Elemente der Zahlentheorie, Aufbau des Zahlensystems

Helmut Schwichtenberg

Mathematisches Institut der Universität München
Wintersemester 2007/2008

Inhaltsverzeichnis

KAPITEL 1

Einführung

Diese einführende Vorlesung für Studienanfänger soll die Grundlagen für eine spätere systematische Bahndlung von Gegenständen der Mathematik legen. Die soll im wesentlichen anhand von Beispielen geschehen, und die Vorlesung soll die Materialien dazu bereitstellen. Die notwendigen allgemeinen Begriffsbildungen (etwa induktive Datentypen, induktive Definitionen) werden anhand einfacher Beispiele eingeführt. Grundkenntnisse der Logik und einfache Beweisprinzipien wie etwa die Induktion sollen eingeübt werden.

Folgende wichtige Begriffe sollen diskutiert werden: was sind Prädikate über (oder Eigenschaften von, Mengen von) etwa natürlichen Zahlen? Die Abstraktion zu „irgendwelche“ ist hier zu grob. Wichtig sind (1) durch Entscheidungsverfahren gegebene Eigenschaften, (2) induktiv definierte Eigenschaften, und (3) daraus durch die logischen Verknüpfungen $\to$ und $\forall$ definierte Eigenschaften (man kann auch noch die induktiv definierten Verknüpfungen $\exists$, $\wedge$, $\vee$ hinzunehmen).

Ziele der Vorlesung sind elementare Begriffe und Resultate der Zahlentheorie, wie etwa der Begriff der Kongruenz, der chinesische Restsatz, Eigenschaften der Primzahlen wie der kleine Fermatsche Satz. Gruppentheorie wird in dem benötigten Umfang entwickelt. Einen wichtigen Abschnitt bilden die reellen Zahlen, deren Vollständigkeit bewiesen wird. Komplexe Zahlen werden wie üblich als Paare reeller Zahlen eingeführt.

Allgemein soll der Unterschied zwischen der konstruktiven Existenz $\exists$ und der schwachen Existenz $\tilde{\exists}$ bewußt gemacht werden. Dies ist aus grundsätzlichen Erwägungen wichtig, aber auch für Anwendungen, wenn man etwa aus Beweisen ihren rechnerischen Gehalt extrahieren möchte. In der mathematischen Literatur wird diese Unterscheidung oft ignoriert; dies ist möglich, weil die allgemeinen logischen Eigenschaften (genauer: die Einführungs- und Beseitigungsaxiome) von $\exists$ auch für $\tilde{\exists}$ gelten. Ferner hat $\tilde{\exists}$ zusätzliche Eigenschaften, etwa $\neg\neg\tilde{\exists} \to \tilde{\exists}$. Der Preis, den man dafür zahlen muß, ist der Verlust des konstruktiven Charakters eines Arguments, oder genauer des rechnerischen Gehalts eines Beweises. In den folgenden Entwicklungen wird

wann immer möglich versucht, den konstruktiven Existenzquantor $\exists$ zu verwenden; die bewiesenen Aussagen werden dann stärker.

KAPITEL 2

Logik und Grundlagen

Vor unseren ersten Schritten in die Mathematik wollen wir die anfänglichen Grundbegriffe festlegen (hier: natürliche Zahlen und Operationen auf ihnen). Ferner wird es nötig sein, eine formale Sprache zu verwenden, die im Vergleich mit der Umgangssprache weniger ausdrucksfähig, aber dafür präzise ist. Mit Bezug auf die formale Sprache können wir dann die logischen Grundlagen entwickeln, auf denen alles Folgende beruht.

2.1. Typen

2.1.1. Datentypen. Wir betrachten induktiv erzeugte *Typen* (oft auch *Datentypen* genannt). Das für uns wichtigste Beispiel ist der Typ **N** der natürlichen Zahlen. Sie werden aus der Null 0 durch die einstellige Nachfolgeroperation S erzeugt. Daneben betrachten wir noch den Typ **P** der binär dargestellten positiven Zahlen, erzeugt aus der Eins 1 durch zwei einstellige Nachfolgeroperation, S_0 und S_1, sowie den Typ **B** der Fregeschen Wahrheitswerte $\mathtt{tt}$ und $\mathtt{ff}$ (oft auch „boolesche Objekte“ genannt). Ferner erlauben wir Typen, die aus anderen, vorher erzeugten Typen aufgebaut sind:

- Produkte $\rho \times \sigma$, erzeugt durch Paarbildung $\langle x^\rho, y^\sigma \rangle$;
- Summen $\rho + \sigma$, erzeugt durch die Einbettungsoperationen $\mathrm{inl}(x^\rho)$ und $\mathrm{inr}(y^\sigma)$;
- Listen $\mathbf{L}(\rho)$, erzeugt aus der leeren Liste nil durch die Operation $x ::_\rho l$, die ein Objekt x vom Typ ρ vorne an die Liste l anhängt.

Unsere Schreibweise für die Mitteilung dieser Definitionen ist

$$
\begin{aligned}
\mathbf{B} &:= \mu_\alpha(\alpha, \alpha) && \text{(Wahrheitswerte)},\\
\mathbf{N} &:= \mu_\alpha(\alpha, \alpha \to \alpha) && \text{(natürliche Zahlen, unär)},\\
\mathbf{P} &:= \mu_\alpha(\alpha, \alpha \to \alpha, \alpha \to \alpha) && \text{(positive Zahlen, binär)},\\
\rho \times \sigma &:= \mu_\alpha(\rho \to \sigma \to \alpha) && \text{(Produkt)},\\
\rho + \sigma &:= \mu_\alpha(\rho \to \alpha, \sigma \to \alpha) && \text{(Summe)},\\
\mathbf{L}(\rho) &:= \mu_\alpha(\alpha, \rho \to \alpha \to \alpha) && \text{(Listen)}.
\end{aligned}
$$

2.1.2. Funktionstypen. Eine zentrale weitere Begriffsbildung ist die des *Funktionstyps* $\rho \to \sigma$. Unter Objekten dieses Typs stellen wir uns beliebige Funktionen f vor, die einem Argument x des Typs ρ einen Wert $f(x)$ des Typs σ zuordnen.

Terme können wir aus Variablen und Funktionskonstanten mit Hilfe der Anwendungsoperation bilden. Ferner erlauben wir die sogenannte *lambda-Abstraktion*: Ist r ein Term vom Typ σ und x eine Variable vom Typ ρ, so ist $\lambda_x r$ ein Term vom Typ $\rho \to \sigma$.

BEZEICHNUNGEN. $\rho \to \sigma \to \tau$ steht für $\rho \to (\sigma \to \tau)$ und allgemein

$$\rho_1 \to \rho_2 \to \dots \rho_{n-1} \to \rho_n \quad \text{für} \quad \rho_1 \to (\rho_2 \to \dots (\rho_{n-1} \to \rho_n) \dots),$$

wir verwenden also Rechtsklammerung.

Wir schreiben x^ρ oder auch $x\colon \rho$ für Variablen „des Typs ρ“. Inhaltlich bedeutet diese Schreibweise, daß die Variable über Objekte des Typs ρ läuft. Den Typzusatz lassen wir oft weg und schreiben einfach x statt x^ρ, wenn der Typ ρ aus dem Zusammenhang klar oder unwesentlich ist.

Bei zweistelligen Funktionen verwenden wir die *Infix* Schreibweise, also zum Beispiel $x + y$ anstelle von $+(x, y)$.

Beim Schreiben von Termen können wir Klammern sparen, wenn wir vereinbaren, daß λ stärker bindet als Anwendungen. Zum Beispiel ist $\lambda_x rs$ zu lesen als $(\lambda_x r)s$. Ferner vereinbaren wir, daß Anwendungen links geklammert werden, daß also rst steht für $(rs)t$.

Zur Klammerersparung schreiben wir z.B. $fxyz$, $ft_0t_1t_2$ anstelle von $f(x, y, z)$, $f(t_0, t_1, t_2)$, wobei f eine Funktion ist, und entsprechend bei einer einstelligen Funktion mit einem (typographisch) einfachen Argument, also fx für $f(x)$, etc. Aus Gründen der Lesbarkeit schreiben wir jedoch $f(gy, hz)$ anstelle von $fgyhz$.

2.1.3. Substitution, freie und gebundene Variablen. Ausdrücke $\mathcal{E}, \mathcal{E}'$, die sich nur durch die Namen der gebundenen Variablen unterscheiden, wollen wir als gleich betrachten. Dies wird manchmal durch die Redeweise „$\mathcal{E}$ und $\mathcal{E}'$ sind α-äquivalent“ ausgedrückt. Mit anderen Worten, wir interessieren uns nur für Ausdrücke „modulo Umbenennung von gebundenen Variablen“. Es gibt Methoden, eindeutige Bezeichnungen für solche Ausdrücke zu finden, zum Beispiel die namenfreien Terme von de Bruijn (1972). Für den menschlichen Leser sind solche Darstellungen jedoch weniger bequem, so daß wir bei der Verwendung von gebundenen Variablen bleiben wollen.

In der Definition der „Substitution des Ausdrucks $\mathcal{E}'$ für eine Variable x in einem Ausdruck $\mathcal{E}$“ verlangt man entweder, daß *keine* in $\mathcal{E}'$ freie Variable durch einen Variablen-Bindungsoperator in $\mathcal{E}$ gebunden wird, wenn man die freien Vorkommen von x durch $\mathcal{E}'$ ersetzt (dies drückt man oft

dadurch aus, daß es keine „Variablenkollisionen“ gibt), oder daß die Substitutionsoperation eine systematische Umbenennung für gebundene Variablen enthält, die Variablenkollisionen vermeidet. Da wir nur an Ausdrücken modulo Umbenennung gebundener Variablen interessiert sind, können wir ohne Beschränkung der Allgemeinheit annehmen, daß die Substitution immer möglich ist.

Bezeichnungen. „FV“ wird für die Menge der freien Variablen eines Ausdrucks verwendet. Also ist $\mathrm{FV}(r)$ die Menge der in r freien Variablen.

$\mathcal{E}[x := r]$ bezeichnet das Resultat der Substitution des Terms r für die Variable x in dem Ausdruck $\mathcal{E}$. Entsprechend bezeichnet $\mathcal{E}[\vec{x} := \vec{r}]$das Resultat der *simultanen* Substitution der Terme $\vec{r} = r_1, \ldots, r_n$ für die Variablen $\vec{x} = x_1, \ldots, x_n$.

Lokal verwenden wir die folgende Konvention. Wenn in einer Überlegung ein Ausdruck in der Form $\mathcal{E}(x)$ eingeführt wurde, also als $\mathcal{E}$ mit einer ausgezeichneten Variablen x, so schreiben wir $\mathcal{E}(r)$ für $\mathcal{E}[x := r]$, und entsprechend für mehrere Variablen.

2.1.4. Explizite Definitionen. Eine Funktion f heißt *explizit definiert*, wenn sie in der Form

$$f(x_1, \ldots, x_n) := r(x_1, \ldots, x_n)$$

definiert ist, wobei $r(x_1, \ldots, x_n)$ ein Term ist, der aus den (verschiedenen) Variablen $x_1, \ldots, x_n$ und Konstanten für bereits eingeführte Funktionen aufgebaut ist (z.B. den „Konstruktoren“ der verwendeten Datentypen, wie etwa 0 und S im Fall von $\mathbf{N}$).

Beispiele für explizite Definitionen sind

(1) $f\colon \rho \to \mathbf{N}$, definiert durch $f(x) := 0$. Hier handelt es sich um die konstante Funktion auf ρ mit dem Wert 0. Unter Verwendung der eben eingeführten lambda-Abstraktion können wir f auch durch $\lambda_x 0$ bezeichnen.
(2) $f\colon \rho_1 \to \ldots \to \rho_n \to \rho_i$, definiert durch $f(x_1, \ldots, x_n) := x_i$. Man spricht hier von der *Projektion* auf die i-te Komponente, und bezeichnet sie durch $\lambda_{x_1,\ldots,x_n} x_i$.
(3) Sind $f\colon \rho \to \sigma$ und $g\colon \sigma \to \tau$ Funktionen, so definiert man die *Komposition* oder *Hintereinanderschaltung* $g \circ f\colon \rho \to \tau$ (gelesen g *nach* f) durch $(g \circ f)(x) := g(f(x))$. Die Bezeichnung ist $\lambda_x(g(f(x)))$.

Natürlich wollen wir auch allgemeinere Formen der Definition von Funktionen zulassen, zum Beispiel rekursive Definitionen. Mit ihnen befassen wir uns im nächsten Abschnitt.

2.2. Rekursive Definitionen

Nehmen wir an, wir haben schon die Multiplikation $\cdot$ auf $\mathbf{N}$ definiert. Dann können wir die Funktion 2^x wie folgt bestimmen. Intuitiv ergibt sich der Wert, indem man x-mal die 2 mit sich selbst multipliziert. Es ist $2^1 = 2$, $2^2 = 2 \cdot 2$, $2^3 = (2 \cdot 2) \cdot 2 = 2^2 \cdot 2$ und $2^4 = ((2 \cdot 2) \cdot 2) \cdot 2 = 2^3 \cdot 2$, also

$$2^{\mathrm{S}x} = 2^x \cdot 2.$$

Setzt man noch $2^0 = 1$, so erhält man daraus auch $2^1 = 2$.

2.2.1. Primitive Rekursion. Allgemein haben wir das Scheme der *primitiven Rekursion*, zur Definition einer Funktion $f\colon \rho_1 \to \ldots \to \rho_n \to \mathbf{N} \to \sigma$ aus gegebenen Funktionen $g\colon \rho_1 \to \ldots \to \rho_n \to \sigma$ und $h\colon \rho_1 \to \ldots \to \rho_n \to \mathbf{N} \to \sigma \to \sigma$:

$$\begin{aligned} f(x_1, \ldots, x_n, 0) &:= g(x_1, \ldots, x_n), \\ f(x_1, \ldots, x_n, \mathrm{S}(y)) &:= h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)). \end{aligned}$$

Beispiele sind die folgenden Gleichungen für die Addition $+$, die Multiplikation $\cdot$ und die Exponentiation exp, alle vom Typ $\mathbf{N} \to \mathbf{N} \to \mathbf{N}$ (wir verwenden wo immer möglich die übliche Infix-Schreibweise, schreiben also $n + m$ anstelle von $+(n, m)$):

$$\begin{aligned} n + 0 &:= n, \quad n + \mathrm{S}(m) := \mathrm{S}(n + m), \\ n \cdot 0 &:= 0, \quad n \cdot \mathrm{S}(m) := (n \cdot m) + n, \\ n^0 &:= 0, \quad n^{\mathrm{S}(m)} := (n^m) \cdot n \end{aligned}$$

wobei wir n^m für $\exp(n, m)$ geschrieben haben).

Definitionen durch primitive Rekursion sind auch über anderen Datentypen möglich. Ein besonders einfaches, aber wichtiges Beispiel für den Typ $\mathbf{B}$ der booleschen Objekte ist die *Fallunterscheidung*:

$$\mathcal{C}(\mathtt{tt}, x, y) := x, \quad \mathcal{C}(\mathtt{ff}, x, y) := y.$$

Wir schreiben [**if** b **then** x **else** y] für $\mathcal{C}(b, x, y)$.

2.2.2. Rekursionsgleichungen. Im Schema der primitiven Rekursion kommt die definierte Funktion auf der rechten Seite einer Gleichung wieder vor; man spricht deshalb auch von Rekursionsgleichungen.

Wir wollen das Schema der primitiven Rekursion noch einmal verallgemeinern und von den Rekursionsgleichungen nur noch verlangen, daß die linken Seiten aus Konstruktoren (wie zum Beispiel 0 und S) und verschiedenen Variablen aufgebaut sind. Es ist zugelassen, daß zwei linke Seiten sich überlappen. Dann müssen jedoch die rechten Seiten bei jeder Substitution, die die linken Seiten gleich macht, auch gleich werden.

Ein Beipiel für eine solche Situation ist die Definition der booleschen Verknüpfungen andb, impb und orb, die alle vom Typ $\mathbf{B} \to \mathbf{B} \to \mathbf{B}$ sind:

$$\begin{array}{lll} \mathtt{tt}\ \mathrm{andb}\ c := c, & \mathtt{ff}\ \mathrm{impb}\ c := \mathtt{tt}, & \mathtt{tt}\ \mathrm{orb}\ c := \mathtt{tt}, \\ b\ \mathrm{andb}\ \mathtt{tt} := b, & \mathtt{tt}\ \mathrm{impb}\ c := c, & b\ \mathrm{orb}\ \mathtt{tt} := \mathtt{tt}, \\ \mathtt{ff}\ \mathrm{andb}\ c := \mathtt{ff}, & b\ \mathrm{impb}\ \mathtt{tt} := \mathtt{tt}, & \mathtt{ff}\ \mathrm{orb}\ c := c, \\ b\ \mathrm{andb}\ \mathtt{ff} := \mathtt{ff}, & & b\ \mathrm{orb}\ \mathtt{ff} := b. \end{array}$$

Wir verwenden die Rekursionsgleichungen – in der Richtung von links nach rechts – zum Berechnen von Funktionswerten oder allgemeiner zum Umformen von Termen; sie heißen deshalb auch *Berechnungsregeln*. Es wird nicht verlangt, daß diese Umformungen abbrechen.

2.2.3. Booleschwertige Funktionen. Relationen können durch booleschwertige Funktionen definiert werden. Beispiele sind die Funktionen $<$ und $=$, beide vom Typ $\mathbf{N} \to \mathbf{N} \to \mathbf{B}$. Sie sind definiert durch

$$(0 = 0) := \mathtt{tt},\ (\mathrm{S}(n) = 0) := \mathtt{ff},\ (0 = \mathrm{S}(m)) := \mathtt{ff},\ (\mathrm{S}(n) = \mathrm{S}(m)) := (n = m),$$
$$(n < 0) := \mathtt{ff}, \quad (0 < \mathrm{S}(m)) := \mathtt{tt}, \quad (\mathrm{S}(n) < \mathrm{S}(m)) := (n < m).$$

2.3. Prädikate und logische Formeln

Wir wollen jetzt von Termen – die Objekte bezeichnen – zu Aussagen übergehen. Eine *Aussage* ist nach Aristoteles „ein sprachliches Gebilde, von dem es sinnvoll ist zu sagen, es sei wahr oder falsch“. In der Mathematik verwendet man anstelle der Umgangssprache künstliche, formale Sprachen, um Eindeutigkeit und Einfachheit zu gewährleisten.

2.3.1. Prädikate, Primformeln und Formeln. Zum Aufbau einer solchen formalen Sprache benötigt man als erstes *Prädikate* (oder besser Prädikatenkonstanten), mit denen man aus Termen *Primformeln* herstellen kann. Ein wichtiges Beispiel ist die (Leibniz)-Gleichheit $\mathrm{Eq}(r^\rho, s^\rho)$. *Formeln* bilden wir dann aus Primformeln durch die Operationen der

- *Implikation* $A \to B$ (gelesen „wenn A, so B“), und der
- *All-Quantifizierung* $\forall_x A$ (gelesen „für alle x gilt A“).

Wir schreiben $A \to B \to C$ für $A \to (B \to C)$ und allgemein

$$A_1 \to A_2 \to \ldots A_{n-1} \to A_n \quad \text{für} \quad A_1 \to (A_2 \to \ldots (A_{n-1} \to A_n) \ldots),$$

verwenden also wieder Rechtsklammerung für die Implikation $\to$. In Formeln können wir Klammern sparen, wenn wir vereinbaren, daß $\forall$ stärker bindet als $\to$. Zum Beispiel ist $\forall_x A \to B$ zu lesen als $(\forall_x A) \to B$. Führende Allquantoren lassen wir oft weg.

2.3.2. Beispiele induktiv definierter Prädikate. Ähnlich wie wir bei Funktionen Definitionen durch Rekursionsgleichungen zugelassen haben, wollen wir auch Prädikate induktiv definieren. Eine induktive Definition eines Prädikats verwendet sogenannte *Klauseln*. Zum Beispiel kann man die geraden Zahlen definieren durch die Klauseln

$$\begin{aligned}&\mathrm{Even}_1^+ \colon \mathrm{Even}(0),\\ &\mathrm{Even}_2^+ \colon \mathrm{Even}(n) \to \mathrm{Even}(\mathrm{S}(\mathrm{S}n)).\end{aligned}$$

Die transitive Hülle einer Relation $\prec$ ist definiert durch

$$\begin{aligned}&\mathrm{TrCl}_1^+ \colon x \prec y \to \mathrm{TrCl}(x,y),\\ &\mathrm{TrCl}_2^+ \colon x \prec y \to \mathrm{TrCl}(y,z) \to \mathrm{TrCl}(x,z).\end{aligned}$$

Die Leibniz Gleichheit Eq ist definiert durch die Klausel

$$\mathrm{Eq}^+ \colon \mathrm{Eq}(x,x).$$

Die Bedeutung einer solchen induktiven Definition ist, daß es sich um das kleinstmögliche Prädikat handeln soll, das unter den Klauseln abgeschlossen ist. Dieses Verständnis formulieren wir durch sogenannte *Beseitigungsaxiome*, die genau das ausdrücken.

Das Beseitigungsaxiom für Even ist

$$\mathrm{Even}^- \colon \mathrm{Even}(m) \to A(0) \to \forall_n(\mathrm{Even}(n) \to A(n) \to A(\mathrm{S}(\mathrm{S}n))) \to A(m).$$

Für die transitive Hülle TrCl haben wir das Beseitigungsaxiom TrCl^-:

$$\begin{aligned}\mathrm{TrCl}^- \colon \mathrm{TrCl}(x_1,y_1) \to \forall_{x,y}(x \prec y \to A(x,y)) \to\\ \forall_{x,y,z}(x \prec y \to \mathrm{TrCl}(y,z) \to A(y,z) \to A(x,z)) \to\\ A(x_1,y_1).\end{aligned}$$

Für die Leibniz Gleichheit Eq lautet das Beseitigungsaxiom

$$\mathrm{Eq}^- \colon \mathrm{Eq}(x,y) \to \forall_z A(z,z) \to A(x,y).$$

2.3.3. Formeln, Klauseln und Prädikate. Der Vollständigkeit halber geben wir jetzt noch eine genaue (simultane) Definition der Begriffe Formel, Klausel und Prädikat. Sie wird aber in dieser Allgemeinheit im Folgenden nicht benötigt; die behandelten Beispiele genügen.

Definition (Formel, Klausel, Prädikat). Sei X eine Prädikatenvariable einer festen „Stelligkeit“ $(\rho_1,\dots,\rho_n)$.

(1) (a) Ist P ein Prädikat und $\vec{r} := r_1,\dots,r_n$ ein Tupel von Termen der Typen $\rho_1,\dots,\rho_n$, so ist $P(\vec{r})$ eine Formel.
(b) Sind A, B Formeln, so auch $A \to B$.
(c) Ist A eine Formel, so auch $\forall_x A$.

(2) Sind A, $B_0, \dots, B_{n-1}$ Formeln, so ist
$$\forall_{\vec{x}}\big(\vec{A} \to \big(\forall_{\vec{y}_\nu}(\vec{B}_\nu \to X(\vec{s}_\nu))\big)_{\nu<n} \to X(\vec{t}\,)\big)$$
eine Klausel.

(3) (a) Ist A eine Formel, so ist $\{\,\vec{x} \mid A\,\}$ ein Prädikat.
(b) Sind $K_0, \dots, K_{k-1}$ Klauseln ($k \geq 1$), so ist $\mu_X(K_0, \dots, K_{k-1})$ ein (induktiv definiertes) Prädikat.

Um leere induktiv definierte Prädikate zu vermeiden, verlangen wir, daß immer eine nullstellige Klausel (ohne „rekursive“ Prämissen) vorhanden ist.

Sind alle Klauseln einer induktiven Definition nullstellig, und kommt in ihnen das zu definierende Prädikat P nur als letzte Konlusion und in der Form $Px_1 \dots x_n$ mit verschiedenen Variablen x_i vor, so spricht man von einer *expliziten Definition*. Ein Prädikate der Form $\{\,\vec{x} \mid A\,\}$ heißt auch *Komprehensionsterm*. Wir identifizieren $\{\,\vec{x} \mid A(\vec{x}\,)\,\}(\vec{r}\,)$ mit $A(\vec{r}\,)$.

Die *Einführungsaxiome* eines induktiv definierten Prädikats I entstehen aus seinen Klauseln, indem man X durch I ersetzt. Das *Beseitigungsaxiom* besagt, daß I „enthalten“ ist in jedem Komprehensionsterm, der auch unter den Klauseln abgeschlossen ist. Wir verzichten hier auf die allgemeine Definition; sie sollte klar sein aus den obigen Beispielen der Beseitigungsaxiome für Even, TrCl und Eq.

2.3.4. Boolesche Terme als Primformeln, Falschheit. Eine wichtige Verwendung der Leibniz Gleichheit Eq in unserer formalen Theorie besteht darin, daß aus einem booleschen Term $r^{\mathbf{B}}$ eine Formel gemacht wird. Wir schreiben
$$\mathrm{atom}(r^{\mathbf{B}}) := \mathrm{Eq}(r^{\mathbf{B}}, \mathtt{tt}).$$
Damit ergibt sich ein bequemer Weg, mit der Gleichheit für Grundtypen umzugehen. In 2.2.3 hatten wir die (entscheidbare) Gleichheit für einen Datentyp ι als booleschwertige Funktion $=_\iota\colon \iota \to \iota \to \mathbf{B}$ eingeführt. Die Definitionsgleichungen (auch Berechnungsregeln genannt) stellen sicher, daß etwa der boolesche Term $\mathrm{S}(r) =_{\mathbf{N}} \mathrm{S}(s)$ identifiziert wird mit $r =_{\mathbf{N}} s$. Wir können jetzt diesen booleschen Term zu einer Formel $\mathrm{Eq}(\mathrm{S}(r) =_{\mathbf{N}} \mathrm{S}(s), \mathtt{tt})$ machen, die wir wieder durch $\mathrm{S}(r) =_{\mathbf{N}} \mathrm{S}(s)$ abkürzen, dieses Mal jedoch mit dem Verständnis, daß es eine Formel ist. Die beiden Formeln $\mathrm{S}(r) =_{\mathbf{N}} \mathrm{S}(s)$ und $r =_{\mathbf{N}} s$ sind also identifiziert, und infolgedessen müssen wir derartige einfache Aussagen nicht separat beweisen.

Eine zweite wichtige Verwendung der Leibniz Gleichheit ist die Definition der *Falschheit* F als
$$F := \mathrm{Eq}(\mathtt{ff}, \mathtt{tt}).$$
Wir werden später sehen, daß bei dieser Definition das Schema $F \to A$ des „ex-falso-quodlibet“ leicht bewiesen werden kann.

Negation, schwache (oder „klassische“) *Disjunktion*, und den schwachen („klassischen“) *Existenzquantor* kann man jetzt definieren durch

$$\begin{aligned} \neg A &:= A \to F, \\ A \mathbin{\tilde{\vee}} B &:= \neg A \to \neg B \to F, \\ \tilde{\exists}_x A &:= \neg \forall_x \neg A. \end{aligned}$$

2.3.5. Konjunktion, Disjunktion und Existenz. Die folgenden Definitionen der Konjunktion $\wedge$, der (starken) Disjunktion $\vee$ und des (starken) Existenzquantors $\exists$ können als Beispiele (expliziter) induktiver Definitionen gesehen werden, die noch von vorgegebenen Parametern abhängen. Wir erhalten so zusätzliche Operationen zum Bilden von *Formeln*:

- *Konjunktion* $A \wedge B$ (gelesen „A und B“),
- *Disjunktion* $A \vee B$ (gelesen „A oder B“), und
- *Existenz-Quantifizierung* $\exists_x A$ (gelesen „es gibt ein x mit A“).

Die Klausel für $\wedge$ ist

$$\wedge^+ \colon A \to B \to A \wedge B$$

mit Parametern A und B. Das Beseitigungsaxiom ist dann

$$\wedge^- \colon A \wedge B \to (A \to B \to C) \to C.$$

Die Disjunktion hat die beiden Klauseln:

$$\vee_0^+ \colon A \to A \vee B, \quad \vee_1^+ \colon B \to A \vee B,$$

und das Beseitigungsaxiom

$$\vee^- \colon A \vee B \to (A \to C) \to (B \to C) \to C.$$

Für $\exists$ hat man eine Klausel mit Parametern x und A

$$\exists^+ \colon A \to \exists_x A$$

und dem Beseitigungsaxiom

$$\exists^- \colon \exists_x A \to \forall_x (A \to B) \to B \quad (x \text{ nicht frei in in } B).$$

Bezeichnungen (Klammerersparung). Beim Schreiben von Formeln können wir wieder Klammern sparen, wenn wir annehmen, daß $\forall, \exists, \tilde{\exists}, \neg$ stärker binden als $\wedge, \vee, \tilde{\vee}$, und daß ferner $\wedge, \vee, \tilde{\vee}$ stärker binden als $\to, \leftrightarrow$ (wobei $A \leftrightarrow B$ steht für $(A \to B) \wedge (B \to A)$). Zum Beispiel ist $A \wedge \neg B \to C$ zu lesen als $(A \wedge (\neg B)) \to C$.

Zur Klammerersparung schreiben wir z.B. $Rxyz$, $Rt_0t_1t_2$ anstelle von $R(x, y, z)$, $R(t_0, t_1, t_2)$, wobei R ein Prädikat ist. Aus Gründen der Lesbarkeit schreiben wir jedoch $R(fx, gy, hz)$ anstelle von $Rfxgyhz$.

Auch bei zweistelligen Relationen verwenden wir wie üblich die *Infix* Schreibweise, also zum Beispiel $x < y$ anstelle von $<(x, y)$. Wir schreiben $r \neq s$ für $\neg(r = s)$ und $r \not< s$ für $\neg(r < s)$.

2.3.6. Beispiele für Formeln. Wir arbeiten über dem Typ $\mathbf{N}$ der natürlichen Zahlen. $\exists_k\, n \cdot k = m$ wird abgekürzt durch $n \mid m$, und bedeutet „n teilt m“. Die Formel

$$n \neq 0 \wedge n \neq 1 \wedge \forall_k\big(k \mid n \to k = 1 \vee k = n\big)$$

bedeutet „n ist eine Primzahl“.

2.4. Mengen, Äquivalenzrelationen, Strukturen

Mengen fassen wir auf als gegeben durch eine Eigenschaft, genauer durch eine Formel mit einer ausgezeichneten Variablen. Wir bilden hier Mengen nur durch Aussonderung aus Typen, also in der Form $\{\, x^\rho \mid A \,\}$, und schreiben $r \in \{\, x \mid A(x) \,\}$ für $A(r)$. Beispiele sind

$$\{\, n^{\mathbf{N}} \mid n \text{ ist Primzahl} \,\},$$
$$\{\, f^{\mathbf{N}\to\mathbf{N}} \mid \forall_n\, f(n) \leq 1 \,\},$$
$$\mathbf{N}.$$

2.4.1. Teilmengen, Durchschnitt, Vereinigung. Sind

$$M := \{\, x \mid A \,\}, \qquad N := \{\, x \mid B \,\}$$

Mengen, so heißt M *Teilmenge* von N (geschrieben $M \subseteq N$), wenn jedes Element von M auch Element von N ist, d.h., wenn $A \to B$ gilt. Für $M \subseteq N$ schreibt man auch $N \supseteq M$. Sind $M := \{\, x \mid A \,\}$ und $N := \{\, x \mid B \,\}$ Mengen, so definieren wir

$$M \cap N := \{\, x \mid A \wedge B \,\} \quad \textit{Durchschnitt} \text{ von } M \text{ und } N,$$
$$M \cup N := \{\, x \mid A \vee B \,\} \quad \textit{Vereinigung} \text{ von } M \text{ und } N,$$
$$M \setminus N := \{\, x \mid A \wedge \neg B \,\} \quad \textit{Differenz} \text{ von } M \text{ und } N.$$

Wir sprechen von einer *schwachen* Vereinigung und schreiben $M \mathbin{\tilde\cup} N$, wenn anstelle von $\vee$ die schwache Disjunktion $\tilde\vee$ verwendet wurde.

Zwei Mengen M und N heißen *disjunkt*, wenn sie keine gemeinsamen Elemente haben, also wenn $M \cap N = \emptyset := \{\, x \mid F \,\}$.

Sind M und N Mengen, so nennt man die Menge

$$M \times N := \{\, (x, y) \mid x \in M \text{ und } y \in N \,\}$$

das *kartesische Produkt* der Mengen M und N.

Unter einer *Relation* R zwischen (Elementen von) M und (Elementen von) N versteht man eine Teilmenge $R \subseteq M \times N$. Statt $(x, y) \in R$ schreibt man oft xRy. Ist speziell $M = N$, so spricht man von einer *Relation auf* M.

Beispiel. Die Teilbarkeitsrelation auf $\mathbf{N}$ ist die Menge

$$\{\,(n,m) \mid \exists_k\, n \cdot k = m\,\} \subseteq \mathbf{N} \times \mathbf{N}.$$

2.4.2. Ein naiver Mengenbegriff; die Russellsche Antinomie. Cantor gab 1895 die folgende „allgemeinere Definition“:

> Unter einer *Menge* verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen.

Insbesondere ist eine Menge durch ihre Elemente vollständig bestimmt (Extensionalitätsprinzip).

Man kann versuchen, diese Definition wie folgt zu verstehen. Sei V die Gesamtheit aller Objekte (unserer Anschauung oder unseres Denkens). Dann kann man

$$\{\,x \mid A\,\}$$

bilden, die Menge aller Objekte x aus V mit der Eigenschaft A. Man beachte, daß $\{\,x \mid A\,\}$ wieder ein Objekt aus V ist. Da man hier alle Objekte mit einer gewissen Eigenschaft zusammenfaßt, spricht man von einem (naiven) *Komprehensionsprinzip*.

Cantors Definition – oder genauer unsere naive Auffassung davon – ist jedoch so nicht haltbar, da sie zu Widersprüchen führt. Am bekanntesten ist die *Russellsche Antinomie*: Sei

$$x_0 := \{\,x \mid \mathrm{Mg}(x) \wedge x \notin x\,\},$$

wobei $\mathrm{Mg}(x)$ die Eigenschaft „x ist Menge“ ausdrücken soll. Dann erhält man $x \in x_0 \leftrightarrow \mathrm{Mg}(x) \wedge x \notin x$ für alle Objekte x, also insbesondere

$$x_0 \in x_0 \leftrightarrow \mathrm{Mg}(x_0) \wedge x_0 \notin x_0 \leftrightarrow x_0 \notin x_0,$$

denn x_0 ist Menge. Einen Grund für diesen Widerspruch kann man darin sehen, daß wir hier – unter Verwendung des naiven Komprehensionsprinzips – von der Vorstellung einer fertigen Gesamtheit aller Mengen ausgegangen sind. Dies ist aber weder notwendig noch entspricht es dem Vorgehen in der Mathematik. Es reicht vollkommen aus, wenn man eine Menge nur dann bildet, wenn ihre Elemente bereits „zur Verfügung stehen“, etwa dadurch, daß sie Objekte eines festen Typs sind.

Für eine genauere Diskussion der historischen Entwicklung der Mengenlehre und insbesondere eine präzise axiomatische Entwicklung der Mengenlehre müssen wir auf die Literatur (etwa das Buch von Deiser (2004)) oder Vorlesungen über mathematische Logik verweisen.

2.4.3. Äquivalenzrelationen. In dieser Vorlesung und auch sonst in der Mathematik spielen Relationen eine besondere Rolle, die man als eine Art „Gleichheit“ ansehen kann, in unserem Fall für die hier einzuführenden Zahlbereiche (ganze, rationale, reelle und komplexe Zahlen).

DEFINITION. Sei $M = \{\, x^\rho \mid A \,\}$ eine Menge und $R(x, y)$ eine zweistellige Relation auf ρ, d.h., eine Formel mit zwei ausgezeichneten Variablen x, y vom Typ ρ. Wir schreiben $x \sim y$ für $R(x, y)$. $R(x, y)$ heißt *Äquivalenzrelation* auf M, wenn für alle $x, y, z \in M$ gilt

(a) $x \sim x$ (Reflexivität),
(b) $x \sim y \to y \sim x$ (Symmetrie),
(c) $x \sim y \to y \sim z \to x \sim z$ (Transitivität).

Ein Beispiel ist die durch $x \sim y := 3 \mid |x - y|$ gegebene Relation auf $\mathbf{N}$.

Es ist möglich und oft üblich, das explizite Auftreten einer Äquivalenzrelation zu vermeiden und stattdessen mit der vertrauten Gleichheit zu arbeiten. Dazu faßt man äquivalente Objekte zusammen zu einer sogenannten Äquivalenzklasse (richtiger wäre „Äquivalenzmenge“, aber „Äquivalenzklasse“ hat sich eingebürgert).

Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Eine nicht leere Teilmenge N von M heißt eine *Äquivalenzklasse* der Relation $\sim$, wenn gilt:

$$\forall_{x,y\in M}\big(x \in N \to y \sim x \to y \in N\big) \quad (N \text{ ist } \sim\text{-}\textit{abgeschlossen}), \tag{2.1}$$

$$\forall_{x,y\in M}\big(x, y \in N \to x \sim y\big). \tag{2.2}$$

BEHAUPTUNG. *Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Jedes $x \in M$ liegt in genau einer Äquivalenzklasse; sie wird mit $[x]$ bezeichnet.*

BEWEIS. Existenz. Setze $[x] := \{\, y \in M \mid y \sim x \,\}$. Dann ist $x \in [x]$ wegen der Reflexivität von $\sim$. Zu zeigen bleibt, daß $[x]$ eine Äquivalenzklasse ist. Zu (2.1). Sei $y \in [x]$ und $z \sim y$. Dann gilt $y \sim x$, also auch $z \sim x$ wegen der Transitivität von $\sim$, also $z \in [x]$. Zu (2.2). Seien $y, z \in [x]$. Dann gilt $y \sim x$ und $z \sim x$. Aus $z \sim x$ folgt $x \sim z$ wegen der Symmetrie von $\sim$, also auch $y \sim z$ wegen der Transitivität von $\sim$.

Eindeutigkeit. Seien N_1, N_2 Äquivalenzklassen mit $x \in N_1$ und $x \in N_2$. Zu zeigen ist $N_1 = N_2$; aus Symmetriegründen genügt $N_1 \subseteq N_2$. Sei also $z \in N_1$. Zu zeigen ist $z \in N_2$. Wegen $z, x \in N_1$ folgt $z \sim x$ nach (2.2) für N_1, also auch $z \in N_2$ nach (2.1) für N_2. □

Aus dem Eindeutigkeitsteil dieser Aussage folgt, daß je zwei verschiedene Äquivalenzklassen disjunkt sind, d.h., daß aus $N_1 \neq N_2$ folgt $N_1 \cap N_2 = \emptyset$.

Eine Äquivalenzrelation auf M zerlegt also die „Trägermenge“ M vollständig in paarweise disjunkte Äquivalenzklassen.

DEFINITION. Seien $M, \sim$ und $M', \sim'$ Mengen von Objekten der Typen ρ bzw. ρ', jeweils gegeben mit einer Äquivalenzrelation. Eine Funktion $f\colon \rho \to \rho'$ heißt (mit $\sim$, $\sim'$ verträgliche) Abbildung von $M, \sim$ in $M', \sim'$, wenn gilt

$$\forall_{x\in M}\, f(x) \in M',$$
$$\forall_{x,y\in M}\big(x \sim y \to f(x) \sim' f(y)\big).$$

DEFINITION. Sei f eine Abbildung von $M, \sim$ in $M', \sim'$. f heißt (als Abbildung von $M, \sim$ in $M', \sim'$)

(a) *injektiv*, wenn gilt

$$\forall_{x,y\in M}\big(f(x) \sim' f(y) \to x \sim y\big);$$

(b) *surjektiv*, wenn gilt

$$\forall_{z\in M}\exists_{x\in M} f(x) \sim' z;$$

(c) *bijektiv*, wenn f injektiv und surjektiv ist.

Wir nennen f *schwach* surjektiv (bijektiv), wenn anstelle von $\exists$ der schwache Existenzquantor $\tilde{\exists}$ verwendet wurde.

2.4.4. Mathematische Strukturen, Isomorphie. Eine *mathematische Struktur* besteht aus einer Menge M von Objekten eines Typs ρ, einer Äquivalenzrelation $\sim$ auf M, endlich vielen (eventuell mehrstelligen) mit $\sim$ verträglichen Abbildungen auf M, sowie endlich vielen (eventuell mehrstelligen) mit $\sim$ verträglichen Relationen auf M.

Dabei heißt eine Funktion f vom Typ $\rho \to \ldots \rho \to \rho$ mit $\sim$ *verträgliche* Abbildung auf M, wenn

$$\forall_{x_1,\ldots,x_n\in M}\, f(x_1,\ldots,x_n) \in M,$$
$$\forall_{x_1,\ldots,x_n,y_1,\ldots,y_n\in M}\big(x_1{\sim}y_1 \to \ldots x_n{\sim}y_n \to f(x_1,\ldots,x_n) \sim' f(y_1,\ldots,y_n)\big).$$

Ferner heißt eine Relation R auf M mit $\sim$ *verträglich*, wenn gilt

$$\forall_{x_1,\ldots,x_n,y_1,\ldots,y_n\in M}\big(x_1{\sim}y_1 \to \ldots x_n{\sim}y_n \to R(x_1,\ldots,x_n) \to R(y_1,\ldots,y_n)\big).$$

Zwei gegebene mathematische Strukturen $\langle M, \sim, f_1, \ldots, f_k, R_1, \ldots, R_l\rangle$ und $\langle M', \sim', f'_1, \ldots, f'_k, R'_1, \ldots, R'_l\rangle$ heißen *isomorph*, wenn es eine bijektive Abbildung g von $M, \sim$ auf $M', \sim'$ gibt mit

$$\forall_{x_1,\ldots,x_n\in M}\, g(f_i(x_1,\ldots,x_n)) \sim' f'_i(g(x_1),\ldots,g(x_n)),$$
$$\forall_{x_1,\ldots,x_n\in M}\big(R_j(x_1,\ldots,x_n)) \leftrightarrow R'_j(g(x_1),\ldots,g(x_n)\big).$$

2.5. Beweise

Zur Darstellung von Beweisen verwenden wir Gerhard Gentzens System des natürlichen Schließens, von (1934). Der wesentliche Grund für diese Wahl ist, daß man auf diese Weise – wie schon der Name sagt – einen *natürlichen* Begriff formaler Beweise erhält. Dies bedeutet, daß die Art, in der formale Beweise dargestellt sind, genau dem entspricht, was ein sorgfältig vorgehender Mathematiker tut, wenn er alle Einzelheiten eines Beweises aufschreibt.

Wir beginnen mit einigen Beispielen. Der Einfachheit halber betrachten wir Beweise in der reinen Logik, d.h., ohne Annahmen über Funktionen und Prädikate.

2.5.1. Beispiel für natürliche Beweise.

$$(A \to B \to C) \to (A \to B) \to A \to C. \tag{2.3}$$

Gelte $A \to B \to C$. Zu zeigen: $(A \to B) \to A \to C$. Gelte also $A \to B$. Zu zeigen: $A \to C$. Gelte also A. Zu zeigen: C. Wir haben A, nach der letzten Annahme. Also auch $B \to C$, nach der ersten Annahme, und B, nach der vorletzten Annahme. Aus $B \to C$ und B erhalten wir C, wie behauptet. □

$$\forall_x(A \to B) \to A \to \forall_x B, \quad \text{falls } x \notin \mathrm{FV}(A). \tag{2.4}$$

Gelte $\forall_x(A \to B)$. Zu zeigen: $A \to \forall_x B$. Gelte also A. Zu zeigen: $\forall_x B$. Sei x beliebig; man beachte, daß wir bisher keine Annahmen über x gemacht haben. Zu zeigen: B. Wir haben $A \to B$, nach der ersten Annahme. Also auch B, nach der zweiten Annahme. □

$$(A \to \forall_x B) \to \forall_x(A \to B), \quad \text{falls } x \notin \mathrm{FV}(A). \tag{2.5}$$

Gelte $A \to \forall_x B$. Zu zeigen: $\forall_x(A \to B)$. Sei x beliebig; man beachte, daß wir bisher keine Annahmen über x gemacht haben. Zu zeigen: $A \to B$. Gelte also A. Zu zeigen: B. Wir haben $\forall_x B$, nach der ersten und zweiten Annahme. Also auch B. □

Ein Charakteristikum dieser Beweise ist es, daß Annahmen eingeführt und wieder beseitigt werden: Zu jedem Zeitpunkt im Beweis kennt man die jetzt freien Annahmen.

Wir reservieren das Wort *Beweis* für die Meta–Stufe; eine formale Darstellung eines Beweises nennen wir *Herleitung* oder *Ableitung*.

Eine anschauliche Art, Herleitungen zu definieren, besteht darin, sie als beschriftete Bäume aufzufassen. Die Beschriftungen der inneren Knoten sind Formeln, die der Blätter sind Formeln oder Terme. Die Beschriftungen der Nachfolger eines Knotens ν sind die *Prämissen* einer Regelanwendung, die Formel am Konten ν ist ihre *Konklusion*. An der Wurzel des Baums befindet sich die Konklusion der gesamten Herleitung. Im natürlichen Schließen

arbeitet man mit *Annahmen*, die an Blättern des Baums stehen; sie können offen oder geschlossen (man sagt auch: *gestrichen*) sein.

Jede dieser Annahmen ist mit einer *Marke* versehen. Als Marken verwenden wir *Annahmenvariablen* $\Box_0, \Box_1, \ldots$; Mitteilungszeichen für Annahmenvariablen sind u, v, w. Die (bisherigen) Variablen nennen wir oft auch *Objektvariablen*, um sie von den Annahmenvariablen zu unterscheiden. Wenn an einer späteren Stellen (d.h. an einem Knoten im Baum unterhalb dieser Annahme) die Abhängigkeit von dieser Annahme beseitigt wird, notieren wir dies durch Angabe der Annahmenvariablen. Da wir dieselbe Annahme auch mehrfach verwenden können, darf in einem Baum eine mit u markierte Annahme A (mitgeteilt durch $u\colon A$) auch mehrfach vorkommen. Wir verlangen jedoch, daß verschiedene Annahmeformeln stets verschiedene Marken bekommen.

Einen inneren Knoten im Baum verstanden wir als Resultat eines Übergangs von *Prämissen* zu einer *Konklusion*. Die zulässigen Übergänge werden durch die *Regeln* bestimmt. Die Beschriftung des Knotens enthält dann neben der Konklusion noch den Namen der verwendeten Regel. In manchen Fällen bindet eine Regel eine Annahmenvariable u (und beseitigt damit die Abhängigkeit von allen darüber stehenden, mit u markierten Annahmen $u\colon A$) oder eine Objektvariable x (und beseitigt damit die Abhängigkeit von x). Dann wird die abgebundene Annahmen– oder Objektvariable der Beschriftung hinzugefügt.

2.5.2. Einführungs- und Beseitigungsregeln für $\to$ und $\forall$. Wir formulieren jetzt die Regeln des natürlichen Schließens. Zunächst haben wir eine Annahmenregel, die es erlaubt, eine beliebige Formel A anzunehmen, zusammen mit einer Marke u:

$$u\colon A \quad \text{Annahme}$$

Die restlichen Regeln des natürlichen Schließens gliedern sich in Einführungs- und Beseitigungsregeln für die Verknüpfungen $\to$ und $\forall$. Für die Implikation $\to$ gibt es also eine Einführungsregel $\to^+ u$ und eine Beseitigungsregel $\to^-$, die auch *modus ponens* genannt wird. Die linke Prämisse $A \to B$ in $\to^-$ heißt *Hauptprämisse*, und die rechte Prämisse A *Nebenprämisse*. Man beachte, daß bei Anwendung der $\to^+ u$-Regel *alle* darüberstehenden mit $u\colon A$ markierten Annahmen gestrichen werden. Für den Allquantor $\forall$ gibt es eine Einführungsregel $\forall^+ x$ und eine Beseitigungsregeln $\forall^-$, deren rechte Prämisse der zu substituierende Term r ist. Die Regel $\forall^+ x$ unterliegt der folgenden *Variablenbedingung*: Die Herleitung M der Prämisse A darf keine offenen Annahmen enthalten, in denen x frei vorkommt.

$$\frac{\begin{array}{c}[u\colon A]\\ \mid M\\ B\end{array}}{A \to B}\,{\to}^{+}u \qquad \frac{\begin{array}{cc}\mid M & \mid N\\ A \to B & A\end{array}}{B}\,{\to}^{-}$$

Abbildung 1. Einführungs- und Beseitigungsregeln für $\to$

$$\frac{\begin{array}{c}\mid M\\ A\end{array}}{\forall_x A}\,\forall^{+}x \qquad \frac{\begin{array}{cc}\mid M & \\ \forall_x A(x) & r\end{array}}{A(r)}\,\forall^{-}$$

Abbildung 2. Einführungs- und Beseitigungsregeln für $\forall$

Wir geben jetzt Herleitungen für die Beispielsformeln (2.3) – (2.5) an. Da die verwendete Regel oft durch die jeweilige Formel bestimmt ist, lassen wir in solchen Fällen den Namen der Regel weg.

(2.3):

$$\dfrac{\dfrac{\dfrac{\dfrac{u\colon A \to B \to C \qquad w\colon A}{B \to C} \qquad \dfrac{v\colon A \to B \qquad w\colon A}{B}}{C}}{A \to C}\,{\to}^{+}w}{(A \to B) \to A \to C}\,{\to}^{+}v}{(A \to B \to C) \to (A \to B) \to A \to C}\,{\to}^{+}u$$

(2.4):

$$\dfrac{\dfrac{\dfrac{\dfrac{u\colon \forall_x(A \to B) \qquad x}{A \to B} \qquad v\colon A}{B}}{\forall_x B}\,\forall^{+}x}{A \to \forall_x B}\,{\to}^{+}v}{\forall_x(A \to B) \to A \to \forall_x B}\,{\to}^{+}u$$

Man beachte, daß hier die Variablenbedingung erfüllt ist: x ist nicht frei in A (und auch nicht frei in $\forall_x(A \to B)$).

(2.5):

$$\dfrac{\dfrac{\dfrac{\dfrac{u\colon A \to \forall_x B \qquad v\colon A}{\forall_x B} \qquad x}{B}}{A \to B}\,{\to}^{+}v}{\forall_x(A \to B)}\,\forall^{+}x}{(A \to \forall_x B) \to \forall_x(A \to B)}\,{\to}^{+}u$$

Auch hier ist die Variablenbedingung erfüllt: x ist nicht frei in A.

2.5.3. Regeln für $\wedge$, $\vee$ und $\exists$. Es ist meist bequemer, anstelle der oben angegebenen Einführungs- und Beseitigungsaxiome für $\wedge$, $\vee$ und $\exists$ die folgenden „zulässigen“ Regeln zu verwenden

Konjunktion. Die Einführungsregel ist

$$\frac{\begin{array}{cc} \mid M & \mid N \\ A & B \end{array}}{A \wedge B}\,\wedge^+$$

und die Beseitigungsregeln sind

$$\frac{\begin{array}{c} \mid M \\ A \wedge B \end{array}}{A}\,\wedge_0^- \qquad \frac{\begin{array}{c} \mid M \\ A \wedge B \end{array}}{B}\,\wedge_1^-$$

Disjunktion. Die Einführungsregeln sind

$$\frac{\begin{array}{c} \mid M \\ A \end{array}}{A \vee B}\,\vee_0^+ \qquad \frac{\begin{array}{c} \mid M \\ B \end{array}}{A \vee B}\,\vee_1^+$$

und die Beseitigungsregel

$$\frac{\begin{array}{ccc} & [u\colon A] & [v\colon B] \\ \mid M & \mid N & \mid K \\ A \vee B & C & C \end{array}}{C}\,\vee^- u, v$$

Existenzquantor. Die Einführungsregel ist

$$\frac{\begin{array}{cc} & \mid M \\ r & A(r) \end{array}}{\exists_x A(x)}\,\exists^+$$

and die Beseitigungsregel

$$\frac{\begin{array}{cc} & [u\colon A] \\ \mid M & \mid N \\ \exists_x A & B \end{array}}{B}\,\exists^- x, u \text{ (mit Variablenbedingung)}$$

Die Regel $\exists^- x, u$ benötigt die folgende Variablenbedingung: Die Herleitung N darf keine offenen Annahmen außer $u\colon A$ enthalten, in denen x frei vorkommt, und auch in B darf x nicht frei vorkommen.

Es ist leicht zu sehen, daß für die Verknüpfungen $\wedge$, $\vee$, $\exists$ die Regeln und die Axiome äquivalent sind in dem Sinn, daß aus den Axiomen und den Prämissen einer Regel ihre Konklusion hergeleitet werden kann (natürlich

ohne Verwendung der $\wedge, \vee, \exists$-Regeln), und umgekehrt daß man die Axiome aus den Regeln für $\wedge$, $\vee$ und $\exists$ hergeleiten kann. Dies ist eine einfache Übung.

Die linke Prämisse in jeder der Beseitigungsregeln $\vee^-$, $\wedge^-$ und $\exists^-$ heißt *Hauptprämisse*, und jede der rechten Prämissen *Nebenprämisse*.

2.5.4. Herleitbare Eigenschaften der Leibniz Gleichheit. Man beweist leicht Symmetrie, Transitivität und die *Verträglichkeit* von Eq:

LEMMA. $\forall_{x,y}\big(\mathrm{Eq}(x,y) \to A(x) \to A(y)\big)$.

BEWEIS. Wir verwenden das Beseitigungsaxiom für die Leibniz Gleichheit

$$\mathrm{Eq}^- : \forall_x \forall_y \big(\mathrm{Eq}(x,y) \to \forall_z C(z,z) \to C(x,y)\big) =: B$$

mit $C(x,y) := A(x) \to A(y)$. Eine Herleitung ist

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{B \quad x}{\cdots}}{\cdots}\, y \qquad u\colon \mathrm{Eq}(x,y)}{\forall_z(A(z) \to A(z)) \to A(x) \to A(y)} \qquad \dfrac{\dfrac{v\colon A(z)}{A(z) \to A(z)} \to^+ v}{\forall_z(A(z) \to A(z))} \forall^+ z}{A(x) \to A(y)} \to^+ u}{\mathrm{Eq}(x,y) \to A(x) \to A(y)} \forall^+ y}{\forall_y(\mathrm{Eq}(x,y) \to A(x) \to A(y))} \forall^+ x}{\forall_x \forall_y(\mathrm{Eq}(x,y) \to A(x) \to A(y))}$$

Man beachte, daß die Variablenbedingung bei allen Anwendungen von $\forall^+$ erfüllt ist. □

Die Falschheit hatten wir definiert durch $F := \mathrm{Eq}(\mathtt{ff}, \mathtt{tt})$. Wir können jetzt beweisen

SATZ (Ex-Falso-Quodlibet). $F \to A$.

BEWEIS. Wir haben $F \to \mathrm{Eq}(x^\rho, y^\rho)$, denn aus $\mathrm{Eq}(\mathtt{ff}, \mathtt{tt})$ folgt mit dem Verträglichkeitslemma $\mathrm{Eq}[\textbf{if } \mathtt{tt} \textbf{ then } x \textbf{ else } y][\textbf{if } \mathtt{ff} \textbf{ then } x \textbf{ else } y]$, also $\mathrm{Eq}(x^\rho, y^\rho)$.

Die Behauptung erhält man jetzt durch Induktion über die Formel A. Im Fall $I(\vec{s})$ wähle man eine nullstellige Klausel K_i mit Konklusion $I(\vec{t})$. Nach IH kann man aus F alle Prämissen herleiten, also auch $I(\vec{t}\,)$. Aus F ergibt sich $\mathrm{Eq}(s_i, t_i)$, nach der obigen Bemerkung. Deshalb hat man $I(\vec{s})$, wieder nach dem Verträglichkeitslemma.

Die Fälle $A \to B$ und $\forall_x A$ sind einfach zu behandeln, ebenso auch die Fälle $A \wedge B$, $A \vee B$ und $\exists_x A$. □

2.5.5. Stabilität. Eine Formel A heißt *stabil*, wenn für sie das „Prinzip des indirekten Beweisens“ hergeleitet werden kann, also

$$\neg\neg A \to A.$$

In 2.3.4 hatten wir gesehen, wie man mit Hilfe der Leibniz Gleichheit aus einem booleschen Term $r^{\mathbf{B}}$ eine Formel herstellen kann, nämlich als

$$\mathrm{atom}(r^{\mathbf{B}}) := \mathrm{Eq}(r^{\mathbf{B}}, \mathtt{tt}).$$

Mit Hilfe der im nächsten Abschnitt einzuführenden Induktionsaxiome werden wir zeigen können, daß jede Formel der Gestalt $\mathrm{atom}(r^{\mathbf{B}})$ stabil ist, insbesondere also auch jede Gleichung $r =_{\mathbf{N}} s$ und die Falschheit F.

Satz. *Enthält eine Formel A nur stabile Primformeln und verwendet man anstelle von $\vee$ und $\exists$ nur die schwachen Verknüpfungen $\tilde{\vee}$ und $\tilde{\exists}$, so ist A stabil.*

Beweis. Induktion über A. Zur Vereinfachung lassen wir in den konstruierten Herleitungen Anwendungen von $\to^+$ am Ende weg. Für Primformeln gilt die Behauptung nach Annahme. Im Fall einer Implikation $A \to B$ verwendet man $(\neg\neg B \to B) \to \neg\neg(A \to B) \to A \to B$; eine Herleitung ist

$$\dfrac{u\colon \neg\neg B \to B \qquad \dfrac{v\colon \neg\neg(A \to B) \qquad \dfrac{\dfrac{u_1\colon \neg B \qquad \dfrac{u_2\colon A \to B \qquad w\colon A}{B}}{F}\to^+ u_2}{\neg(A \to B)}}{F}\to^+ u_1}{\neg\neg B}}{B}$$

Im Fall $\forall_x A$ genügt $(\neg\neg A \to A) \to \neg\neg\forall_x A \to A$; eine Herleitung ist

$$\dfrac{u\colon \neg\neg A \to A \qquad \dfrac{v\colon \neg\neg\forall_x A \qquad \dfrac{\dfrac{u_1\colon \neg A \qquad \dfrac{u_2\colon \forall_x A \qquad x}{A}}{F}\to^+ u_2}{\neg\forall_x A}}{F}\to^+ u_1}{\neg\neg A}}{A}$$

Damit ist alles gezeigt. □

Man zeigt leicht, daß für die schwachen Verknüpfungen $\tilde{\vee}$ und $\tilde{\exists}$ fast dieselben Regeln hergeleitet werden können wir für $\vee$ und $\exists$: in den Beseitigungsregeln brauchen wir die Einschränkumg, daß die Konklusion C bzw. B stabil ist.

Daraus ergibt sich insbesondere, daß $\tilde{\vee}$ und $\tilde{\exists}$ tatsächlich schwächer sind als $\vee$ und $\exists$:

$$A \vee B \to A \,\tilde{\vee}\, B, \quad \exists_x A \to \tilde{\exists}_x A.$$

Die Beweise dafür seien dem Leser als Übung überlassen.

2.5.6. Eigenschaften der Negation. Die Negation $\neg A$ hatten wir definiert durch $A \to F$. Einige der im folgenden aufgelisteten Eigenschaften der Negation benötigen des Prinzip des Ex-Falso-Quodlibet; dies wird jeweils mit angegeben.

Für die Negationen unserer Verknüpfungen gilt folgendes.

$$\neg(A \to B) \leftrightarrow \neg\neg A \wedge \neg B \quad (\text{„}\to\text{“ braucht } F \to B),$$
$$\neg(A \wedge B) \leftrightarrow \neg A \,\tilde{\vee}\, \neg B,$$
$$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B,$$
$$\neg\forall_x A \leftrightarrow \tilde{\exists}_x \neg A,$$
$$\neg\exists_x A \leftrightarrow \forall_x \neg A,$$
$$\neg(A \,\tilde{\vee}\, B) \leftrightarrow \neg A \wedge \neg B,$$
$$\neg\tilde{\exists}_x A \leftrightarrow \forall_x \neg A.$$

Für die doppelte Negation hat man

$$A \to \neg\neg A,$$
$$\neg\neg\neg A \leftrightarrow \neg A,$$
$$\neg\neg(A \to B) \leftrightarrow (\neg\neg A \to \neg\neg B) \quad (\text{„}\leftarrow\text{“ braucht } F \to B),$$
$$\neg\neg(A \wedge B) \leftrightarrow \neg\neg A \wedge \neg\neg B,$$
$$\neg\neg\forall_x A \to \forall_x \neg\neg A.$$

Etwa die letzte Behauptung ergibt sich aus

$$\dfrac{u\colon \neg\neg\forall_x A \qquad \dfrac{\dfrac{\dfrac{w\colon \forall_x A \qquad x}{A}}{F}}{\neg\forall_x A}\,{\to}^{+}w}{F}$$

KAPITEL 3

Natürliche Zahlen

Wir verlassen jetzt den Bereich der allgemeinen Logik und beginnen den Aufbau des Zahlensystems mit den natürlichen Zahlen. Ziel dieses Kapitel ist es, das Induktionsprinzip genauer kennenzulernen und mit seiner Hilfe grundlegende Eigenschaften einfacher arithmetischer Funktionen und Relationen zu beweisen. Dabei verwenden wir den allgemeinen Beweisbegriff aus dem vorangehenden Kapitel.

Wir untersuchen natürliche Zahlen sowohl in in Unär- als auch in Binärdarstellung, also als Objekte der Typen $\mathbf{N}$ bzw. $\mathbf{P}$. Es ist bequem, nur die positiven Zahlen als Binärzahlen darzustellen.

3.1. Einfache arithmetische Beweise

3.1.1. Induktion. Beweise über natürliche Zahlen führt man meist durch Induktion. Die Induktionsschemata für einige unserer Basistypen sind

$$\mathrm{Ind}_{b,A}\colon \forall_b\big(A(\mathtt{tt}) \to A(\mathtt{ff}) \to A(b^{\mathbf{B}})\big),$$
$$\mathrm{Ind}_{m,A}\colon \forall_m\big(A(0) \to \forall_n(A(n) \to A(\mathrm{S}n)) \to A(m^{\mathbf{N}})\big),$$
$$\mathrm{Ind}_{q,A}\colon \forall_q\big(A(1) \to \forall_p(A(p) \to A(S_0 p)) \to \forall_p(A(p) \to A(S_1 p)) \to A(q^{\mathbf{P}})\big),$$
$$\mathrm{Ind}_{l,A}\colon \forall_l\big(A(\mathrm{nil}) \to \forall_{x,l'}(A(l') \to A(x :: l')) \to A(l^{\mathbf{L}(\rho)})\big),$$
$$\mathrm{Ind}_{x,A}\colon \forall_x\big(\forall_{y_1} A(\mathrm{inl}\, y_1) \to \forall_{y_2} A(\mathrm{inr}\, y_2) \to A(x^{\rho_1+\rho_2})\big),$$
$$\mathrm{Ind}_{x,A}\colon \forall_x\big(\forall_{y^\rho,z^\sigma} A(\langle y,z\rangle) \to A(x^{\rho\times\sigma})\big),$$

wobei $x :: l$ steht für $\mathrm{cons}\, x\, l$ und $\langle y,z\rangle$ für $\times^+ yz$.

3.1.2. Stabilität von atomaren Formeln.

Lemma. $\neg\neg\mathrm{atom}(b) \to \mathrm{atom}(b)$.

Beweis. Wir führen den Beweis durch boolesche Induktion. Es genügt deshalb, die Behauptung für $\mathtt{tt}$ und für $\mathtt{ff}$ zu zeigen.

Fall $\mathtt{tt}$. Zu zeigen ist $\neg\neg\mathrm{atom}(\mathtt{tt}) \to \mathrm{atom}(\mathtt{tt})$. Es genügt, $\mathrm{atom}(\mathtt{tt})$ zu beweisen. Es war $\mathrm{atom}(b) := \mathrm{Eq}(b,\mathtt{tt})$. Die Behauptung folgt aus der Reflexivität von Eq, also dem Axiom Eq^+.

Fall $\mathtt{ff}$. Zu zeigen ist $\neg\neg\mathrm{atom}(\mathtt{ff}) \to \mathrm{atom}(\mathtt{ff})$. Wir hatten $\neg A$ definiert durch $A \to F$, und F als $\mathrm{atom}(\mathtt{ff})$. Zu zeigen ist also $\neg\neg\mathrm{atom}(\mathtt{ff}) \to \mathrm{atom}(\mathtt{ff})$, das heißt, $((F \to F) \to F) \to F$. Da $F \to F$ offenbar gilt, folgt die Behauptung. □

Diesem Beweis entspricht die folgende Herleitung. Wir verwenden als Abkürzung $A(b) := \neg\neg\mathrm{Eq}(b,\mathtt{tt}) \to \mathrm{Eq}(b,\mathtt{tt})$.

$$\dfrac{\dfrac{\dfrac{\mathrm{Ind}_{b,A}\colon \forall_b\big(A(\mathtt{tt}) \to A(\mathtt{ff}) \to A(b)\big) \qquad b}{A(\mathtt{tt}) \to A(\mathtt{ff}) \to A(b)} \qquad \begin{array}{l} \\ \mid M_{\mathtt{tt}} \end{array}}{A(\mathtt{ff}) \to A(b)} \qquad \begin{array}{l} A(\mathtt{tt}) \\ \\ \end{array}}{A(b)} \qquad \begin{array}{l} \\ \\ \mid M_{\mathtt{ff}} \end{array} \qquad \begin{array}{l} \\ \\ A(\mathtt{ff}) \end{array}$$

mit

$$M_{\mathtt{tt}} := \dfrac{\dfrac{\mathrm{Eq}^+\colon \forall_b \mathrm{Eq}(b,b) \qquad \mathtt{tt}}{\mathrm{Eq}(\mathtt{tt},\mathtt{tt})}}{\neg\neg\mathrm{Eq}(\mathtt{tt},\mathtt{tt}) \to \mathrm{Eq}(\mathtt{tt},\mathtt{tt})}$$

$$M_{\mathtt{ff}} := \dfrac{\dfrac{u\colon (F \to F) \to F \qquad \dfrac{v\colon F}{F \to F}\to^+ v}{F}}{((F \to F) \to F) \to F} \to^+ u$$

Wegen $F := \mathrm{Eq}(\mathtt{ff},\mathtt{tt})$ ist $A(\mathtt{ff})$ die Endformel von $M_{\mathtt{ff}}$.

3.1.3. Leibniz Gleichheit auf N. In 2.2.3 hatten wir die Gleichheit $=_{\mathbf{N}}$ als booleschwertige Funktion vom Typ $\mathbf{N} \to \mathbf{N} \to \mathbf{B}$ definiert, mit den Berechnungsregeln

$$(0 =_{\mathbf{N}} 0) := \mathtt{tt}, \quad (\mathrm{S}n =_{\mathbf{N}} 0) := \mathtt{ff},$$
$$(0 =_{\mathbf{N}} \mathrm{S}m) := \mathtt{ff}, \quad (\mathrm{S}n =_{\mathbf{N}} \mathrm{S}m) := (n =_{\mathbf{N}} m).$$

Wir zeigen jetzt, daß die so definierte Gleichheit mit der Leibniz Gleichheit für den Typ $\mathbf{N}$ übereinstimmt.

Lemma (Reflexivität von $=_{\mathbf{N}}$). $n =_{\mathbf{N}} n$.

Beweis. Induktion nach n. *Basis.* Zu zeigen ist $0 =_{\mathbf{N}} 0$. Nach Definition von $=_{\mathbf{N}}$ ist dies dasselbe wie $\mathtt{tt}$, und da $\mathrm{atom}(\mathtt{tt})$ definiert ist als $\mathrm{Eq}(\mathtt{tt},\mathtt{tt})$, können wir es aus Eq^+ herleiten. *Schritt* $n \mapsto \mathrm{S}n$: Nach IH (Induktionshypothese) haben wir $n =_{\mathbf{N}} n$. Zu zeigen ist $\mathrm{S}n =_{\mathbf{N}} \mathrm{S}n$. Nach Definition von $=_{\mathbf{N}}$ ist dies dasselbe wie die IH $n =_{\mathbf{N}} n$. □

Die zugehörige Herleitung besteht aus sechs Regelanwendungen und verwendet die Axiome $\mathrm{Ind}_{m,A}$ und Eq^+:

$$\dfrac{\dfrac{\dfrac{\mathrm{Ind}_{m,A}\colon \ldots \qquad m}{A(0)\to\forall_n(A(n)\to A(\mathrm{S}n))\to A(m)} \qquad \begin{array}{c}\mid M_0\\ A(0)\end{array}}{\forall_n(A(n)\to A(\mathrm{S}n))\to A(m)} \qquad \begin{array}{c}\mid M_{\mathrm{S}}\\ \forall_n(A(n)\to A(\mathrm{S}n))\end{array}}{A(m)}$$

mit $A(n) := (n = n)$ und

$$M_0 := \dfrac{\mathrm{Eq}^+\colon \forall_b \mathrm{Eq}(b,b) \qquad \mathtt{tt}}{\mathrm{Eq}(\mathtt{tt},\mathtt{tt})}, \quad M_{\mathrm{S}} := \dfrac{\dfrac{\begin{array}{c}u\colon n=n\\ \hline n=n\to \mathrm{S}n=\mathrm{S}n\end{array}\to^+ u}{\forall_n(n=n\to \mathrm{S}n=\mathrm{S}n)}$$

Lemma. $\mathrm{Eq}(n,m)\to n =_{\mathbf{N}} m$.

Beweis. Man verwendet $\mathrm{Eq}^-\colon \mathrm{Eq}(n,m)\to\forall_n n =_{\mathbf{N}} n\to n =_{\mathbf{N}} m$ und die Reflexivität von $=_{\mathbf{N}}$. □

Den Beweis der anderen Richtung führen wir wieder durch Induktion. Das Induktionsschema wird hier u.a. in einer Form angewandt, in der die IH nicht benutzt wird; wir nennen es dann *Fallunterscheidung*. Beispiele sind

$$\begin{aligned}
&\mathrm{Cases}_{m,A}\colon \forall_m\big(A(0)\to\forall_n A(\mathrm{S}n)\to A(m^{\mathbf{N}})\big),\\
&\mathrm{Cases}_{q,A}\colon \forall_q\big(A(1)\to\forall_p A(S_0 p)\to\forall_p A(S_1 p)\to A(q^{\mathbf{P}})\big),\\
&\mathrm{Cases}_{l,A}\colon \forall_l\big(A(\mathrm{nil})\to\forall_{x,l'} A(x::l')\to A(l^{\mathbf{L}(\rho)})\big).
\end{aligned}$$

Lemma. $n =_{\mathbf{N}} m\to\mathrm{Eq}(n,m)$.

Beweis. Induktion nach n. Wir schreiben $n = m$ für $n =_{\mathbf{N}} m$. *Basis.* Zu zeigen ist $\forall_m(n = m\to\mathrm{Eq}(n,m))$. Dies beweisen wir durch Fallunterscheidung nach m. *Fall* 0. Zu zeigen ist $0 = 0\to\mathrm{Eq}(0,0)$. Dies folgt aus Eq^+. *Fall* Sm. Zu zeigen ist $0 = \mathrm{S}m\to\mathrm{Eq}(0,\mathrm{S}m)$. Nun ist $0 = \mathrm{S}m$ dasselbe wie $\mathtt{ff}$, also die Behauptung eine Instanz von Ex-Falso-Quodlibet.

Schritt $n\mapsto \mathrm{S}n$: Nach IH haben wir $\forall_m(n = m\to\mathrm{Eq}(n,m))$. Zu zeigen ist $\forall_m(\mathrm{S}n = m\to\mathrm{Eq}(\mathrm{S}n,m))$. Dies beweisen wir wieder durch Fallunterscheidung nach m. *Fall* 0. Zu zeigen ist $\mathrm{S}n = 0\to\mathrm{Eq}(\mathrm{S}n,0)$, was wieder eine Instanz von Ex-Falso-Quodlibet ist. *Fall* Sm. Zu zeigen ist $\mathrm{S}n = \mathrm{S}m\to\mathrm{Eq}(\mathrm{S}n,\mathrm{S}m)$. Gelte also $\mathrm{S}n = \mathrm{S}m$. Nach Definition von $=_{\mathbf{N}}$ ist dies dasselbe wie $n = m$. Nach der IH folgt $\mathrm{Eq}(n,m)$. Aus $\mathrm{Eq}(\mathrm{S}n,\mathrm{S}n)$ und dem Verträglichkeitslemma folgt $\mathrm{Eq}(\mathrm{S}n,\mathrm{S}m)$. □

3.1.4. Ersetzungsregeln für Addition und Multiplikation. Die arithmetischen Funktionen + und · hatten wir bereits in 2.2.2 durch ihre

Berechnungsregeln definiert:

$$n + 0 := n, \quad n + \mathrm{S}m := \mathrm{S}(n + m),$$
$$n \cdot 0 := 0, \quad n \cdot \mathrm{S}m := (n \cdot m) + n.$$

Wir beweisen jetzt einige einfache Eigenschaften dieser Funktionen, und zwar durch geeignete Induktionen. In vielen Fällen sind diese Eigenschaften Gleichungen zwischen Termen. Wir nennen solche Gleichungen *Ersetzungsregeln*, wenn wir sie im Folgenden stillschweigend zur Vereinfachung von Termen verwenden (in der Richtung von links nach rechts).

(3.1) $$0 + n = n \quad \text{(Ersetzungsregel).}$$

Beweis. Induktion nach n. *Basis.* Zu zeigen ist $0 + 0 = 0$. Nach Definition von $+$ ist dies dasselbe wie $0 = 0$. Dies folgt aus der Reflexivität von $=_{\mathbf{N}}$. *Schritt* $n \mapsto \mathrm{S}n$: Nach IH haben wir $0 + n = n$. Zu zeigen ist $0 + \mathrm{S}n = \mathrm{S}n$. Nach Definition von $+$ ist dies dasselbe wie $\mathrm{S}(0 + n) = \mathrm{S}n$, also nach Definition von $=_{\mathbf{N}}$ dasselbe wie $0 + n = n$. Dies ist aber die IH. □

Die zugehörige Herleitung besteht aus denselben Regelanwendungen und Axiomen wie oben, nur die Formeln sind anders, und zwar hier $A(n) := (0 + n = n)$. Man hat dann

$$M_{\mathrm{S}} := \dfrac{\dfrac{u\colon 0 + n = n}{0 + n = n \to 0 + \mathrm{S}n = \mathrm{S}n} \to^{+} u}{\forall_n(0 + n = n \to 0 + \mathrm{S}n = \mathrm{S}n)}$$

Das Entsprechende gilt für (3.2), (3.3) und (3.4).

(3.2) $$\mathrm{S}n + m = \mathrm{S}(n + m) \quad \text{(Ersetzungsregel).}$$

Beweis. Wir fixieren n und führen den Beweis durch Induktion nach m. *Basis.* $\mathrm{S}n + 0 = \mathrm{S}(n + 0)$ ist nach Definition von $+$ dasselbe wie $\mathrm{S}n = \mathrm{S}n$. Dies folgt wieder aus der Reflexivität von $=_{\mathbf{N}}$. *Schritt* $m \mapsto \mathrm{S}m$: Nach IH haben wir $\mathrm{S}n + m = \mathrm{S}(n + m)$. Zu zeigen ist $\mathrm{S}n + \mathrm{S}m = \mathrm{S}(n + \mathrm{S}m)$. Nach Definition von $+$ ist dies dasselbe wie $\mathrm{S}(\mathrm{S}n + m) = \mathrm{S}(\mathrm{S}(n + m))$, also nach Definition von $=_{\mathbf{N}}$ dasselbe wie $\mathrm{S}n + m = \mathrm{S}(n + m)$. Dies ist die IH. □

Jetzt können wir die Kommutativität der Addition beweisen. Diese Gleichung läßt sich nicht als (stets anzuwendende) Ersetzungsregel verwenden, da ihre Anwendung nicht terminieren würde.

(3.3) $$n + m = m + n$$

BEWEIS. Wir fixieren n und führen den Beweis durch Induktion nach n. *Basis.* Zu zeigen ist $0 + m = m + 0$. Wegen (3.1) und der Definition von $+$ folgt dies aus der Reflexivität von $=_{\mathbf{N}}$. *Schritt* $n \mapsto \mathrm{S}n$: Nach IH haben wir $n+m = m+n$. Zu zeigen ist $\mathrm{S}n+m = m+\mathrm{S}n$. Nach (3.2) und der Definition von $+$ ist dies dasselbe wie $\mathrm{S}(n + m) = \mathrm{S}(m + n)$, also nach Definition von $=_{\mathbf{N}}$ dasselbe wie die IH. □

Wir beweisen die Assoziativität der Addition:

$$n + (m + k) = (n + m) + k \quad \text{(Ersetzungsregel).} \tag{3.4}$$

BEWEIS. Wir fixieren n, m und führen den Beweis durch Induktion nach k. *Basis.* $n+(m+0) = (n+m)+0$ gilt nach Definition von $+$. *Schritt* $k \mapsto \mathrm{S}k$. Nach IH haben wir $n+(m+k) = (n+m)+k$. Zu zeigen ist $n+(m+\mathrm{S}k) = (n+m) + \mathrm{S}k$. Nach dreimaliger Anwendung der Ersetzungsregel (3.2) (zweimal links und einmal rechts) ist dies dasselbe wie $\mathrm{S}(n+(m+k)) = \mathrm{S}((n+m)+k)$, also nach Definition von $=_{\mathbf{N}}$ dasselbe wie die IH. □

LEMMA (Kürzungsregel für $+$). $n + k = m + k \to n = m$.

Man zeigt dies durch Induktion nach k. Der Beweis ist eine einfache Übung.

Entsprechend erhält man für die Multiplikation

$$0 \cdot m = 0 \quad \text{(Ersetzungsregel),} \tag{3.5}$$

$$\mathrm{S}n \cdot m = (n \cdot m) + m \quad \text{(Ersetzungsregel).} \tag{3.6}$$

Der Beweis ist eine einfache Übung. — Im folgenden schreiben wir wie üblich nm für $n \cdot m$. Ferner vereinbaren wir, daß $\cdot$ stärker bindet als $+$.

$$n(m + k) = nm + nk \quad \text{(Ersetzungsregel).} \tag{3.7}$$

BEWEIS. Wir fixieren n, m und führen den Beweis durch Induktion nach k. *Basis.* Die Behauptung $n(m+0) = nm+n0$ ist nach Definition von $+$ und $\cdot$ dasselbe wie $nm = nm$. *Schritt* $k \mapsto \mathrm{S}k$: Nach IH haben wir $n(m + k) = nm + nk$. Zu zeigen ist $n(m + \mathrm{S}k) = nm + n\mathrm{S}k$. Die linke Seite ist nach Definition von $+$ und $\cdot$ dasselbe wie $n(m + k) + n$. Die rechte Seite ist nach Definition von $\cdot$ dasselbe wie $nm + (nk + n)$, also wegen des Assoziativität der Addition dasselbe wie $(nm + nk) + n$. Da $=_{\mathbf{N}}$ und $\mathrm{Eq}_{\mathbf{N}}$ äquivalent sind, folgt dies aus der IH mit dem Verträglichkeitslemma. □

Wir zeigen jetzt die Kommutativität der Multiplikation.

$$nm = mn. \tag{3.8}$$

BEWEIS. Wir fixieren n und führen den Beweis durch Induktion nach m. *Basis.* Die Behauptung $n0 = 0n$ ist nach Definition von $\cdot$ und (3.5) dasselbe wie $0 = 0$. *Schritt* $m \mapsto \mathrm{S}m$: Nach IH haben wir $nm = mn$. Zu zeigen ist $n\mathrm{S}m = (\mathrm{S}m)n$. Die linke Seite ist nach Definition von $\cdot$ dasselbe wie $nm+n$. Die rechte Seite ist nach (3.6) dasselbe wie $mn+n$. Da $=_{\mathbf{N}}$ und $\mathrm{Eq}_{\mathbf{N}}$ äquivalent sind, folgt dies aus der IH mit dem Verträglichkeitslemma. □

Als unmittelbare Folgerung ergibt sich

$$(n + m)k = nk + mk \quad \text{(Ersetzungsregel)}. \tag{3.9}$$

Schließlich beweisen wir noch die Assoziativität der Multiplikation:

$$n(mk) = (nm)k \quad \text{(Ersetzungsregel)}. \tag{3.10}$$

BEWEIS. Wir fixieren n, m und führen den Beweis durch Induktion nach k. *Basis.* $n(m0) = (nm)0$ ist nach Definition von $\cdot$ dasselbe wie $0 = 0$. *Schritt* $k \mapsto \mathrm{S}k$. Nach IH haben wir $n(mk) = (nm)k$. Zu zeigen ist $n(m \cdot \mathrm{S}k) = (nm) \cdot \mathrm{S}k$. Die linke Seite ist nach Definition von $\cdot$ dasselbe wie $n(mk + m)$, also nach (3.7) dasselbe wie $n(mk)+nm$. Die rechte Seite ist nach Definition von $\cdot$ dasselbe wie $(nm)k + nm$. Da $=_{\mathbf{N}}$ und $\mathrm{Eq}_{\mathbf{N}}$ äquivalent sind, folgt dies aus der IH mit dem Verträglichkeitslemma. □

3.1.5. Weitere arithmetische Relationen und Funktionen. Wir hatten in 2.2.3 die booleschwertige Funktion $<$ definiert durch die Berechnungsregeln

$$(n < 0) := \mathsf{ff}, \quad (0 < \mathrm{S}m) := \mathsf{tt}, \quad (\mathrm{S}n < \mathrm{S}m) := (n < m).$$

Wir fügen noch hinzu

$$(0 \leq m) := \mathsf{tt}, \quad (\mathrm{S}n \leq 0) := \mathsf{ff}, \quad (\mathrm{S}n \leq \mathrm{S}m) := (n \leq m).$$

Die folgenden Eigenschaften lassen sich wie im vorangehenden Abschnitt leicht durch geeignete Induktionen beweisen:

$$(n < \mathrm{S}n) = \mathsf{tt} \quad \text{(Ersetzungsregel)}, \tag{3.11}$$

$$(n < n) = \mathsf{ff} \quad \text{(Ersetzungsregel)}, \tag{3.12}$$

$$(n \leq n) = \mathsf{tt} \quad \text{(Ersetzungsregel)}, \tag{3.13}$$

$$(\mathrm{S}n \leq n) = \mathsf{ff} \quad \text{(Ersetzungsregel)}. \tag{3.14}$$

Ferner haben wir einige Transitivitätseigenschaften:

$$n < m \to m < k \to n < k, \tag{3.15}$$

$$n \leq m \to m \leq k \to n \leq k, \tag{3.16}$$

$$n < m \to m \leq k \to n < k, \tag{3.17}$$

$$n \leq m \to m < k \to n < k. \tag{3.18}$$

Nützliche Zusammenhänge zwischen $<$, $\leq$ und $=$ sind

$$n < \mathrm{S}m \leftrightarrow n \leq m, \tag{3.19}$$

$$n < m \leftrightarrow \mathrm{S}n \leq m, \tag{3.20}$$

$$(n < m \to F) \leftrightarrow m \leq n, \tag{3.21}$$

$$(n \leq m \to F) \leftrightarrow m < n, \tag{3.22}$$

$$n \leq m \to m \leq n \to n = m. \tag{3.23}$$

Für Fallunterscheidungen verwenden wir

$$n \leq m \to (n < m \to A) \to (n = m \to A) \to A, \tag{3.24}$$

$$(n \leq m \to A) \to (m \leq n \to A) \to A. \tag{3.25}$$

Die Potenz und die Vorgängerfunktion P hatten wir definiert durch die Berechnungsregeln

$$n^0 := 1, \quad n^{\mathrm{S}m} := (n^m) \cdot n,$$
$$\mathrm{P}(0) := 0, \quad \mathrm{P}(\mathrm{S}(n)) := n.$$

Wir ergänzen diese Liste durch die Berechnungsregeln für $n \dot{-} m$ (die „abgeschnittene“ Subtraktion), das Minimum und das Maximum:

$$n \dot{-} 0 := n, \quad n \dot{-} \mathrm{S}m := \mathrm{P}(n \dot{-} m),$$
$$\max(n, 0) := n, \quad \max(0, m) := m, \quad \max(\mathrm{S}n, \mathrm{S}m) := \max(n, m),$$
$$\min(n, 0) := 0, \quad \min(0, m) := 0, \quad \min(\mathrm{S}n, \mathrm{S}m) := \min(n, m).$$

Wieder lassen sich oft verwendete Eigenschaften durch Induktion beweisen. Wir geben einige davon an.

$$\mathrm{P}(\mathrm{S}n \dot{-} m) = n \dot{-} m \quad \text{(Ersetzungsregel)}, \tag{3.26}$$

$$n \dot{-} n = 0 \quad \text{(Ersetzungsregel)}, \tag{3.27}$$

$$\mathrm{S}n \dot{-} n = 1 \quad \text{(Ersetzungsregel)}, \tag{3.28}$$

$$\max(n, n) = n \quad \text{(Ersetzungsregel)}, \tag{3.29}$$

$$\max(n, \max(m, k)) = \max(\max(n, m), k) \quad \text{(Ersetzungsregel)}, \tag{3.30}$$

$$\max(n, m) = \max(m, n), \tag{3.31}$$

$$n \leq \max(n, m), \tag{3.32}$$

$$m \leq \max(n, m), \tag{3.33}$$

$$n \leq k \to m \leq k \to \max(n, m) \leq k \tag{3.34}$$

und entsprechend für das Minimum.

Schließlich formulieren wir noch Monotonieeigenschaften von Addition und Multiplikation:

$$n < m \to n + k < m + k, \tag{3.35}$$

$$n \leq m \to n + k \leq m + k, \tag{3.36}$$

$$n < m \to n \cdot \mathrm{S}k < m \cdot \mathrm{S}k, \tag{3.37}$$

$$n \leq m \to nk \leq mk. \tag{3.38}$$

Auch dies ist leicht durch Induktion (nach k) zu beweisen.

3.2. Teilbarkeit

3.2.1. Division mit Rest. Wir zeigen, daß sich jede natürliche Zahl durch eine gegebene positive Zahl m mit einem Rest $r < m$ dividieren läßt.

SATZ. *Seien natürliche Zahlen n, m gegeben mit $0 < m$. Dann gibt es eindeutig bestimmte natürliche Zahlen q, r mit*

$$n = mq + r \quad \textit{und} \quad r < m.$$

BEWEIS. *Existenz.* Induktion nach n. *Basis.* Man wähle $q := r := 0$. Die Behauptung $0 = m0 + 0$ ist nach den Definitionen von $+$ und $\cdot$ dasselbe wie $0 = 0$, und die Behauptung $0 < m$ gilt nach Voraussetzung. *Schritt* $n \mapsto \mathrm{S}n$. Nach IH haben wir q, r mit $n = mq + r$ und $r < m$. Aus (3.20) folgt $\mathrm{S}r \leq m$. Wir verwenden jetzt eine Fallunterscheidung gemäß (3.24).

Fall $\mathrm{S}r < m$. Setze $q' := q$ und $r' := \mathrm{S}r$. Zu zeigen ist $\mathrm{S}n = mq + \mathrm{S}r$ und $\mathrm{S}r < m$. Die zweite Behauptung ist die Fallunterscheidungsannahme, und die erste ist nach den Definitionen von $+$ und $=_{\mathbf{N}}$ dasselbe wie die IH.

Fall $\mathrm{S}r = m$. Setze $q' := \mathrm{S}q$ und $r' := 0$. Zu zeigen ist $\mathrm{S}n = m \cdot \mathrm{S}q + 0$ und $0 < m$. Die zweite Behauptung gilt nach Voraussetzung, und die erste ist dasselbe wie $\mathrm{S}n = mq + m$. Wegen $\mathrm{S}r = m$ folgt dies aus $\mathrm{S}n = mq + \mathrm{S}r$, was nach den Definitionen von $+$ und $=_{\mathbf{N}}$ dasselbe ist wie die IH.

Eindeutigkeit. Sei wieder $0 < m$. Aus den Annahmen $mq + r = mq' + r'$ und $r, r' < m$ wollen wir zunächst $q = q'$ beweisen. Wegen (3.23) und der Symmetrie der Annahmen genügt $q \leq q'$. Nach (3.21) genügt es, $q' < q \to F$ zu beweisen. Gelte also $q' < q$. Man erhält

$$\begin{aligned} mq' + r' &< mq' + m \quad \text{nach (3.35) und (3.3) wegen } r' < m \\ &= m \cdot \mathrm{S}q' \\ &\leq mq \quad \text{nach (3.20), (3.38) und (3.8) wegen } q' < q \\ &\leq mq + r \quad \text{nach (3.36) und (3.3) wegen } 0 \leq r \end{aligned}$$

und damit einen Widerspruch zur Annahme $mq + r = mq' + r'$.

Aus der Annahme $mq + r = mq' + r'$ erhalten wir $mq + r = mq + r'$ wegen $q = q'$. Jetzt folgt $r = r'$ aus der Kürzungsregel für $+$ und der Kommutativität der Addition. □

3.2.2. Größter gemeinsamer Teiler. Wir definieren die Teilbarkeit $m \mid n$ durch die Formel $\exists_q\, n = mq$.

LEMMA. (a) $n \mid 0$.
(b) $0 \mid n \to n = 0$.
(c) $1 \mid n$.
(d) $n \mid 1 \to n = 1$.
(e) $n \mid n$.
(f) $n \mid m \to m \mid k \to n \mid k$.
(g) $n \mid m \to m \mid n \to n = m$.
(h) $n \mid m \to n \mid mk$.
(i) $n \mid m \to n \mid k \to n \mid m + k$.
(j) $n \mid m \to n \mid m + k \to n \mid k$.

BEWEIS. Die Beweise zu (a) - (c), (e), (f), (h), (i) und (j) sind einfach.

(d). Gelte $n \mid 1$, also $1 = nq$. Es folgt $n \neq 0$. Wegen $n \leq 0 \to n = 0$ (nach (3.23)) folgt $n \leq 0 \to F$, also $0 < n$ nach (3.22), also $1 \leq n$ nach (3.20). Nach (3.23) genügt es, $n \leq 1$ zu zeigen, also nach (3.21) auch $1 < n \to F$. Gelte also $1 < n$. Wegen $1 \leq q$ (Beweis wie eben für n) ist $q = \mathrm{S}(\mathrm{P}q)$, also $q = 1q < nq = 1$ wegen (3.37), also $q < 1$. Damit ergibt sich der gesuchte Widerspruch.

(g). Gelte $n = mq$ und $m = nk$, also $n = nkq$. Zu zeigen ist $n = m$. Wir verwenden eine Fallunterscheidung gemäß (3.24). *Fall* $0 = n$. Dann ist $m = 0$, also $n = m$. *Fall* $0 < n$. Wegen $n = n1 + 0$ und $n = nkq + 0$ folgt $kq = 1$ nach dem Eindeutigkeitsteil des Satzes von der Division mit Rest. Also gilt $k \mid 1$, deshalb $k = 1$ nach (d) und damit wieder $n = m$. □

DEFINITION. Eine natürliche Zahl d heißt *größter gemeinsamer Teiler* von n und m, wenn gilt
(a) $d \mid n$ und $d \mid m$;
(b) $\forall_q(q \mid n \to q \mid m \to q \mid d)$.

Die Eindeutigkeit des größten gemeinsamen Teilers ist eine einfache Folgerung aus dem Teil (g) des Lemmas:

LEMMA. *Sind d_1 und d_2 beide größte gemeinsame Teiler von n und m, so folgt $d_1 = d_2$.*

BEWEIS. Aus der Voraussetzung erhalten wir $d_1 \mid d_2$ und $d_2 \mid d_1$, also nach Teil (g) des Lemmas auch $d_1 = d_2$. □

Offenbar ist 0 größter gemeinsamer Teiler von 0 und 0. Zum Beweis der Existenz in den interessanteren Fällen benötigen wir eine allgemeinere Form der Induktion über natürliche Zahlen, die man oft Wertverlaufsinduktion nennt. Wir wollen sie jetzt einführen.

3.2.3. Wertverlaufsinduktion. Unter dem Schema der allgemeinen Induktion oder der Wertverlaufsinduktion verstehen wir

$$\mathrm{GInd}_{n,A}\colon \forall_n\big(\mathrm{Prog}_n A(n) \to A(n)\big), \tag{3.39}$$

wobei $\mathrm{Prog}_n A(n)$ die „Progressivität“ bezüglich der Ordnung $<$ ausdrückt:

$$\mathrm{Prog}_n A(n) := \forall_n\big(\forall_{m<n} A(m) \to A(n)\big).$$

(3.39) beweisen wir aus dem gewöhnlichen Induktionsschema. Wir fixieren n und nehmen $\mathrm{Prog}_n A(n)$ an. Zu zeigen ist $A(n)$. Wir betrachten die Formel

$$B(n) := \forall_{m<n} A(m) := \forall_m(m < n \to A(m))$$

und beweisen $\forall_n B(n)$ aus $\mathrm{Prog}_n A(n)$ durch gewöhnliche (Null-Nachfolger-) Induktion. Dies genügt, denn aus $B(\mathrm{S}n)$ folgt $A(n)$ wegen $n < \mathrm{S}n$.

Beweis. *Basis.* Zu zeigen ist $\forall_m(m < 0 \to A(m))$. Da $m < 0$ dasselbe ist wie F, folgt dies aus Ex-Falso-Quodlibet.

Schritt $n \mapsto \mathrm{S}n$. Nach IH haben wir $\forall_m(m < n \to A(m))$. Zu zeigen ist $\forall_m(m < \mathrm{S}n \to A(m))$. Sei also m mit $m < \mathrm{S}n$ gegeben. Nach (3.19) ist dies dasselbe wie $m \le n$. Wir beweisen jetzt $A(m)$ durch Fallunterscheidung gemäß (3.24). *Fall* $m < n$. Dann gilt $A(m)$ nach der IH. *Fall* $m = n$. Aus der IH folgt mit der vorausgesetzten Progressivität $A(n)$, also wegen $m = n$ auch $A(m)$. □

Man kann das Schema der allgemeinen Induktion noch weiter verallgemeinern, indem man sich auf eine *Maßfunktion* $\mu\colon \rho \to \mathbf{N}$ bezieht:

$$\mathrm{GInd}^{\mu}_{x,A}\colon \forall_{\mu,x}\big(\mathrm{Prog}^{\mu}_x A(x) \to A(x)\big). \tag{3.40}$$

$\mathrm{Prog}^{\mu}_x A(x)$ drückt jetzt die Progressivität bezüglich des Maßes μ und der Ordnung $<$ aus:

$$\mathrm{Prog}^{\mu}_x A(x) := \forall_x\big(\forall_{y;\mu y<\mu x} A(y) \to A(x)\big),$$

wobei $\forall_{y;\mu y<\mu x} A(y)$ eine Abkürzung ist für $\forall_y(\mu y < \mu x \to A(y))$. (3.39) ist dann ein Spezialfall, in dem $\rho = \mathbf{N}$ und das Maß μ die Identität auf $\mathbf{N}$ ist. Die allgemeine Form (3.40) beweist man ganz ähnlich wie (3.39).

3.2.4. Euklidischer Algorithmus.

Satz (Euklid). *Zu beliebigen natürlichen Zahlen n, m mit $n > m$ gibt es genau einen größten gemeinsamen Teiler d.*

Beweis. Die Eindeutigkeit hatten wir bereits bewiesen. Den Beweis der Existenz führen wir durch Wertverlaufsinduktion über n. Seien also n, m mit $n > m$ gegeben. Wir verwenden eine Fallunterscheidung gemäß (3.24).

Fall $m = 0$. n ist größter gemeinsamer Teiler von n und 0.

Fall $m > 0$. Division mit Rest ergibt

$$n = mq + r \quad \text{und} \quad r < m.$$

Wir zeigen zunächst $d \mid n \to d \mid m \to d \mid r$. Gelte also $d \mid n$ und $d \mid m$. Dann hat man k, l mit $n = dk$ und $m = dl$, also $dk = dlq + r$ und damit $d \mid r$ nach Teil (j) des Lemmas in 3.2.2 Es gilt deshalb für beliebige d

$$d \mid n \wedge d \mid m \leftrightarrow d \mid m \wedge d \mid r.$$

Wir zeigen jetzt

$$d \text{ ist ggT von } n, m \leftrightarrow d \text{ ist ggT von } m, r. \tag{3.41}$$

Sei also d der größte gemeinsame Teiler von n, m. Dann gilt

(a) $d \mid n$ und $d \mid m$;
(b) $\forall_s(s \mid n \to s \mid m \to s \mid d)$.

Wir zeigen, daß d auch der größte gemeinsame Teiler von m, r ist. $d \mid r$ folgt aus der Vorüberlegung. Zu zeigen bleibt $\forall_t(t \mid m \to t \mid r \to t \mid d)$. Gelte also $t \mid m$ und $t \mid r$. Zu zeigen ist $t \mid d$. Wegen $n = mq + r$ folgt $t \mid n$ aus Teil (i) des Lemmas. Also gilt $t \mid d$ nach Voraussetzung. Die umgekehrte Richtung von (3.41) zeigt man ähnlich.

Nach IH haben wir einen größten gemeinsamen Teiler d von m, r. Aufgrund von (3.41) ist d auch größter gemeinsamer Teiler von n, m. □

Definition. Den eindeutig bestimmten größten gemeinsamen Teiler von n und m bezeichnen wir mit $\mathrm{ggT}(n, m)$. Zwei natürliche Zahlen n, m heißen *teilerfremd*, wenn $\mathrm{ggT}(n, m) = 1$.

Das in dem Beweis verwendete Verfahren nennt man den *Euklidischen Algorithmus* zur Berechnung des größten gemeinsamen Teilers zweier Zahlen. Zum Beispiel erhält man $\mathrm{ggT}(66, 27)$ wie folgt.

$$\begin{aligned} 66 &= 27 \cdot 2 + 12 \\ 27 &= 12 \cdot 2 + 3 \\ 12 &= 3 \cdot 4. \end{aligned}$$

Der größte gemeinsame Teiler von 66 und 27 ist also 3.

Wir zeigen jetzt, daß $\mathrm{ggT}(n, m)$ sich linear aus n und m kombinieren läßt. Dazu verwenden wir die Funktion

$$|n - m| := [\textbf{if } (n \leq m) \textbf{ then } n \dot{-} m \textbf{ else } m \dot{-} n].$$

Satz. *Zu beliebigen natürlichen Zahlen n, m mit $n > m$ gibt es k, l mit* $\mathrm{ggT}(n, m) = |nk - ml|$.

BEWEIS. Wir führen den Beweis durch Wertverlaufsinduktion über n. Seien also n, m mit $n > m$ gegeben. Sei $d := \mathrm{ggT}(n, m)$. Wir verwenden eine Fallunterscheidung gemäß (3.24).

Fall $m = 0$. Setze $k := 1$ und $l := 0$.

Fall $m > 0$. Division mit Rest ergibt

$$n = mq + r \quad \text{und} \quad r < m.$$

Nach der IH für m haben wir s, t mit $d = \mathrm{ggT}(m, r) = |ms - rt|$. Wir setzen $k := t$ und $l := qt + s$, und verwenden eine Fallunterscheidung (Induktion nach $\mathbf{B}$). Ist $ms \leq rt$, so erhält man

$$ml = m(qt + s) = mqt + ms \leq mqt + rt = (mq + r)t = nt = nk$$

und

$$nk \dot{-} ml = mqt + rt \dot{-} mqt \dot{-} ms = rt \dot{-} ms = d.$$

Ist umgekehrt $ms \not\leq rt$, so erhält man $ms > rt$, also

$$ml = m(qt + s) = mqt + ms > mqt + rt = (mq + r)t = nt = nk$$

und

$$ml \dot{-} nk = mqt + ms \dot{-} mqt \dot{-} rt = ms \dot{-} rt = d. \qquad \square$$

KOROLLAR. *Sind n und q teilerfremd und gilt $q \mid nm$, so folgt $q \mid m$.*

BEWEIS. Nach Annahme ist $\mathrm{ggT}(n, q) = 1$. Nach dem vorigen Satz gibt es also k, l mit $1 = |nk - ql|$. Sei etwa $nk \leq ql$. Dann hat man $1 = ql \dot{-} nk$, also $1 + nk = ql$, also auch $m + mnk = mql$. Wegen $q \mid mn$ folgt $q \mid m$ aus Teil (j) des Lemmas in 3.2.2. $\square$

3.3. Primzahlen

DEFINITION. Wir nennen eine natürliche Zahl n *zusammengesetzt*, wenn sie Produkt zweier kleinerer Faktoren ist, also

$$Z(n) := \exists_{m,k<n}\,(n = mk),$$

wobei $\exists_{m<n} A := \exists_m(m < n \wedge A)$. Eine natürliche Zahl n heißt *Primzahl*, wenn sie ≥ 2 und nicht zusammengesetzt ist, also

$$P(n) := 2 \leq n \wedge \neg Z(n).$$

Wir verwenden hier den beschränkten Existenzquantor $\exists_{m<n} A$, weil er nicht aus dem Bereich der „entscheidbaren“ Formeln hinausführt, mit denen wir uns gleich befassen. Entscheidbare Formeln A_0 haben den Vorzug, daß man zum Beweis einer beliebigen (nicht notwendig stabilen) Formel eine Fallunterscheidung nach A_0 machen kann.

3.3.1. Entscheidbare Formeln. Wir nennen eine Formel *entscheidbar*, wenn sie äquivalent ist zu einer Formel der Gestalt $\mathrm{atom}(r^{\mathbf{B}})$ mit einem Term $r^{\mathbf{B}}$ vom Typ $\mathbf{B}$.

Zum Beispiel sind alle Gleichungen und Ungleichungen zwischen Termen des Typs $\mathbf{N}$ entscheidbar. Ferner führen die aussagenlogischen Verknüpfungen $\to$, $\wedge$ und $\vee$ nicht aus dem Bereich der entscheidbaren Formeln heraus, denn es gilt

$$\begin{aligned}(\mathrm{atom}(r) \to \mathrm{atom}(s)) &\leftrightarrow \mathrm{atom}(r\ \mathrm{impb}\ s),\\ \mathrm{atom}(r) \wedge \mathrm{atom}(s) &\leftrightarrow \mathrm{atom}(r\ \mathrm{andb}\ s),\\ \mathrm{atom}(r) \vee \mathrm{atom}(s) &\leftrightarrow \mathrm{atom}(r\ \mathrm{orb}\ s)\end{aligned}$$

mit den in 2.2.2 definierten booleschen Funktionen impb, andb und orb.

Wir wollen uns überlegen, daß auch die beschränkten Quantoren nicht aus dem Bereich der entscheidbaren Formeln herausführen. Dazu definieren wir booleschwertige Funktionen $\forall_<$ und $\exists_<$ vom Typ $\mathbf{N} \to (\mathbf{N} \to \mathbf{B}) \to \mathbf{B}$ durch die folgenden Berechnungsregeln. Sei f eine Variable vom Typ $\mathbf{N} \to \mathbf{B}$.

$$\begin{aligned}\forall_<(0, f) &:= \mathtt{tt}, & \exists_<(0, f) &:= \mathtt{ff},\\ \forall_<(\mathrm{S}n, f) &:= \forall_<(n, f)\ \mathrm{andb}\ fn, & \exists_<(\mathrm{S}n, f) &:= \exists_<(n, f)\ \mathrm{orb}\ fn.\end{aligned}$$

Man zeigt dann leicht (durch Induktion über n)

$$\begin{aligned}\mathrm{atom}(\forall_<(n, f)) &\leftrightarrow \forall_{m<n}\,\mathrm{atom}(fm),\\ \mathrm{atom}(\exists_<(n, f)) &\leftrightarrow \exists_{m<n}\,\mathrm{atom}(fm).\end{aligned}$$

Durch Induktion über n beweist man ebenfalls leicht

$$\begin{aligned}\neg\forall_{m<n}\,\mathrm{atom}(fm) &\leftrightarrow \exists_{m<n}\neg\mathrm{atom}(fm),\\ \neg\exists_{m<n}\,\mathrm{atom}(fm) &\leftrightarrow \forall_{m<n}\neg\mathrm{atom}(fm).\end{aligned}$$

Lemma (Fallunterscheidung über entscheidbare Formeln).

$$(\mathrm{atom}(b) \to A) \to (\neg\mathrm{atom}(b) \to A) \to A.$$

Beweis. Durch Induktion nach der booleschen Variablen b. □

3.3.2. Primfaktorzerlegung.

Satz. *Jede natürliche Zahl $n \geq 2$ kann als Produkt von Primfaktoren geschrieben werden. Diese Darstellung ist bis auf die Reihenfolge eindeutig.*

Beweis. Sei $n \geq 2$. *Existenz.* Wir benutzen eine Wertverlaufsinduktion nach n, und verwenden eine Fallunterscheidung nach der (entscheidbaren) Eigenschaft, ob n eine Primzahl ist. *Fall* $P(n)$, also n ist Primzahl. Dann sind wir fertig. *Fall* $\neg P(n)$, also n ist keine Primzahl. Dann ist n zusammengesetzt, es gibt also $m, k < n$ mit $n = mk$. Wegen $2 \leq n$ folgt $2 \leq m, k$. Nach

IH für m und k haben wir Darstellungen $m = p_1 \dots p_r$ und $k = q_1 \dots q_s$, also $n = mk = p_1 \dots p_r q_1 \dots q_s$.

Eindeutigkeit. Wir beginnen mit einer *Vorbemerkung*: Gilt $p \mid q_1 \dots q_s$ mit Primzahlen $p, q_1, \dots, q_s$, so ist $p = q_j$ für ein j. Den Beweis führen wir durch Induktion über s. *Basis.* Aus $p \mid 1$ folgt F und wir können Ex-Falso-Quodlibet verwenden. *Schritt* $s \mapsto s+1$. *Fall* $p = q_{s+1}$. Dann ist die Behauptung offenbar richtig. *Fall* $p \neq q_{s+1}$. Dann sind p und q_{s+1} teilerfremd, also $p \mid q_1 \dots q_s$ nach dem Korollar in 3.2.4. Nach der IH folgt $p = q_j$ für ein j mit $1 \leq j \leq s$.

Sei jetzt $m = p_1 \dots p_r = q_1 \dots q_s$ mit Primzahlen $p_1, \dots, p_r, q_1, \dots, q_s$. Wir beweisen durch Induktion über r, daß dann $r = s$ gilt und und beide Darstellungen bis auf die Reihenfolge gleich sind. *Basis.* Dann ist $m = 1$ und deshalb $s = 0$. *Schritt* $r \mapsto r+1$. Wir haben offenbar $p_{r+1} \mid q_1 \dots q_s$ und $s \geq 1$, also $p_{r+1} = q_j$ für ein j nach der Vorbemerkung. OBdA sei $p_{r+1} = q_s$. Man erhält $p_1 \dots p_r = q_1 \dots q_{s-1}$. Mit der IH folgt die Behauptung. □

3.3.3. Existenz unendlich vieler Primzahlen.

Satz (Euklid). *Es gibt unendlich viele Primzahlen, das heißt, zu jeder endlichen Liste $p_1, \dots, p_n$ von Primzahlen findet man eine von ihnen allen verschiedene Primzahl q.*

Beweis. Wir betrachten $p_1 \dots p_n + 1$ und führen den Beweis durch Fallunterscheidung. *Fall* $p_1 \dots p_n + 1$ ist Primzahl. Dann haben wir eine von $p_1, \dots, p_n$ verschiedene Primzahl gefunden. *Fall* $p_1 \dots p_n + 1$ ist keine Primzahl. Nach dem Satz über die Primfaktorzerlegung gibt es eine Primzahl q mit $q \mid p_1 \dots p_n + 1$. Wäre $q = p_i$ für ein i mit $1 \leq i \leq n$, so folgte $q \mid 1$ und damit ein Widerspruch. □

Definition. Mit p_n bezeichnen wir die (unendliche) Folge der Primzahlen, also $p_0 = 2$, $p_1 = 3$, $p_3 = 5$ und so weiter.

Korollar. *Jede natürliche Zahl $n \geq 1$ läßt sich darstellen in der Form*

$$n = p_0^{i_0} p_1^{i_1} \dots p_r^{i_r}.$$

Diese Darstellung ist eindeutig, wenn man $0 < i_r$ verlangt.

Korollar. *Es seien n, m natürliche Zahlen mit*

$$n = p_0^{i_0} p_1^{i_1} \dots p_r^{i_r}, \qquad m = p_0^{j_0} p_1^{j_1} \dots p_r^{j_r}.$$

Dann ist

$$\mathrm{ggT}(n, m) = p_0^{\min(i_0, j_0)} p_1^{\min(i_1, j_1)} \dots p_r^{\min(i_r, j_r)}.$$

Beweis. Übung. □

3.4. Darstellung natürlicher Zahlen

Wenn man mit konkreten Zahlen rechnen will, ist es aus Effizienzgründen notwendig, eine andere Darstellung als die unäre zu verwenden. Meistens benutzt man die Dezimaldarstellung; wir wollen hier im allgemeinen die Binärdarstellung verwenden (also $b = 2$).

3.4.1. Die b-adische Darstellung natürlicher Zahlen.

SATZ. *Seien a, b natürliche Zahlen mit $a > 0$ und $b > 1$. Dann gibt es ein eindeutig bestimmtes n und eine eindeutig bestimmte Liste $c_0, \ldots, c_n$ natürlicher Zahlen $< b$ mit $c_0 > 0$ so daß*

$$a = \sum_{k=0}^{n} c_k b^{n \dot{-} k}.$$

BEWEIS. Wir verwenden eine Wertverlaufsinduktion nach a. Sei also $a > 0$, und jedes a' mit $0 < a' < a$ habe eine eindeutige Darstellung der gewünschten Form. Ist $a < b$, so kann man $n = 0$ und $c_0 = a$ wählen. Zum Beweis der Eindeutigkeit nehmen wir an, wir hätten eine weitere Darstellung

$$a = \sum_{k=0}^{n'} c'_k b^{n' \dot{-} k}.$$

Ist $n' > 0$, so folgt

$$a = c'_0 b^{n'} + \sum_{k=1}^{n'} c'_k b^{n' \dot{-} k} \geq c'_0 b^{n'} \geq b^{n'} \geq b$$

im Widerspruch zur Annahme $a < b$. Also ist $n' = 0$ und wir erhalten

$$a = c'_0 b^0 = c'_0 = c_0.$$

Sei jetzt also $b \leq a$.

Existenz. Nach dem Satz von der Division mit Rest erhalten wir q, r mit

$$a = bq + r \quad \text{und} \quad r < b.$$

Wegen $r < a$ ist $0 < q$, und wegen $1 < b$ ist $q < bq \leq a$. Nach IH für q findet man m und $d_0, \ldots, d_m$ mit $d_k < b$ und $d_0 > 0$ so daß

$$q = \sum_{k=0}^{m} d_k b^{m \dot{-} k}, \quad \text{also} \quad a = \sum_{k=0}^{m} d_k b^{(m+1) \dot{-} k} + r.$$

Wir können also setzen $n := m + 1$, $c_n := r$ und $c_k := d_k$ für $k < n$.

Eindeutigkeit. Nehmen wir an, wir hätten eine weitere Darstellung

$$a = \sum_{k=0}^{n'} c'_k b^{n' \dot{-} k}.$$

Ist $n' = 0$, so erhalten wir

$$a = c'_0 b^0 = c'_0 < b$$

und damit einen Widerspruch. Also ist $n' > 0$ und deshalb

$$a = \underbrace{\Big(\sum_{k=0}^{n' \dot{-} 1} c'_k b^{(n' \dot{-} 1) \dot{-} k}\Big)}_{q'} \cdot b + c'_{n'}.$$

Wegen $c'_{n'} < b$ folgt aus dem Eindeutigkeitsteil des Satzes von der Division mit Rest, daß $q' = q$ und $c'_{n'} = r$ sein muß. Aus der Eindeutigkeit der Darstellung für q folgt $n' \dot{-} 1 = m$ und $c'_k = d_k$ für $k \leq m$. Deshalb ist

$$\begin{aligned} n' &= m + 1 = n, \\ c'_k &= d_k = c_k \quad \text{für } k \leq m \end{aligned}$$

Das war zu zeigen. □

3.4.2. Algorithmen für Addition und Multiplikation. Man kann jetzt den üblichen Additionsalgorithmus für in b-adischer Darstellung gegebene Zahlen ableiten. Sei

$$a_1 = \sum_{k=0}^{n_1} c_{1,k} b^{n_1 \dot{-} k} \quad \text{und} \quad a_2 = \sum_{k=0}^{n_2} c_{2,k} b^{n_2 \dot{-} k}.$$

Wenn wir auch 0 als Koeffizienten zulassen, können wir $n_1 = n_2$ annehmen und schreiben

$$a_1 = \sum_{k=0}^{n} d_{1,k} b^{n \dot{-} k} \quad \text{und} \quad a_2 = \sum_{k=0}^{n} d_{2,k} b^{n \dot{-} k}.$$

Dann ist

$$a_1 + a_2 = \sum_{k=0}^{n} d_k b^{n \dot{-} k} \quad \text{mit } d_k = d_{1,k} + d_{2,k}.$$

Wir haben dann wir gewünscht $0 < d_0$, aber nur $d_k \leq 2b \dot{-} 2$. Wir müssen deshalb einen Übertrag vorsehen. Ist $d_n < b$ so können wir $c_n := d_n$ setzen. Ist jedoch $d_n = b + r$ mit $r < b$, so setzen wir $c_n := r$ und müssen 1 zu dem b^1-Term $d_{n \dot{-} 1}$ hinzu addieren. Dies kann wieder einen Übertrag erforderlich machen; man muß das Verfahren entsprechend fortsetzen.

Der bekannte Algorithmus zur Multiplikation zweier in b-adischer Darstellung gegebener Zahlen läßt sich ähnlich entwickeln.

3.4.3. Binärzahlen als Datentyp. In 2.1.1 hatten wir den Typ **P** der binär dargestellten positiven Zahlen eingeführt. Er ist erzeugt aus der Eins 1 durch zwei einstellige Nachfolgeroperationen S_0 und S_1, die den Funktionen $n \mapsto 2n$ bzw. $n \mapsto 2n+1$ entsprechen. Es gibt einen offensichtlichen Zusammenhang zwischen dem Typ **P** und der oben eingeführten b-adischen Darstellung im Fall $b = 2$, also der Darstellung

$$a = \sum_{k=0}^{n} c_k 2^{n \dot{-} k}, \qquad c_k \text{ natürliche Zahlen} < 2 \text{ und } c_0 = 1.$$

Ihr entspricht die „Zahldarstellung“

$$\underbrace{c_0}_{1} c_1 c_2 \dots c_n, \qquad c_k \text{ „Ziffern“ 0 oder 1.}$$

In **P** entspricht dem der Term

$$S_{c_n}(\dots S_{c_2}(S_{c_1}1)\dots).$$

Beispiele:

Dezimaldarstellung	Binärdarstellung	Term des Typs **P**
1	1	1
2	10	$S_0 1$
3	11	$S_1 1$
4	100	$S_0(S_0 1)$
5	101	$S_1(S_0 1)$
6	110	$S_0(S_1 1)$
7	111	$S_1(S_1 1)$
8	1000	$S_0(S_0(S_0 1))$
9	1001	$S_1(S_0(S_0 1))$

Wir können jetzt etwa Addition und Multiplikation vom Typ $\mathbf{P} \to \mathbf{P} \to \mathbf{P}$ durch Berechnungsregeln definieren. Vorbereitend dazu benötigen wir eine Nachfolgerfunktion S vom Typ $\mathbf{P} \to \mathbf{P}$. Die Berechnungsregeln für S sind

$$S1 := S_0 1, \quad S(S_0 p) := S_1 p, \quad S(S_1 p) := S_0(Sp).$$

Für die Addition sind die Berechnungsregeln

$$\begin{aligned} p + 1 &:= Sp, & 1 + S_1 q &:= S_0(Sq), \\ 1 + S_0 q &:= S_1 q, & S_0 p + S_1 q &:= S_1(p+q), \\ S_0 p + S_0 q &:= S_0(p+q), & S_1 p + S_1 q &:= S_0(S(p+q)). \\ S_1 p + S_0 q &:= S_1(p+q), \end{aligned}$$

Die Multiplikation ist definiert durch die Berechnungsregeln

$$p \cdot 1 := p, \quad p \cdot S_0 q := S_0(p \cdot q), \quad p \cdot S_1 q := S_0(p \cdot q) + p.$$

Man beachte, daß damit die Algorithmen für Addition und Multiplikation von Binärzahlen vollständig angegeben sind.

Ähnlich wie in 3.1.4 kann man jetzt Eigenschaften der arithmetischen Funktionen $+$ und $\cdot$ beweisen und sie als Ersetzungsregeln verwenden. Die Beweise führt man dann durch Induktion über $\mathbf{P}$, also mit dem bereits in 3.1.1 angegebenen Schema

$$\mathrm{Ind}_{q,A}\colon \forall_q\big(A(1) \to \forall_p(A(p) \to A(S_0p)) \to \forall_p(A(p) \to A(S_1p)) \to A(q^{\mathbf{P}})\big)$$

Auch die in 3.1.5 betrachteten weiteren arithmetischen Relationen und Funktionen wie $<$ und $\leq$ vom Typ $\mathbf{P} \to \mathbf{P} \to \mathbf{B}$ lassen sich durch geeignete (in diesem Fall simultane) Berechnungsregeln einführen:

$$\begin{aligned} (p < 1) &:= \mathtt{ff}, & (1 < S_1q) &:= \mathtt{tt},\\ (1 < S_0q) &:= \mathtt{tt}, & (S_0p < S_1q) &:= (p \leq q),\\ (S_0p < S_0q) &:= (p < q), & (S_1p < S_1q) &:= (p < q)\\ (S_1p < S_0q) &:= (p < q), \end{aligned}$$

und

$$\begin{aligned} (1 \leq q) &:= \mathtt{tt}, & (S_1p \leq 1) &:= \mathtt{ff},\\ (S_0p \leq 1) &:= \mathtt{ff}, & (S_1p \leq S_0q) &:= (p < q),\\ (S_0p \leq S_0q) &:= (p \leq q), & (S_1p \leq S_1q) &:= (p \leq q).\\ (S_0p \leq S_1q) &:= (p \leq q), \end{aligned}$$

Die „abgeschnittene“ Subtraktion und die dafür notwendige Vorgängerfunktion kann man auf $\mathbf{P}$ definieren durch

$$\begin{aligned} & & P(S_01) &:= 1, & & \\ P1 &:= 1, & P(S_0(S_0p)) &:= S_1(P(S_0p)), & P(S_1p) &:= S_0p.\\ & & P(S_0(S_1p)) &:= S_1(S_0p), & & \end{aligned}$$

Für die Subtraktion sind die Berechnungsregeln

$$\begin{aligned} 1 \dot{-} q &:= 1, & S_1p \dot{-} 1 &:= S_0p,\\ S_0p \dot{-} 1 &:= P(S_0p), & S_1p \dot{-} S_0q &:= S_0p \dot{-} P(S_0q),\\ S_0p \dot{-} S_0q &:= S_0(p \dot{-} q), & S_1p \dot{-} S_1q &:= S_0(p \dot{-} q).\\ S_0p \dot{-} S_1q &:= P(S_0(p \dot{-} q)), \end{aligned}$$

Die Beweise der erwarteten Eigenschaften lassen sich wie in 3.1.5 durch geeignete Induktionen über $\mathbf{P}$ führen.

KAPITEL 4

Ganze Zahlen

Unser Ziel ist es, die natürlichen Zahlen zu einem Bereich von „ganzen Zahlen“ zu erweitern, in dem eine Gleichung

$$a + x = b$$

stets lösbar ist.

Wir beginnen mit einer konkreten Konstruktion der ganzen Zahlen, als einer mathematischen Struktur mit gewissen Operationen $+$, $\cdot$ und $\leq$. Wir stellen dann fest, daß in dieser Struktur eine Reihe von Eigenschaften gelten, die auch für viele andere Strukturen erfüllt sind. Dies führt uns auf die Begriffe einer Gruppe und eines Ringes, insbesondere auch den eines geordneten Integritätsbereichs. Viele wichtige Eigenschaften der ganzen Zahlen werden in wir in dieser allgemeinen Form beweisen können. Wir zeigen dann noch, daß man die ganzen Zahlen charakterisieren kann als die in einem gewissen Sinn kleinste Erweiterung der natürlichen Zahlen zu einem geordneten Integritätsbereich.

4.1. Konstruktion der ganzen Zahlen

Ganze Zahlen kann man als Differenz zweier natürlicher Zahlen darstellen, modulo der offensichtlichen Äquivalenz. Dies hat den Vorteil, daß viele Definitionen und Beweise ohne Fallunterscheidungen auskommen. Wir wollen hier eine möglichst knappe Darstellung konkreter Zahlen erreichen und fassen dashalb eine ganze Zahl als negative Binärzahl, Null oder positive Binärzahl auf.

4.1.1. Der Typ Z der ganzen Zahlen. Zur genauen Definition ist es bequem, noch einen besonderen und ganz einfachen „Typ“ einzuführen, der nur aus einem einzigen Objekt besteht. Wir nennen ihn den *Einheitstyp* und bezeichnen ihn mit **U**. Sein einziges Objekt bezeichnen wir mit **u**. Jetzt können wir die den Typ **Z** der ganzen Zahlen definieren als

$$\mathbf{Z} := \mathbf{P} + \mathbf{U} + \mathbf{P}.$$

Jede ganze Zahl ist also entweder

- eine negative Binärzahl, geschrieben $\ominus p$, oder

- die ganze Zahl Null, geschrieben 0, oder
- eine positive Binärzahl, geschrieben $\oplus p$.

4.1.2. Addition und Multiplikation für ganze Zahlen. Die Nachfolgerfunktion $S_{\mathbf{Z}}$ vom Typ $\mathbf{Z} \to \mathbf{Z}$ ist definiert durch die Berechnungsregeln

$$\begin{aligned} S_{\mathbf{Z}}0 &:= \oplus 1, & S_{\mathbf{Z}}(\ominus 1) &:= 0,\\ S_{\mathbf{Z}}(\oplus p) &:= \oplus(Sp), & S_{\mathbf{Z}}(\ominus(S_0 p)) &:= \ominus(P(S_0 p)),\\ & & S_{\mathbf{Z}}(\ominus(S_1 p)) &:= \ominus(S_0 p). \end{aligned}$$

Die Addition für ganze Zahlen benötigt bei unserer Darstellung (leider) eine lange Fallunterscheidung, ist aber abgesehen davon sehr elementar:

$$\begin{aligned} 0 + i &:= i,\\ \oplus p + 0 &:= \oplus p,\\ \oplus p + \oplus q &:= \oplus(p + q)\\ \oplus p + \ominus q &:= \begin{cases} 0 & \text{falls } p = q,\\ \ominus(q \dot{-} p) & \text{falls } p < q,\\ \oplus(p \dot{-} q) & \text{sonst} \end{cases}\\ \ominus p + 0 &:= \ominus p,\\ \ominus p + \oplus q &:= \begin{cases} 0 & \text{falls } p = q,\\ \oplus(q \dot{-} p) & \text{falls } p < q,\\ \ominus(p \dot{-} q) & \text{sonst} \end{cases}\\ \ominus p + \ominus q &:= \ominus(p + q). \end{aligned}$$

Ganz ähnlich läßt sich die Subtraktion für ganze Zahlen definieren.

Bei der Multiplikation kommt man wieder mit relativ wenig Fallunterscheidungen aus

$$\begin{aligned} 0 \cdot i &:= 0, & \ominus p \cdot 0 &:= 0,\\ \oplus p \cdot 0 &:= 0, & \ominus p \cdot \oplus q &:= \ominus(p \cdot q),\\ \oplus p \cdot \oplus q &:= \oplus(p \cdot q), & \ominus p \cdot \ominus q &:= \oplus(p \cdot q).\\ \oplus p \cdot \ominus q &:= \ominus(p \cdot q), \end{aligned}$$

4.1.3. Weitere Relationen und Funktionen auf den ganzen Zahlen. Die $<$-Relation für ganze Zahlen ist definiert durch Rückgriff auf die $<$-Relation für $\mathbf{P}$:

$$\begin{aligned} (0 < 0) &:= \mathsf{ff}, & (\oplus p < 0) &:= \mathsf{ff}, & (\ominus p < 0) &:= \mathsf{tt},\\ (0 < \oplus q) &:= \mathsf{tt}, & (\oplus p < \oplus q) &:= (p < q), & (\ominus p < \oplus q) &:= \mathsf{tt},\\ (0 < \ominus q) &:= \mathsf{ff}, & (\oplus p < \ominus q) &:= \mathsf{ff}, & (\ominus p < \ominus q) &:= (q < p). \end{aligned}$$

Ähnlich definiert man die $\leq$-Relation:

$$\begin{array}{lll} (0 \leq 0) := \mathtt{tt}, & (\oplus p \leq 0) := \mathtt{ff}, & (\ominus p \leq 0) := \mathtt{tt}, \\ (0 \leq \oplus q) := \mathtt{tt}, & (\oplus p \leq \oplus q) := (p \leq q), & (\ominus p \leq \oplus q) := \mathtt{tt}, \\ (0 \leq \ominus q) := \mathtt{ff}, & (\oplus p \leq \ominus q) := \mathtt{ff}, & (\ominus p \leq \ominus q) := (q \leq p). \end{array}$$

Man kann jetzt viele erwartete Eigenschaften der ganzen Zahlen beweisen. Wir wollen hier jeweils einige besonders elementare dieser Eigenschaften zusammenfassen und dann einen Abstraktionsschritt durchführen, in dem wir eine entsprechende allgemeine mathematische Struktur definieren. Weitere Eigenschaften der ganzen Zahlen können wir dann für die jeweilige allgemeine Struktur beweisen. Das macht man nicht nur aus Gründen der Ökonomie (diese Eigenschaften gelten dann in *allen* Strukturen dieser Art), sondern auch deshalb, weil man durch den Abstraktionsschritt von unwesentlichen Einzelheiten des Begriffs der ganzen Zahlen absehen kann und deshalb klarere Beweise bekommt.

4.2. Gruppen

4.2.1. Z als additive Gruppe.

Lemma.

(a) $(i + j) + k = i + (j + k)$ *für alle* $i, j, k \in \mathbf{Z}$.
(b) (i) $0 + i = i$ *für alle* $i \in \mathbf{Z}$;
(ii) *zu jedem* $i \in \mathbf{Z}$ *gibt es ein* $i' \in \mathbf{Z}$ *mit* $i' + i = 0$.
(c) $i + j = j + i$ *für alle* $i, j \in \mathbf{Z}$.

Beweis. (a) und (c) beweist man (leicht aber mühsam) durch Fallunterscheidungen. Teil (i) von (b) folgt aus der Definition von $+$. Teil (ii) beweisen wir durch Fallunterscheidung nach i: Im Fall $\ominus p$ wähle man $i' := \oplus p$; im Fall 0 wähle man $i' := 0$; im Fall $\oplus p$ wähle man $i' := \ominus p$. □

Diese Eigenschaften beinhalten in einem gewissen Sinne alles, was über die additive Struktur der ganzen Zahlen zu sagen ist. Wir führen jetzt einen Abstraktionsschritt durch und definieren den allgemeinen Gruppenbegriff.

4.2.2. Definition und einfache Eigenschaften von Gruppen.

Definition. Seien G eine Menge und $\circ\colon G \to G \to G$ eine Abbildung. $(G, \circ)$ (oder oft nur kurz G) heißt *Gruppe*, wenn gilt

(a) $(x \circ y) \circ z = x \circ (y \circ z)$ für alle $x, y, z \in G$ (*Assoziativgesetz*).
(b) Es gibt ein $e \in G$ (genannt *neutrales Element* von G) mit folgenden Eigenschaften:
(i) $e \circ x = x$ für alle $x \in G$;

(ii) zu jedem $x \in G$ gibt es ein $x' \in G$ mit $x' \circ x = e$ (x' heißt *inverses Element* zu x).

G heißt *abelsch*, wenn außerdem noch gilt $x \circ y = y \circ x$ für alle $x, y \in G$ (*Kommutativgesetz*).

Nach dem eben bewiesenen Lemma ist also $(\mathbf{Z}, +)$ eine abelsche Gruppe.

LEMMA. *Sei G eine Gruppe.*

(a) *(Linksinverse Elemente sind auch rechtsinvers). Sei $e \in G$ ein neutrales Element und $x, x' \in G$ derart, daß $x' \circ x = e$. Dann gilt auch $x \circ x' = e$.*
(b) *(Linksneutrale Elemente sind auch rechtsneutral). Sei $e \in G$ ein neutrales Element. Dann gilt $x \circ e = x$ für alle $x \in G$.*
(c) *Es gibt genau ein neutrales Element $e \in G$.*
(d) *Zu jedem $x \in G$ gibt es genau ein inverses Element $x' \in G$.*

BEWEIS. (a) Wähle x'' mit $x'' \circ x' = e$. Dann gilt

$$x \circ x' = e \circ x \circ x' = x'' \circ \underbrace{x' \circ x}_{e} \circ x' = x'' \circ x' = e.$$

(b) $x \circ e = x \circ x' \circ x = e \circ x = x$ nach (a).
(c) Seien e, e^* neutrale Elemente von G. Nach (b) gilt $e^* = e \circ e^* = e$.
(d) Seien x', x^* inverse Elemente zu $x \in G$. Dann gilt

$$x^* = x^* \circ e = x^* \circ x \circ x' = e \circ x' = x'.$$

Hierbei haben wir (a) - (c) benutzt. □

Das zu x eindeutig bestimmte inverse Element wird mit x^{-1} bezeichnet. Wir schreiben x^n für $x \circ \cdots \circ x$ und x^{-n} für $x^{-1} \circ \cdots \circ x^{-1}$, jeweils mit n Vorkommen von x bzw. x^{-1}. Ferner sei $x^0 := e$.

4.2.3. Charakterisierung des Gruppenbegriffs.

LEMMA. *Seien G eine nicht leere Menge und $\circ\colon G \to G \to G$ eine Abbildung. G ist eine Gruppe genau dann, wenn gilt:*

(a) $(x \circ y) \circ z = x \circ (y \circ z)$ *für alle $x, y, z \in G$ (*Assoziativgesetz*).*
(b) (i) $\forall_{x,y \in G} \exists_{z \in G}\, x \circ z = y$.
(ii) $\forall_{x,y \in G} \exists_{z \in G}\, z \circ x = y$.

BEWEIS. $\rightarrow$. Sei G eine Gruppe. Zum Beweis von $\forall_{x,y \in G} \exists_{z \in G}\, x \circ z = y$ genügt es, $z = x^{-1} \circ y$ zu setzen, und zum Beweis von $\forall_{x,y \in G} \exists_{z \in G}\, z \circ x = y$ genügt es, $z = y \circ x^{-1}$ zu setzen.

$\leftarrow$. G erfülle die im Lemma aufgelisteten Eigenschaften. Zu zeigen ist, daß G eine Gruppe ist. Wir müssen also ein neutrales Element e finden derart, daß gilt

$$e \circ x = x \text{ für alle } x \in G, \text{ und}$$

$$\forall_{x\in G}\exists_{x'\in G}\, x' \circ x = e$$

Wir konstruieren zunächst ein solches e. Wähle $x_0 \in G$ fest (hier wird benötigt, daß G nicht leer ist). Wähle e so, daß $e \circ x_0 = x_0$ ist.

Wir zeigen jetzt die beiden obigen Eigenschaften. Sei $x \in G$ beliebig. Wähle $z \in G$ mit $x_0 \circ z = x$. Dann gilt

$$e \circ x = e \circ x_0 \circ z = x_0 \circ z = x.$$

Die zweite Eigenschaft folgt aus Teil (ii) von (b). □

LEMMA. *Seien G eine Gruppe und $x, y \in G$. Dann gilt*

(a) $(x^{-1})^{-1} = x$.
(b) $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

BEWEIS. (a). Es gilt $(x^{-1})^{-1} \circ x^{-1} = e$ und auch $x \circ x^{-1} = e$. Die Behauptung folgt aus der Eindeutigkeit des Inversen.

(b). $y^{-1} \circ x^{-1} \circ x \circ y = y^{-1} \circ e \circ y = e$. □

BEISPIELE. Seien M eine nicht leere Menge und $S(M)$ die Menge der bijektiven Abbildungen von M auf sich selbst. Mit $\circ$ bezeichnen wir die Komposition (Hintereinanderausführung) von Abbildungen. Dann ist $(S(M), \circ)$ eine Gruppe. $(S(M), \circ)$ heißt die *symmetrische Gruppe* der Menge M. Neutrales Element ist die Identität $\mathrm{id}\colon M \to M$, und das inverse Element zu $f \in S(M)$ ist die Umkehrabbildung f^{-1}.

Man beachte, daß $S(M)$ i.a. nicht abelsch ist. Sei zum Beispiel

$$f\colon \{0,1,2\} \to \{0,1,2\} \qquad g\colon \{0,1,2\} \to \{0,1,2\}$$

$$f(a) = \begin{cases} 0 & \text{falls } a = 0 \\ 2 & \text{falls } a = 1 \\ 1 & \text{falls } a = 2 \end{cases} \quad \text{und} \quad g(a) = \begin{cases} 1 & \text{falls } a = 0 \\ 0 & \text{falls } a = 1 \\ 2 & \text{falls } a = 2. \end{cases}$$

Dann gilt $(g \circ f)(0) = 1$, aber $(f \circ g)(0) = 2$, also $g \circ f \neq f \circ g$.

Im Spezialfall $M = \{1, \ldots, n\}$ schreibt man S_n statt $S(M)$. Jede Abbildung $\sigma \in S_n$ heißt eine *Permutation* der Zahlen $1, \ldots, n$.

Ein wichtiges Beispiel einer endlichen abelschen Gruppe ist die Gruppe $\mathbf{Z}_n := \{\, x \in \mathbf{N} \mid x < n \,\}$ der *ganzen Zahlen modulo n*. Die Gruppenverknüpfung ist die *Addition modulo n*, die für $x, y \in \mathbf{Z}_n$ definiert ist als der (eindeutig bestimmte) Rest bei der Division von $x+y$ durch n. Man schreibt $x + y = r \mod n$, falls $x + y = nq + r$ mit $q, r \in \mathbf{N}$ und $r < n$. Der Beweis der Gruppeneigenschaften ist einfach: für die Assoziativität verwendet man Fallunterscheidungen nach den Summen der jeweiligen Reste. Neutrales Element ist die 0, und das inverse Element zu x ist $n \dot{-} x$.

4.2.4. Untergruppen. Eine Teilmenge $U \subseteq G$ wollen wir eine Untergruppe nennen, wenn die Gruppenstruktur auf G eine Gruppenstruktur auf U induziert. Genauer heißt das:

DEFINITION. Es sei G eine Gruppe und $U \subseteq G$ eine Teilmenge von G. U heißt *Untergruppe* von G, wenn gilt

(a) $xy \in U$ für alle $x, y \in U$,
(b) $e \in U$,
(c) $x^{-1} \in U$ für alle $x \in U$.

Da aus dem Zusammenhang klar ist, welche Gruppenverknüpfung gemeint ist, haben wir hier kurz xy anstelle von $x \circ y$ geschrieben. Dies werden wir auch im folgenden tun.

SATZ (Untergruppenkriterium). *Es sei G eine Gruppe und $U \subseteq G$ eine Teilmenge von G.*

(a) *U ist Untergruppe von G genau dann, wenn*
  (i) *$U \neq \emptyset$,*
  (ii) *$xy^{-1} \in U$ für alle $x, y \in U$.*
(b) *Sei U eine endliche Menge. U ist Untergruppe von G genau dann, wenn*
  (i) *$U \neq \emptyset$,*
  (ii) *$xy \in U$ für alle $x, y \in U$.*

BEWEIS. (a). $\rightarrow$. Dies folgt sofort aus der Definition von Untergruppen. $\leftarrow$. Da $U \neq \emptyset$, existiert ein $x_0 \in U$. Damit haben wir eine Einheit $e := x_0 x_0^{-1} \in U$. Sei jetzt $x \in U$. Dann ist auch $x^{-1} = ex^{-1} \in U$. Seien schließlich $x, y \in U$. Dann ist auch $y^{-1} \in U$ und damit $xy = x(y^{-1})^{-1} \in U$.

(b). $\rightarrow$. Dies folgt wieder sofort aus der Definition von Untergruppen. $\leftarrow$. Sei $x \in U$. Betrachte die Abbildung

$$\hat{x} \colon U \to U \quad \text{mit } \hat{x}(y) := xy.$$

Diese Abbildung ist wohldefiniert nach Bedingung (ii). $\hat{x}$ ist injektiv, denn aus $\hat{x}(y) = \hat{x}(z)$ folgt $xy = xz$, also $x^{-1}xy = x^{-1}xz$ und damit auch $y = z$. Da U endlich ist, ist $\hat{x}$ damit schon bijektiv. Sei nun $x \in U$ beliebig, aber fest (die Existenz ist klar, da $U \neq \emptyset$). Da $\hat{x}$ bijektiv ist, existiert $y \in U$ mit $\hat{x}(y) = x$. Dann gilt $xy = x$ und somit $y = e$, also $e \in U$. Außerdem existiert $z \in U$ mit $\hat{x}(z) = e$; dann gilt $xz = e$ und damit $z = x^{-1}$, also $x^{-1} \in U$.

Da $x \in U$ beliebig gewählt war, folgt die Behauptung. □

4.2.5. Homomorphismen für Gruppen.

DEFINITION. Seien G, H Gruppen und $f \colon G \to H$ eine Abbildung.

(a) f heißt *Homomorphismus* für Gruppen, wenn für alle $x, y \in G$ gilt

$$f(xy) = f(x)f(y).$$

(b) f heißt *Mono-, Epi- bzw. Isomorphismus*, wenn f Homomorphismus und injektiv, surjektiv bzw. bijektiv ist.
(c) f heißt *Endo- bzw. Automorphismus* , wenn $G = H$ und f Homo- bzw. Isomorphismus ist.
(d) G und H heißen *isomorph* ($G \cong H$), wenn es einen Isomorphismus $g\colon G \to H$ gibt.

Bemerkung. Diese Definition könnte man wie in 2.4.4 auf Gruppen mit einer Äquivalenzrelation und einer mit ihr verträglichen Gruppenverknüpfung verallgemeinern. Der Einfachheit halber verzichten wir darauf.

Lemma. *Seien G, H Gruppen und $f\colon G \to H$ ein Homomorphismus. e bzw. e' seien die neutralen Elemente von G bzw. H. Dann gilt*

(a) *$f(e) = e'$, und $f(x^{-1}) = f(x)^{-1}$ für alle $x \in G$.*
(b) *Ist U Untergruppe von G, so ist $f(U)$ Untergruppe von H. Ist V Untergruppe von H, so ist $f^{-1}(V)$ Untergruppe von G. Insbesondere ist also der* Kern *von f, also*

$$\operatorname{Kern}(f) := f^{-1}(\{e'\})$$

eine Untergruppe von G.
(c) $\operatorname{Kern}(f) = \{e\}$ *genau dann, wenn f injektiv ist.*
(d) *f ist Isomorphismus genau dann, wenn ein Homomorphismus $g\colon H \to G$ mit $g \circ f = \mathrm{id}_G$ und $f \circ g = \mathrm{id}_H$ existiert.*

Beweis. (a). $f(e) = f(ee) = f(e)f(e)$, also $f(e) = e'$. Außerdem ist $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$ also $f(x^{-1}) = f(x)^{-1}$.

(b) Sei U Untergruppe von G. Da $U \neq \emptyset$, folgt $f(U) \neq \emptyset$. Ferner gilt für alle $x, y \in U$

$$f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(U).$$

Also ist nach dem Untergruppenkriterium $f(U)$ eine Untergruppe von H.

Sei V Untergruppe von H. Dann gilt $f^{-1}(V) \neq \emptyset$, da $f(e) = e' \in V$, also $e \in f^{-1}(V)$. Seien nun $x, y \in f^{-1}(V)$ und damit $f(x), f(y) \in V$. Da V Untergruppe ist, folgt $f(x)f(y)^{-1} = f(xy^{-1}) \in V$, also $xy^{-1} \in f^{-1}(V)$. Also ist $f^{-1}(V)$ Untergruppe von G nach dem Untergruppenkriterium.

(c) $\rightarrow$. Seien $x, y \in G$ mit $f(x) = f(y)$. Dann gilt $e' = f(x)f(y)^{-1} = f(xy^{-1})$ und somit $xy^{-1} = e$, also $x = y$.

$\leftarrow$. $f(e) = e'$, also $e \in \operatorname{Kern}(f)$. Sei $x \in \operatorname{Kern}(f)$. Dann gilt $f(x) = e'$ und damit $x = e$, da f injektiv ist. Also ist $\operatorname{Kern}(f) = \{e\}$.

(d). $\rightarrow$. Setze $g := f^{-1}$. Zu zeigen bleibt, daß f^{-1} ein Homomorphismus ist. Seien $x, y \in H$ mit $x = f(u)$, $y = f(v)$ für $u, v \in G$. Dann gilt $f^{-1}(x)f^{-1}(y) = uv = f^{-1}(f(uv)) = f^{-1}(f(u)f(v)) = f^{-1}(xy)$. Also ist f^{-1} Homomorphismus.

$\leftarrow$. Klar, da aus der Existenz von g die Bijektivität von f folgt. □

4.2.6. Nebenklassen.

DEFINITION. Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe.

(a) Sei $x \in G$. Dann heißt

$$xU := \{ xu \mid u \in U \}$$

die von x erzeugte *Linksnebenklasse* bzgl. U. Analog heißt

$$Ux := \{ ux \mid u \in U \}$$

die von x erzeugte *Rechtsnebenklasse* bzgl. U.

(b) $G/U := \{ xU \mid x \in G \}$. (Sprechweise: „$G$ modulo U“).

LEMMA. *Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann gilt*

(a) *$xU = yU$ genau dann, wenn $x^{-1}y \in U$. Definiert man für $x, y \in G$*

$$(x \sim_U y) := (x^{-1}y \in U)$$

(Schreibweise: $x \equiv y \mod U$, „x kongruent y modulo U“), so ist also $\sim_U$ eine Äquivalenzrelation auf G.

(b) *$xU = \{ y \mid y \sim_U x \}$ (=: $[x]$, Äquivalenzklasse von x).*

(c) *Wähle in jeder Linksnebenklasse ein Element (Repräsentant) x_i. $(x_i)_{i \in I}$ sei die Familie der Repräsentanten. Dann gilt*

$$G = \bigcup_{i \in I} x_i U \quad \textit{(disjunkte Vereinigung).}$$

BEWEIS. (a). Es genügt, die erste Aussage zu beweisen. $\rightarrow$. Da $y = ye \in yU = xU$, gilt $y = xu$ für ein $u \in U$. Damit folgt $x^{-1}y = u \in U$.

$\leftarrow$. $x^{-1}y = u \in U$, also $y = xu$. Dann folgt für alle $v \in U$, daß $yv = xuv \in xU$, also $yU \subseteq xU$. Wegen $(x^{-1}y)^{-1} = y^{-1}x$ folgt analog $xU \subseteq yU$.

(b). $\subseteq$. Sei $u \in U$. Dann gilt $(xu)^{-1}x = u^{-1}x^{-1}x = u^{-1} \in U$, also $xu \sim_U x$.

$\supseteq$. Sei $y \sim_U x$, also $y^{-1}x \in U$. Dann gibt es ein $u \in U$ mit $y^{-1}x = u$. Folglich gilt $y = xu^{-1}$, also $y \in xU$.

(c). Dies gilt bekanntlich für jede Äquivalenzrelation (siehe 2.4.3). □

DEFINITION (Index einer Untergruppe). Für eine Menge M bezeichnen wir mit $|M|$ die Anzahl der Elemente von M ($|M| = \infty$ ist zugelassen). Sei nun G eine Gruppe und $U \subseteq G$ eine Untergruppe.

$$[G\colon U] := |G/U| \quad \text{heißt } \textit{Index} \text{ von } U \text{ in } G.$$

$[G\colon U]$ gibt die Anzahl der Linksnebenklassen an.

SATZ (Lagrange). *Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann gilt*

$$|G| = |U| \cdot [G\colon U].$$

BEWEIS. Falls $|U| = \infty$, so gilt die Behauptung. Falls $|U| < \infty$, genügt es zu zeigen $|xU| = |U|$ für alle $x \in G$ (mit Teil (c) des obigen Lemmas folgt dann die Behauptung). Betrachte die Abbildungen

$$\begin{aligned} \hat{x}\colon U &\to xU & \bar{x}\colon xU &\to U, \\ \hat{x}(u) &= xu & \bar{x}(v) &= x^{-1}v. \end{aligned}$$

($\bar{x}$ ist wohldefiniert, denn aus $v \in xU$ folgt $x^{-1}v \in U$). Dann ist $\bar{x} \circ \hat{x} = \mathrm{id}_U$ und $\hat{x} \circ \bar{x} = \mathrm{id}_{xU}$. Also ist $\hat{x}$ bijektiv, und damit $|xU| = |U|$. □

KOROLLAR (Kleiner Fermatscher Satz). *Sei G eine endliche Gruppe. Dann gilt für alle $x \in G$*

$$x^{|G|} = e.$$

BEWEIS. Sei $x \in G$ beliebig, aber fest gewählt. $U := \{\, x^n \mid n \in \mathbf{N} \,\}$ ist abelsche Untergruppe von G, da $U \neq \emptyset$ und $x^n x^m = x^{n+m} \in U$. (Untergruppenkriterium für endliche Gruppen). Es gilt $x^{|U|} = e$, denn

$$\begin{aligned} \prod_{y \in U} (xy) &= x^{|U|} \prod_{y \in U} y && \text{da } U \text{ abelsch,} \\ \prod_{y \in U} (xy) &= \prod_{y \in U} y, && \text{da } \hat{x}\colon U \to U,\ \hat{x}(y) = xy \text{ bijektiv ist.} \end{aligned}$$

Also folgt $x^{|G|} = x^{|U| \cdot [G\colon U]} = (x^{|U|})^{[G\colon U]} = e$. □

4.2.7. Zyklische Gruppen.

DEFINITION. Sei $(G, \circ)$ eine Gruppe. G heißt *zyklisch*, wenn es ein $x \in G$ gibt mit $G = \{\, x^i \mid i \in \mathbf{Z} \,\} =: \langle x \rangle$. x^i bedeutet dabei $\hat{x} \circ \hat{x} \circ \cdots \circ \hat{x}$ (i-mal),wobei

$$\hat{x} = \begin{cases} x & \text{für } i \geq 0, \\ x^{-1} & \text{für } i < 0. \end{cases}$$

BEISPIELE. (a) $\mathbf{Z}$ ist zyklisch, denn $\mathbf{Z} = \langle 1 \rangle$.
(b) $n\mathbf{Z} := \{\, nx \mid x \in \mathbf{Z} \,\}$ ($n \in \mathbf{N}$) ist ebenfalls zyklisch, denn $n\mathbf{Z} = \langle n \rangle$.
(c) $\mathbf{Z}_n := \{0, 1, \ldots, n-1\}$ ($n \in \mathbf{N}$, $n > 0$) mit der Addition modulo n als Gruppenverknüpfung ist zyklisch, denn $\mathbf{Z}_n = \langle 1 \rangle$.

Wir wollen jetzt die Untergruppen von $\mathbf{Z}$ bestimmen. Dafür benötigen wir eine Übertragung des Satzes von der Division mit Rest auf $\mathbf{Z}$.

SATZ (Division mit Rest für $\mathbf{Z}$). *Seien $i \in \mathbf{Z}$ und $n \in \mathbf{N}$ gegeben mit $0 < n$. Dann gibt es eindeutig bestimmte $q, r \in \mathbf{Z}$ mit*

$$i = nq + r \quad \textit{und} \quad 0 \leq r < n.$$

BEWEIS. *Existenz.* Für ganze Zahlen $i \geq 0$ folgt dies unmittelbar aus dem Satz von der Division mit Rest für $\mathbf{N}$. Sei nun $i < 0$. Nach dem Satz von der Division mit Rest für $\mathbf{N}$ hat man $-i = nq + r$ mit $q, r \in \mathbf{N}$ und $r < n$. Im Fall $r = 0$ ist $i = n(-q)$, und im Fall $r > 0$ hat man $-i = nq + r = n(q+1) \dot{-} (n \dot{-} r)$, also $i = n(-(q+1)) + (n - r)$.

Eindeutigkeit. Hier läßt sich der Beweis für $\mathbf{N}$ leicht übertragen. □

Ebenfalls benötigen wir das „Prinzip vom kleinsten Element", das sich leicht aus der Wertverlaufsinduktion ergibt. Man beachte, daß der hierbei verwendete Existenzquantor im schwachen Sinn zu verstehen sind (siehe 2.3.4): $\tilde{\exists}_n A(n)$ ist also *definiert* durch $\neg\forall_n\neg A(n)$.

SATZ (Prinzip vom kleinsten Element).

$$\tilde{\exists}_n A(n) \to \tilde{\exists}_n\big(A(n) \wedge \forall_{m<n}\neg A(m)\big).$$

BEWEIS. Ausgeschrieben lautet die Behauptung

$$\neg\forall_n\neg A(n) \to \neg\forall_n\neg\big(A(n) \wedge \forall_{m<n}\neg A(m)\big).$$

Wegen der Herleitbarkeit von $(D \to \neg C) \leftrightarrow \neg(C \wedge D)$ genügt

$$\neg\forall_n\neg A(n) \to \neg\forall_n\big(\forall_{m<n}\neg A(m) \to \neg A(n)\big).$$

Wegen der Herleitbarkeit von $(C \to D) \to \neg D \to \neg C$ genügt auch

$$\forall_n\big(\forall_{m<n}\neg A(m) \to \neg A(n)\big) \to \forall_n\neg A(n).$$

Setzen wir $B(n) := \neg A(n)$, so lautet unsere Behauptung

$$\forall_n\big(\forall_{m<n} B(m) \to B(n)\big) \to \forall_n B(n), \quad \text{also}$$
$$\mathrm{Prog}_n B(n) \to \forall_n B(n).$$

Dies ist aber gerade das Prinzip der Wertverlaufsinduktion für $B(n)$. □

SATZ (Bestimmung der Untergruppen von $\mathbf{Z}$). *Die Untergruppen von* $\mathbf{Z}$ *sind genau alle* $n\mathbf{Z}$, $n \in \mathbf{N}$.

BEWEIS. Alle $n\mathbf{Z}$ sind offenbar Untergruppen von $\mathbf{Z}$. Sei nun $U \subseteq \mathbf{Z}$ eine Untergruppe von $\mathbf{Z}$. Zu zeigen ist

$$\tilde{\exists}_{n\in\mathbf{N}}\, U = n\mathbf{Z}.$$

Sei o.B.d.A. $U \neq \{0\}$ (sonst setze $n := 0$). Sei n die kleinste positive Zahl in U (da U Untergruppe ist, existieren positive Zahlen in U). Dann gilt $U = n\mathbf{Z}$. Begründung: Da $n \in U$ und U Untergruppe, gilt $n\mathbf{Z} \subseteq U$. Sei nun $x \in U$. Es existieren $s \in \mathbf{Z}$ und $r \in \{0, \ldots, n-1\}$ mit $x = s \cdot n + r$. Daraus folgt $r = x - s \cdot n \in U$, also $r = 0$ nach Wahl von n. Damit ist auch $x = s \cdot n \in n\mathbf{Z}$ und folglich $U \subseteq n\mathbf{Z}$, insgesamt also $U = n\mathbf{Z}$. □

SATZ (Bestimmung der zyklischen Gruppen). *Sei G zyklische Gruppe. Dann gilt*

$$G \cong \mathbf{Z} \text{ oder } G \cong \mathbf{Z}_n \text{ für ein } n \in \mathbf{N},\ n > 0.$$

BEWEIS. Sei G eine zyklische Gruppe und $G = \langle x \rangle = \{ x^i \mid i \in \mathbf{Z} \}$. Betrachte die Abbildung

$$f\colon \mathbf{Z} \to \langle x \rangle, \quad f(i) = x^i.$$

f ist Homomorphismus, da $x^{i+j} = x^i \cdot x^j$. f ist auch surjektiv, denn es gilt $f(\mathbf{Z}) = \{ x^i \mid i \in \mathbf{Z} \} = \langle x \rangle$.

Fall $\mathrm{Kern}(f) = \{0\}$. Nach Teil (c) des Lemmas in 4.2.4 ist f dann injektiv, also bijektiv, und damit gilt $\mathbf{Z} \cong \langle x \rangle$.

Fall $\mathrm{Kern}(f) \neq \{0\}$. Da $\mathrm{Kern}(f)$ Untergruppe von $\mathbf{Z}$ ist, existiert nach dem vorigen Satz ein $n > 0$ mit $\mathrm{Kern}(f) = n\mathbf{Z}$. Damit folgt $x^n = e$ und $x^m \neq e$ für alle $m \in \{1, \ldots, n-1\}$. Nun sind alle x^i für $i \in \{0, \ldots, n-1\}$ verschieden (denn für $0 \leq r < s < n$ ist $0 < s - r < n$, also $x^{s-r} \neq e$ und damit $x^r \neq x^s$). Also ist $\langle x \rangle = \{x^0, x^1, \ldots, x^{n-1}\}$. □

DEFINITION. Sei G eine Gruppe und $x \in G$. Dann heißt

$$\mathrm{ord}(x) := \begin{cases} \text{kleinstes } n > 0 \text{ mit } x^n = e & \text{falls eines existiert,} \\ \infty & \text{sonst} \end{cases}$$

die *Ordnung* von x.

SATZ. *Sei G eine endliche Gruppe und $x \in G$. Dann ist* $\mathrm{ord}(x)$ *Teiler der Gruppenordnung $|G|$. Ist $|G|$ eine Primzahl, so ist G zyklisch.*

BEWEIS. $\langle x \rangle$ ist eine Untergruppe von G. Mit dem Satz von Lagrange folgt, daß $|\langle x \rangle|$ ein Teiler von $|G|$ ist, und es ist $|\langle x \rangle| = \mathrm{ord}(x)$. Falls $|G|$ Primzahl ist, so ist demnach $\mathrm{ord}(x) = |G|$ für alle $x \neq e$. Damit ist G zyklisch. □

SATZ. *Jede Untergruppe und jedes homomorphe Bild einer zyklischen Gruppe ist zyklisch.*

BEWEIS. Sei G zyklisch, etwa $G = \langle x \rangle$.

(a). Sei $U \subseteq G$ Untergruppe. Es existiert ein minimales $n > 0$ mit $x^n \in U$. Dann gilt $U = \langle x^n \rangle$.

(b). Sei H eine weitere Gruppe und $f\colon G \to H$ ein Homomorphismus. Dann gilt $f(G) = \langle f(x) \rangle$. □

4.2.8. Normalteiler. Ist G eine Gruppe und $U \subseteq G$ eine Untergruppe, so trägt G/U im allgemeinen noch keine Gruppenstruktur. Um dies zu erreichen, benötigen wir eine weitere Eigenschaft von U, daß nämlich U ein Normalteiler ist.

DEFINITION. Eine Untergruppe N einer Gruppe G heißt *Normalteiler*, wenn für alle $x \in G$ gilt

$$xN = Nx,$$

wobei $xN := \{ xy \mid y \in N \}$ und $Nx := \{ yx \mid y \in N \}$.

LEMMA. *Sei G eine Gruppe und $U \subseteq G$ eine Teilmenge. U ist genau dann Normalteiler von G, wenn U eine Untergruppe von G ist und für alle $x \in G$ und $y \in U$ auch $xyx^{-1} \in U$ ist.*

BEWEIS. $\rightarrow$. Aus $xU = Ux$ folgt $xyx^{-1} \in U$. $\leftarrow$. Für alle $x \in G$ gilt $xU \subseteq Ux$. Damit hat man auch $x^{-1}U \subseteq Ux^{-1}$, woraus $Ux \subseteq xU$ folgt. Also ist $xU = Ux$. □

LEMMA. *Seien G, H Gruppen, $f\colon G \to H$ ein Gruppenhomomorphismus. Ist V Normalteiler von H ist, so ist $f^{-1}(V)$ Normalteiler von G.*

BEWEIS. Sei $x \in G$ und $y \in f^{-1}(V)$. Dann gilt

$$f(xyx^{-1}) = f(x)f(y)f(x)^{-1} \in V,$$

da $f(y) \in V$ und V Normalteiler ist. Also ist $xyx^{-1} \in f^{-1}(V)$. □

BEMERKUNG. Sei U Normalteiler in G und $f\colon G \to H$ ein Gruppenhomomorphismus. Dann muß $f(U)$ nicht Normalteiler in H sein. Ist nämlich $G \subseteq H$ Untergruppe, aber kein Normalteiler, und $f\colon G \to H$ die Einbettung von G nach H, so ist $f(G) = G$ kein Normalteiler in H, obwohl G Normalteiler in G ist.

4.2.9. Faktorgruppen. Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler. Wir konstruieren die Faktorgruppe G/N, zusammen mit dem natürlichen (oder „kanonischen“) Gruppenhomomorphismus $\mathrm{id}\colon G \to G/N$. Es zeigt sich, daß hierfür die Eigenschaft von N, Normalteiler zu sein, notwendig ist. Als einfache Folgerung erhalten wir eine Charakterisierung von Normalteilern als Kerne von Gruppenhomomorphismen. Wir beweisen dann die universelle Eigenschaft von Faktorgruppen und als Folgerung den Homomorphiesatz.

DEFINITION. Sei $(G, \cdot)$ eine Gruppe und $N \subseteq G$ ein Normalteiler. Die *Faktorgruppe* G/N ist $(G, \cdot, \sim_N)$, wobei $(x \sim_N y) := (x^{-1}y \in N)$.

SATZ (Konstruktion der Faktorgruppe). *Sei G eine Gruppe und $N \subseteq G$ Normalteiler. Wir betrachten die* kanonische Abbildung

$$\mathrm{id}\colon G \to G/N, \quad x \mapsto x.$$

Auf G/N gibt es genau eine Gruppenstruktur, so daß $\mathrm{id}\colon G \to G/N$ *ein Gruppenhomomorphismus wird. In diesem Fall gilt* $\mathrm{Kern}(\mathrm{id}) = N$.

BEWEIS. *Existenz.* Wir müssen zeigen, daß die Gruppenverknüpfung von G mit $\sim_N$ verträglich ist. Seien also $x, \hat{x}, y, \hat{y} \in G$ mit $x \sim_N \hat{x}$ und $y \sim_N \hat{y}$. Zu zeigen ist $xy \sim_N \hat{x}\hat{y}$. Dies folgt aus

$$\begin{aligned}(xy)^{-1}(\hat{x}\hat{y}) &= y^{-1}\underbrace{x^{-1}\hat{x}}_{\in N}\hat{y} \\ &= y^{-1}\hat{y}n && \text{für ein } n \in N \text{ wegen } N\hat{y} = \hat{y}N, \\ &\in Nn && \text{wegen } y \sim_N \hat{y} \\ &\subseteq N.\end{aligned}$$

id ist offenbar Gruppenhomomorphismus. Ferner gilt $\mathrm{Kern}(\mathrm{id}) = N$, denn $x \sim_N e \leftrightarrow x^{-1}e \in N \leftrightarrow x \in N$.

Eindeutigkeit. Eine Verknüpfung $\circ$ auf G/N, bezüglich derer id Gruppenhomomorphismus ist, muß die Bedingung $\mathrm{id}(xy) \sim_N \mathrm{id}(x) \circ \mathrm{id}(y)$ erfüllen, also $xy \sim_N x \circ y$. □

KOROLLAR. *Sei G eine Gruppe und $N \subseteq G$ Untergruppe. Dann ist N Normalteiler von G genau dann, wenn es eine Gruppe H und einen Gruppenhomomorphismus $f\colon G \to H$ gibt mit $N = \mathrm{Kern}(f)$.*

BEWEIS. $\to$ folgt aus dem eben bewiesenen Satz.
$\leftarrow$. Es ist $N = \mathrm{Kern}(f) = f^{-1}(\{e\})$, und $\{e\}$ ist Normalteiler. □

KOROLLAR. *Sei G eine Gruppe, $N \subseteq G$ Untergruppe und die kanonische Abbildung* $\mathrm{id}\colon G \to G/N$ *Gruppenhomomorphismus bzgl. irgendeiner (fest gewählten) Gruppenstruktur auf G/N. Dann ist N Normalteiler.*

BEWEIS. Es ist $\mathrm{id}(e) = e$ neutrales Element in G/N, da id Gruppenhomomorphismus ist. Ferner ist

$$\mathrm{Kern}(\mathrm{id}) = \{\, x \in G \mid x \sim_N e \,\} = N.$$

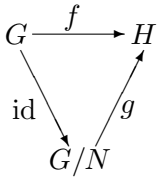
Also ist N Normalteiler, denn dies gilt stets für Kerne von Gruppenhomomorphismen. □

BEISPIEL. Sei $G = \mathbf{Z}$ und $N = n\mathbf{Z}$, etwa $n = 4$. Wir betrachten $\mathbf{Z}/4\mathbf{Z} := (\mathbf{Z}, +, \sim_{4\mathbf{Z}})$ und schreiben wie üblich $x \equiv y \mod 4$ oder auch $x \equiv y(4)$ anstelle von $x \sim_{4\mathbf{Z}} y$. Dann hat man

$$\begin{aligned}2 + 3 \equiv 5 \equiv 1 \mod 4, \\ -1 \equiv 3 \mod 4.\end{aligned}$$

SATZ (Universelle Eigenschaft der Faktorgruppe). *Seien G, H Gruppen, $N \subseteq G$ Normalteiler und $f\colon G \to H$ Gruppenhomomorphismus mit $N \subseteq \mathrm{Kern}(f)$. Dann gibt es genau einen Gruppenhomomorphismus $g\colon G/N \to H$*

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

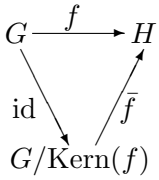


BEWEIS. *Existenz.* Für $x \in G$ definieren wir $g(x) := f(x)$. g ist wohldefiniert, denn für $x, y \in G$ mit $x \sim_N y$ gilt

$$\begin{aligned} &y^{-1}x \in N \\ &x = yn \quad \text{für ein } n \in N \\ &f(x) = f(yn) = f(y)\underbrace{f(n)}_{=e} = f(y). \end{aligned}$$

Eindeutigkeit. Für eine Abbildung g mit den gewünschten Eigenschaften muß gelten $g(x) = (g \circ \mathrm{id})(x) = f(x)$ für alle $x \in G$. □

KOROLLAR (Homomorphiesatz). *Seien G, H Gruppen, $f\colon G \to H$ surjektiver Gruppenhomomorphismus und* $\mathrm{id}\colon G \to G/\mathrm{Kern}(f)$ *die kanonische Abbildung. Dann gibt es genau eine Abbildung $\bar{f}\colon G/\mathrm{Kern}(f) \to H$ mit $\bar{f} \circ \mathrm{id} = f$. Dieses eindeutig bestimmte $\bar{f}$ ist ein Isomorphismus.*



BEWEIS. Nach dem Satz ist $\bar{f}$ ein wohldefinierter Gruppenhomomorphismus. $\bar{f}$ ist surjektiv, denn zu jedem $y \in H$ gibt es ein $x \in G$ mit $y = f(x) = \bar{f}(x)$. $\bar{f}$ ist injektiv, denn für $x \in G$ mit $\bar{f}(x) = e$ gilt $f(x) = \bar{f}(x) = e$, also $x \in \mathrm{Kern}(f)$ und damit $x \sim_{\mathrm{Kern}(f)} e$. □

4.3. Ringe

4.3.1. Z als kommutativer Ring mit Eins.

LEMMA. *Für alle $i, j, k \in \mathbf{Z}$ gilt*

(a) $(ij)k = i(jk)$;
(b) $i(j + k) = (ij) + (ik)$;
(c) $1 \cdot i = i$;
(d) $ij = ji$;
(e) $ij = 0 \to i = 0 \vee j = 0$.

BEWEIS. Alle diese Eigenschaften beweist man (leicht aber mühsam) durch Fallunterscheidungen. □

Wir führen wieder einen Abstraktionsschritt durch und definieren den allgemeinen Ringbegriff.

4.3.2. Definition und einfache Eigenschaften von Ringen.

DEFINITION. Sei A eine Menge und $+\colon A \to A \to A$, $\cdot\colon A \to A \to A$ Abbildungen. A (oder genauer $(A, +, \cdot)$) heißt *Ring*, wenn gilt

(a) $(A, +)$ ist eine abelsche Gruppe.
(b) $x(yz) = (xy)z$ für alle $x, y, z \in A$.
(c) $x(y + z) = (xy) + (xz)$ und $(x + y)z = (xz) + (yz)$ für alle $x, y, z \in A$.

A heißt *kommutativ*, wenn $xy = yx$ für alle $x, y \in A$. Ein Element $1 \in A$ heißt *Einselement* von A, wenn für alle $x \in A$ gilt $1x = x1 = x$.

Zur Vereinfachung beschränken wir uns meistens auf kommutative Ringe mit Eins.

BEZEICHNUNGEN. (a) „$\cdot$“ bindet stärker als „$+$“; beispielsweise steht $xy + xz$ für $(xy) + (xz)$.
(b) $x - y$ steht für $x + (-y)$.
(c) nx steht für $\underbrace{x + x + \cdots + x}_{n\text{-mal}}$, und x^n steht für $\underbrace{x \cdot x \cdot \cdots \cdot x}_{n\text{-mal}}$.

LEMMA. *Sei A ein kommutativer Ring mit 1. Dann besitzt A genau ein Einselement. (Beweis: Seien $1, 1^*$ Einselemente. Dann gilt $1 = 1 \cdot 1^* = 1^*$). Ferner gilt für alle $x, y \in A$:*

(a) $0 \cdot x = 0$
(b) $-x = (-1) \cdot x$
(c) $(-x) \cdot (-y) = xy$

BEWEIS. (a). $0x = (0 + 0)x = 0x + 0x$ und damit $0x = 0$.

(b). Es gilt $x + (-1)x = 1x + (-1)x = (1 + (-1))x = 0x = 0$, also $-x = (-1)x$.

(c). Es ist $1+(-1) = 0$ und damit $1(-1)+(-1)(-1) = 0$, also $(-1)(-1) = 1$. Daraus folgt $(-x)(-y) = (-1)x(-1)y = (-1)(-1)xy = xy$. □

BEISPIELE. (a). $(\mathbf{Z}, +, \cdot)$ ist ein kommutativer Ring mit 1.

(b). Sei A ein kommutativer Ring mit 1 und X eine nicht-leere Menge. Auf

$$A^X := \{\, f\colon X \to A \mid f \text{ Abbildung} \,\}$$

erklärt man $+, \cdot$ komponentenweise, also durch

$$(f + g)(x) := f(x) + g(x),$$
$$(f \cdot g)(x) := f(x) \cdot g(x)$$

für alle $x \in A$. Damit wird A^X zu einem kommutativen Ring mit 1. Einselement ist die Abbildung $X \to A$, $x \mapsto 1$.

(c). Sei $(G, +)$ eine abelsche Gruppe und $\mathrm{End}(G)$ die Menge aller Endomorphismen von G. Mit $+$ (übliche Addition) und $\circ$ (Hintereinanderausführung) wird $(\mathrm{End}(G), +, \circ)$ zwar ein Ring mit Einselement id_G, doch i.a. ist die Kommutativität *nicht* gegeben.

(d). Auch die Menge $\mathbf{Z}^{n\times n}$ der $n \times n$-Matrizen über den ganzen Zahlen mit der üblichen Addition und (Matrizen)-multiplikation ist ein Ring mit der Einheitsmatrix E als Einselement. Er ist für $n \geq 2$ *nicht* kommutativ.

(e). Seien $A_1, \ldots, A_n$ kommutative Ringe mit 1. Auf $A_1 \times \cdots \times A_n$ erkläre man $+, \cdot$ komponentenweise. Damit wird $A_1 \times \cdots \times A_n$ zu einem kommutativen Ring mit 1, dessen Einselement die Spalte aus lauter Einsen ist (*direktes Produkt* von $A_1, \ldots, A_n$).

(f). $\{0\}$ ist ein kommutativer Ring mit Einselement 0.

Definition. Sei A ein kommutativer Ring mit 1. Man nennt A einen *Integritätsbereich* (oder *Integritätsring*), wenn gilt

(a) $1 \neq 0$.
(b) A ist nullteilerfrei, d.h. für alle $x, y \in A$ folgt aus $xy = 0$ stets $x = 0$ oder $y = 0$.

Beispiele. (a). $(\mathbf{Z}, +, \cdot)$ ist ein Integritätsbereich.

(b). Sei A ein Integritätsbereich, X eine Menge mit mindestens zwei Elementen a und b. Dann ist A^X kein Integritätsbereich, denn betrachtet man die Abbildungen

$$f\colon X \to A, \qquad f(x) = \begin{cases} 0 & \text{falls } x = a \\ 1 & \text{falls } x = b \\ 0 & \text{sonst} \end{cases}$$

$$g\colon X \to A, \qquad g(x) = \begin{cases} 1 & \text{falls } x = a \\ 0 & \text{falls } x = b \\ 0 & \text{sonst,} \end{cases}$$

so gilt $f, g \neq 0$, aber $f \cdot g = 0$.

Definition. Seien A ein kommutativer Ring mit 1 und $U \subseteq A$ eine Teilmenge. U heißt *Unterring* mit 1 von A, wenn gilt

(a) $U \neq \emptyset$;
(b) $x + y, xy \in U$ für alle $x, y \in U$;
(c) U bildet zusammen mit den Abbildungen

$$U \to U \to U, \quad (x, y) \mapsto x + y \qquad U \to U \to U, \quad (x, y) \mapsto xy$$

einen kommutativen Ring mit 1.

DEFINITION. Seien A, B kommutative Ringe mit 1 und $f\colon A \to B$ eine Abbildung. f heißt *Homomorphismus* für Ringe, wenn für alle $x, y \in A$ gilt

(a) $f(x+y) = f(x) + f(y)$,
(b) $f(xy) = f(x)f(y)$,
(c) $f(1) = 1$.

Die Begriffe *Mono-, Iso-, Endo-* und *Automorphismus* erklärt man wie für Gruppen.

LEMMA. *Seien A, B kommutative Ringe mit 1 und $f\colon A \to B$ ein Ringhomomorphismus. Dann gilt*

(a) *Ist U Unterring von A, so ist $f(U)$ Unterring von B, und ist V Unterring von B, so ist $f^{-1}(V)$ Unterring von A.*
(b) *Sei wieder* $\mathrm{Kern}(f) := f^{-1}(0)$. *Dann ist* $\mathrm{Kern}(f) = \{0\}$ *genau dann, wenn f injektiv ist.*
(c) *f ist Isomorphismus genau dann, wenn ein Homomorphismus $g\colon B \to A$ existiert mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$.*

BEWEIS. (a). Nach einem Lemma über Gruppenhomomorphismen (in 4.2.5) sind $f(U)$ bzw. $f^{-1}(V)$ additive Untergruppen. Ferner folgt aus $f(1) = 1$ stets $1 \in f(U)$ bzw. $1 \in f^{-1}(V)$. Seien nun $x, y \in f(U)$. Dann existieren $u, v \in U$ so daß $x = f(u)$ und $y = f(v)$, und es gilt $xy = f(u)f(v) = f(uv) \in f(U)$. Seien $w, z \in f^{-1}(V)$. Dann gilt $f(wz) = f(w)f(z) \in V$, also $wz \in f^{-1}(V)$. Daher sind $f(U)$ und $f^{-1}(V)$ Unterringe von B bzw. A.

(b). Dies folgt direkt aus dem entsprechenden Lemma in 4.2.5 über Gruppenhomomorphismen.

(c). $\rightarrow$. $g := f^{-1}$ leistet das Verlangte. Wegen $f^{-1}(1) = 1$ bleibt nur zu zeigen $f^{-1}(x)f^{-1}(y) = f^{-1}(xy)$ für alle $x, y \in B$. Seien dazu $x, y \in B$ und $x = f(u), y = f(v)$ (wobei $u, v \in A$). Dann gilt

$$f^{-1}(x)f^{-1}(y) = uv = f^{-1}(f(uv)) = f^{-1}(f(u)f(v)) = f^{-1}(xy).$$

$\leftarrow$. Klar, da aus der Existenz von g die Bijektivität von f folgt. □

4.3.3. Ideale.

DEFINITION. Sei A ein kommutativer Ring mit 1 und $\mathfrak{a} \subseteq A$ eine Teilmenge. $\mathfrak{a}$ heißt *Ideal* von A, wenn gilt

(a) $\mathfrak{a}$ ist Untergruppe der additiven Gruppe von A.
(b) $A\mathfrak{a} \subseteq \mathfrak{a}$ (wobei $A\mathfrak{a} := \{\, yx \mid y \in A, x \in \mathfrak{a} \,\}$).

BEISPIELE. Sei A ein kommutativer Ring mit 1.

(a). $\{0\}$ und A sind Ideale von A (triviale Ideale).

(b). Ist $x \in A$, so ist $Ax := \{\, yx \mid y \in A \,\}$ ein Ideal von A.

(c). $\mathfrak{a}$ ist Ideal von $\mathbf{Z}$ genau dann, wenn ein $m \in \mathbf{N}$ existiert mit $\mathfrak{a} = m\mathbf{Z}$. Dies beweist man wie folgt. $\leftarrow$. Gilt nach (b). $\rightarrow$. $\mathfrak{a}$ ist eine Untergruppe

von $(\mathbf{Z}, +)$, also $\mathfrak{a} = m\mathbf{Z}$ nach dem Satz, in dem die Untergruppen von $\mathbf{Z}$ bestimmt wurden (in 4.2.7).

LEMMA. *Seien A, B kommutative Ringe mit 1 und $f\colon A \to B$ Ringhomomorphismus. Dann gilt*

(a) *Wenn $\mathfrak{b} \subseteq B$ Ideal von B ist, so ist auch $f^{-1}(\mathfrak{b})$ Ideal von A.*
(b) *Wenn $\mathfrak{a} \subseteq A$ Ideal von A ist und f surjektiv ist, so ist auch $f(\mathfrak{a})$ Ideal von B.*

BEWEIS. (a). Nach dem Lemma in 4.2.5 über Gruppenhomomorphismen ist $f^{-1}(\mathfrak{b})$ Untergruppe von $(A, +)$. Noch zu zeigen ist $Af^{-1}(\mathfrak{b}) \subseteq f^{-1}(\mathfrak{b})$. Seien dazu $y \in A$ und $x \in A$ mit $f(x) \in \mathfrak{b}$. Dann gilt $f(yx) = f(y)f(x) \in \mathfrak{b}$, da $f(x) \in \mathfrak{b}$ und $\mathfrak{b}$ ein Ideal ist. Damit folgt $yx \in f^{-1}(\mathfrak{b})$. (b). Nach dem Lemma über Gruppenhomomorphismen ist $f(\mathfrak{a})$ Untergruppe von $(B, +)$. Noch zu zeigen ist $Bf(\mathfrak{a}) \subseteq f(\mathfrak{a})$. Seien dazu $x \in \mathfrak{a}$ und $y \in B$. Da f surjektiv ist, existiert ein $z \in A$ mit $f(z) = y$. Dann gilt $yf(x) = f(z)f(x) = f(zx) \in f(\mathfrak{a})$, da $zx \in \mathfrak{a}$. □

4.3.4. Restklassenringe. Sei A ein kommutativer Ring mit 1 und $\mathfrak{a} \subseteq A$ ein Ideal. Wir konstruieren den Restklassenring $A/\mathfrak{a}$, zusammen mit dem natürlichen (oder „kanonischen“) Ringhomomorphismus $\mathrm{id}\colon A \to A/\mathfrak{a}$. Es zeigt sich, daß hierfür die Eigenschaft von $\mathfrak{a}$, Ideal zu sein, notwendig ist. Als einfache Folgerung erhalten wir eine Charakterisierung von Idealen als Kerne von Ringhomomorphismen. Wir beweisen dann die universelle Eigenschaft von Restklassenringen und als Folgerung den Homomorphiesatz.

DEFINITION. Sei $(A, +, \cdot)$ ein kommutativer Ring mit 1 und $\mathfrak{a} \subseteq A$ Ideal. Der *Restklassenring* $A/\mathfrak{a}$ ist $(A, +, \cdot, \sim_\mathfrak{a})$, wobei $(x \sim_\mathfrak{a} y) := (y - x \in \mathfrak{a})$.

SATZ (Konstruktion des Restklassenrings). *Sei A ein kommutativer Ring mit 1 und $\mathfrak{a} \subseteq A$ Ideal. Wir betrachten die* kanonische Abbildung

$$\mathrm{id}\colon A \to A/\mathfrak{a}, \quad x \mapsto x.$$

Auf $A/\mathfrak{a}$ gibt es genau eine Ringstruktur, so daß $\mathrm{id}\colon A \to A/\mathfrak{a}$ *ein Ringhomomorphismus wird. In diesem Fall gilt* $\mathrm{Kern}(\mathrm{id}) = \mathfrak{a}$.

BEWEIS. *Existenz.* $(A/\mathfrak{a}, +, \sim_\mathfrak{a})$ ist nach dem Satz über Faktorgruppen eine abelsche Gruppe. Wir müssen nur noch zeigen, daß die Ringmultiplikation von A mit $\sim_\mathfrak{a}$ verträglich ist. Seien also $x, \hat{x}, y, \hat{y} \in A$ mit $x \sim_\mathfrak{a} \hat{x}$ und $y \sim_\mathfrak{a} \hat{y}$. Zu zeigen ist $xy \sim_\mathfrak{a} \hat{x}\hat{y}$. Dies folgt aus

$$\hat{x}\hat{y} - xy = \hat{x}\hat{y} - x\hat{y} + x\hat{y} - xy = \underbrace{(\hat{x} - x)}_{\in\mathfrak{a}}\hat{y} + x\underbrace{(\hat{y} - y)}_{\in\mathfrak{a}} \in \mathfrak{a}.$$

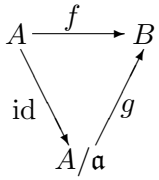
id ist offenbar Ringhomomorphismus. Ferner ist $\mathrm{Kern}(\mathrm{id}) = \mathfrak{a}$, denn es gilt $x \sim_\mathfrak{a} 0 \leftrightarrow 0 - x \in \mathfrak{a} \leftrightarrow x \in \mathfrak{a}$.

Eindeutigkeit. Für + ist dies klar nach dem Satz über Faktorgruppen. Eine Multiplikation $\circ$ auf $A/\mathfrak{a}$, bezüglich derer id Ringhomomorphismus ist, muß die Bedingung $\mathrm{id}(xy) \sim_{\mathfrak{a}} \mathrm{id}(x) \circ \mathrm{id}(y)$ erfüllen, also $xy \sim_{\mathfrak{a}} x \circ y$. □

KOROLLAR. *Sei A ein kommutativer Ring mit 1 und $\mathfrak{a} \subseteq A$ Teilmenge. $\mathfrak{a}$ ist Ideal genau dann, wenn $\mathfrak{a}$ Kern eines Ringhomomorphismus $f\colon A \to B$ ist.*

BEWEIS. $\to$ folgt aus dem eben bewiesenen Satz.
$\leftarrow$. Es ist $\mathfrak{a} = \mathrm{Kern}(f) = f^{-1}(\{0\})$, und $\{0\}$ ist Ideal. □

SATZ (Universelle Eigenschaft des Restklassenrings). *Seien A, B kommutative Ringe mit 1, $f\colon A \to B$ ein Ringhomomorphismus und $\mathfrak{a} \subseteq A$ ein Ideal mit $\mathfrak{a} \subseteq \mathrm{Kern}(f)$. Dann gibt es genau einen Ringhomomorphismus $g\colon A/\mathfrak{a} \to B$ mit $g \circ \mathrm{id} = f$.*



BEWEIS. Es ist nur noch zu zeigen, daß der aufgrund der Eigenschaften der Faktorgruppe eindeutig bestimmte Gruppenhomomorphismus g auch ein Ringhomomorphismus ist. Dies ist aber klar, denn $g(xy) = f(xy) = f(x)f(y) = g(x)g(y)$ und $g(1) = f(1) = 1$. □

KOROLLAR (Homomorphiesatz). *Seien A, B kommutative Ringe mit 1, $f\colon A \to B$ ein surjektiver Ringhomomorphismus und $\mathfrak{a} := \mathrm{Kern}(f)$. Dann gilt $A/\mathfrak{a} \cong B$.*

BEWEIS. Nach der universellen Eigenschafte des Restklassenrings existiert ein Homomorphismus $g\colon A/\mathfrak{a} \to B$. Er ist nach dem Homomorphiesatz für Gruppen bijektiv. □

4.3.5. Summe und Durchschnitt von Idealen. Wir zeigen, daß Summe und Durchschnitt von Idealen wieder Ideale ergeben. Auf diesem Wege ergibt sich ein nützlicher Zusammenhang zwischen den Begriffen des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen einerseits und dem Idealbegriff andererseits.

Zunächst stellen wir fest, daß man den in 3.2.2 eingeführten Begriff des größten gemeinsamen Teilers genauso wie früher auch für mehr als zwei Argumente definieren kann. Den Beweis der Existenz (Satz von Euklid) kann man dann leicht durch Induktion über die Anzahl der Argumente führen. Ebenso beweist man, daß $\mathrm{ggT}(x_1, \ldots, x_k)$ als eine Linearkombination von $x_1, \ldots, x_k$ geschrieben werden kann.

Einen anderen Zugang zum Begriff des größten gemeinsamen Teilers erhält man durch die Theorie der Ideale in einem Ring, und zwar in unserem Fall im Ring $\mathbf{Z}$ der ganzen Zahlen. Dieser Ring hat die besondere Eigenschaft, daß jedes Ideal von einem Ringelement erzeugt ist, sich also in der Form (x) schreiben läßt. Solche Ringe nennt man *Hauptidealringe*; viele unserer Betrachtungen lassen sich auf beliebige Hauptidealringe übertragen.

DEFINITION. Sei A ein kommutativer Ring mit 1.

(a) Für Ideale $\mathfrak{a}, \mathfrak{b} \subseteq A$ definiert man

$$\mathfrak{a} + \mathfrak{b} := \{ x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b} \}, \quad \mathfrak{a} \cap \mathfrak{b} := \{ x \mid x \in \mathfrak{a}, x \in \mathfrak{b} \}.$$

(b) Für eine Teilmenge $M \subseteq A$ sei

$$(M) := \{ x_1 a_1 + \cdots + x_n a_n \mid n \geq 0, a_1, \ldots, a_n \in M, x_1, \ldots, x_n \in A \}.$$

Wir schreiben $(a_1, \ldots, a_n)$ für$(\{a_1, \ldots, a_n\})$.

LEMMA. *Unter den Voraussetzungen der Definition gilt*

(a) $\mathfrak{a} + \mathfrak{b}$ *und* $\mathfrak{a} \cap \mathfrak{b}$ *sind Ideale von* A.
(b) (M) *ist das kleinste* M *umfassende Ideal von* A, *d.h. es gilt*
  (i) (M) *ist ein Ideal.*
  (ii) $(M) \supseteq M$.
  (iii) *Ist* $\mathfrak{a} \supseteq M$ *Ideal von* A, *so ist* $\mathfrak{a} \supseteq (M)$.
(c) *Für* $a, b \in A$ *ist* $(a) + (b) = (a, b)$.

BEWEIS. (a). Unter Benützung des Untergruppenkriteriums läßt sich leicht zeigen, daß $\mathfrak{a} + \mathfrak{b}$ und $\mathfrak{a} \cap \mathfrak{b}$ Untergruppen von $(A, +)$ sind. Seien nun $a \in A$, $w \in \mathfrak{a} + \mathfrak{b}$, $z \in \mathfrak{a} \cap \mathfrak{b}$. Dann existieren $x \in \mathfrak{a}$ und $y \in \mathfrak{b}$ so, daß $w = x + y$ und es gilt $aw = a(x + y) = ax + ay \in \mathfrak{a} + \mathfrak{b}$, da $ax \in \mathfrak{a}$ und $ay \in \mathfrak{b}$ ($\mathfrak{a}$ und $\mathfrak{b}$ sind Ideale), sowie $az \in \mathfrak{a} \cap \mathfrak{b}$, da $az \in \mathfrak{a}$ und $az \in \mathfrak{b}$. Damit folgt, daß $\mathfrak{a} + \mathfrak{b}$ und $\mathfrak{a} \cap \mathfrak{b}$ Ideale von A sind.

(b). Wieder folgt nach dem Untergruppenkriterium sofort, daß (M) Untergruppe von $(A, +)$ ist. Seien $a \in A$ und $x = x_1 a_1 + \cdots + x_n a_n \in (M)$. Dann folgt $ax = (ax_1)a_1 + \cdots + (ax_n)a_n \in (M)$, da $ax_i \in A$ für alle i, also ist (M) ein Ideal. $(M) \supseteq M$ ist klar. Sei $\mathfrak{a} \supseteq M$ Ideal von A. Dann folgt $\mathfrak{a} \supseteq AM (:= \{ yx \mid y \in A, x \in M \})$, da $\mathfrak{a}$ Ideal ist, und damit $\mathfrak{a} \supseteq (M)$, da $\mathfrak{a}$ Untergruppe von $(A, +)$ ist.

(c). Seien $a, b \in A$. Es gilt $(a) \subseteq (a, b)$ und $(b) \subseteq (a, b)$, also $(a) + (b) \subseteq (a, b)$, da (a, b) Untergruppe von $(A, +)$ ist. Nach (a) ist $(a) + (b)$ ein Ideal und damit $(a) + (b) \supseteq (a, b)$ nach (b). Also gilt $(a) + (b) = (a, b)$. □

BEISPIEL. Im Ring $\mathbf{Z}$ der ganzen Zahlen betrachten wir die Ideale (n), (m) mit $n, m \neq 0$. OBdA können wir $n, m > 0$ annehmen. Es gilt

(a) $(m) \supseteq (n)$ genau dann, wenn $m \mid n$ $(:= \exists_{q \in \mathbf{N}}\, mq = n)$.

(b) $(m)+(n)=(m,n)=(d)$ für ein eindeutig bestimmtes $d>0$ (nach dem Satz über die Untergruppen von $\mathbf{Z}$). (d) ist charakterisiert durch

$$(d)\supseteq(m),(n),$$
$$\forall_{q\in\mathbf{N}}\big((q)\supseteq(m),(n)\to(q)\supseteq(d)\big).$$

Also ist d charakterisiert durch

$$d\mid m,n,$$
$$\forall_{q\in\mathbf{N}}(q\mid m,n\to q\mid d).$$

Dieses d hatten wir den *größten gemeinsamen Teiler* von m und n genannt und ihn mit $\mathrm{ggT}(m,n)$ bezeichnet.

(c) $(m)\cap(n)=(v)$ für ein eindeutig bestimmtes $v>0$ (nach der Charakterisierung der Untergruppen von $\mathbf{Z}$). (v) ist charakterisiert durch

$$(m),(n)\supseteq(v),$$
$$\forall_{q\in\mathbf{N}}\big((m),(n)\supseteq(q)\to(v)\supseteq(q)\big).$$

Also ist v charakterisiert durch

$$m,n\mid v,$$
$$\forall_{q\in\mathbf{N}}(m,n\mid q\to v\mid q).$$

Dieses v hatten wir das *kleinste gemeinsame Vielfache* von m und n genannt und es mit $\mathrm{kgV}(m,n)$ bezeichnet.

4.4. Kongruenzen

In 4.2.3 hatten wir $\mathbf{Z}_m:=\{\,a\in\mathbf{N}\mid a<m\,\}$ als Beispiel einer endlichen abelschen Gruppe eingeführt; sie hieß die Gruppe der *ganzen Zahlen modulo* m. Die Gruppenverknüpfung ist die *Addition modulo* m, die für $a,b\in\mathbf{Z}_m$ definiert war als der (eindeutig bestimmte) Rest bei der Division von $a+b$ durch m. Genauso kann man die *Multiplikation modulo* m definieren, als den Rest bei der Division von ab durch m. Es ist leicht zu sehen, daß $\mathbf{Z}_m$ mit dieser Addition und Multiplikation einen kommutativen Ring mit Einselement bildet, und daß er isomorph ist zu dem Restklassenring $\mathbf{Z}/m\mathbf{Z}$. Die hierbei verwendete Äquivalenzrelation auf der Trägermenge $\mathbf{Z}$ nennt man Kongruenz modulo m. Wir wollen diesen Kongruenzbegriff jetzt genauer untersuchen; seine Bedeutung wurde zuerst von Gauß erkannt (Disquisitiones arithmeticae, 1801).

4.4.1. Charakterisierung der Kongruenz modulo m.

Lemma. *Für $a,b\in\mathbf{Z}$ und $m\in\mathbf{N}$, $m>0$ sind äquivalent*

(a) *a und b haben denselben Rest bei der Division durch m.*

(b) *$m\mid a-b$.*

BEWEIS. Seien $a = mp + r$ und $b = mq + s$ mit $p, q \in \mathbf{Z}$ und $r, s \in \mathbf{N}$, $r, s < m$. $\rightarrow$. Gelte $r = s$. Dann ist $a - b = m(p - q)$, also $m \mid a - b$. $\leftarrow$. Es ist $a - b = m(p - q) + (r - s)$. Aus $m \mid a - b$ folgt also $m \mid r - s$. Wegen $0 \leq r, s < m$ folgt $r = s$. □

Falls eine (und damit beide) des Bedingungen des Lemmas erfüllt sind, sagen wir, daß „a kongruent zu b modulo m“ ist. Dafür verwenden wir die Bezeichnung $a \equiv b \mod m$ (oder auch $a \equiv b(m)$ oder $a \equiv_m b$).

LEMMA. *Für $a, b, c, d \in \mathbf{Z}$ und $m \in \mathbf{N}$, $m > 0$ gelte $a \equiv b \mod m$ und $c \equiv d \mod m$. Dann gilt auch*

(a) $a + c \equiv b + d \mod m$,
(b) $-a \equiv -b \mod m$,
(c) $ac \equiv bd \mod m$.

BEWEIS. Übung. □

LEMMA. *Für $a, b \in \mathbf{Z}$ und $m, k \in \mathbf{N}$ mit $m > 0$ folgt aus $a \equiv b \mod m$ stets $a^{k+1} \equiv b^{k+1} \mod m$.*

BEWEIS. Man verwendet

$$
\begin{aligned}
&(a - b) \sum_{i=0}^{k} a^{k-i} b^i = \\
&a \sum_{i=0}^{k} a^{k-i} b^i - b \sum_{i=0}^{k} a^{k-i} b^i = \\
&a^{k+1} + \sum_{i=1}^{k} a^{k+1-i} b^i - \sum_{i=0}^{k-1} a^{k-i} b^{i+1} - b^{k+1} = \\
&a^{k+1} + \sum_{j=0}^{k-1} a^{k-j} b^{j+1} - \sum_{i=0}^{k-1} a^{k-i} b^{i+1} - b^{k+1} = a^{k+1} - b^{k+1}.
\end{aligned}
$$

Aus $m \mid (a - b)$ folgt also $m \mid (a^{k+1} - b^{k+1})$. □

Mit Hilfe dieser Eigenschaften der Kongruenz lassen sich anscheinend schwierige Fragen nach dem Rest einer großen Zahl modulo einer kleinen relativ leicht beantworten. Wichtig ist nur, daß man die gegebene große Zahle faktorisieren, also als Produkt hinreichend kleiner Zahlen darstellen kann. Eine Faktorisierung zufälliger großer Zahlen läßt sich allerdings auch mit modernen und leistungsfähigen Rechnern nicht in vernünftiger Zeit durchführen; auf der praktischen Unmöglichkeit der Faktorisierung beruhen die gängigen Verschlüsselungstechniken.

Als Beispiel betrachten wir das Problem, den Rest von 2^{16} bei der Division durch 11 zu bestimmen. Dazu stellen wir 2^{16} als Produkt $2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4$ dar. Wir verwenden jetzt, daß $2^4 \equiv 5 \mod 11$ ist, also $2^{16} \equiv 5^4 \mod 11$. Ferner ist $5^2 \equiv 3 \mod 11$, also $5^4 \equiv 3^2 \mod 11$. Insgesamt ergibt sich $2^{16} \equiv 9 \mod 11$.

4.4.2. Simultane Kongruenzen. Wir wollen uns überlegen, daß und wie sich ein System simultaner Kongruenzen mit teilerfremden Moduln immer lösen läßt. Ferner werden wir zeigen können, daß das Lösungsverfahren nützliche strukturelle Eigenschaften hat: es ist ein Ringisomorphismus. Davon werden wir im nächsten Abschnitt Gebrauch machen.

Satz (Chinesischer Restsatz). *Seien $m_1, \dots m_r$ teilerfremd, $m := \prod_i m_i$. Das System der Kongruenzen $x \equiv a_i \mod m_i$ hat eine „simultane“ Lösung; sie ist modulo m eindeutig bestimmt. Genauer gilt: Sei $q_i := \prod_{j \neq i} m_j$. Wähle y_i mit $1 \equiv q_i y_i \mod m_i$ und setze $e_i := q_i y_i$.*

(a) *Die Abbildung*

$$f\colon \mathbf{Z}_{m_1} \times \cdots \times \mathbf{Z}_{m_r} \to \mathbf{Z}_m, \quad (a_1, \dots, a_r) \mapsto a_1 e_1 + \cdots + a_r e_r$$

hat die Eigenschaft $f(a_1, \dots, a_r) \equiv a_i \mod m_i$.

(b) *f ist ein Ringisomorphismus.*

Beweis. Eindeutigkeit. Aus $x \equiv a_i \mod m_i$ und $x' \equiv a_i \mod m_i$ folgt $x - x' \equiv 0 \mod m_i$, also $x - x' \equiv 0 \mod m$.

Existenz. Zur Konstruktion von y_i mit $1 \equiv q_i y_i \mod m_i$ benutzt man, daß q_i und m_i teilerfremd sind, sich also 1 linear aus q_i und m_i kombinieren läßt. Für $e_i := q_i y_i$ erhält man

$$e_i \equiv 1 \mod m_i, \qquad e_i \equiv 0 \mod m_j \quad \text{für } i \neq j. \tag{4.1}$$

Also ist $a_1 e_1 + \cdots + a_r e_r \equiv a_i \mod m_i$. Damit ist auch (a) bewiesen.

b. Wir zeigen, daß f ein injektiver Ringhomomorphismus ist. Seien $(a_1, \dots, a_r), (b_1, \dots, b_r) \in \mathbf{Z}_{m_1} \times \cdots \times \mathbf{Z}_{m_r}$. Dann gilt

$$\begin{aligned} f(a_1, \dots, a_r) + f(b_1, \dots, b_r) &= a_1 e_1 + \cdots + a_r e_r + b_1 e_1 + \cdots + b_r e_r \\ &= (a_1 + b_1) e_1 + \cdots + (a_r + b_r) e_r \\ &= f(a_1 + b_1, \dots, a_r + b_r). \end{aligned}$$

Das heißt, daß f ein Gruppenhomomorphismus von der additiven Gruppe $(\mathbf{Z}_{m_1} \times \cdots \times \mathbf{Z}_{m_r}, +)$ in die additive Gruppe $(\mathbf{Z}_m, +)$ ist. Zum Beweis, daß f auch ein Ringhomomorphismus ist, beachte man $e_i^2 - e_i = (e_i - 1) e_i \equiv 0$

mod m wegen (4.1). Man erhält

$$\begin{aligned}
&f(a_1,\dots,a_r)\cdot f(b_1,\dots,b_r)\\
&=(a_1e_1+\cdots+a_re_r)\cdot(b_1e_1+\cdots+b_re_r)\\
&=\sum_{i,j}a_ib_je_ie_j\\
&\equiv\sum_i a_ib_ie_i^2 \mod m \quad \text{denn } e_ie_j\equiv 0 \mod m \text{ für } i\neq j \text{ nach (4.1)}\\
&\equiv\sum_i a_ib_ie_i \mod m \quad \text{denn } e_i^2\equiv e_i \mod m \text{ nach Vorbemerkung}\\
&=f(a_1b_1,\dots,a_rb_r).
\end{aligned}$$

Schließlich ist $\mathrm{Kern}(f)=0$, denn aus $f(a_1,\dots,a_r)\equiv 0 \mod m$ folgt $a_i\equiv 0 \mod m_i$ nach (a).

Damit ist gezeigt, daß f ein injektiver Ringhomomorphismus ist. f ist bijektiv, da $\mathbf{Z}_{m_1}\times\cdots\times\mathbf{Z}_{m_r}$ und $\mathbf{Z}_m$ dieselbe Anzahl von Elementen enthalten, nämlich m. Also ist f ein Ringisomorphismus. □

Beispiel. Sei $m_1:=3$, $m_2:=7$, $m_3:=11$. Dann ist $m:=m_1m_2m_3=231$. Ferner ist $q_1:=m_2m_3=77$, $q_2:=m_1m_3=33$ und $q_3:=m_1m_2=21$. Wir müssen y_i bestimmen mit $1\equiv q_iy_i \mod m_i$.

y_1 bestimmen wir aus $1\equiv 77y_1\equiv 2y_1 \mod 3$, also $y_1:=2$.

y_2 bestimmen wir aus $1\equiv 33y_2\equiv 5y_2 \mod 7$, also $y_2:=3$.

y_3 bestimmen wir aus $1\equiv 21y_3\equiv(-1)y_3 \mod 11$, also $y_3:=-1$.

Daraus ergibt sich $e_1:=q_1y_1=154$, $e_2:=q_2y_2=99$, $e_3:=q_3y_3=-21$. Eine Lösung etwa der simultanen Kongruenzen $x\equiv 1 \mod 3$, $x\equiv 2 \mod 7$, $x\equiv 6 \mod 11$ erhält man nach dem Satz wie folgt. Es ist $a_1=1$, $a_2=2$ und $a_3=6$. Eine Lösung ist also $a_1e_1+a_2e_2+a_3e_3=1\cdot 154+2\cdot 99-6\cdot 21=154+198-126=154+72=226$. Zur Kontrolle verifiziert man leicht $226\equiv 1 \mod 3$, $226\equiv 2 \mod 7$ und $226\equiv 6 \mod 11$.

Man beachte, daß das angegebene Lösungsverfahren besonders vorteilhaft ist, wenn mehrere Systeme von Kongruenzen nach denselben Moduln zu lösen sind. Die e_i hängen nämlich nicht von den a_i ab, müssen also nur einmal berechnet werden. Will man etwa noch die simultanen Kongruenzen $x\equiv 2 \mod 3$, $x\equiv 4 \mod 7$, $x\equiv -3 \mod 11$ lösen, so ist jetzt $a_1=2$, $a_2=4$ und $a_3=-3$. Eine Lösung ist also $a_1e_1+a_2e_2+a_3e_3=2\cdot 154+4\cdot 99+3\cdot 21=308+396+63=767$. Zur Kontrolle verifiziert man leicht $767\equiv 2 \mod 3$, $767\equiv 4 \mod 7$ und $767\equiv -3 \mod 11$.

4.4.3. Einheitengruppe; prime Reste modulo n. Wir betrachten jetzt die multiplikative Struktur des Rings $\mathbf{Z}/n\mathbf{Z}$, genauer seine Einheitengruppe. Sie ist auch unter dem Namen Gruppe der primen Reste modulo

n bekannt. Die Anzahl ihrer Elemente bezeichnet man mit $\varphi(n)$; diese Bezeichnung geht auf Euler zurück. Von besonderem Interesse ist der Fall, daß n eine Primzahl p ist. Dann sind alle Zahlen $1, 2, \ldots, p-1$ prime Reste modulo p, also $\varphi(p) = p-1$. Als Folgerung ergibt sich, daß für jede ganze Zahl $x \neq 0$ gilt $x^p \equiv x \mod p$.

Insbesondere besteht die Einheitengruppe des Rings $\mathbf{Z}/p\mathbf{Z}$ für eine Primzahl p aus allen von 0 verschiedenen Ringelementen. Solche Strukturen nennt man *Körper*; sie werden im nächsten Kapitel genauer untersucht.

Definition. Sei A ein kommutativer Ring mit 1. Dann heißt $u \in A$ *Einheit*, wenn es ein $v \in A$ gibt mit $vu = 1$. Die Menge der Einheiten von A wird mit A^* bezeichnet.

Zum Beispiel ist $\mathbf{Z}^* = \{1, -1\}$.

Lemma. *Sei A ein kommutativer Ring mit* 1. *Dann ist $(A^*, \cdot)$ eine Gruppe, die* Einheitengruppe *von A.*

Beweis. Dies folgt leicht aus der Gruppendefinition.

A^* ist abgeschlossen unter der Ringmultiplikation: Seien $u_1, u_2 \in A^*$. Dann haben wir $v_1, v_2 \in A$ mit $v_i u_i = 1$ für $i = 1, 2$. Es folgt $v_2 v_1 u_1 u_2 = v_2 u_2 = 1$, also $u_1 u_2 \in A^*$.

1 ist offenbar neutrales Element von A^*.

A^* ist abgeschlossen unter Inversenbildung: Sei $u \in A^*$. Dann haben wir ein $v \in A$ mit $vu = 1$. Jetzt folgt $v \in A^*$ aus $vu = uv = 1$. □

Satz. *Sei A ein Integritätsbereich und $a, b \in A$. Dann gilt $(a) = (b)$ genau dann, wenn es ein $u \in A^*$ gibt mit $a = ub$.*

Beweis. $\rightarrow$. Im Fall $a = b = 0$ ist die Behauptung trivial. Sei also oBdA $a \neq 0$. Wegen $a \in (b)$ gibt es ein $u \in A$ mit $a = ub$. Wegen $b \in (a)$ gibt es ein $v \in A$ mit $b = va$. Also ist $a = uva$ und deshalb $a(1 - uv) = 0$. Da A ein Integritätsbereich ist und $a \neq 0$, folgt $1 - uv = 0$ und somit $1 = uv$, also $u \in A^*$.

$\leftarrow$. Sei $a = ub$ mit $u \in A^*$. Es gilt $(a) = Aa = Aub \subseteq Ab = (b)$ und damit $(a) \subseteq (b)$. Analog hat man $(b) \subseteq (a)$, da $b = u^{-1}a$. □

Definition. Die Einheitengruppe $\mathbf{Z}_m^*$ von $\mathbf{Z}_m$ nennt man die *Gruppe der primen Reste modulo m.*

Definition. $\varphi(m) :=$ Anzahl der zu m teilerfremden $n \in \{1, \ldots, m-1\}$ (d.h. für die gilt $\mathrm{ggT}(m, n) = 1$) heißt *Eulersche φ-Funktion.*

Die Behandlung der Eulerschen φ-Funktion ordnet sich hier ein, da nach dem folgenden Satz $\varphi(n) = |\mathbf{Z}_n^*|$ gilt.

Satz (Euler-Funktion). *Sei $m \in \mathbf{N}$, $m > 0$. Dann gilt*

(a) $\mathbf{Z}_m^* = \{\, n \in \mathbf{Z}_m \mid m, n \text{ teilerfremd} \,\}$.
(b) $|\mathbf{Z}_m^*| = \varphi(m)$.
(c) *Sei* $m \in \mathbf{N}$, $n > 0$ *und* m, n *teilerfremd. Dann ist* $\varphi(mn) = \varphi(m)\varphi(n)$.
(d) $\varphi(p^r) = p^{r-1}(p-1)$ *für* p *Primzahl und* $r > 0$.

BEWEIS. (a). Sei $n \in \{\, 1, \ldots, m-1 \,\}$. Dann sind folgende Aussagen äquivalent:

$$\begin{aligned} & n \in \mathbf{Z}_m^* \\ & nq \equiv 1 \mod m \quad \text{für ein } q \in \mathbf{Z}_m \\ & \mathrm{ggT}(m, n) = 1. \end{aligned}$$

(b). Folgt aus (a) nach Definition der Eulerschen φ-Funktion.

(c). Seien $n, m > 0$ und teilerfremd. Nach (b) genügt es zu zeigen, daß $\mathbf{Z}_{mn}^* \cong \mathbf{Z}_m^* \times \mathbf{Z}_n^*$. (Hierbei ist das direkte Produkt von Gruppen gemeint: die Verknüpfung geschieht komponentenweise). Nach Teil (b) des chinesischen Restsatzes wissen wir bereits $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$. Zu zeigen bleibt $(\mathbf{Z}_m \times \mathbf{Z}_n)^* = \mathbf{Z}_m^* \times \mathbf{Z}_n^*$. Dies folgt aus der Äquivalenz der folgenden Aussagen.

$$\begin{aligned} & (x, y) \in (\mathbf{Z}_m \times \mathbf{Z}_n)^* \\ & (x, y) \cdot (x', y') = (1, 1) \quad \text{für geeignete } (x', y') \in \mathbf{Z}_m \times \mathbf{Z}_n \\ & xx' = 1 \text{ und } yy' = 1 \text{ für geeignete } x' \in \mathbf{Z}_m \text{ und } y' \in \mathbf{Z}_n \\ & (x, y) \in \mathbf{Z}_m^* \times \mathbf{Z}_n^*. \end{aligned}$$

(d). Betrachte

$$0 \ldots p \ldots 2p \ldots lp \ldots (l+1)p \ldots p^{r-1}p.$$

Es genügt zu zeigen, daß jedes m mit $lp < m < (l+1)p$ zu p teilerfremd ist. (Denn da es genau p^{r-1} Intervalle $\{\, m \mid lp < m < (l+1)p \,\}$ gibt und in jedem $p-1$ Elemente liegen, folgt daraus $\varphi(p^r) = p^{r-1}(p-1)$). Nehmen wir $p \mid m$ an. Dann folgt $m = kp$ für ein $k \in \mathbf{Z}$ und damit $lp < kp < (l+1)p$; dies ist aber nicht möglich. □

In 4.2.6 hatten wir den kleinen Fermatschen Satz bewiesen. Er sagte für eine beliebige endliche Gruppe G aus, daß für alle $x \in G$ gilt

$$x^{|G|} = e.$$

Wir wollen diesen allgemeinen gruppentheoretischen Satz jetzt auf die multiplikative Gruppe $\mathbf{Z}_m^*$ anwenden. Dadurch ergeben sich interessante zahlentheoretische Aussagen.

SATZ (Fermat). *Sei* p *eine Primzahl. Dann gilt* $x^{p-1} \equiv 1 \mod p$ *für jedes* $x \in \{1, \ldots, p-1\}$.

BEWEIS. Die multiplikative Gruppe $\mathbf{Z}_p^*$ der primen Reste modulo p hat genau $p-1$ Elemente, nämlich $\{1,\dots,p-1\}$. □

Eine unmittelbare Folgerung ist, daß für Primzahlen p gilt $x^p \equiv x \mod p$ für jedes $x \in \{1,\dots,p-1\}$. Da wir auch für beliebiges $m>0$ die Anzahl der Elemente der multiplikativen Gruppe $\mathbf{Z}_m^*$ bestimmt hatten, erhalten wir den allgemeineren Satz von Euler-Fermat:

SATZ (Euler-Fermat). *Sei $m>0$. Dann gilt $x^{\varphi(m)} \equiv 1 \mod m$ für jeden primen Rest x modulo m.*

4.4.4. Der Satz von Wilson. Als Anwendung der Gruppeneigenschaften von $\mathbf{Z}_m^*$, also der Gruppe der primen Reste modulo m, wollen wir ein nützliches Kriterium für die Primzahleigenschaft beweisen.

SATZ (Wilson). *Sei $p \in \mathbf{N}$, $p \geq 1$. Dann ist p Primzahl genau dann, wenn $(p-1)! \equiv -1 \mod p$ ist.*

BEWEIS. $\leftarrow$. Gelte $(p-1)! \equiv -1 \mod p$. Dann ist p Teiler von $(p-1)!+1$, und kein n mit $1<n<p$ ist Teiler von $(p-1)!+1$. Also ist p Primzahl.

$\rightarrow$. Für $p=2,3$ ist die Behauptung offenbar richtig. Sei also $p \geq 5$. Betrachte $\mathbf{Z}_p^* = \{1,2,\dots,p-1\}$, und ein beliebiges a darin. Es gibt dann ein eindeutig bestimmtes $a' \in \mathbf{Z}_p^*$ mit $aa' \equiv 1 \mod p$. Im Fall $a \equiv a' \mod p$ muß $a \equiv \pm 1 \mod p$ sein, denn aus $a \equiv a' \mod p$ folgt $p \mid a^2-1$, also $p \mid (a-1)(a+1)$. Aus den Gruppeneigenschaften von $\mathbf{Z}_p^*$ (insbesondere der Eindeutigkeit des Inversen) folgt, daß sich alle Elemente aus $\mathbf{Z}_p^* \setminus \{1, p-1\}$ zu $\frac{p-1}{2}$ Paaren a, a' mit $aa' \equiv 1 \mod p$ zusammenfassen lassen. Also ist

$$(p-1)! \equiv (+1)(-1)\prod aa' \equiv -1 \mod p. \qquad \square$$

4.5. Geordnete Integritätsbereiche

Wir definieren den Begriff eines geordneten Integritätsbereichs und zeigen, daß man die ganzen Zahlen charakterisieren kann als die in einem gewissen Sinn kleinste Erweiterung der natürlichen Zahlen zu einem geordneten Integritätsbereich.

4.5.1. Definition und einfache Eigenschaften geordneter Integritätsbereiche.

DEFINITION. Sei A eine Menge, $+,\cdot\colon A \to A \to A$ Abbildungen und $\leq \subseteq A \times A$. Dann heißt A (genauer $(A,+,\cdot,\leq)$) *geordneter Integritätsbereich*, wenn $(A,+,\cdot)$ Integritätsbereich ist und folgendes erfüllt ist.

(a) $(A,\leq)$ ist eine vollständige Ordnung, d.h., für alle $x,y,z \in A$ gilt

$$x \leq x \quad \text{(Reflexivität)},$$

$$x \leq y \to y \leq x \to x = y \quad \text{(Antisymmetrie)},$$
$$x \leq y \to y \leq z \to x \leq z \quad \text{(Transitivität)},$$
$$x \leq y \vee y \leq x \quad \text{(Vergleichbarkeit)}.$$

(b) $x \leq y \to x + z \leq y + z$ für alle $x, y, z \in A$.
(c) $x \leq y \to 0 \leq z \to xz \leq yz$ für alle $x, y, z \in A$.

LEMMA. *Sei A geordneter Integritätsbereich, $A^{0+} := \{\, x \in A \mid 0 \leq x \,\}$. Dann gilt für alle $x, y \in A$*

(a) $x \leq y \leftrightarrow y - x \in A^{0+}$;
(b) $x, y \in A^{0+} \to x + y, xy \in A^{0+}$;
(c) $x \in A^{0+} \vee -x \in A^{0+}$;
(d) $x \in A^{0+} \to -x \in A^{0+} \to x = 0$;
(e) $x^2 \in A^{0+}$;
(f) $1 \in A^{0+}$.

BEWEIS. (a). Folgende Aussagen sind äquivalent:

$$x \leq y$$
$$x - x \leq y - x$$
$$y - x \in A^{0+}.$$

(b). Seien $0 \leq x, y$. Zu $+$. Aus $0 \leq x$ folgt $0 + y \leq x + y$. Mit $0 \leq y$ und der Transitivität folgt $0 \leq x + y$. Zu $\cdot$. Aus $0 \leq x$ und $0 \leq y$ folgt $0 \cdot y \leq xy$, also $0 \leq xy$.

(c). Es gilt $0 \leq x \vee x \leq 0$, und aus $x \leq 0$ folgt $x - x \leq -x$, also $0 \leq -x$.

(d). Gelte $0 \leq x$ und $0 \leq -x$. Dann ist auch $x \leq 0$, und mit der Antisymmetrie folgt $x = 0$.

(e). Wir unterscheiden zwei Fälle gemäß (c). Im Fall $0 \leq x$ haben wir $0 = 0 \cdot x \leq x \cdot x$, und im Fall $0 \leq -x$ gilt $0 = 0 \cdot (-x) \leq (-x) \cdot (-x) = x^2$.

(f). Dies folgt aus (e). □

Die Teile (a)-(d) des Lemmas führen auf eine andere Charakterisierung geordneter Integritätsbereiche.

LEMMA. *Sei A Integritätsbereich und* $\mathrm{Nneg} \subseteq A$. *Für alle $x, y \in A$ gelte*

(a) $x, y \in \mathrm{Nneg} \to x + y, xy \in \mathrm{Nneg}$.
(b) $x \in \mathrm{Nneg} \vee -x \in \mathrm{Nneg}$.
(c) $x \in \mathrm{Nneg} \to -x \in \mathrm{Nneg} \to x = 0$.

Definiert man $x \leq y$ durch $y - x \in \mathrm{Nneg}$, so ist $(A, +, \cdot, \leq)$ ein geordneter Integritätsbereich (mit $A^{0+} = \mathrm{Nneg}$).

BEWEIS. Wir zeigen zunächst, daß $(A, \leq)$ eine vollständige Ordnung ist.

Reflexivität. Zu zeigen ist $x \leq x$, also $0 = x - x \in \text{Nneg}$. Dies folgt aber aus (b).

Antisymmetrie. Gelte $x \leq y$ und $y \leq x$, also $y-x \in \text{Nneg}$ und $-(y-x) = x - y \in \text{Nneg}$. Aus (c) folgt $x - y = 0$, also $x = y$.

Transitivität. Gelte $x \leq y$ und $y \leq z$, also $y-x \in \text{Nneg}$ und $z-y \in \text{Nneg}$. Aus (a) folgt $y - x + z - y = z - x \in \text{Nneg}$, also $x \leq z$.

Zu $x \leq y \to x + z \leq y + z$. Gelte $x \leq y$, also $y - x \in \text{Nneg}$. Wegen $y + z - (x + z) = y - x$ folgt $x + z \leq y + z$.

Zu $x \leq y \to 0 \leq z \to xz \leq yz$. Gelte $x \leq y$ und $0 \leq z$, also $y - x \in \text{Nneg}$ und $z \in \text{Nneg}$. Wegen (a) gilt dann $yz - xz = (y - x)z \in \text{Nneg}$. □

In einem beliebigen geordneten Integritätsbereich A kann man definieren $2 := 1 + 1$, $3 := 1 + 1 + 1$ etc. Wir schreiben $n1$ für $1 + 1 + \cdots + 1$ mit n Vorkommen von 1.

LEMMA. *In jedem geordneten Integritätsbereich A sind alle Elemente $n1$ ($n \in \mathbf{N}$) verschieden.*

BEWEIS. Sei etwa $n < m$ und $n1 = m1$. Dann gilt $(m - n)1 = 0$. Es genügt also zu zeigen, daß $(k + 1)1 \neq 0$ für alle $k \in \mathbf{N}$. Nehmen wir $(k+1)1 = 0$ an. Wegen $0 \leq k1$ ist $1 = 0+1 \leq (k+1)1$, also nach Annahme $1 \leq 0$. Mit $0 \leq 1$ folgt $0 = 1$, was nicht sein kann. □

Die natürlichen Zahlen lassen sich also in jeden geordneten Integritätsbereich einbetten. Insbesondere gestatten die Integritätsbereiche $\mathbf{Z}_p$ (p Primzahl) keine Ordnung.

4.5.2. Charakterisierung von Z. Wir betrachten die folgende Eigenschaft geordneter Integritätsbereiche A:

$$\forall_{x \in A} \exists_{n \in \mathbf{N}} (x = n1 \vee x = -n1). \tag{4.2}$$

Offenbar stellt diese Eigenschaft sicher, daß A „wie $\mathbf{Z}$ aussieht“. Insbesondere erfüllt $\mathbf{Z}$ (4.2).

Gezeigt werden soll, daß je zwei geordnete Integritätsbereiche mit der Eigenschaft (4.2) isomorph sind. Etwas allgemeiner gilt sogar:

SATZ. *Sei A ein geordneter Integritätsbereich mit der Eigenschaft* (4.2) *und A' ein beliebiger geordneter Integritätsbereich. In A' definieren wir*

$$U' := \{\, x \in A' \mid \exists_{n \in \mathbf{N}} (x = n1' \vee x = -n1') \,\}.$$

Dann gilt

(a) $A \cong U'$.

(b) *Hat A' die Eigenschaft* (4.2)*, so ist $U' = A$.*

BEWEIS. (b) ist klar. (a). Wir geben eine Beweisskizze. Man definiert eine Abbildung

$$f\colon A \to U'$$
$$f(x) := \begin{cases} n1' & \text{falls } \exists_{n\in\mathbf{N}}(x = n1) \\ -n1' & \text{falls } \exists_{n\in\mathbf{N}}(x = -n1). \end{cases}$$

f ist offenbar wohldefiniert, surjektiv und auch injektiv; die Injektivität folgt aus dem vorangehenden Lemma. Man zeigt dann leicht

$$f(x+y) = f(x) +' f(y),$$
$$f(x\cdot y) = f(x) \cdot' f(y),$$
$$x \le y \leftrightarrow f(x) \le' f(y).$$

Also ist f der gesuchte Isomorphismus. □

Man kann diesen Satz als eine Rechtfertigung ansehen, daß wir uns auf unser speziell konstruiertes $\mathbf{Z}$ konzentriert haben.

KAPITEL 5

Rationale Zahlen

Unser Ziel ist es, die ganzen Zahlen zu einem Bereich von „rationalen Zahlen“ zu erweitern, in dem eine Gleichung

$$a \cdot x = b \quad (a \neq 0)$$

stets lösbar ist.

Wir beginnen wieder mit einer konkreten Konstruktion der rationalen Zahlen, als einer mathematischen Struktur mit gewissen Operationen $+$, $\cdot$ und $\leq$. Wir stellen dann fest, daß in dieser Struktur eine Reihe von Eigenschaften gelten, die auch für viele andere Strukturen erfüllt sind. Dies führt uns auf den Begriff eines (geordneten) Körpers. Viele wichtige Eigenschaften der rationalen Zahlen werden in wir in dieser allgemeinen Form beweisen können. Wir zeigen dann, daß der Weg von den genzen Zahlen zu den rationalen ein Beispiel einer allgemeinen Konstruktion ist, die aus einem (geordneten) Integritätsbereich einen (geordneten) Körper herstellt, in den der Integritätsbereich eingebettet werden kann; man nennt ihn den Quotientenkörper. Er läßt sich durch einfache Eigenschaften charakterisieren.

5.1. Konstruktion der rationalen Zahlen

5.1.1. Der Typ Q der rationalen Zahlen. Eine rationale Zahl stellen wir dar als Paar einer ganzen Zahl i und einer positiven Zahl p. Den Typ $\mathbf{Q}$ der rationalen Zahlen definieren wir deshalb als

$$\mathbf{Q} := \mathbf{Z} \times \mathbf{P}.$$

Da wir zwei rationale Zahlen als gleich betrachten wollen, wenn sie denselben gekürzten Bruch darstellen, definieren wir eine Relation $\sim$ durch

$$\big((i_1, p_1) \sim (i_2, p_2)\big) := (i_1 p_2 = i_2 p_1).$$

Man sieht leicht, daß $\sim$ eine Äquivalenzrelation ist.

Die *Addition rationaler Zahlen* wird definiert durch

$$(i_1, p_1) + (i_2, p_2) := (i_1 p_2 + i_2 p_1, p_1 p_2).$$

Die Addition ist verträglich mit der Äquivalenzrelation $\sim$, d.h. aus $(i_1, p_1) \sim (i_1', p_1')$ und $(i_2, p_2) \sim (i_2', p_2')$ folgt $(i_1, p_1) + (i_2, p_2) \sim (i_1', p_1') + (i_2', p_2')$. Die

rationale Zahl *Null* wird dargestellt durch $(0,1)$; sie hat die Eigenschaft $(0,1)+(i_2,p_2)\sim(i_2,p_2)$ (es gilt sogar die Gleichheit). Das *Negative* (oder *additive Inverse*) einer rationalen Zahl ist

$$-(i_1,p_1):=(-i_1,p_1).$$

Die Bildung des Negativen ist wieder verträglich mit $\sim$: aus $(i_1,p_1)\sim(i_1',p_1')$ folgt $-(i_1,p_1)\sim-(i_1',p_1')$. Wir erhalten wie bei den ganzen Zahlen, daß die rationalen Zahlen zusammen mit der Addition eine abelsche Gruppe bilden.

Die *Multiplikation* rationaler Zahlen wird definiert durch

$$(i_1,p_1)\cdot(i_2,p_2):=(i_1i_2,p_1p_2).$$

Die rationale Zahl *Eins* wird dargestellt durch $(1,1)$; sie hat die Eigenschaft $(1,1)\cdot(i_2,p_2)\sim(i_2,p_2)$ (es gilt sogar die Gleichheit). Das *multiplikative Inverse* einer rationalen Zahl $(i_1,p_1)\not\sim(0,1)$ ist

$$(i_1,p_1)^{-1}:=\begin{cases}(p_1,i_1) & \text{falls } i_1>0\\ (-p_1,-i_1) & \text{falls } i_1<0.\end{cases}$$

Alle diese Operationen sind verträglich mit $\sim$. Wir erhalten wie bei den ganzen Zahlen, daß die rationalen Zahlen ohne die Null zusammen mit der Multiplikation eine abelsche Gruppe bilden. Ferner gilt das Distributivgesetz

$$(i_1,p_1)\cdot\big((i_2,p_2)+(i_2',p_2')\big)=\big((i_1,p_1)\cdot(i_2,p_2)\big)+\big((i_1,p_1)\cdot(i_2',p_2')\big).$$

Schließlich kann man noch eine Ordnung definieren durch

$$((i_1,p_1)\le(i_2,p_2)):=(i_1p_2\le i_2p_1).$$

Man überlegt sich leicht, daß $\mathbf{Q}$ damit zu einer vollständigen Ordnung wird.

Diese Eigenschaften beinhalten wieder alles das, was über die additive und multiplikative Struktur der rationalen Zahlen zu sagen ist. Wir führen einen Abstraktionsschritt durch und definieren den allgemeinen Begriff eines (geordneten) Körpers.

5.2. Körper, geordnete Körper

Man überprüft leicht, daß für die eben konkret definierten rationalen Zahlen viele erwartete Eigenschaften gelten. Wir können dies jetzt kurz formulieren, indem wir sagen, daß $\mathbf{Q}$ ein geordneter Integritätsbereich ist, in dem die Einheitengruppe aus allen von 0 verschiedenen Elementen besteht.

5.2.1. Definition und einfache Eigenschaften von Körpern.

Definition. Eine Struktur $\langle K,+,\cdot\rangle$ bzw. $\langle K,+,\cdot,\le\rangle$ heißt (geordneter) Körper, wenn sie ein (geordneter) Integritätsbereich ist, in dem die Einheitengruppe K^* aus allen von 0 verschiedenen Elementen besteht. Ihr neutrales Element wird mit 1, das zu $x\in K^*$ inverse Element mit x^{-1} bezeichnet.

BEISPIELE. $\mathbf{Q}$ mit der eben definierten Addition und Multiplikation ist ein Körper, aber $(\mathbf{Z}, +, \cdot)$ ist *keiner*.

DEFINITION. Sei K ein Körper und $k \subseteq K$ eine Teilmenge. k heißt Unterkörper von K, wenn folgendes gilt.

(a) Mit x und y liegen auch $x + y$ und xy in k.
(b) k bildet zusammen mit den induzierten Verknüpfungen

$$\begin{aligned} k \times k &\to k & k \times k &\to k \\ (x, y) &\mapsto x + y & (x, y) &\mapsto x \cdot y \end{aligned}$$

einen Körper.

Ein Paar (K, k) bestehend aus einem Körper K und einem Unterkörper k heißt *Körpererweiterung*. Schreibweise: $K \supseteq k$ statt (K, k).

BEMERKUNG (Unterkörperkriterium). Sei K ein Körper und $k \subseteq K$ eine Teilmenge. Dann ist k ein Unterkörper von K genau dann, wenn gilt

(a) k enthält mindestens zwei Elemente.
(b) $x - y \in k$ für alle $x, y \in k$.
(c) Für alle $x, y \in k$ mit $y \neq 0$ ist $xy^{-1} \in k$.

BEWEIS. $\to$. Dies folgt direkt aus der Definition von Unterkörpern.

$\leftarrow$. Aus Bedingung (b) folgt mit dem Untergruppenkriterium, daß $(k, +)$ Untergruppe von $(K, +)$ ist. Nach Bedingung (a) gilt $k^* \neq \emptyset$, also folgt aus Bedingung (c), wieder mit dem Untergruppenkriterium, daß $(k^*, \cdot)$ Untergruppe von $(K^*, \cdot)$ ist. □

Das einfachste Beipiel eines Körpers ist $\mathbf{Z}_2$, also die Menge $\{0, 1\}$ mit folgender Multiplikation und Addition:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Durch Unterscheiden der endlich vielen Fälle kann man leicht verifizieren, daß alle Körperaxiome erfüllt sind. In $\mathbf{Z}_2$ (oft auch mit $\mathbb{F}_2$ bezeichnet) gilt $1 + 1 = 0$. Man kann also $1 + 1 \neq 0$ nicht für beliebige Körper beweisen.

Weitere wichtige Beispiele für Körper ergeben sich durch die folgende Konstruktion. Seien K ein Körper und $\xi \in K$ kein Quadrat in K (d.h. es gibt kein $x \in K$ mit $x^2 = \xi$). Wir wollen einen Körper $K \times K$ definieren. Stellt man sich (außerhalb der Legalität) (x, y) als $x + y\sqrt{\xi}$ vor, so liegt die folgende Definition nahe:

$$\begin{aligned} (x, y) + (x', y') &:= (x + x', y + y'), \\ (x, y) \cdot (x', y') &:= (xx' + yy'\xi, xy' + yx'). \end{aligned}$$

Wir wollen uns überlegen, daß $K \times K$ mit dieser Addition $+$ und Multiplikation $\cdot$ zu einem Körper wird. Man bezeichnet ihn mit $(K(\sqrt{\xi}), +, \cdot)$ oder kurz $K(\sqrt{\xi})$.

BEWEIS. Daß $(K(\sqrt{\xi}), +)$ eine abelsche Gruppe ist, ergibt sich leicht aus der komponentenweisen Definition der Addition. Das neutrale Element ist $(0,0)$, und das inverse Element zu $(x,y) \in K(\sqrt{\xi})$ ist $(-x,-y)$. Wir zeigen jetzt, daß $(K(\sqrt{\xi})^*, \cdot)$ eine abelsche Gruppe ist. Assoziativität und Kommutativität sind leicht nachzurechnen. Wir wollen zeigen, daß $(1,0)$ neutrales Element ist. Zu (a). Es gilt $(1,0)\cdot(x,y) = (x,y)$. Zu (b). Gegeben sei $(x,y) \neq (0,0)$. Gesucht ist (x',y') mit

$$(x',y')(x,y) = (1,0) \tag{5.1}$$

Ansatz: Nehmen wir an, wir hätten schon (x',y') mit (5.1). Multiplikation beider Seiten mit $(x,-y)$ ergibt

$$(x',y')(x^2 - y^2\xi, 0) = (x,-y).$$

Nun gilt $x^2 - y^2\xi \neq 0$, da ξ kein Quadrat ist und $(x,y) \neq (0,0)$. Also können wir definieren

$$x' := \frac{x}{x^2 - y^2\xi} \quad \text{und} \quad y' := \frac{-y}{x^2 - y^2\xi}.$$

Man verifiziert leicht (5.1). Die Distributivität ergibt sich durch Nachrechnen. □

LEMMA. *Sei K ein Körper, $x, z \in K$ und $y, u, v \in K^*$. Wir schreiben $\frac{x}{y}$ für $y^{-1}x$. Dann gilt*

(a) $\frac{x}{y} = 0 \leftrightarrow x = 0$.
(b) $\frac{x}{y} = \frac{z}{u} \leftrightarrow xu = zy$.
(c) $\frac{x}{y} = \frac{xv}{yv}$.
(d) $\frac{x}{y} + \frac{z}{u} = \frac{xu+yz}{yu}$.
(e) $\frac{x}{y} \cdot \frac{z}{u} = \frac{xz}{yu}$.
(f) $-\frac{x}{y} = \frac{-x}{y}$.
(g) $x \in K^* \to (\frac{x}{y})^{-1} = \frac{y}{x}$.

BEWEIS. (a). $\leftarrow$ ist klar. $\rightarrow$. Sei $\frac{x}{y} = 0$, also $y^{-1}x = 0$ und deshalb auch $0 = yy^{-1}x = x$. (b) und (c) sind klar. (d).

$$\frac{x}{y} + \frac{z}{u} = y^{-1}x + u^{-1}z = u^{-1}uy^{-1}x + y^{-1}yu^{-1}z = (yu)^{-1}(xu+yz) = \frac{xu+yz}{yu}.$$

(e) ist klar. (f). $\frac{x}{y} + \frac{-x}{y} = \frac{xy-xy}{y^2} = 0$. (g). Für $x \in K^*$ ist $\frac{x}{y} \cdot \frac{y}{x} = \frac{xy}{xy} = 1$.

(b). $\rightarrow$. Man multipliziere mit yu. $\leftarrow$. Man multipliziere mit $\frac{1}{y^2u^2}$. □

LEMMA. *Sei K ein geordneter Körper, $x, z \in K$ und $y, u \in K^*$. Dann gilt*

(a) $0 \leq \frac{x}{y} \leftrightarrow 0 \leq xy$.
(b) $\frac{x}{y} \leq \frac{z}{u} \leftrightarrow xuyu \leq yzyu$.
(c) $0 < yu \rightarrow (\frac{x}{y} \leq \frac{z}{u} \leftrightarrow xu \leq yz)$.
(d) $0 < u \leq y \rightarrow 0 < \frac{1}{y} \leq \frac{1}{u}$.

BEWEIS. (a). Stets gilt $0 \leq y^2$, und wegen $y \in K^*$ ist $y^2 \in K^*$. $\rightarrow$. Aus $0 \leq \frac{x}{y}$ und $0 \leq y^2$ folgt $0 \leq \frac{x}{y} \cdot y^2 = xy$. $\leftarrow$. Wegen $y \in K^*$ ist $\frac{1}{y} \in K^*$. Aus $0 \leq xy$ und $0 \leq \frac{1}{y^2}$ folgt $0 \leq \frac{xy}{y^2} = \frac{x}{y}$.

(b). $\rightarrow$. Man multipliziere mit yu. $\leftarrow$. Man multipliziere mit $\frac{1}{y^2u^2}$.

(c). Gelte $0 < yu$. $\rightarrow$. Man multipliziere mit yu. $\leftarrow$. Wegen $y, u \in K^*$ ist $\frac{1}{yu} \in K^*$, und nach (a) ist $0 \leq \frac{1}{yu}$. Man multipliziere mit $\frac{1}{yu}$.

(d). Gelte $0 < u \leq y$. Dann ist $0 \leq uy$. Die Behauptung folgt mit (a) und (c). $\leftarrow$. Gelte $0 < \frac{1}{y} \leq \frac{1}{u}$. Dann ist $0 \leq \frac{1}{uy}$. Die Behauptung folgt mit (a) und (c). □

LEMMA (Dichtheit). *Sei K ein geordneter Körper und $x, y \in K$ mit $x < y$. Dann gibt es ein $z \in K$ mit $x < z < y$.*

BEWEIS. Wir zeigen $x < \frac{x+y}{2} < z$. Wegen $x < y$ genügt $x \leq \frac{x+y}{2} \leq z$. Nach Teil (c) des vorherigen Lemmas folgt die erste Ungleichung aus $2x \leq x + x$ und die zweite aus $x + y \leq 2y$. □

Nachzutragen bleibt, daß für Primzahlen p stets $\mathbf{Z}_p$ ein Körper ist. Wir zeigen allgemeiner:

SATZ. *Jeder endliche Integritätsbereich ist ein Körper.*

BEWEIS. Sei A ein endlicher Integritätsbereich und $x \in A$, $x \neq 0$. Zu zeigen ist $x \in A^*$. Die Abbildung

$$f_x \colon A \to A, \quad y \mapsto xy$$

ist injektiv, denn aus $xy = xz$ folgt $x(y - z) = 0$, also $y = z$ wegen $x \neq 0$ und der Nullteilerfreiheit von A.. Da A endlich ist, muß f_x auch surjektiv sein. Also gibt es ein $y \in A$ mit $f_x(y) = xy = 1$, das heißt, daß $x \in A^*$. □

KOROLLAR. *Für Primzahlen p ist $\mathbf{Z}_p$ ein Körper.*

5.3. Quotientenkörper: Existenz und Eindeutigkeit

Die obige Konstruktion der rationalen Zahlen läßt sich allgemein für beliebige Integritätsbereiche durchführen. Genauer gilt:

SATZ (Konstruktion des Quotientenkörpers). *Sei A ein (geordneter) Integritätsbereich. Dann findet man einen (geordneten) Körper $Q(A)$ und eine isomorphe Einbettung $i\colon A \to Q(A)$ so daß sich jedes Körperelement in der Form $\frac{i(x)}{i(y)}$ mit $x, y \in A$, $y \neq 0$ darstellen läßt.*

BEWEIS. Wir definieren auf $Q(A) := \{\, (x,y) \mid x, y \in A, y \neq 0 \,\}$ eine Relation $\sim$ durch

$$\big((x_1,y_1) \sim (x_2,y_2)\big) := (x_1 y_2 = x_2 y_1).$$

Man sieht leicht, daß $\sim$ eine Äquivalenzrelation ist. Die *Addition* wird definiert durch

$$(x_1,y_1) + (x_2,y_2) := (x_1y_2 + x_2y_1, y_1y_2).$$

Sie ist verträglich mit der Äquivalenzrelation $\sim$, d.h. aus $(x_1,y_1) \sim (x_1',y_1')$ und $(x_2,y_2) \sim (x_2',y_2')$ folgt $(x_1,y_1)+(x_2,y_2) \sim (x_1',y_1')+(x_2',y_2')$. Die *Null* wird dargestellt durch $(0,1)$; sie hat die Eigenschaft $(0,1)+(x_2,y_2) \sim (x_2,y_2)$ (es gilt sogar die Gleichheit). Das *Negative* (oder *additive Inverse*) eines $(x,y) \in Q(A)$ ist

$$-(x,y) := (-x,y).$$

Die Bildung des Negativen ist wieder verträglich mit $\sim$: aus $(x,y) \sim (x',y')$ folgt $-(x,y) \sim -(x',y')$. Man zeigt leicht, daß $Q(A)$ mit der Addition eine abelsche Gruppe bildt.

Die *Multiplikation* wird definiert durch

$$(x_1,y_1) \cdot (x_2,y_2) := (x_1x_2, y_1y_2).$$

Die *Eins* wird dargestellt durch $(1,1)$; sie hat die Eigenschaft $(1,1)\cdot(x_2,y_2) \sim (x_2,y_2)$ (es gilt sogar die Gleichheit). Das *multiplikative Inverse* eines Elements $(x,y) \in Q(A)$ mit $(x,y) \not\sim (0,1)$ ist

$$(x,y)^{-1} := (y,x)$$

Alle diese Operationen sind verträglich mit $\sim$. Man zeigt leicht, daß die Einheitengruppe $Q(A)^*$ aus allen zu $(0,1)$ nicht äquivalenten Elementen besteht, und abelsch ist. Ferner gilt das Distributivgesetz

$$(x_1,y_1) \cdot \big((x_2,y_2) + (x_2',y_2')\big) = \big((x_1,y_1)\cdot(x_2,y_2)\big) + \big((x_1,y_1)\cdot(x_2',y_2')\big).$$

Schließlich kann man noch eine Ordnung definieren durch

$$((x_1,y_1) \leq (x_2,y_2)) := (x_1y_2y_1y_2 \leq x_2y_1y_1y_2).$$

Man überlegt sich leicht, daß $Q(A)$ damit zu einer vollständigen Ordnung wird.

Wir definieren eine Abbildung $i\colon A \to Q(A)$ durch $i(x) := (x,1)$. i ist offenbar injektiv, und es gilt

$$i(x+y) = i(x) + i(y), \quad i(x\cdot y) = i(x)\cdot i(y).$$

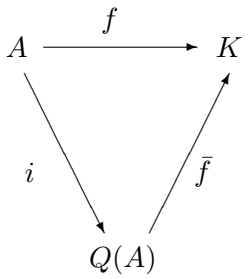
Ferner ist $(x,y) \sim \frac{(x,1)}{(y,1)}$, denn es gilt $(x,y)\cdot(y,1) \sim (x,1)$ wegen $(x,y)\cdot(y,1) = (xy,y)$.

Schließlich gilt noch $x \leq y \leftrightarrow i(x) \leq i(y)$. □

BEISPIELE. (a). $\mathbf{Q}$ ist Quotientenkörper von $\mathbf{Z}$.

(b). $K(X) := \{ \frac{f}{g} \mid g \neq 0,\ f,g \in K[X] \}$ ist Quotientenkörper von $K[X]$.

SATZ (Universelle Eigenschaft des Quotientenkörpers). *Sei A Integritätsbereich, K ein Körper und $f\colon A \to K$ ein Ringmonomorphismus. Dann gibt es genau einen Körpermonomorphismus $\bar{f}\colon Q(A) \to K$ mit $\bar{f} \circ i = f$.*



BEWEIS. *Existenz.* Definiere

$$\begin{aligned} \bar{f}\colon Q(A) &\to K, \\ (x,y) &\mapsto \frac{f(x)}{f(y)}. \end{aligned}$$

$\bar{f}$ ist verträglich mit $\sim$, denn $(x_1,y_1) = (x_2,y_2)$ bedeutet $x_1y_2 = x_2y_1$, also $f(x_1y_2) = f(x_2y_1)$ und somit

$$\frac{f(x_1)}{f(y_1)} = \frac{f(x_2)}{f(y_2)}.$$

$\bar{f}$ ist ein Homomorphismus, denn es gilt für alle $(x_1,y_1),(x_2,y_2) \in Q(A)$

$$\begin{aligned} \bar{f}((x_1,y_1) + (x_2,y_2)) &= \bar{f}(x_1y_2 + x_2y_1, y_1y_2) \\ &= \frac{f(x_1y_2 + x_2y_1)}{f(y_1y_2)} \\ &= \frac{f(x_1)}{f(y_1)} + \frac{f(x_2)}{f(y_2)} = \bar{f}(x_1,y_1) + \bar{f}(x_2,y_2) \end{aligned}$$

und

$$\begin{aligned} \bar{f}((x_1,y_1)\cdot(x_2,y_2)) &= \bar{f}(x_1x_2, y_1y_2) \\ &= \frac{f(x_1x_2)}{f(y_1y_2)} \end{aligned}$$

$$= \frac{f(x_1)}{f(y_1)} \cdot \frac{f(x_2)}{f(y_2)} = \bar{f}(x_1, y_1) \cdot \bar{f}(x_2, y_2).$$

$\bar{f}$ ist injektiv, denn Kern$(\bar{f}) = \{0\}$: Sei $(x, y) \in Q(A)$ mit $\bar{f}(x, y) = 0$. Dann folgt $\frac{f(x)}{f(y)} = 0$, damit auch $f(x) = 0$ und $x = 0$, also $(x, y) = 0$.

Eindeutigkeit. Sei $\bar{f}$ mit $\bar{f} \circ i = f$ gegeben. Dann gilt für alle $(x, y) \in Q(A)$

$$\bar{f}(x, y) = \bar{f}(i(x)i(y)^{-1}) = \bar{f}(i(x))\bar{f}(i(y))^{-1} = f(x)f(y)^{-1} = \frac{f(x)}{f(y)}. \quad \square$$

Bemerkung. Statt von $y \neq 0$ kann man allgemeiner ausgehen von $y \in N$, wobei N eine (feste) multiplikativ abgeschlossene Menge ist. Dann erhält man i.a. jedoch nur einen Quotientenring (s. Kunz, Algebra, Braunschweig 2-te Auflage 1994, §4.V).

KAPITEL 6

Reelle Zahlen

Ein wesentlicher Defekt des Körpers der rationalen Zahlen ist es, daß in ihm nicht jede „Fundamentalfolge“ einen Grenzwert besitzt. So ist zum Beispiel die Länge der Diagonale in einem Quadrat der Seitenlänge 1 zwar beliebig genau durch rationale Zahlen approximierbar, aber selbst nicht rational; dies war schon in der griechischen Antike bekannt. Eine andere Formulierung desselben Sachverhalts ist es, daß die Gleichung

$$x^2 = 2$$

in den rationalen Zahlen nicht lösbar ist. Wir erweitern deshalb die rationalen Zahlen zu den reellen Zahlen, in denen dieser Defekt nicht mehr auftritt. Um dies zu erreichen, müssen wir reelle Zahlen als unendliche Objekte auffassen. Genauer heißt das, daß wir unter einer reellen Zahl eine Folge von rationalen Approximationen verstehen, die zusammen mit einem „Modul“ vorliegt. Zu jeder vorgegebenen Genauigkeit gibt der Modul an, ab welchem Glied der Approximationsfolge diese Genauigkeit erreicht ist.

6.1. Konstruktion der reellen Zahlen

6.1.1. Approximation von $\sqrt{2}$. Zur Motivation des Einführung der reellen Zahlen zeigen wir, daß es eine Fundamentalfolge rationaler Zahlen gibt, die gegen keine rationale Zahl konvergiert. Zunächst beweisen wir

LEMMA (Irrationalität von $\sqrt{2}$). *2 ist kein Quadrat in* $\mathbf{Q}$.

BEWEIS. Andernfalls wäre $2 = \frac{m^2}{n^2}$ mit teilerfremden $m, n \in \mathbf{N}$, also $2n^2 = m^2$, also m gerade, d.h. von der Form $2k$, also $n^2 = 2k^2$ und damit n^2 gerade, d.h. von der Form $2l$. Also wäre 2 ein gemeinsamer Teiler von m und n: Widerspruch. □

SATZ (Approximation von $\sqrt{a}$). *Sei $a > 0$ und $a_0 > 0$ gegeben. Wir definieren eine Folge a_n rekursiv durch*

$$a_{n+1} := \frac{1}{2}\Big(a_n + \frac{a}{a_n}\Big).$$

Dann gilt:

(a) $(a_n)_{n\in\mathbf{N}}$ *ist eine Fundamentalfolge, das heißt*

$$\forall_k \exists_N \forall_{n,m\geq N}\ |a_n - a_m| \leq 2^{-k}.$$

(b) *Ist* $\lim_{n\to\infty} a_n = c$*, so folgt* $c^2 = a$*.*

Beweis. Durch Induktion über n zeigt man leicht, daß $a_n > 0$ für alle $n \in \mathbf{N}$. Ferner gilt

$$a_{n+1}^2 \geq a \quad \text{für alle } n; \tag{6.1}$$

dies folgt aus

$$a_{n+1}^2 - a = \frac{1}{4}\Big(a_n^2 + 2a + \frac{a^2}{a_n^2}\Big) - a = \frac{1}{4}\Big(a_n^2 - 2a + \frac{a^2}{a_n^2}\Big) = \frac{1}{4}\Big(a_n - \frac{a}{a_n}\Big)^2 \geq 0.$$

Weiter gilt

$$a_{n+2} \leq a_{n+1} \quad \text{für alle } n, \tag{6.2}$$

denn

$$a_{n+1} - a_{n+2} = a_{n+1} - \frac{1}{2}\Big(a_{n+1} + \frac{a}{a_{n+1}}\Big) = \frac{1}{2a_{n+1}}\Big(a_{n+1}^2 - a\Big) \geq 0.$$

Setze

$$b_n := \frac{a}{a_n}.$$

Dann gilt $b_{n+1}^2 \leq a$ für alle n, denn nach (6.1) gilt $\frac{1}{a_{n+1}^2} \leq \frac{1}{a}$, also auch

$$b_{n+1}^2 = \frac{a^2}{a_{n+1}^2} \leq \frac{a^2}{a} = a.$$

Aus (6.2) erhalten wir $b_{n+1} \leq b_{n+2}$ für alle n. Ferner haben wir

$$b_{n+1} \leq a_{m+1} \quad \text{für alle } n, m \in \mathbf{N}. \tag{6.3}$$

Um dies zu sehen, beachte man, daß – etwa für $n \geq m$ – gilt $b_{n+1} \leq a_{n+1}$ (dies folgt aus (6.1) durch Multiplikation mit $1/a_{n+1}$), und $a_{n+1} \leq a_{m+1}$ nach (6.2).

Wir zeigen jetzt

$$a_{n+1} - b_{n+1} \leq \frac{1}{2^n}(a_1 - b_1), \tag{6.4}$$

durch Induktion über n. Basis: für $n = 0$ sind beide Seiten gleich. Schritt $n \mapsto n + 1$:

$$\begin{aligned} a_{n+2} - b_{n+2} \leq a_{n+2} - b_{n+1} &= \frac{1}{2}(a_{n+1} + b_{n+1}) - b_{n+1} \\ &= \frac{1}{2}(a_{n+1} - b_{n+1}) \leq \frac{1}{2^{n+1}}(a_1 - b_1) \quad \text{nach IH.} \end{aligned}$$

$(a_n)_{n\in\mathbf{N}}$ ist Fundamentalfolge, da für $n \le m$ nach (6.2), (6.3) und (6.4) gilt

$$|a_{n+1} - a_{m+1}| = a_{n+1} - a_{m+1} \le a_{n+1} - b_{n+1} \le \frac{1}{2^n}(a_1 - b_1).$$

Nehmen wir jetzt an $\lim a_n = c$. Dann wäre auch $\lim b_n = c$, denn

$$|c - b_{n+1}| \le |c - a_{n+1}| + |a_{n+1} - b_{n+1}|,$$

und beide Summanden können Wahl eines hinreichend großen n beliebig klein gemacht werden, wegen (6.4). Also

$$c^2 = (\lim b_n)^2 = \lim b_n^2 \le a \le \lim a_n^2 = (\lim a_n)^2 = c^2$$

wegen $b_{n+1}^2 \le a \le a_{n+1}^2$, und deshalb $c^2 = a$. □

6.1.2. Reelle Zahlen, Gleichheit reeller Zahlen. Unter einer reellen Zahl verstehen wir eine Fundamentalfolge rationaler Zahlen zusammen mit einem separat gegebenen Modul.

Definition. Eine reelle Zahl x ist ein Paar $((a_n)_{n\in\mathbf{N}}, M)$ mit $a_n \in \mathbf{Q}$ und $M\colon \mathbf{N} \to \mathbf{N}$ so daß $(a_n)_n$ eine *Fundamentalfolge* mit Modul M ist:

$$|a_n - a_m| \le 2^{-k} \quad \text{für } n, m \ge M(k)$$

und M schwach wächst:

$$M(k) \le M(l) \quad \text{für } k \le l.$$

M heißt *Modul* von x.

Wir sprechen kurz von der reellen Zahl $(a_n)_n$ falls der Modul M aus dem Kontext klar oder unwesentlich ist. Jede rationale Zahl a verstehen wir stillschweigend als die reelle Zahl, die durch die konstante Folge $a_n = a$ mit dem konstanten Modul $M(k) = 0$ gegeben ist.

Definition. Zwei reelle Zahlen $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$ heißen *äquivalent* (oder geschrieben $x = y$ und gelesen *gleich*, falls aus dem Kontext klar ist, was gemeint ist), falls

$$|a_{M(k+1)} - b_{N(k+1)}| \le 2^{-k} \quad \text{für alle } k \in \mathbf{N}.$$

Wir zeigen, daß es sich hierbei um eine Äquivalenzrelation handelt. Reflexivität und Symmetrie sind klar. Für die Transitivität verwenden wir:

Lemma. *Für reelle Zahlen $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$ sind folgende Aussagen äquivalent*

(a) $x = y$;
(b) $\forall_k \exists_q \forall_{n\ge q}\ |a_n - b_n| \le 2^{-k}$.

BEWEIS. (a) → (b). Für $n \geq M(k+2), N(k+2)$ haben wir

$$\begin{aligned}|a_n - b_n| &\leq |a_n - a_{M(k+2)}| + |a_{M(k+2)} - b_{N(k+2)}| + |b_{N(k+2)} - b_n| \\ &\leq 2^{-k-2} + 2^{-k-1} + 2^{-k-2}.\end{aligned}$$

(b) → (a). Sei $l \in \mathbf{N}$ und q gemäß (b) zu l gewählt. Dann gilt für alle $n \geq q, M(k+1), N(k+1)$

$$\begin{aligned}|a_{M(k+1)} - b_{N(k+1)}| &\leq |a_{M(k+1)} - a_n| + |a_n - b_n| + |b_n - b_{N(k+1)}| \\ &\leq 2^{-k-1} + 2^{-l} + 2^{-k-1}.\end{aligned}$$

Die Behauptung folgt, da dies für alle $l \in \mathbf{N}$ gilt. □

LEMMA. *Die Gleichheit reeller Zahlen ist transitiv.*

BEWEIS. Seien $(a_n)_n$, $(b_n)_n$, $(c_n)_n$ Fundamentalfolgen für x, y, z. Gelte $x = y$, $y = z$. Gegeben sei ein $k \in \mathbf{N}$. Wir wählen p, q nach dem vorigen Lemma zu $x = y$, $y = z$ und $k+1$. Dann gilt $|a_n - c_n| \leq |a_n - b_n| + |b_n - c_n| \leq 2^{-k-1} + 2^{-k-1}$ für $n \geq p, q$. □

6.1.3. Das Archimedische Axiom. Für Funktionen auf den reellen Zahlen wollen wir sicherlich die Verträglichkeit mit der Gleichheit haben. Dies ist jedoch nicht immer möglich, wie das folgende Beispiel zeigt.

LEMMA. *Für jede reelle Zahl $x := ((a_n)_n, M)$ findet man eine obere Schranke 2^{k_x} für alle Elemente der Fundamentalfolge, also $|a_n| \leq 2^{k_x}$ für alle n.*

BEWEIS. Man wähle k_x so daß $\max\{\, |a_n| \mid n \leq M(0) \,\} + 1 \leq 2^{k_x}$, also $|a_n| \leq 2^{k_x}$ für alle n. □

Offenbar ist diese Zuordnung von k_x zu $x := ((a_n)_n, M)$ nicht verträglich mit der Gleichheit. Man kann nämlich eine reelle Zahl äquivalent immer so abändern, daß endliche viele Anfangsglieder der Fundamentalfolge $(a_n)_n$ vorgeschriebene Werte annehmen.

6.1.4. Nicht negative and positive reelle Zahlen. Eine reelle Zahl $x := ((a_n)_n, M)$ ist *nicht negativ* (geschrieben $x \in \mathbf{R}^{0+}$) wenn

$$-2^{-k} \leq a_{M(k)} \quad \text{für alle } k \in \mathbf{N}.$$

Sie ist *k-positiv* (geschrieben $x \in_k \mathbf{R}^+$, oder $x \in \mathbf{R}^+$ wenn k nicht gebraucht wird) falls

$$2^{-k} \leq a_{M(k+1)}.$$

Wir wollen zeigen, daß beide Eigenschaften verträglich mit der Gleichheit sind. Zuerst beweisen wir eine nützliche Charakterisierung der nicht negativen reellen Zahlen.

LEMMA. *Für eine reelle Zahl* $x := ((a_n)_n, M)$ *sind folgende Aussagen äquivalent:*

(a) $x \in \mathbf{R}^{0+}$.

(b) $\forall_k \exists_p \forall_{n \geq p} -2^{-k} \leq a_n$.

BEWEIS. (a) $\rightarrow$ (b). Für $n \geq M(k+1)$ gilt

$$\begin{aligned} -2^{-k} &\leq -2^{-k-1} + a_{M(k+1)} \\ &= -2^{-k-1} + (a_{M(k+1)} - a_n) + a_n \\ &\leq -2^{-k-1} + 2^{-k-1} + a_n. \end{aligned}$$

(b) $\rightarrow$ (a). Sei $l \in \mathbf{N}$ und $n \geq p, M(k)$ mit p aus (b) (für l). Dann

$$\begin{aligned} -2^{-k} - 2^{-l} &\leq -2^{-k} + a_n \\ &= -2^{-k} + (a_n - a_{M(k)}) + a_{M(k)} \\ &\leq -2^{-k} + 2^{-k} + a_{M(k)}. \end{aligned}$$

Die Behauptung folgt, da dies für jedes l gilt. □

LEMMA. *Ist* $x \in \mathbf{R}^{0+}$ *und* $x = y$*, so ist auch* $y \in \mathbf{R}^{0+}$.

BEWEIS. Sei $x := ((a_n)_n, M)$ und $y := ((b_n)_n, N)$. Wir nehmen an $x \in \mathbf{R}^{0+}$ und $x = y$; ferner sei k gegeben. Wähle p nach dem obigen Lemma, und q gemäß der Charakterisierung der Gleichheit der reellen Zahlen (beides für $k+1$). Dann gilt für $n \geq p, q$

$$-2^{-k} \leq -2^{-k-1} + a_n \leq (b_n - a_n) + a_n.$$

Also ist $y \in \mathbf{R}^{0+}$ nach Definition. □

Wir zeigen jetzt die Verträglichkeit der Positivität mit der Gleichheit. Dafür verwenden wir wieder ein Lemma:

LEMMA. *Für eine reelle Zahl* $x := ((a_n)_n, M)$ *sind folgende Aussagen äquivalent:*

(a) $\exists_k\ x \in_k \mathbf{R}^+$.

(b) $\exists_{l,p} \forall_{n \geq p}\ 2^{-l} \leq a_n$.

Für $\forall_{n \geq p}\ 2^{-l} \leq a_n$ *schreiben wir* $x \in_{l,p} \mathbf{R}^+$ *oder auch* $0 <_{l,p} x$.

BEWEIS. (a) $\rightarrow$ (b). Sei $x \in_k \mathbf{R}^+$, also $2^{-k} \leq a_{M(k+1)}$. Dann gilt

$$2^{-k-1} \leq -2^{-k-1} + a_{M(k+1)} = -2^{-k-1} + (a_{M(k+1)} - a_n) + a_n \leq a_n$$

für $M(k+1) \leq n$. Also können wir $l := k+1$ und $p := M(k+1)$ wählen.

(b) $\rightarrow$ (a).

$$2^{-l-1} < -2^{-l-2} + 2^{-l}$$

$$\begin{aligned} &\le -2^{-l-2} + a_n && \text{für } p \le n \\ &\le (a_{M(l+2)} - a_n) + a_n && \text{für } M(l+2) \le n. \end{aligned}$$

Also können wir $k := l + 1$ wählen; dann ist x k-positiv. □

LEMMA. *Die Positivität reeller Zahlen ist verträglich mit der Gleichheit.*

BEWEIS. Sei $0 <_{k,p} x$ und es gelte $x = y$. Dann haben wir ein q mit $\forall_{n \ge q} |a_n - b_n| \le 2^{-k-1}$. Also gilt für $n \ge \max(p, q)$

$$2^{-k-1} = -2^{-k-1} + 2^k \le (b_n - a_n) + a_n = b_n$$

und deshalb $0 <_{k+1,\max(p,q)} y$. □

6.1.5. Arithmetische Funktionen. Gegeben seien reelle Zahlen $x := ((a_n)_n, M)$ und $y := ((b_n)_n, N)$. Wir definieren $x + y$, $-x$, $|x|$, $x \cdot y$, und $\frac{1}{x}$ (letzteres nur im Fall $|x| \in_l \mathbf{R}^+$) als repräsentiert durch eine Folge $(c_n)_n$ rationaler Zahlen mit Modul L:

	c_n	$L(k)$
$x + y$	$a_n + b_n$	$\max\big(M(k+1), N(k+1)\big)$
$-x$	$-a_n$	$M(k)$
$\lvert x\rvert$	$\lvert a_n\rvert$	$M(k)$
$x \cdot y$	$a_n \cdot b_n$	$\max\big(M(k+1+k_{\lvert y\rvert}), N(k+1+k_{\lvert x\rvert})\big)$
$\frac{1}{x}$ für $\lvert x\rvert \in_l \mathbf{R}^+$	$\begin{cases} \frac{1}{a_n} & \text{if } a_n \neq 0 \\ 0 & \text{if } a_n = 0 \end{cases}$	$M(2(l+1)+k)$,

wobei 2^{k_x} die in 6.1.3 konstruierte obere Schranke ist.

LEMMA. *Für reelle Zahlen x, y sind auch $x + y$, $-x$, $|x|$, $x \cdot y$ und (im Fall $|x| \in_l \mathbf{R}^+$) auch $1/x$ reelle Zahlen.*

BEWEIS. Wir beschränken uns auf die Fälle $x \cdot y$ und $1/x$.

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n(b_n - b_m) + (a_n - a_m)b_m| \\ &\le |b_n - b_m| \cdot |a_n| + |a_n - a_m| \cdot |b_m| \\ &\le |b_n - b_m| \cdot 2^{k_{|x|}} + |a_n - a_m| \cdot 2^{k_{|y|}} \le 2^{-k} \end{aligned}$$

für $n, m \ge \max\big(M(k + 1 + k_{|y|}), N(k + 1 + k_{|x|})\big)$.

Für $1/x$ nehmen wir $|x| \in_l \mathbf{R}^+$ an. Dann gilt nach (dem Beweis) unserer Charakterisierung der Positivität $2^{-l-1} \le |a_n|$ für $M(l+1) \le n$. Also

$$\begin{aligned} \Big|\frac{1}{a_n} - \frac{1}{a_m}\Big| &= \frac{|a_m - a_n|}{|a_n a_m|} \\ &\le 2^{2(l+1)} |a_m - a_n| \quad \text{für } n, m \ge M(l+1) \\ &\le 2^{-k} \quad \text{für } n, m \ge M(2(l+1)+k). \end{aligned}$$

Die Behauptung folgt jetzt, da M schach wächst. □

LEMMA. *Die Funktionen $x+y$, $-x$, $|x|$, $x\cdot y$ und (im Fall $|x|\in_l \mathbf{R}^+$) auch $1/x$ sind verträglich mit der Gleichheit.*

BEWEIS. Routine. □

LEMMA. *Für reelle Zahlen x,y,z gilt*

$$x+(y+z)=(x+y)+z \qquad x\cdot(y\cdot z)=(x\cdot y)\cdot z$$
$$x+0=x \qquad x\cdot 1=x$$
$$x+(-x)=0 \qquad 0<|x|\to x\cdot\frac{1}{x}=1$$
$$x+y=y+x \qquad x\cdot y=y\cdot x$$
$$x\cdot(y+z)=x\cdot y+x\cdot z$$

BEWEIS. Routine. □

LEMMA. *Für reelle Zahlen x,y folgt aus $x\cdot y=1$ stets $0<|x|$.*

BEWEIS. Man wähle k so daß $|b_n|\le 2^k$ für alle n. Wähle q so daß $q\le n$ impliziert $1/2\le a_n\cdot b_n$. Dann gilt für $q\le n$ daß $1/2\le |a_n|\cdot 2^k$, und deshalb $2^{-k-1}\le |a_n|$. □

LEMMA. (a) $x,y\in\mathbf{R}^{0+}\to x+y, x\cdot y\in\mathbf{R}^{0+}$,
(b) $x,y\in\mathbf{R}^{+}\to x+y, x\cdot y\in\mathbf{R}^{+}$,
(c) $x\in\mathbf{R}^{0+}\to -x\in\mathbf{R}^{0+}\to x=0$.

BEWEIS. (a), (b). Routine. (c). Sei k gegeben. Wähle p so daß $-2^{-k}\le a_n$ und $-2^{-k}\le -a_n$ für $n\ge p$. Dann ist $|a_n|\le 2^{-k}$. □

6.1.6. Vergleich reeller Zahlen. Wir schreiben $x\le y$ für $y-x\in\mathbf{R}^{0+}$ und $x<y$ für $y-x\in\mathbf{R}^{+}$. Nach unseren Definitionen besagt $x\le y$, daß für jedes k gilt $a_{L(k)}\le b_{L(k)}+2^{-k}$, mit $L(k):=\max(M(k),N(k))$. Eine äquivalente Formulierung (aufgrund der Charakterisierung in 6.1.4) ist, daß es für jedes k ein p gibt mit $a_n\le b_n+2^{-k}$ für alle $n\ge p$. Ferner ist $x<y$ eine Abkürzung für das Vorhandensein eines k mit $a_{L(k+1)}+2^{-k}\le b_{L(k+1)}$, wobei L das Maximum of M and N ist, oder äquivalent (wieder aufgrund der Charakterisierung in 6.1.4) für das Vorhandensein von k,q mit $a_n+2^{-k}\le b_n$ für alle $n\ge q$; wir schreiben $x<_k y$ (oder auch $x<_{k,q} y$), wenn wir diese „Zeugen“ benennen wollen.

Jede reelle Zahl läßt sich belienig gut durch eine rationale approximieren:

LEMMA. $\forall_{x,k}\exists_a\ |a-x|\le 2^{-k}$.

BEWEIS. Sei $x = ((a_n), M)$. Zu einem gegebenen k wähle man $a_{M(k)}$. Zu zeigen ist $|a_{M(k)} - x| \leq 2^{-k}$, also $|a_{M(k)} - a_{M(l)}| \leq 2^{-k} + 2^{-l}$ für jedes l. Dies folgt aber aus

$$|a_{M(k)} - a_{M(l)}| \leq |a_{M(k)} - a_{M(k+l)}| + |a_{M(k+l)} - a_{M(l)}| \leq 2^{-k} + 2^{-l}. \quad \square$$

LEMMA. *Aus* $0 \leq x$ *und* $0 <_k y$ *folgt* $0 <_{k+1} x + y$.

BEWEIS. Aus $0 \leq x$ folgt $\forall_l \exists_p \forall_{n \geq p} \; -2^{-l} \leq a_n$. Aufgrund von $0 <_k y$ haben wir ein q so daß $\forall_{n \geq q} \, 2^{-k} \leq b_n$. Man wähle p für $k+1$. Aus $p, q \leq n$ folgt $0 \leq a_n + 2^{-k-1}$ und $2^{-k-1} \leq b_n - 2^{-k-1}$, also $2^{-k-1} \leq a_n + b_n$. $\square$

LEMMA. *Für reelle Zahlen* x, y, z *gilt*

$$\begin{array}{ll} x \leq x & x \not< x \\ x \leq y \to y \leq x \to x = y & x < y \to y < z \to x < z \\ x \leq y \to y \leq z \to x \leq z & x < y \to x + z < y + z \\ x \leq y \to x + z \leq y + z & x < y \to 0 < z \to x \cdot z < y \cdot z \\ x \leq y \to 0 \leq z \to x \cdot z \leq y \cdot z & \end{array}$$

BEWEIS. Siehe 6.1.5. $\square$

LEMMA. $x \leq y \to y <_k z \to x <_{k+1} z$.

BEWEIS. Dies folgt aus dem vorletzten Lemma. $\square$

Wie zu erwarten ergibt sich aus dem universellen bzw. existentiellen Charakter der Prädikate $<$ und $\leq$ auf den reellen Zahlen, daß gilt

LEMMA. $x \leq y \leftrightarrow y \not< x$.

BEWEIS. $\to$. Gelte $x \leq y$ und $y < x$. Nach dem vorangehenden Lemma erhalten wir $x < x$, also einen Widerspruch.

$\leftarrow$. Offenbar genügt es zu zeigen, daß $0 \not< z \to z \leq 0$, für eine beliebige durch $(c_n)_n$ gegebene reelle Zahl z. Sei also $0 \not< z$. Zu zeigen ist dann $\forall_k \exists_p \forall_n (p \leq n \to c_n \leq 2^{-k})$. Sei k gegeben. Nach Annahme ist $0 \not< z$, also $\neg \exists_l (2^{-l} \leq c_{M(l+1)})$, also $\forall_l (c_{M(l+1)} < 2^{-l})$. Für $l := k+1$ impliziert das $c_{M(k+2)} < 2^{-k-1}$, also $c_n \leq c_{M(k+2)} + 2^{-k-2} < 2^{-k}$ für $M(k+2) \leq n$. $\square$

Konstruktiv, also im Sinn von $\vee$, können wir zwei beliebig gegebene reelle Zahlen nicht vergleichen. Wir können jedoch jede reelle Zahl mit einem nicht leeren Intervall vergleichen („approximative Fallunterscheidung“):

LEMMA. *Seien* x, y, z *gegeben mit* $x < y$. *Dann ist* $z \leq y$ *oder* $x \leq z$.

BEWEIS. Sei $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$, $z := ((c_n)_n, L)$. Gelte $x <_k y$, also $1/2^k \leq b_p - a_p$ für $p := \max(M(k+2), N(k+2))$. Setze $q := \max(p, L(k+2))$ und $d := (b_p - a_p)/4$.

Fall $c_q \leq \frac{a_p+b_p}{2}$. Wir zeigen $z \leq y$. Es genügt zu zeigen $c_n \leq b_n$ für $n \geq q$. Dies folgt aus

$$c_n \leq c_q + \frac{1}{2^{k+2}} \leq \frac{a_p+b_p}{2} + \frac{b_p-a_p}{4} = b_p - \frac{b_p-a_p}{4} \leq b_p - \frac{1}{2^{k+2}} \leq b_n.$$

Fall $c_q \not\leq \frac{a_p+b_p}{2}$. Wir zeigen $x \leq z$. Dies folgt aus $a_n \leq c_n$ für $n \geq q$:

$$a_n \leq a_p + \frac{1}{2^{k+2}} \leq a_p + \frac{b_p-a_p}{4} \leq \frac{a_p+b_p}{2} - \frac{b_p-a_p}{4} \leq c_q - \frac{1}{2^{k+2}} \leq c_n. \quad \square$$

Man beachte, daß das boolesche Objekt, welches bestimmt ob $z \leq y$ oder $x \leq z$ gilt, von der Repräsentation von x, y und z abhängt. Insbesondere ist diese Zuordnung nicht verträglich mit unserer oben definierten Gleichheit reeller Zahlen.

Man könnte meinen, daß die Nicht-Verfügbarkeit eines Vergleichs reeller Zahlen durch die Verwendung einer Maximum-Funktion umgangen werden kann. Eine solche Funktion kann in der Tat leicht (komponentenweise) definiert werden, und sie hat die erwarteten Eigenschaften $x, y \leq \max(x, y)$ und $x, y \leq z \to \max(x, y) \leq z$. Es fehlt jedoch die Kenntnis darüber, daß $\max(x, y)$ gleich einem seiner Argumente ist: wir können nicht beweisen, daß $\max(x, y) = x \vee \max(x, y) = y$.

In vielen Fällen ist es jedoch ausreichend, aus endlich vielen reellen Zahlen eine bis auf ein ε größte auszuwählen. Das ist in der Tat immer möglich. Wie beweisen dies hier für zwei reelle Zahlen:

LEMMA. *Seien* $x := ((a_n)_n, M)$ *und* $y := ((b_n)_n, N)$ *reelle Zahlen, und* $k \in \mathbf{N}$. *Dann gilt für* $\varepsilon := 2^{-k}$, *daß* $x \leq y + \varepsilon$ *oder* $y \leq x + \varepsilon$.

BEWEIS. Sei $p := \max\big(M(k+1), N(k+1)\big)$.
Fall $a_p \leq b_p$. Dann gilt für $p \leq n$

$$a_n \leq a_p + \frac{\varepsilon}{2} \leq b_p + \frac{\varepsilon}{2} \leq b_n + \varepsilon.$$

Dies hat man für alle n, also $x \leq y + \varepsilon$.
Fall $b_p < a_p$. Dann gilt für $p \leq n$

$$b_n \leq b_p + \frac{\varepsilon}{2} < a_p + \frac{\varepsilon}{2} \leq a_n + \varepsilon.$$

Dies hat man wieder für alle n, also $y \leq x + \varepsilon$. $\square$

6.1.7. Reinigung reeller Zahlen. Nach einigen Berechnungen mit konkreten reellen Zahlen kann man erwarten, daß die in den Fundamentalfolgen vorkommenden rationalen Zahlen recht kompliziert geworden sind. Unter rechnerischen Gesichtspunkten ist es deshalb notwendig, eine reelle Zahl zu „reinigen“. Dies ist einfach möglich.

LEMMA. *Für jede reelle Zahl $x = ((a_n)_n, M)$ kann man eine äquivalente reelle Zahl $y = ((b_n)_n, N)$ konstruieren, in der die rationalen Zahlen b_n von der Form $c_n/2^n$ sind mit ganzen Zahlen c_n, und mit dem Modul $N(k) = k+2$.*

BEWEIS. Sei $c_n := \lfloor a_{M(n)} \cdot 2^n \rfloor$ und $b_n := c_n \cdot 2^{-n}$, also

$$\frac{c_n}{2^n} \le a_{M(n)} < \frac{c_n}{2^n} + \frac{1}{2^n} \quad \text{mit } c_n \in \mathbf{Z}.$$

Dann gilt für $m \le n$

$$\begin{aligned} |b_m - b_n| &= |c_m \cdot 2^{-m} - c_n \cdot 2^{-n}| \\ &\le |c_m \cdot 2^{-m} - a_{M(m)}| + |a_{M(m)} - a_{M(n)}| + |a_{M(n)} - c_n \cdot 2^{-n}| \\ &\le 2^{-m} + 2^{-m} + 2^{-n} \\ &< 2^{-m+2}, \end{aligned}$$

also $|b_m - b_n| \le 2^{-k}$ für $n \ge m \ge k+2 =: N(k)$. Demnach ist $(b_n)_n$ eine Fundamentalfolge mit Modul N.

Wir zeigen, daß x äquivalent zu $y := ((b_n)_n, N)$ ist. Man beachte, daß

$$\begin{aligned} |a_n - b_n| &\le |a_n - a_{M(n)}| + |a_{M(n)} - c_n \cdot 2^{-n}| \\ &\le 2^{-k-1} + 2^{-n} \quad \text{für } n, M(n) \ge M(k+1) \\ &\le 2^{-k} \quad \text{falls zusätzlich } n \ge k+1. \end{aligned}$$

Also ist $|a_n - b_n| \le 2^{-k}$ für $n \ge \max(k+1, M(k+1))$, und deshalb $x = y$. □

6.2. Reelle Zahlen als schwach geordneter Körper

In 4.5.1 wurde die folgende Charakterisierung gordneter Integritätsbereiche bewiesen. Sei A Integritätsbereich und $\mathrm{Nneg} \subseteq A$. Für alle $x, y \in A$ gelte

(a) $x, y \in \mathrm{Nneg} \to x + y, xy \in \mathrm{Nneg}$.
(b) $x \in \mathrm{Nneg} \vee -x \in \mathrm{Nneg}$.
(c) $x \in \mathrm{Nneg} \to -x \in \mathrm{Nneg} \to x = 0$.

Definiert man $x \le y$ durch $y - x \in \mathrm{Nneg}$, so ist $(A, +, \cdot, \le)$ ein geordneter Integritätsbereich (mit $A^{0+} = \mathrm{Nneg}$).

Die Frage liegt nahe, ob $\mathbf{R}$ mit $\mathbf{R}^{0+}$ als Teilmenge der nicht-negativen Elemente diese Charakterisierung erfüllt. Die Antwort ist „nein“, wenn man die Disjunktion $\vee$ in (b) als die *starke* Disjunktion versteht. Verwendet man jedoch stattdessen die schwache Disjunktion $\tilde{\vee}$ (definiert durch $A \mathbin{\tilde{\vee}} B := \neg(\neg A \wedge \neg B)$), so kann man diese Aussage beweisen. Man spricht deshalb von einem *schwach geordneten Integritätsbereich*.

LEMMA. *Für alle $x \in \mathbf{R}$ gilt $x \in \mathbf{R}^{0+} \mathbin{\tilde{\vee}} -x \in \mathbf{R}^{0+}$.*

BEWEIS. Sei $x = ((a_n)_{n\in\mathbf{N}}, M) \in \mathbf{R}$. Wir nehmen an, daß $\neg x \geq 0$ und $\neg 0 \leq x$. Zu zeigen ist, daß dies nicht möglich ist.

$\neg x \geq 0$ ist definiert durch $\neg\forall_k\, -2^{-k} \leq a_{M(k)}$, also $\tilde{\exists}_k\, -2^{-k} \not\leq a_{M(k)}$.

$\neg 0 \leq x$ ist definiert durch $\neg\forall_l\, a_{M(l)} \leq 2^{-l}$, also $\tilde{\exists}_l\, a_{M(l)} \not\leq 2^{-l}$.

Wir haben also $a_{M(k)} < -2^{-k} < 0 < 2^{-l} < a_{M(l)}$, wobei wir ohne Beschränkung der Allgemeinheit $k \leq l$ annehmen können. Dann gilt auch $M(k) \leq M(l)$. Mit $|a_{M(l)} - a_{M(k)}| \leq 2^{-k}$ ergibt sich ein Widerspruch. □

Als nächstes wollen wir untersuchen, ob $\mathbf{R}$ ein Körper ist. Dies ist der Fall, wenn wir in der Definition eines Körpers in 5.2.1 (daß nämlich die Einheitengruppe K^* aus allen von 0 verschiedenen Elementen besteht), die Aussage „von 0 verschiedenen“ im positiven Sinne, also als „von 0 getrennt“ verstehen.

LEMMA. *Die Einheitengruppe $\mathbf{R}^*$ von $\mathbf{R}$ besteht aus allen von 0 getrennten Elementen von $\mathbf{R}$, ist also gleich der Menge $\mathbf{R}^\# := \{\, x \in \mathbf{R} \mid |x| \in \mathbf{R}^+ \,\}$.*

BEWEIS. $\mathbf{R}^* \subseteq \mathbf{R}^\#$. Nach einem Lemma in 6.1.5 folgt aus $xy = 1$ stets $0 < |x|$. $\mathbf{R}^\# \subseteq \mathbf{R}^*$. Sei $|x| \in_l \mathbf{R}^+$. Dann ist $\frac{1}{x}$ definiert, und $\frac{1}{x} \cdot x = 1$. □

6.3. Überabzählbarkeit, Vollständigkeit

6.3.1. Überabzählbarkeit. Jede rationale Zahl a hatten wir aufgefaßt als diejenige reelle Zahl, die durch die konstante Folge $a_n = a$ mit dem konstanten Modul $M(k) = 0$ gegeben ist.

LEMMA ($\mathbf{Q}$ ist dicht in $\mathbf{R}$). *Für reelle Zahlen $x < y$ gibt es eine rationale Zahl a so daß $x < a < y$.*

BEWEIS. Sei $z := (x + y)/2$ gegeben durch $(c_n)_n$. Dann gilt $x <_k z <_k y$ für ein k. Setze $a := c_{M(k+1)}$. □

Man beachte, daß a von den Repräsentationen von x und y abhängt.

SATZ (Cantor). *Gegeben sei eine Folge (x_n) reeller Zahlen. Dann findet man eine reelle Zahl y mit $0 \leq y \leq 1$, die von jedem x_n in dem folgenden starken Sinn verschieden ist: es gilt $x_n < y \vee y < x_n$.*

BEWEIS. Wir konstruieren rekursiv zwei Folgen $(a_n)_n$, $(b_n)_n$ rationaler Zahlen, und zwar so, daß für alle n gilt

$$0 = a_0 \leq a_1 \leq \cdots \leq a_n < b_n \leq \cdots \leq b_1 \leq b_0 = 1, \tag{6.5}$$

$$x_n < a_{n+1} \vee b_{n+1} < x_n, \tag{6.6}$$

$$b_n - a_n \leq 2^{-n}. \tag{6.7}$$

Seien $a_0, \dots, a_n$ und $b_0, \dots, b_n$ mit den Eigenschaften (6.5)-(6.7) bereits konstruiert (soweit sie definiert sind). Man vergleicht jetzt die reelle Zahl x_n mit $a_n < b_n$.

Fall 1. $x_n < b_n$. Setze $b_{n+1} := b_n$. Da $\mathbf{Q}$ in $\mathbf{R}$ dicht ist, findet man eine rationale Zahl a_{n+1} mit

$$\max\bigl(x_n, a_n, b_n - 2^{-n-1}\bigr) < a_{n+1} < b_{n+1} = b_n.$$

Fall 2. $a_n < x_n$. Setze $a_{n+1} := a_n$, und konstruiere eine rationale Zahl b_{n+1} mit

$$a_n = a_{n+1} < b_{n+1} < \min\bigl(x_n, b_n, a_n + 2^{-n-1}\bigr).$$

Offenbar gelten (6.5)-(6.7) (soweit definiert) auch für $n+1$. Also ist $y := (a_n)_n$ eine Fundamentalfolge, denn für $m \geq n$ gilt $|a_m - a_n| = a_m - a_n \leq b_n - a_n \leq 2^{-n}$. Entsprechend ist auch $z := (b_n)_n$ eine Fundamentalfolge. $y = z$ folgt aus (6.7), und aus (6.6), (6.5) erhalten wir $x_n < y \vee z < x_n$. □

6.3.2. Vollständigkeit.

Definition. Eine Folge $(x_n)_{n\in\mathbf{N}}$ reeller Zahlen heißt *Fundamentalfolge* mit Modul $M\colon \mathbf{N} \to \mathbf{N}$, wenn $|x_n - x_m| \leq 2^{-k}$ für $n, m \geq M(k)$, und sie *konvergiert* mit Modul $M\colon \mathbf{N} \to \mathbf{N}$ gegen eine reelle Zahl y, ihren *Grenzwert*, wenn $|x_n - y| \leq 2^{-k}$ für $n \geq M(k)$.

Offenbar ist der Grenzwert einer konvergenten Folge reeller Zahlen eindeutig bestimmt.

Lemma. *Jede mit einem Modul versehene Fundamentalfolge rationaler Zahlen konvergiert mit demselben Modul gegen die durch sie repräsentierte reelle Zahl.*

Beweis. Sei $x := ((a_n)_n, M)$ eine reelle Zahl. Wir zeigen, daß $|a_n - x| \leq 2^{-k}$ für $n \geq M(k)$. Man fixiere ein $n \geq M(k)$. Es genügt zu zeigen, daß $|a_n - a_m| \leq 2^{-k}$ für $m \geq M(k)$. Dies gilt aber nach Annahme. □

Nach der Dreiecksungleichung ist jede konvergente Folge reeller Zahlen mit Modul M eine Fundamentalfolge mit Modul $k \mapsto M(k+1)$. Wir beweisen jetzt die Umkehrung

Satz (Folgenvollständigkeit). *Für jede Fundamentalfolge reeller Zahlen gibt es eine reelle Zahl, gegen die sie konvergiert.*

Beweis. Sei $(x_n)_{n\in\mathbf{N}}$ eine Fundamentalfolge reeller Zahlen mit Modul M, etwa $x_n = ((a_{nk})_k, N_n)$. Man beachte zunächst, daß für jedes $n \in \mathbf{N}$ und jedes p nach dem obigen Lemma gilt $|x_n - a_{nl}| \leq 2^{-p}$ für alle $l \geq N_n(p)$. Setze

$$b_n := a_{nN_n(n)}$$

für jedes $n \in \mathbf{N}$. Dann gilt

$$|x_n - b_n| \leq 2^{-n} \quad \text{für alle } n \in \mathbf{N}$$

nach dem Spezialfall $l = N_n(n)$ der vorangehenden Betrachtung. Also ist

$$|b_m - b_n| \leq |b_m - x_m| + |x_m - x_n| + |x_n - b_n| \leq 2^{-m} + 2^{-q-1} + 2^{-n} \leq 2^{-q}$$

für alle $m, n \geq \max(M(q+1), q+2)$, das heißt, daß $y := (b_n)_n$ eine Fundamentalfolge mit Modul $L(q) := \max(M(q+1), q+2)$ ist. Ferner gilt, wieder nach dem obigen Lemma

$$|x_n - y| \leq |x_n - b_n| + |b_n - y| \leq 2^{-n} + 2^{-q-1} \leq 2^{-q}$$

für alle $n \geq L(q+1)$. Mit anderen Worten: (x_n) konvergiert gegen y mit Modul $q \mapsto L(q+1)$. □

Man kann sogar zeigen, daß (x_n) gegen y mit demselben Modul konvergiert, den (x_n) als Fundamentalfolge hat. Mit anderen Worten, der obige Satz gilt auch für Fundamentalfolgen reeller Zahlen.

LEMMA. *Jede mit einem Modul versehene Fundamentalfolge reeller Zahlen konvergiert mit demselben Modul gegen ihren Grenzwert.*

BEWEIS. Sei $(x_n)_n$ eine Fundamentalfolge reeller Zahlen mit Modul M, also

$$|x_n - x_m| \leq 2^{-k} \quad \text{für } n, m \geq M(k).$$

Sei y der Grenzwert von $(x_n)_n$, also

$$|x_n - y| \leq 2^{-l} \quad \text{für } n \geq L(l).$$

Wir zeigen

$$|x_n - y| \leq 2^{-k} \quad \text{für } n \geq M(k).$$

Man fixiere $n \geq M(k)$, und wähle ein beliebiges $l \in \mathbf{N}$. Dann gilt

$$\begin{aligned} |x_n - y| &\leq |x_n - x_m| + |x_m - y| \quad \text{für } m \geq M(k), L(l) \\ &\leq 2^{-k} + 2^{-l}. \end{aligned}$$

Die Behauptung folgt, da dies für jedes l gilt. □

Wir beweisen noch ein nützliches Kriterium für die Konvergenz einer Folge reeller Zahlen, das sich auf ihre Approximationen stützt.

LEMMA. *Die reellen Zahlen x_n, x seien repräsentiert durch $(a_{nk})_k, (b_k)_k$. Dann folgt die Konvergenz von $(x_n)_n$ gegen x, also*

$$\forall_p \exists_q \forall_{n \geq q} \; |x_n - x| \leq 2^{-p}$$

aus

$$\forall_p \exists_q \forall_{n,k \geq q} \; |a_{nk} - b_k| \leq 2^{-p}.$$

BEWEIS. Zu einem gegebenen p wollen wir ein q finden mit $|x_n - x| \leq 2^{-p}$ für $n > q$. Nach der Charakterisierung der nicht negativen reellen Zahlen in 6.1.4 genügt $|a_{nk} - b_k| \leq 2^{-p} + 2^{-l}$ für $k \geq r$, wobei r l abhängt. Aber nach Annahme haben wir sogar $|a_{nk} - b_k| \leq 2^{-p}$ für $k \geq q$. □

6.4. Erweiterung der reellen zu den komplexen Zahlen

Seien $K = \mathbf{R}$ und $\xi = -1$; man beachte, daß -1 kein Quadrat in $\mathbf{R}$ ist. Man schreibt $\mathbf{C} := \mathbf{R}(\sqrt{-1})$ (vgl. 5.2.1) und nennt $\mathbf{C}$ den Körper der *komplexen Zahlen*. Die Abbildung

$$\begin{array}{ccc} \mathbf{R} & \to & \mathbf{R}(\sqrt{-1}) \\ x & \mapsto & (x, 0) \end{array}$$

ist injektiv. Da

$$\begin{aligned} (x,0) + (y,0) &= (x+y,0) \\ (x,0) \cdot (y,0) &= (x \cdot y, 0), \end{aligned}$$

braucht man zwischen $\mathbf{R}$ und $\mathbf{R} \times \{0\} = \{\, (x,0) \mid x \in \mathbf{R} \,\}$ bzgl. Addition und Multiplikation nicht zu unterscheiden. Man kann also $\mathbf{R}$ mit $\mathbf{R} \times \{0\}$ identifizieren. In diesem Sinn ist $\mathbf{R} \subseteq \mathbf{C}$. Man setzt noch

$$i := (0,1) \quad (\textit{imaginäre Einheit}).$$

Offenbar läßt sich jedes $z \in \mathbf{C}$ eindeutig darstellen als $z = x + iy$ mit $x, y \in \mathbf{R}$, denn es gilt $x + iy = (x, y)$. Die *konjugiert komplexe Zahl* zu $z = x + iy$ ist $\overline{z} := x - iy$. Man verifiziert leicht, daß gilt

$$\begin{array}{ll} \overline{\overline{z}} = z, & \overline{0} = 0, \\ \overline{z+u} = \overline{z} + \overline{u}, & \overline{1} = 1. \\ \overline{zu} = \overline{z}\,\overline{u}, & \end{array}$$

Ferner ist $z\overline{z} = x^2 + y^2$ für $z = x + iy$. Wegen $x^2 + y^2 \geq 0$ kann man $\sqrt{x^2 + y^2} \in \mathbf{R}$ bilden; man setzt $|z| := \sqrt{x^2 + y^2}$ und nennt dies den *Betrag* von $z \in \mathbf{C}$. Für eine ausführlichere Diskussion des Körpers $\mathbf{C}$ der komplexen Zahlen sei auf die Analysis-Vorlesung verwiesen.

Literaturverzeichnis

N. G. de Bruijn. Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem. *Indagationes Math.*, 34:381–392, 1972.

O. Deiser. *Einführung in die Mengenlehre.* Springer Verlag, Berlin, Heidelberg, New York, 2nd edition, 2004.

S. Feferman. *The Number Systems. Foundations of Algebra and Analysis.* Addison-Wesley, 1964.

G. Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1934.

K. Reiss and G. Schmieder. *Basiswissen Zahlentheorie.* Springer Verlag, 2nd edition, 2007.

Index