Lineare Algebra

Vorlesungsmitschrift von
Frank Schmidt

Korrekturgelesen von
Oliver Müller

§1 Die ganzen Zahlen

$\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\} \supseteq \mathbb{N}$

Menge der ganzen Zahlen

(1.1) Eigenschaften

I. **Addition** gegeben $a,b \in \mathbb{Z}$
$\Rightarrow a+b$ wohldefiniert

(a) Assoziativgesetz: $(a+b)+c = a+(b+c)$
(b) Kommutativgesetz: $a+b = b+a$
(c) $0 \in \mathbb{Z}$ erfüllt $0+a=a \quad \forall a \in \mathbb{Z}$
(d) Für $a \in \mathbb{Z}$ erfüllt $-a : a+(-a)=0$

II. **Multiplikation** $a,b \in \mathbb{Z}$
$\Rightarrow a \cdot b$ wohldefiniert

(a) Assoziativgesetz: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
(b) Kommutativgesetz: $a \cdot b = b \cdot a$
(c) $1 \in \mathbb{Z}$ erfüllt $1 \cdot a = a \quad \forall a \in \mathbb{Z}$

III. **Distributivgesetz**
$a \cdot (b+c) = a \cdot b + a \cdot c$

IV. $\leq$ ist Totalordnung auf $\mathbb{Z}$. Es gelten

(a) $a \leq b \Rightarrow a+c \leq b+c$
(b) $a \leq b, c > 0 \Rightarrow a \cdot c \leq b \cdot c$

Bemerkung:
Die Eigenschaften I-III sind gerade die Merkmale eines **kommutativen Rings**.

(1.2) Teilbarkeit

Sei $a,b \in \mathbb{Z}$, $b \neq 0$

Definition:
b teilt a, b|a, wenn ein $c \in \mathbb{Z}$ existiert mit $a = b \cdot c$.

(1.3) Satz

Seien $a,b \in \mathbb{Z}$, sei $b \neq 0$. Dann existieren eindeutige Zahlen $q,r \in \mathbb{Z}$ mit

$$a = q \cdot b + r \quad \text{und} \quad 0 \leq r < |b|$$

Beispiele:

(1) $23_{(a)} = 2_{(q)} \cdot 8_{(b)} + 7_{(r)}$

(2) $-23 = (-3) \cdot 8 + 1$

Beweis:

Existenz

Fall 1: $a \geq 0$, $b > 0$

Induktion über a (bei festem b)

I.A. $a = 0$ $\qquad 0 = 0 \cdot b + 0$ ✔

Sei die Behauptung bewiesen für alle $a' \leq a$

Betrachte $a = 1$

- Ist $a + 1 < b$, so zeigt $a + 1 = 0 \cdot b + (a+1)$ die Behauptung
- Andernfalls

  Ist $0 \leq a + 1 - b \leq a$

  $\underset{I.V.}{\Rightarrow} \exists q,r : a + 1 - b = q \cdot b + r \qquad 0 \leq r < b$

  $\Rightarrow a + 1 = (q+1)b + r \qquad \Rightarrow$ Fall 1

Fall 2: Sei $a < 0$, $b > 0$

$\underset{Fall1}{\Rightarrow} -a = qb + r \qquad 0 \leq r < b$

- Ist $r = 0$

  $\Rightarrow a = (-q) \cdot b$
- Ist $r > 0$

  $\Rightarrow a = (-q)b - r$

  $= (-q-1)b + (b-r) \quad = \quad q'b + r' \quad , \quad 0 < r' < b$

Fall 3: a beliebig, $b < 0$

$\underset{Fall1+2}{\Rightarrow} a = q(-b) + r$

$= (-q) \cdot b + r \quad \Rightarrow$ *Behauptung*

Eindeutigkeit

Sei $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2 \qquad 0 \leq r_1, r_2 < |b|$

$\Rightarrow 0 = (q_1 - q_2)b + (r_1 - r_2), \quad (o.E.)\ r_1 \geq r_2$

$0 \leq r_1 - r_2 < |b| \quad , \quad (r_1 - r_2) = (q_2 - q_1)b$

$\Rightarrow q_1 = q_2 \quad \Rightarrow \quad r_1 = r_2$

q.e.d.

(1.4) Definition Primzahlen

Eine Zahl $p \in \mathbb{Z}$ heißt **Primzahl** wenn gilt

(1) $p \neq -1,0,1$

(2) Die einzigen Teiler von p sind $-p, -1, 1, p$
z.B. –2,2,-3,3,-5,5

(1.5) Satz

Sei $n \in \mathbb{Z},\ n \neq -1,0,1$
Dann ist n ein Produkt von Primzahlen

Beweis:
o.E. sei $n \in \mathbb{N},\ n \geq 2$
Induktion über n
n=2 ist prim.
Der Satz gelte für alle $n' \leq n$
Betrachte n+1:

1.Fall: $n+1$ ist prim $\Rightarrow$ Satz gilt für $n+1$
2.Fall: $n+1$ nicht prim $\Rightarrow \exists d, e \geq 2$ mit $n+1 = d \cdot e$

$\Rightarrow d < n+1, e < n+1$

$\underset{I.V.}{\Rightarrow} \exists d = p_1 \cdot \ldots \cdot p_r, p_k \ prim$

$\Rightarrow \exists e = q_1 \cdot \ldots \cdot q_s, q_k \ prim$

$\Rightarrow n+1 = p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s \Rightarrow$ Behauptung q.e.d.

Von nun an betrachten wir nur natürliche Zahlen.

(1.6) Definition größter gemeinsamer Teiler

Seien $a, b \in \mathbb{N}_+$
$d \in \mathbb{N}_+$ heißt **größter gemeinsamer Teiler**, ggT von a, b, wenn gilt

(a) $d \mid a$ und $d \mid b$

(b) Ist $e \in \mathbb{N}_+$ mit $e \mid a$ und $e \mid b$
$\Rightarrow e \mid d$

(1.7) Satz

Seien $a, b \in \mathbb{N}_+$ Dann existiert $\text{ggT}(a, b)$

Beweis:
Sei o.E. $a \geq b$

Induktion über a
I.A. $a = 1 \Rightarrow b = 1$ $\quad ggT(1,1) = 1$
I.V. Satz gelte $\forall a' \leq a$
I.S. Betrachte $a+1$ und $b \leq a+1$
Fall 1: $b \mid a+1 \Rightarrow ggT(a+1,b) = b$
Fall 2: $b \nmid a+1$
$\exists q,r : a+1 = q \cdot b + r$, $0 < r < b$
Behauptung: c ist gemeinsamer Teiler von $a+1, b$
$\Leftrightarrow$ c ist gemeinsamer Teiler von b, r
Sei $c \mid a+1, c \mid b \Rightarrow a+1 = \underbrace{x \cdot c}_{a+1} = q \cdot \underbrace{y \cdot c}_{b} + r$
$\Rightarrow c \mid r$ da $r = c(x - qy)$
Sei $c \mid r$ und $c \mid b \Rightarrow c \mid a+1$ $\quad \exists ggT(b,r)$
Dieser ist auch $ggT(a+1,b)$ $\Rightarrow$ Behauptung q.e.d.

(1.8) Der Euklidische Algorithmus

Sei $a_0 := a$, $a_1 := b$
Seien $a_{n'}$ definiert für $n' \leq n$
Falls $a_n \mid a_{n-1}$ so sei a_{n+1} nicht definiert
Falls $a_n \nmid a_{n-1}$ so sei a_{n+1} definiert durch
$a_{n-1} = q \cdot a_n + a_{n+1}$, wobei $0 < a_{n+1} < a_n$

Die Folge ist endlich, da spätestens für $a_n = 1$ der Fall 1 eintritt
$\Rightarrow ggT(a,b) = ggT(a_0, a_1) = ggT(a_1, a_2)$
$\Rightarrow ggT(a_2, a_3) ... = ggT(a_{n-1}, a_n)$ wobei $a_n \mid a_{n-1}$

Beispiel:

$a_0 = 83$ $\quad a_1 = 77$

$83 = 1 \cdot 77 + 6$
$77 = 12 \cdot 6 + 5$
$6 = 1 \cdot 5 + 1$ $\quad 1 \mid 5$

(1.9) Lemma von Bezout

Seien $a, b \in \mathbb{N}_+$

$\Rightarrow \exists A, B \in \mathbb{Z}$ mit $ggT(a,b) = A \cdot a + B \cdot b$

Beweis:
Seien $a_0 = a, a_1 = b, ...a_n$ die Reste des Euklidischen Algorithmus
Es gibt Zahlen $A_1, A_2, ..., B_1, B_2, ...$ so dass $a_k = A_k a + B_k b$

I.A. Dies gilt für k=1
$a_1 = 0 \cdot a_0 + 1 \cdot a_1$
I.V. $a_k = A_k a + B_k b$
I.S. falls $k < n$
$\Rightarrow a_{k-1} = q_k a_k + a_{k+1}$
$\Rightarrow A_{k-1} a + B_{k-1} b = q_k (A_k a + B_k b) + a_{k+1}$
$\Rightarrow (A_{k-1} - qA_k) \cdot a + (B_{k-1} - qB_k) b = a_{k+1}$ $\Rightarrow$ Behauptung q.e.d.

(1.10) Lemma von Euklid

Sei p eine Primzahl und $a, b \in \mathbb{N}_+$
Falls $p \mid a \cdot b \Rightarrow p \mid a$ *oder* $p \mid b$

Beweis:
Angenommen $p \nmid a$ und $p \nmid b$
Dann gilt: $\text{ggT}(p, a) = 1$ $\text{ggT}(p, b) = 1$
$\underset{(1.9)}{\Rightarrow} \exists A, B, C, D \in \mathbb{Z}$
$1 = Ap + Ba$, $1 = Cp + Db$
$\Rightarrow 1 = (Ap + Ba)(Cp + Db)$
$= Acp^2 + ADbp + BCap + BDab$

Sei $ab = px$:
$\Rightarrow 1 = (ACp + ADb + BCa + BDx) \cdot p$ ↯
$\Rightarrow$ Behauptung q.e.d.

(1.11) Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl $n \geq 2$ ist eindeutig ein Produkt von Primzahlen.

Beweis:
- **Existenz:** (1.5)
- **Eindeutigkeit:**
  Sei $n = p_1 \cdot ... \cdot p_r = q_1 \cdot ... \cdot q_s$
  $p_1 \leq p_2 \leq ... \leq p_r, q_1 \leq ... \leq q_s$
  Sei $p_r \leq q_s$
  Wäre $p_r < q_s \Rightarrow q_s \nmid p_k$ $1 \leq k \leq r$
  $\underset{(1.10)}{\Rightarrow} q_s \nmid p_1 \cdot ... \cdot p_r = n$ ↯

$\Rightarrow q_s = p_r$

$\frac{n}{q_s} = p_1 \cdot \ldots \cdot p_{r-1} = q_1 \cdot \ldots \cdot q_{s-1}$

$\underset{I.V.}{\Rightarrow} r = s \quad p_k = q_k$ $\Rightarrow$ Behauptung q.e.d.

(1.12) Satz

Sei M Menge, für $x \in M$ sei A(x) Aussage
$A(x)$ gilt für fast alle $x \in M$ (f.f.a.)
$:\Leftrightarrow A(x)$ gilt höchstens für endlich viele x nicht

Beispiele:

(a) Sei $C \in \mathbb{N} \Rightarrow x > C$ f.f.a. $x \in \mathbb{N}$

(b) Sei $(a_n)_{n \in N}$ eine Familie von Zahlen mit $a_n = 1$ f.f.a. n

$\Rightarrow \exists n_0 : \forall n \geq n_0 : a_n = 1$

$$\prod_{n \in N} a_n := \prod_{k=1}^{n_0} a_k$$

(c) Sei P die Menge der Primzahlen

$\Rightarrow$ Jede Zahl $n \in \mathbb{N}_+$ hat eine eindeutige Darstellung

$$n = \prod_{p \in P} p^{\nu_p(n)}, \nu_p(n) = 0 \text{ f.f.a. } p \in P$$

$252 = 2^2 \cdot 3^2 \cdot 7$

$\nu_2(252) = 2$
$\nu_3(252) = 2$ $\qquad \nu_p(252) = 0 \qquad p \neq 2,3,7$
$\nu_7(252) = 1$

(1.14) Satz

(a) Seien $a, b \in \mathbb{N}_+$. Dann gilt

$a \mid b \Leftrightarrow \nu_p(a) \leq \nu_p(b) \qquad \forall p \in P$

(b) Sei $d = ggT(a,b)$. Dann gilt:

$\nu_p(d) = \min(\nu_p(a), \nu_p(b))$

Beispiel:

$48 = 2^4 \cdot 3$
$36 = 2^2 \cdot 3^2$ $\qquad$ ggT $= 2^2 \cdot 3^1$ (immer die kleinste Hochzahl)

Beweis:

- (a) folgt aus (1.11)
- Sei $d' = \prod_{p \in P} p^{\min(\nu_p(a),\nu_p(b))}$

  $d' \mid a$ und $d' \mid b$

  Sei e gemeinsamer Teiler von a,b

  $\Rightarrow \nu_p(e) \le \nu_p(a) \quad , \quad \nu_p(e) \le \nu_p(b) \quad \forall p \in P$

  $\Rightarrow \nu_p(e) \le \min(\nu_p(a),\nu_p(b)) = \nu_p(d')$

  $\Rightarrow e \mid d'$

  $\Rightarrow d' = \text{ggT}(a,b)$ $\Rightarrow$ Behauptung

(1.13) Definition

Seien $a,b \in \mathbb{N}_+$

$m \in \mathbb{N}_+$ heißt kleinstes gemeinsames Vielfaches von a,b $\text{kgV}(a,b)$, wenn gilt:

(a) $a \mid m$ und $b \mid m$

(b) Ist n ein gemeinsames Vielfaches von a,b, so gilt $m \mid n$

$$a = \prod_{p \in P} p^{\nu_p(a)}$$

$$\text{kgV}(a,b) = \prod_{p \in P} p^{\max(\nu_p(a),\nu_p(b))}$$

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

$$\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)$$

$$\max(\nu_p(a),\nu_p(b)) = \nu_p(a) + \nu_p(b) - \min(\nu_p(a),\nu_p(b))$$

(1.15) Satz (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis:

Behauptung: Sei $\{p_1,\ldots p_n\}$ eine endliche Menge von Primzahlen. Dann existiert eine Primzahl $q \notin \{p_1,\ldots p_n\}$

Sei $a := \left(\prod_{k=1}^{n} p_k\right) + 1$ und $a = q_1 \cdot \ldots \cdot q_r$ die Primfaktorzerlegung

$p_k \nmid a \ \forall 1 \le k \le n$ $\Rightarrow$ $q_1 \notin \{p_1,\ldots p_n\}$ $\Rightarrow$ Behauptung q.e.d.

(1.16) Lemma

Sei $n \in \mathbb{Z},\ n \neq -1,0,1$
Definiere Relation auf $\mathbb{Z}$
$a \sim b :\Leftrightarrow a-b$ ist durch n teilbar
~ ist eine **Äquivalenzrelation**.

Beweis:
(r) $a \sim a$: $a-a=0$ ist durch n teilbar
(s) $a \sim b \Rightarrow n \mid a-b \Rightarrow n \mid b-a \Rightarrow b \sim a$
(t) $a \sim b, b \sim c \Rightarrow n \mid a-b, n \mid b-c \quad \Rightarrow \quad n \mid a-c \quad \Rightarrow a \sim c$ q.e.d.

$a \sim b \Leftrightarrow a,b$ lassen bei Division durch n den selben Rest
$a = q_1 \cdot n + r_1$ o.E. $r_1 \leq r_2$
$b = q_2 \cdot n + r_2$ $b-a = (q_2-q_1)n + (r_2-r_1)$

(1.17) Lemma

Sei $a \sim a', b \sim b'$
Dann gilt: $a+b \sim a'+b'$
$a \cdot b \sim a' \cdot b'$

Beweis:
$a' = a + A \cdot n \quad , \quad b' = b + B \cdot n \quad , \quad A, B \in \mathbb{Z}$ geeignet
$a'+b' = a+b+An+Bn = a+b+(A+B)n$ } $a'+b' \sim a+b$
$a' \cdot b' = (a+An)(b+Bn) = ab+aBn+bAn+ABn^2 = ab+(aB+bA+ABn)n$ } $a' \cdot b' \sim a \cdot b$
q.e.d.

Sei $[a] = \bar{a}$ die Äquivalenzklasse von a

(1.18) Korollar

Durch $\begin{matrix}[a]+[b] := [a+b] \\ [a] \cdot [b] := [a \cdot b]\end{matrix}$ ist eine Addition und eine Multiplikation auf den Äquivalenzklassen wohldefiniert.

Es gelten die Gesetze I-III in (1.1)
$([a]+[b])+[c] = [a]+([b]+[c])$ usw.

Die Menge der Äquivalenzklassen (Restklassen): $\mathbb{Z}/\mathbb{Z} \cdot n$ ($\mathbb{Z}$ modulo $\mathbb{Z} \cdot n$)

$a \sim b = a \equiv b \bmod n$ (a kongruent b modulo n)

(1.19) Beispiel

$n = 12 \qquad \mathbb{Z}/\mathbb{Z}\cdot 12 = \{\bar{0}, \bar{1}, ..., \overline{11}\}$

$\bar{7} + \bar{6} = \overline{13} = \bar{1}$
$\bar{7} \cdot \bar{8} = \overline{56} = \bar{8}$
$\bar{5}^{1000} = \bar{1}^{500} = \bar{1}$
$\bar{6} \cdot \bar{2} = \overline{12} = \bar{0}$

(1.20) Satz

Sei $\text{ggT}(n, a) = 1$
Dann existiert $\bar{b} \in \mathbb{Z}/\mathbb{Z}\cdot n$ so dass $\bar{a} \cdot \bar{b} = 1$

Beweis:
Nach dem Lemma von Bezout $\exists A, B \in \mathbb{Z}$ mit

$1 = An + Ba$
$\Rightarrow \quad 1 = \bar{A} \cdot \bar{n} + \bar{B} \cdot \bar{a}$ (1.17) $\Rightarrow 1 = \bar{B} \cdot \bar{a}$ $\Rightarrow$ Behauptung q.e.d.

i.A. ist $\overline{a^{-1}}$ nicht definiert

$\bar{a} + (\overline{-a}) = \bar{0}$
$(\overline{-a}) := -\bar{a}$

Sei $\text{ggT}(a, n) = 1$
$\Rightarrow \bar{a}x = \bar{b}$ hat genau eine Lösung
$x = \bar{a}^{-1} \cdot \bar{b}$

(1.21) Anwendungen

$41271 = 1 \cdot 10^0 + 7 \cdot 10^1 + 2 \cdot 10^2 + 1 \cdot 10^3 + 4 \cdot 10^4 \bmod 3$
$10 \equiv 1 \bmod 3$
$41271 \equiv 1 \cdot 1 + 7 \cdot 1 + 2 \cdot 1 + 1 \cdot 1 + 4 \cdot 1 \bmod 3$

3-Probe: Jede Dezimalzahl ist mod 3 kongruent zu ihrer Quersumme.

9-Probe: $10 \equiv 1 \bmod 9$
$\Rightarrow$ Jede Dezimalzahl ist kongruent zu ihrer Quersumme mod 9

11-Probe: $10 \equiv -1 \bmod 11$

$10^n \equiv (-1)^n \bmod 11$

$41271 = 1 - 7 + 2 - 1 + 4 = -1 \equiv 10$

$\Rightarrow$ Jede Dezimalzahl ist kongruent zu ihrer alternierenden Quersumme mod 11