Elementare Zahlentheorie

WS 14/15

Gegenstand der Zahlentheorie : $\mathbb{N} = \{1, 2, 3, \dots\}$.

Methode : Die halbe Mathematik (mindestens)

In dieser Vorlesung weniger als 1%.

§1 Fundamentalsatz der elementaren Arithmetik [1]

Terminologie[2]: Sei R ein kommutativer Ring mit $1 \neq 0$. Ein solcher heißt Integritätsring (bzw. nullteilerfrei), wenn:

$$ab = 0 \implies a = 0 \text{ oder } b = 0.$$

Beispiele: ① $\mathbb{Z}$, aber auch

② $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$

$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ $\quad i = \sqrt{-1}$

③ $\mathbb{Z}[\sqrt{-5}] = \dots$, etc.

④ $K[X]$, K Körper (Polynomring über K)

⑤ $\mathbb{Z}[X]$ (Polynomring über $\mathbb{Z}$)

⑥ K Körper

---

1) vgl. Stoff der 5. Klasse

2) Wiederholung aus Anfängervorlesungen, vgl. z.B. LA II, S. 143ff

⑦ $\mathcal{C}[0,1] := \{ f : [0,1] \to \mathbb{R} \text{ stetig} \}$, ist nicht nullteilerfrei

⑧ $\mathbb{C}\langle z\rangle := \{ \text{konv. Potenzreihen } \sum_{n=0}^{\infty} a_n z^n \}$, ist nullteilerfrei

Def. 1: $a, b \in R$

a teilt b : $\exists q \in R: \; b = qa \quad (*)$

(a Teiler von b, b teilbar durch a, ...)

in Zeichen: $\quad a \mid b \qquad$ Negation: $a \nmid b$

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

F1 (triviale Teilbarkeitsregeln):

(i) $a \mid 0, \quad 1 \mid a, \quad a \mid a$

(ii) $a \mid b,\ b \mid c \Rightarrow a \mid c$

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

(iv) $a_1 \mid b_1,\ a_2 \mid b_2 \Rightarrow a_1 a_2 \mid b_1 b_2$

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

Def. 2: (i) $e \in R$ heißt eine Einheit in R, falls gilt

$$e \mid 1$$

[d.h. $\exists f \in R$ mit $ef = 1$; f eind. bestimmt, setze $e^{-1} := f$. schreibe auch $e^{-1} = \frac{1}{e}$]

$R^\times := \{ \text{Einheiten von } R \}$

(ii) a assoziiert zu b, in Zeichen $a \triangleq b$, falls: $a \mid b$ und $b \mid a$.

Bem'n: 1) K Körper, dann $K^\times = K \setminus \{0\}$, $\quad \mathbb{Z}^\times = \{1, -1\}$

$K[X]^\times = K^\times, \quad \mathcal{C}[0,1]^\times = \{ f \in \mathcal{C}[0,1] \mid f(x) \neq 0 \text{ für alle } x \in [0,1] \}$

$\mathbb{Z}[\sqrt{2}]^\times \neq \{1,-1\}$, denn z.B. $(\sqrt{2}+1)(\sqrt{2}-1) = 1$,
übrigens $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^k \mid k\in\mathbb{Z}\}$ (beim Nachdenken, vgl. 1. Übungsstunde)

$\mathbb{Z}[X]^\times = \{1,-1\}$

$\mathbb{C}\langle z\rangle^\times = \{\sum a_n z^n \in \mathbb{C}\langle z\rangle \mid a_0 \neq 0\}$

2) $e \in R^\times \iff e \mid a$ für jedes $a \in R$

<u>FZ:</u> $a,b\in R$, $b\neq 0$, R Integritätsring. Dann:

$$a \triangleq b \iff \exists e\in R^\times \text{ mit } b = ea$$

<u>Bew.</u> $\Leftarrow$: $a\mid b$, $e^{-1}b = a$, $b \mid a$.

$\Rightarrow$: $\left.\begin{matrix} a\mid b \\ b\mid a\end{matrix}\right\} \Rightarrow \exists e,f:\ \begin{matrix} b = ea \\ a = fb\end{matrix}$, $\Rightarrow b = efb \underset{\text{Nullteilerfrei}}{\overset{b\neq 0}{\Longrightarrow}} ef = 1$.

<u>Ab jetzt (wenn nichts anderes gesagt):</u> <u>R Integritätsring</u>.

<u>Def. 3</u>: $a\in R$, $a\notin R^\times$. a heißt dann <u>unzerlegbar</u>* (in R), wenn gilt: $a = bc$ in $R \Longrightarrow b\in R^\times$ oder $c \in R^\times$

*oder auch: <u>irreduzibel</u>

Andernfalls heißt a <u>zerlegbar</u> (oder <u>zusammengesetzt</u>).

<u>Bem.</u> a unzerlegbar $\iff$ jeder Teiler von a ist Einheit oder assoz. zu a.
a zerlegbar $\iff$ a hat echten Teiler (d.h. einen Teiler, der weder eine Einheit ist noch assoz. zu a)

<u>Def. 3'</u>: Ein $p\in\mathbb{Z}$ heißt <u>Primzahl</u>, wenn p unzerlegbar (in $\mathbb{Z}$) und $p\in\mathbb{N}$.

$\mathbb{P}$ Menge der Primzahlen von $\mathbb{Z}$

$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$

a unzerlegbar in $\mathbb{Z}$ $\iff$ $a = p$ oder $a = -p$ mit $p \in \mathbb{P}$

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

__Bew.__ a besitzt jedenfalls echten Teiler b, o.E. $b \in \mathbb{N}$ (sonst $-b \in \mathbb{N}$)
Sei p die kleinste natürliche Zahl > 1, die a teilt.
p ist Primzahl! Ferner: $a = cp$

$$|a| = |c|\,|p| \geq p \cdot p = p^2, \Rightarrow p \leq \sqrt{|a|}.$$

__Def. 4__: Wir sagen, $a \in R$ besitze (in R) eine Zerlegung in unzerlegbare Faktoren, wenn

(*) $\quad a = e p_1 p_2 \cdots p_r$ mit $e \in R^\times$ und $p_1, \dots, p_r$ unzerlegbar.

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

__F3:__ In $\mathbb{Z}$ besitzt jedes $a \neq 0$ eine Zerlegung in unzerlegbare Faktoren.

__Bew.__ o.E. $a \in \mathbb{N}$. o.E. a keine Primzahl, $a \neq 1$.
Nach obiger Bem. gibt es $p \in \mathbb{P}$ und $c \in \mathbb{N}$ mit

(×) $\quad a = p \cdot c$

Es folgt $1 \leq c < a$, $c \in \mathbb{N}$. Per Induktion besitzt c eine Zerlegung in unzerlegbare Faktoren. Wegen (×) dann auch a.

__F3':__ Jede natürliche Zahl $a > 1$ besitzt Zerlegung

$$a = p_1 p_2 \cdots p_r$$

mit Primzahlen $p_1, \dots, p_r$ und $r \geq 1$.

__Bem'n:__ 1) Die Aussage von F3 gilt auch für die Beispiele ④–⑥, sowie ②.

2) Sei R ein Integritätsring, der die "Teilerkettenbedingung für Hauptideale" erfüllt, so besitzt jedes $a \neq 0$ aus R eine Zerlegung in unzerlegbare Faktoren. [vgl. LA II, S. 140]

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

4) Im Bsp. ⑧ gibt es (bis auf Assoziiertheit) nur das einzige unzerlegbare Elt z (und dieses ist ein Primelement; zu diesem Begriff siehe w.u.)

<u>Satz 1:</u> Es gibt unendlich viele Primzahlen.

<u>Beweis</u> (Euklid, ca. −300): Seien $p_1, p_2, \dots, p_n$ Primzahlen ($n \geq 1$).

z.B. $p_1 = 2$

<u>z.z.</u>: Es gibt ein $p \in \mathbb{P}$ mit $p \neq p_1, \dots, p_n$. Setze:

$$a := p_1 p_2 \cdots p_n + 1 \qquad a \in \mathbb{N},\ a > 1$$

Nach F3' gibt es ein $p \in \mathbb{P}$ mit $p \mid a$.

<u>Ann.</u> $p = p_i$. Dann $p \mid p_1 \cdots p_n$, $p \mid a \implies$

$$p \mid \underbrace{a - p_1 \cdots p_n}_{=1}, \implies p \mid 1 \quad W!$$

<u>Bem.:</u> Es sei $p_1, p_2, \dots$ die Folge der Primzahlen mit $p_1 < p_2 < \dots$

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \dots$$

1) $a_n = p_1 p_2 \cdots p_n + 1$ ist Primzahl für $n \leq 5$, aber nicht allgemein:

$2+1=3 \quad 2\cdot3+1=7 \quad 2\cdot3\cdot5+1=31 \quad 2\cdot3\cdot5\cdot7+1=211$

$2\cdot3\cdot5\cdot7\cdot11+1 = 2311$ Primzahl!

$2\cdot3\cdot5\cdot7\cdot11\cdot13+1 = 30031 = 59\cdot509$ keine Primzahl!

Ist a_n für unendlich viele n eine Primzahl?
Ist a_n für unendlich viele n keine Primzahl?

Antworten (mir) nicht bekannt.

2) $x \in \mathbb{R}_{>0}$ $\qquad \pi(x) :=$ Anzahl der Primzahlen $\le x$

$$\pi(x) = \sum_{p \le x} 1$$

$\pi(10) = 4, \quad \pi(100) = 25, \quad \pi(1000) = 168$

<u>Beh.</u> $\quad p_n \le 2^{2^{n-1}} \qquad n=1: \quad 2 \le 2^{2^0} = 2^1$

$$p_{n+1} \overset{\text{Euklid}}{\le} p_1 \cdots p_n + 1 \overset{\text{Ind.}}{\le} 2^{1+2^1+2^2+\dots+2^{n-1}} + 1 = 2^{2^n-1} + 1 \le 2^{2^n}. \checkmark$$

Also $\quad \pi(2^{2^{n-1}}) \ge n, \quad \overset{\text{ÜA}}{\Longrightarrow}$

(*) $\quad \pi(x) \ge \frac{1}{\log 2} \log(\log x)$ für $x \ge 2$. Liefert

$\pi(10) \ge 2, \quad \pi(100) \ge 3, \quad \pi(10^6) \ge 4$

miserable Abschätzung.

*) Notiz 1796 in seiner Logarithmentafel (Gauß: 30.4.1777)

<u>Primzahlsatz</u> (Gauß*), Legendre; 1. Bew. von Hadamard und de la Vallée-Poussin 1896)

(1) $\qquad \pi(x) \sim \frac{x}{\log x}$,

d.h. $\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1. \qquad$ Daher [ÜA]

$$p_n \sim n \log n, \quad \text{d.h.} \quad \frac{p_n}{n \log n} \to 1 \text{ für } n \to \infty.$$

Setze $f(x) = \frac{x}{\log x}$

$f(10) = 4{,}34\ldots$	$\pi(10) = 4$
$f(100) = 21{,}71\ldots$	$\pi(100) = 25$
$f(1000) = 144{,}76\ldots$	$\pi(1000) = 168$

$f(10^6) = 72.382,\ldots \qquad \pi(10^6) = 78.498$

$\frac{\pi(100)}{f(100)} = 1{,}151\ldots \qquad \frac{\pi(1000)}{f(1000)} = 1{,}160\ldots$

$\frac{\pi(10^6)}{f(10^6)} = 1{,}084\ldots \qquad \frac{\pi(10^9)}{f(10^9)} = 1{,}053\ldots$

Heuristik: Nach (1) ist Primzahldichte $\frac{\pi(x)}{x} \sim \frac{1}{\log x}$.

Daher vermutet Gauß

$$(2) \qquad \pi(x) \sim \int_2^x \frac{1}{\log t}\,dt =: li(x) \quad \text{[Integrallogarithmus]}^{*)}$$

ÜA: Zeige die Äquivalenz von (1) und (2). (Hinweis: Regel von L'Hospital). Aber:

(2) gibt für große x bessere Approximation! z.B.

$\frac{\pi(10^6)}{li(10^6)} = 0{,}9983\ldots \qquad \frac{\pi(10^9)}{li(10^9)} = 0{,}9996\ldots$

Gauß vermutet auch: $li(x) > \pi(x)$.

Dies ist richtig für $x \leq 10.000.000$, sogar 10^{16}, aber nicht allgemein (Littlewood 1912, rein theoretisch, ohne jede Angabe einer Schranke).

1933: $\exists x > 10^{10^{10^{34}}}$ mit $li(x) < \pi(x)$.

---

uneigentlich in $t=1$ (in $t=0$ o.k.)

*) Gauß, Bessel u.a. betrachten $Li(x) = \int_0^x \frac{1}{\log t}\,dt$, obwohl dieses uneigentliche Integral gar nicht konvergent ist; man nehme den sogenannten Hauptwert. Wie dem auch sei, es ist

$Li(x) = li(x) + c$ mit $c = 1{,}04\ldots$, also macht es wenig aus, ob man $Li(x)$ oder $li(x)$ betrachtet.

Nach Littlewood wechselt

$$li(x) - \pi(x)$$

sogar unendlich oft das Vorzeichen.

Hingegen kann man (mit Methoden, die noch über den Beweis des Primzahlsatzes (1) hinausgehen) zeigen, daß

$$(3) \qquad \pi(x) > \frac{x}{\log x} \quad \text{für alle } x \geq 17$$

gilt. Was anscheinend weithin unbekannt ist, teste etwa das internet.

Für natürliche Zahlen $x = n \in \mathbb{N}$ gilt sogar

$$(4) \qquad \pi(n) > \frac{n}{\log n} \quad \text{für alle } n \geq 11$$

<u>Def. 5</u> R komm. Ring mit $1 \neq 0$.
Wir sagen, $a \neq 0$ aus R hat <u>eindeutige Zerlegung in unzerlegbare Faktoren</u>, wenn a eine Zerlegung

$$a = e p_1 p_2 \cdots p_r$$

in unzerlegbare Faktoren besitzt und eine solche eindeutig bestimmt ist in folgendem Sinne: Ist auch

$$a = e' p_1' p_2' \cdots p_{r'}'$$

eine solche Zerlegung, so gilt $r' = r$ und nach Umnumerierung
$p_i' \mathrel{\hat{=}} p_i \quad (p_i' = e_i p_i,\ e_i \in R^\times)$ für alle $1 \leq i \leq r$.

<u>F4</u>: 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 <u>eindeutige</u> Zerlegung in unzerlegbare Faktoren

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

<u>Bew.</u> (i) $\Rightarrow$ (ii): $a = e p_1 \cdots p_r$, $b = f q_1 \cdots q_s$

$ab = e f p_1 \cdots p_r q_1 \cdots q_s$ ist Zerlegung von ab in unzerlegbare Faktoren.

$p \mid ab \Rightarrow ab = pc$, p kommt vor, $\xRightarrow{\text{Eindeutigkeit}}$

$p \mathrel{\hat{=}} p_i$ oder $p \mathrel{\hat{=}} q_j$, $\Rightarrow$ $p \mid a$ oder $p \mid b$.

(ii) $\Rightarrow$ (i): Sei $a = e p_1 \cdots p_r = e' p_1' \cdots p_{r'}'$ wie oben. O.E. $r \geq 1$, $\Rightarrow$

$p_1 \mid a$, $\Rightarrow$ $p_1 \mid e' p_1' \cdots p_{r'}'$, $\xRightarrow{(ii)}$ $\exists i : p_1 \mid p_i'$ o.E. $i = 1$.

$p_1' = e_1 p_1,\ e_1 \in R^\times$, $\Rightarrow$ $e p_1 p_2 \cdots p_r = (e' e_1) p_1 p_2' \cdots p_{r'}'$ $\xRightarrow{R \text{ nullteilerfrei}}$

$$e p_2 \cdots p_r = (e' e_1) p_2' \cdots p_{r'}'.$$

Per Induktion: $r' = r$, $p_i' \mathrel{\hat{=}} p_i$ nach Umnumerierung. □

<u>Def. 6:</u> R komm. Ring mit $1 \neq 0$. Ein $p \in R$ heißt <u>Primelement</u> (von R), wenn stets:

(*) $\quad p \mid ab \implies p \mid a$ oder $p \mid b$

und außerdem $p \notin R^\times$.

<u>Bem'n:</u> 1) 0 ist Primelement in $R \iff R$ ist Integritätsring.

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

<u>Bew.</u> $p = ab \Rightarrow p \mid ab \Rightarrow$ o.E. $p \mid a \Rightarrow \exists c: a = pc = abc \overset{a \neq 0}{\Rightarrow} 1 = bc \Rightarrow b \in R^\times$.

Existenz von m klar: Menge $\neq \emptyset$ (sie enthält ab), Induktionsaxiom für $\mathbb{N}$

<u>Lemma:</u> $a, b \in \mathbb{N}$. Sei m das kleinste gemeinsame Vielfache von a und b. (Es sei m also das kleinste Element der Menge $\{c \in \mathbb{N} \mid a \mid c$ und $b \mid c\}$ bzgl. $\leq$)

Dann gilt:

$a \mid c$ und $b \mid c \implies m \mid c$

(d.h. c gemeinsames Vielfaches von a, b)

m ist also auch minimal bzgl. der Teilbarkeitsrelation $\mid$.

<u>Bew.</u> Annahme: $\exists c \in \mathbb{N}$ mit $a \mid c, b \mid c$, aber $m \nmid c$. Sei c das kleinste solche Element.

Nach Wahl von m gilt nun jedenfalls $m < c$, also $c - m \in \mathbb{N}$.

$c-m$ ist gemeinsames Vielfaches von a, b.

$$\xrightarrow[c \text{ minimal}]{c-m < c} m \mid c-m, \quad \Rightarrow m \mid c. \quad \text{W!}$$