Komposition. Da die Gruppen keine Menge bilden (es gibt „zu viele“ davon), handelt es sich um keine kleine Kategorie. Wie wir noch sehen werden, bildet ein einzelner Graph oder eine einzelne partielle Ordnung ein Beispiel für eine kleine Kategorie.
Man beachte, dass weder die Objekte einer Kategorie mit einer bestimmten Trägermenge einhergehen müssen, noch Morphismen mit Abbildungen im herkömmlichen Sinn. Legt man jedoch auf diese Sichtweise Wert, kann man die Definition folgendermaßen ergänzen.

[56] Statt $\mathrm{Hom}_{\mathcal{C}}(A,B)$ ist auch die Schreibweise $\mathcal{C}(A,B)$ üblich. Statt $\mathrm{Hom}_{\mathcal{T}op}(A,B)$ schreibt man dann $\mathcal{T}op(A,B)$, etc.

Definition 2.3.1.2. Gibt es zu einer Kategorie $\mathcal{C}$ zusätzlich eine Funktion[57][58] U, die jedem $A \in \mathrm{Ob}(\mathcal{C})$ eine Menge (ein *Universum*) $\mathsf{U}(A)$ und jedem Morphismus $f\colon A \to B$ eine Abbildung $\mathsf{U}(f)\colon \mathsf{U}(A) \to \mathsf{U}(B)$ im herkömmlichen Sinne zuordnet, sodass gilt:

(i) $\mathsf{U}(1_A)$ ist die identische Abbildung auf $\mathsf{U}(A)$,

(ii) die Komposition in $\mathcal{C}$ entspricht der Abbildungskomposition (d. h. $\mathsf{U}(f \circ g) = \mathsf{U}(f) \circ \mathsf{U}(g)$), wobei die erste Komposition jene in der Kategorie $\mathcal{C}$ und die zweite die gewöhnliche Abbildungskomposition in der Kategorie der Mengen ist, siehe Unterabschnitt 2.3.2,

(iii) die Abbildung U ist auf jeder der Mengen $\mathrm{Hom}_{\mathcal{C}}(A, B)$, mit $A, B \in Ob(\mathcal{C})$ injektiv,

dann heißt $\mathcal{C}$ *konkrete Kategorie*.

Die Zuordnung U, die in der Definition 2.3.1.2 einer konkreten Kategorie auftritt, ist ein erstes Beispiel eines Funktors, siehe Definition 2.3.4.1. Und zwar nennt man diesen Funktor U (wie auch ähnliche in vergleichbaren Situationen) den *Vergissfunktor*. Denn wendet man ihn beispielsweise auf die Kategorie der Gruppen an, so „vergisst“ man beim Übergang von der Gruppe zur Trägermenge gewissermaßen die algebraische Struktur auf dieser Trägermenge.
In vielen Gebieten der Mathematik gibt es einen natürlichen Begriff von „Morphismus“ zwischen den Strukturen, die in diesem Gebiet betrachtet werden (Homomorphismus in der Algebra, stetige Funktion in der Topologie, messbare Funktion in der Maßtheorie, etc.); somit bilden diese Strukturen oft in natürlicher Weise eine konkrete Kategorie, wobei die Klasse aller betrachteten Strukturen oft eine echte Klasse und keine Menge ist – so wie für den Fall der Gruppen bereits erwähnt.

2.3.2. Beispiele von Kategorien

Inhalt in Kurzfassung: Varietäten sind wichtige Beispiele von Kategorien. Von anderer Art aber gleichfalls von Interesse ist, dass man auch Graphen als Kategorien auffassen kann. Grob gesagt sind die Knoten die Objekte der Kategorie, Kanten sind (gewisse) Morphismen.

Die für uns wichtigsten Beispiele von Kategorien sind Varietäten. Und zwar lässt sich jede Varietät $\mathcal{V}$ in natürlicher Weise als konkrete Kategorie auffassen:

Beispiel 2.3.2.1. $\mathrm{Ob}(\mathcal{V})$ ist die Klasse aller Algebren in $\mathcal{V}$ und die Morphismen sind

[57] Eine *relationale Klasse* ist eine Klasse, deren Elemente Paare sind; eine *funktionale Klasse* ist eine relationale Klasse, die rechtseindeutig ist, d. h. niemals Paare (a, b) und (a, b') mit $b \neq b'$ enthält. Da der Definitionsbereich der hier betrachteten „Funktion“ U eine echte Klasse sein kann, ist im Allgemeinen auch U eine echte Klasse; der Ausdruck „Funktion“ ist dann als Abkürzung für „funktionale Klasse“ zu lesen.

[58] U ist der Buchstabe U, nicht das Symbol $\bigcup$ für die Vereinigung von Mengen.

die Homomorphismen. Aus technischen Gründen[59] kann man hier allerdings nicht die Graphen der Abbildungen verwenden. Für $\mathfrak{A}, \mathfrak{B} \in \mathcal{V}$ setzen wir stattdessen

$$\mathrm{Hom}(\mathfrak{A}, \mathfrak{B}) = \{(\mathfrak{A}, f, \mathfrak{B}) \mid f \text{ ist Homomorphismus von } \mathfrak{A} \text{ nach } \mathfrak{B}\}.$$

Die Komposition ist die Abbildungskomposition. Genauer: Für $F = (\mathfrak{A}, f, \mathfrak{B}) \in \mathrm{Hom}(\mathfrak{A}, \mathfrak{B})$ und $G = (\mathfrak{B}, g, \mathfrak{C}) \in \mathrm{Hom}(\mathfrak{B}, \mathfrak{C})$ ist $G \circ F := (\mathfrak{A}, g \circ f, \mathfrak{C})$.
Weil die Komposition assoziativ ist und die identischen Abbildungen Homomorphismen sind, die als Einselemente im Sinne von Definition 2.3.1.1 fungieren, erhält man tatsächlich eine Kategorie.
Diese Kategorie wird zur konkreten Kategorie, indem man U jeder Algebra ihre Trägermenge und jedem Homomorphismus die entsprechende Abbildung zwischen Mengen zuordnen lässt. Denn offensichtlich sind alle drei Bedingungen in Definition 2.3.1.2 erfüllt.
Äquivalenz im kategorientheoretischen Sinn entspricht hier der Isomorphie von Algebren.

Folgende Spezialfälle von Varietäten als Kategorien begegnen uns besonders häufig:

Beispiele 2.3.2.2. Sind sowohl der Typ τ als auch die $\mathcal{V}$ definierende Menge Γ von Gesetzen leer, so erhält man die Kategorie $\mathcal{S}ets$ der Mengen.
Ist $\tau = (0)$ einelementig mit einer nullstelligen Operation und weiterhin $\Gamma = \emptyset$, so entsteht die Kategorie $\mathcal{S}ets_*$ der *punktierten Mengen*, oder *Mengen mit einem ausgezeichneten Punkt*; diese Algebren haben eine einzige nullstellige Operation $*$ und die Morphismen sind Homomorphismen im Sinne der Algebra, das heißt also: Abbildungen f, die $f(*) = *$ erfüllen, ausgezeichnete Punkte also auf ausgezeichnete Punkte abbilden.
Von Interesse sind auch die Kategorien $\mathcal{G}rp$ und $\mathcal{A}b$ der Gruppen bzw. der abelschen Gruppen, außerdem die Kategorien $\mathcal{R}ng$ der Ringe bzw. $\mathcal{R}ng_1$ der Ringe mit Einselement sowie die Kategorie $\mathcal{V}ec_K$ der Vektorräume über dem Körper K.

Beispiele 2.3.2.3. Keine Varietäten aber dennoch interessante konkrete Kategorien sind (jeweils: Angabe der Objekte mit den Morphismen): die Kategorie $\mathcal{T}op$ der topologischen Räume mit stetigen Abbildungen sowie die Kategorie $\mathcal{T}op_*$ der punktierten topologischen Räume (topologische Räume mit einem ausgezeichneten Element) mit stetigen Abbildungen, die ausgezeichnete Punkte auf ausgezeichnete Punkte abbilden, analog zu $\mathcal{S}ets_*$. Wir werden auch noch einige interessante Beispiele komplizierterer Art kennen lernen.

Von gänzlich anderer Art ist das folgende Beispiel einer Kategorie.

[59] Wir haben verlangt, dass die Morphismenmengen paarweise disjunkt sind. Wenn nun $\mathfrak{A}$ und $\mathfrak{A}'$ verschiedene Algebren aus $\mathcal{V}$ mit derselben Trägermenge sind, $\mathfrak{B}$ eine weitere Algebra in $\mathcal{V}$, dann könnte die selbe Funktion f sowohl Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ als auch von $\mathfrak{A}'$ nach $\mathfrak{B}$ sein; wir führen daher eine künstliche Unterscheidung zwischen dem (konkreten) Homomorphismus f und dem (abstrakten) Morphismus $(\mathfrak{A}, f, \mathfrak{B})$ bzw. $(\mathfrak{A}', f, \mathfrak{B})$ ein.

Auch in den folgenden Beispielen können wir die Morphismenmengen disjunkt machen, indem wir jede Funktion $f\colon A \to B$ durch das Tripel (A, f, B) ersetzen. Wohlgemerkt muss man für A und B die Objekte der Kategorie nehmen, nicht schlicht die Trägermengen.

Definition 2.3.2.4. Sei R eine reflexive und transitive Relation auf einer Menge V. Wir können (V, R) in folgender Weise als kleine Kategorie auffassen:

- Die Objekte der Kategorie (V, R) sind die Elemente von V.
- Für alle $a, b \in V$ mit $(a, b) \in R$ sei $\mathrm{Hom}_{(V,R)}(a, b)$ die einelementige Menge $\{(a, b)\}$. (Insbesondere ist $\mathrm{Hom}_{(V,R)}(a, a) = \{(a, a)\}$.)

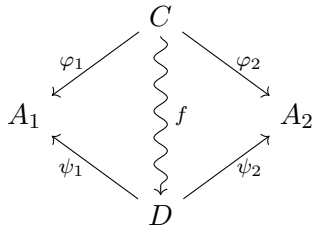
  Für alle $a, b \in V$ mit $(a, b) \notin R$ sei $\mathrm{Hom}_{(V,R)}(a, b)$ die leere Menge.
- Komposition ist in natürlicher Weise definiert: Wenn $a\ R\ b\ R\ c$ gilt, dann liefert die Komposition der Elemente von $\mathrm{Hom}_{(V,R)}(a, b)$ und $\mathrm{Hom}_{(V,R)}(b, c)$ das (einzige) Element von $\mathrm{Hom}_{(V,R)}(a, c)$: $(b, c) \circ (a, b) = (a, c)$ – hier geht die Transitivität von E ein.

Wenn E eine beliebige binäre Relation auf eine Menge V ist, bezeichnen wir mit E^* die reflexive transitive Hülle von E, das ist die kleinste E umfassende Relation, die reflexiv und transitiv ist. (Eine solche gibt es, weil die Relationen mit dieser Eigenschaft durchschnittsstabil sind und somit nach 2.1.2.19 einen vollständigen Verband bilden.) Dann können wir (V, E) als die durch (V, E^*) gegebene Kategorie auffassen.

Für Relationen E auf kleinen endlichen Mengen V stellt man (V, E) oft so dar, dass man eine möglichst kleine Menge E_0 mit $E_0^* = E^*$ findet, und dann (V, E_0) als gerichteten Graphen $\Gamma = (V, E_0)$ auffasst, mit Kantenmenge E_0.
Also induziert jeder gerichtete Graph $\Gamma = (V, E)$ eine Kategorie, die wir auch mit $\mathcal{C}(\Gamma)$ bezeichnen. Etwas später, wenn wir auch noch den Begriff des Funktors zur Verfügung haben, werden wir damit definieren, was unter einem kommutativen Diagramm zu verstehen ist.
Typisch für die Konstruktion von neuen Kategorien aus einer bereits vorliegenden ist das folgende Beispiel.

Beispiel 2.3.2.5. Sei $\mathcal{C}$ eine Kategorie, und seien A_1 und A_2 Objekte in $\mathcal{C}$. Die Kategorie $\mathcal{C} \downarrow \{A_1, A_2\}$ ist so[60] definiert:

- Objekte von $\mathcal{C} \downarrow \{A_1, A_2\}$ sind Tripel $(C, \varphi_1, \varphi_2)$, wobei C ein Objekt von $\mathcal{C}$ ist, und φ_1, φ_2 Morphismen von C nach A_1 bzw. A_2.
- $\mathrm{Hom}_{\mathcal{C}\downarrow\{A_1,A_2\}}(\,(C, \varphi_1, \varphi_2),\ (D, \psi_1, \psi_2)\,)$ besteht aus allen Tripeln (C, f, D) mit einem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(C, D)$, der $\psi_i \circ f = \varphi_i$ für $i = 1, 2$ erfüllt.



[60] Die Kategorie $\mathcal{C} \downarrow \{A_1, A_2\}$ ist ein spezielles Beispiel einer sogenannten *Komma-Kategorie*.

- Die Komposition ist durch

$$(D, g, E) \circ (C, f, D) := (C, g \circ f, E)$$

gegeben, wobei $g \circ f$ die Komposition in $\mathcal{C}$ bezeichnet.

Im nächsten Unterabschnitt werden wir diese und eine ähnliche Kategorie verwenden, um direkte Produkte (siehe Unterabschnitt 2.2.2) und direkte Limiten (siehe Unterabschnitt 2.2.4) kategorientheoretisch aufzufassen.

2.3.3. Universelle Objekte und ihre Eindeutigkeit

Inhalt in Kurzfassung: Der einzige rein kategorientheoretische Satz, den wir später verwenden werden (das dafür sehr häufig), besagt, dass universelle (genauer: initiale und terminale) Objekte einer Kategorie bis auf Äquivalenz eindeutig bestimmt sind. Die Definition all dieser Begriffe sowie der (kurze aber sehr typische) Beweis dieses Satzes sind wichtige Inhalte dieses Unterabschnitts. Außerdem deuten wir die bereits bekannten algebraischen Konstruktionen der direkten Produkte sowie der direkten Limiten auf kategorientheoretische Weise. Der eingangs erwähnte Satz liefert uns somit eine Eindeutigkeitsaussage dieser Konstruktionen.

Definition 2.3.3.1. Sei $\mathcal{C}$ eine Kategorie.

- $I \in Ob(\mathcal{C})$ heißt *initiales Objekt*, wenn es für alle $A \in Ob(\mathcal{C})$ einen *eindeutigen* Morphismus $f\colon I \to A$ gibt.
- $T \in Ob(\mathcal{C})$ heißt *terminales Objekt*, wenn es für alle $A \in Ob(\mathcal{C})$ einen *eindeutigen* Morphismus $f\colon A \to T$ gibt.

Initiale und terminale Objekte nennt man auch *universelle Objekte*. (Manchmal werden auch nur die initialen Objekte als universell bezeichnet und die terminalen als *kouniversell*.)

Satz 2.3.3.2. *Initiale Objekte einer Kategorie $\mathcal{C}$ sind, sofern es welche gibt, bis auf Äquivalenz eindeutig bestimmt; ebenso terminale Objekte.*

Beweis. Seien I, J initiale Objekte von $\mathcal{C}$. Weil I initial ist, existiert genau ein $f\colon I \to J$. Weil J initial ist, existiert genau ein $g\colon J \to I$. Nun sind $g \circ f\colon I \to I$ und $f \circ g\colon J \to J$ Morphismen von $\mathcal{C}$, aber auch $1_I\colon I \to I$ und $1_J\colon J \to J$ sind Morphismen von $\mathcal{C}$. Da I initial ist, gibt es genau einen Morphismus $I \to I$ (setze $A = I$ in der Definition). Daraus folgt $g \circ f = 1_I$. Analog ergibt sich $f \circ g = 1_J$, womit I und J äquivalent sind.
Genauso behandelt man den Fall terminaler Objekte. □

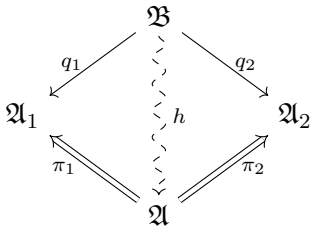
UE 105 ► **Übungsaufgabe 2.3.3.3.** (F) Geben Sie initiale und terminale Objekte in folgenden Kategorien an (bzw. beweisen Sie, dass solche Objekte nicht existieren): $\mathcal{Sets}$, $\mathcal{Sets}_*$, $\mathcal{Grp}$, $\mathcal{Vec}_{\mathbb{Q}}$. (Hinweis: Vergessen Sie nicht, dass die leere Menge auch eine Menge ist.) ◄ **UE 105**

Viele algebraische Konstruktionen (oft in einer Varietät), die wir bereits kennen oder in den nächsten Kapiteln kennenlernen werden, lassen sich als universelle Objekte in einer geeigneten Kategorie auffassen, z. B. Produkte, Koprodukte, direkte Limiten, Quotientenmonoide, -gruppen und -körper, freie Algebren, Polynomalgebren. Typischerweise funktioniert das so, dass man von einer „universellen Eigenschaft“ ausgeht und eine Kategorie definiert, die die Varietät derart anreichert, dass die universelle Eigenschaft genau mit der eindeutigen Existenz von Morphismen in der Kategorie korrespondiert. Für Produkte und direkte Limiten können wir diesen Zugang bereits hier vorstellen. Wir beginnen mit Produkten, genauer mit dem Spezialfall eines Produkts von zwei Algebren.

Beispiel 2.3.3.4 (Das Produkt zweier Algebren als universelles (terminales) Objekt)**.** Seien $\mathfrak{A}_1, \mathfrak{A}_2$ Algebren desselben Typs. Bezeichne weiters $\mathfrak{A} := \mathfrak{A}_1 \times \mathfrak{A}_2$ deren Produkt und $\pi_i : \mathfrak{A} \to \mathfrak{A}_i$, $i = 1, 2$, die Projektionshomomorphismen. Nach Proposition 2.2.2.4 gilt die folgende universelle Eigenschaft:

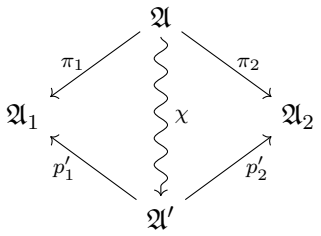
> Für jede Algebra $\mathfrak{B}$ desselben Typs wie die $\mathfrak{A}_i$ und alle Homomorphismen $q_i : \mathfrak{B} \to \mathfrak{A}_i$, $i = 1, 2$, gibt es genau einen Homomorphismus $h : \mathfrak{B} \to \mathfrak{A}$ mit $\pi_i \circ h = q_i$ für $i = 1, 2$.

Zur kategorientheoretischen Deutung gehen wir aus von der Kategorie $\mathcal{C}$ aller Algebren desselben Typs wie die $\mathfrak{A}_i$ mit den üblichen Morphismen und der üblichen Komposition. Dann betrachten wir die Kategorie $\mathcal{C} \downarrow \{\mathfrak{A}_1, \mathfrak{A}_2\}$ aus Beispiel 2.3.2.5. Die universelle Eigenschaft des Produkts lässt sich wie folgt umformulieren: Für alle Objekte $(\mathfrak{B}, q_1, q_2)$ von $\mathcal{C} \downarrow \{\mathfrak{A}_1, \mathfrak{A}_2\}$ gibt es genau einen $\mathcal{C} \downarrow \{\mathfrak{A}_1, \mathfrak{A}_2\}$-Morphismus $h : (\mathfrak{B}, q_1, q_2) \to (\mathfrak{A}, \pi_1, \pi_2)$. Nochmal anders gesagt: $(\mathfrak{A}, \pi_1, \pi_2)$ ist ein terminales Objekt in $\mathcal{C} \downarrow \{\mathfrak{A}_1, \mathfrak{A}_2\}$.



Mit Satz 2.3.3.2 ergibt sich die folgende Eindeutigkeitsaussage des direkten Produkts:

> Sei $\mathfrak{A}'$ eine weitere Algebra desselben Typs wie die $\mathfrak{A}_i$ samt Homomorphismen $p'_i : \mathfrak{A}' \to \mathfrak{A}_i$ mit der Eigenschaft, dass es für alle Algebren $\mathfrak{B}$ dieses Typs und alle Homomorphismen $q_i : \mathfrak{B} \to \mathfrak{A}_i$, $i = 1, 2$ genau einen Homomorphismus $h' : \mathfrak{B} \to \mathfrak{A}'$ mit $p'_i \circ h = q_i$ für $i = 1, 2$ gibt. Dann sind $(\mathfrak{A}, \pi_1, \pi_2)$ und $(\mathfrak{A}', p'_1, p'_2)$ in $\mathcal{C} \downarrow \{\mathfrak{A}_1, \mathfrak{A}_2\}$ äquivalent, d. h. explizit: Es existiert ein Isomorphismus $\chi : \mathfrak{A} \to \mathfrak{A}'$ mit $p'_i \circ \chi = \pi_i$ für $i = 1, 2$.



Ist $\mathcal{V}$ eine Varietät und sind $\mathfrak{A}_1, \mathfrak{A}_2 \in \mathcal{V}$, so wissen wir aus Folgerung 2.2.2.9 bereits, dass auch $\mathfrak{A}$ in $\mathcal{V}$ liegt. Somit können wir das obige Argument statt in $\mathcal{C}$ und $\mathcal{C} \downarrow \{\mathfrak{A}_1, \mathfrak{A}_2\}$ auch in $\mathcal{V}$ und $\mathcal{V} \downarrow \{\mathfrak{A}_1, \mathfrak{A}_2\}$ durchführen.

Für den Schritt von Produkten zweier Algebren zu Produkten beliebig vieler Algebren müssen wir nur die Kategorie $\mathcal{C} \downarrow \{\mathfrak{A}_1, \mathfrak{A}_2\}$ verallgemeinern.

Definition 2.3.3.5. Sei $\mathcal{C}$ eine Kategorie, und seien A_k, $k \in K$, Objekte in $\mathcal{C}$. Die Kategorie $\mathcal{C} \downarrow \{A_k \mid k \in K\}$ ist so definiert:

- Objekte von $\mathcal{C} \downarrow \{A_k \mid k \in K\}$ sind Paare $(C, (\varphi_k)_{k\in K})$, wobei C ein Objekt von $\mathcal{C}$ ist, und φ_k für $k \in K$ ein Morphismus von C nach A_k.
- $\mathrm{Hom}_{\mathcal{C}\downarrow\{A_k|k\in K\}}(\,(C, (\varphi_k)_{k\in K}),\, (D, (\psi_k)_{k\in K})\,)$ besteht aus allen Tripeln (C, f, D) mit einem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(C, D)$, der $\psi_k \circ f = \varphi_k$ für alle $k \in K$ erfüllt.
- Die Komposition ist durch

  $$(D, g, E) \circ (C, f, D) := (C, g \circ f, E)$$

  gegeben, wobei $g \circ f$ die Komposition in $\mathcal{C}$ bezeichnet.

Damit ergibt sich:

Proposition 2.3.3.6. *Sei $\mathcal{V}$ eine Varietät und seien $\mathfrak{A}_k \in \mathcal{V}$, $k \in K$. Dann gelten die folgenden Aussagen:*

(1) *Setzt man $\mathfrak{A} := \prod_{k\in K} \mathfrak{A}_k \in \mathcal{V}$, so ist $(\mathfrak{A}, (\pi_k)_{k\in K})$ ein terminales Objekt in $\mathcal{V} \downarrow \{A_k \mid k \in K\}$.*

(2) *Sei $\mathfrak{A}' \in \mathcal{V}$ samt Homomorphismen $p'_j : \mathfrak{A}' \to \mathfrak{A}_j$ mit der Eigenschaft, dass es für alle Algebren $\mathfrak{B} \in \mathcal{V}$ und alle Homomorphismen $q_j : \mathfrak{B} \to \mathfrak{A}_j$, $j \in K$, genau einen Homomorphismus $h' : \mathfrak{B} \to \mathfrak{A}'$ mit $p'_j \circ h = q_j$ für alle $j \in K$ gibt. Dann sind $(\mathfrak{A}, (\pi_k)_{k\in K})$ und $(\mathfrak{A}', (p'_k)_{k\in K})$ in $\mathcal{V} \downarrow \{\mathfrak{A}_k \mid k \in K\}$ äquivalent, d. h. explizit: Es existiert ein Isomorphismus $\chi : \mathfrak{A} \to \mathfrak{A}'$ mit $p'_j \circ \chi = \pi_j$ für alle $j \in K$.*

Nun kommen wir zu direkten Limiten, die wir ebenfalls als universelle Objekte identifizieren werden, diesmal aber als initiale Objekte. Wir wiederholen zunächst die Ausgangssituation und die universelle Eigenschaft aus Satz 2.2.4.6:
Sei $\mathcal{K}$ eine Varietät von Algebren (oder die Klasse aller Körper) und seien $\mathfrak{A}_n$, $n \in \mathbb{N}$, Algebren in $\mathcal{K}$ gemeinsam mit Homomorphismen $\iota_n \colon \mathfrak{A}_n \to \mathfrak{A}_{n+1}$. Der direkte Limes $\mathfrak{A}_\infty \in \mathcal{K}$ samt Homomorphismen $\varphi_n \colon \mathfrak{A}_n \to \mathfrak{A}_\infty$, die $\varphi_n = \varphi_{n+1} \circ \iota_n$ für alle $n \in \mathbb{N}$ erfüllen, hat die folgende universelle Eigenschaft:

Für jede Algebra $\mathfrak{D} \in \mathcal{K}$ und jede Familie $(\psi_n \mid n \in \mathbb{N})$ von Homomorphismen $\psi_n \colon \mathfrak{A}_n \to \mathfrak{D}$, die $\psi_n = \psi_{n+1} \circ \iota_n$ für alle $n \in \mathbb{N}$ erfüllen, gibt es genau einen Homomorphismus $\theta \colon \mathfrak{A}_\infty \to \mathfrak{D}$ mit $\theta \circ \varphi_n = \psi_n$ für alle $n \in \mathbb{N}$.

Wir definieren wieder eine geeignete Kategorie:

Definition 2.3.3.7. Sei $\mathcal{C}$ eine Kategorie, und seien A_n, $n \in \mathbb{N}$, Objekte in $\mathcal{C}$, sodass für alle $n \in \mathbb{N}$ Morphismen $\iota_n : A_n \to A_{n+1}$ bzgl. $\mathcal{C}$ gegeben seien (d. h. $\iota_n \in \mathrm{Hom}_{\mathcal{C}}(A_n, A_{n+1})$). Die Kategorie $\mathcal{C} \uparrow \{A_n, \iota_n \mid n \in \mathbb{N}\}$ ist so definiert:

- Objekte von $\mathcal{C} \uparrow \{A_n, \iota_n \mid n \in \mathbb{N}\}$ sind Paare $(C, (\varphi_n)_{n\in\mathbb{N}})$, wobei C ein Objekt von $\mathcal{C}$ ist, und φ_n für $n \in \mathbb{N}$ ein Morphismus von A_n nach C ist, sodass zusätzlich $\varphi_n = \varphi_{n+1} \circ \iota_n$ für alle $n \in \mathbb{N}$ gilt.
- $\mathrm{Hom}_{\mathcal{C}\uparrow\{A_n,\iota_n|n\in\mathbb{N}\}}(\,(C, (\varphi_n)_{n\in\mathbb{N}}), (D, (\psi_n)_{n\in\mathbb{N}})\,)$ besteht aus allen Tripeln (C, f, D) mit einem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(C, D)$, der $f \circ \varphi_n = \psi_n$ für alle $n \in \mathbb{N}$ erfüllt.
- Die Komposition ist durch

  $$(D, g, E) \circ (C, f, D) := (C, g \circ f, E)$$

  gegeben, wobei $g \circ f$ die Komposition in $\mathcal{C}$ bezeichnet.

Wie im Fall der direkten Produkte ergibt sich durch Einsetzen der Definitionen unmittelbar:

Proposition 2.3.3.8. *Sei $\mathcal{K}$ eine Varietät von Algebren (oder die Klasse aller Körper) und seien $\mathfrak{A}_n$, $n \in \mathbb{N}$, Algebren in $\mathcal{K}$ gemeinsam mit Homomorphismen $\iota_n \colon \mathfrak{A}_n \to \mathfrak{A}_{n+1}$ gegeben. Dann gelten die folgenden Aussagen:*

(1) *Bezeichnet $\mathfrak{A}_\infty \in \mathcal{V}$ den direkten Limes und $\varphi_n : \mathfrak{A}_n \to \mathfrak{A}_\infty$ die Homomorphismen aus Satz 2.2.4.6, so ist $(\mathfrak{A}_\infty, (\varphi_n)_{n\in\mathbb{N}})$ ein initiales Objekt in der Kategorie $\mathcal{V} \uparrow \{\mathfrak{A}_n, \iota_n \mid n \in \mathbb{N}\}$.*

(2) *Sei $\mathfrak{A}' \in \mathcal{K}$ samt Homomorphismen $\varphi'_n : \mathfrak{A}_n \to \mathfrak{A}'$, die $\varphi'_n = \varphi'_{n+1} \circ \iota_n$ für alle $n \in \mathbb{N}$ erfüllen, und der folgenden Eigenschaft: Für jede Algebra $\mathfrak{D} \in \mathcal{K}$ und jede Familie $(\psi_n \mid n \in \mathbb{N})$ von Homomorphismen $\psi_n \colon \mathfrak{A}_n \to \mathfrak{D}$, die $\psi_n = \psi_{n+1} \circ \iota_n$ für alle $n \in \mathbb{N}$ erfüllen, gibt es genau einen Homomorphismus $\theta' \colon \mathfrak{A}' \to \mathfrak{D}$ mit $\theta' \circ \varphi'_n = \psi_n$ für alle $n \in \mathbb{N}$.*

   Dann sind $(\mathfrak{A}_\infty, (\varphi_n)_{n\in\mathbb{N}})$ und $(\mathfrak{A}', (\varphi'_n)_{n\in\mathbb{N}})$ in $\mathcal{V} \uparrow \{\mathfrak{A}_n, \iota_n \mid n \in \mathbb{N}\}$ äquivalent, d. h. explizit: Es existiert ein Isomorphismus $\chi : \mathfrak{A}_\infty \to \mathfrak{A}'$ mit $\chi \circ \varphi_n = \varphi'_n$ für alle $n \in \mathbb{N}$.

Die jeweils ersten Aussagen von Proposition 2.3.3.6 bzw. Proposition 2.3.3.8 geben Anlass zu einer Definition von direkten Produkten und direkten Limiten in allgemeinen Kategorien.

Definition 2.3.3.9. Sei $\mathcal{C}$ eine Kategorie.

- Seien A_k, $k \in K$, Objekte in $\mathcal{C}$. Jedes terminale Objekt $(A, (\varphi_k)_{k\in K})$ in der Kategorie $\mathcal{C} \downarrow \{A_k \mid k \in K\}$ (wenn ein solches existiert) heißt *direktes Produkt* der A_k, $k \in K$.

- Seien A_n, $n \in \mathbb{N}$, Objekte in $\mathcal{C}$ und $\iota_n \in \mathrm{Hom}_{\mathcal{C}}(A_n, A_{n+1})$, d. h., ι_n sei für jedes $n \in \mathbb{N}$ ein Morphismus $A_n \to A_{n+1}$. Jedes initiale Objekt $(A_\infty, (\varphi_n)_{n\in\mathbb{N}})$ in der Kategorie $\mathcal{C} \uparrow \{A_n, \iota_n \mid n \in \mathbb{N}\}$ (wenn ein solches existiert) heißt *direkter Limes* der A_n, $n \in \mathbb{N}$, bezüglich ι_n, $n \in \mathbb{N}$.

Man beachte, dass diese Definition nichts über eine etwaige Existenz der definierten Objekte aussagt. Unsere bisherigen Resultate lassen sich auch so umformulieren, dass

- in der von einer Varietät gebildeten Kategorie direkte Produkte stets existieren.
- in der von einer Varietät gebildeten Kategorie sowie in der Kategorie der Körper direkte Limiten (vorerst von abzählbar vielen Objekten[61]) stets existieren.

Auch die jeweils zweiten Aussagen (Eindeutigkeitsaussagen) von Proposition 2.3.3.6 bzw. Proposition 2.3.3.8 verdienen genauere Betrachtung. In Unterabschnitt 2.2.2 bzw. Unterabschnitt 2.2.4 haben wir direkte Produkte bzw. direkte Limiten konkret definiert und konstruiert. Die kategorientheoretischen Eindeutigkeitsaussagen lassen aber auch den abstrakteren (eben *kategoriellen*) Zugang zu, sich auf die universellen Eigenschaften zurückzuziehen und von der kategorientheoretischen Definition auszugehen. Jedes so erhaltene Objekt wird isomorph zum konkret konstruierten direkten Produkt bzw. direkten Limes sein, wobei der Isomorphismus auch die entsprechenden Abbildungen (Projektionen des Produkts in die Faktoren bzw. Homomorphismen von den Objekten in den Limes) ineinander übersetzt. Prinzipiell lassen sich also alle Aussagen, die man für die konkreten Objekte zeigen kann, auch für die kategoriell definierten Objekte nachweisen. Bei direkten Produkten erweist sich dieser Zugang selten als sinnvoll, da das konkret definierte direkte Produkt derart transparent und intuitiv zu verstehen ist, dass die meisten Sachverhalte damit einfacher zu fassen sind. Bei direkten Limiten hingegen ist der kategorielle Zugang manchmal nützlich, da die konkrete Konstruktion aus Satz 2.2.4.4 bzw. Satz 2.2.4.6 vergleichsweise kompliziert ist und somit der Blick auf Wesentliches durch technische Details verdeckt werden kann. Anders verhält es sich wieder, wenn man die Familie der Strukturen, deren Limes man bilden möchten, als aufsteigende Familie auffassen kann. In diesem Fall ist der direkte Limes ja gegeben durch eine geeignete, intuitiv konstruierte Struktur auf der Vereinigung aller Trägermengen – damit kann man gut arbeiten.
Zum Abschluss dieses Unterabschnitts zwei Übungsaufgaben zur kategorientheoretischen Deutung der Konstruktion der Zahlenbereiche aus Kapitel 1:

UE 106 ▶ **Übungsaufgabe 2.3.3.10.** (F) Sei $\iota : \mathbb{N} \to \mathbb{Z}$ die Identität auf $\mathbb{N}$ (komplizierter gesagt: der eindeutig bestimmte Halbgruppenhomomorphismus, der 1 auf 1 abbildet). ◀ **UE 106**
Geben Sie eine Kategorie $\mathcal{D}$ an, sodass erstens gilt:

$$(*) \qquad (\mathbb{Z}, \iota) \text{ ist initial in } \mathcal{D},$$

und sodass zweitens die Aussage $(*)$ eine Umformulierung von Satz 1.2.1.1(3) ist.

[61] Wir werden in Unterabschnitt 7.1.5 auch direkte Limiten von beliebig vielen Objekten betrachten, die ebenfalls in Varietäten sowie der Klasse aller Körper existieren.

UE 107 ► **Übungsaufgabe 2.3.3.11.** (D,E) Jeder der Zahlenbereiche $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ wurde so konstruiert, dass gewisse Mindestanforderungen auf minimale Weise erfüllt wurden. Die entsprechende Minimalität hatte jeweils einen Eindeutigkeitssatz zur Folge, der sich auch in eine universelle (initiale) Eigenschaft innerhalb einer geeigneten Kategorie übersetzen lässt. In der vorigen Übungsaufgabe haben wir dies für $\mathbb{Z}$ getan; finden Sie nun entsprechende Sätze für $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ und/oder $\mathbb{C}$.
(Hinweis: Die Lösungen sind keineswegs eindeutig. Es kann durchaus sinnvoll und interessant sein, jeweils mehrere unterschiedliche Lösungen zu betrachten und miteinander zu vergleichen.) ◄ **UE 107**

2.3.4. Funktoren

Inhalt in Kurzfassung: Funktoren zwischen Kategorien spielen ziemlich genau die Rolle, die Homomorphismen zwischen Algebren desselben Typs spielen. Allerdings sind ko- von kontravarianten Funktoren zu unterscheiden. Wir werden wenig Gebrauch von Funktoren machen, von zentraler Bedeutung sind sie in Gebieten wie etwa der algebraischen Topologie. Da werden topologischen Räumen und stetigen Abbildungen durch Funktoren in verträglicher und sehr effektiver Weise gewisse algebraische Strukturen und Homomorphismen zugeordnet. Hier begnügen wir uns mit sehr einfachen Beispielen von Funktoren.

So wie algebraische Strukturen durch Homomorphismen zueinander in Beziehung gesetzt werden können, ist eine analoge Betrachtungsweise auch für Kategorien möglich. Dies führt zum Begriff des *Funktors*.

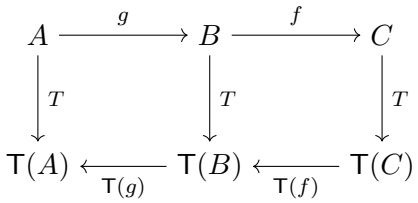
Definition 2.3.4.1. Seien $\mathcal{C}_1$ und $\mathcal{C}_2$ Kategorien. Wir betrachten Abbildungen T (als Abbildungen sind hier auch beliebige Klassen von Paaren zugelassen, nicht nur Mengen) folgender Art:
T ordnet jedem Objekt $A \in \mathcal{C}_1$ ein Objekt $\mathsf{T}(A) \in \mathcal{C}_2$ zu, außerdem jedem Morphismus $f\colon A \to B$ in $\mathcal{C}_1$ einen Morphismus $\mathsf{T}(f)$ in $\mathcal{C}_2$. Man nennt T einen *Funktor* von $\mathcal{C}_1$ nach $\mathcal{C}_2$, wenn erstens $\mathsf{T}(1_A) = 1_{\mathsf{T}(A)}$ (Funktoren bilden die Identität stets wieder auf die Identität ab) und zweitens eine der folgenden beiden Situationen vorliegt. Dabei spricht man im ersten Fall von einem *kovarianten*, im zweiten von einem *kontravarianten* Funktor.

kovarianter Funktor Für alle $A, B \in \mathcal{C}_1$ und für alle $f \in \mathrm{Hom}_{\mathcal{C}_1}(A, B)$ gilt $\mathsf{T}(f) \in \mathrm{Hom}_{\mathcal{C}_2}(\mathsf{T}(A), \mathsf{T}(B))$, kurz gesagt: Wenn $f\colon A \to B$, dann $\mathsf{T}(f)\colon \mathsf{T}(A) \to \mathsf{T}(B)$.

Weiters soll für alle $A, B, C \in \mathcal{C}_1$ und alle $g\colon A \to B$, $f\colon B \to C$ die Gleichung $\mathsf{T}(f \circ g) = \mathsf{T}(f) \circ \mathsf{T}(g)$ gelten.

$$\begin{array}{ccccc} A & \xrightarrow{\ g\ } & B & \xrightarrow{\ f\ } & C \\ \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} \\ \mathsf{T}(A) & \xrightarrow{\ \mathsf{T}(g)\ } & \mathsf{T}(B) & \xrightarrow{\ \mathsf{T}(f)\ } & \mathsf{T}(C) \end{array}$$

kontravarianter Funktor Hier drehen sich alle Richtungen um. Für $f\colon A \to B$ verlangen wir $\mathsf{T}(f)\colon \mathsf{T}(B) \to \mathsf{T}(A)$. Die Verträglichkeit mit der Komposition hat die Form $\mathsf{T}(f \circ g) = \mathsf{T}(g) \circ \mathsf{T}(f)$.



UE 108 ► **Übungsaufgabe 2.3.4.2.** (F) Sei T ein Funktor von der Kategorie $\mathcal{C}_1$ in die Kategorie $\mathcal{C}_2$ und $A, B \in \mathcal{C}_1$. Zeigen Sie: Sind A, B äquivalent in $\mathcal{C}_1$, so auch $\mathsf{T}(A)$ und $\mathsf{T}(B)$ in $\mathcal{C}_2$. ◄ **UE 108**

Sehr wichtige Anwendungen finden Funktoren in der algebraischen Topologie. Zum Beispiel treten Funktoren von der Kategorie der topologischen Räume in die Kategorie der Gruppen auf. Einem topologischen Raum wird dabei beispielsweise seine Fundamentalgruppe, allgemeiner seine Homotopiegruppe oder auch seine Homologiegruppe zugeordnet. Übungsaufgabe 2.3.4.2 garantiert, dass topologische Räume mit nicht isomorphen Gruppen nicht homöomorph sein können. Nützlich ist das zum Beispiel deshalb, weil oft die Nichtisomorphie von Gruppen offensichtlich ist, während sich der direkte Nachweis der Nichthomöomorphie topologischer Räume als sehr schwierig erweist.
Wir betrachten nun einige einfache Beispiele von Funktoren.
Auf jeder konkreten Kategorie $\mathcal{C}$ ist die Abbildung U, die jedem Objekt $A \in \mathcal{C}$ seine Trägermenge $\mathsf{U}(A)$ und jedem Morphismus $f\colon A \to B$ in $\mathcal{C}$ die zugehörige Mengenabbildung $\mathsf{U}(f)\colon \mathsf{U}(A) \to \mathsf{U}(B)$ gemäß Definition 2.3.1.2 zuordnet, ein kovarianter Funktor in die Kategorie $\mathcal{Sets}$ der Mengen. Man nennt U auch den *Vergissfunktor*[62], weil allfällige zusätzliche Struktur, welche die Mengen $\mathsf{U}(A)$ als Objekte A von $\mathcal{C}$ tragen, nach Anwendung von U vergessen wird.
Die gleiche Sprechweise ist auch in allgemeineren Situationen üblich. Zum Beispiel kann man bei Ringen die multiplikative Struktur ignorieren (vergessen) und nur noch die additive Gruppe betrachten. Dies liefert einen Funktor von der Kategorie der Ringe in die Kategorie der abelschen Gruppen.
Wir wenden uns einem Beispiel zu, in dem umgekehrt von Mengen ausgegangen wird, denen durch einen Funktor eine reichere Struktur zugeordnet wird.

Beispiel 2.3.4.3. Wir betrachten einen festen Körper K und die Kategorie $\mathcal{Vec}_K$ aller K-Vektorräume, wobei die Morphismen die K-linearen Abbildungen sind.

- Wir ordnen jeder Menge X den Vektorraum $\mathsf{V}(X)$ aller Familien $(k_x)_{x\in X} \in K^X$ zu, in denen $k_x \neq 0$ nur für endlich viele $x \in X$ gilt. Die Vektorraumoperationen sind dabei die kanonischen: $(k_x)_{x\in X} + (l_x)_{x\in X} := (k_x + l_x)_{x\in X}$ und $\lambda(k_x)_{x\in X} := (\lambda k_x)_{x\in X}$.

[62] englisch: *forgetful functor*

Jedem $x_0 \in X$ können wir in natürlicher Weise ein Element $b^X(x_0) \in \mathsf{V}(X)$ (genauer: in der Menge $\mathsf{U}(\mathsf{V}(X))$) zuordnen, nämlich jenes Element $(k_x)_{x\in X}$, welches $k_{x_0} = 1$ und $k_x = 0$ für alle $x \neq x_0$ erfüllt.
Die Familie $(b^X(x))_{x\in X}$ ist offensichtlich eine Basis für $\mathsf{V}(X)$.

- Sei nun $f\colon X \to Y$ eine beliebige Mengenabbildung, also $f \in \mathrm{Hom}_{\mathcal{S}ets}(X, Y)$. Nach dem Fortsetzungssatz der linearen Algebra gibt es eine eindeutige lineare Abbildung $\mathsf{V}(f)\colon \mathsf{V}(X) \to \mathsf{V}(Y)$, die $\mathsf{V}(f)(b^X(x)) = b^Y(f(x))$ für alle $x \in X$ erfüllt.

Der so definierte Funktor V von $\mathcal{S}ets$ nach $\mathcal{V}ec_K$ heißt auch der Freie Funktor (für K-Vektorräume).

UE 109 ► **Übungsaufgabe 2.3.4.4.** (V) Erläutern Sie ausführlich, warum V tatsächlich ein kovarianter Funktor ist. ◄ **UE 109**

Zwei weitere sehr einfache Beispiele von Funktoren innerhalb der Kategorie der Mengen entstehen durch Bildung der Potenzmenge.

Definition 2.3.4.5. Der kovariante Potenzmengenfunktor $\mathfrak{P}$ von $\mathcal{S}ets$ nach $\mathcal{S}ets$ ist so definiert:

- $\mathfrak{P}(M)$ ist die Potenzmenge von M, für alle Objekte M in $\mathcal{S}ets$.
- $\mathfrak{P}(f)\colon \mathfrak{P}(A) \to \mathfrak{P}(B)$ ist die Abbildung $S \mapsto \{f(x) \mid x \in S\} = f(S)$, für alle $f \in \mathrm{Hom}_{\mathcal{S}ets}(A, B)$.

Der kontravariante Potenzmengenfunktor $\bar{\mathfrak{P}}$ von $\mathcal{S}ets$ nach $\mathcal{S}ets$ ist so definiert:

- $\bar{\mathfrak{P}}(M) := \mathfrak{P}(M)$.
- $\bar{\mathfrak{P}}(f)\colon \bar{\mathfrak{P}}(B) \to \bar{\mathfrak{P}}(A)$ ist die Abbildung $T \mapsto \{x \in A \mid f(x) \in T\} = f^{-1}(T)$, für alle $f \in \mathrm{Hom}_{\mathcal{S}ets}(A, B)$.

UE 110 ► **Übungsaufgabe 2.3.4.6.** (F) Überprüfen Sie, dass die in Definition 2.3.4.5 definierten Zuordnungen tatsächlich ko- bzw. kontravariante Funktoren sind. ◄ **UE 110**

In gewisser Weise verwandt ist der folgende Funktor:

UE 111 ► **Übungsaufgabe 2.3.4.7.** (F) Sei $\mathcal{K}$ eine Klasse von Algebren gleichen Typs, in natürlicher Weise als Kategorie aufgefasst (d. h., die Morphismen sind die Homomorphismen). Sei $\mathcal{V}$ die Kategorie der $\wedge$-Halbverbände. Die Abbildung Con ordnet jedem Objekt A in $\mathcal{K}$ den Kongruenzhalbverband[63] $(\mathrm{Con}(A), \wedge)$ zu, und jedem Homomorphismus $f : A \to B$ die Abbildung $\mathrm{Con}(f) : \mathrm{Con}(B) \to \mathrm{Con}(A)$, die durch ◄ **UE 111**

$$\mathrm{Con}(f)(\theta) := \{(a, a') \mid f(a)\ \theta\ f(a')\} = (f \times f)^{-1}(\theta)$$

definiert ist.

[63] Die Operation $\vee$ wird hier ignoriert. Von Morphismen in $\mathcal{V}$ verlangen wir nur, dass sie mit der Operation $\wedge$ verträglich sind.

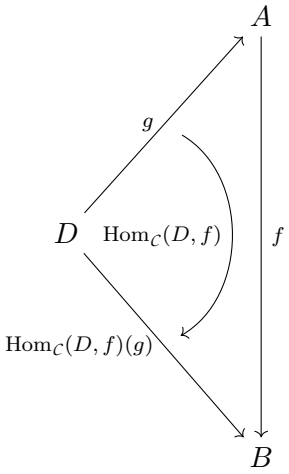
(1) Zeigen Sie, dass Con ein kontravarianter Funktor von $\mathcal{K}$ nach $\mathcal{V}$ ist.

(2) Con(A) ist nicht nur ein $\wedge$-Halbverband sondern sogar ein Verband. Hätte diese Aufgabe auch funktioniert, wenn wir als Kategorie $\mathcal{V}$ die Kategorie aller Verbände (Morphismen=Verbandshomomorphismen) gewählt hätten?

Hinweis: Wählen Sie $\mathcal{K}$ als die Klasse von Algebren mit leerer Signatur, d. h. einfach nur *Sets*. (Wie sieht dann der Kongruenzverband eines Objekts A aus?) Betrachten Sie eine injektive Abbildung f von einer 2- in eine 3-elementige Menge.

Weitere einfach definierte Funktoren sind die Hom-Funktoren:

Definition 2.3.4.8. Sei $\mathcal{C}$ eine Kategorie, $D \in Ob(\mathcal{C})$.



Der *kovariante Hom-Funktor*, der oft mit $\mathrm{Hom}_{\mathcal{C}}(D, -)$ bezeichnet wird, geht von der Kategorie $\mathcal{C}$ in die Kategorie *Sets*. Er

- ordnet jedem Objekt $A \in Ob(\mathcal{C})$ die Menge $\mathrm{Hom}_{\mathcal{C}}(D, A)$ zu;
- ordnet jedem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ die Abbildung $\mathrm{Hom}_{\mathcal{C}}(D, f)$ zu. Diese Abbildung geht von $\mathrm{Hom}_{\mathcal{C}}(D, A)$ nach $\mathrm{Hom}_{\mathcal{C}}(D, B)$, und ist durch die Vorschrift

$$\mathrm{Hom}_{\mathcal{C}}(D, f)(g) = f \circ g$$

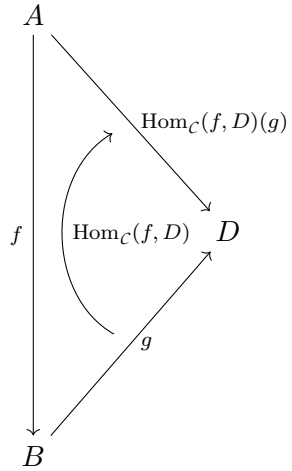
(für alle $g \in \mathrm{Hom}_{\mathcal{C}}(D, A)$) definiert.

Der *kontravariante Hom-Funktor*, der oft mit $\mathrm{Hom}_{\mathcal{C}}(-, D)$ bezeichnet wird, geht von der Kategorie $\mathcal{C}$ in die Kategorie *Sets*. Er

- ordnet jedem Objekt $A \in Ob(\mathcal{C})$ die Menge $\mathrm{Hom}_{\mathcal{C}}(A, D)$ zu;
- ordnet jedem Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ die Abbildung $\mathrm{Hom}_{\mathcal{C}}(f, D)$ zu. Diese Abbildung geht von $\mathrm{Hom}_{\mathcal{C}}(B, D)$ nach $\mathrm{Hom}_{\mathcal{C}}(A, D)$, und ist durch die Vorschrift

$$\mathrm{Hom}_{\mathcal{C}}(f, D)(g) = g \circ f$$

(für alle $g \in \mathrm{Hom}_{\mathcal{C}}(B, D)$) definiert.



UE 112 ► **Übungsaufgabe 2.3.4.9.** (V) Prüfen Sie nach, dass $\mathrm{Hom}_{\mathcal{C}}(D, -)$ bzw. $\mathrm{Hom}_{\mathcal{C}}(-, D)$ ◄ **UE 112** ein ko- bzw. kontravarianter Funktor ist.

UE 113 ▶ **Übungsaufgabe 2.3.4.10.** (F) Zeigen Sie dass folgender Funktor (wir schreiben ihn als nachgestelltes Symbol *) auf der Kategorie $\mathcal{Vec}_K$ ein kontravarianter Funktor ist. ◀ **UE 113**
Dabei wird

- jedem $V \in \mathcal{Vec}_K$ sein Dualraum V^* zugeordnet.
  (Zur Erinnerung: V^* ist der Raum aller linearen Abbildungen von V nach K, genannt auch Funktionale, mit den punktweise definierten Operationen.)
- Jedem Morphismus, d. h. jeder linearen Abbildung $f\colon V \to W$, wird ihre sogenannte *transponierte* Abbildung[64] $f^*\colon W^* \to V^*$ zugeordnet, die jedem Funktional $\ell \in W^*$ das Funktional $a \mapsto \ell(f(a))$ zuordnet.

Klarerweise ist die Zusammensetzung zweier kontravarianter Funktoren ein kovarianter Funktor. Insbesondere kann man den Funktor * aus ÜbungsaAufgabe 2.3.4.10 iterieren und erhält einen kovarianten Funktor ** auf der Kategorie der Vektorräume über dem Körper K. Beschränkt man sich auf endlichdimensionale Vektorräume V, so ist bekanntlich der Dualraum V^* isomorph zu V. Die Angabe eines Isomorphismus zwischen beiden ist aber willkürlich. Im Gegensatz dazu gibt es für jeden Vektorraum V eine kanonische (natürliche) Abbildung $\alpha\colon V \to V^{**}$, gegeben durch $v \mapsto v^{**}$. Dabei ist $v^{**}\colon V^* \to K$ definiert durch $v^{**}(\ell) := \ell(v)$, $\ell \in V^*$. Aus der linearen Algebra wissen wir, dass α genau dann ein Isomorphismus ist, wenn V endlichdimensional ist. In Übungsaufgabe 2.3.6.11 werden wir diese Tatsache nochmal beleuchten.
In der Funktionalanalysis betrachtet man normierte (oder allgemeiner: topologische) Vektorräume über dem Grundkörper $K = \mathbb{R}$ oder $K = \mathbb{C}$ und definiert den Dualraum V' anders, nämlich als Menge der *stetigen* linearen Abbildungen von V nach K.
Hier kann es auch bei unendlichdimensionalen Räumen vorkommen, dass die kanonische Abbildung $\alpha\colon V \to V''$ ein Isomorphismus ist; V heißt in diesem Fall ein *reflexiver Raum*.
Prominente reflexive Räume sind die Räume $\mathcal{L}_p(\mu)$ mit $1 < p < \infty$ über einem Maß μ. Ihre Dualräume erhält man (bis auf isometrische Isomorphie) jeweils, wenn man p durch jenes (sogenannte *konjugierte*) q ersetzt, welches durch $\frac{1}{p} + \frac{1}{q} = 1$ definiert ist.
Die Sprache der Kategorien und Funktoren ermöglicht es, ähnliche Situationen in einem sehr allgemeinen Kontext zu beschreiben. Hier wollen wir uns allerdings mit diesem sparsamen Hinweis begnügen.

2.3.5. Kommutative Diagramme als Funktoren

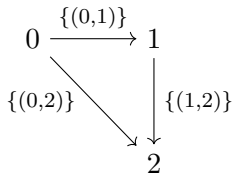
Inhalt in Kurzfassung: Kommutative Diagramme sind graphische Darstellungen dafür, dass verschiedene Verkettungen gewisser Abbildungen übereinstimmen. Situationen, in denen es genau darum geht, sind in der Algebra ubiquitär. Sehr reizvoll ist die Einsicht, dass derartige Konstellationen auch in der Sprache der Kategorien und Funktoren, angewandt auf Kategorien von Graphen, ausgedrückt werden können.

Wir haben schon wiederholt kommutative Diagramme auf intuitive Weise verwendet als Illustrationen für „kompatible“ Abbildungen in dem Sinne, dass je zwei „Pfade“ von

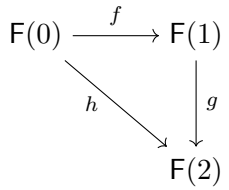
[64] oder auch *adjungierte* Abbildung

Abbildungen zwischen zwei Objekten dasselbe Ergebnis liefern sollen. Interessanterweise lassen sich kommutative Diagramme auch formal als Funktoren betrachten.

Beispiel 2.3.5.1. Sei $V := \{0,1,2\}$, $E := \{(0,1),(1,2)\}$. Die transitive Hülle von E ist dann $E^* = \{(0,1),(1,2),(0,2)\}$. Durch (V,E) bzw. durch (V,E^*) wird (wie in Definition 2.3.2.4 beschrieben) eine Kategorie $\mathcal{3}$ mit 3 Objekten und 3 Morphismen (sowie 3 identischen Morphismen) definiert:

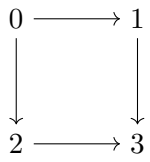


Sei nun $\mathcal{C}$ eine beliebige Kategorie. Dann wird ein kovarianter Funktor $\mathsf{F}\colon \mathcal{3} \to \mathcal{C}$ durch die drei Objekte $\mathsf{F}(0)$, $\mathsf{F}(1)$, $\mathsf{F}(2)$ und durch die drei Morphismen[65] $f := \mathsf{F}(0,1)$, $g := \mathsf{F}(1,2)$ und $h := \mathsf{F}(0,2)$ beschrieben, wobei (wegen der Homomorphieeigenschaft von F) die Bedingung $h = g \circ f$ gelten muss.



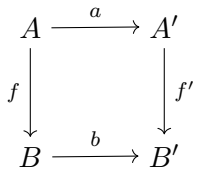
Ein Funktor $\mathsf{F}\colon \mathcal{3} \to \mathcal{C}$ ist also ein *kommutierendes* oder *kommutatives Dreieck* von $\mathcal{C}$-Morphismen.

Beispiel 2.3.5.2. Sei $V := \{0,1,2,3\}$, $E := \{(0,1),(0,2),(1,3),(2,3)\}$. Durch (V,E) (bzw. durch (V,E^*)) wird eine Kategorie mit 4 Objekten und 5 Morphismen (sowie 4 identischen Morphismen) beschrieben, die wir $\square$ nennen. (Im folgenden Diagramm ist der Pfeil $(2,3) \circ (0,2) = (0,3) = (1,3) \circ (0,1)$ nicht eingezeichnet.)



Ein Funktor $\mathsf{F}\colon \square \to \mathcal{C}$ wird durch die vier $\mathcal{C}$-Objekte $A = \mathsf{F}(0), A' = \mathsf{F}(1), B = \mathsf{F}(2), B' = \mathsf{F}(3)$ und durch die vier Morphismen f, f', a, b gegeben, die $f' \circ a = b \circ f$ erfüllen müssen, wodurch ein fünfter (diagonaler) Morphismus definiert wird.

[65] Statt $f := \mathsf{F}(0,1)$ könnte man genauer $f := \mathsf{F}(\,(0,1)\,)$ schreiben, da ja F keine zweistellige Funktion ist, die zwei Argumente 0 und 1 erhält, sondern eine einstellige Funktion, die das Argument $(0,1)$ erhält. Dies wäre aber mühsamer zu lesen.



So ein Funktor beschreibt also ein *kommutierendes* oder *kommutatives Quadrat* von $\mathcal{C}$-Morphismen.

Definition 2.3.5.3. Sei V Menge, $E \subseteq V \times V$ eine Relation. Die Struktur $\Gamma = (V, E)$ bezeichnen wir als *gerichteten Graphen*. Die reflexive transitive Hülle E^* von E fassen wir wie in Definition 2.3.2.4 als Kategorie auf, die wir auch mit Γ bezeichnen.
Sei $\mathcal{C}$ eine Kategorie. Unter einem *kommutativen Γ-Diagramm in $\mathcal{C}$* verstehen wir einen kovarianten Funktor von Γ nach $\mathcal{C}$.

Anmerkung 2.3.5.4. Man könnte hier auch kontravariante Funktoren betrachten. Einen kontravarianten Funktor $(V, E) \to \mathcal{C}$ fassen wir aber lieber als kovarianten Funktor $(V, E^{op}) \to \mathcal{C}$ auf, wobei $E^{op} := \{(y, x) \mid (x, y) \in E\}$.

Das folgende Lemma zeigt, dass unsere Definition auch tatsächlich die gewünschte Intuition von „miteinander kompatiblen“ Abbildungen formalisiert.

Lemma 2.3.5.5. *Sei $\Gamma = (V, E)$ ein Graph und $\mathcal{C}$ eine Kategorie.*
Dann ist jedes kommutative Γ-Diagramm F (also: jeder Funktor $\mathsf{F}\colon \Gamma \to \mathcal{C}$) durch die Familie $(\mathsf{F}(e) \mid e \in E)$ eindeutig bestimmt.
Umgekehrt gilt: Sei $(f_e \mid e \in E)$ eine mit E indizierte Familie von $\mathcal{C}$-Morphismen. Dann gibt es ein kommutatives Γ-Diagramm F mit $\mathsf{F}(e) = f_e$ für alle $e \in E$ genau dann, wenn

- *erstens für alle $(x, y), (y, z) \in E$ gilt, dass das Ziel von $f_{(x,y)}$ gleich der Quelle von $f_{(y,z)}$ ist;*
- *zweitens für alle $(x, y) \in E^*$ und für beliebige Pfade $(x, z_1), (z_1, z_2), \ldots, (z_k, y)$ in E und $(x, z'_1), (z'_1, z'_2), \ldots, (z'_{k'}, y)$ in E die Gleichheit $f_{z_k,y} \circ \cdots \circ f_{x,z_1} = f_{z'_{k'},y} \circ \cdots \circ f_{x,z'_1}$ gilt. (Es genügt, dies für Pfade zu überprüfen, bei denen $\{z_1, \ldots, z_k\}$ und $\{z'_1, \ldots, z'_{k'}\}$ disjunkt sind.)*

UE 114 ► Übungsaufgabe 2.3.5.6. (V) Beweisen Sie Lemma 2.3.5.5. **◄ UE 114**

2.3.6. Natürliche Transformationen

Inhalt in Kurzfassung: Stehen zwei Funktoren in einer Beziehung, die durch ein bestimmtes kommutatives Diagramm dargestellt werden kann, stößt man schnell auf den Begriff der natürlichen Transformation zwischen zwei Funktoren. Hier berühren wir diesen Themenkreis nur sehr oberflächlich, um die vorliegende Darstellung einiger Grundbegriffe der Kategorientheorie etwas abzurunden. Wir werden diese Konzepte später nicht mehr brauchen.

Beispiel 2.3.6.1. Wir betrachten die Menge $\mathbb{Z}$ mit der Relation $\{(n, n+1) \mid n \in \mathbb{Z}\}$.

$$\cdots \to -2 \to -1 \to 0 \to 1 \to 2 \to \cdots$$

Die transitive reflexive Hülle dieser Relation ist die wohlbekannte Relation $\leq$; wie in Definition 2.3.2.4 wird $\mathbb{Z}$ dadurch zu einer Kategorie.
Sei $\mathcal{C}$ eine beliebige Kategorie. Ein kovarianter Funktor $\mathsf{F}\colon \mathbb{Z} \to \mathcal{C}$ wird dann durch eine Familie $(A_n \mid n \in \mathbb{Z})$ von $\mathcal{C}$-Objekten zusammen mit einer Familie $(f_n \mid n \in \mathbb{Z})$ von $\mathcal{C}$-Morphismen gegeben, wobei $f_n \in \mathrm{Hom}_{\mathcal{C}}(A_n, A_{n+1})$ gilt.
Seien die $\mathbb{Z}$-Diagramme F und G durch $(A_n, f_n \mid n \in \mathbb{Z})$ bzw. $(B_n, g_n \mid n \in \mathbb{Z})$ gegeben. Eine *natürliche Transformation* (oder ein *Morphismus von Diagrammen*) ist dann eine Familie $(\varphi_n \mid n \in \mathbb{Z})$ von Morphismen, $\varphi_n\colon A_n \to B_n$, wobei

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & A_{n-1} & \xrightarrow{f_{n-1}} & A_n & \xrightarrow{f_n} & A_{n+1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \varphi_{n-1}} & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n+1}} & & \\
\cdots & \longrightarrow & B_{n-1} & \xrightarrow{g_{n-1}} & B_n & \xrightarrow{g_n} & B_{n+1} & \longrightarrow & \cdots
\end{array}$$

aus lauter kommutativen Quadraten besteht.
Anders formuliert: Für alle n gilt $\varphi_{n+1} \circ f_n = g_n \circ \varphi_n$.

$$\begin{array}{ccc}
A_n & \xrightarrow{f_n} & A_{n+1} \\
\downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n+1}} \\
B_n & \xrightarrow{g_n} & B_{n+1}
\end{array}$$

Dieses Konzept wird zum Beispiel in der Modultheorie im Zusammenhang mit (exakten) Sequenzen in 7.2.3 wichtige Anwendungen finden.

Definition 2.3.6.2. Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien, und seien F und G kovariante Funktoren von $\mathcal{C}$ nach $\mathcal{D}$. Eine *natürliche Transformation* τ von F nach G ist eine mit $Ob(\mathcal{C})$ indizierte Familie von Morphismen in $\mathcal{D}$

$$(\tau_A \mid A \in Ob(\mathcal{C})) \qquad \text{mit} \qquad \tau_A \in \mathrm{Hom}_{\mathcal{D}}(\mathsf{F}(A), \mathsf{G}(A)) \text{ für alle } A \in Ob(\mathcal{C})$$

für die das unten stehende Quadrat kommutiert, also: für alle $A, B \in Ob(\mathcal{C})$ und alle $h \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ ist die Bedingung $\tau_B \circ \mathsf{F}(h) = \mathsf{G}(h) \circ \tau_A$ erfüllt.

$$\begin{array}{ccc}
\mathsf{F}(A) & \xrightarrow{\mathsf{F}(h)} & \mathsf{F}(B) \\
\downarrow{\scriptstyle \tau_A} & & \downarrow{\scriptstyle \tau_B} \\
\mathsf{G}(A) & \xrightarrow{\mathsf{G}(h)} & \mathsf{G}(B)
\end{array}$$

Wir kürzen den Sachverhalt „τ ist natürliche Transformation von F nach G“ durch den Ausdruck $\tau\colon \mathsf{F} \to \mathsf{G}$ ab.

Beispiel 2.3.6.3. Sei $\mathfrak{P}\colon \mathcal{Sets} \to \mathcal{Sets}$ der kovariante Potenzmengenfunktor aus Definition 2.3.4.5, und sei $I\colon \mathcal{Sets} \to \mathcal{Sets}$ der identische Funktor ($I(A) = A$, $I(f) = f$ für alle Objekte A bzw. Morphismen f in $\mathcal{Sets}$.)
Für jede Menge A sei $\tau_A\colon A \to \mathfrak{P}(A)$ die durch $\tau_A(x) = \{x\}$ definierte Abbildung. Dann ist $\tau = (\tau_A \mid A \in \mathcal{Sets})$ eine natürliche Transformation von I nach $\mathfrak{P}$.

UE 115 ► **Übungsaufgabe 2.3.6.4.** (E) Für jede punktierte Menge $(A, a_0) \in Ob(\mathcal{Sets}_*)$ definieren wir $\mathfrak{P}^*(A, a_0) := (\{B \subseteq A \mid a_0 \in B\}, \{a_0\}) \in Ob(\mathcal{Sets}_*)$.
Sei $I\colon \mathcal{Sets}_* \to \mathcal{Sets}_*$ der Identitätsfunktor. Zeigen Sie, dass $\mathfrak{P}^*$ (bei geeigneter Definition auf den Morphismen) ein kovarianter Funktor von $\mathcal{Sets}_*$ nach $\mathcal{Sets}_*$ ist, und geben Sie eine natürliche Transformation von $\mathfrak{P}^*$ nach I an. ◄ **UE 115**

Lemma 2.3.6.5. *Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien.*

(1) *Seien $\mathsf{F}, \mathsf{G}, \mathsf{H}$ Funktoren von $\mathcal{C}$ nach $\mathcal{D}$, und seien $\sigma\colon \mathsf{F} \to \mathsf{G}$ und $\tau\colon \mathsf{G} \to \mathsf{H}$ natürliche Transformationen. Dann ist $\tau \circ \sigma$, definiert durch $(\tau \circ \sigma)_A := \tau_A \circ \sigma_A : \mathsf{F}(A) \to \mathsf{H}(A)$ für alle $A \in \mathrm{Ob}(\mathcal{C})$, eine natürliche Transformation von F nach H.*

(2) *Sei F ein Funktor von $\mathcal{C}$ nach $\mathcal{D}$. Die Familie $\mathrm{id}_{\mathsf{F}} := (\mathrm{id}_{\mathsf{F}(A)} \mid A \in Ob(\mathcal{C}))$ ist stets eine natürliche Transformation von F nach F.*

UE 116 ► **Übungsaufgabe 2.3.6.6.** (E) Beweisen Sie Lemma 2.3.6.5. ◄ **UE 116**

Man kann Beispiel 2.3.6.1 verallgemeinern, indem man statt der Kategorie $\mathbb{Z}$ eine beliebige kleine Kategorie als „Indexmenge“ zulässt. Damit kann man die Klasse aller kovarianten Funktoren $\mathsf{F}\colon \mathcal{J} \to \mathcal{D}$ in natürlicher Weise ebenfalls als Kategorie auffassen:

Definition 2.3.6.7. Sei $\mathcal{J}$ eine kleine Kategorie und $\mathcal{D}$ eine Kategorie. Die *Potenzkategorie* $\mathcal{D}^{\mathcal{J}}$ ist so definiert:

- $Ob(\mathcal{D}^{\mathcal{J}})$ ist die Klasse aller kovarianten Funktoren $\mathsf{F}\colon \mathcal{J} \to \mathcal{D}$.
- Für alle $\mathsf{F}, \mathsf{G}\colon \mathcal{J} \to \mathcal{D}$ ist $\mathrm{Hom}_{\mathcal{D}^{\mathcal{J}}}(\mathsf{F}, \mathsf{G})$ die Klasse aller natürlichen Transformationen $\tau\colon \mathsf{F} \to \mathsf{G}$.
- Komposition und Identität sind gemäß Lemma 2.3.6.5 definiert.

UE 117 ► **Übungsaufgabe 2.3.6.8.** (E) Überprüfen Sie, dass $\mathcal{D}^{\mathcal{J}}$ tatsächlich eine Kategorie ist. ◄ **UE 117**

UE 118 ► **Übungsaufgabe 2.3.6.9.** (E) Sei K ein Körper. Sei $\mathsf{V} : \mathcal{Sets} \to \mathcal{Vec}_K$ der in Beispiel 2.3.4.3 definierte Freie Funktor. Sei $\mathsf{U} : \mathcal{Vec}_K \to \mathcal{Sets}$ der Vergissfunktor, und sei $\mathsf{I} : \mathcal{Sets} \to \mathcal{Sets}$ der Identitätsfunktor. Geben Sie eine natürliche Transformation $\tau : \mathsf{I} \to \mathsf{U} \circ \mathsf{V}$ an. ◄ **UE 118**

UE 119 ► **Übungsaufgabe 2.3.6.10.** (E) Seien K ei Körper, seien $\mathsf{V} : \mathcal{Sets} \to \mathcal{Vec}_K$ und $\mathsf{U} : \mathcal{Vec}_K \to \mathcal{Sets}$ wie in der vorigen Aufgabe, und sei $\mathsf{I}' : \mathcal{Vec}_K \to \mathcal{Vec}_K$ der Identitätsfunktor. Geben Sie eine natürliche Transformation $\tau : \mathsf{V} \circ \mathsf{U} \to \mathsf{I}'$ an. (Bemühen Sie sich, eine interessante natürliche Transformation zu finden, und nicht einfach jene, für die jede Abbildung τ_A die Nullabbildung ist.) ◄ **UE 119**

UE 120 ► **Übungsaufgabe 2.3.6.11.** (E) Sei K ein Körper und sei $\mathcal{V}$ die Klasse aller endlichdimensionalen K-Vektorräume (die Morphismen sind die linearen Abbildungen). Sei $^*\colon \mathcal{V} \to \mathcal{V}$ die Einschränkung des kontravarianten Funktors aus Übungsausgabe 2.3.4.10 (dies ist natürlich wieder ein kontravarianter Funktor). Sei weiters $^{**}\colon \mathcal{V} \to \mathcal{V}$ der kovariante Funktor, der sich durch Iteration von * ergibt. Schließlich bezeichne $\mathsf{I} : \mathcal{V} \to \mathcal{V}$ den Identitätsfunktor.
Geben Sie natürliche Transformationen $\tau\colon {}^{**} \to \mathsf{I}$ und $\sigma\colon \mathsf{I} \to {}^{**}$ an, sodass $\sigma \circ \tau = \mathrm{id}_{**}$ und $\tau \circ \sigma = \mathrm{id}_{\mathsf{I}}$ gilt.
(Die beiden Funktoren ** und I sind also in kategoriellem Sinne *isomorph*, was als abstrakte Formulierung der bekannten „natürlichen“ Isomorphie von V und V^{**} für endlichdimensionales V aufgefasst werden kann.) ◄ **UE 120**

3. Elementare Strukturtheorien

Nachdem wir im vorigen Kapitel einen allgemeinen begrifflichen Rahmen zur algebraischen Strukturanalyse aufgebaut haben, sollen nun, sowohl zur Illustration wie auch um für das Weitere wichtige Beispiele kennenzulernen, Ansätze allgemeiner Strukturtheorien für Halbgruppen und Monoide (3.1), Gruppen (3.2), Moduln und abelsche Gruppen (3.3), Ringe (3.4), geordnete Gruppen und Körper (3.5) sowie für Verbände und Boolesche Algebren (3.6) entwickelt werden. Viel davon wird in späteren Kapiteln noch vertieft werden.

3.1. Halbgruppen und Monoide

In diesem Abschnitt geht es durchwegs um Strukturen mit einer binären Operation. Diese Operation schreiben wir aber nur dann an, wenn es zur Unterscheidung vorteilhaft erscheint. Das Produkt zweier Elemente a und b wird also statt mit Infixnotation $a \cdot b$ schlicht als ab notiert. Sehr bald werden wir uns auf assoziative Operationen, also auf Halbgruppen, und dann weiter auf Monoide, also Halbgruppen mit Einselement, konzentrieren. Zu Beginn (3.1.1) geht es um Potenzen von Elementen und ihre Rechenregeln, 3.1.2 bringt wichtige Beispiele (freies und symmetrisches Monoid), in 3.1.3 wird die eindeutige Primfaktorzerlegung in $\mathbb{N}$ unter algebraischen Gesichtspunkten behandelt und in 3.1.4 behandeln wir die Erweiterung von Monoiden um inverse Elemente in Richtung Gruppe.

3.1.1. Potenzen und Inverse

Inhalt in Kurzfassung: Wir beginnen die Halbgruppentheorie mit einfachen Konzepten, die weitgehend aus der elementaren Arithmetik in den Zahlbereichen vertraut sind. Die Tatsache, dass Inverse nicht zu allen Elementen eines Monoids existieren, führt zum Begriff der Einheiten, die stets eine Untergruppe bilden und auch in späteren Kapiteln eine wichtige Rolle spielen werden. Die üblichen Rechenregeln für Potenzen gelten allgemeiner in Halbgruppen bzw. in kommutativen Halbgruppen und zeigen überdies, dass sich jede abelsche Gruppe in natürlicher Weise auch als $\mathbb{Z}$-Modul auffassen lässt.

Die übliche rekursive Definition von *Produkten* auch von mehr als nur zwei Elementen a_i einer Halbgruppe ist offenbar ganz allgemein für binäre Operationen $\cdot$ auf einer Menge A sinnvoll:

$$a_1 \dots a_{n+1} := (a_1 \dots a_n)a_{n+1}.$$

Entsprechend setzt man für *Potenzen*

$$a^1 := a \quad a^{n+1} := a^n \cdot a \quad \text{für } a \in A \text{ und } n \in \mathbb{N}^+ = \mathbb{N} \setminus \{0\}.$$

Gibt es ein bezüglich $\cdot$ neutrales Element $e \in A$, so ergänzt man diese rekursive Definition durch

$$a^0 := e.$$

Existiert überdies ein Inverses a^* zu $a \in A$, setzt man

$$a^{-n} := (a^*)^n.$$

Ist die binäre Operation nicht assoziativ, kann man diese Festsetzung jedoch als willkürlich ansehen, weil Klammerung z. B. von rechts statt von links zu anderen Ergebnissen führen könnte.

UE 121 ► **Übungsaufgabe 3.1.1.1.** (F) Geben Sie eine Menge A und eine binäre Operation $\cdot$ auf A derart an, dass $a^3 \neq a \cdot (a \cdot a)$ für ein $a \in A$. ◄ **UE 121**

Für assoziative Operationen jedoch ist das Anschreiben von Klammern bei Produkten von drei oder mehr Elementen nicht erforderlich, wie wir aus Übungsaufgabe 2.1.3.5 ersehen. Explizit gilt also: Ist H eine Halbgruppe und sind $a_1, \ldots, a_n \in H$, so definiert das *Produkt* $a_1 a_2 \ldots a_n$ ein eindeutiges Element, unabhängig davon, wie die Klammern gesetzt werden.
Wir erinnern an Proposition 2.1.3.9. Aus ihr folgt insbesondere, dass in einer Halbgruppe $(H, \cdot)$ mit einem Element $e \in H$, welches $ae = ea = a$ für alle $a \in H$ erfüllt, dieses eindeutig bestimmt ist, d. h., es gibt nur ein Element, für das $(H, \cdot, e)$ sogar ein Monoid ist. In diesem Fall ist dann auch für jedes $a \in H$ ein Inverses a^{-1}, sofern es existiert, eindeutig bestimmt. Gibt es in einem Monoid $(M, \cdot, e)$ für alle $a \in M$ ein a^{-1}, so liegt demnach eine eindeutige unäre Operation $.^{-1} : M \to M$, $a \mapsto a^{-1}$ vor, die $(M, \cdot, e, .^{-1})$ zu einer Gruppe macht. Haben nicht alle $a \in M$ ein Inverses, so liegt die folgende Begriffsbildung nahe.

Definition 3.1.1.2. Ist $\mathfrak{M} = (M, \cdot, e)$ ein Monoid, so nennt man ein Element $a \in M$, zu dem es in M ein Inverses a^{-1} (also ein Element mit $aa^{-1} = a^{-1}a = e$) gibt, eine *Einheit*. Die Menge $E = E(\mathfrak{M}) = \mathfrak{M}^*$ aller Einheiten heißt die *Einheitengruppe* von $\mathfrak{M}$.

Diese Terminologie ist berechtigt:

Proposition 3.1.1.3. *Die Einheitengruppe eines Monoids ist eine Gruppe.*

UE 122 ► **Übungsaufgabe 3.1.1.4.** (V) Beweisen Sie Proposition 3.1.1.3. ◄ **UE 122**

Im Zusammenhang mit Homomorphismen sind folgende einfache Beobachtungen nützlich:

Proposition 3.1.1.5. *Seien H und H' Halbgruppen und $\varphi : H \to H'$ ein Homomorphismus.*

1. *Ist e links- bzw. rechtsneutral in H, so ist $\varphi(e)$ links- bzw. rechtsneutral in $\varphi(H)$.*

2. *Ist $e \in H$ neutral in H und $e' \in H'$ neutral in H', so folgt im Allgemeinen* nicht $\varphi(e) = e'$.

3. *Seien $(H, \cdot, e)$ und $(H', \cdot, e')$ sogar Monoide und $\varphi\colon H \to H'$ ein Monoidhomomorphismus. Ist a_l ein Linksinverses von a, dann ist $\varphi(a_l)$ ein Linksinverses von $\varphi(a)$. Analog gilt dann auch: Ist a_r ein Rechtsinverses von a, dann ist $\varphi(a_r)$ ein Rechtsinverses von $\varphi(a)$. Inbesondere gilt: Wenn a ein Inverses hat, dann auch $\varphi(a)$, wobei $\varphi(a)^{-1} = \varphi(a^{-1})$.*

4. *Seien $(H, \cdot, e, ^{-1})$ und $(H', \cdot, e', ^{-1})$ sogar Gruppen und $\varphi\colon H \to H'$ ein Monoidhomomorphismus. Dann ist φ automatisch ein Gruppenhomomorphismus.*

UE 123 ► Übungsaufgabe 3.1.1.6. (V) Beweisen Sie Proposition 3.1.1.5. **◄ UE 123**

Die vorletzte Aussage der vorangehenden Proposition liefert die Verträglichkeit von Inversen mit Homomorphismen. Ein weiteres einfaches Verträglichkeitsresultat lässt sich für Inverse und Kommutativität beweisen.

Lemma 3.1.1.7. *Sei H eine Halbgruppe und seien $a, b \in H$ mit $ab = ba$. Wenn a ein Inverses a^{-1} hat, dann gilt $a^{-1}b = ba^{-1}$. Hat b ebenfalls ein Inverses b^{-1}, dann gilt auch $a^{-1}b^{-1} = b^{-1}a^{-1}$.*

UE 124 ► Übungsaufgabe 3.1.1.8. Beweisen Sie Proposition 3.1.1.7. Geben Sie explizit an, wo und wie Sie das Assoziativgesetz verwenden. („Wie“ bedeutet: Geben Sie an, für welche A, B, C Sie $(AB)C = A(BC)$ verwenden.) **◄ UE 124**

Unabhängig davon, ob es in einer Halbgruppe bereits ein neutrales Element gibt, kann ein neues Element hinzugefügt werden, das diese Rolle übernimmt. Man rechnet leicht nach:

Proposition 3.1.1.9. *Ist H eine Halbgruppe und $e \notin H$, so wird $M := H \cup \{e\}$ zum Monoid mit Einselement e, wenn man die binäre Operation auf H auf M fortsetzt durch $eh = he := h$ für alle $h \in M$.*

Sehr häufig werden wir statt von Halbgruppen gleich von Monoiden ausgehen, insbesondere wenn wir uns damit lästige Fallunterscheidungen oder Sonderfälle ersparen können. Dank Proposition 3.1.1.9 bedeutet das keine schwerwiegende Einschränkung. Zu beachten ist eventuell, dass durch die in Proposition 3.1.1.9 beschriebene Konstruktion ein in H möglicherweise bereits existierendes Einselement e_H wegen $e_H e = e e_H = e_H \neq e$ in $M = H \cup \{e\}$ diesen Status an e abgeben muss.

Wir kehren zurück zu Potenzen in Halbgruppen, Monoiden und Gruppen. Offenbar gelten die folgenden von den klassischen Zahlenbereichen vertrauten Rechenregeln auch in unserem allgemeineren Kontext:

Proposition 3.1.1.10. *In Halbgruppen H gelten folgende Rechenregeln:*

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

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

(3) $(ab)^n = a^n b^n$, *sofern* $ab = ba$, *insbesondere also wenn die binäre Operation kommutativ ist,*

für alle $a, b \in H$ und $m, n \in \mathbb{N}^+$. Ist H ein Monoid, so sind auch $m = 0$ und/oder $n = 0$ zugelassen, im Fall der Existenz von Inversen a^{-1} von a und b^{-1} von b auch beliebige $m, n \in \mathbb{Z}$.

UE 125 ► **Übungsaufgabe 3.1.1.11.** (V) Beweisen Sie Proposition 3.1.1.10. Gehen Sie dabei von der induktiven Definition von a^n aus: a^0 ist das neutrale Element, $a^1 := a$, $a^{n+1} := a^n \cdot a$ für $n \geq 0$, a^{-1} ist invers zu a, $a^{-n} := (a^{-1})^n$ für $n \geq 2$. Verwenden Sie vollständige Induktion, und geben Sie explizit an, auf welche Teilmenge von $\mathbb{N}$ Sie das Induktionsprinzip anwenden. Achtung: Gelegentlich sind Fallunterscheidungen wie $n \geq 0$, $n < 0$ notwendig. Geben Sie explizit an, wo und wie Sie das Assoziativgesetz verwenden. („Wie“ bedeutet: Geben Sie an, für welche A, B, C Sie $(AB)C = A(BC)$ verwenden.) ◄ **UE 125**

Die Rechenregel $a^m a^n = a^{m+n}$ spielt im Beweis der folgenden Aussage die entscheidende Rolle. In Kapitel 4 werden wir die dabei auftretenden abstrakten Gesichtspunkte noch in allgemeinerem Zusammenhang vertiefen.

Proposition 3.1.1.12. *Ist H eine Halbgruppe und $a \in H$, so gibt es genau einen Halbgruppenhomomorphismus $\varphi\colon \mathbb{N}^+ \to H$ von der additiven Halbgruppe $\mathbb{N}^+$ nach H mit $\varphi(1) = a$, nämlich $\varphi : n \mapsto a^n$. Der Bildbereich von φ ist die von a erzeugte Halbgruppe $\langle a \rangle$. Ist H sogar ein Monoid mit Einselement e, so lässt sich φ durch $\varphi(0) := e$ sogar zu einem ebenfalls eindeutigen Monoidhomomorphismus $\mathbb{N} \to H$ fortsetzen.*

UE 126 ► **Übungsaufgabe 3.1.1.13.** (V,W) Beweisen Sie Proposition 3.1.1.12 und deuten Sie diese Aussage als universelle Eigenschaft in einer geeigneten Kategorie. Bereits früher bewiesene Tatsachen dürfen und sollen Sie möglichst verwenden. ◄ **UE 126**

Als Verallgemeinerung davon lässt sich die folgende Tatsache auffassen:

Proposition 3.1.1.14. *Sei H eine Halbgruppe und $X \subseteq H$. Die von X erzeugte Unterhalbgruppe $\langle X \rangle$ ist die Menge M aller Produkte $x_1 x_2 \dots x_n$ (wie in der Definition zu Beginn linksgeklammert zu denken) mit $n \in \mathbb{N}^+$ und $x_i \in X$ für $i = 1, \dots, n$.*

UE 127 ► **Übungsaufgabe 3.1.1.15.** (F) Beweisen Sie Proposition 3.1.1.14 unter Verwendung von Proposition 2.2.1.14. Finden Sie außerdem ein Beispiel einer Algebra $(H, \cdot)$ vom Typ (2) und einer Teilmenge $X \subseteq H$, sodass $M \neq \langle X \rangle$ gilt. Welche Inklusion muss aber jedenfalls gelten? ◄ **UE 127**

Fast selbsterklärend ist die Schreibweise für Komplexprodukte.

Definition 3.1.1.16. Ist H eine Halbgruppe, $n \in \mathbb{N}$, und sind $A_1, \ldots, A_n \subseteq H$ Teilmengen von H, so heißt die Teilmenge

$$A_1 \cdots A_n := \{a_1 \ldots a_n : \ a_i \in A_i \text{ für } i = 1, \ldots, n\}$$

Komplexprodukt von $A_1, \ldots, A_n$.[1]
Falls mindestens eine der Mengen A_1, ..., A_n leer ist, so ist auch das Komplexprodukt $A_1 \cdots A_n$ leer.

3.1.2. Wichtige Beispiele von Halbgruppen

Inhalt in Kurzfassung: Als wichtigste Beispiele von Halbgruppen bzw. Monoiden werden das freie und das symmetrische Monoid samt Darstellungssatz von Cayley ausführlicher besprochen.

Die wichtigste Halbgruppe, die wir bisher behandelt haben, ist $\mathbb{N}$ bezüglich $+$. Ihre Bedeutung liegt primär an der Rolle der natürlichen Zahlen als Kardinalitäten endlicher Mengen (siehe Unterabschnitt 1.1.1), kommt aber auch unter abstrakt algebraischen Gesichtspunkten in Proposition 3.1.1.12 zum Ausdruck. In Verallgemeinerung davon könnte man nach einer Halbgruppe $F = F(X)$ (oder einem Monoid) mit der Eigenschaft suchen, dass jede Abbildung $j : X \to H$ in eine Halbgruppe (oder in ein Monoid) H zu einem eindeutigen Homomorphismus $F(X) \to H$ fortgesetzt werden kann. Der Buchstabe F steht für *frei*, weil so eine Struktur eine *freie Halbgruppe* (oder ein *freies Monoid*) heißt. Der Hintergrund wird im allgemeineren Kontext von Abschnitt 4.1 deutlich werden.
Die Konstruktion eines solchen $F(X)$ ist ziemlich einfach. Als Trägermenge hat man lediglich die Menge X^* aller endlichen (Zeichen-)Folgen (Strings, Wörter über X) $x_1 \ldots x_n$ mit $n \in \mathbb{N} \setminus \{0\}$ und $x_i \in X$ für $i = 1, \ldots, n$ zu nehmen, als Operation die *Konkatenation*

$$(x_1 \ldots x_n) \cdot (y_1 \ldots y_m) := x_1 \ldots x_n y_1 \ldots y_m.$$

Wem die Arbeit mit mathematisch etwas vagen Objekten wie „Zeichenketten“ $x_1 \ldots x_n$ missfällt, kann stattdessen Tupel $(x_1, \ldots, x_n)$ verwenden und formal etwas korrekter definieren: $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_m) := (z_1, \ldots, z_{n+m})$ mit $z_i := x_i$ für $i = 1, \ldots, n$ und $z_{n+j} := y_j$ für $j = 1, \ldots, m$. Will man analog ein freies Monoid statt einer freien Halbgruppe, so erweitert man die Menge aller endlichen Zeichenketten um das sogenannte *leere Wort* , das wir oft mit dem Buchstaben ε bezeichnen. Formal kann man es als Folge der Länge 0 auffassen, also als Funktion mit leerem Definitionsbereich. Das leere Wort ist das neutrale Element bezüglich der Konkatenation. Auch diese erweiterte Menge wird als X^* bezeichnet.

[1] Die naheliegende Schreibweise A^n für den Fall $A_1 = \ldots = A_n$ ist problematisch, weil sie sehr leicht zur Verwechslung mit dem kartesischen Produkt $A \times A \times \ldots \times A$ führen kann, außerdem zur Verwechslung mit der Menge $\{a^n : mid\ a \in A\}$.

UE 128 ▶ **Übungsaufgabe 3.1.2.1.** (V) Begründen Sie, dass die oben beschriebene Struktur tatsächlich die oben formulierte Eigenschaft einer freien Halbgruppe bzw. eines freien Monoids hat: Jede Abbildung $j : X \to H$ in eine Halbgruppe bzw. in ein Monoid H kann zu einem eindeutigen Homomorphismus $X^* \to H$ fortgesetzt werden kann. Deuten Sie die Situation auch als universelle Eigenschaft in einer geeigneten Kategorie. ◀ **UE 128**

Freie Halbgruppen und Monoide über Alphabeten spielen eine wichtige Rolle in der Theorie der formalen Sprachen und somit in der theoretischen Informatik.
Hätten wir uns auf abelsche Halbgruppen/Monoide beschränkt, so würde sich die Konstruktion vereinfachen, weil es nicht auf die Reihenfolge der x_i in einer Zeichenkette ankommt, sondern nur auf die Anzahl $n_x \in \mathbb{N}$ der Vorkommnisse jedes $x \in X$ (wobei in jeder Zeichenkette nur endlich viele x vorkommen dürfen). Die Verfolgung dieses Programms ist Gegenstand einer Übungsaufgabe:

UE 129 ▶ **Übungsaufgabe 3.1.2.2.** (V) Für jede Menge X sei für alle $x_0 \in X$ das Tupel[2] $e_{x_0} \in \mathbb{N}^X$ durch ◀ **UE 129**

$$e_{x_0}(x_0) := 1,\ \forall x \in X \setminus \{x_0\} : e_{x_0}(x) := 0$$

definiert. Sei $\mathbb{N}^{\langle X \rangle}$ die von $\{e_{x_0} \mid x_0 \in X\}$ erzeugte Unterhalbgruppe des direkten Produkts $\mathbb{N}^X$ von $|X|$ Kopien von $(\mathbb{N}, +, 0)$.

(1) Geben Sie eine explizite Beschreibung der Elemente von $\mathbb{N}^{\langle X \rangle}$ und begründen Sie, dass $\mathbb{N}^{\langle X \rangle}$ ein Monoid ist (geben Sie das neutrale Element an).

(2) Zeigen Sie: Für alle abelschen Monoide H und alle Funktionen $j : X \to H$ gibt es genau einen Homomorphismus $h : \mathbb{N}^{\langle X \rangle} \to H$, der $\forall x_0 \in X : h(e_{x_0}) = j(x_0)$ erfüllt. An welcher Stelle des Beweises verwenden Sie, dass H ein neutrales Element enthält?

(3) Geben Sie eine ähnliche Konstruktion (das heißt: es soll das Analogon von (2) gelten) für abelsche Halbgruppen statt Monoide an.

Hinweis: Betrachten Sie eine Teilmenge von $\mathbb{N}^{\langle X \rangle}$.

Aus dem Bisherigen ist ersichtlich, dass freie Monoide (analog freie Halbgruppen, freie abelsche Monoide, freie abelsche Halbgruppen) insofern *universell* unter allen Monoiden sind, als jedes beliebige Monoid M homomorphes Bild eines freien Monoids ist, nämlich z. B. mit der Trägermenge von M als X:

UE 130 ▶ **Übungsaufgabe 3.1.2.3.** (F+) Sei M ein Monoid. Zeigen Sie: Es gibt einen surjektiven Homomorphismus $\alpha : M^* \to M$. ◀ **UE 130**

In gewissem Sinn dual wäre die Eigenschaft, dass jedes beliebige Monoid in ein geeignetes Monoid aus einer bestimmten Teilklasse von Monoiden isomorph eingebettet werden kann. Das ist tatsächlich möglich, wenn man als Teilklasse die symmetrischen Halbgruppen nimmt.

[2] ausführlicher: e_{X,x_0}

Definition 3.1.2.4. Sei X eine beliebige Menge und M_X (oder auch X^X) die Menge aller Abbildungen $f\colon X \to X$. Die Abbildungsmultiplikation $\circ$ als binäre Operation zusammen mit der identischen Abbildung $\mathrm{id}_X : x \mapsto x$ als neutralem Element macht M_X zu einem Monoid, dem sogenannten *symmetrischen Monoid* auf X.

Mit dieser Definition gilt der *Darstellungssatz von Cayley für Monoide*:

Satz 3.1.2.5. *Jedes Monoid M lässt sich vermittels der Einbettung $\iota : a \mapsto f_a$, $f_a(x) := ax$ für $a, x \in M$ isomorph in das symmetrische Monoid M_X einbetten, wenn man für X die Trägermenge von M wählt.*

Beweis. Klarerweise ist $\iota\colon M \to M_X$ wohldefiniert mit Definitionsbereich M und Werten in M_X. Weiters ist ι injektiv, denn $\iota(a) = \iota(b)$ bedeutet $f_a = f_b$ und somit speziell $a = ae = f_a(e) = f_b(e) = be = b$, wenn e das neutrale Element in M bezeichnet. Wegen $f_e(x) = ex = x$ bildet ι das neutrale Element e in M auf $\iota(e) = f_e = \mathrm{id}_X$, das neutrale Element in M_X, ab. Schließlich ist auch die Homomorphiebedingung für die binäre Operation erfüllt:

$$f_{ab}(x) = (ab)x = a(bx) = f_a(bx) = f_a(f_b(x)) = (f_a \circ f_b)(x)$$

(erst jetzt haben wir die Assoziativität verwendet) für alle $x \in X$, also $\iota(ab) = f_{ab} = f_a \circ f_b = \iota(a) \circ \iota(b)$. □

Die Einbettung ι aus Satz 3.1.2.5 nennt man die *reguläre Darstellung* des Monoids M. Sie wird auch im ganz analogen und noch wichtigeren Darstellungssatz von Cayley für Gruppen (siehe Unterabschnitt 3.2.5) verwendet. Bedenkt man die Möglichkeit, beliebige Halbgruppen zu Monoiden zu ergänzen (siehe Proposition 3.1.1.9), so zeigen die Cayleyschen Sätze, dass die Komposition von Abbildungen die allgemeinste assoziative Operation repräsentieren kann.

UE 131 ► **Übungsaufgabe 3.1.2.6.** (F) In dieser Aufgabe beschäftigen wir uns mit einem zum Darstellungssatz von Cayley ähnlichen Satz für Halbgruppen statt für Monoide. ◄ **UE 131**

1. Sei H eine Halbgruppe. Finden Sie eine Menge S und eine isomorphe Einbettung $\iota : H \to S^S$. Hinweis: Proposition 3.1.1.9
2. Finden Sie eine Halbgruppe H, sodass die Abbildung $\varphi : H \to H^H$, $a \mapsto f_a$, wobei $f_a(x) := ax$, nicht injektiv ist.

Wichtige Halbgruppen ganz anderer Art treten in der Maßtheorie, Fourieranalysis und Wahrscheinlichkeitstheorie mit der Faltung $*$ von Funktionen oder von Maßen als assoziativer Operation auf. Und zwar ist für zwei Wahrscheinlichkeitsmaße μ und ν ihre Faltung $\mu * \nu$ so definiert, dass sie die Verteilung der Summe $X + Y$ zweier unabhängiger Zufallsgrößen X und Y mit Verteilungen μ bzw. ν ist. So bildet die Menge aller Normalverteilungen $\nu_{m,v}$ auf $\mathbb{R}$ mit Mittelwert $m \in \mathbb{R}$ und Varianz $v \geq 0$ bezüglich der Faltung ein Monoid, das der Rechenregel $\nu_{m_1,v_1} * \nu_{m_2,v_2} = \nu_{m_1+m_2,v_1+v_2}$ genügt, folglich isomorph ist zum (additiven) Monoid $\mathbb{R} \times \mathbb{R}_0^+$.

Hier verzichten wir auf eine Vertiefung solcher Beispiele, weil wir dafür zu weit in die Maßtheorie ausholen müssten. An die Faltung wird uns an späterer Stelle das gleichfalls aus der Analysis vertraute Cauchyprodukt von Potenzreihen (in der Algebra: von formalen Potenzreihen, siehe Unterabschnitt 3.4.6) erinnern, aber auch die Konstruktion des Gruppenrings (siehe Unterabschnitt 4.2.4).

3.1.3. Algebraische Strukturanalyse auf $\mathbb{N}$

Inhalt in Kurzfassung: Wir geben einen ersten Beweis von der Existenz und Eindeutigkeit der Primfaktorzerlegung natürlicher Zahlen und deuten diesen als Struktursatz: Das multiplikative Monoid auf $\mathbb{N}^+$ ist isomorph zur direkten Summe abzählbar unendlich vieler Kopien des additiven Monoids auf $\mathbb{N}$. Ein damit verwandter Struktursatz beschreibt den vollständigen Verband, der durch die Teilerrelation auf $\mathbb{N}$ gegeben ist. Für spätere Zwecke wird auch die Division mit Rest auf $\mathbb{N}$ und $\mathbb{Z}$ bereitgestellt.

Wir wollen wieder mit der Menge $\mathbb{N}$ der natürlichen Zahlen beginnen und wählen ihre sehr einfache additive Struktur zum Bezugspunkt für die Analyse der multiplikativen Struktur. Dabei ist es keine wesentliche Einschränkung, wenn wir uns der einfacheren Notation halber auf das kommutative Monoid (Halbgruppe mit Einselement) $(\mathbb{N}^+, \cdot, 1)$ mit $\mathbb{N}^+ := \mathbb{N} \setminus \{0\}$ konzentrieren. Eine sehr befriedigende Beschreibung liefert der sogenannte *Fundamentalsatz der Arithmetik* oder auch der *Zahlentheorie*. Zur Erinnerung folgen die wichtigsten Definitionen. Dabei ist es manchmal vorteilhaft, statt $\mathbb{N}$ die gesamte Menge $\mathbb{Z}$ heranzuziehen.

Definition 3.1.3.1. Eine ganze Zahl $a \in \mathbb{Z}$ heißt *Teiler* von $b \in \mathbb{Z}$, falls es ein $c \in \mathbb{Z}$ gibt mit $b = ac$, symbolisch $a|b$ (a *teilt* b). Man sagt in diesem Fall auch, b ist ein *Vielfaches* von a. Eine Zahl $p \in \mathbb{N}$ heißt *Primzahl*, falls p innerhalb $\mathbb{N}$ genau die beiden Teiler 1 und $p \neq 1$ hat.[3] Die Menge aller Primzahlen bezeichnen wir mit $\mathbb{P}$.

Satz 3.1.3.2 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl $n > 0$ hat eine (bis auf die Reihenfolge der Faktoren) eindeutige Darstellung als Produkt von Primzahlen, genannt* Primfaktorzerlegung *(*1 *fassen wir als leeres Produkt auf), genauer: Zu jedem $n \in \mathbb{N}$ gibt es genau eine Familie $(e_p)_{p\in\mathbb{P}}$ von Exponenten $e_p \in \mathbb{N}$ mit $n = \prod_{p\in\mathbb{P}} p^{e_p}$. Dabei sind nur endlich viele e_p von* 0 *verschieden, weshalb das Produkt, weil nur endlich viele Faktoren von* 1 *verschieden sind, wohldefiniert ist.*

Beweis. Die Behauptung lässt sich in eine Existenz- und eine Eindeutigkeitsaussage aufspalten.
Zunächst zur Existenz so einer Darstellung: Gäbe es, indirekt, eine positive natürliche Zahl ohne Primfaktorzerlegung, so auch eine kleinste, die wir n nennen. Diese Zahl n ist weder 1 (leeres Produkt) noch eine Primzahl (Produkt aus einem Faktor), hat also einen von 1 und n verschiedenen Teiler $a \in \mathbb{N}$. Also gibt es ein $b \in \mathbb{N}$ mit $n = ab$. Offenbar gilt $1 < a, b < n$. Da n minimal gewählt war, müssen a und b Primfaktorzerlegungen haben, deren Produkt aber eine Primfaktorzerlegung von n ist, Widerspruch.

[3] 1 selbst ist also definitionsgemäß keine Primzahl.

Noch interessanter ist die Eindeutigkeitsaussage: Wieder gehen wir indirekt von einem kleinsten n mit mehr als einer Primfaktorzerlegung aus:

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

mit $p_i, q_j \in \mathbb{P}$ für $1 \leq i \leq r, 1 \leq j \leq s$. Wäre $p_i = q_j$ für gewisse Indizes i, j, so ließe sich durch diese Zahl durchdividieren, und auch $\frac{n}{p_i} < n$ hätte mehr als eine Primfaktorzerlegung, Widerspruch. Also gilt $p_i \neq q_j$ für alle i, j. Insbesondere ist $p_1 \neq q_1$, oBdA $p_1 < q_1$. Wir betrachten die Zahl

$$n' := (q_1 - p_1)q_2 \cdot \ldots \cdot q_s = n - p_1(q_2 \cdot \ldots \cdot q_s) = p_1(p_2 \cdot \ldots \cdot p_r - q_2 \cdot \ldots \cdot q_s) = p_1 m$$

mit $m := p_2 \cdot \ldots \cdot p_r - q_2 \cdot \ldots \cdot q_s$. Wegen $n' > 0$ ist auch $m > 0$. Einerseits gilt nun: Indem man m in Primfaktoren zerlegt, erhält man aus der Gleichung $n' = p_1 m$ eine Primfaktorzerlegung von n' mit mindestens einem Primfaktor p_1. Andererseits überlegen wir, dass p_1 kein Teiler von $q_1 - p_1$ sein kann, weil es sonst auch ein Teiler der Primzahl $q_1 > p_1$ wäre, was unmöglich ist. Deshalb erhält man, wenn man in der Gleichung $n' = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_2$ auch noch eine Primfaktorzerlegung von $q_1 - p_1$ einsetzt, eine Primfaktorzerlegung von n', die p_1 sicher nicht enthält.
Wir haben also zwei verschiedene Primfaktorzerlegungen für n' gefunden, was wegen $n' < n$ im Widerspruch steht zur Minimalität von n. □

Wir verwenden

$$\prod_{p \in \mathbb{P}}^{w} \mathbb{N} = \{(e_p)_{p \in \mathbb{P}} \mid e_p \in \mathbb{N}, e_p \neq 0 \text{ für nur endlich viele } p\},$$

das schwache Produkt (siehe auch Definition 3.2.3.10 für den Fall von Gruppen) abzählbar unendlich vieler (hier mit $p \in \mathbb{P}$ indizierter) Kopien von $\mathbb{N}$. Es enthält jene Elemente des vollen kartesischen Produktes, die nur endlich viele von 0 verschiedene Eintragungen haben. Mit dieser Notation lässt sich Satz 3.1.3.2 auch so formulieren:
Die Abbildung

$$\varphi \colon \prod_{p \in \mathbb{P}}^{w} \mathbb{N} \to \mathbb{N}^+, \quad (e_p)_{p \in \mathbb{P}} \mapsto \prod_{p \in \mathbb{P}} p^{e_p}$$

ist bijektiv.
Doch φ ist nicht nur bijektiv. Für $x = (e_p)_{p \in \mathbb{P}}, y = (f_p)_{p \in \mathbb{P}} \in \prod_{p \in \mathbb{P}}^{w} \mathbb{N}$ ist, wenn wir komponentenweise addieren, wegen

$$\begin{aligned} \varphi(x + y) = \varphi((e_p)_{p \in \mathbb{P}} + (f_p)_{p \in \mathbb{P}}) = \prod_{p \in \mathbb{P}} p^{e_p + f_p} = \prod_{p \in \mathbb{P}} p^{e_p} \cdot \prod_{p \in \mathbb{P}} p^{f_p} = \\ = \varphi((e_p)_{p \in \mathbb{P}}) \cdot \varphi((f_p)_{p \in \mathbb{P}}) = \varphi(x) \cdot \varphi(y) \end{aligned}$$

offenbar auch die Homomorphiebedingung erfüllt. Außerdem gilt $\varphi((0)_{p \in \mathbb{P}}) = 1$. In algebraische Sprache übersetzt haben wir bewiesen:

Satz 3.1.3.3. *Das multiplikative Monoid* $(\mathbb{N}^+, \cdot, 1)$ *der positiven natürlichen Zahlen ist isomorph zum schwachen Produkt abzählbar vieler Kopien des additiven Monoids* $(\mathbb{N}, +, 0)$ *aller natürlichen Zahlen (inklusive* 0*). Ein Isomorphismus* $\varphi\colon \prod^w_{p\in\mathbb{P}}(\mathbb{N}, +, 0) \to (\mathbb{N}^+, \cdot, 1)$ *ist gegeben durch*

$$(e_p)_{p\in\mathbb{P}} \mapsto \prod_{p\in\mathbb{P}} p^{e_p}.$$

Die Macht dieses Satzes wird offensichtlich, wenn man sich folgende Zusammenhänge klar macht. Schreiben wir $(e_p(n))_{p\in\mathbb{P}} := \varphi^{-1}(n)$ mit dem Isomorphismus φ aus Satz 3.1.3.3, so lesen wir für $a, b \in \mathbb{N}^+$ ab, dass Teilbarkeit $a|b$ genau dann gilt, wenn $e_p(a) \leq e_p(b)$ für alle $p \in \mathbb{P}$ gilt. Die relationale Struktur $(\mathbb{N}, |)$ ist also isomorph zu einer relationalen Struktur, die sich in naheliegender Weise als Unterstruktur eines direkten Produktes deuten lässt. Als Totalordnung ist $(\mathbb{N}, \leq)$ verbandsgeordnet im ordnungstheoretischen Sinn. Der zugeordnete Verband $(\mathbb{N}, \max, \min)$ im algebraischen Sinn ist sogar distributiv. Weil die distributiven Verbände als gleichungsdefinierte Klasse (Varietät) abgeschlossen sind bezüglich der Bildung direkter Produkte, ist auch $\prod_{p\in\mathbb{P}}(\mathbb{N}, \max, \min)$ ein distributiver Verband, wobei die Operationen max und min komponentenweise auszuführen sind. $\prod^w_{p\in\mathbb{P}} \mathbb{N}$ ist eine (Trägermenge einer) Unteralgebra dieses Verbandes, somit selbst ein distributiver Verband. Aufgrund der obigen Überlegungen ist φ ein Isomorphismus der zugeordneten Halbordnungen $(\mathbb{N}^+, |)$ und $(\prod^w_{p\in\mathbb{P}} \mathbb{N}, \leq)$, wenn man $\leq$ komponentenweise auffasst. Leicht überlegt man sich, dass der Verband $(\mathbb{N}^+, |)$ distributiv bleibt, wenn man das Element 0 mit $n|0$ für alle $n \in \mathbb{N}$, d. h. als größtes Element, hinzufügt. Wie man sich ebenfalls schnell klar macht, wird der Verband dadurch sogar vollständig. Damit ist ein Beweis für folgenden Satz angedeutet:

Satz 3.1.3.4. *Die Menge* $\mathbb{N}$ *der natürlichen Zahlen bildet bezüglich Teilbarkeit einen distributiven, vollständigen Verband. Kleinstes Element ist* 1*, größtes Element ist* 0*. Das Supremum ist das* kleinste gemeinsame Vielfache*, abgekürzt kgV. Das Infimum ist der* größte gemeinsamer Teiler*, abgekürzt ggT. Sowohl kgV als auch ggT einer Teilmenge* $T \subseteq \mathbb{N}$ *lassen sich aus der Primfaktorzerlegung gewinnen, indem man für jedes* $p \in \mathbb{P}$ *als Exponenten* e_p *(Notation wie oben) das Maximum bzw. das Minimum (sofern vorhanden) aller* $e_p(t)$ *mit* $t \in T$ *nimmt, allerdings mit folgenden Ausnahmen: Für unendliches* T *sowie im Falle* $0 \in T$ *ist* $kgV(T) = 0$*, und für* $T \subseteq \{0\}$ *ist* $ggT(T) = 0$*.*

UE 132 ► Übungsaufgabe 3.1.3.5. (V) Vervollständigen Sie den Beweis von Satz 3.1.3.4. **◄ UE 132**

UE 133 ► Übungsaufgabe 3.1.3.6. (E,D) In den Überlegungen zu Satz 3.1.3.4 hat man sich nicht nur für die algebraische Struktur auf Produkten interessiert, sondern auch für Halbordnungen darauf. Gehen Sie dem nach, indem Sie folgende Schritte ausführen: **◄ UE 133**

(1) Definieren Sie eine Ihnen für das Folgende sinnvoll erscheinende Kategorie $\mathcal{C}$, deren Objekte alle Halbordnungen sind.

(2) Begründen Sie Ihre Wahl der Morphismen in $\mathcal{C}$.

(3) Gibt es in $\mathcal{C}$ uneingeschränkt Produkte?

(4) Schränken Sie $\mathcal{C}$ auf jene Halbordnungen ein, die verbandsgeordnet sind. Wie verhält sich die resultierende Kategorie zur Kategorie der Verbände im algebraischen Sinn, aufgefasst als Varietät?

Auf der Hand liegen Satz 3.1.3.4 entsprechende Aussagen über die multiplikative Struktur von $\mathbb{Z}$. Zu beachten ist lediglich, dass $m|n$ und $n|m$ dann nicht automatisch $n = m$ impliziert, sondern lediglich $n = m$ oder $n = -m$. Entsprechend sind ggT und kgV dann nur bis aufs Vorzeichen eindeutig bestimmt etc. Wir werden davon schon ab jetzt Gebrauch machen, in allgemeinerem Kontext und systematisch wird das Gegenstand der Teilbarkeitslehre in Kapitel 5 sein.
Die multiplikative Halbgruppe von $\mathbb{Z}$ lässt sich in ziemlich offensichtlicher Weise als direktes Produkt von zwei Faktoren beschreiben.

UE 134 ▶ Übungsaufgabe 3.1.3.7. (F) Beschreiben Sie, wie und warum die Halbgruppe $(\mathbb{Z} \setminus \{0\}, \cdot)$ isomorph ist zum direkten Produkt von $(\mathbb{N}^+, \cdot)$ und einer zweiten Halbgruppe. Welcher? ◀ **UE 134**

Zur Erinnerung: Auf einer beliebigen Menge A sind die *Gleichheitsrelation* $\Delta_A := \{(x, x) \mid x \in A\}$ (auch genannt *Identität*), und die *Allrelation* $\nabla_A = A \times A$ stets Äquivalenzrelationen, genannt die *trivialen Äquivalenzrelationen* auf A. Alle anderen Äquivalenzrelationen heißen „nichttrivial“.

UE 135 ▶ Übungsaufgabe 3.1.3.8. (F) Finden Sie nichttriviale Kongruenzrelationen R und S auf der Struktur $(\mathbb{N}, +)$ mit folgenden Eigenschaften: ◀ **UE 135**

- $(3, 14) \in R$
- Es gibt mindestens zwei R-Äquivalenzklassen, die 1-elementig sind, und mindestens zwei, die nicht einelementig sind.
- $(3, 14) \in S$
- Keine S-Äquivalenzklasse ist 1-elementig.

UE 136 ▶ Übungsaufgabe 3.1.3.9. (F+) Finden Sie alle Kongruenzrelationen auf $(\mathbb{N}, +)$. Zeigen Sie insbesondere, dass Sie keine vergessen haben. ◀ **UE 136**
Hinweis: Betrachten Sie die Faktorstruktur $(\mathbb{N}, +)/_\sim$.

UE 137 ▶ Übungsaufgabe 3.1.3.10. (D) In dieser Übungsaufgabe interessieren wir uns für Unteralgebren und Kongruenzrelationen auf $\mathbb{N}$ bezüglich additiver und/oder multiplikativer Struktur. Versuchen Sie jeweils alle Objekte der angegebenen Art zu beschreiben. Wenn Ihnen das zu schwierig erscheint (was in der Mehrzahl der Fälle wahrscheinlich ist), ermitteln Sie, wie viele es davon gibt. Unterscheiden Sie dabei verschiedene unendliche Kardinalitäten, insbesondere $|\mathbb{N}|$ und $|\mathbb{R}|$. ◀ **UE 137**

(1) Unteralgebren von $(\mathbb{N}, +, 0)$
(2) Kongruenzrelationen von $(\mathbb{N}, +, 0)$
(3) Unteralgebren von $(\mathbb{N}, \cdot, 1)$
(4) Kongruenzrelationen von $(\mathbb{N}, \cdot, 1)$
(5) Unteralgebren von $(\mathbb{N}, +, 0, \cdot, 1)$
(6) Kongruenzrelationen von $(\mathbb{N}, +, 0, \cdot, 1)$

Der folgende einfache Sachverhalt verbindet Addition mit Multiplikation und wird sich vielfach als äußerst wichtig erweisen.

Satz 3.1.3.11 (Division mit Rest)**.** *Sei $m > 0$ eine positive ganze Zahl, b eine beliebige ganze Zahl. Dann gibt es genau ein Paar (q, r) von ganzen Zahlen mit folgenden Eigenschaften:*

- $b = qm + r$
- $0 \leq r < m$

q heißt der Quotient*, r der* Rest *der Division. Es ist genau dann $r = 0$, wenn b durch m teilbar ist. (Man beachte, dass $b - r$ jedenfalls durch m teilbar ist.) Genau für $b \in \mathbb{N}$ ist auch $q \in \mathbb{N}$.*

Beweis. Existenz: Wir setzen $q := \lfloor \frac{b}{m} \rfloor$ (die größte ganze Zahl $\leq \frac{b}{m}$) und $r := b - qm$. Aus $q \leq \frac{b}{m} < q + 1$ erhalten wir $qm \leq b < qm + m$, also $0 \leq r < m$.
Eindeutigkeit: Wenn $b = qm + r = q'm + r'$ mit $0 \leq r \leq r' < m$ ist, dann gilt $0 \leq qm - q'm = r' - r < m$. Die Zahl $r' - r$ ist also durch m teilbar; da alle Vielfachen von m entweder ≤ 0 oder $\geq m$ sind, und $r' - r$ im halboffenen Intervall $[0, m)$ liegt, muss $r' - r = 0$, also $r' = r$ gelten, somit auch $q = q'$ (Kürzungsregel).
Ist $b \geq 0$, so zeigt der Beweis der Existenz auch $q \geq 0$. Die Umkehrung ist aus $b = qm + r \geq qm$ und $m > 0$ ersichtlich. □

In der folgenden Übungsaufgabe wird dieser Satz auf beliebige $m \neq 0$ verallgemeinert.

UE 138 ► **Übungsaufgabe 3.1.3.12.** (F) Sei $m \neq 0$ eine ganze Zahl, b eine beliebige ganze Zahl. ◄ **UE 138**
Dann gibt es genau ein Paar (q, r) von ganzen Zahlen mit folgenden Eigenschaften:

- $b = qm + r$
- $0 \leq r < |m|$

Anmerkung 3.1.3.13. Wenn m und b ganze Zahlen mit $b, m \neq 0$ sind, dann gibt es

- genau ein Paar (q_1, r_1) von ganzen Zahlen mit $b = mq_1 + r_1$ und $0 \leq |r_1| < |m|$ und $r_1 \geq 0$
- genau ein Paar (q_2, r_2) von ganzen Zahlen mit $b = mq_2 + r_2$ und $0 \leq |r_2| < |m|$ und $\operatorname{sgn}(r_2) = \operatorname{sgn}(b)$
- genau ein Paar (q_3, r_3) von ganzen Zahlen mit $b = mq_3 + r_3$ und $0 \leq |r_3| < |m|$ und $\operatorname{sgn}(r_3) = \operatorname{sgn}(m)$

Sowohl die Zahl r_1 (die nichtnegativ ist) als auch die Zahl r_2 (die das gleiche Vorzeichen wie b hat) als auch die Zahl r_3 (die das gleiche Vorzeichen wie m hat) könnte man als „Rest bei Division von b durch m“ bezeichnen, und mit $b \bmod m$ oder $b \,\%\, m$ abkürzen. Wenn Sie also diese Sprechweise oder Notation verwenden, dann stellen Sie zunächst klar, welche Definition Sie verwenden.

Anmerkung 3.1.3.14. Gelegentlich (etwa beim Euklidischen Algorithmus) ist die folgende Variante praktischer:
Sei $m \neq 0$ eine ganze Zahl, b eine beliebige ganze Zahl. Dann gibt es ein eindeutiges Paar (q, r) von ganzen Zahlen mit folgenden Eigenschaften:

- $b = qm + r$
- $-q/2 < r \leq q/2$.

3.1.4. Quotienten- bzw. Differenzenmonoid

Inhalt in Kurzfassung: Hat man die Konstruktion der additiven Gruppe $\mathbb{Z}$ aus der Halbgruppe $\mathbb{N}$ vor Augen, so stellt sich die Frage, unter welchen Bedingungen sich diese Konstruktion von $\mathbb{N}$ auf beliebige Halbgruppen bzw. Monoide M verallgemeinern lässt. Wie man sich schnell überzeugt, ist für die Existenz von Inversen eines Halbgruppenelements dessen Kürzbarkeit notwendig. Ist diese für alle Elemente gegeben, so ist Kommutativität hinreichend (nicht notwendig) für die Existenz einer Erweiterung zu einer Gruppe, der sogenannten Quotienten- oder (bei additiver Notation) Differenzengruppe. Varianten dieser Konstruktion betreffen die Möglichkeit, Inverse nicht für alle Elemente, sondern nur für jene aus einem kürzbaren Untermonoid zu fordern. Die resultierenden Strukturen lassen sich durch eine universelle Eigenschaft charakterisieren, nämlich als initiale Objekte in einer geeigneten Kategorie.

Wir erinnern uns an den Übergang von $\mathbb{N}$ zu $\mathbb{Z}$, bei dem ein Monoid zu einer Gruppe erweitert wurde. Dabei müssen also zumindest Inverse hinzugefügt werden. Unser Interesse wird vor allem hinreichenden Bedingungen an ein zunächst beliebiges Monoid M gelten, die garantieren, dass eine analoge Konstruktion möglich ist. In Hinblick auf allgemeinere Situationen ziehen wir die Variante in Betracht, dass nur gewisse Elemente aus M, nämlich jene aus einer Teilmenge $K \subseteq M$, Inverse bekommen müssen. Gesucht ist zunächst also eine isomorphe Einbettung $\iota : M \to Q$ in ein Monoid Q, in dem sämtliche $\iota(k)$ mit $k \in K$ ein Inverses besitzen. So ein k muss jedenfalls kürzbar sein: Aus $xk = yk$ folgt

$$\iota(x) = \iota(x)\iota(k)\iota(k)^{-1} = \iota(xk)\iota(k)^{-1} = \iota(yk)\iota(k)^{-1} = \iota(y)\iota(k)\iota(k)^{-1} = \iota(y),$$

wegen der Injektivität einer isomorphen Einbettung also $x = y$. Somit ist k rechtskürzbar und analog linkskürzbar, insgesamt also tatsächlich kürzbar. Mit $K(M)$ bezeichnen wir die Menge aller kürzbaren Elemente in M. Es ist eine leichte Übungsaufgabe nachzuprüfen, dass $K(M)$ stets ein Untermonoid von M ist.

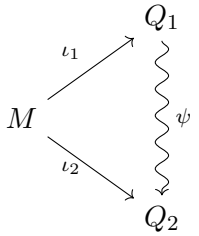
UE 139 ► **Übungsaufgabe 3.1.4.1.** (F) Zeigen Sie: Sowohl die Menge $K_l(M)$ aller links- als auch die Menge $K_r(M)$ aller rechtskürzbaren Elemente in einem Monoid M bilden Untermonoide. Also ist auch $K(M) = K_l(M) \cap K_r(M)$ ein Untermonoid von M. ◄ **UE 139**

Folglich können wir uns auf jene K beschränken, die Untermonoide $K \leq M$ sind.

Definition 3.1.4.2. Seien M und Q Monoide, sei $K \leq M$ kürzbar und sei $\iota : M \to Q$ eine isomorphe Einbettung. Wir sagen, (Q, ι) ist ein *Quotientenmonoid im weiteren Sinn* (*Quotientenmonoid iwS*) bezüglich $K \leq M$, wenn $\iota(k)$ für alle $k \in K$ ein Inverses $\iota(k)^{-1}$ in Q hat. Das von $\iota(M)$ und allen $\iota(k)^{-1}$, $k \in K$, erzeugte Untermonoid von Q bezeichnen wir mit $Q_{(M,\iota)}$.

Für gegebenes kürzbares $K \leq M$ definieren wir die folgende Kategorie $\mathcal{C}(M, K)$.

Definition 3.1.4.3. Die Objekte in $\mathcal{C}(M, K)$ seien die Quotientenmonoide iwS (Q, ι) bezüglich $K \leq M$. Die Morphismen bezüglich $\mathcal{C}(M, K)$ von einem Quotientenmonoid iwS (Q_1, ι_1) in ein Quotientenmonoid iwS (Q_2, ι_2) seien jene isomorphen Einbettungen $\psi\colon Q_1 \to Q_2$, für die $\iota_2 = \psi \circ \iota_1$ gilt.



Die Komposition in $\mathcal{C}(M, K)$ sei die übliche Komposition von Abbildungen.

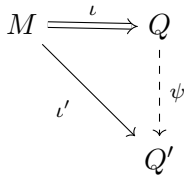
UE 140 ► **Übungsaufgabe 3.1.4.4.** (V) Überzeugen Sie sich davon, dass $\mathcal{C}(M, K)$ tatsächlich eine Kategorie ist und dass darin zwei Quotientenmonoide iwS (Q_1, ι_1) und (Q_2, ι_2) genau dann äquivalent sind, wenn es einen Monoidisomorphismus $\psi : Q_1 \to Q_2$ gibt mit $\iota_2 = \psi \circ \iota_1$. Insbesondere sind in diesem Fall Q_1 und Q_2 als Monoide isomorph. ◄ **UE 140**

Wir erinnern uns nochmals an die Situation $M = K = \mathbb{N}$ und $Q = \mathbb{Z}$. Die Inklusionsabbildung $\iota : \mathbb{N} \to \mathbb{Z}$ hat nach Satz 1.2.1.1 die Eigenschaft, dass es zu jeder isomorphen Einbettung $\iota' : \mathbb{N} \to G$ des additiven Monoids $\mathbb{N}$ in eine Gruppe G eine eindeutige isomorphe Gruppeneinbettung $\psi : \mathbb{Z} \to G$ mit $\iota' = \psi \circ \iota$ gibt. Es gilt sogar etwas mehr, und zwar muss G nicht zwingend eine Gruppe sein – es reicht, dass alle $\iota'(n)$, $n \in \mathbb{N}$, ein Inverses in G haben. Anders ausgedrückt:

UE 141 ► **Übungsaufgabe 3.1.4.5.** (F+) Zeigen Sie, dass $(\mathbb{Z}, \iota)$ ein initiales Objekt in $\mathcal{C}(\mathbb{N}, \mathbb{N})$ ist. ◄ **UE 141**

Als Verallgemeinerung fühlen wir uns zu folgender Definition motiviert:

Definition 3.1.4.6. Sei $K \leq M$ ein kürzbares Untermonoid von M. Ist das Quotientenmonoid iwS (Q, ι) ein initiales Objekt in der Kategorie $\mathcal{C}(M, K)$, so heißt Q zusammen mit ι (formal: das Paar (Q, ι)) ein *Quotientenmonoid im eigentlichen Sinn* (Quotientenmonoid ieS) oder schlicht *Quotientenmonoid* bezüglich $K \leq M$. Ist außerdem $K = M$, so heißt Q zusammen mit ι eine *Quotientengruppe* des Monoids M. Wenn M kommutativ ist und die Verknüpfung additiv geschrieben wird, dann spricht man statt von einem Quotientenmonoid bzw. einer Quotientengruppe auch oft von einem *Differenzenmonoid* bzw. einer *Differenzengruppe*.



Nach Satz 2.3.3.2 sind initiale Objekte in einer Kategorie eindeutig bis auf Äquivalenz. Somit sind zu gegebenem M und K sämtliche Quotienten- bzw. Differenzenmonoide von M bezüglich K zueinander äquivalent, insbesondere (siehe Übungsaufgabe 3.1.4.4) als Monoide isomorph.
Eine Untersuchung der einzelnen Schritte in der Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$, wie sie in Unterabschnitt 1.2.1 behandelt wurde, zeigt sehr schnell, dass von der Kommutativität der Addition auf $\mathbb{N}$ wesentlich Gebrauch gemacht wurde. Sie ist zwar nicht immer notwendig für die Möglichkeit einer Erweiterung eines Monoids M zu einer Gruppe (beispielsweise könnte M selbst bereits eine nichtabelsche Gruppe sein). Allerdings gäbe es ohne diese Voraussetzung (wenn auch recht komplizierte) Gegenbeispiele. Eine technische Komplikation wird sich daraus ergeben, dass Quotientenmonoide iwS im Allgemeinen nicht kommutativ sind. Die folgende Übungsaufgabe zeigt allerdings, dass der „wesentliche“ Teil eines Quotientenmonoids iwS sehr wohl kommutativ ist, wenn wir von einem kommutativen Monoid ausgehen.

UE 142 ► **Übungsaufgabe 3.1.4.7.** (W) Sei M ein Monoid, sei $K \leq M$ kürzbar, sei (Q, ι) ein Quotientenmonoid iwS bezüglich $K \leq M$ und sei $Q_{(M,\iota)}$ wie in Definition 3.1.4.2. Zeigen Sie: Ist M kommutativ, dann auch $Q_{(M,\iota)}$. ◄ **UE 142**

Satz 3.1.4.8. *Sei M ein kommutatives Monoid mit Einselement $1 \in M$ und $K \leq M$ ein kürzbares Untermonoid. Dann wird auf dem direkten Produkt $S := M \times K$ durch*

$$(m_1, k_1) \sim (m_2, k_2) :\Leftrightarrow m_1 k_2 = m_2 k_1, \quad m_1, m_2 \in M,\ k_1, k_2 \in K,$$

eine Kongruenzrelation definiert. Die Abbildung $\iota\colon M \to Q := S/_\sim$, $m \mapsto [(m, 1)]_\sim$, ist eine isomorphe Einbettung des Monoids M in Q. Das Faktormonoid $Q := S/_\sim$ bildet zusammen mit ι ein Quotientenmonoid von Q bezüglich K.

Beweis. Die Relation $\sim$ ist auf S klarerweise reflexiv und symmetrisch. Die Transitivität ergibt sich so: $(m_1, k_1) \sim (m_2, k_2)$ und $(m_2, k_2) \sim (m_3, k_3)$ bedeutet $m_1 k_2 = m_2 k_1$ und $m_2 k_3 = m_3 k_2$. Daraus folgt (u.a. wegen der Kommutativität) $m_1 k_2 k_3 = m_2 k_1 k_3 =$

$m_3k_1k_2$. Die Kürzbarkeit von k_2 liefert $m_1k_3 = m_3k_1$ also $(m_1, k_1) \sim (m_3, k_3)$. Also ist $\sim$ transitiv und somit eine Äquivalenzrelation.
Um die Verträglichkeit von $\sim$ mit der binären Operation nachzuweisen, seien $(m_1, k_1) \sim (m_1', k_1')$ (also $m_1k_1' = m_1'k_1$) und $(m_2, k_2) \sim (m_2', k_2')$ (also $m_2k_2' = m_2'k_2$). Zu zeigen ist $(m_1m_2, k_1k_2) \sim (m_1'm_2', k_1'k_2')$. Das folgt unter abermaliger Verwendung der Kommutativität tatsächlich aus $m_1m_2k_1'k_2' = (m_1k_1')(m_2k_2') = (m_1'k_1)(m_2'k_2) = m_1'm_2'k_1k_2$. Somit ist $\sim$ eine Kongruenzrelation.
Also dürfen wir das Faktormonoid $Q := S/_\sim$ bilden und darin gemäß der Rechenregel $[(m_1, k_1)]_\sim \cdot [(m_2, k_2)]_\sim = [(m_1m_2, k_1k_2)]_\sim$ rechnen. Für $k_1 = k_2 = 1$ folgt daraus speziell die Homomorphiebedingung

$$\iota(m_1m_2) = [(m_1m_2, 1)]_\sim = [(m_1, 1)]_\sim \cdot [(m_2, 1)]_\sim = \iota(m_1) \cdot \iota(m_2).$$

Klarerweise bildet ι das Einselement $1 \in M$ auf das Einselement $[(1, 1)]_\sim \in Q$ ab.
Die Injektivität von ι ergibt sich so: Aus $\iota(m_1) = \iota(m_2)$ folgt $[(m_1, 1)]_\sim = [(m_2, 1)]_\sim$, d. h. $(m_1, 1) \sim (m_2, 1)$ oder $m_1 = m_1 1 = 1m_2 = m_2$. Damit ist gezeigt, dass $\iota : M \to Q$ eine isomorphe Einbettung ist.
Für $k \in K$ gilt

$$\iota(k) \cdot [(1, k)]_\sim = [(k, 1)] \cdot [(1, k)]_\sim = [(k, k)]_\sim = [(1, 1)]_\sim.$$

Also hat $\iota(k)$ in Q das Inverse $[(1, k)]_\sim$. Somit ist (Q, ι) ein Quotientenmonoid iwS, also ein Objekt der Kategorie $\mathcal{C}(M, K)$ aus Definition 3.1.4.6.
Zu zeigen bleibt, dass (Q, ι) in $\mathcal{C}(M, K)$ sogar ein initiales Objekt ist. Sei dazu (Q', ι') irgendein anderes Quotientenmonoid iwS. Wir müssen zeigen, dass es eine eindeutige isomorphe Einbettung $\psi : Q \to Q'$ gibt mit $\iota' = \psi \circ \iota$.
Ein beliebiges Element in Q ist von der Gestalt $[(m, k)]_\sim$ mit $m \in M$ und $k \in K$. Nach Definition von $\mathcal{C}(M, K)$ hat $\iota'(k)$ ein Inverses in Q'. Wir setzen daher

$$\psi : [(m, k)]_\sim \mapsto \iota'(m)\iota'(k)^{-1}.$$

Der Beweis des Satzes ist erbracht, wenn wir Wohldefiniertheit, Injektivität, Homomorphieeigenschaft und Eindeutigkeit von ψ zeigen.
Zur Wohldefiniertheit von ψ: Zu zeigen ist, dass aus $[(m_1, k_1)]_\sim = [(m_2, k_2)]_\sim$ stets $\iota'(m_1)\iota'(k_1)^{-1} = \iota'(m_2)\iota'(k_2)^{-1}$ folgt. Tatsächlich bedeutet $[(m_1, k_1)]_\sim = [(m_2, k_2)]_\sim$ nichts anderes als $m_1k_2 = m_2k_1$. Wir wenden ι' an und erhalten

$$\iota'(m_1)\iota'(k_2) = \iota'(m_1k_2) = \iota'(m_2k_1) = \iota'(m_2)\iota'(k_1).$$

Wir müssen also durch $\iota'(k_1)$ und $\iota'(k_2)$ kürzen – dazu beachten wir, dass die Elemente $\iota'(m_1), \iota'(m_2), \iota'(k_1)^{-1}, \iota'(k_2)^{-1} \in M_{(Q', \iota')}$ nach Übungsaufgabe 3.1.4.7 miteinander kommutieren, und multiplizieren obige Gleichung von links mit $\iota'(k_1)^{-1}$ und von rechts mit $\iota'(k_2)^{-1}$, um

$$\begin{aligned}\iota'(m_1)\iota'(k_1)^{-1} = \iota'(k_1)^{-1}\iota'(m_1) &= \iota'(k_1)^{-1}\iota'(m_2)\iota'(k_1)\iota'(k_2)^{-1} \\ &= \iota'(m_2)\iota'(k_1)^{-1}\iota'(k_1)\iota'(k_2)^{-1} = \iota'(m_2)\iota'(k_2)^{-1}\end{aligned}$$

zu erhalten.
Zur Injektivität von ψ: Zu zeigen ist, dass aus $\iota'(m_1)\iota'(k_1)^{-1} = \iota'(m_2)\iota'(k_2)^{-1}$ auch umgekehrt stets $[(m_1,k_1)]_\sim = [(m_2,k_2)]_\sim$ folgt. Ähnlich wie oben multiplizieren wir $\iota'(m_1)\iota'(k_1)^{-1} = \iota'(m_2)\iota'(k_2)^{-1}$ von links mit $\iota'(k_1)$ sowie von rechts mit $\iota'(k_2)$ und verwenden, dass die Elemente $\iota'(m_1), \iota'(m_2), \iota'(k_1)^{-1}, \iota'(k_2)^{-1} \in M_{(Q',\iota')}$ miteinander kommutieren, um

$$\iota'(m_1k_2) = \iota'(m_1)\iota'(k_2) = \iota'(m_2)\iota'(k_1) = \iota'(m_2k_1)$$

zu erhalten. Da ι' eine isomorphe Einbettung ist, folgt $m_1k_2 = m_2k_1$, also tatsächlich $[(m_1,k_1)]_\sim = [(m_2,k_2)]_\sim$.
Zur Homomorphieeigenschaft von ψ: Mit Hilfe der Wohldefiniertheit von ψ und der Homomorphieeigenschaft von ι' erhalten wir

$$\begin{aligned}\psi([(m_1,k_1)]_\sim\cdot[(m_2,k_2)]_\sim) = \psi([(m_1m_2,k_1k_2]_\sim) = \iota'(m_1m_2)\iota'(k_1k_2)^{-1} = \\ = \iota'(m_1m_2)\Big(\iota'(k_1)\iota'(k_2)\Big)^{-1} = \iota'(m_1m_2)\iota'(k_2)^{-1}\iota'(k_1)^{-1} \\ = \iota'(m_1)\iota'(m_2)\iota'(k_1)^{-1}\iota'(k_2)^{-1} = \iota'(m_1)\iota'(k_1)^{-1}\iota'(m_2)\iota'(k_2)^{-1} \\ = \psi([(m_1,k_1)]_\sim)\cdot\psi([(m_2,k_2)]_\sim).\end{aligned}$$

Die hier verwendeten Kommutativitäten ergeben sich wieder aus Übungsaufgabe 3.1.4.7.
Abschließend zur Eindeutigkeit von ψ: Jedes Element $q \in Q$ ist von der Gestalt $q = [(m,k)]_\sim = m_Qk_Q^{-1}$ mit $m_Q := \iota(m)$ und $k_Q := \iota(k)$. Wenn $\iota' = \tilde{\psi}\circ\iota$ gilt, bedeutet das zunächst, dass $\tilde{\psi}(m_Q) = \tilde{\psi}(\iota(m)) = \iota'(m) = \psi(\iota(m)) = \psi(m_Q)$ gilt; analog auch $\tilde{\psi}(k_Q) = \psi(k_Q)$. Wir erhalten unter Verwendung von $\tilde{\psi}(k_Q^{-1}) = \tilde{\psi}(k_Q)^{-1}$ sowie der analogen Tatsache für ψ (siehe Proposition 3.1.1.5)

$$\tilde{\psi}(q) = \tilde{\psi}(m_Qk_Q^{-1}) = \tilde{\psi}(m_Q)\tilde{\psi}(k_Q)^{-1} = \psi(m_Q)\psi(k_Q)^{-1} = \psi(m_Qk_Q^{-1}) = \psi(q),$$

also die Eindeutigkeit von ψ bei vorgegebenem ι'. □

Die Eindeutigkeit initialer Objekte modulo Äquivalenz nehmen wir als Rechtfertigung dafür, einfach von *dem* Quotientenmonoid zu sprechen. Seine Elemente schreibt man oft als Brüche $\frac{m}{k} = mk^{-1} = [(m,k)]_\sim$ mit der Notation aus Satz 3.1.4.8.

3.2. Gruppen

Eine der wichtigsten, wenn nicht die wichtigste Klasse algebraischer Strukturen ist die der Gruppen. In diesem Abschnitt beschäftigen wir uns zunächst mit den gruppentheoretischen Spezifika der in Abschnitt 2.2 in allgemeinem Rahmen behandelten Konzepte algebraischer Strukturanalyse: Unterstrukturen in 3.2.1, Faktorisierung in 3.2.2 und direkte Produkte in 3.2.3. Sodann untersuchen wir einige wichtige und in gewisser Hinsicht sehr repräsentative, konkrete Beispiele: Zyklische Gruppen (3.2.4), Permutationsgruppen (3.2.5) und Gruppen, die unterschiedlichen Strukturtheorien entstammen (3.2.6).

3.2.1. Nebenklassenzerlegung

Inhalt in Kurzfassung: Jede Untergruppe induziert zwei Partitionen der Gruppe, nämlich in Links- und in Rechtsnebenklassen. Jeweils eine Links- bzw. Rechtsnebenklasse ist dabei die Untergruppe selbst. Alle Nebenklassen haben die gleiche Mächtigkeit wie die Untergruppe, und es gibt gleich viele Links- wie Rechtsnebenklassen. Deren Anzahl nennt man den Index der Untergruppe in der Gruppe. Offensichtlich folgt: Die Ordnung (= Kardinalität) der Gruppe ist das Produkt aus der Ordnung der Untergruppe und dem Index. Daraus ergibt sich für endliche Gruppen der Satz von Lagrange: Die Ordnung einer Untergruppe ist Teiler der Ordnung der Gruppe.

Wir beginnen mit der Ordnung einer Gruppe und ihrer Elemente sowie daran anknüpfenden Begriffen.

Definition 3.2.1.1. Sei G eine Gruppe. Dann nennt man die Kardinalität $|G|$ die *Ordnung* von G. Unter der *Ordnung eines Elements* $g \in G$ versteht man die Ordnung $|\langle g\rangle|$ der von g erzeugten Untergruppe. Wir schreiben dafür $\mathrm{ord}(g)$. Offenbar kommen für $\mathrm{ord}(g)$ genau die Kardinalitäten aus $\mathbb{N}^+$ sowie $\aleph_0$ in Frage. Statt $\mathrm{ord}(g) = \aleph_0$ schreibt man vorzugsweise $\mathrm{ord}(g) = \infty$. Ist $\mathrm{ord}(g) < \infty$ endlich, so heißt $g \in G$ ein *Torsionselement*. Gilt sogar $\mathrm{ord}(g) = p^n$ mit $p \in \mathbb{P}$ und $n \in \mathbb{N}$, so heißt g ein *p-Element*. G heißt eine *p-Gruppe*, wenn jedes $g \in G$ ein p-Element ist. G heißt eine *Torsionsgruppe*, wenn jedes $g \in G$ ein Torsionselement ist. G heißt *zyklisch*, wenn es ein $g \in G$ (ein sogenanntes *erzeugendes Element* von G) gibt mit $G = \langle g\rangle$.

Gemäß der allgemeinen Definition 2.2.1.1 von Unteralgebren ist eine Teilmenge $U \subseteq G$ einer Gruppe G genau dann eine Untergruppe, wenn sie abgeschlossen ist bezüglich aller drei Operationen, der binären Gruppenoperation (wenn also aus $a, b \in U$ stets $ab \in U$ folgt), der nullstelligen (wenn also das neutrale Element $1_G \in G$ auch in U liegt) und der unären (wenn also mit jedem $a \in U$ auch das Inverse a^{-1} in U liegt). Ein Spezifikum der Gruppen mit sehr interessanten Konsequenzen besteht darin, dass jede Untergruppe $U \leq G$ in natürlicher Weise Zerlegungen von G in gleich große Teile induziert, von denen einer U selbst ist.

Definition 3.2.1.2. Sei G eine Gruppe und $U \leq G$ eine Untergruppe von G. Für jedes Element $g \in G$ nennen wir

$$gU := \{gu \mid u \in U\}$$

die *Linksnebenklasse* von g nach U (oder auch modulo U, bzgl. U). Analog definieren wir die *Rechtsnebenklasse* $Ug := \{ug \mid u \in U\}$.

Proposition 3.2.1.3 (Nebenklassenzerlegung einer Gruppe nach einer Untergruppe)**.** *Seien G eine Gruppe und $U \leq G$ sowie $g_1, g_2 \in G$. Für die Linksnebenklassen nach U gilt entweder $g_1U = g_2U$ (nämlich genau dann, wenn $g_1^{-1}g_2 \in U$) oder $g_1U \cap g_2U = \emptyset$. Die Linksnebenklassen nach U bilden eine Partition von G. Analoges gilt für die Rechtsnebenklassen, wobei $Ug_1 = Ug_2$ genau dann gilt, wenn $g_1g_2^{-1} \in U$.*

Beweis. Wir zeigen die Aussage für Linksnebenklassen. Die Nebenklassen g_1U und g_2U haben genau dann nichtleeren Schnitt, wenn es $u_1, u_2 \in U$ gibt mit $g_1u_1 = g_2u_2$. Für beliebiges $u_3 \in U$ folgt daraus

$$g_2u_3 = g_2u_2u_2^{-1}u_3 = g_1u_1u_2^{-1}u_3 \in g_1U.$$

Also gilt $g_2U \subseteq g_1U$, aus Symmetriegründen auch $g_1U \subseteq g_2U$, also $g_1U = g_2U$. Somit sind verschiedene Linksnebenklassen zueinander disjunkt. Wegen $g \in gU$ für alle $g \in G$ ist die Vereinigung aller Linksnebenklassen ganz G, womit tatsächlich eine Partition von G vorliegt. Mit der Beobachtung, dass $g_1U = g_2U$ äquivalent ist zu $U = g_1^{-1}g_2U$ und somit $g_1^{-1}g_2 \in U$, ist der Beweis der Aussage für Linksnebenklassen erbracht. Der für Rechtsnebenklassen verläuft völlig analog. □

Satz 3.2.1.4 (Satz von Lagrange)**.** *Sei G eine Gruppe und $U \leq G$.*

(1) *Die durch $x \sim y \;:\Leftrightarrow\; xU = yU \;\Leftrightarrow\; x^{-1}y \in U$ definierte Relation ist eine Äquivalenzrelation auf G. Die Äquivalenzklasse von $g \in G$ ist genau die Linksnebenklasse gU. Die analoge Aussage gilt für Rechtsnebenklassen.*

(2) *Für alle Links- und Rechtsnebenklassen gilt $|gU| = |U| = |Ug|$.*

(3) *Ist G endlich und $U \leq G$, so ist $|U|$ ein Teiler von $|G|$. („Untergruppenordnung teilt Gruppenordnung“)*

(4) *Ist G endlich und $g \in G$, so ist $\operatorname{ord}(g) = |\langle g\rangle|$ ein Teiler von $|G|$. („Elementordnung teilt Gruppenordnung“)*

Beweis.

(1) Proposition 3.2.1.3.

(2) Für jede Linksnebenklasse gU ist die Abbildung $x \mapsto gx$ eine Bijektion zwischen U und gU, weil sie mit $x \mapsto g^{-1}x$ eine Inverse besitzt. Folglich sind alle Linksnebenklassen gU, $g \in G$, zu U und somit auch zueinander gleichmächtig. Analoges gilt für Rechtsnebenklassen, also auch $|g_1U| = |U| = |Ug_2|$ für beliebige $g_1, g_2 \in G$.

(3) Folgt aus den vorigen Punkten: Sei $|U| = n$ und k die Anzahl der Äquivalenzklassen. Wegen (2) haben alle Klassen die Kardinalität n, folglich ist $|G| = nk$.

(4) Man muss nur (3) auf die von g erzeugte Untergruppe $U := \langle g\rangle$ anwenden. □

Ist G nicht abelsch, so müssen Links- und Rechtsnebenklassen nicht übereinstimmen. Man findet aber für endliche wie unendliche Gruppen sehr leicht eine Bijektion:

UE 143 ► **Übungsaufgabe 3.2.1.5.** (F) Sei G eine Gruppe. Zeigen Sie, dass es zu gegebenem $U \leq G$ gleich viele Links- wie Rechtsnebenklassen gibt. (Beachten Sie, dass Ihr Beweis auch im unendlichen Fall gelten soll. Hinweis: Der Kandidat $aU \mapsto Ua$ für eine Bijektion zwischen den Links- und Rechtsnebenklassen funktioniert nicht, da er nicht wohldefiniert ist (wieso?). Wie könnte man diese Definition verbessern?) ◄ **UE 143**

Deshalb gibt es in G gleich viele Links- wie Rechtsnebenklassen von $U \leq G$.

Definition 3.2.1.6. Ist G eine Gruppe und $U \leq G$, so nennt man die Kardinalität der Menge aller Linksnebenklassen oder, äquivalent, aller Rechtsnebenklassen den *Index* von U in G. Man schreibt dafür $[G : U]$.

Für eine endliche Gruppe G lässt sich der Beweis der dritten Aussage von Satz 3.2.1.4 mithilfe des Begriffs des Index zu $|G| = |U| \cdot [G : U]$ umformulieren. Tatsächlich lässt sich das Argument auch auf unendliche Gruppen G übertragen, formal:

Folgerung 3.2.1.7. *Sei G eine Gruppe und $U \leq G$.*
Dann gibt es eine Bijektion $\varphi\colon U \times \{gU \mid g \in G\} \to G$, mit anderen Worten gilt $|G| = |U| \cdot [G : U]$. Wenn G endlich ist, gilt $[G : U] = \frac{|G|}{|U|}$.

UE 144 ▶ **Übungsaufgabe 3.2.1.8.** (V) Zeigen Sie Folgerung 3.2.1.7. ◀ **UE 144**
Hinweis: Wählen Sie ein *vollständiges Vertretersystem* der Nebenklassen, also eine Menge $M \subseteq G$ mit $\{gU \mid g \in G\} = \{gU \mid g \in M\}$ und $gU \neq g'U$ für alle $g, g' \in M$, $g \neq g'$.

Als unmittelbare Konsequenz daraus ergibt sich für eine endliche Gruppe G und Untergruppen $U \leq V \leq G$, dass $[G : U] = [G : V] \cdot [V : U]$. Auch diese Aussage gilt für unendliche Gruppen G:

Satz 3.2.1.9 (Indexsatz)**.** *Für eine Gruppe G und $U \leq V \leq G$ gilt*

$$[G : U] = [G : V] \cdot [V : U].$$

UE 145 ▶ **Übungsaufgabe 3.2.1.10.** (V) Beweisen Sie den Indexsatz 3.2.1.9. ◀ **UE 145**
Hinweis: Finden Sie eine (wohldefinierte!) surjektive Abbildung φ von der Menge der Linksnebenklassen von U in G in die Menge der Linksnebenklassen von V in G, wobei jede Linksnebenklasse von V in G unter φ genau $[V : U]$ Urbilder hat.
Anmerkung: Der im Hinweis angedeutete Beweis lässt sich als Anwendung des Homomorphiesatzes (Satz 2.2.3.17) für Mengen ohne weitere Struktur (d. h. für Algebren vom leeren Typ) deuten.

3.2.2. Faktorgruppen und Normalteiler

Inhalt in Kurzfassung: Im Zusammenhang mit Kongruenzrelationen und Faktoralgebren ist bei Gruppen eine Beobachtung zentral: Kennt man die Kongruenzklasse des neutralen Elementes, so kennt man die gesamte Partition (Kongruenzrelation). Deshalb spielen jene Teilmengen von Gruppen eine besondere Rolle, die als Kongruenzklassen des neutralen Elements auftreten. Sie heißen Normalteiler und sind dadurch charakterisiert, dass es sich bei ihnen um Untergruppen handelt, für die überdies Links- und Rechtsnebenklassenzerlegung übereinstimmen oder, äquivalent, die invariant bezüglich sämtlicher innerer Automorphismen sind. Zahlreiche interessante Sachverhalte lassen sich mit Hilfe von Normalteilern einfach formulieren. Wichtige Beispiele dafür sind die Isomorphiesätze. Der vorliegende Unterabschnitt bringt aber auch einige andere einfache Sachverhalte,

die in der Gruppentheorie immer wieder nützlich sind.

Aufgrund des Homomorphiesatzes hängen in beliebigen universellen Algebren Homomorphismen aufs Engste mit Kongruenzrelationen und somit mit Faktoralgebren zusammen. Für die Klasse der Gruppen treten auch diesbezüglich zahlreiche Besonderheiten auf, mit denen wir uns nun beschäftigen wollen. Erste einfache, aber immer wieder hilfreiche Beobachtungen sind die folgenden.

Proposition 3.2.2.1. *Seien G, H Gruppen, $\sim$ eine Äquivalenzrelation auf G und $f\colon G \to H$ eine Abbildung.*

(1) *Ist f ein Homomorphismus bezüglich der binären Operation auf G, dann sogar schon ein Gruppenhomomorphismus.*

(2) *Ist $\sim$ eine Kongruenzrelation auf G bezüglich der binären Operation, dann sogar bezüglich der Gruppenstruktur.*

Beweis. Die erste Behauptung folgt aus der vierten Aussage in Proposition 3.1.1.5. Die zweite ist eine einfache Übungsaufgabe. □

UE 146 ▶ Übungsaufgabe 3.2.2.2. (V) Beweisen Sie die zweite Behauptung in 3.2.2.1. **◀ UE 146**

Wir beginnen unser Studium von Kongruenzrelationen. Ähnlich wie bei Ringen, für die wir die analoge Frage schon im Einleitungskapitel diskutiert haben (siehe Proposition 1.2.3.4), lässt sich die Situation bei Gruppen besonders einfach beschreiben, nämlich durch die Äquivalenzklasse des neutralen Elements. Zuvor die zugehörige Definition:

Definition 3.2.2.3. Eine Teilmenge N der Gruppe G heißt *Normalteiler* von G, symbolisch $N \lhd G$, wenn eine und damit alle der zueinander äquivalenten Bedingungen im folgenden Satz 3.2.2.4 erfüllt sind.[4]

Satz 3.2.2.4. *Sei $(G, \cdot, 1, {}^{-1})$ eine Gruppe und $N \subseteq G$. Dann sind die folgenden Aussagen äquivalent:*

(1) *Es gibt genau eine Kongruenzrelation $\sim$ auf G mit $N = [1]_\sim$, nämlich $x \sim y :\Leftrightarrow x^{-1}y \in N$.*

(1′) *Es gibt eine Kongruenzrelation $\sim$ auf G mit $N = [1]_\sim$.*

(2) *Es gibt eine Gruppe H und einen Homomorphismus $\varphi\colon G \to H$ mit $N = \varphi^{-1}(\{1_H\})$.*

(2′) *Es gibt eine Gruppe H und einen surjektiven Homomorphismus $\varphi\colon G \to H$ mit $N = \varphi^{-1}(\{1_H\})$.*

(3) *N ist eine Untergruppe von G mit $xNx^{-1} = N$ für alle $x \in G$.*

(3′) *N ist eine Untergruppe von G mit $xNx^{-1} \subseteq N$ für alle $x \in G$.*

(4) *N ist eine Untergruppe von G mit $xN = Nx$ für alle $x \in G$.*

(4′) *N ist eine Untergruppe von G mit $xN \subseteq Nx$ für alle $x \in G$.*

[4] Achtung: die Relation $\lhd$ ist reflexiv, dennoch schreibt man üblicherweise $\lhd$ und nicht $\trianglelefteq$.

Beweis. Wir führen den Beweis der Äquivalenz zyklisch:
(1) $\Rightarrow$ (1′): Trivial.
(1′) $\Rightarrow$ (2): Folgt direkt aus dem Homomorphiesatz 2.2.3.17 ($H = G/_\sim$, $\varphi : x \mapsto [x]_\sim$).
(2) $\Rightarrow$ (2′): Man ersetze H durch die Untergruppe $\varphi(G)$ (Proposition 2.2.1.28).
(2′) $\Rightarrow$ (3′): Das Urbild $N = \varphi^{-1}(\{1_H\})$ der einelementigen Untergruppe von H ist eine Untergruppe von G (Proposition 2.2.1.28). Außerdem gilt für ein beliebiges Element $y = xnx^{-1} \in xNx^{-1}$ mit $n \in N$, also $\varphi(n) = 1_H$, auch

$$\varphi(y) = \varphi(xnx^{-1}) = \varphi(x)\varphi(n)\varphi(x^{-1}) = \varphi(x)\varphi(x)^{-1} = 1_H.$$

Also ist $y \in N$ und somit $xNx^{-1} \subseteq N$.
(3′) $\Rightarrow$ (3): Sei $xNx^{-1} \subseteq N$ für alle $x \in G$. Zu vorgegebenem $x \in G$ verwenden wir die Voraussetzung (3′) speziell für x^{-1} anstelle von x, also $x^{-1}Nx \subseteq N$. Daraus folgt $N = x(x^{-1}Nx)x^{-1} \subseteq xNx^{-1}$. Insgesamt gilt also $xNx^{-1} = N$ für alle $x \in G$.
(3) $\Rightarrow$ (4): Multipliziert man $xNx^{-1} = N$ von rechts mit x, erhält man $xN = Nx$.
(4) $\Rightarrow$ (4′): Trivial.
(4′) $\Rightarrow$ (1): Sei also N eine Untergruppe mit $xN \subseteq Nx$ für alle $x \in G$. Wenn es überhaupt eine Kongruenzrelation $\sim$ mit $N = [1]_\sim$ gibt, dann gilt sicher die Äquivalenz $x \sim y \Leftrightarrow 1 \sim x^{-1}y \Leftrightarrow x^{-1}y \in N$. Es gibt also höchstens eine Kongruenzrelation $\sim$ mit $N = [1]_\sim$, nämlich die durch

$$x \sim y \ :\Leftrightarrow \ x^{-1}y \in N$$

definierte Relation. Wir müssen nur noch überprüfen, dass dies tatsächlich eine Kongruenzrelation ist.
Nach der ersten Aussage in Satz 3.2.1.4 ist $\sim$ eine Äquivalenzrelation.
Zu zeigen ist weiters die Verträglichkeit von $\sim$ mit den Operationen. Wegen Proposition 3.2.2.1 genügt es die Verträglichkeit mit der binären Operation nachzuweisen. Wir gehen von $x \sim x'$ und $y \sim y'$ aus und haben $xy \sim x'y'$ zu zeigen, mit anderen Worten $(xy)^{-1}(x'y') \in N$. Aus $x \sim x'$ folgt $x^{-1}x' \in N$ und daher $y^{-1}x^{-1}x' \in y^{-1}N$. Nach Voraussetzung (mit y^{-1} anstelle von x) ist Letzteres in Ny^{-1} enthalten, also gibt es $\tilde{n} \in N$ mit $y^{-1}x^{-1}x' = \tilde{n}y^{-1}$. Wegen $y^{-1}y' \in N$ und $N \leq G$ erhalten wir daraus $(xy)^{-1}(x'y') = (y^{-1}x^{-1}x')y' = \tilde{n}(y^{-1}y') \in N$, also $xy \sim x'y'$. Daher ist $\sim$ eine Kongruenzrelation. Nach Definition ist schließlich auch

$$[1]_\sim = \{x \mid 1 \sim x\} = \{x \mid 1^{-1}x \in N\} = N.$$

□

Anmerkung 3.2.2.5. Alle vier Paare von Bedingungen aus Satz 3.2.2.4 lassen sich auch sehr ansprechend verbal fassen:
(1) und (1') beschreiben den bijektiven Zusammenhang Kongruenzrelation – Normalteiler, den wir im Anschluss noch ausführlicher diskutieren werden.
(2) und (2') übersetzen diese Korrespondenz im Sinne des Homomorphiesatzes. Die Normalteiler treten also genau als die *Kerne* von Gruppenhomomorphismen, d. h. als homomorphe Urbilder von neutralen Elementen auf. Entsprechend schreibt man für einen Gruppenhomomorphismus $\varphi : G \to H$ oft $\ker \varphi := \varphi^{-1}(\{1_H\}) = \{x \in G \mid \varphi(x) = 1_H\}$.

(Man beachte den Unterschied zum allgemeineren Begriff des Kerns einer Abbildung als induzierte Äquivalenzrelation, d. h. als Menge von Paaren. Die Sprechweise in der Gruppentheorie – ebenso bei Ringen, Moduln etc. – entspricht also der in der Linearen Algebra üblichen.)
(4) und äquivalent (4') besagen, dass die Zerlegungen in Links- bzw. in Rechtsnebenklassen genau dann identisch sind, wenn die Untergruppe ein Normalteiler ist.
(3) und (3') schließlich bedeuten, dass Normalteiler invariant sind unter allen Abbildungen $\pi_x : g \mapsto xgx^{-1}$, $x \in G$, den sogenannten *inneren Automorphismen*, mit denen wir uns in Unterabschnitt 3.2.5 noch intensiver beschäftigen werden.

Hervorzuheben ist der Fall abelscher Gruppen, da dann die Aussage $xN = Nx$ in Bedingung (4) aus Satz 3.2.2.4 automatisch erfüllt ist. Wir erhalten:

Folgerung 3.2.2.6. *Sei $(G, +, 0, -)$ eine abelsche Gruppe und $N \subseteq G$. Dann ist N genau dann ein Normalteiler, wenn N eine Untergruppe ist.*

In der folgenden Übungsaufgabe betrachten wir zwei weitere Charakterisierungen von Normalteilern in allgemeinen Gruppen:

UE 147 ► Übungsaufgabe 3.2.2.7. (F+) Sei $(G, \cdot, 1, ^{-1})$ eine Gruppe, $N \leq G$ eine Untergruppe und $K := \{gN \mid g \in G\}$ die Menge der Linksnebenklassen. Zeigen Sie, dass folgende Aussagen äquivalent sind: **◄ UE 147**

(1) N ist ein Normalteiler.
(2) Für alle $x, y \in G$ gilt: $xy^{-1} \in N \Leftrightarrow y^{-1}x \in N$.
(3) Die Vorschrift $xN * yN := (xy)N$ liefert eine wohldefinierte Abbildung von $K \times K$ nach K.

Bevor Sie etwas beweisen, schreiben Sie mit Hilfe der üblichen logischen Zeichen an, was „wohldefiniert“ hier bedeutet.

Achtung: Bevor Sie irgendwelche Rechenregeln (wie zum Beispiel das Assoziativgesetz), die in einer Gruppe gelten, auch auf andere Strukturen anwenden wollen, müssen Sie erstens behaupten und zweitens überprüfen, dass diese Regeln im neuen Kontext weiterhin gelten. Beispiel: Wir haben xU bereits definiert. Dadurch sind für $x, y \in G$ auch $x(yU)$ und $(xy)U$ definiert. Sind diese beiden Mengen gleich? Warum?)

Zurück zur bijektiven Korrespondenz Φ zwischen den Kongruenzrelationen $\sim$ und den Normalteilern N auf einer Gruppe G, die sich durch (1) aus Satz 3.2.2.4 ergibt. Es ordnet Φ jeder Kongruenzrelation $\sim$ auf G die Klasse $[1]_\sim$ des neutralen Elements 1 in G bezüglich $\sim$ zu, und Φ^{-1} jedem Normalteiler $N \lhd G$ die Äquivalenzrelation $\sim_N$ definiert durch $x \sim_N y :\Leftrightarrow x^{-1}y \in N$. Hieraus ist auch ersichtlich, dass die zu einer Kongruenzrelation $\sim$ auf einer Gruppe G gehörige Partition gerade die (Links- gleich Rechts-) Nebenklassenzerlegung nach dem zu $\sim$ gehörigen Normalteiler ist. Die Bijektion Φ ist offenbar auch mit der mengentheoretischen Inklusion $\subseteq$ verträglich: $\sim_1 \subseteq \sim_2$ genau dann, wenn $\Phi(\sim_1) \subseteq \Phi(\sim_2)$. Weil jeder Kongruenzverband vollständig ist, ergibt sich daraus:

Folgerung 3.2.2.8. *Die Normalteiler einer Gruppe G bilden bezüglich der Inklusion $\subseteq$ als Halbordnungsrelation einen vollständigen Verband, den* Normalteilerverband. *Dieser ist isomorph zum Kongruenzverband* $(\mathrm{Con}(G), \subseteq)$ *von G. Der kanonische Isomorphismus Φ ordnet jeder Kongruenzrelation $\sim$ den Normalteiler $[1]_\sim$ zu.*

Das Infimum im Kongruenz- wie auch im Normalteilerverband ist der mengentheoretische Schnitt. Im Vergleich zum komplizierten Erzeugungsprozess von Untergruppen lässt sich das Supremum von Normalteilern recht handlich als Komplexprodukt beschreiben. Für die folgende Zusammenstellung einiger in diesem Zusammenhang nützlicher Tatsachen sei an die Schreibweise $AB := \{ab \mid a \in A, b \in B\}$ sowie $A_1A_2 \dots A_nA_{n+1} := (A_1A_2 \dots A_n)A_{n+1}$ für Komplexprodukte von Teilmengen $A, B \subseteq G$ von Gruppen erinnert.

Proposition 3.2.2.9. *Seien G eine Gruppe und $A, B \subseteq G$ Teilmengen.*

(1) *Aus $A, B \leq G$ folgt im Allgemeinen nicht $AB \leq G$.*

(2) *Aus $A \lhd G$ und $B \leq G$ folgt $AB = BA \leq G$.*

(3) *Aus $A, B \lhd G$ folgt $AB \lhd G$.*

(4) *Im Normalteilerverband ist das Supremum zweier oder, allgemeiner, endlich vieler Normalteiler $N_1, \dots, N_k \lhd G$ gegeben durch das Komplexprodukt $N_1N_2 \dots N_k$.*

(5) *Sind $N_i \lhd G$, $i \in I \neq \emptyset$, Normalteiler der Gruppe G, so ist ihr Supremum $N := \sup_{i\in I} N_i$ im Verband aller Normalteiler gegeben durch die Vereinigung aller endlichen Komplexprodukte $N_{i_1} \dots N_{i_n}$, $n \in \mathbb{N}$ und $i_1, \dots i_n \in I$.*

UE 148 ► Übungsaufgabe 3.2.2.10. (V,W) Beweisen Sie Proposition 3.2.2.9. **◄ UE 148**

Für die Faktorgruppe $G/_\sim$ nach einer Kongruenzrelation $\sim$ schreiben wir im Folgenden meistens G/N, wenn N und $\sim$ einander in der Korrespondenz Φ aus Folgerung 3.2.2.8 entsprechen, d. h. wenn $N = \Phi(\sim) = [1_G]_\sim$ ist. Die Elemente der Faktorgruppe sind Nebenklassen $gN = Ng = [g]_\sim$, mit denen man nach den Regeln

$$(gN)(hN) = [g]_\sim \cdot [h]_\sim = [gh]_\sim = (gh)N$$
$$(gN)^{-1} = [g]_\sim^{-1} = [g^{-1}]_\sim = g^{-1}N$$

rechnet (siehe auch Übungsaufgabe 3.2.2.7). Neutrales Element in G/N ist $[1_G]_\sim = 1_GN = N1_G = N$ selbst.
Nach dem allgemeinen Homomorphiesatz 2.2.3.17 induziert jeder Gruppenhomomorphismus $f\colon G \to H$ eine Kongruenzrelation $\sim$. Nach obigen Überlegungen ist $\sim$ bereits durch die eine Klasse $N := [1_G]_\sim = f^{-1}(1_H) \lhd G$ eindeutig bestimmt, und zwar über die Nebenklassenzerlegung nach N.
Folgerung 3.2.2.8 zeigt insbesondere, dass es in jeder Gruppe G einen kleinsten und einen größten Normalteiler gibt. Klarerweise sind das $\{1_G\}$ und G, genannt die *trivialen Normalteiler*. Sie entsprechen den trivialen Kongruenzrelationen, der identischen Kongruenzrelation (Diagonale) mit $a \sim b$ nur für $a = b$, und der Allrelation mit $a \sim b$ für

alle $a, b \in G$. Über den Homomorphiesatz gehören dazu im ersten Fall injektive Homomorphismen, im zweiten konstante. Weil die Urbilder eines Elements Nebenklassen nach dem Kern sind, bedeutet das:

Folgerung 3.2.2.11. *Ein Gruppenhomomorphismus $f\colon G \to H$ ist genau dann injektiv, wenn* $\ker f = \{1_G\}$.

Die allgemeine Definition 2.2.3.14 einer einfachen Algebra führt im Fall von Gruppen zu:

Folgerung 3.2.2.12. *Eine Gruppe G ist einfach genau dann, wenn $N = \{1_G\}$ und $N = G$ die einzigen Normalteiler von G sind.*

Achtung, die Relation $\lhd$ ist nicht transitiv (siehe Übungsaufgabe 3.2.5.15).

Die Isomorphiesätze werden für Gruppen üblicherweise mit Normalteilern statt mit Kongruenzrelationen formuliert. Das folgende Lemma hilft bei der Übersetzung.

Lemma 3.2.2.13. *Sei G eine Gruppe, $U \leq G$ und $N \lhd G$ mit zugehöriger Kongruenzrelation $\sim$. Dann ist $[U]_\sim := \bigcup_{u\in U}[u]_\sim = UN = NU$.*
Die Einschränkung von $\sim$ auf U (formal ist das die Schnittmenge von $\sim$ und $U \times U$) ist eine Kongruenz auf U und entspricht dem Normalteiler[5] *$N \cap U \lhd U$.*

Beweis. Wenn $x \in UN$, dann gibt es $u \in U$, $n \in N$ mit $x = un$. Daher ist $u^{-1}x \in N$, also $u \sim x$. Das zeigt $UN \subseteq [U]_\sim$. Ist umgekehrt $x \in [U]_\sim$, so folgt $u \sim x$ mit einem $u \in U$, also $u^{-1}x \in N$, und es gibt ein $n \in N$ mit $u^{-1}x = n$, daher $x = un$. Das zeigt $[U]_\sim \subseteq UN$, insgesamt also $[U]_\sim = UN$. Die Gleichung $UN = NU$ folgt schließlich aus der zweiten Aussage von Proposition 3.2.2.9. Die zweite Aussage ist offensichtlich. □

Folgerung 3.2.2.14 (Isomorphiesätze für Gruppen)**.** *Sei G eine Gruppe.*

(1) *Für $U \leq G$ und $N \lhd G$ ist $NU = UN \leq G$ eine Untergruppe von G, $N \cap U \lhd U$ ein Normalteiler von U, und es gilt die Isomorphie*

$$U/(N \cap U) \cong UN/N.$$

Ein Isomorphismus ist gegeben durch

$$u(N \cap U) \mapsto uN, \quad u \in U.$$

(2) *Für Normalteiler $N_1, N_2 \lhd G$ mit $N_1 \subseteq N_2$ ist auch $N_1 \lhd N_2$ und $N_2/N_1 := \{xN_1 \mid x \in N_2\} \lhd G/N_1$, und es gilt die Isomorphie*

$$(G/N_1)/(N_2/N_1) \cong G/N_2.$$

Ein Isomorphismus ist gegeben durch

$$(gN_1)(N_2/N_1) \mapsto gN_2.$$

[5] Achtung: $N \cap U$ ist ein Normalteiler von U, aber im Allgemeinen ist $N \cap U$ kein Normalteiler von G.

UE 149 ► **Übungsaufgabe 3.2.2.15.** (V,W) Beweisen Sie die Isomorphiesätze 3.2.2.14 für Gruppen unter Verwendung von Satz 2.2.6.3, Satz 2.2.6.7 und Lemma 3.2.2.13. ◄ **UE 149**

Eine Illustration dazu folgt etwas später in 3.2.5, wenn wir mehr interessante Beispiele zur Verfügung haben.

Wir schließen mit einem immer wieder nützlichen Beispiel einer Faktorisierung, das gleichzeitig eine gute Illustration einer recht allgemeinen Vorgangsweise ist. Oft ist es möglich, aus einer algebraischen Struktur gewisse unliebsame Eigenschaften zu eliminieren oder – wie man gerne sagt – *wegzufaktorisieren*. So kann man aus einer beliebigen, im Allgemeinen nicht abelschen Gruppe G durch Faktorisierung nach einem Normalteiler $N \lhd G$ eine abelsche Gruppe G/N machen. Auf triviale Weise ist das mit $N = G$ der Fall, weil die einelementige Gruppe G/G natürlich abelsch ist. Das ist aber nicht sehr befriedigend, weil man möglichst viel von der Struktur von G erhalten möchte und deshalb wenig vergröbernde Faktorisierungen (d. h. mit kleinen Normalteilern N) bevorzugt. Eine etwas feinere Analyse zeigt: Sollen für $a, b \in G$ die Nebenklassen kommutieren, soll also $abN = baN$ gelten, so lässt sich das mit den Regeln für das Rechnen in Faktorgruppen zu $[a, b] := aba^{-1}b^{-1} = ab(ba)^{-1} \in N$ umschreiben und vice versa. Notwendig und hinreichend für die Kommutativität von G/N ist also, dass N sämtliche sogenannte *Kommutatoren* $[a, b]$, $a, b \in G$, und somit den von diesen erzeugten Normalteiler enthält, die sogenannte *Kommutatorgruppe* G' (manchmal auch die *abgeleitete Gruppe* genannt). Die Situation wird durch folgenden Satz beschrieben:

Satz 3.2.2.16. *Sei G eine Gruppe und bezeichne G' die von allen Kommutatoren $[a, b] = aba^{-1}b^{-1}$, $a, b \in G$, erzeugte Untergruppe, $G' := \langle\{[a, b] \mid a, b \in G\}\rangle$. Dann gilt:*

(1) *$G' \lhd G$ ist sogar ein Normalteiler.*

(2) *G/G' (die sogenannte* Abelisierung *von G) ist abelsch.*

(3) *Für einen beliebigen Normalteiler $N \lhd G$ ist G/N genau dann abelsch, wenn $G' \subseteq N$.*

Beweis. Die dritte Aussage geht aus der oben durchgeführten Überlegung hervor. Die zweite Aussage folgt unmittelbar aus der ersten und dritten. Folglich bleibt nur noch die erste zu zeigen. Wegen Anmerkung 3.2.2.5 genügt dafür wiederum der Nachweis, dass G' unter allen inneren Automorphismen $\pi_x : g \mapsto xgx^{-1}$ invariant ist. Der Kommutator $[a, b]$ wird von π_x auf

$$\begin{aligned}\pi_x([a, b]) &= xaba^{-1}b^{-1}x^{-1} = xax^{-1}xbx^{-1}xa^{-1}x^{-1}xb^{-1}x^{-1} \\ &= xax^{-1}xbx^{-1}(xax^{-1})^{-1}(xbx^{-1})^{-1} = [xax^{-1}, xbx^{-1}]\end{aligned}$$

abgebildet, also wieder auf ein Element von G'. Damit ist auch das Erzeugnis G' der Kommutatoren unter inneren Automorphismen invariant. □

In Algebra II (genauer in Unterabschnitt 8.3.2 über auflösbare Gruppen) wird die Konstruktion der Untergruppe G' aus G nochmals aufgegriffen werden. Führt die Iteration

nach endlich vielen Schritten zur einelementigen Gruppe, nennt man G *auflösbar*, siehe Definition 8.3.2.1.
Wir schließen mit einer einfachen, beim Umgang mit konkreten Beispielen von Gruppen aber häufig nützlichen Beobachtung:

Proposition 3.2.2.17. *Jede Untergruppe U einer Gruppe G vom Index $[G : U] = 2$ ist sogar ein Normalteiler von G.*

UE 150 ▶ Übungsaufgabe 3.2.2.18. (V) Beweisen Sie Proposition 3.2.2.17. **◀ UE 150**

3.2.3. Direkte und schwache Produkte von Gruppen

Inhalt in Kurzfassung: Im Gegensatz zum allgemeinen Fall direkter Produkte treten bei Gruppen die einzelnen Faktoren nicht nur als homomorphe Bilder, sondern auch als Unterstrukturen auf. Somit ergibt sich umgekehrt die Frage, ob eine gegebene Gruppe als direktes Produkt gewisser Untergruppen gedeutet werden kann. Die Ergebnisse dieses Unterabschnitts beschäftigen sich mit dieser und ähnlichen Fragen, zunächst für den Fall endlich vieler Faktoren. Anschließend betrachten wir auch die Situation für beliebig viele Faktoren, was uns auf den Begriff des schwachen Produkts führt.

Wie bereits in Unterabschnitt 2.2.2 angeklungen, treten, wenn man die allgemeine Konstruktion direkter Produkte von Algebren auf Gruppen G_i, $i \in I$, spezialisiert, zusätzliche Aspekte auf. Denn neben den *kanonischen Projektionen*

$$\pi_{i_0} \colon \prod_{i\in I} G_i \to G_{i_0}, \quad (g_i)_{i\in I} \mapsto g_{i_0}$$

für alle $i_0 \in I$ gibt es noch eine zweite Familie natürlicher Abbildungen in die umgekehrte Richtung, nämlich, gleichfalls für alle $i_0 \in I$, die *kanonischen Einbettungen*

$$\iota_{i_0} \colon G_{i_0} \to \prod_{i\in I} G_i, \quad g \mapsto (g_i)_{i\in I}$$

mit $g_{i_0} := g$ und $g_i = e_i$ (Einselement in G_i). Somit treten im direkten Produkt $G := \prod_{i\in I} G_i$ die Faktoren G_i auch in natürlicher Weise als Untergruppen auf, nämlich in Form ihrer isomorphen Kopien $U_{i_0} := \iota_{i_0}(G_{i_0}) \leq G$. Bei der Strukturanalyse einer gegebenen Gruppe G liegt es daher nahe, nach Untergruppen zu suchen, die als solche U_{i_0} interpretiert werden können. Die wichtigsten Aspekte treten bereits bei zwei Faktoren auf. Diesen Fall wollen wir sorgfältig studieren, die offensichtlichen Verallgemeinerungen auf endlich viele Faktoren verbleiben als Übungsaufgabe, bevor wir uns mit dem unendlichen Fall beschäftigen.

Definition 3.2.3.1. Die Gruppe G habe zwei Untergruppen $U_1, U_2 \leq G$ derart, dass die Abbildung $\varphi : U_1 \times U_2 \to G$, $(u_1, u_2) \mapsto u_1u_2$, vom direkten Produkt von U_1 und U_2 nach G ein Isomorphismus ist. In diesem Fall nennen wir G das *innere direkte Produkt* seiner Untergruppen U_1 und U_2 und schreiben $G = U_1 \odot U_2$.

Die Projektionen $\pi_i : (u_1, u_2) \mapsto u_i$, $i = 1, 2$ sind Homomorphismen, ebenso wie die Abbildungen $\pi_i \circ \varphi^{-1}$, $i = 1, 2$, deren Kern U_2 bzw. U_1 ist. Also handelt es sich um Normalteiler. Klarerweise müssen U_1 und U_2 wegen der Injektivität von φ trivialen Schnitt $U_1 \cap U_2 = \{e_G\}$ haben. Wegen der Surjektivität von φ schließlich muss $U_1U_2 = G$ gelten. Diese drei notwendigen Bedingungen erweisen sich gemeinsam aber auch als hinreichend. Um das einzusehen, beweisen wir zunächst das folgende Lemma.

Lemma 3.2.3.2. *Sei G eine Gruppe mit neutralem Element e_G und $U, V \lhd G$ Normalteiler von G mit $U \cap V = \{e_G\}$. Dann gilt $uv = vu$ für alle $u \in U$ und $v \in V$.*

Beweis. Die zu beweisende Gleichheit $uv = vu$ gilt genau dann, wenn der Kommutator $k := [u, v] = uvu^{-1}v^{-1}$ von u und v das neutrale Element e_G ist. Das ist tatsächlich der Fall, denn k lässt sich auf zwei Weisen klammern:

$$k = uvu^{-1}v^{-1} = (uvu^{-1})v^{-1} = u(vu^{-1}v^{-1})$$

Wegen $V \lhd G$ ist $uvu^{-1} \in uVu^{-1} = V$, also auch $k = (uvu^{-1})v^{-1} \in V$. Analog zeigt die zweite Klammerung $k \in U$. Also gilt $k \in U \cap V = \{e_G\}$, mit anderen Worten $k = e_G$, was zu zeigen war. □

Proposition 3.2.3.3. *Seien G eine Gruppe mit neutralem Element e_G und $U, V \leq G$ Untergruppen. Genau dann ist $G = U_1 \odot U_2$ das innere direkte Produkt von U und V, wenn folgende drei Bedingungen erfüllt sind:*

(1) $U, V \lhd G$
(2) $U \cap V = \{e_G\}$
(3) $G = UV$

Beweis. Die vorangegangene Diskussion zeigt, dass alle drei Bedingungen notwendig sind. Für den Beweis genügt es daher zu zeigen, dass die Abbildung $\varphi : U \times V \to G$, $(u, v) \mapsto uv$ ein Isomorphismus ist.
Die Surjektivität von φ folgt unmittelbar aus der dritten Bedingung.
Um die Injektivität von φ nachzuprüfen, ist von einer Relation $u_1v_1 = u_2v_2$ mit $u_1, u_2 \in U$ und $v_1, v_2 \in V$ auszugehen. Wir formen um zu $u_2^{-1}u_1 = v_2v_1^{-1}$. Da die linke Seite in U und die rechte in V liegt, müssen wegen der zweiten Bedingung $U \cap V = \{e_G\}$ beide Ausdrücke das neutrale Element darstellen. Die Relation $u_2^{-1}u_1 = e_G = v_2v_1^{-1}$ bedeutet aber nichts anderes als $u_1 = u_2$ und $v_1 = v_2$, was zu zeigen war.
Die Homomorphiebedingung folgt aus

$$\varphi((u_1, v_1)(u_2, v_2)) = \varphi(u_1u_2, v_1v_2) = u_1u_2v_1v_2 \overset{(*)}{=} u_1v_1u_2v_2 = \varphi(u_1, v_1)\varphi(u_2, v_2),$$

wobei wir in $(*)$ die Gleichung $u_2v_1 = v_1u_2$ für $u_2 \in U$ und $v_1 \in V$ verwenden, was wegen Lemma 3.2.3.2 erlaubt ist. □

Ein rekapitulierender Blick auf den Beweis von Proposition 3.2.3.3 zeigt sehr deutlich die Rolle der drei Bedingungen in Hinblick auf die Zerlegung $g = uv$ eines Elementes $g \in G$ in zwei Faktoren $u \in U$ und $v \in V$: (3) garantiert, dass so eine Zerlegung möglich

ist, (2) die Eindeutigkeit derselben und (1) zusammen mit (2) die Verträglichkeit der Zerlegung mit der Gruppenoperation.

UE 151 ► **Übungsaufgabe 3.2.3.4.** (F) Die Gruppe $G = U \odot V$ sei das innere direkte Produkt der Untergruppen U, V. Man zeige mit Hilfe des Homomorphiesatzes, dass $G/U \cong V$ und $G/V \cong U$. ◄ **UE 151**

Die Verallgemeinerung von zwei auf endlich viele Faktoren liegt auf der Hand:

Definition 3.2.3.5. Sei G eine Gruppe mit Untergruppen $U_1, \ldots, U_n \leq G$. Dann heißt G *inneres direktes Produkt* von $U_1, \ldots, U_n$, wenn die Abbildung

$$\varphi_{U_1,\ldots,U_n} = \varphi : \begin{cases} U_1 \times \cdots \times U_n & \to G \\ (u_1, \ldots, u_n) & \mapsto u_1 \cdots u_n \end{cases}$$

ein Isomorphismus zwischen dem direkten Produkt $\prod_{i=1}^n U_i = U_1 \times \cdots \times U_n$ der Gruppen U_i einerseits und G andererseits ist. In diesem Fall schreibt man oft auch $G = U_1 \odot \ldots \odot U_n$.

Will man direkte Produkte von Gruppen im Sinne von Definition 2.2.2.3 von inneren direkten Produkten im Sinne von Definition 3.2.3.5 unterscheiden, so spricht man bei ersteren auch von *äußeren* direkten Produkten. Offenbar gilt:

Proposition 3.2.3.6. *Das äußere direkte Produkt $G := \prod_{i=1}^n G_i$ endlich vieler Gruppen G_i ist das innere direkte Produkt der Untergruppen $U_i := \iota_i(G_i)$ mit den kanonischen Einbettungen ι_i.*

UE 152 ► **Übungsaufgabe 3.2.3.7.** (V) Zeigen Sie Proposition 3.2.3.6. ◄ **UE 152**

Der folgende Satz ist die natürliche Verallgemeinerung von Proposition 3.2.3.3 und liefert einige nützliche Kriterien zur Überprüfung, ob eine Gruppe G ein direktes Produkt von Untergruppen ist.

Satz 3.2.3.8. *Seien G eine Gruppe und $U_1, \ldots, U_n \leq G$ Untergruppen. Wir betrachten folgende Bedingungen:*

(A) Die Abbildung φ aus Definition 3.2.3.5 ist surjektiv.

(B) Für alle $i \neq j$ und alle $x \in U_i$, $y \in U_j$ gilt $xy = yx$.

(B') $U_i \lhd G$ für alle $i = 1, \ldots, n$.

(C) Für $i = 1, \ldots, n$ sei V_i das Komplexprodukt aller U_j mit Ausnahme von U_i, also: $V_1 := U_2 \cdots U_n$, $V_2 := U_1 U_3 \cdots U_n$, etc. Dann ist $U_i \cap V_i = \{e_G\}$ für $i = 1, \ldots, n$.

(C') Für $i = 1, \ldots, n-1$ gilt $(U_1 \cdots U_i) \cap U_{i+1} = \{e_G\}$.

Dann sind folgende Aussagen äquivalent:

(1) $G = U_1 \odot \cdots \odot U_n$ *ist das innere direkte Produkt von* $U_1, \ldots, U_n$.

(2) Es gelten die Bedingungen (A), (B) und (C).

(3) Es gelten die Bedingungen (A), (B) und (C').

(4) Es gelten die Bedingungen (A), (B') und (C).

(5) Es gelten die Bedingungen (A), (B') und (C').

Der Beweis ergibt sich aus der folgenden Übungsaufgabe.

UE 153 ▶ **Übungsaufgabe 3.2.3.9.** (V,W) Beweisen Sie Satz 3.2.3.8. (Hinweis: Verwenden Sie für $n = 2$ Proposition 3.2.3.3 und gehen Sie dann mittels Induktion nach n vor.) ◀ **UE 153**

Wir wollen uns nun dem allgemeinen Fall eines direkten Produkts $G := \prod_{i\in I} G_i$ von Gruppen zuwenden, die mit einer beliebigen Indexmenge indiziert sind. Betrachten wir die Gruppe G „von innen“, so entspricht dem eine unendliche Familie $(U_i \mid i \in I)$ von Untergruppen, nämlich $U_{i_0} = \iota_{i_0}(G_{i_0})$ für die kanonischen Einbettungen $\iota_{i_0} : G_{i_0} \to \prod_{i\in I} G_i$. Der Versuch, Definition 3.2.3.5 unmittelbar zu verallgemeinern, indem man eine Abbildung

$$\varphi : \prod_{i\in I} U_i \to G$$

definiert und die Isomorphismuseigenschaft fordert, schlägt fehl: Wir müssten ein Tupel $(u_i)_{i\in I}$ so nach G abbilden, dass der endliche Fall umfasst wird. Dies würde auf das unendliche Produkt $\prod_{i\in I} u_i$ von Elementen hinauslaufen, das aber nicht definiert ist[6]. Ein weiteres Indiz dafür, dass das volle direkte Produkt zu groß sein kann, liefert die Beobachtung, dass – anders als im endlichen Fall – alle isomorphen Kopien $\iota_{i_0}(G_{i_0})$ zusammen das direkte Produkt nicht erzeugen: Mit (endlichen!) Produkten von Elementen dieser Kopien erhält man nämlich nur Elemente $(g_i)_{i\in I} \in \prod_{i\in I} G_i$, die nur an endlich vielen Stellen einen vom neutralen Element verschiedenen Eintrag haben. Beide Tatsachen zusammen geben Anlass für die folgende Definition:

Definition 3.2.3.10. Seien G_i, $i \in I$, Gruppen mit Einselementen $e_i \in G_i$. Die Untergruppe (siehe Übungsaufgabe 3.2.3.11)

$$\prod_{i\in I}^{w} G_i := \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i \;\middle|\; g_i \neq e_i \text{ nur für endlich viele } i \in I \right\} \leq \prod_{i\in I} G_i$$

des direkten Produkts $\prod_{i\in I} G_i$ heißt *schwaches Produkt* der G_i („w“ steht für englisch „weak“). Wenn I endlich ist, dann stimmen das schwache und das direkte Produkt überein.
Ist $g = (g_i)_{i\in I}$, so heißt die Menge $\mathrm{supp}(g) := \{i \in I \mid g_i \neq e_i\}$ der *Träger*[7] von g.

[6] Man beachte, dass wir im Allgemeinen keine Topologie auf G zur Verfügung haben, sodass auch eine Definition als Grenzwert nicht sinnvoll ist.

[7] englisch: *support*

UE 154 ► **Übungsaufgabe 3.2.3.11.** (F) Zeigen Sie, dass das schwache Produkt $\prod_{i\in I}^{w} G_i$ eine Untergruppe des direkten Produkts $\prod_{i\in I} G_i$ ist. Zeigen Sie außerdem, dass die kanonischen Abbildungen $\iota_{i_0} : G_{i_0} \to \prod_{i\in I} G_i$ sogar in das schwache Produkt abbilden. ◄ **UE 154**

Das schwache Produkt ist tatsächlich die geeignete Definitionsmenge der Abbildung φ in der Verallgemeinerung des inneren direkten Produkts auf beliebige Indexmengen.

Definition 3.2.3.12. Sei G eine Gruppe und seien $U_i \leq G$, $i \in I$, Untergruppen. Dann heißt G *inneres direktes Produkt* der U_i, $i \in I$, wenn die Abbildung

$$\varphi_{(U_i|i\in I)} = \varphi : \begin{cases} \prod_{i\in I}^{w} U_i & \to G \\ (u_i)_{i\in I} & \mapsto \prod_{i\in I} u_i \end{cases}$$

ein Isomorphismus zwischen dem schwachen Produkt $\prod_{i\in I}^{w} U_i$ der Gruppen U_i einerseits und G andererseits ist. In diesem Fall schreiben man auch oft $G = \bigodot_{i\in I} U_i$.

Die Abbildung φ ist wohldefiniert, da für $u = (u_i)_{i\in I} \in \prod_{i\in I}^{w} U_i$ das Produkt $\prod_{i\in I} u_i$ tatsächlich ein endliches Produkt (nämlich über $i \in \operatorname{supp}(u)$) ist.
Analog zum Fall endlich vieler Gruppen (siehe Proposition 3.2.3.6) gilt:

Proposition 3.2.3.13. *Das schwache Produkt $G := \prod_{i\in I}^{w} G_i$ von Gruppen G_i ist das innere direkte Produkt der Untergruppen $U_i := \iota_i(G_i)$ mit den kanonischen Einbettungen ι_i.*

Um eine Satz 3.2.3.8 verallgemeinernde Charakterisierung zu zeigen, führen wir die allgemeine Situation mit dem folgenden Lemma auf den endlichen Fall zurück.

Lemma 3.2.3.14. *Sei G eine Gruppe und seien $U_i \leq G$, $i \in I$, Untergruppen. Dann sind die folgenden Aussagen äquivalent:*

(1) *$G = \bigodot_{i\in I} U_i$ ist das innere direkte Produkt der U_i, $i \in I$.*

(2) *(a) Die Abbildung φ aus Definition 3.2.3.12 ist surjektiv UND*

(b) Für alle endlichen Teilmengen $F = \{i_1, \ldots, i_n\} \subseteq I$ ist $\langle \bigcup_{j=1}^{n} U_{i_j} \rangle$ das innere direkte Produkt der Gruppen U_{i_j}, $j = 1, \ldots, n$.

Beweis. Sei zunächst (1) angenommen. Aussage (2)(a) gilt trivialerweise, also ist nur (2)(b) zu zeigen. Sei dazu $F = \{i_1, \ldots, i_n\} \subseteq I$ endlich. Die Abbildung $\psi_F : \prod_{j=1}^{n} U_{i_j} \to \prod_{i\in I}^{w} U_i$, $(u_{i_1}, \ldots, u_{i_n}) \mapsto (\tilde{u}_i)_{i\in I}$, wobei $\tilde{u}_{i_j} := u_{i_j}$ für $j = 1, \ldots, n$ und $\tilde{u}_i := e_G$ für $i \in I \setminus F$, ist eine isomorphe Einbettung. Daher ist die Verkettung $\varphi \circ \psi_F$ ein Isomorphismus von $\prod_{j=1}^{n} U_{i_j}$ auf das Bild von $\varphi \circ \psi_F$, das wir mit M bezeichnen. Da die Verkettung $\varphi \circ \psi_F$ nichts anderes als die Abbildung $(u_{i_1}, \ldots, u_{i_n}) \mapsto \prod_{j=1}^{n} u_{i_j}$ ist, also $\varphi \circ \psi_F = \varphi_{U_{i_1},\ldots,U_{i_n}}$, haben wir nur $M = \langle \bigcup_{j=1}^{n} U_{i_j} \rangle$ zu zeigen. Da alle Elemente $\prod_{j=1}^{n} u_{i_j}$ in $\langle \bigcup_{j=1}^{n} U_{i_j} \rangle$ enthalten sind, gilt jedenfalls $M \subseteq \langle \bigcup_{j=1}^{n} U_{i_j} \rangle$. Umgekehrt ist ein beliebiges $U_{i_1} \ni u_{i_1} = \varphi \circ \psi_F(u_{i_1}, e_G, \ldots, e_G)$ in M enthalten; analog gilt $U_{i_j} \subseteq M$ für alle $j = 1, \ldots, n$. Da M als Bild eines Homomorphismus eine Untergruppe ist, folgt $\langle \bigcup_{j=1}^{n} U_{i_j} \rangle \subseteq M$ wie behauptet.

Sei jetzt (2) angenommen. Es ist wegen (2)(a) nur zu zeigen, dass φ injektiv und ein Homomorphismus ist. Angenommen, $\varphi(u) = e_G$ für ein $u = (u_i)_{i\in I} \in \prod_{i\in I}^{w} U_i$, $u \neq (e_G)_{i\in I}$. Setzen wir $F = \{i_1, \ldots, i_n\} := \operatorname{supp}(u)$, so gilt

$$\varphi_{U_{i_1},\ldots,U_{i_n}}(u_{i_1}, \ldots, u_{i_n}) = \varphi \circ \psi_F(u_{i_1}, \ldots, u_{i_n}) = \varphi(u) = e_G,$$

im Widerspruch dazu, dass $\varphi_{U_{i_1},\ldots,U_{i_n}}$ nach (2)(b) injektiv ist. Angenommen, φ ist kein Homomorphismus, also $\varphi(uv) \neq \varphi(u)\varphi(v)$ für $u = (u_i)_{i\in I}, v = (v_i)_{i\in I} \in \prod_{i\in I}^{w} U_i$. Setzen wir $F = \{i_1, \ldots, i_n\} := \operatorname{supp}(u) \cup \operatorname{supp}(v)$, so gilt analog zu oben

$$\begin{aligned}\varphi_{U_{i_1},\ldots,U_{i_n}}(u_{i_1}v_{i_1}, \ldots, u_{i_n}v_{i_n}) = \varphi(uv) &\neq \varphi(u)\varphi(v)\\ &= \varphi_{U_{i_1},\ldots,U_{i_n}}(u_{i_1}, \ldots, u_{i_n})\varphi_{U_{i_1},\ldots,U_{i_n}}(v_{i_1}, \ldots, v_{i_n}),\end{aligned}$$

was erneut der Voraussetzung (2)(b) widerspricht. □

Setzen wir in Bedingung (2)(b) die Charakterisierung aus Satz 3.2.3.8 ein, so erhalten wir die gesuchte allgemeine Charakterisierung:

Satz 3.2.3.15. *Sei G eine Gruppe und seien $U_i \leq G$, $i \in I$, Untergruppen. Wir betrachten folgende Bedingungen:*

(A) Die Abbildung φ aus Definition 3.2.3.12 ist surjektiv.

(B) Für alle $i \neq j$ und alle $x \in U_i$, $y \in U_j$ gilt $xy = yx$.

(B') $U_i \lhd G$ für alle $i \in I$.

(C) Ist $i \in I$ und verschieden von $i_1, \ldots, i_n \in I$ und bezeichnet V das Komplexprodukt aller U_{i_j}, also $V = U_{i_1} \cdots U_{i_n}$, so ist $U_i \cap V = \{e_G\}$.

Dann sind folgende Aussagen äquivalent:

(1) $G = \bigodot_{i\in I} U_i$ ist das innere direkte Produkt der U_i, $i \in I$.

(2) Es gelten die Bedingungen (A), (B) und (C).

(3) Es gelten die Bedingungen (A), (B') und (C).

3.2.4. Zyklische Gruppen

Inhalt in Kurzfassung: Eine Gruppe heißt zyklisch, wenn sie von einem Element erzeugt wird. Die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen ist bis auf Isomorphie die einzige unendliche zyklische Gruppe. Darüber hinaus gibt es zu jeder positiven Zahl bis auf Isomorphie genau eine zyklische Gruppe dieser Ordnung und keine weiteren. Jede zyklische Gruppe lässt sich als homomorphes Bild von $\mathbb{Z}$ realisieren (Restklassengruppen modulo n). Im vorliegenden Unterabschnitt werden diese und einige weitere Strukturaussagen über zyklische Gruppen hergeleitet. Eine Folgerung, die auch in anderem Zusammenhang immer wieder eine Rolle spielen wird, betrifft ganzzahlige Linearkombinationen zweier ganzer Zahlen: Ihre Werte sind genau die Vielfachen des größten gemeinsamen Teilers dieser

Zahlen.

Die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen spielt eine besonders wichtige Rolle. Wir wollen uns deshalb einen Überblick über ihre Untergruppen und homomorphen Bilder machen. Damit erfassen wir die Klasse der zyklischen Gruppen.
Zunächst einige Wiederholungen (z. B. aus Definition 3.2.1.1): Eine Gruppe heißt *zyklisch*, wenn es ein $g \in G$ gibt (ein sogenanntes *erzeugendes Element*), von dem G erzeugt wird, $G = \langle g \rangle$.
Ist G eine Gruppe, so verwenden wir wie bei Halbgruppen die Schreibweise g^n (bei additiver Notation ng) für Potenzen von Gruppenelementen $g \in G$, wobei nun der Exponent n ohne Einschränkungen alle ganzen Zahlen durchlaufen kann.
Bevor wir die Struktur beliebiger zyklischer Gruppen analysieren, betrachten wir, wie oben angekündigt, zunächst die additive Gruppe $\mathbb{Z}$ und verschaffen uns einen Überblick über alle Untergruppen.

Proposition 3.2.4.1. *Für jedes $m \in \mathbb{Z}$ bezeichne $U_m := \langle m \rangle = m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\}$ die von m erzeugte Untergruppe der additiven Gruppe $\mathbb{Z}$.*

(1) *$\mathbb{Z}$ und alle U_m sind zyklisch.*

(2) *Sämtliche Untergruppen von $\mathbb{Z}$ sind selbst zyklisch, also gegeben durch alle U_m, $m \in \mathbb{Z}$.*

(3) *Für $m, n \in \mathbb{Z}$ gilt $U_m \subseteq U_n$ genau dann, wenn $n|m$. (Achtung! Die (absolut) kleinere Zahl erzeugt eine größere Gruppe.)*

(4) *Für $m, n \in \mathbb{Z}$ gilt $U_m = U_n$ genau dann, wenn $n = m$ oder $n = -m$.*

(5) *Die Abbildung $\kappa : \mathbb{N} \to \mathrm{Sub}(\mathbb{Z})$, $m \mapsto U_m = \langle m \rangle$ ist ein Isomorphismus zwischen dem Teilerverband $(\mathbb{N}, |)$ und dem Halbgruppenverband $(\mathrm{Sub}(\mathbb{Z}), \supseteq)$ bezüglich der Obermengenrelation.*

(6) *Für $T \subseteq \mathbb{Z}$ gilt*

$$U := \langle T \rangle = \left\{ \sum_{i=1}^{n} k_i t_i \;\middle|\; n \in \mathbb{N},\ k_1, \ldots, k_n \in \mathbb{Z},\ t_1, \ldots, t_n \in T \right\} = U_{\mathrm{ggT}(T)}.$$

Beweis.

(1) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ und $U_m = \langle m \rangle = \langle -m \rangle$.

(2) Sei $U \leq \mathbb{Z}$.
$U = \{0\}$ (1.Fall) ist wegen $U = \langle 0 \rangle$ zyklisch.
Für $U \neq \{0\}$ (2.Fall) gibt es ein $m \in U \subseteq \mathbb{Z}$ mit $m \neq 0$. Ist $m < 0$, so ist das Inverse $-m > 0$ und auch in U. In jedem Fall gibt es also ein positives $m \in U$. Wir wählen das kleinste solche m und behaupten $U = \langle m \rangle$.

Die Inklusion $\supseteq$ ist klar, weil die von m erzeugte Untergruppe von jeder anderen Untergruppe, die m enthält, umfasst wird. Sei daher umgekehrt $u \in U$ beliebig. Wir müssen $u \in \langle m \rangle = \{km \mid k \in \mathbb{Z}\}$ zeigen. Laut 3.1.3.11 (Division mit Rest) gibt es ein $q \in \mathbb{Z}$ und ein $r \in \{0, 1, \ldots, m-1\}$ mit $u = qm + r$. Wegen $qm \in \langle m \rangle \subseteq U$

liegt auch $r = u - qm \in U$. Weil m das kleinste positive Element in U ist, folgt $r = 0$, also $u = qm \in \langle m \rangle$.

(3) Ist $U_m \subseteq U_n$, so gilt insbesondere $m \in U_n = \{kn \mid k \in \mathbb{Z}\}$. Also gibt es ein $k \in \mathbb{Z}$ mit $m = kn$, was $n|m$ bedeutet. Gilt umgekehrt $n|m$, also $m = kn$ mit einem $k \in \mathbb{Z}$, so liegt mit $m \in U_n$ auch die von m erzeugte Untergruppe U_m in U_n, also $U_m \subseteq U_n$.

(4) Folgt aus (3). Aus $m|n$ und $n|m$ folgt nämlich $|m| \mid |n|$ und $|n| \mid |m|$, daher $|m| = |n|$, also $m = n$ oder $m = -n$. (Umgekehrt folgt aus $m = -n$ natürlich $U_m = U_n$.)

(5) Folgt aus (2), (3) und (4).

(6) Nach Satz 3.1.3.4 ist $(\mathbb{N}, |)$ ein vollständiger Verband mit ggT als Infimum. Via κ aus dem letzten Punkt entspricht dem das Infimum in $(\mathrm{Sub}(\mathbb{Z}), \supseteq)$, also das Supremum in $(\mathrm{Sub}(\mathbb{Z}), \subseteq)$ – das ist nichts anderes als die erzeugte Untergruppe. Offenbar ist die von einer Teilmenge $T \subseteq \mathbb{Z}$ erzeugte Untergruppe die Menge aller Linearkombinationen der Form $\sum_{i=1}^{n} k_i t_i$, welche folglich mit $U_{\mathrm{ggT}(T)}$ übereinstimmt. □

Eine nützliche Folgerung aus Aussage (6) ist die folgende Tatsache, die wir in Satz 5.2.2.7 nochmal in allgemeinerem Kontext beleuchten werden:

Folgerung 3.2.4.2 (Lemma von Bézout)**.** *Sei $T \subseteq \mathbb{Z}$ eine Menge ganzer Zahlen. Dann lässt sich eine ganze Zahl $n \in \mathbb{Z}$ genau dann als Linearkombination von Elementen aus T mit ganzzahligen Koeffizienten darstellen, wenn* $\mathrm{ggT}(T)|n$ *gilt.*

UE 155 ► Übungsaufgabe 3.2.4.3. (V,W) Beweisen Sie Folgerung 3.2.4.2. **◄ UE 155**

In einem zweiten Schritt zeigen wir einige wichtige Strukturaussagen über allgemeine zyklische Gruppen, die bereits den Weg zum Klassifikationssatz 3.2.4.9 weisen.

Proposition 3.2.4.4.

(1) *Eine Gruppe G ist genau dann zyklisch, wenn G ein homomorphes Bild von $\mathbb{Z}$ ist.*

(2) *Jede zyklische Gruppe ist abelsch.*

(3) *Homomorphe Bilder zyklischer Gruppen sind zyklisch.*

(4) *Untergruppen zyklischer Gruppen sind selbst zyklisch.*

Beweis.

(1) Sei G zyklisch mit erzeugendem Element g. Die Abbildung $\varphi : \mathbb{Z} \mapsto G$, $k \mapsto g^k$ ist nach der ersten Aussage aus Proposition 3.1.1.10 ein Gruppenhomomorphismus, der wegen $G = \{g^n \mid n \in \mathbb{Z}\}$ surjektiv ist.

Ist umgekehrt $G = \varphi(\mathbb{Z})$ mit irgendeinem Homomorphismus $\varphi : \mathbb{Z} \mapsto G$, so ist $G = \langle \varphi(1) \rangle$ zyklisch.

(2) $\mathbb{Z}$ ist abelsch, wegen Folgerung 2.2.3.23 folglich auch alle homomorphen Bilder von $\mathbb{Z}$, womit die Behauptung aus (1) folgt.

(3) Sei $G = \varphi(C)$ das Bild der zyklischen Gruppe C unter dem Homomorphismus φ. Nach (1) ist $C = \psi(\mathbb{Z})$ homomorphes Bild von $\mathbb{Z}$ unter einem Homomorphismus ψ. Also ist $G = \varphi \circ \psi(\mathbb{Z})$ homomorphes Bild von $\mathbb{Z}$ unter dem Homomorphismus $\varphi \circ \psi$, wieder nach 1. daher zyklisch.

(4) Sei G eine zyklische Gruppe und $H \leq G$. Nach (1) gibt es einen surjektiven Homomorphismus $\varphi\colon \mathbb{Z} \to G$. Das Urbild $U := \varphi^{-1}(H)$ von $U \leq G$ ist nach Proposition 2.2.1.28 eine Untergruppe von $\mathbb{Z}$, laut der zweiten Aussage in Proposition 3.2.4.1 also zyklisch. Nach (1) ist das homomorphe Bild $H = \varphi(U)$ von U ebenfalls zyklisch. □

UE 156 ▶ **Übungsaufgabe 3.2.4.5.** (F) Man zeige: Ist $(G, \cdot, e, ^{-1})$ eine Gruppe, dann ist jede endliche nichtleere Unterhalbgruppe H von $(G, \cdot)$ eine Untergruppe. (Hinweis: Betrachten Sie für jedes $x \in H$ die von x erzeugte Halbgruppe $\langle x \rangle_{\text{Halbgruppe}}$, und zeigen Sie, dass diese das Element e enthält.) ◀ **UE 156**

Wenn wir die Struktur beliebiger zyklischer Gruppen verstehen wollen, genügt es nach der ersten Aussage von Proposition 3.2.4.4, die homomorphen Bilder von $\mathbb{Z}$ zu betrachten. Mithilfe des Homomorphiesatzes ist das (bis auf Isomorphie) gleichbedeutend damit, die Faktorgruppen von $\mathbb{Z}$ nach Normalteilern zu studieren. Das soll nun geschehen.

Definition 3.2.4.6. Für $m \in \mathbb{Z}$ betrachten wir wieder $U_m = m\mathbb{Z} := \{mk \mid k \in \mathbb{Z}\}$. Die Äquivalenzrelation zur zugehörigen Nebenklassenzerlegung bezeichnen wir mit $\equiv_m$:

$$a \equiv_m b \;\Leftrightarrow\; a - b \in m\mathbb{Z} \;\Leftrightarrow\; m|(a-b)$$

Statt $a \equiv_m b$ schreibt man oft auch $a \equiv b \pmod m$, in Worten: *a ist kongruent zu b modulo m.*

Insbesondere gilt $a \equiv_0 b$ genau dann, wenn $a = b$. Weiters gilt $a \equiv_1 b$ für alle $a, b \in \mathbb{Z}$.

Anmerkung 3.2.4.7. Mit der ersten in Anmerkung 3.1.3.13 erwähnten Notation gilt

$$a \equiv b \pmod m \quad \Leftrightarrow \quad a \bmod m = b \bmod m,$$

also: a und b sind kongruent modulo m genau dann, wenn sie bei Division durch m den gleichen nichtnegativen Rest lassen.
Man beachte den notationellen Unterschied zwischen

$$a \equiv b \pmod m \quad \text{und} \quad a = (b \bmod m).$$

Zum Beispiel gilt $13 \equiv 8 \pmod 5$ (also: „$13 - 8$ ist ohne Rest durch 5 teilbar“), aber nicht $13 = (8 \bmod 5)$, weil mit $8 \bmod 5$ die Zahl 3 gemeint ist.

Aus Folgerung 3.2.2.6 erkennen wir, dass in der abelschen Gruppe $\mathbb{Z}$ die Normalteiler genau die Untergruppen sind. In Proposition 3.2.4.1 haben wir alle Untergruppen von $G = \mathbb{Z}$ bestimmt – und zwar sind es genau die (paarweise verschiedenen) Gruppen $U_m = m\mathbb{Z} \leq \mathbb{Z}$ mit $m \in \mathbb{N}$. Nach dem Homomorphiesatz sind damit alle homomorphen Bilder von $\mathbb{Z}$ bis auf Isomorphie gegeben durch die folgenden Gruppen:

Definition 3.2.4.8. Sei $m \in \mathbb{N}$. Wir definieren die Faktorgruppe $C_m := \mathbb{Z}/m\mathbb{Z}$ und nennen dies die *Restklassengruppe* modulo m.
(Diese zyklische Gruppe C_m ist zu unterscheiden vom Restklassenring $\mathbb{Z}_m$ auf derselben Trägermenge, mit C_m als additiver Gruppe, den wir erst später betrachten werden.)
Der kanonische Homomorphismus $\kappa_m \colon \mathbb{Z} \to C_m$ ordnet jedem $k \in \mathbb{Z}$ die Klasse

$$k + m\mathbb{Z} = \{\ldots, k-3m, k-2m, k-m, k, k+m, k+2m, k+3m, \ldots\} \in C_m$$

zu, genannt die *Restklasse* von k modulo m. Für gegebenes m bezeichnet man $k + m\mathbb{Z}$ oft auch mit $\overline{k}$.[8]

Wegen Proposition 3.2.4.4 sind die Gruppen C_m, $m \in \mathbb{N}$, bis auf Isomorphie gleichzeitig genau die zyklischen Gruppen.
Offenbar gilt $|C_m| = m$ für $m \in \mathbb{N}^+$. Im Fall $m = 0$ sind die Kongruenzklassen einelementig, der kanonische Homomorphismus daher ein Isomorphismus $C_0 \cong \mathbb{Z}$. Somit unterscheiden sich alle C_m, $m \in \mathbb{N}$, schon hinsichtlich ihrer Kardinalität und können erst recht nicht isomorph sein. Somit haben wir einen ersten, wenn auch noch nicht besonders tiefen Klassifikationssatz bewiesen:

Satz 3.2.4.9. *Sämtliche zyklische Gruppen sind bis auf Isomorphie gegeben durch die Restklassengruppen C_m, $m \in \mathbb{N}$. Dabei ist $C_0 \cong \mathbb{Z}$ die einzige unendliche zyklische Gruppe. Alle Gruppen C_m sind paarweise nichtisomorph.*

Ist G irgendeine Gruppe mit $|G| = p \in \mathbb{P}$ und $g \in G \setminus \{e\}$, so kommt wegen des Satzes 3.2.1.4 von Lagrange als Ordnung $\mathrm{ord}(g)$ nur p in Frage. Die von g erzeugte Untergruppe ist also bereits ganz G. Also:

Proposition 3.2.4.10. *Jede Gruppe G von Primzahlordnung $|G| = p \in \mathbb{P}$ ist zyklisch, also $G \cong C_p$. Jedes $g \in G \setminus \{e\}$ ist ein erzeugendes Element.*

Für den nächsten Satz brauchen wir ein einfaches zahlentheoretisches Lemma:

Lemma 3.2.4.11. *Wir betrachten Teilbarkeit in den natürlichen Zahlen.*

(1) *Für alle $a, b, c \in \mathbb{N} \setminus \{0\}$ gilt: $ab|ac \Leftrightarrow b|c$.*
(2) *Wenn a und c teilerfremd sind ($\mathrm{ggT}(a,c) = 1$), dann gilt $a|bc \Leftrightarrow a|b$.*
(3) *Für alle $a, b, c \in \mathbb{N} \setminus \{0\}$ gilt: $a|bc \Leftrightarrow \frac{a}{\mathrm{ggT}(a,c)}|b$.*

Beweis.

(1) $abx = ac \Leftrightarrow bx = c$ (Kürzungsregel).
(2) Die Implikation $\Leftarrow$ ist klar. Wir zeigen $\Rightarrow$.

    Sei $a|bc$. Wenn p ein beliebiger Primfaktor von a ist, und $a = pa'$, dann muss wegen $\mathrm{ggT}(a,c) = 1$ die Primzahl p ein Faktor von b sein, sagen wir $b = pb'$. Aus $pa'|pb'c$ folgt nun wegen (1) die Beziehung $a'|b'c$. Wenn $a'|b'$, dann folgt $a|b$.

    Mit vollständiger Induktion nach der Anzahl der Primfaktoren (gerechnet mit ihrer Vielfachheit, so hat z. B. 12 die drei Primfaktoren 2,2,3) von a führt die Überlegung im vorigen Absatz zu $a|b$.

[8] Wenn wir etwa $m := 8$ setzen, gilt $3 + 7 \equiv 2 \pmod 8$, gleichbedeutend mit $\overline{3} + \overline{7} = \overline{2}$. Das erste Additionssymbol bezeichnet die Addition von natürlichen Zahlen, das zweite die Addition in C_m.

(3) Sei $t := \mathrm{ggT}(a, c)$, und $a't = a$, $c't = c$. Es gilt nach Punkt (1)

$$a|bc \;\Leftrightarrow\; a't|bc't \;\Leftrightarrow\; a'|bc'$$

Weil a', c' teilerfremd sind, folgt aus Punkt (2) die Äquivalenz zu $a'|b$. □

Wir können eine weitere interessante Aussage herleiten, wenn wir uns vor Augen führen, dass wir die zu einer beliebigen zyklischen Gruppe $G = \langle g\rangle \cong C_m$ gehörige Zahl m auf zwei Arten verstehen können, falls m endlich ist: Einerseits ist $m = |C_m| = |G|$ die Kardinalität von G, somit nach Definition 3.2.1.1 die Ordnung von g. Andererseits haben wir m konstruiert als erzeugendes Element des Kerns von $\varphi : \mathbb{Z} \to G$, $n \mapsto g^n$, woraus wir für $n \in \mathbb{Z}$ die Äquivalenz $g^n = e \;\Leftrightarrow\; m|n$ erhalten. Insbesondere gilt $\mathrm{ord}(g) = \min\{n \in \mathbb{N}^+ \mid g^n = e\}$. Diese Tatsache können wir auch in beliebigen Gruppen G nutzbringend einsetzen, wenn wir sie nämlich für die von g erzeugte Untergruppe von G anwenden. Damit erhalten wir den ersten Punkt des folgenden Resultats über Teilbarkeitsaussagen von Ordnungen:

Proposition 3.2.4.12. *Seien G eine Gruppe und die Ordnungen von $g, h \in G$ endlich. Dann gilt:*

(1) *Für $n \in \mathbb{Z}$ ist $g^n = e$ äquivalent zu $\mathrm{ord}(g)|n$.*
Insbesondere gilt $\mathrm{ord}(g) = \min\{n \in \mathbb{N}^+ \mid g^n = e\}$.

(2) *Für $k \in \mathbb{Z}$ gilt $\mathrm{ord}(g^k) = \frac{\mathrm{ord}(g)}{t}$ mit $t := \mathrm{ggT}(\mathrm{ord}(g), k) > 0$.*

(3) *Aus $gh = hg$ folgt $\mathrm{ord}(gh) | \mathrm{kgV}(\mathrm{ord}(g), \mathrm{ord}(h))$. (Insbesondere gilt das in abelschen Gruppen uneingeschränkt.)*

(4) *Gilt $gh = hg$ und zusätzlich $\langle g\rangle \cap \langle h\rangle = \{e\}$ (äquivalent: ist $\langle g, h\rangle$ ein inneres direktes Produkt von $\langle g\rangle$ und $\langle h\rangle$), dann folgt sogar $\mathrm{ord}(gh) = \mathrm{kgV}(\mathrm{ord}(g), \mathrm{ord}(h))$. Das ist insbesondere dann der Fall, wenn $\mathrm{ord}(g)$ und $\mathrm{ord}(h)$ teilerfremd sind (und dann gilt $\mathrm{ord}(gh) = \mathrm{ord}(g) \cdot \mathrm{ord}(h)$).*

Beweis.

(1) Folgt aus den obigen Bemerkungen.

(2) Nach (1) und wegen $(g^k)^l = g^{kl}$ gilt

$$\mathrm{ord}(g^k)|\ell \;\Leftrightarrow\; (g^k)^\ell = e \;\Leftrightarrow\; \mathrm{ord}(g)|k\ell \;\Leftrightarrow\; \frac{\mathrm{ord}(g)}{t}|\ell$$

wobei die letzte Äquivalenz aus der dritten Aussage von Lemma 3.2.4.11 folgt. Daher gilt $\mathrm{ord}(g^k) = \frac{\mathrm{ord}(g)}{t}$.

(3) Nach (1) müssen wir nur $(gh)^{\mathrm{kgV}(\mathrm{ord}(g),\mathrm{ord}(h))} = e$ nachrechnen. Nach der Voraussetzung $gh = hg$ gilt $(gh)^k = g^k h^k$, und wir erhalten

$$(gh)^{\mathrm{kgV}(\mathrm{ord}(g),\mathrm{ord}(h))} = g^{\mathrm{kgV}(\mathrm{ord}(g),\mathrm{ord}(h))} h^{\mathrm{kgV}(\mathrm{ord}(g),\mathrm{ord}(h))} = e.$$

(4) Wegen (3) genügt es, $\mathrm{ord}(g) | \mathrm{ord}(gh)$ und $\mathrm{ord}(h) | \mathrm{ord}(gh)$ zu zeigen. Dafür reicht es wiederum nach (1), aus $e = (gh)^k$ die Folgerungen $\mathrm{ord}(g)|k$ und $\mathrm{ord}(h)|k$ zu ziehen.

Tatsächlich schließen wir aus $e = (gh)^k = g^k h^k$, dass die Potenzen $h^k = g^{-k}$ übereinstimmen. Nach Voraussetzung ist dies nur möglich, wenn $h^k = g^{-k} = e$ gilt. Wegen (1) liefert dies das Gewünschte.

Seien nun $\mathrm{ord}(g)$ und $\mathrm{ord}(h)$ teilerfremd und sei $x := h^k = g^\ell$. Nach (2) ist die Ordnung von x ein Teiler von sowohl $\mathrm{ord}(g)$ als auch $\mathrm{ord}(h)$, also muss $\mathrm{ord}(x) = 1$ bzw. $x = e$ gelten. □

Anmerkung 3.2.4.13. Einige Autorinnen[9] definieren die Ordnung eines Elements g als $\inf\{n \in \mathbb{N}^+ \mid g^n = e\}$. Nach dem letzten Resultat ist diese Definition zu unserer äquivalent, und zwar auch für unendliche Ordnung, wenn man $\inf \emptyset = \infty$ setzt.

Im abelschen Fall, in dem man sich über die Zusatzvoraussetzung $gh = hg$ keine Gedanken machen muss, werden wir das letzte Resultat in Lemma 3.3.3.1 noch etwas ausbauen. Die Kombination von zyklischen Gruppen mit inneren direkten Produkten und inneren Automorphismen lässt sich zur Strukturanalyse von gewissen Gruppen einsetzen, wie die folgende Übungsaufgabe zeigt:

UE 157 ► Übungsaufgabe 3.2.4.14. (E) Sei G eine Gruppe mit pq Elementen, wobei $q < p$ gilt und p eine Primzahl ist. (Wir setzen nicht voraus, dass G kommutativ ist.) **◄ UE 157**

(1) Sei $U \leq G$ mit $|U| = p$. Zeigen Sie: U ist ein Normalteiler von G. (Hinweis: Sei $x \in G$ beliebig. Welche Möglichkeiten gibt es für die Anzahl der Elemente von $U \cap (xUx^{-1})$? Schließen Sie eine der Möglichkeiten aus, indem Sie in diesem Fall die Elemente von $U(xUx^{-1})$ zählen.)

(2) Wir nehmen ab jetzt an, dass $|G| = 15$ und dass es Untergruppen $U, V \leq G$ mit $|U| = 5$ und $|V| = 3$ gibt[10]. Zeigen Sie: Für jedes $v \in V$ ist die Abbildung $\psi_v : U \to U$, die durch $\psi_v(u) = vuv^{-1}$ definiert ist, ein Automorphismus von U. (Ist $\psi_v(U) \subseteq U$?)

(3) Finden Sie alle Automorphismen der Gruppe C_5, sowie für alle $\alpha \in \mathrm{Aut}(C_5)$ die Ordnung $\mathrm{ord}(\alpha)$ von α in $\mathrm{Aut}(C_5)$. Zeigen Sie, dass die gerade betrachteten Abbildungen ψ_v die Identität auf U sein müssen.
(Hinweis: Jedes $\alpha \in \mathrm{Aut}(C_5)$ ist durch das Bild eines Erzeugers von C_5 eindeutig bestimmt.)

(4) Schließen Sie, dass für alle $v \in V$ auch die analog definierte Abbildung auf G, $\pi_v : G \to G$, $\pi_v(x) = vxv^{-1}$, die Identität ist und dass auch V ein Normalteiler von G ist.

(5) Schließen Sie, dass $G = U \odot V$ gilt. Folgern Sie die Isomorphie $G \cong U \times V \cong C_3 \times C_5$.
Anmerkung: In Übungsaufgabe 3.3.2.13 bzw. als Konsequenz von Lemma 3.3.3.1 werden wir sehen, dass $C_3 \times C_5 \cong C_{15}$ (da 3 und 5 teilerfremd sind). Somit haben Sie mit zwei Vorgriffen bewiesen, dass C_{15} bis auf Isomorphie die einzige Gruppe der Ordnung 15 ist.

[9] Die Fußnote auf Seite 107 ist geeignet zu adaptieren.

[10] Tatsächlich kann man mit den sogenannten *Sylowsätzen* zeigen, dass solche Untergruppen stets existieren; siehe Algebra II, genauer Satz 8.1.4.2

Wir haben in Proposition 3.2.4.1 bereits den Untergruppenverband von $\mathbb{Z}$ analysiert. Mit dem Bisherigen lässt sich auch der Untergruppenverband einer endlichen zyklischen Gruppe beschreiben. Die nächste Aussage gibt ein vollständiges Bild in jedem dieser beiden Fälle.

Satz 3.2.4.15. *Sei $G = \langle g \rangle$ eine zyklische Gruppe.*

(1) *Sei G unendlich. Für den Untergruppenverband sowie Kongruenzverband von G gilt die Isomorphie*

$$(\mathbb{N}, |) \cong (\mathrm{Sub}(G), \supseteq) \cong (\mathrm{Con}(G), \supseteq).$$

Ein Isomorphismus für die erste Beziehung ist gegeben durch

$$\kappa : \mathbb{N} \to \mathrm{Sub}(G), \quad t \mapsto \langle g^t \rangle,$$

für die zweite (wie in jeder abelschen Gruppe) durch

$$\psi : \mathrm{Sub}(G) \to \mathrm{Con}(G), \quad U \mapsto \sim_U,$$

mit $a \sim_U b$ genau dann, wenn $ab^{-1} \in U$.
Dabei ist $\kappa(t) = \langle g^t \rangle$ für $t \in \mathbb{N}$ zyklisch und hat unendlich viele Elemente. Als Untergruppen von G treten also insgesamt abzählbar unendlich viele verschiedene Kopien von $\mathbb{Z}$ auf.

(2) *Sei G endlich und $m := \mathrm{ord}(g) = |G|$. Bezeichnet T die Menge der Teiler von m, so gilt für den Untergruppenverband sowie Kongruenzverband von G die Isomorphie*

$$(T, |) \cong (\mathrm{Sub}(G), \supseteq) \cong (\mathrm{Con}(G), \supseteq).$$

Ein Isomorphismus für die erste Beziehung ist gegeben durch

$$\kappa : T \to \mathrm{Sub}(G), \quad t \mapsto \langle g^t \rangle,$$

für die zweite (wie in jeder abelschen Gruppe) durch

$$\psi : \mathrm{Sub}(G) \to \mathrm{Con}(G), \quad U \mapsto \sim_U,$$

mit $a \sim_U b$ genau dann, wenn $ab^{-1} \in U$.
Es gilt aber auch umgekehrt die Isomorphie

$$(T, |) \cong (\mathrm{Sub}(G), \subseteq) \cong (\mathrm{Con}(G), \subseteq).$$

Ein Isomorphismus für die erste Beziehung ist gegeben durch

$$\lambda : T \to \mathrm{Sub}(G), \quad t \mapsto \kappa\left(\frac{m}{t}\right) = \langle g^{m/t} \rangle,$$

für die zweite wieder durch ψ.
Für $t \in T$ hat die Untergruppe $\lambda(t) = \langle g^{m/t} \rangle$ genau t Elemente. Als Untergruppen von G treten also zyklische Gruppen auf, deren Ordnung m teilt, wobei jeder Teiler von m genau einmal als Gruppenordnung auftritt.

Beweis.

(1) Nach Satz 3.2.4.9 sind G und $\mathbb{Z}$ isomorph über die Abbildung $\varphi : \mathbb{Z} \ni n \mapsto g^n \in G$, sodass sich die Aussage aus der fünften Aussage von Proposition 3.2.4.1 ergibt, wenn wir noch berücksichtigen, dass die Untergruppen U_n aus Proposition 3.2.4.1 abzählbar unendlich viele Elemente haben.

(2) Wir verwenden die Darstellung $G = \varphi(\mathbb{Z})$ als Bild von $\mathbb{Z}$ unter dem Homomorphismus $\varphi : n \mapsto g^n$. Für jede Untergruppe $U \leq G$ gilt $U = \varphi(U')$ mit $U' := \varphi^{-1}(U) \leq \mathbb{Z}$. Nach Aussage (2) von Proposition 3.2.4.1 ist $U' = U_t = t\mathbb{Z}$ für ein $t \in \mathbb{Z}$, wobei wir nach Aussage (4) derselben Proposition $t \in \mathbb{N}$ wählen dürfen. Jedenfalls gilt $\varphi(m) = g^m = e \in U$, also $m \in U_t$ und somit $t|m$, folglich $t \in T$. Außerdem gilt $U = \varphi(U_t) = \langle g^t \rangle$. Umgekehrt ist für jeden nichtnegativen Teiler t von m eine Untergruppe $\varphi(t\mathbb{Z})$ gegeben. Sobald wir gezeigt haben, dass für zwei Teiler t_1, t_2 von m die Relation $\varphi(t_1\mathbb{Z}) \subseteq \varphi(t_2\mathbb{Z})$ genau dann gilt wenn $t_2|t_1$, ist der Beweis abgeschlossen.

Aus $t_2|t_1$ folgt $t_1\mathbb{Z} \subseteq t_2\mathbb{Z}$ und daher auch $\varphi(t_1\mathbb{Z}) \subseteq \varphi(t_2\mathbb{Z})$. Gilt umgekehrt $\varphi(t_1\mathbb{Z}) \subseteq \varphi(t_2\mathbb{Z})$, so haben wir $t_2|t_1$ zu zeigen. Für $t_1 = m$ ist das klar, sodass wir von $t_1 < m$ ausgehen. Nach Annahme gilt $\varphi(t_1) \in \varphi(t_2\mathbb{Z}) = \langle g^{t_2} \rangle$. Die Elemente von $\langle g^{t_2} \rangle$ sind genau $(g^{t_2})^k$ für $k = 0, \ldots, \mathrm{ord}(g^{t_2}) - 1$. Nach Aussage (2) in Proposition 3.2.4.12 gilt $\mathrm{ord}(g^{t_2}) = \frac{\mathrm{ord}(g)}{\mathrm{ggT}(\mathrm{ord}(g), t_2)} = \frac{m}{t_2}$. Insgesamt erhalten wir also $g^{t_1} = \varphi(t_1) = (g^{t_2})^k = g^{t_2 k}$ für ein $k \in \{0, \ldots, \frac{m}{t_2} - 1\}$. Daraus folgt $g^{t_1 - t_2 k} = e$ bzw. $\mathrm{ord}(g)|t_1 - t_2 k$. Wegen $0 < t_1, t_2 k < m = \mathrm{ord}(g)$, somit $|t_1 - t_2 k| < m$, ist das nur für $t_1 - t_2 k = 0$ möglich, was $t_2|t_1$ impliziert.

Für die Behauptung zu den Ordnungen verwenden wir nochmals Aussage (2) in Proposition 3.2.4.12, um $|\langle g^{m/t} \rangle| = \mathrm{ord}(g^{m/t}) = \frac{m}{m/t} = t$ für $t \in T$ zu zeigen.

□

Anmerkung 3.2.4.16.

- A priori sind mit der Notation des letzten Beweises *alle* Bilder $\varphi(t\mathbb{Z})$ für beliebige t (und nicht nur für $t|m$) Untergruppen von G. Allerdings sind diese Untergruppen nicht alle verschieden: Setzen wir beispielsweise $m = 4$, so gilt $\varphi(3\mathbb{Z}) = \langle g^3 \rangle = \{g^3, g^2, g, e\} = \langle g \rangle$. Im zweiten Absatz des Beweises der zweiten Aussage geht es faktisch darum zu beweisen, dass man keine Untergruppe doppelt erhält, sobald man sich auf die Teiler von m einschränkt.
- In der zweiten Aussage des letzten Satzes haben wir $(T, |) \cong (\mathrm{Sub}(G), \subseteq)$ und $(T, |) \cong (\mathrm{Sub}(G), \supseteq)$ gezeigt. Definieren wir $t_1 \,\mathrm{vf}\, t_2 :\Leftrightarrow t_2|t_1$ (in Worten: t_1 ist ein Vielfaches von t_2), so können wir die zweite Isomorphie umformulieren zu $(T, \mathrm{vf}) \cong (\mathrm{Sub}(G), \subseteq)$. Folglich ist $(\mathrm{Sub}(G), \subseteq)$ sowohl zu $(T, |)$ als auch zu (T, vf) isomorph. Das ist kein Wunder, denn $(T, |)$ und (T, vf) sind ihrerseits vermöge der Abbildung $t \mapsto \frac{m}{t}$ isomorph – man beachte, dass wir genau diese Abbildung auch im obigen Satz verwendet haben, um λ aus κ zu definieren.
- Wir betonen explizit die folgende Feinheit in den Überlegungen zur Ordnung der Untergruppen in der zweiten Aussage des letzten Satzes: Wegen der Tatsache, dass

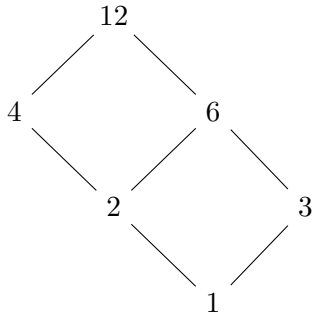
Untergruppen von G zyklisch sind (Proposition 3.2.4.4) kombiniert mit Satz 3.2.4.9 ist ohne weitere Überlegung unmittelbar klar, dass G *bis auf Isomorphie* höchstens eine Untergruppe von einer gewissen Ordnung haben kann. Die zweite Aussage ist aber viel stärker: Tatsächlich gibt es *als Teilmenge* von G höchstens eine einzige Untergruppe von einer gewissen Ordnung (und sogar *genau* eine, wenn man sich auf die Teiler von m beschränkt). Dieses Phänomen ist sehr spezifisch für endliche zyklische Gruppen. Die unendliche zyklische Gruppe $\mathbb{Z}$ hat beispielsweise die zwei abzählbar unendlichen Untergruppen $2\mathbb{Z}$ und $4\mathbb{Z}$, die zwar isomorph (und sogar ineinander enthalten) aber trotzdem verschieden sind. Die endliche nichtzyklische Gruppe $C_2 \times C_2$ wiederum hat die zwei verschiedenen Untergruppen

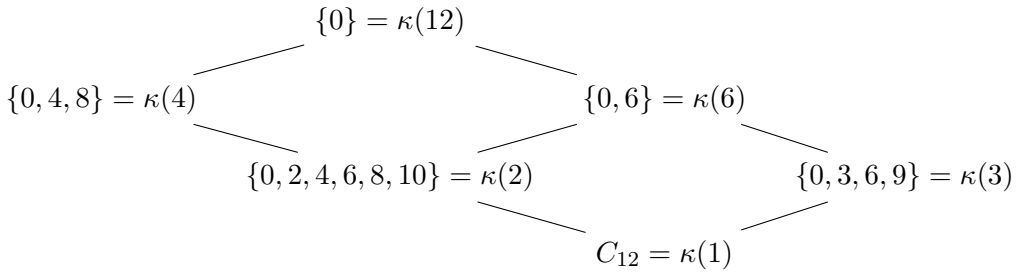
$$\langle(\bar{0},\bar{1})\rangle = \{(\bar{0},\bar{0}),(\bar{0},\bar{1})\} \quad \text{und} \quad \langle(\bar{1},\bar{0})\rangle = \{(\bar{0},\bar{0}),(\bar{1},\bar{0})\}$$

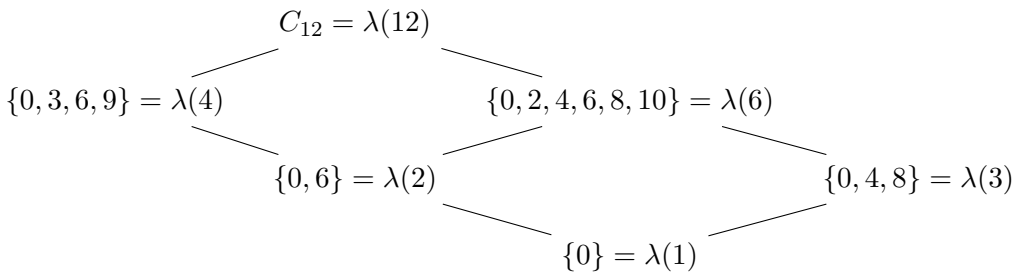
der Ordnung 2. Für endliche abelsche Gruppen kann man die Frage nach der Anzahl von Untergruppen einer gewissen Ordnung mit noch zu entwickelnden Methoden beleuchten; siehe Unterabschnitt 3.3.4, insbesondere Übungsaufgaben 3.3.4.6 und 3.3.4.7.

Beispiel 3.2.4.17. Die Gruppe $C_{12} = \{\bar{0},\bar{1},\bar{2},\bar{3},\ldots,\overline{10},\overline{11}\}$ hat die folgenden Untergruppen:

- $C_{12} = \langle\bar{1}\rangle = \langle\bar{5}\rangle = \langle\bar{7}\rangle = \langle\overline{11}\rangle = \kappa(1) = \lambda(12)$.
- $\{0,2,4,6,8,10\} = \langle\bar{2}\rangle = \langle\overline{10}\rangle = \kappa(2) = \lambda(6)$.
- $\{0,3,6,9\} = \langle\bar{3}\rangle = \langle\bar{9}\rangle = \kappa(3) = \lambda(4)$.
- $\{0,4,8\} = \langle 4\rangle = \langle\bar{8}\rangle = \kappa(4) = \lambda(3)$.
- $\{0,6\} = \langle\bar{6}\rangle = \kappa(6) = \lambda(2)$.
- $\{0\} = \langle\bar{0}\rangle = \langle\overline{12}\rangle = \kappa(12) = \lambda(1)$.
  (Es geht um Teiler von 12, daher $\kappa(12)$ statt $\kappa(0)$!)







Als Folgerung lässt sich eine Formel über eine wichtige zahlentheoretische Funktion gewinnen, die *Eulersche φ-Funktion*. Diese Funktion zählt für $n \in \mathbb{N}$ die sogenannten *primen Restklassen* modulo n. Es gibt mehrere Möglichkeiten, diese zu definieren, die aber alle äquivalent sind.

UE 158 ► Übungsaufgabe 3.2.4.18. (F) Sei $n \in \mathbb{N}^+$. **◄ UE 158**

(a) Zeigen Sie, dass für jedes k die folgenden Aussagen äquivalent sind:

(1) $\mathrm{ggT}(k,n) = 1$
(2) Für alle $\ell \in k + n\mathbb{Z}$ gilt $\mathrm{ggT}(\ell,n) = 1$.
(3) Es gibt ein $\ell \in k + n\mathbb{Z}$ mit $\mathrm{ggT}(\ell,n) = 1$.

(d) Zeigen Sie, dass die folgenden Mengen gleichmächtig sind:

(1) $A := \{k + n\mathbb{Z} \mid k \in \mathbb{Z} \wedge \mathrm{ggT}(n,k) = 1\}$
(2) $B := \{k + n\mathbb{Z} \mid k \in \{0,\ldots,n-1\} \ \wedge \ \mathrm{ggT}(n,k) = 1\}$
(3) $C := \{k \mid k \in \{0,\ldots,n-1\} \ \wedge \ \mathrm{ggT}(n,k) = 1\}$

Definition 3.2.4.19.

- Für $n \in \mathbb{N}^+$ heißt $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ eine *prime Restklasse* modulo n oder auch *teilerfremde Restklasse* modulo n, wenn eine der äquivalenten Bedingungen (1)−(3) aus Übungsaufgabe 3.2.4.18(a) gilt, in Worten:
  - k ist zu n teilfremd.
  - Alle Repräsentanten von $k + n\mathbb{Z}$ sind zu n teilerfremd.
  - Irgendein Repräsentant von $k + n\mathbb{Z}$ ist zu n teilerfremd.
- Für $n \in \mathbb{N}^+$ ist $\varphi(n)$ definiert als die Anzahl der primen Restklassen modulo n, also als die gemeinsame Mächtigkeit der drei Mengen A,B,C aus Übungsaufgabe 3.2.4.18(b):

$$\begin{aligned}\varphi(n) &= |\{k + n\mathbb{Z} \mid k \in \mathbb{Z} \wedge \mathrm{ggT}(n,k) = 1\}| \\ &= |\{k + n\mathbb{Z} \mid k \in \{0,\ldots,n-1\} \ \wedge \ \mathrm{ggT}(n,k) = 1\}| \\ &= |\{k \mid k \in \{0,\ldots,n-1\} \ \wedge \ \mathrm{ggT}(n,k) = 1\}|.\end{aligned}$$

  Die dadurch definierte Funktion φ heißt *Eulersche φ-Funktion*.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	...

Folgerung 3.2.4.20. *Für die Eulersche φ-Funktion und $n \in \mathbb{N}^+$ gilt: $n = \sum_{t|n} \varphi(t)$.*

UE 159 ► **Übungsaufgabe 3.2.4.21.** (V) Folgern Sie 3.2.4.20 aus Satz 3.2.4.15 und Proposition 3.2.4.12. ◄ **UE 159**

Eine explizite Formel für die Eulersche φ-Funktion werden wir mit Hilfe des Chinesischen Restsatzes erhalten, siehe Satz 3.4.7.3.

3.2.5. Permutationsgruppen

Inhalt in Kurzfassung: Die große Bedeutung von Permutationsgruppen für die gesamte Gruppentheorie ergibt sich aus dem Darstellungssatz von Cayley: Jede Gruppe ist isomorph zu einer Untergruppe der symmetrischen Gruppe auf ihrer Trägermenge, also zu einer Gruppe von Permutationen (= Permutationsgruppe). Dies allein rechtfertigt ein etwas ausführlicheres Studium von Permutationsgruppen, es ergeben sich aber darüber hinaus einige weitere reizvolle Aspekte. Einiges aus diesem Unterabschnitt dürfte schon aus dem Kapitel über Determinanten aus der Linearen Algebra bekannt sein, insbesondere die Unterscheidung zwischen geraden und ungeraden Permutationen.

Wir rufen uns den Darstellungssatz 3.1.2.5 von Cayley für Monoide in Erinnerung. Ihm zufolge lässt sich jedes Monoid M vermittels der regulären Darstellung $\iota : a \mapsto f_a$, $f_a(x) := ax$ für $a, x \in M$ isomorph in das symmetrische Monoid auf der Menge M einbetten. Wendet man diese Konstruktion auf eine Gruppe G an, so sind alle f_g, $g \in G$, sogar Permutationen, d. h. Bijektionen von G nach G: Für vorgegebenes $y \in G$ ist $f_a(x) = ax = y$ genau dann, wenn $x = a^{-1}y$ gilt. Also hat y genau ein Urbild unter f_a, was Bijektivität von f_a zeigt. Folglich ist die laut Satz 3.1.2.5 isomorphe Einbettung ι von G als Monoid sogar eine isomorphe (Monoid-)Einbettung der Gruppe G in die symmetrische Gruppe S_G auf der Trägermenge G (die Gruppe aller Permutationen von G bezüglich der Komposition, siehe Definition 2.1.3.6). Nach Proposition 3.1.1.5 liegt tatsächlich eine isomorphe Gruppen-Einbettung vor. Somit gilt der *Darstellungssatz von Cayley für Gruppen*:

Satz 3.2.5.1. *Jede Gruppe G lässt sich vermittels der Einbettung $\iota : a \mapsto f_a$, $f_a(x) := ax$ für $a, x \in G$ isomorph in die symmetrische Gruppe S_G auf der Trägermenge G einbetten.*

Nennt man, wie üblich, jede Untergruppe einer symmetrischen Gruppe S_X (auf irgendeiner Menge X) eine *Permutationsgruppe*, so lautet der Darstellungssatz von Cayley für Gruppen: Jede Gruppe G ist isomorph zu einer Permutationsgruppe auf der Trägermenge von G.
Dieser Sachverhalt legt es nahe, verschiedenste Aspekte der Gruppentheorie insbesondere für Permutationsgruppen zu untersuchen. Als Beispiel wählen wir den Themenkreis

innere Automorphismen (siehe auch schon Anmerkung 3.2.2.5) und *Konjugation*, was speziell bei endlichen Permutationsgruppen zu reizvollen Einsichten führt.

Definition 3.2.5.2. Seien X und Y Mengen, $\phi\colon X \to Y$ bijektiv und $f\colon X \to X$. Dann heißt $f_\phi := \phi \circ f \circ \phi^{-1}\colon Y \to Y$ die bezüglich ϕ *Konjugierte* von f. Die Zuordnung $\Phi : f \mapsto f_\phi$ heißt *Konjugation*.[11]

Proposition 3.2.5.3. *Mit der Notation aus Definition 3.2.5.2 ist die Konjugation Φ ein Isomorphismus zwischen dem symmetrischen Monoid M_X und dem symmetrischen Monoid M_Y. Die Einschränkung von Φ auf die symmetrische Gruppe S_X ist ein Gruppenisomorphismus zwischen der symmetrischen Gruppe S_X und der symmetrischen Gruppe S_Y.*

UE 160 ▶ Übungsaufgabe 3.2.5.4. (V) Beweisen Sie Proposition 3.2.5.3. **◀ UE 160**

Den Darstellungssatz von Cayley im Hinterkopf untersuchen wir nun eine ähnliche Situation für den Fall, dass $X = Y = G$ eine Gruppe ist. Zunächst aber eine Definition, die auch in anderem Zusammenhang von Interesse ist.

Definition 3.2.5.5. Ist G eine Gruppe, so heißt

$$Z(G) := \{g \in G \mid \forall h \in G : gh = hg\} \subseteq G$$

das *Zentrum* von G.

Die folgenden Aussagen knüpfen an Anmerkung 3.2.2.5 an.

Proposition 3.2.5.6. *Sei G eine Gruppe. Für alle $g \in G$ definieren wir $\pi_g\colon G \to G$ $x \mapsto gxg^{-1}$ und betrachten die Abbildung $\Phi : g \mapsto \pi_g$. Dann gilt:*

(1) *Für $g, h \in G$ gilt $\pi_g \circ \pi_h = \pi_{gh}$.*

(2) *Für alle $g \in G$ ist π_g ein Automorphismus (genannt der durch* Konjugation *mit g induzierte* innere Automorphismus *von G).*

Somit ist Φ ein Homomorphismus von G in die Automorphismengruppe $\mathrm{Aut}(G)$.

(3) *Für den Kern von Φ gilt*

$$\ker(\Phi) = \{g \in G \mid \forall h \in G : gh = hg\} = Z(G).$$

Insbesondere ist das Zentrum ein Normalteiler. Außerdem ist $\Phi\colon G \to \mathrm{Aut}(G)$ eine isomorphe Einbettung genau dann, wenn das Einselement $e \in G$ das einzige ist, das mit allen $g \in G$ vertauscht.

(4) *Die inneren Automorphismen bilden einen Normalteiler $\Phi(G) \lhd \mathrm{Aut}(G)$ der Automorphismengruppe von G. (Die Faktorgruppe* $\mathrm{Aut}(G)/\Phi(G)$ *nennt man auch die* äußere Automorphismengruppe *von G.)*

[11] Dieser Begriff von Konjugation und Konjugierten ist von anderen zu unterscheiden, die mit ähnlichen Vokabeln bezeichnet werden. Später werden wir beispielsweise Wurzeln eines irreduziblen Polynoms im Zerfällungskörper kennenlernen, von denen komplex konjugierte Zahlen ein Spezialfall sind.

UE 161 ► Übungsaufgabe 3.2.5.7. (V,W) Beweisen Sie Proposition 3.2.5.6. **◄ UE 161**

Eigenschaft (3) in Satz 3.2.2.4 zeigt:

Folgerung 3.2.5.8. *Eine Untergruppe $N \leq G$ ist genau dann Normalteiler, wenn sie invariant ist unter allen inneren Automorphismen, d. h. wenn $\pi_g(N) = N$ für alle $g \in G$ gilt.*

Interessant ist der Spezialfall, dass G eine symmetrische Gruppe ist. Dabei erweist sich die *Zyklenschreibweise* von Permutationen als sehr nützlich. Zunächst sei daran erinnert, dass wegen Proposition 3.2.5.3 die Struktur der symmetrischen Gruppe S_X auf der Menge X nur von der Kardinalität $|X|$ abhängt. Im endlichen Fall $|X| = n \in \mathbb{N}$ schreiben wir S_n für S_X, wobei wir oBdA meist $X = \{1, 2, \ldots, n\}$ annehmen. Jede Permutation $\pi \in S_n$ lässt sich auf ein beliebiges $a = a_1 \in X$ iteriert anwenden. Weil X endlich ist, muss es irgendwann zu einer Wiederholung kommen, genauer: Es gibt ein minimales $k \in \mathbb{N}$ derart, dass alle $a_1 = \pi^0(a_1), a_2 := \pi^1(a_1), \ldots, a_k := \pi^{k-1}(a_1)$ paarweise verschieden sind, $a_{k+1} := \pi^k(a_1)$ jedoch mit einem a_i mit $1 \leq i \leq n$ übereinstimmt. Weil π injektiv ist, folgt daraus $a_{k+1} = a_1$ (andernfalls hätte a_{k+1} neben a_k noch ein zweites Urbild unter π), also $i = 1$. Lässt π alle anderen Elemente fest, so spricht man von einer *zyklischen Permutation*, einem *k-Zyklus* oder auch von einem Zyklus der Länge k. Diesen Zyklus schreibt man in sogenannter Zyklenschreibweise als $\pi = (a_1 a_2 \ldots a_k)$ an. Ist bereits $X = \{a_1, a_2, \ldots, a_k\}$, so ist $\pi = (a_1 a_2 \ldots a_k)$. Andernfalls gibt jedes $b \in X \setminus \{a_1, a_2, \ldots, a_k\}$ Anlass zu einem weiteren Zyklus $(b_1 b_2 \ldots b_l)$, wobei die b_j nicht unter den a_i vorkommen. Weil X endlich ist, bricht dieser Prozess ab, und man kann π allgemein als Produkt paarweise elementfremder Zyklen schreiben:

$$\pi = (a_{1,1} a_{1,2} \ldots a_{1,k_1})(a_{2,1} a_{2,2} \ldots a_{2,k_2}) \ldots (a_{m,1} a_{m,2} \ldots a_{m,k_m})$$

Ein Zyklus (a) der Länge 1 bedeutet, dass $a = \pi(a)$ Fixpunkt von π ist. Zur Vereinfachung der Notation vereinbart man, dass solche Zyklen nicht angeschrieben werden müssen. Zyklen der Länge 2 nennt man auch *Transpositionen*.
Man beachte, dass erstens alle zyklischen Vertauschungen

$$(a_1 a_2 \ldots a_{k-1} a_k), (a_2 a_3 \ldots a_k a_1), \ldots, (a_k a_1 \ldots a_{k-2} a_{k-1})$$

denselben Zyklus darstellen. Zweitens haben Vertauschungen von elementfremden Zyklen keinen Einfluss auf die dargestellte Permutation. Dabei unterstellen wir, was ganz allgemein vereinbart sein soll: Sind $z_1, z_2, \ldots, z_m$ Zyklen (aufgefasst als Symbolketten), die Permutationen $\pi_1, \pi_2, \ldots, \pi_m \in S_n$ darstellen, so möge die *Juxtaposition* (die durch schlichte Aneinanderreihung entstehende Zeichenkette) $z_1 z_2 \ldots z_m$ die Komposition $\pi_1 \circ \pi_2 \circ \ldots \circ \pi_m$ bezeichnen, wobei wir das Symbol $\circ$ allerdings meist weglassen werden. Zu beachten ist, dass wegen der Assoziativität von $\circ$ beliebige Klammernsetzungen dasselbe Ergebnis liefern und somit auf weitere Klammern verzichtet werden kann.
Ist X unendlich, so kann die Zyklenschreibweise offenbar auch verwendet werden, allerdings nur für jene $\pi \in S_X$ mit endlichem Träger $\{a \in X \mid \pi(x) \neq x\}$.
Wir fassen die wichtigsten Tatsachen über endliche Permutationsgruppen und ihre Zyklenschreibweise zusammen:

Proposition 3.2.5.9.

(1) *Die Ordnung von S_n ist gegeben durch $|S_n| = n!$.*

(2) *Jedes $\pi \in S_n$ hat eine Darstellung als Produkt paarweise elementfremder Zyklen. Diese Darstellung ist eindeutig bis auf a) Weglassen und Hinzufügen von 1-Zyklen, b) die Reihenfolge der Zyklen und c) zyklische Vertauschungen innerhalb der Zyklen.*

(3) *Jedes $\pi \in S_n$ hat eine Darstellung als Produkt von (i.A. nicht paarweise elementfremden) Transpositionen.*

(4) *Ist für $\pi \in S_n$ die Zahl*

$$f(\pi) := |\{(i,j) \mid 1 \leq i < j \leq n \text{ und } \pi(i) > \pi(j)\}|$$

der sogenannten Fehlstände *von π gerade, so ist in jeder Darstellung von $\pi \in S_n$ als Produkt von Transpositionen deren Anzahl gerade. So ein π heißt eine* gerade Permutation.

Ist hingegen $f(\pi)$ ungerade, so ist in jeder Darstellung von $\pi \in S_n$ als Produkt von Transpositionen deren Anzahl ungerade. So ein π heißt eine ungerade Permutation.

(5) *Die sogenannte* Signumfunktion $\operatorname{sgn}\colon S_n \to \{-1,1\}$*, die geraden Permutationen den Wert 1 und ungeraden den Wert -1 zuweist, ist ein Gruppenhomomorphismus von S_n in die multiplikative Gruppe $\{-1,1\}$.*

(6) *Die geraden Permutationen $\pi \in S_n$ bilden einen Normalteiler $A_n \lhd S_n$ der Ordnung $|A_n| = \frac{n!}{2}$ für $n \geq 2$ bzw. $|A_1| = 1$.*

(7) *Ein Zyklus der Länge k ist gerade (ungerade) genau dann, wenn k ungerade (gerade) ist.*

Beweis.

(1) Für $k \leq n \in \mathbb{N}$ sei $A(k,n)$ die Anzahl der injektiven Abbildungen von einer k- in eine n-elementige Menge. Dann ist $A(0,n) = 1$, $A(1,n) = n$, $A(2,n) = n(n-1)$, allgemein (Induktion nach k) $A(k,n) = \frac{n!}{(n-k)!}$, insbesondere also $|S_n| = A(n,n) = n!$.

(2) Folgt aus den Bemerkungen vor dieser Proposition.

(3) Wegen $(a_1 a_2 \dots a_k) = (a_1 a_2)(a_2 a_3)\dots(a_{k-1} a_k)$ gilt die Behauptung für Zyklen, und wegen (2) überträgt sie sich von Zyklen auf beliebige $\pi \in S_n$.

(4) Offenbar hat die identische Permutation id keinen Fehlstand, also ist $f(\mathrm{id}) = 0$ gerade. Weil sich nach (3) jedes beliebige $\pi \in S_n$ als Produkt von Transpositionen schreiben lässt, genügt es zu zeigen, dass sich durch Multiplikation mit einer einzigen Transposition die Parität der Anzahl der Fehlstände (gerade oder ungerade, Anzahl modulo 2) ändert, was aus Übungsaufgabe 3.2.5.10 folgt – dies zeigt auch, dass für eine feste Permutation entweder in jeder Darstellung eine gerade oder in jeder Darstellung eine ungerade Anzahl an Transpositionen auftritt.

(5) Mittels (4) überzeugt man sich unmittelbar, dass für jeden der vier Fälle (ge-

rade/gerade, gerade/ungerade, ungerade/gerade, ungerade/ungerade) die Homomorphiebedingung $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$ erfüllt ist.

(6) Wegen (5) ist die Menge A_n der geraden Permutationen der Kern des Homomorphismus sgn und als solcher ein Normalteiler. Für $n \geq 2$ gibt es mindestens eine Transposition $\tau \in S_n$. Die Nebenklasse τA_n besteht genau aus den ungeraden Permutationen und hat gleich viele Elemente wie A_n, woraus $|A_n| = \frac{n!}{2}$ folgt. Die Behauptung $|A_1| = 1$ schließlich ist trivial.

(7) In der Produktdarstellung $(a_1 a_2 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)$ ist die Anzahl der Transpositionen $k-1$, woraus mit (4) die Behauptung folgt. □

UE 162 ► **Übungsaufgabe 3.2.5.10.** (V) Zeigen Sie: Ist $\pi \in S_n$ und $\tau = (k, k+1)$ eine Transposition benachbarter Elemente, so gilt entweder $f(\tau\circ\pi) = f(\pi)+1$ oder $f(\tau\circ\pi) = f(\pi)-1$. Zeigen Sie außerdem, dass sich eine beliebige Transposition τ' als Produkt einer *ungeraden* Anzahl von Transpositionen benachbarter Elemente schreiben lässt.
Schließen Sie $f(\tau' \circ \pi) \equiv f(\pi) + 1 \pmod 2$.
(Bezeichnungsweisen wie in (4) von Proposition 3.2.5.9.) ◄ **UE 162**

Aus der letzten Proposition stellen wir die folgende Definition explizit heraus:

Definition 3.2.5.11. Für $n \geq 1$ nennt man die Gruppe A_n der geraden Permutationen die *alternierende Gruppe* auf n Elementen (oder vom Grad n).

Mit Hilfe der Zyklenschreibweise wiederholen wir bzw. sieht man sehr leicht:

Proposition 3.2.5.12.

(1) *Die Permutationen $\pi, \pi' \in S_n$ mögen die Darstellungen $\pi = \zeta_1\zeta_2 \dots \zeta_m$ und $\pi' = \zeta'_1\zeta'_2 \dots \zeta'_{m'}$ als Produkte von Zyklen ζ_i bzw. ζ'_i haben. Sind alle ζ_i zu allen ζ'_j elementfremd, so vertauschen π und π', d. h. $\pi\pi' = \pi'\pi$.*

(2) *Sei $\pi = \zeta_1\zeta_2 \dots \zeta_m$ eine Darstellung der Permutation $\pi \in S_n$ als Produkt paarweise elementfremder Zyklen der Längen $k_1, k_2, \dots, k_m$. Dann ist die Ordnung von π gegeben durch* $\operatorname{ord}(\pi) = \operatorname{kgV}(k_1, k_2, \dots, k_m)$.

(3) *Sei*

$$\pi = (a_{1,1}a_{1,2} \dots a_{1,k_1}) \dots (a_{m,1}a_{m,2} \dots a_{m,k_m})$$

eine Darstellung der Permutation $\pi \in S_n$ als Produkt von Zyklen und $\sigma \in S_n$ beliebig. Dann erhält man eine Darstellung der zu π bezüglich σ konjugierten Permutation $\sigma\pi\sigma^{-1}$, indem man in der Zyklendarstellung von π jedes $a_{i,j}$ durch $\sigma(a_{i,j})$ ersetzt, also:

$$\sigma\pi\sigma^{-1} = (\sigma(a_{1,1})\sigma(a_{1,2}) \dots \sigma(a_{1,k_1})) \dots (\sigma(a_{m,1})\sigma(a_{m,2}) \dots \sigma(a_{m,k_m}))$$

(4) *Eine Untergruppe $N \leq S_n$ ist genau dann Normalteiler $N \lhd S_n$ von S_n, wenn sie von jedem Permutationstyp entweder kein oder alle $\pi \in S_n$ dieses Typs enthält. Unter dem Permutationstyp von $\pi \in S_n$ sei dabei die Familie $(v_k(\pi))_{k\in\mathbb{N}}$ verstanden, wobei $v_k(\pi)$ die Anzahl der Zyklen der Länge k in einer (und damit in jeder beliebigen) Darstellung von π als Produkt elementfremder Zyklen ist.*

Beweis.

(1) Haben wir schon verwendet.

(2) Ein Zyklus der Länge k hat offenbar die Ordnung k. Sind $\pi = \zeta_1\zeta_2\dots\zeta_m$ und $\pi' = \zeta'_1\zeta'_2\dots\zeta'_{m'}$ zwei Produkte paarweise elementfreier Zyklen, wobei zusätzlich auch ζ_i und ζ'_j kein Element gemeinsam haben, so erhalten wir $\pi\pi' = \pi'\pi$ aus (1). Außerdem gilt $\langle\pi\rangle \cap \langle\pi'\rangle = \{\mathrm{id}\}$: Jede Permutation in $\langle\pi\rangle$ hält alle Elemente fest, die in der Zyklendarstellung von π nicht vorkommen. Dieselbe Aussage gilt für π'. Somit muss eine Permutation $\sigma \in \langle\pi\rangle \cap \langle\pi'\rangle$ jedes Element festhalten, das nicht in beiden Zyklendarstellungen vorkommt. Nach Annahme kann kein Element in beiden Zyklendarstellungen vorkommen, womit σ alle Elemente festhalten muss, also $\sigma = \mathrm{id}$. Mit dieser Tatsache folgt die Behauptung aus der ersten Aussage zusammen mit Aussage (4) aus 3.2.4.12 mittels Induktion nach m.

(3) Ergibt sich unmittelbar aus $\sigma\pi\sigma^{-1}(\sigma(a)) = \sigma(\pi(a))$.

(4) Laut Folgerung 3.2.5.8 ist eine Untergruppe genau dann Normalteiler, wenn sie bezüglich innerer Automorphismen, d. h. bezüglich Konjugationen, abgeschlossen ist. Das wiederum ist laut (3) genau dann der Fall, wenn sie mit jedem π eines gewissen Permutationstyps alle Permutationen dieses Typs enthält. □

Die Nützlichkeit all dieser Erkenntnisse zeigt sich zum Beispiel im Folgenden.

Proposition 3.2.5.13. *Sei $G := S_X$ die symmetrische Gruppe auf der Menge X.*

1. *Für $|X| \geq 3$ ist das Zentrum von G trivial: $Z(S_X) = \{\mathrm{id}_X\}$. Folglich ist in diesem Fall der Homomorphismus $\Phi\colon G \to \mathrm{Aut}(G)$ aus Proposition 3.2.5.6 eine isomorphe Einbettung.*

2. *Ist $|X| \geq 3$ und $|X| \neq 6$, so ist jeder Automorphismus von $G = S_X$ ein innerer Automorphismus. Folglich ist $\Phi\colon G \to \mathrm{Aut}(G)$ sogar ein Isomorphismus.*

3. *Für $|X| = 6$ gibt es Automorphismen von $G = S_X$, die keine inneren Isomorphismen sind.*

UE 163 ► **Übungsaufgabe 3.2.5.14.** (V,E) Beweisen Sie Proposition 3.2.5.13. Zur Orientierung: Die erste Aussage ist relativ leicht. Die zweite braucht vor allem kombinatorische Überlegungen. Die dritte ist sehr anspruchsvoll. ◄ **UE 163**

UE 164 ► **Übungsaufgabe 3.2.5.15.** (B) Geben Sie eine Gruppe G mit zwei Untergruppen H und J mit $J \subseteq H \subseteq G$ an, sodass $J \lhd H$ und $H \lhd G$, nicht aber $J \lhd G$. (Hinweis: Sei G z. B. die alternierende Gruppe A_4 oder die Gruppe aller Drehungen und Spiegelungen, die ein festes Quadrat auf sich abbilden.) ◄ **UE 164**

Im folgenden Beispiel wird anhand der symmetrischen Gruppe S_4 der erste Isomorphiesatz für Gruppen (Satz 3.2.2.14, erste Aussage) illustriert.

UE 165 ► **Übungsaufgabe 3.2.5.16.** (F) Sei $G := S_4$. Wir geben die Elemente von G in Zyklenschreibweise an. Sei U die vom Element (1234) erzeugte Untergruppe und $N = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Begründen Sie, warum $N \lhd S_4$ ein Normalteiler ist. Bestimmen Sie die Gruppen NU, $N \cap U$, NU/N, $U/(N \cap U)$ und geben Sie den kanonischen Isomorphismus zwischen NU/N und $U/(N \cap U)$ explizit an. ◄ **UE 165**

UE 166 ► **Übungsaufgabe 3.2.5.17.** (F) Sei $N_i \lhd G_i$ für $i = 1, 2$ mit $N_1 \cong N_2$ sowie $G_1/N_1 \cong G_2/N_2$. Folgt daraus $G_1 \cong G_2$? ◄ **UE 166**

3.2.6. Symmetrie

Inhalt in Kurzfassung: Der Begriff der Symmetrie hat eindeutig geometrischen Ursprung. Die adäquate mathematische Fassung dieses Phänomens fußt jedoch auf dem Gruppenbegriff. Im vorliegenden, letzten Unterabschnitt zur elementaren Gruppentheorie wird das ausblicksartig beleuchtet, vorwiegend unter historischen Gesichtspunkten und völlig ohne neue Resultate.

Der Begriff der Gruppe hat die Entwicklung der Mathematik im Laufe des 19. Jahrhunderts in ähnlicher Weise vorangetrieben wie der des Grenzwertes. Beim Grenzwert ging es vor allem um die Exaktifikation eines intuitiv recht eingängigen Konzeptes, das schon seit etwa 200 Jahren im Zentrum vieler Bestrebungen stand. Doch erst mit dem Begriff der Gruppe begann jene Tendenz zur Abstraktion, die wesentliche Teile der modernen Mathematik durchzieht, insbesondere die Algebra.
Historischer Ausgangspunkt war die Galoistheorie[12], siehe Kapitel 9 (Algebra II). In heutiger Sprechweise spielen darin Gruppen von Automorphismen von Körpern eine zentrale Rolle. Die Struktur dieser Gruppen ermöglicht entscheidende Rückschlüsse auf die ursprünglich gegebenen Objekte (der Körper, in denen Lösungen von algebraischen Gleichungen liegen). Ähnliche Motivationen veranlassten Felix Klein (1849 – 1925) im Jahr 1872, sein berühmtes *Erlanger Programm* zu formulieren, das – sehr verkürzt formuliert – darin besteht, geometrische Eigenschaften als Invarianten unter gewissen Transformationen zu begreifen, die eine Gruppe bilden. Beiden Situationen gemeinsam ist das Bestreben, eine Struktur über ihre inhärenten abstrakten Symmetrien zu verstehen. Diesem ersten Abstraktionsschritt von elementaren Objekten hin zu ihren Symmetriegruppen sind in der neueren Entwicklung der Mathematik noch zahlreiche ähnliche gefolgt. Kleine Kostproben davon haben wir schon kennengelernt, indem wir zunächst von arithmetischen Gesetzen zu Strukturen übergingen, in denen solche Gesetze gelten, und dann weiter zu Klassen (Varietäten, Kategorien) solcher Strukturen.
Unter speziell gruppentheoretischem Gesichtspunkt seien als Beispiele hier lediglich lineare Gruppen erwähnt. Geht man von einem Vektorraum V über einem Körper K aus, so bietet sich die Automorphismengruppe $\mathrm{Aut}(V)$ an, die man auch *allgemeine lineare Gruppe* nennt. Ist V von endlicher Dimension n, so lässt sich diese Gruppe identifizieren

[12] benannt nach dem französischen Mathematiker Évariste Galois (1811-1832)

mit der multiplikativen Gruppe aller regulären $n \times n$-Matrizen über K. Man schreibt für diese Gruppe auch $\mathrm{GL}(n, K)$ (für *General Linear Group*). Darin liegt als Untergruppe die sogenannte *spezielle lineare Gruppe* $\mathrm{SL}(n, K)$, die nur die Matrizen mit Determinante 1 enthält. Faktorisiert man die allgemeine lineare Gruppe nach $K \setminus \{0\}$, so erhält man die ebenfalls wichtige *projektive lineare Gruppe* $\mathrm{PGL}(n, K)$. Weitere sehr interessante Gruppen linearer Transformationen sind die *orthogonale Gruppe* $\mathrm{O}(n)$ aller orthogonalen $n \times n$-Matrizen über $\mathbb{R}$ und die *unitäre Gruppe* $\mathrm{U}(n)$ aller unitären $n \times n$-Matrizen über $\mathbb{C}$.
Die Strukturanalyse der linearen Gruppen ist so weit fortgeschritten, dass man versucht, beliebige Gruppen mit linearen Gruppen in Verbindung zu bringen. Insbesondere ist das der Zugang der sogenannten *Darstellungstheorie*, in der man versucht für eine Gruppe G sämtliche Homomorphismen von G in eine lineare Gruppe (sogenannte *lineare Darstellungen* von G) zu verstehen und damit von diesen auf G rückzuschließen.

3.3. Moduln, insbesondere abelsche Gruppen

Moduln interessieren uns an dieser Stelle vor allem deshalb, weil abelsche Gruppen stets auch unitäre Moduln über dem Ring $\mathbb{Z}$ und in gewissen Fällen auch über $\mathbb{Z}_m$ sind (3.3.1). Das ergibt einen klareren Blick auf ihre Struktur. Aufgrund dieser Fokussierung benötigen wir – obwohl der Ringbegriff im Modulbegriff vorkommt – in diesem Abschnitt keine tieferen Kenntnisse über Ringe, wie wir sie in Abschnitt 3.4 entwickeln werden.
In 3.3.2 befassen wir uns mit den grundlegenden Konstruktionen, bevor in 3.3.3 und 3.3.4 als Hauptergebnis dieses Abschnitts die Struktur endlicher abelscher Gruppen geklärt wird. Eine vertiefende Fortsetzung des Themas, insbesondere die Analyse von Auswirkungen gewisser Eigenschaften des zugrundeliegenden Rings, ist Inhalt von Kapitel 7.

3.3.1. Abelsche Gruppen als Moduln über $\mathbb{Z}$ und $\mathbb{Z}_m$

Inhalt in Kurzfassung: Die übliche Notation für additive Potenzen zusammen mit den elementaren Potenzrechenregeln aus Unterabschnitt 3.1.1 zeigt unmittelbar, dass jede abelsche Gruppe in natürlicher Weise auch ein Modul über dem Ring $\mathbb{Z}$ ist. In diesem Zusammenhang werden für abelsche Gruppen auch Begriffe wie Torsionselement, Torsionsanteil, p-Element ($p \in \mathbb{P}$) und Exponent definiert.

Im Folgenden schreiben wir abelsche Gruppen stets in additiver Notation $(A, +, 0, -)$ und verwenden folgende Notationen und Sprechweisen:

Definition 3.3.1.1. Sei A eine abelsche Gruppe. Dann heißt jedes $a \in A$ mit endlicher Ordnung $\mathrm{ord}(a)$ *Torsionselement*. Gilt stärker $\mathrm{ord}(a) = p^e$ mit $p \in \mathbb{P}$ und $e \in \mathbb{N}$, so heißt a auch *p-Element*. Die Menge aller Torsionselemente von A heißt der *Torsionsanteil*. Wir bezeichnen ihn mit A_t. Die Menge aller p-Elemente von A heißt der *p-Anteil* von A. Wir bezeichnen ihn mit A_p. Gibt es ein $m \in \mathbb{N}^+$ mit $ma = 0$ für alle $a \in A$, so heißt das kleinste unter diesen m auch der *Exponent* der abelschen Gruppe A. Dieser wird auch mit $\exp(A)$ bezeichnet.

Schreiben wir die Potenzrechenregeln aus Proposition 3.1.1.10 für abelsche Gruppen in additiver Schreibweise an, so erhalten wir[13]

(1) $(m+n)a = ma + na$
(2) $m(na) = (mn)a$
(3) $n(a+b) = na + nb$

für alle $a, b \in A$ und alle $m, n \in \mathbb{Z}$. Gemeinsam mit der nach Definition geltenden Gleichung $1a = a$ (für alle $a \in A$) sind das genau die definierenden Gesetze eines unitären $\mathbb{Z}$-Moduls, siehe Definition 2.1.3.7.

Bevor wir fortfahren, erinnern wir an $\mathbb{Z}_m$, den Restklassenring modulo m aus Beispiel 2.2.3.21; siehe auch Definition 3.4.1.15: Das ist der Faktorring von $\mathbb{Z}$ nach der Kongruenzrelation $\equiv_m$, die durch $a \equiv_m b \Leftrightarrow m|(b-a)$ (äquivalent: $b - a \in m\mathbb{Z}$) definiert ist. Mit der schon bei Gruppen verwendeten Notation $k + m\mathbb{Z}$ für die Restklasse (anstatt $[k]_{\equiv_m}$) rechnen wir gemäß $(k_1 + m\mathbb{Z}) + (k_2 + m\mathbb{Z}) = (k_1 + k_2) + m\mathbb{Z}$ und $(k_1 + m\mathbb{Z}) \cdot (k_2 + m\mathbb{Z}) = k_1k_2 + m\mathbb{Z}$. Die additive Gruppe des Restklassenrings $\mathbb{Z}_m$ ist also genau die Restklassengruppe C_m.

Sei nun angenommen, dass es ein $m \in \mathbb{N}^+$ gibt mit $ma = 0$ für alle $a \in A$. Das bedeutet, dass m ein Vielfaches aller additiven Ordnungen von Elementen $a \in A$ und somit des Exponenten von A ist. In diesem Fall ist A sogar ein $\mathbb{Z}_m$-Modul, weil dann ka von k nur über die Restklasse von k modulo m abhängt, genauer: Aus $k_1 \equiv_m k_2$ folgt $k_2 = k_1 + nm$ mit $n \in \mathbb{Z}$, also $k_2a = (k_1 + nm)a = k_1a + n(ma) = k_1a$. Somit ist in diesem Fall durch $(k + m\mathbb{Z})a := ka$, $k \in \mathbb{Z}$ und $a \in A$, eine Struktur auf A wohldefiniert. Die Gesetze für einen unitären $\mathbb{Z}_m$-Modul vererben sich direkt von denen eines unitären $\mathbb{Z}$-Moduls. Wir erhalten also:

Proposition 3.3.1.2. *Jede abelsche Gruppe A ist ein unitärer $\mathbb{Z}$-Modul vermittels $(k, a) \mapsto ka$, $k \in \mathbb{Z}$ und $a \in A$. Im Fall $\exp(A)|m$ mit positivem $m \in \mathbb{N}$ ist A auch ein unitärer $\mathbb{Z}_m$-Modul vermittels $(k + m\mathbb{Z}, a) \mapsto ka$, $k \in \mathbb{Z}$ und $a \in A$.*

Über den Begriff der Ordnung bzw. des Exponenten erscheint klar, dass das Studium von Elementen ka mit $k \in \mathbb{Z}$ und $a \in A$ lohnend ist. In Proposition 3.2.4.12 klingen bereits zwei wichtige Tatsachen an: Einerseits spielen Teilbarkeitsüberlegungen (zu den ganzen Zahlen k) eine wesentliche Rolle, andererseits gelten manche Aussagen nur unter einer zusätzlichen Kommutativitätsvoraussetzung. Daher entwickelt dieser Ansatz seine volle Stärke erst im Fall abelscher Gruppen; tatsächlich bilden derartige Teilbarkeitsüberlegungen das Rückgrat der Strukturanalyse abelscher Gruppen, wie wir sie in diesem Abschnitt anstellen wollen. Aus diesem Grund ist es erhellend, die Operationen $a \mapsto ka$ für festes $k \in \mathbb{Z}$ bzw. $\mathbb{Z}_m$ als Teil der Struktur der abelschen Gruppe zu sehen – genau das leistet der Begriff des Moduls.

[13] Es sei explizit betont, dass die Kommutativität der Gruppenoperation dabei nur beim Distributivgesetz von rechts $n(a+b) = na + nb$ eingeht; die anderen Aussagen würden auch ohne diese Voraussetzung gelten.

3.3.2. Unter- und Faktormoduln, Homomorphismen, Produkte und direkte Summen

Inhalt in Kurzfassung: Die grundlegenden Konstruktionen für Moduln verlaufen weitgehend analog zur Situation bei Gruppen bzw. bei Vektorräumen aus der Linearen Algebra. Wegen der Kommutativität der additiven Gruppe eines Moduls vereinfacht sich die Situation bei inneren direkten Produkten/Summen im Vergleich zu beliebigen Gruppen.

Sei A ein R-Modul, d. h. ein Modul über einem Ring R. Eine Teilmenge $U \subseteq A$ ist genau dann ein Untermodul $U \leq A$, wenn $U \leq A$ als (abelsche) Gruppe und zusätzlich $ru \in U$ für alle $r \in R$ und $u \in U$ gilt. Das ist genau dann der Fall, wenn U abgeschlossen ist bezüglich der Bildung von *Linearkombinationen*, d. h. wenn für alle $r_1, \ldots, r_n \in R$ und $a_1, \ldots, a_n \in U$ auch

$$\sum_{i=1}^{n} r_i a_i \in U.$$

Entsprechend dienen Linearkombinationen auch zur Charakterisierung von R-Modul-Homomorphismen, den sogenannten *R-linearen Abbildungen*. Nach der allgemeinen Definition von Homomorphismen muss ein R-Modul-Homomorphismus $f\colon A \to B$ zwischen zwei R-Moduln A und B verträglich sein mit den fundamentalen Operationen: Addition, Nullelement, additives Inverses und Multiplikation mit r für alle $r \in R$. Offenbar ist das genau dann der Fall, wenn für alle $r_1, \ldots, r_n \in R$ und $a_1, \ldots, a_n \in A$

$$f\left(\sum_{i=1}^{n} r_i a_i\right) = \sum_{i=1}^{n} r_i f(a_i)$$

gilt, wenn also f verträglich mit allen Linearkombinationen ist.
Wie bei Gruppen nennt man

$$\ker(f) := \{a \in A \mid f(a) = 0\}$$

den *Kern* von f. Weil f auch ein Homomorphismus von Gruppen ist, kommen als Kerne nur Normalteiler von A in Frage, also additive Untergruppen von A. Diese stehen mit den Kongruenzrelationen $\sim$ auf A durch die Bedingung $K = [0]_\sim$ in einer bijektiven Beziehung. Der Kern von f hat noch die zusätzliche Eigenschaft, ein Untermodul zu sein: $r \in R$ und $a \in \ker(f)$ impliziert $f(a) = 0$ und somit auch $f(ra) = rf(a) = r0 = 0$,[14] also $ra \in \ker(f)$. Umgekehrt definiert jeder Untermodul $U \leq A$ eine Kongruenzrelation $\sim$, indem man definiert: $a \sim b$ genau dann, wenn $a - b \in U$. Die Verträglichkeit von $\sim$ mit der Gruppenstruktur wissen wir schon von den Gruppen, und für die Multiplikation mit einem Ringelement $r \in R$ gilt: Aus $a \sim b$ folgt $a - b \in U$, wegen der Untermoduleigenschaft von U weiter $ra - rb = r(a - b) \in U$ und somit $ra \sim rb$. Also:

[14] Es gilt $r0 = 0$ für alle $r \in R$: Wir rechnen nämlich $r0 = r(0 + 0) = r0 + r0$, woraus durch Kürzen (Addition von $-r0$) $r0 = 0$ folgt. Analog sieht man $0a = 0$ für alle $a \in A$.

Proposition 3.3.2.1. *Ist A ein Modul über dem Ring R, so stehen die Kongruenzrelationen $\sim$ auf A und die Untermoduln $U \leq A$ durch die Bedingung*

$$\forall a, b \in A: \ a \sim b \quad \text{genau dann wenn} \quad a - b \in U$$

in einer bijektiven Beziehung zueinander.

Schreiben wir A/U für den Faktormodul $A/_\sim$, wenn $U \leq A$ und die Kongruenzrelation $\sim$ gemäß Proposition 3.3.2.1 zusammengehören, so bedeutet das: Sämtliche Faktormoduln eines R-Moduls A sind gegeben durch sämtliche A/U mit $U \leq A$. Die Elemente von A/U sind wie bei Faktorgruppen Nebenklassen $a + U$ und gehorchen den Operationen $r(a + U) = ra + U$, $(a_1 + U) + (a_2 + U) = (a_1 + a_2) + U$ und $-(a + U) = -a + U$. Das Nullelement in A/U ist $0 + U = U$.
Unter Verwendung des Homomorphiesatzes 2.2.3.17 ergibt das auch eine Beschreibung sämtlicher Homomorphismen auf A: Ist $f\colon A \to B$ irgendein oBdA surjektiver Modulhomomorphismus, dann ist $U := \ker(f) \leq A$ mit $A/U \cong B$ vermittels des Isomorphismus $a + U \mapsto f(a)$.

Wir wenden uns nun direkten Produkten zu. Sei I eine (im Allgemeinen unendliche) Indexmenge und für jedes $i \in I$ ein R-Modul A_i gegeben. Wie im Fall von Gruppen enthält das direkte Produkt $A := \prod_{i\in I} A_i$ der A_i den Untermodul

$$\bigoplus_{i\in I} A_i := \left\{ (a_i)_{i\in I} \in \prod_{i\in I} A_i \;\middle|\; a_i \neq 0 \text{ nur für endlich viele } i \in I \right\},$$

den wir im Kontext von Moduln und (additiv geschriebenen) abelschen Gruppen nur selten als schwaches Produkt sondern meistens als *(äußere) direkte Summe* der A_i bezeichnen und mit dem Symbol $\bigoplus$ statt $\prod^w$ anschreiben. Die kanonischen Einbettungen $\iota_{i_0} : A_{i_0} \to \prod_{i\in I} A_i$ bilden in die direkte Summe $\bigoplus_{i\in I} A_i$ ab. Ist I endlich, so stimmen direktes Produkt und direkte Summe wieder überein.
Eine der wichtigsten Eigenschaften der direkten Summe von Moduln bzw. abelschen Gruppen ist die folgende Beobachtung.

Proposition 3.3.2.2. *Seien A_i, $i \in I$, R-Moduln, sei B ein weiterer R-Modul und seien $f_i : A_i \to B$ Modulhomomorphismen. Bezeichnet $\iota_{i_0} : A_{i_0} \to \prod_{i\in I} A_i$ die kanonischen Einbettungen, dann gibt es einen eindeutigen Homomorphismus $h : \bigoplus_{i\in I} A_i \to B$, der $h \circ \iota_{i_0} = f_{i_0}$ für alle $i_0 \in I$ erfüllt.*

UE 167 ▶ Übungsaufgabe 3.3.2.3. (V) Beweisen Sie Proposition 3.3.2.2. **◀ UE 167**

In Proposition 3.3.2.2 kommt eine Dualität zu Proposition 2.2.2.4 zum Ausdruck, die in Unterabschnitt 4.2.1 Anlass zur Definition sogenannter *Koprodukte* geben wird. Man beachte, dass wir dabei auf Moduln, somit abelschen Gruppen, arbeiten müssen. Für beliebige Gruppen ist die Proposition tatsächlich falsch. Der in diesem Zusammenhang entscheidende Unterschied zwischen abelschen und allgemeinen Gruppen bzw. die dahinterstehende Problematik kommt bereits in der folgenden Übungsaufgabe zum Ausdruck:

UE 168 ► **Übungsaufgabe 3.3.2.4.** (F) Wir betrachten die Gruppe $\mathbb{Z} \times \mathbb{Z}$ mit der punktweisen Addition. Sei $b_1 := (1, 0)$, $b_2 := (0, 1)$. Welche der folgenden Aussagen ist wahr? (Beweis bzw. Gegenbeispiel.) ◄ **UE 168**

(1) Für alle Gruppen H und alle $h_1, h_2 \in H$ gibt es einen eindeutig bestimmten Homomorphismus $\varphi\colon \mathbb{Z} \times \mathbb{Z} \to H$ mit $\varphi(b_1) = h_1$, $\varphi(b_2) = h_2$.

(2) Für alle abelschen Gruppen H und alle $h_1, h_2 \in H$ gibt es einen eindeutig bestimmten Homomorphismus $\varphi\colon \mathbb{Z} \times \mathbb{Z} \to H$ mit $\varphi(b_1) = h_1$, $\varphi(b_2) = h_2$.

Wie in Gruppen unterscheidet man von dieser *äußeren* direkten Summe die *innere* direkte Summe:

Definition 3.3.2.5. Ein R-Modul A heißt *innere direkte Summe* seiner Untermoduln $U_i \leq A$, wenn die Abbildung

$$\varphi\colon \bigoplus_{i\in I} U_i \to A, \quad (u_i)_{i\in I} \mapsto \sum_{i\in I} u_i$$

ein Isomorphismus von R-Moduln ist. Man schreibt in diesem Fall auch oft $A = \bigoplus_{i\in I} U_i$ oder im Fall von $|I| = n$, sagen wir $I = \{1, \dots, n\}$, auch $A = U_1 \oplus \cdots \oplus U_n$.

Man beachte, dass die Abbildung φ aus Definition wieder deshalb wohldefiniert ist, weil die Summe, wenn man alle Summanden mit $a_i = 0$ weglässt, zur endlichen Summe wird.

Anmerkung 3.3.2.6. Ganz analog zu Gruppen (vgl. Proposition 3.2.3.13) ist eine äußere direkte Summe von Moduln immer auch eine innere direkte Summe der Bilder dieser Moduln unter den kanonischen Einbettungen. Umgekehrt ist jede innere direkte Summe nach Definition isomorph zur äußeren direkten Summe derselben Objekte. Daher kann man Resultate über äußere direkte Summen auf innere direkte Summen übertragen – besonders hervorgehoben sei das an dieser Stelle für Proposition 3.3.2.2.
Diese Übertragbarkeit bzw. Isomorphie rechtfertigt auch, wieso wir das Symbol $\oplus$ sowohl für äußere als auch für innere direkte Summen verwenden.

Wie bei Gruppen gibt es sehr nützliche Charakterisierungen, wann ein Modul bzw. eine abelsche Gruppe die innere direkte Summe von gegebenen Untermoduln bzw. Untergruppen ist. Wir konzentrieren uns in der Herleitung auf abelsche Gruppen, da sich hier die Resultate direkt durch Spezialisierung der entsprechenden Charakterisierungen für Gruppen (Proposition 3.2.3.3, Satz 3.2.3.8 und Satz 3.2.3.15) ergeben. Geht man die Beweise der Ergebnisse für Gruppen durch, so stellt man fest, dass die Beweise genauso auch für Moduln funktionieren,[15] sodass wir die Charakterisierungen für Moduln formulieren werden.
Bevor wir dazu kommen, müssen wir noch eine formale Frage klären. Fasst man abelsche Gruppen als $\mathbb{Z}$-Moduln auf, so können wir die grundlegenden Konstruktionen im Kontext abelscher Gruppen auf zwei Arten durchführen – einmal als Spezialisierung von

[15] Der entscheidende Grund ist, dass im Modulfall die Abbildung $\varphi\colon \bigoplus_{i\in I} U_i \to A, \quad (u_i)_{i\in I} \mapsto \sum_{i\in I} u_i$ wegen der Distributivgesetze automatisch mit der Multiplikation mit Ringelementen verträglich ist, unabhängig von besonderen Eigenschaften der Untermoduln U_i.

beliebigen Gruppen und einmal als Spezialisierung von Moduln. Es macht dabei keinen Unterschied, welche dieser Varianten man wählt, wie die folgende Übungsaufgabe zeigt. Diese Tatsache rechtfertigt einmal mehr unser Vorgehen, abelsche Gruppen als $\mathbb{Z}$-Moduln zu betrachten.

Proposition 3.3.2.7. *Seien A und B abelsche Gruppen, $U, U_i \leq A$, $i \in I$, Untergruppen von A und m eine positive natürliche Zahl. Dann gilt:*

(1) *$U \leq A$ ist auch ein Unter-$\mathbb{Z}$-Modul von A. Im Fall $\exp(A)|m$ ist U überdies ein Unter-$\mathbb{Z}_m$-Modul von A.*

(2) *Jeder Gruppenhomorphismus $\varphi : A \to B$ ist auch ein $\mathbb{Z}$-Modulhomomorphismus, im Fall $\exp(A)|m$ überdies ein $\mathbb{Z}_m$-Modulhomomorphismus.*

(3) *Ist A die innere direkte Summe der U_i als (abelsche) Gruppe (gemäß Definition 3.2.3.12), so auch als $\mathbb{Z}$-Modul (gemäß Definition 3.3.2.5), im Fall $\exp(A)|m$ überdies als $\mathbb{Z}_m$-Modul (ebenfalls gemäß Definition 3.3.2.5).*

UE 169 ► Übungsaufgabe 3.3.2.8. (V) Beweisen Sie Proposition 3.3.2.7. **◄ UE 169**

Die entscheidende Beobachtung bei der Spezialisierung der Charakterisierungen auf abelsche Gruppen ist, dass jede Untergruppe automatisch ein Normalteiler ist und dass für $x \in U_i$ und $y \in U_j$ automatisch $xy = yx$ gilt. Somit sind die Bedingungen (2) in Proposition 3.2.3.3 und (B) sowie (B') in Satz 3.2.3.8 und Satz 3.2.3.15 stets erfüllt und daher überflüssig. Wir erhalten also:

Proposition 3.3.2.9. *Ein R-Modul A ist genau dann die innere direkte Summe von Untermoduln $U, V \leq A$, wenn sowohl $U \cap V = \{0\}$ als auch $A = U + V$ gilt.*

Folgerung 3.3.2.10. *Ein R-Modul A ist genau dann die innere direkte Summe von Untermoduln $U_1, \ldots, U_n$, wenn folgende zwei Bedingungen erfüllt sind:*

(1) *$A = U_1 + U_2 + \ldots + U_n$*

(2) *Für alle $i = 1, \ldots, n$ gilt $U_i \cap (U_1 + U_2 + \ldots U_{i-1} + U_{i+1} + \ldots + U_n) = \{0\}$.*

Satz 3.3.2.11. *Ein R-Modul A ist genau dann die innere direkte Summe von Untermoduln $U_i \leq A$, $i \in I$, wenn die folgenden beiden Bedingungen erfüllt sind:*

(1) *Zu jedem $a \in A$ gibt es endlich viele $i_1, \ldots, i_n \in I$ und $u_1 \in U_{i_1}, \ldots, u_n \in U_{i_n}$ mit $a = \sum_{i=1}^{n} u_i$.*

(2) *Ist $i \in I$ und verschieden von allen $i_1, \ldots, i_n \in I$, so ist $U_i \cap (U_{i_1} + \ldots + U_{i_n}) = \{0\}$.*

Anmerkung 3.3.2.12. Sei A sogar ein unitärer R-Modul, d. h., R habe ein Einselement 1_R, für das $1_R a = a$ für alle $a \in A$ gilt. Beachtet man, dass die U_i stets Untermoduln sind und daher $ru \in U_i$ für alle $r \in R$ und $u \in U_i$ gilt, so ist die erste Bedingung aus Satz 3.3.2.11 äquivalent zur folgenden Bedingung:

Zu jedem $a \in A$ gibt es endlich viele $i_1, \ldots, i_n \in I$, $u_1 \in U_{i_1}, \ldots, u_n \in U_{i_n}$ und $r_1, \ldots, r_n \in R$ mit $a = \sum_{i=1}^{n} r_i u_i$.

Mit anderen Worten ist diese Bedingung also äquivalent dazu, dass A von den U_i erzeugt wird, siehe auch Proposition 2.2.1.19.

Wir werden in den nächsten beiden Unterabschnitten sehen, dass sich aus den zyklischen Gruppen sämtliche endlichen abelschen Gruppen ergeben; siehe Satz 3.3.4.2 (in Algebra II, vgl. Satz 7.4.3.1, werden wir dasselbe sogar für endlich *erzeugte* abelsche Gruppen zeigen). Die folgende Übungsaufgabe, die auf unserem Wissen über zyklische Gruppen fußt, kann sowohl als Vorbereitung darauf als auch als Gruppenversion (der klassischen Fassung) des chinesischen Restsatzes (siehe Satz 3.4.7.2) betrachtet werden.

UE 170 ► Übungsaufgabe 3.3.2.13. (W) **◄ UE 170**

(1) $C_n \times C_m$ ist genau dann zyklisch, wenn n und m keinen gemeinsamen Teiler $d > 1$ haben. Finden Sie einen expliziten Isomorphismus $f : C_{mn} \to C_m \times C_n$, indem Sie zuerst einen Wert für $f(1)$ vorschreiben.

(2) Zeigen Sie (äußere direkte Summe)

$$C_n \cong \bigoplus_{p \in \mathbb{P}} C_{p^{e_p}}$$

für die zyklische Gruppe C_n der Ordnung $n = \prod_{p \in \mathbb{P}} p^{e_p}$.

Anmerkung 3.3.2.14. Die (innere) direkte Summe von Moduln spielt (in der Spezialisierung auf Vektorräume) schon in der linearen Algebra eine Rolle. Auch Proposition 3.3.2.2 wird zumindest implizit in der linearen Algebra verwendet, nämlich bei *Blockdiagonalmatrizen*: Beispielhaft betrachten wir für einen Körper K den Vektorraum K^5 mit der kanonischen Basis $\{e_1, e_2, e_3, e_4, e_5\}$. Eine 5×5-Matrix über K, sagen wir

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix} \in K^{5\times 5},$$

induziert gemäß $x = (x_i)_{i=1,\dots,5} \mapsto Ax = (\sum_{j=1}^{5} a_{ij} x_j)_{i=1,\dots,5}$ eine lineare Abbildung $K^5 \to K^5$, die für größere Dimensionen (anstelle von 5) zumindest aus numerischer Sicht immer komplexer werden – man denke nur an die Bestimmung der Eigenwerte oder an die Lösung von linearen Gleichungssystemen. Wenn die Matrix hingegen Blockdiagonalform hat, d. h.

$$A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

für beispielsweise $B \in K^{3\times 3}$ und $C \in K^{2\times 2}$, dann lässt sich das Verhalten der linearen Abbildung zu A auf das Verhalten der niedrigerdimensionalen Abbildungen zu B und C zurückführen. Aus abstrakter Sicht betrachtet man dabei die Unterräume $U_1 := \langle e_1, e_2, e_3 \rangle$ sowie $U_2 := \langle e_4, e_5 \rangle$, die nach Proposition 3.3.2.9 eine innere direkte Summe von K^5 bilden. Sind $f_1 : U_1 \to K^5$ bzw. $f_2 : U_2 \to K^5$ die von B bzw. C

induzierten linearen Abbildungen auf U_1 bzw. U_2 (betrachtet als Abbildungen nach K^5 anstatt nach U_i), so gibt es nach Proposition 3.3.2.2 bzw. Anmerkung 3.3.2.6 eine eindeutige lineare Abbildung $h : K^5 \to K^5$, die f_1 und f_2 fortsetzt – dies ist genau die von A induzierte lineare Abbildung, die wir somit durch f_1 und f_2 beschrieben haben.

Zum Abschluss des Unterabschnitts führen wir ein weiteres Beispiel direkter Summen von Vektorräumen an.

UE 171 ► **Übungsaufgabe 3.3.2.15.** (F) Sei K eine beliebige Indexmenge. Für $k \in K$ sei $V_k := \mathbb{R}$ als Vektorraum über $\mathbb{R}$. Lösen Sie zwei der folgenden drei Aufgaben: ◄ **UE 171**

(1) Was ist die Dimension von V_k?

(2) Geben Sie eine Basis für $\bigoplus_{k\in K} V_k$ an.

(3) Geben Sie eine Basis für $\prod_{k\in K} V_k$ an.

3.3.3. Zerlegung von Torsionsgruppen in ihre p-Anteile

Inhalt in Kurzfassung: Technische Vorüberlegungen zur Ordnung von Elementen in abelschen Gruppen zielen auf das Hauptergebnis dieses Unterabschnitts ab: Jede Torsionsgruppe ist die direkte Summe ihrer p-Komponenten. Abschließend wird dieser Satz auf die universelle Prüfergruppe und ihre p-Anteile, die p-Prüfergruppen, angewendet.

Wie bereits angekündigt verfeinern wir nun Proposition 3.2.4.12 für den abelschen Fall.

Lemma 3.3.3.1. *Sei A eine abelsche Gruppe und seien $a_i \in A$ Torsionselemente.*

(1) *Es gilt*

$$\operatorname{ord}\left(\sum_{i=1}^{n} a_i\right) \mid \prod_{i=1}^{n} \operatorname{ord}(a_i).$$

(2) *Sind die* $\operatorname{ord}(a_i)$, $i = 1, \ldots, n$ *paarweise teilerfremd, so gilt sogar Gleichheit:*

$$\operatorname{ord}\left(\sum_{i=1}^{n} a_i\right) = \prod_{i=1}^{n} \operatorname{ord}(a_i)$$

(3) *Es gibt ein Element $a \in A$ mit*

$$\operatorname{ord}(a) = \operatorname{kgV}(\operatorname{ord}(a_1), \ldots, \operatorname{ord}(a_n)).$$

Beweis. Die erste bzw. zweite Aussage folgt mit Induktion aus der dritten bzw. vierten Aussage von Proposition 3.2.4.12 – man beachte, dass je zwei Elemente stets kommutieren.
Für die dritte Aussage sei $P := \{p \in \mathbb{P} \mid \exists i : p \mid \operatorname{ord}(a_i)\}$. Die Menge P ist endlich. Für jedes $p \in \mathbb{P}$ sei $a(p)$ ein a_i, sodass die Primfaktorzerlegung der Ordnung von a_i einen maximalen Exponenten e_p zu p hat. Dann ist $\operatorname{ord}(a(p)) = p^{e_p} k_p$ mit einem zu p teilerfremden k_p. Das Element $b_p := k_p a(p)$ hat die Ordnung p^{e_p}, und die Summe $a := \sum_{p\in P} b_p$ nach (2) die Ordnung $\operatorname{ord}(a) = \prod_p p^{e_p} = \operatorname{kgV}(\operatorname{ord}(a_1), \operatorname{ord}(a_2), \ldots, \operatorname{ord}(a_k))$. □

Folgerung 3.3.3.2. *Hat die abelsche Gruppe A endlichen Exponenten m, so gibt es ein $a \in A$ mit* $\operatorname{ord}(a) = m$.

Beweis. Für alle $a \in A$ ist $\operatorname{ord}(a)|m$. Insbesondere kommen unter sämtlichen $\operatorname{ord}(a)$, $a \in A$, nur endlich viele natürliche Zahlen o_i, $i = 1, \ldots, k$, mit $k \in \mathbb{N}$ vor. Zu jedem i gibt es ein $a_i \in A$ mit $o_i = \operatorname{ord}(a_i)$. Laut Aussage (3) in Lemma 3.3.3.1 gibt es ein $a \in A$ mit $\operatorname{ord}(a) = \operatorname{kgV}(o_1, \ldots, o_k)$. Das ist nur für $\operatorname{ord}(a) = m$ möglich. □

Für die weitere Strukturanalyse sehr wichtig ist die folgende Aussage:

Proposition 3.3.3.3. *Sei A eine abelsche Gruppe. Dann sind sowohl die Menge A_t aller Torsionselemente von A als auch für jede Primzahl $p \in \mathbb{P}$ die Menge A_p aller p-Elemente (der* p-Anteil *oder die* p-Komponente *von A) Untergruppen von A:*

$$A_p \leq A_t \leq A$$

Beweis. A_t und A_p enthalten wegen $\operatorname{ord}(0) = 1 = p^0$ das Nullelement und sind wegen $\operatorname{ord}(a) = \operatorname{ord}(-a)$ abgeschlossen bezüglich additiver Inversenbildung. Sind $\operatorname{ord}(a)$ und $\operatorname{ord}(b)$ endlich, so wegen Lemma 3.3.3.1 auch $\operatorname{ord}(a+b) | \operatorname{ord}(a) \operatorname{ord}(b)$. Also ist A_t abgeschlossen bezüglich $+$. Auch A_p hat diese Eigenschaft, denn aus $a, b \in A_p$ folgt $\operatorname{ord}(a) = p^{e_a}$ und $\operatorname{ord}(b) = p^{e_b}$ mit $e_a, e_b \in \mathbb{N}$ und somit wieder wegen Lemma 3.3.3.1 $\operatorname{ord}(a+b) | \operatorname{ord}(a) \operatorname{ord}(b) = p^{e_a + e_b}$, also $\operatorname{ord}(a+b) = p^e$ mit einem $e \in \mathbb{N}$. □

Klarerweise haben die A_p für verschiedene p nur 0 gemeinsam. Aus Lemma 3.3.3.1 folgt sogar:

Lemma 3.3.3.4. *Sei A eine abelsche Gruppe, und seien $p, p_1, \ldots, p_n$ paarweise verschiedene Primzahlen. Dann gilt*

$$A_p \cap (A_{p_1} + \ldots + A_{p_n}) = \{0\}.$$

Beweis. Für $a \in A_p$ gilt $\operatorname{ord}(a) = p^e$ mit $e \in \mathbb{N}$. Für $a \in A_{p_1} + \ldots + A_{p_n}$ gibt es Elemente $a_i \in A_{p_i}$ mit $a = a_1 + \ldots + a_n$ sowie $\operatorname{ord}(a_i) = p_i^{e_i}$ und $e_i \in \mathbb{N}$. Laut Lemma 3.3.3.1 folgt daraus $\operatorname{ord}(a) | \prod_{i=1}^n p_i^{e_i}$. Beides ist nur für $\operatorname{ord}(a) = 1$ möglich, also $a = 0$. □

Verwenden wir die Charakterisierung 3.3.2.11 direkter Summen von Moduln für den Spezialfall abelscher Gruppen zusammen mit Anmerkung 3.3.2.12, so zeigt Lemma 3.3.3.4, dass die von den p-Komponenten A_p, $p \in \mathbb{P}$, erzeugte Untergruppe U einer abelschen Gruppe A sogar die (innere) direkte Summe der A_p ist. Jedes Element von U ist eine endliche Summe von Elementen gewisser A_p, insbesondere von Torsionselementen, folglich in A_t. Tatsächlich gilt $U = A_t$:

Lemma 3.3.3.5. *Sei A eine abelsche Gruppe und $a \in A_t$. Für die Ordnung von a gelte* $\operatorname{ord}(a) = \prod_{i=1}^n p_i^{e_i}$ *mit paarweise verschiedenen $p_i \in \mathbb{P}$ und $e_i \in \mathbb{N}^+$. Dann gilt $a \in A_{p_1} + \ldots + A_{p_n}$.*

Beweis. Wir betrachten die Komplementärteiler $t_i := \frac{\mathrm{ord}(a)}{p_i^{e_i}}$ der $p_i^{e_i}$ von $\mathrm{ord}(a)$. Für die Elemente $a_i := t_i a$ gilt dann $\mathrm{ord}(a_i) = p_i^{e_i}$, also $a_i \in A_{p_i}$. Wegen $1 = \mathrm{ggT}(t_1, \ldots, t_n)$ gibt es laut Aussage (6) in Proposition 3.2.4.1 ganze Zahlen $k_1, \ldots, k_n$ mit $1 = \sum_{i=1}^n k_i t_i$. Es folgt

$$a = 1a = \left(\sum_{i=1}^n k_i t_i\right) a = \sum_{i=1}^n k_i (t_i a) = \sum_{i=1}^n k_i a_i \in A_{p_1} + \ldots + A_{p_n}.$$

□

Wir fassen zusammen:

Satz 3.3.3.6. *Ist A eine abelsche Gruppe, so gilt für ihren Torsionsanteil A_t die direkte Zerlegung (Darstellung als innere direkte Summe)*

$$A_t = \bigoplus_{p \in \mathbb{P}} A_p.$$

Insbesondere ist jede abelsche Torsionsgruppe direkte Summe ihrer p-Komponenten.

Beweis. Die beiden Bedingungen aus Satz 3.3.2.11 dafür, dass die behauptete Darstellung gilt, sind laut Lemmata 3.3.3.4 und 3.3.3.5 erfüllt. □

Als Anwendungsbeispiel der Zerlegung in p-Komponenten wollen wir nun die sogenannten *Prüfergruppen* kennenlernen. Die einfachste Beschreibung gelingt als Gruppe komplexer Einheitswurzeln, alternativ als direkte Limiten endlicher zyklischer Gruppen.

Satz 3.3.3.7.

(1) *Für jedes $p \in \mathbb{P}$ bildet die Menge C_{p^∞} aller $z \in \mathbb{C}^*$, für die es ein $n \in \mathbb{N}$ gibt mit $z^{p^n} = 1$, eine multiplikative Untergruppe von $\mathbb{C}^*$, die sogenannte* p-Prüfergruppe.

(2) *Für alle festen $p \in \mathbb{P}$ und $n \in \mathbb{N}$ ist die Menge U_{p^n} aller $z \in \mathbb{C}^*$ mit $z^{p^n} = 1$ eine zyklische Untergruppe von C_{p^∞} mit p^n Elementen und Erzeuger $e^{\frac{2\pi i}{p^n}}$. Setzen wir $U_{p^\infty} := C_{p^\infty}$, so ist $\mathrm{Sub}(C_{p^\infty}) = \{U_{p^n} \mid n \in \mathbb{N} \cup \{\infty\}\}$. Dabei gilt $U_{p^m} \subseteq U_{p^n}$ genau dann, wenn $m \leq n$.*

(3) *Die p-Prüfergruppe C_{p^∞} lässt sich in natürlicher Weise als direkter Limes der zyklischen Gruppen C_{p^n}, $n \in \mathbb{N}$, auffassen.*

(4) *Die Menge C_∞ aller $z \in \mathbb{C}^*$, für die es ein $N \in \mathbb{N}$ gibt mit $z^N = 1$, ist eine multiplikative Untergruppe von $\mathbb{C}$, die sogenannte* universelle Prüfergruppe.

(5) *Die universelle Prüfergruppe ist (in additiver Notation) die direkte Summe aller p-Prüfergruppen:*

$$C_\infty \cong \bigoplus_{p \in \mathbb{P}} C_{p^\infty}$$

(6) *Jede Untergruppe U von C_∞ ist (wieder in additiver Notation) die innere direkte Summe von Untergruppen der p-Prüfergruppen:*

$$U \cong \bigoplus_{p \in \mathbb{P}} U_{p^{n(p)}}$$

Dabei gilt $U_{p^{n(p)}} = U \cap C_{p^\infty}$, womit die $n(p) \in \mathbb{N} \cup \{\infty\}$ durch U eindeutig bestimmt sind.

UE 172 ► Übungsaufgabe 3.3.3.8. (V) Beweisen Sie Satz 3.3.3.7. **◄ UE 172**

UE 173 ► Übungsaufgabe 3.3.3.9. (B) **◄ UE 173**

(1) Geben Sie ein Beispiel einer Gruppe G an, in der die Menge der Torsionselemente keine Untergruppe von G ist.
Hinweis: Betrachten Sie zum Beispiel die Permutation $\pi_3 : \mathbb{Z} \to \mathbb{Z}$, die durch $\pi_3(x) = 3 - x$ definiert ist.

(2) Geben Sie ein Beispiel einer nichtabelschen Gruppe an, in der die Menge der Torsionselemente eine nichttriviale Untergruppe von G ist.

3.3.4. Endliche abelsche Gruppen

Inhalt in Kurzfassung: Im Falle endlicher abelscher Gruppen führt die Zerlegung in ihre p-Anteile zum Hauptsatz, wonach eine direkte Zerlegung in zyklische Gruppen möglich ist. Allerdings muss man zuvor die entsprechende Aussage für Gruppen von Primzahlpotenzordnung beweisen.

Im Fall einer endlichen abelschen Gruppe A können wir die Zerlegung aus Satz 3.3.3.6 noch weiter treiben. Denn dann lassen sich auch noch die p-Komponenten in direkte Summen zyklischer Gruppen zerlegen. Entscheidend ist der folgende Hilfssatz, der auch für unendliches A gilt.

Lemma 3.3.4.1. *Sei A eine abelsche p-Gruppe, $p \in \mathbb{P}$ und $a \in A$ ein Element maximaler Ordnung $\operatorname{ord}(a) = p^n$. Bezeichne $\langle b \rangle$ für beliebige $b \in A$ wie üblich die von b erzeugte zyklische Untergruppe von A. Dann gilt:*

(1) *Ist $\langle a \rangle \neq A$, dann gibt es ein $b \in A \setminus \{0\}$ mit $\langle a \rangle \cap \langle b \rangle = \{0\}$.*

(2) *Es gibt ein $U \leq A$ mit $A = U \oplus \langle a \rangle$.*

Beweis.

(1) Unter der Annahme $\langle a \rangle \neq A$ sei $c \in A \setminus \langle a \rangle$. Mit Hilfe dieses Elements werden wir ein b der Ordnung p konstruieren, das nicht in $\langle a \rangle$ liegt, woraus automatisch $\langle a \rangle \cap \langle b \rangle = \{0\}$ folgt. Wegen $p^n \cdot c = 0 \in \langle a \rangle$ gibt es ein minimales $j > 0$ mit $p^j c \in \langle a \rangle$, also $p^j c = m_1 a$, wobei $m_1 = p^k m$ mit $k \in \mathbb{N}$, $m \in \mathbb{Z}$ und $\operatorname{ggT}(p, m) = 1$ sei. Es folgt

$$0 = p^n c = p^{n-j}(p^j c) = p^{n-j} m_1 a = p^{n-j}(mp^k)a = p^{n-j+k} ma.$$

Wegen $p^{n-1}a \neq 0$ und $\operatorname{ggT}(p, m) = 1$ muss $n - j + k \geq n$ sein, also $k \geq j > 0$. Wir wählen

$$b := \underbrace{p^{j-1}c}_{\notin \langle a \rangle} - \underbrace{mp^{k-1}a}_{\in \langle a \rangle} \notin \langle a \rangle.$$

Wegen $pb = p^j c - mp^k a = p^j c - m_1 a = 0$ hat dieses b die gewünschten Eigenschaften.

(2) Sei $U \leq A$ maximal mit $U \cap \langle a \rangle = \{0\}$ (die Existenz eines solchen U folgt in der üblichen Weise aus dem Lemma von Zorn). Nach Proposition 3.3.2.9 (oder alternativ Folgerung 3.3.2.10 bzw. Satz 3.3.2.11) ist $A_0 = U + \langle a \rangle = U \oplus \langle a \rangle$. Somit bleibt lediglich $A_0 = A$ zu zeigen. Dazu gehen wir indirekt vor:

Angenommen es wäre $A_0 \neq A$. Dann ist die von $a + U$ in der Faktorgruppe A/U erzeugte zyklische Untergruppe nicht ganz A/U. Außerdem hat $a + U$ in A/U die Ordnung p^n, was in A/U sicher maximal ist. Nach Teil 1 (angewendet auf A/U statt A und $a+U$ statt a) gibt es folglich ein $b \in A \setminus U$ mit $\langle a+U \rangle \cap \langle b+U \rangle = \{U\}$. Damit wäre die Untergruppe $U' := U + \langle b \rangle \leq A$ eine echte Obermenge von U, die außerdem $U' \cap \langle a \rangle = \{0\}$ erfüllt (denn wenn $u+mb = m'a$ für $u \in U$ und $m, m' \in \mathbb{Z}$ ist, so folgt $mb + U = m'a + U \in \langle a + U \rangle \cap \langle b + U \rangle = \{U\}$, also $mb \in U$ und daher $u + mb = m'a \in U \cap \langle a \rangle = \{0\}$). Dies ist ein Widerspruch zur Maximalität von U, sodass $A_0 = A$ gelten muss. □

Damit wird es leicht, den *Hauptsatz über endliche abelsche Gruppen* zu beweisen:

Satz 3.3.4.2. *Jede endliche abelsche Gruppe A ist direkte Summe von zyklischen Gruppen von Primzahlpotenzordnung:*

$$A \cong \bigoplus_{p \in \mathbb{P}} \bigoplus_{n=1}^{\infty} C_{p^n}^{e_{p,n}},$$

mit Vielfachheiten $e_{p,n} \in \mathbb{N}$, von denen nur endlich viele $\neq 0$ sind. Alle $e_{p,n}$ sind durch A eindeutig bestimmt.

Beweis. Zunächst zur Existenz einer Darstellung wie behauptet: Wegen Satz 3.3.3.6 genügt es, den Satz für festes $p \in \mathbb{P}$ und eine endliche abelsche p-Gruppe A zu beweisen. Wir gehen mittels Induktion nach $|A|$ vor. Die einelementige Gruppe ist zyklisch von der Ordnung p^0, also ist die Aussage des Satzes für $|A| = 1$ mit $e_{p,n} = 0$ für alle p und n trivialerweise erfüllt. Angenommen $|A| > 1$ und die Aussage gelte für alle p-Gruppen der Ordnung $< |A|$. In diesem Fall ist die maximale Ordnung eines Elements $a \in A$ und somit die Ordnung der von diesem a erzeugten zyklischen Gruppe $\langle a \rangle$ größer als 1. Nach dem Satz 3.2.1.4 von Lagrange muss $\operatorname{ord}(a) = p^k$ für ein $k > 0$ gelten, also $\langle a \rangle = C_{p^k}$. Wegen Lemma 3.3.4.1 gibt es ein $U \leq A$ mit $A = U \oplus \langle a \rangle$. Wegen $n = |A| = |U| \cdot |\langle a \rangle| > |U|$ ist auf U die Induktionsvoraussetzung anwendbar. Also ist U inneres direktes Produkt zyklischer p-Gruppen, somit auch $A = U \oplus \langle a \rangle$. Folglich ist A isomorph zu einer äußeren direkten Summe der kanonischen zyklischen p-Gruppen C_{p^n}.
Nun zur Eindeutigkeit: Die p-Komponenten A_p sind durch A eindeutig bestimmt. Wieder dürfen wir uns deshalb auf p-Gruppen für ein festes p beschränken. Wir führen Induktion nach der maximalen p-Potenz, die unter den Ordnungen der Elemente von A vorkommt. Wieder ist der Induktionsanfang (für die einelementige Gruppe) trivialerweise erfüllt. Sei also A eine endliche p-Gruppe. In einer Darstellung

$$A \cong \bigoplus_{n=1}^{\infty} C_{p^n}^{e_{p,n}}$$

sei n_0 das größte n mit $e_{p,n} > 0$. Es ist durch A deshalb eindeutig bestimmt, weil p^{n_0} die maximale Ordnung von Elementen $a \in A$ ist. Sei $U \leq A$ die von allen $a \in A$ mit maximaler Ordnung n_0 erzeugte Untergruppe. Aus obiger Darstellung liest man $|U| = (p^{n_0})^{e_{p,n_0}} = p^{n_0 e_{p,n_0}}$ ab. Wegen $n_0 > 0$ ist dadurch auch e_{p,n_0} eindeutig bestimmt. Die maximale p-Potenz von Elementen in A/U ist $< n_0$, also ist die Induktionsvoraussetzung auf diese Faktorgruppe

$$A/U \cong \bigoplus_{n=1}^{n_0-1} C_{p^n}^{e_{p,n}}$$

anwendbar, weshalb auch alle $e_{p,n}$ mit $n < n_0$ durch A eindeutig bestimmt sind. □

Es gilt ein analoger Satz unter allgemeineren Bedingungen: Schwächt man die Voraussetzung *endlich* an A ab zu *endlich erzeugt*, so tritt neben den endlichen zyklischen Gruppen auch noch die unendliche zyklische Gruppe $\mathbb{Z}$ als möglicher direkter Summand auf. Statt abelscher Gruppen, das heißt statt unitärer $\mathbb{Z}$-Moduln, kann man den gleichen Beweis auch für endlich erzeugte Moduln über beliebigen Hauptidealringen führen. Das werden wir in Algebra II, Abschnitt 7.4 tun.

UE 174 ► Übungsaufgabe 3.3.4.3. (F) Begründen Sie: **◄ UE 174**

(1) Die Gruppe C_{50} ist isomorph zum Produkt $C_{25} \times C_2$.

(2) Die Gruppe $C_2 \times C_{10}$ ist isomorph zu $C_2 \times C_2 \times C_5$.

(3) Die Gruppe $C_2^2 \times C_4^2 \times C_7^3$ ist isomorph zu $C_2 \times C_{14} \times C_{28} \times C_{28}$.

UE 175 ► Übungsaufgabe 3.3.4.4. (E) Beweisen Sie folgende Variante des Hauptsatzes 3.3.4.2: **◄ UE 175**
Jede endliche abelsche Gruppe A ist direkte Summe zyklischer Gruppen C_{m_i}, $i = 1, \ldots, n$ ($n \geq 1$), deren Ordnungen $m_i > 1$ eine Teilerkette $m_n | m_{n-1} | \ldots | m_2 | m_1$ bilden. Die m_i sind durch A eindeutig bestimmt. Hinweis: Nach Übungsaufgabe 3.3.2.13 bzw. als Konsequenz von Lemma 3.3.3.1 sind direkte Summen zyklischer Gruppen mit teilerfremden Ordnungen wieder zyklisch. Damit lässt sich die hier zu beweisende Variante ohne große Mühe aus dem Hauptsatz in der Version von 3.3.4.2 ableiten.

UE 176 ► Übungsaufgabe 3.3.4.5. (F) Geben Sie bis auf Isomorphie alle abelschen Gruppen an, deren Ordnung ein Teiler von 75 ist. (Das heißt: Geben Sie eine Liste von paarweise nichtisomorphen Gruppen an, sodass erstens die Ordnung jeder Gruppe Ihrer Liste ein Teiler von 75 ist, und sodass zweitens jede Gruppe, deren Ordnung ein Teiler von 75 ist, zu einer Gruppe auf Ihrer Liste isomorph ist. Anmerkung: Die Teiler von 75 sind 1, 3, 5, 15, 25, 75.) **◄ UE 176**

UE 177 ► Übungsaufgabe 3.3.4.6. (F) Sei p eine Primzahl. **◄ UE 177**

(1) Wie viele Untergruppen hat $C_p \times C_p$?

(2) Wie viele Untergruppen hat C_{p^2}?

(Hinweis: Überlegen Sie sich zuerst, dass alle nichttrivialen Untergruppen zyklisch sein müssen.)

UE 178 ▶ **Übungsaufgabe 3.3.4.7.** (F) Finden Sie zwei zueinander nicht isomorphe abelsche Gruppen der Ordnung 75, und bestimmen Sie für beide Gruppen und für jedes $d \in \{1, 3, 5, 15, 25, 75\}$ ◀ **UE 178**

(1) die Anzahl aller zyklischen Untergruppen der Ordnung d.

(2) die Anzahl aller nicht-zyklischen Untergruppen der Ordnung d.

(Hinweis: Es kann hilfreich sein, die Anzahl aller Elemente der Ordnung d zu bestimmen. In C_{15} gibt es 8 Elemente der Ordnung 15, in C_{75} gibt es 40 Elemente der Ordnung 75.)

UE 179 ▶ **Übungsaufgabe 3.3.4.8.** (A) Sei p eine Primzahl. Wie viele Automorphismen hat $C_p \times C_p$? (Hinweis: Verwenden Sie Ihr Wissen aus der Linearen Algebra.) ◀ **UE 179**

3.4. Ringe

Grundsätzlich verfolgen wir im Abschnitt über Ringe ein ähnliches Programm wie im Abschnitt 3.2 über Gruppen: Wir wollen erstens die allgemeinen Konzepte algebraischer Strukturanalyse aus Abschnitt 2.2 von beliebigen universellen Algebren so auf die speziellere Klasse der Ringe übertragen, dass schärfere Aussagen möglich werden, und zweitens diese an wichtigen Beispielen illustrieren. Neben starken Analogien (wie etwa jener zwischen Normalteilern und Idealen) verschieben sich allerdings bei manchen Aspekten die Gewichtungen, was sich auf die Struktur des Abschnitts auswirkt. Die meisten Ringe, mit denen wir uns beschäftigen werden, sind Ringe mit 1. Häufig spielt auch Kommutativität eine entscheidende Rolle.

Wir beginnen mit dem Studium von Kongruenzrelationen und den ihnen (analog zu den Normalteilern bei Gruppen) entsprechenden Idealen (3.4.1 für den allgemeinen und 3.4.2 für den kommutativen Fall mit 1). Wie schon bei den Gruppen spielt $\mathbb{Z}$ auch in der Kategorie der Ringe eine besondere Rolle. Sie hängt mit dem Konzept der Charakteristik eines Ringes mit 1 zusammen (3.4.3), zeigt sich aber auch an der wohlbekannten binomischen Formel (3.4.4). In 3.4.5 beschäftigen wir uns mit der (uneingeschränkt nur im Fall von Integritätsbereichen bestehenden) Möglichkeit, kommutative Ringe zu Körpern zu erweitern. Die neben $\mathbb{Z}$ und den darauf aufbauenden Zahlenbereichen wichtigsten Beispiele kommutativer Ringe werden von Polynomen und (formalen) Potenzreihen gebildet (3.4.6). Direkte Produkte spielen bei Ringen eine geringere Rolle als bei Gruppen. Von Bedeutung ist immerhin der Chinesische Restsatz (3.4.7). Als wichtigste Beispiele nichtkommutativer Ringe (3.4.8) schließlich sind Matrizenringe und Endomorphismenringe abelscher Gruppen und Moduln wenigstens zu erwähnen – insbesondere weil sie zu natürlichen Beispielen natürlicher Moduln über nichtkommutativen Ringen führen, nämlich abelschen Gruppen über ihren Endomorphismenringen.

3.4.1. Kongruenzrelationen und Ideale

Inhalt in Kurzfassung: Ideale spielen in der Ringtheorie die völlig analoge Rolle zu Normalteilern in der Gruppentheorie. Entsprechend folgt der vorliegende Unterabschnitt auch ganz analogen Gesichtspunkten wie jener aus der Gruppentheorie über Normalteiler. Betrachtet man einen Ring als Links- bzw. Rechtsmodul über sich selbst, so stößt man analog auf Links- bzw. Rechtsideale.

Obwohl wir schon in Unterabschnitt 1.2.3 zwangsläufig auf den Begriff des Ideals gestoßen sind, wollen wir das Thema Kongruenzrelationen und Homomorphismen auf Ringen nochmals systematisch aufrollen und unter den zusätzlichen, teils allgemeineren Gesichtspunkten beleuchten, die mit denen wir nunmehr vertraut sind. Dabei ist es zielführend, sich am Beispiel der Gruppen zu orientieren (siehe Unterabschnitt 3.2.2). Denn jede Kongruenzrelation $\sim$ auf einem Ring R ist insbesondere auch eine Kongruenzrelation auf der additiven Gruppe von R, wird also eindeutig durch die Klasse $[0]_\sim$ von $0 \in R$ bestimmt. Folglich muss $\sim$ erst recht als Kongruenzrelation des Ringes durch $I := [0]_\sim$ eindeutig bestimmt sein. Die Klasse eines beliebigen Elements $x \in R$ ist von der Form $[x]_\sim = x + I$.

Definition 3.4.1.1. Eine Teilmenge I eines Ringes R heißt *Ideal* von R, symbolisch $I \lhd R$, wenn es eine Kongruenzrelation $\sim$ auf R gibt mit $I := [0]_\sim$ (was nach dem allgemeinen Homomorphiesatz 2.2.3.17 gleichbedeutend damit ist, dass es einen Ringhomomorphismus gibt, dessen Kern I ist).
Die Kongruenzklasse $[x]_\sim = x + I$ von $x \in R$ heißt auch *Nebenklasse* von x modulo I. Im Fall $x + I = y + I$ (d. h. $x \sim y$) schreibt man auch $x \equiv y \pmod{I}$.

Anmerkung 3.4.1.2. Die gerade eingeführte Notation harmoniert mit derjenigen aus Definition 3.2.4.6: für ganze Zahlen a, b könnten wir statt $a \equiv b \pmod{m}$ genauso auch $a \equiv b \pmod{m\mathbb{Z}}$ schreiben.

Die Ideale in Ringen spielen folglich eine völlig analoge Rolle zu den Normalteilern in Gruppen:

Proposition 3.4.1.3. *Zwischen der Menge der Kongruenzrelationen $\sim$ eines Ringes R und der Menge der Ideale I von R wird durch die Relation $I = [0]_\sim$ eine Bijektion hergestellt. Dabei handelt es sich sogar um einen Isomorphismus zwischen den jeweils durch $\subseteq$ geordneten Verbänden aller Kongruenzrelationen bzw. aller Ideale von R.*

Wie bei Gruppen schreiben wir R/I für den Faktorring $R/_\sim$, wenn $\sim$ die Kongruenzrelation mit $I = [0]_\sim$ ist. Den trivialen Kongruenzrelationen auf R entsprechen dabei die *trivialen Ideale*: R (für die Allrelation) und $\{0\}$ (für die identische Relation). Der Ring R/R hat nur ein Element, während $R/\{0\}$ zu R isomorph ist (der kanonische Homomorphismus ist ein Isomorphismus). Weiter analog zu den Gruppen führt die allgemeine Definition 2.2.3.14 einer einfachen Algebra bei Ringen zu:

Folgerung 3.4.1.4. *Ein Ring R ist genau dann einfach, wenn R und $\{0\}$ die einzigen Ideale von R sind.*

Jedes Ideal I ist ein Normalteiler der additiven Gruppe von R, was wegen der Kommutativität von $+$ gleichbedeutend damit ist, dass I eine additive Untergruppe von R ist. Weil diese Bedingung keinerlei Rücksicht auf die multiplikative Struktur von R nimmt, dürfen wir nicht erwarten, dass umgekehrt jede additive Untergruppe von R schon einer Kongruenzrelation der Ringes entspricht. Tatsächlich muss, anders als für beliebige additive Untergruppen, für alle $r \in R$ zum Beispiel $rI \subseteq I$ und $Ir \subseteq I$ gelten: Denn für die I entsprechende Kongruenzrelation $\sim$ und $i \in I$ gilt ja $ri \sim r0 = 0$, also $ri \in I$ und analog $ir \in I$.[16] Bemerkenswert ist, dass diese zusätzliche Eigenschaft bereits ausreicht, um Ideale zu charakterisieren.

Satz 3.4.1.5. *Sei R ein Ring und $I \subseteq R$. Dann sind die folgenden Aussagen äquivalent:*

(1) *I ist ein Ideal. (Definitionsgemäß heißt das, dass es eine Kongruenzrelation $\sim$ auf R mit $I = [0]_\sim$ gibt.)*

(1′) *Es gibt genau eine Kongruenzrelation $\sim$ auf R mit $I = [0]_\sim$.*

(2) *Es gibt einen Ring S und einen (surjektiven) Homomorphismus $\varphi\colon R \to S$ mit $I = \varphi^{-1}(\{0_S\})$.*

(3) *I ist eine additive Untergruppe von R mit $rI, Ir \subseteq I$ für alle $r \in R$ (folglich $RI, IR \subseteq I$).*

Beweis. Aufgrund der vorangegangenen Überlegungen dürfen wir uns auf den Nachweis der einzig noch ausstehenden Implikation beschränken, nämlich auf den Schritt von (3) nach (1):
Wenn I die Bedingung (3) erfüllt, dann definieren wir eine Relation $\sim_I$ durch $x \sim_I y \ :\Leftrightarrow\ x - y \in I$. Weil I als Untergruppe auch ein Normalteiler der kommutativen additiven Gruppe auf R, ist $\sim_I$ auf dieser eine Kongruenzrelation. Wie folgende Schlusskette zeigt, ist $\sim_I$ aber auch mit der Multiplikation verträglich:

$$\begin{aligned} x \sim_I x',\, y \sim_I y' \ &\Rightarrow\ (x - x'),\, (y - y') \in I \\ &\Rightarrow\ (x - x')y',\, x(y - y') \in I \\ &\Rightarrow\ xy - x'y' = x(y - y') + (x - x')y' \in I \\ &\Rightarrow\ xy \sim_I x'y'. \end{aligned}$$

Also ist $\sim_I$ eine Kongruenzrelation. Aus $x \sim_I 0 \Leftrightarrow x - 0 \in I$ folgt $I = [0]_\sim$. □

UE 180 ► **Übungsaufgabe 3.4.1.6.** (B) Geben Sie ein Beispiel eines kommutativen Rings R und eines Unterrings $U \leq R$ an, der *kein* Ideal ist. ◄ **UE 180**

Analog zu den Normalteilern einer Gruppe (siehe Folgerung 3.2.2.8) bilden auch die Ideale eines Ringes wegen Proposition 3.4.1.3 einen vollständigen Verband mit dem mengentheoretischen Schnitt als Infimum. Auch das Supremum einer Menge von Idealen (definitionsgemäß der Schnitt aller diese umfassenden Ideale) lässt sich recht leicht beschreiben:

[16] In beliebigen Ringen R gilt $r0 = 0r = 0$ für alle $r \in R$: Aus $r0 = r(0+0) = r0 + r0$ folgt nach Addition von $-r0$ sofort $r0 = 0$, analog $0r = 0$; siehe auch die Fußnote auf Seite 184.

Proposition 3.4.1.7. *Sei R ein Ring mit* 1 *und $A \subseteq R$. Bezeichne I den Schnitt aller Ideale $J \lhd R$ mit $A \subseteq J$. (I ist also das kleinste A umfassende Ideal in R, genannt das von A* erzeugte Ideal*, symbolisch $I = (A)$, im Fall $A = \{a_1, \ldots, a_n\}$ auch $I = (a_1, \ldots, a_n)$.) Dann gilt:*

(1) *I ist die Menge aller*

$$\sum_{i=1}^{n} r_i a_i s_i + \sum_{j=1}^{m'} r'_j b_j + \sum_{k=1}^{n'} c_k s'_k + \sum_{l=1}^{N} d_l$$

mit $n, m', n', N \in \mathbb{N}$, $a_i, b_j, c_k, d_l \in A$ und $r_i, s_i, r'_j, s'_k \in R$.

(2) *Hat R ein Einselement, so ist I auch darstellbar als die Menge aller*

$$\sum_{i=1}^{n} r_i a_i s_i$$

mit $n \in \mathbb{N}$, $a_i \in A$ und $r_i, s_i \in R$.

(3) *Ist R kommutativ mit* 1*, so ist I darstellbar als die Menge aller Summen (Linearkombinationen)*

$$\sum_{i=1}^{n} r_i a_i$$

mit $n \in \mathbb{N}$, $a_i \in A$ und $r_i \in R$. Ist speziell $A = \{a\}$ einelementig, so ist

$$I = (a) = \{ra \mid r \in R\}.$$

UE 181 ► Übungsaufgabe 3.4.1.8. (V) Beweisen Sie Proposition 3.4.1.7. **◄ UE 181**

Die Idealbedingung $rI \subseteq I$ ist eine Verschärfung der Abgeschlossenheit von I bezüglich der Multiplikation. Ideale sind also insbesondere Unterringe. Diese Sichtweise ist allerdings nicht nur wegen Übungsaufgabe 3.4.1.6 problematisch, sondern vor allem weil sie falsch wird, wenn man Ringe R mit 1 als 0-stelliger Operation betrachtet. Denn jede Unteralgebra eines Ringes mit 1 muss selbst 1 enthalten, was im Falle eines Ideals I mit $1 \in I$ wegen $R = R1 \subseteq RI \subseteq I \subseteq R$ nur für das triviale Ideal $I = R$ möglich ist. Also:

Proposition 3.4.1.9. *Ist R ein Ring mit* 1 *und $I \lhd R$, so gilt $1 \in I$ genau dann, wenn $I = R$.*

Unteralgebren sind Ideale I allerdings dann, wenn man R als Links- bzw. Rechts-Modul über sich selbst auffasst (mit den Operationen $\omega_r(a) := ra$ bzw. $\tilde{\omega}_r(a) := ar$ für $r \in R$). Über nichtkommutativen Ringen ist dafür nicht die volle Idealeigenschaft erforderlich. Deshalb spielen dort auch Links- und Rechtsideale eine wichtige Rolle.

Definition 3.4.1.10. Eine Teilmenge I eines Rings R heißt *Linksideal*, wenn I additive Untergruppe von R ist und abgeschlossen ist bezüglich der Multiplikation mit beliebigen Ringelementen von links: $rI \subseteq I$ für alle $r \in R$. *Rechtsideale* sind analog definiert mit Multiplikation von rechts ($Ir \subseteq I$ für alle $r \in R$) statt von links.

UE 182 ▶ **Übungsaufgabe 3.4.1.11.** (B) Geben Sie ein Beispiel eines Rings und eines Linksideals I an, sodass I kein Ideal ist. (Hinweis: Matrizen.) ◀ **UE 182**

Sehr leicht überprüft man:

Proposition 3.4.1.12. *Sind $I, J \lhd R$ Ideale von R, dann auch die Komplexsumme $I + J := \{i + j \mid i \in I, j \in J\}$. Dabei gilt $I + J = (I \cup J) = \sup\{I, J\}$, wobei das Supremum im Idealverband zu verstehen ist.*

UE 183 ▶ **Übungsaufgabe 3.4.1.13.** (V) Beweisen Sie Proposition 3.4.1.12. ◀ **UE 183**

Definition 3.4.1.14. Ein Ideal $I \lhd R$ eines Ringes R heißt *Hauptideal*[17], wenn I von einem Element erzeugt wird, d. h. $\exists a \in I : I = (a)$.
Ein Integritätsbereich, dessen sämtliche Ideale Hauptideale sind, heißt *Hauptidealring*[18].

Das Paradebeispiel eines Hauptidealringes ist $\mathbb{Z}$: Als Ideale kommen nur die uns bereits aus Proposition 3.2.4.1 bekannten additiven Untergruppen $m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$ in Frage. Offenbar sind diese Mengen auch bezüglich der Multiplikation mit beliebigen ganzen Zahlen abgeschlossen, sind also Ideale. Jede dieser Mengen $m\mathbb{Z}$ wird von einem einzigen Element erzeugt, nämlich von m (oder auch von $-m$).

Definition 3.4.1.15. Für $m \in \mathbb{N}$ definieren wir den *Restklassenring* von $\mathbb{Z}$ modulo m durch[19] $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$.

Proposition 3.4.1.16. *Sämtliche Faktorringe (und somit bis auf Isomorphie auch alle homomorphen Bilder) von $\mathbb{Z}$ sind gegeben durch die Restklassenringe $\mathbb{Z}_m$, $m \in \mathbb{N}$.*

UE 184 ▶ **Übungsaufgabe 3.4.1.17.** (F,B) Zeigen Sie: Ist R ein Hauptidealring und $J \lhd R/I$, so ist J ein Hauptideal. Trotzdem muss R/I kein Hauptidealring sein. ◀ **UE 184**

Hauptidealringe werden uns im Rahmen der Teilbarkeitslehre noch intensiv beschäftigen. Die Ringe $\mathbb{Z}_m$ entsprechen für $m > 0$ dem Rechnen modulo m, wobei die additive Struktur die uns bereits bekannte zyklische Gruppe C_m ist. Weil alle Untergruppen (sprich Normalteiler) von $\mathbb{Z}$ Ideale sind, entspricht der Kongruenz- (= Ideal-) Verband auch des *Ringes* $\mathbb{Z}$ der umgekehrten Teilbarkeitsrelation auf $\mathbb{N}$, siehe Satz 3.2.4.15.
Im Vergleich zu beliebigen Ringen rücken bei kommutativen Ringen mit 1 zahlreiche weitere Besonderheiten ins Zentrum des Interesses.

[17] englisch: *principal ideal (Achtung! „principal“, nicht „principle“)*
[18] englisch: *principal ideal domain*
[19] Siehe auch Beispiel 2.2.3.21.

3.4.2. Ideale in kommutativen Ringen mit 1

Inhalt in Kurzfassung: Unter den kommutativen Ringen mit 1 spielen die Integritätsbereiche und Körper eine besondere Rolle. Diese ergeben sich durch Faktorisierung nach Prim- bzw. maximalen Idealen. Im endlichen Fall ist jeder Integritätsbereich sogar ein Körper. Generell sind Körper unter den kommutativen Ringen mit 1 genau die einfachen (die also nur die trivialen Ideale enthalten).

Sei R ein kommutativer Ring mit 1 und $I \lhd R$ ein Ideal. Wir fragen uns, unter welchen Bedingungen R/I ein Integritätsbereich oder gar ein Körper ist. Nicht überraschend lässt sich das durch Eigenschaften von I charakterisieren. Doch zunächst eine einfache Beobachtung.

Satz 3.4.2.1. *Jeder endliche Integritätsbereich ist ein Körper.*

Beweis. Sei R ein Integritätsbereich und $r \in R \setminus \{0_R\}$. Wir betrachten die Abbildung $m_r \colon R \to R$, $x \mapsto rx$. Aus $rx = ry$ folgt wegen der Kürzungsregel in Integritätsbereichen $x = y$. Also ist m_r injektiv. Weil R endlich ist, muss m_r auch surjektiv sein. Somit gibt es ein $x_r \in R$ mit $rx_r = m_r(x_r) = 1_R$, und x_r ist ein multiplikatives Inverses von r. □

In Hinblick auf unsere Ausgangsfrage betreffend Körper ist die folgende Beobachtung nützlich.

Proposition 3.4.2.2. *Ein kommutativer Ring R mit $1_R \neq 0_R$ ist genau dann ein Körper, wenn er einfach ist (d. h. definitionsgemäß, wenn R nur die trivialen Kongruenzrelationen und somit nur die trivialen Ideale hat). Äquivalent: R ist genau dann ein Körper, wenn jeder Ringhomomorphismus $R \to S$ in irgendeinen Ring S entweder injektiv oder konstant ist (in zweiterem Fall muss S der triviale Ring sein, also $1_S = 0_S$ gelten).*

Beweis. Sei zunächst R ein Körper und $I \lhd R$ ein Ideal mit $I \neq \{0_R\}$, d. h. $i \in I$ für ein $i \neq 0_R$. Es genügt zu zeigen, dass daraus $R \subseteq I$ folgt. Weil R ein Körper ist, hat i ein Inverses $i^{-1} \in R$. Weil I ein Ideal ist, liegt somit auch das Element $1_R = i^{-1}i$ in I und die Aussage folgt aus Proposition 3.4.1.9.
Sei nun umgekehrt R einfach. Zu einem beliebigem $r \in R \setminus \{0_R\}$ müssen wir ein multiplikatives Inverses in R finden. Weil R einfach ist, muss jedes Ideal I, in dem das Element r liegt, schon ganz R sein. Insbesondere muss das von r erzeugte Ideal $I_r = \{sr \mid s \in R\}$ (Proposition 3.4.1.7) das Einselement 1_R enthalten. Also gibt es ein $s \in R$ mit $1_R = sr$. Dieses $s \in R$ ist das gesuchte Inverse von r. □

Wir gehen nun von irgendeinem kommutativen Ring R mit Einselement und einem Ideal $I \lhd R$ aus. Nach dem zweiten Isomorphiesatz 2.2.6.7 ist der Kongruenz- und somit der Idealverband von R/I isomorph zum Verband der Ideale $J \lhd R$ mit $I \subseteq J$. Gemäß Proposition 3.4.2.2 ist R/I also genau dann ein Körper, wenn es zwischen I und R keine weiteren Ideale gibt. Solche Ideale nennt man *maximal*.
Ähnlich einfach zu verstehen ist, wann R/I ein Integritätsbereich ist. Denn die Integritätsbereiche definierende Nullteilerfreiheit liegt im Faktorring R/I genau dann vor, wenn das Produkt $(a + I)(b + I) = ab + I$ zweier Nebenklassen $a + I$ und $b + I$ nur dann

wieder I ist, wenn schon $a + I = I$ oder $b + I = I$ gilt. Anders ausgedrückt: Wenn aus $ab \in I$ folgt, dass $a \in I$ oder $b \in I$. Ein Ideal I mit diesen Eigenschaften nennt man ein *Primideal*.
Die allgemeinen Definitionen lauten also:

Definition 3.4.2.3. Sei R ein Ring und $I \lhd R$ ein Ideal in R. Dann sagt man:

(1) I ist ein *echtes Ideal*, wenn $I \neq R$.

(2) I ist ein *maximales Ideal*, wenn I ein echtes Ideal ist und jedes Ideal $J \lhd R$ mit $I \subseteq J$ entweder $J = I$ oder $J = R$ erfüllt. (Mit anderen Worten: Wenn I ein maximales Element in der partiellen Ordnung aller echten Ideale ist; Ideale sind hier durch die Inklusionsrelation $\subseteq$ partiell geordnet.)

(3) I ist ein *Primideal*, wenn I ein echtes Ideal ist und für $a, b \in R$ aus $ab \in I$ stets $a \in I$ oder $b \in I$ folgt.

Wir fassen unsere obigen Überlegungen zusammen und ergänzen sie zu folgendem Satz:

Satz 3.4.2.4. *Sei R ein kommutativer Ring mit Einselement $1_R \in R$ und $I \lhd R$ ein Ideal. Dann gilt:*

(1) *I ist genau dann ein echtes Ideal, wenn $1_R \notin I$.*

(2) *R/I ist genau dann ein Körper, wenn I ein maximales Ideal ist.*

(3) *R/I ist genau dann ein Integritätsbereich, wenn I ein Primideal ist.*

(4) *Jedes maximale Ideal ist ein Primideal.*

(5) *Ist I ein echtes Ideal, so gibt es ein maximales (und somit Prim-) Ideal $J \lhd R$ mit $I \subseteq J$.*

(6) *Ist $R \neq \{0_R\}$, so gibt es ein maximales Ideal in R.*

Beweis. Die erste Aussage ist eine Umformulierung von Proposition 3.4.1.9, hier für kommutative Ringe. Die zweite und dritte Behauptung ergeben sich aus den Überlegungen, die Definition 3.4.2.3 vorangegangen sind. Die vierte Behauptung folgt aus der zweiten und dritten, weil jeder Körper ein Integritätsbereich ist.
Der Beweis der fünften Behauptung erfolgt in typischer Weise mit Hilfe das Lemmas von Zorn (siehe Anhang, A.4.2.4). Das System $\mathcal{S}$ aller echten Ideale $J \lhd R$ mit $I \subseteq J$ ist wegen $I \in \mathcal{S}$ nicht leer und bezüglich $\subseteq$ halbgeordnet. Man überzeugt sich unmittelbar davon, dass die Vereinigung V einer $\subseteq$-Kette von Idealen wieder ein Ideal ist. Weil alle $J \in \mathcal{S}$ echte Ideale sind, enthält (erste Behauptung) keines davon 1_R, also auch $1_R \notin V$. Somit sind die Voraussetzungen des Lemmas von Zorn erfüllt. Folglich gibt es ein $\subseteq$-maximales Element $J \in \mathcal{S}$. Dieses ist offenbar ein maximales Ideal mit $I \subseteq J$, wie behauptet.
Besteht R nicht nur aus 0_R, so ist $I := \{0_R\}$ ein echtes Ideal, auf das die fünfte Aussage angewendet werden kann. Damit ist auch die sechste Aussage bewiesen. □

Bereits an dieser Stelle sei bemerkt, dass nicht jedes Primideal maximal ist – darauf werden wir in Übungsaufgabe 3.4.6.10 zurückkommen, sobald wir mehr Beispiele zur Verfügung haben.

3.4.3. Charakteristik

Inhalt in Kurzfassung: So wie $\mathbb{Z}$ haben auch alle endlichen zyklische Gruppen mit Ordnungen $n \in \mathbb{N}^+$ neben der additiven auch eine multiplikative Struktur, die sie zu kommutativen Ringen mit 1 machen. Jeder kommutative Ring mit 1 enthält die Kopie genau eines dieser Ringe als Unteralgebra. Ist dies $\mathbb{Z}$, so definiert man die Charakteristik des Ringes als 0, sonst als das entsprechende n. Dies drückt sich auch dadurch aus, dass $\mathbb{Z}$ ein initiales Objekt in der Kategorie der kommutativen Ringe mit 1 ist. Die Charakteristik eines Integritätsbereichs ist stets entweder 0 oder eine Primzahl.

In Unterabschnitt 3.2.4 haben wir gesehen, dass für jedes Element g einer Gruppe G die Abbildung $\varphi : k \mapsto kg$ (additive Notation) ein Gruppenhomomorphismus $\varphi\colon \mathbb{Z} \to G$ ist. Ersetzen wir G durch einen Ring mit 1 und betrachten $g = 1$, so gilt, wie man leicht überprüft, sogar:

Proposition 3.4.3.1. *Sei R ein Ring mit Einselement 1_R. Dann ist die Abbildung*

$$\varphi\colon \mathbb{Z} \to R, \quad k \mapsto k_R := k1_R$$

ein Ringhomomorphismus. $\mathbb{Z}$ ist sogar ein initiales Objekt in der Kategorie der Ringe mit 1.

UE 185 ► Übungsaufgabe 3.4.3.2. (V) Beweisen Sie Proposition 3.4.3.1. **◄ UE 185**

Der Kern von φ aus 3.4.3.1 ist ein Ideal von $\mathbb{Z}$, also nach Proposition 3.4.1.16 gleich $m\mathbb{Z}$ für ein $m \in \mathbb{N}$. Das Bild $\varphi(\mathbb{Z})$ ist offenbar der kleinste Unterring von R mit 1 und nach dem Homomorphiesatz isomorph zu $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$. Jeder Ring mit 1 enthält als kleinsten Unterring folglich eine isomorphe Kopie entweder von $\mathbb{Z}$ (falls $m = 0$) oder vom Restklassenring $\mathbb{Z}_m$. Die Zahl m heißt auch die *Charakteristik* von R. Da der Erzeuger m des Ideals $m\mathbb{Z}$ im Fall $m \neq 0$ daran zu erkennen ist, dass er das kleinste positive Element des Ideals ist, können wir die Charakteristik auch expliziter fassen:

Definition 3.4.3.3. Sei R ein Ring mit Einselement 1_R. Wenn es eine positive Zahl $m \geq 1$ gibt mit

$$m1 = \underbrace{1_R + \cdots + 1_R}_{m\text{-fach}} = 0,$$

dann heißt das kleinste derartige m die *Charakteristik* von R, symbolisch $\operatorname{char} R = m$. Wenn es kein positives m mit dieser Eigenschaft gibt, dann sagen wir, dass R die Charakteristik 0 hat, $\operatorname{char} R = 0$.

Ist $m > 0$, so stimmt m genau mit der additiven Ordnung von 1_R überein. Klarerweise ist $\operatorname{char} \mathbb{Z}_m = m$ $(m \in \mathbb{N})$ und $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.
Wir ziehen nun Satz 3.4.2.4 zu Rate, wonach $\mathbb{Z}_m$ genau dann ein Körper ist, wenn $m\mathbb{Z}$ ein maximales Ideal von $\mathbb{Z}$ ist. Weil $m\mathbb{Z} \subseteq n\mathbb{Z}$ genau für $n|m$ gilt, ist folglich $\mathbb{Z}_m$ genau dann ein Körper, wenn m außer 1 keine echten Teiler in $\mathbb{N}$ hat, wenn also $m = p$ eine Primzahl

ist. Ist $m \in \mathbb{N}$ hingegen keine Primzahl, so sind drei Möglichkeiten zu unterscheiden: $\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \cong \mathbb{Z}$ ist ein Integritätsbereich, $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} \cong \{0\}$ ist einelementig. Ist jedoch $m = ab$ mit $1 < a, b < m$ zusammengesetzt, so sind $a_R \neq 0_R \neq b_R$ wegen $a_R b_R = m_R = \varphi(m) = 0_R$ Nullteiler. Wir fassen zusammen:

Satz 3.4.3.4. *Für die Restklassenringe $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{N}$, sind folgende vier Fälle zu unterscheiden:*

1. *Für $m = p \in \mathbb{P}$ ist $\mathbb{Z}_m = \mathbb{Z}_p$ ein endlicher Körper.*
2. *Für eine zusammengesetzte Zahl $m > 1$ ist $\mathbb{Z}_m$ ein endlicher Ring mit Nullteilern (also weder Integritätsbereich noch Körper).*
3. *Für $m = 0$ ist $\mathbb{Z}_m = \mathbb{Z}_0 \cong \mathbb{Z}$ ein Integritätsbereich, aber kein Körper.*
4. *Für $m = 1$ ist $\mathbb{Z}_m = \mathbb{Z}_1 \cong \{0\}$ ein trivialer, einelementiger Ring (also weder Integritätsbereich noch Körper).*

Schreibweise 3.4.3.5. Oft werden wir in der Notation weniger genau sein: Für das Element $n_R := n \cdot 1_R = n1_R \in R$ schreiben wir meistens nur n. Der Kontext[20] entscheidet, ob etwa mit „3“ die natürliche Zahl 3 gemeint ist, oder das Ringelement $3_R := 1_R + 1_R + 1_R$. Man beachte, dass die natürliche Zahl 3 verschieden von der Zahl 0 ist, aber das Ringelement 3_R durchaus gleich dem Nullelement $0_R \in R$ sein kann, nämlich wenn $\operatorname{char} R = 3$.

3.4.4. Die binomische Formel

Inhalt in Kurzfassung: Die aus der elementaren Arithmetik bekannte binomische Formel für die Potenz einer Summe gilt allgemeiner in beliebigen kommutativen Ringen mit 1. Besonders einfache Gestalt nimmt diese Formel an, wenn die Charakteristik des Ringes eine Primzahl ist und der Exponent eine Potenz dieser Primzahl. In diesem Fall ist das Potenzieren nämlich ein Homomorphismus nicht nur bezüglich der Multiplikation, sondern auch bezüglich der Addition. Dies wird in der Theorie endlicher Körper noch eine wichtige Rolle spielen.

Vor allem bei Körpern ist der Unterschied zwischen Charakteristik 0 und Primzahlcharakteristik sehr häufig gravierend. Ein Beispiel dafür bereiten wir mit dem schon aus der Elementarmathematik bekannten und auch für die Analysis wichtigen[21] *binomischen Lehrsatz* (oder auch *binomische Formel*) vor:

[20] Achtung! Der Exponent der Unbestimmten in einem Polynom wird immer als natürliche Zahl interpretiert. So ist etwa im Polynom $2x^3$ die Zahl 2 Abkürzung für $1_R + 1_R$ („+“ ist hier die Ringaddition), während mit „3“ tatsächlich die natürliche Zahl gemeint ist. Formal ist dieses Polynom ja eine Potenzreihe $0 + 0x + 0x^2 + 2x^3 + 0x^4 + \cdots$, also ganz formal die Folge $(0_R, 0_R, 0_R, 2_R, 0_R, \ldots)$; die Zahl 3 kommt hier nur als Index des Elements $2_R = 1_R + 1_R$ vor, also sicher nicht als Ringelement.
Daher: Wenn zum Beispiel $\operatorname{char}(R) = 2$ ist, dann gilt zwar $2_R x = x + x = (1_R + 1_R)x = 0$, aber $x \cdot x = x^2 \neq x^0 = 1_R$.

[21] Man denke beispielsweise an die Herleitung von $\exp(a + b) = \exp(a)\exp(b)$ über das Cauchyprodukt zweier Exponentialreihen.

Satz 3.4.4.1. *Sei R ein Ring mit 1, $a, b \in R$, $ab = ba$ und $n \in \mathbb{N}$. Dann gilt*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Dabei sind die sogenannten Binomialkoeffizienten $\binom{n}{i} := \frac{n!}{i!(n-i)!}$ *(mit durch* $0! := 1$, $(n+1)! := (n+1)n!$ *rekursiv definierten Zahlen* $n!$*, sprich* n faktorielle *oder* n Fakultät*) stets natürliche Zahlen, weshalb die Summe rechts ein wohldefiniertes Element in R darstellt.*

UE 186 ▶ **Übungsaufgabe 3.4.4.2.** (V,W) Beweisen Sie den binomischen Lehrsatz auf zwei Arten: ◀ **UE 186**

1. Mittels Induktion nach n. Hinweis: Dazu ist eine Identität für Binomialkoeffizienten erforderlich, die Sie gleichfalls beweisen müssen.
2. Durch kombinatorische Deutung. (Welche Objekte zählt ein Binomialkoeffizient?)

Damit ergibt sich leicht:

Satz 3.4.4.3. *Sei $(R, +, 0, -, \cdot, 1)$ ein kommutativer Ring mit 1 und sei* $\operatorname{char} R = p \in \mathbb{P}$*. Dann ist die Abbildung $\varphi : R \to R$, $\varphi(x) := x^p$ ein Homomorphismus, d. h., es gilt*

$$(a+b)^p = a^p + b^p$$

für alle $a, b \in R$. Allgemeiner sind für $k \in \mathbb{N}$ die Abbildungen $\varphi_k : R \to R$, $\varphi_k(x) := x^{p^k}$ Homomorphismen, d. h., es gilt

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

für alle $a, b \in R$.

Beweis. Wir betrachten zunächst $\varphi = \varphi_1$. In Satz 3.4.4.1 hat man lediglich zu beachten, dass für $0 < i < p$ der Binomialkoeffizient $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdots i} \in \mathbb{Z}$ nicht nur ganzzahlig ist, sondern einen Faktor p im Zähler, nicht aber im Nenner hat, also durch p teilbar ist (hier geht ein, dass p prim ist). Wegen $\operatorname{char} R = p$ fallen deshalb die Summanden für diese i weg. Für $i = 0$ und $i = p$ ist hingegen $\binom{p}{i} = 1$, weshalb nur die Summanden b^p und a^p übrig bleiben. Damit ist die Behauptung, für diesen Fall bewiesen.
Für die zweite Behauptung ist nur mit Induktion nach k zu beweisen, dass $\varphi_k = \varphi^k$ gilt (k-fache Anwendung von φ hintereinander, d. h. $\varphi_k = \underbrace{\varphi \circ \cdots \circ \varphi}_{k}$). □

Zum Abschluss des Unterabschnitts ein Ausblick auf endliche Körper:

UE 187 ▶ **Übungsaufgabe 3.4.4.4.** (F+) Man zeige: Ist K ein endlicher Körper der Charakteristik $p \in \mathbb{P}$, dann sind die Abbildungen φ_k aus der Formulierung von Satz 3.4.4.3 Automorphismen von K, die sogenannten *Frobeniusautomorphismen* (siehe auch Satz 6.3.3.6). ◀ **UE 187**

3.4.5. Quotientenkörper

Inhalt in Kurzfassung: Wendet man die Konstruktion der Quotientengruppe aus einem Monoid auf die multiplikative Struktur eines Integritätsbereichs an, so entspricht dies dem Übergang von ganzen Zahlen zu Brüchen. So wie dort (d. h. beim elementaren Bruchrechnen) kann auch im allgemeinen Fall die additive Struktur ebenfalls ausgedehnt werden. Wir konzentrieren uns hauptsächlich auf kommutative Ringe mit 1 und erhalten einen Körper (den Quotientenkörper). Auch die Beschränkung auf kürzbare multiplikative Teilmengen als zugelassene „Nenner“ ist möglich. Die abstrakte Definition der resultierenden Objekts erfolgt als initiales Objekt in einer geeigneten Kategorie, legt die Struktur daher bis auf Äquivalenz (insbesondere also bis auf Isomorphie) eindeutig fest.

In Analogie zur bzw. gestützt auf die Konstruktion des Quotientenmonoids eines Monoids bezüglich eines Untermonoids (siehe Unterabschnitt 3.1.4) wollen wir nun einen Ring R mit 1 so erweitern, dass gewisse Elemente multiplikative Inverse bekommen. Sofern sich dies als möglich erweist, ist der Weg durch die Konstruktion des Quotientenmonoids aus besagtem Unterabschnitt 3.1.4, angewendet auf die multiplikative Halbgruppe des Ringes, vorgezeichnet. Dieser Ansatz wird tatsächlich zum Erfolg führen, weil sich die bei der Konstruktion auftretende Faktorisierung auch mit der additiven Struktur verträgt.

Um das Programm im Detail durchzuführen, analysieren wir zunächst die erforderliche multiplikative Kürzbarkeit im Kontext der Ringstruktur. Um langweilige Fallunterscheidungen zu vermeiden, setzen wir $1 \neq 0$ voraus, was äquivalent ist zu $|R| \geq 2$. Soll $r \in R$ in einer Erweiterung von R ein Inverses r^{-1} haben, so kann r kein *Nullteiler* sein, weil aus $rs = 0$ sofort $s = 1s = (r^{-1}r)s = r^{-1}(rs) = r^{-1}0 = 0$ folgt. Umgekehrt sind Nichtnullteiler r stets kürzbar: Aus $xr = yr$ folgt $(x - y)r = 0$, also $x - y = 0$ wenn r kein Nullteiler ist, d. h. $x = y$. Wir müssen unsere Ambitionen also auf Nichtnullteiler beschränken; wünschen wir uns, dass jedes Element des Rings ungleich 0 ein Inverses bekommt, so müssen wir von einem Integritätsbereich ausgehen. In diesem Fall werden wir einen Körper (den Quotientenkörper) erhalten. Präziser (und allgemeiner) sind wir interessiert an Quotientenringen im Sinne der folgenden Definition.

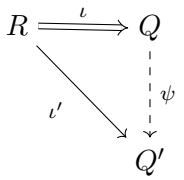
Definition 3.4.5.1. Sei R ein kommutativer Ring mit 1 und K ein kürzbares multiplikatives Untermonoid von R. Dann heißt Q zusammen mit $\iota\colon R \to Q$ ein *Quotientenring* oder auch *Bruchring* von R bezüglich K, wenn folgendes gilt:

(1) Q ist ein kommutativer Ring mit 1.

(2) Die Abbildung $\iota\colon R \to Q$ ist eine isomorphe Einbettung von R als Ring mit 1 in Q.

(3) Jedes Element $\iota(r)$ mit $r \in K$ hat in Q ein multiplikatives Inverses.

(4) Ist Q' irgendein anderer kommutativer Ring mit Einselement mit einer isomorphen Einbettung $\iota'\colon R \to Q'$ derart, dass jedes $\iota'(r)$ mit $r \in K$ ein multiplikatives Inverses in Q' hat, so gibt es eine eindeutige isomorphe Einbettung $\psi\colon Q \to Q'$ von Q als Ring mit Einselement in Q', sodass $\iota' = \psi \circ \iota$.



Ist R ein Integritätsbereich und $K = R^* = R \setminus \{0\}$, so heißt der Quotientenkörper von R bezüglich K zusammen mit ι auch *Quotientenkörper* von R.

Statt wie in Definition 3.4.5.1 lässt sich ein Quotientenring bzw. -körper bei vorgegebenem R und K auch als initiales Objekt in einer geeigneten Kategorie $\mathcal{C} = \mathcal{C}(R, K)$ definieren. Die Objekte sind alle kommutativen Ringe zusammen mit Einbettungen ι mit den ersten drei Eigenschaften aus 3.4.5.1. Die Morphismen sind Abbildungen φ wie in der vierten Eigenschaft. Dann folgt aus Satz 2.3.3.2:

Folgerung 3.4.5.2. *Quotientenringe (insbesondere auch Quotientenkörper) sind bis auf Isomorphie eindeutig bestimmt.*

UE 188 ► Übungsaufgabe 3.4.5.3. (V) Führen Sie die Begründung von Folgerung 3.4.5.2 im Detail aus. **◄ UE 188**

Wir wollen zeigen, dass ein Quotientenring stets existiert. Die Konstruktion des Quotientenmonoids des multiplikativen Monoids von R bezüglich eines kürzbaren multiplikativen Untermonoids K von R gelingt gemäß Satz 3.1.4.8 durch Betrachten des Faktormonoids von $R \times K$ nach der Kongruenzrelation $\sim$. Dabei ist $\sim$ definiert durch $(r, r_0) \sim (s, s_0)$ genau dann, wenn $rs_0 = sr_0$. Die Elemente der so konstruierten Struktur sind $\sim$-Kongruenzklassen $[(r, r_0)]_\sim$. Entscheidend für die Erweiterung der Konstruktion von Monoiden auf Ringe ist, dass $\sim$ nicht nur mit der Multiplikation verträglich ist (was wir aus Unterabschnitt 3.1.4 wissen), sondern auch mit der Addition auf $R \times K$, die der elementaren Bruchrechnung nachgebildet ist:

Lemma 3.4.5.4. *Ist R ein kommutativer Ring mit 1 und K ein kürzbares multiplikatives Untermonoid von R, so wird auf $R \times K$ durch die Addition*

$$(r, r_0) + (s, s_0) := (rs_0 + sr_0, r_0 s_0)$$

eine binäre Gruppenoperation mit neutralem Element $(0, 1)$ und Inversen $-(r, r_0) := (-r, r_0)$ definiert.

UE 189 ► Übungsaufgabe 3.4.5.5. (V) Beweisen Sie Lemma 3.4.5.4. **◄ UE 189**

Für die weitere Konstruktion entscheidend ist:

Lemma 3.4.5.6. *Die Relation $\sim$ ist eine Kongruenzrelation auf der Gruppe aus Lemma 3.4.5.4.*

Beweis. Wegen Proposition 3.2.2.1 genügt es die Verträglichkeit von $\sim$ mit der Addition zu überprüfen. Seien also $(r, r_0) \sim (r', r'_0)$, d. h. $rr'_0 = r'r_0$, und $(s, s_0) \sim (s', s'_0)$, d. h. $ss'_0 = s's_0$. Zu zeigen ist

$$(rs_0 + sr_0, r_0s_0) = (r, r_0) + (s, s_0) \quad \sim \quad (r', r'_0) + (s', s'_0) = (r's'_0 + s'r'_0, r'_0s'_0),$$

was sich aus der Rechnung

$$(rs_0 + sr_0)(r'_0s'_0) = rr'_0s_0s'_0 + ss'_0r_0r'_0 = r'r_0s_0s'_0 + s's_0r_0r'_0 = (r's'_0 + s'r'_0)(r_0s_0)$$

ergibt. □

Da die Verträglichkeit von $\sim$ mit den nullstelligen Operationen 0 und 1 trivial ist, ist die Faktorstruktur $Q := (R \times K)/_\sim$ vom Typ $(2, 0, 1, 2, 0)$ wohldefiniert.

Satz 3.4.5.7. *Sei R ein kommutativer Ring mit 1 und K ein kürzbares multiplikatives Untermonoid von R. Dann ist die oben definierte Algebra $Q := (R \times K)/_\sim$ zusammen mit $\iota\colon R \to Q$, $r \mapsto [(r, 1)]_\sim$ ein Quotientenring von R bezüglich K. Ist R ein Integritätsbereich und $K = R \setminus \{0\}$, so liegt sogar ein Quotientenkörper vor.*

Beweis. Wir beweisen die vier Bedingungen aus Definition 3.4.5.1:

(1) Q ist ein kommutativer Ring mit 1: Alle Aussagen über die multiplikative Struktur von Q (kommutatives Monoid) folgen aus den entsprechenden Konstruktionen für Quotientenmonoide, insbesondere aus Satz 3.1.4.8. Nach Lemma 3.4.5.4 ist $R \times K$ eine kommutative Gruppe, was sich wegen Lemma 3.4.5.6 bei Faktorisierung bezüglich $\sim$ auf $Q = (R \times K)/_\sim$ überträgt. Distributivität gilt zwar nicht auf $R \times K$, man rechnet aber leicht

$$(r, r_0)((s, s_0) + (s', s'_0)) \sim (r, r_0)(s, s_0) + (r, r_0)(s', s'_0)$$

nach (Übung), was für die zu beweisende Distributivität auf Q ausreicht.

(2) ι ist eine isomorphe Einbettung von R als Ring mit 1: Von der Konstruktion des Quotientenmonoids ist bekannt, dass ι eine isomorphe Einbettung des multiplikativen Monoids von R in Q ist. Für die Verträglichkeit mit der additiven Gruppenstruktur genügt es nach Proposition 3.2.2.1 die Verträglichkeit mit $+$ nachzuweisen:

$$\iota(r + s) = [(r + s, 1)]_\sim = [(r \cdot 1 + s \cdot 1, 1 \cdot 1)]_\sim = [(r, 1)]_\sim + [(s, 1)]_\sim = \iota(r) + \iota(s)$$

(3) Jedes $\iota(r)$, $r \in R$, hat in Q ein multiplikatives Inverses: Das folgt wieder aus der Konstruktion des Quotientenmonoids.

(4) Universelle Eigenschaft: Sei Q' irgendein anderer kommutativer Ring mit Einselement mit einer isomorphen Einbettung $\iota' \colon R \to Q'$ derart, dass alle $\iota'(r)$ mit $r \in K$ ein multiplikatives Inverses in Q' haben. Weil Q ein Quotientenmonoid des multiplikativen Monoids R bezüglich des kürzbaren Untermonoids K ist, gibt es eine eindeutige isomorphe Einbettung $\varphi \colon Q \to Q'$ des multiplikativen Monoids Q in Q' mit $\iota' = \varphi \circ \iota$. Somit muss erst recht jede Einbettung φ von Q in Q' als Ring mit 1 eindeutig sein, nämlich, wie aus dem Beweis von Satz 3.1.4.8 ersichtlich ist, $\varphi([(r, r_0)]_\sim) = \iota'(r)\iota'(r_0)^{-1}$. Weil die Verträglichkeit von φ mit der multiplikativen Struktur gleichfalls schon aus Satz 3.1.4.8 bekannt ist, bleibt einzig die mit der Addition zu zeigen. Es ist also lediglich nachzurechnen (Übung), dass

$$\varphi([(r, r_0)]_\sim + [(s, s_0)]_\sim) = \varphi([(r, r_0)]_\sim) + \varphi([(s, s_0)]_\sim)$$

gilt. □

Wie schon bei Quotientenmonoiden schreibt man meistens $\frac{r}{r_0}$ für $[(r, r_0)]_\sim$.

UE 190 ► **Übungsaufgabe 3.4.5.8.** (V) Tragen Sie die im ersten und vierten Teil des Beweises von Satz 3.4.5.7 nicht durchgeführten Rechnungen nach. ◄ **UE 190**

Quotientenringe und -körper existieren also unter sehr allgemeinen Voraussetzungen. Darüber hinaus geben die folgenden Aussagen nützliche Illustrationen zu diesen Begriffen. Die Beweise sind nicht schwierig und Gegenstand der darauffolgenden Übungsaufgabe.

Proposition 3.4.5.9. *Sei R ein Unterring mit 1 eines Körpers K.*

(1) *Dann ist*
$$K' := \{pq^{-1} \mid p, q \in R, q \neq 0\}$$
ein Unterkörper von K.

(2) *Der Körper K' aus dem ersten Teil ist der kleinste Unterkörper von K, der R enthält, symbolisch $K' = \langle R \rangle_{\text{Körper}}$. Explizit bedeutet das: Jeder Unterkörper K'' von K mit $R \subseteq K''$ umfasst K'.*

(3) *Der Körper K' aus dem ersten Teil ist (zusammen mit der Inklusionsabbildung) ein Quotientenkörper von R.*

UE 191 ► **Übungsaufgabe 3.4.5.10.** (V,W) Beweisen Sie Proposition 3.4.5.9. ◄ **UE 191**

Man sieht unmittelbar ein: Der Quotientenkörper des Integritätsbereiches $\mathbb{Z}$ ist der Körper $\mathbb{Q}$ der rationalen Zahlen. Der Quotientenkörper eines Körpers K ist zu K isomorph bzw. nach dem Prinzip der isomorphen Einbettung K selbst. Von besonderem Interesse wird später auch der Quotientenkörper eines Polynomrings sein, der sogenannte *Körper der gebrochen rationalen Funktionen*.

UE 192 ► **Übungsaufgabe 3.4.5.11.** (F) Beschreiben Sie Quotientenkörper von $R := \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ und von $S := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ mithilfe von Proposition 3.4.5.9, ohne auf die Konstruktion, auf die sich Satz 3.4.5.7 bezieht, zurückzugreifen. ◄ **UE 192**

Aus der Konstruktion des Quotientenringes geht hervor, dass sich die Darstellung rationaler Zahlen als Brüche auf allgemeinere Strukturen übertragen lässt. In $\mathbb{Q}$ gibt es unter den verschiedenen Darstellungen immer eine als gekürzter Bruch, etwa $\frac{16}{12} = \frac{4}{3}$. Der Grund ist offenbar die Existenz eines größten gemeinsamen Teilers von Zähler und Nenner in $\mathbb{Z}$, durch den gekürzt werden kann. Diese Möglichkeit besteht nicht immer, wenn man von $\mathbb{Z}$ zu beliebigen Intrgritätsbereichen übergeht. Im Kapitel 5 über Teilbarkeitslehre werden wir solche Aspekte nochmals behandeln.

3.4.6. Polynome und formale Potenzreihen

Inhalt in Kurzfassung: Formale Potenzreihen über einem kommutativen Ring R mit 1 (d. h. mit Koeffizienten aus R) sind durch die Folge ihrer Koeffizienten gegeben, können daher als eben diese Folgen definiert werden. In üblicher Weise kann die Menge $R[[x]]$ aller formalen Potenzreihen sowohl mit einer additiven als auch mit einer multiplikativen Struktur (gliedweise bzw. Cauchyprodukt) ausgestattet werden. Offenbar enthält $R[[x]]$ auch den Ring $R[x]$ aller Polynome über R (nur endlich viele Koeffizienten $\neq 0$). Ist R ein Integritätsbereich, so auch $R[[x]]$ und $R[x]$, und es kann der Quotientenkörper von $R[[x]]$ gebildet werden. Dieser lässt sich als Ring $R[[[x]]]$ der formalen Laurentreihen auffassen, die auch endlich viele Glieder mit negativen Potenzen enthalten dürfen. Durch Iteration des Übergangs von R zu $R[x]$ lassen sich auch Polynomringe in mehreren Variablen bilden. Polynomringe zeichnen sich durch eine universelle Eigenschaft aus, die in Unterabschnitt 4.2.3 noch näher beleuchtet werden wird.

In der naiven Auffassung wird der Polynomring $R[x]$ über einem kommutativen Ring R mit 1 beschrieben als Menge aller formalen Summen

$$p(x) = \sum_{k=0}^{n} a_k x^k.$$

Da der Begriff einer *formalen Summe* (noch) auf unklarem begrifflichen Fundament steht, machen wir uns zur Präzisierung zunutze, dass p allein durch die a_k eindeutig bestimmt ist, also mit der Folge $(a_k)_{k\in\mathbb{N}}$ identifiziert werden kann.

Definition 3.4.6.1. Sei R ein kommutativer Ring mit 1. Die Menge $R[[x]]$ der *formalen Potenzreihen* ist definiert als die Menge aller Folgen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in R$ für alle $n \in \mathbb{N}$. Statt $(a_n)_{n\in\mathbb{N}}$ schreiben wir für eine Potenzreihe allerdings meist $\sum_{n=0}^{\infty} a_n x^n$; den n-ten Eintrag a_n der Folge $(a_n)_{n\in\mathbb{N}}$ nennen wir den *Koeffizienten* von x^n oder auch den *n-ten Koeffizienten* der Potenzreihe.
Auf $R[[x]]$ ist durch

$$(a_k)_{k\in\mathbb{N}} + (b_k)_{k\in\mathbb{N}} := (a_k + b_k)_{k\in\mathbb{N}}$$

eine Addition definiert und durch

$$(a_k)_{k\in\mathbb{N}} \cdot (b_k)_{k\in\mathbb{N}} := (c_k)_{k\in\mathbb{N}} \quad \text{mit} \quad c_k := \sum_{i=0}^{k} a_i b_{k-i}$$

eine Multiplikation (*Cauchyprodukt*), die den üblichen Produkten von Polynomen bzw. Potenzreihen entspricht.
Jedes Element $a \in R$ identifizieren wir mit der Potenzreihe $\sum a_{n=0}^{\infty} x^n$ mit $a_0 = a$ und $a_n = 0$ für $n > 0$. Insbesondere schreiben wir 0 für die konstante Folge $(0)_{n\in\mathbb{N}}$ (also $a_n = 0$ für alle $n \in \mathbb{N}$, das neutrale Element in $R[[x]]$ bezüglich der Addition) und 1 für die Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_0 = 1$ und $a_n = 0$ für $n > 0$ (das neutrale Element bezüglich der Multiplikation).
Die Potenzreihe $\sum_{n=0}^{\infty} a_n x^n$, die $a_0 = 0 = a_n$ für $n > 1$ und $a_1 = 1$ erfüllt, bezeichnen wir mit x.

Definition 3.4.6.2. Die Menge der *Polynome* über R, geschrieben $R[x]$, ist die Menge aller Potenzreihen $\sum_{n=0}^{\infty} a_n x^n \in R[[x]]$, für die es ein m gibt mit $a_n = 0$ für alle $n > m$. Statt $\sum_{n=0}^{\infty} a_n x^n$ schreiben wir dann auch $\sum_{n=0}^{m} a_n x^n$ oder $a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$.

Proposition 3.4.6.3. *Sei R ein komutativer Ring mit 1.*

(1) *$R[[x]]$ mit den soeben definierten Operationen ist ein kommutativer Ring mit* 1*, genannt der* Ring der formalen Potenzreihen über *R.*

(2) *$R[x]$ ist Unterstruktur von $R[[x]]$ (betrachtet als Ring mit* 1*), genannt der* Polynomring über *R.*

UE 193 ► Übungsaufgabe 3.4.6.4. (V) Beweisen Sie Proposition 3.4.6.3. **◄ UE 193**

Jedes $a \in R$ lässt sich nach Definition 3.4.6.1 als Potenzreihe $p(x) = \sum_{n=0}^{\infty} a_n x^n$ mit $a_0 = a$ und $a_n = 0$ für alle $n > 0$ auffassen, die sogar ein Polynom ist. Weil es sich bei dieser Identifikation sogar um eine isomorphe Einbettung handelt, gilt die Unteralgebrenbeziehung $R \leq R[x] \leq R[[x]]$ (als kommutative Ringe mit 1).

Definition 3.4.6.5. Ist $p \in R[[x]] \setminus \{0\}$, so gibt es Koeffizienten $a_n \neq 0$. Insbesondere gibt es ein kleinstes derartiges n, genannt die *Ordnung* von p, symbolisch

$$\operatorname{ord}(p) := \min\{n \in \mathbb{N} \mid a_n \neq 0\}.$$

Einen größten Index gibt es genau dann, wenn $p \in R[x] \setminus \{0\}$. Dieser Index heißt der *Grad* von p, symbolisch

$$\operatorname{grad}(p) := \max\{n \in \mathbb{N} \mid a_n \neq 0\}.$$

Um manch mühsame Fallunterscheidung zu vermeiden, vereinbaren wir außerdem

$$\operatorname{grad}(0) = -\infty \quad \text{und} \quad \operatorname{ord}(0) = \infty$$

und, sofern $p \in R[[x]] \setminus R[x]$, $\operatorname{grad}(p) = \infty$; außerdem für alle $k \in \mathbb{Z}$ die Beziehungen $-\infty < k < \infty$, $k + \infty = \infty$ und $k + (-\infty) = -\infty$.

Ziemlich leicht zu beweisen sind folgende Aussagen:

Proposition 3.4.6.6. *Sei R ein kommutativer Ring mit 1, außerdem $p, q \in R[[x]]$ mit $p(x) = \sum_{n=0}^{\infty} a_n x^n$ und $q(x) = \sum_{n=0}^{\infty} b_n x^n$. Mit R^*, $R[[x]]^*$ und $R[x]^*$ seien die Einheitengruppen der Ringe R, $R[[x]]$ und $R[x]$ bezeichnet. Dann gilt:*

(1) $\operatorname{ord}(p+q) \geq \min\{\operatorname{ord}(p), \operatorname{ord}(q)\}$.

(2) $\operatorname{grad}(p+q) \leq \max\{\operatorname{grad}(p), \operatorname{grad}(q)\}$, *wenn* $p, q \in R[x]$.

(3) $\operatorname{ord}(pq) \geq \operatorname{ord}(p) + \operatorname{ord}(q)$.
Ist R ein Integritätsbereich, so gilt sogar Gleichheit.

(4) $\operatorname{grad}(pq) \leq \operatorname{grad}(p) + \operatorname{grad}(q)$, *wenn* $p, q \in R[x]$.
Ist R ein Integritätsbereich, so gilt sogar Gleichheit.

(5) *Ist R ein Integritätsbereich, so auch $R[[x]]$ und $R[x]$.*

(6) *Genau dann ist $p \in R[[x]]^*$, wenn $a_0 \in R^*$. Ist $q = p^{-1}$ das multiplikative Inverse von p, dann erfüllen die Koeffizienten $b_0 = a_0^{-1}$ und für alle $n = 1, 2, \ldots$ die Rekursion $b_n = -b_0(a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_n b_0)$. Ist speziell R ein Körper, so ist $p \in R[[x]]^*$ genau dann, wenn $\operatorname{ord}(p) = 0$.*

(7) *Wenn R Integritätsbereich ist, dann gilt für alle $p \in R[x]$: Genau dann ist $p \in R[x]^*$, wenn $\operatorname{grad}(p) = 0$ und $p = a_0$ mit $a_0 \in R^*$.*

UE 194 ▶ **Übungsaufgabe 3.4.6.7.** (V,B) Beweisen Sie Proposition 3.4.6.6, und zeigen Sie durch Beispiele, dass man „$\leq$“ bzw. „$\geq$“ im Allgemeinen nicht durch „$=$“ ersetzen kann. ◀ **UE 194**

Ist n der Grad des Polynoms[22] p, so nennt man a_n den *führenden Koeffizienten* von p, a_0 den *konstanten*, a_1 den *linearen* etc. Ist $a_n = 1$, so heißt p *normiert* oder *monisch*.
Nach Proposition 3.4.6.6 bilden Polynome wie auch formale Potenzreihen keinen Körper, selbst wenn R einer ist. Dennoch ist bei Polynomen, ähnlich wie in den ganzen Zahlen, Division mit Rest möglich. Genauer:

Satz 3.4.6.8. *Sei R ein kommutativer Ring mit Einselement, $a \in R[x]$ mit einem führenden Koeffizienten, der eine Einheit ist, und $b \in R[x]$ beliebig. (Die Voraussetzung bedeutet insbesondere, dass $a \neq 0$. Ist R sogar ein Körper, so erfüllt umgekehrt jedes $a \neq 0$ diese Voraussetzung.)*
Dann gibt es $q, r \in R[x]$ mit $b = qa + r$ und $\operatorname{grad}(r) < \operatorname{grad}(a)$.

UE 195 ▶ **Übungsaufgabe 3.4.6.9.** (V,W) Beweisen Sie Satz 3.4.6.8 mittels Induktion nach $\operatorname{grad}(b)$. Inwiefern lässt sich aus Ihrem Beweis ein Algorithmus zur Polynomdivision gewinnen? ◀ **UE 195**

Wir haben bereits in Unterabschnitt 3.4.2 angekündigt, dass Primideale im Allgemeinen keine maximalen Ideale sind:

[22] Für $p(x)$ schreiben wir oft auch einfacher (und durchaus konsistent; ausnahmsweise also keine Schlamperei!) p und sprechen von einem *Polynom* in einer Variablen über R.

UE 196 ► **Übungsaufgabe 3.4.6.10.** (B) Geben Sie einen kommutativen Ring R mit 1 an, sowie ein Primideal $I \neq \{0\}$ in R, welches nicht maximal ist. ◄ **UE 196**
Hinweis: Beachten Sie Satz 3.4.2.4.

Quotientenkörper von $R[x]$ und $R[[x]]$ existieren genau dann, wenn diese Integritätsbereiche sind, also wenn R selbst einer ist.

Definition 3.4.6.11. Sei R ein Integritätsbereich. Dann heißt der Quotientenkörper von $R[x]$ auch der Körper der *gebrochen rationalen Funktionen* über R (siehe auch Unterabschnitt 5.3.5). Wir schreiben für ihn $R(x)$.

Der Körper $R(x)$ lässt sich deuten als Menge aller Ausdrücke der Gestalt $\frac{p(x)}{q(x)}$ mit $p, q \in R[x]$ und $q \neq 0$, wobei Kürzung von Brüchen in üblicher Weise möglich ist. Insbesondere enthält der Körper der gebrochen rationalen Funktionen auch den Quotientenkörper K von R, bestehend aus allen $\frac{p}{q}$ mit $p, q \in R \leq R[x]$ und $q \neq 0$. Es gibt dann einen natürlichen Isomorphismus zwischen $R(x)$ und $K(x)$; daher werden wir Körper der Form $R(x)$ vor allem dann betrachten, wenn R bereits ein Körper ist.
Sei nun R ein Körper. Dann lässt sich der Quotientenkörper Q von $R[[x]]$ wie folgt beschreiben:

Definition 3.4.6.12. Wir schreiben eine sogenannte *formale Laurentreihe* $q = q(x)$ in der Form

$$q(x) = \sum_{n=-N}^{\infty} a_n x^n$$

mit einem beliebigen $N \in \mathbb{Z}$ und Koeffizienten $a_n \in R$ an. Der Unterschied zu den formalen Potenzreihen besteht lediglich darin, dass dort $N = 0$ fest ist. Für $a_N \neq 0$ nennt man in Analogie zu früher $N =: \operatorname{ord}(q)$ die *Ordnung* von q. Die Menge aller formalen Laurentreihen (streng gesprochen die Menge aller $(a_n)_{n\in\mathbb{Z}}$, zu denen es ein $N \in \mathbb{Z}$ gibt mit $a_n = 0$ für alle $n < N$) bezeichnet man mit $R[[[x]]]$.

Auf $R[[[x]]]$ definiert man die Operationen auf natürliche Weise (Addition komponentenweise, Cauchyprodukt so erweitert, dass die Rechenregel $x^{m+n} = x^m \cdot x^n$ gilt). So erhält man wieder einen Integritätsbereich, in dem jedes $q \neq 0$ sogar ein multiplikatives Inverses hat. Denn für $N = \operatorname{ord}(q)$ ist

$$q(x) = \sum_{n=N}^{\infty} a_n x^n = x^N \sum_{n=0}^{\infty} a_{n+N} x^n$$

mit $a_{0+N} = a_N \neq 0$. Ist $q_0^{-1} \in R[[x]]$ das multiplikative Inverse von $q_0 := \sum_{n=0}^{\infty} a_{n+N} x^n \in R[[x]]^*$, so ergibt sich damit auch das Inverse q^{-1} von q als $q^{-1} = (x^N q_0)^{-1} = x^{-N} q_0^{-1}$. Somit ist $R[[[x]]]$ ein Körper, in den $R[[x]]$ in offensichtlicher Weise isomorph eingebettet ist. Folglich enthält $R[[[x]]]$ nach Proposition 3.4.5.9 einen Quotientenkörper Q von $R[[x]]$. Klarerweise ist $R[[[x]]]$ selbst aber der kleinste Unterkörper von $R[[[x]]]$, der $R[[x]]$ enthält (denn ein solcher muss sowohl x^{-N} für alle $n \in \mathbb{Z}$ als auch alle $p \in R[[x]]$ enthalten, somit auch deren Produkte), also ist $R[[[x]]] = Q$ selbst der gesuchte Quotientenkörper von $R[[x]]$.

Satz 3.4.6.13. *Ist R ein Körper, so bilden die formalen Laurentreihen (zusammen mit der Inklusionsabbildung $\iota\colon R[[x]] \to R[[[x]]]$, $(a_n)_{n\in\mathbb{N}} \mapsto (a_n)_{n\in\mathbb{Z}}$ mit $a_n = 0$ für alle $n < 0$, als isomorpher Einbettung) einen Quotientenkörper von $R[[x]]$.*

UE 197 ► Übungsaufgabe 3.4.6.14. (V) Beweisen Sie Satz 3.4.6.13, indem Sie jene Beweisschritte, die oben nur skizzenhaft angedeutet worden sind, ausführlich durchführen. Genauer sind folgende Schritte zu tun: **◄ UE 197**

1. Definieren Sie sorgfältig die fundamentalen Operationen von $R[[[x]]]$ (Addition, Nullelement, additive Inverse, Multiplikation, Einselement).
2. Zeigen Sie, dass es sich dabei um einen kommutativen Ring mit 1 handelt.
3. Zeigen Sie, dass sich jedes $q \in R[[[x]]]\setminus\{0\}$ *eindeutig* in der Form $x^N q_0(x)$ schreiben lässt, mit $N \in \mathbb{Z}$, und $q_0(x) \in R[[x]]^*$. (Mit $R[[x]]^*$ bezeichnen wir die Einheiten von $R[[x]]$, siehe Proposition 3.4.6.6.)
4. Zeigen Sie, dass jedes $q \in R[[[x]]] \setminus \{0\}$ ein multiplikatives Inverses in $R[[[x]]]$ hat. (Somit ist $R[[[x]]]$ ein Körper.)
5. Schließen Sie den Beweis ab, dass $R[[[x]]]$ mit ι tatsächlich ein Quotientenkörper von $R[[x]]$ ist.

Auf Satz 3.4.6.13 beruhen beträchtliche Teile der Theorie der erzeugenden Funktionen, die zum Beispiel in der Kombinatorik ein unglaublich mächtiges Instrument darstellt. Der Kern dieser Macht besteht darin, dass auf der Seite der Polynome und gebrochen rationalen Funktionen die Teilbarkeitslehre mit Faktorisierungseigenschaften, Partialbruchzerlegung etc. zur Verfügung steht und über die durch Satz 3.4.6.13 beschriebene Verbindung zu den formalen Laurentreihen in Eigenschaften von Folgen (nämlich der Koeffizienten) übersetzt werden können. Die prominenteste Anwendung ist die Lösungstheorie linearer Rekursionen.

Die besondere Bedeutung von Polynomen in der klassischen Algebra lässt sich besonders klar auf den Punkt bringen, wenn man Polynome über einem kommutativen Ring mit 1 nicht nur in einer Variablen x betrachtet, sondern in mehreren Variablen, die einer Variablenmenge X entnommen sind. Statt $R[x]$ schreibt man für den resultierenden Ring $R[X]$. Für endliches X lässt sich rekursiv definieren

$$R[x_1,\dots,x_n,x_{n+1}] := R[x_1,\dots,x_n][x_{n+1}].$$

Elemente des resultierenden Ringes $R[x_1,\dots,x_n]$ stellt man als endliche Summen von Ausdrücken der Form $ax_1^{k_1}\dots x_n^{k_n}$ dar mit $a \in R$ und $k_1,\dots,k_n \in \mathbb{N}$. Formal gesprochen ist ein Element von $R[x_1,\dots,x_n]$ also gegeben durch das Koeffiziententupel $(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n}$ mit $a_{(k_1,\dots,k_n)} \in R$, wobei nur endlich viele $a_{(k_1,\dots,k_n)}$ von 0 verschieden sind. Das Tupel $(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n}$ entspricht dabei der (formal unendlichen, tatsächlich endlichen) Summe $\sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} a_{(k_1,\dots,k_n)} x_1^{k_1} x_2^{k_2}\dots x_n^{k_n}$.

Für unendliches X kann man $R[X]$ zum Beispiel auch als direkten Limes (siehe Unterabschnitt 2.2.4) der Ringe $R[x_1, \ldots, x_n]$ mit $\{x_1, \ldots, x_n\} \subseteq X$ definieren. Der Einfachheit halber beschreiben wir die Vorgangsweise nur für eine abzählbar unendliche Menge $X = \{x_1, x_2, x_3, \ldots\}$. Wir setzen $R_n := R[x_1, \ldots, x_n]$. Die zugehörigen Einbettungen $\iota_n : R_n \to R_{n+1} = R_n[x_{n+1}]$ liegen auf der Hand: Wir bilden $p \in R_n$ auf das bezüglich x_{n+1} konstante Polynom mit Wert p ab. Der Polynomring $R[X]$ ist dann die durch Satz 2.2.4.6 erhaltene Struktur $\mathfrak{A}_\infty$. Für überabzählbare Mengen wird dieses schrittweise Vorgehen unelegant, weil man den Wohlordnungssatz aus der Mengenlehre (siehe Anhang, Satz A.4.2.6) benötigt. Stattdessen kann man eine allgemeinere Version des direkten Limes verwenden, nämlich den direkten Limes einer Familie von Algebren, die durch eine gerichtete Menge anstatt einer Totalordnung indiziert sind; siehe Algebra II (Unterabschnitt 7.1.5). Als Vorgriff sei erwähnt: Mit diesen Mitteln kann man $R[X]$ als Limes von $(R[x_1, \ldots, x_n])_{\{x_1,\ldots,x_n\} \in \mathfrak{P}_{\text{fin}}(X)}$ definieren, wobei $\mathfrak{P}_{\text{fin}}(X)$ durch $\subseteq$ geordnet sei.

Eine andere, konkretere Realisierung von $R[X]$ verallgemeinert unsere Definition von $R[x]$ und die obige Realisierung des Rings $R[x_1, \ldots, x_n]$ in unmittelbarer Weise. Wir betrachten eine beliebige Menge X und stellen Elemente des Rings $R[X]$ wieder als endliche Summen von Ausdrücken $a x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ dar mit $a \in R$, $n \in \mathbb{N}$, $x_1, \ldots, x_n \in X$ und $k_1, \ldots, k_n \in \mathbb{N}$. Bei der Präzisierung müssen wir noch darauf achten, dass jeder solche Ausdruck nur endlich viele Variablen enthalten darf. Daher definieren wir die Indexmenge $M := \{\vec{k} = (k_x)_{x \in X} \in \mathbb{N}^X \mid k_x \neq 0 \text{ nur für endlich viele } x \in X\}$ und betrachten $R[X]$ als Menge aller Koeffiziententupel $(a_{\vec{k}})_{\vec{k} \in M}$, wobei wieder nur endlich viele $a_{\vec{k}}$ von 0 verschieden sind. Wir haben in den konkreten Realisierungen von sowohl $R[x_1, \ldots, x_n]$ als auch $R[X]$ nur die Grundmengen angegeben, nicht aber die Operationen. Dies holen wir im Rahmen einer Übungsaufgabe nach:

UE 198 ► **Übungsaufgabe 3.4.6.15.** (V) Sei R ein kommutativer Ring mit 1. Betrachten Sie die oben definierten konkreten Realisierungen von $R[x_1, \ldots, x_n]$ und $R[X]$ als Mengen von Koeffiziententupeln. Definieren Sie die Operationen $+, -, \cdot$ und die Konstanten $0, 1$ auf diesen beiden Mengen. Zeigen Sie außerdem, dass $(R[x_1, \ldots, x_n], +, 0, -, \cdot, 1)$ sowie $(R[X], +, 0, -, \cdot, 1)$ kommutative Ringe mit 1 sind. Wenn Ihnen das zu langwierig ist: Geben Sie sorgfältig an, welche Aussagen nachzuprüfen sind. ◄ **UE 198**

Von besonderem Interesse ist die folgende Eigenschaft von $R[X]$, die an die Termalgebra aus Unterabschnitt 2.1.8 oder auch an die freie Halbgruppe aus 3.1.2 erinnert:

Proposition 3.4.6.16. *Sei R ein kommutativer Ring mit 1 und X eine Variablenmenge. Sei S ein kommutativer Ring mit 1, der R erweitert, also $R \leq S$. Dann lässt sich jede Abbildung $\iota\colon X \to S$ (Variablenbelegung mit Elementen aus S) in eindeutiger Weise zu einem Ringhomomorphismus $\varphi\colon R[X] \to S$ fortsetzen, nämlich durch*

$$\varphi : p = \sum_{i \in I} a_i x_{i,1}^{k_1} \ldots x_{i,n_i}^{k_{n_i}} \mapsto \sum_{i \in I} a_i \iota(x_{i,1})^{k_1} \ldots \iota(x_{i,n_i})^{k_{n_i}}.$$

UE 199 ► **Übungsaufgabe 3.4.6.17.** (V) Beweisen Sie Proposition 3.4.6.16. Wenn Ihnen das zu langwierig ist: Geben Sie wenigstens sorgfältig an, welche Schritte in so einem Beweis auszuführen sind, und wo die Kommutativität der Multiplikation verwendet wird. ◄ **UE 199**

Der Homomorphismus φ lässt sich so interpretieren, dass schlicht in der Summendarstellung des Polynoms für jede Variable $x \in X$ das Ringelement $\iota(x) \in S$ eingesetzt wird. Deshalb spricht man auch vom *Einsetzungshomomorphismus*, der durch ι induziert wird. Dass es sich um einen Homomorphismus handelt, liegt daran, dass die Operationen für die Elemente von $R[X]$ (Polynome) so definiert sind, dass man mit ihnen so rechnen kann wie in beliebigen Ringen mit 1. Der Polynomring $R[X]$ ist also in gewisser Weise die allgemeinste Ringerweiterung von R um $|X|$ viele Elemente.
Diese Sichtweise wird im Mittelpunkt von Kapitel 4 stehen. Insbesondere werden wir dort Polynomalgebren über allgemeinen Algebren durch eine Eigenschaft wie in Proposition 3.4.6.16 definieren.
Beim Einsetzungshomomorphismus wurde die Variablenbelegung $\iota\colon X \to S$ vorgegeben und $p \in R[X]$ als Argument von $\varphi = \varphi_\iota\colon R[X] \to S$ betrachtet. Man kann auch umgekehrt vorgehen und p festhalten. Die durch das Polynom p induzierte Zuordnung $\iota \mapsto \varphi_\iota(p)$ entspricht für $S = R$ dann dem, was man gemeinhin unter einer *Polynomfunktion* in den Variablen $x \in X$ versteht. Ist $X = \{x_1, \ldots, x_n\}$ endlich, so ist jedes ι von der Form $x_j \mapsto r_j \in R$, entspricht also dem Ersetzen der Elemente $r_j \in R$ für die Variablen x_j in p. Deshalb schreibt man $p(r_1, \ldots, r_n)$ für $\varphi_\iota(p)$.
In offensichtlicher Weise, nämlich vermittels punktweiser Definition wie z. B.

$$(p_1 + p_2)(r_1, \ldots, r_n) := p_1(r_1, \ldots, r_n) + p_2(r_1, \ldots, r_n)$$

etc., bilden die Polynomfunktionen in n (oder auch beliebig vielen) Variablen selbst wieder einen kommutativen Ring mit 1, der in kanonischer Weise ein homomorphes Bild von $R[X]$ ist. Ist beispielsweise $R = \mathbb{R}$ der Ring der reellen Zahlen, so handelt es sich sogar um eine Isomorphie. Denn jede Polynomfunktion wird von nur einem einzigen reellen Polynom induziert. Ist R hingegen ein endlicher Körper, so gilt dies nicht: Zum Beispiel ist $x^2 - x \in \mathbb{Z}_2[x]$ nicht das Nullpolynom, induziert aber die konstante Funktion mit Wert 0 auf $\mathbb{Z}_2$. Später werden wir uns damit noch ausführlich beschäftigen.
Besonders interessant sind *Nullstellen* von Polynomen. Das sind jene n-Tupel $(r_1, \ldots, r_n)$, $r_i \in R$ mit $p(r_1, \ldots, r_n) = 0$. Für $n = 1$ wird sich dieser Aspekt fast durch das gesamte Kapitel 6 über Körper ziehen, in Algebra II durch die Galoistheorie (Kapitel 9). Für $n > 1$ ist in diesem Zusammenhang vor allem der *Hilbertsche Nullstellensatz* zu nennen; siehe Abschnitt 10.3.

3.4.7. Der Chinesische Restsatz

Inhalt in Kurzfassung: Darstellungen als direkte Produkte spielen bei Ringen keine so große Rolle wie bei Gruppen. Von Interesse ist aber immerhin der Chinesische Restsatz. Er wird zunächst in einer allgemeinen, dann in seiner klassischen Fassung gebracht.

Sei $R = R_1 \times R_2$ das direkte Produkt der Ringe R_1 und R_2. Wohl liegen in Analogie zu Gruppen sowohl kanonische Projektionen $\pi_1 : R \to R_1$, $(r_1, r_2) \mapsto r_1$ und $\pi_2 : R \to R_2$, $(r_1, r_2) \mapsto r_2$, als auch kanonische Einbettungen $\iota_1 : R_1 \to R$, $r_1 \mapsto (r_1, 0)$, und $\iota_2 : R_2 \to R$, $r_2 \mapsto (0, r_2)$, vor. Es ist aber zu beachten, dass im Falle von Ringen mit $1 \neq 0$ die Einbettungen wegen $\iota_1(1_{R_1}) = (1, 0) \neq (1, 1) = 1_R$ und $\iota_2(1_{R_2}) = (0, 1) \neq (1, 1) = 1_R$ nicht mit 1 verträglich sind. So wie bei allgemeineren Klassen von Algebren ist es deshalb angemessen, die Komponenten R_1 und R_2 nicht als Unter-, sondern nur als Faktorstrukturen von R aufzufassen, die nach dem Homomorphiesatz den Homomorphismen π_2 bzw. π_1 entsprechen. Schreibt man so wie bei Gruppen $R_1 \cong R/\iota_2(R_2)$ und $R_2 \cong R/\iota_1(R_1)$, so wird deutlich, dass die eingebetteten Kopien $\iota_i(R_i)$ der R_i in R nicht die Rollen von Unterringen, sondern von Idealen spielen.
Unter diesem Gesichtspunkt ist auch der sogenannte *Chinesische Restsatz* zu verstehen. In seiner klassischen zahlentheoretischen Form bezieht er sich darauf, die Lösung von Kongruenzen in ganzen Zahlen modulo m zurückzuführen auf Kongruenzen modulo p^e, wenn $p \in \mathbb{P}$ und p^e die höchste p-Potenz ist, die m teilt. Eine abstraktere, algebraische Fassung im Sinn der einleitenden Bemerkungen ist die folgende.

Satz 3.4.7.1 (Chinesischer Restsatz, allgemeine Fassung)**.** *Seien R ein Ring mit 1 und $I_1, \ldots, I_n$, $n \geq 2$, Ideale von R mit $I_j + I_k = R$ für alle $j \neq k$. Weiters sei $I := I_1 \cap \ldots \cap I_n$.*

(1) *Dann gibt es zu beliebig vorgegebenen Elementen $r_1, \ldots, r_n \in R$ ein modulo I eindeutig bestimmtes $r \in R$ mit $r \equiv r_j \pmod{I_j}$, $j = 1, \ldots, n$.*

(2) *Es gilt $R/I \cong \prod_{j=1}^{n} R/I_j$, wobei $\psi : r + I \mapsto (r + I_1, \ldots, r + I_n)$ ein Ringisomorphismus ist.*

Beweis.

(1) Mittels Induktion nach i sieht man $R = I + (I_2 \cap \cdots \cap I_i)$ für alle $i = 2, \ldots, n$ wie folgt: Der Induktionsanfang $i = 2$ gilt nach Voraussetzung. Für den Induktionsschritt von i auf $i + 1$ behaupten wir

$$R = R \cdot R = (I_1 + (I_2 \cap \ldots \cap I_i))(I_1 + I_{i+1}) \subseteq I_1 + (I_2 \cap \ldots \cap I_{i+1}) \subseteq R.$$

Dabei folgt die erste Gleichheit wegen $1 \in R$, die zweite mittels Induktionsannahme und der Voraussetzung $I_j + I_k = R$ für alle $j \neq k$. Die erste Mengeninklusion rechts wiederum ergibt sich durch Ausmultiplizieren unter Verwendung der Idealeigenschaft für alle I_j, und die letzte Inklusion ist trivial. Aus dieser Formel folgt wie gewünscht $R = I + (I_2 \cap \cdots \cap I_{i+1})$. Für festes $k = 1, \ldots, n$ sieht man ganz analog $R = I_k + I'_k$ mit $I'_k := \cap_{j \neq k} I_j$. Also gibt es zu jedem k Elemente $a_k \in I_k$ und $a'_k \in I'_k$ mit $r_k = a_k + a'_k$, folglich $a'_k \equiv r_k \pmod{I_k}$ und $a'_k \equiv 0 \pmod{I_j}$ für $j \neq k$. Das Element $r := \sum_{k=1}^{n} a'_k$ hat somit die gewünschten Eigenschaften. Ein beliebiges weiteres Element r' erfüllt $r \equiv r_j \pmod{I_j}$, $j = 1, \ldots, n$, offenbar genau dann, wenn $r - r' \in I$ gilt, d. h. wenn $r \equiv r \pmod{I}$. Damit ist Behauptung (1) bewiesen.

(2) Die Abbildung ψ ist wegen $I \subseteq I_j$ für alle $j = 1, \ldots, n$ wohldefiniert und offensichtlich ein Ringhomomorphismus. Wir zeigen die Bijektivität, indem wir die

Umkehrfunktion λ von ψ angeben. Zu $(r_1 + I_1, \ldots, r_n + I_n) \in \prod_{j=1}^n R/I_j$ betrachten wir das Gleichungssystem $r \equiv r_j \mod I_j$, $j = 1, \ldots, n$ (klarerweise hängt dieses Gleichungssystem nicht von der konkreten Wahl der Repräsentanten r_j ab). Nach (1) gibt es ein modulo I eindeutig bestimmtes Element $r \in R$, das dieses Gleichungssystem löst, d. h. $(r_1 + I_1, \ldots, r_n + I_n) = (r + I_1, \ldots, r + I_n)$ und die I-Äquivalenzklasse $r + I$ der Lösung ist eindeutig bestimmt. Somit können wir $\lambda(r_1 + I_1, \ldots, r_n + I_n) := r + I$ setzen. Wir erhalten $\psi \circ \lambda = \mathrm{id}_{\prod_{j=1}^n R/I_j}$ nach Definition von λ. Umgekehrt ergibt sich $\lambda \circ \psi = \mathrm{id}_{R/I}$ unmittelbar daraus, dass für beliebiges $r \in R$ eine Lösung des zu $\psi(r + I)$ gehörigen Gleichungssystems offensichtlich durch $r + I$ gegeben ist, also $\lambda(\psi(r + I)) = r + I$.

□

Wir kehren kurz zum klassischen Fall des Hauptidealrings $R = \mathbb{Z}$ der ganzen Zahlen zurück. Seien die Ideale von der Form $I_j = m_j\mathbb{Z}$ mit $m_j = p_j^{e_j}$ mit paarweise verschiedenen $p_j \in \mathbb{P}$ und geeigneten $e_j \in \mathbb{N}$. Dann sind die m_j paarweise teilerfremd. Wegen Folgerung 3.2.4.2 bedeutet das $1 = xm_j + ym_k \in I_j + I_k$ für geeignete $x, y \in \mathbb{Z}$, sofern $j \neq k$, und, wegen $I_j + I_k \lhd \mathbb{Z}$ (siehe Proposition 3.4.1.12), $I_j + I_k = \mathbb{Z}$. Das ist gerade die Voraussetzung in Satz 3.4.7.1. In diesem Fall besagt der Chinesische Restsatz daher:

Folgerung 3.4.7.2 (Chinesischer Restsatz, klassische Fassung)**.** *Sei $m = \prod_{j=1}^n p_j^{e_j} \in \mathbb{N}$ mit paarweise verschiedenen $p_j \in \mathbb{P}$ und mit Exponenten $e_j \in \mathbb{N}$. Dann gilt die Isomorphie der Restklassenringe*

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_{j=1}^n (\mathbb{Z}/p_j^{e_j}\mathbb{Z}).$$

Ignoriert man die multiplikative Struktur und betrachtet nur die additive Gruppe der jeweiligen Ringe, so wird die klassische Fassung des chinesischen Restsatzes zu einer Umformulierung von Übungsaufgabe 3.3.2.13, wie wir dort bereits bemerkt haben. Der wesentliche Unterschied zur allgemeinen Fassung besteht darin, dass im klassischen Fall die auftretenden Faktorringe $\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/p_j^{e_j}\mathbb{Z}$ (sowie natürlich das Produkt der letzteren) alle endlich sind, während im allgmeinen Fall die Ringe $R/I, R/I_j$ auch unendlich sein dürfen.

Eine weitere Folgerung ist die Formel für die Eulersche φ-Funktion (siehe Definition 3.2.4.19). Zur Erinnerung: Für eine positive Zahl $n \in \mathbb{N}^+$ ist $\varphi(n)$ definiert als die Anzahl der primen Restklassen modulo n. Dabei heißt eine Restklasse prim modulo n, wenn alle ihre Elemente (oder äquivalent: ein Element; siehe Übungsaufgabe 3.2.4.18) zu n teilerfremd ist.

Satz 3.4.7.3. *Ist $n = \prod_{i=1}^k p_i^{e_i}$ mit $k \in \mathbb{N}$, paarweise verschiedenen $p_i \in \mathbb{P}$ und $e_i \in \mathbb{N}^+$, so gilt für die Eulersche φ-Funktion die Formel*

$$\varphi(n) = \prod_{i=1}^k (p_i - 1)p_i^{e_i - 1}.$$

UE 200 ► **Übungsaufgabe 3.4.7.4.** (V,W) Beweisen Sie die Formel aus 3.4.7.3, indem Sie folgende Aussagen begründen: ◄ **UE 200**

1. Die Formel gilt für Primzahlpotenzen $n = p^e$.

2. Eine Restklasse ist genau dann prim modulo m, wenn sie eine Einheit in der multiplikativen Halbgruppe von $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ ist. Hinweis: Folgerung 3.2.4.2

3. Man verwende Folgerung 3.4.7.2, um mittels 2. das Problem für ein beliebiges n auf Primzahlpotenzen zurückzuführen.

3.4.8. Beispiele nichtkommutativer Ringe

Inhalt in Kurzfassung: Die wichtigsten Beispiele nichtkommutativer Ringe entstehen als Endomorphismenringe von abelschen Gruppen oder von Moduln. Umgekehrt erhält man sehr natürliche Beispiele von Moduln über im Allgemeinen nichtkommutativen Ringen in Gestalt von abelschen Gruppen über ihrem Endomorphismenring. Wir begnügen uns mit einer sehr kurzen Präsentation.

Sehr wichtige Beispiele nichtkommutativer Ringe sind bereits aus der Linearen Algebra bekannt, nämlich Ringe quadratischer Matrizen bzw., äquivalent, linearer Abbildungen eines (endlichdimensionalen) Vektorraums in sich selbst. Dabei ist die Summe zweier Abbildungen gegeben durch die punktweise Addition, $(f+g)(a) := f(a)+g(a)$, und die Multiplikation zweier Abbildungen gegeben durch die Komposition, $fg(a) := f(g(a))$. Versucht man, die Gesetze eines Rings nachzurechnen, so stellt man fest, dass sich die allermeisten Gesetze von entsprechenden Gesetzen auf der zugrundeliegenden Struktur (hier: ein Vektorraum) vererben. Beispielsweise ist dies für das Assoziativgesetz $(f+g)+h = f+(g+h)$ der Fall: Da in der additiven Gruppe des Vektorraums das Assoziativgesetz gilt, folgt für jedes a aus dem Vektorraum

$$\begin{aligned}((f+g)+h)(a) &= (f+g)(a)+h(a) = (f(a)+g(a))+h(a) = f(a)+(g(a)+h(a)) \\ &= f(a)+(g+h)(a) = (f+(g+h))(a).\end{aligned}$$

Andere Gesetze wiederum folgen aus entsprechenden Gesetzen der Funktionskomposition (beliebiger!) Abbildungen, beispielsweise das Assoziativgesetz der Multiplikation (also der Komposition) oder auch das Distributivgesetz $(f+g)h = fh+gh$: Für jedes Element a des Vektorraums gilt nämlich

$$((f+g)h)(a) = (f+g)(h(a)) = f(h(a))+g(h(a)) = (fh)(a)+(gh)(a) = (fh+gh)(a).$$

Dass wir es nicht mit irgendwelchen Abbildungen sondern mit *linearen* Abbildungen zu tun haben, geht nur beim Distributivgesetz $f(g+h) = fg+fh$ ein – dieses ist somit

das einzige „nichttriviale“ Gesetz[23]. Für jedes a aus dem Vektorraum berechnet man

$$\begin{aligned}(f(g+h))(a) = f((g+h)(a)) = f(g(a)+h(a)) &\overset{(*)}{=} f(g(a))+f(h(a))\\ &= (fg)(a)+fh(a) = (fg+fh)(a);\end{aligned}$$

man sieht, dass in $(*)$ die Linearität von f wesentlich ist. Etwas allgemeiner kann man von Endomorphismen abelscher Gruppen ausgehen und dann auf Moduln und Vektorräume spezialisieren.

Proposition 3.4.8.1. *Ist A eine abelsche Gruppe, so bildet die Menge* $\mathrm{End}(A)$ *aller Endomorphismen $f\colon A \to A$ bezüglich der wie folgt definierten Operationen einen Ring mit* 1*:*

- $(f+g)(a) := f(a)+g(a)$
- $0(a) := 0$
- $(-f)(a) := -f(a)$
- $fg(a) := f(g(a))$
- $1(a) := a$.

Ist A auch ein Modul über einem Ring R, so bilden die R-Modulendomorphismen von A einen Unterring $\mathrm{End}_R(A) \leq \mathrm{End}(A)$.
$\mathrm{End}_R(A)$ *ist zum Beispiel dann sicher nicht kommutativ, wenn R ein Körper und A ein Vektorraum über R einer Dimension ≥ 2 ist. Insbesondere ist auch* $\mathrm{End}(A)$ *im Allgemeinen nicht kommutativ.*

UE 201 ► Übungsaufgabe 3.4.8.2. (V) Beweisen Sie Prop 3.4.8.1. **◄ UE 201**

UE 202 ► Übungsaufgabe 3.4.8.3. (D) Untersuchen Sie, für welche endlichen abelschen Gruppen A der Endomorphismenring aus Proposition 3.4.8.1 kommutativ ist, für welche nicht. Beginnen Sie mit sehr einfachen Beispielen für A und versuchen Sie nach und nach eine möglichst große Klasse abelscher Gruppen zu erfassen. Wie weit kommen Sie? (Hinweis: Der Hauptsatz 3.3.4.2 könnte sehr nützlich sein.) **◄ UE 202**

UE 203 ► Übungsaufgabe 3.4.8.4. (B) **◄ UE 203**

(1) Zeigen Sie: Ist V ein endlichdimensionaler Vektorraum über einem Körper, so ist $\mathrm{End}(V)$ als Ring einfach (besitzt also nur die trivialen Ideale).

(2) Zeigen Sie, dass dies für unendlichdimensionale Vektorräume nicht gilt.
Hinweis: Betrachten Sie alle Endomorphismen mit endlichdimensionalem Bild.

[23] Verzichtet man darauf und begnügt sich mit dem Distributivgesetz $(f+g)h = fh+gh$, so erhält man die Klasse der sogenannten *Fastringe*, für die auch nichtlineare Abbildungen auf geeigneten Strukturen Beispiele liefern.

Bisher haben wir an konkreten Beispielen von Moduln lediglich abelsche Gruppen, aufgefasst als Moduln über den Ringen $\mathbb{Z}$ oder $\mathbb{Z}_m$, kennen gelernt. Beide Ringe sind kommutativ. Da wir mit dem Endomorphismenring einer abelschen Gruppe nun einen mit der Struktur dieser Gruppe eng verbundenen, im Allgemeinen nichtkommutativen Ring zur Verfügung haben, wollen wir zum Abschluss des Abschnitts der Frage nachgehen, ob bzw. wie sich die abelsche Gruppe als Modul über ihrem Endomorphismenring auffassen lässt.
Sei A eine abelsche Gruppe. Definieren wir für festes $f \in \mathrm{End}(A)$ die Multiplikation

$$A \to A, \quad a \mapsto f(a),$$

setzen wir also $fa := f(a)$ für $f \in \mathrm{End}(A)$ und $a \in A$, so gelten tatsächlich alle Gesetze für einen unitären $\mathrm{End}(A)$-Modul:

- $(f+g)a = (f+g)(a) = f(a) + g(a) = fa + ga$
- $f(a+b) = f(a) + f(b) = fa + fb$
- $(fg)a = (f \circ g)a = f(g(a)) = f(ga)$
- $1a = \mathrm{id}_A(a) = a$

Wir erhalten also:

Proposition 3.4.8.5. *Jede abelsche Gruppe A ist mit der Multiplikation $fa := f(a)$, $f \in \mathrm{End}(A)$ und $a \in A$, auch ein unitärer $\mathrm{End}(A)$-Modul.*

Analoges gilt, wenn man von Vektorräumen über einem Körper K ausgeht. Von den Endomorphismen verlangt man dann anstatt der Homomorphieeigenschaft bezüglich der Addition sogar Linearität, also zusätzlich $f(\lambda a) = \lambda f(a)$ für $\lambda \in K$. Strukturen dieser Art spielen beim Normalformenproblem quadratischer Matrizen bzw. von Endomorphismen eines endlichdimensionalen Vektorraums eine wichtige Rolle. Wir werden darauf in Algebra II nochmals zu sprechen kommen (siehe Unterabschnitt 7.4.6).
Einige andere Konstruktionen von Moduln über im Allgemeinen nichtkommutativen Ringen ergeben sich aus der folgenden Übungsaufgabe.

UE 204 ► Übungsaufgabe 3.4.8.6. (F) Begründen Sie: **◄ UE 204**

(1) Ist $R \leq S$ ein Unterring von S, dann ist S in natürlicher Weise ein R-Modul.

(2) Fasst man einen Ring (in natürlicher Weise) als Linksmodul über sich selbst auf, so sind seine Linksideale genau die Untermoduln.

(3) Ist R ein Ring und I ein Linksideal von R, dann ist R/I ein Links-R-Modul (obwohl R/I nur für ein beidseitiges Ideal $I \lhd R$ ein Ring ist).

(4) Sind R, S Ringe, $\varphi\colon R \to S$ ein Ringhomomorphismus und A ein S-Modul, dann ist A mit der Funktion $R \times A \to A, (r, a) \mapsto \varphi(r)a$ ein R-Modul.

3.5. Geordnete Gruppen und Körper

Das Monotoniegesetz als Verträglichkeit einer binären Operation mit einer (Halb-)Ordnungsrelation lässt sich ziemlich allgemein fassen (3.5.1). Etwas genauer werden wir uns geordneten Gruppen (3.5.2) und geordneten Körpern, vor allem nochmals $\mathbb{R}$ zuwenden (3.5.3).

3.5.1. Grundlegende Definitionen

Inhalt in Kurzfassung: So wie in den reellen Zahlen das Monotoniegesetz für die Addition (eingeschränkt auch für die Multiplikation) gilt, treten auch allgemeinere relationale Strukturen auf, in denen Verträglichkeitsbedingungen für Operationen und Relationen gelten.

Geordnete Gruppen und ihre Verwandten stellen eine wichtige Brücke zur Modelltheorie und somit zur mathematischen Logik dar, weil sie algebraische mit Ordnungsstruktur verbinden und somit sehr typische Beispiele für relationale Strukturen sind. Ausgangspunkt ist das von den Zahlenbereichen vertraute Monotoniegesetz.

Definition 3.5.1.1. Sei A eine Menge, auf der eine binäre Operation $\circ$ und eine Halbordnung $\leq$ definiert sind. Man sagt, auf $(A, \circ, \leq)$ gilt das *Monotoniegesetz* bezüglich $c \in A$, sofern für alle $a, b \in A$ gilt: $a \leq b$ impliziert $a \circ c \leq b \circ c$ und $c \circ a \leq c \circ b$. Das Monotoniegesetz gilt schlechthin, wenn es für alle $c \in A$ gilt.

Sowohl an die Operation $\circ$ als auch an die Halbordnung $\leq$ können zusätzliche Bedingungen gestellt werden, beispielsweise kann A bezüglich der Halbordnung $\leq$ verbandsgeordnet oder sogar totalgeordnet sein, und die Operation kann assoziativ oder sogar eine Gruppenoperation sein. Auch kann eine weitere binäre Operation ins Spiel kommen, für die wenigstens bezüglich gewisser Elemente das Monotoniegesetz gilt und so, dass beispielsweise ein Ring oder gar ein Körper entsteht. Auf diese Weise lassen sich zahlreiche Begriffe bilden wie halbgeordnete Halbgruppe, verbandsgeordnete Gruppe, geordneter Ring, vollständig angeordnete Körper. Die zugehörigen Strukturtheorien dienen wie gesagt besonders in der Modelltheorie als sehr illustrative Beispiele.
Zum Beispiel fordert man von einem *angeordneten Ring*, dass die Addition das Monotoniegesetz schlechthin erfüllt, die Multiplikation bezüglich positiver Elemente $c > 0$. Ein *angeordneter Körper* ist ein angeordneter Ring, der auch ein Körper ist.
Hier wollen wir uns auf einige wenige Bemerkungen zu geordneten Gruppen und zu angeordneten Körpern beschränken.

3.5.2. Geordnete Gruppen

Inhalt in Kurzfassung: Unter den geordneten abelschen Gruppen sind die archimedisch angeordneten insofern von besonderem Interesse, als es sich dabei bis auf Isomorphie genau um die additiven Untergruppen von $\mathbb{R}$ handelt.

Der Deutlichkeit halber stellen wir die Definition explizit voran:

Definition 3.5.2.1. Eine (*total-*)*geordnete Gruppe* ist eine Gruppe G zusammen mit einer binären Relation $\leq$, die G zu einer Totalordnung macht, sodass bezüglich der binären Gruppenoperation das Monotoniegesetz gilt. Ist e das Einheitselement, so heißt $G^+ := \{g \in G \mid g > e\}$ der *Positivteil* von G und $G^- := \{g \in G \mid g < e\}$ der *Negativteil* von G. Die Elemente von G^+ heißen *positiv*. Wir schreiben auch $G^* := G \backslash \{e\} = G^+ \cup G^-$.

Ziemlich leicht beweist man folgende elementare Sachverhalte:

Proposition 3.5.2.2. *Sei G eine geordnete Gruppe mit Elementen $a, b, c \in G$. Dann gilt:*

(1) *G^+ und G^- sind Unterhalbgruppen von G.*

(2) *Die Beziehung $a \leq b$ gilt genau dann, wenn $b^{-1} \leq a^{-1}$.*

(3) *$G^- = \{g^{-1} \mid g \in G^+\}$*

(4) *Alle $g \in G^*$ haben unendliche Ordnung.*

UE 205 ▶ Übungsaufgabe 3.5.2.3. (V) Beweisen Sie Proposition 3.5.2.2. **◀ UE 205**

Definition 3.5.2.4. Eine geordnete Gruppe heißt *archimedisch angeordnet*, wenn es zu je zwei Elementen $a, b \in G^*$ ein $k \in \mathbb{Z}$ gibt mit $b < a^k$.

Die additive Gruppe der reellen Zahlen und alle ihre Untergruppen (wie z. B. $\mathbb{Z}$ und $\mathbb{Q}$) sind Beispiele archimedisch geordneter Gruppen. Im kommutativen Fall handelt es sich dabei im Wesentlichen sogar um die einzigen Beispiele:

Satz 3.5.2.5. *Jede archimedisch angeordnete abelsche Gruppe G lässt sich isomorph in die geordnete additive Gruppe $\mathbb{R}$ der reellen Zahlen einbetten. (Umgekehrt ist jede additive Untergruppe von $\mathbb{R}$ archimedisch angeordnet.) Ist $\iota : G \to \mathbb{R}$ eine solche isomorphe Einbettung, so sind alle anderen gegeben durch sämtliche Abbildungen $\lambda\iota$ mit reellem $\lambda > 0$.*

UE 206 ▶ Übungsaufgabe 3.5.2.6. (V,W) Beweisen Sie Satz 3.5.2.5. Anleitung für die Existenz von ι: Gehen Sie für nichttriviales G von einem positiven Element $g \in G$ aus, das Sie auf die reelle Zahl $1 = \iota(g)$ abbilden. Wegen der archimedischen Eigenschaft definiert das einen eindeutigen ordnungsverträglichen Homomorphismus ι, der (wieder wegen der archimedischen Eigenschaft) sogar injektiv sein muss. **◀ UE 206**

Nicht archimedisch angeordnet ist beispielsweise $\mathbb{Z} \times \mathbb{Z}$ mit der sogenannten *lexikographischen Ordnung*: $(k_1, l_1) < (k_2, l_2)$ genau dann, wenn $k_1 < k_2$ oder $k_1 = k_2 \wedge l_1 < l_2$ gilt.

UE 207 ▶ Übungsaufgabe 3.5.2.7. (B) Beweisen Sie, dass diese Festlegung $\mathbb{Z} \times \mathbb{Z}$ zu einer geordneten Gruppe macht, die jedoch nicht archimedisch geordnet ist. **◀ UE 207**

UE 208 ▶ Übungsaufgabe 3.5.2.8. (B) Zeigen Sie, dass es überabzählbar viele Ordnungsrelationen gibt, die die Gruppe $\mathbb{Z} \times \mathbb{Z}$ zu einer archimedisch geordneten Gruppe machen. Hinweis: Betrachten Sie für irrationales α die Abbildung $\varphi_\alpha \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$, definiert durch $\varphi_\alpha(a, b) := a + \alpha b$, und übertragen Sie damit die Struktur von $\mathbb{R}$ als geordnete Gruppe auf $\mathbb{Z} \times \mathbb{Z}$. **◀ UE 208**

3.5.3. Angeordnete Körper und nochmals $\mathbb{R}$

Inhalt in Kurzfassung: Wir besprechen die bereits in Unterabschnitt 1.2.3 angekündigte Konstruktion der reellen Zahlen mittels Dedekindscher Schnitte und die Tatsache, dass $\mathbb{R}$ bis auf Isomorphie eindeutig bestimmt ist durch die Eigenschaften eines vollständig angeordneten Körpers. Dies zu beweisen ist das Ziel. Die wichtigsten Zwischenergebnisse auf diesem Weg sind auch für sich bemerkenswert. Sie lauten: Jeder vollständig angeordnete Körper ist archimedisch angeordnet. Jeder archimedisch angeordnete Körper lässt sich (sogar auf eindeutige Weise) in $\mathbb{R}$ einbetten. Abschließend wird der Körper der gebrochen rationalen Funktionen über $\mathbb{Q}$ betrachtet.

Wir beginnen mit den Grundgedanken der Konstruktion von $\mathbb{R}$ mit Hilfe Dedekindscher Schnitte:
Jede irrationale Zahl $r \in \mathbb{R} \setminus \mathbb{Q}$ definiert eine Zerlegung (einen Schnitt) der Menge $\mathbb{Q}$ in die beiden Mengen $A_r = \{q \in \mathbb{Q} \mid q < r\}$ und $B_r = \mathbb{Q} \setminus A_r = \{q \in \mathbb{Q} \mid q > r\}$. Es liegt also nahe, die Zahl r mit der Partition von $\mathbb{Q}$ in die Mengen A_r und B_r zu identifizieren. Will man (das bietet gewisse formale Annehmlichkeiten) auch rationale $r \in \mathbb{Q}$ so repräsentieren, hat man zusätzlich lediglich festzulegen, wie man mit r selbst umgeht. (Wir entscheiden uns hier für die Konvention, r in der Menge A_r aufzunehmen und nicht in B_r und dann r durch (A_r, B_r) zu ersetzen.) Bei diesem auf Richard Dedekind (1831–1916) zurückgehenden Zugang fasst man also $\mathbb{R}$ im Wesentlichen auf als die Menge aller Zerlegungen (A, B) von $\mathbb{Q}$ in einen linken Teil A (im rationalen Fall mit Endpunkt) und einen rechten Teil B (ohne Endpunkt). Setzt man $(A_1, B_1) \leq (A_2, B_2)$ sofern $A_1 \subseteq A_2$, beweist man für die resultierende Struktur leicht die Vollständigkeit, dass nämlich jede nichtleere und beschränkte Teilmenge ein Supremum besitzt.

UE 209 ► **Übungsaufgabe 3.5.3.1.** (E,D) Zeigen Sie, dass sich die oben skizzierte Dedekind-Vervollständigung in allgemeinerem Kontext durchführen lässt. In einer beliebigen Halbordnung $(H, \leq)$ kann man nämlich jedem $h \in H$ die Menge $\iota(h) := \{x \in H \mid x \leq h\}$ zuordnen. Gehen Sie diesem Ansatz nach und versuchen Sie einen möglichst allgemeinen Satz über die Möglichkeit der Vervollständigung von Halbordnungen zu formulieren und zu beweisen. Gibt es dazu auch eine kategorientheoretische Formulierung? (Die resultierende Konstruktion heißt *Dedekind-MacNeille-Vervollständigung*.) ◄ **UE 209**

Zurück zu den reellen Zahlen: Als Nächstes definieren wir die Rechenoperationen Addition und Multiplikation auf der Menge $\mathbb{R}$. Dies erfordert etwas mühsame Fallunterscheidungen, der Beweis, dass sich ein angeordneter Körper ergibt, noch mühsamere Rechnungen. Mit etwas Fleiß verifiziert man aber, dass alle Punkte aus der Definition des angeordneten Körpers erfüllt sind.

Definition 3.5.3.2. Seien (A, B) und (A', B') zwei Dedekindschnitte. Wir setzen $A_0 := \{q \in \mathbb{Q} \mid q \leq 0\}$, $B_0 := \mathbb{Q} \setminus A_0 = \{q \in \mathbb{Q} \mid q > 0\}$ und definieren

- Addition: $(A, B) + (A', B') := \Big(A + A', \mathbb{Q} \setminus (A + A')\Big)$
  (wobei bekanntlich $A + A' = \{a + a' \mid a \in A, a' \in A'\}$)

- Multiplikation:
  - Wenn $(A, B), (A', B') \geq (A_0, B_0)$, dann
    $(A, B) \cdot (A', B') := \Big(A \cdot A', \mathbb{Q} \setminus (A \cdot A')\Big)$.
  - Wenn $(A, B) \geq (A_0, B_0)$ und $(A', B') \leq (A_0, B_0)$, dann
    $(A, B) \cdot (A', B') := \Big(-(A \cdot (-A')), \mathbb{Q} \setminus -(A \cdot (-A'))\Big)$.
  - Wenn $(A, B) \leq (A_0, B_0)$ und $(A', B') \geq (A_0, B_0)$, dann
    $(A, B) \cdot (A', B') := \Big((-A) \cdot A', \mathbb{Q} \setminus ((-A) \cdot A')\Big)$.
  - Wenn $(A, B), (A', B') \leq (A_0, B_0)$, dann
    $(A, B) \cdot (A', B') := \Big((-A) \cdot (-A'), \mathbb{Q} \setminus ((-A) \cdot (-A'))\Big)$.

  (wobei bekanntlich $A \cdot A' = \{a \cdot a' \mid a \in A, a' \in A'\}$ und $-A = \{-a \mid a \in A\}$)

Zur Erinnerung die Definition nochmals explizit:

Definition 3.5.3.3. Ist K ein Körper und $\leq$ eine Totalordnung auf K, so sprechen wir von einem *angeordneten Körper*, wenn sowohl K bezüglich der Addition als auch die positiven Elemente bezüglich der Multiplikation mit $\leq$ eine geordnete Gruppe bilden. Explizit bedeutet dies, dass die Monotoniegesetze erfüllt sind: Aus $a \leq b \in K$ und $c \in K$ folgt $a + c \leq b + c$ und, sofern $c \geq 0$, auch $ac \leq bc$.
Ein angeordneter Körper K heißt *vollständig angeordnet*, wenn er als Ordnung bedingt vollständig ist, also wenn jede nichtleere beschränkte Teilmenge ein Supremum und ein Infimum hat.
Ein angeordneter Körper K heißt *archimedisch angeordnet*, wenn seine additive Gruppe archimedisch angeordnet ist.

UE 210 ► **Übungsaufgabe 3.5.3.4.** (A) Zeigen Sie für jeden Körper K die folgenden beiden Aussagen: ◄ **UE 210**

1. Sei $\leq$ eine Ordnungsrelation auf K, die K zu einem angeordneten Körper macht. Dann bilden die Mengen $K^+ := \{x \in K \mid x > 0\}$, $K^- := \{-x \mid x \in K^+\}$ und $\{0\}$ eine Partition von K. (Man beachte, dass K^+ additiv und multiplikativ abgeschlossen ist.)

2. Sei K^+ eine additiv und multiplikativ abgeschlossene Teilmenge von K derart, dass für $x \in K$ genau eine der drei Bedingungen $x \in K^+$, $-x \in K^+$ oder $x = 0$ erfüllt ist. Wir definieren eine binäre Relation $\leq$ auf K durch: $a \leq b$ genau dann, wenn $b - a \in K^+ \cup \{0\}$. Dann wird K durch $\leq$ zu einem angeordneten Körper.

Für die Vollständigkeit gibt es zahlreiche äquivalente Bedingungen, wie die folgende Übungsaufgabe zeigt.

UE 211 ► Übungsaufgabe 3.5.3.5. (F,D) Sei K bezüglich $\leq$ ein angeordneter Körper. **◄ UE 211**

1. Zeigen Sie, dass genau dann ein vollständig angeordneter Körper vorliegt, wenn zu je zwei nichtleeren Teilmengen $A, B \subseteq K$ mit $a \leq b$ für alle $a \in A$ und $b \in B$ ein Element $x \in K$ gibt mit $a \leq x \leq b$ für alle $a \in A$ und $b \in B$.

2. Finden Sie noch weitere zur Vollständigkeit des angeordneten Körpers äquivalente Bedingungen.

Doch nochmals zurück zur Konstruktion von $\mathbb{R}$.

UE 212 ► Übungsaufgabe 3.5.3.6. (V) Besprechen Sie die einzelnen Schritte, die für die eingangs skizzierte Konstruktion von $\mathbb{R}$ mittels Dedekindscher Schnitte nötig sind sowie für den Beweis, dass man so wirklich einen vollständig angeordneten Körper erhält. **◄ UE 212**

Jeder angeordnete Körper K enthält eine Kopie von $\mathbb{N}, \mathbb{Z}$ und $\mathbb{Q}$, genauer:

Definition 3.5.3.7. Sei K ein angeordneter Körper. Dann bezeichne $\mathbb{N}_K$ den Durchschnitt (d. h. die kleinste) aller bezüglich $+$ abgeschlossenen Teilmengen von K, die 0 und 1 enthalten (also die von 0 und 1 erzeugte additive Unterhalbgruppe). Ähnlich bezeichne $\mathbb{Z}_K$ die von 1 erzeugte additive Untergruppe und $\mathbb{Q}_K$ den von $\mathbb{Z}_K$ erzeugten Unterkörper von K, den sogenannten *Primkörper*.

UE 213 ► Übungsaufgabe 3.5.3.8. (W) Zeigen Sie für einen angeordneten Körper K: **◄ UE 213**

(1) $(\mathbb{N}_K, 0_K, \nu_K, +_K, \cdot_K, \leq_K)$ (bei kanonischer Interpretation, insbesondere der Nachfolgerfunktion $\nu_K : k \mapsto k +_K 1_K$) ist ein Modell der Peano-Arithmetik. Also lässt sich $\mathbb{N}_K$ auch als Halbring auffassen, der isomorph ist zum Halbring $\mathbb{N}$ der natürlichen Zahlen.

(2) $\mathbb{Z}_K$ ist sogar ein Unterring von K und als solcher isomorph zum Ring $\mathbb{Z}$ der ganzen Zahlen.

(3) $\mathbb{Q}_K$ ist isomorph zum Körper $\mathbb{Q}$ der rationalen Zahlen.

(4) Die Isomorphismen aus (1), (2) und (3) sind eindeutig und setzen einander fort.

(5) Die Isomorphismen aus (1), (2) und (3) sind auch mit der Ordnungsstruktur verträglich.

(Geben Sie jeweils explizite Isomorphismen an und begründen Sie, warum Ihre Definitionen tatsächlich wohldefinierte Abbildungen liefern.)

Wir wenden uns nun der Rolle der archimedischen Eigenschaft zu.

UE 214 ► Übungsaufgabe 3.5.3.9. (V) Zeigen Sie, dass für einen angeordneten Körper K folgende Eigenschaften äquivalent sind: **◄ UE 214**

(1) K ist archimedisch angeordnet.

(2) $\mathbb{N}_K$ ist unbeschränkt.

(3) Sei $a \in K$ und gelte $a \leq \frac{1}{n} = n^{-1}$ für alle $n \in \mathbb{N}_K \setminus \{0\}$. Dann folgt $a \leq 0$.

(4) $\mathbb{Q}_K$ liegt dicht in K. Definitionsgemäß bedeutet dies: Für beliebige $a, b \in K$ mit $a < b$ gibt es $q \in \mathbb{Q}_K$ mit $a < q < b$.

Wichtig ist folgender Satz:

Satz 3.5.3.10. *Jeder vollständig angeordnete Körper ist archimedisch angeordnet. Insbesondere ist $\mathbb{R}$ archimedisch angeordnet.*

Beweis. Wir nehmen indirekt an, der vollständig angeordnete Körper K sei nicht archimedisch angeordnet. Dann folgt mit Übungsaufgabe 3.5.3.9, dass die Menge $\mathbb{N}_K$ beschränkt ist und somit auch ein Supremum s hat. Nach der Definition des Supremum ist die Zahl $s - 1 < s$ sicher keine obere Schranke von $\mathbb{N}_K$. Also gibt es ein $n \in \mathbb{N}_K$ mit $s - 1 < n$. Die Monotonie der Addition liefert $s = (s - 1) + 1 < n + 1 \in \mathbb{N}_K$. Das steht aber im Widerspruch dazu, dass s eine obere Schranke von $\mathbb{N}_K$ ist. □

Aus der Dichtheit von $\mathbb{Q}_K$ in einem archimedisch angeordneten Körper K folgt, dass jedes Element $k \in K$ eindeutig bestimmt ist durch den von k induzierten Dedekindschen Schnitt, d. h. durch die Menge $A_k := \{q \in \mathbb{Q}_K \mid q < k\}$ sowie durch die Menge $B_k := \{q \in \mathbb{Q}_K \mid q \geq k\}$. Ist K sogar vollständig angeordnet, entspricht umgekehrt jedem Dedekindschen Schnitt (A, B) ein eindeutiges $k \in K$ mit $(A, B) = (A_k, B_k)$. Sei $\varphi\colon \mathbb{Q} \to \mathbb{Q}_K$ der Körperisomorphismus aus Übungsaufgabe 3.5.3.8. Aus unseren Überlegungen folgt, dass sich φ zu einem eindeutigen Isomorphismus zwischen den vollständig angeordneten Körpern $\mathbb{R}$ und K fortsetzen lässt. Damit haben wir im Wesentlichen folgenden wichtigen Satz bewiesen, der die ausgezeichnete Rolle der reellen Zahlen (sowohl als System als auch auf jede einzelne reelle Zahl bezogen) zum Ausdruck bringt.

Satz 3.5.3.11. *Ist K ein archimedisch angeordneter Körper, so gibt es eine eindeutige isomorphe Einbettung $\varphi\colon K \to \mathbb{R}$ (als angeordneter Körper). Ist K vollständig, so ist φ sogar surjektiv, also ein Isomorphismus.*

UE 215 ▶ **Übungsaufgabe 3.5.3.12.** (V) Rekapitulieren Sie den Beweis von Satz 3.5.3.11 und führen Sie allfällige bisher nur knapp dargestellte Argumente sorgfältig aus. ◀ **UE 215**

Bemerkenswerterweise muss man für die Eindeutigkeit des Isomorphismus $\varphi\colon K_1 \to K_2$ zwischen zwei vollständig angeordneten Körpern nicht einmal die Verträglichkeit mit der Ordnungsstruktur verlangen. Denn in diesem Fall ist jeder algebraische Isomorphismus automatisch auch ein Ordnungsisomorphismus. Das ergibt sich aus der folgenden Übungsaufgabe.

UE 216 ▶ **Übungsaufgabe 3.5.3.13.** (V) Seien K, K_1, K_2 angeordnete Körper. Zeigen Sie: ◀ **UE 216**

(1) Für $x \in K$ gilt stets $x^2 \geq 0$ (Quadrate sind nichtnegativ).

(2) Ist K sogar vollständig angeordnet, so ist umgekehrt jedes nichtnegative Element ein Quadrat, also: für $y \in K$, $y \geq 0$, gibt es $x \in K$ mit $y = x^2$.

(3) Ist K_1 vollständig angeordnet, so bildet jeder algebraische Isomorphismus $\varphi\colon K_1 \to K_2$ positive Elemente auf positive ab, negative auf negative.

(4) Sei die Abbildung $\varphi\colon K_1 \to K_2$ verträglich mit der Addition (d. h. $\varphi(a+b) = \varphi(a) + \varphi(b)$ für alle $a, b \in K_1$). Außerdem sei $\varphi(a) \geq 0$ für alle $a \geq 0$. Dann ist φ monoton, also für $a, b \in K$ mit $a \leq b$ folgt stets $\varphi(a) \leq \varphi(b)$.

(5) Sind K_1 und K_2 vollständig angeordnete Körper, so gibt es genau einen algebraischen Isomorphismus $\varphi\colon K_1 \to K_2$. Dieses φ ist auch ein ordnungstheoretischer Isomorphismus. Insbesondere besitzt jeder vollständig angeordnete Körper nur einen einzigen algebraischen Automorphismus, nämlich die Identität.

Folgerung 3.5.3.14. *Jeder vollständig angeordnete Körper K ist als angeordneter Körper zu $\mathbb{R}$ isomorph. Der Isomorphismus ist sogar als algebraischer Isomorphismus eindeutig bestimmt. Insbesondere ist die Identität der einzige Automorphismus des Körpers $\mathbb{R}$.*

Diese Eindeutigkeitsaussagen rechtfertigen, dass man, obwohl formal nicht ganz präzise, schlicht von *den reellen Zahlen* sprechen kann, wenn von irgendeinem vollständig angeordneten Körper die Rede ist. Ebenso kann man die übliche Darstellung reeller Zahlen mit Hilfe unendlicher (meist dekadischer) Ziffernfolgen für die Elemente eines beliebigen vollständig angeordneten Körpers verwenden. Man beachte, dass es wegen der Überabzählbarkeit von $\mathbb{R}$ grundsätzlich unumgänglich ist, unendliche Symbolketten zur Darstellung reeller Zahlen zuzulassen. Denn über einer endlichen (oder auch abzählbar unendlichen) Menge von Symbolen gibt es nur abzählbar viele endliche Symbolketten (oder auch Konfigurationen in einem weiteren Sinne).

UE 217 ► **Übungsaufgabe 3.5.3.15.** (E,D) Rekapitulieren Sie die Darstellung reeller Zahlen als unendliche Dezimalbrüche. Gehen Sie dabei folgendermaßen vor. ◄ **UE 217**

1. Definieren Sie eine fast (in welchem Sinne?) bijektive Abbildung φ zwischen gewissen Symbolketten und den Elementen von $\mathbb{R}$ (gemäß einer Konstruktion Ihrer Wahl).

2. Geben Sie an, auf welcher maximalen Menge die Abbildung φ aus Teil 1 bijektiv ist und wo nicht.

3. Beweisen Sie Ihre Behauptungen aus 2.

4. Welche Probleme treten bei der Suche nach Algorithmen für die Grundrechnungsarten reeller Zahlen auf? Welche Auswege schlagen Sie vor? (Hinweis: Denken Sie etwa an die Addition $\frac{2}{3} + \frac{1}{3}$ oder an die Multiplikation $\sqrt{2} \cdot \sqrt{2}$ in Dezimaldarstellung.)

UE 218 ► **Übungsaufgabe 3.5.3.16.** (E) Zeigen Sie die Überabzählbarkeit[24] von $\mathbb{R}$ auf mehrere Arten: ◄ **UE 218**

1. Unter Verwendung der Zifferndarstellung.
2. Indem Sie zeigen, dass die Potenzmenge einer Menge M echt größer ist als M selbst, und dass die Potenzmenge von $\mathbb{N}$ injektiv nach $\mathbb{R}$ abgebildet werden kann.
3. Indem Sie explizit die Vollständigkeit von $\mathbb{R}$ verwenden: Für jede beliebige Abbildung $f\colon \mathbb{N} \to \mathbb{R}$ können wir ausgehend von der Folge der Werte $f(0), f(1), \ldots$ eine konvergente Folge konstruieren, die gegen ein r konvergiert, das von allen $f(n)$ verschieden ist. Dieses r liegt dann nicht im Wertebereich von f.

Zum Abschluss sei noch kurz auf Beispiele nichtarchimedisch angeordneter Körper eingegangen. Das einfachste ergibt sich fast von selbst aus der folgenden (etwas lückenhaften) Überlegung: Ist K ein angeordneter Körper, so ist $\mathrm{char}(K) = 0$. Also ist der Primkörper $\mathbb{Q}_K$ zum archimedisch angeordneten Körper $\mathbb{Q}$ isomorph (siehe auch Übungsaufgabe 3.5.3.8). Wenn K nicht archimedisch angeordnet ist, muss es folglich Elemente $x \notin \mathbb{Q}_K$ geben. Soll K nicht archimedisch angeordnet sein, so muss es (warum genau?) auch solche geben, die größer als alle rationalen Elemente sind. Halten wir solch ein x mit $x > q$ für alle $q \in \mathbb{Q}_K$ fest. Dann muss auch $x < x^2 < x^3 < \ldots$ gelten, ganz analog zum asymptotischen Verhalten von Polynomen und auch gebrochen rationalen Funktionen $q(x)$ über $\mathbb{Q}$ für $x \to \infty$. Der Körper der gebrochen rationalen Funktionen wird tatsächlich auf diese Weise zu einem nichtarchimedisch angeordneten Körper, der sich überdies in jeden anderen nichtarchimedisch angeordneten Körper einbetten lässt:

Satz 3.5.3.17. *Auf dem Körper $\mathbb{Q}(x)$ der gebrochen rationalen Funktionen sei eine Relation $<$ definiert durch $q_1(x) \leq q_2(x)$, falls $q_1 = q_2$ oder es ein $r_0 > 0$ gibt mit $q_1(r) < q_2(r)$ (in $\mathbb{R}$) für alle $r > r_0$. Zeigen Sie:*

(1) *Mit der so definierten Relation $\leq$ ist $\mathbb{Q}(x)$ ein nichtarchimedisch angeordneter Körper.*

(2) *$\mathbb{Q}(x)$ lässt sich als angeordneter Körper in jeden anderen nichtarchimedisch angeordneten Körper isomorph einbetten.*

UE 219 ► **Übungsaufgabe 3.5.3.18.** (V) Beweisen Sie Satz 3.5.3.17. ◄ **UE 219**

Eine besondere Rolle spielen nichtarchimedisch angeordnete Körper als sogenannte Nonstandard-Modelle von $\mathbb{R}$. Obwohl sie zum Körper der reellen Zahlen natürlich nicht isomorph sein können haben Sie dieselbe Theorie erster Ordnung. Ihre Konstruktion ist in höchstem Maße nichtkonstruktiv und verwendet typischerweise Ultrafilter bzw. Ultraprodukte.

[24] Definitionsgemäß heißt eine unendliche Menge M überabzählbar, wenn es keine bijektive Abbildung von M nach $\mathbb{N}$ gibt; äquivalent dazu: M ist nicht leer, und es gibt keine surjektive Abbildung von $\mathbb{N}$ nach M. Weiters äquivalent: Es gibt keine injektive Abbildung von M nach $\mathbb{N}$.

3.6. Verbände und Boolesche Algebren

Im Vergleich zu den bisher untersuchten klassischen algebraischen Strukturen spielen Verbände eine deutlich andere Rolle. Das liegt zu einem guten Teil an ihrem ordnungstheoretischen Charakter. Dieser zeigt sich an elementaren Eigenschaften (3.6.1), an ihren Unter- (3.6.2) und Faktorstrukturen (3.6.3) wie auch an der besonderen Rolle der vollständigen Verbände (3.6.4). Interessante Untervarietäten bilden distributive wie auch modulare Verbände (3.6.5). Besonders wichtig sind Boolesche Algebren, die sich wiederum sogar als spezielle (kommutative) Ringe, sogenannte Boolesche Ringe auffassen lassen (3.6.6). Nach der Behandlung von Atomen (3.6.7) schließen wir in 3.6.8 mit dem wichtigsten Ergebnis dieses Abschnitts, dem Stoneschen Darstellungssatz. Ihm zufolge ist jede Boolesche Algebra isomorph zu einer Mengenalgebra.

3.6.1. Elementare Eigenschaften

Inhalt in Kurzfassung: Einfachste Begriffe, Rechenregeln und Beispiele zu Verbänden.

Ist $(V, \wedge, \vee)$ ein Verband, so wegen der Symmetrie der Verbandsgesetze auch $(V, \vee, \wedge)$.

Definition 3.6.1.1. Wenn wir den Verband $(V, \wedge, \vee)$ kurz auch mit V bezeichnen, so nennen wir den Verband $(V, \vee, \wedge)$ den zu V *dualen Verband* und bezeichnen ihn mit V^d. Zu jeder Aussage φ über Verbände (im ordnungstheoretischen oder auch im algebraischen Sinn) definieren wir eine Aussage φ^d, die *duale Aussage*, so: Wir ersetzen in φ das Symbol $\wedge$ durch $\vee$, $\vee$ durch $\wedge$, $\leq$ durch $\geq$. (Alle weiteren verbandstheoretischen Konzepte müssen natürlich ebenfalls durch die dualen ersetzt werden – „minimal“ durch „maximal“, inf durch sup, etc.)

Wenn nun die Aussage φ für den Verband V zutrifft (z. B.: „V hat ein größtes Element“), dann trifft die Aussage φ^d auf den Verband V^d zu (z. B.: „V^d hat ein kleinstes Element“). Wenn eine Aussage φ auf alle Verbände zutrifft, dann trifft auch φ^d auf alle Verbände zu.[25] Man nennt dies das *Dualitätsprinzip für Verbände.*

Satz 3.6.1.2 (Rechenregeln für Verbände)**.**

(1) *Die Operationen $\vee$ und $\wedge$ sind monoton. Das heißt, aus $a_1 \leq a_2$ und $b_1 \leq b_2$ folgt $a_1 \wedge b_1 \leq a_2 \wedge b_2$ und $a_1 \vee b_1 \leq a_2 \vee b_2$.*

(2) *$a \leq b \wedge c \Leftrightarrow a \leq b$ und $a \leq c$.*

(3) *$a \geq b \vee c \Leftrightarrow a \geq b$ und $a \geq c$.*

Beweis. (1) ist ein Übungsbeispiel. (2) gilt, weil $b \wedge c$ die *größte* untere Schranke für b und c ist. (3) ist zu (2) dual. □

Wir sammeln einige Beispiele von Verbänden und spezielleren Strukturen (siehe Definition 2.1.3.7 sowie Definition 2.1.4.3).

[25] Achtung: Es kann aber natürlich vorkommen, dass φ nur auf einen bestimmten Verband V zutrifft, nicht aber φ^d.

Proposition 3.6.1.3. *Jede totalgeordnete Menge ist ein distributiver Verband.*

UE 220 ► Übungsaufgabe 3.6.1.4. (V) Beweisen Sie Proposition 3.6.1.3. **◄ UE 220**

UE 221 ► Übungsaufgabe 3.6.1.5. (F) Zeigen Sie: **◄ UE 221**

(1) $(\mathfrak{P}(M), \cap, \cup)$ ist ein Verband und als solcher sogar distributiv.

(2) $(\mathfrak{P}(M), \cap, \cup, \emptyset, M)$ ist ein Verband mit Null- und Einselement.

(3) $(\mathfrak{P}(M), \cap, \cup, \emptyset, M)$ ist ein komplementärer Verband, wobei für $A \subseteq M$ das (eindeutig bestimmte) Komplement durch $A' = M \setminus A$ gegeben ist.

(4) $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ ist eine Boolesche Algebra (und somit auch ein Boolescher Verband).

(5) Sei V Vektorraum über einem Körper K, und sei P die Menge aller Unterräume von V. Für beliebige Unterräume $U_1, U_2 \leq V$ ist auch $U_1 \wedge U_2 := U_1 \cap U_2$ ein Unterraum, ebenso die Menge $U_1 \vee U_2 := [U_1 \cup U_2]$ (die lineare Hülle der Vereinigung der beiden Räume).

Dann ist $(P, \wedge, \vee)$ ein komplementärer Verband. Wenn V mindestens 2-dimensional ist, dann ist P nicht distributiv, und Komplemente sind nicht eindeutig bestimmt.

UE 222 ► Übungsaufgabe 3.6.1.6. (F+) Zeigen Sie: Ist $(V, \wedge, \vee, 0, 1)$ ein beschränkter distributiver Verband, so gibt es zu jedem $a \in V$ höchstens ein Komplement. Was folgt daraus über die Beziehung zwischen Booleschen Algebren und Booleschen Verbänden? **◄ UE 222**

3.6.2. Unterverbände

Inhalt in Kurzfassung: Der Begriff des Unterverbandes fügt sich nahtlos in das allgemeinere Konzept der Unteralgebra ein.

Sei $(V, \wedge, \vee)$ ein Verband. Gemäß unserer allgemeinen Begriffsbildung einer Unteralgebra ist ein *Unterverband* eine Teilmenge von V, die unter $\wedge$ und $\vee$ abgeschlossen ist.

Beispiel 3.6.2.1. Sei $(V, \wedge, \vee)$ ein Verband und sei $\leq$ die zugehörige Ordnung. Wenn $K \subseteq V$ eine Kette in $(V, \leq)$ ist, dann ist K ein Unterverband von V. Insbesondere ist jede einelementige Teilmenge ein Unterverband, ebenso die leere Menge.

Anmerkung 3.6.2.2. Sei V ein Verband mit den Operationen $\wedge$ und $\vee$ und der Ordnung $\leq$. Sei W ein Unterverband; die Operationen von W sind dann die Einschränkungen von $\wedge$ und $\vee$ auf die Menge $W \times W$; wir schreiben wie bisher aber meist $\wedge$ und $\vee$ (oder gelegentlich $\wedge_W$ und $\vee_W$) für diese Operationen, statt genauer $\wedge|_{W\times W}$ und $\vee|_{W\times W}$ zu schreiben.
Die partielle Ordnung von W ist die Einschränkung von $\leq$ auf die Menge W, d. h. formal: die Menge $\{(x, y) \in W \times W \mid x \leq y\}$, oder kürzer $\leq \cap (W \times W)$; wir schreiben $\leq$ oder $\leq_W$ für diese Relation. Die Struktur $(W, \leq)$ ist ein verbandsgeordnete Menge.

UE 223 ► **Übungsaufgabe 3.6.2.3.** (B) Geben Sie einen Verband $(V, \wedge, \vee)$ (mit zugehöriger Ordnungsrelation $\leq$) sowie zwei Untermengen $S_1, S_2 \subseteq V$ an, sodass S_1 ein Unterverband von V ist, S_2 hingegen nicht, aber die partiellen Ordnungen $(S_1, \leq)$ und $(S_2, \leq)$ isomorph sind. ◄ **UE 223**
(Hinweis: Der kleinste solche Verband hat 5 Elemente.)

3.6.3. Kongruenzrelationen; Filter und Ideale

Inhalt in Kurzfassung: Kongruenzrelationen auf Verbänden haben auch ordnungstheoretisch interessante Eigenschaften. So sind die Kongruenzklassen stets konvexe Unterverbände. Eine besondere Rolle spielen Filter und noch spezieller Primfilter und maximale Filter (Ultrafilter). Dual zu Filtern definiert man Ideale (im ordnungs- oder verbandstheoretischen Sinn), Primideale und maximale Ideale.

Lemma 3.6.3.1. *Seien $(V_1, \wedge_1, \vee_1)$ und $(V_2, \wedge_2, \vee_2)$ Verbände mit den zugehörigen Ordnungen $\leq_1$, $\leq_2$, und sei $f\colon V_1 \to V_2$ ein Verbandshomomorphismus.*
Dann erhält f die Ordnung, also: $x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$ für alle $x, y \in V_1$.

Beweis. Wenn $x \leq_1 y$, dann $x \wedge_1 y = x$. Daher $f(x) \wedge_2 f(y) = f(x \wedge_1 y) = f(x)$, also $f(x) \leq_2 f(y)$. □

Eine Kongruenzrelation ist eine Äquivalenzrelation $\theta \subseteq V \times V$, die mit den Operationen $\wedge$ und $\vee$ verträglich ist:

$$\forall a_1, a_2, b_1, b_2 \in V : a_1 \theta a_2, b_1 \theta b_2 \Rightarrow (a_1 \vee b_1)\theta(a_2 \vee b_2),\ (a_1 \wedge b_1)\theta(a_2 \wedge b_2).$$

Aus dem allgemeinen Homomorphiesatz folgt, dass für jeden Verbandshomomorphismus $f\colon V \to W$ die Relation $\{(x, y) \mid f(x) = f(y)\}$ eine Kongruenzrelation ist, und dass alle Kongruenzrelationen diese Form haben.
Es ist nicht immer leicht, festzustellen, ob eine vorliegende Partition tatsächlich von einer Kongruenzrelation kommt. Das folgende Konzept kann manchmal hilfreich sein:

Definition 3.6.3.2. Sei $(L, \leq)$ eine partielle Ordnung.

- Für $a \leq b$ in L definieren wir das *Intervall* $[a, b]$ oder ausführlicher $[a, b]_L$ durch $[a, b] := \{x \in L \mid a \leq x \leq b\}$.
- Eine Teilmenge $A \subseteq L$ heißt *konvex*, wenn $\forall a, b \in A : a < b \Rightarrow [a, b] \subseteq A$ gilt.

Lemma 3.6.3.3. *Sei θ eine Kongruenzrelation auf einem Verband $(V, \wedge, \vee)$. Dann ist jede Kongruenzklasse eine konvexe Menge und ein Unterverband von V.*

Beweis. Es gibt einen Homomorphismus $f\colon (V, \wedge, \vee) \to (W, \wedge, \vee)$, dessen Kern genau θ ist. Jede Klasse $[v]_\theta$ ist von der Form $f^{-1}(w)$ für ein $w \in W$ (nämlich $w := f(v)$).
Wir zeigen zunächst die Konvexität von $[v]_\theta$. Dazu geben wir uns $a \leq x \leq b$ mit $a, b \in [v]_\theta$ (also $f(a) = f(b) = w$) vor; zu zeigen ist $x \in [v]_\theta$ (also $f(x) = w$). Aus Lemma 3.6.3.3 wissen wir $w = f(a) \leq f(x) \leq f(b) = w$ und daher $f(x) = w$.

Nun zeigen wir, dass $[v]_\theta$ ein Unterverband ist. Seien $v_1, v_2 \in [v]_\theta$, d. h. $f(v_1) = f(v_2) = w$. Dann ist $f(v_1 \vee v_2) = w \vee w = w$, also $v_1 \vee v_2 \in [v]_\theta$. Dual ist $[v]_\theta$ auch unter $\wedge$ abgeschlossen. □

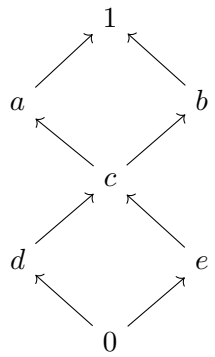
Nicht jede Äquivalenzrelation, deren Klassen konvexe Unterverbände sind, ist eine Kongruenzrelation:

UE 224 ▶ Übungsaufgabe 3.6.3.4. (B) Finden Sie auf dem Verband $\mathfrak{P}(\{1,2\})$ **◀ UE 224**

- ... alle Kongruenzrelationen.
- ... alle Partitionen, deren Klassen konvexe Unterverbände sind.

UE 225 ▶ Übungsaufgabe 3.6.3.5. (B) **◀ UE 225**

Sei $(V, \wedge, \vee)$ der durch das nebenstehende Diagramm gegebene Verband.
Finden Sie alle Kongruenzrelationen von V, geben Sie für jede dieser Kongruenzrelationen θ einen surjektiven Homomorphismus auf einen Verband V_θ an, und beschreiben Sie V_θ durch sein Hasse-Diagramm.



Definition 3.6.3.6. Sei $(V, \leq)$ ein Verband, und sei $\emptyset \neq A \subseteq V$.

- Die Menge A heißt *Filter*, wenn A unter $\wedge$ und nach oben abgeschlossen ist: $x, y \in A \Rightarrow x \wedge y \in A$ und $x \in A, a \in V, a \geq x \Rightarrow a \in A$.
- Dual dazu: Die Menge A heißt *Ideal*, wenn A unter $\vee$ und nach unten abgeschlossen ist: $x, y \in A \Rightarrow x \vee y \in A$ und $x \in A, a \in V, a \leq x \Rightarrow a \in A$.
- Ein Filter $F \subsetneq V$ heißt *Primfilter*, wenn

  $$\forall x, y \in V : x \vee y \in F \Rightarrow x \in F \text{ oder } y \in F,$$

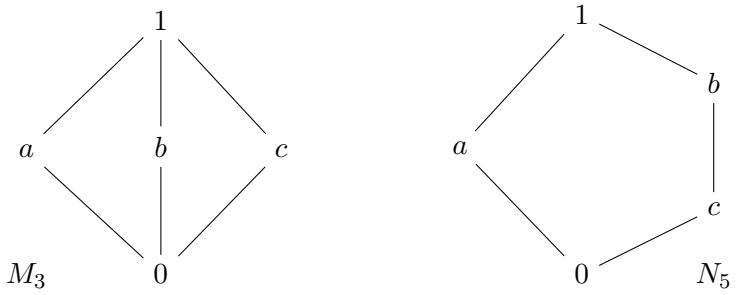
  oder äquivalent, wenn $V \setminus F$ ein Ideal ist.
- Ein Ideal $I \subsetneq V$ heißt *Primideal*, wenn $V \setminus I$ ein Filter ist.
- Ein Filter $F \subsetneq V$ heißt *maximaler Filter*, wenn es außer V selbst keine Obermenge von F gibt, die ein Filter ist.

Die leere Menge ist weder Ideal noch Filter. Der ganze Verband V gilt als *uneigentliches Ideal* bzw. als *uneigentlicher Filter*. Maximale Filter sind maximale Elemente in der durch $\subseteq$ gegebenen partiellen Ordnung aller eigentlichen Filter.

UE 226 ► **Übungsaufgabe 3.6.3.7.** (F) Sei V Verband, $F \subsetneq V$ ein Filter. Dann ist F genau dann maximal, wenn für alle $x \in V \setminus F$ gilt: Für alle $v \in V$ gibt es ein $f \in F$ mit $x \wedge f \leq v$. ◄ **UE 226**

UE 227 ► **Übungsaufgabe 3.6.3.8.** (B) Finden Sie im Verband $(\{0,1,2,3\}, \min, \max)$ alle echten Filter, alle maximalen Filter und alle Primfilter. ◄ **UE 227**

Definition 3.6.3.9. Mit M_3 bezeichnen wir jenen 5-elementigen Verband, der neben seinem kleinsten Element 0 und dem größten Element 1 noch 3 paarweise unvergleichbare Elemente enthält. Der Verband N_5 hat ebenfalls 5 Elemente; neben 0 und 1 enthält er 3 Elemente, von denen zwei vergleichbar sind.



UE 228 ► **Übungsaufgabe 3.6.3.10.** (B) Finden Sie alle Primfilter und alle maximalen Filter auf M_3 und N_5. ◄ **UE 228**

UE 229 ► **Übungsaufgabe 3.6.3.11.** (F) Seien V_1 und V_2 Verbände, und sei F_2 ein Filter auf V_2. Sei $f : V_1 \to V_2$ surjektiver Homomorphismus. Dann ist $f^{-1}(F_2)$ Filter auf V_1. Insbesondere ist das Urbild der 1 in F_2 (sofern vorhanden) ein Filter in V_1. ◄ **UE 229**

3.6.4. Vollständige Verbände

Inhalt in Kurzfassung: Wiederholung des Begriffs des vollständigen Verbands, hauptsächlich in Form von Übungsaufgaben.

Definition 3.6.4.1. Wir nennen einen Verband $(V, \wedge, \vee)$ *vollständig*, wenn V mit der Verbandsordnung vollständig ist, also wenn jede Menge ein Infimum und ein Supremum hat.

Insbesondere ist jede vollständige partielle Ordnung eine verbandsgeordnete Menge, kann also als vollständiger Verband aufgefasst werden.

UE 230 ► **Übungsaufgabe 3.6.4.2.** (F) Ist jede bedingt vollständige Halbordnung ein Verband? ◄ **UE 230**

Aus Proposition 2.1.2.17 wissen wir: Wenn $(P, \leq)$ eine Halbordnung ist, in der jede Teilmenge ein Infimum hat, dann hat auch jede Teilmenge von P ein Supremum. Insbesondere liegt ein vollständiger Verband vor.

UE 231 ► **Übungsaufgabe 3.6.4.3.** (F) Man formuliere die duale Aussage und führe einen Beweis unter Verwendung der bereits bewiesenen. ◄ **UE 231**

UE 232 ► **Übungsaufgabe 3.6.4.4.** (B) Man bestimme das Hasse-Diagramm des Verbandes der Untergruppen der Symmetriegruppe D_4 des Quadrats, das ist die Menge der Isometrien auf $\mathbb{R}^2$, die das Quadrat $\{(1,0),(0,1),(-1,0),(0,-1)\}$ als Menge invariant lassen (also Drehungen und Spiegelungen). ◄ **UE 232**

UE 233 ► **Übungsaufgabe 3.6.4.5.** (E) Geben Sie einen Verband V an, der zu keinem Verband $\mathrm{Sub}(\mathfrak{A})$ isomorph ist: $\forall \mathfrak{A} : \mathfrak{A}$ Algebra $\Rightarrow V \ncong \mathrm{Sub}(\mathfrak{A})$.
(Hinweis: Vergleichen Sie mit der Formulierung der nächsten Übungsaufgabe.) ◄ **UE 233**

UE 234 ► **Übungsaufgabe 3.6.4.6.** (E) Geben Sie einen vollständigen Verband V an, der zu keinem Verband $\mathrm{Sub}(\mathfrak{A})$ isomorph ist.
(Das ist sehr anspruchsvoll. Hinweis: Recherchieren Sie den Begriff des *algebraischen Verbandes*.) ◄ **UE 234**

UE 235 ► **Übungsaufgabe 3.6.4.7.** (D) Man gebe weitere Beispiele von vollständigen Verbänden an, die in der Mathematik eine wichtige Rolle spielen. ◄ **UE 235**

UE 236 ► **Übungsaufgabe 3.6.4.8.** (E) Sei L ein beliebiger Verband. Dann gibt es einen vollständigen Verband V und einen injektiven Verbandshomomorphismus $f : L \to V$. (Der Verband V ist eine Art „Vervollständigung“ von L.)
Hinweis: OBdA (warum?) hat L ein kleinstes Element. Sei V die Menge aller Ideale von L; dann bildet $(V, \subseteq)$ einen vollständigen Verband (warum?), in den man L einbetten kann (wie?). ◄ **UE 236**

UE 237 ► **Übungsaufgabe 3.6.4.9.** (B) Sei P die Familie aller höchstens abzählbaren Teilmengen $M \subseteq \mathbb{R}$, zusammen mit $\mathbb{R}$ selbst, geordnet durch $\subseteq$:

$$P := \{A \subseteq \mathbb{R} \mid A \text{ abzählbar unendlich}\} \cup \{A \subseteq \mathbb{R} \mid A \text{ endlich}\} \cup \{\mathbb{R}\}.$$

Ist $(P, \subseteq)$ ein vollständiger Verband? ◄ **UE 237**

UE 238 ► **Übungsaufgabe 3.6.4.10.** (E) Geben Sie einen beschränkten Verband an, in dem jede abzählbare Menge eine kleinste obere Schranke hat, der aber nicht σ-vollständig[26] ist. (Hinweis: modifizieren Sie Übungsaufgabe 3.6.4.9.) ◄ **UE 238**

3.6.5. Distributive und modulare Verbände

Inhalt in Kurzfassung: Eine wichtige Abschwächung der Distributivität von Verbänden ist die Modularität. Es folgen die Definitionen sowie Charakterisierungen durch die Nichtexistenz gewisser Unterverbände.

Eine Verschärfung des Begriffs des Verbands bilden die distributiven und die sogenannten *modularen* Verbände. Zur Einstimmung einige Ungleichungen, die in beliebigen Verbänden gelten:

Lemma 3.6.5.1. *In einem Verband $(V, \wedge, \vee)$ gelten stets die folgenden Aussagen:*

1. $\forall x, y, z \in V : x \leq z \Rightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge z$
2. $\forall x, y, z \in V : x \vee (y \wedge (x \vee z)) \leq (x \vee y) \wedge (x \vee z)$
3. $\forall x, y, z \in V : x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$

3'. $\forall x, y, z \in V : x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

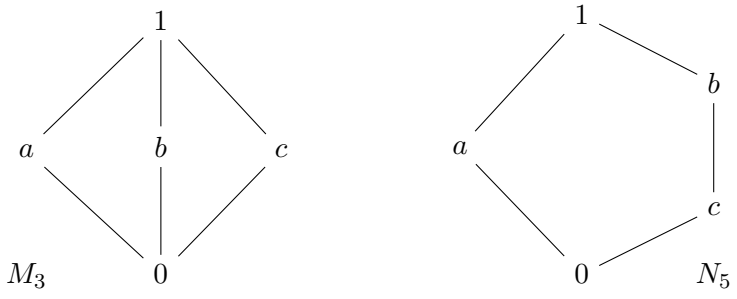
4. $\forall x, y, z \in V : (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \leq (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

UE 239 ► **Übungsaufgabe 3.6.5.2.** (V) Beweisen Sie Lemma 3.6.5.1. ◄ **UE 239**

Die erste Aussage gibt Anlass zur folgenden Definition:

Definition 3.6.5.3. Ein Verband $(V, \wedge, \vee)$ heißt modular, wenn für alle $x, y, z \in V$ aus $x \leq z$ stets $x \vee (y \wedge z) = (x \vee y) \wedge z$ folgt.

Wichtige Beispiele modularer Verbände sind – wie man leicht nachprüft – Totalordnungen $(P, \min, \max)$, Potenzmengenverbände $(\mathfrak{P}(M), \cap, \cup)$ oder auch der Verband M_3 aus Definition 3.6.3.9. Kein modularer Verband ist N_5, wie man unmittelbar erkennt, wenn man $x = c$, $y = a$ und $z = b$ setzt[27].



[26] Ein Verband V heißt σ-vollständig, wenn jede abzählbar unendliche Teilmenge von V eine kleinste obere und eine größte untere Schranke hat.

[27] Tatsächlich steht M_3 für **m**odular und N_5 für **n**ichtmodular.

Weitere Beispiele und Nicht-Beispiele ergeben sich aus den folgenden Übungsaufgaben:

UE 240 ► Übungsaufgabe 3.6.5.4. (B) Man zeige: **◄ UE 240**

(1) Der Verband der Normalteiler einer Gruppe ist modular, ebenso der Verband der Ideale in einem Ring.

(2) Der Verband der Äquivalenzrelationen auf einer Menge M mit $|M| \geq 4$ ist nicht modular. Geben Sie eine Varietät $\mathcal{V}$ an, sodass nicht alle Strukturen aus $\mathcal{V}$ einen modularen Kongruenzverband haben.

UE 241 ► Übungsaufgabe 3.6.5.5. (B) Man zeige am Beispiel der alternierenden Gruppe A_4, dass der Untergruppenverband einer Gruppe nicht modular sein muss. **◄ UE 241**

Da die obige Definition eines modularen Verbands kein Gesetz im Sinne von Definition 2.1.8.6 ist (das Problem ist nicht die Ungleichung, die man nämlich auch als $x \wedge z = x$ umformulieren könnte, sondern die Implikation), ist bisher noch nicht klar, ob die modularen Verbände eine Varietät bilden. Dass folgende Lemma zeigt unter anderem, dass dies tatsächlich der Fall ist.

Lemma 3.6.5.6. *Sei $(M, \wedge, \vee)$ ein Verband. Dann sind die folgenden Aussagen äquivalent:*

(1) $\forall x, y, z \in M : x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$ *(d. h., M ist modular)*

(2) $\forall x, y, z \in M : x \leq z \Rightarrow x \vee (y \wedge z) \geq (x \vee y) \wedge z$

(3) $\forall x, y, z \in M : x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$

(4) $\forall x, y, z \in M : x \vee (y \wedge (x \vee z)) \geq (x \vee y) \wedge (x \vee z)$

Insbesondere (Aussage (3)) ist die Klasse der modularen Verbände eine Varietät.

UE 242 ► Übungsaufgabe 3.6.5.7. (V) Beweisen Sie Lemma 3.6.5.6. **◄ UE 242**

Als wesentliche Aussage über modulare Verbände wollen wir die folgende Charakterisierung beweisen:

Satz 3.6.5.8. *Für einen Verband $(M, \wedge, \vee)$ sind die folgenden Bedingungen äquivalent:*

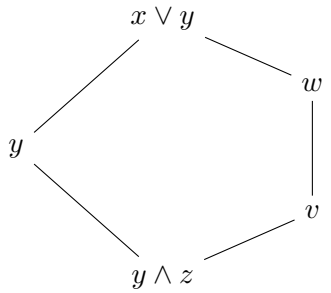
(1) *M ist modular.*

(2) *M besitzt keinen Unterverband, der zum Fünfeck N_5 isomorph ist*[28].

Beweis. Wir zeigen die Äquivalenz der Negationen. Wenn M einen zu N_5 isomorphen Unterverband hat, dann folgt die Nichtmodularität von M genauso wie die Nichtmodularität von N_5 – die Tatsache, dass die Kopie von N_5 ein Unterverband von M ist, geht dadurch ein, dass dann die sich aus dem Hasse-Diagramm ergebenden Infima und Suprema genau die Ergebnisse der Operationen $\wedge$ und $\vee$ in M sind.

[28] Man beachte: *nicht* als Unterverband mit $0, 1$, d. h., selbst wenn M ein größtes und ein kleinstes Element hat, können das größte bzw. kleinste Element der Kopie von N_5 davon verschieden sein.

Sei umgekehrt M nicht modular. Nach Lemma 3.6.5.6 bzw. Lemma 3.6.5.1 gibt es $x, y, z \in M$ mit $x \leq z$ und $x \vee (y \wedge z) < (x \vee y) \wedge z$. Jedenfalls muss $x < z$ sein (da im Falle $x = z$ beide Seiten gleich x sind). Wir setzen $v := x \vee (y \wedge z)$ und $w := (x \vee y) \wedge z$ und behaupten, dass die Elemente $y \wedge z$, y, v, w, $x \vee y$ wie abgebildet einen zu N_5 isomorphen Unterverband bilden.



Jedenfalls klar ist

$$y \wedge z \leq v < w \leq x \vee y.$$

Wäre $y = y \wedge z$, dann würde der Widerspruch $v < w \leq x \vee y = x \vee (y \wedge z) = v$ folgen. Genauso zeigt man $y \neq x \vee y$ und wir erhalten

$$y \wedge z < v < w < x \vee y.$$

Als Nächstes zeigen wir, dass y mit v bzw. w unvergleichbar ist, indem wir jede der vier Möglichkeiten $v \lesseqgtr y \lesseqgtr w$ auf einen Widerspruch führen – daraus folgt dann

$$y \wedge z < y < x \vee y,$$

mit anderen Worten, dass $y \wedge z$, y, v, w, $x \vee y$ eine Kopie von N_5 bilden. Wäre $y \geq w$, dann wäre $w = w \wedge y = (x \vee y) \wedge z \wedge y = y \wedge z$ nach der Kommutativität von $\wedge$ und dem Verschmelzungsgesetz. Aus $y \leq w$ würde genauso $y = y \wedge z$ folgen; aus $v \leq y$ analog $y = x \vee y$. Wäre schließlich $v \geq y$, so wären auch w und y vergleichbar. Zu guter Letzt ist zu beweisen, dass $\{y \wedge z, y, v, w, x \vee y\}$ auch ein Unterverband von M ist. Dazu ist noch $y \wedge v = y \wedge w = y \wedge z$ und $y \vee v = y \vee w = x \vee y$ zu zeigen. Dabei ist $y \wedge w = y \wedge z$ und $y \vee v = x \vee y$ durch Einsetzen unmittelbar klar, für $y \wedge v = y \wedge z$ beachten wir $y \wedge z \leq y, v$ und somit $y \wedge z \leq y \wedge v \leq y \wedge w = y \wedge z$. Analog zeigt man auch $y \vee w = x \vee y$. □

Wir beenden die Untersuchungen modularer Verbände mit einigen weiteren Übungsaufgaben.

UE 243 ► Übungsaufgabe 3.6.5.9. (E) Sei $(M, \wedge, \vee)$ modularer Verband, und seien $a, b \in M$. **◄ UE 243**
Dann sind die Intervalle (siehe Definition 3.6.3.2)

$$[a \wedge b, a] := \{x \in M \mid a \wedge b \leq x \leq a\} \text{ und } [b, a \vee b] := \{x \in M \mid b \leq x \leq a \vee b\}$$

zueinander (verbands)isomorph, und die Abbildung $x \mapsto x \vee b$ ist ein Isomorphismus. Beweisen Sie dies, und geben Sie eine explizite Formel für die Umkehrabbildung an.

UE 244 ► **Übungsaufgabe 3.6.5.10.** (B) Geben Sie einen nichtmodularen Verband V mit der Eigenschaft ◄ **UE 244**

$$\forall a, b \in V : [a \wedge b, a] \cong [b, a \vee b]$$

an. (Hinweis: Erweitern Sie zwei Kopien von $\mathbb{Q}$ auf geeignete Weise zu einem Verband.)

Für distributive Verbände (siehe Definition 2.1.3.7) kann man analog zu Lemma 3.6.5.6 äquivalente Bedingungen finden (man beachte auch Lemma 3.6.5.1):

Lemma 3.6.5.11. *Sei $(V, \wedge, \vee)$ ein Verband. Dann sind die folgenden Aussagen äquivalent:*

(1) $\forall x, y, z \in V : x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ *und* $\forall x, y, z \in V : x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ *(d. h., V ist distributiv)*

(2) $\forall x, y, z \in V : x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

(2') $\forall x, y, z \in V : x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

(3) $\forall x, y, z \in V : x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$

(3') $\forall x, y, z \in V : x \vee (y \wedge z) \geq (x \vee y) \wedge (x \vee z)$

(4) $\forall x, y, z \in V : (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

(5) $\forall x, y, z \in V : (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \geq (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

UE 245 ► **Übungsaufgabe 3.6.5.12.** (V) Beweisen Sie Lemma 3.6.5.11. ◄ **UE 245**
Hinweis für die Implikation (4) ⇒ (2): Zeigen Sie zunächst, dass V modular ist, und betrachten Sie dann $x \wedge \Big((x \vee y) \wedge (y \vee z) \wedge (z \vee x)\Big)$.

Unmittelbar aus der Definition (bzw. als Nebenprodukt des obigen Hinweises) ergibt sich:

Lemma 3.6.5.13. *Wenn ein Verband $(V, \wedge, \vee)$ distributiv ist, dann ist er auch modular.*

Prominente Beispiele distributiver Verbände sind erneut Totalordnungen $(P, \min, \max)$ sowie Potenzmengenverbände $(\mathfrak{P}(M), \cap, \cup)$. Der Verband N_5 kann wegen Lemma 3.6.5.13 nicht distributiv sein, aber auch M_3 ist nicht distributiv – dazu ist nur $x = a$, $y = b$ und $z = c$ zu setzen. Ein weiteres Beispiel ergibt sich durch die folgende Serie an Übungsaufgaben, die zugleich einen Blick auf die Beweismethode des Darstellungssatzes von Stone für Boolesche Algebren (Satz 3.6.8.17) erlaubt.

UE 246 ► **Übungsaufgabe 3.6.5.14.** (F+) Sei $(V, \cap, \cup)$ Mengenverband (das heißt, V ist Teilmenge der Potenzmenge einer Menge M, und $\cap$ bzw. $\cup$ sind mengentheoretischer Durchschnitt bzw. Vereinigung). Man zeige, dass für jedes $m \in M$ die Abbildung $f_m \colon V \to \{0, 1\}$, $f_m(A) = 1$ für $m \in A$, $f_m(A) = 0$ sonst, ein Homomorphismus auf den zweielementigen Verband ist. ◄ **UE 246**

UE 247 ▶ **Übungsaufgabe 3.6.5.15.** (F+) Man verwende die Homomorphismen f_m aus dem vorigen Beispiel, um zu zeigen, dass jeder Mengenverband isomorph zu einem Unterverband eines direkten Produktes von zweielementigen Verbänden ist. (Anleitung: Man betrachte die Einbettung $A \mapsto (f_m(A))_{m\in M}$.) ◀ **UE 247**

UE 248 ▶ **Übungsaufgabe 3.6.5.16.** (F+) Man folgere aus obigen Beispielen, dass Mengenverbände distributiv sind. ◀ **UE 248**

Eine interessante Eigenschaft distributiver Verbände ist:

UE 249 ▶ **Übungsaufgabe 3.6.5.17.** (F) ◀ **UE 249**

(1) Sei $(V, \wedge, \vee)$ ein distributiver Verband, und seien $a, x, y \in V$ mit $a \wedge x = a \wedge y$ und $a \vee x = a \vee y$. Zeigen Sie, dass dann $x = y$.
(Hinweis: Überlegen Sie zunächst ob/warum $(x \wedge y) \vee (x \wedge a) = (x \wedge y) \vee (a \wedge y)$ gilt.)

(2) Finden Sie Elemente $a, x, y \in M_3$ mit $x \neq y$ aber $a \wedge x = a \wedge y$ und $a \vee x = a \vee y$.

(3) Finden Sie Elemente $a, x, y \in N_5$ mit $x \neq y$ aber $a \wedge x = a \wedge y$ und $a \vee x = a \vee y$.

In Analogie zu Satz 3.6.5.8 kann man auch die Klasse der distributiven Verbände durch das Nichtenthalten gewisser Unterverbände charakterisieren.

Satz 3.6.5.18. *Für einen modularen Verband $(V, \wedge, \vee)$ sind die folgenden Bedingungen äquivalent:*

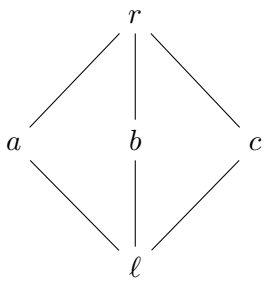
(1) *V ist distributiv.*

(2) *V besitzt keinen Unterverband, der zu M_3 isomorph ist*[29]*.*

Beweis. Wir zeigen wieder die Äquivalenz der Negationen, wobei aus der Existenz eines zu M_3 isomorphen Unterverbands erneut sehr leicht folgt, dass V nicht distributiv ist. Sei also V nicht distributiv. Nach Lemma 3.6.5.11 bzw. Lemma 3.6.5.1 gibt es $x, y, z \in V$ mit

$$\ell := (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) < (x \vee y) \wedge (y \vee z) \wedge (z \vee x) =: r.$$

Wir setzen $a := (r \wedge x) \vee \ell$, $b := (r \wedge y) \vee \ell$, $c := (r \wedge z) \vee \ell$ und behaupten, dass die Elemente ℓ, a, b, c, r wie abgebildet einen zu M_3 isomorphen Unterverband von V bilden.



[29] Siehe Fußnote auf Seite 236.

Mit der Kommutativität und dem Verschmelzungsgesetz ergibt sich $r \wedge x = x \wedge (y \vee z)$, $r \wedge y = y \wedge (z \vee x)$ und $r \wedge z = z \wedge (x \vee y)$. Wegen $\ell \leq (x \wedge (y \vee z)) \vee (y \wedge (z \vee x))$ folgt

$$a \vee b = \Big(x \wedge (y \vee z)\Big) \vee \ell \vee \Big(y \wedge (z \vee x)\Big) = \Big(x \wedge (y \vee z)\Big) \vee \Big(y \wedge (z \vee x)\Big).$$

Unter zweimaliger Verwendung der Modularität (mit den Ungleichungen $x \wedge (y \vee z) \leq z \vee x$ sowie $y \leq y \vee z$) erhalten wir

$$\begin{aligned} a \vee b &= \Big(x \wedge (y \vee z)\Big) \vee \Big(y \wedge (z \vee x)\Big) = \Big[\Big(x \wedge (y \vee z)\Big) \vee y\Big] \wedge (z \vee x) \\ &= \Big[y \vee \Big(x \wedge (y \vee z)\Big)\Big] \wedge (z \vee x) = (y \vee x) \wedge (y \vee z) \wedge (z \vee x) = r. \end{aligned}$$

Analog sieht man $a \vee c = r = b \vee c$. Aufgrund von $\ell < r$ liefert die Modularität $a = r \wedge (x \vee \ell)$, $b = r \wedge (y \vee \ell)$ und $c = r \wedge (z \vee \ell)$, sodass man dual zu oben $a \wedge b = a \wedge c = b \wedge c = \ell$ schließen kann.
Es bleibt zu zeigen, dass die Elemente ℓ, a, b, c, r paarweise verschieden sind. Aus $a = b$ würde der Widerspruch $r = a \vee b = a = a \wedge b = \ell$ folgen; analog beweist man $a \neq c$ und $b \neq c$. Sei jetzt $a = \ell$ angenommen. Dann folgt $a \leq b$, also $b = a \vee b = r$. Genauso ergibt sich $c = r$ und daher der Widerspruch $r = b \wedge c = \ell$. Analog zeigt man $b, c \neq \ell$ sowie $a, b, c \neq r$, was den Beweis abschließt. □

Kombinieren wir Satz 3.6.5.8 mit Satz 3.6.5.18 und beachten, dass ein nichtmodularer Verband auch nicht distributiv sein kann, so ergibt sich:

Folgerung 3.6.5.19. *Für einen Verband $(V, \wedge, \vee)$ sind die folgenden Bedingungen äquivalent:*

(1) *V ist distributiv.*

(2) *V besitzt keinen Unterverband, der zu N_5 oder zu M_3 isomorph ist.*

UE 250 ► **Übungsaufgabe 3.6.5.20.** (D) Man ermittle (bis auf Isomorphie) alle modularen Verbände bis zu einer möglichst großen Kardinalität. Welche davon sind distributiv? ◄ **UE 250**

3.6.6. Boolesche Algebren und Boolesche Ringe

Inhalt in Kurzfassung: Boolesche Algebren sind sehr reichhaltige Spezialisierungen von Verbänden, für die starke Strukturaussagen möglich sind. Ein prominentes Beispiel ist der Potenzmengenverband zusammen mit der mengentheoretischen Komplementbildung. Boolesche Ringe sind Ringe mit 1, in denen die Multiplikation idempotent ist. Sie entsprechen in bijektiver Weise den Booleschen Algebren mit derselben Trägermenge. Dieser Zusammenhang ermöglicht es, Konzepte und Ergebnisse aus der Ringtheorie auf Boolesche Algebren zu übertragen.

Zur Wiederholung: Eine Algebra $(B, \wedge, \vee, 0, 1, ')$ vom Typ $(2, 2, 0, 0, 1)$ ist genau dann eine *Boolesche Algebra*, wenn die folgenden Gesetze gelten (jeweils quantifiziert für alle $a, b, c \in B$):

$$\begin{aligned} a \wedge b &= b \wedge a & a \vee b &= b \vee a \\ a \wedge (b \wedge c) &= (a \wedge b) \wedge c & a \vee (b \vee c) &= (a \vee b) \vee c \\ a \wedge (a \vee b) &= a & a \vee (a \wedge b) &= a \\ a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) & a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \\ 1 \wedge a &= a & 0 \vee a &= a \\ a \wedge a' &= 0 & a \vee a' &= 1 \end{aligned}$$

Anmerkung 3.6.6.1. Manche Autoren[30] verwenden für die Operationen $\vee$, $\wedge$ der Booleschen Algebra die Symbole $+$ und $\cdot$. Wir tun dies nicht, um Verwechslungen mit Booleschen Ringen (siehe Definition 3.6.6.4) zu vermeiden, und um die Verwandtschaft zu Verbänden zu betonen.
Für das Komplement x' werden auch oft andere Symbole verwendet, wie x^c, $-x$, $\neg x$, $\sim x$, $\bar{x}$. In der (sehr wichtigen) Booleschen Algebra $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ ist $X \cap Y'$ genau die Mengendifferenz $X \setminus Y$, weshalb man auch für allgemeine Boolesche Algebren manchmal $x \setminus y := x \wedge y'$ schreibt.

Das Dualitätsprinzip für Verbände lässt sich auf Boolesche Algebren spezialisieren: Ist φ eine Aussage über Boolesche Algebren, so entsteht die duale Aussage φ^d wieder durch Ersetzen von $\wedge$ durch $\vee$, von $\vee$ durch $\wedge$ und von $\leq$ durch $\geq$; neu bei Booleschen Algebren sind die von beschränkten Verbänden kommenden Konstantensymbole 0 und 1 – diese werden vertauscht – und das Komplementsymbol $'$ – dieses bleibt unverändert. Aufseite der Strukturen beobachten wir: Ist $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra, dann ist auch $B^d = (B, \vee, \wedge, 1, 0, ')$ eine Boolesche Algebra. Das *Dualitätsprinzip für Boolesche Algebren* besagt dann: Wenn in B die Aussage φ gilt, dann gilt in B^d die Aussage φ^d. Wenn insbesondere φ in alle Booleschen Algebren gilt, dann auch φ^d.

Satz 3.6.6.2 (Satz über Komplemente)**.** *Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra. Dann gilt:*

(1) *Sind a, a^* Elemente von B mit $a \vee a^* = 1$ und $a \wedge a^* = 0$, so gilt $a^* = a'$.*
(2) *$(a')' = a$ für alle $a \in B$.*
(3) *$0' = 1$ und $1' = 0$.*
(4) *$(a \vee b)' = a' \wedge b'$ und $(a \wedge b)' = a' \vee b'$ für alle $a, b \in B$* (De Morgan'sche Gesetze).

Beweis. (1) folgt aus Übungsaufgabe 3.6.1.6; (2), (3) und (4) folgen aus (1). □

Satz 3.6.6.3 (Rechenregeln für Boolesche Algebren)**.** *Sei B eine Boolesche Algebra. Dann gilt für alle $a, b \in B$:*

(1) *$a \leq b \Leftrightarrow b' \leq a'$. (Man sagt auch, dass die Abbildung $a \mapsto a'$ antimonoton ist.)*

[30] Die Fußnote auf Seite 107 ist geeignet zu adaptieren.

(2) $a \leq b \;\Leftrightarrow\; a' \vee b = 1 \;\Leftrightarrow\; a \wedge b' = 0$.
In Analogie zur Logik wird der Ausdruck $a' \vee b$ manchmal auch mit $a \to b$ abgekürzt, d. h., $\to$ wird als Name einer 2-stelligen Operation verstanden.

(3) $a \leq b' \;\Leftrightarrow\; a \wedge b = 0 \;\Leftrightarrow\; b \leq a'$.
Für die Gleichung $a \wedge b = 0$ verwendet man (in Analogie zur linearen Algebra) auch die Abkürzung $a \perp b$ ab. In diesem Fall heißen a und b disjunkt*.*

Beweis.

(1) Wir verwenden die Regel von de Morgan, $(c')' = c$ sowie die Tatsache, dass man $x \leq y$ in äquivalenter Weise sowohl durch $x \wedge y = x$ als auch durch $x \vee y = y$ definieren kann:

$$a \leq b \;\Leftrightarrow\; a \wedge b = a \;\Leftrightarrow\; (a \wedge b)' = a' \;\Leftrightarrow\; a' \vee b' = a' \;\Leftrightarrow\; b' \leq a'.$$

(2) Wenn $a \leq b$, dann ist $a' \vee b = a' \vee (a \vee b) = 1$. Wenn umgekehrt $a' \vee b = 1$ ist, dann gilt:

$$a = a \wedge 1 = a \wedge (a' \vee b) = (a \wedge a') \vee (a \wedge b) = a \wedge b,$$

also $a \leq b$. Die zweite Äquivalenz folgt dann aus dem Gesetz von de Morgan.

(3) (3) folgt aus (2).

□

Eng mit dem Begriff der Booleschen Algebra verwandt ist das Konzept des Booleschen Rings.

Definition 3.6.6.4. Ein Ring $(R, +, 0, -, \cdot, 1)$ mit Einselement heißt *Boolescher Ring*, wenn $\forall x \in R : x \cdot x = x$ gilt.

Zunächst eine einfache Beobachtung:

Lemma 3.6.6.5. *In jedem Booleschen Ring $(R, +, 0, -, \cdot, 1)$ gilt $x + x = 0$ für alle $x \in R$. Daher ist $-x = x$ für alle x; statt $x - y$ kann man also genauso gut $x + y$ schreiben.*

Beweis. Man berechnet $x + 1 = (x + 1)(x + 1) = xx + x + x + 1 = (x + x) + (x + 1)$ und subtrahiert auf beiden Seiten $x + 1$. □

Die Beziehung zwischen Booleschen Algebren und Booleschen Ringen kommt im folgenden Satz zum Ausdruck.

Satz 3.6.6.6.

(1) *Sei $(R, +, 0, -, \cdot, 1)$ ein Boolescher Ring. Mit den Operationen*

$$x \wedge y := xy, \qquad x \vee y := x + y + xy, \qquad x' := 1 + x \;(= 1 - x)$$

ist die Algebra $(R, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra,
und es gilt $x + y = (x \wedge y') \vee (x' \wedge y)$.

(2) *Sei* $(B, \wedge, \vee, 0, 1, ')$ *eine Boolesche Algebra. Mit den Operationen*

$$x \cdot y := x \wedge y, \qquad x + y := (x \wedge y') \vee (x' \wedge y), \qquad -x := x$$

ist $(B, +, 0, -, \cdot, 1)$ *ein Boolescher Ring,*
und es gilt $x \vee y = x + y + xy = 1 + (1 + x)(1 + y)$.

(3) *Die in (1) und (2) beschriebenen Abbildungen zwischen Booleschen Algebren und Booleschen Ringen sind invers zueinander.*

Weiters gilt: Seien $(R_i, +, 0, -, \cdot, 1)$ *(für* $i = 1, 2$*) Boolesche Ringe, mit zugehörigen Booleschen Algebren* $(R_i, \wedge, \vee, 0, 1, ')$*. Eine Abbildung* $f\colon R_1 \to R_2$ *ist genau dann Ringhomomorphismus, wenn sie ein Homomorphismus von Booleschen Algebren ist.*

UE 251 ▶ **Übungsaufgabe 3.6.6.7.** (V) Beweisen Sie Satz 3.6.6.6. ◀ **UE 251**

Anmerkung 3.6.6.8. Für die Boolesche Algebra $(\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ ist die additive Operation im zugehörien Booleschen Ring genau $X + Y = (X \wedge Y') \vee (Y \wedge X') = X \,\Delta\, Y$, also die symmetrische Differenz der beiden Mengen $X, Y \in \mathfrak{P}(M)$. Daher nennt man die Operation + auch im Allgemeinen „symmetrische Differenz“ und schreibt sie manchmal als $x \,\Delta\, y$.

Boolesche Algebren und Boolesche Ringe beschreiben also „im Wesentlichen“ dieselben Strukturen. Das bedeutet, dass man Boolesche Algebren auch mit Mitteln der Ringtheorie untersuchen kann. Als Beispiel dafür kann der Homomorphiesatz für Boolesche Algebren gesehen haben, dessen Beweis weitgehend parallel zum Beweis des Homomorphiesatzes für Ringe verläuft.

Satz 3.6.6.9 (Homomorphiesatz für Boolesche Algebren)**.** *Sei* $f\colon B_1 \to B_2$ *ein surjektiver Homomorphismus von Booleschen Algebren.*
Dann ist B_2 *zu* $B_1/f^{-1}(0)$ *isomorph, wobei* $B_1/f^{-1}(0)$ *die Menge aller Äquivalenzklassen der Relation*

$$x \sim y \Leftrightarrow x + y \in f^{-1}(0)$$

bezeichnet.

Beweis. Nach dem allgemeinen Homomorphiesatz gilt $B_2 \cong B_1/\ker(f)$, wobei $\ker(f)$ die durch

$$(x, y) \in \ker(f) \;\Leftrightarrow\; f(x) = f(y)$$

definierte Äquivalenzrelation ist. Nun gilt aber

$$f(x) = f(y) \;\Leftrightarrow\; f(x) - f(y) = 0 \;\Leftrightarrow\; f(x) + f(y) = 0 \;\Leftrightarrow\; f(x+y) = 0 \;\Leftrightarrow\; x + y \in f^{-1}\{0\},$$

also stimmt $\ker(f)$ mit $\sim$ überein. □

Jede Kongruenzrelation $\sim$ auf einem Ring, erst recht also auf jedem Booleschen Ring, ist durch ein Ideal charakterisiert, nämlich die Äquivalenzklasse von 0. Da die Ringoperationen durch die Operationen der Booleschen Algebra beschrieben werden (und umgekehrt), sind die Kongruenzrelationen eines Booleschen Rings genau die Kongruenzrelationen der entsprechenden Booleschen Algebra. Die Ringkongruenzen kann man durch Ringideale beschreiben; es wird sich als Nächstes herausstellen, dass diese genau den in Definition 3.6.3.6 definierten Idealen entsprechen.

Definition 3.6.6.10. Für $T \subseteq B$ schreiben wir $T^* := \{b' \mid b \in T\}$.

Von besonderem Interesse sind die Mengen T^*, wenn T ein Filter oder ein Ideal ist. Man zeigt leicht:

Lemma 3.6.6.11. *Sei B Boolesche Algebra. Dann ist $I \subseteq B$ genau dann ein Ideal (im Sinn von Definition 3.6.3.6), wenn I ein Ideal (im ringtheoretischen Sinn) des zugeordneten Booleschen Rings ist.*
$F \subseteq B$ ist genau dann ein Filter, wenn F^* ein Ideal ist.
$I \subseteq B$ ist genau dann ein Ideal, wenn I^* ein Filter ist.

UE 252 ► Übungsaufgabe 3.6.6.12. (F) Beweisen Sie Lemma 3.6.6.11. **◄ UE 252**

Definition 3.6.6.13. Sei B eine Boolesche Algebra und sei $I \subseteq B$ ein Ideal. Dann definieren wir die Äquivalenzrelation $\sim_I$ durch $x \sim_I y :\Leftrightarrow x - y \in I$. ($x - y = x + y$ ist hier die Ringoperation.)
Dual dazu: Sei $F \subseteq B$ ein Filter. Dann definieren wir die Äquivalenzrelation $\sim_F$ durch $x \sim_F y \Leftrightarrow (x - y)' \in F$.

Lemma 3.6.6.14. *Sei B Boolesche Algebra, und sei I Ideal. Sei $F := I^* = \{b' \mid b \in I\}$ der dazu duale Filter. Dann sind für alle $b, c \in B$ die folgenden Aussagen äquivalent:*

(1) $b \sim_I c$.
(2) $b \sim_F c$.
(3) $\exists f \in F : b \wedge f = c \wedge f$.
(4) $\exists i \in I : b \wedge i' = c \wedge i'$.
(5) $\exists i \in I : b \vee i = c \vee i$.

Beweis. Die Äquivalenzen (1) $\Leftrightarrow$ (2) und (3) $\Leftrightarrow$ (4) sind klar.
(4) $\Rightarrow$ (5): Für alle x gilt $x \vee i = (x \wedge i) \vee (x \wedge i') \vee i$. Somit folgt aus $b \wedge i' = c \wedge i'$ sofort $b \vee i = (b \wedge i') \vee i = (c \wedge i') \vee i = c \vee i$.
(5) $\Rightarrow$ (4): Dual zu „(4) $\Rightarrow$ (5)“.
Die Äquivalenz zwischen (2) und (3) folgt aus der Beziehung

$$b \wedge f = c \wedge f \;\Leftrightarrow\; b + c \leq f'.$$

Beweis dieser Äquivalenz: Wenn $b \wedge f = c \wedge f$, dann ist

$$b \wedge c' = (b \wedge c' \wedge f) \vee (b \wedge c' \wedge f') = (c \wedge c' \wedge f) \vee (b \wedge c' \wedge f') \leq 0 \vee f' = f',$$

analog $b' \wedge c \leq f'$, daher $b + c = (b \wedge c') \vee (b' \wedge c) \leq f'$.
Wenn umgekehrt $b + c \leq f'$ gilt, dann ist $b \wedge c' \leq b + c \leq f'$ und daher $b \wedge f = (b \wedge c \wedge f) \vee (b \wedge c' \wedge f) \leq (b \wedge c \wedge f) \vee (f' \wedge f) = (b \wedge c \wedge f) \leq b \wedge f$, also $b \wedge f = b \wedge c \wedge f$.
Analog $c \wedge f = b \wedge c \wedge f$, also $b \wedge f = c \wedge f$. □

Beispiel 3.6.6.15. Sei $B = \mathfrak{P}(\mathbb{N})$ die Potenzmenge der natürlichen Zahlen. Mit den Operationen $\cup$, $\cap$ wird B zu einer Booleschen Algebra ($1 = \mathbb{N}$, etc.).
Sei I die Famile aller endlichen Teilmengen von $\mathbb{N}$, $F := I^*$ die Familie aller ko-endlichen Teilmengen von $\mathbb{N}$ (d. h. Mengen mit endlichem Komplement). Dann gilt für beliebige Teilmengen $X, Y \subseteq \mathbb{N}$:

$$\begin{aligned} X \sim_I Y &\Leftrightarrow X \sim_F Y \\ &\Leftrightarrow \exists n \in \mathbb{N} : X \cap \{n, n+1, n+2, \dots\} = Y \cap \{n, n+1, n+2, \dots\}, \end{aligned}$$

d. h. genau dann, wenn X und Y bis auf endlich viele Elemente übereinstimmen.

Beispiel 3.6.6.16. Sei B die Familie aller Borelmengen $X \subseteq [0, 1]$. B ist eine Boolesche Algebra (mit den üblichen Operationen $\cup, \cap, \dots$). Sei λ das Lebesguemaß.
Sei $I := \{X \in B \mid \lambda(X) = 0\}$, die Familie der Nullmengen. Der dazu *duale Filter* ist die Familie der Einsmengen: $F := I^* = \{Y \in B \mid \lambda(Y) = 1\}$.
Dann gilt $X \sim_I Y$ genau dann, wenn $\lambda(X \,\Delta\, Y) = 0$, also wenn X und Y „bis auf eine Lebesgue-Nullmenge“ übereinstimmen. Da I nicht nur bezüglich endlicher, sondern sogar bezüglich abzählbarer Vereinigungen abgeschlossen ist, spricht man sogar von einem σ-Ideal, entsprechend bei F von einem σ-Filter.

3.6.7. Atome

Inhalt in Kurzfassung: Atome in Booleschen Algebren sind definitionsgemäß obere Nachbarn der 0. Der Stonesche Darstellungssatz für endliche Boolesche Algebren besagt, dass jede solche isomorph ist zur Potenzmengenalgebra über der Menge ihrer Atome. Die allgemeinere Version dieses Satzes folgt dann in Unterabschnitt 3.6.8.

Das wichtigste Ergebnis dieses Unterabschnitts, den Satz von Stone für endliche Boolesche Algebren (3.6.7.6), werden wir auch als Folgerung der allgemeinen Version des Stoneschen Satzes (3.6.8.17) erhalten. Daher werden wir den Beweis selbst nicht detailliert ausführen, sondern konzentrieren uns auf das dafür erforderliche Konzept der sogenannten Atome, die auch anderweitig wichtig und interessant sind.

Definition 3.6.7.1. Sei $(V, \wedge, \vee)$ ein Verband mit kleinstem Element 0. Dann heißt $a \in V$ ein *Atom* :$\Leftrightarrow$

1. $0 < a$ und
2. $\forall b \in V : \; 0 < b \leq a \Rightarrow b = a$

(d. h., a ist ein oberer Nachbar von 0).
Wir schreiben $\mathrm{At}(V)$ für die Menge aller Atome von V.

Lemma 3.6.7.2 (Rechenregeln für Atome)**.** *Sei B Boolesche Algebra, $a \in B$ ein Atom. Dann gilt für alle $b, c \in B$:*

(A1) $a \leq b$ *genau dann, wenn* $a \wedge b \neq 0$. *Anders gesagt:* $a \not\leq b \;\Leftrightarrow\; a \wedge b = 0$.

(A2) $a \leq b'$ *genau dann, wenn* $a \not\leq b$.

(A3) $a \leq b \wedge c$ *genau dann, wenn* $a \leq b$ *und* $a \leq c$. *(Das gilt nicht nur für Atome a, sondern für beliebige Verbandselemente.)*

(A4) $a \leq b \vee c$ *genau dann, wenn* $a \leq b$ *oder* $a \leq c$.

UE 253 ► Übungsaufgabe 3.6.7.3. (V) Beweisen Sie Lemma 3.6.7.2. **◄ UE 253**

Anmerkung 3.6.7.4. Die Regeln (A2), (A3), (A4) geben eine Korrespondenz zwischen den algebraischen Operationen $'$, $\wedge$, $\vee$ und den logischen Junktoren „nicht“, „und“ und „oder“. Im nächsten Satz übersetzen wir diese logischen Junktoren in die mengentheoretischen Operationen $'$, $\cap$ und $\cup$.

Lemma 3.6.7.5. *Sei $(B, \wedge, \vee, 0, 1, ')$ eine endliche Boolesche Algebra. Dann gibt es zu jedem Element $b \in B \setminus \{0\}$ ein Atom $a \in \mathrm{At}(B)$ mit $a \leq b$. (Dies gilt sogar für beliebige endliche Verbände.)*

Beweis. Sei $b \in B \setminus \{0\}$. Ist b ein Atom, so kann man $a = b$ setzen. Ist b kein Atom, so gibt es ein $b_1 \in B$ mit $0 < b_1 < b$. Ist b_1 ein Atom, so kann man $a = b_1$ setzen. Andernfalls setzt man das Verfahren fort und erhält eine Kette $b > b_1 > b_2 > \ldots$, die, da B endlich ist, bei einem b_i abbrechen muss. Dann setzt man $a = b_i$. □

Satz 3.6.7.6 (Satz von Stone für endliche Boolesche Algebren)**.** *Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra und $A := \mathrm{At}(B)$ die Menge der Atome von B.*
Sei $\varphi : B \to \mathfrak{P}(A)$ gegeben durch $\varphi(b) := \{a \in A \mid a \leq b\}$.
Dann ist φ ein Homomorphismus von Booleschen Algebren. Ist B endlich, so ist φ sogar ein Isomorphismus der Booleschen Algebren B und $(\mathfrak{P}(A), \cap, \cup, \emptyset, A, ')$.

UE 254 ► Übungsaufgabe 3.6.7.7. (V,W) Beweisen Sie Satz 3.6.7.6. **◄ UE 254**

UE 255 ► Übungsaufgabe 3.6.7.8. (B) Geben Sie eine Boolesche Algebra B an, sodass die Abbildung $\varphi\colon B \to \mathfrak{P}(\mathrm{At}(B))$, $b \mapsto \{a \in \mathrm{At}(B) \mid a \leq b\}$ nicht surjektiv ist. **◄ UE 255**

UE 256 ► Übungsaufgabe 3.6.7.9. (B) Geben Sie eine Boolesche Algebra B an, sodass die Abbildung $\varphi\colon B \to \mathfrak{P}(\mathrm{At}(B))$, $b \mapsto \{a \in \mathrm{At}(B) \mid a \leq b\}$ nicht injektiv ist. **◄ UE 256**

Folgerung 3.6.7.10. *Ist B eine endliche Boolesche Algebra, dann gilt $|B| = 2^n$ für ein $n \in \mathbb{N}$. Zu jedem $n \in \mathbb{N}$ gibt es somit – bis auf Isomorphie – genau eine Boolesche Algebra mit 2^n Elementen, nämlich $\mathfrak{P}(\{0, 1, \ldots, n-1\})$.*

Beweis. Nach dem Satz von Stone ist B isomorph zu $\mathfrak{P}(A)$ für eine endliche Menge A (nämlich $A = \mathrm{At}(B)$, aber das benötigen wir hier nicht). Setzen wir $n = |A|$, so folgt $|B| = |\mathfrak{P}(A)| = 2^n$.
Sei B' eine weitere Boolesche Algebra mit 2^n Elementen. Dann gilt $B' \cong \mathfrak{P}(A')$ für eine Menge A' mit $|A'| = n = |A|$. Ist $\rho : A \to A'$ eine Bijektion, so ist $\hat{\rho} : \mathfrak{P}(A) \to \mathfrak{P}(A')$, $\hat{\rho}(A) := \{\rho(a) \mid a \in A\}$ ein Isomorphismus zwischen Booleschen Algebren. Also sind auch B und B' isomorph. □

Im nächsten Abschnitt wollen wir diesen Satz auf beliebige Boolesche Algebren verallgemeinern. Man kann nicht erwarten, dass jede Boolesche Algebra zu einer Potenzmengenalgebra isomorph ist; es gibt nämlich abzählbar unendliche Boolesche Algeben (siehe Übungsaufgabe 3.6.7.17), während die Potenzmenge einer Menge nicht abzählbar unendlich sein kann: die Potenzmenge jeder endlichen Menge ist endlich, und die Potenzmenge jeder unendlichen Menge ist überabzählbar.

Definition 3.6.7.11. Sei M Menge. Eine Menge $\mathfrak{K} \subseteq \mathfrak{P}(M)$ heißt *Mengenalgebra*[31], wenn für alle $A, B \in \mathfrak{K}$ die folgenden Eigenschaften gelten:

(1) $A \cup B \in \mathfrak{K}$,
(2) $A \cap B \in \mathfrak{K}$,
(3) $A' := M \setminus A \in \mathfrak{K}$,
(4) $A \cap B' = A \setminus B \in \mathfrak{K}$,
(5) $M \in \mathfrak{K}$.

Anmerkung 3.6.7.12. Die Liste (1)–(5) ist redundant.

Beispiel 3.6.7.13. $\mathfrak{P}(M)$ ist eine Mengenalgebra, genauso wie $\{M, \emptyset\}$.

Anmerkung 3.6.7.14. Jede Mengenalgebra ist Unteralgebra der Potenzmengenalgebra (mit den üblichen Operationen Schnitt, Vereinigung, Komplement), und ist daher selbst eine Boolesche Algebra.

Die folgenden Beispiele zeigen, dass eine Mengenalgebra Atome haben kann, aber nicht haben muss.

Beispiele 3.6.7.15.

(1) Sei $(0, 1]$ das halboffene Intervall der reellen Zahlengeraden und $\mathfrak{K} \subseteq \mathfrak{P}((0, 1])$ gegeben durch $\mathfrak{K} := \{\emptyset\} \cup \{\bigcup_{1 \le i \le n}(a_i, b_i] \mid 0 \le a_i < b_i \le 1,\ n \in \mathbb{N}^+\}$. Dann ist $\mathfrak{K}$ Unteralgebra von $(\mathfrak{P}((0, 1]), \cap, \cup, \emptyset, (0, 1], ')$.
$\mathfrak{K}$ enthält keine Atome.

(2) Sei X eine beliebige unendliche Menge; sei I die Menge aller endlichen Teilmengen von X, und sei $F := I^* = \{A' \mid A \in I\}$ die Menge der *ko-endlichen Teilmengen* von X. Dann ist $I \cup F$ eine Unteralgebra von $(\mathfrak{P}(X), \cap, \cup, \emptyset, X, ')$. Es ist I nämlich unter Schnitten und Vereinigungen abgeschlossen, daher auch F: wenn nämlich $A, B \in F$, dann $A', B' \in I$, also $A' \vee B' \in I$, daher $A \wedge B = (A' \vee B')' \in F$.
Die Atome von $I \cup F$ sind genau die einelementigen Teilmengen von X.

[31] englisch: *field of sets*

UE 257 ► **Übungsaufgabe 3.6.7.16.** (F) Für eine beliebige Boolesche Algebra B bezeichne ◄ **UE 257**
$\mathrm{At}(B)$ die Menge der Atome von B. Seien B_1 und B_2 Boolesche Algebren mit Nullelementen 0_1 und 0_2. Betrachten Sie die Boolesche Algebra $B_1 \times B_2$ und zeigen Sie:

$$\mathrm{At}(B_1 \times B_2) = \mathrm{At}(B_1) \times \{0_2\} \cup \{0_1\} \times \mathrm{At}(B_2)$$

UE 258 ► **Übungsaufgabe 3.6.7.17.** (B) Finden Sie möglichst viele (mindestens 4) nichtisomorphe abzählbar unendliche Boolesche Algebren. ◄ **UE 258**

UE 259 ► **Übungsaufgabe 3.6.7.18.** (E) Gibt es eine abzählbar unendliche Boolesche Algebra, die ein vollständiger Verband ist? ◄ **UE 259**

3.6.8. Der Darstellungssatz von Stone

Inhalt in Kurzfassung: Der Darstellungssatz von Stone in seiner allgemeinen Formulierung besagt, dass sich jede Boolesche Algebra in eine Potenzmengenalgebra einbetten lässt. Die Menge, deren Potenzmenge hier auftritt, ist die Menge aller Ultrafilter in der gegebenen Booleschen Algebra. Die Beweismethode ist insofern sehr lehrreich, als ähnliche Methoden in verschiedenen Teilgebieten der Mathematik auftreten. Aus dem Darstellungssatz kann u.a. die sehr bemerkenswerte Aussage gefolgert werden, dass jedes Gesetz, das in der zweielementigen Booleschen Algebra gilt, automatisch in allen Booleschen Algebren gilt.

Wir beginnen mit einer informellen Überlegung:
Sei $\mathfrak{K} \leq (\mathfrak{P}(M), \cap, \cup, \emptyset, M, ')$ eine Mengenalgebra. Wie weit können wir die Menge M aus $\mathfrak{K}$ bestimmen, wenn wir $\mathfrak{K}$ nur bis auf Isomorphie, d. h. als abstrakte Boolesche Algebra kennen? Unsere Aufgabe lautet also: Für eine Boolesche Algebra B ist eine Menge M gesucht, sodass B isomorph ist zu einer Unteralgebra von $\mathfrak{P}(M)$.
Im vorigen Abschnitt haben wir uns mit endlichen Booleschen Algebren B beschäftigt. Die Menge M haben wir als die Menge der Atome von B identifiziert, wobei der Isomorphismus jedes Element $b \in B$ auf die Menge $\{m \in M \mid m \leq b\} \in \mathfrak{P}(M)$ abbildet. Derselbe Beweis zeigt, dass für jede Boolesche Algebra B mit M als Menge der Atome die Abbildung $b \mapsto \{a \in M \mid a \leq b\}$ ein Homomorphismus von B in $\mathfrak{P}(M)$ ist.
Für unendliche Boolesche Algebren kann es aber vorkommen, dass es keine Atome gibt, oder dass es nur so wenige Atome gibt, dass die obige Abbildung nicht injektiv ist, oder dass es so viele Atome gibt, dass die obige Abbildung nicht surjektiv ist (Surjektivität bedeutet hier, dass man zu jeder Menge von Atomen ein Element finden kann, das *genau* über den Atomen aus der gegebenen Menge liegt); siehe Beispiel 3.6.7.15 sowie Übungsaufgabe 3.6.7.8 und 3.6.7.9. Die Rolle der Atome im vorigen Beweis werden in diesem Abschnitt gewisse Ideale (oder äquivalent: Filter) spielen. Das wird klar, wenn man annimmt, dass bereits eine Einbettung $f\colon B \to \mathfrak{P}(M)$ mit irgendeiner Menge M

gefunden ist. Für jedes $m \in M$ ist nämlich die Menge $F_m := \{b \in B \mid m \in f(b)\}$ ein Filter auf B, und die Menge $I_m := \{b \in B \mid m \notin f(b)\}$ ist das zugehörige Ideal ($I_m = F'_m = \{b' \mid b \in F_m\}$), da $f(b') = M \setminus f(b)$. Überdies ist $I_m \cup F_m = B$. Jedes Element m von M induziert also auf B einen Filter F_m, für den $F_m \cup F'_m = B$ gilt (bzw. ein Ideal I_m, für das $I_m \cup I'_m = B$ gilt). Unsere Strategie wird daher sein, alle echten Ideale $I \subseteq B$ mit $I \cup I' = B$ zu betrachten, und mit Hilfe dieser Ideale[32] die Menge M zu rekonstruieren. Zu diesem Zweck ist es nützlich und auch erhellend, einige äquivalente Bedingungen zu kennen.
Zur Vorbereitung:

Anmerkung 3.6.8.1. Ein Filter $F \subseteq B$ ist genau dann echt (d. h. $F \neq B$), wenn $0 \notin F$. (Aus $0 \in F$ folgt nämlich $x \in F$ für alle $x \in B$, weil für alle $x \in B$ gilt: $0 \leq x$.)

Und nun die angekündigten Äquivalenzen:

Proposition 3.6.8.2. *Sei B eine Boolesche Algebra und $F \neq B$ ein echter Filter auf B. Dann sind die folgenden Aussagen äquivalent:*

(1) *F ist ein* maximaler Filter*, d. h., der unechte Filter B ist der einzige Filter auf B, der F echt umfasst.*

(2) $\forall x \in B : \; x \notin F \;\Rightarrow\; x' \in F$.

(3) *F ist ein* Ultrafilter*:* $\forall x \in B : \; x \notin F \;\Leftrightarrow\; x' \in F$.

(4) *F ist ein* Primfilter*:* $\forall x, y \in B : \; x \vee y \in F \;\Leftrightarrow\; x \in F$ *oder* $y \in F$.
(Anmerkung: Die Implikation $\Leftarrow$ gilt für alle Filter. Ebenfalls für alle Filter gilt die Äquivalenz $\forall x, y \in B : \; x \wedge y \in F \;\Leftrightarrow\; x \in F$ *und* $y \in F$*.)*

(5) *F ist das Urbild der* 1 *unter einem Epimorphismus von B auf die zweielementige Boolesche Algebra* $\{0, 1\}$.

(6) *$B \setminus F$ ist ein Ideal.*

(7) $F^* = B \setminus F$.

Beweis. Wir werden nur die Implikationen (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (2) $\Rightarrow$ (1), also die Äquivalenz von (1), (2), (3) und (4) zeigen. Die Äquivalenz mit (5), (6) und (7) verbleibt als Übungsaufgabe.
(1) $\Rightarrow$ (2): Sei F maximal, und $x \in B$, $x \notin F$. Wir wollen $x' \in F$ zeigen.
Wir betrachten die Menge $G := \{b \in B \mid \exists f \in F : x \wedge f \leq b\}$. Offensichtlich gilt $F \cup \{x\} \subseteq G$. Die Menge G ist offensichtlich nach oben abgeschlossen. Überdies ist G

[32] Daher auch der Name: wie die Fernpunkte in der projektiven Geometrie stellen die Ideale sozusagen „ideale“ Elemente dar, die nicht in der Algebra B selbst liegen, wohl aber in der umgebenden Algebra $\mathfrak{P}(M)$. Ein Fernpunkt repräsentiert eine Richtung der affinen Ebene; während ein Fernpunkt in der projektiven Ebene einfach ein Punkt ist, kann man eine Richtung in der Sprache der affinen Ebene nur als komplizierteres Objekt, nämlich als „Klasse paralleler Geraden“ betrachten. Ebenso sind die Filter, die wir in der umgebenden Potenzmengenalgebra verwenden, einfach durch ihre kleinsten Punkte (Singletons) beschrieben, während sie in der ursprünglichen Algebra eine Familie von Elementen darstellen.

ein Filter, denn wenn $x \wedge f_1 \leq b_1$ und $x \wedge f_2 \leq b_2$ mit $f_1, f_2 \in F$ ist, dann gilt mit $f := f_1 \wedge f_2 \in F$ auch die Beziehung $x \wedge f \leq b_1 \wedge b_2$.
Da F maximal war, muss $G = B$ gelten, also insbesondere $0 \in G$. Es gibt also ein $f_0 \in F$ mit $f_0 \wedge x = 0$. Für dieses f_0 gilt $f_0 \leq x'$, daher $x' \in F$.
(2) $\Rightarrow$ (3): Aus $x \notin F$ und Bedingung (2) folgt $x' \in F$. Umgekehrt gilt $x' \in F \Rightarrow x \notin F$, weil nicht x und x' gleichzeitig in F sein können, da sonst $0 = x \wedge x' \in F$ und F kein echter Filter wäre (siehe Anmerkung 3.6.8.1).
(3) $\Rightarrow$ (4): Unter der Annahme (3) gilt die Äquivalenzkette

$$x \vee y \notin F \;\Leftrightarrow\; (x \vee y)' \in F \;\Leftrightarrow\; x' \wedge y' \in F \;\Leftrightarrow\; x' \in F \text{ und } y' \in F \;\Leftrightarrow\; x \notin F \text{ und } y \notin F.$$

Also gilt auch die Äquivalenz der Negationen: $x \vee y \in F \;\Leftrightarrow\; x \in F$ oder $y \in F$.
(4) $\Rightarrow$ (2): Sei F Primfilter. Wegen $x \vee x' = 1 \in F$ folgt aus der Annahme $x \notin F$ sofort $x' \in F$.
(2) $\Rightarrow$ (1): Angenommen, es gibt einen Filter G mit $F \subseteq G$ und $F \neq G$. Zu zeigen ist, dass dann $G = B$ kein echter Filter ist. Sei also $g \in G \setminus F$. Wegen Voraussetzung (2) folgt $g' \in F$ für das Komplement g' von g. Wegen $F \subseteq G$ folgt $g' \in G$, wegen der Abgeschlossenheit eines Filter bezüglich $\wedge$ daher auch $0 = g \wedge g' \in G$. Also ist G kein echter Filter (siehe Anmerkung 3.6.8.1). □

UE 260 ► **Übungsaufgabe 3.6.8.3.** (V) Beweisen Sie die ausständigen Implikationen aus Proposition 3.6.8.2. ◄ **UE 260**

Von den verschiedenen Bezeichnungen aus Proposition 3.6.8.2 werden wir am häufigsten *Ultrafilter* verwenden. Vereinfacht ausgedrückt konnten wir für endliche Boolesche Algebren in Lemma 3.6.7.5 zeigen, dass es „genügend“ Atome gibt. Daher stellt sich nun die Frage, ob auch im Fall allgemeiner Boolescher Algebren „genügend“ Ultrafilter existieren, anders gesagt ob der Begriff des Ultrafilters eine passende Verallgemeinerung des Atombegriffs ist. Dass dies tatsächlich der Fall ist, zeigt der sogenannte Ultrafiltersatz.

Satz 3.6.8.4 (Ultrafiltersatz[33])**.** *Sei B eine Boolesche Algebra und F_0 ein echter Filter auf B. Dann gibt es einen Ultrafilter U mit $F_0 \subseteq U \subseteq B$.*

UE 261 ► **Übungsaufgabe 3.6.8.5.** (V) Beweisen Sie den Ultrafiltersatz 3.6.8.4... ◄ **UE 261**

(1) ... indem Sie die fünfte Aussage von Satz 3.4.2.4 auf Boolesche Ringe anwenden.

(2) ... indem Sie das Lemma von Zorn auf die Menge aller $F \subseteq B$ anwenden, die

$$\forall x_1, \ldots, x_n \in F \; \forall y \in F_0 : x_1 \wedge \cdots \wedge x_n \wedge y \neq 0$$

erfüllen.

[33] Dieser Satz wird oft mit BPI abgekürzt: „Boolean prime ideal theorem.“

UE 262 ► **Übungsaufgabe 3.6.8.6.** (A,E) Sei B eine höchstens abzählbare Boolesche Algebra mit mehr als einem Element. (B ist also entweder endlich oder es gibt eine Bijektion $f : \mathbb{N} \to B$.) Zeigen Sie (ohne Verwendung des Auswahlaxioms, des Zornschen Lemmas etc.), dass es einen Ultrafilter auf B gibt. ◄ **UE 262**

Das folgende Lemma ist lediglich eine Umformulierung von Proposition 3.6.8.2. Wir schreiben es extra an, um die Analogie zwischen Ultrafiltern und Atomen hervorzuheben; siehe Lemma 3.6.7.2.

Lemma 3.6.8.7 (Rechenregeln für Ultrafilter)**.** *Sei B Boolesche Algebra, $F \subseteq B$ ein Ultrafilter. Dann gilt für alle $b, c \in B$:*

(U2) $b' \in F$ genau dann, wenn $b \notin F$.

(U3) $b \wedge c \in F$ genau dann, wenn $b \in F$ und $c \in F$.

(U4) $b \vee c \in F$ genau dann, wenn $b \in F$ oder $c \in F$.

Die Begriffe *maximales Ideal* und *Primideal* sind analog definiert. Insbesondere heißt ein echtes Ideal *Primideal*, wenn $\forall x, y \in B : \; x \wedge y \in I \;\Leftrightarrow\; x \in I$ oder $y \in I$ gilt.

UE 263 ► **Übungsaufgabe 3.6.8.8.** (D) Untersuchen Sie die Beziehung des Begriffs *Primideal* im Kontext von Booleschen Algebren wie im Kontext von Ringen. ◄ **UE 263**

Beispiele 3.6.8.9.

(1) Sei B eine Boolesche Algebra, und sei $a \in B$ ein Atom. Dann ist die Menge $\{x \in B \mid a \leq x\}$ ein Primfilter und Ultrafilter. (In Analogie zur Terminologie bei Ringen heißen Filter von der Form $\{x \in B \mid b_0 \leq x\} = \{x \vee b_0 \mid x \in B\}$ auch *Hauptfilter*, und Ideale der Form $\{x \in B \mid x \leq c_0\} = \{x \wedge c_0 \mid x \in B\}$ auch *Hauptideale*[34]) mit b_0 bzw. c_0 als *erzeugendem Element*. Das erzeugende Element eines Hauptfilters F ist eindeutig bestimmt: Denn wenn b_0 und b_1 beide F erzeugen, dann liegt auch $b := b_0 \wedge b_1 \leq b_0, b_1$ in F und muss nach Definition von $F_{b_0} = F_{b_1} = F$ gleichzeitig $b \geq b_0, b_1$ erfüllen, also $b_0 = b = b_1$. Ein Ultrafilter, der kein Hauptfilter ist, heißt auch ein *freier Ultrafilter*.

(2) Sei $B = \mathfrak{P}(\mathbb{N})$. Sei I die Menge aller endlichen Teilmengen von $\mathbb{N}$, $F = I'$ die Menge aller ko-endlichen Mengen.
Dann ist F zwar Filter (und I Ideal) auf B, aber F ist kein Ultrafilter.

(3) Seien B, I, F wie in (2). Sei nun $B_0 := I \cup F$. B_0 ist Unteralgebra von $\mathfrak{P}(\mathbb{N})$. I und F sind Ideal bzw. Filter auf B_0; tatsächlich ist F sogar maximaler Filter (Ultrafilter) auf B_0, und I ist maximales Ideal (Primideal) auf B_0.

UE 264 ► **Übungsaufgabe 3.6.8.10.** (D) Untersuchen Sie die Beziehung des Begriffs *Hauptideal* im Kontext von Booleschen Algebren wie im Kontext von Ringen. ◄ **UE 264**

[34] englisch: *principal filter*, *principal ideal* (Achtung! „principal“, nicht „principle“)

Der Fall endlicher Boolescher Algebren verdient in Hinblick auf Filter und Ultrafilter extra Beachtung:

Proposition 3.6.8.11. *In einer endlichen Booleschen Algebra B ist jeder Filter F ein Hauptfilter, d. h. von der Form $F = F_b := \{x \in B \mid b \leq x\}$ mit eindeutig bestimmtem $b \in B$. Somit ist die Zuordnung $b \mapsto F_b$ eine Bijektion zwischen B und der Menge aller Filter auf B. Dabei gilt $b_1 \leq b_2$ genau dann, wenn $F_{b_2} \subseteq F_{b_1}$ gilt. Der Filter F_b ist genau dann ein Ultrafilter, wenn b ein Atom ist. Somit ist die Zuordnung $a \mapsto F_a$ eine Bijektion zwischen der Menge* $\mathrm{At}(B)$ *der Atome von B und der Menge aller Ultrafilter von B.*

Beweis. Wir zeigen zunächst, dass jeder Filter F ein Hauptfilter F_b mit eindeutig bestimmtem b ist. Als Teilmenge von B ist auch F endlich. Daher ist $b := \bigwedge_{x \in F} x$ wohldefiniert. Nach Definition gilt $F \subseteq \{x \in B \mid b \leq x\} = F_b$. Um umgekehrt $F_b \subseteq F$ zu zeigen, beobachten wir zunächst, dass b in F liegt, da F unter $\wedge$ abgeschlossen ist. Weil F auch nach oben abgeschlossen ist, folgt $F_b \subseteq F$. Die Eindeutigkeit von b haben wir bereits im ersten Unterpunkt von Beispiel 3.6.8.9 nachgewiesen.
Dass für $b_1, b_2 \in B$ aus $b_1 \leq b_2$ stets $F_{b_2} \subseteq F_{b_1}$ folgt, ist klar; für die umgekehrte Richtung ist nur zu bemerken, dass $F_{b_2} \subseteq F_{b_1}$ jedenfalls $b_2 \in F_{b_1}$ nach sich zieht.
Es bleibt zu zeigen, dass F_b genau dann ein Ultrafilter ist, wenn b ein Atom ist. Sei F_b ein Ultrafilter. Da $0 \neq b$ (als Ultrafilter ist F_b nach Definition ein echter Filter) und jedenfalls $0 \leq b$ gilt, erhalten wir $0 < b$. Für $0 < b' \leq b$ folgt $F_{b'} \supseteq F_b$ nach dem bereits Bewiesenen, also $F_{b'} = F_b$, weil F_b ein Ultrafilter ist. Daraus folgt $b = b'$ wegen der Eindeutigkeit des erzeugenden Elements. Somit ist b als Atom nachgewiesen. Sei umgekehrt b ein Atom. Für einen echten Filter $F' \supseteq F_b$ gibt es nach dem ersten Punkt ein Element $b' \in B$ mit $F' = F_{b'}$. Da F' ein echter Filter ist, gilt dabei $0 < b'$. Aus $F_{b'} \supseteq F_b$ folgt $b' \leq b$. Da b ein Atom ist, erhalten wir $b' = b$ und weiter $F' = F_{b'} = F_b$. Folglich ist F_b ein Ultrafilter. □

Auch im unendlichen Fall besteht ein enger Zusammenhang zwischen Ultrafiltern und Atomen. Wie schon in den einleitenden Bemerkungen zu diesem Unterabschnitt angedeutet, kann das einem Ultrafilter entsprechende Atom aber auch „außerhalb“ der Booleschen Algebra liegen. Zur Präzisierung dieser Idee dient die folgende Übungsaufgabe:

UE 265 ► **Übungsaufgabe 3.6.8.12.** (F+) Sei B eine Boolesche Algebra mit kleinstem Element 0_B und größtem Element 1_B, sei $U \subseteq B$ ein Ultrafilter und sei $I := U' = B \setminus U$ das entsprechende Ideal. Wir betrachten die zweielementige Boolesche Algebra $\{0, 1\}$ und definieren das direkte Produkt $B_{ext} := B \times \{0, 1\}$. Schließlich definieren wir die Abbildung $\varphi : B \to B_{ext}$ durch

$$\varphi(b) := \begin{cases} (b, 0), & b \in I \\ (b, 1), & b \in U \end{cases}$$

◄ **UE 265**

Zeigen Sie:

(1) φ ist eine isomorphe Einbettung, also ist $\varphi : B \to \varphi(B)$ ein Isomorphismus und man kann B als Unteralgebra von B_{ext} auffassen, wenn man $b \in B$ mit $\varphi(b)$ identifiziert.

(2) Es gilt $B_{ext} = \langle \varphi(B) \cup \{(0_B, 1)\}\rangle$.

(3) $(0_B, 1)$ ist ein Atom in B_{ext} und $\varphi(U) \cup \{(0_B, 1)\}$ ist der von $(0_B, 1)$ in B_{ext} erzeugte Hauptfilter.

Anmerkung: Man kann diese Aufgabe so interpretieren, dass man ein Atom zur gegebenen Booleschen Algebra hinzufügt, sodass der gegebene Ultrafilter ein Hauptfilter wird. Dabei ist die erweiterte Algebra wegen Aussage (2) so klein wie möglich.

UE 266 ► **Übungsaufgabe 3.6.8.13.** (W) Sei B eine unendliche Boolesche Algebra. Zeigen Sie, dass es einen Ultrafilter gibt, der kein Atom enthält. (Hinweis: Zeigen Sie, dass die Menge I aller $b \in B$, zu denen es Atome $a_1, \ldots, a_k$ von B mit $b \leq a_1 \vee \cdots \vee a_k$ gibt, ein echtes Ideal von B ist, und betrachten Sie B/I.) ◄ **UE 266**

UE 267 ► **Übungsaufgabe 3.6.8.14.** (B) Sei B die Menge aller endlichen und ko-endlichen Teilmengen der natürlichen Zahlen. Finden Sie alle Ultrafilter auf B. ◄ **UE 267**

Eine Hauptrolle im Beweis des Satzes von Stone spielen die sogenannten charakteristischen Funktionen:

Definition 3.6.8.15. Sei B eine Boolesche Algebra und sei $A \subseteq B$. Die *charakteristische Funktion* mit Träger A ist die Funktion $\chi_A : B \to \{0, 1\}$ mit $\chi(x) = 1$ für $x \in A$ und $\chi(x) = 0$ für $x \notin A$.

Die Rechenregeln aus Lemma 3.6.8.7 liefern unmittelbar die folgende entscheidende Tatsache:

Lemma 3.6.8.16. *Sei B Boolesche Algebra, $F \subseteq B$ ein Ultrafilter. Dann ist die Abbildung $\chi_F : B \to \{0, 1\}$ ein Boolescher Homomorphismus von B in die zweielementige Boolesche Algebra $\{0, 1\}$.*

Damit haben wir alle Vorarbeiten für den Beweis des Darstellungssatzes von Stone geleistet.

Satz 3.6.8.17 (Darstellungssatz von Stone)**.** *Sei $(B, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra. Dann gibt es eine Menge M und ein $\mathcal{B} \subseteq \mathfrak{P}(M)$, sodass $(B, \wedge, \vee, 0, 1, ') \cong (\mathcal{B}, \cap, \cup, \emptyset, M, ')$.*
Zusatz: Ist B endlich, so kann $\mathcal{B}$ als Potenzmenge von $\mathrm{At}(B)$, der Menge der Atome von B, gewählt werden. Jede endliche Boolesche Algebra ist also isomorph zu einer Potenzmengenalgebra über einer endlichen Menge, also von einer Kardinalität 2^n mit einem $n \in \mathbb{N}$.

Beweis. Sei B eine beliebige Boolesche Algebra. Wir betrachen die Menge

$$\mathcal{U} = \{F \subseteq B \mid F \text{ ist Ultrafilter}\}$$

und die Abbildung

$$f\colon \begin{cases} B & \to \{0,1\}^{\mathcal{U}} \\ b & \mapsto (\chi_F(b))_{F\in\mathcal{U}} \end{cases}$$

Zunächst behaupten wir, dass f ein Boolescher Homomorphismus ist; wenn wir mit $\pi_F : \{0,1\}^{\mathcal{U}} \to \{0,1\}$ die Projektion auf die F-Koordinate bezeichnen, so genügt es nachzurechnen, dass $\pi_F \circ f$ für alle $F \in \mathcal{U}$ ein Homomorphismus ist. Letzteres ist klar, weil $\pi_F \circ f = \chi_F$ gilt.
Für die erste Behauptung des Satzes ist noch die Injektivität von f zu zeigen, d. h. $f(a) \neq f(b)$ für $a \neq b$. Nach Definition von f ist dafür ein Ultrafilter F zu finden, der eines der beiden Elemente enthält und das andere nicht. Dazu beobachten wir, dass aus $a \wedge b' = 0$ die Gleichung

$$a = a \wedge 1 = a \wedge (b \vee b') = (a \wedge b) \vee (a \wedge b') = (a \wedge b) \vee 0 = a \wedge b$$

und somit $a \leq b$ folgt. Analog folgt $a \geq b$ aus $a' \wedge b = 0$. Für $a \neq b$ muss also wenigstens eines der beiden Elemente $a \wedge b'$ und $a' \wedge b$ von 0 verschieden sein, oBdA $c := a \wedge b' \neq 0$. Nach dem Ultrafiltersatz 3.6.8.4 folgt, dass sich der von $c \in B \setminus \{0\}$ erzeugte Hauptfilter $\{x \in B \mid x \geq c\}$ zu einem Ultrafilter $F \in \mathcal{U}$ fortsetzen lässt. Wegen $c \in F$ und $c = a \wedge b' \leq a, b'$ liegen a und b' in F, also nicht b (siehe Proposition 3.6.8.2). F hat also die gewünschte Eigenschaft. Somit ist $f\colon B \to \{0,1\}^{\mathcal{U}}$ eine isomorphe Einbettung der Booleschen Algebra B in die Boolesche Algebra $\{0,1\}^{\mathcal{U}}$, die wiederum in kanonischer Weise isomorph ist zur Potenzmengenalgebra $\mathfrak{P}(\mathcal{U})$. (Jeder Teilmenge wird ihre charakteristische Funktion zugeordnet.) Damit ist die erste Aussage des Satzes gezeigt.

Für den Zusatz betreffend endliches B erinnern wir uns an Proposition 3.6.8.11. Demnach ist im endlichen Fall ein Filter genau dann ein Ultrafilter, wenn $F = F_a = \{x \mid a \leq x\}$ für ein Atom a ist. Es genügt somit, wenn wir zeigen können, dass die oben definierte Abbildung f surjektiv auf $\{0,1\}^{\mathcal{U}}$ ist. Dazu werden wir zu jeder Menge $T \subseteq \mathrm{At}(B)$ von Atomen von B ein Element $b = b_T \in B$ finden, für das $\chi_{F_a}(b) = 1$ für $a \in T$ und $\chi_{F_a}(b) = 0$ für $a \in \mathrm{At}(B) \setminus T$ gilt. Und zwar behaupten wir, dass für $T = \{a_1, \ldots, a_k\}$ das Element $b := a_1 \vee \ldots \vee a_k$ diese Eigenschaft hat. Aus $b \geq a_i$ folgt $b \in F_{a_i}$ für alle $i = 1, \ldots, k$, also tatsächlich $\chi_{F_a}(b) = 1$ für alle $a \in T$. Sei nun $a \in \mathrm{At}(B) \setminus T$. Weil es sich um Atome handelt, gilt dann $a_i \wedge a = 0$ für alle $a_i \in T$ und somit

$$b \wedge a = (a_1 \vee \ldots \vee a_k) \wedge a = (a_1 \wedge a) \vee \ldots \vee (a_k \wedge a) = 0.$$

Es gilt also nicht $b \geq a$, d. h., b liegt nicht in F_a. Also gilt $\chi_{F_a}(b) = 0$ für alle $a \in \mathrm{At}(B) \setminus T$, und der Satz ist bewiesen. □

Folgerung 3.6.8.18. *Jede Boolesche Algebra B ist isomorph zu einem subdirekten Produkt der zweielementigen Booleschen Algebra, d. h.*

$$B \leq \prod_{F\in\mathcal{U}} \{0,1\}.$$

Jedes Gesetz, welches in der Booleschen Algebra $\{0,1\}$ *mit den Operationen*

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$'$	
0	1
1	0

gilt, muss daher in allen Booleschen Algebren gelten.

4. Universelle Konstruktionen in Varietäten

In Varietäten gibt es weitreichende Möglichkeiten, Algebren zu konstruieren, die gewisse vorgegebene Strukturen enthalten und unter dieser Bedingung als universelle Objekte aufgefasst werden können. Hier beschäftigen uns vor allem freie Algebren (die eine vorgegebene Menge von Variablen enthalten), siehe Abschnitt 4.1, Koprodukte (die, etwas ungenau gesprochen, alle Algebren einer vorgegebenen Familie enthalten) und Polynomalgebren (Koprodukt einer vorgegebenen mit einer freien Algebra), siehe Abschnitt 4.2.

4.1. Freie Algebren und der Satz von Birkhoff

Wir kennen bereits den Begriff der Varietät, also einer gleichungsdefinierten Klasse von Algebren. Diese Definition ist nach dem Vorbild der bekannten Beispiele aus der klassischen Algebra (Halbgruppen, Gruppen, etc.) gebildet. Neben dieser syntaktischen Beschreibung drängt sich aus algebraischer Sicht auch die Frage nach einer semantischen Charakterisierung auf, also nach strukturellen Eigenschaften, die unter allen Klassen von Algebren genau die Varietäten auszeichnen. Diese Frage wird vom Satz von Birkhoff beantwortet, wonach die Abgeschlossenheit unter den grundlegenden Konstruktionen (Unteralgebren, direkte Produkte und homomorphe Bilder/Faktoralgebren) entscheidend ist, wie in 4.1.1 motiviert wird. Eine gemeinsame Eigenschaft von Vektorräumen, universellen Termalgebren und freien Halbgruppen dient in 4.1.2 als Vorbild für die allgemeine Definition einer freien Algebra in einer Varietät bzw. eines freien Objekts in einer konkreten Kategorie. In 4.1.3 wird für eine vorgegebene Varietät die freie Algebra über einer beliebigen Variablenmenge konstruiert. Das wichtigste Beispiel, die freie Gruppe, ist Gegenstand von 4.1.4, die freie Boolesche Algebra wird in 4.1.5 behandelt. Eine alternative, vielleicht abstrakter anmutende Konstruktion der freien Algebra gelingt in 4.1.6 mit Hilfe subdirekter Produkte. Der Vorteil besteht darin, dass dabei nur die Abgeschlossenheit von Varietäten bezüglich Unteralgebren, direkter Produkte und homomorpher (hier genügt sogar: isomorpher) Bilder verwendet wird. Denn damit gelingt in 4.1.7 der Beweis des Satzes von Birkhoff.

4.1.1. Motivation

Inhalt in Kurzfassung: Motivation des Satzes von Birkhoffs, des Hauptergebnisses dieses Abschnitts.

Definition 4.1.1.1. Für eine Klasse $\mathcal{K}$ von Algebren sei

- $\mathsf{I}\mathcal{K}$ die Klasse aller Algebren $\mathfrak{A}$, die zu einer Algebra $\mathfrak{A}' \in \mathcal{K}$ isomorph sind.

- $\mathsf{H}\mathcal{K}$ Klasse aller Algebren $\mathfrak{A}$, die homomorphes Bild einer Algebra $\mathfrak{A}' \in \mathcal{K}$ sind.
- $\mathsf{S}\mathcal{K}$ die Klasse aller Algebren $\mathfrak{A}$, die zu einer Unteralgebra einer Algebra $\mathfrak{A}' \in \mathcal{K}$ isomorph sind.
- $\mathsf{P}\mathcal{K}$ die Klasse aller Algebren $\mathfrak{A}$, die zu einem Produkt[1] von Algebren aus $\mathcal{K}$ isomorph sind.

Offensichtlich ist $\mathcal{K}$ in jeder der Klassen $\mathsf{I}\mathcal{K}$, $\mathsf{H}\mathcal{K}$, $\mathsf{S}\mathcal{K}$ und $\mathsf{P}\mathcal{K}$ enthalten. Wir sagen, dass $\mathcal{K}$ unter H abgeschlossen ist, wenn sogar $\mathcal{K} = \mathsf{H}\mathcal{K}$ gilt, analog für S, P, I.

Nach Proposition 2.2.1.3 sowie den Folgerungen 2.2.2.9 und 2.2.3.23 gilt

Proposition 4.1.1.2. *Gesetze im Sinne von Definition 2.1.8.6 vererben sich auf Unteralgebren, direkte Produkte und auf homomorphe Bilder. Wenn $\mathcal{K}$ eine Varietät ist, dann gilt also: $\mathcal{K} = \mathsf{H}\mathcal{K} = \mathsf{S}\mathcal{K} = \mathsf{P}\mathcal{K}$.*

Es gilt aber auch die Umkehrung: Jede unter $\mathsf{H}, \mathsf{S}, \mathsf{P}$ abgeschlossene Klasse ist von der Form $\mathcal{V}(\Gamma)$ für eine geeignete Menge Γ von Gesetzen – dies ist der Satz von Birkhoff (siehe Satz 4.1.7.1). Der Beweis dieses Satzes ist eines der wichtigsten Ziele dieses Kapitels. Dabei spielt der Begriff der freien Algebra eine zentrale Rolle.

4.1.2. Bekannte Beispiele und Definition einer freien Algebra

Inhalt in Kurzfassung: Der aus der Linearen Algebra bekannte Satz von der linearen Fortsetzbarkeit von Abbildungen, die zunächst nur auf einer Basis eines Vektorraums definiert sind, die bereits in Unterabschnitt 3.1.2 behandelte freie Halbgruppe und die universelle Eigenschaft der Termalgebra aus Definition 2.1.8.1 sind Beispiele für ein uns denselben allgemeinen Begriff: den der freien Algebra. Die Definition ist sowohl in der Sprache der universellen Algebra als auch, noch allgemeiner, in jener der Kategorientheorie (freies Objekt) möglich. Freie Objekte in einer Kategorie sind nach Definition initiale Objekte in einer geeignet angepassten anderen Kategorie. Daraus folgt, dass sie bis auf Isomorphie eindeutig bestimmt sind. Der Unterabschnitt schließt mit einigen einfachen Beispielen, meist in Form von Übungsaufgaben.

Wir beginnen mit einer wohlbekannten Eigenschaft von Vektorräumen, Termalgebren und der freien Halbgruppe, aus der wir dann die Definition einer freien Algebra in einer Klasse von Algebren bzw. eines freien Objektes in einer konkreten Kategorie abstrahieren.
Sei V ein Vektorraum über einem Körper K und X eine Basis von V. Dann gibt es zu jedem Vektorraum W über K und jedem $j\colon X \to W$ eine eindeutige lineare Abbildung $f\colon V \to W$, die j fortsetzt. Bezeichnen wir die Inklusionsabbildung von X in V mit $\iota : X \to V$, so lässt sich die Fortsetzungseigenschaft auch durch die Bedingung $f \circ \iota = j$ ersetzen. Im Sinne der nachfolgenden Definition 4.1.2.1 lässt sich daher sagen: Jeder

[1] Wir erlauben hier beliebige Indexmengen, insbesondere auch unendliche Mengen sowie die leere Menge. Das leere Produkt $\prod_{i\in I} A_i$ wird als die einelementige Menge $\{\emptyset\}$ definiert, die nur das leere $\emptyset$-Tupel enthält; diese Algebra ist definitionsgemäß immer in $\mathsf{P}\mathcal{K}$ enthalten, sogar wenn $\mathcal{K}$ leer ist.

Vektorraum V ist frei über jeder Basis X bzw. V ist frei über (X, ι). Schematisch als Diagramm:

Ganz ähnlich verhält es sich mit der freien Halbgruppe aus 3.1.2. Bezeichne $F(X)$ die freie Halbgruppe über der Variablenmenge X, realisiert als Menge aller Zeichenketten $x_1 \dots x_n$ mit $x_i \in X$ und der Konkatenation (Aneinanderreihung) von Zeichenketten als binärer Operation. Dann gibt es zu jeder Halbgruppe H und jeder Variablenbelegung $j\colon X \to H$ genau einen Halbgruppenhomomorphismus f mit $f(x) = j(x)$ für alle $x \in X$. Bezeichnen wir mit $\iota\colon X \to F(X)$ jene Abbildung, die jedem $x \in X$ die Zeichenkette aus $F(X)$ zuordnet, die nur aus dem einen Zeichen x besteht, so bedeutet dies $f \circ \iota = j$. Die schematische Darstellung entspricht derjenigen oben für Vektorräume, lediglich mit folgenden Ersetzungen: An die Stelle der K-Vektorräume treten die Halbgruppen, an die Stelle der linearen Abbildungen die Halbgruppenhomomorphismen, V ist durch $F(X)$ zu ersetzen und W durch H. Im Sinne von Definition 4.1.2.1 bedeutet das: $F(X)$ ist frei über X bzw. über (X, ι) in der Klasse der Halbgruppen.

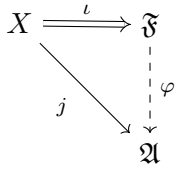
Ein drittes Beispiel ist die Termalgebra aus Definition 2.1.8.1. Sei dazu $\mathcal{K}$ die Klasse aller Algebren eines fixen Typs $\tau = (n_i)_{i\in I}$. Dann hat die Termalgebra $\mathfrak{T}(X, \tau) \in \mathcal{K}$ in den Variablen X die folgende Eigenschaft: Zu jeder Algebra $\mathfrak{A} \in \mathcal{K}$ und jeder Variablenbelegung $j\colon X \to A$ gibt es einen eindeutigen Homomorphismus $f\colon \mathfrak{T}(X, \tau) \to \mathfrak{A}$ (den Einsetzungshomomorphismus) mit $f(x) = j(x)$ für alle $x \in X$ bzw. mit $f \circ \iota = j$ für jenes $\iota\colon X \to \mathfrak{T}(X, \tau)$, das der Variablen $x \in X$ den Term $x \in \mathfrak{T}(X, \tau)$ zuordnet. Im Diagramm oben tritt $\mathcal{K}$ an die Stelle der Klasse aller K-Vektorräume, lineare Abbildungen sind durch Homomorphismen in $\mathcal{K}$ zu ersetzen, V durch $\mathfrak{T}(X, \tau)$ und W durch $\mathfrak{A}$. Im Sinne von Definition 4.1.2.1 bedeutet das: $\mathfrak{T}(X, \tau)$ ist frei über X bzw. über (X, ι) in $\mathcal{K}$. Die Termalgebra $\mathfrak{T}(X, \tau)$ heißt manchmal auch die (bezüglich des Typs τ) *absolut freie Algebra* über X.

Wir verallgemeinern zur Definition freier Algebren innerhalb einer beliebigen Klasse von Algebren desselben Typs:

Definition 4.1.2.1. Sei

- $\mathcal{K}$ eine Klasse von Algebren gleichen Typs,
- $\mathfrak{F} = (F, (\omega_i)_{i\in I})$ in $\mathcal{K}$,
- X eine Menge
- und $\iota\colon X \to F$ eine Funktion.

$\mathfrak{F}$ heißt *frei* über (X, ι) in $\mathcal{K}$, wenn für alle $\mathfrak{A} \in \mathcal{K}$ mit Trägermenge A und für alle $j\colon X \to A$ ein eindeutiger Homomorphismus φ mit $j = \varphi \circ \iota$ existiert.



(Zur Bedeutung der verschieden gestalteten Pfeile in diesem Diagramm sei auf die einführenden „Notationellen Bemerkungen“ verwiesen.)
Im Folgenden werden wir meist nur den Fall $X \subseteq F$ und $\iota = \mathrm{id}_X$ betrachten. Statt „$\mathfrak{F}$ ist frei in $\mathcal{K}$ über (X, id_X)“ schreiben wir dann nur „$\mathfrak{F}$ ist frei in $\mathcal{K}$ über X“. Die Algebra $\mathfrak{F}$ heißt *frei* in $\mathcal{K}$, wenn es eine Menge X gibt, sodass F frei über X in $\mathcal{K}$ ist.

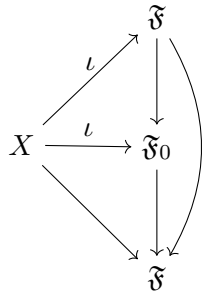
Statt „$\mathcal{F}$ ist in $\mathcal{K}$ frei über X“ sagt man auch „$\mathcal{F}$ ist in $\mathcal{K}$ von X frei erzeugt“; dies wird durch das folgende Lemma gerechtfertigt.

Lemma 4.1.2.2. *Sei $\mathcal{K}$ eine Klasse von Algebren des gleichen Typs, die $\mathsf{S}\mathcal{K} = \mathcal{K}$ erfüllt. (z. B. erfüllt jede Varietät diese Bedingung.) Sei $\mathfrak{F} \in \mathcal{K}$ eine Algebra mit Grundmenge F und sei $\iota : X \to F$. Die Algebra $\mathfrak{F}$ ist genau dann frei über (X, ι), wenn die folgenden beiden Aussagen gelten:*

(1) *Für alle Algebren $\mathfrak{A} \in \mathcal{K}$ mit Trägermenge A und alle Funktionen $j\colon X \to A$ gibt es* mindestens *einen Homomorphismus $\varphi\colon \mathfrak{F} \to \mathfrak{A}$ mit $\varphi \circ \iota = j$.*

(2) *Die Algebra $\mathfrak{F}$ wird von $\iota(X)$ erzeugt, das heißt: Es gibt keine echte Unteralgebra von $\mathfrak{F}$, die die Menge $\iota(X)$ enthält.*

UE 268 ► **Übungsaufgabe 4.1.2.3.** (V,A) Beweisen Sie Lemma 4.1.2.2. Hinweis: Die eine Richtung ergibt sich aus Proposition 2.2.1.17. Für die andere Richtung: finden Sie eine sinnvolle Bedeutung von $\mathfrak{F}_0$ sowie sinnvolle Namen und Eigenschaften der Pfeile im folgenden Diagramm: ◄ **UE 268**



Im Folgenden werden wir nur Klassen von Algebren betrachten, die unter Unteralgebren abgeschlossen sind. In solchen Klassen muss man also statt der Eindeutigkeit des gesuchten Homomorphismus nur nachprüfen, dass die angeblich freie Algebra $\mathfrak{F}$ tatsächlich von

der angegebenen Menge X erzeugt wird. Man beachte, dass dies oft leichter nachzuprüfen ist, da man eine Eindeutigkeitsaussage nur die Algebra $\mathfrak{F}$ und nicht für alle Algebren $\mathfrak{A} \in \mathcal{K}$ untersuchen muss.

Noch allgemeiner ist die Definition freier Objekte in konkreten Kategorien.

Definition 4.1.2.4. Sei $\mathcal{C}$ eine konkrete Kategorie mit Funktor $\mathsf{U}\colon \mathcal{C} \to \mathcal{S}ets$, $F \in Ob(\mathcal{C})$, X eine Menge und $\iota \in \mathrm{Hom}_{\mathcal{S}ets}(X, \mathsf{U}(F))$.[2] Das Objekt F heißt *frei* über X (bezüglich ι), i.Z. $F = F(X)$, wenn gilt: Für alle Objekte $A \in Ob(\mathcal{C})$ und alle Morphismen $f \in \mathrm{Hom}_{\mathcal{S}ets}(X, \mathsf{U}(A))$ gibt es einen eindeutigen Morphismus $\overline{f} \in \mathrm{Hom}_{\mathcal{C}}(F, A)$ mit $f = (\mathsf{U}\overline{f}) \circ \iota$ in $\mathcal{S}ets$.

Offensichtlich lässt sich die definierende Eigenschaft freier Objekte als universelle Eigenschaft in einer geeigneten Kategorie interpretieren. Dazu gehen wir wie in Definition 4.1.2.4 aus von einer Kategorie $\mathcal{C}$ und einer Menge X. Wir betrachten eine neue Kategorie, die wir mit $\mathcal{C}(X)$ bezeichnen. Ihre Objekte seien sämtliche Paare (A, ι), wobei A ein Objekt in $\mathcal{C}$ mit „Trägermenge“ $\mathsf{U}(A)$ und $\iota\colon X \to \mathsf{U}(A)$ eine Funktion sei. Die Morphismen $f\colon (A_1, \iota_1) \to (A_2, \iota_2)$ seien jene Morphismen $f\colon A_1 \to A_2$ in $\mathcal{C}$, die zusätzlich mit den ι_i verträglich sind, d. h. $\mathsf{U}(f) \circ \iota_1 = \iota_2$ erfüllen. Die Komposition in $\mathcal{C}(X)$ sei wie üblich die Abbildungskomposition. Dann besagt Definition 4.1.2.4 nichts anderes, als dass das dortige Paar (F, ι) ein initiales, insbesondere also universelles Objekt in $\mathcal{C}(X)$ ist. Nach Satz 2.3.3.2 sind universelle Objekte eindeutig bis auf Äquivalenz. Im Fall, dass $\mathcal{C}$ eine Varietät ist, bedeutet Äquivalenz in $\mathcal{C}$ erst recht Isomorphie in $\mathcal{C}$. Somit haben wir bewiesen:

Satz 4.1.2.5. *Freie Algebren sind in Varietäten (allgemeiner: in Klassen von Algebren gleichen Typs) bis auf Isomorphie eindeutig bestimmt. Genauer:*
Sind $\mathcal{K}$ eine Klasse von Algebren gleichen Typs, X eine Menge, $(\mathfrak{F}_1, \iota_1)$ frei in $\mathcal{K}$ über (X, ι_1) und $(\mathfrak{F}_2, \iota_2)$ frei in $\mathcal{K}$ über (X, ι_2). Dann sind $\mathfrak{F}_1$ und $\mathfrak{F}_2$ isomorph. Der Isomorphismus $\varphi\colon \mathfrak{F}_1 \to \mathfrak{F}_2$ kann so gewählt werden, dass $\iota_2 = \varphi \circ \iota_1$ gilt.

Freie Algebren über verschieden großen endlichen Mengen sind in vielen Fällen hingegen nicht isomorph:

UE 269 ► **Übungsaufgabe 4.1.2.6.** (F) Sei $\mathcal{K}$ eine Klasse von Algebren gleichen Typs, die mindestens eine endliche Algebra $\mathfrak{A}$ mit mehr als einem Element enthält. Seien $k, k' \in \mathbb{N}$ verschieden und seien X_k bzw. $X_{k'}$ Mengen mit k bzw. k' Elementen. Sei weiters $\mathfrak{F}_k$ frei in $\mathcal{K}$ über (X_k, ι_k) und $\mathfrak{F}_{k'}$ frei in $\mathcal{K}$ über $(X_{k'}, \iota_{k'})$. Zeigen Sie: $\mathfrak{F}_k \ncong \mathfrak{F}_{k'}$.
(Hinweis: Zählen Sie Homomorphismen. Wo verwenden Sie $|A| > 1$?) ◄ **UE 269**

[2] ι ist also eine gewöhnliche Abbildung von der Menge X in die Trägermenge von F.

In der letzten Übungsaufgabe ist die Voraussetzung, dass es $\mathfrak{A} \in \mathcal{K}$ mit $1 < |A| < \infty$ gibt, zwingend notwendig, wie das folgende Gegenbeispiel zeigt:

UE 270 ▶ **Übungsaufgabe 4.1.2.7.** (B,E) Sei $\mathcal{V}$ die Varietät aller Algebren $\mathfrak{A} = (A, *, l, r)$ vom Typ $(2, 1, 1)$, die die Gesetze $l(x * y) \approx x$, $r(x * y) \approx y$, $l(z) * r(z) \approx z$ erfüllen. (l und r stehen für „links“ und „rechts“.) ◀ **UE 270**

(1) Zeigen Sie, dass für jede Algebra $\mathfrak{A} \in \mathcal{V}$ die Abbildung $* : A \times A \to A$ eine Bijektion ist, indem Sie die Umkehrabbildung angeben.

(2) Beschreiben Sie alle endlichen Algebren in $\mathcal{V}$, und geben Sie mindestens eine unendliche Algebra in $\mathcal{V}$ an.

(Hinweis: Betrachten Sie $A = \mathbb{N}^{\mathbb{N}}$, die Menge der Folgen natürlicher Zahlen.)

(3) Sei $\mathfrak{F}_2 \in \mathcal{V}$ die von zwei Elementen a, b frei erzeugte Algebra, und sei $\mathfrak{F}_1 \in \mathcal{V}$ die von einem Element c frei erzeugte Algebra. Zeigen Sie $\mathfrak{F}_1 \cong \mathfrak{F}_2$.

(Hinweis: Sei $\varphi\colon \mathfrak{F}_1 \to \mathfrak{F}_2$ der Homomorphismus mit $\varphi(c) = a * b$, und sei $\psi\colon \mathfrak{F}_2 \to \mathfrak{F}_1$ der Homomorphismus mit $\psi(a) = ??$ und $\psi(b) = ??$. Zeigen Sie, dass ψ zu φ invers ist.)

(4) (Für Fleißige:) Für alle natürlichen Zahlen $k > 0$ gilt $\mathfrak{F}_k \cong \mathfrak{F}_1$.

(5) (Für Ehrgeizige:) Sei $\mathfrak{F}_{\aleph_0}$ die von einer abzählbar unendlichen Menge frei erzeugte Algebra. Ist $\mathfrak{F}_{\aleph_0} \cong \mathfrak{F}_1$?

Wir betrachten einige weitere bekannte Beispiele freier Algebren in Form zweier Übungsaufgaben:

UE 271 ▶ **Übungsaufgabe 4.1.2.8.** (F) Sei $\mathcal{S} = (S, +, 0, -, \cdot, 1)$ ein beliebiger Ring mit 1. Dann gibt es bekanntlich genau einen $\mathcal{Rng}_1$-Homomorphismus $f\colon \mathbb{Z} \to \mathcal{S}$. Deuten Sie diese Aussage als eine über eine freie Algebra. ◀ **UE 271**

UE 272 ▶ **Übungsaufgabe 4.1.2.9.** (F) Deuten Sie Übungsaufgabe 3.1.2.2 als Aussage über den Zusammenhang zwischen direkten Summen $\bigoplus_{i \in X}(\mathbb{N}, +, 0)$ von Kopien des abelschen Monoids $(\mathbb{N}, +, 0)$ und freien abelschen Monoiden. Beschreiben Sie außerdem die freie Algebra über einer Menge X in der Klasse aller abelschen Gruppen sowie aller abelschen Halbgruppen. ◀ **UE 272**

In Unterabschnitt 4.1.3 werden wir sehen, dass es in Varietäten freie Algebren in Hülle und Fülle gibt. In der Klasse der Körper ist das nicht der Fall. Die folgende Übungsaufgabe soll dies illustrieren.

UE 273 ▶ **Übungsaufgabe 4.1.2.10.** (F+) ◀ **UE 273**

(1) Sei $\mathcal{K}$ die Klasse aller Körper der Charakteristik 0 mit $\mathcal{Rng}_1$-Homomorphismen. Zeigen Sie, dass $\mathbb{Q}$ in dieser Klasse frei ist (über welcher Menge?).

(2) Sei K ein Körper der Charakteristik 0 und sei $b \in K$. Dann gibt es einen Körper L mit Charakteristik 0 sowie ein Element $c \in L$, sodass kein $\mathcal{Rng}_1$-Homomorphismus φ mit $\varphi(b) = c$ existiert.

(3) Über welchen Mengen gibt es freie Körper der Charakteristik 0?

4.1.3. Die freie Algebra in Varietäten, Konstruktion über die Termalgebra

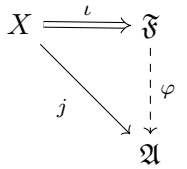
Inhalt in Kurzfassung: Für uns mit Abstand am wichtigsten sind freie Algebren innerhalb von Varietäten. Sie existieren immer und können ziemlich anschaulich verstanden werden als Termalgebren, wobei allerdings manche Terme identifiziert werden, und zwar genau dann, wenn sie stets dieselben Elemente darstellen. Abstrakt formuliert: Die freie Algebra ist ein homomorphes Bild der Termalgebra mit einem Kern, der sich als Durchschnitt aller möglichen Kerne in irgendwelchen Algebren der Varietät ergibt. Erwas anders und ungenau gesprochen: In der freien Algebra gelten genau jene Gesetze, die in allen Algebren und für alle Elemente der Varietät gelten.

Eine sehr transparente, weil vergleichsweise konkrete Konstruktion einer freien Algebra innerhalb einer Varietät geht von der Termalgebra (siehe Definition 2.1.8.1) aus und faktorisiert nach einer geeigneten Kongruenzrelation. Nach dem Homomorphiesatz lässt sich das auch so formulieren: Die freie Algebra ist ein homomorphes Bild der Termalgebra. Genauer: Sei X eine beliebige Menge (Variablenmenge), $\tau = (n_i)_{i\in I}$ ein Typ und $\mathcal{K} = \mathcal{K}(\tau)$ die Klasse aller Algebren des Typs τ. Die Termalgebra $\mathfrak{T}(X,\tau) = (T, (\omega_i^{\mathfrak{T}(X,\tau)})_{i\in I})$ (die absolut freie Algebra des Typs τ über X) ist (zusammen mit der Inklusionsabbildung $\iota_{\mathfrak{T}(X,\tau)}\colon X \to T$, die jeder Variablen $x \in X$ den Term $x \in T$ zuordnet) frei in $\mathcal{K}$. Haben wir es jedoch mit einer speziellen Varietät $\mathcal{V} \subseteq \mathcal{K}$ vom Typ τ, die durch eine Menge Γ von Gesetzen definiert ist, zu tun, so liegen in $\mathcal{V}$ nur jene Algebren $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I})$ aus $\mathcal{K}$, die alle Gesetze $\gamma \in \Gamma$ erfüllen. Eine beliebige Abbildung $j\colon X \to A$ lässt sich in eindeutiger Weise zu einem Homomorphismus $\varphi\colon \mathfrak{T}(X,\tau) \to \mathfrak{A}$ fortsetzen (Einsetzungshomomorphismus). Wir betrachten die durch φ induzierte Kongruenzrelation $\sim_\varphi$ (den Kern von φ), definiert durch: $t_1 \sim_\varphi t_2$ genau dann, wenn $\varphi(t_1) = \varphi(t_2)$. Bezeichne $\sim$ den Durchschnitt aller Kongruenzrelationen auf $\mathfrak{T}(X,\tau)$, die als so ein $\sim_\varphi$ zustandekommen. Auch $\sim$ ist eine Kongruenzrelation auf $\mathfrak{T}(X,\tau)$. Nach Konstruktion stehen zwei Terme t_1 und t_2 über X genau dann in der Relation $t_1 \sim t_2$, wenn für alle Algebren $\mathfrak{A} \in \mathcal{V}$ und alle $a_1, a_2, \ldots \in A$ Einsetzen in t_1 bzw. t_2 dasselbe Element $t_1(a_1, a_2, \ldots) = t_2(a_1, a_2, \ldots) \in A$ liefert. Die resultierende Faktoralgebra $\mathfrak{T}(X,\tau)/_\sim$ zusammen mit der kanonischen Einbettung $x \mapsto [x]_\sim$ von X erweist sich als die in $\mathcal{V}$ freie Algebra über X.

Satz 4.1.3.1. *Varietäten enthalten freie Algebren über beliebigen Mengen, genauer: Sei $\mathcal{V}$ eine Varietät vom Typ τ, X eine Variablenmenge, $\mathfrak{T} = \mathfrak{T}(X,\tau) = (T, (\omega_i^{\mathfrak{T}(X,\tau)})_{i\in I})$ die zugehörige Termalgebra, Γ die $\mathcal{V}$ definierende Menge von Gesetzen (aufgefasst als Teilmenge von T^2) und $\sim$ der Durchschnitt aller Kerne von Homomorphismen $\varphi\colon \mathfrak{T} \to \mathfrak{A}$ mit $\mathfrak{A} \in \mathcal{V}$. Dann ist $\sim$ eine Kongruenzrelation auf $\mathfrak{T}(X,\tau)$, und die Faktoralgebra $\mathfrak{F} := \mathfrak{T}/_\sim = (F, (\omega_i^{\mathfrak{F}})_{i\in I})$ ist frei über (X,ι) mit $\iota\colon X \to T/_\sim$, $x \mapsto [x]_\sim$.*

Beweis. Zunächst beobachten wir, dass $\iota(X)$ ein Erzeugendensystem der Algebra $\mathfrak{F}$ ist: Weil die Variablenmenge X die Termalgebra $\mathfrak{T}$ erzeugt, erzeugt auch $\iota(X)$ die Faktoralgebra $\mathfrak{F} = \mathfrak{T}/_\sim$. Nach unseren bisherigen Überlegungen sowie Lemma 4.1.2.2 sind damit nur noch die folgenden beiden Aussagen zu beweisen:

1. Für $\mathfrak{F}$, X und ι ist die Bedingung, die eine freie Algebra definiert, erfüllt: Für jedes $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I}) \in \mathcal{V}$ und jede Funktion $j\colon X \to A$ gibt es einen Homomorphismus $\varphi\colon \mathfrak{F} \to \mathfrak{A}$ mit $j = \varphi \circ \iota$.



2. $\mathfrak{F} \in \mathcal{V}$, d. h., in $\mathfrak{F}$ gelten alle Gesetze aus Γ.

Nun zum Beweis dieser beiden Aussagen:

1. Wir betrachten die kanonische Einbettung $\iota_{\mathfrak{T}(X,\tau)}\colon X \to T$, die jeder Variablen x den Term x zuordnet. Die universelle Eigenschaft der Termalgebra (nämlich absolut frei über $(X, \iota_{\mathfrak{T}(X,\tau)})$ zu sein; siehe Satz 2.1.8.4) garantiert die Existenz eines eindeutigen Homomorphismus $\psi\colon \mathfrak{T} \to \mathfrak{A}$ mit $j = \psi \circ \iota_{\mathfrak{T}(X,\tau)}$. Durch $\varphi\colon [t]_\sim \mapsto \psi(t)$ ist eine Abbildung $\varphi\colon \mathfrak{F} \to \mathfrak{A}$ wohldefiniert: Denn aus $t_1 \sim t_2$ folgt wegen $\mathfrak{A} \in \mathcal{V}$ und der Definition von $\sim$ insbesondere $t_1 \sim_\psi t_2$, also $\psi(t_1) = \psi(t_2)$. Klarerweise erbt φ von ψ auch die Eigenschaft, ein Homomorphismus zu sein, und erfüllt überdies $j = \varphi \circ \iota$. Damit ist die Existenz eines φ mit den behaupteten Eigenschaften gezeigt. Die Eindeutigkeit schließlich folgt mit Proposition 2.2.1.17, weil φ durch die Bedingung $j = \varphi \circ \iota$ auf dem Bild von ι, bestehend aus allen $[x]_\sim$, $x \in X$, eindeutig bestimmt ist, und diese Menge ein Erzeugendensystem für $\mathfrak{F}$ bildet.

2. Sei $\gamma = (t_1, t_2) \in \Gamma$, wobei die Terme $t_1 = t_1(x_1, \ldots, x_n)$ und $t_2 = t_2(x_1, \ldots, x_n)$ insgesamt von den endlich vielen Variablen $x_1, \ldots, x_n$ abhängen mögen. Zu zeigen ist, dass für alle $z_1, \ldots, z_n \in F$ die Beziehung $t_1^{\mathfrak{F}}(z_1, \ldots, z_n) = t_2^{\mathfrak{F}}(z_1, \ldots, z_n)$ für die entsprechenden Termfunktionen gilt. Wir schreiben $z_i = [s_i]_\sim$ für Terme $s_i \in T$ (die Terme $s_1, \ldots, s_n$ hängen ihrerseits von gewissen Variablen ab, die allerdings weiter keine Rolle spielen). Nach Proposition 2.2.3.22, angewandt auf den kanonischen Homomorphismus $\mathfrak{T} \to \mathfrak{F} = \mathfrak{T}/_\sim$, $t \mapsto [t]_\sim$, gilt $t_1^{\mathfrak{F}}(z_1, \ldots, z_n) = [t^{\mathfrak{T}}(s_1, \ldots, s_n)]_\sim$ (und analog für t_2). Somit haben wir einen beliebigen Homomorphismus $\psi\colon \mathfrak{T} \to \mathfrak{A}$ mit $\mathfrak{A} \in \mathcal{V}$ zu betrachten und für diesen $\psi(t_1^{\mathfrak{T}}(s_1, \ldots, s_n)) = \psi(t_2^{\mathfrak{T}}(s_1, \ldots, s_n))$ zu zeigen. Erneut nach Proposition 2.2.3.22 gelten wegen der Homomorphieeigenschaft von ψ die Gleichungen $\psi(t_1^{\mathfrak{T}}(s_1, \ldots, s_n)) = t_1^{\mathfrak{A}}(\psi(s_1), \ldots, \psi(s_n))$ und $\psi(t_2^{\mathfrak{T}}(s_1, \ldots, s_n)) = t_2^{\mathfrak{A}}(\psi(s_1), \ldots, \psi(s_n))$. Die Elemente $\psi(s_i)$, $i = 1, \ldots, n$, liegen in der Algebra $\mathfrak{A}$, die zur Varietät $\mathcal{V}$ gehört, also insbesondere das Gesetz $\gamma = (t_1, t_2) \in \Gamma$ erfüllt. Folglich gilt tatsächlich

$$\begin{aligned}\psi(t_1^{\mathfrak{T}}(s_1, \ldots, s_n)) &= t_1^{\mathfrak{A}}(\psi(s_1), \ldots, \psi(s_n)) \\ &= t_2^{\mathfrak{A}}(\psi(s_1), \ldots, \psi(s_n)) = \psi(t_2^{\mathfrak{T}}(s_1, \ldots, s_n)).\end{aligned}$$

Somit gilt das Gesetz (t_1, t_2) in $\mathfrak{F}$. Weil $\gamma = (t_1, t_2) \in \Gamma$ beliebig gewählt war, zeigt dies $\mathfrak{F} \in \mathcal{V}$. □

Nach dieser Konstruktion beschäftigen wir uns mit weitergehenden Eigenschaften freier Algebren in Varietäten. Vielfältige Anwendungen hat der folgende Satz:

Satz 4.1.3.2. *Ist $\mathcal{V}$ eine Varietät, $\mathfrak{A} \in \mathcal{V}$ mit Trägermenge A und $X \subseteq A$ ein Erzeugendensystem von $\mathfrak{A}$, so ist $\mathfrak{A}$ homomorphes Bild der in $\mathcal{V}$ über X freien Algebra $\mathfrak{F}$. Insbesondere ist jede Algebra in einer Varietät homomorphes Bild einer freien Algebra.*

Beweis. Laut Satz 4.1.3.1 gibt es in $\mathcal{V}$ eine über X freie Algebra $\mathfrak{F}$. Nach Definition der freien Algebra (4.1.2.4) lässt sich die Inklusionsabbildung $\iota : X \to A$, $x \mapsto x$, (sogar eindeutig) zu einem Homomorphismus $f : \mathfrak{F} \to \mathfrak{A}$ fortsetzen. Das Bild der Algebra $\mathfrak{F}$ unter dem Homomorphismus f ist eine Unteralgebra von $\mathfrak{A}$ (siehe Proposition 2.2.1.28), die X enthält, also, weil X ein Erzeugendensystem von $\mathfrak{A}$ ist, bereits ganz $\mathfrak{A}$. Folglich ist f surjektiv, $\mathfrak{A}$ also homomorphes Bild von $\mathfrak{F}$.
Jede Algebra hat ein Erzeugendensystem, beispielsweise die gesamte Trägermenge. Nach dem bereits Bewiesenen ist also jede Algebra einer Varietät homomorphes Bild einer freien Algebra dieser Varietät. □

UE 274 ► **Übungsaufgabe 4.1.3.3.** (F) Zeigen Sie, dass es in jeder Varietät sowohl initiale als auch terminale Objekte gibt und beschreiben Sie diese. ◄ **UE 274**

Proposition 4.1.3.4. *Sei $\mathcal{V}$ eine nichttriviale Varietät, $\mathfrak{F} \in \mathcal{V}$ mit Trägermenge F und $\iota\colon X \to F$ so, dass $\mathfrak{F}$ in $\mathcal{V}$ frei über (X, ι) ist. Dann ist $\iota\colon X \to F$ injektiv. (Mit anderen Worten: Nach Identifikation vermittels ι kann X als Teilmenge der freien Algebra F aufgefasst werden und ι als die Identität auf X.)*

Beweis. Weil die Varietät $\mathcal{V}$ nicht trivial ist, enthält sie laut Proposition 2.2.5.1 eine Algebra $\mathfrak{A}$ mit einer Trägermenge A mit $|A| \geq |X|$. Dann gibt es eine injektive Variablenbelegung $j\colon X \to A$. Somit gibt es einen eindeutigen Homomorphismus $\varphi\colon \mathfrak{F} \to \mathfrak{A}$ mit $j = \varphi \circ \iota$. Aus der Injektivität von j folgt auch die von ι. □

Die Konstruktion der freien Algebra über einer Variablenmenge X innerhalb einer Varietät $\mathcal{V}$ aus Satz 4.1.3.1 lässt sich so verstehen, dass man sämtliche Terme bildet und Identifikationen genau in dem Maße durchführt, wie es durch die Gesetze in $\mathcal{V}$ erzwungen wird. Allerdings darf das nicht dahingehend missverstanden werden, dass in *jeder* freien Algebra *nur* die Gesetze der Varietät gelten. Beispielsweise liegt die leere Algebra in jeder Varietät $\mathcal{V}$ ohne nullstellige Operationen, ist frei über der leeren Menge und erfüllt überhaupt alle Gesetze, nicht nur diejenigen, die in $\mathcal{V}$ generell gelten. Analoges gilt für die einelementige Algebra. Ein etwas weniger triviales Beispiel ist die vom Element 1 frei erzeugte Gruppe $\mathbb{Z}$. Sie ist abelsch, obwohl das Kommutativgesetz nicht in beliebigen Gruppen gilt. Ein anderes Beispiel ist der von zwei Elementen frei erzeugte Verband. Er erweist sich als distributiv, obwohl das Distributivgesetz nicht in allen Verbänden gilt.

UE 275 ▶ **Übungsaufgabe 4.1.3.5.** (F) Beschreiben Sie den von einer zweielementigen Menge frei erzeugten Verband und zeigen Sie, dass er distributiv ist. ◀ **UE 275**

Das Phänomen, dass in gewissen freien Algebren zusätzliche Gesetze gelten können, hängt damit zusammen, dass in den Gesetzen der Varietät mehr Variablen vorkommen können als es freie Erzeuger gibt:

Satz 4.1.3.6. *Sei $\mathcal{V}$ eine Varietät und $\mathfrak{F}$ frei in $\mathcal{V}$ über (X, ι). Die Variablenmenge X enthalte mindestens n verschiedene Elemente $x_1, \ldots, x_n$. Seien $t_1 = t_1(x_1, \ldots, x_n)$ und $t_2 = t_2(x_1, \ldots, x_n)$ Terme, in denen jeweils nur die Variablen $x_1, \ldots, x_n$ (oder Teilmengen davon) vorkommen. Setzt man $b_i := \iota(x_i)$, so sind die folgenden Aussagen äquivalent:*

(a) In $\mathfrak{F}$ gilt $t(b_1, \ldots, b_n) = t'(b_1, \ldots, b_n)$.

(b) Für alle $\mathfrak{C} \in \mathcal{V}$ gilt $\mathfrak{C} \models t \approx t'$.

(c) Es gilt $\mathfrak{F} \models t \approx t'$.

An dieser Stelle wollen wir zwei bemerkenswerte Konsequenzen dieses Satzes betonen: Zum einen gelten, wie oben bereits angedeutet, in der freien Algebra über zumindest n Erzeugern keine Gesetze zwischen n Variablen, die nicht bereits in sämtlichen Algebren aus der Varietät gelten. Zum anderen ist die Gültigkeit eines Gesetzes in allen Algebren der Varietät – eine Aussage, die über *alle* Elemente quantifiziert – bereits charakterisiert durch die Gültigkeit auf n *konkreten* Elementen in $\mathfrak{F}$.

UE 276 ▶ **Übungsaufgabe 4.1.3.7.** (V) Beweisen Sie Satz 4.1.3.6. ◀ **UE 276**

Steht eine wenigstens abzählbar unendliche Variablenmenge X zur Verfügung, lassen sich also alle Gesetze hinsichtlich Gültigkeit oder Ungültigkeit einfangen, genauer:

Satz 4.1.3.8. *Sei $\mathcal{V}$ eine Varietät und die Variablenmenge X unendlich. Dann gelten in der in $\mathcal{V}$ über X freien Algebra genau jene Gesetze, die in ganz $\mathcal{V}$ gelten.*

Doch zurück zu einer möglichst expliziten Beschreibung freier Algebren. Im Idealfall lässt sich ein algorithmisches Verfahren angeben, wie aus jeder Äquivalenzklasse bezüglich $\sim$ (Bezeichnungsweise aus Satz 4.1.3.1) ein ausgezeichneter Vertreter in *Normalform* ausgewählt werden kann. In konkreten Fällen kann das sehr unterschiedlich kompliziert sein. Der Fall von Monoiden (abelsch oder nicht) wurde bereits in Unterabschnitt 3.1.2 abgehandelt, der abelsche Fall zusammen mit abelschen Gruppen unter einem etwas anderen Gesichtspunkt in Unterabschnitt 4.1.2. Ähnlich leicht ist es auch im Fall von Moduln über einem Ring, nicht viel schwerer für distributive Verbände. Auch für Gruppen und Boolesche Algebren kann man dieses Programm durchführen; wegen der Wichtigkeit freier Gruppen bzw. freier Boolescher Algebren wollen wir uns damit in den nächsten beiden Unterabschnitten 4.1.4 und 4.1.5 näher beschäftigen.

UE 277 ▶ **Übungsaufgabe 4.1.3.9.** (B) Beschreiben Sie freie Algebren in der Varietät $\mathcal{V}$, indem Sie Normalformen angeben. ◀ **UE 277**

1. $\mathcal{V}$ = Varietät der unitären Moduln über einem festen Ring mit 1
2. $\mathcal{V}$ = Varietät der distributiven Verbände

UE 278 ► **Übungsaufgabe 4.1.3.10.** (F) Sei $\mathcal{K}$ die Klasse aller Algebren vom Typ (1), d. h. mit einer einstelligen Operation. Beschreiben Sie die von 2 Elementen frei erzeugte Algebra $F_{\mathcal{K}}(2)$ in $\mathcal{K}$. (geben Sie explizit die Trägermenge von $F_{\mathcal{K}}(2)$ an, z. B. als Teilmenge von $\mathbb{N}$ oder $\mathbb{N} \times \mathbb{Z}$, etc., sowie eine explizite einstellige Operation.) ◄ **UE 278**

UE 279 ► **Übungsaufgabe 4.1.3.11.** (F) Sei $\mathcal{K}$ die Klasse aller Algebren vom Typ $(1, 1)$, d. h. mit zwei einstelligen Operationen. Beschreiben Sie die von einem Element frei erzeugte Algebra $F_{\mathcal{K}}(1)$ in $\mathcal{K}$. (Hinweis: Verwenden Sie das von zwei Elementen frei erzeugte Monoid.) ◄ **UE 279**

4.1.4. Die freie Gruppe

Inhalt in Kurzfassung: Freie Gruppen spielen nicht nur unter den Gesichtspunkten der Universellen Algebra eine wichtige Rolle, sondern treten auch in anderen mathematischen Zusammenhängen auf. Die Elemente freier Gruppen stellt man sich am besten als „reduzierte“ Gruppenwörter vor, also als Ausdrücke wie $x^2y^{-1}x^5$, d. h. als Zeichenfolgen, in denen Potenzen der frei erzeugenden Variablen so aneinandergefügt sind, dass keine Kürzungen mehr möglich sind. Eine sorgfältige Durchführung dieser Konstruktion ist Hauptgegenstand dieses Unterabschnitts.

In diesem Unterabschnitt widmen wir uns einer weit über die Algebra hinaus (zum Beispiel in der algebraischen Topologie, aber auch beim legendären Paradoxon von Hausdorff-Banach-Tarski) wichtigen Klasse freier Algebren, nämlich den freien Gruppen. Wir wollen die allgemeine Konstruktion in Varietäten aus Satz 4.1.3.1 für den Fall der Gruppen konkretisieren. Wir kennen bereits die über einer Menge B freie Halbgruppe. Sie besteht aus allen Zeichenfolgen, die sich mit den Elementen aus B bilden lassen. Wegen des Assoziativgesetzes muss man nicht zwischen verschiedenen Klammerungen unterscheiden. Das gilt bei Gruppen weiterhin. Darüber hinaus ist aber Rücksicht zu nehmen auf die inversen Elemente, durch die sich Gruppen ja von Halbgruppen unterscheiden. Dies ist möglich, indem man für jedes $b \in B$ ein zusätzliches Symbol für sein Inverses einsetzt. In den sich so ergebenden Wörtern muss dann nur noch beachtet werden, dass man kürzen darf, wann immer ein Element aus B direkt mit seinem Inversen zusammentrifft. Dieses Programm soll nun umgesetzt werden.

Konstruktion der freien Gruppe: Sei B eine Menge von „Buchstaben“. Sei $\bar{B}$ eine zu B disjunkte Menge, die gleichmächtig zu B ist, wobei $\bar{\cdot} : B \to \bar{B}$, $x \mapsto \bar{x}$ eine Bijektion sein soll. Sei $M := (B \cup \bar{B})^*$ das freie Monoid. Seine Trägermenge ist die Menge aller Zeichenfolgen, die man mit den „Buchstaben“ aus B und $\bar{B}$ bilden kann (inklusive der

leeren Folge ε). Die Folgen der Länge 1, die nur aus einem Element von $B \cup \bar{B}$ bestehen, identifizieren wir mit dem entsprechenden Element, sodass wir $B \cup \bar{B} \subseteq M$ annehmen dürfen.
Wir setzen die Abbildung $x \mapsto \bar{x}$ zunächst von B auf $B \cup \bar{B}$ fort, indem wir $\bar{\bar{x}} := x$ definieren, und dann auf ganz $M = (B \cup \bar{B})^*$, indem wir $\overline{x_1 \cdots x_n} := \overline{x_n} \cdots \overline{x_1}$ verlangen.
Ein Buchstabenpaar $(x, \bar{x})$, hier gilt also $x \in B \cup \bar{B}$, oder allgemeiner ein Wortpaar $(w, \bar{w})$ nennen wir „komplementär".
Wir nennen ein Element $w \in (B \cup \bar{B})^*$ *reduziert* , wenn in w keine aufeinander folgenden zueinander inversen Buchstaben vorkommen, also wenn w nicht von der Form $w_1 x y w_2$ ist, wobei (x, y) ein komplementäres Buchstabenpaar ist.[3].
Offenbar ist die Konkatenation $w_1 w_2$ genau dann reduziert, wenn sowohl w_1 und w_2 reduziert sind, und überdies der letzte Buchstabe von w_1 nicht komplementär zum ersten Buchstaben von w_2 ist.
Daraus folgt: $w_1 w_2 w_3$ ist genau dann reduziert, wenn sowohl $w_1 w_2$ als auch $w_2 w_3$ reduziert sind.
Sei nun G die Menge aller reduzierten Wörter. Auf der Menge G definieren wir die folgende zweistellige Operation $*$:

- Gegeben $u, v \in G$.
  Sei m das längste Wort mit der Eigenschaft, dass u mit m endet und v mit $\bar{m}$ beginnt, also $u = u'm$, $v = \bar{m}v'$. Wir nennen das Paar $(m, \bar{m})$ den Mittelteil von u, v.
  Dann definieren wir $u * v := u'v'$. Nach Wahl von m ist $u'v'$ reduziert.

- Spezialfall: Wenn uv bereits reduziert ist, dann ist $m = \varepsilon$, und $u * v := uv$.

- Spezialfall: Wenn $v = \bar{u}$, dann ist $m = u$, und $u * v = \varepsilon$.

Man sieht nun leicht, dass das leere Wort ε in dieser Struktur ein neutrales Element ist, und dass mit w auch $\bar{w}$ reduziert ist, wobei $\bar{w}$ bezüglich $*$ zu w invers ist.
Wir überprüfen nun das Assoziativgesetz $u*(v*w) = (u*v)*w$. Sei $(\bar{m}, m)$ der Mittelteil von u, v und $(n, \bar{n})$ der Mittelteil von[4] v, w. Wir unterscheiden zwei Fälle:

- m und n überlappen sich nicht. Das heißt, v hat die Form $v = mtn$, $u = u'\bar{m}$, $w = \bar{n}w'$, und $u't$ sowie tw' sind reduziert.
  Dann ist $(u * v) * w = (u'\bar{m} * mtn) * \bar{n}w' = u'tn * \bar{n}w' = u'tw'$, und analog $u * (v * w) = u'\bar{m} * (mtn * \bar{n}w') = u'\bar{m} * mtw' = u'tw'$.

- m und n überlappen sich in q. Das heißt, v hat die Form $v = pqr$, mit $m = pq$ und $n = qr$. (Die Mittelteile $m = pq$ und $n = qr$ überlappen sich also in q.) Dann gilt $u = u'\bar{m}' = u'\bar{q}\bar{p}$ und $w = \bar{n}w' = \bar{r}\bar{q}w'$, und $u'\bar{q}$ sowie $\bar{q}w'$ sind reduziert.
  Somit folgt $(u * v) * w = (u'\bar{q}\bar{p} * pqr) * w = u'r * \bar{r}\bar{q}w' = u'\bar{q}w'$, und analog erhalten wir $u * (v * w) = u * (pqr * \bar{r}\bar{q}w') = u'\bar{q}\bar{p} * (pw') = u'\bar{q}w'$.

[3] Man beachte die Analogie zur gekürzten Darstellung von rationalen Zahlen.
[4] Achtung: einmal $\bar{\cdot}$ vorne, einmal $\bar{\cdot}$ hinten!

Somit ist $(G, *, \varepsilon, \bar{\cdot})$ eine Gruppe.

G ist frei über B: Sei $j\colon B \to H$ eine beliebige Abbildung von B in eine Gruppe $H = (H, \cdot, 1, {}^{-1})$. Wir müssen zeigen, dass es einen eindeutigen Gruppenhomomorphimus $G \to H$ gibt, der j fortsetzt.

1. Zuerst setzen wir j zu einer Abbildung $\bar{j} : B \cup \bar{B} \to H$ fort, indem wir $\bar{j}(\bar{b}) := j(b)^{-1}$ definieren.

2. Weil M als Monoid frei über $B \cup \bar{B}$ ist, können wir $\bar{j}$ zu einem Monoidhomomorphismus $j^* : M \to H$ fortsetzen.

3. Mit vollständiger Induktion über die Wortlänge sieht man, dass $j^*(\bar{w}) = (j^*(w))^{-1}$ für alle reduzierten Worte w gilt.

4. Wir zeigen nun, dass die Einschränkung von j^* auf die Menge der reduzierten Wörter ein Homomorphismus bezüglich der neu definierten Operation $*$ ist: Wenn $u = u'm$, $v = \bar{m}v'$ und $u * v = u'v'$ ist, dann ist $j^*(u) = j^*(u') \cdot j^*(m)$ und $j^*(v) = j^*(\bar{m}) \cdot j^*(v')$. Da $j^*(m)$ und $j^*(\bar{m})$ in H nach dem letzten Punkt zueinander invers sind, folgt wie gewünscht $j^*(u * v) = j^*(u) \cdot j^*(v)$.

5. Als Letztes zeigen wir, dass die Einschränkung von j^* auf G der einzige Gruppenhomomorphismus $G \to H$ ist, der j fortsetzt. Dies folgt unmittelbar aus Proposition 2.2.1.17, sobald wir gezeigt haben, dass G von B erzeugt wird, in Zeichen $G = \langle B \rangle$. Da die Buchstaben aus $\bar{B}$ genau die Inversen (in G) der Buchstaben aus B sind, umfasst das Erzeugnis von B jedenfalls $B \cup \bar{B}$. Ist $w = x_1 \cdots x_n$ ein beliebiges reduziertes Wort, wobei $x_i \in B \cup \bar{B}$, so gilt auch $w = x_1 * \cdots * x_n$ bezüglich der neu definierten Operation $*$ (da auch die Teilwörter $x_1 * \cdots * x_k$ reduziert sind). Daraus folgt $w \in \langle B \rangle$.

Zum Abschluss noch eine Bemerkung mit Ausblick auf das berühmte *Paradoxon von Hausdorff-Banach-Tarski*. Dieses macht Gebrauch davon, dass bereits in der von zwei Elementen x, y frei erzeugten Gruppe $F(x, y)$ eine Vorstellung, die in vielen Gruppen sinnvolle Intuitionen nahelegt, in $F(x, y)$ an ihre Grenzen stößt: nämlich dass Translationen in Gruppen die Größe von Teilmengen erhalten. Denn es liegt nahe, $F(x, y)$ als Vereinigung des Singletons $\{\varepsilon\}$ (leeres Wort) mit den vier zueinander gleich großen, unendlichen Teilmengen F_x, $F_{x^{-1}}$, F_y und $F_{y^{-1}}$ anzusehen, die aus all jenen Zeichenketten bestehen, die mit x, x^{-1}, y bzw. mit y^{-1} beginnen. Jede dieser vier unendlichen Mengen, so könnte man argumentieren, entspricht also etwa einem Viertel der Gruppe $F(x, y)$. Für die Translation $t_x : w \mapsto xw$, die ein Element $w \in F(x, y)$ von links mit x multipliziert gilt jedoch einerseits

$$t_x(F(x, y) \setminus F_{x^{-1}}) = t_x(F_x \cup F_y \cup F_{y^{-1}} \cup \{\varepsilon\}) = F_x \quad \text{(aus drei Vierteln wird eines)},$$

andererseits

$$t_x(F_{x^{-1}}) = F_{x^{-1}} \cup F_y \cup F_{y^{-1}} \cup \{\varepsilon\} = F(x, y) \setminus F_x \quad \text{(aus einem Viertel werden drei)}.$$

Man spricht von einer *paradoxen Zerlegung* von $F(x, y)$. Man kann eine zu $F(x, y)$ isomorphe Gruppe von Rotationen der dreidimensionalen Kugel finden und die paradoxe Zerlegung von $F(x, y)$ ausnutzen, um eine Einheitsvollkugel in mehrere Teile zu zerlegen, die, wenn man sie geeignet im Raum bewegt, wieder zusammensetzt zwei Einheitsvollkugeln ergeben. Da Bewegungen Volumina (d. h. das dreidimensionale Lebesguemaß) erhalten, ist dies nur möglich, wenn die Teile, die in der Zerlegung der Kugel vorkommen, nicht alle messbar sind. Tatsächlich ist die Konstruktion auch nur mit Hilfe des Auswahlaxioms möglich, ohne das die Existenz nicht messbarer Mengen nicht bewiesen werden kann.

UE 280 ► **Übungsaufgabe 4.1.4.1.** (D,E) Beweisen Sie das Paradoxon von Hausdorff-Banach-Tarski. Wenn das zu schwierig ist: Machen Sie sich so weit kundig, dass Sie wichtige Grundideen präsentieren können, die das Paradoxon wenigstens plausibel machen. ◄ **UE 280**

4.1.5. Die freie Boolesche Algebra

Inhalt in Kurzfassung: Nun wird für Boolesche Algebren das analoge Ziel verfolgt wie zuletzt für Gruppen. Wir geben eine Beschreibung freier Boolescher Algebren als Mengenalgebren. Anwendungen haben sie beispielsweise in der Aussagenlogik.

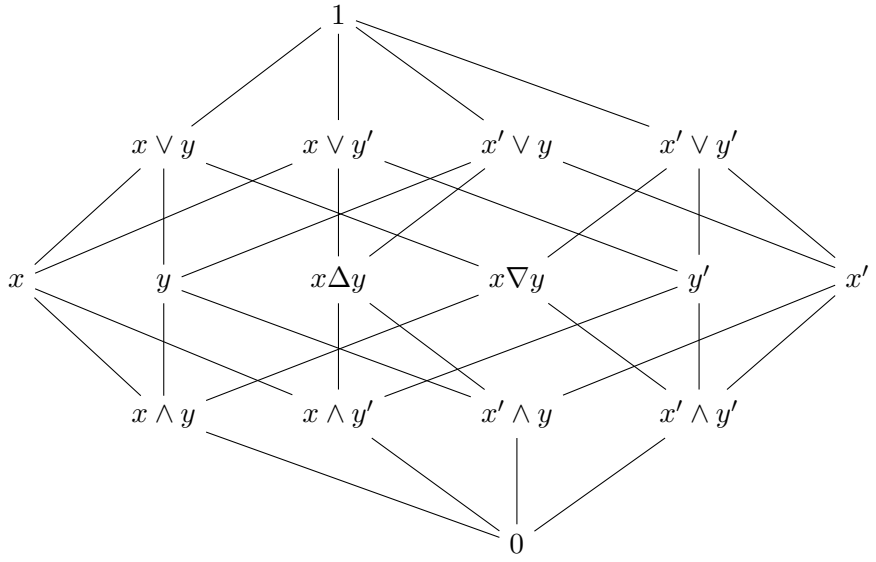
Zum Abschluss unserer Untersuchungen der konkreten Beispiele wollen wir noch freie Boolesche Algebren als Mengenalgebren darstellen. Sei die Menge X vorgegeben. Gesucht ist eine Boolesche Algebra $F(X)$ zusammen mit einer Einbettung $\iota\colon X \to F(X)$, sodass $F(X)$ frei ist über (X, ι). Der Satz 4.1.3.1 liefert eine abstrakte Methode zur Konstruktion, genauso wie auch Satz 4.1.6.1 im nächsten Unterabschnitt. Der Darstellungssatz von Stone 3.6.8.17 sagt uns darüber hinaus, dass wir uns die Elemente von $F(X)$ auch als Teilmengen einer Menge M denken dürfen, wobei die Operationen in der Booleschen Algebra gerade die entsprechenden mengentheoretischen sind. Eine konkrete Beschreibung gelingt wie folgt:

> Als Trägermenge wählt man die Menge $M := \{0,1\}^X$ aller Funktionen $f\colon X \to \{0,1\}$.
>
> Jedem Element $x \in X$ ordnen wir die Menge
>
> $$\iota(x) := \{f\colon X \to \{0,1\} \mid f(x) = 1\}$$
>
> zu. (Für endliches X ist das genau die Hälfte aller Elemente von M. Für unendliches X hat diese Menge das Maß $1/2$, wenn man das kanonische Produktmaß auf M verwendet; überdies sind die Mengen $\iota(x)$ alle voneinander im wahrscheinlichkeitstheoretischen Sinn unabhängig. Insbesondere sind alle endlichen Schnitte der Form $\iota(x_1) \cap (M \setminus \iota(x_2)) \cap \iota(x_3) \cap \cdots$ nicht leer.)
>
> $F(X)$ kann nun realisiert werden als jene Boolesche Unteralgebra von $\mathfrak{P}(M)$, die von den $\iota(x)$ (mit $x \in X$) erzeugt wird.

Satz 4.1.5.1. *Mit den obigen Bezeichnungsweisen gilt: Die Algebra $F(X)$ ist in der Varietät der Booleschen Algebren frei über (X, ι).*

UE 281 ► Übungsaufgabe 4.1.5.2. (V) Beweisen Sie Satz 4.1.5.1. **◄ UE 281**

Ist $|X| = n \in \mathbb{N}$ endlich, so folgt $|M| = 2^n$. Man überlegt sich schnell, dass jede Teilmenge von M als Element von $F(X)$ auftritt. Folglich ist $|F(X)| = 2^{2^n}$. Die von 0 Elementen frei erzeugte Boolesche Algebra ist, wenig überraschend, die triviale zweielementige. Für $X = \{x\}$, also $n = 1$, hat $F(x)$ vier Elemente.
Die von 2 Elementen x und y frei erzeugte Boolesche Algebra hat die 4 Atome $x \wedge y$, $x' \wedge y$, $x \wedge y'$ und $x' \wedge y'$ und insgesamt 16 Elemente. Im folgenden Diagramm verwenden wir die Abkürzungen $x\Delta y := (x' \wedge y) \vee (x \wedge y')$ und $x\nabla y := (x\Delta y)'$.



Die Atome entsprechen den möglichen Belegungen von 2 aussagenlogischen Variablen, also den Zeilen in einer Wahrheitstabelle; die 16 Elemente der Booleschen Algebra entsprechen den möglichen Werteverläufen, die durch eine Formel induziert werden. So entspricht etwa die Vereinigung der 3 Atome $x \wedge y$, $x' \wedge y$, $x \wedge y'$ einer Formel mit den beiden Variablen x und y, die immer dann wahr ist, wenn zumindest eine der beiden Variablen den Wert wahr erhält — also zum Beispiel der Formel $x \vee y$ oder der dazu äquivalenten Formel $y \vee (x \wedge x)$.
In der von 3 Elementen x, y, z frei erzeugten Booleschen Algebra gibt es 64 Elemente und 8 Atome, darunter etwa $x \wedge y \wedge z$ und $x \wedge y' \wedge z'$.
Jede von unendlich vielen Elementen frei erzeugte Boolesche Algebra ist atomlos. Die von abzählbar vielen Elementen frei erzeugte Boolesche Algebra ist isomorph zur Booleschen Algebra der *clopen* (d. h. sowohl „closed“, also abgeschlossenen, als auch „open“, also offenen) Teilmengen der Cantormenge.

4.1.6. Die freie Algebra als subdirektes Produkt

Inhalt in Kurzfassung: Die Konstruktion der freien Algebra innerhalb einer Varietät als homomorphes Bild der Termalgebra aus Unterabschnitt 4.1.3 ergänzen wir nun durch

eine zweite Konstruktion, nämlich als subdirektes Produkt, d. h. als Unteralgebra eines (in der Regel sehr „großen“) direkten Produktes. Diese Konstruktion ist zwar abstrakter und weniger anschaulich als jene mit Hilfe der Termalgebra, sie hat aber einen entscheidenden Vorteil in Hinblick auf den Beweis des Satzes von Birkhoff im nachfolgenden Unterabschnitt: In der Konstruktion muss man nicht alle Eigenschaften einer Varietät voraussetzen, sondern nur die Abgeschlossenheit bezüglich dreier Konstruktionen, nämlich bezüglich Unteralgebren, direkter Produkte und isomorpher Bilder. Genau das wird hinreichen, um die nichttriviale Implikation im Satz von Birkhoff zu beweisen.

Es soll noch ein zweites Verfahren zur Konstruktion einer freien Algebra innerhalb einer Klasse $\mathcal{K}$ beschrieben werden, und zwar als sogenanntes subdirektes Produkt. Zum Ersten ist diese Konstruktion deshalb von Interesse, weil sie nicht nur in der Algebra häufig vorkommt, sondern in ähnlicher Form auch in anderen Teilen der Mathematik auftritt. Zum Zweiten werden dabei etwas schwächere Voraussetzungen an die Klasse $\mathcal{K}$ hinreichen als in Unterabschnitt 4.1.3. Und zwar ist es nicht notwendig, dass $\mathcal{K}$ eine Varietät ist. Es genügt, wenn $\mathcal{K}$ abgeschlossen ist bezüglich der Bildung von isomorphen Kopien, direkten Produkten und Unteralgebren. Das wird sich als nützlich beim Beweis des Satzes von Birkhoff erweisen. Der Grundgedanke der Konstruktion ist der Folgende: Wir beginnen mit der Beobachtung, dass sich jede Algebra $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I})$ eines Typs $\tau = (n_i)_{i\in I}$ als homomorphes, insbesondere surjektives Bild der Termalgebra $\mathfrak{T} = \mathfrak{T}(A,\tau) = (T, (\omega_i^{\mathfrak{T}(A,\tau)})_{i\in I})$ (die Elemente von A werden also als Variable verwendet) darstellen lässt, woraus $|A| \leq |T|$ folgt. (Um einen Epimorphismus $\varphi\colon \mathfrak{T} \to \mathfrak{A}$ zu erhalten, geht man von der Inklusionsabbildung $\iota : A \mapsto T$ aus, wählt als $j\colon A \to A$ die Identität und wählt, gemäß der universellen Eigenschaft der Termalgebra, einen Homomorphismus φ mit $j = \varphi \circ \iota$.) Ist die Erzeugendenmenge X, über der die gesuchte Algebra $\mathfrak{F}$ in $\mathcal{K}$ frei sein soll, vorgegeben, so ist die Kardinalität der Termmenge a priori durch $|T| \leq \kappa := \max\{|X|, |I|, |\mathbb{N}|\}$ beschränkt (siehe Übungsaufgabe 4.1.6.2). Weil $\mathcal{K}$ abgeschlossen ist bezüglich isomorpher Bilder, gibt es daher eine Menge Z mit folgender Eigenschaft (jede Menge Z mit $|Z| \geq \kappa$ leistet das): Zu jeder Algebra $\mathfrak{A} \in \mathcal{K}$, die von X erzeugt wird, gibt es eine isomorphe Kopie in $\mathcal{K}$, deren Trägermenge eine Teilmenge von Z ist. Dies vor Augen definieren wir die Teilklasse $\mathcal{K}(Z)$ als die Menge aller $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I}) \in \mathcal{K}$ mit $A \subseteq Z$. Man beachte, dass es sich bei $\mathcal{K}(Z)$ tatsächlich um eine Menge handelt (siehe Übungsaufgabe 4.1.6.2). Nun betrachten wir die Menge P aller Paare $p = (\mathfrak{A}, j)$ mit $\mathfrak{A} = (A, (\omega_i^{\mathfrak{A}})_{i\in I}) \in \mathcal{K}(Z)$ und $j\colon X \to A$, wobei wir auch $\langle j(X)\rangle = A$ voraussetzen, dass also das Bild von X unter j ganz A erzeugt. Laut Voraussetzung liegt das direkte Produkt

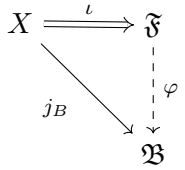
$$\mathfrak{M} := \prod_{p=(\mathfrak{A},j)\in P} \mathfrak{A} = (M, (\omega_i^{\mathfrak{M}})_{i\in I})$$

in $\mathcal{K}$. Wir definieren $\iota\colon X \to M$ durch $\iota : x \mapsto (j(x))_{p=(\mathfrak{A},j)\in P}$ und $\mathfrak{F} := \langle \iota(X)\rangle = (F, (\omega_i^{\mathfrak{F}})_{i\in I})$ als die vom Bild $\iota(X) \subseteq M$ erzeugte Unteralgebra von $\mathfrak{M}$. Als Unteralgebra (Subalgebra) des direkten Produktes $\mathfrak{M}$ mit auch auf der Einschränkung auf $\mathfrak{F}$ surjektiven Projektionen $\pi_{p_0} : (a_p)_{p\in P} \mapsto a_{p_0}$ (nur deshalb die Voraussetzung $\langle j(X)\rangle = \mathfrak{A}$

für alle $p = (\mathfrak{A}, j) \in P$, siehe Übungsaufgabe 4.1.6.2) ist $\mathfrak{F}$ ein sogenanntes *subdirektes Produkt*. Die Behauptung lautet nun:

Satz 4.1.6.1. *Sei $\mathcal{K}$ eine Klasse von Algebren des gleichen Typs und abgeschlossen unter isomorphen Bildern, direkten Produkten und Unteralgebren. Dann ist das oben konstruierte subdirekte Produkt $\mathfrak{F}$ frei über (X, ι) in $\mathcal{K}$.*

Beweis. Aus den bisherigen Überlegungen folgt $\mathfrak{M} \in \mathcal{K}$, wegen der Abgeschlossenheit von $\mathcal{K}$ bezüglich Unteralgebren also auch $\mathfrak{F} \in \mathcal{K}$. Zu zeigen bleibt, dass es zu jedem $j_B \colon X \to B$ und $\mathfrak{B} = (B, (\omega_i^{\mathfrak{B}})_{i \in I}) \in \mathcal{K}$ einen eindeutigen Homomorphismus $\varphi \colon \mathfrak{F} \to \mathfrak{B}$ mit $j_B = \varphi \circ \iota$ gibt.



OBdA (siehe Übungsaufgabe 4.1.6.2) dürfen wir annehmen, dass $\mathfrak{B}$ vom Bild $j_B(X)$ erzeugt wird. Die Eindeutigkeit von φ folgt, weil $\mathfrak{F}$ von $\iota(X)$ erzeugt wird (Übungsaufgabe 2.2.1.17). Zur Existenz: Laut Konstruktion und wegen $\mathfrak{B} = \langle j_B(X) \rangle$ gibt es ein $p = (\mathfrak{A}, j) \in P$, sodass $(\mathfrak{B}, j_B)$ und $(\mathfrak{A}, j)$ äquivalent sind, genauer: Es gibt einen Isomorphismus $\psi \colon \mathfrak{A} \to \mathfrak{B}$ mit $j_B = \psi \circ j$. Die Projektionsabbildung $\varphi = \varphi_p \colon \mathfrak{F} \to \mathfrak{A}$ mit $p = (\mathfrak{A}, j)$ (das ist die Einschränkung der auf ganz M definierten Projektion π_p auf die Teilmenge $F \subseteq M$), definiert durch $(a_{p'})_{p' \in P} \mapsto a_p$, ist dann der gesuchte Homomorphismus mit $j_B = \varphi \circ \iota$. □

In den Vorbereitungen bzw. im Beweis von Satz 4.1.6.1 wurden der Übersichtlichkeit halber an einigen Stellen gewisse Details nicht in maximaler Ausführlichkeit abgehandelt. Das soll nun im Rahmen einer Übungsaufgabe nachgeholt werden.

UE 282 ► **Übungsaufgabe 4.1.6.2.** (V) Führen Sie die oben knapp behandelten Argumente an folgenden Stellen genau aus: ◄ **UE 282**

1. Begründen Sie die Ungleichung $|T| \leq \kappa := \max\{|X|, |I|, |\mathbb{N}|\}$. Hinweis: Bedienen Sie sich des mengentheoretischen Anhangs (Kapitel A).

2. Warum ist $\mathcal{K}(Z)$ eine Menge? (Kapitel A)

3. Erläutern Sie, warum die Projektionen π_p surjektiv sind, auch wenn man sie auf $\mathfrak{F}$ einschränkt.

4. Erläutern Sie, inwiefern das Argument nach der Abkürzung *OBdA* wirklich *ohne Beschränkung der Allgemeinheit* beweist, was behauptet wird.

4.1.7. Der Satz von Birkhoff

Inhalt in Kurzfassung: Mit dem Beweis des Satzes von Birkhoff, einem der wichtigsten Ergebnisse der Universellen Algebra, erreichen wir nun das erste große Ziel dieses Kapitels.

Wie schon angekündigt ist die Konstruktion der freien Algebra aus Unterabschnitt 4.1.6 ein wesentliches Hilfsmittel beim Beweis des für die Gleichungstheorie der Universellen Algebra zentralen Satzes von Birkhoff.

Satz 4.1.7.1. *(Satz von Birkhoff) Eine Klasse $\mathcal{V}$ von Algebren vom gleichen Typ ist genau dann gleichungsdefiniert, wenn sie unter $\mathsf{H}, \mathsf{S}, \mathsf{P}$, d. h. unter der Bildung von homomorphen Bildern, Unteralgebren und direkten Produkten, abgeschlossen ist (siehe Definition 4.1.1.1).*

Beweis. Wir wissen bereits, dass jede Varietät $\mathcal{V}$ die genannten Abschlusseigenschaften hat. Zu beweisen bleibt deshalb, dass es zu jeder Klasse $\mathcal{V}$, die unter H, S und P abgeschlossen ist, eine Menge Γ von Gesetzen mit $\mathcal{V} = \mathrm{Mod}(\Gamma)$ gibt, also sodass $\mathcal{V}$ die durch Γ definierte Varietät ist. Da $\mathcal{V}$ vorgegeben ist, liegt es nahe, die Menge Γ *aller* Gesetze zu betrachten, die in sämtlichen $\mathfrak{A} \in \mathcal{V}$ gelten. Aus der Definition von Γ ergibt sich, dass $\mathcal{V} \subseteq \mathrm{Mod}(\Gamma)$ gilt. Zu zeigen bleibt die umgekehrte Inklusion, nämlich dass jede Algebra, die alle Gesetze aus Γ erfüllt, in $\mathcal{V}$ liegt.
Sei also $\mathfrak{A} \in \mathrm{Mod}(\Gamma)$ beliebig, mit Trägermenge A. Die Klasse $\mathcal{V}$ erfüllt die Voraussetzungen an $\mathcal{K}$ in Satz 4.1.6.1. Also gibt es eine Algebra $\mathfrak{F} = \mathfrak{F}(A) = (F, (\omega_i^{\mathfrak{F}})_{i \in I}) \in \mathsf{SP}(\mathcal{V}) \subseteq \mathcal{V}$, die von der Menge A frei erzeugt wird. Jedes Element von $\mathfrak{F}$ hat nach Proposition 2.2.1.14 die Form $t^{\mathfrak{F}}(a_1, \ldots, a_n)$, wobei t ein Term ist und $a_1, \ldots, a_n$ Elemente der Erzeugendenmenge A sind. (Allerdings sind weder der Term t noch die a_i im Allgemeinen eindeutig bestimmt.) Aus Satz 4.1.3.6 folgt, dass durch

$$\varphi(t^{\mathfrak{F}}(a_1, \ldots, a_n)) := t^{\mathfrak{A}}(a_1, \ldots, a_n)$$

ein Homomorphismus $\varphi : \mathfrak{F} \to \mathfrak{A}$ *wohldefiniert* wird. Offensichtlich ist φ surjektiv. Daher ist $\mathfrak{A}$ ein homomorphes Bild von $\mathfrak{F} \in \mathcal{V}$, also $\mathfrak{A} \in \mathsf{H}(\mathcal{V}) \subseteq \mathcal{V}$. □

Anmerkung 4.1.7.2. Achtung: Man darf den letzten Beweisschritt (aus $\mathfrak{A} \in \mathrm{Mod}(\Gamma)$ folgt $\mathfrak{A} \in \mathsf{H}(\mathcal{V})$) nicht abkürzen, indem man den Beweis von Satz 4.1.3.2 wiederholt (also durch die Freiheit einen Homomorphismus $\varphi : \mathfrak{F} \to \mathfrak{A}$ erhält, der die identische Abbildung $j : A \to \mathfrak{A}$ fortsetzt). Der Grund dafür ist, dass $\mathfrak{F}$ nur in $\mathcal{V}$ frei ist, wir aber an dieser Stelle noch nicht wissen, dass $\mathfrak{A}$ tatsächlich in $\mathcal{V}$ liegt – das wollen wir ja gerade erst zeigen.

4.2. Koprodukte und Polynomalgebren

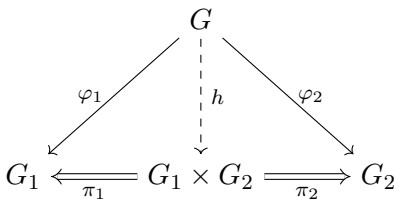
Koprodukte (einfache Beispiele und Definition in 4.2.1) ähneln freien Algebren in vielerlei Hinsicht. Grob lässt sich der Unterschied so fassen: Freie Algebren werden von den

Elementen einer gegebenen Menge ohne weitere Struktur auf möglichst *freie* Weise erzeugt, Koprodukte von zwei oder mehreren vorgegebenen Strukturen. Tatsächlich lässt sich die freie Algebra verwenden, um in einer Varietät auch beliebige Koprodukte zu konstruieren (4.2.2). Unsere wichtigste Anwendung sind Polynomalgebren in der Varietät der kommutativen Ringe mit 1 (4.2.3). Eine ähnliche universelle Eigenschaft, allerdings als Verbindung zweier Strukturen unterschiedlichen Typs, hat der Gruppenring bzw. der Monoidring (4.2.4).

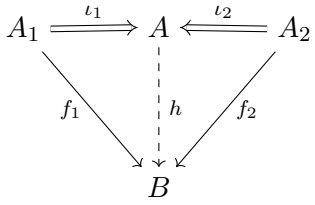
4.2.1. Bekannte Beispiele und Definition des Koproduktes

Inhalt in Kurzfassung: In Koprodukten wie in freien Algebren (in Varietäten) geht es darum, Elemente, die zunächst nichts miteinander zu tun haben, so in einer einzigen Algebra der Varietät unterzubringen, dass sie sich im Rahmen gewisser Vorgaben möglichst ungebunden verhalten. Der Unterschied: Bei freien Algebren waren die Elemente völlig ohne Beziehung zueinander, wie Variablen, die nur den Gesetzen der Varietät unterworfen sind. Bei Koprodukten entstammen die Elemente bereits vorgegebenen Algebren der Varietät, wobei die Struktur der beteiligten Algebren möglichst erhalten bleiben soll, Elemente aus derselben Algebra sich also sehr wohl weiterhin als solche verhalten sollen. Tatsächlich ähneln Koprodukte in vielen Varietäten tatsächlich freien Algebren (z. B. Gruppen und Vektorräume). Die allgemeine Definition ist aber kategorientheoretischer Natur ohne Bezugnahme auf Varietäten, wieder als initiales Objekt in einer geeigneten Kategorie. Als Folgerung sind Koprodukte bis auf Isomorphie eindeutig bestimmt.

Beispiel 4.2.1.1 (Das Produkt als universelles Objekt)**.** Wir erinnern uns: Sind G_1 und G_2 Gruppen oder sonst zwei Algebren desselben Typs, dann hat das direkte Produkt $G_1 \times G_2$ zusammen mit den Projektionen $\pi_i \colon G_1 \times G_2 \to G_i$ $(i = 1, 2)$, definiert durch $\pi_1(x, y) = x$ und $\pi_2(x, y) = y$, nach Proposition 2.2.2.4 folgende universelle Eigenschaft: Für jede Gruppe G und beliebige Homomorphismen $\varphi_i \colon G \to G_i$, $i = 1, 2$, gibt es genau einen Homomorphismus $h \colon G \to G_1 \times G_2$ mit $\varphi_i = \pi_i \circ h$ für $i = 1, 2$.



Beispiel 4.2.1.2 (Die direkte Summe als universelles Objekt)**.** Andererseits erinnern wir uns an die direkte Summe von abelschen Gruppen (bzw. von Moduln, spezieller von Vektorräumen): Sind A_1 und A_2 abelsche Gruppen, dann hat die direkte Summe $A = A_1 \oplus A_2$ zusammen mit den kanonischen Einbettungen $\iota_i \colon A_i \to A$ $(i = 1, 2)$, definiert durch $\iota_1(a_1) = (a_1, 0)$ und $\iota_2(a_2) = (0, a_2)$, nach Proposition 3.3.2.2 folgende universelle Eigenschaft:
Für jede abelsche Gruppe B und beliebige Homomorphismen $f_i : A_i \to B$, $i = 1, 2$, gibt es genau einen Homomorphismus $h : A \to B$ mit $f_i = h \circ \iota_i$ für $i = 1, 2$.



Man beachte, dass die charakteristische Eigenschaft der direkten Summe sehr ähnlich der charakteristischen Eigenschaft des Produktes ist; nur zeigen alle Pfeile nun in die entgegengesetzte Richtung.
Die Verallgemeinerung der direkten Summe zum Koprodukt von mehr als zwei Faktoren sowie auf beliebige Kategorien liegt mit dieser Sichtweise auf der Hand:

Definition 4.2.1.3. Sei $\mathcal{C}$ eine Kategorie und seien A_i, $i \in I$ (Indexmenge), Objekte in $\mathcal{C}$. Ein Paar $(A, (\iota_i)_{i\in I})$ heißt *Koprodukt* der A_i in $\mathcal{C}$, wenn folgende Bedingungen erfüllt sind:

- $A \in \mathrm{Ob}(\mathcal{K})$.
- Für alle $i \in I$ ist $\iota_i \colon A_i \to A$ ein Morphismus in $\mathcal{C}$.
- Für alle Objekte B in $\mathcal{C}$ und alle Familien von Morphismen $f_i \colon A_i \to B$, $i \in I$, gibt es genau einen Morphismus $f \colon A \to B$, der $f \circ \iota_i = f_i$ für alle $i \in I$ erfüllt.

Ein Objekt A heißt Koprodukt der A_i in $\mathcal{C}$, wenn es Morphismen $\iota_i \colon A_i \to A$, $i \in I$, gibt, sodass $(A, (\iota_i)_{i\in I})$ Koprodukt der A_i in $\mathcal{C}$ ist. Symbolisch schreibt man kurz:

$$A = \coprod_{i\in I} A_i$$

Im Fall von nur zwei Objekten, also $|I| = 2$, oBdA $I = \{1, 2\}$ schreibt man das Koprodukt vorzugsweise in Infixnotation als $A = A_1 \amalg A_2$.

UE 283 ► **Übungsaufgabe 4.2.1.4.** (F) Sei $\mathcal{C}$ eine Kategorie, und seien A_1, A_1', A_2, A_2' Objekte von $\mathcal{C}$, wobei A_1 und A_1' in $\mathcal{C}$ äquivalent (in Kategorien von algebraischen Strukturen: isomorph) sind, ebenso A_2 und A_2'. Sei (s, ι_1, ι_2) ein Koprodukt von A_1 und A_2 in $\mathcal{C}$. Zeigen Sie, dass es auch ein Koprodukt von A_1' und A_2' in $\mathcal{C}$ gibt, und zwar eines der Form $(s, ?, ?)$.
Formulieren Sie einen analogen Satz für Produkte. ◄ **UE 283**

Offenbar lässt sich das Koprodukt gegebener Algebren $V_i \in \mathcal{K}$ als initiales Objekt in einer geeigneten Kategorie $\mathcal{C} = \mathcal{C}((V_i)_{i\in I})$ deuten, weshalb jedes Koprodukt einer gegebenen Familie von Algebren bis auf Isomorphie eindeutig bestimmt ist, wobei der Isomorphismus mit den ι_i verträglich ist, vgl. Satz 2.3.3.2.

UE 284 ► **Übungsaufgabe 4.2.1.5.** (V) Führen Sie dieses Argument im Detail aus, indem Sie insbesondere die von den V_i abhängige Kategorie $\mathcal{C}((V_i)_{i\in I})$ definieren. ◄ **UE 284**

Das Koprodukt von zwei (oder mehr) Strukturen hängt nicht nur von den Strukturen selbst ab, sondern auch von der Klasse, in der man das Koprodukt sucht. In der Klasse $\mathcal{Ab}$ aller abelschen Gruppen ist das Koprodukt zweier abelscher Gruppen durch die direkte Summe gegeben. In der Klasse $\mathcal{Grp}$ aller Gruppen ist bereits das Koprodukt zweier abelscher Gruppen komplizierter, wie die folgenden Aufgaben zeigen (vgl. auch Übungsaufgabe 3.3.2.4).

UE 285 ► **Übungsaufgabe 4.2.1.6.** (B) Sei G ein Koprodukt von $\mathbb{Z}$ mit $\mathbb{Z}$ in $\mathcal{Grp}$. Zeigen Sie, dass G nicht kommutativ und daher insbesondere nicht die Gruppe $\mathbb{Z} \times \mathbb{Z}$ sein kann. ◄ **UE 285**
Hinweis: Wählen sie geeignete Homomorphismen $f_1, f_2 \colon \mathbb{Z} \to H$ in eine (beliebige) nichtkommutative Gruppe H.

UE 286 ► **Übungsaufgabe 4.2.1.7.** (B,E) Sei (G, i_1, i_2) ein Koprodukt von C_2 und C_2 in $\mathcal{Grp}$. (Ja, 2 Mal die 2-elementige Gruppe.) Sei F_2 die von 2 Elementen frei erzeugte Gruppe. ◄ **UE 286**

(1) Zeigen Sie, dass G unendlich groß ist, und dass G nicht kommutativ ist.
Hinweis: Finden Sie verschiedene Homomorphismen von C_2 in die Gruppe H aller Permutationen von $\mathbb{Z}$, die benachbarte Elemente immer auf benachbarte Elemente abbilden. Anders gesagt: Sei $A := \{(x, y) \in \mathbb{Z}^2 : |x - y| = 1\}$; die Gruppe H ist dann die Menge aller Automorphismen der relationalen Struktur $(\mathbb{Z}, A)$.

(2) Zeigen Sie, dass G nicht zu F_2 isomorph ist.

UE 287 ► **Übungsaufgabe 4.2.1.8.** (W) Sei $\mathcal{Grp}$ die Klasse aller Gruppen, und sei (C, ι_1, ι_2) Koprodukt von G_1 und G_2 in $\mathcal{Grp}$. Dann sind ι_1 und ι_2 injektiv. (Hinweis: Betrachten Sie $D := G_1$.) Verallgemeinern Sie Ihr Argument auf Koprodukte beliebig vieler Gruppen. ◄ **UE 287**
Warum funktioniert Ihr Beweis nicht für die Klasse aller kommutativen Ringe mit Einselement? Weisen Sie auf den Schritt in Ihrem Beweis hin, den Sie in der Klasse der kommutativen Ringe mit Einselement nicht durchführen können.

UE 288 ► **Übungsaufgabe 4.2.1.9.** (F) Sei $\mathcal{Rng}_1$ die Klasse aller kommutativen Ringe mit 1. Zeigen Sie, dass der einelementige Ring in $\mathcal{Rng}_1$ ein Koprodukt von $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ ist, und kontrastieren Sie dieses Resultat mit der vorigen Aufgabe. ◄ **UE 288**

UE 289 ► **Übungsaufgabe 4.2.1.10.** (E) Seien G_1 und G_2 zwei Gruppen (nicht notwendig abelsch). Beschreiben Sie das Koprodukt von G_1 und G_2 in der Kategorie $\mathcal{Grp}$ der Gruppen. ◄ **UE 289**
Hinweis: Orientieren Sie sich an der Konstruktion freier Gruppen.

4.2.2. Konstruktion des Koproduktes als freie Algebra

Inhalt in Kurzfassung: Die bereits in Unterabschnitt 4.2.1 angedeutete Ähnlichkeit zwischen freien Algebren und Koprodukten schlägt sich auch technisch wieder: In Varietäten existieren Koprodukte uneingeschränkt, und der Beweis dafür lässt sich zurückführen auf die uneingeschränkte Existenz freier Objekte in Varietäten.

Koprodukte existieren nicht in beliebigen Kategorien.

UE 290 ► **Übungsaufgabe 4.2.2.1.** (B) Finden Sie eine (möglichst interessante) Kategorie, in der es nicht beliebige Koprodukte gibt. ◄ **UE 290**

Ähnlich wie bei freien Algebren erweist sich aber die Voraussetzung, dass es sich bei der Kategorie um eine Varietät handelt, als hinreichend für die Existenz beliebiger Koprodukte. In der Konstruktion kann man sich die Arbeit erleichtern, wenn man von der Existenz freier Algebren in Varietäten Gebrauch macht.

Satz 4.2.2.2. *Ist $\mathcal{V}$ eine Varietät, so existieren Koprodukte in $\mathcal{V}$ uneingeschränkt.*

Beweis. Sei $\mathcal{V}$ gegeben durch eine Familie Ω von Operationssymbolen ω_i, $i \in I$ mit Stelligkeiten n_i sowie durch eine Menge Γ von Gesetzen. Gegeben seien Algebren $\mathfrak{A}_k = (A_k, \Omega_k) \in \mathcal{V}$, $k \in K$, mit Trägermengen A_k und Familien Ω_k von Operationen $\omega_{i,k} \colon A_k^{n_i} \to A$, $i \in I$. Gesucht ist ein Koprodukt $\coprod_{k\in K} \mathfrak{A}_k$ in $\mathcal{V}$. Zu diesem Zweck werden wir eine Varietät $\mathcal{V}'$ geeignet definieren. Die in $\mathcal{V}'$ über der leeren Menge $\emptyset$ freie Algebra $F_{\mathcal{V}'}$ zusammen mit geeigneten ι_k, $k \in K$, wird sich als das gesuchte Koprodukt deuten lassen. Die neue Varietät $\mathcal{V}'$ entsteht aus $\mathcal{V}$, indem die Familie der ω_i wie auch Γ ergänzt werden. Und zwar verwenden wir alle Elemente der A_k als nullstellige Operationensymbole, genauer: Sei $\Omega_c := \bigcup_{k\in K} A_k \times \{k\}$ (disjunkte Vereinigung der A_k). Für jedes $(a, k) \in \Omega_c$ sei $\omega_{(a,k)}$ ein Operationssymbol mit Stelligkeit 0. Damit sich in den Algebren aus $\mathcal{V}'$ die den neu hinzugefügten nullstelligen Operationen zugeordneten Elemente wie die entsprechenden Elemente der Strukturen $\mathfrak{A}_k$ verhalten, fügen wir zu Γ für alle $k \in K$, $i \in I$ und alle $a_1, \ldots, a_{n_i} \in \mathfrak{A}_k$ das Gesetz (siehe Definition 2.1.8.6)

$$\omega_i(\omega_{(a_1,k)}, \ldots, \omega_{(a_{n_i},k)}) \approx \omega_{(\omega_{i,k}(a_1,\ldots,a_{n_i}),k)}$$

hinzu, das wir mit $\gamma(k, i, a_1, \ldots, a_{n_i})$ bezeichnen. Wir definieren also Γ' als die Vereinigung von Γ und allen $\gamma(k, i, a_1, \ldots, a_{n_i})$. In der Varietät $\mathcal{V}'$ gibt es nach Satz 4.1.3.1 über jeder Menge X eine freie Algebra, insbesondere auch über der leeren Menge $X = \emptyset$. Diese Algebra bezeichnen wir mit $\mathfrak{F}'$, ihre Trägermenge mit F. Außerdem definieren wir für jedes $k \in K$ die Abbildung $\iota_k \colon A_k \to F$ durch $a \mapsto \omega_{(a,k)}^{\mathfrak{F}'}$, wobei $\omega_{(a,k)}^{\mathfrak{F}'}$ die in $\mathfrak{F}'$ dem Operationssymbol $\omega_{(a,k)}$ zugeordnete nullstellige Operation, genauer: das entsprechende Element, bezeichne. Wir behaupten, dass $\mathfrak{F}'$, aufgefasst als Algebra $\mathfrak{F} \in \mathcal{V}$, zusammen mit den ι_k ein Koprodukt der $\mathfrak{A}_k$ in $\mathcal{V}$ ist.
Um das zu beweisen, ist einerseits zu zeigen, dass die Abbildungen $\iota_k : \mathfrak{A}_k \to \mathfrak{F}$ Homomorphismen sind – dies folgt unmittelbar daraus, dass in $\mathfrak{F}'$ die Gesetze $\gamma(k, i, a_1, \ldots, a_{n_i})$

gelten. Andererseits müssen wir von einer beliebigen Algebra $\mathfrak{B} \in \mathcal{V}$ zusammen mit Homomorphismen $j_k\colon \mathfrak{A}_k \to \mathfrak{B}$, $k \in K$, ausgehen und zeigen, dass es einen eindeutigen $\mathcal{V}$-Homomorphismus $\varphi\colon \mathfrak{F} \to \mathfrak{B}$ gibt mit $j_k = \varphi \circ \iota_k$ für alle $k \in K$. Für jedes $k \in K$ und $a \in A_k$ definieren wir auf B die nullstellige Operation $\omega_{(a,k)}^{\mathfrak{B}'} := j_k(a)$ und erhalten eine Algebra $\mathfrak{B}'$. Mit diesen Operationen erfüllt $\mathfrak{B}'$ auch jedes Gesetz $\gamma(k, i, a_1, \ldots, a_{n_i})$, das sich ja vermittels des Homomorphismus j_k von $\mathfrak{A}_k$ auf B überträgt. Da $\mathfrak{F}'$ frei in $\mathcal{V}'$ über der leeren Menge ist, gibt es einen eindeutigen $\mathcal{V}'$-Homomorphismus $\varphi\colon \mathfrak{F}' \to \mathfrak{B}'$. Das bedeutet insbesondere auch $\varphi : \omega_{(a,k)}^{\mathfrak{F}'} \mapsto \omega_{(a,k)}^{\mathfrak{B}'}$ und deshalb $j_k(a) = \varphi \circ \iota_k(a)$ für alle $k \in K$ und $a \in A_k$, also $j_k = \varphi \circ \iota_k$ für alle $k \in K$. Als $\mathcal{V}'$-Homomorphismus ist φ erst recht $\mathcal{V}$-Homomorphismus und hat daher die gewünschten Eigenschaften. Zuletzt haben wir die Eindeutigkeit von φ zu zeigen: $\mathfrak{F}'$ wird als Algebra in $\mathcal{V}'$ von der leeren Menge erzeugt, d. h. als Algebra $\mathfrak{F}$ in $\mathcal{V}$ von den hinzugefügten 0-stelligen Operationen, nach Konstruktion also von der Vereinigung der $\iota_k(A_k)$, $k \in K$. Jeder Homomorphismus ist durch seine Werte auf einem Erzeugendensystem eindeutig bestimmt (Proposition 2.2.1.17), somit insbesondere φ durch die Forderung $j_k = \varphi \circ \iota_k$ für alle $k \in K$. □

Die freie Algebra über einer gewissen Menge kann man mithilfe des Koprodukts aus freien Algebren über kleineren Mengen zusammensetzen.

Proposition 4.2.2.3. *Sei $\mathcal{V}$ eine nichttriviale Varietät. Für $i = 1, 2$ sei $\mathfrak{F}_i \in \mathcal{V}$ frei über (B_i, ι_i), wobei der Einfachheit halber $B_1 \cap B_2 = \emptyset$ sei. Weiters sei $(\mathfrak{F}, j_1, j_2)$ ein Koprodukt von $\mathfrak{F}_1$ und $\mathfrak{F}_2$. Dann gilt*

1. *$(j_1 \circ \iota_1)(B_1) \cap (j_2 \circ \iota_2)(B_2) = \emptyset$.*
2. *Setzt man $B = B_1 \cup B_2$ und $\iota := (j_1 \circ \iota_1) \cup (j_2 \circ \iota_2)$ (also $\iota(b_i) = j_i(\iota_i(b_i))$ für $b_i \in B_i$ und $i = 1, 2$), dann ist $\mathfrak{F}$ frei über (B, ι).*

UE 291 ► Übungsaufgabe 4.2.2.4. (V) Beweisen Sie Proposition 4.2.2.3. **◄ UE 291**

4.2.3. Polynomalgebren

Inhalt in Kurzfassung: Schon bei der Einführung von Polynomringen im klassischen Sinn in Unterabschnitt 3.4.6 haben wir eine universelle Eigenschaft festgestellt (siehe Proposition 3.4.6.16), die nun zum Ausgangspunkt für den viel allgemeineren Begriff der Polynomalgebra über einer beliebigen Algebra einer Varietät wird. Und zwar handelt es sich um die Kombination der beiden wichtigsten Konstruktionen dieses Kapitels, nämlich der freien Algebra und des Koproduktes. Der Beweis, dass auch Polynomalgebren in Varietäten uneingeschränkt existieren, ergibt sich nun mehr oder weniger als Folgerung bereits verfügbarer Ergebnisse.

Wir gehen von der folgenden grundlegenden Eigenschaft von Polynomen $f \in R[X]$ über einem kommutativen Ring R mit 1 in Variablen aus der Variablenmenge X aus: Zu jedem

kommutativen Ring S mit 1, der R als Unterring mit 1 enthält, und jeder Variablenbelegung $j\colon X \to S$ mit Elementen aus S gibt es einen eindeutigen Ringhomomorphismus $\varphi\colon R[X] \to S$, der j fortsetzt. Dieses φ ist der Einsetzungshomomorphismus

$$f(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n} \mapsto \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} s_1^{i_1} \ldots s_n^{i_n}$$

mit $s_i := j(x_i)$ für $x_i \in X$ und $i = 1, \ldots, n$. Nun versuchen wir, den Polynomring $R[X]$ durch allgemeine Konstruktionen zu erhalten, die in beliebigen Varietäten verfügbar sind.
Wir gehen in zwei Schritten vor. Im ersten bilden wir den von der Variablenmenge X frei erzeugten kommutativen Ring $F(X)$ mit 1. Weil die kommutativen Ringe mit 1 eine Varietät bilden, gibt es so ein $F(X)$ (siehe Satz 4.1.3.1). Die bestimmende Eigenschaft von $F(X)$ lautet: Sind irgendein Ring S mit 1 und eine Variablenbelegung $j\colon X \to S$ vorgegeben, so gibt es einen eindeutigen Homomorphismus $\varphi_S\colon F(X) \to S$ mit $\varphi_S(x) = j(x)$ für alle $x \in X$. Nun wollen wir statt $F(X)$ allerdings einen Ring, der überdies R umfasst. Es liegt nahe, das Koprodukt von R und $F(X)$ zu betrachten. Wieder weil die kommutativen Ringe mit 1 eine Varietät bilden, ist die Existenz so eines Koproduktes garantiert (Satz 4.2.2.2).

Definition 4.2.3.1. Sei $\mathcal{C}$ eine konkrete Kategorie, A ein Objekt in $\mathcal{C}$, und X eine Menge (Variablenmenge). Gibt es in $\mathcal{C}$ ein über X freies Objekt $(F(X), \iota)$, so heißt jedes Koprodukt $A \amalg F(X)$ (mit Morphismen $\iota_A\colon A \to A \amalg F(X)$ und $\iota_{F(X)}\colon F(X) \to A \amalg F(X)$) eine *Polynomalgebra* in den *Unbestimmten* oder *Variablen* $x \in X$ über A in $\mathcal{C}$, symbolisch $A[X]$. Die Elemente von $A[X]$ heißen *verallgemeinerte Polynome*. Im Fall endlich vieler Variablen $X = \{x_1, \ldots, x_n\}$ schreiben wir oft $A[x_1, \ldots, x_n]$ für $A[X]$.

Man beachte, dass in dieser Definition nichts über die Existenz von Polynomalgebren ausgesagt wird!
Wie bereits erwähnt ergibt sich aus den Sätzen 4.1.3.1 und 4.2.2.2:

Folgerung 4.2.3.2. *Ist $\mathcal{V}$ eine Varietät, $\mathfrak{A} \in \mathcal{V}$ und X irgendeine Menge, dann gibt es eine Polynomalgebra $\mathfrak{A}[X]$ in den Variablen aus X über $\mathfrak{A}$ in $\mathcal{V}$.*

Meist ist es gewünscht, $\mathfrak{A}$ und $\mathfrak{F}(X)$ als Unteralgebren der Polynomalgebra $\mathfrak{A}[X]$ sowie $\iota_{\mathfrak{A}}\colon \mathfrak{A} \to \mathfrak{A}[X]$ und $\iota_{\mathfrak{F}(X)}\colon \mathfrak{F}(X) \to \mathfrak{A}[X]$ als Inklusionsabbildungen auffassen zu können. Das klappt aber nur, wenn diese Homomorphismen $\iota_{\mathfrak{A}}$ und $\iota_{\mathfrak{F}(X)}$ injektiv sind. Für $\iota_{\mathfrak{A}}$ ist dies stets der Fall:

Proposition 4.2.3.3. *Sei $\mathfrak{A}[X]$ die Polynomalgebra über $\mathfrak{A}$ in der Varietät $\mathcal{V}$ in der Variablenmenge X und $\mathfrak{F}(X)$ die in $\mathcal{V}$ von X frei erzeugte Algebra. Die dem Koprodukt $\mathfrak{A}[X] = \mathfrak{A} \amalg \mathfrak{F}(X)$ zugehörigen Homomorphismen seien mit $\iota_{\mathfrak{A}}\colon \mathfrak{A} \to \mathfrak{A}[X]$ und $\iota_{\mathfrak{F}(X)}\colon \mathfrak{F}(X) \to \mathfrak{A}[X]$ bezeichnet. Dann ist der Homomorphismus $\iota_{\mathfrak{A}}$ injektiv, d. h. eine isomorphe Einbettung von $\mathfrak{A}$ in die Polynomalgebra $\mathfrak{A}[X]$. Folglich darf $\mathfrak{A}$ oBdA als Unteralgebra der Polynomalgebra $\mathfrak{A}[X]$ aufgefasst werden.*

Beweis. Ist $\mathfrak{A}$ die leere Algebra, so ist die Behauptung trivial. Sei daher $a \in A$. Wir betrachten einerseits die Identität $\mathrm{id}\colon \mathfrak{A} \to \mathfrak{A}$, andererseits den die konstante Variablenbelegung $x \mapsto a$ auf die freie Algebra $\mathfrak{F}(X)$ fortsetzenden Homomorphismus $\varphi_a\colon \mathfrak{F}(X) \to \mathfrak{A}$. Nach Definition des Koproduktes gibt es einen Homomorphismus $\varphi\colon \mathfrak{A}[X] \to \mathfrak{A}$ mit $\mathrm{id}_{\mathfrak{A}} = \varphi \circ \iota_{\mathfrak{A}}$. Das ist nur möglich, wenn $\iota_{\mathfrak{A}}$ injektiv ist. □

Mit der Injektivität von $\iota_{\mathfrak{F}(X)}$ in Proposition 4.2.3.3 verhält es sich komplizierter als mit jener von $\iota_{\mathfrak{A}}$. Es ist eine lehrreiche Übung, sich das zu überlegen:

UE 292 ▶ **Übungsaufgabe 4.2.3.4.** (A) Für uns besonders interessant ist die Varietät der kommutativen Ringe mit 1. Zeigen Sie, dass die Einschränkung von $\iota_{\mathfrak{F}(X)}\colon \mathfrak{F}(X) \to \mathfrak{A}[X]$ auf X (gemäß Proposition 4.1.3.4 aufgefasst als Teilmenge von $\mathfrak{F}(X)$) injektiv ist. Folglich darf in diesem Fall X oBdA auch als Teilmenge der Polynomalgebra $\mathfrak{A}[X]$ aufgefasst werden. Beweisen Sie das abstrakt, ohne Bezugnahme auf die konkrete Darstellung von Polynomen über einem kommutativen Ring mit 1. ◀ **UE 292**

Nach Konstruktion ist die Polynomalgebra durch folgende Eigenschaft charakterisiert, die wir im Fall der kommutativen Ringe mit 1 eingangs zur Motivation der allgemeinen Definition genommen haben:

Satz 4.2.3.5. *Sei $\mathcal{V}$ eine nichttriviale Varietät, $\mathfrak{A} \leq \mathfrak{B} \in \mathcal{V}$ und X eine Variablenmenge. Dann gibt es zu jeder Variablenbelegung $j\colon X \to B$ von X mit Elementen aus B einen eindeutigen Homomorphismus $\varphi\colon \mathfrak{A}[X] \to \mathfrak{B}$ mit $\varphi(a) = a$ für alle $a \in \mathfrak{A} \leq \mathfrak{A}[X]$ (gemäß Proposition 4.2.3.3) und $\varphi(x) = j(x)$ für alle $x \in X \subseteq \mathfrak{F}(X)$ (gemäß Proposition 4.1.3.4 für nichttriviales $\mathcal{V}$).*

Beweis. Laut Proposition 4.1.3.4 dürfen wir die Variablenmenge X als Teilmenge der von X in $\mathcal{V}$ frei erzeugten Algebra $\mathfrak{F}(X)$ auffassen. Nach Definition der freien Algebra lässt sich die Variablenbelegung j eindeutig zu einem auf ganz $\mathfrak{F}(X)$ definierten Homomorphismus $\varphi_0\colon \mathfrak{F}(X) \to \mathfrak{B}$ fortsetzen. Nach Definition ist $\mathfrak{A}[X]$ ein Koprodukt $\mathfrak{A} \amalg \mathfrak{F}(X)$. Die diesem Koprodukt zugehörigen Homomorphismen seien $\iota_{\mathfrak{A},\mathfrak{A}[X]}\colon \mathfrak{A} \to \mathfrak{A}[X]$ und $\iota_{\mathfrak{F}(X),\mathfrak{A}[X]}\colon \mathfrak{F}(X) \to \mathfrak{A}(X)$. Außerdem bezeichne $\iota_{\mathfrak{A},\mathfrak{B}}\colon \mathfrak{A} \to \mathfrak{B}$, $a \mapsto a$, die Inklusionsabbildung. Die definierende Eigenschaft des Koproduktes garantiert, dass es einen eindeutigen Homomorphismus $\varphi\colon \mathfrak{A}[X] \to \mathfrak{B}$ gibt mit $\varphi \circ \iota_{\mathfrak{A},\mathfrak{A}[X]} = \iota_{\mathfrak{A},\mathfrak{B}}$ und $\varphi \circ \iota_{\mathfrak{F}(X),\mathfrak{A}[X]} = \varphi_0$. Die erste dieser Beziehungen bedeutet $\varphi(\iota_{\mathfrak{A},\mathfrak{A}[X]}(a)) = \iota_{\mathfrak{A},\mathfrak{B}}(a) = a$ für alle $a \in A$, die erste Behauptung. Aus der zweiten Beziehung folgt analog $\varphi(\iota_{\mathfrak{F}(X),\mathfrak{A}[X]}(x)) = j(x)$ für alle $x \in X \subseteq \mathfrak{F}(X)$. Die Eindeutigkeit von φ folgt in gewohnter Weise, weil φ auf dem Erzeugendensystem $A \cup X$ von $\mathfrak{A}[X]$ vorgegeben ist. □

UE 293 ▶ **Übungsaufgabe 4.2.3.6.** (W) Zeigen Sie, dass Polynomalgebren $\mathfrak{A}[X]$ für gegebenes $\mathfrak{A}$ und X bis auf Äquivalenz in einer geeigneten Kategorie eindeutig bestimmt sind. In Varietäten sind Polynomalgebren bis auf Isomorphie eindeutig bestimmt. ◀ **UE 293**

Für die Varietät der kommutativen Ringe mit Einselement erhält man tatsächlich die klassischen Polynomringe:

UE 294 ► **Übungsaufgabe 4.2.3.7.** (A) Sei $\mathcal{V} = \mathcal{Rng}_1$ die Varietät der kommutativen Ringe mit 1, $R \in \mathcal{Rng}_1$ und X eine Variablenmenge. ◄ **UE 294**

(1) Zeigen Sie: Ist $X = \{x\}$, so lässt sich der Polynomring $R[x]$ im Sinn von Unterabschnitt 3.4.6 auch als Polynomalgebra $R[\{x\}]$ im Sinn von Definition 4.2.3.1 deuten.

(2) Zeigen Sie: Definiert man rekursiv $R[x_1, \ldots, x_{n+1}] := R[x_1, \ldots, x_n][x_{n+1}]$, so lässt sich $R[x_1, \ldots, x_n]$ auch als Polynomalgebra $R[\{x_1, \ldots, x_n\}]$ im Sinn von Definition 4.2.3.1 deuten.

Als Hintergrund sind abstraktere Verträglichkeiten zwischen freien Algebren und Polynomalgebren interessant:

UE 295 ► **Übungsaufgabe 4.2.3.8.** (F) Sei $\mathcal{V}$ eine Varietät und $\mathfrak{A} \in \mathcal{V}$. Zeigen Sie: ◄ **UE 295**

(1) Sind X_1 und X_2 disjunkte Variablenmengen, so gilt $\mathfrak{A}[X_1][X_2] \cong \mathfrak{A}[X_1 \cup X_2]$.

(2) Ist $X = \{x_1, x_2, \ldots\}$ eine abzählbar unendliche Variablenmenge, so ist $\mathfrak{A}[X]$ ein direkter Limes der $\mathfrak{A}[x_1, \ldots, x_n]$, wobei $n \in \mathbb{N}$. Präzisieren Sie diese Aussage und führen Sie den Beweis.

Sei p ein Polynom über der Algebra $\mathfrak{A} \in \mathcal{V}$ in Variablen aus $X = \{x_1, \ldots, x_n\}$, d. h. $p \in \mathfrak{A}[x_1, \ldots, x_n]$. Wir schreiben in dieser Situation auch $p = p(x_1, \ldots, x_n)$. Zu einer Variablenbelegung $j : x_i \mapsto a_i$ gibt es laut Satz 4.2.3.5 ($\mathfrak{B} = \mathfrak{A}$ setzen) genau einen Homomorphismus (*Einsetzungshomomorphismus*) $\varphi_j \colon \mathfrak{A}[x_1, \ldots, x_n] \to \mathfrak{A}$, der j fortsetzt, also $\varphi_j(x_i) = a_i$ für $i = 1, \ldots, n$ erfüllt, und auf $\mathfrak{A}$ die Identität ist. Wir nennen $p(a_1, \ldots, a_n) := \varphi_j(p)$ den *Wert* des Polynoms p an der Stelle $(a_1, \ldots, a_n)$. Die Funktion $A^n \to A$, $(a_1, \ldots, a_n) \mapsto p(a_1, \ldots, a_n)$ heißt die vom Polynom p induzierte *verallgemeinerte Polynomfunktion* und wird meist gleichfalls mit p bezeichnet, obwohl es sich begrifflich um verschiedene Objekte handelt. Der historische Grund: In vielen interessanten Fällen, insbesondere im klassischen Fall von Polynomen über einem unendlichen Körper, induzieren verschiedene Polynome verschiedene Polynomfunktionen. (Denn sind zwei Polynomfunktionen gleich, so ist ihre Differenz die Nullfunktion, die nur vom Nullpolynom dargestellt wird, weil jedes andere Polynom nur endlich viele Nullstellen hat. Also stimmen die Polynome überein.) Aber schon über einem endlichen Körper mit q Elementen stellt nicht nur das Nullpolynom, sondern auch das Polynom $x^q - x$ die Nullfunktion dar (siehe Kapitel 6).

UE 296 ► **Übungsaufgabe 4.2.3.9.** (V) Zeigen Sie: Ist $\mathfrak{A} \in \mathcal{V}$, so bildet die Menge $P(x_1, \ldots, x_n)$ aller Polynomfunktionen von $A^n \to A$ bezüglich der punktweise definierten Funktionen selbst wieder eine Algebra aus $\mathcal{V}$. Dabei ist $P(x_1, \ldots, x_n)$ ein homomorphes Bild der Polynomalgebra $\mathfrak{A}[x_1, \ldots, x_n]$. ◄ **UE 296**
(vgl. die Übungsaufgaben 2.1.8.8 und 2.2.2.11 über Termfunktionen)

UE 297 ► Übungsaufgabe 4.2.3.10. (B) Sei $\mathcal{Ab}$ die Klasse aller abelschen Gruppen. **◄ UE 297**

(1) Beschreiben Sie (möglichst explizit) das Koprodukt einer abelschen Gruppe G mit der von einem Element frei erzeugten abelschen Gruppe, also die Polynomalgebra $G[x]$ (in $\mathcal{Ab}$). (Genauer: Beschreiben Sie die Elemente dieser Algebra, und erklären Sie, was die Gruppenoperation mit zwei solchen Elementen macht.)

(2) Sei X nun eine beliebige Menge von Variablen. Beschreiben Sie die Polynomalgebra $G[X]$.

(3) Beschreiben Sie die von einem beliebigen Element von $G[X]$ induzierte Polynomfunktion.

4.2.4. Der Gruppenring und Monoidring

Inhalt in Kurzfassung: Auch beim Gruppenring werden (so wie beim Koprodukt zweier Algebren) zwei Strukturen in eine einzige „verklebt“, sodass man darin beide ursprünglichen möglichst „frei“ wiederfindet. Allerdings handelt es sich diesmal nicht um Algebren des gleichen Typs, sondern um eine Verschmelzung aus Gruppe und Ring. Als Anwendung beleuchten wir den Polynomring über einem kommutativen Ring mit 1 noch von einer weiteren Seite.

Eine gewisse Ähnlichkeit mit Koprodukten, bei denen zu gegebenen Strukturen eine diese umfassende konstruiert wird, hat auch der Gruppenring. Wie sein Name schon andeutet, liefert seine Konstruktion, ausgehend von einer Gruppe G und einem Ring R, eine Struktur $R(G)$, in die sowohl G als auch R eingebettet werden können. In Hinblick auf Polynomringe über kommutativen Ringen mit 1 wollen wir auch die etwas allgemeineren aber völlig analog definierten Monoidringe betrachten.

Definition 4.2.4.1. Sei R ein Ring mit Einselement $1_R \neq 0_R$ und M ein Monoid. Der *Monoidring* $R(M)$ von R über M trägt die additive Struktur der direkten Summe $\bigoplus_{m\in M} R$. Für ein Element $r = (r_m)_{m\in M} \in R(M)$ schreiben wir auch $\sum_{m\in M} r_m m$, wobei nur für endlich viele $m \in M$ der Koeffizient r_m von 0_R verschieden ist. Mit dieser Notation hat die Addition die Form

$$\sum_m r_m m + \sum_m s_m m = \sum_m (r_m + s_m)m.$$

Die Multiplikation dehnt die Festsetzung $(r_{m_1} m_1)(s_{m_2} m_2) := (r_{m_1} s_{m_2})(m_1 m_2)$ in distributiver Weise aus, also

$$\left(\sum_{m_1} r_{m_1} m_1\right) \cdot \left(\sum_{m_2} s_{m_2} m_2\right) := \sum_m t_m m.$$

Dabei entspricht

$$t_m := \sum_{(m_1,m_2)\in M^2:\ m_1 m_2 = m} r_{m_1} s_{m_2}$$

der *Faltung* bezüglich der Halbgruppenoperation. Zu beachten ist, dass de facto nur endliche Summen auftreten. Ist M sogar eine Gruppe, so heißt $R(M)$ auch *Gruppenring*.

Von Interesse sind folgende Beobachtungen.

Proposition 4.2.4.2. *Sei R ein kommutativer Ring mit 1 und M ein Monoid mit Einselement e_M.*

(1) *Bei der in Definition 4.2.4.1 definierten Struktur $R(M)$ handelt es sich um einen Ring mit Einselement.*

(2) *Die Abbildung $\iota_{R,R(M)}\colon R \to R(M)$, $r \mapsto re_M = \sum_{m\in M} r_m m$ mit $r_{e_M} = r$ und $r_m = 0_R$ für alle $m \in M \setminus \{e_M\}$, ist eine isomorphe Einbettung des Ringes R in $R(M)$.*

(3) *Die Abbildung $\iota_{M,R(M)}\colon M \to R(M)$, $m_0 \mapsto 1_R m_0 = \sum_{m\in M} r_m m$ mit $r_{m_0} = 1_R$ und $r_m = 0_R$ für alle $m \in M \setminus \{m_0\}$, ist eine isomorphe Einbettung von M in die multiplikative Halbgruppe von $R(M)$.*

(4) *Bei festem M induziert jeder Homomorphismus $f\colon R_1 \to R_2$ kommutativer Ringe R_1 und R_2 einen eindeutigen Ringhomomorphismus $\bar{f}\colon R_1(M) \to R_2(M)$ mit $\bar{f} \circ \iota_{R_1,R_1(M)} = \iota_{R_2,R_2(M)} \circ f$.*

(5) *Bei festem R induziert jeder Monoidhomomorphismus $g\colon M_1 \to M_2$ einen eindeutigen Ringhomomorphismus $\hat{g}\colon R(M_1) \to R(M_2)$ mit $\hat{g} \circ \iota_{M_1,R(M_1)} = \iota_{M_2,R(M_2)} \circ g$.*

$$\begin{array}{ccc} R_1 & \xrightarrow{f} & R_2 \\ {\scriptstyle \iota_{R_1,R_1(M)}}\Downarrow & & \Downarrow{\scriptstyle \iota_{R_2,R_2(M)}} \\ R_1(M) & \overset{\bar{f}}{\dashrightarrow} & R_2(M) \end{array} \qquad \begin{array}{ccc} M_1 & \xrightarrow{g} & M_2 \\ {\scriptstyle \iota_{M_1,R(M_1)}}\Downarrow & & \Downarrow{\scriptstyle \iota_{M_2,R(M_2)}} \\ R(M_1) & \overset{\hat{g}}{\dashrightarrow} & R(M_2) \end{array}$$

UE 298 ► Übungsaufgabe 4.2.4.3. (V) Beweisen Sie Proposition 4.2.4.2. **◄ UE 298**

Wir wollen uns zum Abschluss überlegen, dass der Polynomring über einem beliebigen kommutativen Ring R mit 1 und einer beliebigen Variablenmenge X als Monoidring realisiert werden kann. Und zwar nehmen wir als Monoid das additive Monoid $M := \bigoplus_{x\in X} \mathbb{N}$. Ein typisches Element des Monoidrings $R(M)$ hat die Gestalt $\sum_{m\in M} r_m m$, wobei $r_m \neq 0$ nur für endlich viele m gilt. Ein Element $m \in M$ ist von der Form $m = (n_x)_{x\in X}$, $n_x \in \mathbb{N}$, wieder mit $n_x \neq 0$ nur für endlich viele $x \in X$, etwa $x_1, \ldots, x_k$. Dann schreiben wir das Element m auch als *Monom* $x_1^{n_{x_1}} x_2^{n_{x_2}} \ldots x_k^{n_{x_k}}$ an, wobei es auf die Reihenfolge der Faktoren nicht ankommt. Somit ist jedes $\sum_{m\in M} r_m m \in R(M)$ auch als Polynom über R in den Variablen $x \in X$ lesbar. Mit einiger Arbeit aber ohne grundsätzliche Schwierigkeiten überzeugt man sich davon, dass sich diese formale Ähnlichkeit auch inhaltlich rechtfertigen lässt:

Satz 4.2.4.4. *Sei R ein kommutativer Ring mit 1 und X eine Menge von Variablen. Dann lässt sich der Monoidring $R(M)$ von R über dem Monoid $M := \bigoplus_{x\in X} \mathbb{N}$ (direkte Summe von $|X|$ Kopien des additiven Monoids $\mathbb{N}$) als Polynomalgebra (= Polynomring) $R[X]$ im Sinne von Definition 4.2.3.1 über R in der Variablenmenge X auffassen.*

UE 299 ► Übungsaufgabe 4.2.4.5. (V) Beweisen Sie Satz 4.2.4.4. **◄ UE 299**

5. Teilbarkeit

Die Frage nach Teilbarkeit stellt sich, weil die Multiplikation in Ringen wie $\mathbb{Z}$ nicht uneingeschränkt zur Division umkehrbar ist. Für den Großteil dieses Kapitels orientieren wir uns an der Teilbarkeitslehre in den natürlichen bzw. ganzen Zahlen, insbesondere am Fundamentalsatz der Arithmetik von der eindeutigen Primfaktorzerlegung (Satz 3.1.3.2). Unsere Untersuchungen sind von der Frage geleitet, in welchen Strukturen ähnliche Begriffsbildungen und Resultate möglich sind. Beginnend mit Halbgruppen werden wir in Abschnitt 5.1 Integritätsbereiche und in Abschnitt 5.2 noch speziellere Klassen betrachten: faktorielle, Hauptideal- und Euklidische Ringe. Abschnitt 5.3 enthält schließlich Anwendungen und Ergänzungen.

5.1. Elementare Teilbarkeitslehre

Wir beginnen in 5.1.1 mit einer Rekapitulation der eindeutigen Primfaktorzerlegung in $\mathbb{N}$. Dabei fällt auf, dass Teilbarkeit alleine über die multiplikative Struktur definiert ist. Um klarer zu sehen, worauf es ankommt, stellen wir zunächst einfache Beobachtungen an, die sich auf kommutative Monoide ohne zusätzliche Struktur beziehen (5.1.2). Bald jedoch (5.1.3) wird sich unser Interesse der multiplikativen Halbgruppe von Ringen und vor allem Integritätsbereichen zuwenden. Für das bessere Verständnis der Problemlage entscheidend sind ein einfacher Zusammenhang zwischen Teilbarkeit von Elementen und den erzeugten Hauptidealen sowie zwischen primen und irreduziblen Elementen (5.1.4).

5.1.1. Der Fundamentalsatz der Zahlentheorie als Paradigma

Inhalt in Kurzfassung: Erste Überlegungen zur Frage, was bei einer eventuellen Verallgemeinerung des Satzes von der eindeutigen Primfaktorzerlegung in $\mathbb{N}$ auf allgemeinere Situationen zu beachten ist.

Wie wir schon in Unterabschnitt 3.1.3 gesehen haben, eröffnet der Satz von der eindeutigen Primfaktorzerlegung in den natürlichen Zahlen einen äußerst klaren Blick auf die multiplikative Struktur. Und zwar lässt sich aufgrund dieses Satzes das multiplikative Monoid von $\mathbb{N}^+$ als mit der Menge $\mathbb{P}$ der Primzahlen indizierte unendliche direkte Summe von Kopien des additiven Monoids auf $\mathbb{N}$ interpretieren, also als freies abelsches Monoid über der (abzählbar unendlichen) freien Erzeugendenmenge $\mathbb{P}$. Daraus lässt sich weiters ablesen, dass es ggT (größte gemeinsame Teiler) und kgV (kleinste gemeinsame Vielfache) nicht nur für je zwei Zahlen gibt, sondern sogar für beliebige Teilmengen von $\mathbb{N}$ (inklusive 0). Es liegt also ein vollständiger Verband vor, der überdies distributiv ist. Unser Ziel ist es, ähnliche Einsichten in die Struktur einer möglichst großen Klasse von algebraischen Strukturen zu bekommen.

Schon angesichts der Erweiterung von $\mathbb{N}$ auf $\mathbb{Z}$ stößt man auf eine Schwierigkeit. Weil für alle $a \in \mathbb{Z}$ sowohl $a|-a$ als auch $-a|a$ gilt, lässt sich die Antisymmetrie der Teilerrelation nicht aufrecht erhalten. Es zeigt sich, dass so wie in $\mathbb{Z}$ auch in allgemeinerem Kontext diese Schwierigkeit leicht ausgeräumt werden kann, indem man zur von der Quasiordnung induzierten Halbordnung übergeht (siehe Definition 2.1.1.14 und die im nächsten Unterabschnitt folgende Definition 5.1.2.3).
Es fällt auf, dass die Teilbarkeitsrelation in $\mathbb{N}$ nur von der multiplikativen Struktur bestimmt ist. Es liegt also auf der Hand, mit Halbgruppen oder sogar beliebigen Algebren vom Typ (2) zu beginnen und zu studieren, welche zusätzlichen Eigenschaften der natürlichen Zahlen entscheidend sind, um die Begriffsbildungen und Ergebnisse von dort auf allgemeinere Strukturen übertragen zu können. Wenig überraschend spielen sowohl Assoziativität, Einselement als auch Kommutativität eine wichtige Rolle, aber auch Kürzbarkeit. Abgesehen von der Sonderrolle der 0 sind all diese Bedingungen in der multiplikativen Halbgruppe eines Integritätsbereichs erfüllt. Tatsächlich erweist sich die Klasse der Integritätsbereiche als geeignet, um eine elementare Teilbarkeitslehre sinnvoll zu formulieren. Will man auch Analoga zur Eindeutigkeit der Primzahlzerlegung beweisen (gilt eine solche, so spricht man von einem faktoriellen Ring), muss man allerdings speziellere Bedingungen voraussetzen, was Abschnitt 5.2 vorbehalten sein wird.

5.1.2. Teilbarkeit als Quasiordnung auf kommutativen Monoiden

Inhalt in Kurzfassung: Der Begriff der Teilbarkeit wird von $\mathbb{N}$ auf kommutative Monoide verallgemeinert. Dabei erhält man im Allgemeinen zwar keine Halbordnung, immerhin aber eine Quasiordnung. Die zugehörige Äquivalenzrelation (im Sinne von Definition 2.1.1.14) nennt man Assoziiertheit.

Will man lediglich die Definition von Teilbarkeit vom System $\mathbb{N}$ der natürlichen Zahlen auf möglichst allgemeine Strukturen verallgemeinern, so reicht dafür eine binäre Operation $\circ$ auf irgendeiner Trägermenge.

Definition 5.1.2.1. Sei $\mathfrak{G} = (G, \cdot)$ eine Algebra vom Typ (2). Sind $a, b \in G$, dann heißt a ein *Teiler* von b, b durch a *teilbar* und b ein *Vielfaches* von a, wenn es ein $c \in G$ gibt mit $b = ac := a \cdot c$. In diesem Fall sagen wir auch a *teilt* b, symbolisch: $a|b$. Liegt ein Ring vor, so beziehen wir uns in Teilbarkeitsfragen stets auf die binäre Operation der multiplikativen Halbgruppe des Ringes.

Man könnte Teilbarkeit genauso durch die Gleichung $b = ca$ definieren statt durch $b = ac$ und z. B. zwischen Links- bzw. Rechtsteilbarkeit unterscheiden. Sehr bald werden wir uns aber auf den kommutativen Fall konzentrieren, für den dies hinfällig ist.

Proposition 5.1.2.2. *Für die Teilbarkeitsrelation $|$ auf einer Algebra $\mathfrak{G} = (G, \cdot)$ vom Typ (2) gilt:*

(1) *Gibt es in $\mathfrak{G}$ ein neutrales Element 1_G bezüglich $\cdot$, so ist $|$ reflexiv. In diesem Fall ist 1_G ein kleinstes Element bezüglich $|$, d. h. $1_G|a$ für alle $a \in G$.*

(2) *Ist $\cdot$ assoziativ, so ist $|$ transitiv.*

(3) *Ist $\mathfrak{G}$ ein Monoid, so ist $|$ eine Quasiordnung.*

(4) *Gibt es ein absorbierendes Element $0_G \in G$ (das ist ein Element mit $0_G a = a 0_G = 0_G$ für alle $a \in G$), so ist 0_G ein größtes Element bezüglich $|$, d. h. $a|0_G$ für alle $a \in G$.*

Beweis. Die erste Behauptung liest man aus $a = 1_G a$ ab. Für die zweite schließt man von $a|b$ und $b|c$ auf die beiden Gleichungen $b = at_1$ und $c = bt_2$ mit geeigneten $t_1, t_2 \in G$. Setzt man die erste in die zweite ein, erhält man mithilfe der Assoziativität $c = (at_1)t_2 = a(t_1 t_2)$, also $a|c$. Die dritte Behauptung fasst lediglich die ersten beiden zusammen, und die vierte ist aus $0_G = a0_G$ für alle $a \in G$ ersichtlich. □

Wir wollen ab nun voraussetzen, dass wir es mit einem Monoid $\mathfrak{M} = (M, \cdot, 1_M)$ und somit mit einer Quasiordnung $|$ auf $\mathfrak{M}$ zu tun haben.

Definition 5.1.2.3. Laut Satz 2.1.1.12 induziert $|$ als Quasiordnung eine Äquivalenzrelation $\sim$, die durch

$$a \sim b :\Leftrightarrow a|b \text{ und } b|a$$

definiert ist. Elemente mit $a \sim b$ heißen *assoziiert*.
Gleichfalls nach Satz 2.1.1.12 sind die Relationen $|$ und $\sim$ miteinander verträglich in dem Sinn, dass die Definition

$$[a]_\sim \mid [b]_\sim :\Leftrightarrow a|b$$

der Teilbarkeit zwischen Äquivalenzklassen nicht von der speziellen Wahl der Vertreter a, b abhängt und somit diese Relation $|$ auf der Menge $M/_\sim$ der Äquivalenzklassen sogar eine Halbordnungsrelation ist mit kleinstem Element $[1_M]_\sim$.

Im kommutativen Fall ist nicht nur die Teilerrelation, sondern auch die binäre Operation auf $\mathfrak{M}$ mit der Assoziiertheitsrelation $\sim$ verträglich:

Satz 5.1.2.4. *Sei $\mathfrak{M} = (M, \cdot, 1_M)$ ein kommutatives Monoid. Dann gilt:*

(1) *Die Assoziiertheitsrelation $\sim$ auf $\mathfrak{M}$ ist eine Kongruenzrelation.*

(2) *Die Teilbarkeitsrelation im Faktormonoid $\mathfrak{M}/_\sim$ erhält man auch als die von der Teilbarkeitsquasiordnung auf $\mathfrak{M}$ auf der Faktormenge bezüglich $\sim$ induzierte Halbordnung. Diese Halbordnung nennen wir auch die* Teilbarkeitshalbordnung *von $\mathfrak{M}$* modulo Assoziiertheit.

(3) *Die Menge*

$$E = E(\mathfrak{M}) := \mathfrak{M}^* := [1_M]_\sim = \{m \in M \mid m \sim 1_M\} = \{m \in M \mid m|1_M\}$$

ist eine Gruppe, genannt die Einheitengruppe *von $\mathfrak{M}$, deren Elemente (= Teiler von 1_M)* Einheiten *heißen.*

(4) *Allgemein gilt $aE \subseteq [a]_\sim$ für alle $a \in M$. Ist das Monoid $\mathfrak{M}$ kürzbar*[1]*, dann gilt sogar $[a]_\sim = aE$.*

[1] Zur Erinnerung: Eine binäre Operation heißt kürzbar, wenn aus $ax = bx$ oder $xa = xb$ stets $a = b$ folgt.

Beweis.

(1) Nach Satz 2.1.1.12 ist $\sim$ eine Äquivalenzrelation. Es genügt daher, die Verträglichkeit mit der binären Operation nachzuweisen. Um das zu zeigen, sei $a_1 \sim a_2$ und $b_1 \sim b_2$. Insbesondere bedeutet dies $a_1|a_2$ und $b_1|b_2$. Folglich gibt es $x, y \in M$ mit $a_2 = a_1x$ und $b_2 = b_1y$. Aufgrund von Assoziativität und Kommutativität folgt daraus $a_2b_2 = a_1xb_1y = (a_1b_1)(xy)$, also $a_1b_1|a_2b_2$. Symmetrisch zeigt man $a_2b_2|a_1b_1$; insgesamt gilt also $a_1b_1 \sim a_2b_2$.

(2) Folgt direkt aus den Konstruktionen.

(3) Das war Inhalt von Proposition 3.1.1.3.

(4) Wenn $a' \in aE$ ist, dann gibt es eine Einheit $e \in E = E(\mathfrak{M})$ mit $a' = ae$. Weil $\sim$ eine Kongruenz ist, können wir wegen $e \sim 1$ auf $a' = ae \sim a1 = a$ schließen, also $a' \in [a]_\sim$.
Sei umgekehrt $a' \in [a]_\sim$ beliebig. Nach Definition von $\sim$ gibt es $x, y \in M$ mit $a' = ax$ und $a = a'y$. Daraus erhalten wir $a = a'y = (ax)y = a(xy)$, also $a1 = a(xy)$. Aus der Kürzbarkeit folgt $1 = xy$. Folglich sind $x, y \in E$ Einheiten und $a' = ay \in aE$. Damit ist auch die Inklusion $[a]_\sim \subseteq aE$ gezeigt. □

UE 300 ► **Übungsaufgabe 5.1.2.5.** (B) Geben Sie ein kommutatives (notwendig nicht kürzbares) Monoid an, in dem die Gleichheit aus der vierten Aussage von Satz 5.1.2.4 nicht gilt. ◄ **UE 300**

5.1.3. Teilbarkeit in Integritätsbereichen

Inhalt in Kurzfassung: Von besonderem Interesse ist Teilbarkeit bezüglich des multiplikativen Monoids in Integritätsbereichen. Zusätzliche Aspekte kommen ins Spiel, weil es in diesem Kontext mit der Addition ja auch noch eine zweite binäre Operation gibt, die durch das Distributivgesetz mit der Multiplikation verbunden ist. Als interessante Beispiele kommen quadratische Zahlringe zur Sprache, das sind Unterringe der komplexen Zahlen, die von $\mathbb{Z}$ und der Quadratwurzel einer quadratfreien ganzen Zahl erzeugt werden.

Das kommutative Monoid, dessen Teilbarkeitshalbordnung uns besonders interessiert, ist die multiplikative Halbgruppe eines kommutativen Ringes mit 1, für den wir in üblicher Weise $(R, +, 0, -, \cdot, 1)$ (und meist nur R) schreiben. Sei $H := R/_\sim$ und $(H, |)$ die Teilbarkeitshalbordnung auf R. Hat $A \subseteq H$ ein Supremum $v \in H$, so heißt v das *kleinste gemeinsame Vielfache* der Elemente aus A, abgekürzt $\mathrm{kgV}(A)$; analog heißt das Infimum von A (sofern vorhanden) *größter gemeinsamer Teiler* der Elemente von A, abgekürzt $\mathrm{ggT}(A)$. Die entsprechenden Sprechweisen verwendet man auch für die Elemente der Assoziiertenklassen $a \in A$. Genauer: Das Ringelement s heißt *ein* kgV der Ringelemente r_i, $i \in I$, wenn $[s]_\sim = \mathrm{kgV}(A)$ in H mit $A = \{[r_i]_\sim \mid i \in I\}$; analog für ggT. Man beachte, dass mit s auch jedes $s' \sim s$ ein kgV bzw. ein ggT der r_i oder auch von zu den r_i assoziierten $r_i' \sim r_i$ ist.

In ähnlicher Weise werden wir auch andere Begriffe, die mit der Bildung von Assoziierten verträglich sind, von H auf R übertragen oder umgekehrt, ohne dies nochmals ausführlich zu diskutieren. Weitere Beispiele dieser Art (bei irreduziblen Elementen auf Definition 5.1.4.5 vorausgreifend):

Definition 5.1.3.1. Ein *unechter Teiler* von $r \in R$ ist ein solcher, der zu r assoziiert ist. Jeder andere Teiler heißt ein *echter Teiler*. Ein *trivialer Teiler* von r ist ein solcher, der bis auf Assoziiertheit mit 1 oder r übereinstimmt. Ein Teiler, der kein trivialer Teiler ist, heißt ein *nichttrivialer Teiler* von r. Ein Element $r \in R$ heißt *irreduzibel*, wenn es bezüglich Teilbarkeit oberer Nachbar von $1 \in R$ ist, was eigentlich bedeutet: wenn $[r]_\sim$ in H ein oberer Nachbar des (in H kleinsten) Elements $[1]_\sim = E(R)$ ist.

Diese Diskussion wird obsolet, wenn es eine Teilmenge $T \subseteq R$ gibt, die aus jeder Assoziiertenklasse genau einen Vertreter enthält und außerdem ein multiplikatives Untermonoid des Ringes R bildet. So ein T wollen wir eine *Transversale* nennen. Die Elemente von T nennt man oft auch *normiert*. Die wichtigsten Beispiele: $\mathbb{N}$ ist eine Transversale im Ring $\mathbb{Z}$. Im Polynomring $K[x]$ bilden die Polynome mit höchstem Koeffizienten 1 (die sogenannten *monischen* oder *normierten*) zusammen mit dem Nullpolynom eine Transversale.
Mit $E(R)$ oder auch R^* bezeichnen wir die Einheitengruppe des multiplikativen Monoids $(R, \cdot, 1)$. Tatsächlich sind alle Voraussetzungen von Satz 5.1.2.4 erfüllt, überdies gibt es ein absorbierendes Element, nämlich $0 \in R$. Deshalb gelten Teilbarkeitsregeln in Monoiden auch für Elemente a, b, c eines kommutativen Rings R mit 1:

- $a|0$
- $1|a$
- $a|a$
- $a|b$ und $b|c \Rightarrow a|c$
- $a|b \Rightarrow a|bc$
- $a|b$ und $c|d \Rightarrow ac|bd$
- für $c = d$ daher $a|b \Rightarrow ac|bc$ und für kürzbares c sogar $a|b \Leftrightarrow ac|bc$ (man beachte, dass im Fall eines Integritätsbereichs alle $c \neq 0$ kürzbar sind)
- $aE := \{ae : \ e \in E\} \subseteq [a]_\sim$ mit Gleichheit in Integritätsbereichen
- $a|b$ und $a|c \Rightarrow a|b+c$ (weil ja aus $b = xa$ und $c = ya$ sofort $b+c = xa+ya = (x+y)a$ folgt; dies stellt eine Verbindung zur additiven Struktur von R her)

Zur Illustration folgen nun einige Beispiele:

Beispiele 5.1.3.2.

(1) Im Integritätsbereich $(\mathbb{Z}, +, 0, -, \cdot, 1)$ der ganzen Zahlen ist die Einheitengruppe $E(\mathbb{Z})$ gegeben durch $\{-1, 1\}$. Die Assoziiertenklasse $[a]_\sim$ eines $a \in \mathbb{Z}$ ist $\{a, -a\}$.

(2) In einem Körper $(K, +, 0, -, \cdot, 1)$ ist $E(K) = K \setminus \{0\}$. Es gibt nur zwei Assoziiertenklassen, nämlich $[0]_\sim = \{0\}$ und $[1]_\sim = K \setminus \{0\}$.

(3) (vgl. Proposition 3.4.6.6) Im Polynomring $(R[x], +, 0, -, \cdot, 1)$ über einem gegebenen Ring $(R, +, 0, -, \cdot, 1)$ stimmen die Einheiten mit denen von R überein, sofern man die konstanten Polynome mit den Elementen von R identifiziert. Ist R sogar ein Körper, so ist $E(R[x]) = E(R) = R \setminus \{0\}$ und folglich $[p]_\sim = \{rp : \ r \in R, r \neq 0\}$ für $p \in R[x]$.

(4) Sei $D \neq 1$ eine quadratfreie ganze Zahl, also $t^2|D$ für $t \in \mathbb{Z}$ nur, wenn $t \in \{1, -1\}$. Die Menge $\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ bildet, wie man unschwer nachweist, einen Unterring von $\mathbb{C}$, einen sogenannten *quadratischen Zahlring*. Ein nützliches Instrument bei der Analyse quadratischer Zahlringe ist die sogenannte *Normfunktion* $N\colon \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$, $N(a + b\sqrt{D}) := (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2D$, weil sie als multiplikativer Homomorphismus (es gilt $N(xy) = N(x)N(y)$) die Möglichkeit eröffnet, Teilbarkeitsfragen in den sehr gut verstandenen Ring $\mathbb{Z}$ der ganzen Zahlen zu übertragen.

UE 301 ► **Übungsaufgabe 5.1.3.3.** (B) Sei D eine quadratfreie ganze Zahl und $R = \mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$. ◄ **UE 301**

(1) Man bestimme für $D < 0$ die Einheiten in R.

(2) Man zeige, dass für $D = 2$ unendlich viele verschiedene Einheiten in $R = \mathbb{Z}[\sqrt{D}] \leq \mathbb{R}$ existieren.

Hinweis: Übersetzen Sie die Eigenschaft „$a + b\sqrt{D}$ ist eine Einheit“ in eine Eigenschaft von $N(a + b\sqrt{D})$.

5.1.4. Teilbarkeit und Hauptideale – prime und irreduzible Elemente

Inhalt in Kurzfassung: Die Teilbarkeit von Elementen übersetzt sich in die umgekehrte Inklusionsbeziehung der erzeugten Hauptideale, was besonders in Hauptidealringen (das sind Integritätsbereiche, in denen jedes Ideal ein Hauptideal ist) wirksame Möglichkeiten der Strukturanalyse eröffnet. Eine wichtige Rolle spielen dabei irreduzible und Primelemente. In $\mathbb{Z}$ sind beide Begriffe äquivalent, in beliebigen Integritätsbereichen ist jedes Primelement irreduzibel, nicht jedoch umgekehrt.

Wir wollen nun den engen Zusammenhang zwischen der Teilbarkeit von Elementen und den Hauptidealen $(a) = Ra = \{ra \mid r \in R\}$, $a \in R$, in einem kommutativen Ring R mit Einselement studieren. Teilbarkeit und Assoziiertheit beziehen sich dabei natürlich auf das multiplikative Monoid von R.

Proposition 5.1.4.1. *Für zwei Elemente $a, b \in R$ gilt:*

(1) *$a|b$ genau dann, wenn $(b) \subseteq (a)$.*

(2) *$a \sim b$ genau dann, wenn $(b) = (a)$.*

(3) *$(a) = R$ genau dann, wenn a eine Einheit ist.*

Beweis. Aus $a|b$ folgt $b = ra$ mit $r \in R$, also $b \in (a)$ und $(b) \subseteq ((a)) = (a)$. Umgekehrt folgt aus $(b) \subseteq (a)$ insbesondere $b \in (a)$, wegen Proposition 3.4.1.7 also $b = ra$ mit einem

$r \in R$, folglich $a|b$. Damit ist die erste Äquivalenz bewiesen. Die zweite Äquivalenz folgt daraus unmittelbar und somit, indem man $R = (1_R)$ beachtet, auch die dritte. □

Teilbarkeit zweier Elemente lässt sich also durch die Obermengenbeziehung der von diesen Elementen erzeugten Hauptideale beschreiben, Assoziiertheit der Elemente durch die Gleichheit der von ihnen erzeugten Hauptideale. Auch die Frage, wann ein Hauptideal ein Primideal ist, lässt sich in eine Eigenschaft eines beliebigen erzeugenden Elementes übersetzen.

Proposition 5.1.4.2. *Für ein Element $p \in R$ sind die folgenden beiden Aussagen äquivalent:*

(1) *Das von p erzeugte Ideal $(p) = \{rp \mid r \in R\}$ ist ein Primideal.*

(2) *Das Element p ist keine Einheit, und für alle $a, b \in R$ gilt die Implikation*

$$p|ab \quad \textit{impliziert} \quad p|a \textit{ oder } p|b.$$

Beweis. Für die Implikation (1) ⇒ (2) sei (p) ein Primideal. Nach Definition von Primidealen folgt daraus $(p) \neq R$, weshalb p nach der dritten Aussage in Proposition 5.1.4.1 keine Einheit sein kann. Gilt nun $p|ab$, so bedeutet das nach der ersten Aussage in Proposition 5.1.4.1 genau $ab \in (p)$. Nochmals nach Definition von Primidealen heißt das $a \in (p)$ oder $b \in (p)$, d. h. $p|a$ oder $p|b$. Alle Schlüsse lassen sich auch umkehren, weshalb auch die Implikation (2) ⇒ (1) gilt. □

Definition 5.1.4.3. Gilt eine der beiden Aussagen in Proposition 5.1.4.2 (und damit auch die andere) und ist $p \neq 0_R$, so nennt man p ein *Primelement* in R.

Dass im Ring $R = \mathbb{Z}$ die Primelemente genau die Primzahlen sind, folgt leicht aus Satz 3.1.3.2 von der eindeutigen Primfaktorzerlegung:

UE 302 ► **Übungsaufgabe 5.1.4.4.** (F) Beweisen Sie, dass $p \in \mathbb{N}$ genau dann eine Primzahl ist, wenn $p \neq 0$ und im Ring $\mathbb{Z}$ ein Primelement im Sinne von Definition 5.1.4.3 ist. ◄ **UE 302**

Wir haben bereits gesehen, dass alle Ideale $I \lhd \mathbb{Z}$ mit $I \neq \{0\}$ von der Gestalt $I = (m)$ mit $m = 1, 2, \ldots$ sind. Die Faktorringe $\mathbb{Z}/(m)$ sind die Restklassenringe $\mathbb{Z}_m$. Nach Satz 3.4.2.4 handelt es sich genau dann um Integritätsbereiche, wenn (m) ein Primideal, also $m = p$ eine Primzahl ist. Weil alle $\mathbb{Z}_m$ endlich sind, ist $\mathbb{Z}_p$ nach Satz 3.4.2.1 sogar ein Körper, der sogenannte *Primkörper* mit p Elementen. Wir bezeichnen ihn auch mit $\mathrm{GF}(p)$ als Abkürzung für *Galoisfeld* mit p Elementen.

Es fällt auf, dass die Definition von Primzahlen (über sogenannte Irreduzibilität) eine andere war als die der Primelemente. Der Zusammenhang ergab sich erst durch den Satz von der eindeutigen Primfaktorzerlegung. Die allgemeine Definition von Irreduzibilität lautet wie folgt.

Definition 5.1.4.5. Sei R ein kommutativer Ring mit Einselement und $p \in R$ keine Einheit. Dann heißt p *irreduzibel*, wenn p in der Teilbarkeitshalbordnung oberer Nachbar von 1 ist. Explizit bedeutet das: In jeder Darstellung $p = ab$ mit $a, b \in R$ ist einer der Faktoren a oder b eine Einheit.

Enthält R wenigstens zwei verschiedene Elemente $0_R \neq 1_R$, so ist 0 keine Einheit, und man kann $a := 0$ und $b := 0$ setzen, um zu sehen, dass $p := 0$ nicht irreduzibel ist.

UE 303 ▶ **Übungsaufgabe 5.1.4.6.** (F) Sei R ein Integritätsbereich und seien $q, r, s \in R \setminus \{0\}$ mit $q = rs$. Zeigen Sie: Bei r handelt es sich genau dann um eine Einheit, wenn $q \sim s$. Schließen Sie daraus, dass für jedes $p \in R \setminus \{0\}$ die folgenden Bedingungen äquivalent sind: ◀ **UE 303**

(1.) Für alle $a, b \in R : (p = ab \;\Rightarrow\; a \sim 1 \;\vee\; b \sim 1)$.

(1'.) Für alle $a, b \in R : (p = ab \;\Rightarrow\; a|1 \;\vee\; b|1)$.

(2.) Für alle $a, b \in R : (p = ab \;\Rightarrow\; a \sim p \;\vee\; b \sim p)$.

(2'.) Für alle $a, b \in R : (p = ab \;\Rightarrow\; p|a \;\vee\; p|b)$.

(3.) Für alle $a, b \in R : (p = ab \;\Rightarrow\; a$ trivialer Teiler $\vee\; b$ trivialer Teiler$)$.

UE 304 ▶ **Übungsaufgabe 5.1.4.7.** (F) Man bestimme im Ring $\mathbb{Z}_2[x]$ alle irreduziblen Polynome bis zum Grad 3. (Der Aufwand, der mit den an dieser Stelle verfügbaren Mitteln erforderlich ist, wird sich später mit etwas Theorie, die noch kommen wird, deutlich reduzieren lassen; siehe Übungsaufgabe 5.3.3.4.) ◀ **UE 304**

In Ringen mit Nullteilern lässt sich über die Beziehung zwischen Primelementen und irreduziblen Elementen wenig sagen. So ist beispielsweise in $\mathbb{Z}_6$ das Element 2 (Kurzschreibweise für $2 + 6\mathbb{Z}$) wegen $2 = 2 \cdot 4$ nicht irreduzibel jedoch prim: Aus $2|ab$ mit $a, b \in \mathbb{Z}_6$ folgt $ab \in \{0, 2, 4\}$. Weil jedes Produkt, das aus den übrigen Elementen $1, 3, 5$ gebildet werden kann, ungerade ist, muss wenigstens einer der Faktoren a oder b selbst in $\{0, 2, 4\}$ liegen, also durch 2 teilbar sein. Also ist 2 tatsächlich prim in $\mathbb{Z}_6$.
In Integritätsbereichen ist das jedoch unmöglich:

Proposition 5.1.4.8. *Jedes Primelement $p \in R$ in einem Integritätsbereich R ist irreduzibel.*

Beweis. Gilt $p = ab$, insbesondere $p|ab$, so folgt nach Definition des Primelements $p|a$ oder $p|b$. OBdA nehmen wir $p|a$ an, also $a = pr$ mit $r \in R$. Folglich ist $p = ab = prb$. Kürzen von p liefert $rb = 1_R$. Somit ist b eine Einheit, p also irreduzibel. □

Wie man am folgenden Beispiel sieht, gilt, anders als zum Beispiel im Ring $R = \mathbb{Z}$, die Umkehrung nicht allgemein.

UE 305 ▶ **Übungsaufgabe 5.1.4.9.** (B) Sei $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$. ◀ **UE 305**

(1) Zeigen Sie, dass die Elemente 2 und 3 in R irreduzibel aber nicht prim sind.
(2) Finden Sie eine Primzahl $p \in \mathbb{Z}$, die im Ring $\mathbb{Z}[\sqrt{-5}]$ nicht irreduzibel ist.

Als Konsequenz dieser Übungsaufgabe werden wir den Ring $\mathbb{Z}[\sqrt{-5}]$ später auch als Beispiel eines nicht faktoriellen Ringes bemühen.

5.2. Faktorielle, Hauptideal- und Euklidische Ringe

Von nun an beschränken wir unsere Untersuchungen auf Integritätsbereiche. Unter ihnen sind die *faktoriellen Ringe* definitionsgemäß genau jene, für die ein Analogon zum Fundamentalsatz der Zahlentheorie gilt (5.2.1). Sie lassen sich aber auch durch andere interessante Eigenschaften charakterisieren. Integritätsbereiche, in denen alle Ideale Hauptideale sind – sogenannte *Hauptidealringe* (5.2.2); $\mathbb{Z}$ und der Polynomring $K[x]$ über einem beliebigen Körper K sind die prominentesten Beispiele – sind stets faktorielle Ringe. Dabei haben $\mathbb{Z}$ und $K[x]$ sogar eine noch stärkere Eigenschaft, nämlich Division mit Rest zu ermöglichen, was sie zu *Euklidischen Ringen* macht (5.2.3).
In faktoriellen Ringen gibt es stets kgV und ggT beliebiger Teilmengen. In Hauptidealringen lässt sich jeder ggT sogar als Linearkombination darstellen; in Euklidischen Ringen gibt es, noch stärker, einen Algorithmus, um so eine Darstellung zu erhalten.

5.2.1. Faktorielle Ringe

Inhalt in Kurzfassung: Faktorielle Ringe sind so definiert, dass für sie ein Analogon des Satzes von der eindeutigen Primfaktorzerlegung gilt. Präziser lässt sich diese Eigenschaft durch mehrere äquivalente Bedingungen charakterisieren, die ungenau (modulo Assoziiertheit und Reihenfolge von Faktoren und bei Vernachlässigung der 0) durch folgende Schlagworte angedeutet seien: Existenz und Eindeutigkeit von Faktorisierungen in irreduzible Elemente; Existenz von Faktorisierungen in Primelemente; irreduzible Elemente sind prim plus Teilerkettenbedingung (d. h., es gibt keine unendlichen echt absteigenden Teilerketten); das multiplikative Monoid ist frei. Der Hauptteil dieses Unterabschnitts ist dem Beweis der Äquivalenz gewidmet. Ordnungstheoretisch gelten, wenig überraschend, für den Teilerverband eines faktoriellen Ringes modulo Assoziiertheit ganz ähnliche Aussagen wie für den Teilerverband von $\mathbb{N}$. Insbesondere gibt es größte gemeinsame Teiler etc.

Ringe mit eindeutiger Primfaktorzerlegung lassen sich auf mehrere Arten charakterisieren. Die Situation in $\mathbb{N}$ bzw. in $\mathbb{Z}$ im Auge führen wir dazu die folgende Terminologie ein.

Definition 5.2.1.1. Sei R ein Integritätsbereich und $\sim$ die Assoziiertheitsrelation auf R. Wir vereinbaren folgende Sprechweisen:
In R gilt *Zerlegbarkeit in irreduzible* bzw. in *Primelemente*, wenn es zu jedem $a \in R$ mit $a \neq 0_R$ endlich viele irreduzible bzw. prime Elemente $p_1, \ldots, p_r \in R$ (nicht notwendiger-

weise paarweise verschieden!) gibt mit

$$a \sim \prod_{i=1}^{r} p_i.$$

(Für $r = 0$ ist das Produkt als 1_R zu lesen.) Das Produkt rechts heißt auch eine *Zerlegung* oder *Faktorisierung* von a.
Man spricht von *eindeutiger* Zerlegbarkeit, wenn je zwei derartige Darstellungen bis auf Assoziiertheit und bis auf die Reihenfolge der Faktoren übereinstimmen, genauer: Für je zwei Darstellungen

$$a \sim \prod_{i=1}^{r} p_i \quad \text{und} \quad a \sim \prod_{j=1}^{s} q_j$$

eines beliebigen $a \in R$ mit irreduziblen bzw. mit Primelementen $p_1, \ldots, p_r, q_1, \ldots, q_s \in R$ (wobei die $p_1, \ldots, p_r$ wieder nicht paarweise verschieden müssen; analog für $q_1, \ldots, q_s$) gilt $r = s$, und es gibt eine Permutation π der Menge $\{1, \ldots, r\}$ mit $q_i \sim p_{\pi(i)}$ für alle $i = 1, \ldots, r$.

Eine erste Beobachtung zeigt:

Proposition 5.2.1.2 (Eindeutigkeit der Primelementzerlegung)**.** *Sei R ein Integritätsbereich, $a \in R \setminus E(R)$, $a \neq 0$, und sei $a = p_1 \cdots p_r = q_1 \cdots q_s$ mit Primelementen $p_1, \ldots, p_r$ und $q_1, \ldots, q_s$. Dann ist $r = s$, und es gibt eine Permutation π von $\{1, \ldots, r\}$ mit $p_i \sim q_{\pi(i)}$, $i = 1, \ldots, r$. Folglich bedeutet für einen Integritätsbereich Zerlegbarkeit in Primelemente bereits die eindeutige Zerlegbarkeit in Primelemente.*

Beweis. Wegen $p_1 | q_1 \cdot \ldots \cdot q_s$ und weil p_1 prim ist, muss $p_1 | q_j$ für ein geeignetes $j =: \pi(1)$ gelten. Als Primelement ist q_j auch irreduzibel (siehe Proposition 5.1.4.8), folglich muss $p_1 \sim q_j$ gelten, d. h. $p_1 = q_j e_1$ mit einer geeigneten Einheit e_1. Nach Kürzen von q_j liefert das

$$e_1 p_2 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdots q_s = q_1 \cdot \ldots \cdot q_{\pi(1)-1} \cdot q_{\pi(1)+1} \cdots q_s.$$

Durch wiederholte Anwendung dieser Überlegung erhält man schließlich die Behauptung. □

Für irreduzible Elemente gilt die entsprechende Aussage nicht.

UE 306 ► **Übungsaufgabe 5.2.1.3.** (W) Verwenden Sie Übungsaufgabe 5.1.4.9, um einen Ring R und ein Element $a \in R$ anzugeben, das in irreduzible Elemente zerlegbar ist, aber nicht *eindeutig* in irreduzible Elemente zerlegbar ist. ◄ **UE 306**

Sehr wohl ist die Zerlegung in irreduzible Elemente eindeutig, wenn in R jedes irreduzible Element auch prim ist (wegen Proposition 5.2.1.2). Wir werden sehen, dass dies die Klasse der faktoriellen Ringe sogar charakterisiert. Zunächst definieren wir diese Klasse so, wie es sich anbietet, wenn man die traditionelle Definition von Primzahlen (nämlich als irreduzible Elemente) und ihre Rolle im Integritätsbereich $\mathbb{Z}$ direkt verallgemeinert.

Definition 5.2.1.4. Ein Integritätsbereich R heißt ein *faktorieller Ring*, wenn in R eindeutige Zerlegbarkeit in irreduzible Elemente gilt. Alternative Bezeichnungen sind auch *Ring mit eindeutiger Primfaktorzerlegung*, *Gaußscher Ring*, manchmal *ZPE-Ring*[2].

Um eine äquivalente Charakterisierung der faktoriellen Ringe zu finden, verwenden wir die folgende Definition:

Definition 5.2.1.5. Ein Integritätsbereich R erfüllt die *Teilerkettenbedingung*, wenn es keine unendlichen absteigenden Folgen echter Teiler gibt, bzw. anders formuliert:
Für alle Folgen $(a_n)_{n\in\mathbb{N}}$ von Elementen in R mit $a_{n+1}|a_n$ für alle $n \in \mathbb{N}$ gibt es ein $n_0 \in \mathbb{N}$, sodass für $n \geq n_0$ stets $a_n \sim a_{n_0}$ gilt.

Die Teilerkettenbedingung ist eng mit dem Begriff der Irreduzibilität verbunden, wie der folgende Satz zeigt.

Proposition 5.2.1.6. *Wenn der Integritätsbereich R die Teilerkettenbedingung erfüllt, dann gilt in R Zerlegbarkeit in irreduzible Elemente.*

Beweis. Wir nehmen an, dass es ein $a_0 \in R \setminus \{0\}$ gibt, welches nicht zu einem endlichen Produkt irreduzibler Elemente assoziiert ist. Dann kann a_0 weder eine Einheit noch ein irreduzibles Element sein, also lässt sich (nach Übungsaufgabe 5.1.4.6) a_0 als Produkt $a_0 = rs$ schreiben, wobei weder $r \sim a_0$ noch $s \sim a_0$ gilt. Einer der beiden Teiler hat keine Zerlegung in irreduzible Elemente (sonst hätte ja auch a_0 eine). Wir haben also einen echten Teiler $a_1|a_0$ gefunden, der keine Zerlegung in irreduzible Elemente hat. Auf diese Weise ist es möglich, induktiv (hier spielt auch das Auswahlaxiom mit, um aus den möglicherweise zahlreichen Zerlegungen $a_i = rs$ jeweils eine auszuwählen) eine unendliche echte Teilerkette $a_0, a_1, a_2, \ldots$ zu konstruieren. □

Der folgende Satz gibt liefert alternative äquivalente Möglichkeiten, faktorielle Ringe zu definieren.

Satz 5.2.1.7. *Sei $(R, +, 0_R, -, \cdot, 1_R)$ ein Integritätsbereich, $\sim$ die Assoziiertheitsrelation auf R und $(M, \cdot, 1_M)$ das Faktormonoid auf $M := (R \setminus \{0\})/_\sim$. Dann sind folgende Bedingungen äquivalent:*

(1) *R ist ein faktorieller Ring (es gilt also eindeutige Zerlegbarkeit in irreduzible Elemente, siehe Definition 5.2.1.4).*

(2) *In R gilt Zerlegbarkeit in Primelemente.*

(3) *In R gelten die folgenden beiden Bedingungen:*

   (a) *Jedes irreduzible Element ist prim.*

   (b) *Teilerkettenbedingung: Es gibt keine unendlich absteigenden Folgen echter Teiler.*

(4) *Das multiplikative Monoid M ist frei in der Klasse der abelschen Monoide, d. h. eine direkte Summe von Kopien des Monoids $(\mathbb{N}, +, 0)$.*

[2] Z für Zerlegung, P für Primfaktor, E für Eindeutigkeit

Ein Vergleich der ersten mit der zweiten Bedingung zeigt, dass der Übergang von irreduziblen zu primen Elementen die Eindeutigkeit der behaupteten Faktorisierung erzwingt, ohne dass sie extra gefordert werden muss. Das spiegelt sich auch in der dritten Bedingung wider, in der (a) im Wesentlichen für die Eindeutigkeit und (b) für die Existenz der Darstellung verantwortlich ist. Die vierte Bedingung, so sehr sie auch völlig andere Begriffe bemüht, entpuppt sich als schlichte Übersetzung der ersten beiden Bedingungen, sobald man erkannt hat, dass die freien Erzeugenden des Monoids M mit den irreduziblen/primen Elementen von R (genauer: mit deren Assoziiertenklassen) korrespondieren. Der Beweis der behaupteten Äquivalenzen ist Gegenstand des nun Folgenden.

Proposition 5.2.1.8. *Erfüllt ein Integritätsbereich R Bedingung (1) aus Satz 5.2.1.7 (eindeutige Zerlegung in irreduzible Elemente), so ist in R jedes irreduzible Element auch Primelement. Folglich gilt Bedingung (2) aus Satz 5.2.1.7 (Zerlegung in Primelemente).*

Beweis. Sei p irreduzibel und $p|ab$. Nach Definition der Teilbarkeit gibt es ein c mit $ab = pc$. Laut Voraussetzung gibt es Zerlegungen $a = p_1 \cdot \ldots \cdot p_l$, $b = q_1 \cdot \ldots \cdot q_m$ und $c = r_1 \cdot \ldots \cdot r_n$ von a, b und c in irreduzible Elemente p_i $(i = 1, \ldots, l)$, q_j $(j = 1, \ldots, m)$, und r_k $(k = 1, \ldots, n)$. Folglich gilt

$$p_1 \cdot \ldots \cdot p_l \cdot q_1 \cdot \ldots \cdot q_m = a \cdot b \sim p \cdot c = p \cdot r_1 \ldots \cdot r_n,$$

wobei ganz links alle Faktoren irreduzibel sind, ebenso ganz rechts. Wegen der vorausgesetzten Eindeutigkeit von Darstellungen als Produkte irreduzibler Elemente (Bedingung (1)) muss der Faktor p bis auf Assoziiertheit auch links vorkommen. Ist $p \sim p_i$ für ein i, so folgt $p|a$; ist $p \sim q_j$ für ein j so folgt $p|b$ – also ist p prim.
Offensichtlich folgt aus dem soeben Gezeigten unmittelbar Bedingung (2) aus Satz 5.2.1.7. □

Proposition 5.2.1.9. *In einem Ring R, der Bedingung (2) aus Satz 5.2.1.7 (Zerlegung in Primelemente) erfüllt, ist jedes irreduzible Element prim.*

Beweis. Sei $r \in R$ irreduzibel. Laut Voraussetzung gibt es Primelemente $p_i \in R$, $i = 1, \ldots, n$, mit $r = p_1 \cdot \ldots \cdot p_n$. Wäre $n > 1$, so läge damit eine Zerlegung von r vor, die der Irreduzibilität widerspricht. Also ist $n = 1$ und $r = p_1$ prim. □

Folgerung 5.2.1.10. *Für einen Integritätsbereich R sind die Bedingungen (1) (eindeutige Zerlegung in irreduzible Elemente) und (2) (Zerlegung in Primelemente) aus Satz 5.2.1.7 äquivalent.*

Beweis. (1) $\Rightarrow$ (2): Siehe Proposition 5.2.1.8.
(2) $\Rightarrow$ (1): Nach den Propositionen 5.1.4.8 und 5.2.1.9 sind in R die primen Elemente genau die irreduziblen. Laut Bedingung (2) hat jedes Element eine Zerlegung in prime und somit in irreduzible Elemente. Diese Zerlegung ist, nochmals wegen der Übereinstimmung von irreduziblen und primen Elementen in R sowie wegen Proposition 5.2.1.2, eindeutig bis auf Assoziiertheit. □

Proposition 5.2.1.11. *In jedem Integritätsbereich R, der Bedingung (1) (eindeutige Zerlegung in irreduzible Elemente) oder (2) (Zerlegung in Primelemente) aus Satz 5.2.1.7 erfüllt, gilt die Teilerkettenbedingung.*

Beweis. Gegeben sei eine Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen von R, sodass für alle $n \in \mathbb{N}$ das Element a_{n+1} ein Teiler von a_n ist. Nach Voraussetzung gibt es zu jedem $a \in R$ mit $a \neq 0$ eine eindeutig bestimmte Zahl $k = k(a)$, sodass sich a als Produkt von k Primelementen schreiben lässt. (Für Einheiten a setzen wir $k(a) = 0$.) Wenn a ein Teiler von b ist, dann gilt $k(a) \leq k(b)$, wenn a echter Teiler von b ist, sogar $k(a) < k(b)$. Die absteigende Folge natürlicher Zahlen $k(a_0) \geq k(a_1) \geq \ldots \geq 0$ muss ab einem gewissen Index n_0 konstant sein. Also sind die Teilbarkeiten $a_{n+1}|a_n$ für alle $n \geq n_0$ keine echten mehr, was zu zeigen war. □

Wir sind nun in der Lage, zu beweisen, dass für einen Integritätsbereich die eindeutige Faktorisierbarkeit in irreduzible Elemente (Bedingung (1) in Satz 5.2.1.7) oder auch Faktorisierbarkeit in Primelemente (Bedingung (2) in Satz 5.2.1.7) äquivalent ist zu Teilerkettenbedingung plus Übereinstimmung von primen und irreduziblen Elementen (Bedingung (3) in Satz 5.2.1.7).

Proposition 5.2.1.12. *Ein Integritätsbereich R erfüllt eine und somit beide der Bedingungen (1) (eindeutige Zerlegung in irreduzible Elemente) und (2) (Zerlegung in Primelemente) aus Satz 5.2.1.7 genau dann, wenn er die Bedingung (3) erfüllt, also explizit:*

(*a*) *Jedes irreduzible Element ist prim.*
(*b*) *Teilerkettenbedingung: Es gibt keine unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen in R, sodass für alle $n \in \mathbb{N}$ das Element a_{n+1} ein echter Teiler von a_n ist.*

Beweis. Nach Proposition 5.2.1.9 und Proposition 5.2.1.11 gelten in jedem Ring, der (1) oder (2) erfüllt, auch die Bedingungen (a) und (b). Umgekehrt folgt aus (b) nach Proposition 5.2.1.6 Zerlegbarkeit in irreduzible Elemente, also nach (a) Zerlegbarkeit in Primelemente.

□

Damit wissen wir, dass die ersten drei Bedingungen in Satz 5.2.1.7 äquivalent sind und können die letzte noch ausständige Äquivalenz beweisen:

Proposition 5.2.1.13. *Die Bedingung (4) aus Satz 5.2.1.7 ist äquivalent zu den Bedingungen (1) bis (3).*

Beweis. Zunächst erinnern wir uns an Übungsaufgabe 4.1.2.9. Daraus geht hervor, dass die freien abelschen Monoide genau diejenigen sind, die isomorph zu einer direkten Summe $\bigoplus_{i\in I}(\mathbb{N}, +, 0)$ von Kopien des abelschen Monoids $(\mathbb{N}, +, 0)$ sind.
Erfülle R die Bedingungen (1) bis (3) in Satz 5.2.1.7. Wir wählen eine Indexmenge I für ein Vertretersystem für alle Assoziiertenklassen irreduzibler (= primer, siehe Bedingung (3)) Elemente p_i in R. Wir definieren eine Zuordnung $\varphi\colon \bigoplus_{i\in I}(\mathbb{N}, +, 0) \to M$ (Notation wie in Satz 5.2.1.7) durch

$$\varphi : (e_i)_{i\in I} \mapsto \left[\prod_{i\in I} p_i^{e_i}\right]_{\sim}.$$

Man beachte, dass diese Abbildung wohldefiniert ist, weil nur endlich viele der natürlichen Zahlen e_i von 0 verschieden sind. Man macht sich unmittelbar klar, dass φ ein Isomorphismus ist – die Injektivität folgt wegen der vorausgesetzten Eindeutigkeit der Zerlegung in irreduzible Elemente, die Surjektivität aus der ebenfalls vorausgesetzten Existenz einer solchen Zerlegung (durch Gruppieren der auftretenden irreduziblen Faktoren; die Exponenten e_i entstehen durch Abzählen, wie oft der irreduzible Faktor p_i vorkommt).
Gelte umgekehrt die Bedingung (4) aus Satz 5.2.1.7, d. h., für eine geeignete Indexmenge I gelte $M \cong S := \bigoplus_{i\in I}(\mathbb{N}, +, 0)$ vermittels eines Isomorphismus $\varphi\colon S \to M$. Für jedes $i_0 \in I$ sei $b_{i_0} := (e_i)_{i\in I}$ das entsprechende kanonische Basiselement mit $e_{i_0} = 1$ und $e_i = 0$ für alle $i \neq i_0$. Dann sind die $\varphi(b_i)$, $i \in I$, bezüglich Teilbarkeit in M obere Nachbarn von 1_R, also Assoziiertenklassen irreduzibler Elemente. Weil φ surjektiv ist, tritt jede Assoziiertenklasse $[a]_\sim$, $a \neq 0$, als $\varphi(s)$ mit einem $s = (e_i)_{i\in I} \in S$ auf. Folglich gilt die Zerlegung $a \sim \prod_{i\in I} \varphi(b_i)^{e_i}$ von a in irreduzible Elemente. Man beachte dabei, dass wieder nur endlich viele e_i von 0 verschieden sind, das Produkt also de facto ein endliches und somit wohldefiniert ist. Wegen der Injektivität von φ ist diese Zerlegung bis auf Assoziiertheit aber auch eindeutig. Damit ist Bedingung (1) aus Satz 5.2.1.7 nachgewiesen. □

In den folgenden Übungsaufgaben wird gezeigt, dass keine der beiden Bedingungen

(a) irreduzibel = prim

(b) Teilerkettenbedingung

ausreicht, um zu zeigen, dass ein Ring faktoriell ist.

UE 307 ► Übungsaufgabe 5.2.1.14. (B) Zeigen Sie, dass in $\mathbb{Z}[\sqrt{-5}]$ die Teilerkettenbedingung gilt. ◄ **UE 307**

UE 308 ► Übungsaufgabe 5.2.1.15. (B) Sei $\mathbb{Q}_{2^\infty}$ die Menge aller Brüche der Form $n/2^k$, wobei n und k beliebige natürliche Zahlen sind. Sei R der Ring aller „Polynome“ mit Koeffizienten in $\mathbb{C}$, wobei aber als Exponenten alle Elemente von $\mathbb{Q}_{2^\infty}$ erlaubt sind.
Formal ist R die Menge aller Funktionen von $\mathbb{Q}_{2^\infty}$ nach $\mathbb{C}$, die aber fast überall den Wert 0 annehmen; die „Länge“ eines solchen Polynom f ist die Kardinalität der Menge $\{q \in \mathbb{Q}_{2^\infty} \mid f(q) \neq 0\}$, also die Anzahl der vorkommenden „Monome“.
Addition wird punktweise definiert, Multiplikation ist Cauchymultiplikation. Monome sind Funktionen der Länge 1; das Monom, das nur an der Stelle q den Wert b annimmt, sonst überall den Wert 0, heißt bx^q; es gilt $(bx^q) \cdot (b'x^{q'}) = (bb')x^{q+q'}$.
Polynome der „Länge“ 2 nennen wir „Binome“.
Zeigen Sie, dass R ein Integritätsbereich ist, und dass sogar Folgendes gilt: ◄ **UE 308**

(∗) Jeder endlich erzeugte Unterring von R ist isomorph zu einem Unterring des Polynomrings $\mathbb{C}[x]$.

(Hinweis: gemeinsamen Nenner suchen.)

UE 309 ► **Übungsaufgabe 5.2.1.16.** (B) Sei R der Ring aus Übungsaufgabe 5.2.1.15. Zeigen Sie, dass die Einheiten von R genau die „konstanten“ Polynome bx^0 sind. ◄ **UE 309**

UE 310 ► **Übungsaufgabe 5.2.1.17.** Sei R der Ring aus Übungsaufgabe 5.2.1.15. Finden sie in R eine unendliche Teilerkette. ◄ **UE 310**

UE 311 ► **Übungsaufgabe 5.2.1.18.** Sei R der Ring aus Übungsaufgabe 5.2.1.15. Zeigen Sie, dass es in R keine irreduziblen Elemente gibt, und schließen Sie, dass in R die Äquivalenz „irreduzibel $\Leftrightarrow$ prim“ gilt.
Hinweis: Verwenden Sie die algebraische Abgeschlossenheit von $\mathbb{C}$ sowie die obige Eigenschaft $(*)$. Als Aufwärmübung empfehlen wir, die Reduzibilität von $x+1$ zu zeigen. (Es gibt sogar Faktoren mit reellen Koeffizienten.) ◄ **UE 311**

Beispiele 5.2.1.19. Die Ringe $\mathbb{Z}$ und $K[x]$ (K Körper) sind faktoriell. Für $K[x]$ wird das erst aus Proposition 5.2.3.3 sowie den Sätzen 5.2.3.4 und 5.2.2.2 folgen.

Etwas später (in Unterabschnitt 5.3.2) werden wir den wichtigen Satz beweisen, dass der Polynomring nicht nur über einem Körper, sondern über einem beliebigen faktoriellen Ring wieder faktoriell ist. Mittels Induktion wird daraus folgen, dass dies auch für Polynomringe in mehreren und, wie einfache Überlegungen zeigen, sogar in beliebig vielen Variablen gilt.
Ein weiterer Aspekt der Struktur des Teilerverbandes ergibt sich durch folgenden Satz, im Wesentlichen eine Verallgemeinerung von Satz 3.1.3.4.

Satz 5.2.1.20.

(1) *Jede Totalordnung/Kette ist eine verbandsgeordnete Menge, die sogar einen distributiven Verband bildet.*

(2) *Bezeichne $K := (\mathbb{N}_\infty, \leq)$ die totalgeordnete Menge der natürlichen Zahlen ergänzt um ein größtes Element ∞. Diese Kette ist als Verband sogar vollständig, d. h., jede Teilmenge besitzt Supremum und Infimum.*

(3) *Sei R ein faktorieller Ring und I eine Indexmenge für ein Vetretersystem für alle Assoziierternklassen irreduzibler/primer Elemente p_i in R. Wir betrachten den Isomorphismus $\varphi : \bigoplus_{i\in I}(\mathbb{N},+,0) \to (R\setminus\{0\})/_\sim$ aus dem Beweis von Proposition 5.2.1.13 und seine Inverse $\psi : [a]_\sim \mapsto (e_i)_{i\in I} = (e_i(a))_{i\in I}$, gegeben durch $[a]_\sim = \left[\prod_{i\in I} p_i^{e_i(a)}\right]_\sim$ für $a \neq 0$. Für $a = 0$ schließlich setzen wir ψ fort durch $\psi([a]_\sim) = \psi([0]_\sim) = (\infty)_{i\in I}$. Dann ist $\psi\colon R/_\sim \to K^I$ eine isomorphe Einbettung der Ordnung $(R/_\sim, |)$ in das direkte Produkt $|I|$ vieler Kopien des in (2) definierten Verbandes, also $(K^I, \leq)$ mit $(e_i)_{i\in I} \leq (f_i)_{i\in I} :\Leftrightarrow \forall i \in I : e_i \leq f_i$.*

(4) *Sei R ein faktorieller Ring. Dann ist $R/_\sim$ ein distributiver vollständer Verband, der sogenannte* Teilerverband.

UE 312 ► Übungsaufgabe 5.2.1.21. (V) Beweisen Sie Satz 5.2.1.20. **◄ UE 312**

Formuliert man Aussage (4) um, so erhält man:

Folgerung 5.2.1.22. *In einem faktoriellen Ring R existieren für alle Mengen $A \subseteq R$ sowohl* $\mathrm{ggT}(A)$ *als auch* $\mathrm{kgV}(A)$.

5.2.2. Hauptidealringe

Inhalt in Kurzfassung: Hauptidealringe erweisen sich als faktoriell. Der Beweis erfolgt mit Hilfe des Kriteriums mit der Teilerkettenbedingung. Als Folgerung klärt sich die ordnungstheoretische Struktur des Kongruenzverbandes (d. h. des Idealverbandes) eines Hauptidealrings mit Hilfe der bereits aus Unterabschnitt 5.2.1 bekannten Ergebnisse über den Teilerverband eines faktoriellen Ringes auf sehr befriedigende Weise. Als Folgerung erhält man den wichtigen, im Falle des Ringes $\mathbb{Z}$ bereits bekannten Satz, dass sich der größte gemeinsame Teiler von Elementen in einem Hauptidealring als Linearkombination dieser Elemente schreiben lässt.

Zur Erinnerung:

Definition 5.2.2.1. Ein Integritätsbereich R heißt *Hauptidealring*, wenn jedes Ideal $I \lhd R$ ein Hauptideal ist.

Der wichtigste Inhalt dieses Unterabschnitts ist der folgende Satz.

Satz 5.2.2.2. *Jeder Hauptidealring ist ein faktorieller Ring.*

Beweis. Laut der dritten Bedingung in Satz 5.2.1.7 genügt es, für einen Hauptidealring R folgende zwei Aussagen zu beweisen:

(a) Jedes irreduzible Element $p \in R$ ist prim.

(b) In R gibt es keine unendlichen echt absteigenden Teilerketten, ausführlicher: Sei eine unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen $a_n \in R$ gegeben, sodass für alle n das Element a_{n+1} ein Teiler von a_n ist. Dann gibt es ein $n \in \mathbb{N}$ mit $a_n \sim a_{n+1} \sim a_{n+2} \sim \ldots$.

Zum Beweis dieser beiden Aussagen:

(a) Sei $p \in R$ irreduzibel. Das bedeutet, dass p in der Teilerhalbordnung ein oberer Nachbar von 1_R ist. Für die erzeugten Hauptideale bedeutet das nach Proposition 5.1.4.1: (p) ist ein unterer Nachbar von $(1) = R$ in der Ordnung der Hauptideale. Weil R ein Hauptidealring ist, sind das bereits alle Ideale, also ist (p) ein maximales Ideal, also erst recht Primideal (vierte Aussage in Satz 3.4.2.4). Nach Proposition 5.1.4.2 ist daher p ein Primelement.

(b) Die von den a_n erzeugten Hauptideale bilden (siehe Proposition 5.1.4.1) eine aufsteigende Kette

$$(a_0) \subseteq (a_1) \subseteq \ldots \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \ldots.$$

Für $J := \bigcup_{n=0}^{\infty}(a_n)$ gilt dann $J \lhd I$: $0 \in J$ ist klar. Für $a, b \in J$ gibt es $n, m \in \mathbb{N}$ mit $a \in (a_n)$ und $b \in (a_m)$. Sei oBdA $n \geq m$, also $a, b \in (a_n)$. Weil (a_n) ein Ideal ist, folgt $a + b, -a \in (a_n) \subseteq J$ und, für beliebiges $r \in R$, auch $ra \in (a_n) \subseteq J$. Also ist wirklich $J \lhd R$. Weil R ein Hauptidealring ist, gibt es ein $d \in R$ mit $J = (d)$. Wegen $d \in J$ ist $d \in (a_n)$ für ein $n \in \mathbb{N}$ und damit sowohl $(d) \subseteq (a_n)$ als auch $(a_n) \subseteq J = (d)$. Daraus folgt aber auch $(a_n) = (a_{n+1}) = \ldots = (d)$ und somit, wieder wegen Proposition 5.1.4.1, $a_n \sim a_{n+1} \sim a_{n+2} \sim \ldots$, was zu zeigen war. □

Im Beweis von Satz 5.2.2.2 kommt ein sehr ähnliches Argument wie im Beweis von Satz 2.2.1.26 vor, den man tatsächlich zu einer (geringfügigen) Verkürzung des Beweises in Satz 5.2.2.2 verwenden könnte.

UE 313 ▶ **Übungsaufgabe 5.2.2.3.** (A) Wie könnte man im Beweis von Satz 5.2.2.2 unter Zuhilfenahme von Satz 2.2.1.26 etwas direkter argumentieren? ◀ **UE 313**

Die Umkehrung von Satz 5.2.2.2 gilt nicht. Das folgt aus:

Proposition 5.2.2.4. *Sei R ein Integritätsbereich. Wenn der Polynomring $R[x]$ ein Hauptidealring ist, dann ist R ein Körper.*

UE 314 ▶ **Übungsaufgabe 5.2.2.5.** (V,W) Beweisen Sie Proposition 5.2.2.4. Hinweis: Betrachten Sie das von a und x erzeugte Ideal in $R[x]$, wobei $a \neq 0$ eine Nichteinheit von R ist. ◀ **UE 314**

Beispielsweise ist, weil $\mathbb{Q}[x]$ kein Körper ist, $\mathbb{Q}[x, y] \cong \mathbb{Q}[x][y]$ kein Hauptidealring, wegen des späteren Satzes 5.3.2.1 aber faktoriell. Sehr wohl Hauptidealringe sind hingegen $\mathbb{Z}$ (folgt wegen der Diskussion vor Proposition 3.4.1.16 oder auch mithilfe des nächsten Abschnitts wegen Satz 5.2.3.4 kombiniert mit Proposition 5.2.3.3), jeder Körper K ($\{0\} = (0)$ und $K = (1)$ sind die einzigen Ideale, da K einfach ist) sowie $K[x]$ für einen Körper K (siehe erneut Proposition 5.2.3.3 und Satz 5.2.3.4).

Proposition 5.1.4.1 hat bereits im Beweis von Satz 5.2.2.2 eine wesentliche Rolle gespielt. Aus ihr lesen wir ab, dass die Teilerhalbordnung eines Integritätsbereichs isomorph ist zur Halbordnung der Hauptideale bezüglich $\supseteq$. Weil das in einem Hauptidealring bereits alle Ideale sind, bedeutet das:

Proposition 5.2.2.6. *Ist R ein Hauptidealring, so ist die Teilerhalbordnung $(R/_\sim, |)$ isomorph zu $(\mathrm{Con}(R), \supseteq)$. Also gilt auch für die Verbände im algebraischen Sinn:*

$$(R/_\sim, \mathrm{ggT}, \mathrm{kgV}) \cong (\mathrm{Con}(R), \vee, \wedge).$$

Der Kongruenzverband ist vollständig. Also erhalten wir nochmals, dass es zu beliebigen Teilmengen des Ringes sowohl ggT als auch kgV gibt, wobei – das ist neu – diese dem Erzeugnis $\bigvee$ bzw. dem Schnitt $\bigcap$ der entsprechenden Hauptideale entsprechen. Das von einer beliebigen Menge A in R erzeugte Ideal $(A) = \bigvee A$ wird in Proposition 3.4.1.7 als

Menge aller Linearkombinationen von Elementen aus A beschrieben. Im Falle von Hauptidealen genügt es, Linearkombinationen der Erzeugenden der Hauptideale zu betrachten. Somit gilt für Hauptidealringe die folgende Verschärfung der Existenz beliebiger ggT in faktoriellen Ringen (für $R = \mathbb{Z}$ haben wir das bereits in Folgerung 3.2.4.2 gezeigt):

Satz 5.2.2.7 (Lemma von Bézout)**.** *Sei R ein Hauptidealring und $A \subseteq R$. Dann lässt sich jeder größte gemeinsame Teiler d von A als Linearkombination von Elementen aus A schreiben, d. h., es gibt ein $n \in \mathbb{N}$, $x_1, \ldots, x_n \in R$ und $a_1, \ldots, a_n \in A$ mit*

$$d = x_1 a_1 + \cdots + x_n a_n.$$

5.2.3. Euklidische Ringe

Inhalt in Kurzfassung: Euklidische Ringe sind solche Integritätsbereiche, in denen eine Art Division mit Rest möglich ist. Sehr schnell sieht man, dass es sich dabei um Hauptideal- und somit um faktorielle Ringe handelt. Iterierte Division mit Rest führt zum Euklidischen Algorithmus zur algorithmischen Berechnung des größten gemeinsamen Teilers zweier Ringelemente und darüber hinaus zur Darstellung desselben als Linearkombination. (Später wird das auch eine effektive Berechnung multiplikativer Inverser in endlichen Körpern mit p Elementen, p Primzahl, ermöglichen.) Wichtige Beispiele Euklidischer Ringe sind $\mathbb{Z}$, $K[x]$ und $K[[x]]$ (K Körper) und $\mathbb{Z}[i]$, der Ring der ganzen Gaußschen Zahlen.

Definition 5.2.3.1. Ein Integritätsbereich R heißt ein *Euklidischer Ring*, wenn es eine Abbildung $H : R \setminus \{0\} \to \mathbb{N}$ („Euklidische Bewertung“) mit folgender Eigenschaft gibt: Für alle $a \in R \setminus \{0\}$, $b \in R$ gibt es $q, r \in R$, sodass $b = aq + r$ mit $r = 0$ oder $H(r) < H(a)$ („Division mit Rest“).

Manchmal ist es praktisch, auch $H(0)$ zu definieren, etwa $H(0) := 0$ sofern es sonst keine Elemente $r \in R$ mit $H(r) = 0$ gibt, gelegentlich auch $H(0) := -\infty$. Überdies wird in der Literatur von einer Euklidischen Bewertung oft auch die Ungleichung $H(ab) \geq H(a)$ für alle $b \neq 0$ gefordert. Diese Modifikation des Begriffs der Euklidischen Bewertung ändert aber nichts am Begriff des Euklidischen Ringes:

UE 315 ► **Übungsaufgabe 5.2.3.2.** (A) Sei R ein Euklidischer Ring mit der Euklidischen Bewertung $H : R \setminus \{0\} \to \mathbb{N}$. Zeigen Sie, dass es dann eine Euklidische Bewertung $H' : R \setminus \{0\} \to \mathbb{N}$ gibt, die zusätzlich $H'(ab) \geq H'(a)$ für alle $b \neq 0$ erfüllt. ◄ **UE 315**

Körper sind auf triviale Weise Euklidische Ringe (H konstant, $q = a^{-1}b$ und $r = 0$ setzen). Die typischen Beispiele Euklidischer Ringe sind $\mathbb{Z}$ (mit $H(a) := |a|$) und, wegen der Polynomdivision aus Satz 3.4.6.8, Polynomringe $K[x]$ über einem Körper K (mit $H(f) := \operatorname{grad}(f)$). Also:

Proposition 5.2.3.3. *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Euklidischer Ring, außerdem der Polynomring $K[x]$ in einer Variablen über einem beliebigen Körper K.*

Euklidische Ringe sind stets Hauptidealringe, also eine Verschärfung der bisherigen Begriffe aus diesem Abschnitt. Im Beweis orientieren wir uns am Beweis der zweiten Aussage von Proposition 3.2.4.1 und ersetzen die dort verwendete Division mit Rest durch die analoge Eigenschaft der Euklidischen Bewertung.

Satz 5.2.3.4. *Jeder Euklidische Ring R ist ein Hauptidealring und somit (nach Satz 5.2.2.2) auch ein faktorieller Ring.*

Beweis. Sei $I \lhd R$, $I \neq (0) = \{0\}$. Zu zeigen ist, dass es ein $a \in R$ gibt mit $I = (a) = \{aq \mid q \in R\}$. Sei $a \in I \setminus \{0\}$ so gewählt, dass $H(a) = \min\{H(x) \mid x \in I \setminus \{0\}\}$. Wir behaupten, dass dann $I = (a)$ gilt. Trivialerweise ist $(a) \subseteq I$. Sei umgekehrt $b \in I$. Wegen $a \neq 0$ gibt es $q, r \in R$ mit $b = aq + r$ und $r = 0 \vee H(r) < H(a)$. Es ist $r = b - aq \in I$ (wegen $I \lhd R$), woraus (wegen der Minimalität von $H(a)$) schon $r = 0$ und damit $b = aq \in (a)$ folgt. Somit gilt auch $I \subseteq (a)$, also $I = (a)$. □

Die Umkehrung dieses Satzes gilt nicht, wie beispielsweise der quadratische Zahlring $\mathbb{Z}[\alpha]$ mit $\alpha = \frac{1+\sqrt{-19}}{2}$ zeigt. Der Nachweis ist keineswegs trivial. In Unterabschnitt 10.2.5 findet sich eine Anleitung.
Kombinieren wir Proposition 5.2.3.3 mit Satz 5.2.3.4 und Proposition 5.2.2.4, so erhalten wir:

Proposition 5.2.3.5. *Sei R ein Integritätsbereich. Der Polynomring $R[x]$ ist genau dann ein Hauptidealring, wenn R ein Körper ist.*

In Euklidischen Ringen kann man mit dem sogenannten *Euklidischen Algorithmus* den ggT und seine Darstellung als Linearkombination berechnen.

Sei R ein Euklidischer Ring und $a, b \in R$. Für $a = b = 0$ ist $\mathrm{ggT}(a, b) = 0$. Sei oBdA $a \neq 0$.

$$
\begin{aligned}
&\Rightarrow \exists q_1, r_1 \in R : b = aq_1 + r_1,\ r_1 = 0 \vee H(r_1) < H(a),\\
\text{falls } r_1 \neq 0 &\Rightarrow \exists q_2, r_2 \in R : a = r_1 q_2 + r_2,\ r_2 = 0 \vee H(r_2) < H(r_1),\\
\text{falls } r_2 \neq 0 &\Rightarrow \exists q_3, r_3 \in R : r_1 = r_2 q_3 + r_3,\ r_3 = 0 \vee H(r_3) < H(r_2),\\
&\ \ \vdots\\
&\text{allgemein:}\\
\text{falls } r_i \neq 0 &\Rightarrow \exists q_{i+1}, r_{i+1} \in R : r_{i-1} = r_i q_{i+1} + r_{i+1},\ r_{i+1} = 0 \vee H(r_{i+1}) < H(r_i).\\
&\qquad \text{(Dabei ist } a = r_0 \text{ und } b = r_{-1} \text{ zu setzen.)}
\end{aligned}
$$

Nach endlich vielen Schritten (wegen $H(a) = H(r_0) > H(r_1) > H(r_2) > \ldots$) erhält man ein k mit $r_k = 0$ und $r_{k-1} \neq 0$. Wir zeigen nun: $r_{k-1} = \mathrm{ggT}(a, b)$. Wir haben:

$$
\begin{aligned}
r_{k-2} = r_{k-1} q_k + 0 &\Rightarrow r_{k-1} | r_{k-2},\\
r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} &\Rightarrow r_{k-1} | r_{k-3},\\
r_{k-4} = r_{k-3} q_{k-2} + r_{k-2} &\Rightarrow r_{k-1} | r_{k-4},\\
&\ \ \vdots\\
r_1 = r_2 q_3 + r_3 &\Rightarrow r_{k-1} | r_1,\\
a = r_1 q_2 + r_2 &\Rightarrow r_{k-1} | a,\\
b = a q_1 + r_1 &\Rightarrow r_{k-1} | b,
\end{aligned}
$$

also gilt $r_{k-1}|a \wedge r_{k-1}|b$. Somit ist r_{k-1} ein gemeinsamer Teiler von a und b. Um zu zeigen, dass es sich sogar um einen *größten* gemeinsamen Teiler handelt, geben wir uns irgendeinen weiteren gemeinsamen Teiler t, also $t|a$ und $t|b$ vor. Ähnlich wie oben folgt daraus

$$\begin{aligned} r_1 = b - aq_1 &\Rightarrow t|r_1 \\ r_2 = a - r_1q_2 &\Rightarrow t|r_2 \\ r_3 = r_1 - r_2q_3 &\Rightarrow t|r_3 \\ &\vdots \\ r_{k-3} = r_{k-5} - r_{k-4}q_{k-3} &\Rightarrow t|r_{k-3} \\ r_{k-2} = r_{k-4} - r_{k-3}q_{k-2} &\Rightarrow t|r_{k-2} \\ r_{k-1} = r_{k-3} - r_{k-2}q_{k-1} &\Rightarrow t|r_{k-1}. \end{aligned}$$

Folglich ist r_{k-1} tatsächlich ein ggT von a und b.

Wir haben für Hauptidealringe gezeigt: $\mathrm{ggT}(a,b) = ax + by$ mit $x, y \in R$. In Euklidischen Ringen kann man die Koeffizienten x, y sogar explizit algorithmisch berechnen. Und zwar startet man mit der Darstellung $r_{k-1} = r_{k-3} + r_{k-2}(-q_{k-1})$ von r_{k-1} als Linearkombination der vorangegangenen Reste r_{k-2} und r_{k-3}. Sodann verwendet man die vorangegangenen Gleichungen, um für r_{k-2} eine Linearkombination von r_{k-3} und r_{k-4} einzusetzen, die auch eine für r_{k-1} liefert. Schritt für Schritt die anderen Gleichungen verwendend landet man schließlich bei einer Linearkombination von a und b:

$$\begin{aligned} \mathrm{ggT}(a,b) = r_{k-1} = r_{k-3} + r_{k-2}(-q_{k-1}) = r_{k-3} + (r_{k-4} - r_{k-3}q_{k-2})(-q_{k-1}) = \\ = r_{k-4}(-q_{k-1}) + r_{k-3}(1 + q_{k-2}q_{k-1}) = \ldots = ax + by. \end{aligned}$$

Wir fassen die Unterschiede zwischen den Begriffen von Abschnitt 5.2 zusammen:

1. In jedem faktoriellen Ring R gibt es zu beliebigen Elementen a, b immer einen größten gemeinsamen Teiler.
2. Wenn R ein Hauptidealring ist, weiß man überdies, dass sich der größte gemeinsame Teiler von a und b als R-Linearkombination von a und b schreiben lässt.
3. Wenn schließlich R ein Euklidischer Ring ist, dann haben wir sogar einen Algorithmus, der den ggT sowie diese Linearkombination findet. (Für den Fall $R = \mathbb{Z}$ ist dieser Algorithmus weit schneller als das Finden der Primfaktorzerlegung.)

Die Darstellung des ggT als Linearkombination kann man zu einer weiteren Beweisvariante für die eindeutige Primfaktorzerlegung in $\mathbb{Z}$ ausnutzen. Das wird in der folgenden Übungsaufgabe getan.

UE 316 ► Übungsaufgabe 5.2.3.6. (A) Zeigen Sie direkt mit Hilfe des Euklidischen Algorithmus, dass in einem Euklidischen Ring jedes irreduzible Element p prim ist. (Anleitung: Angenommen $p|ab$ und p sei kein Teiler von a. Weil p irreduzibel ist, folgt $\mathrm{ggT}(a,p) = 1$.) Beweisen Sie damit neuerlich, dass $\mathbb{Z}$ ein faktorieller Ring ist. **◄ UE 316**

Außerdem lässt sich der Euklidische Algorithmus durch Iteration auf mehr als zwei Elemente im Ring ausdehnen.

UE 317 ▶ **Übungsaufgabe 5.2.3.7.** (F+) Zeigen Sie, dass sich in Euklidischen Ringen der ggT nicht nur von zwei Elementen als deren Linearkombination schreiben lässt, sondern für eine beliebige endliche Anzahl. Beschreiben Sie, wie man diese Darstellung algorithmisch erhalten kann. Wie verhält es sich mit dem ggT unendlich vieler Elemente? ◀ **UE 317**

UE 318 ▶ **Übungsaufgabe 5.2.3.8.** (F) ◀ **UE 318**

(1) Man bestimme in $\mathbb{Z}$ den ggT von 525 und 231 und stelle ihn als Linearkombination der beiden Zahlen dar.

(2) Man bestimme in $\mathbb{Q}[x]$ alle ggT von $2x^6+3x^5-4x^4-5x^3-2x-2$ und x^5-2x^3-1 und stelle den normierten ggT als Linearkombination der beiden Polynome dar.

Ein weiteres reizvolles Beispiel eines Euklidischen Ringes ist das folgende:

Proposition 5.2.3.9. *Der von $\mathbb{Z}$ und der imaginären Einheit i erzeugte Ring $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$ (genannt der* Ring der ganzen Gaußschen Zahlen*) ist Euklidisch vermittels der Euklidischen Bewertung $H(z) := |z|^2$, folglich also auch ein Hauptidealring und faktoriell.*

UE 319 ▶ **Übungsaufgabe 5.2.3.10.** (V) Beweisen Sie Proposition 5.2.3.9. ◀ **UE 319**

Man kann zeigen, dass (bis auf multiplikative Faktoren, die Einheiten sind) sämtliche Primelemente in $\mathbb{Z}[i]$ gegeben sind durch die Primzahlen der Form $4k+3$ mit $k \in \mathbb{N}$ und durch jene $a+bi$ mit $a,b \in \mathbb{Z}$, für die a^2+b^2 eine Primzahl ist. Zur Übung begnügen wir uns mit ein paar leichteren Aufgaben zu $\mathbb{Z}[i]$:

UE 320 ▶ **Übungsaufgabe 5.2.3.11.** (B) Begründen Sie folgende Aussagen über den (nach Proposition 5.2.3.9) Euklidischen Ring $\mathbb{Z}[i]$. ◀ **UE 320**

(1) Für die Einheitengruppe von $\mathbb{Z}[i]$ gilt $E(\mathbb{Z}[i]) = \{1,-1,i,-i\}$.

(2) Ist p prim in $\mathbb{Z}[i]$ und eine natürliche Zahl, so auch eine Primzahl.

(3) Die Umkehrung gilt nicht: Es gibt Primzahlen, die nicht prim in $\mathbb{Z}[i]$ sind.

(4) Lässt sich $p = a^2+b^2 = (a+ib)(a-ib) \in \mathbb{P}$ als Summe zweier Quadrate positiver ganzer Zahlen a,b darstellen, so sind die Faktoren $a+ib$ und $a-ib$ prim in $\mathbb{Z}[i]$.

(5) Man bestimme alle primen Elemente $z \in \mathbb{Z}[i]$ mit $|z|^2 \leq 10$.

(6) Man bestimme in $\mathbb{Z}[i]$ die Primfaktorzerlegungen von $27+6i$ und $-3+4i$.

(7) Man bestimme in $\mathbb{Z}[i]$ einen ggT der Elemente $a = 7+i$ und $b = 5$ und stelle ihn in der Form $ax+by$ mit $x,y \in \mathbb{Z}[i]$ dar.

UE 321 ► **Übungsaufgabe 5.2.3.12.** (E) Zeigen Sie, dass der Ring $K[[x]]$ der formalen Potenzreihen über einem Körper K Euklidisch, folglich auch ein Hauptidealring und faktoriell ist. Bestimmen Sie alle irreduziblen Elemente modulo Assoziiertheit und geben Sie sämtliche Ideale durch Erzeugende an, jedes genau einmal. ◄ **UE 321**

5.3. Anwendungen und Ergänzungen

Der folgende Abschnitt bringt einige wichtige Themen, die, wenn auch in teilweise unterschiedliche Richtungen, an die bisherigen Untersuchungen zur Teilbarkeit anschließen. Zunächst gilt es in 5.3.1 einige nützliche Beobachtungen über Quotientenkörper anzustellen, wenn der zugrunde liegende Integritätsbereich sogar ein faktorieller Ring ist. Sodann beweisen wir in 5.3.2 den wichtigen Satz, dass der Polynomring über einem faktoriellen Ring selbst wieder faktoriell ist. Das reichert die Klasse verfügbarer Beispiele faktorieller Ringe wesentlich an. Klassisch sind die Inhalte von 5.3.3 über die Faktorisierung komplexer und reeller Polynome sowie von 5.3.4 über den Satz von Vieta (Beziehung zwischen den Nullstellen und den Koeffizienten eines Polynoms vermittels der elementarsymmetrischen Polynome). Auch der Partialbruchzerlegung (5.3.5) gebrochen rationaler Funktionen liegen Teilbarkeitsüberlegungen zugrunde. Den Abschluss von Abschnitt und Kapitel bildet Polynominterpolation nach Lagrange bzw. Newton (5.3.6), also ein ebenfalls klassisches Thema.

5.3.1. Der Quotientenkörper eines faktoriellen Rings

Inhalt in Kurzfassung: Ist ein Integritätsbereich sogar ein faktorieller oder gar Euklidischer Ring, so wird das Rechnen im Quotientenkörper besonders übersichtlich, weil dort jedes Element als Bruch gekürzte Darstellungen hat, unter denen durch eine sogenannte Normierungsfunktion sogar eine Normalform ausgezeichnet werden kann. Das wichtigste Beispiel (neben dem Ring $\mathbb{Z}$ und seinem Quotientenkörper $\mathbb{Q}$) ist der Polynomring über einem Körper mit dem Körper der gebrochen rationalen Funktionen als Quotientenkörper.

Wir erinnern an die Konstruktion des Quotientenkörpers K eines Integritätsbereichs R aus Unterabschnitt 3.4.5. Auf der Menge $R \times (R \setminus \{0_R\})$ erweist sich die durch $(r_1, s_1) \equiv (r_2, s_2) :\Leftrightarrow r_1 s_2 = s_1 r_2$ definierte Relation als Kongruenzrelation[3] bezüglich der Operationen

$$\begin{aligned}(r_1, s_1) + (r_2, s_2) &:= (r_1 s_2 + r_2 s_1, s_1 s_2),\\ -(r, s) &:= (-r, s),\\ (r_1, s_1) \cdot (r_2, s_2) &:= (r_1 r_2, s_1 s_2).\end{aligned}$$

Die Faktoralgebra $(K, +, 0_K, -, \cdot, 1_K)$ mit $K := (R \times R \setminus \{0\})/_{\equiv}$, den auf K induzierten Operationen $+, -$ und $\cdot$ sowie $0_K := [(0_R, 1_R)]_{\equiv}$ und $1_K := [(1_R, 1_R)]_{\equiv}$ erweist sich als

[3] Die ungewöhnliche Bezeichnung $\equiv$ dient der Unterscheidung von der Assoziiertheitsrelation $\sim$ auf R.

Körper. Die multiplikativen Inversen sind $[(r,s)]_{\equiv}^{-1} = [(s,r)]_{\equiv}$. Die Abbildung $\iota\colon R \to K$, $r \mapsto [(r,1_R)]_{\equiv}$ ist eine isomorphe Einbettung von R in K, und K wird als Körper von $\iota(R)$ erzeugt. Für jeden anderen Körper K', in den R durch ein $\iota'\colon R \to K'$ isomorph eingebettet werden kann, gibt es eine eindeutige isomorphe Einbettung $\varphi\colon K \to K'$ mit $\iota' = \varphi \circ \iota$. Ein Element $[(r,s)]_{\equiv}$ des Quotientenkörpers K wird üblicherweise als *Bruch* $\frac{r}{s}$ notiert, wobei r der *Zähler* und s der *Nenner* des Bruches heißt. Wir nennen das die *kanonische Darstellung* des Quotientenkörpers eines Integritätsbereichs.
Die Äquivalenzrelation $\equiv$ ist nicht trivial. Deshalb können verschiedene Brüche $\frac{r_1}{s_1}$ und $\frac{r_2}{s_2}$ dasselbe Element in K darstellen. Wünschenswert wären kanonische Vertreter. In einem ersten Schritt zeigen wir, dass es (so wie in den rationalen Zahlen) stets gekürzte Darstellungen im Quotientenkörper eines faktoriellen Rings gibt.

Proposition 5.3.1.1. *Sei R ein faktorieller Ring, K der Quotientenkörper von R in kanonischer Darstellung wie oben, und $[(r,s)]_{\equiv} \in K$. Dann gibt es ein $(r',s') \in R\times R\setminus\{0\}$ mit $(r',s') \equiv (r,s)$ und $\mathrm{ggT}(r',s') = 1$. Der Bruch $\frac{r'}{s'}$ heißt eine* gekürzte Darstellung *von $\frac{r}{s}$ und ergibt sich durch Kürzen von $\mathrm{ggT}(r,s)$ in $\frac{r}{s}$. Jede weitere gekürzte Darstellung $\frac{r''}{s''}$ von $\frac{r}{s}$ ist dazu assoziiert, d. h., es gilt $r'' \sim r'$ und $s'' \sim s'$.*

Beweis. Man geht von Primfaktorzerlegungen von $r = p_1 \cdot \ldots \cdot p_m$ und $s = q_1 \ldots q_n$ aus. Gibt es assoziierte Faktoren $p_i \sim q_j$, so unterscheiden sich diese nur um eine multiplikative Einheit e, d. h. $p_i = eq_j$, und man kann kürzen. Führt man sämtliche möglichen Kürzungen durch (insgesamt kürzt man also $\mathrm{ggT}(r,s)$), so verbleiben Zähler und Nenner, die teilerfremd sind, aber, wie man aus der Definition von $\equiv$ nachprüft, immer noch dasselbe Element von K darstellen.
Auch dass zwei gekürzte Darstellungen assoziiert sind, erhält man sehr leicht unter Verwendung der Primfaktorzerlegung in R und der Definition von $\equiv$ (Übung). □

UE 322 ► **Übungsaufgabe 5.3.1.2.** (V) Beweisen Sie die Assoziiertheitsaussage in Proposition 5.3.1.1. ◄ **UE 322**

Wir können die Eindeutigkeitsaussage modulo Assoziiertheit aus Proposition 5.3.1.1 zu einer Eindeutigkeitsaussage schlechthin verschärfen, nämlich mithilfe einer Auswahlfunktion aus den Assoziiertenklassen, einer sogenannten Normierungsfunktion. Aus technischen Gründen definieren wir diese Funktion wie folgt:

Definition 5.3.1.3. Sei R ein faktorieller Ring. Unter einer *Normierungsfunktion* verstehen wir eine Abbildung $\nu : R \to R$, die zu jedem $r \in R$ ein assoziiertes $\nu(r) \sim r$ auswählt derart, dass stets $\nu(rs) = \nu(r)\nu(s)$ und für $r \sim s$ auch $\nu(r) = \nu(s)$ gilt.

Aus der Definition folgt insbesondere $\nu(\nu(r)) = \nu(r)$. Wegen $\nu(1_R) = \nu(1_R \cdot 1_R) = \nu(1_R)\nu(1_R)$ gilt außerdem $\nu(1_R) = 1_R$. Die Elemente $\nu(r)$, $r \in R$, nennen wir dann *normiert*. Im Quotientenkörper K (in kanonischer Darstellung) eines faktoriellen Ringes R mit Normierungsfunktion ν ist es möglich, unter allen gekürzten Brüchen $\frac{r}{s} = [(r,s)]_{\equiv} \in K$ jenen auszuwählen, dessen Nenner $s = \nu(s)$ normiert ist. Diesen Bruch nennen wir die *normierte Darstellung* von $\frac{r}{s} = [(r,s)]_{\equiv} \in K$.

UE 323 ▶ **Übungsaufgabe 5.3.1.4.** (V) Zeigen Sie: Sei R ein faktorieller Ring mit einer Normierungsfunktion ν und sei K der Quotientenkörper von R in kanonischer Darstellung. Dann hat jedes Element aus K genau eine normierte Darstellung $\frac{r}{s}$. ◀ **UE 323**

Es stellt sich Frage, ob in allen faktoriellen Ringen Normierungsfunktionen existieren. Bevor wir uns diesem Problem widmen, betrachten wir die für uns wichtigsten Beispiele. Neben dem Körper $\mathbb{Q}$ der rationalen Zahlen als Quotientenkörper von $\mathbb{Z}$ ist das der Quotientenkörper eines Polynomrings.

Definition 5.3.1.5. Sind R und somit auch die Polynomringe $R[x]$ in einer Variablen x und $R[X]$ in einer beliebigen Variablenmenge X Integritätsbereiche, so heißen die Elemente der Quotientenkörper $R(x)$ bzw. $R(X)$ von $R[x]$ bzw. $R[X]$ *gebrochen rationale Funktionen* über R in einer Variablen x bzw. in den Variablen $x \in X$.

Beispiel 5.3.1.6.

(1) Im faktoriellen Ring $R = \mathbb{Z}$ gibt es die Normierungsfunktion $\nu : k \mapsto |k|$. Damit erhalten wir die bekannte Aussage, dass jede rationale Zahl (= jedes Element des Quotientenkörpers $K = \mathbb{Q}$ von $R = \mathbb{Z}$) genau eine gekürzte Darstellung mit einem Nenner hat, der eine natürliche Zahl ist.

(2) Ist $R = K[x]$ der Polynomring über einem Körper K, so gibt es die Normierungsfunktion $\nu : a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0 \mapsto x^n + \frac{a_{n-1}}{a_n} + \ldots + \frac{a_1}{a_n}x + \frac{a_0}{a_n}$ für $a_n \neq 0$, die jedem Polynom $\neq 0$ jenes assoziierte zuordnet, dessen führender Koeffizient 1 ist, das also normiert oder, wie man auch sagt, monisch ist. Entsprechend hat jede gebrochen rationale Funktion (= jedes Element des Quotientenkörpers $K(x)$ von $K[x]$) eine eindeutige gekürzte Darstellung mit normiertem Nenner.

Wie wir im nächsten Unterabschnitt sehen werden, bilden auch die Polynome in mehreren Variablen über beispielsweise einem Körper einen faktoriellen Ring. Auch hier lässt sich eine manchmal praktische Normierungsfunktion finden; in Unterabschnitt 5.3.4 werden wir diese als Nebenprodukt definieren.
Tatsächlich erlaubt die Primfaktorzerlegung in faktoriellen Ringen, dass wir stets Normierungsfunktionen definieren können:

Lemma 5.3.1.7. *Sei R ein faktorieller Ring. Dann existiert eine Normierungsfunktion $\nu : R \to R$.*

Beweis. Sei $P \subseteq R$ ein Vertretersystem der irreduziblen (also primen) Elemente modulo Assoziiertheit, d. h., für jedes irreduzible Element $q \in R$ existiere ein eindeutiges $p \in P$ mit $p \sim q$. Man überlegt sich sehr schnell, dass sich jedes Element $r \in R$ *eindeutig* in der Form $r = a \prod_{p \in P} p^{e_p}$ mit einer Einheit $a \in E(R)$ und Exponenten $e_p \in \mathbb{N}$ (wobei fast alle gleich 0 sind) schreiben lässt. Die Abbildung $\nu : R \to R$, $\nu(r) := \prod_{p \in P} p^{e_p}$, wobei $r = a \prod_{p \in P} p^{e_p}$ diese eindeutige Darstellung ist, ist wohldefiniert und eine Normierungsfunktion. □

Es sei angemerkt, dass die gerade konstruierte Normierungsfunktion sowohl konzeptuell als auch in puncto effektiver Berechenbarkeit manches zu wünschen übrig lässt – schließlich erfordert die Berechnung von $\nu(r)$ die Bestimmung der Primelemente. Selbst wenn

die Primelemente bekannt sind, muss man eine Primfaktorzerlegung durchführen, was bereits in $\mathbb{Z}$ sehr aufwendig ist. Viel praktischer – sowohl abstrakt als auch in konkreten Berechnungen – ist es, wenn die Normierungsfunktion wie in $\mathbb{Z}$ oder $K[x]$ ohne Rückgriff auf die Primfaktorzerlegung direkt bestimmt werden kann.

5.3.2. Polynomringe über faktoriellen Ringen sind faktoriell

Inhalt in Kurzfassung: Dieser Unterabschnitt steht gänzlich im Zeichen des Beweises des folgenden Satzes von Gauß: Der Polynomring über einem faktoriellen Ring ist wieder faktoriell.

In diesem Abschnitt soll vor allem der folgende Satz von Gauß bewiesen werden:

Satz 5.3.2.1 (Gauß)**.** *Ist R ein faktorieller Ring (z. B. ein Körper), so ist auch der Polynomring $R[x]$ über R in einer Variablen x faktoriell. Folglich sind auch die Ringe $R[x_1, \ldots, x_n]$ in n Variablen und sogar der Polynomring $R[X]$ über R in einer beliebigen Variablenmenge X faktoriell.*

Offenbar genügt es, den Satz für eine einzige Variable zu beweisen. Denn dann folgt er mittels Induktion für endlich viele und, weil auch bei unendlicher Variablenmenge X jedes Polynom nur endlich viele Variablen enthält, auch für den allgemeinen Fall.

UE 324 ▶ **Übungsaufgabe 5.3.2.2.** (V) Führen Sie diese Überlegungen im Detail aus: Beweisen Sie Satz 5.3.2.1 unter der Voraussetzung, dass er für den Polynomring $R[x]$ in einer Variablen über einem beliebigen faktoriellen Ring R gilt. ◀ **UE 324**

Die Grundidee des Beweises für eine Variable besteht darin, die Frage auf zwei bekanntermaßen faktorielle Ringe zurückzuspielen: den Koeffizientenbereich R und den Polynomring $Q[x]$ über dem Quotientenkörper Q von R. Die Ausgangsüberlegung ist sehr natürlich und führt sehr schnell zum entscheidenden Punkt: Wir gehen von einem Polynom $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ aus. Ist $c_f \in R$ ein ggT der Koeffizienten a_i, so können wir diesen herausheben und $f = c_f f_0$ schreiben mit einem $f_0 \in R[x]$ dessen Koeffizienten teilerfremd sind. Polynome mit dieser Eigenschaft wollen wir der einfacheren Sprechweise halber und nur in diesem Kontext *primitiv*[4] nennen. (Offenbar ist jedes über R irreduzible Polynom $f \in R[x]$ primitiv.) Sowohl c_f als auch f_0 lassen sich in irreduzible Faktoren zerlegen: Bei $c_f \in R$ ist das klar, weil R faktoriell ist. Und für f_0 – sofern es nicht schon selbst irreduzibel ist – müssen die Faktoren in einer echten Zerlegung gleichfalls primitiv sein (andernfalls hätten die a_i einen nichttrivialen ggT, was der Primitivität von f_0 widerspräche) und kleineren Grad haben als f. Deshalb muss fortgesetzte Faktorisierung nach endlich vielen Schritten zu einer Zerlegung in irreduzible Faktoren führen. Somit ist klar, dass Zerlegung in irreduzible Faktoren auch im Polynomring $R[x]$ möglich ist:

$$f = c_1 \cdot \ldots \cdot c_k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

[4] Diese Bedeutung des Wortes *primitiv* darf nicht mit jener verwechselt werden, die in der Theorie der endlichen Körper eine wichtige Rolle spielt (siehe Definition 6.3.3.2) und die sich ebenfalls auf Polynome beziehen kann.

mit irreduziblen (daher primen, da R faktoriell ist) Elementen $c_i \in R$ und irreduziblen (folglich primitiven) Polynomen $p_j \in R[x]$ vom Grad ≥ 1. Zu zeigen bleibt nach Definition des faktoriellen Rings noch die Eindeutigkeit dieser Zerlegung bis auf Reihenfolge der Faktoren und Assoziiertheit $\sim$ in $R[x]$. Die Einheiten von $R[x]$ sind genau die Einheiten von R, siehe Proposition 3.4.6.6, Aussage 7. Also gilt $f \sim g$ genau dann, wenn es eine Einheit $e \in E(R)$ in R mit $f = eg$ gibt.

Wir wollen uns nun überlegen, dass der Beweis des Satzes von Gauß vollständig ist, sofern wir zeigen können, dass in $R[x]$ irreduzible Polynome f sogar über dem Quotientenkörper Q von R irreduzibel sind – obwohl a priori ja Zerlegungen $f = f_1 f_2$ mit $f_i \in Q[x] \setminus R[x]$ denkbar wären. Unter dieser Voraussetzung (nämlich dass Irreduzibilität über R auch jene über Q impliziert) führen nämlich je zwei Zerlegungen

$$f = c_1 \cdot \ldots \cdot c_k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r = d_1 \cdot \ldots \cdot d_l \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

mit irreduziblen $c_1, c_2, \ldots, c_k$ und $d_1, d_2, \ldots, d_l$ aus R sowie irreduziblen (folglich auch primitiven) Polynomen $p_1, p_2, \ldots, p_r$ und $q_1, q_2, \ldots, q_s$ aus $R[x]$ zu zwei irreduziblen Zerlegungen

$$f = c \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r = d \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

über Q, wobei $c := c_1 \cdot \ldots \cdot c_k$ und $d := d_1 \cdot \ldots \cdot d_l$ Einheiten in $Q[x]$ sind. Weil $Q[x]$ als Euklidischer Ring faktoriell ist, müssen die p_i und die q_j bis auf Reihenfolge und Assoziiertheit in $Q[x]$ übereinstimmen. Assoziiertheit in $Q[x]$ bedeutet Übereinstimmung bis auf einen multiplikativen Faktor, der eine Einheit in Q ist, d. h. ein Element von $Q \setminus \{0\}$. Also gilt $p_i = \frac{a}{b} q_j$ mit gekürzten $a, b \in R$, $b \neq 0$. Daraus folgt $bp_i = aq_j$, womit a ein gemeinsamer Teiler der Koeffizienten von p_i und b ein gemeinsamer Teiler der Koeffizienten von q_j ist. Nun sind sowohl die p_i als auch die q_j aber primitiv. Somit müssen a und b und damit auch $\frac{a}{b}$ Einheiten in R sein. Folglich gilt die Assoziiertheit jedes p_i mit dem zugehörigen q_j sogar über R, womit auch c zu d über R assoziiert sein muss. Da R ein faktorieller Ring ist, ist die Zerlegung von $c \sim d$ in irreduzible Elemente eindeutig bis auf Reihenfolge und Assoziiertheit, also muss jedes $c_{\hat{i}}$ zu einem entsprechenden $d_{\hat{j}}$ über R assoziiert sein. Dies schließt den Beweis des Satzes 5.3.2.1 von Gauß ab.

Offen ist damit nur noch „irreduzibel über R impliziert irreduzibel über Q“ für Polynome $f \in R[x]$. Um das zu beweisen, beobachten wir zunächst, dass die Zerlegung $f = c_f f_0$ mit einem primitiven $f_0 \in R[x]$ (!) auch für jedes $f \in Q[x]$ möglich ist, sofern wir $c_f \in Q$ zulassen (Herausheben eines gemeinsamen Nenners). Außerdem sind c_f und f_0 durch f bis auf $\sim$ eindeutig bestimmt. Zusammengefasst:

Proposition 5.3.2.3. *Sei Q der Quotientenkörper des faktoriellen Ringes R und $f \in Q[x]$. Dann gibt es ein $c_f \in Q$ (genannt auch ein* Inhalt *von f) und ein primitives Polynom $f_0 \in R[x]$ mit $f = c_f f_0$. Im folgenden Sinn besteht sogar Eindeutigkeit: Ist $f \neq 0$ und gilt überdies $f = c_f f_0 = d_f g_0$ mit $d_f \in Q$ und einem weiteren primitiven Polynom $g_0 \in R[x]$, dann gibt es eine Einheit $e \in E(R)$ von R mit $c_f = d_f e$ und $g_0 = f_0 e$.*

UE 325 ► **Übungsaufgabe 5.3.2.4.** (V) Beweisen Sie Proposition 5.3.2.3 in aller Ausführlichkeit. ◄ **UE 325**

Damit können wir das entscheidende Lemma beweisen, aus dessen letzter – auch anderweitig immer wieder nützlicher – Aussage nach unseren Überlegungen weiter oben auch der Satz von Gauß folgt:

Lemma 5.3.2.5. *Seien $f, g \in Q[x]$.*

(1) *Sind f und g aus $R[x]$ und primitiv, so auch fg.*

(2) *Es gibt eine Einheit $e \in E(R)$ mit $c_f c_g = e c_{fg}$.*

(3) *Ist $f \in R[x]$ mit $\operatorname{grad}(f) \geq 1$ irreduzibel über R, so auch über Q.*

Beweis.

(1) Sei $f(x) = a_m x^m + \cdots + a_1 x + a_0$, $g(x) = b_n x^n + \cdots + b_1 x + b_0$ und $fg(x) = c_{m+n} x^{m+n} + c_1 x + c_0$. Weil f und g in $R[x]$ liegen, gilt das auch für fg. Angenommen fg wäre nicht primitiv, dann gäbe es ein Primelement $p \in R$, das $c_0, ..., c_{m+n}$ teilt. Da f und g primitiv sind, gibt es ein i und ein j mit $0 \leq i \leq m$ und $0 \leq j \leq n$, sodass $p|a_0, ..., p|a_{i-1}$, $p \nmid a_i$ und $p|b_0, ..., p|b_{j-1}, p \nmid b_j$. Nun ist $c_{i+j} = \sum_{\mu+\nu=i+j} a_\mu b_\nu = a_i b_j + \sum'$, wobei $\sum'$ für alle anderen Summanden aus der Summe steht (für die entweder $\mu < i$ oder $\nu < j$ ist). Klarerweise teilt p jeden Summanden aus $\sum'$ und somit auch $\sum'$ selbst. Da $p|c_{i+j}$, folgt daraus, dass $p|a_i b_j$. Da p Primelement ist, folgt $p|a_i$ oder $p|b_j$, im Widerspruch zu $p \nmid a_i$ und $p \nmid b_j$.

(2) Sei $f = c_f f_0$ und $g = c_g g_0$ mit primitiven Anteilen $f_0, g_0 \in R[x]$. Dann gilt $fg = (c_f c_g) f_0 g_0$, wobei $f_0 g_0$ nach dem ersten Teil primitiv ist. Also folgt die Behauptung aus der Eindeutigkeitsaussage in Proposition 5.3.2.3.

(3) Als über R irreduzibles Polynom muss f primitiv sein, weil andernfalls $f = c_f f_0$ eine nichttriviale Zerlegung über R wäre. Ist $\operatorname{grad}(f) = 1$, so ist f jedenfalls irreduzibel über Q. Wir haben also lediglich die indirekte Annahme $f = gh$ mit $g, h \in Q[x]$ und $\operatorname{grad}(g), \operatorname{grad}(h) \geq 1$ auf einen Widerspruch zu führen. Es gibt primitive Polynome $g_0, h_0 \in R[x]$ mit $g = c_g g_0$ und $h = c_h h_0$. Weil f primitiv ist, können wir $c_f = 1$ annehmen. Wegen der zweiten Aussage gibt es eine Einheit $e \in E(R)$ mit $1 = c_f = c_{gh} = e c_g c_h$, insbesondere gilt $c_g c_h \in R$. Folglich ist $f = gh = (c_g c_h) g_0 h_0$ eine Zerlegung von f in R mit nichttrivialen Faktoren g_0 und h_0, was der Irreduzibilität von f über R widerspricht. □

In unseren Überlegungen haben wir Assoziiertheitsrelationen bezüglich verschiedener Ringe verwendet. Dabei ist durchaus Sorgfalt geboten, wie die folgende Übungsaufgabe zeigt.

UE 326 ► **Übungsaufgabe 5.3.2.6.** (E) Finden Sie drei faktorielle Ringe $R_1 \leq R_2 \leq R_3$, sodass aber die von $E(R_1)$ auf R_3 definierte Äquivalenzrelation $\sim_1$ ◄ **UE 326**

$$x \sim_1 y :\Leftrightarrow \exists e \in E(R_1) : y = ex,$$

die von $E(R_2)$ auf R_3 definierte Äquivalenzrelation $\sim_2$

$$x \sim_2 y :\Leftrightarrow \exists e \in E(R_2) : y = ex$$

und die Assoziiertheitsrelation $\sim$ auf R_3 (die ja analog von $E(R_3)$ induziert wird) paarweise verschieden sind.
Hinweis: Man kann $R_3 = \mathbb{Q}$ wählen.
(Wenn das zu leicht ist: Finden Sie möglichst viele Unterringe von $\mathbb{Q}$, die auf $\mathbb{Q}$ lauter verschiedene Äquivalenzrelationen induzieren.)

Mit einer ähnlichen Idee wie Teil 1 in Lemma 5.3.2.5 beweist man auch die folgende nützliche Aussage:

Proposition 5.3.2.7 (Eisensteinsches Kriterium)**.** *Sei R ein faktorieller Ring. Ist $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit Grad ≥ 1 ein primitives Polynom und $p \in R$ irreduzibel mit*

$$p \nmid a_n,\ p \mid a_i \text{ für } i = 0, \ldots, n-1, \text{ und } p^2 \nmid a_0,$$

dann ist f irreduzibel in $R[x]$.

UE 327 ► Übungsaufgabe 5.3.2.8. (V,W) Beweisen Sie Proposition 5.3.2.7. **◄ UE 327**

Hilfreich bei der Suche nach rationalen Nullstellen eines Polynoms mit ganzen Koeffizienten ist:

Proposition 5.3.2.9. *Seien R ein faktorieller Ring, $f \in R[x]$ mit führendem Koeffizienten a_n und konstantem Koeffizienten a_0, seien $p, q \in R$ teilerfremd und sei das Element $\frac{p}{q}$ des Quotientenkörpers Q von R eine Nullstelle von f. Dann gilt $p|a_0$ und $q|a_n$.*

UE 328 ► Übungsaufgabe 5.3.2.10. (V,W) Beweisen Sie Proposition 5.3.2.9. **◄ UE 328**

Bevor wir uns in den nächsten Unterabschnitten mit zusätzlichen Teilbarkeitsüberlegungen in einem Polynomring über einem Körper beschäftigen, wollen wir im Rahmen einer Übungsaufgabe die Verträglichkeit von ggT mit Ringerweiterungen untersuchen. Dies wird in Unterabschnitt 6.2.6 noch nützlich sein.

UE 329 ► Übungsaufgabe 5.3.2.11. (F) Sind R, S faktorielle Ringe mit $R \leq S$ und sind $a, b \in R$, so können wir den ggT von a und b bezüglich R oder bezüglich S betrachten, was wir als $\mathrm{ggT}_R(a, b)$ bzw. $\mathrm{ggT}_S(a, b)$ anschreiben. Zeigen Sie: **◄ UE 329**

(1) Sei R sogar ein Hauptidealring. Dann ist $\mathrm{ggT}_R(a, b)$ auch ein ggT bezüglich S, also sind $\mathrm{ggT}_R(a, b)$ und $\mathrm{ggT}_S(a, b)$ in S assoziiert.

(2) Spezialfall: Seien K, L Körper mit $K \leq L$ und seien $R := K[x]$ sowie $S := L[x]$. Sind $f, g \in R$, so ist der (eindeutig bestimmte) normierte $\mathrm{ggT}_S(f, g)$ bereits in R enthalten.

(3) In (1) ist die Voraussetzung, dass R ein Hauptidealring ist, notwendig. (Das heißt: Finden Sie zwei faktorielle Ringe $R \leq S$ und Elemente $a, b \in R$, sodass $\mathrm{ggT}_R(a, b)$ und $\mathrm{ggT}_S(a, b)$ *nicht* in S assoziiert sind.)
Hinweis: Man kann $S := \mathbb{Z}[\frac{x}{2}] = \{\sum_{i=0}^{n} a_i (\frac{x}{2})^i \mid n \in \mathbb{N}, a_i \in \mathbb{Z}\}$ wählen.

5.3.3. Faktorisierung von Polynomen

Inhalt in Kurzfassung: Aus der Polynomdivision mit Rest folgt sehr schnell: Ein Polynom ist genau dann durch einen Linearfaktor mit Nullstelle α teilbar, wenn es selbst α als Nullstelle hat. Daraus ergibt sich eine Verschärfung des Fundamentalsatzes der Algebra: Jedes komplexe Polynom lässt sich in Linearfaktoren zerlegen. Daraus wiederum lässt sich folgern, dass jedes reelle Polynom in Linear- und quadratische Faktoren zerfällt. Das Ende des Unterabschnitts bildet die bekannte Lösungsformel für quadratische Gleichungen und ein kurzer Ausblick auf die Frage nach Lösungsformeln für Gleichungen höheren Grades (Schlagwort Galoistheorie, Kapitel 9).

Schon die bisherigen Untersuchungen legen das genauere Studium der Faktorisierung von Polynomen über Körpern nahe. Tatsächlich handelt es sich dabei um einen der zentralen Themenbereiche der klassischen Algebra. Das liegt zu einem guten Teil am engen Zusammenhang mit der Lösung algebraischer Gleichungen und somit mit Nullstellen von Polynomen. Entsprechend rückt auch der aus der Analysis vertraute Aspekt von Polynomen in den Vordergrund, nämlich Funktionen darzustellen. Die erste wichtige Beobachtung gilt auch allgemein:

Proposition 5.3.3.1. *Sei R ein kommutativer Ring mit 1, $f \in R[x]$ und $\alpha \in R$. Dann sind die folgenden beiden Aussagen äquivalent:*

(1) $f(\alpha) = 0$.

(2) *Das Polynom p mit $p(x) = x - \alpha$ ist ein Teiler von f.*

Beweis. (1) $\Rightarrow$ (2): Weil der führende Koeffizient von $p(x) = x - \alpha = 1_R x - \alpha$ das Einselement ist, lässt sich Division mit Rest durchführen (vgl. Satz 3.4.6.8) und liefert eine Darstellung $f = pq + r$ mit einem $q \in R[x]$ und einem Rest $r \in R[x]$, dessen Grad kleiner ist als der von p, also 0. Somit ist $r \in R$ eine Konstante. Einsetzen von α für x liefert $0_R = f(\alpha) = (\alpha - \alpha)q(\alpha) + r = r$. Also ist $f = pq$ teilbar durch $p(x) = x - \alpha$.
(2) $\Rightarrow$ (1): Ist p ein Teiler von f, so gibt es ein $q \in R[x]$ mit $f = pq$. Wieder setzen wir α für x ein und erhalten $f(\alpha) = p(\alpha)q(\alpha) = (\alpha - \alpha)q(\alpha) = 0_R$. □

Häufig nützlich ist auch die folgende einfache Tatsache:

Proposition 5.3.3.2. *Sei R ein Integritätsbereich. Ein Polynom f über R vom Grad 2 oder 3 ist genau dann irreduzibel, wenn f in R keine Nullstelle hat.*

UE 330 ► Übungsaufgabe 5.3.3.3. (V) Beweisen Sie Proposition 5.3.3.2. **◄ UE 330**

UE 331 ► Übungsaufgabe 5.3.3.4. (F) Man bestimme im Ring $\mathbb{Z}_2[x]$ alle irreduziblen Polynome bis zum Grad 4. **◄ UE 331**

Hat ein Polynom f neben $\alpha = \alpha_1$ noch weitere Nullstellen $\alpha_2, \ldots, \alpha_n$ (paarweise verschieden), so lässt sich Proposition 5.3.3.1 induktiv fortlaufend anwenden. Es gilt zunächst $f(x) = (x - \alpha_1)q_1(x)$ mit einem $q_1 \in R[x]$. Einsetzen von α_2 liefert $0_R = f(\alpha_2) = (\alpha_2 - \alpha_1)q_1(\alpha_2)$. Für $\alpha_1 \neq \alpha_2$ ist der erste Faktor $\alpha_2 - \alpha_1$ von 0_R verschieden. Wenn R ein Integritätsbereich ist, folgt daraus $q_1(\alpha_2) = 0$ und somit, wieder wegen Proposition 5.3.3.1, $q_1(x) = (x-\alpha_2)q_2(x)$ mit einem $q_2 \in R[x]$, also $f = (x-\alpha_1)(x-\alpha_2)q_2(x)$. Fährt man in dieser Weise fort, erhält man:

Proposition 5.3.3.5. *Seien R ein Integritätsbereich, $f \in R[x]$ und $\alpha_i \in R$, $i = 1, \ldots, n$, paarweise verschieden mit $f(\alpha_i) = 0_R$. Dann gibt es ein $q \in R[x]$ mit*

$$f(x) = q(x) \prod_{i=1}^{n} (x - \alpha_i).$$

Folglich ist der Grad von f mindestens n (die Anzahl der verschiedenen Nullstellen).

Ein Polynom kann auch durch höhere Potenzen $(x-\alpha)^e$ von Linearfaktoren teilbar sein. Entsprechend definiert man:

Definition 5.3.3.6. Hat das Polynom f über dem Integritätsbereich R die Zerlegung

$$f(x) = q(x) \prod_{j=1}^{m} (x - \alpha_j)^{e_j}$$

mit paarweise verschiedenen α_j, ganzzahligen Exponenten $e_j \geq 1$ und einem Polynom q ohne Nullstellen in R, so heißt e_j die *Vielfachheit* der Nullstelle α_j in f.

Ist R ein faktorieller Ring (z. B. ein Körper), so nach Satz 5.3.2.1 auch $R[x]$, woraus die Eindeutigkeit der α_j und e_j folgt.

UE 332 ► Übungsaufgabe 5.3.3.7. (V) Begründen Sie diese Behauptung. **◄ UE 332**

Der wichtigste Fall für R ist der eines Körpers K. Von besonderem Interesse ist dabei der Körper $\mathbb{C}$ der komplexen Zahlen. Weil nach dem Fundamentalsatz der Algebra (Satz 1.2.4.8) jedes komplexe Polynom vom Grad ≥ 1 mindestens eine Nullstelle hat, lässt sich die Abspaltung gemäß Proposition 5.3.3.5 so lange durchführen, bis q den Grad 0 hat, also konstant ist. Damit ergibt sich die zweite Fassung des Fundamentalsatzes:

Satz 5.3.3.8 (Fundamentalsatz der Algebra, Fassung 2)**.** *Jedes komplexe Polynom*

$$f(x) = \sum_{k=0}^{n} a_k x^k,$$

$a_k \in \mathbb{C}$, mit $n \geq 1$ und $a_n \neq 0$ zerfällt in den führenden Koeffizienten a_n und in bis auf die Reihenfolge eindeutig bestimmte normierte Linearfaktoren:

$$f(x) = a_n \prod_{j=1}^{m} (x - \alpha_j)^{e_j}$$

mit paarweise verschiedenen $\alpha_j \in \mathbb{C}$ und $\sum_{j=1}^{m} e_j = n$.

Das hat auch bemerkenswerte Konsequenzen für reelle Polynome $f(x) = \sum_{k=0}^{n} a_k x^k$, $a_k \in \mathbb{R}$, mit einer komplexen Nullstelle $\alpha \in \mathbb{C}$. Verwendet man, dass die komplexe Konjugation $\varphi : z = a + ib \mapsto \overline{z} = a - ib$ (a, b sind der Real- bzw. Imaginärteil der komplexen Zahl z) ein Automorphismus des Körpers $\mathbb{C}$ ist (das folgt aus Satz 1.2.4.3), der $\mathbb{R}$ punktweise fest lässt, rechnet man nämlich nach:

$$f(\varphi(\alpha)) = \sum_{k=0}^{n} a_k \varphi(\alpha)^k = \sum_{k=0}^{n} \varphi(a_k)\varphi(\alpha)^k = \varphi\left(\sum_{k=0}^{n} a_k \alpha^k\right) = \varphi(f(\alpha)) = \varphi(0) = 0$$

Also ist mit $\alpha = a + ib$ auch die Konjugierte $\varphi(\alpha) = \overline{\alpha} = a - ib$ eine Nullstelle von f. Die zugehörigen komplexen Linearfaktoren multiplizieren sich zum rein reellen Polynom

$$\begin{aligned}(x - \alpha)(x - \overline{\alpha}) = (x - a - ib)(x - a + ib) = (x - a)^2 - (ib)^2 = \\ = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x].\end{aligned}$$

Die Nullstellen reeller Polynome treten also einerseits als reelle auf, denen Linearfaktoren entsprechen, und andererseits als Paare komplexer, denen jeweils ein quadratisches Polynom ohne reelle Nullstellen entspricht. Nach Proposition 5.3.3.2 muss dieses quadratische Polynom über R irreduzibel sein.
Wir fassen zusammen:

Satz 5.3.3.9 (Fundamentalsatz der Algebra, reelle Fassung)**.** *Jedes reelle Polynom*

$$f(x) = \sum_{k=0}^{n} a_k x^k,$$

$a_k \in \mathbb{R}$*, mit* $n \geq 1$ *und* $a_n \neq 0$ *zerfällt in ein Produkt der Gestalt*

$$f(x) = a_n \prod_{i=1}^{m} (x - \alpha_i)^{e_i} \prod_{j=1}^{l} (x^2 + \beta_j x + \gamma_j)^{f_j}$$

mit $m, l, e_i, f_j \in \mathbb{N}$, $e_i \geq 1$, $f_j \geq 1$ *und* $\sum_{i=1}^{m} e_i + 2\sum_{j=1}^{l} f_j = n$*, wobei die Polynome* $x^2 + \beta_j x + \gamma_j$ *reell irreduzibel sind. Die reellen Nullstellen* α_i, $i = 1, \ldots, m$*, können paarweise verschieden gewählt werden, ebenso die Polynome* $x^2 + \beta_j x + \gamma_j$*. Bis auf die Nummerierung sind sie dann samt zugehörigen Vielfachheiten* e_i *bzw.* f_j *eindeutig bestimmt, ebenso wie* m *und* l*.*

Die konkrete Ermittlung der Nullstellen eines komplexen Polynoms f vom Grad n erfolgt für $n = 2$ nach der bekannten Formel: Durch Normierung bringt man f auf die Form $f(x) = x^2 + px + q$ mit $p, q \in \mathbb{C}$ und formt mittels Ergänzung auf ein vollständiges Quadrat um zu

$$f(x) = x^2 + px + q = \left(x + \frac{p}{2}\right)^2 - \frac{p^2}{4} + q.$$

Also ist $f(\alpha) = 0$ äquivalent zu $(\alpha + \frac{p}{2})^2 = \frac{p^2}{4} - q$ oder

$$\alpha = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Weil in $\mathbb{C}$ Quadratwurzeln uneingeschränkt existieren, sind somit zwei Nullstellen von f gefunden, die genau dann zusammenfallen, wenn[5] $4q = p^2$.
Allgemeine Lösungsformeln ähnlicher Art gibt es nur noch für die Grade $n = 3, 4$. Diese sind allerdings schon einigermaßen kompliziert. Für Grade $n \geq 5$ lässt sich zeigen, dass es überhaupt keine vergleichbaren Formeln mehr gibt. Dieses Thema ist der historische Ursprung der Galoistheorie, siehe Kapitel 9.

5.3.4. Symmetrische Polynome

Inhalt in Kurzfassung: Ein Polynom oder eine gebrochen rationale Funktion in mehreren Variablen heißt symmetrisch, wenn es invariant bleibt unter allen Permutationen der Variablen. Einfache Beispiele symmetrischer Polynome sind die elementarsymmetrischen. Der Hauptsatz über symmetrische Polynome besagt, dass sich jedes beliebige symmetrische Polynom in eindeutiger Weise als Polynom in diesen elementarsymmetrischen Polynomen darstellen lässt. Die elementarsymmetrischen Polynome treten auch im Satz von Vieta auf.

Im gesamten Unterabschnitt sei K ein Körper.

Definition 5.3.4.1. Sei $f \in K[x_1, \ldots, x_n]$ ein Polynom. Wir nennen f *symmetrisch*, wenn für alle Permutationen $\pi \in S_n$ der n Indizes gilt:

$$f(x_{\pi(1)}, \ldots, x_{\pi(n)}) = f(x_1, \ldots, x_n).$$

Man beachte, dass in dieser ziemlich unmissverständlichen Schreibweise so wie auch weiter unten ein Einsetzungshomorphismus im Spiel ist. Und zwar gibt es genau einen Homomorphismus $\varphi : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ mit $\varphi(x_i) = x_{\pi(i)}$ für $i = 1, \ldots, n$. Mit $f(x_{\pi(1)}, \ldots, x_{\pi(n)})$ ist das Polynom $\varphi(f)$ gemeint.

UE 333 ► **Übungsaufgabe 5.3.4.2.** (V) Zeigen Sie: Ist $g(y_1, \ldots, y_m) \in K[y_1, \ldots, y_m]$ ein beliebiges Polynom über K, und sind $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ symmetrische Polynome über K, so entsteht durch Einsetzen der f_i für die y_i wieder ein symmetrisches Polynom $h := g(f_1, \ldots, f_m)$ in den Variablen $x_1, \ldots, x_n$. ◄ **UE 333**

Bemerkenswert ist, dass auch eine Art Umkehrung von Übungsaufgabe 5.3.4.2 gilt. Dazu definieren wir:

Definition 5.3.4.3. Für $n \in \mathbb{N}$ seien die *elementarsymmetrischen Polynome* $s_{n,k}$ in n

[5] Selbstverständlich kann man auch für nicht normierte quadratische Polynome der Form $ax^2 + bx + c$ eine analoge Lösungsformel angeben. Obwohl sie statt der beiden Parameter p und q drei Parameter a, b und c enthält und entsprechend komplizierter ist, erfreut sie sich unter dem Titel „große Lösungsformel“ im Schulunterricht mancherorts erstaunlicher Beliebtheit. Weil jedes quadratische Polynom mühelos normiert werden kann, leistet sie aber nicht mehr als die im Haupttext angegebene „kleine Lösungsformel“.

Variablen mit Multiplikationszahl $k = 1, \ldots, n$ gegeben durch

$$\begin{aligned} s_{n,1} &= \sum_{i=1}^{n} x_i \\ s_{n,2} &= \sum_{1 \le i < j \le n} x_i \cdot x_j \\ &\vdots \\ s_{n,k} &= \sum_{i \le i_1 < \ldots < i_k \le n} x_{i_1} \cdot \ldots \cdot x_{i_k} \\ &\vdots \\ s_{n,n} &= x_1 \cdot \ldots \cdot x_n \end{aligned}$$

Damit können wir formulieren:

Satz 5.3.4.4 (Hauptsatz über symmetrische Polynome)**.** *Für jedes symmetrische Polynom $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ in n Variablen über einem Körper K gibt es ein eindeutiges Polynom $g \in K[x_1, \ldots, x_n]$ mit $f = g(s_{n,1}, \ldots, s_{n,n})$ für die elementarsymmetrischen Polynome $s_{n,k}$ in n Variablen.*

Für den Beweis verallgemeinern wir den Gradbegriff auf Polynome in mehreren Variablen. Der Grad eines Monoms $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \in K[x_1, \ldots, x_n]$ ist leicht zu definieren, nämlich als das Tupel $\vec{i} = (i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$. Um beliebigen Polynomen einen Grad zuordnen zu können, betrachten wir die *lexikographische Ordnung* $\le_{n,\text{lex}}$ auf $\mathbb{N}^n$ (siehe auch Übungsaufgabe 2.1.10.11):
Für $\vec{i} := (i_1, \ldots, i_n) \neq \vec{j} := (j_1, \ldots, j_n)$ sei $k := k_{\vec{i},\vec{j}}$ der minimale Index mit $i_k \neq j_k$. Wir setzen $\vec{i} <_{n,\text{lex}} \vec{j}$ genau dann, wenn $i_{k_{\vec{i},\vec{j}}} < j_{k_{\vec{i},\vec{j}}}$. Weiters sei $\vec{i} \le_{n,\text{lex}} \vec{j}$ genau dann, wenn $\vec{i} <_{n,\text{lex}} \vec{j}$ oder $\vec{i} = \vec{j}$. Man überzeugt sich leicht, dass $(\mathbb{N}^n, \le_{n,\text{lex}})$ eine Totalordnung ist. Aus technischen Gründen definieren wir den Grad nur für Polynome, die nicht das Nullpolynom sind.

Definition 5.3.4.5. Für $f = \sum_{\vec{i}=(i_1,\ldots,i_n)} c_{\vec{i}} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \in K[x_1, \ldots, x_n]$ mit $f \neq 0$ definieren wir den *Grad* von f durch

$$\text{grad}(f) := \max_{\le_{n,\text{lex}}} \left\{ \vec{i} \,\middle|\, c_{\vec{i}} \neq 0 \right\}.$$

(Nach der Annahme $f \neq 0$ ist die rechte Seite nicht leer.)
Unter dem *führenden Koeffizienten* von f verstehen wir $c_{\text{grad}(f)}$.

Der führende Koeffizient tritt also bei einem der Monome mit dem höchsten Grad in x_1 auf, und zwar unter diesen bei einem der Monome mit dem höchsten Grad in x_2, ..., und zwar unter diesen bei dem (eindeutigen!) Monom mit dem höchsten Grad in x_n. Die Definition des Grads wird anhand eines Beispiels transparent:

Beispiel 5.3.4.6.

(1) Ist $f = 3x_1^2x_2x_3^5 + 5x_1^2x_2x_3 - x_1x_2^4x_3^{10}$, so gilt $\operatorname{grad}(f) = (2,1,5)$ und der führende Koeffizient ist 3.

(2) Es gilt $\operatorname{grad}(s_{n,k}) = (\underbrace{1,\ldots,1}_{k \text{ Stellen}},0,\ldots,0)$ und der führende Koeffizient von $s_{n,k}$ ist 1.

Die folgenden Aussagen werden sich im Beweis des Hauptsatzes über symmetrische Polynome als zentral herausstellen.

Lemma 5.3.4.7. *Sei* $g = \sum_{\vec{h}} a_{\vec{h}} x_1^{h_1}x_2^{h_2}\ldots x_n^{h_n} \in K[x_1,\ldots,x_n]$, $g \neq 0$. *Dann gilt*

$$\operatorname{grad}(g(s_{n,1},\ldots,s_{n,n})) = \max\left\{(h_1+h_2+\cdots+h_n, h_2+\cdots+h_n,\ldots,h_n) \,\middle|\, a_{\vec{h}} \neq 0\right\}.$$

Insbesondere ist $g(s_{n,1},\ldots,s_{n,n}) \neq 0$. *Schreibt man* $\operatorname{grad}(g(s_{n,1},\ldots,s_{n,n})) = \vec{j}$, *so ist der führende Koeffizient von* $g(s_{n,1},\ldots,s_{n,n})$ *genau* $a_{\vec{j}}$.

UE 334 ► Übungsaufgabe 5.3.4.8. (V) Zeigen Sie Lemma 5.3.4.7. **◄ UE 334**

Lemma 5.3.4.9. *Sei* $f = \sum_{\vec{j}} c_{\vec{j}} x_1^{j_1}x_2^{j_2}\ldots x_n^{j_n} \in K[x_1,\ldots,x_n]$, $f \neq 0$, *ein symmetrisches Polynom. Für* $\operatorname{grad} f = (i_1,\ldots,i_n)$ *gilt dann* $i_1 \geq i_2 \geq \cdots \geq i_n$. *Außerdem ist* i_1 *der höchste Exponent* irgendeiner *Variable irgendeines Monoms, das in* f *vorkommt, d. h.*

$$i_1 := \max\left\{\max_{\ell=1,\ldots,n} j_\ell \,\middle|\, c_{\vec{j}} \neq 0\right\}.$$

Beweis. Wir beobachten zunächst die folgende Tatsache: Sei $c_{\vec{j}} x_1^{j_1}x_2^{j_2}\ldots x_n^{j_n}$ ein Monom, das in f vorkommt. Ist $\sigma \in S_n$ eine Permutation[6] von $\{1,\ldots,n\}$ mit $j_{\sigma(1)} \geq j_{\sigma(2)} \geq \cdots \geq j_{\sigma(n)}$, so kommt wegen der Symmetrie von f auch das Monom $c_{\vec{j}} x_1^{j_{\sigma(1)}}x_2^{j_{\sigma(2)}}\ldots x_n^{j_{\sigma(n)}}$ in f vor.
Daraus folgt, dass es zu jedem Monom, das in f vorkommt, ein weiteres Monom in f gibt, dessen Grad absteigend sortiert und $\leq_{n,\text{lex}}$-größer als der Grad des ursprünglichen Monoms ist – was die erste behauptete Aussage impliziert. Weiters folgt daraus, dass f ein Monom enthält, dessen Grad in der x_1-Komponente genau

$$\max\left\{\max_{\ell=1,\ldots,n} j_\ell \,\middle|\, c_{\vec{j}} \neq 0\right\}$$

ist – womit auch die zweite behauptete Aussage gezeigt ist. □

Der Beweis des Hauptsatzes wird gelingen, indem wir schrittweise vorgehen und den Grad von f mithilfe von Lemma 5.3.4.7 durch Subtraktion eines geeigneten Polynoms in $s_{n,1},\ldots,s_{n,n}$ laufend reduzieren. Vergleichbare Beweise für Polynome in einer Variablen funktionieren deshalb, weil es nur endlich viele mögliche Grade gibt, die kleiner oder gleich dem Grad des Ausgangspolynoms sind. Daher muss das Verfahren irgendwann zu einem Ende kommen. Bei Polynomen in mehreren Variablen ist das nicht ganz

[6] Wenn in $\vec{j}$ ein gewisser Wert mehrfach vorkommt, dann gibt es mehrere solcher Permutationen.

so einfach, da ein festes Element von $\mathbb{N}^n$ bezüglich $\leq_{n,\text{lex}}$ unendlich viele Vorgänger haben kann, z.B hat im Fall $n = 2$ das Paar $(1,0)$ die unendlich vielen Vorgänger $(0,0),(0,1),\ldots,(0,m),\ldots$, etc. Schränkt man sich aber auf symmetrische Polynome ein, dann kann dieses Phänomen wegen der zweiten Aussage von Lemma 5.3.4.9 nicht auftreten.

Lemma 5.3.4.10. *Sei $f \in K[x_1,\ldots,x_n]$, $f \neq 0$, ein symmetrisches Polynom. Dann ist die Menge*

$$E := \{\text{grad}(f') \mid f' \in K[x_1,\ldots,x_n] \text{ symmetrisch}, \text{grad}(f') \leq_{n,lex} \text{grad}(f)\} \subseteq \mathbb{N}^n$$

endlich.

Beweis. Wir schreiben $(i_1,\ldots,i_n) = \vec{i} := \text{grad}(f)$ und für ein beliebiges symmetrisches f' außerdem $(i'_1,\ldots,i'_n) = \vec{i'} := \text{grad}(f')$.
Nach der zweiten Aussage von Lemma 5.3.4.9 ist i'_1 der höchste Exponent irgendeiner Variable irgendeines Monoms, das in f' vorkommt. Aus $\text{grad}(f') \leq_{n,\text{lex}} \text{grad}(f)$ folgt $i'_1 \leq i_1$, also können in f' nur Monome mit Exponenten kleiner oder gleich i_1 vorkommen. Somit gilt $E \subseteq \{0,\ldots,i_1\}^n$, womit die Behauptung bewiesen ist. □

Nach diesen Vorarbeiten können wir den Hauptsatz zeigen.

Beweis (von Satz 5.3.4.4). Wir zeigen zunächst die Existenz von g. Sei dazu ein symmetrisches Polynom $f \in K[x_1,\ldots,x_n]$ gegeben. Wenn f das Nullpolynom ist, so können wir $g = 0$ setzen. Wenn $f = \sum_{\vec{j}} c_{\vec{j}} x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$ nicht das Nullpolynom ist, dann betrachten wir $(i_1,\ldots,i_n) = \vec{i} := \text{grad}(f)$ und den führenden Koeffizienten $c_{\vec{i}}$. Nach Lemma 5.3.4.9 gilt $i_1 \geq i_2 \geq \cdots \geq i_n$. Wir definieren $g_1 := c_{\vec{i}} x_1^{i_1-i_2} x_2^{i_2-i_3} \ldots x_{n-1}^{i_{n-1}-i_n} x_n^{i_n}$ und beobachten, dass nach Lemma 5.3.4.7

$$\text{grad}(g_1(s_{n,1},\ldots,s_{n,n})) = (i_1,\ldots,i_n) = \vec{i}$$

sowie dass der führende Koeffizient von $\text{grad}(g_1(s_{n,1},\ldots,s_{n,n}))$ genau $c_{\vec{i}}$ ist. Somit ist $f' := f - g_1(s_{n,1},\ldots,s_{n,n})$ ein symmetrisches Polynom, das bezüglich $\leq_{n,\text{lex}}$ einen strikt kleineren Grad als f hat. Wir iterieren diesen Prozess und finden ein Polynom g_2, sodass $f' - g_2(s_{n,1},\ldots,s_{n,n})$ einen bezüglich $\leq_{n,\text{lex}}$ nochmals echt kleineren Grad hat. So fortfahrend erhalten wir eine echt absteigende Folge von Graden symmetrischer Polynome, die alle $\leq_{n,\text{lex}}$-kleiner als $\text{grad}(f)$ sind. Wegen Lemma 5.3.4.10 muss der Prozess nach endlich vielen Schritten stoppen, sagen wir nach ℓ Schritten. Anders formuliert muss das symmetrische Ausgangspolynom von Schritt ℓ mit dem gefundenen Polynom $g_\ell(s_{n,1},\ldots,s_{n,n})$ übereinstimmen. Somit gilt $f = g_1(s_{n,1},\ldots,s_{n,n}) + \cdots + g_\ell(s_{n,1},\ldots,s_{n,n})$ und wir setzen $g := g_1 + \cdots + g_\ell$.
Der Beweis der Eindeutigkeit verläuft sehr ähnlich. Wir beweisen, dass für Polynome $g,h \in K[x_1,\ldots,x_n]$ aus $g(s_{n,1},\ldots,s_{n,n}) = f = h(s_{n,1},\ldots,s_{n,n})$ bereits $g = h$ folgt. Wenn f das Nullpolynom ist, dann folgt $g = 0 = h$ aus Lemma 5.3.4.7. Wenn f nicht das Nullpolynom ist, dann gilt jedenfalls $g,h \neq 0$. Wir schreiben $g = \sum_{\vec{h}} a_{\vec{h}} x_1^{h_1} x_2^{h_2} \ldots x_n^{h_n}$. Wir verwenden wieder Lemma 5.3.4.7 und erhalten

$$\text{grad}(g(s_{n,1},\ldots,s_{n,n})) = \max\left\{(h_1+h_2+\cdots+h_n, h_2+\cdots+h_n,\ldots,h_n) \,\middle|\, a_{\vec{h}} \neq 0\right\},$$

wobei der führende Koeffizient von $g(s_{n,1},\dots,s_{n,n})$ genau $a_{\vec{j}}$ ist, wenn

$$\operatorname{grad}(g(s_{n,1},\dots,s_{n,n})) = (j_1+j_2+\dots+j_n, j_2+\dots+j_n,\dots,j_n).$$

Analoges gilt für $h(s_{n,1},\dots,s_{n,n})$, also muss das Monom $x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}$ auch in h vorkommen, und zwar mit demselben Koeffizienten $a_{\vec{j}}$. Definieren wir das Monom $g_1 := a_{\vec{j}}x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}$, so hat folglich das symmetrische Polynom

$$f' := (g-g_1)(s_{n,1},\dots,s_{n,n}) = (h-g_1)(s_{n,1},\dots,s_{n,n})$$

einen bezüglich $\leq_{n,\mathrm{lex}}$ strikt kleineren Grad als f. Wenn wir das Argument wie im ersten Teil des Beweises iterieren, so muss dieser Prozess wieder wegen Lemma 5.3.4.10 nach endlich vielen Schritten stoppen, d. h., im ℓ-ten Schritt muss das symmetrische Polynom das Nullpolynom sein. Somit sind auch die im ℓ-ten Schritt erhaltenen Differenzpolynome $g-g_1-\dots-g_\ell$ und $h-g_1-\dots-g_\ell$ gleich dem Nullpolynom, woraus sich $g=h$ ergibt. □

Aus der Verallgemeinerung des Gradbegriffs für Polynome in mehreren Variablen ergibt sich eine Normierungsfunktion im Sinne von Definition 5.3.1.3, wie wir bereits in Unterabschnitt 5.3.1 angekündigt haben.

Beispiel 5.3.4.11. Für Polynome $f,g\in K[x_1,\dots,x_n]$ gilt $\operatorname{grad}(fg)=\operatorname{grad}(f)\operatorname{grad}(g)$. Auf dem Ring $R := K[x_1,\dots,x_n]$ ist daher

$$\nu : f=\sum_{\vec{i}} c_{\vec{i}}x_1^{i_1}x_2^{i_2}\dots x_n^{i_n} \mapsto \sum_{\vec{i}} \frac{c_{\vec{i}}}{c_{\operatorname{grad}(f)}}x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$$

eine Normierungsfunktion, zu deren Berechnung keine Primfaktorzerlegung notwendig ist.

Als mächtig in der Galoistheorie erweist sich Satz 5.3.4.4 vor allem in Verbindung mit der folgenden, auch als *Satz von Vieta*[7] bekannten Tatsache:

Proposition 5.3.4.12 (Satz von Vieta)**.** *Die Koeffizienten eines in Linearfaktoren zerfallenden normierten Polynoms*

$$f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_0=\prod_{i=1}^{n}(x-\alpha_i)$$

erfüllen

$$a_k=(-1)^{n-k}s_{n,n-k}(\alpha_1,\dots,\alpha_n).$$

Wie oben bezeichnet dabei $s_{n,n-k}$ das elementarsymmetrische Polynom in n Variablen mit Multiplikationszahl $n-k$.

[7] Benannt nach dem französischen Mathematiker François Viète (1540-1603), der sich latinisiert Franciscus Vieta nannte.

UE 335 ▶ Übungsaufgabe 5.3.4.13. (V) Zeigen Sie Proposition 5.3.4.12. **◀ UE 335**

UE 336 ▶ Übungsaufgabe 5.3.4.14. (B) Gegeben sei das Polynom $f(x) = x^4+x^3+x^2+x^1+1 = \frac{x^5-1}{x-1}$. **◀ UE 336**

(1) Zerlegen Sie f in seine irreduziblen Faktoren über $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.

(2) Finden Sie Wurzelausdrücke für die reellen Zahlen $\cos\frac{k\pi}{5}$, $k = 1, 2, 3, 4$.

5.3.5. Gebrochen rationale Funktionen und ihre Partialbruchzerlegung

Inhalt in Kurzfassung: Gebrochen rationale Funktionen in einer Variablen können als Brüche dargestellt werden, die vermittels Kürzung und Normierung in eine Normalform gebracht werden können. Eine weitere Normalform gebrochen rationaler Funktionen ist aus der elementaren Analysis bekannt, wenn es um die Ermittlung einer Stammfunktion geht. Der Hintergrund ist ein algebraischer, nämlich die Primfaktorzerlegung. Dies soll nun dargelegt werden.

Gebrochen rationale Funktionen $r(x)$ in einer Variablen x über einem Körper K sind nach Definition Elemente des Quotientenkörpers $K(x)$ des Polynomrings $K[x]$ über K. Als solche haben Sie eine Darstellung als Brüche $r(x) = \frac{p(x)}{q(x)}$ mit $p(x), q(x) \in K[x]$. Durch die Forderung der Teilerfremdheit von p und q sowie der Normiertheit von q kann man diese Darstellung eindeutig machen, womit sogar eine Normalform vorliegt, siehe Unterabschnitt 5.3.1. Andere Normalformen, die zum Beispiel in der Analysis bei der Integration gebrochen rationaler reeller Funktionen sehr nützlich sind, ergeben sich durch die sogenannte *Partialbruchzerlegung*, die wir nun besprechen wollen.
Für ein beliebiges $r(x) = \frac{p(x)}{q(x)} \in K(x)$ liefert Polynomdivision mit Rest von p durch q eine Darstellung $r(x) = f(x) + \frac{p_0(x)}{q(x)}$ mit Polynomen $f, p_0, q \in K[x]$, wobei $\operatorname{grad}(p_0) < \operatorname{grad}(q)$. Dabei ist f jedenfalls eindeutig. Setzt man Teilerfremdheit von p und q sowie Normiertheit von q voraus (was stets durch Kürzen sowie Division durch den höchsten Koeffizienten von q erreicht werden kann), so sind auch p_0 und q eindeutig und ebenfalls teilerfremd. Die Partialbruchzerlegung bezieht sich auf solche Brüche von Polynomen, bei denen der Zählergrad kleiner ist als der Nennergrad.
Sei dazu $q = q_1^{e_1} \cdot \ldots \cdot q_k^{e_k}$ mit positiven $e_i \in \mathbb{N}$ die Zerlegung des normierten Polynoms q in paarweise verschiedene irreduzible und normierte Faktoren q_i der Grade $m_i := \operatorname{grad}(q_i) > 0$. Wir betrachten $K(x)$ als Vektorraum über dem Körper K und zwei Unterräume $U_1, U_2 \leq K(x)$, von denen wir zeigen werden, dass sie übereinstimmen. Und zwar werde U_1 erzeugt von den gebrochen rationalen Funktionen

$$r_{i,e,j} := \frac{x^j}{q_i^e}, \quad i = 1, \ldots, k, \quad e = 1, \ldots, e_i \quad j = 0, \ldots, m_i - 1.$$

Für die Anzahl n der $r_{i,e,j}$ gilt

$$n = \sum_{i=1}^{k} \sum_{e=1}^{e_i} m_i = \sum_{i=1}^{k} e_i \operatorname{grad}(q_i) = \operatorname{grad}(q).$$

Andererseits werde U_2 von den (offenbar über K linear unabhängigen) gebrochen rationalen Funktionen $\frac{x^l}{q}$ $(l = 0, \ldots, n-1 = \operatorname{grad}(q) - 1)$ erzeugt. Es gilt also jedenfalls $\dim U_2 = n$. Jede Linearkombination der $r_{i,e,j}$ lässt sich auf gemeinsamen Nenner q bringen, wobei der Grad des resultierenden Zählerpolynoms stets kleiner als $n = \operatorname{grad}(q)$ bleibt. Somit ist U_1 in U_2 enthalten. Stimmen die Dimensionen überein, so folgt daraus sogar Gleichheit. Um $\dim U_1 = n = \dim U_2$ zu zeigen, genügt es nach obigen Überlegungen, die lineare Unabhängigkeit der $r_{i,e,j}$ zu überprüfen. Das ist eine Routineaufgabe:

UE 337 ► **Übungsaufgabe 5.3.5.1.** (V) Zeigen Sie, dass die oben definierten gebrochen rationalen Funktionen $r_{i,e,j} \in K(x)$ $(i = 1, \ldots, k;\ e = 1, \ldots, e_i;\ j = 0, \ldots, m_i - 1)$ linear unabhängig über K sind. ◄ **UE 337**

Damit folgt zusammenfassend der Satz von der *Partialbruchzerlegung*:

Satz 5.3.5.2. *Sei K ein Körper und $r = \frac{p}{q}$ eine gebrochen rationale Funktion über K, $p, q \in K[x]$, q normiert. Sei*

$$q = q_1^{e_1} \cdot \ldots \cdot q_n^{e_n}$$

die Zerlegung des Nennerpolynoms q in Potenzen irreduzibler und normierter Faktoren q_i, die sowohl paarweise als auch zu p teilerfremd sind, und Vielfachheiten $e_i \geq 1$ haben mögen. Dann gibt es eindeutig bestimmte Polynome f und $t_{i,e}$, $i = 1, \ldots, n$, $e = 1, \ldots, e_i$, mit $\operatorname{grad}(t_{i,e}) < \operatorname{grad}(q_i)$, sodass gilt:

$$r = f + \sum_{i=1}^{n} \sum_{e=1}^{e_i} \frac{t_{i,e}}{q_i^e}$$

Anmerkung 5.3.5.3.

(1) Sind im vorherigen Satz alle Primfaktoren q_i linear, so sind die Zähler der Partialbrüche Konstante. Das ist sicher der Fall, wenn K algebraisch abgeschlossen ist, also z. B. für $K = \mathbb{C}$.

(2) Ist $K = \mathbb{R}$, so sind alle q_i linear (reelle Nullstelle des Nennerpolynoms, dann sind die $t_{i,j}$ konstant) oder quadratisch (Paar konjugiert komplexer Nullstellen des Nennerpolynoms, dann sind die $t_{i,j}$ höchstens linear).

UE 338 ► **Übungsaufgabe 5.3.5.4.** (D) Satz 5.3.5.2 spielt in der Analysis bei der Integration gebrochen rationaler Funktionen eine wichtige Rolle. Rekapitulieren Sie jene Integrationsregeln, mit deren Hilfe man zu jeder beliebigen in Partialbruchzerlegung vorgegebenen gebrochen rationalen Funktion eine Stammfunktion finden kann. Ist damit das Integrationsproblem für gebrochen rationale Funktionen auch in konventioneller Darstellung, d. h. als Quotient zweier Polynome, gelöst? ◄ **UE 338**

5.3.6. Interpolation nach Lagrange und nach Newton

Inhalt in Kurzfassung: Zu je $n+1$ Elementen eines Körpers K zusammen mit vorgegebenen Funktionswerten gibt es genau eine interpolierende Polynomfunktion vom Grad $\leq n$. Die Formel von Lagrange liefert eine Darstellung dieses Interpolationspolynoms, dem man die geforderte Eigenschaft sehr unmittelbar ansieht. Vom algorithmischen Standpunkt ist die Interpolation nach Newton effektiver. Die Eindeutigkeit der Lösung folgt, weil die Differenz zweier Interpolationspolynome höchstens Grad n und mindestens $n+1$ Nullstellen hat, also das Nullpolynom sein muss.

Untersucht man Polynome unter dem Gesichtspunkt der Funktionen, die sie darstellen, so stellt sich die Frage, wie weit sich beliebige Funktionen als Polynomfunktionen darstellen lassen. Klarerweise gilt das nicht uneingeschränkt, sehr wohl aber bei Betrachtung endlich vieler Punkte (*Interpolation nach Lagrange*).

Satz 5.3.6.1. *Seien K ein Körper, $a_0, \ldots, a_n \in K$ (*Stützstellen*) paarweise verschieden und $b_0, \ldots, b_n \in K$ (*Funktionswerte*) beliebig. Dann gibt es genau ein Polynom $p \in K[x]$ (*Interpolationspolynom*) vom Grad $\leq n$ mit $p(a_i) = b_i$ für $i = 0, 1, \ldots, n$. Dieses Polynom ist gegeben durch die Formel*

$$p(x) = \sum_{i=0}^{n} b_i \delta_i(x) \quad \textit{mit} \quad \delta_i(x) = \frac{\prod_{0 \leq j \leq n, j \neq i}(x - a_j)}{\prod_{0 \leq j \leq n, j \neq i}(a_i - a_j)}.$$

(Die Polynome $\delta_i(x)$ heißen auch Lagrange-Basispolynome*.)*

Beweis. Jedes δ_i ist nach Definition ein Polynom vom Grad n, daher ist p als Summe der b_i-fachen der δ_i ein Polynom vom Grad $\leq n$. Außerdem gilt $\delta_j(a_i) = 0$ für $i \neq j$ und $\delta_i(a_i) = 1$. Hieraus liest man $p(a_i) = b_i$ für alle $i = 0, 1, \ldots, n$ ab.
Die Eindeutigkeit von p ergibt sich so: Sei q ein weiteres Polynom vom Grad $\leq n$ mit $q(a_i) = b_i$ für $i = 0, 1, \ldots, n$. Dann ist auch die Differenz $p - q$ ein Polynom vom Grad $\leq n$ mit den $n + 1$ verschiedenen Nullstellen $a_0, a_1, \ldots, a_n$. Das ist aber nur für das Nullpolynom $p - q = 0$ möglich, also gilt $q = p$. □

Für Anwendungen (auch) weit abseits der Algebra ist es von Interesse, das Interpolationspolynom p aus Satz 5.3.6.1 auch auf algorithmisch effektive Weise zu ermitteln. Die dort angegebene Formel lässt diesbezüglich manche Wünsche offen, insbesondere die Hoffnung, dass aus einem bereits berechneten p möglichst rasch ein modifiziertes Polynom berechnet werden kann, wenn n um 1 erhöht wird, also wenn über die bereits gegebenen a_i und b_i hinausgehend für eine weitere Stelle a_{n+1} ein Funktionswert b_{n+1} vorgegeben wird. Mit dieser Motivation gelangt man zur *Interpolation nach Newton*:
Für die Folge $a_0, a_1, \ldots$ (paarweise verschieden) definieren wir die Polynome

$$q_j(x) := \prod_{k=0}^{j-1}(x - a_k)$$

und können Koeffizienten λ_i (in eindeutiger Weise) so wählen, dass

$$p_i(x) := \sum_{j=0}^{i} \lambda_j q_j(x)$$

das Interpolationspolynom für $a_0, a_1, \ldots, a_i$ und $b_0, b_1, \ldots, b_i$ ist. Dass dies tatsächlich möglich ist, ergibt sich mittels Induktion: Für $i = 0$ ist $q_i = 1$ (leeres Produkt) und daher $\lambda_0 = b_0$ zu setzen. Angenommen, p_i habe die behauptete Interpolationseigenschaft $p_i(a_j) = b_j$ für $j = 0, 1, \ldots, i$. Aus p_i ergibt sich $p_{i+1} = p_i + \lambda_{i+1} q_{i+1}$ durch Addition des λ_{i+1}-fachen von q_{i+1}.
Offenbar ist q_{i+1} so definiert, dass $q_{i+1}(a_j) = 0$ für $j = 0, 1, \ldots, i$ gilt, aber $q_{i+1}(a_{i+1}) \neq 0$. Folglich gilt $p_{i+1}(a_j) = p_i(a_j) + \lambda_{i+1} q_{i+1}(a_j) = p_i(a_j) = b_j$ für $j = 0, 1, \ldots, i$ und $p_{i+1}(a_{i+1}) = p_i(a_{i+1}) + \lambda_{i+1} q_{i+1}(a_{i+1}) = b_{i+1}$, wenn $\lambda_{i+1} = \frac{b_{i+1} - p_i(a_{i+1})}{q_{i+1}(a_{i+1})}$ gewählt wird.
Somit ist p_n ein Interpolationspolynom wie p in Satz 5.3.6.1, muss aufgrund der dortigen Eindeutigkeitsaussage daher mit diesem übereinstimmen.

Satz 5.3.6.2. *Seien K ein Körper, $a_0, \ldots, a_n \in K$ (*Stützstellen*) paarweise verschieden und $b_0, \ldots, b_n \in K$ (*Funktionswerte*) beliebig. Setzt man*

$$q_j(x) := \prod_{k=0}^{j-1} (x - a_k),$$

dann kann man das eindeutige Interpolationspolynom vom Grad $\leq n$ mit $p(a_i) = b_i$ für $i = 0, 1, \ldots, n$ auch rekursiv durch die folgende Prozedur erhalten: Man setzt

$$p_0(x) := b_0$$

und

$$p_{i+1}(x) := \sum_{j=0}^{i+1} \lambda_j q_j(x),$$

wobei $\lambda_0 = b_0$ und $\lambda_{j+1} = \frac{b_{j+1} - p_j(a_{j+1})}{q_{j+1}(a_{j+1})}$. Das Interpolationspolynom ist dann $p(x) := p_n(x)$.
Das Polynom p_j hängt dabei nur von den ersten $j+1$ Stützstellen $a_0, \ldots, a_j$ sowie von den ersten $j+1$ Funktionswerten $b_0, \ldots, b_j$ ab und kann außerdem aus dem Polynom $p_{j-1}(x)$ zusammen mit b_j, a_j und dem Polynom $q_j(x)$ berechnet werden. Das Polynom $q_j(x)$ hängt weiters nur von den ersten j Stützstellen $a_0, \ldots, a_{j-1}$ ab.
(Die Polynome $q_j(x)$ heißen auch Newton-Basispolynome.*)*

6. Körper

Von den klassischen, an die Zahlenbereiche angelehnten algebraischen Strukturen haben die Körper die reichhaltigste Struktur und ermöglichen entsprechend die stärksten Aussagen. Recht schnell macht man sich einen Überblick über sämtliche minimalen Körper, die sogenannten Primkörper. Bis auf Isomorphie sind sie gegeben durch die endlichen Restklassenringe modulo einer Primzahl p sowie durch den Körper der rationalen Zahlen. Alle anderen Körper sind Erweiterungen (siehe Abschnitt 6.1) von Primkörpern. Erweiterungen lassen sich verstehen als Zusammensetzung einer rein transzendenten Erweiterung, gefolgt von einer rein algebraischen, d. h. einer Adjunktion von Nullstellen von Polynomen. Solchen Adjunktionen ist Abschnitt 6.2 gewidmet. Einen vollständigen Überblick hat man über die endlichen Körper, genannt auch Galoisfelder. Ihre Kardinalität ist stets eine Primzahlpotenz p^n, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$. Umgekehrt gibt es zu jedem solchen p^n einen bis auf Isomorphie eindeutig bestimmten Körper (siehe Abschnitt 6.3).

6.1. Prim-, Unter- und Erweiterungskörper

Varietäten sind nach dem Satz von Birkhoff 4.1.7.1 charakterisiert durch ihre Abgeschlossenheit unter direkten Produkten, homomorphen Bildern und Unteralgebren. Bei Körpern verhält es sich anders: Das direkte Produkt von zwei oder mehr Körpern hat stets Nullteiler, ist also kein Körper. Homomorphe Bilder von Körpern gibt es nur die trivialen: isomorphe Bilder und den einelementigen Ring, der kein Körper ist. (Allerdings können Körper als nichttriviale homomorphe Bilder kommutativer Ringe mit 1 auftreten, wobei vor allem Polynomringe eine wichtige Rolle spielen werden.)
Nichttriviale Unterkörper hingegen kann es zuhauf geben. (Man beachte, dass es sich dabei wegen der Einschränkung bei der Bildung multiplikativer Inverser allerdings nicht um Spezialfälle des Konzepts der Unteralgebra eines Typs handelt. So ist $\mathbb{Z}$ Unteralgebra von $\mathbb{Q}$ als Ring mit 1, nicht aber Unterkörper.) Es überrascht daher nicht, dass die Theorie der Körper sehr stark um das Konzept von Unterkörpern bzw., von der anderen Seite betrachtet, von Körpererweiterungen kreist.
Die Inhalte des Abschnitts im Überblick: Jeder Körper hat einen kleinsten Unterkörper, seinen sogenannten *Primkörper* (6.1.1), lässt sich also als dessen Erweiterung auffassen. Nützlich ist es, Erweiterungskörper auch als Vektorraum über dem Grundkörper aufzufassen (6.1.2), weil dadurch mit Dimensionen gearbeitet werden kann. Von besonderem Interesse sind algebraische und transzendente Elemente (6.1.3) bzw. Körpererweiterungen (6.1.4 und 6.1.5). Jede beliebige Körpererweiterung ist eine Kombination der beiden reinen Typen, genauer: lässt sich als eine rein transzendente, gefolgt von einer rein algebraischen auffassen. Abschließend kommen wir noch auf die berühmten Konstruktionsprobleme mit Zirkel und Lineal aus der griechischen Antike zu sprechen (6.1.6), die

sich alle als unmöglich erweisen: Würfelverdoppelung, Winkeldreiteilung, Quadratur des Kreises.

6.1.1. Primkörper

Inhalt in Kurzfassung: Der Durchschnitt beliebig vieler Unterkörper eines Körpers K ist wieder ein Unterkörper. Folglich erhält man, wenn man überhaupt alle Unterkörper schneidet, den kleinsten, den man auch den sogenannten Primkörper von K nennt. Umgekehrt bedeutet das: Jeder Körper lässt sich als Erweiterung eines Primkörpers auffassen. Die Charakteristik eines Integritätsbereichs und erst recht eines Körpers kann nur 0 oder eine Primzahl p sein. Im ersten Fall erhält man einen Primkörper, der zu $\mathbb{Q}$ isomorph ist, im zweiten Fall zum Restklassenkörper $\mathbb{Z}_p$. Jeder Primkörper hat die Identität als einzigen Automorphismus.

Wir wiederholen und bauen aus:

Definition 6.1.1.1. Sei L ein Körper, $K \subseteq L$ Unteralgebra von L als Ring mit 1 und für sich genommen sogar ein Körper. Dann heißt K *Unterkörper* von L und L *Oberkörper* oder *Erweiterungskörper* von K. Zusammen bilden K und L eine sogenannte *Körpererweiterung*. Das ist in diesem Kapitel mit der Schreibweise $K \leq L$ oder auch $L : K$ gemeint.

Eine Teilmenge $K \subseteq L$ eines Körpers L ist genau dann Unterkörper von L, wenn $0_L, 1_L \in K$, $-a, a+b, ab \in K$ für alle $a, b \in K$ und $a^{-1} \in K$ für alle $a \in K^* = K \setminus \{0_L\}$.
So wie der Schnitt von Unteralgebren ist auch der Schnitt von Unterkörpern eines gegebenen Körpers K wieder ein Unterkörper.

UE 339 ▶ **Übungsaufgabe 6.1.1.2.** (V) Beweisen Sie, dass der Schnitt von Unterkörpern eines Körpers wieder ein Unterkörper ist, indem Sie Folgerung 2.2.1.10 möglichst wirkungsvoll einsetzen. Erklären Sie, warum es nicht genügt, sich ohne weitere Argumentation ausschließlich auf Folgerung 2.2.1.10 zu berufen. ◀ **UE 339**

Die Unterkörper von K bilden deshalb einen vollständigen Verband, und wir können in gewohnter Weise von *Erzeugnissen* sprechen. Insbesondere enthält dieser Verband ein kleinstes Element:

Definition 6.1.1.3. Ist K ein Körper und P der Durchschnitt sämtlicher Unterkörper von K (= der kleinste Unterkörper von K), so heißt P der *Primkörper* von K.

Vielfach nützlich ist folgende Beobachtung:

Proposition 6.1.1.4. *Ist P der Primkörper des Körpers K und $\sigma : K \to K$ ein Automorphismus von K, so gilt $\sigma(\alpha) = \alpha$ für alle $\alpha \in P$.*

UE 340 ► **Übungsaufgabe 6.1.1.5.** (V) Beweisen Sie Proposition 6.1.1.4. Gehen Sie ähnlich vor wie in Übungsaufgabe 6.1.1.2, indem Sie diesmal Proposition 2.2.1.17 möglichst wirkungsvoll einsetzen. ◄ **UE 340**

Bei Erzeugnissen ist zwischen Körpererzeugnissen und Ringerzeugnissen, die auch im Kontext der Körper nützlich sind, zu unterscheiden. Wir verwenden folgende Notation.

Definition 6.1.1.6. Ist L Oberkörper von K und $S \subseteq L$, so definieren wir den Erweiterungskörper $K(S)$ von K durch

$$K(S) := \bigcap \{E \subseteq L \mid E \text{ ist Unterkörper von } L, \text{ der } K \cup S \text{ enthält}\}.$$

Ist $S = \{\alpha_1, \ldots, \alpha_r\}$ endlich, so schreiben wir $K(S) =: K(\alpha_1, \ldots, \alpha_r)$. Eine Erweiterung L von K heißt *einfache Erweiterung von* K, wenn es ein α mit $L = K(\alpha)$ gibt.
Das *Ringerzeugnis* $K[S]$ definieren wir wie in bisherigen Kapiteln durch[1]

$$K[S] := \bigcap \{E \subseteq L \mid E \text{ ist Unterring mit 1 von } L, \text{ der } K \cup S \text{ enthält}\}.$$

Ist $S = \{\alpha_1, \ldots, \alpha_r\}$ endlich, so schreiben wir $K[S] =: K[\alpha_1, \ldots, \alpha_r]$.

Anmerkung 6.1.1.7. Es sei daran erinnert, dass wir auch für den Polynomring die Schreibweise $R[x]$ verwenden, siehe Definition 3.4.6.2. Tatsächlich ist aber der Polynomring $R[x]$ das Ringerzeugnis von $R \cup \{x\}$ im Ring der formalen Potenzreihen $R[[x]]$. Daher ist die Schreibweise $K[x]$ für das Ringerzeugnis gerechtfertigt[2].
Außerdem wird der Quotientenkörper des Polynomrings $K[x]$ wie der oben definierte Erweiterungskörper mit $K(x)$ bezeichnet, siehe Definition 3.4.6.11. Also verwenden wir die Schreibweise $K(\cdot)$ wieder für zwei scheinbar verschiedene Operationen. Tatsächlich ergibt sich aber, dass der Körper $K(x)$ aus Definition 3.4.6.11 ein Spezialfall von Definition 6.1.1.6 ist: Schreiben wir nämlich $K(\alpha)$ (wenn $\alpha \in L \geq K$) für den kleinsten Unterkörper von L, der $K \cup \{\alpha\}$ enthält, und $K\langle x\rangle$ für den Quotientenkörper von $K[x]$, dann lässt sich jedes Element aus $K\langle x\rangle$ als Quotient $p(x)/q(x)$ mit $p(x), q(x) \in K[x]$, $q(x) \neq 0$ schreiben.
Offenbar enthält $K\langle x\rangle$ den gesamten Ring $K[x]$ und ist daher insbesondere eine Obermenge von $K \cup \{x\} \subseteq K[x]$. Sei umgekehrt $E \leq K\langle x\rangle$ ein beliebiger Unterkörper, der $K \cup \{x\}$ enthält, dann muss E zunächst ganz $K[x]$, aber dann auch ganz $K\langle x\rangle$ enthalten. Somit ist $K\langle x\rangle$ der kleinste Unterkörper von $K\langle x\rangle$, der $K \cup \{x\}$ enthält, also $K\langle x\rangle = K(x)$.
Daher ist auch die Schreibweise $K(x)$ an Stelle von $K\langle x\rangle$ gerechtfertigt.

In Unterabschnitt 3.4.3 wurde für einen Ring R mit Einselement 1_R der eindeutig bestimmte Homomorphismus $\varphi_R = \varphi\colon \mathbb{Z} \to R$ mit $1 \mapsto 1_R$ und sein Bild $R_0 = \varphi_R(\mathbb{Z})$ betrachtet. Der Kern $\ker \varphi_R$ ist ein Ideal im Hauptidealring $\mathbb{Z}$, wird also von einem Element $m \in \mathbb{N}$ erzeugt. Definitionsgemäß ist dieses m die Charakteristik von R, symbolisch $\operatorname{char} R$.

[1] Hier verwenden wir ein anderes Symbol als früher.
[2] Wir haben sie sinngemäß auch bereits bei den quadratischen Zahlringen $\mathbb{Z}[\sqrt{D}]$ verwendet.

Wir wollen nun annehmen, dass R nullteilerfrei ist mit $\operatorname{char} R = m$. Dann ist auch sein Unterring $R_0 \cong \mathbb{Z}/m\mathbb{Z}$ nullteilerfrei, was wiederum nur möglich ist, wenn $m = p \in \mathbb{P}$ oder $m = 0$. Im ersten Fall ist R_0 sogar ein Körper. Weil R_0 als Ring von 1_R erzeugt wird, handelt es sich dann um die kleinste Unteralgebra von R als Ring mit 1 und erst recht um den kleinsten Unterkörper. Im zweiten Fall, nämlich bei $\operatorname{char} R = 0$, ist $R_0 \cong \mathbb{Z}$. Ist R wieder ein Körper, so enthält R eine isomorphe Kopie Q_R des Quotientenkörpers von $\mathbb{Z}$, also von $\mathbb{Q}$. Dabei erhält man sämtliche Elemente von Q_R, indem man alle Brüche aus Elementen von R_0 mit Nenner $\neq 0_R$ bildet (siehe Proposition 3.4.5.9). Wir fassen unsere Erkenntnisse für Körper zusammen:

Satz 6.1.1.8. *Die Charakteristik eines Integritätsbereichs oder gar Körpers ist entweder* 0 *oder eine Primzahl* p*. Jeder Körper* $(K, +, 0, -, \cdot, 1)$ *enthält einen kleinsten Unterkörper* P*, seinen sogenannten* Primkörper*. Je nach Charakteristik* $\operatorname{char} K$ *sind folgende Fälle zu unterscheiden:*

1. *Für* $\operatorname{char} K = p \in \mathbb{P}$ *ist* $P = \varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ *isomorph zum Restklassenkörper modulo* p*.*

2. *Für* $\operatorname{char} K = 0$ *ist* $P \cong \mathbb{Q}$ *isomorph zum Körper* $\mathbb{Q}$ *der rationalen Zahlen, und es gilt* $P = \{ab^{-1} \mid a, b \in \varphi(\mathbb{Z}),\ b \neq 0_R\}$*.*

Dabei bezeichnet φ *den Homomorphismus* $\varphi\colon \mathbb{Z} \to R$*,* $k \mapsto k \cdot 1_R$ *aus Lemma 3.4.3.1.*

Klarerweise können endliche Körper nur Primzahlcharakteristik haben. Die Umkehrung gilt aber nicht, wie der unendliche Körper $\mathbb{Z}_p(x)$ der gebrochen rationalen Funktionen über $\mathbb{Z}_p$ beweist. Wir werden aber auch noch ein anderes wichtiges Beispiel kennen lernen, nämlich den algebraischen Abschluss $\mathrm{GF}(p^\infty)$ der endlichen Körper mit Charakteristik $p \in \mathbb{P}$.

6.1.2. Das Vektorraumargument

Inhalt in Kurzfassung: Jeder Erweiterungskörper lässt sich auch als Vektorraum über dem Grundkörper auffassen. Bei dieser Sichtweise schwächt man zwar die Struktur ab, gleichzeitig wird aber der Begriff der Dimension auch für Körpererweiterungen verfügbar. Der äußerst nützliche Gradsatz besagt, dass sich bei iterierten Körpererweiterungen Dimensionen aufmultiplizieren.

Ist L Oberkörper von K, dann ist L auch Vektorraum über K mit den Operationen

$$\begin{aligned} a + b &\ \ldots \text{ Summe in } L\ (a, b \in L), \\ \lambda a &\ \ldots \text{ Produkt in } L\ (a \in L,\ \lambda \in K). \end{aligned}$$

Das gilt auch, wenn man auf die Kommutativität verzichtet und zulässt, dass K ein Unterschiefkörper (Unterdivisionsring) von L ist. In jedem Fall existiert daher eine Vektorraumbasis von L über K. Diese bestimmt die Dimension $\dim_K L$. Wir definieren:

Definition 6.1.2.1. Für eine Körpererweiterung $K \leq L$ nennt man die Dimension $[L : K] := \dim_K L$ von L als Vektorraum über K den *Grad der Körpererweiterung* $K \leq L$ bzw. von L über K. Ist $[L : K] < \infty$, so heißt L eine *endlichdimensionale Erweiterung* von K. Wegen Folgerung 1.3.3.2 ist auch im Fall unendlicher Basen deren Kardinalität und somit die Dimension von L (dann als unendliche Kardinalität) wohldefiniert. Somit kann unmissverständlich auch von *unendlichdimensionalen Erweiterungen* gesprochen werden.

Wenn $K \leq E \leq L$, dann ist $[L : E] \leq [L : K]$, weil jedes Erzeugendensystem des K-Vektorraums L auch den E-Vektorraum L erzeugt. Überdies ist $[E : K] \leq [L : K]$, weil E Untervektorraum des K-Vektorraums L ist. Weitreichende Konsequenzen hat der *Gradsatz*, der diese Beobachtungen verallgemeinert:

Satz 6.1.2.2 (Gradsatz)**.** *Für $K \leq E \leq L$ (als Körper oder auch als Schiefkörper) gilt*

$$[L : K] = [L : E] \cdot [E : K].$$

UE 341 ► **Übungsaufgabe 6.1.2.3.** (V,W) Beweisen Sie den Gradsatz, indem Sie zeigen: Ist die Familie $(a_i)_{i\in I}$ eine Basis von E über K, und die Familie $(b_j)_{j\in J}$ eine Basis von L über E, so ist die Familie $(a_i b_j)_{(i,j)\in I\times J}$ eine Basis von L über K. (Achtung: Ihre Argumentation muss auch für unendliches I und J gelten.) ◄ **UE 341**

UE 342 ► **Übungsaufgabe 6.1.2.4.** (F) Wir fassen $\mathbb{R}$ als Vektorraum über dem Körper $\mathbb{Q}$ auf. Zeigen Sie, dass $\{1, \sqrt{5}\}$ eine linear unabhängige Menge ist. Bestimmen Sie weiters den Grad $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$ von $\mathbb{Q}(\sqrt{5})$ über $\mathbb{Q}$. ◄ **UE 342**

6.1.3. Algebraische und transzendente Elemente

Inhalt in Kurzfassung: Für ein Element α eines Erweiterungskörpers sind in Bezug auf den Grundkörper K zwei grundsätzlich verschiedene Möglichkeiten denkbar. Im ersten Fall besteht eine algebraische Beziehung zwischen α und Elementen aus K. Dann gibt es auch eine einfachste solche Beziehung, nämlich $f(\alpha) = 0$, wobei $f \in K[x] \setminus \{0\}$ das normierte Polynom von kleinstem Grad über K mit dieser Eigenschaft ist, das sogenannte Minimalpolynom von α. Dieses ist stets irreduzibel. Alle weiteren Polynome über K mit α als Nullstelle sind Vielfache des Minimalpolynoms. In diesem Fall heißt α algebraisch über K. Im anderen Fall, also wenn α nicht Nullstelle eines $f \in K[x] \setminus \{0\}$ ist, heißt α transzendent über K. In beiden Fällen lässt sich die Struktur des Erweiterungskörpers einfach beschreiben: $K(\alpha) \cong K[x]/(f)$ (Faktorisierung des Polynomrings nach dem vom Minimalpolynom erzeugten Hauptideal) im algebraischen Fall und $K(\alpha) \cong K(x)$ (Körper der gebrochen rationalen Funktionen über K) im transzendenten Fall. Auch einige verfeinerte Aussagen in diese Richtung, die später noch verwendet werden, sind Inhalt dieses Unterabschnitts.

Sei $\alpha \in L$, L Körper, und $K \leq L$ ein Unterkörper. Das Verhalten von α in Bezug auf K lässt sich mit Hilfe des Polynomringes $K[x]$ und des durch α induzierten Einsetzungshomomorphismus sehr gut verstehen. Der Hintergrund ist die universelle Eigenschaft der Polynomalgebra, wie sie in Proposition 3.4.6.16 bzw. in Abschnitt 4.2 behandelt wurde. Im Kontext der Körpertheorie ist es zunächst wichtig, sich zu vergegenwärtigen:

Definition 6.1.3.1. Seien $K \leq L$ Körper, und sei $\alpha \in L$. Sei $\varphi_\alpha \colon K[x] \to L$ der natürliche *Einsetzungshomomorphismus*:

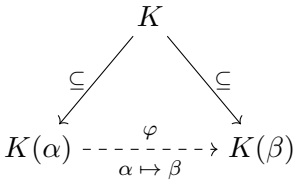
$$a_0 + a_1 x + \cdots + a_n x^n \quad \mapsto \quad a_0 + a_1 \alpha + \cdots + a_n \alpha^n.$$

Offenbar ist die Wertemenge von φ_α genau das Ringerzeugnis $K[\alpha]$, der kleinste $K \cup \{\alpha\}$ enthaltende Unterring von L.
Aus dem Homomorphiesatz für Ringe wissen wir, dass der Kern $\ker(\varphi_\alpha)$ von φ_α ein Ideal von $K[x]$ ist, und dass $K[\alpha] \cong K[x]/\ker(\varphi_\alpha)$. Als Unterring von L ist $K[\alpha]$ ein Integritätsbereich, also ist $\ker(\varphi_\alpha)$ nach Proposition 3.4.2.4 ein Primideal. Weil der Polynomring $K[x]$ über dem Körper K ein Hauptidealring ist, gibt es ein erzeugendes Element $m = m_\alpha = m_\alpha(x)$ von $\ker(\varphi_\alpha)$. Ist $m = 0$, so ist φ_α injektiv und man nennt α *transzendent*, andernfalls *algebraisch*. Man kann die Definition explizit auch so fassen:

Definition 6.1.3.2. Sei L Oberkörper von K und $\alpha \in L$. Das Element α heißt *algebraisch* über K, wenn es ein $f \in K[x] \setminus \{0\}$ gibt mit $f(\alpha) = 0$. Ist n der minimale Grad eines solchen f, so sagt man auch, α ist *algebraisch vom Grad n*. Ist α nicht algebraisch, so heißt α *transzendent* über K. Im algebraischen Fall gibt es unter allen Polynomen, die $\ker(\varphi_\alpha)$ erzeugen, genau ein normiertes, d. h. mit höchstem Koeffizienten 1. Dieses Polynom $m(x) \in K[x]$ nennt man das *Minimalpolynom* von α über K.

Zunächst zum transzendenten Fall:

Satz 6.1.3.3 (Einfache transzendente Erweiterungen)**.** *Sei $K \leq L$ und sei $\alpha \in L$ transzendent über K. Dann ist $K(x) \cong K(\alpha)$ (wobei $K(x)$ der Quotientenkörper des Polynomrings $K[x]$ ist). Es gibt einen eindeutig bestimmten Isomorphismus $\varphi \colon K(x) \to K(\alpha)$, der K punktweise fest lässt und x auf α abbildet.*
Insbesondere gilt: Seien $K \leq L_\alpha$ und $K \leq L_\beta$ irgendwelche Körpererweiterungen und $\alpha \in L_\alpha$ sowie $\beta \in L_\beta$ transzendent über K. Für die Körper $K(\alpha) \leq L_\alpha$ und $K(\beta) \leq L_\beta$ gilt dann $K(\alpha) \cong K(\beta)$, mit einem eindeutigen Isomorphismus, der K punktweise fest lässt und α auf β abbildet.



Beweis. Wir definieren $\varphi : K(x) \to K(\alpha)$ durch $\frac{p(x)}{q(x)} \mapsto \frac{p(\alpha)}{q(\alpha)}$ – hier ist entscheidend, dass $q(\alpha) \neq 0$ wegen der Transzendenz von α. Diese Abbildung ist wohldefiniert: Wenn $\frac{p(x)}{q(x)} =$

$\frac{p'(x)}{q'(x)}$, d. h. $p(x)q'(x) = p'(x)q(x)$, dann ist $p(x)q'(x) - p'(x)q(x)$ das Nullpolynom, womit insbesondere $p(\alpha)q'(\alpha) - p'(\alpha)q(\alpha) = 0$, also $\frac{p(\alpha)}{q(\alpha)} = \frac{p'(\alpha)}{q'(\alpha)}$. Man rechnet unmittelbar nach, dass φ ein Homomorphismus ist. Die Injektivität folgt wieder aus der Transzendenz von α: wenn $\frac{p(\alpha)}{q(\alpha)} = 0$, dann ist $p(\alpha) = 0$ und daher $p(x)$ das Nullpolynom. Die Surjektivität ist klar (siehe auch Übungsaufgabe 2.2.1.21). Da $K(x)$ als Körper von $K \cup \{x\}$ erzeugt wird, ergibt sich auch die behauptete Eindeutigkeit von φ. □

Jetzt zum algebraischen Fall:

Satz 6.1.3.4 (Einfache algebraische Erweiterungen)**.** *Sei $K \leq L$ und $\alpha \in L$ algebraisch über K. Sei m das Minimalpolynom von α über K und $k = \operatorname{grad}(m)$. Dann gilt:*

(1) *$m(x)$ ist das normierte Polynom über K kleinsten Grades mit $m(\alpha) = 0$. Außerdem ist $m(x)$ irreduzibel, und zwar das eindeutig bestimmte irreduzible normierte Polynom in $K[x]$ mit Nullstelle α.*

(2) *Die Abbildung*

$$\psi : a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + (m) \quad \mapsto \quad a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$$

ist wohldefiniert und ein Isomorphismus $K[x]/(m) \cong K[\alpha]$, und zwar der einzige mit $x + (m) \mapsto \alpha$ und $c + (m) \mapsto c$ für alle $c \in K$.

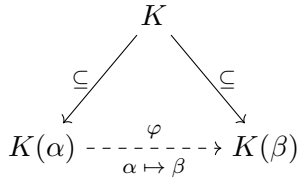
(3) *$K(\alpha) = K[\alpha]$.*

(4) *Jedes Element $\beta \in K(\alpha)$ lässt sich eindeutig in der Form $\beta = a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1}$ mit $a_0, \ldots, a_{k-1} \in K$ darstellen.*

(5) *Die Elemente $1 = \alpha^0, \alpha = \alpha^1, \alpha^2, \ldots, \alpha^{k-1}$ bilden eine Basis des Vektorraums $K(\alpha)$ über K.*

(6) *$[K(\alpha) : K] = k = \operatorname{grad}(m)$.*

(7) *Wenn $\alpha, \beta \in L$ dasselbe Minimalpolynom $m(x)$ über K haben, dann gibt es einen eindeutigen Isomorphismus $\varphi\colon K(\alpha) \to K(\beta)$ mit $\varphi(\alpha) = \beta$ und $\varphi(c) = c$ für alle $c \in K$.*



Beweis.

(1) Nach Definition ist m jenes (eindeutig bestimmte) normierte Polynom, das $\ker(\varphi_\alpha)$ erzeugt, wobei φ_α der Einsetzungshomomorphismus bezüglich α ist. Also besteht $\ker(\varphi_\alpha)$ aus den Polynomen über K mit Nullstelle α, und der normierte Erzeuger m ist das normierte Polynom aus $\ker(\varphi_\alpha)$ mit dem kleinsten Grad (siehe auch den Beweis von Satz 5.2.3.4).

Wir haben oben schon überlegt, dass $\ker(\varphi_\alpha) = (m)$ ein Primideal in $K[x]$ ist, also muss m ein Primelement sein. Im (Euklidischen, insbesondere faktoriellen) Ring $K[x]$ ist das gleichbedeutend damit, dass m irreduzibel ist. Wenn schließlich $m' \in K[x]$ normiert und irreduzibel ist mit $m'(\alpha) = 0$, dann ist m' in $\ker(\varphi_\alpha) = (m)$ enthalten, also ein Vielfaches von m. Da m' irreduzibel ist und m, m' normiert sind, folgt $m = m'$.

(2) Aus dem Homomorphiesatz folgt, dass $p(x) + (m) \mapsto p(\alpha)$ ein Isomorphismus $K[x]/(m) \to K[\alpha]$ ist. Für die erste Aussage bleibt noch zu zeigen, dass man jede Äquivalenzklasse $p(x) + (m)$ einen Repräsentanten $a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + (m)$ hat – dies ergibt sich unmittelbar aus der Division mit Rest (Satz 3.4.6.8). Die Eindeutigkeitsaussage folgt daraus, dass $K[x]/(m)$ von $x + (m)$ zusammen mit den Elementen $c + (m)$, $c \in K$, erzeugt wird.

(3) Da $m(x)$ irreduzibel ist, ist $K[x]/(m)$ sogar ein Körper, also ist auch $K[\alpha]$ ein Körper und wir erhalten $K[\alpha] = K(\alpha)$.

(4) bis (6) folgen aus (2).

(7) Analog zum Isomorphismus ψ_α aus Punkt (2) gibt es den ausgehend von β definierten Isomorphismus $\psi_\beta : K[x]/(m) \to K(\beta)$. Die Verkettung $\varphi := \psi_\beta \circ \psi_\alpha^{-1} : K(\alpha) \to K(\beta)$, $a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1} \mapsto a_0 + a_1\beta + \cdots + a_{k-1}\beta^{k-1}$ ist der gesuchte Isomorphismus. Analog zu oben folgt die Eindeutigkeitsaussage daraus, dass $K(\alpha)$ von $K \cup \{\alpha\}$ erzeugt wird. □

Die in (7) vorausgesetzte Eigenschaft spielt oft eine wichtige Rolle.

Definition 6.1.3.5. Sei $K \leq L$ eine Körperweiterung und seien $\alpha, \beta \in L$. Wenn α und β algebraisch über K sind und dasselbe Minimalpolynom über K haben, so heißen α und β *konjugiert* über K.

Für eine spätere Anwendung formulieren wir auch folgende Variante von (7) explizit:

Proposition 6.1.3.6. *Sei $\varphi\colon K_1 \to K_2$ ein Körperisomorphismus und sei $\varphi_x\colon K_1[x] \to K_2[x]$ der eindeutig bestimmte Isomorphismus, der auf den konstanten Polynomen mit φ übereinstimmt und $x \in K_1[x]$ auf $x \in K_2[x]$ abbildet. Weiters seien $K_1 \leq L_1$ und $K_2 \leq L_2$ Körpererweiterungen. Das Element $\alpha_1 \in L_1$ sei algebraisch über K_1 mit Minimalpolynom m_1, und $\alpha_2 \in L_2$ sei eine Nullstelle von $m_2 := \varphi_x(m_1)$.*
Dann ist m_2 irreduzibel und es gibt einen eindeutigen Isomorphismus $\psi\colon K_1(\alpha_1) \to K_2(\alpha_2)$, der φ fortsetzt und α_1 auf α_2 abbildet.

$$\begin{array}{ccc} K_1 & \xrightarrow{\ \varphi\ } & K_2 \\ \subseteq\downarrow & & \downarrow\subseteq \\ K_1(\alpha_1) & \overset{\psi}{\underset{\alpha_1 \mapsto \alpha_2}{\dashrightarrow}} & K_2(\alpha_2) \end{array}$$

UE 343 ▶ **Übungsaufgabe 6.1.3.7.** (V) Zeigen Sie Proposition 6.1.3.6. ◀ **UE 343**

Beispiele 6.1.3.8.

(1) Für $\alpha \in K$ ist $x - \alpha$ Minimalpolynom von α über K.

(2) $x^2 - 2$ ist Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$.

(3) $x^3 - 3$ ist Minimalpolynom von $\sqrt[3]{3}$ über $\mathbb{Q}$.

(4) $x^2 + 1$ ist Minimalpolynom von i über $\mathbb{R}$ und auch über $\mathbb{Q}$.

(5) Sei $\alpha := \frac{\sqrt{2}}{2}(1+i)$. Dann ist $\alpha^2 = i$, $\alpha^4 = -1$. Das Minimalpolynom von α über $\mathbb{R}$ ist $x^2 - \sqrt{2}x + 1$, über $\mathbb{Q}$ ist es $x^4 + 1$.

(6) Das Minimalpolynom der Kreiszahl π über $\mathbb{Q}(\pi^2)$ ist $x^2 - \pi^2$, über $\mathbb{Q}(\pi)$ ist es $x - \pi$, und über $\mathbb{Q}$ hat π kein Minimalpolynom, weil π transzendent ist. Analoges gilt für die ebenfalls transzendente Eulersche Zahl e. Für die Beweise der Transzendenz von π und e müssen wir auf zahlentheoretische Lehrveranstaltungen verweisen. Hier würden sie den Rahmen sprengen.

UE 344 ▶ **Übungsaufgabe 6.1.3.9.** (F) Sei p eine Primzahl. Zeigen Sie, dass das Polynom $q(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ (das man auch als $\frac{x^p-1}{x-1}$ schreiben kann) in $\mathbb{Z}[x]$ irreduzibel ist.
Hinweis: Betrachten Sie stattdessen das Polynom $r(x) = q(x+1)$ und verwenden Sie Proposition 5.3.2.7. ◀ **UE 344**

UE 345 ▶ **Übungsaufgabe 6.1.3.10.** (F) Geben Sie ein irreduzibles Polynom $p(x) \in \mathbb{Z}[x]$ vom Grad 6 an, welches die Nullstelle

$$\cos\frac{2\pi}{7} + i\,\sin\frac{2\pi}{7}$$

hat. Finden Sie alle Nullstellen dieses Polynoms. (Hinweis: Siehe Übungsaufgabe 6.1.3.9) ◀ **UE 345**

UE 346 ▶ **Übungsaufgabe 6.1.3.11.** (B) Sei $p \in \mathbb{Z}$ eine Primzahl. Wir betrachten das Polynom $f(x) := x^3 - p$ zunächst über $\mathbb{Q}$.

(1) Geben Sie sämtliche Nullstellen von f in der Form $a + ib$ mit $a, b \in \mathbb{R}$ an und skizzieren Sie diese in der komplexen Zahlenebene.

(2) Zeigen Sie, dass f über $\mathbb{Q}$ (d. h. im Ring $\mathbb{Q}[x]$) irreduzibel ist.

(3) Sei L ein Körper mit $\mathbb{Q} \leq L$ und $\alpha \in L$ mit $\alpha^3 = p$. Zeigen Sie, dass das Polynom $(x^3 - p)/(x - \alpha) = x^2 + \alpha x + \alpha^2$ über $\mathbb{Q}(\alpha)$ irreduzibel ist. (Hinweis: Betrachten Sie zunächst den Fall $\alpha = \sqrt[3]{p} \in \mathbb{R}$ und überlegen Sie dann, dass es genügt, diesen Fall zu betrachten.) ◀ **UE 346**

UE 347 ► **Übungsaufgabe 6.1.3.12.** (F) Für $a \in \mathbb{R}$ sei $\varphi_a \colon \mathbb{Z}[x] \to \mathbb{R}$ durch $\varphi_a(p(x)) = p(a)$ ◄ **UE 347** definiert. Finden Sie Polynome $p(x)$, $q(x)$, $r(x) \in \mathbb{Z}[x]$, sodass

- $\ker(\varphi_0) = (p(x))$,
- $\ker(\varphi_1) = (q(x))$,
- $\ker(\varphi_{\sqrt{2}}) = (r(x))$.

6.1.4. Algebraische Erweiterungen und endliche Dimension

Inhalt in Kurzfassung: Auf den ersten Blick ist überhaupt nicht klar, dass die Iteration rein algebraischer Körpererweiterungen stets wieder rein algebraische Erweiterungen erzeugt. Verständlich wird dies aber sehr schnell mit Hilfe des Dimensionsarguments, weil nämlich Endlichdimensionalität und Algebraizität sehr eng miteinander zusammenhängen. Denn die Iteration endlichdimensionaler Erweiterungen ist wegen des Gradsatzes in offensichtlicher Weise wieder endlichdimensional.

Ist wieder L ein Körper, $K \leq L$ ein Unterkörper und $\alpha \in L$ algebraisch über K mit Minimalpolynom m über K, so haben wir gesehen, dass der von K und α erzeugte Unterkörper $K(\alpha) = K[\alpha] \leq L$ endliche Dimension $[K(\alpha) : K] = \operatorname{grad}(m)$ über K hat. Es gilt aber auch die Umkehrung im folgenden Sinn: Ist $[L : K] = n < \infty$ und $\alpha \in L$, so muss zwischen den $n + 1$ Elementen $1, \alpha, \alpha^2, \ldots, \alpha^n$ eine lineare Abhängigkeit

$$\sum_{i=0}^{n} a_i \alpha^i = 0$$

mit Koeffizienten $a_i \in K$ bestehen. Also ist $f(\alpha) = 0$ für das Polynom $f(x) := \sum_{i=0}^{n} a_i x^i$ mit $a_i \in K$. Folglich ist α algebraisch über K. Also ist jede endlichdimensionale Körpererweiterung $K \leq L$ *algebraisch* im folgenden Sinne:

Definition 6.1.4.1. Eine Körpererweiterung $K \leq L$ heißt *algebraisch*, wenn alle $\alpha \in L$ algebraisch über K sind.

Aufgrund des Gradsatzes 6.1.2.2 führt endliche Iteration von endlichdimensionalen Erweiterungen immer wieder nur zu endlichdimensionalen, also algebraischen Erweiterungen. Also lässt sich auch folgern: Endliche Iteration von einfachen algebraischen Erweiterungen führt stets zu algebraischen Erweiterungen. Explizit formuliert: Wenn α algebraisch über K und β algebraisch über $K(\alpha)$ ist, dann ist $K \leq K(\alpha, \beta)$ eine algebraische Erweiterung.
Wir fassen zusammen und ergänzen:

Satz 6.1.4.2. *Sei $K \leq L$. Algebraizität und endliche Dimension von Körpererweiterungen hängen zusammen bzw. vererben sich in folgender Weise:*

(1) *Ist $[L : K] < \infty$, so ist L algebraisch über K (d. h., alle Elemente von L sind algebraisch über K).*

(2) *Genau dann ist $\alpha \in L$ algebraisch über K, wenn $[K(\alpha) : K] < \infty$.*

(3) *Ist $K \leq L \leq M$, L algebraisch über K und M algebraisch über L, so ist M algebraisch über K.*

(4) *Die Menge aller über K algebraischen Elemente in L bildet einen Unterkörper von L.*

Beweis.

(1) Das haben wir gerade bewiesen.

(2) Man muss nur die Sätze 6.1.3.3 und 6.1.3.4 kombinieren.

(3) Sei $\alpha \in M$. Dann ist α algebraisch über L, also gibt es ein Minimalpolynom von α mit Koeffizienten $\beta_0, \ldots, \beta_n \in L$, die selbst algebraisch über K sind. Also liegt α in einer Erweiterung von K, die durch endlich viele einfache algebraische Erweiterungen zustande kommt: nämlich zunächst um β_0, dann um β_1, …, um β_n und zuletzt um α selbst. Also ist α nach dem obigen algebraisch auch über K.

(4) Seien $\alpha, \beta \in L$ algebraisch über K. Dann liegen α und β gemeinsam in der Erweiterung $K(\alpha, \beta)$ von K, die durch endlich viele einfache algebraische Erweiterungen zustande kommt: nämlich zuerst um α und dann um β. Nach dem obigen ist $K \leq K(\alpha, \beta)$ eine algebraische Erweiterung. Somit sind $\alpha + \beta$, $-\alpha$, $\alpha \cdot \beta$ und, wenn α ungleich 0 ist, α^{-1} als Elemente von $K(\alpha, \beta)$ allesamt algebraisch über K. Schließlich sind $0, 1 \in K$ selbstverständlich algebraisch über K.

□

UE 348 ▶ Übungsaufgabe 6.1.4.3. (B) Man gebe das Minimalpolynom von ◀ **UE 348**

(1) $\sqrt{2} + \sqrt{3}$,

(2) $\sqrt{3} + i$

über $\mathbb{Q}$ an.

UE 349 ▶ Übungsaufgabe 6.1.4.4. (B) Man bestimme den Grad von $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$ über $\mathbb{Q}$. ◀ **UE 349**

UE 350 ▶ Übungsaufgabe 6.1.4.5. (F) Seien $\alpha, \beta, \gamma \in \mathbb{C}$ die Nullstellen von $x^3 - 2$. Man bestimme den Grad des Körpers $\mathbb{Q}(\alpha, \beta, \gamma)$ (des Zerfällungskörpers, siehe Unterabschnitt 6.2.1) über $\mathbb{Q}$. ◀ **UE 350**

Hinweis: Übungsaufgabe 6.1.3.11.

UE 351 ▶ Übungsaufgabe 6.1.4.6. (E) Eine komplexe Zahl α heißt *ganz algebraisch*, wenn es ein ganzzahliges und monisches (normiertes) Polynom $p(x) = \sum_{i=0}^{n} a_i x^i$ (also mit $a_i \in \mathbb{Z}$ für $i = 0, \ldots, n$ und mit $a_n = 1$) mit $p(\alpha) = 0$ gibt. ◀ **UE 351**

(1) Zeigen Sie, dass $\alpha := \frac{1}{2}(1 + \sqrt{5})$ ganz algebraisch ist.

(2) Zeigen Sie, dass eine rationale Zahl genau dann ganz algebraisch ist, wenn sie in $\mathbb{Z}$ liegt. Folgern Sie daraus, dass für $m, n \in \mathbb{N}^+$ die Wurzel $\sqrt[n]{m}$ entweder ganz oder irrational ist.

Anmerkung 6.1.4.7. Man kann zeigen, dass die Menge der ganzen algebraischen Zahlen einen Unterring von $\mathbb{C}$ bildet, siehe Satz 10.2.2.2. Die Methode ähnelt dem Beweis, dass die algebraischen Zahlen einen Körper bilden (siehe Satz 6.1.4.2), wobei die Rolle der endlichen Dimension von Körpererweiterungen übernommen wird von der endlichen Erzeugtheit von Moduln.

Nachdem wir uns mit algebraischen Körpererweiterungen einigermaßen vertraut gemacht haben, wenden wir uns nun den transzendenten zu.

6.1.5. Transzendente Körpererweiterungen

Inhalt in Kurzfassung: Rein transzendente Körpererweiterungen E eines Grundkörpers K lassen sich (bis auf Isomorphie) recht klar beschreiben, nämlich als Körper gebrochen rationaler Funktionen $K(X)$ in einer geeigneten Menge X von Variablen. Aber auch beliebige Körpererweiterungen werden dadurch zugänglich. Und zwar lassen sie sich beschreiben als Iteration einer vorangehenden rein transzendenten Körpererweiterung, gefolgt von einer rein algebraischen Erweiterung. Dabei geht es lediglich darum, eine sogenannte Transzendenzbasis, d. h. eine maximale algebraisch unabhängige Menge, zu finden. Das gelingt ganz ähnlich (z. B. mit Hilfe des Lemmas von Zorn) wie bei dem Satz aus der Linearen Algebra, dass sich linear unabhängige Mengen in Vektorräumen zu Basen ergänzen lassen. Es gilt auch ein Analogon zum Austauschsatz von Steinitz, wonach (hier für den endlichen Fall bewiesen) je zwei Transzendenzbasen gleich viele Elemente haben, weshalb der Begriff des Transzendenzgrades einer Körpererweiterung wohldefiniert ist.

Die folgenden Begriffsbildungen lassen sich am besten in weitgehender Analogie zu den Konzepten rund um lineare (Un-)Abhängigkeit, siehe Unterabschnitt 1.3.3, verstehen.

Definition 6.1.5.1. Ist $K \leq E$ eine Körpererweiterung, so heißt eine Menge $S \subseteq E$ *algebraisch abhängig* über K, falls es ein positives $n \in \mathbb{N}$, ein $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ und paarweise verschiedene $s_1, \ldots, s_n \in S$ gibt mit $f(s_1, \ldots, s_n) = 0$. Andernfalls heißt S *algebraisch unabhängig*.
Ist $E = K(S)$ mit einer algebraisch unabhängigen Menge S, so heißt $K \leq E$ eine *rein transzendente Erweiterung*.
Eine Menge $S \subseteq E$ heißt *Transzendenzbasis* von E über K, falls S algebraisch unabhängig und mit dieser Eigenschaft maximal ist.

Nicht schwer ist der Beweis folgender Verallgemeinerung von Satz 6.1.3.3:

Proposition 6.1.5.2. *Seien L_1 und L_2 Erweiterungskörper von K, und seien $S_1 \subseteq L_1$ und $S_2 \subseteq L_2$ jeweils algebraisch unabhängig über K. Gilt überdies $|S_1| = |S_2|$ vermittels einer Bijektion $\varphi : S_1 \to S_2$, dann folgt $K(S_1) \cong K(S_2)$ vermittels eines eindeutig bestimmten Isomorphismus, der sowohl die Identität auf K als auch φ fortsetzt.*

UE 352 ▶ **Übungsaufgabe 6.1.5.3.** (V) Beweisen Sie Proposition 6.1.5.2. ◀ **UE 352**

Lemma 6.1.5.4. *Sei $K \leq E$ eine Körpererweiterung, und sei $S \subseteq E$. Dann sind die folgenden Aussagen äquivalent:*

(1) *S ist maximale algebraisch unabhängige Teilmenge.*

(2) *E ist algebraisch über $K(S)$ und S ist minimal (bezüglich $\subseteq$) mit dieser Eigenschaft.*

(3) *S ist algebraisch unabhängig und E ist algebraisch über $K(S)$.*

UE 353 ▶ **Übungsaufgabe 6.1.5.5.** (F) Beweisen Sie Lemma 6.1.5.4. ◀ **UE 353**

Satz 6.1.5.6. *Für jede Körpererweiterung $K \leq E$ existiert eine Transzendenzbasis $S \subseteq K$. Folglich lässt sich $K \leq E$ als rein transzendente Erweiterung $K \leq K(S)$, gefolgt von der algebraischen Erweiterung $K(S) \leq E$ auffassen.*

Beweis. Analog zum Beweis der Existenz einer Basis in Vektorräumen: Das System aller algebraisch unabhängigen Teilmengen bildet eine $\subseteq$-Halbordnung und ist abgeschlossen bezüglich der Vereinigung von Ketten. Nach dem Lemma von Zorn (A.4.2.4) gibt es daher ein maximales Element.[3] Jedes solche maximale Element ist eine Transzendenzbasis. Damit ist die erste Behauptung bewiesen. Die zweite folgt daraus in offensichtlicher Weise. □

Klarerweise ist eine Transzendenzbasis S genau dann leer, wenn $K \leq E$ algebraisch ist. Wir modifizieren nun die Sätze und Beweise über Basen und die Dimension eines Vektorraums aus Unterabschnitt 1.3.2 so, dass wir analoge Sätze über Transzendenzbasen und den Transzendenzgrad bekommen.

Definition 6.1.5.7. Für jede Körpererweiterung $K \leq E$ und jede Teilmenge $A \subseteq E$ schreiben wir $[A]$ für die *algebraische Hülle* von A über K, das heißt: für die Menge aller Elemente $e \in E$, die über $K(A)$ algebraisch sind.
Wenn $E = [K(A)]$ ist, also wenn E algebraisch über $K(A)$ ist, dann nennen wir A ein *algebraisches Erzeugendensystem* für E über K.

Ähnlich wie im Fall der linearen Hülle gilt $[[A]] = [A]$ für alle A (siehe Satz 6.1.4.2).

Lemma 6.1.5.8 (Algebraisches Austauschlemma)**.** *Sei $K \leq E$ Körpererweiterung, $A \subseteq E$, $b, c \in E$. Wenn $c \in [A \cup \{b\}]$ aber $c \notin [A]$ gilt, dann ist $b \in [A \cup \{c\}]$.*

Beweis. Sei $f(x)$ ein Polynom in $K(A \cup \{b\})[x] \setminus \{0\}$ mit $f(c) = 0$. Nach Multiplikation mit einem geeigneten Element von $K[A \cup \{b\}]$ (gemeinsamer Nenner der Koeffizienten) erhalten wir ein Polynom $g(x) \in K[A \cup \{b\}][x] \setminus \{0\}$ mit Nullstelle c. Man findet ein Polynom $\tilde{g}(x, y) \in K[A][x, y] \setminus \{0\}$ mit $\tilde{g}(x, b) = g(x)$, also $\tilde{g}(c, b) = 0$. Das Polynom

[3] Alternativ: Das System aller algebraisch unabhängigen Teilmengen hat offensichtlich endlichen Charakter, daher nach dem Lemma von Teichmüller-Tukey (A.4.2.5) ein maximales Element.

$\tilde{g}(x,y)$, aufgefasst als Element des Polynomrings $K[x][y]$ über dem Ring $K[x]$, hat (in Bezug auf y) mindestens Grad 1 (denn sonst wäre $\tilde{g}(x,b)$ ein Polynom über $K[A]$ mit $\tilde{g}(c,b)=0$, also $c\in[A]$).
Daher ist $\hat{g}(y):=\tilde{g}(c,y)$ ein nichtkonstantes Polynom über $K[A\cup\{c\}]$ mit Nullstelle b. □

Folgerung 6.1.5.9. *Wenn $K\leq E$, A, b, c die Voraussetzungen des algebraischen Austauschlemmas erfüllen, dann gilt $[A\cup\{b\}]=[A\cup\{c\}]$.*
Wenn A überdies algebraisch unabhängig war, dann sind auch $A\cup\{b\}$ und $A\cup\{c\}$ algebraisch unabhängig.

Folgerung 6.1.5.10. *Wenn B und C Transzendenzbasen für $K\leq E$ sind, dann gibt es für jedes $b\in B$ ein $c\in C$, sodass $(B\setminus\{b\})\cup\{c\}$ wiederum eine Transzendenzbasis ist.*

Beweis. Sei $b\in B$. Die Annahme $C\subseteq[B\setminus\{b\}]$ führt via $V=[C]\subseteq[[B\setminus\{b\}]]=[B\setminus\{b\}]$ zu einem Widerspruch, daher gibt es ein $c\in C$ mit $c\notin[B\setminus\{b\}]$. Nach dem algebraischen Austauschlemma gilt $b\in[(B\setminus\{b\})\cup\{c\}]$. Daher ist $(B\setminus\{b\})\cup\{c\}$ ein algebraisches Erzeugendensystem, und nach Folgerung 6.1.5.9 sogar eine Transzendenzbasis. □

Lemma 6.1.5.11. *Sei $K\leq E$ Körpererweiterung, und sei $B\subseteq E$ eine endliche Transzendenzbasis von E über K. Dann gilt: Für jede Transzendenzbasis C von E gilt $|B|=|C|$, also: alle Transzendenzbasen von E haben die gleiche (endliche) Kardinalität.*

Beweis. Sei $B=\{b_1,\ldots,b_n\}$. Nach Folgerung 6.1.5.10 gibt es $c_1\in C$, sodass $(B\setminus\{b_1\})\cup\{c_1\}=\{c_1,b_2,\ldots,b_n\}$ ebenfalls eine Transzendenzbasis ist. Genauso existiert $c_2\in C$, sodass $\{c_1,c_2,b_3,\ldots,b_n\}$ eine Transzendenzbasis ist; induktiv fortfahrend erhalten wir $c_3,\ldots,c_n\in C$, sodass schließlich $\{c_1,\ldots,c_n\}\subseteq C$ eine Transzendenzbasis ist. Da auch C eine Transzendenzbasis ist, muss $\{c_1,\ldots,c_n\}=C$ gelten, insbesondere $|C|=n=|B|$. □

Für *unendliche* Transzendenzbasen gilt ein analoger Satz, allerdings mit einem anderen Beweis:

Lemma 6.1.5.12. *Sei $K\leq E$ Körpererweiterung, und sei $B\subseteq E$ eine unendliche Transzendenzbasis von E über K. Für jede Transzendenzbasis C von V gilt dann $|B|=|C|$, also: alle Transzendenzbasen von V haben die gleiche (unendliche) Kardinalität.*

Beweis. So wie sich der Beweis von Lemma 6.1.5.11 durch geringfügige Umformulierungen aus dem Beweis von Lemma 1.3.2.4 ergibt, lässt sich auch der Beweis der aktuellen Aussage aus dem Beweis von Folgerung 1.3.3.2 gewinnen. Der entscheidende Punkt ist der Folgende: wenn $c\in[K(B)]$, etwa bezeugt durch ein Polynom $f(x)\in K(B)[x]$, dann gibt es eine endliche Teilmenge $B'\subseteq B$, sodass alle Koeffizienten von $f(x)$ bereits in $K(B')$ liegen. □

Die letzten beiden Lemmata motivieren die folgenden Definition:

Definition 6.1.5.13. Die (nach den Lemmata 6.1.5.11 und 6.1.5.12 eindeutig bestimmte) Kardinalität einer Transzendenzbasis von E über K heißt *Transzendenzgrad* von E über K.

Anmerkung 6.1.5.14. Ist α transzendent über K, dann ist der Körpergrad $[K(\alpha) : K]$ unendlich, weil die Potenzen α^n linear unabhängig über K sind.
Wenn K endlich ist, dann ist $K(\alpha)$ abzählbar unendlich und daher $[K(\alpha) : K] = \aleph_0$ (abzählbar unendlich). Wenn K unendlich ist, so kann man in $K(\alpha)$ eine über K linear unabhängige Menge finden, die gleichmächtig zu K ist, zum Beispiel $\{\frac{1}{q-\alpha} \mid q \in K\}$. Also gilt $[K(\alpha) : K] \geq |K|$. Wegen $|K(\alpha)| = |K|$ ist aber auch $[K(\alpha) : K] \leq |K|$, insgesamt also $[K(\alpha) : K] = |K|$.

6.1.6. Anwendung: Konstruierbarkeit mit Zirkel und Lineal

Inhalt in Kurzfassung: Übersetzt man die klassischen geometrischen Konstruktionsaufgaben mittels Zirkel und Lineal in eine algebraische Sprache, so entsprechen sie der Lösung von Gleichungen ersten und zweiten Grades, ausgehend vom Grundkörper $\mathbb{Q}$. Gleichungen ersten Grades haben innerhalb eines Körpers stets eine Lösung, bei zweitem Grad sind in der Regel Quadratwurzeln zu adjungieren, d. h. Körpererweiterungen vom Grad 2 nötig. Durch Iteration entstehen laut Gradsatz Erweiterungen, deren Dimension in jedem Fall von der Form 2^n sind. Dies hat beispielsweise zur Folge, dass Konstruktionen dritter Wurzeln wie $\sqrt[3]{2}$ (Diagonale des Würfels vom Volumen 2, Delisches Problem der Würfelverdoppelung), sofern sie nicht schon im Grundkörper liegen, ebenso wenig mit Zirkel und Lineal ausgeführt werden können wie die Dreiteilung beliebig vorgegebener Winkel. Auch die Konstruktion regelmäßiger n-Ecke mit Zirkel und Lineal wird durch derartige Überlegungen angreifbar, auch wenn für eine endgültige Klassifikation jener n, für die das möglich ist, auch noch Galoistheorie erforderlich wird. Weiß man, dass die Kreizahl π transzendent ist, folgt auch die Unmöglichkeit der legendären Quadratur des Kreises, d. h. die Konstruktion des Radius eines Kreises mit Einheitsfläche.

Definition 6.1.6.1. Sei A eine Menge von Punkten in der Ebene $\mathbb{R} \times \mathbb{R}$, die die Punkte $(0, 0)$ und $(1, 0)$ enthält. Unter einer *Konstruktion (mit Zirkel und Lineal)* aus A verstehen wir eine endliche Folge $(X_1, \ldots, X_n)$, sodass für alle $i = 1, \ldots, n$ gilt:

(1) X_i ist entweder ein Punkt, oder eine Gerade, oder ein Kreis in der Ebene, oder eine reelle Zahl.

(2) Wenn X_i ein Punkt p ist, dann gilt $p \in A$, oder p wird als Durchschnitt von früheren Kreisen und/oder Geraden erhalten, d. h.: es gibt $j_1, j_2 < i$, sodass p im Durchschnitt von X_{j_1} und X_{j_2} enthalten ist, wobei X_{j_1} und X_{j_2} verschieden[4] sind und X_{j_1} ein Kreis oder eine Gerade ist, ebenso X_{j_2}.

(3) Wenn X_i eine Gerade g ist, dann geht g durch zwei vorher konstruierte Punkte, d. h.: es gibt $j_1, j_2 < i$, sodass $p_1 = X_{j_1}$ und $p_2 = X_{j_2}$ zwei verschiedene Punkte sind, die beide auf g liegen.

(4) Wenn X_i ein Kreis k mit Mittelpunkt M und Radius r ist, dann wurden Mittelpunkt und Radius schon früher konstruiert, d. h.: es gibt $j_1, j_2 < i$, sodass $M = X_{j_1}$ und $r = X_{j_2}$.

[4] Äquivalent: Der Durchschnitt von X_{j_1} und X_{j_2} ist endlich.

(5) Wenn X_i eine Zahl $z \in \mathbb{R}$ ist, dann ist $|z|$ die Distanz zwischen zwei früher konstruierten Punkten, d. h.: es gibt $j_1, j_2 < i$ (nicht notwendigerweise verschieden), sodass $p_1 := X_{j_1}$ und $p_2 := X_{j_2}$ Punkte mit Abstand $|z|$ sind.

Wir nennen einen Punkt / eine Gerade / einen Kreis / eine Zahl *konstruierbar (mit Zirkel und Lineal)* aus A, wenn der Punkt / die Gerade / der Kreis / die Zahl in einer Konstruktion aus A vorkommen.
Statt „konstruierbar aus A“ schreiben wir oft einfach „konstruierbar“, wenn sich die Menge A aus dem Kontext ergibt. Insbesondere werden wir im folgenden zumeist Konstruierbarkeit aus der Menge $A = \{(0,0),(1,0)\}$ betrachten.

UE 354 ► **Übungsaufgabe 6.1.6.2.** (F) Zeigen Sie: Wenn die Gerade g und der Punkt P aus A konstruierbar sind, dann sind sowohl die Parallele zu g durch P als auch die Normale von P auf g aus A konstruierbar. ◄ **UE 354**

UE 355 ► **Übungsaufgabe 6.1.6.3.** (F) Zeigen Sie, dass für $a, b \in \mathbb{R}$ sind die folgenden Aussagen äquivalent sind: ◄ **UE 355**

(1) Der Punkt $(a,b) \in \mathbb{R}^2$ ist konstruierbar.
(2) Die Punkte $(a,0)$ und $(b,0)$ sind beide konstruierbar.
(3) Die Zahlen a und b sind beide konstruierbar.

Um die Koordinaten von konstruierbaren Punkten oder deren Distanzen zueinander zu berechnen, muss man offensichtlich endlich oft ein Gleichungssystem aus 2 Gleichungen mit 2 Unbekannten lösen, wobei

- entweder beide Gleichungen linear sind
- oder eine Gleichung linear ist, die andere die Form $(x-a)^2+(y-b)^2-c^2=0$ hat,
- oder beide Gleichungen die Form $(x-a)^2+(y-b)^2-c^2=0$ haben.

In jedem Fall[5] kann man explizite Formeln für die Lösungen angeben, die nur Körperoperationen sowie das Ziehen von Quadratwurzeln verwenden.
Umgekehrt kann man (zum Beispiel) den Strahlensatz verwenden, um das Produkt bzw. den Quotienten von zwei bereits konstruierten Zahlen zu erhalten, und den Höhensatz samt Thaleskreis, um aus einer bereits konstruierten positiven Zahl ihre Quadratwurzel zu erhalten:

UE 356 ► **Übungsaufgabe 6.1.6.4.** (W) Die Menge aller konstruierbaren reellen Zahlen bildet einen Unterkörper von $\mathbb{R}$, der unter Quadratwurzeln abgeschlossen ist. ◄ **UE 356**

Dies legt folgende Definition nahe:

[5] Man beachte, dass man aus dem Gleichungssystem $(x-a)^2+(y-b)^2=c^2$, $(x-p)^2+(y-q)^2=r^2$ durch Substraktion eine lineare Gleichung erhält; indem man diese in eine der quadratischen Gleichungen substituiert, lässt sich die Lösung auf die Lösung einer quadratischen Gleichung mit einer Unbekannten zurückführen.

Definition 6.1.6.5. Sei K Körper. Unter einer *Quadratwurzelerweiterung* von K verstehen wir einen Erweiterungskörper $L \geq K$, für den es eine endliche Folge $K = K_1 \leq K_2 \leq \cdots \leq K_n = L$ von Körpererweiterungen mit folgender Eigenschaft gibt: Für alle $i = 1, \ldots, n-1$ existiert $\alpha_i \in K_{i+1}$, sodass $K_{i+1} = K_i(\alpha_i)$ und $\alpha_i^2 \in K_i$.

Lemma 6.1.6.6. *Sei L Quadratwurzelerweiterung von K. Dann gibt es eine natürliche Zahl n mit $[L : K] = 2^n$.*

Beweis. Als Dimension $[K_{i+1} : K_i]$ jeder einzelnen Körpererweiterung kommt nur 1 oder 2 in Frage. Nach dem Gradsatz multiplizieren sich diese Dimensionen auf. □

Daraus erhält man recht schnell zusammenfassend:

Satz 6.1.6.7. *Sei A eine Menge von Punkten, die den Ursprung $(0, 0)$ und den Punkt $(1, 0)$ enthält. Dann gilt:*

(1) *Ein Punkt p ist genau dann aus A konstruierbar, wenn seine beiden Koordinaten aus A konstruierbar sind.*

(2) *Die Menge der aus A konstruierbaren reellen[6] Zahlen bilden einen Körper K_A, der unter Quadratwurzelziehen abgeschlossen ist, d. h.:*

$$\forall \alpha \in K_A : \alpha > 0 \Rightarrow \exists \beta \in K_A : \beta^2 = \alpha.$$

(3) *Sei B die Menge aller Koordinaten von Punkten in A. Dann ist $z \in \mathbb{R}$ genau dann aus A konstruierbar, wenn z in einer Quadratwurzelerweiterung von $\mathbb{Q}(B)$ liegt.*

UE 357 ► Übungsaufgabe 6.1.6.8. (V) Beweisen Sie Satz 6.1.6.7. **◄ UE 357**

Folgerung 6.1.6.9. *Sei A eine Menge von Punkten mit rationalen Koordinaten. Dann gilt:*

(1) *$\sqrt[3]{2}$ ist nicht aus A konstruierbar.*

(2) *Keine transzendente Zahl (wie etwa π) ist aus A konstruierbar.*

(3) *Eine Dreiteilung des Winkels $60°$ ist unmöglich, genauer: Die Eckpunkte eines Dreiecks mit den Winkeln $90°$, $70°$, $20°$ sind nicht alle aus A konstruierbar.*

Beweis.

(1) Angenommen, es gibt eine Quadratwurzelerweiterung L von $\mathbb{Q}$ mit $\sqrt[3]{2} \in L$. Dann ist $[L : \mathbb{Q}] = 2^n$ für eine natürliche Zahl n; nach dem Gradsatz gilt andererseits

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}],$$

also müsste $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ein Teiler von $[L : \mathbb{Q}] = 2^n$ sein.

[6] Man könnte auch für *komplexe* Zahlen den Begriff der Konstruierbarkeit einführen, z. B. indem man definiert, dass $z \in \mathbb{C}$ genau dann konstruierbar ist, wenn sowohl Real- als auch Imaginärteil von z konstruierbar sind; die hier angeführten Sätze lassen sich leicht auf komplexe Zahlen übertragen.

(2) Jede Quadratwurzelerweiterung von $\mathbb{Q}$ ist algebraisch über $\mathbb{Q}$.

(3) Wenn so ein Dreieck konstruierbar wäre, könnte man auch so ein Dreieck mit Hypotenuse der Länge 1 konstruieren und hätte somit die Zahl $\alpha := \cos(20°)$ konstruiert.

Aus $\cos(60°)+i\sin(60°) = (\cos(20°)+i\sin(20°))^3$ erhält man aus dem Vergleich der Realteile unter Verwendung von $\sin^2 t = 1-\cos^2 t$ die Beziehung $\frac{1}{2} = \cos(60°) = 4\cos^3(20°) - 3\cos(20°)$. Daher ist α Nullstelle des Polynoms $4x^3 - 3x - \frac{1}{2}$ bzw., gleichbedeutend, des ganzzahligen Polynoms $f(x) := 8x^3 - 6x - 1$. Wegen Proposition 5.3.2.9 kommen als rationale Nullstellen α von f nur die Möglichkeiten $\alpha = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ in Frage. Einsetzen dieser acht Werte liefert aber stets $f(\alpha) \neq 0$. Also hat dieses Polynom keine rationalen Nullstellen. Als Polynom vom Grad 3 ohne rationale Nullstellen muss f sogar irreduzibel über $\mathbb{Q}$ sein (Proposition 5.3.3.2). Für eine (notwendig irrationale) Nullstelle α von f ist somit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Wie in (1) folgt nun, dass α nicht aus A konstruierbar ist. □

Weitere prominente Beispiele in diesem Zusammenhang sind die regelmäßigen n-Ecke (auf dem Einheitskreis). Elementare Konstruktionen mit Zirkel und Lineal sind bis $n = 6$ möglich, nicht jedoch für $n = 7$, dann wieder für $n = 8, 10, 12$ etc. Gauß konnte beweisen, dass das regelmäßige n-Eck sicher dann konstruiert werden kann, wenn $n = 2^k p_1 \dots p_n$ mit $k \in \mathbb{N}$ und paarweise verschiedenen sogenannten *Fermatschen Primzahlen* $p_1, \dots, p_n$. Dabei heißt eine Primzahl p eine Fermatsche Primzahl, wenn sie von der Form $p = 2^{2^e} + 1 =: F_e$ mit $e \in \mathbb{N}$ ist. (Man beachte, dass für solche n die Eulersche φ-Funktion als Wert $\varphi(n)$ eine Potenz von 2 annimmt.) Allerdings sind bisher nur die Zahlen F_e für $e = 0, 1, 2, 3, 4$, also $p = 3, 5, 17, 257, 65537$ als Primzahlen ausgewiesen. Die Zahl $F_5 = 4294967297$ ist, wie Euler entdeckte, durch 641 teilbar. Weil Primzahlen immer seltener[7] und die Fermatschen Zahlen F_e mit wachsendem e extrem schnell riesengroß werden, vermutet man, dass es außer den genannten keine weiteren Fermatschen Primzahlen gibt. Dem Franzosen Pierre-Laurent Wantzel (1814-1848) gelang der Nachweis, dass außer den von Gauß angegebenen keine weiteren regelmäßigen n-Ecke mit Zirkel und Lineal konstruiert werden können. Das auszuführen übersteigt an dieser Stelle aber unsere Möglichkeiten, es erfordert Methoden und Ergebnisse aus der Galoistheorie (siehe Übungsaufgabe 9.5.7.10).

UE 358 ► Übungsaufgabe 6.1.6.10. (D) Versuchen Sie wenigsten gewisse der oben aufgestellten Behauptungen im Zusammenhang mit dem regelmäßigen n-Eck zu beweisen. **◄ UE 358**

[7] Der erstmals 1793 vom damals erst 16-jährigen Gauß und 1798 von Legendre vermutete, aber erst 1896 von den beiden Franzosen Hadamard und de la Vallée Poussin unabhängig voneinander bewiesene Primzahlsatz besagt, dass für die Anzahl $\pi(x)$ der Primzahlen $p \leq x$ die asymptotische Formel $\pi(x) \sim \frac{x}{\ln x}$ gilt. Ein Vergleich diese Häufigkeitsaussage mit der Seltenheit Fermatscher Zahlen kann als Indiz dafür angesehen werden, dass es gar keine weiteren Fermatschen Primzahlen gibt.

6.2. Adjunktion von Nullstellen von Polynomen

Im vorigen Abschnitt haben wir die Situation studiert, dass zwei Körper bereits vorliegen, von denen einer, der Grund- oder Unterkörper K, im anderen, dem Erweiterungs- oder Oberkörper L, enthalten ist. Für Elemente $\alpha \in L$ war vor allem von Interesse, ob es ein Polynom $f \in K[x]$, $f \neq 0$, mit $f(\alpha) = 0$ gibt, also ob α algebraisch oder transzendent über K ist. Nun gehen wir umgekehrt vor, indem wir uns neben K ein $f \in K[x]$ vorgeben, das in K eventuell keine Nullstelle hat. Wir suchen nach einer Erweiterung L von K mit einer oder mehreren Lösungen α der Gleichung $f(x) = 0$. In einem weiteren Schritt sucht man Erweiterungen für nicht nur ein solches f, sondern für beliebige Teilmengen von $K[x]$. Es zeigt sich, dass solche Erweiterungen in Form von Nullstellen- bzw. Zerfällungskörpern stets existieren.
Man beachte die Analogie zu den Zahlenbereichserweiterungen von $\mathbb{N}$ zu $\mathbb{Z}$ und $\mathbb{Q}$ sowie von $\mathbb{R}$ zu $\mathbb{C}$, die auch durch die Lösung von Gleichungen motiviert waren. Gleichungen der Form $a + x = b$ machen, sofern $a > b$, die Erweiterung von $\mathbb{N}$ zu $\mathbb{Z}$ erforderlich, Gleichungen der Form $ax = b$, sofern a kein Teiler von b ist, die von $\mathbb{Z}$ zu $\mathbb{Q}$. Die sehr spezielle Gleichung $f(x) := x^2 + 1 = 0$ führt von $\mathbb{R}$ zu $\mathbb{C}$. Letzteres soll in diesem Abschnitt auf beliebige Polynome f über irgendeinem Körper K (statt $\mathbb{R}$) verallgemeinert werden.
Der Überblick über den Abschnitt: In 6.2.1 behandeln wir den entscheidenden Schritt der Adjunktion einer Nullstelle eines gegebenen irreduziblen Polynoms. Iteriert man diesen Schritt geeignet (nötigenfalls auch unendlich oft), so erhält man den Zerfällungskörper einer beliebigen Menge von Polynomen. Nimmt man die Menge aller Polynome über dem Ausgangskörper, so landet man beim algebraischen Abschluss des Ausgangskörpers (6.2.2). In 6.2.3 ergibt sich die Eindeutigkeit des Zerfällungskörpers (bis auf Isomorphie bzw. sogar Äquivalenz). Die Frage, wann Polynome in ihrem Zerfällungskörper mehrfache Nullstellen haben können, lässt sich mit Hilfe einer formalen Ableitung erfolgreich untersuchen (6.2.4). Reizvoll ist auch die Untersuchung von Einheitswurzeln und Kreisteilungspolynomen (6.2.5). Den Abschnitt schließen zwei Ergebnisse ab, nach denen gewisse Körpererweiterungen (eine algebraische und eine transzendente) von einem einzigen geeigneten Element erzeugt werden (6.2.6).

6.2.1. Adjunktion einer Nullstelle

Inhalt in Kurzfassung: Die Erkenntnisse aus dem vorangegangenen Abschnitt über algebraische Körpererweiterungen werden nun verwendet, um den umgekehrten Weg zu beschreiten. Zu gegebenem Körper K und Polynom $f \in K[x]$ ist ein Erweiterungskörper L von K gesucht, der eine Nullstelle von f enthält. Ist f irreduzibel (andernfalls ist f durch einen irreduziblen Faktor zu ersetzen), so gelingt dies mit $L := K[x]/(f)$, der Faktorisierung des Polynomrings nach dem von f erzeugten Hauptideal (Satz von Kronecker).

Wir gehen aus vom Beispiel der Adjunktion der imaginären Einheit i zu $\mathbb{R}$, wodurch $\mathbb{C}$ entsteht. Wegen $i^2 = -1$ ist i Nullstelle des Polynoms $f(x) = x^2 + 1$, das in $\mathbb{R}$

bekanntlich keine Nullstelle hat. Durch diese Eigenschaft ist das Rechnen in $\mathbb{C}$ eindeutig festgelegt, wobei sich jede komplexe Zahl als Linearkombination von 1 und i ergibt. Ganz Ähnliches gilt, wenn wir von einer Nullstelle α eines beliebigen irreduziblen Polynoms $f \in K[x]$ über irgendeinem Körper K ausgehen. OBdA dürfen wir annehmen, dass f monisch ist, also $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ mit $a_i \in K$. Dann gilt $\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0$, wodurch iterativ auch noch höhere Potenzen von α als Linearkombinationen von $1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ ausgedrückt werden können, zum Beispiel

$$\begin{aligned}\alpha^{n+1} &= \alpha \cdot \alpha^n = -a_{n-1}\alpha^n - \ldots - a_1\alpha^2 - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0) - a_{n-2}\alpha^{n-1} \ldots - a_1\alpha^2 - a_0\alpha\end{aligned}$$

Es zeigt sich, dass die Linearkombinationen von $1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ bereits einen Körper bilden, der die Nullstelle α von f enthält. Etwas präziser formuliert lässt sich diese Konstruktion wie folgt fassen:

Proposition 6.2.1.1 (Satz von Kronecker)**.** *Sei $f \in K[x]$ irreduzibel. Dann ist der Faktorring $L := K[x]/(f)$ des Polynomrings $K[x]$ nach dem von f erzeugten Hauptideal (f) ein Körper. Die Abbildung $\iota\colon K \to L = K[x]/(f)$, $k \mapsto k + (f)$, ist eine isomorphe Einbettung. Die eindeutige homomorphe Fortsetzung $\bar{\iota}\colon K[x] \to L[x]$ von ι auf $K[x]$ mit $\bar{\iota} : x \mapsto x$ ist gleichfalls eine isomorphe Einbettung, und zwar des Polynomrings über K in den über L. Das Element $x + (f) \in K[x]/(f) = L$ ist Nullstelle von $\bar{f} := \bar{\iota}(f) \in L[x]$. Identifizieren wir K und $\iota(K)$ vermittels ι sowie $K[x]$ und $\bar{\iota}(K[x]) \leq L[x]$ vermittels $\bar{\iota}$, so ist mit L also eine Erweiterung von K mit einer Nullstelle von f gefunden. Die Dimension $[L : K]$ stimmt mit dem Grad* $\operatorname{grad}(f)$ *überein. Als endlichdimensionale Erweiterung ist L also insbesondere algebraisch über K.*

Beweis. Weil $f \in K[x]$ irreduzibel und $K[x]$ ein Hauptidealring ist, ist das von f erzeugte Ideal (f) maximal wegen Proposition 5.1.4.1 und $L = K[x]/(f)$ tatsächlich ein Körper (siehe Satz 3.4.2.4). Klarerweise ist ι ein Homomorphismus und wegen $\operatorname{grad}(f) \geq 1$ injektiv, also eine isomorphe Einbettung. Die einzige homomorphe Fortsetzung $\bar{\iota}$ ist

$$\bar{\iota} : \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \iota(a_i) x^i,$$

offenbar ebenfalls eine isomorphe Einbettung $\bar{\iota}\colon K[x] \to L[x]$. Aufgrund der Rechenregeln für Nebenklassen von Idealen in Faktorringen gilt:

$$(\bar{\iota}(f))(\bar{\iota}(x)) = \bar{f}(x + (f)) = f(x) + (f) = (f) = 0_{K[x]/(f)} = 0_L.$$

Also ist die Behauptung betreffend die Nullstelle im Erweiterungskörper bewiesen. Jene betreffend die Dimension der Körpererweiterung ergibt sich aus Satz 6.1.3.4, da $\bar{\iota}(f)$ (bzw. nach Identifikation f) das Minimalpolynom von $\bar{\iota}(x)$ ist und da $L = K(\bar{\iota}(x))$ ist. □

Den in Proposition 6.2.1.1 beschriebenen Erweiterungsprozess von K nennt man auch *Adjunktion einer Nullstelle* des irreduziblen Polynoms f. Durch iterierte Adjunktion

von Nullstellen irreduzibler Polynome kann man sogenannte Zerfällungskörper von Polynomen oder, nach eventuell transfiniter Fortsetzung, von beliebigen Polynommengen $P \subseteq K[x]$ konstruieren. Dem wollen wir uns nun zuwenden.

6.2.2. Die Konstruktion von Zerfällungskörpern und algebraischem Abschluss

Inhalt in Kurzfassung: Durch Iteration der Konstruktion aus Unterabschnitt 6.2.1 lässt sich zu vorgegebenem $f \in K[x]$ eine Erweiterung E von K konstruieren, in der f nicht nur eine Nullstelle hat, sondern sogar in Linearfaktoren zerfällt. Eine minimale Erweiterung mit dieser Eigenschaft heißt Zerfällungskörper. Offenbar ist damit auch die Verallgemeinerung zunächst auf endlich viele Polynome $f_1, \ldots, f_n$ möglich, sodann, bei transfiniter Fortsetzung des Erweiterungsprozesses, auf eine beliebige Teilmenge von $K[x]$. Im Extremfall kann man auch die gesamte Menge $K[x]$ wählen. Der resultierende Zerfällungskörper Z erweist sich sogar als algebraisch abgeschlossen, enthält also nicht nur sämtliche Nullstellen aller Polynome aus $K[x]$ sondern sogar aller Polynome aus $Z[x]$. Man spricht auch von einem algebraischen Abschluss von K.

Zu Beginn dieses Unterabschnitts definieren wir die zentralen Begriffe:

Definition 6.2.2.1. Sei $K \leq E$ eine Körpererweiterung und $P \subseteq K[x]$ eine Menge von Polynomen. Zerfällt jedes $f \in P$ über E in Linearfaktoren, so heißt E ein *Nullstellenkörper* von P. Ist überdies E minimal mit dieser Eigenschaft (anders gesagt: E wird von K und sämtlichen Nullstellen aller $f \in P$ erzeugt), so heißt E ein *Zerfällungskörper* von P. Ist $P = \{f\}$ einelementig, so heißt E auch Nullstellen- bzw. Zerfällungskörper von f. Der Körper K heißt *algebraisch abgeschlossen*, wenn jedes nichtkonstante Polynom $p(x) \in K[x]$ über K in Linearfaktoren zerfällt, also wenn es (nicht notwendigerweise paarweise verschiedene) $\alpha_1, \ldots, \alpha_n \in K$ und ein $a \in K$ gibt mit $p(x) = a(x - \alpha_1) \cdot \cdots \cdot (x - \alpha_n)$. Unter einem *algebraischen Abschluss* von K versteht man einen Erweiterungskörper L, sodass $K \leq L$ eine algebraische Erweiterung ist und sodass L algebraisch abgeschlossen ist.

Einfach einzusehen sind folgende Charakterisierungen algebraisch abgeschlossener Körper:

Proposition 6.2.2.2. *Für einen Körper K sind die folgenden Aussagen äquivalent:*

(1) *K ist algebraisch abgeschlossen.*
(2) *Jedes nichtkonstante Polynom $p(x) \in K[x]$ hat eine Nullstelle in K.*
(3) *Jedes nichtkonstante irreduzible Polynom $p(x) \in K[x]$ hat eine Nullstelle in K.*
(4) *Jedes nichtkonstante irreduzible Polynom $p(x) \in K[x]$ hat Grad 1.*
(5) *Für jede algebraische Erweiterung $L \geq K$ gilt $L = K$.*

UE 359 ► Übungsaufgabe 6.2.2.3. (V) Beweisen Sie Proposition 6.2.2.2. **◄ UE 359**

Von ähnlichem Charakter sind die folgenden Charakterisierungen eines algebraischen Abschlusses:

Proposition 6.2.2.4. *Für eine Körpererweiterung $K \leq L$ sind die folgenden Aussagen äquivalent:*

(1) *L ist ein algebraischer Abschluss von K.*

(2) *L ist ein Nullstellenkörper von $K[x]$ und L ist algebraisch über K.*

(3) *L ist ein Zerfällungskörper von $K[x]$ über K.*

(4) *L ist algebraisch über K und für alle $L' \geq L$ gilt: Wenn L' algebraisch über K ist, dann ist $L = L'$.*

UE 360 ▶ Übungsaufgabe 6.2.2.5. (V) Beweisen Sie Proposition 6.2.2.4. **◀ UE 360**

UE 361 ▶ Übungsaufgabe 6.2.2.6. (F) Sei K ein Körper und sei X eine Variablenmenge. Zeigen Sie, dass der Körper $K(X)$ der gebrochen rationalen Funktionen in X über K nicht algebraisch abgeschlossen ist. **◀ UE 361**

Wir wollen uns nun an die Konstruktion von Nullstellen- und Zerfällungskörpern machen. Das gelingt mittels iterierter Adjunktion von Nullstellen gemäß Unterabschnitt 6.2.1, und zwar für eine beliebig vorgegebene Menge $P \subseteq K[x]$ von Polynomen über einem ebenfalls beliebigen Körper K. Insbesondere erhält man gemäß Proposition 6.2.2.4 mit $P = K[x]$ so auch einen algebraischen Abschluss von K. Nützlich sind dabei die folgende Abschätzung der Kardinalität algebraischer Erweiterungen sowie die daran anschließenden Überlegungen. (Man beachte die Ähnlichkeit zu Überlegungen bei der Konstruktion freier Algebren in Unterabschnitt 4.1.6.)

Proposition 6.2.2.7. *Sei L eine algebraische Körpererweiterung von K. Dann gilt $|L| \leq \max\{|K|, |\mathbb{N}|\}$.*

Beweis. Für jedes $f \in K[x] \setminus \{0\}$ sei N_f die (endliche) Menge der Nullstellen von f in L. Weil L algebraisch über K ist, folgt

$$L \subseteq \bigcup_{f \in K[x] \setminus \{0\}} N_f.$$

Zu jedem Grad n gibt es $|K^{n+1}| = |K|^{n+1}$ Polynome vom Grad $\leq n$. Ist K endlich, so sind das für jedes n endlich viele, insgesamt also abzählbar unendlich viele, womit auch L abzählbar ist.
Ist K hingegen unendlich, so ist $|K|^{n+1} = |K|$ (siehe Satz A.5.6.5 im Anhang). Zu jedem Grad $n \in \mathbb{N}$ gibt es also nicht mehr Polynome als $|K|$, somit auch $|K[x]| \leq |\mathbb{N}| \cdot |K| = |K|$ (nochmals Satz A.5.6.5) und analog weiterschließend $|L| \leq |K|$. Damit ist die Behauptung sowohl für endliches als auch für unendliches K bewiesen. □

Für die Konstruktion benötigen wir die folgende Begriffsbildung, die auch im nächsten Unterabschnitt zur Eindeutigkeit des Zerfällungskörpers eine tragende Rolle spielen wird.

Definition 6.2.2.8. Seien $K_1 \leq E_1$ und $K_2 \leq E_2$ Körpererweiterungen und $\varphi : K_1 \to K_2$ ein Isomorphismus. Ein Isomorphismus $\psi : E_1 \to E_2$ heißt *Äquivalenz* und die Erweiterungen E_1 und E_2 heißen *äquivalent* bezüglich φ, wenn ψ auf K_1 mit φ übereinstimmt. Ist $K_1 = K_2 =: K$ und φ die Identität auf K, so spricht man schlicht von Äquivalenz, auch ohne explizite Bezugnahme auf $\varphi = \mathrm{id}_K$.

UE 362 ▶ **Übungsaufgabe 6.2.2.9.** (F) Die Äquivalenz von zwei Körpererweiterungen $K \leq E_1$ und $K \leq E_2$ bezüglich $\varphi = \mathrm{id}_K$ aus Definition 6.2.2.8 kann auch als Äquivalenz im kategorientheoretischen Sinn aufgefasst werden. Wie? ◀ **UE 362**

Ist X nun irgendeine überabzählbare Obermenge von K mit größerer Kardinalität als $|K|$ (zum Beispiel $X := K \cup \mathfrak{P}(K) \cup \mathbb{R}$), so lässt sich jede algebraische Erweiterung E von K bis auf Äquivalenz auf einer Teilmenge von X realisieren, das heißt genauer: Es gibt eine Teilmenge $E' \subseteq X$ mit $K \subseteq E'$ und Operationen $+_{E'}, 0_{E'}, -_{E'}, \cdot_{E'}, 1_{E'}$ auf E', sodass $(E', +_{E'}, 0_{E'}, -_{E'}, \cdot_{E'}, 1_{E'})$ ein Erweiterungskörper von K ist und sodass die Erweiterungen $K \leq E$ und $K \leq E'$ äquivalent sind[8]. Im Beweis des folgenden Satzes wird es daher möglich sein, sich auf solche Erweiterungen von K zu beschränken, deren Trägermenge eine Teilmenge von X ist.

Satz 6.2.2.10. *Sei K ein Körper. Dann gibt es für jede Teilmenge $P \subseteq K[x]$ einen Zerfällungskörper Z_P. Insbesondere gibt es einen Zerfällungskörper $Z = Z_{K[x]}$ der Menge aller Polynome über K. Alle Z_P sind algebraisch über K. Der Körper Z ist sogar algebraisch abgeschlossen und somit ein algebraischer Abschluss von K. Inbesondere gibt es also zu jedem Körper einen algebraischen Abschluss.*

Beweis. Ist $Z = Z_{K[x]}$ mit den behaupteten Eigenschaften einmal gefunden, so ist für beliebiges $P \subseteq K[x]$ der Körper $Z_P := K(S) \leq Z$ ein Zerfällungskörper von P und algebraisch über K, sofern $S \subseteq Z$ die Menge aller Nullstellen von Polynomen $f \in P$ bezeichnet.
Um Z zu erhalten, betrachten wir für eine (feste) Menge X wie oben (d. h., X sei überabzählbar mit $K \subseteq X$ und $|X| > |K|$) das System[9] $\mathcal{S}$ aller algebraischen Körpererweiterungen E von K mit Trägermenge $\subseteq X$. Dieses System $\mathcal{S}$ ist durch die Relation

[8] Man kann E' und die Operationen folgendermaßen erhalten: Wähle zunächst irgendeine Injektion $\psi : E \to X$, die auf K mit id_K übereinstimmt (insbesondere ist K im Bild von ψ enthalten), setze $E' = \psi(E)$ und definiere die Operationen auf E' so, dass ψ ein Isomorphismus wird, also zum Beispiel $0_{E'} := \psi(0_E) = \psi(0_K) = 0_K$ und $\psi(\alpha) +_{E'} \psi(\beta) := \psi(\alpha + \beta)$.

[9] Das System $\mathcal{S}$ ist tatsächlich eine Menge, weil es aus Elementen einer festen Menge Y besteht: Jedes Element von $\mathcal{S}$ ist ein Tupel $(E, +, 0, -, \cdot, 1)$, wobei E eine Teilmenge von X ist; 0 und 1 Elemente von E sind (insbesondere Elemente von X); $-$ eine Funktion $E \to E$ ist, also eine Teilmenge von $E \times E$ (insbesondere eine Teilmenge von $X \times X$); und $+, \cdot$ Funktionen $E \times E \to E$ sind, also analog Teilmengen von $(E \times E) \times E$ (insbesondere Teilmengen von $(X \times X) \times X$). Zusammenfassend kann man also $Y := \mathfrak{P}(X) \times \mathfrak{P}((X \times X) \times X) \times X \times \mathfrak{P}(X \times X) \times \mathfrak{P}((X \times X) \times X) \times X$ setzen. Hätten wir beliebige algebraische Körpererweiterungen von K betrachtet, dann wäre $\mathcal{S}$ (sofern nicht K selbst bereits algebraisch abgeschlossen ist) eine echte Klasse, d. h. keine Menge.

$\leq$ (Unterkörper) halbgeordnet und nach der Variante der zweiten Aussage von Übungsaufgabe 2.2.1.11 für Körper (siehe Übungsaufgabe 2.2.1.15) abgeschlossen bezüglich der Vereinigung von Ketten. Nach dem Lemma von Zorn gibt es daher ein bezüglich $\leq$ maximales Element $E_0 \in \mathcal{S}$. Wir wollen zeigen, dass E_0 algebraisch abgeschlossen ist.
Sei also $f \in E_0[x]$ irreduzibel. Nach Proposition 6.2.1.1 gibt es eine algebraische Erweiterung E_1 von E_0 mit einer Nullstelle $\alpha \in E_1$ von f. Der Körper $E_0 \in \mathcal{S}$ ist algebraisch über K, folglich (Satz 6.1.4.2) ist E_1 algebraisch über K. Außerdem können wir wegen der Überlegungen vor diesem Satz annehmen, dass E_1 eine Teilmenge von X ist, mit anderen Worten $E_1 \in \mathcal{S}$. Wegen der Maximalität von E_0 in $\mathcal{S}$ muss $E_1 = E_0$ gelten, also $\alpha \in E_0$. Somit hat f eine Nullstelle in E_0. Nach Proposition 6.2.2.2 ist E_0 algebraisch abgeschlossen.

□

6.2.3. Die Eindeutigkeit von Zerfällungskörpern und algebraischem Abschluss

Inhalt in Kurzfassung: Die Konstruktionen in Unterabschnitt 6.2.2 haben gezeigt, dass es zu jeder Menge von Polynomen über einem Körper einen Zerfällungskörper gibt. Dieser ist (bis auf Äquivalenz, also erst recht bis auf Isomorphie) sogar eindeutig bestimmt. Das entscheidende technische Hilfsmittel für den Beweis ist ein Fortsetzungssatz für Körperisomorphismen.

Bei der Konstruktion des Zerfällungskörpers war der Satz von Kronecker (Proposition 6.2.1.1) das wesentliche technische Instrument. In Satz 6.1.3.4 haben wir aber auch eine Eindeutigkeitsaussage kennen gelernt, nämlich $K(\alpha) \cong K(\beta)$ mit einem Isomorphismus, der α in β überführt, sofern α und β dasselbe Minimalpolynom haben. Weil die Konstruktion jedes Zerfällungskörpers sich als (eventuell transfinite) Iteration dieses zentralen Konstruktionsschrittes deuten lässt, erwarten wir eine ähnliche Eindeutigkeitsaussage für Zerfällungskörper. Satz 6.2.3.1 wird dieser Erwartung gerecht werden. Dabei wird Definition 6.2.2.8 ihre volle Stärke ausspielen – fasst sie doch die Idee von „isomorphen Körpererweiterungen“. Mit dieser Begriffsbildung lässt sich folgender Satz aussprechen:

Satz 6.2.3.1. *Seien $K_1 \cong K_2$ Körper, $\varphi\colon K_1 \to K_2$ ein Isomorphismus und $\varphi_x\colon K_1[x] \to K_2[x]$ jener (eindeutige) Isomorphismus zwischen den Polynomringen, dessen Einschränkung auf die konstanten Polynome mit φ übereinstimmt und der das Polynom $x \in K_1[x]$ auf das Polynom $x \in K_2[x]$ abbildet. Seien weiters $P_1 \subseteq K_1[x]$ und $P_2 \subseteq K_2[x]$ Mengen von Polynomen mit $P_2 = \varphi_x(P_1)$, sowie $Z_1 \geq K_1$ und $Z_2 \geq K_2$ Zerfällungskörper von P_1 über K_1 bzw. von P_2 über K_2.*
Dann sind Z_1 und Z_2 bezüglich φ äquivalent. Insbesondere sind je zwei Zerfällungskörper derselben Menge P von Polynomen über einem Körper K äquivalent.

Beweis. Die letzte Aussage ergibt sich unmittelbar aus der allgemeineren ersten, wenn man $K := K_1 = K_2$, $\varphi = \mathrm{id}_K$ und $P = P_1 = P_2$ setzt. Es genügt deshalb, die erste Aussage zu beweisen. Wie bei der Konstruktion des Zerfällungskörpers verwenden wir zur

Konstruktion des gesuchten Isomorphismus das Lemma von Zorn. Diesmal betrachten wir das System $\mathcal{S}$ aller Tripel (E_1, ψ, E_2) mit $K_1 \leq E_1 \leq Z_1$, $K_2 \leq E_2 \leq Z_2$ und einem Isomorphismus $\psi\colon E_1 \to E_2$, der φ fortsetzt. Die Halbordnungsrelation $\leq$ auf $\mathcal{S}$ sei definiert wir folgt: $(E_1, \psi, E_2) \leq (E_1', \psi', E_2')$ genau dann, wenn $E_1 \leq E_1'$, $E_2 \leq E_2'$ und wenn ψ' auf E_1 mit ψ übereinstimmt. Zu jeder $\leq$-Kette von Elementen $(E_1, \psi, E_2) \in \mathcal{S}$ gibt es die obere Schranke $(E_1^*, \psi^*, E_2^*) \in \mathcal{S}$, in der jede der drei Komponenten als Vereinigung der entsprechenden Komponenten aus der Kette zustande kommt. Nach dem Lemma von Zorn gibt es folglich ein maximales Element in $\mathcal{S}$, das wir der Einfachheit halber wieder mit (E_1, ψ, E_2) bezeichnen. Der Satz ist bewiesen, wenn wir $E_1 = Z_1$ und $E_2 = Z_2$ beweisen können. Nehmen wir zunächst indirekt $E_1 \neq Z_1$ an, also $E_1 < Z_1$.
Weil Z_1 als Zerfällungskörper von P_1 von sämtlichen Nullstellen aller $f \in P_1$ erzeugt wird, muss es eine Nullstelle $\alpha_1 \in Z_1$ eines $f_1 \in P_1$ geben, die nicht in E_1 liegt. Sei m_1 das Minimalpolynom von α_1 über E_1. Klarerweise gilt $m_1 | f_1$ in $E_1[x]$. Wie $\varphi\colon K_1 \to K_2$ induziert auch der Isomorphismus $\psi\colon E_1 \to E_2$ einen (eindeutigen) Isomorphismus $\psi_x\colon E_1[x] \to E_2[x]$ der zugehörigen Polynomringe, der auf den konstanten Polynomen mit ψ übereinstimmt und $x \in E_1[x]$ auf $x \in E_2[x]$ abbildet. Somit geht das irreduzible Polynom m_1 in ein irreduzibles Polynom $m_2 := \psi_x(m_1)$ über, wobei $m_2 | f_2$ für $f_2 := \psi_x(f_1) = \varphi_x(f_1) \in P_2$ gilt. Weil Z_2 ein Zerfällungskörper von P_2 ist, zerfällt f_2 über Z_2 in Linearfaktoren, von denen gewisse den Teiler m_2 aufbauen. Ein solcher (oBdA normierter) sei $x - \alpha_2$.[10] Also ist $m_2(\alpha_2) = 0$ mit $\alpha_2 \in Z_2$. Laut Proposition 6.1.3.6 lässt sich $\psi\colon E_1 \to E_2$ fortsetzen zu einem Isomorphismus $\psi^*\colon E_1(\alpha_1) \to E_2(\alpha_2)$. Dann wäre aber $(E_1(\alpha_1), \psi^*, E_2(\alpha_2)) \in \mathcal{S}$ echt größer als (E_1, ψ, E_2), was der Maximalität von (E_1, ψ, E_2) in $\mathcal{S}$ widerspräche. Folglich wurde die indirekte Annahme widerlegt, und es gilt $E_1 = Z_1$. Aus Symmetriegründen (Rollen von E_1 und E_2 vertauschen und ψ durch ψ^{-1} ersetzen) muss dann auch $E_2 = Z_2$ gelten. Damit ist $\psi\colon Z_1 \to Z_2$ tatsächlich der gesuchte Isomorphismus. □

Anmerkung 6.2.3.2. Man beachte, dass wir (trotz der Tatsache, dass man die Äquivalenz von Körpererweiterungen eines festen Körpers K als kategorientheoretische Äquivalenz auffassen kann) die Eindeutigkeit des Zerfällungskörperes bis auf Äquivalenz *nicht* dadurch beweisen können, dass wir den Zerfällungskörper als universelles Objekt in einer geeigneten Kategorie deuten. Das wesentliche Problem liegt darin, dass – anders als es für ein kategorientheoretisches universelles Objekt gefordert und zentral wäre – der Isomorphismus zwischen zwei Zerfällungskörpern nicht eindeutig sein muss. In sehr vielen Fällen gibt es sogar für eine feste Körpererweiterung $K \leq E$ einen Automorphismus $\psi : E \to E$ mit $\psi \neq \mathrm{id}_E$, der auf K mit id_K übereinstimmt. Das Studium derartiger Automorphismen ist Gegenstand der Galoistheorie und erlaubt tiefe Einsichten über die Körpererweiterung.

Wir ziehen zwei Folgerungen.

Folgerung 6.2.3.3. *Jeder Zerfällungskörper Z einer Menge von Polynomen $P \subseteq K[x]$ ist algebraisch über dem Grundkörper K.*

[10] An dieser Stelle stehen eventuell mehrere Linearfaktoren $x - \alpha$ mit verschiedenen α zur Auswahl. Deshalb muss der Isomorphismus zwischen Z_1 und Z_2 nicht eindeutig sein.

Beweis. Der in Satz 6.2.2.10 konstruierte Zerfällungskörper Z_P ist algebraisch über K. Wegen Satz 6.2.3.1 muss das folglich für jeden Zerfällungskörper von P gelten. □

Folgerung 6.2.3.4. *Jeder algebraische Abschluss E eines Körpers K ist algebraisch über K und bis auf Äquivalenz eindeutig. Wenn K endlich oder abzählbar ist, dann ist E abzählbar, für größeres K gilt stets $|E| = |K|$.*

Beweis. Als Zerfällungskörper über K ist E nach Satz 6.2.3.1 bis auf Äquivalenz eindeutig und nach Folgerung 6.2.3.3 algebraisch über K. Die Kardinalitätsaussage ergibt sich nun fast zur Gänze aus Proposition 6.2.2.7; es bleibt nur zu zeigen, dass E auch im Falle eines endlichen Körpers K immer unendlich ist. Dies übersteigt an dieser Stelle unserer Möglichkeiten, sodass wir den Beweis in Unterabschnitt 6.3.5, inbesondere Satz 6.3.5.1, vollenden werden, wenn wir mehr Theorie zur Verfügung haben (tatsächlich werden wir den algebraischen Abschluss von endlichen Körpern explizit bestimmen). □

Der Körper $\mathbb{C}$ der komplexen Zahlen ist nach dem Fundamentalsatz der Algebra algebraisch abgeschlossen. Insbesondere enthält er den Zerfällungskörper von $P := \mathbb{Q}[x] \subseteq \mathbb{C}[x]$, also einen algebraischen Abschluss $\mathbb{A} := \overline{\mathbb{Q}}$ von $\mathbb{Q}$. Die Elemente von $\mathbb{A}$ heißen *algebraische Zahlen*. Im Gegensatz dazu versteht man unter einer *transzendenten Zahl* ein Element aus $\mathbb{R} \setminus \mathbb{A}$. Nach Folgerung 6.2.3.4 gibt es, weil $\mathbb{Q}$ abzählbar ist, nur abzählbar viele algebraische Zahlen, während $\mathbb{R}$ überabzählbar ist. Cantors „Diagonalverfahren“ liefert (im Prinzip) sogar eine explizite Aufzählung aller algebraischen Zahlen und dadurch eine explizite Intervallschachtelung, deren innerster Punkt transzendent sein muss. Andere Konstruktionen von transzendenten Zahlen (zahlentheoretischer Natur), z. B. von Liouville, waren zu Cantors Zeit schon bekannt. Die Transzendenz von e wurde von Hermite 1873 bewiesen, also im selben Jahr, in dem Cantor die Überabzählbarkeit von $\mathbb{R}$ entdeckte. Der Beweis der Transzendenz von π durch Lindemann folgte 1882.

UE 363 ► **Übungsaufgabe 6.2.3.5.** (E) Geben Sie explizit Glieder $a_n \in \mathbb{Q}$ an, sodass die daraus gebildete unendliche Reihe gegen eine transzendente Zahl s konvergiert. Hinweis: Gehen Sie in folgenden Schritten vor: ◄ **UE 363**

1. Zeigen Sie: Jede algebraische Zahl ist Nullstelle eines Polynoms $f \in \mathbb{Z}[x]$ mit ganzen Koeffizienten.

2. Zeigen Sie: Das ganzzahlige Polynom $f \in \mathbb{Z}[x]$ vom Grad n habe die rationale Zahl $r = \frac{p}{q}$ $(p, q \in \mathbb{Z})$ nicht als Nullstelle. Dann gilt $|f(r)| \geq \frac{1}{q^n}$.

3. Nutzen Sie die Ungleichung aus Teil 2 zu einer unteren asymptotischen Abschätzung für rationale Approximierbarkeit algebraischer Zahlen. Genauer: Ist $\alpha \in \mathbb{R}$ irrational und algebraisch vom Grad n, dann gibt es ein $c > 0$ derart, dass für alle $p \in \mathbb{Z}$, $q \in \mathbb{N}^+$ die Ungleichung $|\alpha - \frac{p}{q}| > \frac{c}{q^n}$ gilt.

4. Finden Sie rationale Zahlen $a_n > 0$, die so schnell gegen 0 konvergieren, dass die Partialsummen der resultierenden Reihe ihren Grenzwert α so gut approximieren, dass wegen Teil 3 die Zahl α nicht algebraisch sein kann.

An dieser Stelle können wir auch einige Aussagen über Automorphismen von $\mathbb{C}$ treffen:

Anmerkung 6.2.3.6. Wir wissen bereits, dass es genau zwei Automorphismen von $\mathbb{C}$ gibt, die alle Elemente von $\mathbb{R}$ punktweise fixieren. Lassen wir diese Forderung fallen und fragen nach beliebigen Automorphismen (die nur noch den Primkörper $\mathbb{Q}$ punktweise fixieren; siehe Proposition 6.1.1.4), so existieren viel mehr Automorphismen. Wir wählen gemäß Satz 6.1.5.6 eine Transzendenzbasis S von $\mathbb{C}$ über $\mathbb{Q}$ und setzen $L := \mathbb{Q}(S)$. Nach Übungsaufgabe 6.2.2.6 gilt $L \neq \mathbb{C}$, also ist die algebraische Erweiterung $L \leq \mathbb{C}$ nichttrivial. Die beiden Schritte $\mathbb{Q} \leq L \leq \mathbb{C}$ geben Anlass zu verschiedenen Möglichkeiten, nichttriviale Automorphismen zu konstruieren; wir beschränken uns hier auf zwei.
Für die erste, „rein transzendente“ Möglichkeit betrachten wir eine Permutation $\sigma : X \to X$ und setzen diese auf offensichtliche Weise zu einem Körperautomorphismus φ von L fort (Permutieren der Variablen). Der Körper $\mathbb{C}$ ist der algebraische Abschluss von L, also der Zerfällungskörper von $L[x] = \varphi_x(L[x])$, wobei φ_x die eindeutige Fortsetzung von φ zu einem Ringautomorphismus von $L[x]$ mit $\varphi_x(x) = x$ bezeichnet. Nach Satz 6.2.3.1 ist $\mathbb{C}$ zu sich selbst bezüglich φ äquivalent – anders gesagt gibt es einen (nicht eindeutigen) Automorphismus ψ von $\mathbb{C}$, der φ fortsetzt.
Für die zweite, „rein algebraische“ Möglichkeit betrachten wir ein Element $\alpha \in \mathbb{C} \setminus L$ und sein Minimalpolynom $m(x)$ über L. Als irreduzibles Polynom über einem Körper der Charakteristik 0 hat $m(x)$ nur einfache Nullstellen (Vorgriff auf Satz 6.2.4.5 im nächsten Unterabschnitt), also muss es eine Nullstelle $\beta \neq \alpha$ geben. Gemäß Satz 6.1.3.4 gibt es einen (eindeutigen) Isomorphismus $\varphi : L(\alpha) \to L(\beta)$, der L punktweise fixiert und $\alpha \mapsto \beta$ leistet. Mit der analogen Notation zu oben gilt für den Isomorphismus $\varphi_x : L(\alpha)[x] \to L(\beta)[x]$ auch jetzt $\varphi_x(L[x]) = L[x]$, sodass wieder nach Satz 6.2.3.1 ein Automorphismus von $\mathbb{C}$ existiert, der φ fortsetzt.

Einschlägig interessierten Leserinnen[11] sei zum Abschluss noch die folgende Übungsaufgabe über die (große) Kardinalität der Körperautomorphismen-Gruppe von $\mathbb{C}$ empfohlen.

UE 364 ► **Übungsaufgabe 6.2.3.7.** (E) Zeigen Sie, dass der Transzendenzgrad von $\mathbb{C}$ über $\mathbb{Q}$ genau $|\mathbb{C}| = 2^{|\mathbb{N}|}$ ist. Beweisen Sie damit, dass $|\operatorname{Aut}(\mathbb{C})| = |\mathbb{C}|^{|\mathbb{C}|} = 2^{2^{|\mathbb{N}|}}$. ◄ **UE 364**
Hinweis: Proposition 6.2.2.7 und Unterabschnitt A.5.6 im Anhang.

6.2.4. Mehrfache Nullstellen und formale Ableitung

Inhalt in Kurzfassung: Hat ein reelles Polynom eine mehrfache Nullstelle, so liegt in dieser eine waagrechte Tangente vor. Es gilt auch die Umkehrung sowie eine Verallgemeinerung auf beliebige Körper. Dazu ist die Definition einer formalen Ableitung erforderlich, für die auch auf rein algebraischem Wege die aus der Analysis vertrauten Differentiationsregeln bewiesen werden können. Mit Hilfe der Produktregel können dann die angedeuteten Zusammenhänge zwischen mehrfachen Nullstellen und dem Verschwinden von Ableitungen bewiesen werden.

[11] Siehe Fußnote auf Seite 107.

An vielen Stellen der Theorie, vor allem bei endlichen Körpern und in der Galoistheorie, wird es von Interesse sein, ob ein (irreduzibles) Polynom in seinem Zerfällungskörper nur einfache oder auch mehrfache Nullstellen hat.
Als Beispiel betrachten wir das Polynom $f(x) := x^p - a$ mit einer Primzahl $p \in \mathbb{P}$ und einem Element a aus dem Grundkörper K. Ist z. B. $K = \mathbb{Q}$ (also $\operatorname{char} K = 0$) und $a \neq 0$, so lassen sich die Nullstellen von f als die p verschiedenen p-ten Wurzeln von a in $\mathbb{C}$ deuten. Ist hingegen $\operatorname{char} K = p$ und α eine Nullstelle von f in irgendeinem Erweiterungskörper L von K, so heißt das $\alpha^p = a$ und somit nach Satz 3.4.4.3: $x^p - a = x^p - \alpha^p = (x - \alpha)^p$. Also ist α sogar eine p-fache Nullstelle von f.
Ein bewährter Trick, um dieses Phänomen in den Griff zu bekommen, liegt in der Verwendung der formalen Ableitung von Polynomen. In der Analysis spiegeln sich Nullstellen höherer Vielfachheit im Verschwinden von Ableitungen wider. Wir nehmen dies zum Vorbild und definieren, allerdings ganz ohne Bezugnahme auf Grenzwerte, die Ableitung von Polynomen über beliebigen Körpern rein formal:

Definition 6.2.4.1. Sei $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, K ein beliebiger Körper. (Diese Definition ist auch allgemeiner für kommutative Ringe mit 1 sinnvoll.) Die *formale Ableitung* $f' \in K[x]$ von f ist definiert durch $f'(x) := \sum_{i=1}^{n} i a_i x^{i-1} = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i \in K[x]$. (Die Multiplikation mit der natürlichen Zahl i ist im Sinne der $\mathbb{Z}$-Modulstruktur abelscher Gruppen zu verstehen, d. h. als i-fache additive Potenz $ia := a + a + \ldots + a$ mit i Summanden.)

Proposition 6.2.4.2. *Die formale Ableitung von Polynomen über einem Körper K erfüllt die üblichen Differentiationsregeln:*

(1) *Summenregel:* $(f + g)' = f' + g'$.
(2) *Multiplikation mit einer Konstanten:* $(cf)' = cf'$ *für* $c \in K$.
(3) *Produktregel:* $(fg)' = fg' + f'g$.
(4) *Kettenregel:* $(f \circ g)'(x) = f'(g(x))g'(x)$.

UE 365 ▶ Übungsaufgabe 6.2.4.3. (V) Beweisen Sie Proposition 6.2.4.2. **◀ UE 365**

Der angekündigte Zusammenhang zwischen mehrfachen Nullstellen und formaler Ableitung lautet wie folgt:

Lemma 6.2.4.4. *Sei $f \in K[x]$ und L der Zerfällungskörper von f. Dann sind die folgenden beiden Aussagen äquivalent:*

(1) *Mindestens eine Nullstelle $\alpha \in L$ von f ist mehrfach.*
(2) *Die Polynome f und f' haben einen nichttrivialen* $\operatorname{ggT}(f, f')$ *in $K[x]$.*

Beweis. (1) $\Rightarrow$ (2): Habe $f \in K[x]$ in L eine mehrfache Nullstelle α, also $f(x) = (x - \alpha)^2 g(x)$ mit $g \in L[x]$. Dann ergibt sich nach der Produktregel aus Proposition 6.2.4.2

$$f'(x) = (x - \alpha)^2 g'(x) + 2(x - \alpha)g(x) = (x - \alpha)\left((x - \alpha)g'(x) + 2g(x)\right),$$

also $f'(\alpha) = 0$. Das Minimalpolynom m von α teilt daher sowohl f als auch f'. Mit anderen Worten: f und f' haben einen nichttrivialen gemeinsamen Teiler.
(2) $\Rightarrow$ (1): Sei nun vorausgesetzt, dass f und f' einen nichttrivialen gemeinsamen Teiler haben und indirekt angenommen, dass f im Zerfällungskörper L nur einfache Nullstellen habe. Ist α eine solche einfache Nullstelle von f in L, also $f(x) = (x - \alpha)g(x)$ mit $g \in L[x]$ und $g(\alpha) \neq 0$, so berechnen wir wieder mit der Produktregel $f'(x) = (x - \alpha)g'(x) + g(x)$, also $f'(\alpha) = g(\alpha) \neq 0$. Weil nichttriviale gemeinsame Teiler von f und f' aber gemeinsame Nullstellen im Zerfällungskörper bedeuten, folgt daraus, dass f und f' teilerfremd sind, Widerspruch. □

Für irreduzibles $f \in K[x]$ hat das bemerkenswerte Konsequenzen. Denn als Teiler von f kommen dann nur konstante Polynome und (bis auf Assoziiertheit, also bis auf multiplikative Konstante) f selbst in Frage. Ist $\mathrm{ggT}(f, f')$ nichttrivial, so folgt also $\mathrm{ggT}(f, f') = f$ und somit $f|f'$. Weil aber $\mathrm{grad}(f) \leq \mathrm{grad}(f')$ nicht möglich ist, gilt $f|f'$ genau dann, wenn $f' = 0$. Das schließt $\mathrm{char}\, K = 0$ aus. Im Fall $\mathrm{char}\, K = p \in \mathbb{P}$ hingegen ist $f' = 0$ sehr wohl möglich, nämlich genau dann, wenn in f nur solche Exponenten von x auftreten, die ein Vielfaches von p sind. In diesem Fall ist tatsächlich $\mathrm{ggT}(f, f') = \mathrm{ggT}(f, 0) = f$. Nach Lemma 6.2.4.4 hat f eine mehrfache Nullstelle. Damit haben wir bewiesen:

Satz 6.2.4.5. *Sei K ein Körper und $f(x) \in K[x]$ irreduzibel. In seinem Zerfällungskörper hat f genau dann eine mehrfache Nullstelle, wenn* $\mathrm{char}\, K = p$ *eine Primzahl und f von der Form $f(x) = g(x^p)$ mit $g \in K[x]$ ist. Insbesondere: Wenn* $\mathrm{char}\, K = 0$ *ist, dann hat f nur einfache Nullstellen.*

6.2.5. Einheitswurzeln und Kreisteilungspolynome

Inhalt in Kurzfassung: Die Zerlegung des Polynoms $x^n - 1$ in Linearfaktoren entspricht dem Aufsuchen von n-ten Einheitswurzeln, was in $\mathbb{C}$ geometrisch als Konstruktion des dem Einheitskreis eingeschriebenen regelmäßigen n-Ecks interpretiert werden kann. Daher rührt die Bezeichnung „Kreisteilungspolynom“ für gewisse, rekursiv definierte (sich bei Charakteristik 0 sogar als irreduzibel erweisende) Faktoren des Polynoms $x^n - 1$, dessen Nullstellen offenbar eine endliche multiplikative Untergruppe des Körpers bilden. Eine solche ist stets zyklisch.

Wir beginnen mit einem Satz, der auch für die Theorie endlicher Körper noch sehr wichtig sein wird.

Satz 6.2.5.1. *Jede endliche Untergruppe G der multiplikativen Gruppe eines Körpers, insbesondere die multiplikative Gruppe jedes endlichen Körpers, ist zyklisch.*

Beweis. Nach Lemma 3.3.3.1 gibt es ein $g_0 \in G$, dessen multiplikative Ordnung n_0 ein Vielfaches aller Ordnungen n_g von Elementen $g \in G$ ist. Also erfüllen alle $g \in G$ die Gleichung $g^{n_0} = 1$. Somit hat das Polynom $x^{n_0} - 1$ mindestens $|G|$ Nullstellen. Es folgt $|G| \leq n_0$ wegen Proposition 5.3.3.5. Da nach dem Satz von Lagrange umgekehrt n_0 ein Teiler von $|G|$ ist, folgt $|G| = n_0$, also ist g_0 erzeugendes Element der zyklischen Gruppe G. □

In jedem Körper K bilden die sogenannten n-ten *Einheitswurzeln*, das sind die Nullstellen des Polynoms $f_n(x) := x^n - 1$ ($n \in \mathbb{N}^+$), eine Untergruppe E_n der multiplikativen Gruppe von K. Weil es nur höchstens n Lösungen dieser Polynomgleichung geben kann, ist E_n endlich, nach Satz 6.2.5.1 also zyklisch. Die nun folgenden Überlegungen beziehen sich auf den Fall von $\operatorname{char} K = 0$, d. h., wir dürfen oBdA $\mathbb{Q}$ als Primkörper von K annehmen. Verwandte Überlegungen bei Primzahlcharakteristik werden in Unterabschnitt 6.3.1 folgen.
Die Ableitung $f_n'(x) = nx^{n-1}$ ist wegen $\operatorname{char} K = 0$ ungleich 0 und hat nur x als irreduziblen Faktor, ist also zu $f_n(x) = x^n - 1$ teilerfremd. Folglich hat f_n nach Lemma 6.2.4.4 in seinem Zerfällungskörper Z_n nur einfache Nullstellen. In Z_n ist also $E_n \cong C_n$ (nochmals wegen Satz 6.2.5.1) eine zyklische Gruppe der Ordnung n. Ihre Erzeugenden heißen *primitive n-te Einheitswurzeln.* Zu ihrer Bezeichnung werden wir traditionsgemäß meist den griechischen Buchstaben ζ verwenden. Sei ζ_n eine primitive n-te Einheitswurzel, also im Falle von $K = \mathbb{Q}$ z. B. $\zeta_n := e^{\frac{2\pi i}{n}} \in \mathbb{C}$ ($i \in \mathbb{C}$ imaginäre Einheit). Dann besteht E_n genau aus den Potenzen ζ_n^j, $j = 0, \ldots, n-1$, der primitiven Einheitswurzel, folglich gilt

$$f_n(x) = x^n - 1 = \prod_{j=0}^{n-1} (x - \zeta_n^j).$$

Insbesondere enthält der von ζ_n erzeugte Körper $K_n := \mathbb{Q}(\zeta_n)$ alle n-ten Einheitswurzeln und stimmt daher bereits mit dem Zerfällungskörper Z_n von $x^n - 1$ überein. Weil die Elemente von E_n in der komplexen Ebene ein regelmäßiges n-Eck auf dem Einheitskreis bilden, heißt K_n auch der n-te *Kreisteilungskörper*. Nach Satz 3.2.4.15 sind die Untergruppen der zyklischen Gruppe E_n genau die Gruppen E_k mit $k|n$. Weil E_k der Zerfällungskörper von $x^k - 1$ ist, gilt $f_k(x) = x^k - 1 | x^n - 1 = f_n(x)$ genau dann, wenn $k|n$. Diese Erkenntnis hilft bei der Suche nach Zerlegungen von $f_n(x) = x^n - 1 = \prod_{j=0}^{n-1}(x - \zeta_n^j)$ über K, bei der es offenbar darum geht, wie man gewisse der Faktoren $x - \zeta_n^j$ zusammenfassen kann, um wieder Polynome mit Koeffizienten in K zu bekommen. Analysiert man die Situation genauer, erkennt man:

Satz 6.2.5.2. *Definiert man die Polynome g_n, die sogenannten* Kreisteilungspolynome, *für $n \in \mathbb{N}^+$ durch $g_1(x) := x - 1$ und*

$$g_n(x) := \prod_{0 \le j < n-1,\ \operatorname{ggT}(j,n)=1} (x - \zeta_n^j),$$

so gilt

$$x^n - 1 = \prod_{d|n, 1 \le d \le n} g_d(x)$$

für alle $n \in \mathbb{N}^+$. Die Kreisteilungspolynome sind normiert, haben ausschließlich ganzzahlige Koeffizienten, der konstante Koeffizient ist entweder 1 oder -1, und die Grade erfüllen $\operatorname{grad}(g_n) = \varphi(n)$ *(Eulersche φ-Funktion).*

Beweis. Beachtet man $x^n - 1 = \prod_{j=0}^{n-1}(x - \zeta_n^j)$, so ergibt sich die behauptete Zerlegung $x^n - 1 = \prod_{d|n} g_d(x)$ aus der Tatsache, dass jede der n-ten Einheitswurzeln ζ_n^j, $j =$

$0, \ldots, n-1$, für genau ein $d|n$ eine primitive d-te Einheitswurzel ist. Außerdem gilt nach Definition $\operatorname{grad}(g_n) = \varphi(n)$. Aus $x^n - 1 = g_n(x)g_n^*(x)$ mit $g_n^*(x) := \prod_{d|n, 1 \leq d < n} g_d(x)$, liest man ab, dass sich induktiv die Normiertheit der g_d mit $d < n$ auf die von g_n^* und somit auf g_n überträgt, analog dass der konstante Koeffizient immer nur ± 1 sein kann. Das Polynom g_n erhält man durch Polynomdivision des ganzzahligen Polynoms $x^n - 1$ durch den normierten und ganzzahligen Teiler g_n^*, was die Ganzzahligkeit sämtlicher Koeffizienten von g_n garantiert. □

UE 366 ► **Übungsaufgabe 6.2.5.3.** (B) Ermitteln Sie die Kreisteilungspolynome $g_n(x)$ für alle $n \leq N$ und möglichst großes N. ◄ **UE 366**

Anmerkung 6.2.5.4. Mit etwas größerem Aufwand lässt sich zeigen, dass die Kreisteilungspolynome g_n sogar irreduzibel über $\mathbb{Q}$ sind, siehe Proposition 9.5.2.5 bzw. Übungsaufgabe 9.5.2.6 und die dortige Anleitung.

6.2.6. Beispiele einfacher Erweiterungen

Inhalt in Kurzfassung: Der Satz vom primitiven Element wird bewiesen: In Charakteristik 0 ist jede endlichdimensionale Erweiterung einfach (d. h., sie wird von einem einzigen, geeignet zu wählenden Element erzeugt). Erwähnt wird außerdem der Satz von Lüroth: Jeder Zwischenkörper Z mit $K \leq Z \leq K(x)$ ist eine einfache, für $K \neq Z$ transzendente Erweiterung über K.

Wir haben bereits systematisch alle Möglichkeiten einfacher Körpererweiterungen $K(\alpha)$ eines Körpers $K \leq L$ mit $\alpha \in L$ untersucht und sind dabei auf die Unterscheidung zwischen algebraischen und transzendenten Elementen α gestoßen. Manchmal ist es umgekehrt von Interesse, von einer gegebenen Erweiterung $K \leq L$ entscheiden zu können, ob sie einfach ist. In diesem Unterabschnitt werden für beide Fälle, algebraisch und transzendent, hinreichende Bedingungen gegeben. Auf den algebraischen Fall bezieht sich der sogenannte *Satz vom primitiven Element*, der übrigens auch unter etwas allgemeineren Voraussetzungen gilt, siehe Übungsaufgabe 9.2.5.8.

Satz 6.2.6.1 (vom primitiven Element)**.** *Ist L eine endlichdimensionale Körpererweiterung von K mit* $\operatorname{char} K = \operatorname{char} L = 0$*, so gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis. Wegen der endlichen Dimension der Erweiterung gibt es $u_1, \ldots, u_r \in L$ mit $L = K(u_1, \ldots, u_r)$. Wir führen den Beweis mittels Induktion nach r.
Für $r = 1$ ist die Aussage trivial. Wir nehmen daher an, der Satz gelte für $r - 1$ ($r > 1$). Wir haben dann: $L = K(u_1, \ldots, u_r) = K(u_1, \ldots, u_{r-1})(u_r) = K(\alpha)(u_r) = K(\alpha, \beta)$ für ein geeignetes $\alpha \in L$ und für $\beta = u_r$. Wegen $[K(\alpha, \beta) : K] < \infty$ sind α, β algebraisch über K. Wir zeigen, dass es ein $\delta \in L$ gibt mit $K(\alpha, \beta) = K(\delta)$.
Seien $f(x)$ bzw. $g(x)$ die Minimalpolynome von α bzw. β. Wir betrachten einen Erweiterungskörper M von L (insbesondere von K), der zugleich Nullstellenkörper von $f(x)$ und $g(x)$ ist, d. h. es gibt $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t \in M$ mit $f(x) = (x - \alpha_1) \cdots (x - \alpha_s)$

und $g(x) = (x-\beta_1)\cdots(x-\beta_t)$. Dabei sei oBdA $\alpha_1 = \alpha$ und $\beta_1 = \beta$. Nach Satz 6.2.4.5 ist $\beta \neq \beta_k$ für $k = 2, \ldots, t$, daher hat die Gleichung $\alpha_i + x\beta_k = \alpha + x\beta$ für jedes $i = 1, \ldots, s$ und $k = 2, \ldots, t$ höchstens eine Lösung in K. Da K unendlich ist (wegen $\operatorname{char} K = 0$), gibt es ein $c \in K$ mit $\alpha_i + c\beta_k \neq \alpha + c\beta$ für alle $i = 1, \ldots, s$ und $k = 2, \ldots, t$. Wir behaupten

$$K(\alpha, \beta) = K(\delta) \text{ mit } \delta := \alpha + c\beta \in L.$$

Trivialerweise ist $K(\delta) \subseteq K(\alpha, \beta)$. Für die umgekehrte Inklusion genügt es zu zeigen, dass $\alpha, \beta \in K(\delta)$. Dazu betrachten wir das Polynom $\bar{f}(x) := f(\delta - cx) \in K(\delta)[x]$. Es ist dann $\bar{f}(\beta) = f(\delta - c\beta) = f(\alpha) = 0$. Andererseits gilt $\bar{f}(\beta_k) = f(\delta - c\beta_k) = f(\alpha + c\beta - c\beta_k) \neq 0$ für $k = 2, \ldots, t$, da ja $\alpha + c\beta - c\beta_k \neq \alpha_i$ für $i = 1, \ldots, s$ nach Wahl von c. Also haben $g(x)$ und $\bar{f}(x)$ genau die eine Nullstelle β gemeinsam. Daher ist $x - \beta$ in $M[x]$ der ggT von $g(x)$ und $\bar{f}(x)$. Nach Aussage (2) von Übungsaufgabe 5.3.2.11 (für $K(\delta)$ statt K und M statt L) muss dieser ggT bereits in $K(\delta)[x]$ enthalten sein, also gilt $\beta \in K(\delta)$ und somit auch $\alpha = \delta - c\beta \in K(\delta)$. □

UE 367 ► Übungsaufgabe 6.2.6.2. (F) Man bestimme $\alpha \in \mathbb{C}$ so, dass $\mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(\alpha)$. **◄ UE 367**

Für transzendente Erweiterungen von Interesse ist der folgende *Satz von Lüroth*, der hier ohne Beweis erwähnt sei:

Satz 6.2.6.3 (von Lüroth)**.** *Sei K ein Körper und $L := K(x)$ der Körper der gebrochen rationalen Funktionen über K. Dann ist jeder Zwischenkörper Z (d. h. jeder Körper mit $K \leq Z \leq L$) eine einfache Körpererweiterung von K. Es gibt also ein $r = r(x) \in K(x)$ mit $Z = K(r(x))$. Ist $K \neq Z$, so ist $r \notin K$ transzendent über K und somit $K(r) \cong K(x) = L$.*

UE 368 ► Übungsaufgabe 6.2.6.4. (E) Beweisen Sie den Satz 6.2.6.3 von Lüroth, eventuell unter Zuhilfenahme von Literatur. **◄ UE 368**

UE 369 ► Übungsaufgabe 6.2.6.5. (B) Sei $L := \mathbb{Q}(x)$ der Körper der gebrochen rationalen Funktionen über $\mathbb{Q}$. **◄ UE 369**

(1) Berechnen Sie $[L : K]$ für $K := \mathbb{Q}(x^3) \leq L$, indem Sie das Minimalpolynom von x über K finden.

(2) Wie Teil (1), nur mit $K := \mathbb{Q}(x + \frac{1}{x})$.

(3) Zeigen Sie: $[L : K]$ ist endlich für jeden Körper $K := \mathbb{Q}(\alpha)$ mit $\alpha \in \mathbb{Q}(x) \setminus \mathbb{Q}$. Schließen Sie, dass jedes $\alpha \in \mathbb{Q}(x) \setminus \mathbb{Q}$ transzendent über $\mathbb{Q}$ ist.

UE 370 ► Übungsaufgabe 6.2.6.6. (F) Sei R der Polynomring $\mathbb{Z}_5[t]$, und sei $U \leq R$ der kleinste Unterring mit 1 von R, der das Polynom t^5 enthält. **◄ UE 370**

(1) Beschreiben Sie U (d.h., erklären Sie, wie Sie von einem beliebigen Polynom in R entscheiden können, ob es in U liegt).

(2) Geben Sie ein irreduzibles Polynom $p(x) \in U[x]$ an, welches in R die Nullstelle t hat.

6.3. Endliche Körper (Galoisfelder)

Die wichtigsten Inhalte dieses Abschnitts sind die folgenden: In 6.3.1 verwenden wir vor allem unser Wissen über Zerfällungskörper, um die endlichen Körper zu klassifizieren: Jeder endliche Körper K hat $|K| = p^n$ Elemente mit einer Primzahl p und $n \in \mathbb{N}$, $n \geq 1$. Umgekehrt gibt es zu jeder Primzahlpotenz p^n bis auf Isomorphie genau ein K mit $|K| = p^n$, nämlich den Zerfällungskörper des Polynoms $x^{p^n} - x$ über dem Primkörper $\mathbb{Z}_p$. Man nennt K das Galoisfeld[12] mit p^n Elementen und schreibt dafür auch $\mathrm{GF}(p^n)$. Üblich ist auch die Bezeichnung $\mathbb{F}_{p^n}$, die wir hier jedoch nicht verwenden. Die additive Gruppe von $\mathrm{GF}(p^n)$ ist isomorph zum n-fachen Produkt $(C_p)^n$ einer zyklischen Gruppe mit p Elementen, die multiplikative Gruppe ist selbst zyklisch, also isomorph zu C_{p^n-1}. Weiter geht es in 6.3.2 mit den Unterkörpern von $\mathrm{GF}(p^n)$: diese sind genau jene $\mathrm{GF}(p^k)$ mit $k|n$. Wegen $\mathrm{GF}(p^n) \cong \mathbb{Z}_p[x]/(f)$ für jedes irreduzible $f \in \mathbb{Z}_p[x]$ vom Grad n muss für die Konstruktion von $\mathrm{GF}(p^n)$ nur so ein f gefunden werden – in 6.3.3 zeigen wir, dass das möglich ist, in 6.3.4 folgt die Konstruktion selbst. Am Ende des Abschnitts wird in 6.3.5 auch noch der algebraische Abschluss $\mathrm{GF}(p^\infty)$ von $\mathbb{Z}_p$ und gleichzeitig jedes endlichen Körpers mit Charakteristik p beschrieben.

6.3.1. Klassifikation endlicher Körper

Inhalt in Kurzfassung: Sei K ein endlicher Körper, sei $P \cong \mathbb{Z}_p$, $p \in \mathbb{P}$, sein Primkörper und sei n die Dimension von K über P. Dann gilt offenbar $|K| = p^n$. Außerdem erweist sich K sehr schnell als Zerfällungskörper des Polynoms $x^{p^n} - x$ über P. Als solcher ist K aufgrund der Ergebnisse aus Unterabschnitt 6.2.3 durch seine Kardinalität bis auf Isomorphie eindeutig bestimmt. Umgekehrt lässt sich mit Hilfe der Methoden aus Unterabschnitt 6.2.2 der Zerfällungskörper des Polynoms $x^{p^n} - x$ über P konstruieren und hat auch tatsächlich p^n Elemente. Damit ist ein Klassifikationssatz für endliche Körper vollständig bewiesen.

Sei K ein endlicher Körper. Dann ist $\mathrm{char}\, K = p \in \mathbb{P}$, und der Primkörper P von K ist isomorph zu $\mathbb{Z}_p$ (vgl. Satz 6.1.1.8). Da K ein Vektorraum über dem Unterkörper P ist, gibt es eine Basis $\{a_1, \ldots, a_n\}$ von K über P, also $[K : P] = n \in \mathbb{N}^+$. Daher ist $K = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in P\}$ und $|K| = p^n$, da jeder Koeffizient λ_i auf $|P| = p$ Arten gewählt werden kann.

Frage: Seien umgekehrt $p \in \mathbb{P}$ und $n \in \mathbb{N}^+$ gegeben. Gibt es einen Körper K mit $|K| = p^n$?

[12] Évariste Galois (1811-1832)

Wenn es einen solchen Körper K gibt, dann mit $\operatorname{char} K = p$, also können wir ihn jedenfalls mit Primkörper $\mathbb{Z}_p$ finden. Die multiplikative Gruppe $K^* = K \setminus \{0\}$ von K hat $p^n - 1$ Elemente. Nach dem Satz von Lagrange gilt daher $a^{p^n-1} = 1$ für alle $a \in K^*$, womit alle $a \in K^*$ Nullstellen des Polynoms $x^{p^n-1} - 1$ sind. Multiplizieren wir dieses Polynom mit x, so erhalten wir das Polynom $f(x) := x^{p^n} - x \in \mathbb{Z}_p[x]$, das auch 0 als Nullstelle hat. Sein Grad ist p^n, und es hat p^n verschiedene Nullstellen, nämlich alle Elemente von K. Es gilt daher:

$$f(x) = x^{p^n} - x = \prod_{\alpha \in K} (x - \alpha),$$

und K ist der Zerfällungskörper von f über $\mathbb{Z}_p$. Als solcher ist K nach Satz 6.2.3.1 bis auf Isomorphie eindeutig bestimmt.
Wir haben also gezeigt: Wenn es einen Körper K mit p^n Elementen gibt, so muss K der Zerfällungskörper des Polynoms $f(x) := x^{p^n} - x$ über $\mathbb{Z}_p$ sein.
Für den angestrebten Klassifikationssatz haben wir nur noch zu beweisen, dass der Zerfällungskörper Z von f wirklich p^n Elemente hat. Zunächst schließen wir aus $f'(x) = p^n x^{p^n-1} - 1 = -1$, dass f und f' teilerfremd sind, was nach Lemma 6.2.4.4 sicherstellt, dass alle Nullstellen von f im Zerfällungskörper Z einfach sind. Die Menge N aller Nullstellen von f in Z hat somit p^n Elemente. Um N bereits als den gesuchten Körper mit p^n Elementen zu identifizieren, genügt der Beweis von:

Lemma 6.3.1.1. *Im Zerfällungskörper Z des Polynoms $f(x) := x^{p^n} - x$ über dem Primkörper $\mathbb{Z}_p$ bildet die Menge N aller Nullstellen von f einen Unterkörper. Folglich ist $N = Z$.*

Beweis. N besteht genau aus jenen $\alpha \in Z$ mit $\alpha^{p^n} = \alpha$, insbesondere also $0, 1 \in N$. Für $\alpha, \beta \in N$, also $\alpha^{p^n} = \alpha$ und $\beta^{p^n} = \beta$, gilt außerdem:

- $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$, also $\alpha + \beta \in N$. (nach Satz 3.4.4.3)
- $(-\alpha)^{p^n} = (-1)^{p^n}(\alpha^{p^n}) = -\alpha$, also $-\alpha \in N$. (Man beachte, dass für $p = 2$ die Gleichung $1 = -1$ gilt.)
- $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$, also $\alpha\beta \in N$.
- $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$, also $\alpha^{-1} \in N$, sofern $\alpha \neq 0$. □

Aus dem Bisherigen folgt nun unmittelbar der *Klassifikationssatz für endliche Körper*:

Satz 6.3.1.2. *Die Kardinalität jedes endlichen Körpers ist eine Primzahlpotenz p^n ($p \in \mathbb{P}$, $n \in \mathbb{N}^+$). Umgekehrt gibt es zu jeder Primzahlpotenz p^n bis auf Isomorphie genau einen Körper K mit $|K| = p^n$, nämlich den Zerfällungskörper des Polynoms $x^{p^n} - x$, der ausschließlich aus den Nullstellen dieses Polynoms besteht.*

Definition 6.3.1.3. Sei $p \in \mathbb{P}$ und $n \in \mathbb{N}^+$. Man schreibt den bis auf Isomorphie eindeutigen Körper mit p^n Elementen als $\mathrm{GF}(p^n)$ und nennt ihn das *Galoisfeld* mit p^n Elementen. Statt $\mathrm{GF}(p)$ schreiben wir wie schon bisher meistens $\mathbb{Z}_p$.

Für die spätere (Wieder-)Verwendung isolieren wir aus den obigen Überlegungen über die formale Ableitung von $x^{p^n} - x$ noch die folgende Tatsache:

Lemma 6.3.1.4. *Das Polynom $x^{p^n} - x \in \mathbb{Z}_p[x]$ hat in seinem Zerfällungskörper nur einfache Nullstellen.*

Der Satz von Wedderburn besagt, dass alle endlichen Schiefkörper kommutativ sind, dass man also keine weiteren Strukturen vorfindet, wenn man auf die Kommutativität der Multiplikation eines Körpers verzichten würde. Der Beweis erfordert die sogenannte *Klassengleichung*, ein Instrument aus der Theorie der *Gruppenaktionen*; siehe Algebra II (Unterabschnitt 8.1.5).

Satz 6.3.1.5. *Jeder endliche Schiefkörper ist ein Körper, also isomorph zu einem* $\mathrm{GF}(p^n)$.

Die Quaternionen als prominentestes Beispiel eines Schiefkörpers belegen, dass unendliche Schiefkörper, die keine Körper sind, sehr wohl existieren.

6.3.2. Die Unterkörper eines endlichen Körpers

Inhalt in Kurzfassung: Ist K ein Unterkörper des endlichen Körpers E, so muss, weil beide denselben Primkörper $P \cong \mathbb{Z}_p$ haben, ihre Charakteristik $p \in \mathbb{P}$ übereinstimmen. Folglich gilt $|K| = p^k$ und $|E| = p^n$ mit geeigneten positiven natürlichen Zahlen k und n. Aus dem Gradsatz folgt daraus fast unmittelbar $k|n$. Umgekehrt erweist sich bei $k|n$ das Polynom $x^{p^k} - x$ (dessen Zerfällungskörper ja K ist) als Teiler des Polynoms $x^{p^n} - x$ (dessen Zerfällungskörper wiederum E ist), sodass jeder Körper E mit p^n Elementen einen (sogar eindeutig bestimmten) Unterkörper K mit p^k Elementen als Unterkörper enthält. Damit sind die Inklusionsbeziehungen zwischen endlichen Körpern vollständig geklärt.

Sei p eine feste Primzahl. Unser Ziel ist zu verstehen, welche Unterkörper ein endlicher Körper hat. Vollständige Auskunft darüber wird Satz 6.3.2.4 geben. Zur Vorbereitung brauchen wir aber noch ein Lemma über die Teilbarkeit gewisser ganzzahliger Polynome:

Lemma 6.3.2.1. *Seien $k, n \in \mathbb{N}$ mit $k|n$ und $p \in \mathbb{P}$. Dann gilt:*

(1) $x^k - 1 | x^n - 1$ *in* $\mathbb{Z}[x]$ *und in* $\mathbb{Z}_p[x]$.

(2) $p^k - 1 | p^n - 1$ *in* $\mathbb{Z}$.

(3) $x^{p^k-1} - 1 | x^{p^n-1} - 1$ *in* $\mathbb{Z}[x]$ *und in* $\mathbb{Z}_p[x]$. *Insbesondere gilt* $x^{p^k} - x | x^{p^n} - x$.

Die dabei auftretenden Polynome können alternativ sogar als Polynome über einem beliebigen kommutativen Ring mit 1 *aufgefasst werden.*

Beweis.

(1) Folgt aus $x^n - 1 = (x^k - 1)(x^{n-k} + x^{n-2k} + \cdots + x^k + 1)$.

(2) In der ersten Behauptung $x = p$ einsetzen.

(3) In Aussage (1) kann (wegen Aussage (2)) k durch $p^k - 1$ sowie n durch $p^n - 1$ ersetzt werden. □

Es stellt sich heraus, dass ein endlicher Körper nur eine einzige Kopie jedes Unterkörpers enthalten kann. Tatsächlich gilt sogar etwas mehr – es kommt nämlich nur darauf an, dass der Unterkörper endlich ist.

Proposition 6.3.2.2. *Sei L ein Körper und seien $K_1, K_2 \leq L$ endliche Unterkörper mit $|K_1| = |K_2| = p^n$. Dann gilt $K_1 = K_2$.*

Beweis. Da L Unterkörper der Kardinalität p^n enthält, muss L Charakteristik p haben, d. h., sein Primkörper ist $P \cong \mathbb{Z}_p$. Wir wissen aus Satz 6.3.1.2, dass alle Elemente von K_1 und von K_2 Nullstellen des Polynoms $x^{p^n} - x \in P[x]$ sind. Würden K_1 und K_2 nicht übereinstimmen, dann würde L mehr als p^n Nullstellen eines Polynoms vom Grad p^n enthalten, was Proposition 5.3.3.5 widerspricht. □

UE 371 ▶ **Übungsaufgabe 6.3.2.3.** (B) Finden Sie zwei Beispiele, die zeigen, dass Proposition 6.3.2.2 für unendliche Körper K_1, K_2 nicht gilt; genauer: Finden Sie zwei Körper L_1, L_2 und jeweils zwei (notwendigerweise unendliche) *isomorphe aber verschiedene* Unterkörper $K_{11}, K_{12} \leq L_1$ sowie $K_{21}, K_{22} \leq L_2$, indem Sie ◀ **UE 371**

(1) L_1 als den Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$ wählen.

(2) $L_2 = \mathbb{Q}(x)$ wählen.

Mit dieser Proposition können wir nun den folgenden Satz beweisen:

Satz 6.3.2.4. *Als Unterkörper von* $\mathrm{GF}(p^n)$ *treten genau die* $\mathrm{GF}(p^k)$ *mit $k|n$ auf, jeder genau einmal.*

Beweis. Dass als Unterkörper von $\mathrm{GF}(p^n)$ nur die $\mathrm{GF}(p^k)$ mit $k|n$ auftreten können, ergibt sich schnell aus dem Gradsatz 6.1.2.2. Sei dazu $\mathrm{GF}(p^k) \leq \mathrm{GF}(p^n)]$ und $d := [\mathrm{GF}(p^n) : \mathrm{GF}(p^k)]$. Es folgt

$$n = [\mathrm{GF}(p^n) : \mathbb{Z}_p] = [\mathrm{GF}(p^n) : \mathrm{GF}(p^k)] \cdot [\mathrm{GF}(p^k) : \mathbb{Z}_p] = d \cdot k,$$

also $k|n$.
Wegen Proposition 6.3.2.2 kann $\mathrm{GF}(p^n)$ höchstens eine einzige Kopie von $\mathrm{GF}(p^k)$ als Unterkörper enthalten. Das ist für $k|n$ auch tatsächlich der Fall: Denn laut der dritten Aussage von Lemma 6.3.2.1 ist $x^{p^k} - x$ ein Teiler von $x^{p^n} - x$ im Polynomring über dem Primkörper $P \cong \mathbb{Z}_p$, weshalb jede Nullstelle von $x^{p^k} - x$ auch eine von $x^{p^n} - x$ ist. Also ist der Zerfällungskörper $\mathrm{GF}(p^k)$ des Polynoms $x^{p^k} - x$ im Zerfällungskörper $\mathrm{GF}(p^n)$ des Polynoms $x^{p^n} - x$ enthalten. □

UE 372 ▶ **Übungsaufgabe 6.3.2.5.** (E) Sei $p \in \mathbb{P}$. Man zeige, dass in jedem Polynomring über einem kommutativen Ring mit 1 gilt: $x^{p^k} - x | x^{p^n} - x \Leftrightarrow k|n$. ◀ **UE 372**

6.3.3. Irreduzible Polynome über endlichen Primkörpern

Inhalt in Kurzfassung: Die Klassifikation endlicher Körper aus Unterabschnitt 6.3.1 und ihrer Unterkörper aus Unterabschnitt 6.3.2 zusammen mit der Zerlegung der Polynome

$x^{p^n} - x$ über dem Primkörper $P \cong \mathbb{Z}_p$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$, in (normierte) irreduzible Faktoren zeigt, dass als solche Faktoren genau jene irreduziblen (und normierten) Polynome über P auftreten, deren Grad ein Teiler von n ist, wobei jeder Faktor Vielfachheit 1 hat. Daraus ergeben sich mehrere interessante Folgerungen: Zu jedem positiven Grad gibt es mindestens ein irreduzibles Polynom über P, das sogar als primitiv gewählt werden kann. Letzteres bedeutet, dass seine Nullstellen die multiplikative Gruppe seines Zerfällungskörpers K erzeugen. Da jeder Automorphismus von K die Nullstellen jedes irreduziblen Faktors von $x^{p^n} - x$ permutiert, schließt man daraus, dass K genau n verschiedene Automorphismen hat – ein erstes Ergebnis im Geiste der Galoistheorie, siehe Kapitel 9.

Nach den Ergebnissen in Unterabschnitt 6.3.1 und Unterabschnitt 6.3.2 sind endliche Körper der Kardinalität p^n eng verbunden mit dem Polynom $x^{p^n} - x$ über dem Primkörper $P \cong \mathbb{Z}_p$. Andererseits führt auch die Konstruktion aus dem Satz von Kronecker (Proposition 6.2.1.1) angewandt auf ein in $\mathbb{Z}_p[x]$ irreduzibles Polynom vom Grad n auf einen Körper vom Grad n über $\mathbb{Z}_p$, also mit p^n Elementen. Die Verbindung dieser beiden Blickwinkel führt auf einige interessante Einsichten, denen wir uns in diesem Unterabschnitt widmen wollen.

Proposition 6.3.3.1. *Sei $n \in \mathbb{N}$ mit $n \geq 1$, p eine Primzahl, $K \cong \mathrm{GF}(p^n)$ ein Körper mit p^n Elementen und $P \cong \mathbb{Z}_p$ der Primkörper von K. Dann gilt:*

(1) *K ist der Zerfällungskörper nicht nur des Polynoms $x^{p^n} - x$, sondern jedes irreduziblen Polynoms $f \in P[x]$ vom Grad n. Ist $\alpha \in K$ eine Nullstelle von f, so gilt sogar $K = P(\alpha)$.*

(2) *Ist $f \in P[x]$ ein irreduzibles Polynom vom Grad n, so ist f in $P[x]$ ein Teiler von $x^{p^n} - x$.*

(3) *Ist $f \in P[x]$ ein irreduzibles Polynom vom Grad n, so hat f genau n paarweise verschiedene Nullstellen in K – es gibt also keine mehrfachen Nullstellen.*

(4) *Die irreduziblen und normierten Faktoren von $x^{p^n} - x$ sind genau jene irreduziblen und normierten Polynome über P, deren Grad ein Teiler von n ist. Die Vielfachheit all dieser Faktoren ist 1.*

Beweis.

(1) Sei $f \in P[x]$ irreduzibel vom Grad n, oBdA normiert. Wir betrachten den Zerfällungskörper der Menge $\{x^{p^n} - x, f\}$ über P und nennen ihn L. Sei weiters $\alpha \in L$ eine Nullstelle von f. Da f irreduzibel ist, ist f sogar das Minimalpolynom von α, sodass $P(\alpha) \leq L$ wegen Satz 6.1.3.4 ein Körper mit $[P(\alpha) : P] = n$ ist. Somit gilt $|P(\alpha)| = p^n$. Der Körper K (mit ebenfalls p^n Elementen) ist als Zerfällungskörper von $x^{p^n} - x$ ebenfalls in L enthalten. Nach Proposition 6.3.2.2 gilt $K = P(\alpha)$, insbesondere $\alpha \in K$. Da α beliebig war, ist K ein Nullstellenkörper von f, der von einer Nullstelle von f (insbesondere also von der Menge aller Nullstellen) erzeugt wird. Mit anderen Worten ist K der Zerfällungskörper von f.

(2) Sei $\alpha \in K$ eine Nullstelle von f. (Nach dem ersten Punkt enthält K sogar alle Nullstellen.) Wir wissen bereits aus Satz 6.3.1.2, dass K genau aus den Nullstellen

von $x^{p^n} - x$ besteht. Als Minimalpolynom von α teilt f jedes Polynom, das α als Nullstelle hat, insbesondere also $x^{p^n} - x$.

(3) Das Polynom $x^{p^n} - x$ hat nach Lemma 6.3.1.4 keine mehrfachen Nullstellen, daher auch nicht sein Teiler f.

(4) Sei $f \in P[x]$ ein irreduzibles (und normiertes) Polynom vom Grad k, das $x^{p^n} - x$ teilt. Im Körper K zerfällt f daher in Linearfaktoren. Sei $\alpha \in K$ eine Nullstelle von f. Dann folgt $P(\alpha) \cong P[x]/(f) \cong \mathrm{GF}(p^k)$ aus dem ersten Punkt (angewandt auf k statt n) und Satz 6.1.3.4. Weil es sich bei $P(\alpha)$ um einen Unterkörper von $K \cong \mathrm{GF}(p^n)$ handelt, erhalten wir $k|n$ gemäß Satz 6.3.2.4.

Sei nun umgekehrt $f \in P[x]$ ein irreduzibles (und normiertes) Polynom vom Grad $k|n$. Nach dem ersten Punkt (angewandt auf k anstatt n) gilt $f|x^{p^k} - x$. Wegen Lemma 6.3.2.1 gilt $x^{p^k} - x|x^{p^n} - x$, sodass insgesamt $f|x^{p^n} - x$ folgt.

Schließlich bemerken wir, dass die Vielfachheit aller irreduzibler normierter Faktoren von $x^{p^n} - x$ genau 1 sein muss, da $x^{p^n} - x$ nach Lemma 6.3.1.4 in seinem Zerfällungskörper (also K) nur einfache Nullstellen hat. □

Der Körper $K \cong \mathrm{GF}(p^n)$ wird also von der Nullstelle eines beliebigen irreduziblen Polynoms über dem Primkörper, das Grad n hat, erzeugt – man beachte, dass es sich dabei um das Erzeugnis als Körper handelt. Tatsächlich kann man dies für gewisse Polynome auf das Erzeugnis in der multiplikativen Gruppe verstärken.

Definition 6.3.3.2. Sei $f \in \mathbb{Z}_p[x]$ ein irreduzibles Polynom vom Grad n. Das Polynom heißt *primitiv*[13], wenn f eine Nullstelle $\alpha \in \mathrm{GF}(p^n)$ hat, die die multiplikative Gruppe $\mathrm{GF}(p^n)^* = \mathrm{GF}(p^n) \setminus \{0\}$ erzeugt, d. h. $\mathrm{GF}(p^n)^* = \{\alpha^j \mid j \in \mathbb{N}\}$ (äquivalent: wenn jede Nullstelle von f die multiplikative Gruppe erzeugt; siehe Übungsaufgabe 6.3.3.3).

UE 373 ► **Übungsaufgabe 6.3.3.3.** (F) Zeigen Sie: Ein irreduzibles Polynom $f \in \mathbb{Z}_p[x]$ vom Grad n ist genau dann primitiv, wenn *jede* Nullstelle $\alpha \in \mathrm{GF}(p^n)$ von f die multiplikative Gruppe von $\mathrm{GF}(p^n)$ erzeugt. ◄ **UE 373**

Äquivalent: Wenn $f \in \mathbb{Z}_p[x]$ primitiv vom Grad n ist und $\alpha \in \mathrm{GF}(p^n)$ eine Nullstelle von f ist, dann gilt $\mathrm{GF}(p^n)^* = \{\alpha^j \mid j = 0, \ldots, p^n - 2\} = \{\alpha^j \mid j = 1, \ldots, p^n - 1\}$.

Will man einen endlichen Körper explizit konstruieren bzw. beschreiben, so sind primitive Polynome sehr nützlich; siehe Unterabschnitt 6.3.4.

Lemma 6.3.3.4. *Zu jedem $n \geq 1$ gibt es mindestens ein primitives (insbesondere also ein irreduzibles) Polynom vom Grad n.*

Beweis. Nach Satz 6.2.5.1 ist die ($(p^n - 1)$-elementige) multiplikative Gruppe $\mathrm{GF}(p^n)^*$ zyklisch, wird also von einem $\alpha \in \mathrm{GF}(p^n)^*$ erzeugt, d. h. $\mathrm{GF}(p^n)^* = \{\alpha^j \mid j = 0, \ldots, p^n - 2\}$. Sei $f \in \mathbb{Z}_p[x]$ das Minimalpolynom über $\mathbb{Z}_p$ von α. Da α jedenfalls den Körper $\mathrm{GF}(p^n)$ erzeugt, also $\mathrm{GF}(p^n) = \mathbb{Z}_p(\alpha)$, schließen wir aus Satz 6.1.3.4, dass $n = [\mathrm{GF}(p^n) : \mathbb{Z}_p] = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = \mathrm{grad}(f)$. Somit haben wir das gesuchte Polynom gefunden. □

[13] Achtung: Dieser Begriff eines primitiven Polynoms ist zu unterscheiden von jenem mit dem gleichem Namen aus Unterabschnitt 5.3.2, als es um Polynome über faktoriellen Ringen ging.

Bemerkenswert ist auch die folgende Betrachtung der Automorphismen eines endlichen Körpers, die auf die Galoistheorie (siehe Kapitel 9) vorausweist.

Proposition 6.3.3.5. *Sei $n \in \mathbb{N}$ mit $n \geq 1$, p eine Primzahl, $K \cong \mathrm{GF}(p^n)$ ein Körper mit p^n Elementen und $P \cong \mathbb{Z}_p$ der Primkörper von K. Dann gilt:*

(1) *Ist f irgendein irreduzibles Polynom über P vom Grad n und sind $\alpha_1, \ldots, \alpha_n \in K$ die Nullstellen von f (nach Proposition 6.3.3.1 paarweise verschieden), so permutiert jeder Automorphismus $\varphi\colon K \to K$ die Elemente $\alpha_1, \ldots, \alpha_n$. Zu jedem $i = 1, \ldots, n$ gibt es genau einen Automorphismus φ_i von K mit $\varphi_i : \alpha_1 \mapsto \alpha_i$.*

(2) *Es gibt genau n Automorphismen von $K \cong \mathrm{GF}(p^n)$.*

Beweis.

(1) Wir schreiben $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ mit $a_0, \ldots, a_{n-1} \in P$. Wegen Proposition 6.1.1.4 hält φ die Elemente des Primkörpers punktweise fest. Insbesondere gilt $\varphi(a_j) = a_j$ für alle $j = 0, \ldots, n-1$. Daraus folgt

$$\begin{aligned} f(\varphi(\alpha_i)) &= \varphi(\alpha_i)^n + a_{n-1}\varphi(\alpha_i)^{n-1} + \cdots + a_0 \\ &= \varphi(\alpha_i^n) + \varphi(a_{n-1})\varphi(\alpha_i^{n-1}) + \cdots + \varphi(a_0) \\ &= \varphi(\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \cdots + a_0) = \varphi(f(\alpha_i)) = \varphi(0) = 0, \end{aligned}$$

also $\varphi(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\}$. Als Automorphismus ist φ und damit auch die Einschränkung auf $\{\alpha_1, \ldots, \alpha_n\}$ jedenfalls injektiv. Da diese Menge endlich ist, folgt, dass die Einschränkung eine Permutation von $\{\alpha_1, \ldots, \alpha_n\}$ ist.

Um die zweite Aussage zu zeigen, bemerken wir, dass es für jedes $i = 1, \ldots, n$ nach Satz 6.1.3.4 genau einen Isomorphismus $\varphi_i : P(\alpha_1) \to P(\alpha_i)$ gibt, der P punktweise festlässt und $\alpha_1 \mapsto \alpha_i$ leistet. Nach Proposition 6.3.3.1 gilt $P(\alpha_1) = K = P(\alpha_i)$. Folglich ist φ_i ein Automorphismus von K. Da jeder Automorphimus von K den Primkörper P jedenfalls festhalten muss, folgt die Eindeutigkeit daraus, dass K von $P \cup \{\alpha_1\}$ erzeugt wird.

(2) Sei $f \in P[x]$ ein irreduzibles Polynom vom Grad n und seien $\alpha_1, \ldots, \alpha_n \in K$ die Nullstellen von K. Im ersten Punkt haben wir bereits n verschiedene Automorphismen gefunden, nämlich die eindeutigen Automorphismen φ_i, die $\alpha_1 \mapsto \alpha_i$ leisten. Es bleibt zu zeigen, dass es keine weiteren Automorphismen geben kann. Nach Proposition 6.3.3.1 gilt $P(\alpha_1) = K$, sodass ein Automorphismus von K durch das Bild von α_1 eindeutig bestimmt ist (da die Elemente des Primkörpers jedenfalls punktweise festgehalten werden müssen). Wieder wegen des ersten Punktes kommen als Bilder nur $\alpha_1, \ldots, \alpha_n$ infrage, also sind $\varphi_1, \ldots, \varphi_n$ tatsächlich die einzigen Automorphismen. □

Die letzte Proposition liefert theoretisch auch eine explizite Beschreibung aller Automorphismen eines endlichen Körpers. Viel praktischer ist aber der folgende Satz:

Satz 6.3.3.6. *Die Automorphismen von $\mathrm{GF}(p^n)$ sind genau die Abbildungen der Form $a \mapsto a^{p^k}$ mit $k = 0, 1, \ldots, n-1$ (die sogenannten* Frobeniusautomorphismen*). Sie bilden eine zyklische Gruppe, die vom Automorphismus $a \mapsto a^p$ erzeugt wird.*

UE 374 ► **Übungsaufgabe 6.3.3.7.** (V,W) Beweisen Sie Satz 6.3.3.6, indem Sie folgendes zeigen: ◄ **UE 374**

(1) Ist p eine Primzahl und ist $n \in \mathbb{N}$, $n \geq 1$, so ist die Abbildung $\varphi : a \mapsto a^p$ ein Automorphismus von $\mathrm{GF}(p^n)$.

(2) Die in der Automorphismengruppe $\mathrm{Aut}(\mathrm{GF}(p^n))$ von φ erzeugte Untergruppe besteht aus allen $\varphi^k : a \mapsto a^{p^k}$ mit $k = 0, \ldots, n-1$.[14] Dabei sind die φ^k für $k = 0, \ldots, n-1$ paarweise verschieden. Wieso ist damit der Beweis abgeschlossen?

Bei unendlichen Körpern hingegen kann es auch Automorphismen geben, die keine Frobeniusautomorphismen sind:

UE 375 ► **Übungsaufgabe 6.3.3.8.** (B) Sei p eine Primzahl. Finden Sie einen Körper K der Charakteristik p und einen nichttrivialen Automorphismus $f\colon K \to K$, der nicht von der Form $f(a) = a^{p^k}$ ist. (Hinweis: Finden Sie zunächst einen nichttrivialen Automorphismus des Rings $\mathbb{Z}_p[x, y]$.) ◄ **UE 375**

Umgekehrt kann $a \mapsto a^p$ bei unendlichen Körpern ein Automorphismus sein, muss es aber nicht.

UE 376 ► **Übungsaufgabe 6.3.3.9.** (B) Geben Sie einen unendlichen Körper K der Charakteristik p an, für den die Abbildung $a \mapsto a^p$ einen Automorphismus von K definiert. (Hinweis: algebraischer Abschluss) ◄ **UE 376**

UE 377 ► **Übungsaufgabe 6.3.3.10.** (B) Geben Sie einen unendlichen Körper K der Charakteristik p an, für den die Abbildung $a \mapsto a^p$ *keinen* Automorphismus von K definiert. ◄ **UE 377**

UE 378 ► **Übungsaufgabe 6.3.3.11.** (F) Sei K ein endlicher Körper, und sei P der Primkörper von K. Zeigen Sie, dass es einen Automorphismus φ von K gibt mit $\{x \in K \mid \varphi(x) = x\} = P$. ◄ **UE 378**

UE 379 ► **Übungsaufgabe 6.3.3.12.** (F) Sei K ein Körper der Charakteristik $p > 0$. Man zeige: $x^p + a \in K[x]$ ist entweder irreduzibel, oder p-te Potenz eines linearen Polynoms. ◄ **UE 379**

6.3.4. Konstruktion endlicher Körper

Inhalt in Kurzfassung: Wir wissen bereits, dass jeder endliche Körper K der Kardinalität p^n, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$, als Zerfällungskörper des Polynoms $x^{p^n} - x$ über seinem Primkörper $P \cong \mathbb{Z}_p$ bis auf Isomorphie eindeutig bestimmt ist. Was also soll es heißen, wenn von der „Konstruktion“ von K die Rede ist? Weil K ein Vektorraum über P ist, entpuppt sich seine additive Struktur als die direkte Summe $C_p \oplus \ldots \oplus C_p$ von n Kopien der

[14] Mit a^{p^k} ist natürlich $a^{(p^k)}$ gemeint, nicht $(a^p)^k = a^{pk}$.

zyklischen Gruppe C_p mit p Elementen. Ähnlich ist die multiplikative Gruppe für sich wegen Satz 6.2.5.1 als zyklische Gruppe zu C_{p^n-1} isomorph. Um mit diesen Darstellungen effektiv zu arbeiten, ist allerdings für die additive Struktur eine Basis von K über P gefragt, für die multiplikative hingegen ein primitives Element, d. h. ein erzeugendes Element der multiplikativen Gruppe. Ein Zusammenhang der beiden ist zunächst aber noch nicht sichtbar. In Hinblick auf eine algorithmische Bewältigung der Körperstruktur von entscheidendem Wert ist daher eine Art „Übersetzungstabelle“. Dafür genügt es, für ein (durch eine multiplikative Eigenschaft definiertes) primitives Element auch die Darstellung seiner Potenzen bezüglich einer Basis der Vektorraumstruktur anzugeben. Wir untersuchen im Folgenden, wie das mit Hilfe der mittlerweile entwickelten Strukturtheorie gelingt. Als Beispiel wird ein Körper mit $9 = 3^2$ Elementen konstruiert.

Jeder endliche Körper K ist isomorph zu einem $\mathrm{GF}(p^n)$ und somit ein n-dimensionaler Vektorraum über dem Primkörper $P \cong \mathbb{Z}_p$. Folglich ist die additive Gruppe isomorph zu $(C_p)^n$, der direkten Summe von n Kopien der zyklischen Gruppe C_p. Auch die multiplikative Struktur von $\mathrm{GF}(p^n)$ ist sehr einfach. Die multiplikative Gruppe $\mathrm{GF}(p^n)^*$ ist nämlich wegen Satz 6.2.5.1 isomorph zu C_{p^n-1}, der zyklischen Gruppe der Ordnung $p^n - 1$. Für endliche Körper kennen wir also sowohl die additive als auch die multiplikative Struktur vollständig. Dennoch ist damit aber noch nicht geklärt, wie additive und multiplikative Struktur zusammenspielen. Auskunft darüber bietet die Theorie, indem sie sagt, dass ein Körper $K \cong \mathrm{GF}(p^n)$, $p \in \mathbb{P}$, $n \in \mathbb{N}^+$ über dem Primkörper $P := \mathbb{Z}_p$ als Faktorring $\mathbb{Z}_p[x]/(f)$ mit einem irreduziblen Polynom $f \in \mathbb{Z}_p$ vom Grad n erhalten werden kann. Aus Lemma 6.3.3.4 wissen wir, dass es so ein f gibt, auch ein primitives. Exemplarisch soll nun $\mathrm{GF}(9)$ konstruiert werden.

Beispiel 6.3.4.1. Bestimmung von $K = \mathrm{GF}(9) = \mathrm{GF}(3^2)$: Wir nehmen $\mathbb{Z}_3 = \{0, 1, 2\}$ als Primkörper. Das Polynom $x^2-x-1 \in \mathbb{Z}_3[x]$ ist irreduzibel, da es in $\mathbb{Z}_3$ keine Nullstelle hat. Somit ist $\mathbb{Z}_3[x]/(x^2 - x - 1) \cong \mathbb{Z}_3(\alpha) = \mathrm{GF}(9)$, wobei $\alpha^2 = \alpha + 1$ gilt. Daraus folgt auch $\alpha^3 = \alpha\alpha^2 = \alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1 + 2\alpha$ etc. Es ist $[\mathrm{GF}(9) : \mathbb{Z}_3] = 2$, und eine Basis ist gegeben durch $\{1, \alpha\}$. Wir berechnen nun die Elemente von $\mathrm{GF}(9)$ sowie deren Koordinatendarstellung in der Basis $\{1, \alpha\}$:

Elemente	Koordinatendarstellung
0	$(0, 0)$
$\alpha^0 = 1$	$(1, 0)$
$\alpha^1 = \alpha$	$(0, 1)$
$\alpha^2 = 1 + \alpha$	$(1, 1)$
$\alpha^3 = 1 + 2\alpha$	$(1, 2)$
$\alpha^4 = 2$	$(2, 0)$
$\alpha^5 = 2\alpha$	$(0, 2)$
$\alpha^6 = 2 + 2\alpha$	$(2, 2)$
$\alpha^7 = 2 + \alpha$	$(2, 1)$
$\alpha^8 = 1$	$(1, 0)$

Hier sind die Potenzen α^j, $0 \le j < 8$, alle verschieden, α ist also ein primitives Element von $\mathrm{GF}(9)$ und $x^2 - x - 1$ ein primitives Polynom in $\mathbb{Z}_3[x]$.

Damit können die Operationstafeln nach folgenden Regeln angegeben werden.

- Multiplikation: $0 \cdot \alpha^i = \alpha^i \cdot 0 = 0$, $\alpha^i \alpha^j = \alpha^{(i+j) \bmod 8}$
  $((\mathrm{GF}(9) \setminus \{0\}, \cdot)$ ist eine von α erzeugte zyklische Gruppe).
- Addition: zum Beispiel

$$\begin{array}{ccccc} \alpha^2 & + & \alpha^4 & = & ? \\ \downarrow & & \downarrow & & \\ (1,1) & + & (2,0) & = & (0,1) \\ \downarrow & & \downarrow & & \downarrow \\ \alpha^2 & + & \alpha^4 & = & \alpha \end{array}$$

In diesem Beispiel haben wir davon profitiert, dass das Polynom $f(x) = x^2 - x - 1$, nach dem wir den Polynomring faktorisiert haben, primitiv ist. Doch ist nicht jedes irreduzible Polynom primitiv, wie wir uns nun anhand des obigen Beispiels mit $p = 3$ und $n = 2$ überlegen wollen. Und zwar gibt es über $\mathbb{Z}_3$ neun normierte quadratische Polynome (der lineare und der konstante Koeffizient können beliebig gewählt werden). Von ihnen sind sechs als Produkte der drei normierten linearen Polynome x, $x + 1$ und $x + 2$ reduzibel, die restlichen drei müssen irreduzibel sein. Schnell findet man, dass es sich dabei neben $f_1(x) := f(x) = x^2 - x - 1$ um die beiden Polynome $f_2(x) := x^2 + x - 1$ und $f_3(x) := x^2 + 1$ handelt.
Nimmt man oben statt $f = f_1$ das Polynom f_2 für die Konstruktion von GF(9), so verläuft alles ganz analog wie mit f_1, weil sich auch f_2 als primitiv erweist. Mit $f_3(x) = x^2+1$ jedoch erhält man für jede Nullstelle α die Beziehung $\alpha^2 = -1$ und somit $\alpha^4 = 1$. Bezeichnen wir eine Nullstelle von f_3 mit α, so ist die zweite Nullstelle gegeben durch $-\alpha = \alpha^3 = 2\alpha$. Die Nullstellen von f_3 können also keine primitiven Elemente in GF(9) sein, daher ist auch f_3 kein primitives Polynom. Jedoch muss z. B. das Element $\beta := \alpha+1$ (genauso könnte man $\alpha+2$, $2\alpha+1$ oder $2\alpha+2$ nehmen) ein primitives sein, weil es nicht in der von α erzeugten multiplikativen Gruppe liegt. Tatsächlich rechnet man sofort $\beta^2 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = -1 + 2\alpha + 1 = 2\alpha$ etc. nach, woraus man ebenfalls eine Übersetzung zwischen den Potenzen von β und den Koordinatendarstellungen bezüglich der Basis $\{1, \alpha\}$ gewinnen kann. Die genaue Ausführung dieses Programms ist eine lehrreiche Übungsaufgabe:

UE 380 ▶ Übungsaufgabe 6.3.4.2. (B) Finden Sie mehrere Darstellungen von GF(9) samt Isomorphismen zwischen denselben, indem Sie wie folgt vorgehen: **◀ UE 380**

(1) Konstruieren Sie GF(9) mit Hilfe von f_2.
(2) Konstruieren Sie GF(9) mit Hilfe von f_3.
(3) Finden Sie Isomorphismen zwischen den drei Darstellungen von GF(9), die vermittels der irreduziblen Polynome f_1 (weiter oben) sowie f_2 und f_3 (als erster und zweiter Teil dieser Aufgabe) gefunden worden sind.

Eine weitere Möglichkeit der Konstruktion besteht darin, auch die Multiplikation direkt im Faktorring $\mathbb{Z}_p/(f)$ für ein irreduzibles (jetzt nicht unbedingt primitives) Polynom

$f \in \mathbb{Z}_p[x]$ vom Grad n durchzuführen, d. h., man multipliziert zwei Repräsentanten und reduziert anschließend modulo f. Beispielsweise kann man in $\mathbb{Z}_3/(x^2-x-1)$

$$\begin{aligned}(x+1+(x^2-x-1))\cdot(2x+1+(x^2-x-1)) &= 2x^2+1+(x^2-x-1)\\ &= 2(x+1)+1+(x^2-x-1) = 2x+(x^2-x-1)\end{aligned}$$

berechnen (dies entspricht der Rechnung $\alpha^2\cdot\alpha^3=\alpha^5$ in der Konstruktion aus Beispiel 6.3.4.1). Etwas schwieriger ist die Bestimmung der multiplikativen Inversen von, sagen wir, $s+(f)\neq 0+(f)$. Wenn s konstant ist, d. h. $s\in\mathbb{Z}_p$, dann können wir s^{-1} in $\mathbb{Z}_p$ berechnen und die Inverse ist gegeben durch $s^{-1}+(f)$. Wenn s zumindest Grad 1 hat, dann gelingt die Berechnung mit dem Euklidischen Algorithmus: Da f irreduzibel und s kein Vielfaches von f ist, gilt $\mathrm{ggT}(s,f)=1$. Der Euklidische Algorithmus, angewendet in $\mathbb{Z}_p[x]$, liefert Polynome $a,b\in\mathbb{Z}_p[x]$ mit $as+bf=1$. Multiplizieren gemäß

$$(a+(f))\cdot(s+(f)) = 1-bf+(f) = 1+(f)$$

zeigt $(s+(f))^{-1}=a+(f)$ (möglicherweise kann man in $a+(f)$ noch reduzieren).

UE 381 ► **Übungsaufgabe 6.3.4.3.** (B) Konstruieren Sie einen Körper mit 8 Elementen als Faktor $\mathbb{Z}_2[x]/(f)$ für ein geeignetes Polynom $f\in\mathbb{Z}_2[x]$. Berechnen Sie weiters die Inverse von $x+(f)$ in $\mathbb{Z}_2[x]/(f)$ mit dem Euklidischen Algorithmus. ◄ **UE 381**

UE 382 ► **Übungsaufgabe 6.3.4.4.** (F) Bestimmen Sie die Anzahl der normierten irreduziblen Polynome vom Grad 2 über $\mathrm{GF}(q)=\mathrm{GF}(p^n)$ mit $p\in\mathbb{P}$ und $n\in\mathbb{N}^+$. ◄ **UE 382**

UE 383 ► **Übungsaufgabe 6.3.4.5.** (A) (Alternativer Beweis der Eindeutigkeit von $\mathrm{GF}(p^n)$. Wir verwenden, dass $\mathrm{GF}(p^n)$ Zerfällungskörper von $x^{p^n}-x$ ist, aber nicht den Satz über die Eindeutigkeit des Zerfällungskörpers.)
Seien K_1 und K_2 endliche Körper der Kardinalität p^n, wobei die multiplikative Gruppe von K_1 von α erzeugt wird; sei $q(x)$ das Minimalpolynom von α über dem Primkörper. Zeigen Sie, dass $q(x)$ eine Nullstelle in K_2 hat, und schließen Sie $K_1\cong K_2$.
Hinweis: $x^{p^n}-x$ zerfällt über dem Primkörper in irreduzible Faktoren; α ist Nullstelle in K_1 eines solchen Faktors. ◄ **UE 383**

6.3.5. Der algebraische Abschluss eines endlichen Körpers

Inhalt in Kurzfassung: Für festes $p\in\mathbb{P}$ haben alle endlichen Körper der Charakteristik p (bis auf Isomorphie) denselben algebraischen Abschluss. Dieser lässt sich als direkter Limes endlicher Körper realisieren.

Es lohnt, die nachfolgende Konstruktion im Lichte von Unterabschnitt 2.2.4 zu betrachten. Und zwar untersuchen wir zu gegebenem $p\in\mathbb{P}$ das System der endlichen Körper $K_n := \mathrm{GF}(p^n)$ mit Charakteristik p. Da sich K_m nur dann als Unterkörper von

K_n auffassen lässt, wenn $m|n$ gilt, ist Satz 2.2.4.2 nur nach einer kleinen (notationell-technischen) Änderung anwendbar. Dazu betrachten wir nur die Körper $K_{k!} = \mathrm{GF}(p^{k!})$ für $k = 1, 2, \ldots$. Indem wir gemäß isomorpher Einbettungen identifizieren, erhalten wir eine aufsteigende Kette:

$$\mathrm{GF}(p) \leq \mathrm{GF}(p^2) \leq \mathrm{GF}(p^6) \leq \mathrm{GF}(p^{24}) \leq \mathrm{GF}(p^{120}) \leq \cdots$$

Die Vereinigung aller dieser Körper bezeichnen wir mit $\mathrm{GF}(p^\infty)$. Offenbar ist $\mathrm{GF}(p^\infty)$ ein unendlicher Körper. Für jede Zahl $k \geq 1$ gilt $\mathrm{GF}(p^k) \leq \mathrm{GF}(p^{k!}) \leq \mathrm{GF}(p^\infty)$, also enthält $\mathrm{GF}(p^\infty)$ alle endlichen Körper der Charakteristik p.

Satz 6.3.5.1. *Der unendliche Körper* $\mathrm{GF}(p^\infty)$ *der Charakteristik* $p \in \mathbb{P}$ *ist ein algebraischer Abschluss jedes endlichen Körpers der Charakteristik* p.

Beweis. Wir haben bereits beobachtet, dass $\mathrm{GF}(p^\infty)$ eine Erweiterung jedes endlichen Körpers ist. Weil jedes $\mathrm{GF}(p^n)$ endlichdimensional und somit algebraisch über dem Primkörper $\mathbb{Z}_p$ ist, ist $\mathrm{GF}(p^\infty)$ als Vereinigung aller $\mathrm{GF}(p^n)$ ebenfalls algebraisch über $\mathbb{Z}_p$. Insbesondere ist $\mathrm{GF}(p^\infty)$ algebraisch über jedem endlichen Körper. Somit bleibt nur noch zu beweisen, dass $\mathrm{GF}(p^\infty)$ algebraisch abgeschlossen ist. Gemäß Proposition 6.2.2.2 genügt es zu zeigen, dass jedes irreduzible Polynom $f \in \mathrm{GF}(p^\infty)[x]$ eine Nullstelle in $\mathrm{GF}(p^\infty)$ hat. Da jeder Koeffizient von f in einem $\mathrm{GF}(p^k)$ enthalten ist und f nur endlich viele von 0 verschiedene Koeffizienten hat, gilt sogar $f \in \mathrm{GF}(p^m)[x]$ für ein $m \geq 1$. Klarerweise ist f auch als Polynom über $\mathrm{GF}(p^m)$ irreduzibel. Somit hat f nach dem Satz von Kronecker (Proposition 6.2.1.1) eine Nullstelle in $\mathrm{GF}(p^m)/(f)$. Bezeichnet n den Grad von f, so ist dieser Körper eine n-dimensionale Erweiterung von $\mathrm{GF}(p^m)$, also ist $\mathrm{GF}(p^m)/(f)$ äquivalent zu $\mathrm{GF}(p^{mn})$ über $\mathrm{GF}(p^m)$. Wählen wir k mit $k! \geq mn$, so erhalten wir, dass f wie gefordert eine Nullstelle in $\mathrm{GF}(p^{k!}) \leq \mathrm{GF}(p^\infty)$ hat. □

A. Anhang: Mengentheoretische Grundlagen

A.1. Wohlordnungen

A.1.1. Grundbegriffe

Definition A.1.1.1. Eine totale Ordnung (= lineare Ordnung = Kette)[1] $(W, <)$ heißt Wohlordnung (WO), wenn jede nichtleere Teilmenge $\emptyset \neq T \subseteq W$ ein kleinstes Element hat.

Die Ordnungsrelation $\leq_M$ in einem Modell $(M, 0_M, \nu_M, +_M, \cdot_M, \leq_M)$ der Peano-Arithmetik (siehe Abschnitt 1.1.2) ist nicht nur linear, sondern sogar eine Wohlordnung. Dies kann man mit Hilfe des Induktionsaxioms (siehe Definition 1.1.2.2) beweisen.

Satz A.1.1.2. *Sei $(M, 0_M, \nu_M, +_M, \cdot_M, \leq_M)$ ein Modell der Peano-Arithmetik. Dann gilt*

(1) *Jede* beschränkte *nichtleere Teilmenge von M hat ein kleinstes Element, das heißt: Für alle $n \in M$ gilt: Jede nichtleere Menge $A \subseteq \{k \in M \mid k \leq_M n\}$ hat ein kleinstes Element.*

(2) *Jede nichtleere Menge $B \subseteq M$ hat ein kleinstes Element.*

Wir beweisen zunächst (1) mit Induktion nach n, und schließen dann daraus (2).

Beweis.

(1) Sei T die Menge aller Elemente $n \in M$, die die Bedingung (1) erfüllen.

Man sieht leicht, dass $0 \in T$ gilt – es gilt ja nach Definition $\{k \in M \mid k \leq_M 0\} = \{0\}$, und die einzige nichtleere Menge $A \subseteq \{0\}$ ist die Menge $\{0\}$ selbst, die ein kleinstes Element hat.

Wir zeigen nun $n \in T \Rightarrow \nu_M(n) \in T$. Sei $A \subseteq \{k \in M \mid k \leq_M \nu_M(n)\}$ nicht leer. Wir definieren $A' := \{k \in A \mid k \neq \nu_M(n)\} = A \setminus \{\nu_M(n)\}$ und unterscheiden zwei Fälle:

a) A' ist leer. Dann ist $A = \{\nu_M(n)\}$, und diese Menge hat sicher ein kleinstes Element.

[1] Wenn kein Irrtum möglich ist, unterscheidet man oftmals nicht zwischen W und $(W, <)$ und bezeichnet folglich W als Wohlordnung. Wir unterscheiden auch nicht streng zwischen reflexiven und irreflexiven Wohlordnungen und deuten lediglich durch die Symbole $\leq$ bzw. $<$ (und ihre Varianten) an, ob wir gerade die reflexive oder irreflexive Version einer Wohlordnung meinen.

b) A' ist nicht leer. Für alle Elemente $k \in A'$ gilt $k \leq \nu_M(n)$, laut Axiom $((\leq))$ folgt also $k \leq n$ oder $k = \nu_M(n)$; der Fall $k = \nu_M(n)$ ist nach Definition von A' unmöglich.
Somit ist A' eine nichtleere Teilmenge von $\{k \in M \mid k \leq_M n\}$ und hat (wegen $n \in T$) ein kleinstes Element k_0. Aus $k_0 \leq n \leq \nu_M(n)$ ergibt sich, dass k_0 auch das kleinste Element von A ist.

(2) Sei nun $B \subseteq M$ beliebig aber nicht leer. Sei also $b_1 \in B$. Wir betrachten die Menge $A := \{k \in B \mid k \leq_M b_1\}$. Diese Menge enthält b_1 und ist daher nicht leer. Laut (1) hat sie ein kleinstes Element b_0, welches natürlich $b_0 \leq_M b_1$ erfüllen muss.

Aus $b_0 = \min(A)$ erhält man (mit Transitivität der Relation $\leq_M$) wie in (1) die Beziehung $b_0 = \min(B)$. □

Definition A.1.1.3. Seien $(W, <)$ und $(W_i, <_i)$, $i \in \{1, 2\}$, Wohlordnungen.

- $(A, <)$ heißt Anfangsabschnitt von $(W, <)$, wenn $A \subseteq W$ und wenn A mit einem α auch alle $\beta < \alpha$ enthält.
- $W_\alpha := \{\beta \in W \mid \beta < \alpha\}$ heißt der von α induzierte Anfangsabschnitt (von W).

Anmerkung A.1.1.4. Wenn (M, R) eine lineare Ordnung ist, wird jede Teilmenge $T \subseteq M$ durch R (genauer: durch die Einschränkung der Relation R auf die Untermenge T, formal ist dies die Relation $R|_T := R \cap (T \times T)$) auch linear geordnet. Wenn (M, R) überdies eine Wohlordnung ist, sieht man leicht, dass auch $(T, R|_T)$ eine Wohlordnung ist.
Statt $(T, R|_T)$ schreiben wir oft der besseren Lesbarkeit halber nur (T, R).

Definition A.1.1.5. In Wohlordnungen unterscheidet man drei Arten von Elementen α:

1. $\alpha = 0 := \min(W)$
2. $\exists \beta \in W : \alpha = \beta + 1$, wobei wir $\beta + 1$ als Abkürzung für $\min\{\gamma \in W \mid \beta < \gamma\}$ verstehen. Dann heißt α *Nachfolger*[2] von β.
3. $\alpha \neq 0 \wedge \forall \beta \in W : \alpha \neq \beta + 1$. Dann heißt α *Limeselement*.[3]

Beispiele A.1.1.6 (von Wohlordnungen)**.**

(a) Jede endliche Kette. (Insbesondere wird auch die leere Menge durch die einzig mögliche Ordnungsrelation wohlgeordnet, ebenso wie jede 1-elementige Menge.)

(b) $\mathbb{N} = \omega = \{0 < 1 < 2 < ...\}$

(c) $\omega + 1 = \omega \cup \{\omega\} = \{0 < 1 < 2 < \cdots < \omega\}$

[2] Um zu betonen, dass es um den Nachfolger im Sinne der Ordnung $(W, <)$ geht, kann man auch $\beta +_W 1$ oder $\beta +_{(W,<)} 1$ schreiben.
[3] Je nachdem, ob es praktisch ist, bezeichnet man manchmal auch 0 als Limeselement.

UE A1 ► **Übungsaufgabe A.1.1.7.** (F) Sei $(W_i, <_i)_{i\in I}$ eine Familie von Wohlordnungen, wobei $(I, <)$ ebenfalls eine Wohlordnung ist. Geben Sie eine Wohlordnung auf $\bigcup_{i\in I}\{i\} \times W_i$ an. ◄ **UE A1**

A.1.2. Transfinite Induktion

Lemma A.1.2.1 (Prinzip der transfiniten Induktion)**.** *Eine Kette $(W, <)$ ist wohlgeordnet genau dann, wenn*

$$\forall T \subseteq W : \Big[(\forall \alpha \in W : (W_\alpha \subseteq T \Rightarrow \alpha \in T)) \;\Rightarrow\; T = W\Big].$$

Beweis. Die folgenden Aussagen sind äquivalent:

- $\forall T \subseteq W : (\forall \alpha \in W : (W_\alpha \subseteq T \Rightarrow \alpha \in T) \Rightarrow T = W)$
- $\forall T \subseteq W : (T \neq W \Rightarrow \neg\forall \alpha \in W : (W_\alpha \subseteq T \;\Rightarrow\; \alpha \in T))$
  (Diese Äquivalenz erhält man, weil allgemein die Aussagen $p \Rightarrow q$ und $\neg q \Rightarrow \neg p$ äquivalent sind.)
- $\forall T \subseteq W : (T \neq W \Rightarrow \exists \alpha \in W : (W_\alpha \subseteq T \;\wedge\; \alpha \notin T))$
  (Die Negation von $p \Rightarrow q$ ist $(p \wedge \neg q)$.)
- $\forall S \subseteq W : (S \neq \emptyset \Rightarrow \exists \alpha \in W : (W_\alpha \subseteq W \setminus S \;\wedge\; \alpha \in S))$
  (Diese Äquivalenz erhält man, wenn man $S := W \setminus T$ bzw. $T := W \setminus S$ setzt.)
- $\forall S \subseteq W : (S \neq \emptyset \Rightarrow \exists \alpha \in W : (\alpha = \min(S)))$.
  (Denn $\alpha = \min(S)$ bedeutet, dass erstens $\alpha \in S$ gilt, aber zweitens kein $\beta < \alpha$ in S liegt, also $W_\alpha \subseteq W \setminus S$.)
- W ist Wohlordnung. (Nach Definition.) □

Anmerkung A.1.2.2. Bei Anwendungen von Lemma A.1.2.1 sprich man von einem *Beweis durch transfinite Induktion.* Der „Induktionsanfang“ entspricht dem Falle $\alpha = \min(W)$, $W_\alpha = \emptyset$. Im „Induktionsschritt“ unterscheidet man meist zwischen Nachfolger- und Limeselement: man überprüft die Implikation $W_\alpha \subseteq T \Rightarrow \alpha \in T$ getrennt für die Fälle „α ist Nachfolger, d. h. $\exists \beta : \alpha = \beta + 1$“, und „$\alpha$ ist Limeselement, d. h. $\forall \beta < \alpha : \beta + 1 < \alpha$“.

UE A2 ► **Übungsaufgabe A.1.2.3.** (B) Finden Sie eine nichtleere Teilmenge $T \subseteq \mathbb{Q}$ der rationalen Zahlen, die zwar ◄ **UE A2**

$$\forall \alpha \in \mathbb{Q} : (\mathbb{Q}_\alpha \subseteq T \Rightarrow \alpha \in T) \qquad (\text{mit } \mathbb{Q}_\alpha := \{x \in \mathbb{Q} \mid x < \alpha\})$$

erfüllt, aber trotzdem nicht $T = \mathbb{Q}$ erfüllt. Wenn möglich, finden Sie so eine Menge T, die alle negativen rationalen Zahlen enthält.

Lemma A.1.2.4. *Sei $(W, <)$ eine Wohlordnung. Dann gilt:*

(a1) $A \subsetneq W$ *echter Anfangsabschnitt* $\Rightarrow A = W_\alpha$, *wobei* $\alpha = \min(W \setminus A)$.

(a2) Die Abbildung $\alpha \mapsto W_\alpha$ *ist ein Isomorphismus zwischen* $(W, \leq)$ *und der Menge der echten Anfangsabschnitte von* W, *geordnet durch* $\subseteq$.
Ebenso ist $(W_\alpha, \leq)$ *isomorph zu* $(\{W_\beta \mid \beta < \alpha\}, \subseteq)$.

(b) $f\colon W \to W$ *streng monoton* $\Rightarrow \forall \alpha \in W : \alpha \leq f(\alpha)$.

(b') Die Identität ist der einzige Automorphismus von $(W, \leq)$.
(Dies folgt aus (b): Wenn f *Automorphismus ist, dann auch* f^{-1}*; wenn nun* $f(x) = y$ *und daher auch* $f^{-1}(y) = x$ *ist, muss* $x \leq y \leq x$ *gelten, also* $x = y$.*)*

(c) $(W, \leq) \cong (W', \leq') \Rightarrow$ *der Isomorphismus* $f\colon W \to W'$ *ist eindeutig.*
(Dies folgt leicht aus (b'): Wenn f_1, f_2 *Isomorphismen sind, so ist* $f_1^{-1} \circ f_2$ *Automorphismus von* W, *also* $f_1^{-1} \circ f_2 = \mathrm{id}_W$.*)*

(d) $\alpha \in W \Rightarrow (\forall T \subseteq W_\alpha : T \ncong W)$*: Eine Wohlordnung ist niemals zu einem echten Anfangsabschnitt oder zu einer Teilmenge eines echten Anfangsabschnitts isomorph.*
(Denn für einen Isomorphismus $f\colon W \to T$ *müsste* $f(\alpha) < \alpha$ *gelten, was (b) widerspricht.)*

(e) $\alpha < \beta \in W \Rightarrow W_\alpha \ncong W_\beta$.
(Dies folgt aus (d) für $W = W_\beta$.*)*

(f) Für jede Kette $(K, <)$ *gilt:* $(K, <)$ *ist Wohlordnung* $\Leftrightarrow \forall \alpha \in K : (K_\alpha, <)$ *ist Wohlordnung.*

UE A3 ► **Übungsaufgabe A.1.2.5.** (V) Zeigen Sie die Unterpunkte (a1), (a2), (b), (f) von Lemma A.1.2.4. ◄ **UE A3**

Satz A.1.2.6 (Vergleichbarkeit von Wohlordnungen)**.** *Seien* $(W, <)$ *und* $(W', <')$ *Wohlordnungen. Dann gilt genau eine der folgenden Aussagen:*

(i) $(W, <) \cong (W', <')$

(ii) $\exists \alpha' \in W' : (W, <) \cong (W'_{\alpha'}, <')$. *Wir schreiben hierfür auch* $(W, <) < (W', <')$ *und sagen, dass* W kürzer *als* W' *ist.*

(iii) $\exists \alpha \in W : (W', <') \cong (W_\alpha, <)$. *Schreib- und Sprechweisen analog.*

Beweis. Sei $T := \{\alpha \in W \mid \exists \alpha' \in W' : W_\alpha \cong W'_{\alpha'}\}$ und $f := \{(\alpha, \alpha') \in W \times W' \mid W_\alpha \cong W'_{\alpha'}\}$. Dann ist f eine Funktion $T \to W'$, denn zu jedem $\alpha \in T$ ist das α' eindeutig, weil aus $(\alpha, \alpha'), (\alpha, \tilde{\alpha}') \in f$ mit $\alpha' \neq \tilde{\alpha}'$ folgt, dass $W'_{\alpha'} \cong W'_{\tilde{\alpha}'}$ im Widerspruch zu A.1.2.4(e). Offensichtlich gilt:

- T ist Anfangsabschnitt von W. (nach Lemma A.1.2.4(a1))

- f ist streng monoton.
- $f(T)$ ist Anfangsabschnitt von W'.

Nun sind 4 Fälle denkbar:

- $T = W$ und $f(T) = W'$.
- $T = W$ und $f(T) \subsetneq W'$.
- $T \subsetneq W$ und $f(T) = W'$.
- $T \subsetneq W$ und $f(T) \subsetneq W'$.

Die ersten drei Fälle entsprechen genau den Punkten (i), (ii), (iii) in unserer Behauptung, und der vierte Fall ist unmöglich. Wäre nämlich $T \neq W \wedge f(T) \neq W'$, so gäbe es nach Lemma A.1.2.4(a1) Elemente $\alpha \in W, \alpha' \in W'$ mit $T = W_\alpha, f(T) = W'_{\alpha'}$. Daher $(\alpha, \alpha') \in f \Rightarrow \alpha \in T = W_\alpha$. Widerspruch. □

A.1.3. Die „Wohlordnung“ aller Wohlordnungen modulo $\cong$

Sei $\mathcal{W}$ eine Menge von Wohlordnungen. Dann definiert

$$(S, <_S) \leq_W (T, <_T) :\Leftrightarrow \exists \text{ Anfangsabschnitt } A \text{ von } T \text{ mit } (S, <_S) \cong (A, <_T)$$

eine Quasiordnung auf $\mathcal{W}$, deren induzierte Halbordnung (Faktorisierung nach $\cong$, vergleiche auch Definition 2.1.1.11) wegen Satz A.1.2.6 eine Totalordnung ist. Diese ist sogar wohlgeordnet: Sei $\emptyset \neq \mathcal{T} \subseteq \mathcal{W}/_\cong$, $(T_1, <_1) \in \mathcal{T}$. Ist $[(T_1, <_1)]_\cong$ nicht selbst minimal in $\mathcal{T}$, so können wir ein minimales $t_0 \in T_1$ finden, sodass der Anfangsabschnitt $((T_1)_{t_0}, <_1)$ Repräsentant einer Äquivalenzklasse in $\mathcal{T}$ ist. Diese Äquivalenzklasse ist nun das gesuchte minimale Element.
In diesem Sinne ist die Klasse[4] (nicht Menge!) aller Wohlordnungen selbst „wohlgeordnet“.

A.2. Definition durch transfinite Rekursion

A.2.1. Der Rekursionssatz

Satz A.2.1.1 (Rekursionssatz)**.** *Sei S eine Menge, $(W, \leq)$ eine Wohlordnung, $\mathcal{F}_0 \subseteq \mathcal{F} := \bigcup_{\alpha \in W} S^{W_\alpha}$, $h\colon \mathcal{F}_0 \to S$, $* \notin S$. Dann gibt es genau ein $F\colon W \to S \cup \{*\}$ mit*

$$\forall \alpha \in W : F(\alpha) = \begin{cases} h(F|_{W_\alpha}) & \text{falls } F|_{W_\alpha} \in \text{ dom } h = \mathcal{F}_0 \\ * & \text{sonst} \end{cases}$$

Ist $\mathcal{F}_0 = \mathcal{F}$, so tritt stets der erste, interessante Fall ein, und es gilt $F\colon W \to S$.

[4] Achtung: Hier ist „Klasse“ als „Sammlung von Objekten mit einer gewissen Eigenschaft“ zu verstehen, nicht als Äquivalenzklasse!

Anmerkung A.2.1.2. Der Satz gilt sinngemäß auch für $W = \mathbb{O}$ (= Klasse der Ordinalzahlen, vgl. Unterabschnitt A.1.3).

Beweis. Die Eindeutigkeit folgt unmittelbar durch transfinite Induktion für $T := \{\alpha \in W \mid F_1(\alpha) = F_2(\alpha)\}$.
Wir fügen zu W ein weiteres Element ∞ hinzu, für welches $(\forall w \in W : w < \infty)$ gelten soll; statt W schreiben wir nun W_∞, an den Mengen W_α ändert sich nichts.
Sei T die Menge aller $\alpha \in W \cup \{\infty\}$, sodass der Satz (Existenz und Eindeutigkeit) für W_α statt für W gilt, und für $\alpha \in T$ sei F_α das dazugehörige $F_\alpha : W_\alpha \to S \cup \{*\}$. Offenbar ist mit $\beta < \alpha \in T$ auch $\beta \in T$ (weil die Einschränkung von $F_\alpha \colon W_\alpha \to S \cup \{*\}$ auf W_β als F_β dienen kann) und wegen der Eindeutigkeit gilt $F_\beta = F_\alpha|_{W_\beta}$.
Behauptung: Es gilt $T = W \cup \{\infty\}$. Laut Lemma A.1.2.1 müssen wir also aus der Annahme $W_\alpha \subseteq T$ die Folgerung $\alpha \in T$ ziehen können. Wenn α_0 ein Limeselement ist, dann wird $\alpha_0 \in T$ von $F_{\alpha_0} := \bigcup_{\alpha<\alpha_0} F_\alpha$ bezeugt. Wenn andererseits $\alpha_0 = \beta + 1$ ein Nachfolger ist, dann wird $\alpha_0 \in T$ von $F_{\alpha_0} := F_{\beta_0} \cup \{(\beta_0, h(F_{\beta_0})\}$ bezeugt.
Also ist $T = W \cup \{\infty\}$ und $F := F_\infty$ ist die gewünschte Funktion. □

A.2.2. Vollständige Induktion auf $\mathbb{N}$

Für $W = \mathbb{N}$ reflektiert Satz A.2.1.1 die Definition durch „Ordnungsinduktion“, bei der auf beliebige Vorgänger zurückgegriffen wird, also $x_{n+1} = f_n(x_1, \ldots, x_n)$. Bei der „gewöhnlichen“ Rekursion $x_{n+1} = f(x_n)$ („Nachfolgerinduktion“) hängt h immer nur von dem letzten Folgenglied ab. Auch diese Variante wollen wir explizit formulieren. Da wir sie später in sehr allgemeinen und grundlagenhaften Überlegungen zu den natürlichen Zahlen einsetzen wollen, ist festzuhalten, dass man diese Variante mit einem analogen Beweis zu Satz A.2.1.1 zeigen kann, sobald man Induktion auf $\mathbb{N}$ und die Ordnungsrelation auf $\mathbb{N}$ zur Verfügung hat.

Satz A.2.2.1. *Sei X eine Menge, $x_0 \in X$ und $f : X \to X$. Dann gibt es genau eine Abbildung $\varphi : \mathbb{N} \to X$ (so etwas nennt man bekanntlich eine* Folge *in X) mit der Eigenschaft $\varphi(0) = x_0$ und $\varphi(n+1) = f(\varphi(n))$ für alle $n \in \mathbb{N}$.*

UE A4 ► Übungsaufgabe A.2.2.2. (V) Beweisen Sie Satz A.2.2.1, indem Sie folgende Sachverhalte überprüfen: **◄ UE A4**

1. Bezeichne T die Menge aller $n \in \mathbb{N}$ mit der Eigenschaft, dass es eine eindeutige Abbildung $\varphi_n : \mathbb{N}_{<n} := \{k \in \mathbb{N} \mid k < n\} \to M$ mit folgenden Eigenschaften gibt:
   - Ist $0 \in \mathbb{N}_{<n}$, so gilt $\varphi_n(0) = x_0$;
   - sind $k, k+1 \in \mathbb{N}_{<n}$, so gilt $\varphi_n(k+1) = f(\varphi_n(k))$.

   Zeigen Sie: $0 \in T$ und $n \in T$ impliziert $n + 1 \in T$.

2. Aus dem Induktionsprinzip auf $\mathbb{N}$ folgt $T = \mathbb{N}$, also ist φ_n für alle $n \in \mathbb{N}$ eindeutig definiert. Zeigen Sie, dass die Vereinigung $\varphi := \bigcup_{n\in\mathbb{N}} \varphi_n$ die gesuchte eindeutige Funktion ist.

   (Hinweis: Zeigen Sie $k < n \Rightarrow \varphi_k \subseteq \varphi_n$.)

A.3. Nachtrag zu den natürlichen Zahlen, Unterabschnitt 1.1

A.3.1. Endliche Mengen

Proposition A.3.1.1 (Siehe Proposition 1.1.1.5)**.**

(1) *Sei M eine beliebige Menge, und $(\mathscr{A}_i : i \in I)$ eine Familie von induktiven Teilmengen von $\mathfrak{P}(M)$. Dann ist auch $\bigcap_i \mathscr{A}_i$ induktiv. Insbesondere ist $\mathfrak{P}_{\mathrm{fin}}(M)$ induktiv.*

(2) *Wenn $A \subseteq M$, dann gilt $\mathfrak{P}_{\mathrm{fin}}(A) = \mathfrak{P}_{\mathrm{fin}}(M) \cap \mathfrak{P}(A)$.*

(3) *Wenn $A \in \mathfrak{P}_{\mathrm{fin}}(M)$, dann gilt $\mathfrak{P}(A) \subseteq \mathfrak{P}_{\mathrm{fin}}(M)$.*

(4) *Die Menge $\mathfrak{P}_{\mathrm{fin}}(M)$ besteht genau aus allen endlichen Teilmengen von M.*

(5) *Hat die leere Menge $\emptyset$ eine gewisse Eigenschaft, die sich von jeder Menge M auf jede Menge der Form $M \cup \{x\}$ (x beliebig) vererbt, so hat jede endliche Menge diese Eigenschaft.*

(6) *Sei M eine beliebige Menge. Dann sind die folgenden Aussagen äquivalent:*
   (a) $\mathfrak{P}(M) = \mathfrak{P}_{\mathrm{fin}}(M)$.
   (b) $M \in \mathfrak{P}_{\mathrm{fin}}(M)$.
   (c) Es gibt ein maximales Element in $\mathfrak{P}_{\mathrm{fin}}(M)$, das heißt: Es gibt $A \in \mathfrak{P}_{\mathrm{fin}}(M)$, sodass es keine echte Obermenge $B \supsetneq A$ in $\mathfrak{P}_{\mathrm{fin}}(M)$ gibt.
   (d) Jede nichtleere Teilmenge $\mathcal{E} \subseteq \mathfrak{P}(M)$ hat ein maximales Element.

(7) *Wenn $A \subseteq B$ gilt, und B endlich ist, dann auch A.*

(8) *Wenn $M \approx N$ durch eine Bijektion $f\colon M \to N$ bezeugt wird, dann induziert f eine natürliche Bijektion zwischen $\mathfrak{P}(M)$ und $\mathfrak{P}(N)$; die Einschränkung dieser Bijektion auf $\mathfrak{P}_{\mathrm{fin}}(M)$ liefert eine Bijektion $g : \mathfrak{P}_{\mathrm{fin}}(M) \to \mathfrak{P}_{\mathrm{fin}}(N)$, die überdies mit der Relation $\approx$ verträglich ist (das heißt: $A_1 \approx A_2$ impliziert $g(A_1) \approx g(A_2)$).*

(9) *Wenn M endlich ist und $M \approx N$, dann ist auch N endlich.*

(10) *Wenn A endlich ist, dann ist auch $A \cup \{a\}$ endlich. (Wenn $a \in A$ gilt, dann ist das trivial, also ist diese Aussage nur für $a \notin A$ interessant.)*

(11) *Wenn A und B endliche Mengen sind, dann ist auch die Vereinigungsmenge $A \cup B$ endlich.*

(12) *Wenn A und B endliche Mengen sind, dann ist auch die Produktmenge $A \times B$ endlich.*

(13) *Wenn A und B endliche Mengen sind, dann ist auch die Menge B^A endlich. (Wir schreiben B^A für die Menge aller Funktionen von A nach B.)*

Beweisskizze.

(2) Der Schnitt $\mathfrak{P}_{\mathrm{fin}}(M) \cap \mathfrak{P}(A)$ ist (als Teilmenge von $\mathfrak{P}(A)$ betrachtet) eine induktive Familie, daher $\mathfrak{P}_{\mathrm{fin}}(A) \subseteq \mathfrak{P}_{\mathrm{fin}}(M) \cap \mathfrak{P}(A)$. Ist umgekehrt $\mathscr{A} \subseteq \mathfrak{P}(A)$ induktiv, so ist $\mathscr{M} := \{X \in \mathfrak{P}(M) \mid X \cap A \in \mathscr{A}\}$, betrachtet als Teilmenge von $\mathfrak{P}(M)$, induktiv. Somit gilt $\mathfrak{P}_{\mathrm{fin}}(M) \subseteq \mathscr{M}$, d. h. $\mathfrak{P}_{\mathrm{fin}}(M) \cap \mathfrak{P}(A) \subseteq \mathscr{M} \cap \mathfrak{P}(A) \subseteq \mathscr{A}$. Da $\mathscr{A}$ beliebig war, folgt $\mathfrak{P}_{\mathrm{fin}}(M) \cap \mathfrak{P}(A) \subseteq \mathfrak{P}_{\mathrm{fin}}(A)$.

(3) Wir betrachten die Menge $\mathscr{M} := \{X \in \mathfrak{P}(M) \mid \mathfrak{P}(X) \subseteq \mathfrak{P}_{\text{fin}}(M)\}$. Diese ist induktiv: Klarerweise gilt $\emptyset \in \mathscr{M}$. Sei $X \in \mathscr{M}$ und $x \in M$ mit oBdA $x \notin X$. Sei weiters $Y \in \mathfrak{P}(X \cup \{x\})$. Wenn $x \notin Y$, dann gilt $Y \in \mathfrak{P}(X) \subseteq \mathfrak{P}_{\text{fin}}(M)$. Wenn andererseits $x \in Y$, dann gilt $Y \setminus \{x\} \in \mathfrak{P}(X) \subseteq \mathfrak{P}_{\text{fin}}(M)$. Da $\mathfrak{P}_{\text{fin}}(M)$ nach (1) induktiv ist, folgt $Y = (Y \setminus \{x\}) \cup \{x\} \in \mathfrak{P}_{\text{fin}}(M)$. In jedem Fall gilt also $\mathfrak{P}(X \cup \{x\}) \subseteq \mathfrak{P}_{\text{fin}}(M)$, wie gewünscht. Wegen $A \in \mathfrak{P}_{\text{fin}}(M)$ erhalten wir daraus $A \in \mathscr{M}$, also $\mathfrak{P}(A) \subseteq \mathfrak{P}_{\text{fin}}(M)$.

(4) Ist $A \subseteq M$ endlich, dann folgt aus (2), dass $\mathfrak{P}(A) = \mathfrak{P}_{\text{fin}}(A) = \mathfrak{P}_{\text{fin}}(M) \cap \mathfrak{P}(A) \subseteq \mathfrak{P}_{\text{fin}}(M)$. Somit erhalten wir $A \in \mathfrak{P}(A) \subseteq \mathfrak{P}_{\text{fin}}(M)$.

Sei umgekehrt $A \in \mathfrak{P}_{\text{fin}}(M)$. Wir müssen $\mathfrak{P}_{\text{fin}}(A) = \mathfrak{P}(A)$ zeigen. Nach (3) gilt $\mathfrak{P}(A) \subseteq \mathfrak{P}_{\text{fin}}(M)$, sodass wir aus (2) die Aussage erhalten: $\mathfrak{P}_{\text{fin}}(A) = \mathfrak{P}_{\text{fin}}(M) \cap \mathfrak{P}(A) = \mathfrak{P}(A)$.

(5) Sei M endlich. Nach Voraussetzung ist das System aller Mengen $X \in \mathfrak{P}(M)$, die die gegebene Eigenschaft erfüllen, induktiv. Somit haben alle Mengen aus $\mathfrak{P}_{\text{fin}}(M)$ die Eigenschaft, insbesondere M (hier geht die Endlichkeit von M ein, d. h. $M \in \mathfrak{P}(M) = \mathfrak{P}_{\text{fin}}(M)$).

(6) (a)⇒(b) ist klar, (b)⇒(a) folgt aus (3).

(b)⇒(c) ist wieder klar; für (c)⇒(b) ist nur Folgendes zu beachten: Wenn A in $\mathfrak{P}_{\text{fin}}(M)$ ist und $x \in M \setminus A$, dann ist $A \cup \{x\} \in \mathfrak{P}_{\text{fin}}(M)$ nach (1) und klarerweise $A \cup \{x\} \supsetneq A$. Somit kann A nicht maximal sein.

(d)⇒(c) ist klar. Um (b)⇒(d) zu zeigen, betrachten wir die Menge

$$\mathscr{M} := \{X \in \mathfrak{P}(M) \mid \forall \emptyset \neq \mathcal{E} \subseteq \mathfrak{P}(X) : \mathcal{E} \text{ hat ein maximales Element}\}.$$

Diese Menge ist induktiv: $\emptyset \in \mathscr{M}$ ist klar; sei $X \in \mathscr{M}$ und $x \in M$ mit oBdA $x \notin X$. Sei außerdem $\mathcal{E} \subseteq \mathfrak{P}(X \cup \{x\})$ nichtleer gegeben. Wir definieren

$$\mathcal{F} := \{E \setminus \{x\} \mid E \in \mathcal{E}\} \subseteq \mathfrak{P}(X).$$

Es gilt $\mathcal{F} \neq \emptyset$, also gibt es wegen $X \in \mathscr{M}$ ein maximales Element $E \setminus \{x\} \in \mathcal{F}$, wobei $E \in \mathcal{E}$. Daher hat $\mathcal{E}$ wie gewünscht ein maximales Element, nämlich E (es muss x aber nicht in E enthalten sein; in diesem Fall gilt $E \setminus \{x\} = E$). Nach (b) erhalten wir $M \in \mathfrak{P}_{\text{fin}}(M) \subseteq \mathscr{M}$ und damit die Aussage.

(7) Nach (3) gilt $\mathfrak{P}_{\text{fin}}(A) = \mathfrak{P}_{\text{fin}}(B) \cap \mathfrak{P}(A) = \mathfrak{P}(B) \cap \mathfrak{P}(A) = \mathfrak{P}(A)$.

(9) Folgt direkt aus (8).

(10) Erneut nach (3) gilt $\mathfrak{P}(A) = \mathfrak{P}_{\text{fin}}(A) = \mathfrak{P}_{\text{fin}}(A \cup \{a\}) \cap \mathfrak{P}(A)$, insbesondere $A \in \mathfrak{P}_{\text{fin}}(A \cup \{a\})$. Wegen (1) ist $\mathfrak{P}_{\text{fin}}(A \cup \{a\})$ induktiv, also folgt $A \cup \{a\} \in \mathfrak{P}_{\text{fin}}(A \cup \{a\})$ und somit die Endlichkeit von $A \cup \{a\}$ nach (6).

(11) Aus (10) folgt, dass die folgende Eigenschaft an eine Menge B die Voraussetzungen aus (5) erfüllt: „Für alle endlichen Mengen A ist auch $A \cup B$ endlich“.

(12) Wir zeigen zunächst: Wenn A und B endlich sind, dann ist für beliebige b auch $A \times (B \cup \{b\})$ endlich. Dies folgt aus $A \times (B \cup \{b\}) = A \times B \cup A \times \{b\}$ kombiniert mit (11) und (9) (angewendet auf $A \approx A \times \{b\}$).

Damit kann man ähnlich wie im Beweis von (11) die Aussage aus (5) anwenden.

(13) Analog zu (12) unter Berücksichtigung von $A^{B \cup \{b\}} \approx A^B \times A$, vermittelt durch die Bijektion $f : A^{B \cup \{b\}} \to A^B \times A$, $h \mapsto (h|_B, h(b))$.

□

A.3.2. Das Modell von John von Neumann

An dieser Stelle wollen wir Folgendes zeigen:

Satz A.3.2.1 (Siehe Satz 1.1.3.3)**.** *Die Struktur* $(\mathbb{N}_{vN}, 0_{vN}, \nu_{vN})$ *(genannt das* Modell von John von Neumann*) mit* ν_{vN}: $\mathbb{N}_{vN} \to \mathbb{N}_{vN}$, $n \mapsto n \cup \{n\}$, *ist ein Modell der Peano-Axiome.*

Das Induktionsprinzip (also Axiom (5)) haben wir bereits vor der Formulierung von Satz 1.1.3.3 in Kapitel 1 gezeigt. Bevor wir den Satz beweisen, dürfen wir daher mit Induktion eine Hilfsaussage herleiten.

Lemma A.3.2.2. *Seien* $k, n \in \mathbb{N}_{vN}$ *und* $k \in n$*. Dann gilt* $k \subseteq n$*.*

Beweis. Induktion nach n: Wir zeigen, dass $T := \{n \in \mathbb{N}_{\text{vN}} \mid \forall k \in n : k \subseteq n\}$ das Element 0_{vN} enthält und unter ν_{vN}-Nachfolgern abgeschlossen ist (mit anderen Worten, dass T vN-induktiv ist). Die erste Behauptung ist klar, da $n = 0_{\text{vN}}$ keine Elemente k enthält; die T definierende Aussage ist also trivial wahr. Sei jetzt $n \in T$ und $k \in \nu_{\text{vN}}(n) = n \cup \{n\}$. Wenn $k \in n$, dann folgt $k \subseteq n$ aus der „Induktionsvoraussetzung“ $n \in T$. Wenn andererseits $k = n$, dann ist $k \subseteq n$ klar. □

Damit kommen wir zum Beweis des Satzes:

Beweis (von Satz A.3.2.1). Das Induktionsprinzip (also Axiom (5)) haben wir bereits gezeigt. Die Axiome (1) und (2) sind klar bzw. folgen daraus, dass $\mathbb{N}_{\text{vN}}$ vN-induktiv ist. Auch Axiom (4) folgt unmittelbar aus der Definition: Für $n \in \mathbb{N}_{\text{vN}}$ gilt $n \in \nu_{\text{vN}}(n)$ und insbesondere $\nu_{\text{vN}}(n) \neq \emptyset = 0_{\text{vN}}$.
Es bleibt also Axiom (3) zu zeigen. Sei dazu $\nu_{\text{vN}}(n) = \nu_{\text{vN}}(k)$ für $n, k \in \mathbb{N}_{\text{vN}}$, d. h. $n \cup \{n\} = k \cup \{k\}$. Wir werden die Annahme $n \neq k$ auf einen Widerspruch führen. Unter dieser Annahme gilt $n \in k$ und $k \in n$. Nach Lemma A.3.2.2 folgt daraus $n \subseteq k$ und $k \subseteq n$, also doch $n = k$ im Widerspruch zur Annahme. □

Es sei noch bemerkt, dass die Relation $<$ im Modell von John von Neumann genau die Elementrelation $\in$ ist und dass die Relation $\leq$ genau die Teilmengenrelation $\subseteq$ ist. Dieses Prinzip tritt auch bei Ordinalzahlen auf, siehe Unterabschnitt A.5.1. Tatsächlich sind die Elemente von $\mathbb{N}_{\text{vN}}$ genau die endlichen Ordinalzahlen und $\mathbb{N}_{\text{vN}}$ selbst ist die erste unendliche Ordinalzahl.

A.3.3. Arithmetik und Ordnung

Satz A.3.3.1 (Siehe Satz 1.1.4.1.)**.** *Sei I eine unendliche Menge und seien $n, k \in \mathbb{N}_I$. Dann gibt es disjunkte Mengen $A, B \in \mathfrak{P}_{\text{fin}}(I)$ mit $n = [A]_{\approx}$, $k = [B]_{\approx}$; für jede solche Wahl von A und B gilt dann auch $A \cup B \in \mathfrak{P}_{\text{fin}}(I)$. Weiters gibt es*

- *eine Menge $C \in \mathfrak{P}_{\text{fin}}(I)$ mit $C \approx A \times B$.*
- *eine Menge $D \in \mathfrak{P}_{\text{fin}}(I)$ mit $D \approx B^A$. (Wir schreiben B^A für die Menge aller Funktionen von A nach B.)*

Beweisskizze. Um die erste Aussage nachzuweisen, zeigen wir für festes $A_0 \in \mathfrak{P}_{\text{fin}}(I)$ Folgendes: $\mathscr{M} := \{B_0 \in \mathfrak{P}_{\text{fin}}(I) \mid \exists A \approx A_0, B \approx B_0 : A, B \text{ disjunkt}\}$ ist induktiv (und stimmt daher mit $\mathfrak{P}_{\text{fin}}(I)$ überein). Für $B_0 = \emptyset$ kann man $A = A_0$ und $B = B_0$ wählen. Wenn $B_0 \in \mathscr{M}$ und $x \in I$ mit $x \notin B_0$, dann gibt es einmal $A \approx A_0, B \approx B_0$ mit $A \cap B = \emptyset$. Nach Proposition A.3.1.1 ist $A \cup B$ endlich. Da I unendlich ist, gilt insbesondere $I \neq A \cup B$, also gibt es $x' \in I \setminus (A \cup B)$. Setzt man $B' := B \cup \{x'\}$, so folgt $B' \approx B_0 \cup \{x\}$ und $A \cap B' = \emptyset$.
Die verbliebenen beiden Aussagen folgen daraus mit analogen Argumenten zum Beweis von Proposition A.3.1.1(12),(13); und zwar die Aussage über Produkte aus der (gerade bewiesenen) Aussage über Vereinigungen und die Aussage über Potenzen aus der Aussage über Produkte. □

Satz A.3.3.2 (siehe Satz 1.1.4.12)**.** *Sei $\leq$ die durch Definition 1.1.4.10 gegebene Relation. Für alle natürlichen Zahlen k, k', n, n' gelten folgende Eigenschaften:*

(1) *$\nu(n) \not\leq n$.*

(2) *Wenn $k \leq n$ und $k \neq n$, dann gilt $\nu(k) \leq n$.*

(3) *$\leq$ ist reflexiv, transitiv und antisymmetrisch, d. h. eine Ordnungsrelation.*

(4) *Es gilt entweder $n \leq k$ oder $k \leq n$, d. h., $\leq$ ist eine lineare Ordnung.*

(5) *Es gilt*

$$((\leq)) \qquad \forall x, y: \ (x \leq 0 \Leftrightarrow x = 0) \text{ und } (x \leq \nu(y) \Leftrightarrow x \leq y \text{ oder } x = \nu(y))$$

(6) *Die Bedingung $((\leq))$ charakterisiert bereits die Relation $\leq$, das heißt: Jede Relation $R \subseteq \mathbb{N} \times \mathbb{N}$, die $x \ R \ 0 \Leftrightarrow x = 0$ und $x \ R \ \nu(y) \ \Leftrightarrow \ x \ R \ y$ oder $x = \nu(y)$ für alle x, y erfüllt, muss die Relation $\leq$ sein.*

(7) *Aus $k \leq k'$ und $n \leq n'$ folgt $k + n \leq k' + n'$. (Monotoniegesetz für $+$)*

(8) *Aus $k \leq k'$ und $n \leq n'$ folgt $k \cdot n \leq k' \cdot n'$. (Monotoniegesetz für $\cdot$)*

Beweisskizze. Im gesamten Beweis fassen wir die natürlichen Zahlen als $\mathbb{N}_I$ für eine unendliche Menge I auf.

(1) Wir zeigen, dass $\mathscr{M} := \{F \in \mathfrak{P}_{\text{fin}}(I) \mid \forall x \in I \setminus F \nexists E' \subseteq F : E' \approx F \cup \{x\}\}$ induktiv ist (und daher mit $\mathfrak{P}_{\text{fin}}(I)$ übereinstimmt). Dabei ist $\emptyset \in \mathscr{M}$ klar, denn die einzige Teilmenge von $\emptyset$ ist die leere Menge, und diese kann nicht gleichmächtig zu $\{x\}$ sein. Sei jetzt $F \in \mathscr{M}$ und $y \in I \setminus F$. Wir wollen $F \cup \{y\} \in \mathscr{M}$ per Widerspruchsbeweis

zeigen. Angenommen, es gibt $x \in I \setminus (F \cup \{y\})$ und $E' \subseteq F \cup \{y\}$ mit $E' \approx (F \cup \{y\}) \cup \{x\}$. Das bedeutet, dass es eine Bijektion $f : (F \cup \{y\}) \cup \{x\} \to E'$ gibt. Wenn $E' \subseteq F$ oder wenn $f(y) = y$, dann ist die Einschränkung von f auf $F \cup \{x\}$ eine Bijektion $g : F \cup \{x\} \to E' \setminus \{f(y)\} \subseteq F$, im Widerspruch zu $F \in \mathscr{M}$. Wenn umgekehrt $E' \not\subseteq F$, d. h. $y \in E'$, und $f(y) \neq y$, dann ist $E' \setminus \{y\} \subseteq F$ und $g : F \cup \{x\} \to E' \setminus \{y\} \subseteq F$ definiert durch

$$g(z) := \begin{cases} f(z), & z \neq f^{-1}(y) \\ f(y), & z = f^{-1}(y) \end{cases}$$

ist eine Bijektion. Dies ist erneut ein Widerspruch zu $F \in \mathscr{M}$.

(2) Sei $k \leq n$, $k \neq n$. Wir können Mengen $K \subseteq I$ und $N \subseteq I$ finden, die $n = [N]_\approx$, $k = [K]_\approx$ und $K \subseteq N$ erfüllen. Wegen $k \neq n$ muss $K \subsetneq N$ gelten. Sei $k_0 \in N \setminus K$ beliebig, dann ist $\nu(k) = [K \cup \{k_0\}]_\approx$ und $K \cup \{k_0\} \subseteq N$, daher $\nu(k) \leq n$.

(3) Reflexivität und Transitivität sind klar bzw. sehr einfach zu zeigen. Die Antisymmetrie folgt aus bereits Bewiesenem: Angenommen, $n \leq k$ und $k \leq n$ aber $n \neq k$. Aus (2) folgt dann $\nu(n) \leq k \leq n$, also mit der Transitivität $\nu(n) \leq n$ im Widerspruch zu (1).

(4) Induktion nach k bei festem n: Wir setzen $T_n := \{k \in \mathbb{N}_I \mid n \leq k \text{ oder } k \leq n\}$ und zeigen, dass T_n das Element 0 enthält und unter Nachfolgern abgeschlossen ist. Die Ungleichung $0 \leq n$ ist klar, daher gilt $0 \in T_n$.

Wenn nun $k \in T_n$ ist, dann betrachten wir 2 Fälle:

- $n \leq k$. Dann ist $n \leq k \leq \nu(k)$, also $\nu(k) \in T_n$.
- $k \leq n$. Wenn $k = n$, dann folgt $n = k \leq \nu(k)$ und daher $\nu(k) \in T_n$. Wenn $k \neq n$, dann gilt $\nu(k) \leq n$ nach (2), daher wieder $\nu(k) \in T_n$.

(5) Die erste Aussage $x \leq 0 \Leftrightarrow x = 0$ (für alle x) folgt daraus, dass die leere Menge die einzige Menge ist, die zu einer Teilmenge der leeren Menge gleichmächtig ist. Bei der zweiten Aussage $x \leq \nu(y) \Leftrightarrow x \leq y$ oder $x = \nu(y)$ (für alle x, y) folgt die Implikation $\Leftarrow$ aus Transitivität bzw. Reflexivität. Für die umgekehrte Implikation seien x, y mit $x \leq \nu(y)$ gegeben. Wir finden Mengen $X, Y \subseteq I$, die $x = [X]_\approx$ und $y = [Y]_\approx$ erfüllen. Es existiert $y' \in I \setminus Y$, eine Teilmenge $Z \subseteq Y \cup \{y'\}$ und eine Bijektion $f : X \to Z$. Wenn $Z = Y \cup \{y'\}$, dann folgt $X \approx Y \cup \{y'\}$ und $x = [X]_\approx = [Y \cup \{y'\}]_\approx = \nu(y)$. Wenn andererseits $Z \subsetneq Y \cup \{y'\}$, dann kann man ähnlich wie in (1) aus f eine Bijektion g zwischen X und einer Teilmenge von Y gewinnen. Es folgt $x \leq y$.

(6) Induktion: Aus $((\leq))$ folgt unmittelbar, dass die Menge

$$T := \{y \in \mathbb{N} \mid \forall x \in \mathbb{N} : x \, R \, y \Leftrightarrow x \leq y\}$$

das Element 0 enthält und unter Nachfolgern abgeschlossen ist. Wir erhalten $T = \mathbb{N}$, womit R mit $\leq$ übereinstimmt.

(7) Seien $A, B, C, D \subseteq I$ mit $k = [A]_\approx$, $n = [B]_\approx$, $k' = [C]_\approx$ und $n' = [D]_\approx$, wobei B und D als disjunkt angenommen seien (siehe Satz A.3.3.1). Nach Voraussetzung

gibt es Mengen $\tilde{A}, \tilde{B} \subseteq I$ mit $A \approx \tilde{A} \subseteq C$ und $B \approx \tilde{B} \subseteq D$. Dann sind $\tilde{A}$ und $\tilde{B}$ disjunkt mit $\tilde{A} \cup \tilde{B} \subseteq C \cup D$. Daraus erhalten wir nach Definition von $+$ und von $\leq$

$$k + n = [\tilde{A} \cup \tilde{B}]_{\approx} \leq [C \cup D]_{\approx} = k' + n'.$$

(8) Ähnlich wie (7): Seien wieder $A, B, C, D \subseteq I$ mit $k = [A]_{\approx}$, $n = [B]_{\approx}$, $k' = [C]_{\approx}$ und $n' = [D]_{\approx}$ sowie $\tilde{A}, \tilde{B} \subseteq I$ mit $A \approx \tilde{A} \subseteq C$ und $B \approx \tilde{B} \subseteq D$. Dann gilt $\tilde{A} \times \tilde{B} \subseteq C \times D$ und weiter

$$k \cdot n = [\tilde{A} \times \tilde{B}]_{\approx} \leq [C \times D]_{\approx} = k' \cdot n'.$$

□

A.3.4. Anwendungen des Rekursionssatzes

Der Beweis einiger Tatsachen, die wir in Abschnitt 1.1 formuliert haben, erfordert den Rekursionssatz auf $\mathbb{N}$, Satz A.2.2.1. Betrachtet man wiederum dessen Beweis, so ist zu bemerken, dass er nur auf dem Induktionsprinzip und den Eigenschaften der Ordnungsrelation $\leq$, die wir bereits gezeigt haben, fußt. Folglich können wir den Rekursionssatz nun einsetzen, um diese Tatsachen nachzuweisen. Falls notwendig können wir dabei $\mathbb{N}$ in der Formulierung des Rekursionssatzes durch $\mathbb{N}_I$ für eine unendliche Menge I ersetzen.

Lemma A.3.4.1 (Siehe Lemma 1.1.1.9.)**.** *Wenn I und I' unendlich sind, dann gibt es (genau) eine Bijektion $\iota\colon \mathbb{N}_I \to \mathbb{N}_{I'}$, die*

$$\forall n \in \mathbb{N}_I : \ \iota(n) \sim n$$

erfüllt.

Beweisskizze. Man wende den Rekursionssatz, Satz A.2.2.1, an auf $X := \mathbb{N}_{I'}$ und $f := \nu_{\mathbb{N}_{I'}} : \mathbb{N}_{I'} \to \mathbb{N}_{I'}$ sowie $x_0 := 0_{\mathbb{N}_{I'}}$. Das dadurch erhaltene eindeutige $\iota : \mathbb{N}_I \to \mathbb{N}_{I'}$ mit $\iota(0_{\mathbb{N}_I}) = 0_{\mathbb{N}_{I'}}$ und $\iota(\nu_{\mathbb{N}_I}(n)) = f(\iota(n)) = \nu_{\mathbb{N}_{I'}}(\iota(n))$ für alle $n \in \mathbb{N}_I$ ist die gesuchte Abbildung. Um die Surjektivität bzw. Injektivität von f zu zeigen, weist man nach, dass die Mengen $\{n' \in \mathbb{N}_I \mid \exists n \in \mathbb{N}_I : n' = f(n)\}$ bzw. $\{n \in \mathbb{N}_I \mid \forall m \in \mathbb{N}_I : (f(n) = f(m) \Rightarrow n = m)\}$ induktiv sind – für die zweite Menge benötigt man im „Induktionsschritt“ die wiederum (auf triviale Art) mit Induktion zu beweisende Tatsache, dass man jedes $m \in \mathbb{N}_I$ mit $m \neq 0_{N_I}$ als $m = \nu_{N_I}(k)$ schreiben kann. □

Satz A.3.4.2 (Siehe Satz 1.1.2.3)**.** *Ist $(M, 0_M, \nu_M)$ eine beliebige Peano-Struktur, so gilt*

$$(\mathbb{N}, 0, \nu) \cong (M, 0_M, \nu_M).$$

Der zugehörige Isomorphismus $\varphi\colon \mathbb{N} \to M$ ist eindeutig bestimmt.

Beweisskizze. Analog zum Beweis von Lemma A.3.4.1. □

A.4. Äquivalenzen des Auswahlaxioms

A.4.1. Präliminarien

Satz A.4.1.1 (Satz von Hartogs)**.** *Zu jeder Menge M gibt es eine Wohlordnung $(W, <)$, sodass es keine injektive Funktion $f\colon W \to M$ gibt.*

Anmerkung A.4.1.2. Man ist geneigt zu sagen, dass es zu jeder Menge M eine Wohlordnung gibt, die „größer“ als M ist.
Der Satz verwendet das Auswahlaxiom nicht!

Beweis. Die Faktormenge $W := \{\,(T, <_T) \mid T \subseteq M, (T, <_T) \text{ ist Wohlordnung}\,\}/_{\cong}$ ist nach Unterabschnitt A.1.3 selbst wohlgeordnet, sagen wir durch $<_W$. Angenommen es gäbe eine injektive Funktion $f\colon W \to M$.
Setzen wir $T := f(W)$, dann ist $f\colon W \to T$ eine Bijektion; es gibt daher eine (eindeutig bestimmte) Relation $<_T$ auf T, sodass $f\colon (W, <_W) \to (T, <_T)$ zu einem Ordnungsisomorphismus wird.
Also ist $w_0 := [(T, <_T)]_{\cong} \in W$.
Die Abbildung $t \mapsto (T_t, <)$ ist ein Ordnungsisomorphismus zwischen $(T, <_T)$ und dem durch w_0 definierten Anfangsabschnitt $(W_{w_0}, <_W)$ von W. Daher gilt

$$(W, <_W) \overset{f}{\cong} (T, <_T) \cong (W_{w_0}, <_W).$$

Also müsste W zu einem Anfangsabschnitt von sich selbst isomorph sein. Dies ist aber nach Lemma A.1.2.4(d) nicht möglich. □

Definition A.4.1.3. Eine Menge $\mathcal{F}$ (von Mengen) hat *endlichen Charakter*, wenn für alle Mengen X die folgende Äquivalenz gilt:

$$X \in \mathcal{F} \;\Leftrightarrow\; [\forall T \subseteq X : (T \text{ endlich } \Rightarrow T \in \mathcal{F})].$$

Das heißt, dass eine Menge X genau dann in $\mathcal{F}$ liegt, wenn es alle ihre endlichen Teilmengen tun.

Beispiel A.4.1.4. Ein klassisches Beispiel einer Menge von endlichem Charakter ist die Menge der linear unabhängigen Teilmengen eines Vektorraums.

Anmerkung A.4.1.5. Jede Familie von endlichem Charakter ist unter Untermengen abgeschlossen. Wenn man zu überprüfen hat, dass eine vorgegebene Familie endlichen Charakter hat, dann ist in vielen Fällen die Implikation

$$X \in \mathcal{F} \;\Rightarrow\; [\forall T \subseteq X : (T \text{ endlich } \Rightarrow T \in \mathcal{F})]$$

und manchmal sogar die stärkere Aussage

$$X \in \mathcal{F} \;\Rightarrow\; (\forall T \subseteq X : T \in \mathcal{F})$$

aus trivialen Gründen erfüllt, und nur die Implikation

$$[\forall T \subseteq X : (T \text{ endlich } \Rightarrow T \in \mathcal{F})] \;\Rightarrow\; X \in \mathcal{F}$$

erfordert ein mathematisches Argument. Meist ist es übersichtlicher, stattdessen die Kontraposition zu beweisen, also:

$$X \notin \mathcal{F} \;\Rightarrow\; [\exists T \subseteq X : (T \text{ endlich } \;\wedge\; T \notin \mathcal{F})]$$

Lemma A.4.1.6. *Sei $\mathcal{F}$ eine Familie von endlichem Charakter. Dann hat jede Kette der Halbordnung $(\mathcal{F}, \subseteq)$ eine obere Schranke (in $\mathcal{F}$).*

Beweis. Sei $\mathcal{K} \subseteq \mathcal{F}$ eine Kette in $(\mathcal{F}, \subseteq)$ und sei $T \subseteq \bigcup \mathcal{K}$ beliebig aber endlich. Dann gibt[5] es ein $K \in \mathcal{K}$ mit $T \subseteq K \in \mathcal{F}$ und damit $T \in \mathcal{F}$. Da $\mathcal{F}$ endlichen Charakter hat, liegt $\bigcup \mathcal{K}$ in $\mathcal{F}$ und ist damit eine obere Schranke für $\mathcal{K}$. □

A.4.2. Formulierung der Äquivalenzen

Definition A.4.2.1 (Auswahlaxiom, Axiom of Choice, AC)**.** Sei $\mathcal{M}$ eine Menge nichtleerer, paarweise disjunkter Mengen. Dann gibt es ein $A \subseteq \bigcup \mathcal{M}$, sodass

$$\forall M \in \mathcal{M} : \exists!\, m \in M \cap A$$

A heißt in diesem Zusammenhang auch eine *Auswahlmenge*.

Lemma A.4.2.2 (Auswahlfunktion, AF)**.** *Sei I eine Menge und $(M_i)_{i \in I}$ eine Familie[6] nichtleerer Mengen, dh. $M_i \neq \emptyset$ für alle $i \in I$. Dann gibt es ein $f \colon I \to \bigcup_{i \in I} M_i$, sodass $f(i) \in M_i$ für alle $i \in I$. In anderen Worten: Das kartesische Produkt nichtleerer Mengen ist nicht leer. Die Funktion f heißt* Auswahlfunktion.

Lemma A.4.2.3 (Hausdorffsches Maximalitätsprinzip, Hausdorffscher Kettensatz, HMP)**.** *Sei $(H, \leq)$ eine Halbordnung, $K_0 \subseteq H$ eine Kette. Dann gibt es eine maximale Kette K mit $K_0 \subseteq K \subseteq H$.*

Lemma A.4.2.4 (Lemma von Zorn, LVZ)**.** *Sei $(H, \leq)$ eine Halbordnung, in der jede Kette eine obere Schranke hat,[7] das heißt:*

$$\forall K \subseteq H : [K \text{ Kette } \Rightarrow \exists h_K \in H \, \forall k \in K : k \leq h_K].$$

Dann gilt: Für alle $h \in H$ gibt es ein Element $m_h \in H$ mit $h \leq m_h$, das maximal in $(H, \leq)$ ist. (Oft verwendet man nur die Tatsache, dass es in $(H, \leq)$ überhaupt ein maximales Element gibt.)

[5] Hier verwendet man Induktion nach der Größe von T.

[6] Es sei bemerkt, dass man jede Menge zu einer Familie machen kann, indem man sie mit sich selbst indiziert.

[7] Eine partielle Ordnung, in der jede Kette eine obere Schranke hat, kann nicht leer sein (weil die leere Menge eine Kette ist, und folglich eine obere Schranke haben müsste). Oft beginnt man in einer Anwendung des Zornschen Lemmas aber mit einem expliziten Beweis, dass die betrachtete bzw. gerade konstruierte Halbordnung nicht leer ist, um sich ab dann nur mit nichtleeren Ketten beschäftigen zu müssen.

Häufig wendet man das Lemma von Zorn auf eine Teilmenge $\mathcal{F} \subseteq \mathfrak{P}(M)$, geordnet durch $\subseteq$ an. Für eine Kette $\mathcal{K} \subseteq \mathcal{F}$ gibt es einen natürlichen Kandidaten für eine obere Schranke, nämlich $S = \bigcup \mathcal{K}$. Kann man zeigen,[8] dass stets $S \in \mathcal{F}$ gilt, so sind die Voraussetzungen des Lemmas von Zorn erfüllt. Hat $\mathcal{F}$ endlichen Charakter, ist dies stets der Fall.

Lemma A.4.2.5 (Lemma von Teichmüller/Tukey, LTT)**.** *Sei $\mathcal{F}$ eine Familie von endlichem Charakter. Dann hat $\mathcal{F}$ ein $\subseteq$-maximales Element.*

Satz A.4.2.6 (Wohlordnungssatz, WOS, Satz von Zermelo)**.** *Sei W eine Menge. Dann gibt es eine Wohlordnung $<$ auf W, dh. es gibt eine Relation $< \subseteq W \times W$, sodass $(W, <)$ eine Wohlordnung ist.*

A.4.3. Beweis der Äquivalenz der Aussagen in A.4.2

Satz A.4.3.1. *Es sind äquivalent:*

AC Das Auswahlaxiom, A.4.2.1

AF Die Existenz einer Auswahlfunktion, A.4.2.2

HMP Das Hausdorffsche Maximalitätsprinzip, A.4.2.3

LVZ Das Lemma von Zorn, A.4.2.4

LTT Das Lemma von Teichmüller/Tukey, A.4.2.5

WOS Der Wohlordnungssatz von Zermelo, A.4.2.6

Der Beweis ergibt sich durch den Nachweis der folgenden Implikationen:

Beweis von $AC \Rightarrow AF$. Seien die nichtleeren Mengen M_i für $i \in I$ gegeben, und sei $M_i^* := \{i\} \times M_i$. Dann ist $\mathcal{M} := (M_i^*)_{i \in I}$ eine paarweise disjunkte Familie und erfüllt damit die Voraussetzungen des Auswahlaxioms, das heißt es gibt eine Auswahlmenge $f \subseteq \bigcup \mathcal{M}$ mit $\forall i \in I : \exists! m_i^* = (i, m_i) \in f \cap M_i^*$, wobei $m_i \in M_i$. Also ist

$$f\colon \begin{cases} I & \to & \bigcup_{i \in I} M_i \\ i & \mapsto & m_i \end{cases}$$

die gesuchte Auswahlfunktion. □

[8] Achtung! Hier kann die üblicherweise verwendete schlampige Notation Verwirrung stiften. Wenn man von der Ordnung $(\mathcal{F}, \subseteq)$ spricht, meint man nämlich die Ordnung $(\mathcal{F}, \leq)$, wobei $\leq$ die Einschränkung der Teilmengenrelation auf $\mathcal{F}$ ist; dies wird durch die Notation aber verschleiert. Wenn man nun $S := \bigcup \mathcal{K}$ setzt, ist $Q \subseteq S$ für alle $Q \in \mathcal{K}$ zwar automatisch erfüllt, aber für $Q \leq S$ muss man erst $S \in \mathcal{F}$ zeigen.

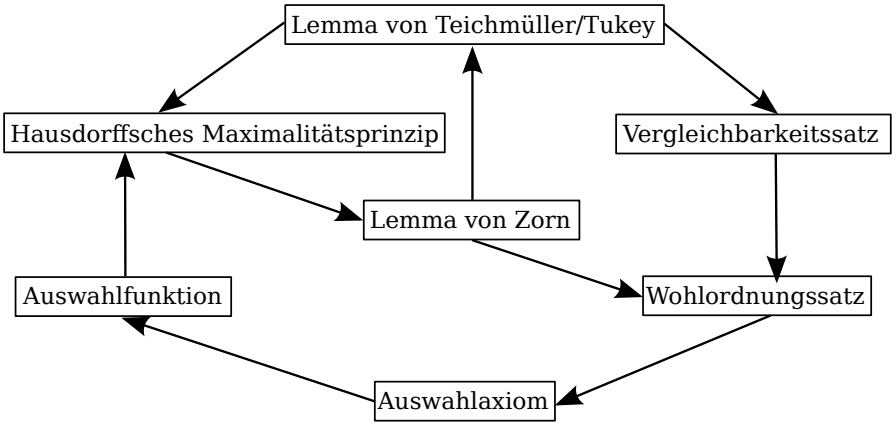


Abbildung A.1.: Die Pfeile symbolisieren die in diesem Unterabschnitt gezeigten Implikationen, mit Ausnahme des Vergleichbarkeitssatzes A.5.2.3, den wir erst in Unterabschnitt A.5.2 betrachten werden; siehe auch Anmerkung A.5.2.5.

Beweis von AF ⇒ HMP. Sei $(H, \leq)$ eine Halbordnung und $K_0 \subseteq H$ eine Kette. Angenommen, es gäbe keine maximale Kette K mit $K_0 \subseteq K \subseteq H$. Das heißt, dass für jede Kette $K \supseteq K_0$ die Menge

$$R(K) := \{x \in H \mid x \notin K,\ K \cup \{x\} \text{ ist Kette in } (H, \leq)\}$$

nicht leer ist.
Mit Satz A.4.1.1 finden wir eine Wohlordnung $(W, <)$, sodass es keine injektive Funktion $W \to H$ gibt. Sei weiters g eine Auswahlfunktion auf $\mathfrak{P}(H)\backslash\{\emptyset\}$, d. h. $g : \mathfrak{P}(H)\backslash\{\emptyset\} \to H$ mit $g(A) \in A$ für alle $A \in \mathfrak{P}(H) \setminus \{\emptyset\}$.
Durch Anwendung des Rekursionssatzes A.2.1.1 erhalten wir eine Funktion $F\colon W \to H \cup \{*\}$, die für alle $\alpha \in W$ die Beziehung

$$F(\alpha) = \begin{cases} g(R(F[W_\alpha])), & \text{wenn } F[W_\alpha] \text{ Kette ist} \\ *, & \text{sonst} \end{cases}$$

Mit transfiniter Induktion kann man zeigen, dass $F[W_\alpha]$ immer eine Kette ist, und dass daher F nie den Wert $*$ annimmt. Da immer $g(R(K)) \notin K$ gilt, sieht man auch, dass F injektiv ist. Dies ist ein Widerspruch zur Definition von W. □

Beweis von HMP ⇒ LVZ. Sei $(H, \leq)$ eine Halbordnung, in der alle Ketten nach oben beschränkt sind, und $h \in H$. Nach HMP gibt es eine maximale Kette K mit $\{h\} \subseteq K \subseteq H$. Sei $m \in H$ eine obere Schranke von K, insbesondere $m \geq h$. Wegen der Maximalität von K folgt, dass $m \in K$ und m maximal in H ist. □

Beweis von LVZ ⇒ LTT. Sei $\mathcal{F}$ eine Familie von endlichem Charakter. Dann ist $(\mathcal{F}, \subseteq)$ eine Halbordnung, in der wegen A.4.1.6 alle Ketten nach oben beschränkt sind. Also gibt es nach LVZ ein maximales Element. □

Beweis von LTT ⇒ HMP. Sei $(H, \leq)$ eine Halbordnung. Man sieht leicht, dass die Menge $\{K \subseteq H \mid K \supseteq K_0 \text{ ist Kette}\}$ endlichen Charakter hat. In der Tat ist ein $K \subseteq H$ genau dann eine Kette, wenn je zwei (also endlich viele) Elemente aus K vergleichbar (also eine Kette) sind. □

Beweis von LVZ ⇒ WOS. Sei W eine beliebige Menge,
$H := \{(T, \leq) \mid T \subseteq W, (T, \leq) \text{ ist Wohlordnung}\}$ und

$$(T_1, \leq_1) \leq (T_2, \leq_2) :\Leftrightarrow T_1 \subseteq T_2 \quad \wedge \quad T_1 \text{ ist Anfangsabschnitt von } (T_2, \leq_2).$$

$(H, \leq)$ ist eine Halbordnung. Sei $K = \{(T_i, \leq_i) \mid i \in I\} \subseteq H$ eine Kette in $(H, \leq)$ und $T = \bigcup_{i\in I} T_i$, $\leq_T = \bigcup_{i\in I} \leq_i$. Dann ist $(T, \leq_T) \in H$ eine Wohlordnung und es gilt $(T_i, \leq_i) \leq (T, \leq_T)$ für alle $i \in I$. Wir können also LVZ anwenden und erhalten ein maximales Element $(T^*, \leq^*)$. Angenommen $T^* \neq W$ und $w \in W \setminus T^*$. Dann ist

$$(T^*, \leq^*) < \Big(T^* \cup \{w\}, \leq^* \cup (T^* \times \{w\}) \cup \{(w, w)\}\Big) \in H,$$

was der Maximalität von $(T^*, \leq^*)$ widerspricht. □

Beweis von WOS ⇒ AC. Sei $\mathcal{M}$ eine Menge nichtleerer, paarweise disjunkter Mengen. Dann gibt es nach WOS eine Wohlordnung $(W, \leq)$ auf $W := \bigcup \mathcal{M}$ und $\{\min(M) \mid M \in \mathcal{M}\}$ ist die gesuchte Auswahlmenge. □

A.5. Ordinal- und Kardinalzahlen

A.5.1. Ordnungstypen

Anmerkung A.5.1.1. In diesem Abschnitt wollen wir, um Missverständnisse zu vermeiden, strikt zwischen Elementen und Teilmengen des Definitionsbereichs von Funktionen unterscheiden. Wie wir sehen werden, spielen Ordinalzahlen oft eine Doppelrolle, sie treten in natürlicher Weise sowohl als Elemente als auch als Teilmengen anderer Ordinalzahlen auf. Dieses Phänomen ist uns bereits bei $\mathbb{N}_{\text{vN}}$, dem Modell von John von Neumann, begegnet; für $n \in \mathbb{N}_{\text{vN}}$ und $k \in n$ gilt ja $k \subseteq n$ (siehe Lemma A.3.2.2). Genauso folgt für $n \in \mathbb{N}_{\text{vN}}$ wegen $n = \{0, \ldots, n-1\}$ auch $n \subseteq \mathbb{N}_{\text{vN}}$.
Bei gegebener Funktion $f\colon A \to B$ und Teilmenge $T \subseteq A$ schreiben wir deshalb für die Menge $\{f(t) \mid t \in T\}$ nicht wie sonst oft $f(T)$, sondern $f[T]$. Der Ausdruck $f(T)$ ist in diesem Abschnitt nur dann definiert, wenn T ein *Element* des Definitionsbereichs von f ist.

Aus jeder Isomorphieklasse von Wohlordnungen möchten wir einen kanonischen Vertreter als *Ordnungstyp* wählen. Wir wollen also eine Klasse $\mathbb{O}$ von *Ordinalzahlen* so definieren, dass es eine natürliche Zuordnung $\text{otp} : (W, <) \mapsto \text{otp}(W, <) \in \mathbb{O}$ gibt, und zwar solcherart, dass für alle Wohlordungen $(W_1, <_1), (W_2, <_2)$ gilt

$$(W_1, <_1) \cong (W_2, <_2) \;\Leftrightarrow\; \text{otp}(W_1, <_1) = \text{otp}(W_2, <_2). \qquad \text{(otp)}$$

Genauso möchten wir eine Klasse $\mathbb{K}$ von *Kardinalzahlen* und eine natürliche Zuordnung $|\cdot| : M \mapsto |M| \in \mathbb{K}$ definieren, sodass für alle Mengen M_1, M_2 gilt

$$M_1 \approx M_2 \text{ (d. h. } \exists f\colon M_1 \to M_2 \text{ bijektiv)} \quad \Leftrightarrow \quad |M_1| = |M_2|.$$

Sei $(W, <)$ eine Wohlordnung. Mittels transfiniter Induktion (siehe Lemma A.1.2.1, bzw. auch Rekursionssatz A.2.1.1) zeigt man, dass es ein M und genau eine Funktion $\rho\colon W \to M$ mit $\forall \alpha \in W : \rho_W(\alpha) = \rho_W[W_\alpha]$ gibt. Diese Funktion ρ (oder auch ρ_W oder $\rho_{(W,<)}$) heißt *Rangfunktion* für $(W, <)$. Dies benötigt das Ersetzungsaxiom, siehe Unterabschnitt A.6.2.

Beispiel A.5.1.2. Sei $(W, <) = (\mathbb{N}, <)$. Dann ist

$$\begin{aligned}
&\rho(0) = \rho[\{n \in \mathbb{N} \mid n < 0\}] = \rho[\emptyset] = \emptyset = 0_{\text{vN}},\\
&\rho(1) = \rho[\{n \in \mathbb{N} \mid n < 1\}] = \rho[\{0\}] = \{\rho(0)\} = \{\emptyset\} = 1_{\text{vN}},\\
&\rho(2) = \{\emptyset, \{\emptyset\}\} = 2_{\text{vN}}, \quad \text{usw.}
\end{aligned}$$

Definition A.5.1.3. Die Menge $\rho_W[W] = \{\rho(\alpha) \mid \alpha \in W\}$ heißt *Ordnungstyp* von $(W, <)$, und wird mit $\operatorname{otp}(W)$ oder $\operatorname{otp}(W, <)$ bezeichnet.

Lemma A.5.1.4. *Für jede Wohlordnung $(W, <)$ ist ρ_W ein Isomorphismus zwischen $(W, <)$ und $(\operatorname{otp}(W), \in)$.*

UE A5 ▶ **Übungsaufgabe A.5.1.5.** (V) Beweisen Sie Lemma A.5.1.4. (Beweisen Sie insbesondere, dass ρ_W injektiv ist.) ◀ **UE A5**

Definition A.5.1.6. α heißt *Ordinalzahl*, symbolisch $\alpha \in \mathbb{O}$ (wobei $\mathbb{O}$ die Klasse der Ordinalzahlen bezeichne), wenn es eine Wohlordnung $(W, <)$ mit $\alpha = \operatorname{otp}(W, <)$ gibt.

Legen wir das von Neumannsche Modell der natürlichen Zahlen zugrunde, so folgt aus Beispiel A.5.1.2 also, dass $\mathbb{N}$ eine Ordinalzahl ist (in diesem Zusammenhang schreibt man oft auch ω für $\mathbb{N}$). Genauso ist jedes $n \in \mathbb{N}$ eine Ordinalzahl – dies erklärt auch den Begriff „Ordinal*zahl*“: Man kann Ordinalzahlen auffassen als Formalisierung der Idee, wie gewohnt $0, 1, 2, 3, \ldots$ zu zählen, „und dann noch weiter“.

Definition A.5.1.7. Eine Menge X heißt *transitiv*, wenn aus $z \in y \in X$ immer $z \in X$ folgt. Mit anderen Worten: wenn für alle $y \in X$ auch $y \subseteq X$ gilt.

UE A6 ▶ **Übungsaufgabe A.5.1.8.** (F) Zeigen Sie, dass jede Ordinalzahl eine transitive Menge ist. Zeigen Sie, dass jede Ordinalzahl durch die Relation $\in$ (irreflexiv) wohlgeordnet wird. ◀ **UE A6**

Satz A.5.1.9. *Sei α eine Menge. Dann gilt:*

$$\alpha \text{ ist Ordinalzahl } \Leftrightarrow \alpha \text{ ist transitiv und durch } \in \text{ wohlgeordnet.}$$

UE A7 ► **Übungsaufgabe A.5.1.10.** (V) Beweisen Sie Satz A.5.1.9. Hinweis für die noch ausstehende Implikation: Zeigen Sie, dass $\rho_{(\alpha,\in)}$ die Identität ist. ◄ **UE A7**

Folgerung A.5.1.11. *Seien α, β Ordinalzahlen.*

(i) $\beta \in \alpha \Rightarrow \beta \subseteq \alpha$.

(ii) $\beta \subsetneq \alpha \Rightarrow \beta \in \alpha$.

(iii) Genau einer der drei Fälle $\alpha \in \beta$, $\beta \in \alpha$, $\alpha = \beta$ trifft zu.

UE A8 ► **Übungsaufgabe A.5.1.12.** (V) Beweisen Sie Folgerung A.5.1.11. Hinweis: Satz A.1.2.6. ◄ **UE A8**

Das nächste Lemma zeigt, dass wir unser Ziel (otp) erreicht haben.

Lemma A.5.1.13. *Seien $(W_i, <_i)$ Wohlordnungen, $\alpha_i = \mathrm{otp}(W_i, <_i)$, $i \in \{1, 2\}$.*

1. *Wenn $\alpha_1 = \alpha_2$, dann ist $(W_1, <_1) \cong (W_2, <_2)$.*
2. *Wenn $f\colon (W_1, <_1) \cong (W_2, <_2)$ ein Isomorphismus ist, dann ist $\rho_{W_1} = \rho_{W_2} \circ f$, und es folgt $\alpha_1 = \alpha_2$.*

UE A9 ► **Übungsaufgabe A.5.1.14.** (V) Beweisen Sie A.5.1.13. ◄ **UE A9**

Definition A.5.1.15. Bezeichnungen wie in A.5.1.13.

$$\alpha_1 < \alpha_2 :\Leftrightarrow \alpha_1 \in \alpha_2$$

bzw. äquivalent dazu $\alpha_1 \subsetneq \alpha_2$ oder $(W_1, \leq_1) < (W_2, \leq_2)$.

Lemma A.5.1.16. *Sei $M \subseteq \mathbb{O}$. Dann ist $(M, <)$ selbst eine Wohlordnung. Dabei gilt $\bigcup M \,(= \bigcup_{\alpha \in M} \alpha) \in \mathbb{O}$ und $\mathrm{otp}(M, <) = \bigcup M$.*

UE A10 ► **Übungsaufgabe A.5.1.17.** (V) Beweisen Sie Lemma A.5.1.16. ◄ **UE A10**

Bei der nächsten Definition lohnt es, erneut das von Neumannsche Modell der natürlichen Zahlen im Hinterkopf zu haben.

Definition A.5.1.18. Sei α eine Ordinalzahl.

- $\alpha + 1 := \alpha \cup \{\alpha\}$ ist eine Ordinalzahl, die man die *Nachfolgerordinalzahl* bzw. den *Nachfolger* von α nennt.
- $\alpha \neq 0$ heißt *Limesordinalzahl* (oder auch kurz *Limeszahl*), wenn es kein $\beta \in \mathbb{O}$ gibt mit $\alpha = \beta + 1$.

UE A11 ► **Übungsaufgabe A.5.1.19.** (F) Zeigen Sie für eine Ordinalzahl α folgende Aussagen: ◄ **UE A11**

(1) $\alpha + 1 = \min\{\beta \in \mathbb{O} \mid \beta > \alpha\}$.

(2) α ist genau dann eine Limeszahl, wenn $\alpha = \bigcup \alpha$ gilt, bzw. wenn $\forall \beta \in \mathbb{O} : \beta < \alpha \Rightarrow \beta + 1 < \alpha$ gilt.

(3) Die kleinste Limesordinalzahl ist $\omega = \mathrm{otp}(\mathbb{N}, <)$.

A.5.2. Größenvergleich von Mengen

Zur Wiederholung: Ohne Verwendung von Ordinalzahlen und des Auswahlaxioms lässt sich für Mengen A, B eine Sprechweise des Größenvergleichs definieren:

Definition A.5.2.1.

- $|A| = |B| :\Leftrightarrow A \approx B \Leftrightarrow \exists f\colon A \to B$ bijektiv
- $|A| \leq |B| :\Leftrightarrow \exists f\colon A \to B$ injektiv
- $|A| \leq^* |B| :\Leftrightarrow \exists f\colon B \to A$ surjektiv oder $A = \emptyset$

Dies versteht sich als Sprech- bzw. Schreibweise, noch ohne $|A|$ als mathematisches Objekt definiert zu haben.

UE A12 ► **Übungsaufgabe A.5.2.2.** (F+) ◄ **UE A12**

- Beweisen Sie: Wenn $|A| \leq |B|$, dann $|A| \leq^* |B|$. (Verwendet Ihr Beweis das Auswahlaxiom?)
- Beweisen Sie: Wenn $|A| \leq^* |B|$, dann $|A| \leq |B|$. (Verwendet Ihr Beweis das Auswahlaxiom?)

Satz A.5.2.3 (Vergleichbarkeitssatz)**.** *Für beliebige Mengen A und B gilt*

$$|A| \leq |B| \ \vee \ |B| \leq |A|.$$

Es gibt also entweder eine Injektion von A nach B oder eine Injektion von B nach A.

UE A13 ► **Übungsaufgabe A.5.2.4.** (V) Beweisen Sie Satz A.5.2.3. Hinweis: Dies benötigt AC. Man überlegt sich, dass injektive partielle Funktion zu sein eine Eigenschaft von endlichem Charakter ist und wendet LTT (Lemma A.4.2.5) an. ◄ **UE A13**

Anmerkung A.5.2.5. Der Vergleichbarkeitssatz ermöglicht uns den folgenden, alternativen Beweis von WOS (Satz A.4.2.6). Für eine Menge M sei $(W, <)$ eine wohlgeordnete Menge, sodass es keine Injektion $f : W \to M$ gibt (Satz von Hartogs, A.4.1.1). Nach dem Vergleichbarkeitssatz A.5.2.3 gibt es eine Injektion $g : M \to W$. Man kann g auch

als Bijektion $g : M \to f(M) \subseteq W$ auffassen. Die Ordnung $(g(M), <)$, d. h. $g(M)$ mit der Einschränkung von $<$ auf $g(M)$, ist ebenfalls eine Wohlordnung. Folglich induziert g gemäß $m_1 <_M m_2 :\Leftrightarrow g(m_1) < g(m_2)$ eine zu $(g(M), <)$ isomorphe Wohlordnung auf M.

Satz A.5.2.6 (Cantor-Schröder-Bernstein)**.** *Für beliebige Mengen A, B gilt*

$$|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|.$$

Anders formuliert: Gibt es eine Injektion von A nach B und eine Injektion von B nach A, so gibt es eine Bijektion zwischen A und B.

Beweis. Dies benötigt nicht AC. Seien $f\colon A \to B$ und $g\colon B \to A$ Injektionen. Wir definieren $C_0 = A \setminus g[B]$, $C_{n+1} = g[f[C_n]]$ für $n \in \mathbb{N}$ (formal steckt hier der Rekursionssatz dahinter) und $C = \bigcup_{n\in\omega} C_n$. Sei $h := f|_C \cup g^{-1}|_{A\setminus C}$, dh. für $a \in A$ ist

$$h(a) = \begin{cases} f(a) & \text{falls } a \in C \\ g^{-1}(a) & \text{falls } a \notin C \end{cases}$$

Die Funktion h ist wohldefiniert, denn für $a \notin C$ gilt insbesondere $a \notin C_0$, d. h., a hat ein Urbild unter g. Zu zeigen bleibt die Bijektivität.

- Surjektivität: Sei $b \in B$. Falls $b \in f[C]$, dann gilt offensichtlich $b \in h[C]$. Für $b \notin f[C]$ sei $a := g(b)$. Es gilt $a \notin C_0$ (nach Definition) und außerdem $b \notin f[C] \supseteq f[C_n]$ für alle n, daher $b \notin f[C_n]$. Daraus folgt $a = g(b) \notin g[f[C_n]] = C_{n+1}$ (hier verwenden wir die Injektivität von g). Also erhalten wir $a \notin C$, daher $b = g^{-1}(a) = h(a) \in h[A]$.

- Injektivität: f und g^{-1} sind für sich genommen jeweils injektiv. Angenommen $f(c) = g^{-1}(a)$ mit $c \in C$ und $a \in A \setminus C$. Also gibt es ein $n \in \mathbb{N}$ sodass $c \in C_n$. Folglich erhalten wir $g(f(c)) \in C_{n+1} \subseteq C$ aber $g(f(c)) = g(g^{-1}(a)) = a \notin C$, einen Widerspruch. □

Folgerung A.5.2.7. *Zusammenfassend gilt:*

- $=, \leq, \leq^*$ *sind reflexiv und transitiv.*
- $|A| \leq |B| \Leftrightarrow |A| \leq^* |B|$ *(Der Beweis von „⇐“ braucht AC.)*
- $|A| \leq |B| \vee |B| \leq |A|$ *(Satz A.5.2.3; das braucht AC.)*
- $|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$ *(Satz A.5.2.6)*

Somit sind Kardinalitäten „totalgeordnet“.

A.5.3. Kardinalzahlen

Definition A.5.3.1. Laut Wohlordnungssatz gibt es auf jeder Menge M eine binäre Relation $<$ (eine Teilmenge von $M \times M$), sodass $(M, <)$ eine Wohlordnung ist. Also

$$\emptyset \neq \{\mathrm{otp}(M, <) \mid \leq \text{ Wohlordnung auf } M\} =: O(M) \subseteq \mathbb{O}$$

und damit (siehe Lemma A.5.1.16) gibt es $\min O(M) =: |M| = \kappa(M)$. Dieses Minimum nennen wir die *Kardinalität* von M.
Alle $\kappa \in \mathbb{O}$, die als Kardinalitäten (d. h. minimale Ordinalzahlen gegebener „Größe“ bezüglich Bijektionen, im Sinne der Sprechweise aus Definition A.5.2.1) auftreten, heißen *Kardinalzahlen*.
Die Klasse $\mathbb{K}$ aller Kardinalzahlen ist als Teilklasse von $\mathbb{O}$ wohlgeordnet. Es gibt sogar eine kanonische Zuordnung (nicht Funktion) der Ordinalzahlen zu den unendlichen Kardinalzahlen $\alpha \mapsto \aleph_\alpha$, wobei[9] $\aleph_0$ die kleinste unendliche Kardinalzahl ist, $\aleph_{\alpha+1}$ die kleinste Kardinalzahl größer als $\aleph_\alpha$ ist und $\aleph_\lambda$ für eine Limeszahl λ die kleinste Kardinalzahl ist, die größer als alle $\aleph_\beta$ mit $\beta < \lambda$ ist.

Beispiel A.5.3.2. $\mathrm{otp}(\mathbb{N}, <) = \omega =: \aleph_0 = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$ ist eine Kardinalzahl. Hingegen ist $\omega + 1 = \omega \cup \{\omega\}$ keine Kardinalzahl, da $|\omega + 1| = |\omega|$.
$2^{\aleph_0} = |2^\omega| = |\mathbb{R}| = |\mathbb{C}| =: \mathfrak{c}$ heißt *Kontinuum*.

Anmerkung A.5.3.3. Die *Kontinuumshypothese* CH besagt, dass jede überabzählbare Teilmenge der reellen Zahlen gleichmächtig zu den reellen Zahlen ist. Unter AC ist das äquivalent dazu, dass die Kardinalität der reellen Zahlen die kleinste überabzählbare Kardinalität ist, also $\mathfrak{c} = \aleph_1$. Die Kontinuumshypothese ist in ZFC weder beweisbar noch widerlegbar.

A.5.4. Operationen für Ordinalzahlen

Summe und Produkt von Wohlordnungen $(W_1, \leq_1), (W_2, \leq_2)$ definiert man wie folgt:

Definition A.5.4.1.

- $\underbrace{(W_1, <_1) + (W_2, <_2)}_{\text{Summe}} := (W_1 \cup W_2, <)$ für $W_1 \cap W_2 = \emptyset$ mit
  $\alpha < \beta :\Leftrightarrow (\alpha \in W_1 \wedge \beta \in W_2) \vee (\exists i \in \{1, 2\} : \alpha, \beta \in W_i \wedge \alpha <_i \beta)$
- $\underbrace{(W_1, <_1) \cdot (W_2, <_2)}_{\text{(lexikographisches) Produkt}} := (W_1 \times W_2, <)$ mit
  $(\alpha_1, \alpha_2) < (\beta_1, \beta_2) :\Leftrightarrow \alpha_2 <_2 \beta_2 \vee (\alpha_2 = \beta_2 \wedge \alpha_1 <_1 \beta_1)$
  (Achtung: Die lexikographische Ordnung wird hier anders als gewohnt „von hinten“ definiert, d. h., die zweite Komponente ist signifikant.)

[9] $\aleph$ (Aleph) ist der erste Buchstabe des hebräischen Alphabets.

Folgerung A.5.4.2. *Man überlegt sich leicht, dass aus* $(W_i, <_i) \cong (W_i', <_i')$ *(für* $i = 1, 2$*) die Beziehung* $(W_1, <_1) + (W_2, <_2) \cong (W_1', <_1') + (W_2', <_2')$ *folgt.*
Also wird durch $\mathrm{otp}(W_1, <_1) + \mathrm{opt}(W_2, <_2) := \mathrm{otp}((W_1, <_1) + (W_2, <_2))$ *(und analog für* $\cdot$*) auf* $\mathbb{O}$ *eine Operation wohldefiniert: die Ordinalzahl-Addition bzw. -Multiplikation. Achtung: Diese Operationen sind nicht kommutativ! Beispielsweise gilt* $\omega + \omega = \omega \cdot 2 \neq 2 \cdot \omega = \omega$.

A.5.5. Operationen auf Kardinalzahlen

Definition A.5.5.1. Seien X, Y Mengen. Mit Y^X (manchmal auch als ${}^X Y$ geschrieben) bezeichnet man die Menge aller Funktionen von X nach Y.

Beispiele A.5.5.2.

(a) Wenn $X = \{a\}$ einelementig ist, dann gibt es eine natürliche Bijektion zwischen Y^X und Y, nämlich die Abbildung, die jeder Funktion $f \in Y^X$ ihren einzigen Wert $f(a)$ zuordnet.

(b) Wenn $X = \{a, b\}$ zwei Elemente hat, bieten sich zwei bijektive Abbildungen von Y^X nach $Y \times Y$ an; die eine bildet f auf das Paar $(f(a), f(b))$ ab (und die andere?).

(c) Wenn X die leere Menge ist, dann gibt es genau eine Funktion $f\colon X \to Y$, nämlich $f = \emptyset$. (Als Funktion betrachtet nennt man die leere Menge auch gelegentlich 0-Tupel.) In diesem Sinne gilt also $Y^\emptyset = \{\emptyset\}$ für alle Mengen Y, insbesondere auch für die leere Menge: $\emptyset^\emptyset = \{\emptyset\}$.

Wir verallgemeinern die Wohldefiniertheit der Rechenoperationen von endlichen Mengen (siehe Definition 1.1.4.2).

Lemma A.5.5.3. *Für Mengen* A_i, B_i, $i \in \{1, 2\}$ *gilt*

$$|A_1| = |A_2|, |B_1| = |B_2| \Rightarrow \begin{cases} |A_1 \cup B_1| & = |A_2 \cup B_2| \quad \text{sofern} A_1 \cap B_1 = \emptyset = A_2 \cap B_2 \\ |A_1 \times B_1| & = |A_2 \times B_2| \\ |A_1^{B_1}| & = |A_2^{B_2}| \end{cases}$$

Daher werden durch

Definition A.5.5.4.

- $|A| + |B| := |A \cup B|$ (sofern $A \cap B = \emptyset$)
- $|A| \cdot |B| := |A \times B|$
- $|A|^{|B|} := |A^B|$

Operationen auf $\mathbb{K}$ wohldefiniert: Kardinalzahl-Addition, -Multiplikation und -Exponentation. Für endliche Mengen A, B stimmen diese Funktionen mit den üblichen Operationen der Addition, Multiplikation und Exponentiation[10] überein.
Achtung 1: $\aleph_0 +_{\mathbb{K}} 1 = \aleph_0$ aber $\omega +_{\mathbb{O}} 1 \neq \omega$ (obwohl $\omega = \aleph_0$)!
Achtung 2: Anders als im vorhergehenden Unterabschnitt bei Ordinalzahlen sind die Kardinalzahl-Addition und -Multiplikation kommutativ!

A.5.6. Unendliche Kardinalzahlarithmetik

Lemma A.5.6.1. *Die folgenden Rechengesetze gelten für alle endlichen und unendlichen Kardinalzahlen κ, λ:*

(a) $\kappa^{\lambda \cdot \mu} = (\kappa^{\lambda})^{\mu}$

(b) $(\kappa \cdot \lambda)^{\mu} = \kappa^{\mu} \cdot \lambda^{\mu}$

(c) $\kappa^{\lambda+\mu} = \kappa^{\lambda} \cdot \kappa^{\mu}$

(d) $\kappa < |\mathfrak{P}(\kappa)| = |2^{\kappa}| = 2^{\kappa}$

UE A14 ► **Übungsaufgabe A.5.6.2.** (V) Beweisen Sie Lemma A.5.6.1. Hinweis: Finden Sie kanonische Bijektionen. Das Auswahlaxiom muss hier nicht verwendet werden. ◄ **UE A14**

Lemma A.5.6.3. *Sei A eine unendliche Menge. Dann gibt es eine abzählbare Teilmenge $T \subseteq A$.*

UE A15 ► **Übungsaufgabe A.5.6.4.** (V) Beweisen Sie Lemma A.5.6.3. Anleitung: Dies benötigt AC. Wenden Sie den Vergleichbarkeitssatz auf A und $\mathbb{N}$ an. (Fallunterscheidung! Eventuell ist es nützlich, zuerst die Situation zu betrachten, dass A eine unendliche Teilmenge von $\mathbb{N}$ ist.) ◄ **UE A15**

Satz A.5.6.5. *Sei A eine unendliche Menge. Dann gilt:*

(1) $A \cup \{a\} \approx A$ *für alle a.*
(2) $A \cup E \approx A$ *für alle endlichen Mengen E.*
(3) $A \times \{0,1\} \approx A$.
(4) $A \cup B \approx A$ *für alle Mengen B mit $|B| \leq |A|$.*
(5) $A \times A \approx A$
(6) $A \times B \approx A$ *für alle nichtleeren Mengen B mit $|B| \leq |A|$.*
(7) $A^n \approx A$ *für $n > 0$.*

[10] In der Analysis wird „0^0“ gelegentlich rein symbolisch als „unbestimmte Form“ verwendet; dies ist als Hinweis darauf zu verstehen, dass man einen Grenzwert zu betrachten hat. In der diskreten Mathematik erweist es sich als sinnvoll und praktisch, immer $0^0 := 1$ zu definieren. Siehe dazu auch Beispiel A.5.5.2(c).

In der Sprache der Kardinalzahlen lassen sich die obigen Aussagen so formulieren:

(1) $\kappa + 1 = \kappa$ *für alle unendlichen* κ.

(2) $\kappa +$ *endlich* $= \kappa$ *für alle unendlichen* κ.

(3) $\kappa \cdot 2 = \kappa$ *oder* $\kappa + \kappa = \kappa$ *für alle unendlichen* κ.

(4) $\kappa + \lambda = \kappa$, *wenn* κ *unendlich ist und* $\lambda \leq \kappa$ *gilt. Äquivalent: Für alle Kardinalzahlen* κ, λ, *von denen mindestens eine unendlich ist, gilt* $\kappa + \lambda = \max(\kappa, \lambda)$.

(5) $\kappa \cdot \kappa = \kappa$ *für alle unendlichen Kardinalzahlen* κ.

(6) $\kappa \cdot \lambda = \kappa$, *wenn* κ *unendlich ist und* $\kappa \geq \lambda > 0$ *gilt. Äquivalent: Für alle Kardinalzahlen* $\kappa, \lambda > 0$, *von denen mindestens eine unendlich ist, gilt* $\kappa \cdot \lambda = \max(\kappa, \lambda)$.

(7) $\kappa^n = \kappa$ *für alle positiven natürlichen Zahlen* n.

Beweis.

(1) OBdA sei $a \notin A$. Laut Lemma A.5.6.3 gibt es eine Bijektion $f\colon \mathbb{N} \to T \subseteq A$. Dann ist die Abbildung $g\colon A \to A$, die durch

$$g(f(n)) := f(n+1) \quad \text{und} \quad \forall x \in A \setminus T : g(x) = x$$

definiert ist, eine Bijektion zwischen A und $A \setminus \{f(0)\}$; sie lässt sich zu einer Bijektion zwischen $A \cup \{a\}$ und A fortsetzen.

(2) Folgt aus (1) mit Induktion.

(3) Wir definieren eine Halbordnung $\mathcal{F}$, deren Elemente gewisse Bijektionen sind:

$$\mathcal{F} := \{\, f \mid \exists X \subseteq A\colon \ f\colon X \times \{0,1\} \to X \text{ ist Bijektion} \,\}.$$

Die Menge $\mathcal{F}$ wird durch die Relation $\subseteq$ partiell geordnet. ($f \subseteq g$, wenn f von g fortgesetzt wird) Die Halbordnung $\mathcal{F}$ enthält die Bijektion zwischen $\emptyset$ und $\emptyset \times \{0,1\} = \emptyset$, ist also nicht leer. Wir wenden das Lemma von Zorn an und erhalten eine maximale Bijektion $g\colon C \times \{0,1\} \to C$, wobei $C \subseteq A$.

Es gilt also $C \times \{0,1\} \approx C$; wenn wir $A \approx C$ zeigen können, erhalten wir leicht $A \times \{0,1\} \approx A$.

Wir unterscheiden zwei Fälle:

1.Fall $A \setminus C$ ist unendlich. Dann enthält $A \setminus C$ eine abzählbare Teilmenge $D \subseteq A \setminus C$ und daher gibt es[11] eine Bijektion $h\colon D \times \{0,1\} \to D$. Dann ist $g \cup h\colon (C \cup D) \times \{0,1\} \to C \cup D$ eine Bijektion, was der Maximalität von g widerspricht.

2.Fall $A \setminus C$ ist endlich. Wie wir in Punkt (2) bewiesen haben, gilt $|A| = |C| + |A \setminus C| = |C|$.

(3) Es gilt $|A| \leq |A \cup B| \leq |A \times \{0,1\}| = |A|$; die zweite Ungleichung lässt sich durch injektive Abbildungen von A nach $A \times \{0\}$ bzw. von B nach $A \times \{1\}$ und die daraus konstruierte injektive Abbildung von $A \cup B$ nach $A \times \{0,1\}$ belegen. Daher folgt $|A| = |A \cup B|$ aus Satz A.5.2.6.

[11] wegen $\mathbb{N} \times \{0,1\} \approx \mathbb{N}$, bezeugt etwa durch die Bijektion $(n,i) \mapsto 2n + i$

(4) Wir gehen ähnlich wie in (3) vor und definieren

$$\mathcal{F} := \{\, f \mid \exists X \subseteq A\colon\ f\colon X \times X \to X \text{ ist Bijektion} \,\}.$$

Wir ordnen $\mathcal{F}$ durch Inklusion (=Fortsetzung), bemerken $\emptyset \in \mathcal{F}$ als Bijektion zwischen $\emptyset$ und $\emptyset \times \emptyset = \emptyset$, benutzen das Lemma von Zorn und erhalten ein maximales $g\colon B \times B \to B$, wobei $|B| = |B \times B|$ nach Definition.

Wir unterscheiden zwei Fälle:

1.Fall Angenommen $|A \setminus B| > |B|$. Dann gibt es eine Teilmenge $C \subseteq A \setminus B$ mit $|C| = |B|$, nämlich das Bild einer Injektion $B \to A \setminus B$. Nun sind die Mengen

$$B \times B, B \times C, C \times B, C \times C$$

alle gleichmächtig zu B bzw. C; nach zweimaliger Anwendung von (4) sehen wir, dass es eine Bijektion

$$h\colon (B \times C) \cup (C \times B) \cup (C \times C) \to C$$

geben muss. Nun ist aber $g \cup h$ eine Bijektion zwischen $B \cup C$ und $(B \cup C) \times (B \cup C)$, was der Maximalität von g widerspricht.

2.Fall $|A \setminus B| \leq B$. Wir erhalten $|A| = |B| + |A \setminus B| = |B|$, wie wir in Punkt (4) gezeigt haben. Wegen $B \approx B \times B$ ergibt sich $A \approx A \times A$.

(3) Wie in (4): Es gilt $|A| \leq |A \times B| \leq |A \times A| = |A|$, sodass aus Satz A.5.2.6 die gewünschte Aussage $|A \times B| = |A|$ folgt.

(4) Folgt mit Induktion aus (5). □

Anmerkung A.5.6.6. Aussage (7) lässt sich nicht auf unendliche Exponenten verallgemeinern. Es gibt zwar (viele) unendliche Kardinalzahlen κ, die $\kappa^{\aleph_0} = \kappa$ erfüllen, es gibt aber auch (viele) unendliche Kardinalzahlen λ, die $\lambda^{\aleph_0} > \lambda$ erfüllen.

Folgerung A.5.6.7.

(1) *Für alle unendlichen Mengen A ist A gleichmächtig zu der Menge $A^{<\omega} := A \cup A^2 \cup A^3 \cup \cdots$, denn die Mächtigkeit der Menge $A^{<\omega}$ ist durch $|A| \cdot \aleph_0 = |A|$ beschränkt.*

(2) *Sei κ eine unendliche Kardinalzahl, und sei $(B_i : i \in I)$ eine Familie von Mengen für die $\forall i : |B_i| \leq \kappa$ und auch $|I| \leq \kappa$ gilt. Dann gilt auch $|\bigcup_{i\in I} B_i| \leq \kappa$.*
(Denn sogar die Kardinalität der disjunkten Vereinigung $\bigcup_{i\in I} B_i \times \{i\}$ ist durch $\kappa \times |I| = |I|$ beschränkt, und es gilt offensichtlich $|\bigcup_{i\in I} B_i| \leq |\bigcup_{i\in I} B_i \times \{i\}|$. Siehe Definition A.5.2.1 und Aufgabe A.5.2.2.)

(3) *Insbesondere gilt: Wenn alle Mengen B_i endlich sind und I unendlich ist, dann ist $|\bigcup_{i\in I} B_i| \leq |I|$.*

Lemma A.5.6.8. *Für unendliche Kardinalzahlen κ gilt:*

(a) $\kappa^\kappa \overset{A.5.6.1(d)}{\leq} (2^\kappa)^\kappa \overset{A.5.6.1(a)}{=} 2^{\kappa\times\kappa} \overset{A.5.6.5(5)}{=} 2^\kappa \leq \kappa^\kappa$, *also* $2^\kappa = \kappa^\kappa$.

(b) $|2^{\mathbb{N}}| = |\mathbb{R}|$. *(Injektionen $2^{\mathbb{N}} \to \mathbb{R}$ und $\mathbb{R} \to 2^{\mathbb{N}}$ finden und Satz A.5.2.6 anwenden)*

(c) $|\mathbb{R}^{\mathbb{N}}| = |(2^{\mathbb{N}})^{\mathbb{N}}| = |2^{\mathbb{N}\times\mathbb{N}}| \overset{A.5.6.5(5)}{=} |2^{\mathbb{N}}| = |\mathbb{R}|$.

A.6. Axiomatische Mengenlehre

A.6.1. Vorbemerkungen

Wozu braucht man Axiome? Es gibt unter den meisten Mathematikerinnen[12] Einigkeit darüber, was ein gültiger Beweis ist. Wenn man also einen Beweis gefunden hat, kann man im Prinzip jeden anderen Mathematiker[13] von dessen Gültigkeit überzeugen. Um aber

- Beweise selbst zum Objekt mathematischer Untersuchungen zu machen,
- insbesondere: um die Nichtexistenz gewisser Beweise zu beweisen,
- sowie: um Überlegungen wie „Ist Satz S auch ohne die Annahme A beweisbar?“ durchzuführen,
- weiters: um wirkliche oder scheinbare Paradoxa (wie etwa das Russell-Paradoxon) zu analysieren/erklären/verstehen/aufzulösen

hat die mathematische Logik den Begriff des formalen Beweises entwickelt. Zunächst legt man in einem Beweissystem fest, welche (einfachen) logischen Wahrheiten, wie etwa $x = y \Rightarrow y = x$, $\forall x(x < 0) \rightarrow (7 < 0)$, $\varphi \Rightarrow \varphi$, etc) man als „logische Axiome“ akzeptiert, sowie welche einfachen Schlussformen, wie etwa

- „Modus ponens“: Aus $\varphi \Rightarrow \psi$ und φ kann man ψ schließen.
- „Einführung von $\vee$“: Aus $(\varphi_1 \Rightarrow \psi)$ und $(\varphi_2 \Rightarrow \psi)$ kann man $(\varphi_1 \vee \varphi_2 \Rightarrow \psi)$ schließen.

zulässig sind. Sodann wählt man „nichtlogische[14] Axiome“, die Information über die betrachteten Objekte enthalten, wie zum Beispiel „zu je zwei verschiedenen Punkten gibt es genau eine Gerade, die diese beiden Punkte enthält“ in der Geometrie, oder „Für alle Mengen x, y gibt es eine Menge P, die sowohl x als auch y als Element enthält“ in der Mengenlehre.
Ein formaler Beweis besteht nun aus endlich[15] vielen Schritten; in jedem Schritt gibt man entweder ein logisches oder nichtlogisches Axiom an, oder man schließt aus früheren Schritten mit Hilfe der erlaubten Schlussformen auf einen neuen Satz.
Ob die so beschriebenen formalen Beweise eine adäquate Interpretation des informellen Begriffs „mathematischer Beweis“ sind, hängt natürlich davon ab, welche logischen Wahrheiten und Schlussformen man zulässt; für das von den meisten Mathematikerinnen[16] betrachtete System der *klassischen Logik*, genauer: der klassischen Prädikatenlogik

[12] Die Fußnote auf Seite 107 ist geeignet zu adaptieren.
[13] Nochmals.
[14] Man beachte den Unterschied zwischen den Begriffen „nichtlogisch“ und „unlogisch“. Die nichtlogischen Axiome wurden früher auch „Eigenaxiome“ genannt.
[15] In der Mathematischen Logik beschäftigt man sich auch mit Logiken, in denen infinitäre Formeln und/oder infinitäre Beweise zugelassen sind; in der Prädikatenlogik erster Stufe, die wir hier betrachten, bestehen aber Formeln aus endlich vielen Zeichen, und Beweise aus endlich vielen Formeln.
[16] Schon wieder.

erster Stufe, gibt es Dutzende von Beweissystemen, die allerdings übereinstimmen, was die beweisbaren Sätze betrifft. Der Gödelsche Vollständigkeitssatz zeigt, dass diese Systeme tatsächlich alle allgemeingültigen Sätze der Prädikatenlogik erster Stufe beweisen. Ob die so beschriebenen formalen Beweise auch wirklich nur Sätze beweisen, die „wahr“ sind, hängt davon ab, ob die nichtlogischen Axiome so gewählt sind, dass sie tatsächlich „wahr“ sind. (Eine zweite Frage ist, ob umgekehrt alle „wahren“ Sätze beweisbar sind; dies hängt davon ab, ob das gewählte System der nichtlogischen Axiome mächtig genug ist. Der Gödelsche Unvollständigkeitssatz verneint diese Frage in vielen Fällen.)

A.6.2. Die Axiome von ZFC

Als Beispiel eines sehr erfolgreichen Systems nichtlogischer Axiome geben wir ohne nähere Erklärung die ZFC-Axiome (Axiome von Zermelo und Fraenkel, mit Auswahlaxiom AC) an. Alle Sätze dieses Skriptums, sowie die meisten Sätze, denen Sie im Mathematikstudium begegnen werden, lassen sich in klassischer Prädikatenlogik mit Hilfe dieser ZFC-Axiome beweisen. (Dies gilt allerdings nur im Prinzip; so lässt sich etwa ein Satz über die natürlichen Zahlen $0, 1, 2, \ldots$ zwar prinzipiell als Satz über die Mengen $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots$ interpretieren und auch beweisen, allerdings mit unverhältnismäßig großem Aufwand.)
Die folgenden Axiome sind informell formuliert. Für eine korrekte Formulierung müsste man noch einige Definitionen hinzufügen, die die verwendeten Begriffe (insbesondere „Funktion“, „Familie“ und „Klasse“) deutlicher in der Sprache der Mengenlehre erklären; statt der Existenz einer unendlichen Menge könnte man die Existenz einer induktiven Menge (siehe Definition 1.1.1.4) fordern. Die Begriffe „Menge“ und „Element“ bedürfen hingegen keiner weiteren Formalisierung; sie werden implizit durch die Axiome beschrieben.

1. *Extensionalitätsaxiom.* Wenn X und Y die selben Elemente haben, dann $X = Y$.

2. *Paarmengenaxiom.* Für alle Mengen a und b gibt es eine Menge $\{a, b\}$, die genau a und b enthält.

3. *Aussonderungsaxiom (Schema).* Wenn P eine Eigenschaft (mit Parameter p) ist, dann gibt es für jedes X und jedes p eine Menge $Y = \{u \in X \mid P(u, p)\}$, die genau jene $u \in X$ enthält, die Eigenschaft P haben.

4. *Vereinigungsmengenaxiom.* Für jedes X gibt es eine Menge $Y = \bigcup X$, die Vereinigung aller Elemente aus X.

5. *Potenzmengenaxiom.* Für jedes X gibt es eine Menge $Y = \mathfrak{P}(X)$, die Menge aller Teilmengen von X.

6. *Unendlichkeitsaxiom.* Es gibt eine unendliche Menge.

7. *Ersetzungsaxiom (Schema).* Wenn eine Klasse F eine Funktion ist, dann gibt es für jede Menge X eine Menge $Y = F[X] = \{F(x) \mid x \in X\}$.

8. *Regularitätsaxiom.* Jede nichtleere Menge hat ein $\in$-minimales Element.

9. *Auswahlaxiom.* Jede Familie nichtleerer Mengen hat eine Auswahlmenge.

Index