Westfälische
Wilhelms-Universität
Münster

Fachbereich 10
Mathematik und
Informatik

Elementare Zahlentheorie

gelesen von Prof. Dr. Falko Lorenz

Mitschrift von Phil Steinhorst

Wintersemester 2014/2015

http://wwwmath.uni-muenster.de/u/karin.halupczok/elZTWiSe14/

Stand: 27. Oktober 2014

Vorwort

Der vorliegende Text ist eine Zusammenfassung zur Vorlesung Elementare Zahlentheorie, gelesen von Prof. Dr. Falko Lorenz an der WWU Münster im Wintersemester 2014/2015. Der Inhalt entspricht weitestgehend dem Skript, welches auf der Vorlesungswebsite bereitsgestellt wird, jedoch wird auf Beweise weitestgehend verzichtet. Für die Korrektheit des Inhalts wird keinerlei Garantie übernommen. Bemerkungen, Korrekturen und Ergänzungen kann man folgenderweise loswerden:

- persönlich durch Überreichen von Notizen oder per E-Mail
- durch Abändern der entsprechenden TeX-Dateien und Versand per E-Mail an mich
- direktes Mitarbeiten via GitHub. Dieses Skript befindet sich im `latex-wwu`-Repository von Jannes Bantje:

  https://github.com/JaMeZ-B/latex-wwu

Themenübersicht

Im Sommersemester 2013 wurden folgende Themen behandelt:

- Ein paar algebraische Grundlagen (Gruppen- und Ringtheorie, Ideale)
- Fundamentalsatz der Arithmetik (Satz von der eindeutigen Primfaktorzerlegung)
- Euklidischer Algorithmus, Kettenbruchdarstellung
- Simultane Kongruenzen, Satz von Euler-Fermat, chinesischer Restsatz
- Restklassengruppen, Hauptsatz über endliche abelsche Gruppen
- Gaußscher Zahlenring $\mathbb{Z}[\mathrm{i}]$
- Quadratische Reste, Quadratisches Reziprozitätsgesetz
- Fermat- und Mersenne-Primzahlen
- Zahlentheoretische Funktionen $\varphi\colon \mathbb{N} \longrightarrow \mathbb{C}$
- Satz von Lagrange (”Vier-Quadrate-Satz”)

Literatur

- F. Ischebeck: Einladung zur Zahlentheorie
- R. Remmert, P. Ullrich: Elementare Zahlentheorie
- A. Scholz, B. Schöneberg: Einführung in die Zahlentheorie
- K. Halupczok: Skript zur Elementaren Zahlentheorie

Vorlesungswebsite

http://wwwmath.uni-muenster.de/u/karin.halupczok/elZTWiSe14/

Phil Steinhorst
p.st@wwu.de

Inhaltsverzeichnis

1 Fundamentalsatz der elementaren Arithmetik **4**

2 Der euklidische Algorithmus **10**

Index **16**

1 Fundamentalsatz der elementaren Arithmetik

Terminologie

14.10. Sei R ein kommutativer Ring mit $1 \neq 0$. R heißt **Integritätsring** bzw. **nullteilerfrei**, wenn gilt:

$$a \cdot b = 0 \quad \Rightarrow \quad a = 0 \text{ oder } b = 0.$$

Beispiel 1.1

- $\mathbb{Z}$
- $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$
  $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$
  $\mathbb{Z}[\sqrt{-5}] := \ldots$
- $K[X]$ für K Körper
  $\mathbb{Z}[X]$
- K Körper
- $\mathbb{C}\langle z\rangle := \{\text{konvergente Potenzreihen } \sum_{n=0}^{\infty} a_n z^n\}$
- Nicht nullteilerfrei ist z.B. $\mathcal{C}[0,1] := \{f \colon [0,1] \to \mathbb{R} \text{ stetig}\}$

Definition 1.1 (Teilbarkeit)

Seien $a, b \in R$. a heißt ein **Teiler** von b, wenn ein $q \in R$ existiert mit $b = qa$, und schreiben:

$$a|b$$

Ist R nullteilerfrei und $a \neq 0$, so ist q eindeutig bestimmt.

F1.1 (Triviale Teilbarkeitsregeln)

(i) $a|0, 1|a, a|a$

(ii) $a|b, b|c \quad \Rightarrow \quad a|c$

(iii) $a|b, a|c \quad \Rightarrow \quad a|b + c, a|b - c$

(iv) $a_1|b_1, a_2|b_2 \quad \Rightarrow \quad a_1 a_2|b_1 b_2$

(v) $ac|bc \quad \Rightarrow \quad a|b$, falls $c \neq 0$ und R nullteilerfrei.

Definition 1.2 (Einheit, assoziiert)

(i) $e \in R$ heißt eine **Einheit** in R, falls $e|1$ gilt, d.h. falls ein $f \in R$ existiert mit $ef = 1$. f ist eindeutig bestimmt.
Wir setzen $e^{-1} := f$ und schreiben auch $\frac{1}{e}$ für e^{-1}.
Wir bezeichnen die **Einheitengruppe** von R mit $R^\times := \{x \in R : x \text{ ist Einheit in } R\}$.

(ii) $a \in R$ heißt **assoziiert** zu $b \in R$, falls $a|b$ und $b|a$ gilt. Schreibe: $a \hat{=} b$.

Beispiel 1.2

1) Sei K ein Körper, dann ist $K^\times = K \setminus \{0\}$. $\quad \mathbb{Z}^\times = \{1, -1\}, \quad K[X]^\times = K^\times,$
$\mathcal{C}[0,1]^\times = \{f \in \mathcal{C}[0,1] : f(x) \neq 0 \text{ für alle } x \in [0,1]\}, \quad \mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^k : k \in \mathbb{Z}\}$
$\mathbb{Z}[X]^\times = \{1, -1\} \quad \mathbb{C}\langle z\rangle^\times = \{\sum a_n z^n \in \mathbb{C}\langle z\rangle : a_0 \neq 0\}$

2) $e \in R^\times \quad \Leftrightarrow \quad e|a$ für jedes $a \in R$.

F1.2
Sei R ein Integritätsring, $a, b \in R$ und $b \neq 0$. Dann gilt:

$$a \mathrel{\hat{=}} b \quad \Leftrightarrow \quad \exists e \in R^\times \text{ mit } b = ea$$

Beweis
"⇐": $a|b, e^{-1}b = a, b|a$

"⇒": Da $a|b$ und $b|a$, existieren $e, f \in R$, sodass $b = ea$ und $a = fb$. $\Rightarrow b = efb \Rightarrow ef = 1$, da $b \neq 0$ und R nullteilerfrei. □

Ab jetzt ist, wenn nichts anderes gesagt, R ein Integritätsring!

Definition 1.3 (unzerlegbar, irreduzibel, zusammengesetzt)
Sei $a \in R \setminus R^\times$. a heißt **unzerlegbar** oder **irreduzibel** in R, wenn gilt:

$$a = bc \text{ in } R \quad \Rightarrow \quad b \in R^\times \text{ oder } c \in R^\times.$$

Andernfalls heißt a **zerlegbar**, **zusammengesetzt** oder **reduzibel**.

Bemerkung
a unzerlegbar $\Leftrightarrow$ jeder Teiler von a ist Einheit oder assoziiert zu a
a zerlegbar $\Leftrightarrow$ a hat echten Teiler, d.h. einen Teiler, der weder eine Einheit ist noch assoziiert zu a

Definition 1.3 (Primzahl)
Ein $p \in \mathbb{Z}$ heißt **Primzahl**, wenn $p \in \mathbb{N}$ und p unzerlegbar in $\mathbb{Z}$. Wir beziehnen mit $\mathbb{P}$ die Menge der Primzahlen von $\mathbb{Z}$. a unzerlegbar in $\mathbb{Z} \Leftrightarrow a = p$ oder $a = -p$ mit $p \in \mathbb{P}$.

Bemerkung
$a \in \mathbb{Z}$ sei zerlegbar, $a \neq 0$. Dann gibt es eine Primzahl p mit $p|a$ und $p \leq \sqrt{|a|}$.

Definition 1.4 (Zerlegung in unzerlegbare Faktoren)
Wir sagen, $a \in R$ besitzt in R eine **Zerlegung in unzerlegbare Faktoren**, wenn

$$a = ep_1p_2 \dots p_r \text{ mit } e \in R^\times \text{ und } p_1, \dots, p_r \text{ unzerlegbar} \tag{1.1}$$

(1.1) heißt eine Zerlegung von a in unzerlegbare Faktoren. Auch $r = 0$ ist erlaubt.

F1.3
In $\mathbb{Z}$ besitzt jedes $a \neq 0$ eine Zerlegung in unzerlegbare Faktoren.

F1.3
Jede natürliche Zahl $a > 1$ besitzt eine Zerlegung $a = p_1p_2 \dots p_r$ mit Primzahlen $p_1, \dots, p_r$ und $r \geq 1$.

Bemerkung
1) Die Aussage F1.3 gilt auch für die Beispiele zu Beginn, mit Ausnahme von $\mathcal{C}[0, 1]$.

2) Sei R ein Integritätsring, der die **Teilbarkeitsbedingung für Hauptideale** erfüllt, so besitzt jedes $a \neq 0$ aus R eine Zerlegung in unzerlegbare Faktoren.

3) Primzahlen sind die multiplikativen Bausteine (Atome) von $\mathbb{N}$.

4) Im Beispiel $\mathbb{C}\langle z\rangle$ von oben gibt es (bis auf Assoziiertheit) nur das einzige unzerlegbare Element z. Dieses ist ein **Primelement** (der Begriff folgt weiter unten).

Satz 1.1 (Existenz unendlich vieler Primzahlen)
Es gibt unendlich viele Primzahlen.

Bemerkungen
Es sei $p_1, p_2, \ldots$ die aufsteigend sortierte Folge der Primzahlen.

1) $a_n := p_1 p_2 \ldots p_n + 1$ ist Primzahl für $n \leq 5$, aber z.B. nicht für $n = 6$. Unklar ist, ob unendlich viele a_n Primzahlen oder keine Primzahlen sind.

2) Für $x \in \mathbb{R}_{>0}$ definieren wir:
$$\pi(x) := \#\{p \in \mathbb{P} : p \leq x\}$$

Primzahlsatz (Gauß, Legendre)
$$\pi(x) \sim \frac{x}{\log x}, \text{ d.h. } \lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$$
$$\pi(x) \sim \int_2^x \frac{1}{\log t} dt =: \mathrm{li}(x)$$
$$\pi(x) > \frac{x}{\log x} \text{ für alle } x \geq 17$$
$$\pi(n) > \frac{n}{\log n} \text{ für alle } n \in \mathbb{N}, n \geq 11$$

Definition 1.5 (eindeutige Zerlegung)
Sei R ein kommutativer Ring mit $1 \neq 0$. Wir sagen, $a \in R \setminus \{0\}$ hat eine **eindeutige Zerlegung in unzerlegbare Faktoren**, wenn a eine Zerlegung
$$a = e p_1 p_2 \ldots p_r$$
in unzerlegbare Faktoren besitzt und eine solche im folgendem Sinne eindeutig ist: Ist auch
$$a = e' p_1' p_2' \ldots p_{r'}'$$
eine solche Zerlegung, so gilt $r = r'$ und nach Umnummerierung $p_i' \mathrel{\hat{=}} p_i$ für alle $1 \leq i \leq r$.

F1.4
In dem Integritätsring R besitze jedes Element $a \neq 0$ eine Zerlegung in unzerlegbare Faktoren. Dann sind äquivalent:

(i) Jedes $a \neq 0$ aus R hat eindeutige Zerlegung in unzerlegbare Faktoren.

(ii) Ist p unzerlegbar, so gilt: $p|ab \Rightarrow p|a$ oder $p|b$.

Definition 1.6 (Primelement)
Sei R ein kommutativer Ring mit $1 \neq 0$. Ein $p \in R \setminus R^\times$ heißt **Primelement** von R, wenn für alle $a, b \in R$ gilt:
$$p|ab \quad \Leftrightarrow \quad p|a \text{ oder } p|b \tag{1.2}$$

Bemerkung

1) 0 ist Primelement in $R \Leftrightarrow R$ ist Integritätsring

2) In einem Integritätsring R gilt: Jedes Primelement $p \neq 0$ ist unzerlegbar.

Lemma 1.1

Seien $a, b \in \mathbb{N}$. Sei $m = \mathrm{kgV}(a, b) \in \mathbb{N}$. Dann gilt:

$$a|c \text{ und } b|c \quad \Rightarrow \quad m|c$$

m ist also auch minimal bzgl. der Teilbarkeitsrelation $|$.

F1.5 (Satz von Euklid)

Jede Primzahl p ist ein Primelement von $\mathbb{Z}$, d.h. es gilt stets (1.2). (Das gleiche gilt für $-p$, also für jedes unzerlegbare Element von $\mathbb{Z}$.) 17.10.

Fundamentalsatz der elementaren Arithmetik

In $\mathbb{Z}$ hat jedes $a \neq 0$ eine eindeutige Zerlegung in unzerlegbare Faktoren.

Bemerkung

Eindeutige Zerlegung in unzerlegbare Faktoren hat man zum Beispiel auch für die Ringe $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[i], K[X]$ und K für K Körper, $\mathbb{Z}[X]$ und $\mathbb{C}\langle z\rangle$, nicht aber für $\mathbb{Z}[\sqrt{-5}]$:

$$3 \cdot 3 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

Dies sind zwei wesentlich verschiedene Zerlegungen in unzerlegbare Faktoren.

Definition 1.7 (Exponent)

Sei p eine Primzahl und $a \in \mathbb{Z} \setminus \{0\}$. Dann heißt

$$w_p(a) := \max\{k \in \mathbb{N}_0 : p^k | a\}$$

der **Exponent** von p in a. Wir setzen $w_p(0) := \infty$.

F1.6 (Eigenschaften der Exponentfunktion)

Die Funktion $w_p \colon \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ hat folgende Eigenschaften:

(i) $w_p(a + b) \geq \min(w_p(a), w_p(b))$ und Gleichheit, falls $w_p(a) \neq w_p(b)$.

(ii) $w_p(ab) = w_p(a) + w_p(b)$

Satz 1.2 (Fundamentalsatz der elementaren Arithmetik)

Für jedes $a \in \mathbb{Z} \setminus \{0\}$ gilt $w_p(a) > 0$ nur für endlich viele p. Es ist

$$a = \mathrm{sgn}(a) \cdot \prod_p p^{w_p(a)} \tag{1.3}$$

Bemerkung

1) w_p lässt sich eindeutig zu einer Abbildung $w_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ fortsetzen, sodass (ii) für alle $a, b \in \mathbb{Q}$ gilt. Es gilt dann auch (i). Für $a \in \mathbb{Q} \setminus \{0\}$ ist $w_p(a) \neq 0$ nur für endlich viele p, und die Formel (1.3) gilt entsprechend. Ferner gilt: $a \in \mathbb{Z} \Leftrightarrow w_p(a) \geq 0$ für alle p.

2) Sei

$$\mathbb{N}_0^{(\mathbb{P})} := \{(e_p)_{p\in\mathbb{P}} : e_p \in \mathbb{N}_0, e_p = 0 \text{ für fast alle } p\}.$$

Nach Satz 1.2 sind $(\mathbb{N}, \cdot)$ und $(\mathbb{N}_0^{(\mathbb{P})}, +)$ zwei zueinander isomorphe Halbgruppen. Nach Bemerkung 1) sind $\mathbb{Q}^\times$ und $\{1, -1\} \times \mathbb{Z}^{(\mathbb{P})}$ sogar zwei zueinander isomorphe Gruppen.

Definition 1.8 (faktorieller Ring, Vertretersystem für Primelemente)
Ein Integritätsring R heißt **faktoriell**, wenn jedes $a \in R \setminus \{0\}$ eine eindeutige Zerlegung in unzerlegbare Faktoren hat. Man spricht dann auch von eindeutiger Primfaktorzerlegung in R.
P heißt **Vertretersystem für die Primelemente** $\neq 0$ von R, wenn:

(1) Zu jedem Primelement $q \neq 0$ von R gibt es ein $p \in P$ mit $q \mathrel{\hat{=}} p$.

(2) Für $p, p' \in P$ mit $p \mathrel{\hat{=}} p'$ gilt $p = p'$, d.h. p in (1) ist eindeutig bestimmt durch q.

Für $R = \mathbb{Z}$ nehme man stets $P = \mathbb{P}$. Für K Körper und $R = K[X]$ nimmt man $P = \{p \in K[X] : p \text{ irreduzibel und normiert}\}$.

F1.7
Sei R faktoriell und P ein Vertretersystem für Primelemente. Es gibt zu jedem $p \in P$ eine Funktion $w_p \colon R \to \mathbb{N}_0 \cup \{\infty\}$ mit den Eigenschaften (i) und (ii) aus F1.6, sodass gilt:

a) Für jedes $a \in R \setminus \{0\}$ ist $w_p(a) > 0$ nur für endlich viele $p \in P$.

b) Für jedes $a \in R \setminus \{0\}$ gilt

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

mit eindeutigem $e \in \mathbb{R}^\times$.

Definition 1.9 (ggT und kgV)
Sei R ein kommutativer Ring mit $1 \neq 0$. Gegeben $a_1, \ldots, a_n \in R$.

a) Ein $d \in R$ heißt ein **größter gemeinsamer Teiler** (ggT) von $a_1, \ldots, a_n$, falls:

1. $d|a_i$ für alle i
2. $t|a_i$ für alle $i \Rightarrow t|d$

b) Ein $m \in R$ heißt ein **kleinstes gemeinsames Vielfaches** (kgV) von $a_1, \ldots, a_n$, falls:

1. $a_i|m$ für alle i
2. $a_i|c$ für alle $i \Rightarrow m|c$

Bemerkung

1) d, d' ggT von $a_1, \ldots, a_n \Rightarrow d \mathrel{\hat{=}} d'$ und m, m' kgV von $a_1, \ldots, a_n \Rightarrow m \mathrel{\hat{=}} m'$

2) Im Allgemeinen ist die Existenz eines ggT und kgV nicht gesichert. In faktoriellen Ringen existieren sie aber immer, siehe dazu folgende Feststellung.

F1.8
21.10. Sei R faktoriell, P wie oben. Es gelten:

(i) $a|b \quad \Leftrightarrow \quad w_p(a) \leq w_p(b)$ für alle $p \in P$.

(ii) Für $a_1, \ldots, a_n \in R$ setze:

$$d := \prod_{p \in P} p^{\min(w_p(a_1), \ldots, w_p(a_n))} =: (a_1, \ldots, a_n)$$

$$m := \prod_{p \in P} p^{\max(w_p(a_1), \ldots, w_p(a_n))} =: [a_1, \ldots, a_n]$$

Hierbei setze $p^\infty = 0$. Dann ist d ein ggT von $a_1, \ldots, a_n$ und m ein kgV von $a_1, \ldots, a_n$.

(iii) $a, b \in R$. Dann ist $a, b \hat{=} [a, b] \cdot (a, b)$ und $m \hat{=} \frac{ab}{(a,b)}$, wenn a, b nicht beide 0.

(iv) $a_1, \ldots, a_n$ paarweise teilerfremd, d.h. $(a_i, a_j) = 1$ für $i \neq j \Leftrightarrow [a_1, \ldots, a_n] \simeq a_1 a_2 \ldots a_n$.

(v) $(a_i, b) = 1$ für $1 \leq i \leq n \Rightarrow (a_1 a_2 \ldots a_n, b) = 1$

(vi) $(a_1 f, \ldots, a_n f) \simeq (a_1, \ldots, a_n) f, [a_1 f, \ldots, a_n f] \simeq [a_1, \ldots, a_n] f$

(vii) $((a_1, \ldots, a_n), a_{n+1}) = (a_1, \ldots, a_n, a_{n+1}), [[a_1, \ldots, a_n], a_{n+1}] = [a_1, \ldots, a_n, a_{n+1}]$

Bemerkung (Verallgemeinerung von (iii))
Seien $a_1, \ldots, a_n \in R$ gegeben. Wähle $q_1, \ldots, q_n$ und c aus R mit

$$a_1 q_1 = a_2 q_2 = \ldots = a_n q_n = c$$

(z.B. $c = a_1 a_2 \ldots a_n, q_i = \prod_{j \neq i} a_j$). Dann gilt

$$c \hat{=} (a_1, \ldots, a_n)[q_1, \ldots, q_n]$$

F1.9
Sei $n \in \mathbb{N}, a \in \mathbb{Z}$. Ist $X^n = a$ lösbar in $\mathbb{Q}$, so ist $X^n = a$ auch lösbar in $\mathbb{Z}$. Anders ausgedrückt: Ist $a \in \mathbb{Z}$ keine n-te Potenz in $\mathbb{Z}$, so ist a auch keine n-te Potenz in $\mathbb{Q}$.

Anwendung
$\sqrt{2}$ ist irrational, denn 2 ist kein Quadrat in $\mathbb{Z}$ aus Größengründen, also ist 2 nach F1.9 auch kein Quadrat in $\mathbb{Q}$, d.h. $\sqrt{2} \in \mathbb{Q}$.

Korollar
Sei $n \in \mathbb{N}, a \in \mathbb{N}$. Dann sind äquivalent:

(i) a ist n-te Potenz in $\mathbb{Z}$.

(ii) $n | w_p(a)$ für alle p.

(iii) a ist n-te Potenz in $\mathbb{Q}$.

F1.10 (Verallgemeinerung von F1.9)
Gegeben sei ein normiertes Polynom $f(X) \in \mathbb{Z}[X]$. Ist dann b eine Nullstelle von f mit $b \in \mathbb{Q}$, so ist notwendigerweise $b \in \mathbb{Z}$ und außerdem ist b ein Teiler des Absolutkoeffizienten a_0 von f.

2 Der euklidische Algorithmus

Sei R kommutativer Ring mit $1 \neq 0$. Für beliebiges $a \in R$ betrachte man die Menge der Vielfachen von $a \in R$, also

$$Ra := xa : x \in R = b \in R : a|b$$

Die Teilmenge $I = Ra$ hat folgende Eigenschaften:

(i) $0 \in I$

(ii) $b_1, b_2 \in I \Rightarrow b_1 + b_2 \in I$

(iii) $c \in R, b \in I \Rightarrow cb \in I$

Definition 2.1 (Ideal, Hauptideal)
Eine Teilmenge I von R heißt ein **Ideal** in R, falls die Eigenschaften (i), (ii), (iii) erfüllt sind. I heißt **Hauptideal**, wenn es ein $a \in R$ gibt mit $I = Ra$. Wir verwenden die Bezeichnung

$$(a) := Ra$$

und nennen (a) das von $a \in R$ erzeugte Hauptideal.

Bemerkung

(1) $(b) \subseteq (a) \Leftrightarrow a|b$

(2) $a \hat{=} b \Leftrightarrow (a) = (b)$

(3) c ist gemeinsames Vielfaches von $a_1, \ldots, a_n \Leftrightarrow (c) \subseteq (a_1) \cap \ldots \cap (a_n)$

(4) m ist ein kgV von $a_1, \ldots, a_n \Leftrightarrow (a_1) \cap \ldots \cap (a_n) = (m)$

(5) d ist ein gemeinsamer Teiler von $a_1, \ldots, a_n \Leftrightarrow (a_i) \subseteq (d)$ für $1 \leq i \leq n$

(6) d ist ein gemeinsamer Teiler von $a_1, \ldots, a_n \Leftrightarrow Ra_1 + Ra_2 + \ldots + Ra_n \subseteq (d)$

(7) d ist ein ggT von $a_1, \ldots, a_n \Leftrightarrow (d)$ ist das kleinste Hauptideal mit $Ra_1 + \ldots Ra_n \subseteq (d)$.

Ein ggT lässt sich also idealtheoretisch nicht so einfach charakterisieren wie oben ein kgV durch (4). Am schönsten wäre es, wenn $Ra_1 + \ldots + Ra_n$ ein Hauptideal wäre, dann würde (7) übergehen in:

$$d \text{ ist ein ggT von } a_1, \ldots, a_n \Leftrightarrow Ra_1 + Ra_2 + \ldots + Ra_n = (d)$$

Definition 2.2 (Hauptidealring)
Ein Integritätsring R heißt ein **Hauptidealring**, wenn jedes Ideal I von R ein Hauptideal ist.

Bezeichnung
Für Elemente $a_1, \ldots, a_n$ in einem beliebigen kommutativen Ring R mit $1 \neq 0$ setze

$$(a_1, \ldots, a_n) := Ra_1 + \ldots + Ra_n$$

Man nennt $(a_1, \ldots, a_n)$ das von $a_1, \ldots, a_n$ erzeugte Ideal in R.

F2.1 (Satz vom größten gemeinsamen Teiler)
Sei R ein Hauptidealring. Dann gilt: Zu jedem System $a_1, \ldots, a_n$ von Elementen aus R existiert ein ggT d von $a_1, \ldots, a_n$ und jedes solche d besitzt eine Darstellung der Gestalt 24.10.

$$d = x_1 a_1 + \ldots + x_n a_n \quad \text{mit } x_i \in R \tag{2.1}$$

Wir sagen, in R gelte der **Satz vom größten gemeinsamen Teiler**.

Bemerkung
Sei R ein beliebiger Integritätsring. Ist d ein gemeinsamer Teiler von $a_1, \ldots, a_n$ aus R und gibt es eine Darstellung der Form (2.1), so ist d ein ggT von $a_1, \ldots, a_n$.

Satz 2.1
$\mathbb{Z}$ ist ein Hauptidealring.

Definition (Gaußklammer)
Für $x \in \mathbb{R}$ setze

$$[x] = \max\{g \in \mathbb{Z} : g \leq x\} \in \mathbb{Z}$$

$[x]$ ist charakterisiert durch folgende zwei Eigenschaften:

(1) $[x] \in \mathbb{Z}$

(2) $[x] \leq x < [x] + 1$

F2.2 (Division mit Rest in $\mathbb{Z}$)
Gegeben $a, b \in \mathbb{Z}$, $a \neq 0$. Dann gibt es eine Darstellung

$$b = qa + r \quad \text{mit } 0 \leq r < |a| \text{ und } q, r \in \mathbb{Z} \tag{2.2}$$

Bemerkung

1) Die Darstellung (2.2) ist eindeutig.

2) Es gibt eine Darstellung
$$b = qa + r \quad \text{mit } |r| < |a|; q, r \in \mathbb{Z},$$
doch diese ist nicht mehr eindeutig, z.B. $27 = 4 \cdot 6 + 3 = 5 \cdot 6 - 3$.

3) Es gibt eine Darstellung
$$b = qa + r \quad \text{mit } -\frac{|a|}{2} < r \leq \frac{|a|}{2}; q, r \in \mathbb{Z},$$
und diese ist eindeutig.

4) Es gibt eine Darstellung
$$b = qa + r \quad \text{mit } |r| \leq \frac{|a|}{2}; q, r \in \mathbb{Z},$$
doch diese ist nicht eindeutig, falls a gerade.

Definition 2.3 (euklidischer Ring)
Ein Integritätsring R heißt ein **euklidischer Ring**, falls eine Funktion $\nu\colon R \to \mathbb{N}_0$ mit $\nu(0) = 0$ existiert, sodass gilt: Zu $a, b \in R$ mit $a \neq 0$ existieren $q, r \in R$ mit

$$b = qa + r \text{ und } \nu(r) = \nu(a)$$

Beispiele

(1) $R = \mathbb{Z}$ mit $\nu(a) = |a|$.

(2) $R = K[X], K$ Körper, mit $\nu(g) = \deg(g) + 1$ für $g \neq 0$, $\nu(0) = 0$.

(3) $R = \mathbb{Z}[i]$ mit $\nu(z) = N(z) = z\overline{z} = |z|^2$.

F2.3

Jeder euklidische Ring ist ein Hauptidealring.

F2.4

Jeder Hauptidealring ist faktoriell.

Im Folgenden sei R ein euklidischer Ring mit euklidischer Normfunktion ν. Allgemein gilt folgende elementare Umformung:

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2 - y_2 a_1, \ldots, a_n - y_n a_1) \text{ für bel. } y_i \in R \tag{2.3}$$

Euklidischer Algorithmus

Gegeben $a_1, \ldots, a_n \in R$. Wir wollen $d \in R$ bestimmen mit

$$(a_1, \ldots, a_n) = (d)$$

Sind alle $a_i = 0$, so ist $d = 0$ und wir sind fertig. Sei daher ohne Einschränkung

$$a_1 \neq 0 \text{ und } \nu(a_1) \leq \nu(a_i), \text{ falls } a_i \neq 0$$

Sei $a_i = q_i a_1 + r_i$ mit $\nu(r_i) < \nu(a_1)$ für $i \geq 2$. Dann ist

$$(a_1, \ldots, a_n) \overset{(2.3)}{=} (a_1, r_2, \ldots, r_n)$$

Fortsetzung des Verfahrens liefert

$$(d, 0, 0, \ldots, 0) = (d)$$

Beispiel

$$\begin{aligned} (27, 63, 114) \quad & 63 = 2 \cdot 27 + 9, 114 = 4 \cdot 27 + 6 \\ = (27, 9, 6) \quad & 27 = 4 \cdot 6 + 3, 9 = 1 \cdot 6 + 3 \\ = (3, 3, 6) \quad & 3 = 1 \cdot 3 + 0, 6 = 2 \cdot 3 + 0 \\ = (3, 0, 0) = (3) & \end{aligned}$$

Beispiel im Fall $n = 2$

28.10. Sei $a, b \in R \setminus \{0\}$.

$$\begin{aligned} b &= q_0 a + r_1 && \nu(r_1) < \nu(a) && \text{Falls } r_1 = 0, \text{ dann Schluss. Sonst weiter:} \\ a &= q_1 r_1 + r_2 && \nu(r_2) < \nu(r_1) \\ r_1 &= q_2 r_2 + r_3 && \nu(r_3) < \nu(r_2) \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n && \nu(r_n) < \nu(r_{n-1}) \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

Also:

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

F2.5

r_n ist ein größter gemeinsamer Teiler von a und b. Es ist

$$r_n = xa + yb \text{ mit } x, y \in R,$$

wobei x und y aus obiger Rechnung rekursiv bestimmbar sind.

Bemerkung

1) Von neuem erhalten wir für jeden euklidischen Ring also den Satz vom größten gemeinsamen Teiler. (Satz 2.1)

2) Sei $R = \mathbb{Z}$. Verlangen wir $0 \leq r_i$ in obiger Rechnung, so sind $q_0, q_1, \ldots, q_n$ sowie die $r_1, \ldots, r_n$ eindeutig bestimmt.

Beispiel

Sei $a = 84, b = 133$.

$$\begin{aligned}
133 &= 1 \cdot 84 + 49 \\
84 &= 1 \cdot 49 + 35 \\
49 &= 1 \cdot 35 + 14 \\
35 &= 2 \cdot 14 + 7 \\
14 &= 2 \cdot 7 \qquad \Rightarrow n = 4, r_4 = 7
\end{aligned}$$

Also ist $(133, 84) = (7)$.

Wir können den euklidischen Algorithmus für a, b auch wie folgt aufschreiben:

$$\begin{array}{ll}
\frac{b}{a} = q_0 + \frac{r_1}{a} & q_0 = \left[\frac{b}{a}\right] \quad 0 < \frac{r_1}{a} < 1, \text{ falls } r_1 \neq 0 \\
\frac{a}{r_1} = q_1 + \frac{r_2}{r_1} & q_1 = \left[\frac{a}{r_1}\right] \\
\frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2} & \\
\quad \vdots & \\
\frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}} & \\
\frac{r_{n-1}}{r_n} = q_n &
\end{array}$$

Zusammengefasst erhalten wir die **Kettenbruchentwicklung** von $\frac{b}{a}$:

$$\frac{b}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

Statt einer rationalen Zahl sei jetzt α allgemeiner eine beliebige reelle Zahl.

Es ist $\alpha = [\alpha] + \varepsilon$ mit $0 \leq \varepsilon < 1$. Falls $\alpha \notin \mathbb{Z}$, d.h. $\varepsilon > 0$, setze $q_0 := [\alpha]$ und $\rho_1 := \frac{1}{\varepsilon}$. Dann:

$$\begin{array}{lll}
\alpha = q_0 + \frac{1}{\rho_1} & \text{mit } \rho_1 > 1. & \text{Falls } \rho_1 \notin \mathbb{Z}, \text{ so setze } [\rho_1] =: q_1 \\
\rho_1 = q_1 + \frac{1}{\rho_2} & \text{mit } \rho_2 > 1. & \text{usw.} \\
\quad \vdots & & \\
\rho_k = q_k + \frac{1}{\rho_{k+1}} & \text{mit } \rho_{k+1} > 1. &
\end{array}$$

Abbrechen, wenn $\rho_{n+1} \in \mathbb{Z}$, sonst weiter. Jedenfalls:

$$\alpha = \frac{b}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_k + \cfrac{1}{\rho_{k+1}}}}}$$

Definition 2.4 (Kettenbruch, k-ter Rest)

1) $q_0, q_1, \ldots, q_n$ seien reelle Zahlen mit $q_1, \ldots, q_n > 0$. Unter dem **endlichen Kettenbruch**

$$[q_0, q_1, \ldots, q_n] \tag{2.4}$$

mit den Teilquotienten q_i verstehen wir sowohl das $(n+1)$-Tupel $(q_0, q_1, \ldots, q_n)$, als auch seinen wie folgt definierten Wert:

$$[q_0, q_1, \ldots, q_n] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}} \tag{2.5}$$

Für $0 \leq k \leq n$ nennen wir den Kettenbruch

$$\rho_k := [q_k, q_{k+1}, \ldots, q_n] \tag{2.6}$$

den k**-ten Rest** des Kettenbruchs (2.4). Für den Wert (2.4) des Kettenbruchs (2.4) gilt:

$$[q_0, q_1, \ldots, q_n] = [q_0, q_1, \ldots, q_{k-1}, \rho_k] \text{ für } 0 \leq k \leq n \tag{2.7}$$

Man kann den Wert (2.5) des Kettenbruchs (2.4) durch (2.7) mit (2.6) rekursiv definieren: Es ist $[q_0] = q_0, [q_0, q_1] = q_0 + \frac{1}{q_1}$, also:

$$[q_0, q_1, \ldots, q_n] = [q_0, \rho_1] = q_0 + \frac{1}{\rho_1} \text{ für } n \geq 1$$

2) Gegeben sei eine Folge $(q_k)_{k \geq 0}$ in $\mathbb{R}$ mit $q_k > 0$ für $k \geq 1$. Unter dem **unendlichen Kettenbruch**

$$[q_0, q_1, q_2, \ldots] \tag{2.8}$$

verstehen wir die Folge der

$$[q_0, q_1, \ldots, q_n] \qquad n = 0, 1, 2, \ldots$$

Falls diese Folge in $\mathbb{R}$ konvergiert, so bezeichnen wir auch deren Limes mit $[q_0, q_1, q_2, \ldots]$. Der unendliche Kettenbruch

$$\rho_k := [q_k, q_{k+1}, \ldots] \qquad k = 0, 1, 2, \ldots \tag{2.9}$$

heißt der k**-te Rest** von (2.8). Formal gilt:

$$[q_0, q_1, q_2, \ldots] = [q_0, q_1, \ldots, q_{k-1}, \rho_k] \tag{2.10}$$

Später werden wir sehen, dass (2.10) auch für die Werte der entsprechenden Kettenbrüche gilt, wenn (2.9) konvergiert.

Definition 2.5 (Näherungsbruch)
Jedem endlichen Kettenbruch $[q_0, q_1, \ldots, q_k]$ ordnen wir rekursiv ein Paar $\binom{c}{d} \in \mathbb{R} \times \mathbb{R}_{>0}$ reeller Zahlen zu mit

$$[q_0, q_1, \ldots, q_k] = \frac{c}{d} \tag{2.11}$$

$k = 0$: Für $[q_0]$ sei $\binom{c}{d} = \binom{q_0}{1}$. Es gilt dann in der Tat $[q_0] = q_0 = \frac{q_0}{1}$.
$k \geq 1$: Zuerst Motivation (Heuristik):

$$[q_0, q_1, \ldots, q_k] = [q_0, \rho_1] = q_0 + \frac{1}{\rho_1}$$

mit $\rho_1 = [q_1, q_2, \ldots, q_k]$. Gehöre $\binom{c'}{d'}$ zu ρ_1. Dann gilt

$$[q_0, q_1, \ldots, q_k] = q_0 + \frac{d'}{c'} = \frac{q_0 c' + d'}{c'}$$

Wir ordnen nun also $[q_0, q_1, \ldots, q_k]$ das Tupel

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} q_0 c' + d' \\ c' \end{pmatrix} = \underbrace{\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}}_{=:M_1} \begin{pmatrix} c' \\ d' \end{pmatrix}$$

zu. Dann gilt (2.11). Sei jetzt

$$[q_0, q_1, \ldots] \tag{2.12}$$

ein endlicher oder unendlicher Kettenbruch. Das dem k-ten Abschnitt

$$[q_0, q_1, \ldots, q_k] \tag{2.13}$$

von (2.12) zugeordnete 2-Tupel

$$\begin{pmatrix} c_k \\ d_k \end{pmatrix}$$

heißt der **k-te Näherungsbruch** von (2.12). Auch $\frac{c_k}{d_k}$ heißt k-ter Näherungsbruch von (2.12). Ist (2.12) der endliche Kettenbruch $[q_0, q_1, \ldots, q_n]$, so ist der n-te Näherungsbruch $\frac{c_n}{d_n}$ gleich dem Wert dieses Kettenbruchs. Allgemein ist $\frac{c_k}{d_k}$ der Wert des Kettenbruchs (2.13). Aus formalen Gründen definieren wir noch

$$\begin{pmatrix} c_{-1} \\ d_{-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} c_{-2} \\ d_{-2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

F2.6 (Rekursionsformeln für Näherungsbrüche)
Mit den Bezeichnungen wie oben gilt:

$$c_k = q_k c_{k-1} + c_{k-1} d_k \quad = q_k d_{k-1} + d_{k-2} \tag{2.14}$$

Dies schreiben wir auch in Matrizenform:

$$\begin{pmatrix} c_k \\ d_k \end{pmatrix} = \underbrace{\begin{pmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{pmatrix}}_{=:M_k} \begin{pmatrix} q_k \\ 1 \end{pmatrix}$$

Bemerkung
$d_k > 0$ für $k \geq 0$ (vgl. Definition 2.5, oder auch (2.14)).

Index

k-ter Rest, 14

assoziiert, 4

Einheit, 4
Einheitengruppe, 4
Euklidischer Algorithmus, 12
euklidischer Ring, 11
Exponent, 7

faktoriell, 8
Fundamentalsatz der elementaren Arithmetik, 7

größter gemeinsamer Teiler, 8

Hauptideal, 10
Hauptidealring, 10

Ideal, 10
Integritätsring, 4
irreduzibel, 5

Kettenbruch, 14
Kettenbruchentwicklung, 13
kleinstes gemeinsames Vielfaches, 8

Nullteiler, 4

Primelement, 6, 8
Primzahl, 5

Satz vom größten gemeinsamen Teiler, 11
Satz von Euklid, 7

Teilbarkeitsbedingung für Hauptideale, 6
Teiler, 4

unzerlegbar, 5

Vertretersystem, 8

Zerlegung in unzerlegbare Faktoren, 5, 6

Liste der Sätze und Definitionen

Definition 1.1	Teilbarkeit	4
F1.1	Triviale Teilbarkeitsregeln	4
Definition 1.2	Einheit, assoziiert	4
Definition 1.3	unzerlegbar, irreduzibel, zusammengesetzt	5
Definition 1.3	Primzahl	5
Definition 1.4	Zerlegung in unzerlegbare Faktoren	5
Satz 1.1	Existenz unendlich vieler Primzahlen	6
Definition 1.5	eindeutige Zerlegung	6
Definition 1.6	Primelement	6
F1.5	Satz von Euklid	7
Definition 1.7	Exponent	7
F1.6	Eigenschaften der Exponentfunktion	7
Satz 1.2	Fundamentalsatz der elementaren Arithmetik	7
Definition 1.8	faktorieller Ring, Vertretersystem für Primelemente	8
Definition 1.9	ggT und kgV	8
F1.10	Verallgemeinerung von F1.9	9
Definition 2.1	Ideal, Hauptideal	10
Definition 2.2	Hauptidealring	10
F2.1	Satz vom größten gemeinsamen Teiler	11
F2.2	Division mit Rest in $\mathbb{Z}$	11
Definition 2.3	euklidischer Ring	11
Definition 2.4	Kettenbruch, k-ter Rest	14
Definition 2.5	Näherungsbruch	15
F2.6	Rekursionsformeln für Näherungsbrüche	15