Lineare Algebra, Teil I

(Folien zur Vorlesung)
Joachim Stöckler

Auszüge aus dem Vorlesungsskript von Prof. Rudolf Scharlau aus dem WS 2009/10 werden auf den Folien verwendet. Für die Bereitstellung dieses Materials und der Tex-Files danke ich herzlich.

Kapitel I. Grundbegriffe

Inhalt:

1. Logik
2. Mengen und Abbildungen
3. Primfaktorzerlegung und euklidischer Algorithmus
4. Algebraische Strukturen: Gruppe, Ring, Körper
5. Äquivalenzrelationen
6. Der Körper der komplexen Zahlen

1 Logik

Die Vorlesung beginnt mit einem kleinen Einstieg in die Aussagenlogik. Dies soll später das Verständnis auch bei komplizierteren Beweisgängen erleichtern.

1.1 Definition: Aussagen

Eine *Aussage* im Sinne der Logik ist eine sprachliche Formulierung, die entweder *wahr (TRUE)* oder *falsch (FALSE)* ist.

1.3 Definition: Logische Verknüpfungen

Aussagen können miteinander verknüpft werden. Die grundlegenden Verknüpfungen werden durch die folgenden Wahrheitstafeln definiert.

a) Logisches *UND*:

A	B	$A \wedge B$
w	w	w
w	f	f
f	w	f
f	f	f

Entspricht dem sprachlichen "sowohl ... als auch"

b) Logisches *ODER*:

A	B	$A \vee B$
w	w	w
w	f	w
f	w	w
f	f	f

Entspricht dem sprachlichen nicht-exklusiven "oder"

c) Negation:

A	$\neg A$
w	f
f	w

Sprich "nicht A"

d) Logische Folgerung, Implikation:

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

Sprich "Aus A folgt B" oder "Wenn A, dann B"

e) Äquivalenz:

A	B	$A \Leftrightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

Sprich "A ist äquivalent zu B" oder "A genau dann, wenn B"

1.5 Bemerkung: Das Wesen einer mathematischen Theorie besteht darin, mathematische Strukturen anhand von *Axiomen* aufzustellen und hieraus weitere Aussagen herzuleiten. Die Axiome sind Aussagen, deren Gültigkeit vorausgesetzt wird (Wahrheitswert TRUE) und die in einer *Definition* der Struktur zusammengefasst werden. Die weiteren Aussagen (sog. *Sätze, Theoreme, Lemmata*) sind kompliziertere Aussagen, die durch logische Schlüsse aus den Axiomen hergeleitet werden. Die Herleitung nennt man *Beweis*.

1.6 Bemerkung: Beweismethoden

Für Beweise (oder einzelne Teile von Beweisen) gibt es gängige Methoden:

a) direkter Beweis: $A \implies B$

b) indirekter Beweis: Um $A \implies B$ zu zeigen, beweist man stattdessen $\neg B \implies \neg A$ (vgl. Beispiel **??**)

c) Widerspruchsbeweis: Um A zu zeigen, nimmt man $\neg A$ als wahr an (*Widerspruchsannahme*) und schließt so lange auf weitere wahre Aussagen, bis eine Aussage entsteht, die im Widerspruch zur Voraussetzung, zu einem Axiom oder zur Widerspruchsannahme steht.

d) Aufteilung der Äquivalenz: Um $A \iff B$ zu zeigen, beweist man $(A \implies B) \wedge (B \implies A)$. (Man prüfe dies anhand der Wahrheitstafeln.)

e) Ringschluss: Sind mehrere Aussagen $A_1, A_2, \ldots, A_n$ als äquivalent nachzuweisen, zeigt man

$$(A_1 \implies A_2) \wedge (A_2 \implies A_3) \wedge \cdots \wedge (A_{n-1} \implies A_n) \wedge (A_n \implies A_1).$$

1.8 Bemerkung: Induktionsbeweis

Für jede natürliche Zahl n sei eine Aussage $A(n)$ formuliert. Wenn wir beweisen, dass die folgenden beiden Aussagen gelten:

(i) $A(1)$ ist wahr. (*Induktionsanfang*)

(ii) Wenn für eine natürliche Zahl n die Aussage $A(n)$ wahr ist, dann ist auch $A(n+1)$ wahr. (*Induktionsschluss* von n auf $n+1$)

Dann ist bewiesen, dass die Aussage $A(n)$ für jede natürliche Zahl n wahr ist.

Formal lautet das Induktionsprinzip:

$$(A(1) \ \wedge \ \text{“Für alle } n \in \mathbb{N} \text{ gilt } A(n) \Rightarrow A(n+1)\text{”}) \Longrightarrow \text{“Für alle } n \in \mathbb{N} \text{ gilt } A(n)\text{”}$$

1.10 Bemerkung: Varianten des Induktionsbeweises

- Als Induktionsanfang beweist man $A(n_0)$ für ein $n_0 \in \mathbb{Z}$. Gilt dann der Induktionsschluss von n nach $n+1$ für jedes $n \geq n_0$, so ist die Aussage $A(n)$ für alle $n \geq n_0$ bewiesen.

$$(A(n_0) \ \wedge \ \text{“Für alle } n \in \mathbb{Z} \text{ mit } n \geq n_0 \text{ gilt } A(n) \Rightarrow A(n+1)\text{”})$$

$$\Longrightarrow \text{“Für alle } n \in \mathbb{Z} \text{ mit } n \geq n_0 \text{ gilt } A(n)\text{”}$$

- Als Voraussetzung für den Induktionsschluss von n nach $n+1$ darf man verwenden, dass $A(k)$ wahr ist für alle $1 \leq k \leq n$:

$$(A(1) \ \wedge \ \text{“Für alle } n \in \mathbb{N} \text{ gilt } (A(1) \wedge A(2) \wedge \cdots \wedge A(n)) \Rightarrow A(n+1)\text{”})$$

$$\Longrightarrow \text{“Für alle } n \in \mathbb{N} \text{ gilt } A(n)\text{”}$$

1.11 Notation: Quantoren

Zur Abkürzung verwendet man in Aussagen die folgenden *Quantoren*:

$\forall$	heißt	“für alle”
$\exists$	heißt	“es gibt ein”, “es existiert”
$\nexists$	heißt	“es gibt kein”, “es existiert kein”

2 Mengen und Abbildungen

Im Zentrum mathematischer Theorien steht die Definition abstrakter, übergreifender Strukturen und deren Verknüpfung. Wir beginnen hier mit Begriffen aus der "Naiven Mengenlehre".

2.1 Erläuterung: *(Georg Cantor 1845 - 1918)*

Eine *Menge* ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens – welche die *Elemente* der Menge genannt werden – zu einem Ganzen.

Schreibweise:

$x \in M$	"x ist ein Element von M"
$x \notin M$	"x ist nicht ein Element von M"

2.2 Standard-Bezeichnungen

$\mathbb{N}$ die Menge der natürlichen Zahlen: $\{1,\ 2,\ 3,\ 4,\ \ldots\}$

$\mathbb{N}_0$ die Menge der natürlichen Zahlen mit Null: $\{0,\ 1,\ 2,\ 3,\ 4,\ \ldots\}$

$\mathbb{Z}$ die Menge der ganzen Zahlen: $\{\ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\}$

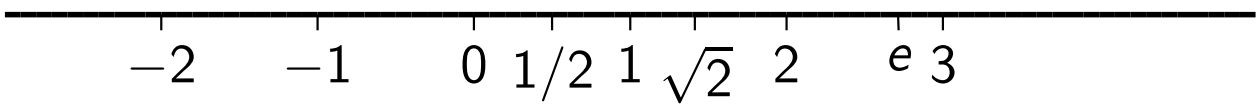
$\mathbb{Q}$ die Menge der rationalen Zahlen: $\left\{\frac{m}{n} \mid m \in \mathbb{Z},\ n \in \mathbb{N}\right\}$

$\mathbb{R}$ die Menge der reellen Zahlen

$\mathbb{C}$ die Menge der komplexen Zahlen

$\emptyset$ die leere Menge

Zur Veranschaulichung dient die Zahlengerade.



Jedem Punkt auf der Zahlengeraden entspricht genau eine reelle Zahl, und umgekehrt.

2.3 Definition

Eine Menge M heißt *endlich*, wenn sie aus nur endlich vielen Elementen besteht. In diesem Fall heißt die Anzahl der Elemente die *Mächtigkeit* oder auch *Kardinalität* von M, in Zeichen: $|M|$ oder $\#M$.

2.5 Definition: Teilmenge

a) Eine Menge N heißt *Teilmenge* einer Menge M, falls jedes Element von N auch Element von M ist. Die entsprechende Beziehung zwischen N und M heißt auch *Inklusion* (von N in M).

Bezeichnung: $N \subseteq M$.

b) Eine Menge N heißt *echte Teilmenge* einer Menge M, falls N Teilmenge von M und $N \neq M$ ist. Die entsprechende Beziehung zwischen N und M heißt auch *echte Inklusion* (von N in M).

Bezeichnung: $N \subsetneq M$ oder $N \subsetneqq M$.

Bemerkung: Die Gleichheit $M = N$ von Mengen wird oft mit folgender Äquivalenz gezeigt:

$$M = N \iff (M \subseteq N) \wedge (N \subseteq M)$$

2.6 Definition: Mengenverknüpfungen

$$
\begin{aligned}
M \cap N &= \{x \mid x \in M \text{ und } x \in N\} && \textit{Durchschnitt, Schnittmenge} \\
M \cup N &= \{x \mid x \in M \text{ oder } x \in N\} && \textit{Vereinigung} \\
M \setminus N &= \{x \mid x \in M \text{ und } x \notin N\} && \textit{Differenz(menge) “M ohne N”}
\end{aligned}
$$

Bemerkung:

a) Falls $M \cap N = \emptyset$ gilt, nennen wir M und N *disjunkt*.

b) Die Vereinigung disjunkter Mengen M und N wird auch mit $M \dot{\cup} N$ bezeichnet.

c) In manchen Situationen ist eine *Grundmenge* Ω vorgegeben und alle betrachteten Mengen sind Teilmengen von Ω. Dann (und nur dann!) verwenden wir die abkürzende Schreibweise

$$\overline{M} := \Omega \setminus M \qquad \text{oder} \qquad \complement M := \Omega \setminus M.$$

2.7 Satz: Rechenregeln

a) Kommutativität von $\cup$, $\cap$: $M \cap N = N \cap M, \quad M \cup N = N \cup M$

b) Assoziativität von $\cup$, $\cap$:
$$(L \cap M) \cap N = L \cap (M \cap N)$$
$$(L \cup M) \cup N = L \cup (M \cup N)$$

c) Distributivität von $\cup$, $\cap$:
$$L \cup (M \cap N) = (L \cup M) \cap (L \cup N)$$
$$L \cap (M \cup N) = (L \cap M) \cup (L \cap N)$$

d) Vereinfachungen: $(M \setminus N) \cup N = M \cup N, \quad (M \setminus N) \cap N = \emptyset$

e) de Morgansche Regeln:
$$L \setminus (M \cap N) = (L \setminus M) \cup (L \setminus N)$$
$$L \setminus (M \cup N) = (L \setminus M) \cap (L \setminus N)$$

2.9 Definition: Kartesisches Produkt

a) Das *kartesische Produkt*[a] zweier Mengen A und B (auch *Produktmenge*) genannt) ist definiert als

$$A \times B := \{(a, b) \mid a \in A \text{ und } b \in B\}.$$

Ein Element $(a, b) \in A \times B$ heißt *geordnetes Paar*.

b) Allgemeiner ist das *kartesische Produkt* von n Mengen $A_1, A_2, \ldots, A_n$ definiert als

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ für } i = 1, \ldots, n\}.$$

Ein Element $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$ heißt *n-Tupel*.

[a] benannt nach René Descartes, 1596 – 1650, französischer Philosoph und Mathematiker

Bemerkung: Nach Definition gilt für beliebige $a_i, b_i \in A_i$, $i = 1, \ldots, n$:

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \text{ genau dann, wenn } a_i = b_i \text{ für } i = 1, \ldots, n.$$

2.10 Satz

Für zwei endliche Mengen M und N gilt

a) $\#(M \cup N) + \#(M \cap N) = \#M + \#N$,

b) $\#(M \times N) = (\#M) \cdot (\#N)$.

2.11 Definition und Satz: Potenzmenge

Die Menge aller Teilmengen einer Menge M heißt *Potenzmenge* von M und wird mit $\mathcal{P}(M)$ bezeichnet:

$$\mathcal{P}(M) := \{X \mid X \subseteq M\}\,.$$

Wenn M endlich mit n Elementen ist, dann besteht $\mathcal{P}(M)$ aus 2^n Elementen:

$$\#\mathcal{P}(M) = 2^{\#M}\,.$$

Abbildungen

2.12 Definition: Abbildung

Es seien X und Y zwei Mengen. Eine *Abbildung* $f : X \to Y$ ist eine Vorschrift, die jedem Element $x \in X$ eindeutig ein Element $y \in Y$ zuordnet.

Man schreibt

$$f : X \to Y, \quad x \mapsto f(x),$$

und spricht "f von X nach Y, x wird abgebildet auf $f(x)$".

$f(x)$	heißt das *Bild von x unter f*.
X	heißt *Definitionsbereich*.
Y	heißt *Zielbereich, Wertevorrat, oder Zielmenge*.

Die Elemente von X heißen auch die *Argumente* der Abbildung.

2.13 Definition

Zwei Abbildungen $f : X \to Y$ und $g : X' \to Y'$ sind genau dann gleich (Schreibweisen $f = g$ oder $f \equiv g$), wenn

$$X = X' \quad \wedge \quad Y = Y' \quad \wedge \quad (\forall x \in X \ : \ f(x) = g(x))$$

gilt.

2.15 Definition: Bild, Urbild, Graph

Es sei $f : X \to Y$ eine Abbildung.

a) Für $A \subseteq X$ ist

$$\begin{aligned} f(A) &:= \{y \in Y \mid \text{ es gibt ein } a \in A \text{ mit } f(a) = y\} \\ &= \{f(a) \mid a \in A\} \end{aligned}$$

das *Bild von A unter f*. Die Menge $f(X)$ (also das Bild von ganz X unter f) heißt auch die *Bildmenge* oder einfach das *Bild* von f.

b) Für $B \subseteq Y$ ist

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\}$$

das *Urbild von B unter f*.

c) Der *Graph* ist die Menge der geordneten Paare $(x, f(x)) \in X \times Y$,

$$\text{Graph}(f) := \{(x, f(x)) \mid x \in X\} \subseteq X \times Y\,.$$

2.17 Definition

Eine Abbildung $f : X \to Y$ heißt

injektiv $:\Longleftrightarrow$ für alle $x, x' \in X$ gilt: $x \neq x' \Longrightarrow f(x) \neq f(x')$;
(Verschiedene Argumente haben verschiedene Bilder unter f.)

surjektiv $:\Longleftrightarrow$ für alle $y \in Y$ gibt es ein $x \in X$ mit $f(x) = y$;
(Jedes Element in Y kommt als Bild unter f vor.)

bijektiv $:\Longleftrightarrow$ f ist injektiv und surjektiv.

Für Selbstabbildungen $f : M \to M$ einer **endlichen** Menge M fallen die drei Begriffe injektiv, surjektiv, bijektiv wieder zusammen. Dies kann man sich mit Pfeildiagrammen leicht veranschaulichen.

2.19 Satz

Es sei M eine endliche Menge und $f : M \to M$ eine Abbildung. Dann sind die folgenden Aussagen äquivalent:

a) f ist injektiv.

b) f ist bijektiv.

c) f ist surjektiv.

2.20 Definition: Komposition

Es seien $f : X \to Y$ und $g : Y' \to Z$ zwei Abbildungen und es gelte $Y \subseteq Y'$; d.h. der Zielbereich von f ist im Definitionsbereich von g enthalten. Die *Komposition*, *Verkettung* oder *Hintereinanderausführung*

$$g \circ f : X \to Z$$

(lies: „g nach f“) ist definiert durch

$$(g \circ f)(x) = g(f(x)) \text{ für alle } x \in X\,.$$

Beachte: Die Reihenfolge beim Einsetzen der Argumente (d.h. Einsetzen von x in f und Einsetzen von $f(x)$ in g) geschieht “von rechts nach links”.

2.21 Bemerkung

Die Komposition ist *assoziativ*: Für Abbildungen $f : X \to Y$, $g : Y' \to Z$ und $h : Z' \to W$, mit $Y \subseteq Y'$ und $Z \subseteq Z'$, gilt

$$h \circ (g \circ f) = (h \circ g) \circ f : X \to W.$$

Sie ist im Allgemeinen **nicht** *kommutativ*.

2.22 Definition und Proposition: identische Abbildung

a) Es sei X eine Menge. Die *identische Abbildung*

$$\mathrm{id}_X : X \to X$$

ist definiert durch $\mathrm{id}_X(x) = x$ für alle $x \in X$.

b) Es seien X und Y Mengen. Für jede Abbildung $f : X \to Y$ gilt dann

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f\,.$$

2.23 Definition: Umkehrabbildung

Es sei $f : X \to Y$ eine Abbildung. Dann heißt eine weitere Abbildung $g : Y \to X$ *inverse Abbildung* oder *Umkehrabbildung*, wenn

$$g \circ f = \mathrm{id}_X \qquad \text{und} \qquad f \circ g = \mathrm{id}_Y$$

gilt.

2.24 Satz

Es sei $f : X \to Y$ eine Abbildung.

a) Genau dann besitzt f eine inverse Abbildung, wenn f bijektiv ist.

b) Falls f eine inverse Abbildung besitzt, so ist diese eindeutig. Sie ist gegeben durch $f^{-1} : Y \to X$ mit der Zuordnungsvorschrift

$$f^{-1}(y) = x \qquad \Longleftrightarrow \qquad f(x) = y.$$

2.25 Satz: Rechenregeln für die inverse Abbildung

Es seien $f : X \to Y$ und $g : Y \to Z$ bijektive Abbildungen. Dann ist die Komposition $g \circ f : X \to Z$ ebenfalls bijektiv, und die inverse Abbildung ist

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1} : Z \to X.$$

2.26 Satz

Es seien $f : X \to Y$ und $g : Y \to Z$ zwei injektive (surjektive, bijektive) Abbildungen. Dann ist auch die Verkettung $g \circ f$ injektiv (bzw. surjektiv, bijektiv).

Die Mächtigkeit von Mengen

2.27 Definition: gleichmächtige Mengen

a) Eine Menge M heißt *gleichmächtig* zu einer Menge N, falls eine bijektive Abbildung $f : M \to N$ existiert.

b) Eine Menge M heißt *abzählbar*, falls sie gleichmächtig zur Menge der natürlichen Zahlen ist.

Bemerkung:

a) Endliche Mengen M und N sind genau dann gleichmächtig, wenn $\#M = \#N$ gilt. Der Beweis ist ganz ähnlich zu Satz 2.19. Was folgt daraus?

Falls $\#M = n$ mit $n \in \mathbb{N}$ gilt, so gibt es eine *Aufzählung* der Elemente von M,

$$M = \{x_1, \ldots, x_n\}.$$

Dies ist gleichbedeutend mit der bijektiven Abbildung

$$\{1, 2, \ldots, n\} \to M \quad , \quad i \mapsto x_i \, .$$

Bemerkung (fortges.):

b) Auch die Elemente abzählbarer Mengen lassen sich "aufzählen", allerdings durch eine *unendliche Folge* mit paarweise verschiedenen Folgengliedern,

$$M = \{x_1, x_2, x_3, \ldots\}.$$

Dies entspricht der Bijektion

$$\mathbb{N} \to M \ , \quad i \mapsto x_i \, .$$

c) Verwendet man anstatt der Bijektion $f : M \to N$ die inverse Abbildung $f^{-1} : N \to M$, so erkennt man, dass die Gleichmächtigkeit von Mengen eine *symmetrische* Eigenschaft ist: M ist gleichmächtig zu N genau dann, wenn N gleichmächtig zu M ist.

3 Primfaktorzerlegung und Euklidischer Algorithmus

Bereits die natürlichen und die ganzen Zahlen geben in der Geschichte der Mathematik Anlass zu umfangreichen strukturellen Überlegungen. Man denke nur an die Primfaktorzerlegung (*Fundamentalsatz der Arithmetik*) oder den erst 1993/95 bewiesenen *Großen Satz von Fermat*[1], der ca. 350 Jahre unbewiesen blieb.

Die allgemeine Vertrautheit mit den ganzen Zahlen nutzen wir, um unsere ersten strukturellen Überlegungen anzustellen. Diese Überlegungen sind auch im Mathematikunterricht verwertbar, da nur einfache Rechenmethoden aus der Unterstufe benötigt werden. Die hier gewählte Darstellung ist jedoch für den Einsatz im Schulunterricht noch nicht geeignet, da sie streng formalisiert ist.

[1] Pierre de Fermat, 1607/8 – 1665, französischer Mathematiker und Jurist

3.A Axiomatische Definition von $\mathbb{N}_0$ und $\mathbb{Z}$

Die *Peano-Axiome*[2] sind eine abstrakte Charakterisierung der Menge $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$. Wir wählen eine Beschreibung, die der heutigen Sprechweise angemessen ist.

3.1 Die natürlichen Zahlen

Die Menge $\mathbb{N}_0$ ist durch die folgenden Festlegungen eindeutig bestimmt:

1. $0 \in \mathbb{N}_0$.
2. Es gibt eine injektive Abbildung $s : \mathbb{N}_0 \to \mathbb{N}_0 \setminus \{0\}$ (die "Nachfolge-Operation").
3. Für jede Menge X gilt: Enthält X die 0 und mit jedem $n \in \mathbb{N}_0$ auch den Nachfolger $s(n)$, so gilt $\mathbb{N}_0 \subset X$.

[2] Giuseppe Peano, Turin, 1858 – 1932

3.2 Rechengesetze und Anordnung natürlicher Zahlen

Peano definierte rekursiv die Operationen der

Addition: $n + 0 = n, \qquad n + s(m) = s(n + m),$

Multiplikation: $n \cdot 0 = 0, \qquad n \cdot s(m) = n \cdot m + n$

der natürlichen Zahlen (mit 0). Setzt man noch $1 := s(0)$, so ist die Nachfolge-Operation offensichtlich gegeben durch

$$s(n) = s(n + 0) = n + s(0) = n + 1.$$

Dies führt zu den üblichen Rechenoperationen auf $\mathbb{N}_0$: Es gelten die Kommutativ-, Assoziativ- und Distributivgesetze für Addition und Multiplikation. Auch die übliche Anordnung

$$0 < 1 < 2 < 3 < \cdots$$

wird axiomatisch definiert durch

$$a < b \quad :\Longleftrightarrow \quad \exists x \in \mathbb{N} : \ a + x = b.$$

Eine axiomatische Einführung der ganzen Zahlen ist nun ein kleiner Schritt.

3.3 Axiomatische Beschreibung von $\mathbb{Z}$

1. Die Menge der ganzen Zahlen $\mathbb{Z}$ enthält die natürlichen Zahlen $\mathbb{N}_0$ als Teilmenge.
2. Zu jedem Paar $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ ist eine Zahl $a + b \in \mathbb{Z}$ definiert derart, dass gilt:
   a) Für alle $a, b, c \in \mathbb{Z}$ ist $(a + b) + c = a + (b + c)$. (Assoziativgesetz)
   b) Für alle $a, b \in \mathbb{Z}$ ist $a + b = b + a$. (Kommutativgesetz)
   c) Das Element $0 \in \mathbb{Z}$ erfüllt $0 + a = a$ für alle $a \in \mathbb{Z}$ (neutrales Element).
   d) Zu jedem Element $a \in \mathbb{Z}$ gibt es ein Element $-a \in \mathbb{Z}$ (das *Negative* zu a), so dass $a + (-a) = 0$ ist.

   Für $a, b \in \mathbb{N}$ hat $+$ dabei die frühere Bedeutung.
3. Zu jedem Paar $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ ist eine Zahl $a \cdot b \in \mathbb{Z}$ definiert derart, dass gilt:
   a) Für alle $a, b, c \in \mathbb{Z}$ ist $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (Assoziativgesetz)
   b) $a \cdot b = b \cdot a$ (Kommutativgesetz)
   c) Für alle $a, b, c \in \mathbb{Z}$ gilt $a \cdot (b + c) = a \cdot b + a \cdot c$. (Distributivgesetz)

   Für $a, b \in \mathbb{N}$ hat $a \cdot b$ dabei die frühere Bedeutung.

4. Wenn man für zwei Elemente $a, b \in \mathbb{Z}$ die "Relation"

$$a < b \quad :\Longleftrightarrow \quad \exists x \in \mathbb{N} : \; a + x = b,$$

definiert, dann gilt für zwei beliebige Elemente $a, b \in \mathbb{Z}$ genau eine der folgenden drei Alternativen:

$$a < b \quad \text{oder} \quad a = b \quad \text{oder} \quad b < a.$$

d.h. die Relation "$<$" definiert eine *totale Ordnung* auf $\mathbb{Z}$.

Als weitere Grundoperation in $\mathbb{Z}$ führen wir ein:

3.4 Definition und Satz: Division mit Rest

a) Es seien $a, b \in \mathbb{Z}$. a heißt *teilbar* durch b, wenn eine Zahl $q \in \mathbb{Z}$ existiert mit $a = qb$.

Schreibweisen: $b \mid a$ b teilt a
$b \nmid a$ b teilt a nicht

b) Es sei $b \in \mathbb{N}$. Dann gibt es zu jedem $a \in \mathbb{Z}$ eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, b-1\}$ so, dass

$$a = qb + r$$

gilt. q heißt der *Quotient* und r heißt der *Rest* von a bei Division durch b.

Schreibweisen: $r = a \bmod b$ oder $r = a \,\%\, b$.

3.B Die eindeutige Primzahlzerlegung natürlicher Zahlen

Der folgende Begriff ist sicher bekannt.

3.5 Definition: Primzahl

Eine natürliche Zahl p mit $p > 1$ heißt *Primzahl*, falls sie nicht als Produkt zweier kleinerer Zahlen dargestellt werden kann. Mit anderen Worten:

$$p = ab \text{ mit } a, b \in \mathbb{N} \quad \Longrightarrow \quad a = 1 \text{ oder } b = 1$$

Der folgende (bekannte) Satz ist nicht so harmlos, wie er auf den ersten Blick aussehen mag.

3.6 Fundamentalsatz der Arithmetik: Eindeutige Primfaktorzerlegung

a) Jede natürliche Zahl $n > 1$ lässt sich als ein Produkt

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

mit Prinzahlen $p_1, p_2, \ldots, p_r \in \mathbb{N}$ schreiben.

b) Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren. D.h., wenn auch

$$n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

mit Primzahlen q_j, $j = 1, \ldots, s$, gilt, so ist $r = s$, und wenn wir ferner

$$p_1 \leq p_2 \leq \ldots \leq p_r \quad \text{und} \quad q_1 \leq q_2 \leq \ldots \leq q_r$$

annehmen, so ist $p_i = q_i$ für $i = 1, \ldots, r$.

Die Eindeutigkeit der Zerlegung in Primfaktoren wird bewiesen mit Hilfe einer zweiten charakteristischen Eigenschaft der Primzahlen.

3.7 Lemma

Wenn eine Primzahl ein Produkt teilt, so teilt sie wenigstens einen der Faktoren:

$$(p \text{ Primzahl} \quad \wedge \quad a, b \in \mathbb{N} \quad \wedge \quad p \mid ab) \quad \Longrightarrow \quad (p \mid a \quad \vee \quad p \mid b)\,.$$

Wenn allgemeiner eine Primzahl p ein Produkt $a_1 a_2 \ldots a_s$ teilt, dann teilt sie einen der Faktoren.

Bemerkung: Man mache sich klar, dass die Aussage nicht einfach aus der Definition einer Primzahl folgt, sondern dass hier eine andere Eigenschaft von Primzahlen beschrieben wird. In allgemeineren algebraischen Strukturen als $\mathbb{Z}$ (sog. Ringen) werden Elemente, die die Eigenschaft im obigen Hilfssatz besitzen, "Primelemente" genannt. Hingegen werden Elemente, die die Eigenschaft in Definition 3.5 besitzen, als "unzerlegbar" (oder "irreduzibel") bezeichnet. In allgemeinen Ringen sind diese Begriffe nicht deckungsgleich!

Den Beweis von Lemma 3.7 verschieben wir ans Ende dieses Abschnitts. Wir benötigen zuerst den (ebenfalls bekannten) Begriff des *größten gemeinsamen Teilers* ggT:

3.8 Satz: Größter gemeinsamer Teiler

Gegeben seien zwei ganze Zahlen $a, b \in \mathbb{Z}$, wovon wenigstens eine von Null verschieden ist. Dann gibt es eine ganze Zahl g mit folgenden Eigenschaften:

(1) $g \mid a$ und $g \mid b$;

(2) für $d \in \mathbb{Z}$ gilt: $(d \mid a \quad \wedge \quad d \mid b) \quad \Rightarrow \quad d \mid g$.

In Worten: g ist ein Teiler von a und von b, und jede ganze Zahl, die gleichzeitig a und b teilt, ist ein Teiler von g.

3.9 Bemerkung:

a) Die Eigenschaften (1) und (2) gelten gleichzeitig für g und $-g$. Wählen wir $g > 0$, so ist die Bezeichnung

$$g = \mathrm{ggT}(a, b) \qquad \text{größter gemeinsamer Teiler}$$

gerechtfertigt, weil g die *größte* natürliche Zahl ist, die sowohl a als auch b teilt.

b) Für $a = 0$ und $b = 0$ ist der ggT nicht definiert.

Der Beweis des Satzes vom ggT wird sich aus folgendem Verfahren ergeben.

3.10 Euklidischer Algorithmus

1. Eingabe: $a \in \mathbb{Z}$, $b \in \mathbb{N}$.
2. Teile a durch b mit Rest r.
3. Ersetze a durch b, ersetze b durch r.
4. Wiederhole Schritt 2 und Schritt 3 mit den neuen Zahlen so lange, bis der Rest 0 wird. Dieses geschieht in endlich vielen Schritten, da b (bzw. r) im Laufe des Verfahrens immer kleiner wird.
5. Ausgabe: der letzte von Null verschiedene Rest

3.12 Satz: Lemma von Bézout

Der größte gemeinsame Teiler g zweier ganzer Zahlen a und b besitzt eine Darstellung

$$g = xa + yb \text{ mit } x, y \in \mathbb{Z}\,.$$

3.13 Der erweiterte euklidische Algorithmus

Gegeben seien ganze Zahlen $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Definiere rekursiv die Zahlen a_k, b_k, r_k, q_k wie im Euklidischen Algorithmus und zusätzlich $x_k, y_k \in \mathbb{Z}$ durch

$$a_0 := a;\ b_0 := b; \qquad x_{-2} := 1;\ y_{-2} = 0; \qquad x_{-1} := 0;\ y_{-1} = 1;$$

Für $k = 0, 1, 2, \ldots$, solange $b_k \neq 0$:

$$\begin{aligned} r_k &:= a_k \bmod b_k; & q_k &:= (a_k - r_k)/b_k; \\ x_k &:= x_{k-2} - q_k x_{k-1}; & y_k &:= y_{k-2} - q_k y_{k-1}; \\ a_{k+1} &:= b_k; & b_{k+1} &:= r_k. \end{aligned}$$

Sei ℓ der kleinste Index mit $r_\ell = 0$. Dann gilt $g := \mathrm{ggT}(a, b) = r_{\ell-1}$ sowie

$$g = x_{\ell-1} a + y_{\ell-1} b.$$