Einführung in die Zahlentheorie – Kurzskript

Vorlesungswebseite: http://reh.math.uni-duesseldorf.de/~internet/ZTh_SS17/

Literatur:

- Schmidt: Einführung in die algebraische Zahlentheorie
- De Koninck, Luca: Analytic Number Theory
- Forster: Algorithmische Zahlentheorie
- Bordellès: Arithmetic Tales

0 Motivation/Ziele

Primzahltheorie

Satz 0.1 (Primzahlsatz; Hadamard, de la Vallée-Poussin; 1896) *Ist $\pi(x)$ die Anzahl der Primzahlen $\leqslant x$, so gilt:* $\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1$.

Vermutung 0.2 (Riemannsche Vermutung) *Alle nicht-trivialen Nullstellen der Riemanschen Zeta-Funktion haben Realteil $\frac{1}{2}$.*

Vermutung 0.3 (Goldbachsche Vermutung) *Jede gerade Zahl $n \geqslant 4$ lässt sich als Summe von zwei Primzahlen schreiben.*

Satz 0.4 (Ternäres Goldbach-Problem) *Jede ungerade Zahl $n \geqslant 7$ lässt sich als Summe von drei Primzahlen schreiben.*

Vermutung 0.5 (Primzahlzwillingsvermutung) *Es gibt unendlich viele Primzahlenzwillinge, d. h. Primzahlen p, p' mit $p' - p = 2$.*

Satz 0.6 (Kleine Primzahllücken; Zhang und andere; 2013) *Es gibt unendlich viele paare von Primzahlen p, p' mit $p' - p \leqslant 246$.*

Satz 0.7 (Primzahlen in arithmetischen Progressionen; Green-Tao; 2004) *Für jedes ℓ gibt es Zahlen a, b, so dass $a, a+b, a+2b, \ldots, a+\ell b$ alle prim sind.*

Diophantische Gleichungen

Satz 0.8 (Hilberts 10. Problem; Robinson, Davis, Putnam, Matiyasevich; 1970) *Es gibt keinen Algorithmus, der ein Polynom $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ als Eingabe nimmt und entscheidet, ob die Gleichung $f(x_1, \ldots, x_n) = 0$ ganzzahlige Lösungen besitzt.*

Satz 0.9 (Fermats Vermutung; Wiles; 1995) *Es gibt keine natürlichen Zahlen a, b, c, k mit $k \geqslant 3$, für die $a^k + b^k = c^k$ gilt.*

Satz 0.10 (Catalans Vermutung; Mihăilescu; 2002) *Die einzige ganzzahlige, nicht-triviale Lösung von $a^b + 1 = c^d$ ist $2^3 + 1 = 3^2$.*

Anderes

Vermutung 0.11 (abc-Vermutung) *Für jedes $\epsilon > 0$ gibt es nur endlich viele teilerfremde natürliche Zahlen $a + b = c$, so dass $\mathrm{rad}(abc)^{1+\epsilon} < c$. Hierbei ist $\mathrm{rad}(d)$ das Produkt aller Primzahlen, die d teilen.*

Satz 0.12 (Waringsches Problem; Hilbert; 1909) *Für jedes k gibt es ein ℓ, so dass sich jede natürliche Zahl als Summe von maximal ℓ k-ten Potenzen schreiben lässt.*

Algorithmisches

Satz 0.13 (Schneller Primzahltest) *Es gibt einen Algorithmus (Agrawal, Kayal, Saxena und andere; 2002), der eine natürliche Zahl n nimmt und in Zeit $\log(n)^6$ rausfindet, ob n prim ist.*

Satz 0.14 (Mersenne-Zahlen) *Es gibt eine schnelle Methode (der Lucas-Lehmer-Test), herauszufinden, ob eine Mersenne-Zahl $M_n := 2^n - 1$ prim ist. Insbesondere ist $2^{74\,207\,281} - 1$ prim.*

1 Primzahltheorie

1.1 Erinnerungen, Notationen

Konvention 1.1.1 (a) $\mathbb{N} = \{1, 2, 3, \dots\}$ *die Menge der natürlichen Zahlen. (In dieser Vorlesung fassen wir 0 nicht als natürliche Zahl auf).* $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$

(b) $\mathbb{P} = \{2, 3, 5, 7, \dots\}$ *die Menge der Primzahlen.*

(c) $\log x$ *ist der Logarithmus zur Basis e.*

(d) *Bis auf weiteres sind, wenn nicht anders angegeben:*

- $d, i, j, k, \ell, m, n, q, M, N$*: natürliche Zahlen*
- p*: Primzahl*
- $x, y, z, \epsilon, \delta$*: reelle Zahlen*
- s*: komplexe Zahl*
- *alle restlichen Kleinbuchstaben: ganze Zahlen*
- C, D*: reelle Zahlen (üblicherweise irgnedwelche Konstanten; meist > 0)*

Notation 1.1.2 (a) $a \mid b$ *bedeutet: a ist ein* ***Teiler*** *von b. (Formal: Es gibt ein c, so dass $ac = b$.) Sage auch: a* ***teilt*** *b, b ist ein* ***Vielfaches*** *von a.*

(b) $p^n \parallel b$ *(für p prim und $n \in \mathbb{N}_0$) bedeutet: $p^n \mid b$ aber $p^{n+1} \nmid b$. (Man sagt: „p^n* ***teilt*** *b* ***exakt***“.)

(c) $\mathrm{ggT}(a_1, \dots, a_n)$ *bezeichnet den* ***größten gemeinsamen Teiler*** *von $a_1, \dots, a_n$. Ausnahme: Falls $a_1 = \cdots = a_n = 0$, setze $\mathrm{ggT}(a_1, \dots, a_n) = 0$. Kurzschreibweise für $\mathrm{ggT}(a_1, \dots, a_n)$: $(a_1, \dots, a_n)$*

Erinnerung 1.1.3 *Jede Zahl n hat eine eindeutige (bis auf Reihenfolge)* ***Primfaktorzerlegung****:*

$$n = \prod_{i=1}^{\ell} p_i^{r_i}$$

für $\ell \in \mathbb{N}_0$, $p_i \in \mathbb{P}$, $r_i \in \mathbb{N}$. (Es gilt: $p_i^{r_i} \parallel n$.)

Erinnerung 1.1.4 *Der ggT von $a_1, \dots, a_n$ lässt sich mit dem Euklidischen Algorithmus berechnen. Dieser liefert auch Zahlen $r_1, \dots, r_n$, so dass $r_1 a_1 + \cdots + r_n a_n = (a_1, \dots, a_n)$.*

Notation 1.1.5 $a \equiv b \mod q$ *(„a ist* ***kongruent*** *b* ***modulo*** *q“) bedeutet: $q \mid a - b$. Hierbei nennt man q den* ***Modul****. Die „****Restklasse*** *von a modulo q“ ist die Menge*

$$a + q\mathbb{Z} = \{b \mid b \equiv a \mod q\}.$$

Notation 1.1.6 *$\lfloor x \rfloor$ ist die größte ganze Zahl kleiner gleich x. (Zu „$\lfloor x \rfloor$“ sagt man auch **Gauß-Klammer** von x.)*

Notation 1.1.7 *Seien $f, g \colon \mathbb{R}_{\geqslant 0} \to \mathbb{C}$ und $h \colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}$, so dass für hinreichend große x gilt: $h(x) \geqslant 0$*

(a) *„$f(x) = O(h(x))$“ bedeutet: Es gibt eine Konstante $C > 0$ so dass für alle hinreichend großen x gilt: $|f(x)| < Ch(x)$. Andere Notation dafür: $f(x) \ll h(x)$*
(b) *„$f(x) = o(h(x))$“ bedeutet: Für jedes $\epsilon > 0$ gibt es ein N, so dass für alle $x > N$ gilt: $|f(x)| < \epsilon h(x)$.*
(c) *Die Notation $f(x) \sim g(x)$ bedeutet: $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.*

Analoge Notationen werden verwendet, wenn f, g, h nur auf $\mathbb{N}$ definiert sind.

Bemerkung: Ist h nie 0, so ist:
(a) $\iff$ $\frac{|f(x)|}{h(x)}$ ist für hinreichend große x beschränkt;
(b) $\iff$ $\lim_{x\to\infty} \frac{|f(x)|}{h(x)} = 0$.

Satz 1.1.8 (a) *$f(x) = O(1)$ genau dann wenn f für hinreichend große x beschränkt ist. $f(x) = o(1)$ genau dann wenn f gegen 0 geht (für $x \to \infty$).*
(b) *Wenn es ein $x_0 \in \mathbb{R}$ gibt so dass $f_1(x) = f_2(x)$ und $h_1(x) = h_2(x)$ für alle $x > x_0$, dann gilt: $f_1(x) = O(h_1(x))$ genau dann wenn $f_2(x) = O(h_2(x))$; analog für $o(\dots)$.*
(c) *Für $r, s \in \mathbb{R}$ gilt: $x^r = O(x^s)$ genau dann wenn $r \leqslant s$, und $x^r = o(x^s)$ genau dann wenn $r < s$.*
(d) *Für jede reelle Zahl $r > 0$ gilt: $\log x = o(x^r)$ für jede, $x^r = o(e^x)$.*
(e) *Aus $f(x) = o(h(x))$ folgt $f(x) = O(h(x))$.*
(f) *Ist $f(x) = O(h(x))$ und ist $z \in \mathbb{C}$, so ist auch $zf(x) = O(h(x))$; analog für $o(\dots)$.*
(g) *Ist $f_1(x) = O(h(x))$ und $f_2(x) = O(h(x))$, so ist $f_1(x) + f_2(x) = O(h(x))$; analog für $o(\dots)$.*
(h) *Ist $f_1(x) = O(h_1(x))$ und $f_2(x) = O(h_2(x))$, so ist $f_1(x) \cdot f_2(x) = O(h_1(x) \cdot h_2(x))$; Ist $f_1(x) = O(h_1(x))$ und $f_2(x) = o(h_2(x))$, so ist $f_1(x) \cdot f_2(x) = o(h_1(x) \cdot h_2(x))$.*
(i) *Aus $f(x) = O(g(x))$ und $g(x) = O(h(x))$ folgt $f(x) = O(h(x))$; wenn sogar $f(x) = o(g(x))$ oder $g(x) = o(h(x))$ gilt, folgt $f(x) = o(h(x))$.*

Notation 1.1.9 *Wird $O(h(x))$ in einem Ausdruck verwendet, so steht es für eine beliebige Funktion $\hat{h}(x)$ mit $\hat{h}(x) = O(h(x))$. Genauer:*

(a) *Wird $O(h(x))$ auf der rechten Seite eines „=“ verwendet, so ist die Bedeutung: Es gibt eine Funktion $\hat{h}(x)$ mit $\hat{h}(x) = O(h(x))$, so dass der Ausdruck richtig wird, wenn man das „$O(h(x))$“ durch $\hat{h}(x)$ ersetzt.*
(b) *Kommt links vom „=“ „$O(g(x))$“ vor und rechts vom „=“ „$O(h(x))$“ (üblicherweise in Gleichungsketten), so ist die Bedeutung: Zu jedem $\hat{g}(x)$ mit $\hat{g}(x) = O(g(x))$ gibt es ein $\hat{h}(x)$ mit $\hat{h}(x) = O(h(x))$ so dass der Ausdruck richtig wird, wenn man die „$O(g(x))$“ und „$O(h(x))$“ durch $\hat{g}(x)$ und $\hat{h}(x)$ ersetzt.*

Analog für $o(h(x))$.

Bemerkung: Aus dieser Konvention folgt: Aus

$$f(x) = \text{ein-Ausdruck-mit-}O \quad \text{und} \quad \text{ein-Ausdruck-mit-}O = \text{anderer-Ausdruck-mit-}O$$

folgt

$$f(x) = \text{anderer-Ausdruck-mit-}O.$$

1.2 Primzahlen: Ziel und erste Resultate

Satz 1.2.1 *Es gibt unendlich viele Primzahlen.*

Satz 1.2.2 *Es gibt beliebig lange Primzahllücken (d. h. für beliebig große n gibt es m, so dass $m, m+1, \ldots, m+n$ alle nicht prim sind).*

Definition 1.2.3 *$\pi(x)$ bezeichnet die Anzahl der Primzahlen kleiner gleich x.*

Hauptziel dieses Kapitels:

Satz 1.2.4 (Primzahlsatz) $\pi(x) \sim \frac{x}{\log x}$.

Satz 1.2.5 *Setze* $\mathrm{li}(x) := \int_2^x \frac{dt}{\log t}$. *Die Riemannsche Vermutung ist äquivalent zu:* $\pi(x) - \mathrm{li}(x) = O(\sqrt{x}\log x)$.

(Ohne Beweis)

Satz 1.2.6 *Für $q \geqslant 1$ und a gilt: Es gibt unendlich viele Primzahlen $p \equiv a \mod q$ genau dann wenn $(a, q) = 1$.*

(Beweis nur von $\Rightarrow$)

Satz 1.2.7 *Es gibt unendlich viele Primzahlen $\equiv -1 \mod 3$ und unendlich viele Primzahlen $\equiv -1 \mod 4$.*

Satz 1.2.8 *Die Summe $\sum_{p\in\mathbb{P}} \frac{1}{p}$ divergiert.*

Lemma 1.2.9 *Sind x_i ($i \in \mathbb{N}$) reelle Zahlen mit $0 < x_i < 1$, so sind äquivalent:*

(a) *Die Summe $\sum_i x_i$ konvergiert.*
(b) *Das Produkt $\prod_i (1 - x_i)$ konvergiert gegen einen Wert größer als 0.*

Definition 1.2.10 *Die Riemannsche Zeta-Funktion $\zeta\colon \mathbb{C}\backslash\{1\} \to \mathbb{C}$ ist für $s \in \mathbb{C}$ mit $\Re(s) > 1$ definiert durch*

$$\zeta(s) = \sum_{n\in\mathbb{N}} \frac{1}{n^s}.$$

Vermutung 1.2.11 (Riemannsche Vermutung) *Alle Nullstellen von ζ haben entweder Imaginärteil 0 oder Realteil $\frac{1}{2}$.*

Satz 1.2.12 $\zeta(2) = \frac{\pi^2}{6}$.

1.3 Der Satz von Chebychev

Satz 1.3.1 (Chebychev-Ungleichungen) *Es gibt Konstanten $C_1, C_2 > 0$ so dass für alle $x \geqslant 2$ gilt:*

$$C_1 \frac{x}{\log x} \leqslant \pi(x) \leqslant C_2 \frac{x}{\log x}$$

Genauer: Dies gilt für $C_1 = \frac{3\log 2}{8} \approx 0,3$ und $C_2 = 6\log 2 \approx 4,2$.

Lemma 1.3.2 *Ist $p^\ell \parallel n!$, so gilt $\ell = \sum_k \lfloor \frac{n}{p^k} \rfloor$.*

Lemma 1.3.3 *Aus $p^\ell \mid \binom{2n}{n}$ folgt $p^\ell \leqslant 2n$*

Korollar 1.3.4 *Sei p_n die n-te Primzahl. Es gibt Konstanten $C_1, C_2 > 0$, so dass für alle n gilt:*

$$C_1 n \log n \leqslant p_n \leqslant C_2 n \log n.$$

1.4 Zahlentheoretische Funktionen

Definition 1.4.1 *Eine natürliche Zahl n heißt **quadrathaltig**, wenn es ein p gibt mit $p^2 \mid n$. Sonst heißt n **quadratfrei**.*

Satz 1.4.2 *Die Wahrscheinlichkeit, dass eine zufällige Zahl quadratfrei ist, ist $\frac{6}{\pi^2}$. Genauer:*

$$\#\{n \leqslant x : n \text{ } \textbf{\textit{quadratfrei}}\} \sim \frac{6}{\pi^2} x$$

Satz 1.4.3 *Die Wahrscheinlichkeit, dass zwei zufällige Zahlen teilerfremd sind, ist auch $\frac{6}{\pi^2}$. Genauer:*

$$\#\{m, n \leqslant x : \mathrm{ggT}(m, n) = 1\} \sim \frac{6}{\pi^2} x^2$$

Satz 1.4.4 *Zahlen $\leqslant x$ haben im Mittel $\log x + C$ Teiler, für eine Konstante $C \approx 0,154$. Genauer:*

$$\frac{1}{x} \sum_{m \leqslant x} \#\{d : d \mid m\} = \log x + C + O(\frac{1}{\sqrt{x}})$$

Definition 1.4.5 (a) *Eine **zahlentheoretisch Funktion** ist eine Funktion $f \colon \mathbb{N} \to \mathbb{C}$.*
(b) *Die **Faltung** von zwei zahlentheoretischen Funktionen f, g ist definiert durch:*

$$(f * g)(n) := \sum_{d \mid n} f(d) g(\frac{n}{d}).$$

Definition 1.4.6 *Man definiert die folgenden zahlentheoretischen Funktionen:*

(a) $\underline{1}(n) := 1$.
(b) $\mathrm{id}(n) := n$
(c) $\epsilon(n) := \begin{cases} 1 & n = 1 \\ 0 & \textit{sonst} \end{cases}$
(d) $d(n) := \#\{d \leqslant n : d \mid n\}$ *(die Anzahl der Teiler von n)*
(e) $\mu(n) := \begin{cases} (-1)^\ell & n = p_1 \cdots p_\ell \textit{ für paarweise verschiedene } p_i \\ 0 & n \textit{ quadrathaltig} \end{cases}$
(f) $\phi(n) := \#\{m \leqslant n : \mathrm{ggT}(m, n) = 1\}$ *(die Eulersche ϕ-Funktion)*

Satz 1.4.7 (a) $\underline{1} * \underline{1} = d$.
(b) $\mu * \underline{1} = \epsilon$
(c) $\phi * \underline{1} = \mathrm{id}$

Satz und Definition 1.4.8 (a) *Die Menge der zahlentheoretischen Funktionen mit punktweiser Addition und $*$ bildet einen kommutativen Ring, mit neutralem Element*

$$\epsilon(n) := \begin{cases} 1 & n = 1 \\ 0 & \textit{sonst} \end{cases}$$

(b) *Gilt $f * g = \epsilon$, so nennt man g **Faltungsinverses** von f. Eine zahlentheoretische Funktion f besitzt ein Faltungsinverses genau dann, wenn $f(1) \neq 0$ ist.*

Bemerkung: Natürlich bilden die zahlentheoretischen Funktionen auch mit punktweiser Addition und punktweiser Multiplikation einen Ring.

Definition 1.4.9 *Das **Radikal** $\mathrm{rad}(n)$ einer Zahl n ist das Produkt aller Primzahlen, die n teilen.*

Lemma 1.4.10 $\mu^2(n) = \sum_{d:d^2|n} \mu(n)$.

Lemma 1.4.11 *Sind f, g zahlentheoretische Funktionen und ist $s \in \mathbb{C}$ so dass $\sum_n f(n)/n^s$ und $\sum_n g(n)/n^s$ absolut konvergent sind, so konvergiert auch $\sum_n (f*g)(n)/n^s$ absolut, und es gilt*

$$\sum_n \frac{f(n)}{n^s} \cdot \sum_n \frac{g(n)}{n^s} = \sum_n \frac{(f*g)(n)}{n^s}.$$

Lemma 1.4.12 $\sum_{m \leqslant x} \frac{\mu(m)}{m^2} = \frac{6}{\pi^2} + O(\frac{1}{x})$

Lemma 1.4.13 *Es gibt eine Zahl $\gamma \in \mathbb{R}$ so dass gilt: $\sum_{n \leqslant x} \frac{1}{n} = \log x + \gamma + O(\frac{1}{x})$. ($\gamma \approx 0,577$ nennt man auch **Eulersche Konstante**; nicht zu verwechseln mit $e \approx 2,718$.)*

1.5 Dirichlet-Reihen

Konvention 1.5.1 *Im Folgenden ist s immer eine komplexe Zahl mit Realteil σ und Imaginärteil t; also $s = \sigma + it$.*

Definition 1.5.2 *Eine **Dirichlet-Reihe** ist eine unendliche Reihe der Form*

$$\sum_n \frac{a_n}{n^s}$$

*für $a_n \in \mathbb{C}$. Die a_n nennt man die **Koeffizienten** der Reihe.*

Satz und Definition 1.5.3 (a) *Zu jeder Dirichlet-Reihe gibt es (genau) ein $\sigma_0 \in \mathbb{R} \cup \{-\infty, +\infty\}$ so dass gilt (für $s = \sigma + it$):*
- *Die Reihe konvergiert falls $\sigma > \sigma_0$.*
- *Die Reihe divergiert falls $\sigma < \sigma_0$.*

*Dieses σ_0 nennt man die **Konvergenz-Abszisse** der Reihe. ($\sigma_0 = -\infty$ bedeutet, dass die Reihe immer konvergiert, $\sigma_0 = +\infty$ bedeutet, dass sie nie konvergiert.)*

(b) *Ist $F(s) = \sum a_n \cdot n^{-s}$ eine Dirichlet-Reihe mit Konvergenz-Abszisse $\sigma_0 < +\infty$, so ist F auf $\{s = \sigma + it \in \mathbb{C} \mid \sigma > \sigma_0\}$ holomorph.*

Bemerkung 1.5.4 *Das Konvergenzverhalten bei $\sigma = \sigma_0$ kann von t abhängen.*

Beispiel 1.5.5 *Die Konvergenz-Abszisse der Dirichlet Reihe $\sum n^{-s}$ ist 1 (vergleiche Definition 1.2.10).*

Satz und Definition 1.5.6 *Für $s > 1$ gilt:*

(a) $\zeta'(s) = \sum_n \frac{-\log n}{n^s}$.

(b) $\frac{\zeta'(s)}{\zeta(s)} = \sum_n \frac{-\Lambda(n)}{n^s}$, *wobei*

$$\Lambda(n) := (\log * \mu)(n) = \begin{cases} \log p & n = p^r \\ 0 & n \text{ ist keine Primpotenz.} \end{cases}$$

1.6 Die Riemannsche Zeta-Funktion

Satz 1.6.1 *Für $\sigma > 0$ und $s \neq 1$ gilt:*

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{x - \lfloor x \rfloor}{x^{s+1}} dx.$$

Lemma 1.6.2 (Abelsche Summenformel, vereinfachte Version) *Sei $f\colon \mathbb{R} \to \mathbb{C}$ differenzierbar und $x \geqslant 0$. Dann gilt:*

$$\sum_{n \leqslant x} f(n) = \lfloor x \rfloor f(x) - \int_1^x \lfloor y \rfloor f'(y)\, dy.$$

Satz 1.6.3 $\sum_n \frac{\mu(n)}{n} = 0$.

Satz 1.6.4 (Newmanscher Taubersatz) *Sei*

$$F(s) := \sum_n \frac{a_n}{n^s}$$

eine Dirichlet-Reihe mit Koeffizienten $a_n \in \mathbb{C}$, $|a_n| \leqslant 1$. (Diese Reihe konvergiert offensichtlich für $\sigma > 1$, wobei $s = \sigma + it$). Wenn sich die Funktion holomorph fortsetzen lässt auf den Bereich $\sigma \geqslant 1$ (genauer: auf eine offene Menge, die diesen Bereich enthält), dann konvergiert auch die Dirichlet-Reihe für $\sigma = 1$ gegen den entsprechenden Funktionswert.

Satz 1.6.5 *ζ hat keine Nullstellen bei $\sigma = 1$.*

1.7 Beweis des Primzahlsatzes

Definition 1.7.1 $\psi(x) := \sum_{n \leqslant x} \Lambda(n)$.

Satz 1.7.2 $\psi(x) \sim \pi(x)\log(x)$.

Satz 1.7.3 (Primzahlsatz, Formulierung mit ψ) $\psi(x) \sim x$.

Lemma 1.7.4 *Ist z_n eine Folge von komplexen Zahlen mit $\sum_n \frac{z_n}{n} = 0$, so gilt $\sum_{n \leqslant x} z_n = o(x)$.*

Insbesondere ist (nach Satz 1.6.3) $\sum_{n \leqslant x} \mu(n) = o(x)$.

Lemma 1.7.5 $\sum_{n \leqslant x} \log(n) = x(\log x - 1) + O(\log x)$.

Lemma 1.7.6 $\sum_{n \leqslant x} \frac{1}{\sqrt{n}} = O(\sqrt{x})$.

2 Kongruenzrechnung

2.1 Diophantische Gleichungen und Kongruenzen

Konvention 2.1.1 *In dieser Vorlesung sind alle Ringe kommutativ und haben ein neutrales Element, und bei **Ringhomomorphismen** $R \to S$ fordern wir, dass sie das neutrale Element von R auf das neutrale Element von S abbilden.*

Bemerkung 2.1.2 *Sei R ein Ring.*

(a) *Es gibt genau einen Ringhomomorphismus $\mathbb{Z} \to R$. Das Bild von $a \in \mathbb{Z}$ unter dem Ringhomomorphismus $\mathbb{Z} \to q\mathbb{Z}$ bezeichnen wir mit $a \bmod q$.*

(b) *Sind $a_1, \ldots, a_n \in R$, so gibt es genau einen Ring-Homomorphismus $\mathbb{Z}[X_1, \ldots, X_n] \to R$, der X_i auf a_i abbildet für alle i. Das Bild von $f \in \mathbb{Z}[X_1, \ldots, X_n]$ unter diesem Homomorphismus wird mit $f(a_1, \ldots, a_n)$ bezeichnet.*

Definition 2.1.3 *Sei R ein Ring und $f \in \mathbb{Z}[X_1, \ldots, X_n]$. Die Menge der „**Lösungen von $f = 0$ in R**“ ist*

$$\{(a_1, \ldots, a_n) \in R : f(a_1, \ldots, a_n) = 0\}$$

*Interessiert man sich für die Lösungen von $f = 0$ in $\mathbb{Z}$, so nennt man dies eine **diophantische Gleichung**. Die Lösungen von $f = 0$ in $\mathbb{Z}/q\mathbb{Z}$ werden auch als „Lösungen von $f = 0$ modulo q“ bezeichnet.*

Satz 2.1.4 *Ist $f \in \mathbb{Z}[X_1, \ldots, X_n]$, ist $\phi\colon R \to S$ ein Ringhomomorphismus und ist $(a_1, \ldots, a_n) \in R^n$ eine Lösung von $f = 0$ in R, so ist $(\phi(a_1), \ldots, \phi(a_n))$ Eine Lösung von f in S. Insbesondere gilt: Wenn es ein $q \in \mathbb{N}$ gibt, so dass $f = 0$ keine Lösung in $\mathbb{Z}/q\mathbb{Z}$ besitzt, so besitzt $f = 0$ auch keine Lösung in $\mathbb{Z}$.*

2.2 Modul wechseln

In diesem Abschnitt sei $f \in \mathbb{Z}[X_1, \ldots, X_n]$ gegeben, und für $q \in \mathbb{N}$ sei $L_q \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ die Menge der Lösungen von $f = 0$ modulo q.

Bemerkung 2.2.1 *Wenn $q \mid q'$ gilt, induziert die Abbildung $\mathbb{Z}/q'\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ eine Abbildung $L_{q'} \to L_q$.*

Satz 2.2.2 (Chinesischer Restsatz, Ring-Version) *Sind $q_1, \ldots, q_k \in \mathbb{N}$ paarweise teilerfremd und $q = q_1 \cdots q_k$, so ist*

$$\mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}, \quad a \bmod q \mapsto (a \bmod q_1, \ldots, a \bmod q_k)$$

ein Isomorphismus von Ringen. Insbesondere ist $\#L_q = \#L_{q_1} \cdot \#L_{q_2} \cdots \#L_{q_k}$.

Satz 2.2.3 (Hensels Lemma) *Seien $p \in \mathbb{P}, r \in \mathbb{N}$, und sei $\underline{a} := (a_1, \ldots, a_n) \in L_{p^r}$ eine Lösung modulo p^r. Wir nehmen an, dass es ein $s < \frac{r}{2}$ und ein ℓ gibt mit*

$$\frac{\partial f}{\partial X_1}(\underline{a}) \equiv \cdots \equiv \frac{\partial f}{\partial X_n}(\underline{a}) \equiv 0 \mod p^s$$

$$\text{und} \qquad \frac{\partial f}{\partial X_\ell}(\underline{a}) \not\equiv 0 \mod p^{s+1}$$

Dann gibt es für jedes $r' \geqslant r$ (mindestens) ein Tupel $\underline{b} := (b_1, \ldots, b_n) \in L_{p^{r'}}$ mit $(\underline{b} \bmod p^{r-s}) = (\underline{a} \bmod p^{r-s})$.

Ist $s = 0$ und $n = 1$, so gibt es sogar genau ein solches $\underline{b}$.

Bemerkungen:

- $\frac{\partial f}{\partial X_\ell}(\underline{a})$ ist ein Element von $\mathbb{Z}/p^r\mathbb{Z}$; die Frage, ob dies kongruent 0 modulo $p^{s'}$ ist, macht also Sinn wenn $s' \leqslant r$ ist. Aus $s < \frac{r}{2}$ folgt in der Tat $s + 1 \leqslant r$.
- Falls $s = 0$ ist, sind die Tupel $\underline{b}$ genau die Urbilder von $\underline{a} \bmod p^r$ unter der Abbildung $L_{p^{r'}} \to L_{p^r}$.
- Die Anzahl der $\underline{b}$ lässt sich auch für $n > 1$ und/oder $s > 0$ explizit angeben. (Sie hängt nur von n, s und p ab.)

2.3 Einheiten in $\mathbb{Z}/q\mathbb{Z}$

Erinnerung 2.3.1 *Eine **Einheit** in einem Ring R ist ein Element $a \in R$, so dass es ein $b \in R$ gibt mit $ab = 1$. Die Menge der Einheiten bildet unter Multiplikation eine Gruppe und wird mit $R^\times$ bezeichnet.*

Satz 2.3.2 *Für $q \geqslant 1$ gilt: $(\mathbb{Z}/q\mathbb{Z})^\times = \{a \bmod q : a < q, (a,q) = 1\}$. Insbesondere ist $\#(\mathbb{Z}/q\mathbb{Z})^\times = \phi(q)$.*

Lemma 2.3.3 *Der größte gemeinsame Teiler von $a_1, a_2 \in \mathbb{Z}$ lässt sich als ganzzahlige Linearkombintation von a_1, a_2 schreiben, d. h. es gibt $b_1, b_2 \in \mathbb{Z}$ mit $\mathrm{ggT}(a_1, a_2) = b_1 a_1 + b_2 a_2$.*

Satz 2.3.4 *Sind $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen, so gilt:*

$$\phi(p_1^{r_1} \cdots p_k^{r_k}) = \prod_{j=1}^{k} p_j^{r_j - 1}(p_j - 1).$$

Satz 2.3.5 (Satz von Euler-Fermat) *Sind $a \in \mathbb{Z}$ und $q \in \mathbb{N}$ teilerfremd, so ist $a^{\phi(q)} \equiv 1 \bmod q$.*

Satz 2.3.6 (Satz von Wilson) *Eine natürliche Zahl n is prim genau dann wenn $(n-1)! \equiv -1 \mod n$.*

2.4 Primitivwurzeln

Definition 2.4.1 *Ist $a \in (\mathbb{Z}/q\mathbb{Z})^\times$, so schreiben wir $\mathrm{ord}(a)$ für die Ordnung von a in dieser Gruppe, d. h. $\mathrm{ord}(a)$ ist die kleinste natürliche Zahl, so dass $a^{\mathrm{ord}(a)} = 1$ ist.*

Satz 2.4.2 *Für $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ gilt: $\mathrm{ord}(a) \mid \phi(a)$.*

Definition 2.4.3 *Eine **Primitivwurzel** modulo q ist ein Element $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ mit $\mathrm{ord}(a) = \phi(q)$. Wir nennen auch $b \in \mathbb{Z}$ eine Primitivwurzel modulo q, wenn $b \mod q$ eine Primitivwurzel modulo q ist.*

Satz 2.4.4 *Ist a eine Primitivwurzel modulo q, so ist $(\mathbb{Z}/q\mathbb{Z})^\times = \{a^0, a^1, a^2, \ldots, a^{\phi(q)-1}\}$.*

Erinnerung 2.4.5 *Wir schreiben C_n für die zyklische Gruppe mit n Elementen.*

(a) *Jede endliche abelsche Gruppe G ist isomorph zu einer Gruppe der Form $C_{p_1^{r_1}} \times \cdots \times C_{p_k^{r_k}}$ (wobei die selbe Primzahl mehrfach auftauchen kann). Dabei sind die $p_i^{r_i}$ bis auf Reihenfolge eindeutig bestimmt.*
(b) *Eine Gruppe der Form $C_{n_1} \times \cdots \times C_{n_k}$ ist zyklisch genau dann, wenn die n_i paarweise teilerfremd sind.*

Satz 2.4.6 *Die multiplikative Gruppe $(\mathbb{Z}/q\mathbb{Z})^\times$ lässt sich wie folgt bestimmen:*

(a) *Für $p \geqslant 3$ gilt: $(\mathbb{Z}/p^r\mathbb{Z})^\times \cong C_{\phi(p^r)}$ (wobei $\phi(p^r) = (p-1)p^{r-1}$).*
(b) *$(\mathbb{Z}/2\mathbb{Z})^\times = C_1$, und für $r \geqslant 2$ gilt: $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong C_2 \times C_{2^{r-2}}$.*
(c) *Ist $q = p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung, so ist $(\mathbb{Z}/q\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{r_k}\mathbb{Z})^\times$.*

Insbesondere gibt es Primitivwurzeln modulo q genau dann wenn q die eine der Formen $1, 2, 4, p^r, 2p^r$ hat für $p \geqslant 3$ und $r \geqslant 1$.

Lemma 2.4.7 *Für p prim und $1 \leqslant r_0 \leqslant r$ ist $(1 + p^{r_0}\mathbb{Z})/p^r\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}p^r\mathbb{Z})^\times$. Falls $p \geqslant 3$ oder $r_0 \geqslant 2$ ist diese Gruppe zyklisch und wird von $1 + p^{r_0}$ erzeugt.*

2.5 Das quadratische Reziprozitätsgesetz

Definition 2.5.1 *Sei $p \geqslant 3$ prim und $a \in \mathbb{Z}$.*

(a) *Man nennt a einen **quadratischen Rest** modulo p, wenn $p \nmid a$ und es ein b gibt mit $b^2 \equiv a \mod p$.*

(b) *Man nennt a einen **quadratischen Nichtrest** modulo p, wenn $p \nmid a$ und es kein b gibt mit $b^2 \equiv a \mod p$.*

(c) *Das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ ist definiert durch:*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ ist ein quadratischer Rest modulo } p \\ -1 & a \text{ ist ein quadratischer Nichtrest modulo } p \\ 0 & p \mid a. \end{cases}$$

Satz 2.5.2 *Sei $p \geqslant 3$ prim, und seien $b, c \in \mathbb{Z}$. Die Gleichung $X^2 + bX + c = 0$ hat $\left(\frac{b^2-4c}{p}\right)+1$ viele Lösungen modulo p.*

Satz 2.5.3 *Für $p \geqslant 3$ gilt: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ für alle a. Insbesondere definiert $a \mapsto \left(\frac{a}{p}\right)$ einen surjektiven Gruppenhomomorphsimus $\mathbb{F}_p^\times \to \{\pm 1\}$, uns es gibt genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste modulo p.*

Satz 2.5.4 (Quadratisches Reziprozitätsgesetz) *Sind $p, p' \geqslant 3$ zwei verschiedene Primzahlen, so gilt: $\left(\frac{p}{p'}\right) \cdot \left(\frac{p'}{p}\right) = (-1)^{\frac{p-1}{2}\frac{p'-1}{2}}$. (Die beiden Legendre-Symbole haben also verschiedene Vorzeichen genau dann, wenn sowohl $p \equiv 3 \mod 4$ als auch $p' \equiv 3 \mod 4$ ist.)*

Satz 2.5.5 (Ergänzungssatz zum quadratischen Reziprozitätsgesetz) *Für $p \geqslant 3$ gilt:*

(a) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, *d. h. -1 ist ein quadratischer Rest modulo p genau dann, wenn $p \equiv 1 \mod 4$ ist.*

(b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, *d. h. 2 ist ein quadratischer Rest modulo p genau dann, wenn $p \equiv \pm 1 \mod 8$ ist.*

Lemma 2.5.6 *Sei $p \geqslant 3$ und $p \nmid a$. Dann ist*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{(p-1)/2} \lfloor \frac{2aj}{p} \rfloor}.$$

Satz 2.5.7 *Es gibt unendlich viele Primzahlen $\equiv 1 \mod 4$.*

2.6 Der Miller-Rabin-Primzahltest

Satz 2.6.1 *Sei $n \geqslant 3$ ungerade und sei $n - 1 = m \cdot 2^k$, für m ungerade.*

(a) *Ist n prim, so gilt für alle $a \in (\mathbb{Z}/n\mathbb{Z})^\times$:*

$$\text{Entweder } a^m = 1 \text{ oder es gibt ein } \ell \in \{0, \ldots, k-1\} \text{ mit } a^{m2^\ell} = -1. \qquad (*)$$

(b) *Ist n nicht prim, so hat die Menge*

$$A := \{a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a \text{ erfüllt } (*)\}$$

höchstens $\frac{1}{4}\phi(n)$ Elemente.

Bemerkung 2.6.2 *Aus der verallgemeinerten Riemannnschen Vermutung folgt: Ist n nicht prim, so ist $\{1, \ldots, \lfloor 2(\log n)^2 \rfloor\} \bmod n \not\subset A$, d h. es reicht, Zahlen $a \leqslant 2(\log n)^2$ zu testen, um sicher rauszufinden, ob n prim ist.*

Satz 2.6.3 *Es gibt einen Algorithmus mit folgenden Eigenschaften:*

- *Eingabe: $n, r, q \in \mathbb{N}$ mit $n < q$.*
- *Ausgabe: $n^r \mod q$*
- *Die Laufzeit (Anzahl der benötigten Rechenschritte) ist $O((\log q)^2 \cdot \log r)$.*

Satz 2.6.4 (Miller-Rabin-Primzahltest) *Es gibt einen randomisierten Algorithmus mit folgenden Eigenschaften:*

- *Eingabe: $n, N \in \mathbb{N}$.*
- *Ist n prim, so antwortet der Algorithmus „prim“. Ist n nicht prim, so antwortet der Algorithmus höchtens mit Wahrscheinlichkeit 2^{-N} „prim“ (und sonst „nicht prim“).*
- *Laufzeit: $O(N(\log n)^3)$.*

2.7 RSA-Verschlüsselung

Lemma 2.7.1 *Sei $q = p_1 \cdot p_2$ das Produkt von zwei verschiedenen Primzahlen, sei λ das kleinste gemeinsame Vielfache von $p_1 - 1$ und $p_2 - 1$ und sei $e \in \mathbb{N}$ teilerfremd zu λ. Dann ist $(\mathbb{Z}/q\mathbb{Z})^\times \to (\mathbb{Z}/q\mathbb{Z})^\times, a \mapsto a^e$ eine Bijektion, und die inverse Abbildung hat die Form $b \mapsto b^d$, für ein (beliebiges) $d \in \mathbb{N}$, das $de \equiv 1 \mod \lambda$ erfüllt.*

RSA-Verschlüsselung funktioniert wie folgt: Der Empfänger wählt zwei Primzahlen p_1, p_2, bestimmt das Produkt $q = p_1 \cdot p_2$, bestimmt das kleinste gemeinsame Vielfache λ von $p_1 - 1$ und $p_2 - 1$, wählt einen „öffentlichen Schlüssel“ e, der teilerfremd zu λ ist und bestimmt ein d („geheimer Schlüssel“) mit $de \equiv 1 \mod \lambda$. Der Empfänger gibt nun q und e bekannt.

Ist a (eine Zahl $< q$) die Nachricht, die gesendet werden soll, so ist $a' := a^e \mod q$ die verschlüsselte Nachricht. Der Empfänger kann sie mit Hilfe des Lemmas entschlüsseln: $a \equiv (a')^d \mod q$.

3 Zahlringe

3.1 Erinnerung: Zahlkörper

Notation 3.1.1 (a) *Wir setzen $\zeta_n := e^{2\pi i/n}$. (Dies ist eine primitive n-te Einheitswurzel: $\zeta_n^n = 1$ und $\zeta_n^k \neq 1$ für $k < n$.)*

(b) *Ist $K \subseteq \mathbb{C}$ ein Körper und sind $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$., so bezeichnet $K(\alpha_1, \ldots, \alpha_k)$ den kleinsten Unterkörper von $\mathbb{C}$, der K und $\alpha_1, \ldots, \alpha_k$ enthält.*

(c) *Ist $R \subseteq \mathbb{C}$ ein Ring und sind $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$, so bezeichnet $R[\alpha_1, \ldots, \alpha_k]$ den kleinsten Unterring von $\mathbb{C}$, der R und $\alpha_1, \ldots, \alpha_k$ enthält.*

Erinnerung 3.1.2 (a) *Ein $\alpha \in \mathbb{C}$ heißt **algebraisch**, wenn es ein Polynom $f \in \mathbb{Q}[X]\backslash\{0\}$ gibt mit $f(\alpha) = 0$. Ist dies der Fall, so gibt es ein Polynom $\mathrm{MiPo}_\alpha \in \mathbb{Q}[X]\backslash\{0\}$, so dass für alle $f \in \mathbb{Q}[X]$ gilt: $f(\alpha) = 0 \iff \mathrm{MiPo}_\alpha \mid f$. Fordert man zusätzlich, dass MiPo_α normiert ist, so ist es eindeutig und wird **Minimalpolynom** von α genannt.*

(b) *Ein Körper $K \subseteq \mathbb{C}$ heißt **Zahlkörper**, wenn die folgenden, äquivalenten Bedingungen gelten:*

(i) K ist als $\mathbb{Q}$-Vektorraum endlich-dimensional.

(ii) Es gibt algebraische $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$, so dass $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$

(iii) Es gibt ein algebraisches $\alpha \in \mathbb{C}$, so dass $K = \mathbb{Q}(\alpha)$.

(c) *Sei $K = \mathbb{Q}(\alpha)$ ein Zahlkörper.*
   (i) Alle Elemente von K sind algebraisch.
   *(ii) Der **Grad** von K über $\mathbb{Q}$ ist die Dimension von K als $\mathbb{Q}$-Vektorraum. Man schreibt $[K : \mathbb{Q}]$ dafür, und es gilt: $[K : \mathbb{Q}] = \deg \mathrm{MiPo}_\alpha$.*
   Im Folgenden sei $n = [K : \mathbb{Q}]$.
   (iii) Die Elemente $1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in K$ bilden eine Basis von K als $\mathbb{Q}$-Vektorraum.
   *(iv) Es gibt genau n verschiedene Ringhomomorphismen $\sigma_j \colon K \to \mathbb{C}$: Sind $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ die Nullstellen von MiPo_α, so ist σ_j festgelegt durch $\sigma_j(\alpha) = \alpha_i$. Diese Ringhomomorphismen sind injektiv (also „Einbettungen" von K nach $\mathbb{C}$). Die Elemente α_j nennt man die **Konjugierten** von α.*

Beispiel 3.1.3 *$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$; die Konjugierten von ζ_n sind genau die Erzeuger der zyklischen (multiplikativen) Gruppe $\boldsymbol{\mu}_n := \{\zeta \in \mathbb{C}^\times \mid \zeta^n = 1\}$.*

Erinnerung 3.1.4 *Seien nun $K \subseteq L$ Zahlkörper.*

(a) *Der **Grad** von L über K ist die Dimension von L als K-Vektorraum; Notation dafür: $[L : K]$.*
(b) *Es gilt: $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}]$.*
(c) *Ein Element $\alpha \in L$ liegt in K genau dann, wenn jede Einbettung $\sigma \colon L \to \mathbb{C}$, die auf K die Identität ist, auch α auf sich selbst abbildet.*

Definition 3.1.5 *Sei K ein Zahlkörper von Grad n und seien $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$ alle Einbettungen und sei $\alpha \in K$. Wir definieren:*

(a) *Das **charakteristische Polynom** von α ist $\chi_{K/\mathbb{Q},\alpha}(X) = \prod_{i=1}^{n}(X - \sigma_i(\alpha))$*
(b) *Die **Norm** von α ist $\mathrm{N}_{K/\mathbb{Q}}(\alpha) := \prod_{j=1}^{n} \sigma_j(\alpha)$.*
(c) *Die **Spur** von α ist $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) := \sum_{j=1}^{n} \sigma_j(\alpha)$.*

Satz 3.1.6 *Ist K ein Zahlkörper und ist $\alpha \in K$, so gilt:*

(a) *Ist $d = \deg \mathrm{MiPo}_\alpha$, so ist $\chi_{K/\mathbb{Q},\alpha} = \mathrm{MiPo}_\alpha^{n/d}$. Insbesondere ist $\chi_{K/\mathbb{Q},\alpha}(X) \in \mathbb{Q}[X]$.*
(b) *Ist $\chi_{K/\mathbb{Q},\alpha}(X) = b_0 + b_1 X + \cdots + b_{n-1}X^{n-1} + X^n$, so ist $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = (-1)^n \cdot b_0$ und $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -b_{n-1}$; insbesondere sind $\mathrm{N}_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$.*

Satz 3.1.7 *Sei K ein Zahlkörper vom Grad n und seien $\alpha, \beta \in K$. Dann gilt:*

(a) $\mathrm{N}_{K/\mathbb{Q}}(\alpha\beta) = \mathrm{N}_{K/\mathbb{Q}}(\alpha) \cdot \mathrm{N}_{K/\mathbb{Q}}(\beta)$
(b) $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta)$
(c) *Ist $\alpha \in \mathbb{Q}$, so ist $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \alpha^n$ und $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = n\alpha$. Insbesondere ist $\mathrm{N}_{K/\mathbb{Q}}(1) = 1$ und $\mathrm{Tr}_{K/\mathbb{Q}}(1) = n$.*

3.2 Definition von Zahlringen

Definition 3.2.1 *Ein $\alpha \in \mathbb{C}$ heißt **ganz-algebraisch**, wenn α algebraisch ist und $\mathrm{MiPo}_\alpha \in \mathbb{Z}[X]$ liegt.*

Satz 3.2.2 *Die folgenden Bedingungen an $\alpha \in \mathbb{C}$ sind äquivalent:*

(a) *α ist ganz-algebraisch.*
(b) *Es gibt ein normiertes Polynom $f \in \mathbb{Z}[X]\backslash\{0\}$ mit $f(\alpha) = 0$.*
(c) *$\mathbb{Z}[\alpha]$ ist endlich erzeugt.*
(d) *Es gibt eine endlich erzeugte Untergruppe $G \subseteq (\mathbb{C}, +)$ mit $\alpha G \subseteq G$.*

Satz 3.2.3 *Die Menge aller ganz-algebraischen Zahlen bildet einen Ring.*

Definition 3.2.4 *Ist K ein Zahlkörper, so schreiben wir $\mathcal{O}_K \subseteq K$ für die Menge der ganzalgebraischen Zahlen in K. Ein solcher Ring $\mathcal{O}_K$ wird* ***Zahlring*** *genannt.*

Bemerkung 3.2.5 *Ist K ein Zahlkörper und $\alpha \in \mathcal{O}_K$, so ist $\chi_{K/\mathbb{Q},\alpha}(X) \in \mathbb{Z}[X]$, $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ und $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Beispiel 3.2.6 *Ist $d \in \mathbb{Z}$ quadratfrei und $K = \mathbb{Q}(\sqrt{d})$, so ist*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1}{2}\sqrt{d} + \frac{1}{2}] & \text{falls } d \equiv 1 \mod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{sonst.} \end{cases}$$

Beispiel 3.2.7 *Ist $K = \mathbb{Q}(\zeta_n)$, so ist $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. (Ohne Beweis.)*

Lemma 3.2.8 *Für jedes Element α eines Zahlkörpers K gibt es ein $d \in \mathbb{N}$ so dass $d \cdot \alpha \in \mathcal{O}_K$ ist.*

Lemma 3.2.9 *Sei K ein Zahlkörper vom Grad n, seien $\sigma_1, \ldots, \sigma_n$ alle Einbettungen von K nach $\mathbb{C}$. Dann ist das Bild von $\mathcal{O}_K$ unter der Abbildung $f\colon K \to \mathbb{C}^n, \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$ diskret, d. h. es gibt ein $\epsilon > 0$, so dass 0 das einzige Element $\alpha \in \mathcal{O}_K$ ist mit $|\sigma_1(\alpha)| < \epsilon, \ldots, |\sigma_n(\alpha)| < \epsilon$. (Hierbei bezeichnet $|\cdot|$ den komplexen Absolutbetrag.)*

Bemerkung: Ist $G \subset (\mathbb{R}^n, +)$ eine diskrete Untergruppe und $M \in \mathbb{R}$, so gibt es nur endlich viele $g \in G$ mit $\|g\| < M$.

Satz 3.2.10 *Ist K ein Zahlkörper vom Grad n, so ist $(\mathcal{O}_K, +) \cong \mathbb{Z}^n$.*

Lemma 3.2.11 (a) *Jede endlich erzeugte Untergruppe von $(\mathbb{Q}^n, +)$ ist isomorph zu $\mathbb{Z}^m$ für ein $m \leqslant n$.*
(b) *jede diskrete Untergruppe von $(\mathbb{R}^n, +)$ ist isomorph zu $\mathbb{Z}^m$ für ein $m \leqslant n$.*

3.3 Einheiten

Konvention: In dieser Vorlesung sind alle Ringe kommutativ und mit 1.

Erinnerung 3.3.1 *Ist R ein Ring, so bezeichnet $R^\times := \{u \in R \mid \exists u' \in R : uu' = 1\}$ die* ***Einheiten*** *in R.*

Lemma 3.3.2 *Ist $\mathcal{O}_K$ ein Zahlring, so ist $\alpha \in \mathcal{O}_K$ eine Einheit genau dann, wenn $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$ ist.*

Definition 3.3.3 *Sei K ein Zahlkörper und seien $\sigma_1, \ldots, \sigma_n\colon K \to \mathbb{C}$ die Einbettungen von K nach $\mathbb{C}$. Die* ***Signatur*** *eines Zahlkörpers K ist das Paar (r_1, r_2) mit:*

- *$r_1 :=$ Anzahl der j, so dass $\sigma_j(K) \subseteq \mathbb{R}$.*
- *$r_2 :=$ Hälfte der Anzahl der j, so dass $\sigma_j(K) \nsubseteq \mathbb{R}$.*

Bemerkung 3.3.4 *$r_2 \in \mathbb{Z}$, und $[K : \mathbb{Q}] = r_1 + 2r_2$.*

Satz 3.3.5 (Dirichletscher Einheitensatz) *Sei K ein Zahlkörper mit Signatur r_1, r_2; setze $r := r_1 + r_2 - 1$. Sei $\boldsymbol{\mu}_K = \{\zeta \in K \mid \exists n : \zeta^n = 1\}$ die Menge der Einheitswurzeln in K. Dann ist $\mathcal{O}_K^\times \cong \boldsymbol{\mu}_K \times \mathbb{Z}^r$; genauer: Es gibt Elemente $\epsilon_1, \ldots, \epsilon_r \in \mathcal{O}_K^\times$, so dass jede Einheit $\alpha \in \mathcal{O}_K^\times$ sich eindeutig schreiben lässt als $\alpha = \zeta \epsilon_1^{n_1} \cdots \epsilon_r^{n_r}$ für $\zeta \in \boldsymbol{\mu}_K$ und $n_i \in \mathbb{Z}$.*

Beispiel 3.3.6 *Sei $d \in \mathbb{Z}$ quadratfrei und $K = \mathbb{Q}(\sqrt{d})$.*

(a) *Ist $d > 0$, so gibt es ein $\epsilon = a + b\sqrt{d} \in \mathcal{O}_K^\times$ mit $\mathcal{O}_K^\times = \{\pm\epsilon^n \mid n \in \mathbb{Z}\}$.*
*Ein solches ϵ nennt man **Grundeinheit**. Es gibt vier Grundeinheiten: Ist ϵ eine davon, so sind alle Grundeinheiten $\pm\epsilon^{\pm 1}$.*

(b) *Ist $d < 0$, so ist*

$$\mathcal{O}_K^\times = \boldsymbol{\mu}_K = \begin{cases} \boldsymbol{\mu}_4 = \{\pm 1, \pm i\} & d = -1 \\ \boldsymbol{\mu}_6 & d = -3 \\ \boldsymbol{\mu}_2 = \{\pm 1\} & \text{sonst.} \end{cases}$$

Satz 3.3.7 *Sei $K = \mathbb{Q}(\sqrt{d})$ mit $d \geqslant 2$. Sei $b \in \mathbb{N}$ minimal, so dass eine der beiden Zahlen $\alpha_\pm = \sqrt{\frac{b^2}{4} \pm 1} + \frac{b}{2}$ in K liegt und > 1 ist. Dann ist dieses α_+ bzw. α_- eine Grundeinheit in $\mathcal{O}_K$.*

Satz 3.3.8 *Sei $d \geqslant 2$ quadratfrei. Die Lösungsmenge der diophantischen Gleichung $X^2 = dY^2 + 1$ (eine **Pellsche Gleichung**) ergibt sich wie folgt:*

(a) *Es gibt eine „**Grundlösung**“ $(a_1, b_1) \in \mathbb{Z}^2$.*
(b) *Die Menge aller Lösungen hat die Form $\{(\pm 1, 0), (\pm a_1, \pm b_1), (\pm a_2, \pm b_2), (\pm a_3, \pm b_3), \dots\}$, wobei $a_{n+1} = a_n a_1 + d b_n b_1$, $b_{n+1} = a_n b_1 + a_1 b_n$.*

3.4 Faktorielle Zahlringe

Erinnerung 3.4.1 *Sei R ein Ring (kommuatativ, mit 1) und seien $a, b \in R$.*

(a) *Wir sagen „a **teilt** b“ (Notation: $a \mid b$), wenn es ein $c \in R$ gibt mit $ac = b$; a heißt auch **Teiler** von b.*
(b) *Wir sagen „a und b sind **assoziiert**“, wenn es eine Einheit $u \in R^\times$ gibt mit $au = b$.*
(c) *Das Element a heißt **irreduzibel**, wenn a keine Einheit ist und wenn jeder Teiler von a entweder eine Einheit oder zu a assoziiert ist.*

Bemerkung 3.4.2 *Sei R ein Ring und seien $a, b, c \in R$. Dann gilt:*

(a) $a \mid b \implies a \mid bc$
(b) $a \mid b \wedge b \mid c \implies a \mid c$
(c) $a \mid b \iff ac \mid bc$
(d) $a \mid b \wedge a \mid c \implies a \mid (b + c)$
(e) *Ist R ein Zahlring, so gilt außerdem: a und b sind assoziiert genau dann, wenn sie die gleichen Teiler haben.*

Lemma 3.4.3 *Ist $\mathcal{O}_K$ ein Zahlring, so lässt sich jedes $\alpha \in \mathcal{O}_K$ als Produkt von einer Einheit und endlich vielen irreduziblen Elementen schreiben.*

Erinnerung 3.4.4 *Ein nullteilerfreier[1] Ring R heißt **faktoriell**, wenn jedes Element $a \in R\backslash\{0\}$ eine „eindeutige Primfaktorzerlegung hat“. Genauer:*

(a) *Es gibt $u, p_1, \dots, p_r$ mit $u \in R^\times$ und $u_j \in R$ irreduzibel, so dass $a = u \cdot p_1 \cdots p_r$.*
(b) *Sind $u', p_1', \dots, p_{r'}'$ auch wie in (a), so ist $r = r'$ und nach umnummerieren ist p_j' zu p_j assoziiert für $j = 1, \dots, r$.*

Beispiel 3.4.5 *$\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell.*

Satz 3.4.6 *Ein Zahlring $\mathcal{O}_K$ is faktoriell genau dann, wenn die folgende Eigenschaft gilt:*

[1] Ein Ring R heißt nullteilerfrei, wenn für alle $a, b \in R\backslash\{0\}$ gilt: $ab \neq 0$. Zahlringe sind immer nullteilerfrei.

(+) Zu beliebigen $\alpha_1, \alpha_2 \in R$ gibt es $\rho_1, \rho_2 \in \mathcal{O}_K$, so dass $\gamma := \alpha_1\rho_1 + \alpha_2\rho_2$ sowohl α_1 als auch α_2 teilt.

Definition 3.4.7 *Sei $\mathcal{O}_K$ ein Zahlring mit (+). Ein γ wie in Satz 3.4.6 nennen wir **größten gemeinsamen Teiler** von α_1 und α_2. Notation dafür: $\mathrm{ggT}(\alpha_1, \alpha_2)$; dies ist allerdings nur wohldefiniert bis auf Assoziiertheit (siehe nächstes Lemma). Ist $\mathrm{ggT}(\alpha_1, \alpha_2)$ eine Einheit, so nennt man α_1 und α_2 **teilerfremd**.*

Lemma 3.4.8 *Sei $\mathcal{O}_K$ ein Zahlring mit der Eigenschaft (+) und seien $\alpha_1, \alpha_2, \beta \in \mathcal{O}_K$.*

(a) *Ist γ ein größter gemeinsamen Teiler von α_1 und α_2, so sind die Teiler von γ genau die gemeinsamen Teiler von α_1 und α_2 (also: $\delta \mid \gamma \iff \delta \mid \alpha_1 \wedge \delta \mid \alpha_2$).*
Insbesondere ist jeder weitere größte gemeinsame Teiler von α_1 und α_2 zu γ assoziiert.

(b) $\mathrm{ggT}(\alpha_1\alpha_2, \beta) \mid \mathrm{ggT}(\alpha_1, \beta) \cdot \mathrm{ggT}(\alpha_2, \beta)$.
Insbesondere: Wenn β teilerfremd zu α_1 und zu α_2 ist, dann auch zu $\alpha_1 \cdot \alpha_2$.

Lemma 3.4.9 *Sei $\mathcal{O}_K$ ein Zahlring und $\alpha \in \mathcal{O}_K$ belieibig. Dann ist $\mathcal{O}_K/\alpha\mathcal{O}_K$ endlich.*

Definition 3.4.10 *Ein Zahlring $\mathcal{O}_K$ heißt **norm-euklidisch**, wenn es zu jedem α und β ein γ und ein ρ gibt mit $|\mathrm{N}_{K/\mathbb{Q}}(\rho)| < |\mathrm{N}_{K/\mathbb{Q}}(\beta)|$ und $\alpha = \gamma\beta + \rho$.*

Satz 3.4.11 *Jeder norm-euklidische Zahlring erfüllt (+).*

Bemerkung 3.4.12 *$\mathcal{O}_K$ ist norm-euklidisch genau dann wenn es zu jedem $\alpha \in K$ ein $\gamma \in \mathcal{O}_K$ gibt mit $|\mathrm{N}_{K/\mathbb{Q}}(\alpha - \gamma)| < 1$.*

Beispiel 3.4.13 *$\mathbb{Z}[\sqrt{-d}]$ ist faktoriell für $d = 1, 2, 3$.*

Beispiel 3.4.14 *$\mathbb{Z}[\sqrt{d}]$ ist faktoriell für $d = 2, 3, 5, 6, 7$.*

3.5 Zerlegung von Primzahlen in Zahlringen

Im folgenden sei $\mathcal{O}_K$ ein faktorieller Zahlring.

Lemma 3.5.1 *Zu jedem jedem irreduziblen Element $\pi \in \mathcal{O}_K$ gibt es eine Primzahl $p \in \mathbb{N}$ mit $\pi \mid p$.*

Lemma 3.5.2 *Jede Primzahl $p \in \mathbb{N}$ zerfällt in $\mathcal{O}_K$ in ein Produkt von maximal $n = [K : \mathbb{Q}]$ vielen (nicht notwendigerweise verschiedenen) irreduziblen Elementen.*

Lemma 3.5.3 *Wir nehmen an, dass $\mathcal{O}_K = \mathbb{Z}[\omega]$ ist für ein $\omega \in \mathcal{O}_K$. Sei $p \in \mathbb{P}$. Dann lässt sich die Zerlegung von p in irreduzible Faktoren in $\mathcal{O}_K$ wie folgt bestimmen:*

Ist $g \in \mathbb{Z}[X]$, so schreiben wir $\bar{g} := \underline{f} \pmod p \in \mathbb{F}_p[X]$. Sei $f = \mathrm{MiPo}_\omega \in \mathbb{Z}[X]$, und seien $f_1, \ldots, f_k \in \mathbb{Z}[X]$ so, dass $\bar{f} = \bar{f}_1 \cdots \bar{f}_k$ die Zerlegung von $\bar{f}$ in irreduzible Faktoren (in $\mathbb{F}_p[X]$) ist.

Setze $\pi_j := \mathrm{ggT}(f_j(\omega), p)$. Dann sind diese π_j irreduzibel, und es gilt: $p = \pi_1 \cdots \pi_k$ (evtl. bis auf einen Faktor aus $\mathcal{O}_K^\times$).

Satz 3.5.4 *Eine Primzahl p lässt sich als Summe von zwei Quadraten schreiben genau dann, wenn $p \not\equiv 3 \mod 4$.*

Definition 3.5.5 *Sei $\mathcal{O}_K$ ein beliebiger Zahlring mit $[K:\mathbb{Q}] = n$, seien $\sigma_1, \dots, \sigma_n \colon K \to \mathbb{C}$ die Einbettungen und seien $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ Erzeuger von $(\mathcal{O}_K, +)$, d. h. $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Dann definiert man die* ***Diskriminante*** *von $\mathcal{O}_K$ durch*

$$\Delta_K = \det(\sigma_j(\alpha_k)_{j,k})^2.$$

Satz 3.5.6 (a) *Δ_K hängt nicht von der Wahl der $\alpha_1, \dots, \alpha_n$ ab.*
(b) *$\Delta_K \in \mathbb{Z}$*
(c) *Ist $\mathcal{O}_K = \mathbb{Z}[\omega]$, so ist*

$$\Delta_K = \prod_{1 \leqslant j < j' \leqslant n} (\sigma_j(\omega) - \sigma_{j'}(\omega))^2.$$

Beispiel 3.5.7 *Ist $K = \mathbb{Q}(\sqrt{d})$, mit d quadratfrei und $\neq 0, \pm 1$, so ist*

$$\Delta_K = \begin{cases} 4d & \text{falls } d \not\equiv 1 \mod 4 \\ d & \text{falls } d \equiv 1 \mod 4. \end{cases}$$

Satz 3.5.8 *Sei p eine Primzahl und sei $p = \pi_1^{r_1} \cdots \pi_k^{r_k} \cdot \epsilon$ die Zerlegung in irreduzible Faktoren in $\mathcal{O}_K$ (mit π_j paarweise nicht assoziiert und $\epsilon \in \mathcal{O}_K^\times$). Dann gibt es j mit $r_j > 1$ genau dann, wenn $p \mid \Delta_K$.*

Satz 3.5.9 *Sei $K = \mathbb{Q}(\sqrt{d})$, mit d quadratfrei und $\neq 0, 1$, und sei $p \in \mathbb{N}$ prim, $p \geqslant 3$. Dann gilt:*

(a) *p ist irreduzibel in $\mathcal{O}_K$ genau dann wenn $\left(\frac{\Delta_K}{p}\right) = -1$.*
(b) *$p = \pi^2 \cdot \epsilon$ für ein irreduzibles $\pi \in \mathcal{O}_K$ (und $\epsilon \in \mathcal{O}_K^\times$) genau dann wenn $\left(\frac{\Delta_K}{p}\right) = 0$.*
(c) *$p = \pi_1 \cdot \pi_2$ für zwei nicht-assoziierte irreduzible $\pi_1, \pi_2 \in \mathcal{O}_K$ genau dann wenn $\left(\frac{\Delta_K}{p}\right) = 1$.*