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/e1ZTWiSe14/

Stand: 18. 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

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
- $\mathbb{C}\langle z\rangle := \{$konvergente Potenzreihen $\sum_{n=0}^{\infty} a_n z^n\}$
- Nicht nullteilerfrei ist z.B. $\mathcal{C}[0,1] := \{f \colon [0,1] \to \mathbb{R}$ 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 $R^\times := \{x \in R : x$ 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 $K^\times = K \setminus \{0\}$. $\quad \mathbb{Z}^\times = \{1, -1\}, \quad K[X]^\times = K^\times,$
$\mathcal{C}[0,1]^\times = \{f \in \mathcal{C}[0,1] : f(x) \neq 0$ 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 $\quad \Leftrightarrow \quad$ jeder Teiler von a ist Einheit oder assoziiert zu a
a zerlegbar $\quad \Leftrightarrow \quad a$ 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 beziechnen 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 $\mathbb{Z}$.)

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.

Index

Liste der Sätze und Definitionen