KAPITEL 2

Zahlen

2.1. Natürlichen Zahlen

Leopold Kronecker (7.12.1823 - 29.12.1891):
Die ganzen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk. (1886)

$$\mathbb{N} := \{0, 1, 2, 3, 4, 5, \ldots\}$$

Wir können addieren und multiplizieren ohne den Zahlbereich zu verlassen. Es gibt kein additiv inverses Element (dann bräuchte man die ganzen Zahlen $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$) und auch kein multiplikativ inverses Element (dann bräuchte man die rationalen Zahlen $\mathbb{Q}$).

AXIOM 2.1.1. *Wohlordnungsprinzip*
Jede nichtleere Menge von natürlichen Zahlen hat ein kleinstes Element

Das ist wichtig und wird noch häufig verwendet. Diese Eigenschaft gilt nicht bei:$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

THEOREM 2.1.2. *Division mit Rest*
Seien $a, b \in \mathbb{N}$ mit $a > 0$. Dann gibt es natürliche Zahlen q, r mit $0 \leq r < a$ sodass

$$b = aq + r$$

*(r ist der **Rest** und q ist der **Quotient** b durch a).*

BEWEIS. Wir zeigen dies mit Hilfe des Wohlordnungsprinzips. Dazu betrachten wir die folgende Menge von natürlichen Zahlen:

$$D := \{b - ak : k \in \mathbb{N}, b - ak \geq 0\}$$

Diese Menge ist nicht leer, denn $k = 0$ liefert die Zahl b, die in D liegt. Damit haben wir die Voraussetzungen für das Wohlordnungsprinzip erfüllt, und dann sei r die kleinste Zahl aus D. Da r aus D ist, hat man

$$r = b - aq.$$

Was schon die gesuchte Darstellung ist, es ist nur noch die zweite Eigenschaft von r nämlich $0 \leq r < a$ zu zeigen. Dies geschieht mit einem Widerspruchsbeweis. Dazu nehmen wir an, dass $r \geq a$ ist. Dann ist aber wegen

$$0 \leq r - a = b - aq - a = b - a(q + 1)$$

auch $r - a$ in der Menge D und $r - a$ ist kleiner als r was ein Widerspruch zu der Minimalität von r ist. □

DEFINITION 2.1.3. Teilbarkeit

Seien $a, b \in \mathbb{Z}$ dann sagt man a **teilt** b (geschrieben als $a|b$), wenn es $k \in \mathbb{Z}$ gibt mit

$$ak = b.$$

a teilt b bedeutet also, dass bei der Division mit Rest der Rest gerade 0 ist.

THEOREM 2.1.4. *Satz vom ggT*

Seien $a, b \in \mathbb{N}_+$, dann existiert ein $d \in \mathbb{N}_+$mit folgenden zwei Eigenschaften:

(1) *d teilt a, d teilt b und*
(2) *ist c ein weiterer Teiler von a und b, dann teilt c auch d.*

BEWEIS. Es wird wieder das Wohlordnungsprinzip verwendet. Dazu betrachten wir die folgende Menge von natürlichen Zahlen:

$$D := \{as + bt : s, t \in \mathbb{Z}, as + bt > 0\}.$$

Diese Menge ist nicht leer, denn z.B. $a = a \times 1 + b \times 0$ liegt in D. Sei also

$$d := as + bt$$

die minimale Zahl aus D. Was bleibt ist zu zeigen, dass beide Eigenschaften aus der Behauptung erfüllt sind.

Beweis von Eigenschaft 2:

Sei c ein gemeinsamer Teiler von a und b, dann existieren g und h, definiert durch $a =: cg$ und $b =: ch$. Damit ist $d = cgs + cht = c(gs + ht)$ und damit teilt c auch die rechte Seite und deshalb auch d.

Beweis von Eigenschaft 1:

Wir zeigen dass $d|a$.Dies reicht völlig aus denn a und b sind vertauschbar, d.h. der Beweis $d|b$ geht genauso. Um zu zeigen, dass $d|a$, betrachten wir die Division mit Rest und wollen zeigen, dass der Rest gerade 0 ist. Nach der Division mit Rest haben wir:

$$a = dq + r,$$

wobei $0 \leq r < d$. Nun gilt aber für den Rest

$$r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq).$$

Also liegt auch r in D, falls es > 0 ist. Da dies aber eine Verletzung der Minimalität von d wäre, folgern wir, dass $r = 0$, und somit ist d ein Teiler von a. □

Man beachte die Ähnlichkeit der beiden Beweise.

REMARK 2.1.5. Die Zahl d aus 2.1.4 ist eindeutig.

BEWEIS. Wir nehmen an es gibt eine zweite Zahl e mit diesen beiden Eigenschaften, dann folgt daraus:

$$d|e \text{ und } e|d$$

was bedeutet dass sich die beiden Zahlen nur durch ihr Vorzeichen unterscheiden können, aber da beide > 0, müssen sie gleich sein. □

Da also die Zahl d eindeutig ist, können wir folgende Definition vornehmen:

DEFINITION 2.1.6. ggT

Die Zahl d aus 2.1.4 mit den Eigenschaften 1) und 2) heißt **größter gemeinsamer Teiler** (kurz **ggT**) von a und b und wird mit $ggT(a, b)$ oder auch kürzer (a, b) bezeichnet.

Ein wichtiges Ergebnis aus obigem Beweis ist die Kenntnis, wie man den ggT auch beschreiben kann, nicht über die Eigenschaft größter gemeinsamer Teiler zu sein, sondern:

COROLLARY 2.1.7. *ggT als kleinste Linearkombination*
Der ggT zweier Zahlen $a, b \in \mathbb{N}_+$ ist die kleinste positive $\mathbb{Z}-$Linearkombination von a und b.

BEWEIS. Dies war genau die Konstruktion von d im Beweis von 2.1.4 □

Die Definition wird erweitert zum ggT mehrerer Zahlen. Dann ist $ggT(x_1, \ldots, x_n)$ der größte gemeinsame Teiler der positiven Zahlen $x_1, \ldots, x_n$.

2.2. Euklidischer Algorithmus

Britannica:Of Euclid's life nothing is known except what the Greek philosopher Proclus (c. AD 410-485) reports in his 'summary' of famous Greek mathematicians. According to him, Euclid taught at Alexandria in the time of Ptolemy I Soter, who reigned over Egypt from 323 to 285 BC. Medieval translators and editors often confused him with the philosopher Eukleides of Megara, a contemporary of Plato about a century before, and therefore called him Megarensis. Proclus supported his date for Euclid by writing 'Ptolemy once asked Euclid if there was not a shorter road to geometry than through the Elements, and Euclid replied that there was no royal road to geometry.' Today few historians challenge the consensus that Euclid was older than Archimedes (c. 290/280-212/211 BC).

LEMMA 2.2.1. *ggT und die Division mit Rest*
Seien $a, b \in \mathbb{N}_+$, und sei $b = aq + r$ eine Division mit Rest wobei $q, r > 0$. Dann ist

$$ggT(a, b) = ggT(a, r).$$

BEWEIS. Wir verwenden hier die kürzere Notation (a, b) anstelle von $ggT(a, b)$. Um zu zeigen, dass $(a, b) = (a, r)$ ist, zeigen wir, dass beide Teiler von einander sind. Da beide ggT positive ganze Zahlen sind, müssen sie dann gleich sein.
Teil 1: (a, b) ist nach Definition des ggT ein Teiler von sowohl a als auch b. Somit teilt (a, b) in der Gleichung

$$r = b - aq$$

beide Summanden der rechten Seite und damit dann auch die linke Seite. Somit ist (a, b) Teiler von r und von a und somit nach Definition des ggT ist (a, b) Teiler von (a, r).
Teil 2: Das gleiche Verfahren geht auch mit (a, r) bei Betrachtung der Gleichung

$$b = r + aq.$$

□

THEOREM 2.2.2. *Euklidischer Algorithmus*
Seien $a, b \in \mathbb{N}_+$, falls a Teiler von b ist, ist $ggT(a, b) = a$. Ansonsten liefert die iterierte Anwendung der Division mit Rest eine Folge $r_1, r_2, \ldots, r_n$:

$$\begin{array}{rcll} b & = & aq_1 + r_1 & (0 < r_1 < a) \\ a & = & r_1q_2 + r_2 & (0 < r_2 < r_1) \\ & \vdots & & \\ r_{n-2} & = & r_{n-1}q_n + r_n & (0 < r_n < r_{n-1}) \\ r_{n-1} & = & r_nq_{n+1} & \end{array}$$

Dann ist r_n der ggT von a und b.

BEWEIS. Die Folge $r_1, \ldots, r_n$ ist streng monoton fallend und da sie aus natürlichen Zahlen besteht, muss sie enden, nämlich bei r_n. Dies wissen wir aus dem Satz 2.1.4 über die Division mit Rest. Das vorbereitende Lemma 2.2.1 liefert folgende Gleichungskette zur Berechnung des ggT:

$$r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = \ldots = (r_1, r_2) = (a, r_1) = (b, a).$$

Damit wissen wir, dass der letzte Wert dieser Folge der ggT ist. □

Darauf lässt sich dann ein Algorithmus aufbauen, denn man sieht an der Endlichkeit der Folge $r_1, r_2, \ldots$, dass das Verfahren terminiert.

ALGORITHM 2.2.3. *Euklidischer Algorithmus*
input: $a, b \in \mathbb{N}_+$
output: $ggT(a, b)$
$r :=$*Rest von* b/a
ist $r = 0$ *so ist das Ergebnis* a
ansonsten $b := a$,$a := r$ *und neu anfangen*

EXAMPLE 2.2.4. Euklidischer Algorithmus als C Programm
while (r=b%a) { b=a; a=r; }
return a;

EXAMPLE 2.2.5. Berechnung des ggT
Wir starten mit $a = 30$,$b = 171$.
Der erste Schritt ist die Division durch 30 mit Rest:

$$171 = 5 \times 30 + 21.$$

Der Rest ist 21 und man weiss aus dem Lemma $(171, 30) = (30, 21)$ und die nächste Iteration ist die Division von 30 durch 21 mit Rest

$$30 = 1 \times 21 + 9$$

der Rest ist 9 und man weiss aus dem Lemma $(171, 30) = (30, 21) = (21, 9)$ und die nächste Iteration ist die Division von 21 durch 9 mit Rest

$$21 = 2 \times 9 + 3$$

der Rest ist 3 und man weiss aus dem Lemma $(171, 30) = (30, 21) = (21, 9) = (9, 3)$ und die nächste Iteration ist die Division von 9 durch 3 mit Rest

$$9 = 3 \times 3 + 0$$

und der Rest ist 0 und man hat den ggT gefunden:

$$(171, 30) = (30, 21) = (21, 9) = (9, 3) = 3.$$

Mit diesem Algorithmus hat man aber noch nicht die $\mathbb{Z}-$Linearkombination des ggT. Ein solcher Algorithmus wird oft als ***erweiterter ggT Algorithmus*** bezeichnet. Die Linearkombination bekommt man z.B. durch Rückwärtseinsetzen.

EXAMPLE 2.2.6. Erweiterter ggt mit Rückwärtseinsetzen
Aus dem Beispiel 2.2.5 wissen wir, dass $(171, 30) = 3$. Setzt man nun rückwärts ein, erhält man folgende Gleichungskette:

$$\begin{aligned} 3 &= 21 - 2 \times 9 \\ &= 21 - 2 \times (30 - 21) \\ &= 3 \times 21 - 2 \times 30 \\ &= 3 \times (171 - 5 \times 30) - 2 \times 30 \\ &= 3 \times 171 - 17 \times 30, \end{aligned}$$

was eine $\mathbb{Z}-$Linearkombination des ggT liefert.

Diese Methode hat den Nachteil, dass erst vorwärts und dann nochmal rückwärts gerechnet wird. Die bessere Methode ist folgende, die in Anlehnung an das bekannte Gaußverfahren zur Lösung von linearen Gleichungssystemen funktioniert. Zur Berechnung von

$$ggT(a, b) = as + bt$$

startet man mit den beiden Gleichungen

$$\begin{aligned} 1 \times a \quad &+0 \times b \quad &= a \\ 0 \times a \quad &+1 \times b \quad &= b \end{aligned}$$

was sich auch kürzer schreibt mittels der Matrix:

$$\left(\begin{array}{cc|c} 1 & 0 & a \\ 0 & 1 & b \end{array}\right).$$

Nun wird der grössere der beiden Einträge in der rechten Spalte klein gemacht, indem man Vielfache der anderen Zeile abzieht. Dies entspricht der Division mit Rest aus einem Schritt beim Euklidischen Algorithmus. Das Verfahren endet, wenn eine Zeile in der rechten Spalte 0 ist, die andere Zeile ist die Linearkombination des ggT.

EXAMPLE 2.2.7. Erweiterter ggT mit Matrixmethode

Wir starten wieder mit $a = 30, b = 171$. Die erste Matrix ist dann

$$\left(\begin{array}{cc|c} 1 & 0 & 30 \\ 0 & 1 & 171 \end{array}\right).$$

Der erste Schritt ist das Abziehen der Zeile mit 30 von der Zeile mit 171. Dabei kann das $5-$fache abgezogen werden:

$$\left(\begin{array}{cc|c} 1 & 0 & 30 \\ 0 & 1 & 171 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 30 \\ -5 & 1 & 21 \end{array}\right)$$

Die nächsten Schritte sind:

$$\left(\begin{array}{cc|c} 1 & 0 & 30 \\ -5 & 1 & 21 \end{array}\right) \to \left(\begin{array}{cc|c} 6 & -1 & 9 \\ -5 & 1 & 21 \end{array}\right) \to \left(\begin{array}{cc|c} 6 & -1 & 9 \\ -17 & 3 & 3 \end{array}\right)$$

Der nächste Schritt ist auch schon der letzte denn es wird eine Zeile erzeugt, wo in der rechten Spalte eine 0 steht:

$$\left(\begin{array}{cc|c} 6 & -1 & 9 \\ -17 & 3 & 3 \end{array}\right) \to \left(\begin{array}{cc|c} 57 & -10 & 0 \\ -17 & 3 & 3 \end{array}\right).$$

Damit hat man als Ergebnis in der unteren Zeile:

$$3 = ggT(30, 171) = -17 \times 30 + 3 \times 171.$$

Zwei natürliche Zahlen a und b heißen ***teilerfremd***, wenn $ggT(a, b) = 1$.

THEOREM 2.2.8. *zwei wichtige Eigenschaften teilerfremder Zahlen*

Seien a, b, c natürliche Zahlen, wobei a und b teilerfremd sind. Dann gilt

(1) *falls bc von a geteilt wird, wird bereits c von a geteilt.*
(2) *falls sowohl a als auch b das c teilen, dann teilt auch ab die Zahl c.*

BEWEIS. Der Beweis geht sehr einfach und schön bei Verwendung der Linearkombination des ggT. Man hat:

$$1 = as + bt.$$

Nach Multiplikation mit c hat man:

$$c = cas + cbt.$$

Beide Behauptungen lassen sich direkt ablesen. □

2.2.1. Kleinste gemeinsame Vielfache. Das *kleinste gemeinsame Vielfache* (kgV) zweier ganzer Zahlen a und b ist definiert als die kleinste positive Zahl m mit der Eigenschaft a teilt m und auch b teilt m. Es wird mit $kgV(a, b)$ bezeichnet. Man muss natürlich nachweisen, dass eine solche Zahl existiert und auch eindeutig ist. Ähnlich wie beim ggT kann man auch den kgV mehrere Zahlen definieren.