Unterlagen zur Vorlesung
Algebra und Geometrie in der Schule:
Grundwissen über Mengen, Funktionen, Ganze Zahlen und Rationale Zahlen

Sommersemester 2010

Franz Pauer

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT INNSBRUCK,
TECHNIKERSTRASSE 13, 6020 INNSBRUCK, AUSTRIA

KAPITEL 1

Mengen und Funktionen

§1. Mengen

Definitionen setzen Vorwissen voraus. Zum Beispiel setzt die Definition

„Ein Quadrat ist ein gleichseitiges Rechteck“

voraus, dass bekannt ist, was „gleichseitig“ und „Rechteck“ bedeuten. Die Definition

„Eine gerade Zahl ist eine ganze Zahl, die von 2 geteilt wird“

setzt voraus, dass bekannt ist, was „ganze Zahl“ und „teilen“ bedeuten. Für Definitionen wird häufig die folgende Kurzschreibweise verwendet:

zu definierender Begriff := *definierende (schon bekannte) Begriffe* .

Zum Beispiel:

Quadrat := gleichseitiges Rechteck

(in Worten: ein *Quadrat* ist ein gleichseitiges Rechteck)
und

gerade Zahl := ganze Zahl, die von 2 geteilt wird

(in Worten: eine *gerade Zahl* ist eine ganze Zahl, die von 2 geteilt wird).

Der Begriff „Menge“ ist jedoch ein Grundbaustein der Mathematik, der nicht definiert, sondern nur umschrieben wird: Eine *Menge* ist eine Zusammenfassung unterscheidbarer Objekte. Diese heißen *Elemente* der Menge.

Eine Menge kann auf zwei Arten angegeben werden:

(1) durch Anschreiben der Elemente zwischen geschweiften Klammern, zum Beispiel $\{7,3,5,8,1\}$, $\{\text{Meier, Müller}\}$;
oder

(2) durch ihre Eigenschaften, zum Beispiel
$\{n \mid n \text{ ganze Zahl, } n \text{ ist größer als 0 und kleiner als 7}\}$
(Sprechweise: „die Menge aller n, für die gilt: n ist eine ganze Zahl, die größer als 0 und kleiner als 7 ist“ oder „die Menge aller ganzen Zahlen, die größer als 0 und kleiner als 7 sind“).

Bezeichnungen:

$\emptyset := \{\}$	*leere Menge* (Menge ohne Elemente)
$\mathbb{N} := \{0,1,2,3,\ldots\}$	Menge der *natürlichen Zahlen*
$\mathbb{Z} := \{0,1,-1,2,-2,\ldots\}$	Menge der *ganzen Zahlen*

Wenn a und b ganze Zahlen sind, schreiben wir $a < b$ bzw. $a \leq b$ bzw. $a > b$ bzw. $a \geq b$ für „a ist kleiner als b“ bzw. „a ist kleiner oder gleich b“ bzw. „a ist größer als b“ bzw. „a ist größer oder gleich b“.

Ist M eine Menge, so wird

$$e \in M$$

für „e ist ein Element von M“ geschrieben, und analog

$$e \notin M$$

für „e ist kein Element von M“.

Auf logische Probleme, die bei der Einführung des Begriffes „Menge“ auftreten, gehen wir hier nicht ein. Das „Russell'sche Paradoxon“ zeigt, dass man nicht zu sorglos sein darf:

$$\text{Gilt für } M := \{A \mid A \text{ Menge}, A \notin A\} \text{ die Beziehung } M \in M \text{ ?}$$

Definition 1: M und N seien Mengen. M heißt *Teilmenge* von N, in Zeichen

$$M \subset N \quad \text{oder} \quad M \subseteq N\,,$$

wenn jedes Element von M auch Element von N ist.

$$M \not\subset N$$

bedeutet, dass M nicht Teilmenge von N ist. Die Mengen M und N sind *gleich*, in Zeichen

$$M = N\,,$$

wenn $M \subset N$ und $N \subset M$ ist. Falls M und N nicht gleich sind, schreibt man

$$M \neq N\,.$$

Schließlich bedeutet

$$M \subsetneq N\,,$$

dass $M \subset N$ und $M \neq N$ ist, und man nennt M eine *echte* Teilmenge von N.

Beispiel 1: Für alle Mengen N ist $N \subseteq N$ und $\emptyset \subseteq N$. Es ist $\{a,b,c\} = \{b,a,c\} = \{c,a,b\}$, beim Anschreiben der Elemente einer Menge kann die Reihenfolge also beliebig gewählt werden.

§2. Durchschnitt, Vereinigung und Komplement

Definition 2: M und N seien Mengen. Der *Durchschnitt* von M und N ist die Menge

$$M \cap N := \{a \mid a \in M \text{ und } a \in N\}\,.$$

Die Mengen M und N sind *disjunkt*, wenn ihr Durchschnitt leer ist.
Die *Vereinigung* von M und N ist die Menge

$$M \cup N := \{a \mid a \in M \text{ oder } a \in N\} ,$$

wobei mit „oder“ das einschließende Oder („und-oder“) und nicht das ausschließende Oder („entweder-oder“) gemeint ist. Das *Komplement* von N in M bzw. die *Mengendifferenz* von M und N ist

$$M \setminus N := \{a \mid a \in M \text{ und } a \notin N\} .$$

Definition 3 : Sind M, N und P Mengen, so bedeutet

$$M \cap (N \cup P) ,$$

dass zuerst die Vereinigung von N und P gebildet wird und danach der Durchschnitt von M mit $N \cup P$. Analog wird für andere Verknüpfungen die Reihenfolge durch Klammerung festgelegt.

§3. Funktionen

M und N seien Mengen. Eine *Abbildung* oder *Funktion* von M nach N ist eine Vorschrift, die jedem Element von M genau ein Element von N zuordnet. M heißt dann der *Definitionsbereich* der Funktion, N der *Bildbereich*. Die Schreibweisen

$$f : M \to N , m \mapsto f(m) ,$$

oder

$$\begin{array}{rccc} f: & M & \longrightarrow & N \\ & m & \mapsto & f(m) \end{array}$$

bedeuten, dass f eine Funktion von M nach N ist, die dem Element $m \in M$ das Element $f(m) \in N$ zuordnet. Das Element $f(m)$ heißt *Bild* von m (bezüglich f). Ein Element $m \in M$ mit $f(m) = n \in N$ heißt ein *Urbild* von n (bezüglich f).

Beispiel 2 : Die Funktion

$$f : \mathbb{N} \to \mathbb{Z} , z \mapsto 2z - 3 ,$$

ordnet jeder natürlichen Zahl z die ganze Zahl $2z - 3$ zu. Das Bild von 0 bzw. 1 bzw. 2 bezüglich f ist -3 bzw. -1 bzw. 1.

Definition 4 : Seien $f : M \to N$ und $g : P \to Q$ Funktionen. Dann sind f und g *gleich*, in Zeichen

$$f = g ,$$

wenn gilt: $M = P$, $N = Q$ und für alle $m \in M$ ist $f(m) = g(m)$.

Definition 5 : Sei M eine beliebige Menge. Dann heißt die Funktion

$$\mathrm{Id}_M : M \to M\,,\ m \mapsto m\,,$$

die *identische Funktion* oder *Identität* auf M.

Definition 6 : Sei $f : M \to N$ eine Funktion, $A \subset M$ und $B \subset N$. Dann heißt

$$f(A) := \{f(a) \mid a \in A\} \subset N$$

das *Bild* von A (bezüglich f),

$$\mathrm{Bild}(f) := f(M)$$

heißt das *Bild von* f, und

$$f^{-1}(B) := \{m \in M \mid f(m) \in B\}$$

heißt das *Urbild* von B (bezüglich f). Die Funktion

$$f|_A : A \to N,\ a \mapsto f(a),$$

heißt die *Einschränkung* von f auf A. Man sagt „f bildet A auf B ab“, wenn $f(A) = B$ ist.

Definition 7 : Seien $f : M \to N$ und $g : P \to Q$ Funktionen mit

$$Bild(f) \subset P\,.$$

Dann heisst die Funktion

$$g \circ f : M \to Q,\ m \mapsto g(f(m)),$$

die *Hintereinanderausführung* oder *Zusammensetzung* von f und g (sprich „g nach f“). Oft wird statt $g \circ f$ nur gf geschrieben.

Satz 1 : *Seien $f : M \to N$, $g : P \to Q$ und $h : R \to S$ Funktionen mit* $\mathrm{Bild}(f) \subset P$ *und $Bild(g) \subset R$. Dann gilt*

$$h \circ (g \circ f) = (h \circ g) \circ f =: h \circ g \circ f\,,$$

d.h. bei mehrfacher Hintereinanderausführung von Funktionen kommt es nicht auf die Reihenfolge an (die Hintereinanderausführung von Funktionen ist assoziativ).

Beweis: Sowohl $h \circ (g \circ f)$ als auch $(h \circ g) \circ f$ sind Funktionen von M nach S. Für jedes $m \in M$ ist

$$\begin{aligned}(h \circ (g \circ f))(m) &= h((g \circ f)(m)) = h(g(f(m))) = (h \circ g)(f(m)) \\ &= ((h \circ g) \circ f)(m).\end{aligned}$$

Definition 8 : Eine Funktion $f : M \to N$ heißt *injektiv* bzw. *surjektiv*, wenn jedes Element von N höchstens bzw. mindestens ein Urbild hat. Eine Funktion $f : M \to N$ heißt *bijektiv*, wenn jedes Element von N genau ein Urbild hat.
Wenn $f : M \to N$ bijektiv ist, dann heißt die (ebenfalls bijektive) Funktion

$$f^{-1} : N \to M, n \mapsto \text{Urbild von } n \text{ bezüglich } f,$$

die zu f *inverse* Funktion oder die *Umkehrfunktion* von f.

Eine Funktion ist also genau dann bijektiv, wenn sie sowohl injektiv als auch surjektiv ist. Eine Funktion ist genau dann surjektiv, wenn ihr Bild und ihr Bildbereich gleich sind. Eine Funktion ist genau dann injektiv, wenn die Bilder von je zwei verschiedenen Elementen wieder verschieden sind.

Definition 9 : Eine Menge M heißt *endlich*, wenn sie leer ist oder es ein $n \in \mathbb{N}$ und eine bijektive Funktion $f : \{1, \ldots, n\} \to M$ gibt. Man nennt dann

$$\#(M) := n$$

die *Anzahl der Elemente* von M. Die leere Menge hat 0 Elemente.
M heißt *unendlich*, wenn M nicht endlich ist.

§4. Familien, Tupel, Folgen und kartesisches Produkt

Eine Funktion $f : I \to M$ wird manchmal in der Form

$$(f(i))_{i \in I} \quad \text{oder} \quad (f_i)_{i \in I}$$

geschrieben und als *Familie* von Elementen in M, indiziert durch I, bezeichnet. I heißt dann die *Indexmenge* der Familie $(f_i)_{i \in I}$. Die Familie $(f_i)_{i \in I}$ heißt *endlich*, wenn I endlich ist.
Wichtige Spezialfälle sind:

(1) Eine Funktion $x : \{1, 2, \ldots, n\} \to M$, $i \mapsto x(i)$, wird in der Form

$$(x_1, \ldots, x_n) = (x_i)_{1 \leq i \leq n} = (x_i)_{i \in \{1, \ldots, n\}}$$

geschrieben und heißt ein *n-Tupel von Elementen in M*. Das Element x_i heißt dann *i-te Komponente* von $(x_1, \ldots, x_n)$. In den Spezialfällen $n = 2, 3$ nennt man $(x_1, \ldots, x_n)$ ein *Paar* bzw. *Tripel*. Die Menge aller n-Tupel von Elementen in M wird mit

$$M^n$$

bezeichnet (sprich „M hoch n“). Für $x, y \in M^n$ gilt

$$x = y$$

genau dann, wenn $x_i = y_i$ für $i = 1, \ldots, n$ ist.

(2) Sei $m \in \mathbb{N}$ und $I := \{i \in \mathbb{N} \mid i \geq m\}$. Eine Funktion $x : I \to M$, $i \mapsto x(i)$, wird in der Form

$$(x_i)_{i \geq m}$$

geschrieben und heißt eine *Folge* in M. Man beachte, dass

$$(x_i)_{i \geq m} \neq \{x_i \mid i \geq m\}$$

ist. Ein Paar (a,b) enthält „mehr Information“ als die Menge $\{a,b\}$. Es ist $\{a,b\} = \{b,a\}$, aber $(a,b) = (b,a)$ nur dann, wenn $a = b$.

Definition 10 : M und N seien Mengen. Dann heißt

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

das *kartesische Produkt* von M und N. Die Funktionen

$$\pi_1 : M \times N \to M, (x,y) \mapsto x, \quad \text{und} \quad \pi_2 : M \times N \to N, (x,y) \mapsto y,$$

heißen *Projektionen* auf den ersten bzw. zweiten Faktor.

Definition 11 : Sei $f : M \to N$ eine Funktion. Dann heißt die Menge

$$\text{Graph}(f) := \{(m, f(m)) \mid m \in M\} \subset M \times N$$

der *Graph* von f.

Satz 2 : *Zwei Funktionen von M nach N sind genau dann gleich, wenn ihre Graphen gleich sind.*

Beweis: Es ist zu zeigen:

1. Wenn zwei Funktionen von M nach N gleich sind, dann sind auch ihre Graphen gleich.
2. Wenn die Graphen zweier Funktionen von M nach N gleich sind, dann sind diese zwei Funktionen gleich.

Seien f und g Funktionen von M nach N.
Zu 1): Wenn $f = g$ ist, dann ist $f(m) = g(m)$ für alle $m \in M$. Daher ist

$$\text{Graph}(f) = \{(m, f(m)) \mid m \in M\} =$$

$$= \{(m, g(m)) \mid m \in M\} = \text{Graph}(g).$$

Zu 2): Wenn $\text{Graph}(f) = \text{Graph}(g)$ ist, dann ist für alle $m \in M$ das Paar $(m, f(m))$ ein Element von $\text{Graph}(g)$. In $\text{Graph}(g)$ gibt es genau ein Element, dessen erste Komponente m ist, nämlich $(m, g(m))$. Also ist $f(m) = g(m)$ für alle $m \in M$, somit ist $f = g$.

Definition 12 : Sei $(M_i)_{i\in I}$ eine Familie von Mengen. Dann heißt

$$\prod_{i\in I} M_i := \{(x_i)_{i\in I} \mid \text{für alle } i \in I \text{ ist } x_i \in M_i\}$$

das *kartesische Produkt* der Mengen M_i, $i \in I$. Für $j \in I$ heißt

$$\pi_j : \prod_{i\in I} M_i \to M_j\,,\ (x_i)_{i\in I} \mapsto x_j\,,$$

die *Projektion* auf den j-ten Faktor.
Im Spezialfall $I = \{1,\ldots,n\}$ wird für $\prod_{i\in I} M_i$ auch

$$\prod_{i=1}^{n} M_i \qquad \text{oder} \qquad M_1 \times \ldots \times M_n$$

geschrieben.

§5. Zusammengesetzte Aussagen

Wir betrachten Aussagen $A, B, C, \ldots$, die nach Vereinbarung entweder wahr oder falsch sind. Mit Hilfe der Worte

„und“	(Zeichen: $\wedge$) ,
„oder“	(Zeichen: $\vee$) ,
„nicht“	(Zeichen: $\neg$) ,
„wenn, dann“	(Zeichen: $\Rightarrow$) ,
„genau dann, wenn“	(Zeichen: $\Leftrightarrow$)

bilden wir *zusammengesetzte* Aussagen, deren „Wahrheitswert“ wir durch die folgende Tabelle definieren. Dabei steht w für „wahr“ und f für „falsch“.

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	w	w	f	w	w
w	f	f	w	f	f	f
f	w	f	w	w	w	f
f	f	f	f	w	w	w

Für $A \Rightarrow B$ verwendet man statt „wenn A, dann B“ auch die Sprechweisen „aus A folgt B“ oder „A impliziert B“.
Man beachte:
A ist genau dann wahr, wenn $\neg A$ falsch ist. Das wird für *indirekte Beweise* verwendet: anstatt zu zeigen, dass eine Aussage A wahr ist, wird gezeigt, dass ihr „Gegenteil“ $\neg A$ falsch ist.
In der Mathematik bedeutet das Wort „oder“ immer das nicht ausschließende „und-oder“ und nicht das ausschließende „entweder-oder“.
Ist A falsch, dann ist die Aussage $A \Rightarrow B$ immer wahr („ex falso quodlibet“).

§6. Der Induktionsbeweis

Sei m eine natürliche Zahl (meistens 0 oder 1) und sei $(A_m, A_{m+1}, A_{m+2}, \ldots)$ eine Folge von Aussagen.

Satz 3 : *Wenn*

(1) A_m *wahr ist und*
(2) *für alle* $n > m$ *aus* A_{n-1} *auch* A_n *folgt,*

dann sind alle Aussagen A_n , $n \geq m$, *wahr.*

Damit erhält man eine Methode, die Gültigkeit der Aussagen A_n, $n \geq m$, zu zeigen („*Beweis durch vollständige Induktion*"): Es genügt zu zeigen, dass (1) (*Induktionsanfang*) und (2) (*Induktionsschluss*) richtig sind.

Beweis: Wir benutzen die folgende Eigenschaft der natürlichen Zahlen: jede Teilmenge von $\mathbb{N}$ hat ein kleinstes Element. Wir führen den Beweis indirekt und nehmen an, dass nicht alle Aussagen A_n , $n \geq m$, wahr sind. Dann ist die Menge

$$M := \{n \in \mathbb{N} \mid n \geq m \text{ und } A_n \text{ ist falsch}\}$$

nicht leer. Daher gibt es eine kleinste Zahl k so, dass $k \geq m$ und A_k falsch ist. Wegen (1) gilt $k \geq m+1$, also $k-1 \geq m$. Weiters muss A_{k-1} wahr sein, weil k die kleinste Zahl in M ist. Aus (2) folgt nun, dass auch A_k wahr ist, was einen Widerspruch bedeutet. Somit muss unsere Annahme am Anfang des Beweises falsch sein, d.h. alle Aussagen A_n , $n \geq m$, sind wahr.

Satz 4 : *Sei n eine natürliche Zahl. Die Summe der Quadrate aller natürlichen Zahlen von* 1 *bis n ist* $S(n) := \frac{1}{6}(2n^3 + 3n^2 + n)$.

Beweis: Induktionsanfang: $S(1) = \frac{1}{6}(2+3+1) = 1 = 1^2$, also ist die Aussage für $n = 1$ wahr.
Induktionsschluss: Wir nehmen an, dass die Summe der Quadrate aller natürlichen Zahlen von 1 bis $n-1$ gleich $S(n-1)$ ist. Die Summe der Quadrate aller natürlichen Zahlen von 1 bis n ist dann

$$S(n-1) + n^2 \ .$$

Wegen

$$S(n-1) + n^2 = \frac{1}{6}(2(n-1)^3 + 3(n-1)^2 + n - 1) + n^2 = S(n)$$

ist die Behauptung richtig.

KAPITEL 2

Rechnen mit ganzen und rationalen Zahlen

§1. Rechenregeln für ganze Zahlen

Für die Menge $\mathbb{Z} := \{\ldots,-2,-1,0,1,2,\ldots\}$ der ganzen Zahlen mit der Addition $\mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$, $(a,b) \longmapsto a+b$, und der Multiplikation $\mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$, $(a,b) \longmapsto a\cdot b$, gelten die folgenden Rechenregeln: Sind a,b,c ganze Zahlen, dann ist

- $(a+b)+c = a+(b+c) =: a+b+c$ („Die Addition von ganzen Zahlen ist assoziativ“, das heißt: auf Klammern kann verzichtet werden).
- $0+a = a+0 = a$ (0 ist das neutrale Element der Addition)
- $a+(-a) = (-a)+a = 0$ (dabei ist $-a := (-1)\cdot a$; $-a$ ist das bezüglich der Addition zu a inverse Element)
- $a+b = b+a$ („Die Addition ist kommutativ“).
- $(a\cdot b)\cdot c = a\cdot(b\cdot c) =: a\cdot b\cdot c$ („Die Multiplikation ist assoziativ“).
- $1\cdot a = a\cdot 1 = a$ (1 ist das neutrale Element der Multiplikation)
- $a\cdot b = b\cdot a$ („Die Multiplikation ist kommutativ“).
- $(a+b)\cdot c = (a\cdot c)+(b\cdot c) =: a\cdot c+b\cdot c$ („Distributivgesetz“)

Kurzsprechweise: Die Menge der ganzen Zahlen mit Addition und Multiplikation ist ein kommutativer Ring.

Sind $m,n\in\mathbb{N}$, $m\le n$ und $a_m,a_{m+1},\ldots,a_n\in\mathbb{Z}$, dann schreiben wir

$$\sum_{i=m}^{n} a_i$$

für $a_m+a_{m+1}+\ldots+a_n$ und

$$\prod_{i=m}^{n} a_i$$

für $a_m\cdot a_{m+1}\cdot\ldots\cdot a_n$. (Sprechweise: „Die Summe bzw. das Produkt aller a_i mit i von m bis n“).
Man prüft leicht nach:
Wenn f eine bijektive Funktion von $\{i \mid m\le i\le n\}$ nach $\{i \mid m\le i\le n\}$ ist, dann ist

$$\sum_{i=m}^{n} a_i = \sum_{i=m}^{n} a_{f(i)}$$

und

$$\prod_{i=m}^{n} a_i = \prod_{i=m}^{n} a_{f(i)}\ .$$

Seien $p,q \in \mathbb{N}$, $p \leq q$ und $b_p,\ldots,b_q \in \mathbb{Z}$. Dann gilt

$$\left(\sum_{i=m}^{n} a_i\right)\cdot\left(\sum_{j=p}^{q} b_j\right) = \sum_{i=m}^{n}\left(\sum_{j=p}^{q} a_i b_j\right) = \sum_{j=p}^{q}\left(\sum_{i=m}^{n} a_i b_j\right).$$

Für $a,b,c \in \mathbb{Z}$ mit $c \neq 0$ folgt aus $ac = bc$, dass $a = b$ ist. („In $\mathbb{Z}$ kann gekürzt werden“). Insbesondere folgt aus $a \cdot b = 0$, dass $a = 0$ oder $b = 0$ ist.
Die *Subtraktion* ist durch $\mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$, $(a,b) \longmapsto a-b := a+(-b)$, gegeben.
Es sei $\leq$ die durch

$$a \leq b :\Leftrightarrow b-a \in \mathbb{N}$$

definierte natürliche Ordnung der ganzen Zahlen, wir schreiben $a < b$ für: $a \leq b$ und $a \neq b$.
Für $a,b,c \in \mathbb{Z}$ gilt:

$a \leq a$,
aus $a \leq b$ und $b \leq a$ folgt $a = b$,
aus $a \leq b$ und $b \leq c$ folgt $a \leq c$,
$a \leq b$ oder $b \leq a$,
$a \leq b$ genau dann, wenn $a+c \leq b+c$
und
wenn $c > 0$, dann ist $a \leq b$ genau dann, wenn $a \cdot c \leq b \cdot c$.

Die ersten vier Eigenschaften bedeuten, dass $\leq$ eine *totale Ordnung* auf $\mathbb{Z}$ ist, die letzten zwei, dass diese mit Addition und Multiplikation *verträglich* ist.
Das *Vorzeichen* $vz(a)$ einer ganzen Zahl a ist 1, wenn $a \in \mathbb{N}$, und -1, wenn $a \notin \mathbb{N}$. Der *Betrag* $|a|$ einer ganzen Zahl a ist $vz(a)\cdot a$. Für Zahlen $a,b \in \mathbb{Z}$ ist $|a\cdot b| = |a|\cdot|b|$ und $|a+b| \leq |a|+|b|$.

§2. Division mit Rest

Wenn Sie einen Sack mit a Euromünzen haben, die Sie an b Personen verteilen sollen (jede soll gleich viel bekommen), dann werden Sie wahrscheinlich zuerst jeder Person einen Euro geben und diesen Vorgang solange wiederholen, bis im Sack weniger als b Euromünzen sind. Sie haben dann *a mit Rest durch b dividiert*.
Der folgende Satz ist grundlegend für alle Rechenverfahren für ganze Zahlen. Seine Bedeutung liegt darin, dass die drei „Strukturen“ $+,\cdot$ und $\leq$ zueinander in Beziehung gesetzt werden.

Satz 5 : (Division mit Rest von ganzen Zahlen)
Zu je zwei ganzen Zahlen a und b mit $b \neq 0$ gibt es eindeutig bestimmte ganze Zahlen m und r mit den Eigenschaften

$$a = m\cdot b + r \quad \textit{und} \quad 0 \leq r < |b| .$$

Die Zahlen m bzw. r heißen ganzzahliger Quotient von a und b *bzw.* Rest von a nach Division durch b. *Die Zahlen m und r können mit dem folgenden Verfahren (*Divisionsalgorithmus*) berechnet werden:*

- *Falls a und b natürliche Zahlen sind:*
  Setze $m := 0$ und $r := a$.
  Solange $r \geq b$ ist, ersetze r durch $r-b$ und m durch $m+1$.
- *Falls $a < 0$ oder $b < 0$ ist:*
  Berechne wie oben n und s so, dass $|a| = n \cdot |b| + s$ und $0 \leq s < |b|$ ist.
  Wenn $a \geq 0$ ist, dann setze $m := -n$ und $r := s$.
  Wenn $a < 0$ und $s > 0$ ist, dann setze $m := -vz(b) \cdot (n+1)$ und $r := |b| - s$.
  Wenn $a < 0$ und $s = 0$ ist, dann setze $m := -vz(b) \cdot n$ und $r := 0$.

Beweis: Wenn a und b natürliche Zahlen sind, dann erhalten wir bei jedem Ersetzen von r durch $r-b$ eine um mindestens 1 kleinere Zahl. Also tritt nach höchstens a Schritten der Fall $r < b$ ein. Somit liefert das obige Verfahren nach endlich vielen Schritten ein Ergebnis m, r. Mit Induktion über $|a|$ ist leicht nachzuprüfen, dass diese Zahlen die angegebenen Bedingungen erfüllen.
Es seien m_1, m_2, r_1, r_2 ganze Zahlen mit $a = m_1 \cdot b + r_1 = m_2 \cdot b + r_2$, $0 \leq r_1, r_2 < |b|$ und o.E.d.A. („ohne Einschränkung der Allgemeinheit“) $r_1 \leq r_2$. Dann ist

$$|b| > r_2 - r_1 = |m_1 - m_2| \cdot |b| \ .$$

Daraus folgt $m_1 = m_2$ und $r_1 = r_2$, also sind der ganzzahlige Quotient von a und b und der Rest von a nach Division durch b eindeutig bestimmt.

§3. Zifferndarstellung von Zahlen

Nehmen wir an, Sie kommen mit einem Sack voller Euromünzen in eine Bank und wollen dieses Geld auf ihr Sparbuch einzahlen. Die Anzahl der Euromünzen im Sack ist eine eindeutig bestimmte natürliche Zahl a. Bevor diese Zahl in Ihr Sparbuch eingetragen werden kann, muss der Bankbeamte ihre *Zifferndarstellung* (zur Basis 10) berechnen. Eine Zahl ist also nicht immer schon in Zifferndarstellung gegeben, sondern diese ist eine „Zusatzinformation“ über die Zahl. Wie wird die Zifferndarstellung zur Basis 10 von a ermittelt? Man bildet aus den Euromünzen solange „Zehnerstapel“, bis nur noch weniger als zehn Münzen übrigbleiben, das heißt: a wird mit Rest durch 10 dividiert. Die Anzahl der übriggebliebenen Euromünzen ist dann die „Einerziffer“ von a. Macht man dasselbe nun mit den Zehnerstapeln statt mit den Münzen, dann erhält man die „Zehnerziffer“ von a, usw.

Satz 6 : (Darstellung von Zahlen durch Ziffern)
Es seien a und b natürliche Zahlen mit $a \neq 0$ und $b \geq 2$. Dann gibt es eindeutig bestimmte natürliche Zahlen $n, z_0, z_1, \ldots, z_n$ so, dass

$$z_n \neq 0,\ 0 \leq z_0, z_1, \ldots, z_n < b$$

und

$$a = z_n b^n + z_{n-1} b^{n-1} + \ldots + z_1 b^1 + z_0 = \sum_{i=0}^{n} z_i b^i$$

ist.
Wenn b fest gewählt ist, dann ist a durch die Zahlen $n, z_0, z_1, \ldots, z_n$ eindeutig bestimmt. Man wählt Zeichen für die Zahlen von 0 bis $b-1$ und schreibt dann

$$z_n z_{n-1} \ldots z_0 \quad \textit{statt} \quad \sum_{i=0}^{n} z_i b^i \quad .$$

Die Zahlen $z_0, z_1, \ldots, z_n$ heißen Ziffern von a zur Basis b *(für b=2 bzw. 10: „Binärziffern“ bzw. „Dezimalziffern“).*

Die Ziffern z_i von $a \neq 0$ zur Basis b können mit dem folgenden Verfahren berechnet werden:

- *Setze $i := 0$.*
- *Solange a nicht 0 ist: Die i-te Ziffer z_i ist der Rest von a nach Division durch b. Ersetze a durch den ganzzahligen Quotienten von a und b. Ersetze i durch $i+1$.*

Beweis: Induktion über a:
Wenn $a = 1$ ist, ist $n = 0$ und $z_0 = 1$.
Für $a > 1$ sei m bzw. r der ganzzahlige Quotient von a und b bzw. der Rest von a nach Division durch b. Wegen $b > 1$ ist $m < a$, also gibt es nach Induktionsannahme eindeutig bestimmte Zahlen $k, y_0, y_1, \ldots, y_k$ so, dass $y_k \neq 0$, $0 \leq y_0, y_1, \ldots, y_k < b$ und

$$m = y_k b^k + y_{k-1} b^{k-1} + \ldots + y_1 b^1 + y_0 \ .$$

Dann ist

$$a = m \cdot b + r = y_k b^{k+1} + y_{k-1} b^k + \ldots + y_1 b^2 + y_0 b + r \ ,$$

und $y_k, \ldots, y_0, r$ sind die Ziffern von a. Aus der Eindeutigkeit von m und r folgt aus der Induktionsannahme die Eindeutigkeit der Ziffern von a zur Basis b.

Wird für die Zifferndarstellung einer Zahl die Basis b gewählt, dann können alle Zahlen durch Aneinanderreihen von b verschiedenen Symbolen angeschrieben werden. Eine kleine Basis (zum Beispiel 2) hat den Vorteil, dass man nur wenige Symbole braucht und dass das „kleine Einmaleins“ sehr einfach ist. Allerdings braucht man dann für größere Zahlen sehr viele Ziffern.

Definition 13 : Es seien $v = (v_1, \ldots, v_n)$ und $w = (w_1, \ldots, w_n)$ zwei verschiedene n-Tupel von ganzen Zahlen und j die kleinste Zahl in $\{1, \ldots, n\}$ mit der Eigenschaft, dass $v_j \neq w_j$.
Dann ist v *lexikographisch kleiner* als w (Schreibweise: $v <_{lex} w$), wenn $v_j < w_j$ ist.

Beispiel 3 : $(1,2,3,4) <_{lex} (1,2,4,3) <_{lex} (2,-7,-3,-5)$

Satz 7 : (Vergleich von zwei Zahlen, die durch Ziffern dargestellt sind) *Es seien b, x, y positive natürliche Zahlen, $b \geq 2$ und*

$$x_k, x_{k-1}, \ldots, x_0 \quad \textit{bzw.} \quad y_\ell, y_{\ell-1}, \ldots, y_0$$

die Ziffern von x bzw. y bezüglich b.
Dann ist x genau dann kleiner als y, wenn

$$k < \ell \quad \textit{oder} \quad (k = \ell \textit{ und } (x_k, x_{k-1}, \ldots, x_0) <_{lex} (y_\ell, y_{\ell-1}, \ldots, y_0)) \textit{ ist.}$$

Beweis: Wenn $k < \ell$ ist, dann ist

$$x = \sum_{i=0}^{k} x_i b^i \leq \sum_{i=0}^{k} (b-1) b^i = \sum_{i=1}^{k+1} b^i - \sum_{i=0}^{k} b^i = b^{k+1} - 1 < b^{k+1} \leq y \, .$$

Es sei $k = \ell$ und j die größte Zahl mit der Eigenschaft, dass $x_j \neq y_j$. Wenn $x_j < y_j$ ist, dann ist

$$\sum_{i=0}^{j} x_i b^i \leq x_j b^j + (b^j - 1) < (x_j + 1) b^j \leq y_j b^j \leq \sum_{i=0}^{j} y_i b^i$$

und

$$x = \sum_{i=j+1}^{k} x_i b^i + \sum_{i=0}^{j} x_i b^i < \sum_{i=j+1}^{k} x_i b^i + \sum_{i=0}^{j} y_i b^i = y \, .$$

Satz 8 : (Addition von zwei Zahlen, die durch Ziffern dargestellt sind) *Es seien b, x, y, k, ℓ natürliche Zahlen, $b \geq 2$ und*

$$x_k, x_{k-1}, \ldots, x_0 \quad \textit{bzw.} \quad y_\ell, y_{\ell-1}, \ldots, y_0$$

die Ziffern von x bzw. y bezüglich b. Für je zwei Zahlen in $\{0, \ldots, b-1\}$ sei die Zifferndarstellung ihrer Summe bekannt. (Wenn diese Summe größer als $b-1$ ist, dann hat sie zwei Ziffern, die erste ist 1 und die zweite ist kleiner als $b-1$). O.E.d.A. sei $k \leq \ell$.
Dann können die Ziffern von $x+y$ mit dem folgenden Verfahren berechnet werden:

- *Ermittle die Ziffern $(x_0+y_0)_1$ und $(x_0+y_0)_0$ von x_0+y_0. Setze $(x+y)_0 := (x_0+y_0)_0$, $u_0 := (x_0+y_0)_1$ und $i := 0$.*

- *Solange $i < k$ ist, setze $i := i+1$ und ermittle die Ziffern $(x_i+y_i+u_{i-1})_1$ und $(x_i+y_i+u_{i-1})_0$ von $x_i+y_i+u_{i-1}$.*
  Setze $(x+y)_i := (x_i+y_i+u_{i-1})_0$ und $u_i := (x_i+y_i+u_{i-1})_1$ („i-ter Übertrag“).
- *Solange $i < \ell$ ist, setze $i := i+1$ und ermittle die Ziffern $(y_i+u_{i-1})_1$ und $(y_i+u_{i-1})_0$ von y_i+u_{i-1}.*
  Setze $(x+y)_i := (y_i+u_{i-1})_0$ und $u_i := (y_i+u_{i-1})_1$.
- *Wenn $u_\ell \neq 0$, setze $(x+y)_{\ell+1} := u_\ell$.*

Beweis: Übung.

Verfahren für die Subtraktion und Multiplikation können in ähnlicher Weise angegeben werden. Hier wird nur noch das Verfahren für die Division mit Rest in einem Satz formuliert. In Satz **??** wurde bereits ein Divisionsalgorithmus angegeben. Wenn eine Zifferndarstellung der gegebenen Zahlen bekannt ist, kann dieses Verfahren mit Hilfe dieser zusätzlichen Information verbessert werden.

Satz 9 : (Division mit Rest von Zahlen, die durch Ziffern dargestellt sind)
Es seien b,x,y,k,ℓ natürliche Zahlen, $b \geq 2$, $y > 0$ und

$$x_k, x_{k-1}, \ldots, x_0 \quad \textit{bzw.} \quad y_\ell, y_{\ell-1}, \ldots, y_0$$

die Ziffern von x bzw. y bezüglich b. O.E.d.A. sei $x \geq y$.
Die Ziffern des ganzzahligen Quotienten m von x und y können mit dem folgenden Verfahren berechnet werden:

- *Setze $j := k-\ell$, wenn $\sum_{i=0}^{\ell} x_{i+k-\ell} b^i \geq y$ ist, und $j := k-\ell-1$, sonst.*
- *Solange $j \geq 0$ ist, berechne (wie in Satz **??**) den ganzzahligen Quotienten m_j von $\sum_{i\geq 0} x_{i+j} b^i$ und y. Dieser ist die j-te Ziffer von m.*
  Ersetze x durch $x - m_j \cdot y \cdot b^j$ und j durch $j-1$.

Beweis: Übung.

Wenn zur Darstellung einer Zahl am Computer 32 bits (also 32 Binärziffern) zur Verfügung stehen, dann können in der *Zweierkomplementdarstellung* die Zahlen in

$$\{-2^{31} = -2147483648, \ldots, -1, 0, 1, \ldots, 2^{31}-1 = 2147483647\}$$

(also insgesamt 2^{32} Zahlen) dargestellt werden.
Ist a eine natürliche Zahl in diesem Zahlenbereich, dann wird a durch

$$0\ a_{30}\ a_{29}\ \ldots\ a_1\ a_0$$

dargestellt, wobei $a_{30}\ a_{29}\ \ldots\ a_1\ a_0$ die Ziffern von a zur Basis 2 sind.
Ist a eine negative Zahl in diesem Zahlenbereich, dann wird a durch

$$1\ a_{30}\ a_{29}\ \ldots\ a_1\ a_0$$

dargestellt, wobei $a_{30}\ a_{29}\ \ldots\ a_1\ a_0$ die Ziffern von $a+2^{31}$ zur Basis 2 sind.

§4. Rationale Zahlen

Es seien a und b ganze Zahlen, wobei $b \neq 0$ ist. Die Aufgabe „Finde eine Zahl z so, dass $b \cdot z = a$ ist“ bezeichnen wir als „Gleichung“ $b \cdot x = a$. Eine Zahl z mit $b \cdot z = a$ heißt *Lösung* von $b \cdot x = a$. Wenn $|b| \neq 1$, dann hat die Aufgabe $b \cdot x = 1$ in $\mathbb{Z}$ keine Lösung. Um Lösungen zu erhalten, müssen wir „den Zahlenbereich erweitern“.

Die Aufgabe $b \cdot x = a$ wird durch das Paar $(a,b) \in \mathbb{Z}^2$ eindeutig beschrieben, also liegt es nahe, die „neuen Zahlen“ durch Paare von ganzen Zahlen zu beschreiben. Allerdings sollten für $t \in \mathbb{Z}$, $t \neq 0$, die Gleichungen $b \cdot x = a$ und $t \cdot b \cdot x = t \cdot a$ dieselbe Lösung haben, daher sollen die Zahlenpaare (a,b) und $(t \cdot a, t \cdot b)$ dieselbe „neue Zahl“ beschreiben.

Definition 14 : Es seien a und b ganze Zahlen, wobei $b \neq 0$. Dann ist die Menge

$$\frac{a}{b} := \{(c,d) \mid c,d \in \mathbb{Z}, ad = bc, d \neq 0\}$$

die durch den „Zähler“ a und den „Nenner“ b gegebene *rationale Zahl* oder *Bruchzahl*. (Beachte: Eine Bruchzahl ist durch Vorgabe von Zähler und Nenner eindeutig bestimmt, aber umgekehrt sind Zähler und Nenner durch die Bruchzahl nicht eindeutig bestimmt). Wir schreiben $\mathbb{Q}$ für die Menge der rationalen Zahlen.
Für die Bruchzahl $\frac{a}{1}$ schreiben wir oft nur a und fassen so $\mathbb{Z}$ als Teilmenge von $\mathbb{Q}$ auf. („Jede ganze Zahl ist eine rationale Zahl“).

Satz 10 : *Es seien a', b' ganze Zahlen und $b' \neq 0$. Dann sind die Bruchzahlen $\frac{a}{b}$ und $\frac{a'}{b'}$ genau dann gleich, wenn $a \cdot b' = a' \cdot b$.*

Beweis: Wenn $\frac{a}{b} = \frac{a'}{b'}$ ist, dann ist insbesondere $(a',b') \in \frac{a}{b}$, also $a \cdot b' = a' \cdot b$.
Sei umgekehrt $a \cdot b' = a' \cdot b$ und $(c,d) \in \frac{a}{b}$, also $b \cdot c = a \cdot d$. Dann ist zu zeigen, dass $(c,d) \in \frac{a'}{b'}$, also $b' \cdot c = a' \cdot d$ ist.
Es ist

$$a \cdot (b' \cdot c) = (a \cdot b') \cdot c = (a' \cdot b) \cdot c = a' \cdot (b \cdot c) = a' \cdot (a \cdot d) = a \cdot (a' \cdot d)\ ,$$

also auch $b' \cdot c = a' \cdot d$.

Satz 11 : *Für den Nenner einer Bruchzahl kann immer eine positive Zahl gewählt werden. Dann wird die totale Ordnung $\leq$ auf $\mathbb{Z}$ durch*

$$\frac{a}{b} \leq \frac{c}{d} :\Leftrightarrow a \cdot d \leq b \cdot c$$

zu einer totalen Ordnung auf $\mathbb{Q}$ erweitert.

Beweis: Zuerst ist zu zeigen, dass die Definition von $\leq$ nicht von der Wahl von Zähler und positivem Nenner abhängt. Seien $a, a', c, c' \in \mathbb{Z}$ und b, b', d, d' positive ganze Zahlen so, dass $a \cdot b' = a' \cdot b$, $c \cdot d' = c' \cdot d$ und $a \cdot d \leq b \cdot c$ ist. Dann ist

$$a' \cdot d' \cdot b \cdot d = a \cdot d' \cdot b' \cdot d \leq b \cdot d' \cdot b' \cdot c = b' \cdot c' \cdot b \cdot d$$

und $a' \cdot d' \leq b' \cdot c'$.
Seien $a, c, e \in \mathbb{Z}$, b, d, f positive ganze Zahlen so, dass $\frac{a}{b} \leq \frac{c}{d}$ und $\frac{c}{d} \leq \frac{e}{f}$ ist. Es ist noch zu zeigen, dass dann auch $\frac{a}{b} \leq \frac{e}{f}$ ist. Aus $a \cdot d \cdot f \leq b \cdot c \cdot f \leq b \cdot d \cdot e$ folgt $a \cdot f \leq b \cdot e$ und daher die Behauptung.

Wir werden nun die Rechenoperationen von $\mathbb{Z}$ auf $\mathbb{Q}$ fortsetzen.

Satz 12 : *Die Funktionen*

$$+ : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} , \quad (\frac{a}{b}, \frac{c}{d}) \longmapsto \frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} ,$$

und

$$\cdot : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} , \quad (\frac{a}{b}, \frac{c}{d}) \longmapsto \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} ,$$

sind wohldefiniert. Diese Rechenoperationen in $\mathbb{Q}$ erfüllen die gleichen Rechenregeln wie Addition und Multiplikation in $\mathbb{Z}$. Darüberhinaus hat jedes Element $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$ ein inverses Element $(\frac{a}{b})^{-1}$ *mit der Eigenschaft*

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

und zwar ist

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

Die Einschränkungen von $+$ und $\cdot$ auf $\mathbb{Z} \times \mathbb{Z}$ stimmen mit der Addition und der Multiplikation auf $\mathbb{Z}$ überein.

Beweis: Wir müssen zuerst zeigen, dass die Funktionen $+$ und $\cdot$ wohldefiniert sind, das heißt: wenn $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$, dann muss auch

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} \quad \text{und} \quad \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

sein.
Aus $a'b = ab'$ und $c'd = cd'$ folgt

$$(ad+bc)b'd' = a'bdd' + bb'c'd = bd(a'd' + b'c')$$

und

$$(ac)b'd' = bd(a'c') \ .$$

Die Rechenregeln können leicht nachgeprüft werden.

§5. Zifferndarstellung von rationalen Zahlen

Definition 15 : Der *Betrag* $|\frac{a}{b}|$ einer rationalen Zahl $\frac{a}{b}$ ist $\frac{|a|}{|b|}$.

Satz 13 : (Zifferndarstellung von rationalen Zahlen)
Es seien b, c, d, p positive ganze Zahlen mit $b \geq 2$. Dann gibt es eindeutig bestimmte natürliche Zahlen $n, z_n, \ldots, z_0, z_{-1}, \ldots, z_{-p}$ so, dass

$$z_n \neq 0 \text{ oder } n = 0, \quad 0 \leq z_n, \ldots, z_0, z_{-1}, \ldots, z_{-p} < b$$

und

$$|\frac{c}{d} - (z_n b^n + z_{n-1} b^{n-1} + \ldots + z_1 b^1 + z_0 + z_{-1} b^{-1} + \ldots + z_{-p} b^{-p})| < b^{-p} \ .$$

Ist b fest gewählt, schreibt man

$$z_n z_{n-1} \ldots z_0 . z_{-1} z_{-2} \ldots z_{-p} \quad \textit{statt} \quad \sum_{i=-p}^{n} z_i b^i \ .$$

Die Zahlen $z_n, \ldots, z_0, z_{-1}, \ldots, z_{-p}$ heißen Ziffern von a zur Basis b. *Die Ziffern z_i von $\frac{c}{d}$ zur Basis b können wie folgt berechnet werden:*

- *Berechne (mit Satz **??**) die Ziffern $y_0, \ldots, y_k$ zur Basis b des ganzzahligen Quotienten m von $c \cdot b^p$ und d .*
- *Setze $z_i := y_{i+p}$, $-p \leq i \leq k-p =: n$.*

Beweis: Sei r der Rest von $c \cdot b^p$ nach Division durch d. Wegen $c \cdot b^p = m \cdot d + r$ ist dann

$$\frac{c \cdot b^p}{d \cdot b^p} = \frac{m \cdot d}{d \cdot b^p} + \frac{r}{d \cdot b^p} \ ,$$

also

$$\frac{c}{d} = \frac{m}{b^p} + \frac{r}{d} . b^{-p} \quad \text{und} \quad \frac{r}{d} < 1 \ .$$

Rationale Zahlen können also „beliebig genau“ durch Zahlen der Form $z_n z_{n-1} \ldots z_0 . z_{-1} z_{-2} \ldots z_{-p}$ angenähert werden, aber es gibt rationale Zahlen, die für alle p von $z_n z_{n-1} \ldots z_0 . z_{-1} z_{-2} \ldots z_{-p}$ verschieden sind.

Eine rationale Zahl

$$z_0 . z_{-1} z_{-2} \ldots z_{-p} \, Ee \ := \ z_0 . z_{-1} z_{-2} \ldots z_{-p} \cdot b^e$$

mit $b \geq 2$ und $z_0 \neq 0$ ist in *Exponentialform* zur Basis b dargestellt. Die Zahlen e und $z_0.z_{-1}z_{-2}\dots z_{-p}$ heißen *Exponent* und *Mantisse*.

Am Computer kann eine Zahl dann durch die Ziffern des Exponenten und der Mantisse zur Basis 2 dargestellt werden. Die Anzahl dieser Ziffern ist durch eine vorgegebene Zahl beschränkt. Die so am Computer verfügbaren Zahlen heißen *Maschinenzahlen*. Es gibt nur endlich viele Maschinenzahlen, alle Maschinenzahlen sind rationale Zahlen.

Beim Rechnen mit so dargestellten Zahlen gibt es im allgemeinen keine exakten Ergebnisse, sondern Rundungsfehler. Bei Rechenverfahren muss daher darauf geachtet werden, dass sich die Fehler nicht akkumulieren. Fehlerabschätzungen sind erforderlich.

Beispiel 4 : Die Zahl 0.1 (Dezimaldarstellung) auf der Tastatur wird vom Computer in Binärdarstellung $0.0001100110011001100\dots$ umgewandelt und zum Beispiel als

$$1.10011001100110011001100110011001100110011001100\,E-4$$

gespeichert. Also ergibt schon die Eingabe von 0.1 einen Rundungsfehler!

Will man mit rationalen Zahlen am Computer exakt rechnen, kann man $\frac{a}{b}$ als Zahlenpaar (a,b) eingeben. Dann müssen für Zahlenpaare die Rechenoperationen

$$(a,b)+(c,d) := (ad+bc,bd) \quad \text{und} \quad (a,b)\cdot(c,d) := (ac,bd)$$

definiert werden.

§6. Der Euklidische Algorithmus

Es seien a,b,c ganze Zahlen und $b \neq 0$, $c \neq 0$. Dann ist

$$\frac{a}{b} = \frac{a\cdot c}{b\cdot c} \in \mathbb{Q}\ .$$

Der Übergang von der Darstellung dieser rationalen Zahl durch das Zahlenpaar $(a\cdot c, b\cdot c)$ zu der durch (a,b) heißt *durch c kürzen*. Rechnet man mit rationalen Zahlen, dann ist es sehr empfehlenswert, alle auftretenden Brüche sofort durch möglichst große Zahlen zu kürzen. Dadurch werden die weiteren Rechnungen oft wesentlich vereinfacht. In diesem Abschnitt wird ein Verfahren zum „optimalen Kürzen“ angegeben. Darüberhinaus lernen wir ein Verfahren zur Berechnung einer Lösung einer „ganzzahligen linearen Gleichung“ kennen.

Definition 16 : Es seien a,b ganze Zahlen mit $b \neq 0$. Dann ist *a Teiler* von b (oder: *a teilt b*), wenn es eine Zahl $c \in \mathbb{Z}$ gibt mit $b = ac$. Die Zahl b heißt *Vielfaches* von a, wenn a ein Teiler von b ist.

Definition 17 : Der *größte gemeinsame Teiler* von zwei von Null verschiedenen ganzen Zahlen ist die größte ganze Zahl, die beide teilt. Das *kleinste gemeinsame Vielfache* von zwei von Null verschiedenen ganzen Zahlen ist die kleinste positive ganze Zahl, die Vielfaches von beiden ist.
Wir schreiben $ggT(a,b)$ bzw. $kgV(a,b)$ für den größten gemeinsamen Teiler bzw. das kleinste gemeinsame Vielfache zweier Zahlen a und b.

Lemma 1 : *Es seien $a,b,c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ und $a \neq c \cdot b$. Dann ist*

$$ggT(a,b) = ggT(|a|,|b|)$$

und

$$ggT(a,b) = ggT(a - c \cdot b, b) \ .$$

Beweis: Übung.

Satz 14 : (Euklidischer Algorithmus für ganze Zahlen)
Es seien $a,b \in \mathbb{Z}$, $a \neq 0$ und $b \neq 0$. Mit dem folgenden Verfahren kann der größte gemeinsame Teiler von a und b berechnet werden:

- *Ersetze a und b durch $|a|$ und $|b|$.*
- *Solange die zwei Zahlen verschieden sind, ersetze die größere durch die Differenz der größeren und der kleineren.*
- *Wenn die zwei Zahlen gleich sind, dann ist $ggT(a,b)$ gleich dieser Zahl.*

Ersetzt man mehrfaches Abziehen derselben Zahl durch eine Division mit Rest, dann hat dieses Verfahren die folgende Form:

- *Ersetze a und b durch $|a|$ und $|b|$.*
- *Solange keine der zwei Zahlen ein Teiler der anderen ist, ersetze die größere der zwei Zahlen durch ihren Rest nach Division durch die kleinere.*
- *Wenn eine der zwei Zahlen ein Teiler der anderen ist, dann ist sie der $ggT(a,b)$.*

Beweis: Es ist $ggT(a,b) = ggT(|a|,|b|)$. Also können wir annehmen, dass a und b positive ganze Zahlen sind. Wenn sie verschieden sind, wird die größere der zwei Zahlen (wir bezeichnen sie mit $max(a,b)$) im nächsten Schritt durch eine kleinere positive ganze Zahl ersetzt. Also sind die zwei Zahlen nach höchstens $max(a,b) - 1$ Schritten gleich. In jedem Schritt wird ein Zahlenpaar durch ein anderes ersetzt, nach Lemma **??** aber so, dass die größten gemeinsamen Teiler der zwei Zahlenpaare gleich sind. Sobald man den größten gemeinsamen Teiler eines Zahlenpaares kennt (das ist spätestens dann der Fall, wenn die zwei Zahlen gleich sind), hat man $ggT(a,b)$ ermittelt.

Im Euklidischen Algorithmus wird die folgende **Strategie zur Lösung von Problemen** verwendet: Wenn man eine Aufgabe nicht sofort lösen kann, ersetzt man diese Aufgabe durch eine einfachere, die aber dieselbe Lösungsmenge hat. Das wiederholt man solange, bis man bei einer Aufgabe landet, deren Lösungen man kennt. Diese Lösungen sind dann auch die Lösungen der ursprünglichen Aufgabe.

Satz 15 : (Erweiterter Euklidischer Algorithmus)
Es seien $a,b \in \mathbb{Z}$, $a \neq 0$ und $b \neq 0$. Es gibt ganze Zahlen u,v so, dass $u \cdot a + v \cdot b = ggT(a,b)$. Diese können mit dem folgenden Verfahren berechnet werden:

- *Setze $A := (A_1,A_2,A_3) := (|a|,1,0) \in \mathbb{Z}^3$ und $B := (B_1,B_2,B_3) := (|b|,0,1) \in \mathbb{Z}^3$.*
- *Solange B_1 die Zahl A_1 nicht teilt, berechne den ganzzahligen Quotienten m von A_1 und B_1 und setze $C := B$, $B := A - m \cdot C := (A_1 - m \cdot C_1, A_2 - m \cdot C_2, A_3 - m \cdot C_3)$ und $A := C$.*
- *Wenn B_1 die Zahl A_1 teilt, dann ist $u := vz(a) \cdot B_2$ und $v := vz(b) \cdot B_3$.*

Beweis: Wenn zwei Zahlentripel S und T die Eigenschaft

$$S_1 = |a| \cdot S_2 + |b| \cdot S_3 \quad \text{bzw.} \quad T_1 = |a| \cdot T_2 + |b| \cdot T_3$$

haben, dann auch alle Tripel $S - m \cdot T$ mit $m \in \mathbb{Z}$. Die ersten zwei Tripel im Algorithmus haben diese Eigenschaft, daher auch alle anderen auftretenden Tripel. Für die ersten Komponenten der Tripel wird der euklidische Algorithmus durchgeführt, für das letzte Tripel B gilt daher $ggT(a,b) = |a| \cdot B_2 + |b| \cdot B_3 = vz(a) \cdot a \cdot B_2 + b \cdot vz(b) \cdot B_3$.

Satz 16 : (Berechnung von $kgV(a,b)$)
Es seien $a,b \in \mathbb{Z}$, $a \neq 0$ und $b \neq 0$. Dann ist

$$kgV(a,b) = \frac{|a|}{ggT(a,b)} \cdot |b| = \frac{|b|}{ggT(a,b)} \cdot |a| \ .$$

Beweis: Es ist klar, dass $\frac{|a|}{ggT(a,b)} \cdot |b| = \frac{|b|}{ggT(a,b)} \cdot |a|$ ein Vielfaches von a und von b ist. Sei z eine positive ganze Zahl, die Vielfaches von a und von b ist. Dann gibt es ganze Zahlen c,d mit $z = c \cdot a$ und $z = d \cdot b$. Nach Satz **??** gibt es Zahlen u,v so, dass $u \cdot a + v \cdot b = ggT(a,b)$. Dann ist

$$z = \frac{u \cdot a + v \cdot b}{ggT(a,b)} \cdot z = \frac{u \cdot a}{ggT(a,b)} \cdot z + \frac{v \cdot b}{ggT(a,b)} \cdot z =$$

$$= \frac{u \cdot a \cdot d \cdot b}{ggT(a,b)} + \frac{v \cdot b \cdot c \cdot a}{ggT(a,b)} = \frac{a \cdot b}{ggT(a,b)} \cdot (u \cdot d + v \cdot c) =$$

$$= \frac{|a| \cdot |b|}{ggT(a,b)} \cdot vz(a \cdot b) \cdot (u \cdot d + v \cdot c)$$

ein Vielfaches von $\frac{|a|}{ggT(a,b)} \cdot |b|$.

Satz 17 : *(„Lösen einer ganzzahligen linearen Gleichung"). Es seien $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ und $b \in \mathbb{Z}$. Die größte ganze Zahl, die $a_1, \ldots, a_n$ teilt, heißt* größter gemeinsamer Teiler *von $a_1, \ldots, a_n$ und wird mit $ggT(a_1, \ldots, a_n)$ bezeichnet. Es ist*

$$ggT(a_1, \ldots, a_n) = ggT(a_1, ggT(a_2, ggT(a_3, ggT(\ldots, a_n)\ldots)) \ ,$$

also kann der größte gemeinsame Teiler von mehreren Zahlen durch sukzessives Berechnen des größten gemeinsamen Teilers von je zwei Zahlen berechnet werden.
Es gibt genau dann ein n-Tupel $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ mit

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n = b \ ,$$

wenn b ein Vielfaches von $g := ggT(a_1, \ldots, a_n)$ ist. In diesem Fall kann ein solches n-Tupel wie folgt berechnet werden:

- *Berechne mit Satz* **??** *Zahlen $u_1, \ldots, u_n$ so, dass $a_1 \cdot u_1 + \ldots + a_n \cdot u_n = g$.*
- *Setze $x_i := u_i \cdot \frac{b}{g}$, $1 \leq i \leq n$.*

Beweis: Für jedes n-Tupel $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ wird $a_1 \cdot x_1 + \ldots + a_n \cdot x_n$ von g geteilt. Also ist die Bedingung, dass b ein Vielfaches von g ist, notwendig für die Existenz einer Lösung. Wenn diese Bedingung erfüllt ist, ist leicht nachzuprüfen, dass $(u_1 \cdot \frac{b}{g}, \ldots, u_n \cdot \frac{b}{g})$ eine Lösung ist.

§7. Primzahlen

Definition 18 : Eine ganze Zahl $p \in \mathbb{Z}$ heißt *Primzahl*, wenn $p \neq 0, p \neq 1, p \neq -1$ und $\{1, -1, p, -p\}$ die Menge der Teiler von p ist.

Lemma 2 : *Es sei p eine Primzahl und $a, b \in \mathbb{Z}$.*
Wenn p die Zahl $a \cdot b$ teilt, dann teilt p auch a oder b.

Beweis: Sei c eine ganze Zahl so, dass $c \cdot p = a \cdot b$ ist. Wenn p die Zahl a nicht teilt, dann ist $ggT(a, p) = 1$. Daher gibt es ganze Zahlen u und v so, dass $1 = u \cdot a + v \cdot p$ ist. Dann ist

$$b = b \cdot u \cdot a + b \cdot v \cdot p = u \cdot c \cdot p + b \cdot v \cdot p = (u \cdot c + b \cdot v) \cdot p \ ,$$

somit ist p ein Teiler von b.

Satz 18 : (Zerlegung in Primfaktoren)
Jede ganze Zahl , die größer als 1 *ist, kann als Produkt von positiven Primzahlen geschrieben werden. Diese Primzahlen heißen* Primfaktoren *der Zahl und sind bis auf die Reihenfolge eindeutig bestimmt.*

Beweis: Es sei a eine ganze Zahl, die größer als 1 ist. Wir beweisen die erste Aussage durch Induktion über a.
Wenn $a = 2$ ist, dann ist a eine Primzahl.
Wenn $a > 2$ ist, dann ist a entweder eine Primzahl oder es gibt ganze Zahlen b, c mit $0 < b, c < a$ so, dass $a = b \cdot c$ ist. Nach Induktionsannahme sind b und c Produkte von positiven Primzahlen, also auch a.
Wir beweisen noch die Eindeutigkeit der Primfaktorzerlegung. Es seien $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ und $a = q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$ zwei Zerlegungen von a in Primfaktoren. Wir beweisen durch Induktion über die größere der zwei Zahlen k, ℓ, dass die Primfaktoren der zwei Zerlegungen bis auf die Reihenfolge gleich sind. Weil p_1 das Produkt $q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$ teilt, gibt es nach Lemma **??** eine Zahl $j \in \{1, \ldots, \ell\}$ so, dass $p_1 = q_j$. Daher ist

$$p_2 \cdot \ldots \cdot p_k = \prod_{1 \leq i \leq \ell, i \neq j} q_i \ ,$$

und die Behauptung folgt aus der Induktionsannahme.

Die Berechnung der Primfaktoren einer Zahl ist sehr aufwendig. Rechenverfahren, in denen Zahlen in Primfaktoren zerlegt werden müssen, sollten nach Möglichkeit vermieden werden.

Satz 19 : *Es gibt unendlich viele positive Primzahlen.*

Beweis: Wenn es nur endlich viele positive Primzahlen gäbe, dann wäre ihr Produkt q eine ganze Zahl und $q + 1$ wäre größer als jede Primzahl. Insbesondere wäre $q + 1$ keine Primzahl. Nach Satz **??** gibt es eine Primzahl p, die $q + 1$ teilt. Da p auch q teilt, würde p dann auch 1 teilen, Widerspruch.

Satz 20 : (Berechnung von ggT und kgV zweier Zahlen, deren Primfaktoren bekannt sind).
Es seien $p_1, \ldots, p_n$ paarweise verschiedene positive Primzahlen und $e_1, \ldots, e_n, f_1, \ldots, f_n$ natürliche Zahlen. Mit $min(e_i, f_i)$ bzw. $max(e_i, f_i)$ bezeichnen wir die kleinere bzw. größere der zwei Zahlen e_i und f_i. Dann ist

$$ggT(\prod_{i=1}^{n} p_i^{e_i}, \prod_{i=1}^{n} p_i^{f_i}) = \prod_{i=1}^{n} p_i^{min(e_i, f_i)}$$

und

$$kgV(\prod_{i=1}^{n} p_i^{e_i}, \prod_{i=1}^{n} p_i^{f_i}) = \prod_{i=1}^{n} p_i^{max(e_i,f_i)} \ .$$

Beweis: Es sei $g := \prod_{i=1}^{n} p_i^{min(e_i,f_i)}$. Es ist klar, dass g die Zahlen $a := \prod_{i=1}^{n} p_i^{e_i}$ und $b := \prod_{i=1}^{n} p_i^{f_i}$ teilt. Da nach Satz **??** die Zerlegung dieser zwei Zahlen in Primfaktoren eindeutig ist, kann ihr größter gemeinsamer Teiler keine anderen Primfaktoren als $p_1, \ldots, p_n$ enthalten. Aus demselben Grund darf p_i in $ggT(a,b)$ nur $min(e_i, f_i)$-mal auftreten. Daher ist $g = ggT(a,b)$. Die Behauptung für $kgV(a,b)$ folgt nun aus Satz **??**.

§8. Anhang: Gruppen, Ringe und Körper

Definition 19 : Sei G eine Menge und $* : G \times G \to G$ eine Funktion. Für Elemente $a, b \in G$ schreiben wir statt $*(a,b)$ kurz $a * b$. Das Paar $(G,*)$ heisst eine *Gruppe*, wenn die folgenden drei Bedingungen („Gruppen-Axiome“) erfüllt sind:

(1) Für alle Elemente $a, b, c \in G$ ist
$a * (b * c) = (a * b) * c =: a * b * c$ (*Assoziativgesetz*).
(2) Es gibt ein Element $e \in G$ so, dass für alle $a \in G$ gilt :
$a * e = e * a = a$ (e heißt dann *neutrales Element*).
(3) Für alle Elemente $a \in G$ gibt es ein $b \in G$ so, dass
$a * b = b * a = e$ (b heißt dann zu a *inverses Element* und wird mit a^{-1} bezeichnet).

Eine Gruppe $(G,*)$ heißt *kommutativ* oder *abelsch*, wenn zusätzlich gilt:

(4) Für alle $a, b \in G$ ist $a * b = b * a$ (*Kommutativgesetz*).

Ist $(G,*)$ eine Gruppe, dann wird die Funktion $*$ als *Gruppenverknüpfung*, *Multiplikation* oder, wenn $(G,*)$ abelsch ist, als *Addition* bezeichnet. Wenn aus dem Zusammenhang ersichtlich ist, welche Verknüpfung auf G betrachtet wird, schreibt man statt $(G,*)$ kürzer G.

Beispiel 5 : $(\mathbb{Z}, +)$, $(\{1,-1\}, \cdot)$, $(\mathbb{Q}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind kommutative Gruppen.

Satz 21 : *Sei G eine Gruppe. Dann gilt:*

(1) *Es gibt genau ein neutrales Element in G.*
(2) *Zu jedem Element in G gibt es genau ein inverses Element in G.*
(3) *Für Elemente* $a, b \in G$ *ist* $(a * b)^{-1} = b^{-1} * a^{-1}$.
(4) *Für Elemente* $a, b, c \in G$ *folgt aus* $a * b = a * c$ *oder* $b * a = c * a$ *auch* $b = c$ *(*Kürzen*).*

Beweis: (1) Seien e und e' neutrale Elemente in G. Dann ist $e' = e * e'$ und $e = e * e'$, also $e = e'$.
(2) Seien b und b' zu a inverse Elemente. Dann ist
$b = e * b = (b' * a) * b = b' * (a * b) = b' * e = b'$.
(3) Es ist $(a * b) * (b^{-1} * a^{-1}) = a * (b * (b^{-1} * a^{-1})) =$
$= a * ((b * b^{-1}) * a^{-1}) = a * (e * a^{-1}) = a * a^{-1} = e$ und
$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * (a * b)) = b^{-1} * ((a^{-1} * a) * b) =$
$b^{-1} * (e * b) = b^{-1} * b = e$.
(4) Aus $a * b = a * c$ folgt $b = a^{-1} * a * b = a^{-1} * a * c = c$.

Definition 20 : Sei R eine Menge und $+ : R \times R \to R$ sowie $\cdot : R \times R \to R$ Funktionen. Wir schreiben statt $+(a,b)$ kurz „$a+b$“ und statt $\cdot(a,b)$ kurz „$a \cdot b$“ oder „ab“. Das Tripel $(R,+,\cdot)$ heißt ein *Ring*, wenn die folgenden Bedingungen („Ring-Axiome“) erfüllt sind:

(1) $(R,+)$ ist eine abelsche Gruppe.
(2) Für alle $a,b,c \in R$ ist $(ab)c = a(bc)$ (*Assoziativgesetz*).
(3) Es gibt ein Element $e \in R$ so, dass für alle $a \in R$ gilt :
$ea = ae = a$ (e heisst dann *Einselement* und wird mit 1_R bezeichnet).
(4) Für alle $a,b,c \in R$ ist $a(b+c) = (ab) + (ac)$ und
$(a+b)c = (ac) + (bc)$ (*Distributivgesetz*).

Ein Ring $(R,+,\cdot)$ heißt *kommutativ*, wenn zusätzlich gilt:

(5) für alle $a,b \in R$ ist $ab = ba$ (*Kommutativgesetz*).

Ist $(R,+,\cdot)$ ein Ring, dann heißt $+$ die *Addition* und $\cdot$ die *Multiplikation* des Ringes. Das neutrale Element von $(R,+)$ heißt *Nullelement* und wird 0_R geschrieben. Das zu $a \in R$ bezüglich $+$ inverse Element wird mit $-a$ bezeichnet. Die *Subtraktion* ist dann definiert durch

$$a - b := a + (-b).$$

Um Klammern einzusparen, wird verabredet, dass die Multiplikation immer vor der Addition ausgeführt wird, ausgenommen bei gegenteiliger Klammerung. Zum Beispiel wird $(ab) + c$ abgekürzt als $ab + c$.

Wenn aus dem Zusammenhang ersichtlich ist, welche Addition und Multiplikation auf der Menge R betrachtet werden, so schreibt man statt $(R,+,\cdot)$ kurz R.

Beispiel 6 : $\mathbb{Z}$ und $\mathbb{Q}$ mit der Addition und Multiplikation sind kommutative Ringe.

Definition 21 : Ein Element a eines Ringes R mit Einselement 1_R ist *invertierbar*, wenn es ein Element $b \in R$ mit

$$ab = 1_R = ba$$

gibt. Das Element b heißt dann zu a (bezüglich $\cdot$) *inverses Element* und wird mit a^{-1} bezeichnet.

Satz 22 : *Die Menge aller invertierbaren Elemente von R ist mit der Multiplikation von R eine Gruppe. Für invertierbare Elemente $a,b \in R$ ist*

$$(ab)^{-1} = b^{-1}a^{-1} \quad \textit{und} \quad (a^{-1})^{-1} = a \; .$$

Beweis: Es ist

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = 1 = b^{-1}(a^{-1}a)b = (b^{-1}a^{-1})(ab) \; .$$

Definition 22 : Sei $(R,+,\cdot)$ ein kommutativer Ring mit mindestens 2 Elementen. R heißt ein *Körper*, wenn jedes Element von $R \setminus \{0\}$ invertierbar ist. Die *Division* in R ist dann durch

$$a/b := ab^{-1}$$

definiert.

Beispiel 7 : $\mathbb{Q}$ mit der in Satz **??** definierten Addition und Multiplikation ist ein Körper. Der Ring der ganzen Zahlen ist kein Körper.

Als Merkregel für diese Definitionen gilt:
In einem Ring kann addiert, subtrahiert und multipliziert werden. In einem Körper kann zusätzlich noch durch Elemente ungleich null dividiert werden. Die Ring-Axiome sind den Rechenregeln für ganze Zahlen nachgebildet.