Elementare Zahlentheorie - Formelsammlung

von Julian Merkert, Skript Dr. Kühnlein

Teilbarkeit und Primzahlen

Aufbau des Zahlensystems

Natürliche Zahlen: $\mathbb{N} = \{1, 2, 3, ...\}$

Natürliche Zahlen mit Null: $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$

Konstruktion der ganzen Zahlen: betrachte Äquivalenzrelation $(a, b) \sim (c, d) :\Leftrightarrow a+d = c+b$ und setze $\mathbb{Z} := \mathbb{N}_0^2/_\sim$

Multiplikation der ganzen Zahlen: Definiere $(a - b) \cdot (c - d) := (ac + bd) - (ad + bc)$

Konstruktion der rationalen Zahlen: betrachte Äquivalenzrel. $(z, n) \sim (w, m) :\Leftrightarrow zm = wn$, setze $\mathbb{Q} := (\mathbb{Z} \times \mathbb{N})/_\sim$

Konstruktion der reellen Zahlen:

1. Statte die rationalen Zahlen mit einer Abstandsfunktion $d(x, y) := |x - y|$ aus
2. Cauchy-Folge in $\mathbb{Q}$: $(x_n)_{n\in\mathbb{N}}$ mit: $\forall\ n, m > N : |x_n - x_m| < \frac{1}{k}$
3. Grenzwerte aller rationalen Cauchy-Folgen mit dazunehmen $\Rightarrow$ reelle Zahlen $\mathbb{R}$

Teilbarkeit

Teiler von $n \in \mathbb{N}$: $d \in \mathbb{N}$, falls ein $t \in \mathbb{N}$ existiert mit $d \cdot t = n$

Teilerfremdheit von $m, n \in \mathbb{N}$: 1 ist der einzige gemeinsame Teiler von n und m

Größter gemeinsamer Teiler von $n, m \in \mathbb{N}$: größtes Element der Menge aller gemeinsamen Teiler von n und m

Kleinstes gemeinsames Vielfaches von $n, m \in \mathbb{N}$: kleinstes Element der Menge aller Vielfachen von n und m

Hilfssatz (Euklidischer Algorithmus): Es seien $a, b \in \mathbb{N}$ gegeben. Dann gibt es $c, d \in \mathbb{Z}$, so dass $ac+bd = \text{ggT}(a, b)$.

Euklidischer Algorithmus:

1. Setze $a_0 := b,\ a_1 := a$
2. Wähle $k_1 := \max\{k \in \mathbb{N}_0 \mid ka_1 \leq a_0\}$
3. Berechne $a_2 := a_0 - k_1a_1$
4. Wiederhole 2. und 3. so lange, bis $a_i = 0$ ist.

Folgerung: Wenn $g = \text{ggT}(a, b)$ gilt, dann sind die natürlichen Zahlen $\frac{a}{g}$ und $\frac{b}{g}$ teilerfremd.

Gekürzte Brüche: Jede rationale Zahl q lässt sich auf genau eine Art als $q = \frac{z}{n},\ z \in \mathbb{Z}, n \in \mathbb{N}$ schreiben, wobei entweder $z = 0,\ n = 1$ gilt oder $|z|$ und n teilerfremd sind.

Teilbarkeit im kommutativen Ring R: $a \in R$ heißt **Teiler** von $b \in R$, falls ein $c \in R$ existiert, sodass $b = c \cdot a$.

Einheitengruppe: $R^\times = \{a \in R \mid\ \exists\ b \in R :\ a \cdot b = 1\}$

Assoziiertheit zweier Elemente $a, b \in R$: es existiert eine Einheit $e \in R^\times$, sodass $b = a \cdot e$

Größter gemeinsamer Teiler von $a, b \in R$ (R kommutativ und nullteilerfrei): $g \in R$ mit g ist gemeinsamer Teiler und jeder gemeinsame Teiler von a und b teilt auch g

Teilerfremdheit von $a, b \in R$: die einzigen gemeinsamen Teiler sind die Einheiten in R

Idealisierung: Wenn es ein $g \in R$ gibt, sodass $\{ax + by \mid x, y \in R\} = Rg := \{rg \mid r \in R\}$ gilt, dann ist g ein ggT von a und b

Ideal: $I \subseteq R$ mit...

(i) $0 \in I$

(ii) I ist unter Addition abgeschlossen

(iii) $\forall\, r \in R,\ i \in I:\ ri \in I$

Hauptideal: $I \subseteq R$ mit: es existiert ein $g \in R$, so dass $I = Rg$ gilt

Erzeuger von I: g mit $I = Rg$

Hauptidealring: nullteilerfreier, kommutativer Ring, in dem jedes Ideal ein Hauptideal ist

Euklidischer Ring (bezüglich $\varphi : R \to \mathbb{N}_0$): R nullteilerfrei, kommutativ und es gelten:

(i) $\varphi(r) = 0 \Leftrightarrow r = 0$

(ii) $\forall\, a, b \in R,\ b \neq 0$ gibt es ein $c \in R$, sodass $\varphi(a - bc) < \varphi(b)$

Primzahlen

Primzahl: natürliche Zahl $p > 1$, die sich nicht als Produkt zweier kleinerer natürlicher Zahlen schreiben lässt

Menge der Primzahlen: $\mathbb{P} = \{n \in \mathbb{N} \mid n > 1 \text{ und } \forall\, d, t < n:\ d \cdot t \neq n\} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...\}$

Primzahl (alternative Charakterisierung): natürliche Zahl $n > 1$ mit: für jedes Produkt $a \cdot b,\ a, b \in \mathbb{N}$ gilt: n teilt $ab :\Leftrightarrow n$ teilt a oder n teilt b

Fundamentalsatz der Arithmetik: Jede natürliche Zahl n lässt sich als Produkt von Primzahlen schreiben. Diese Darstellung ist eindeutig, wenn die Primfaktoren der Größe nach sortiert werden.

p-adische Bewertung von $p \in \mathbb{P}$: für jede ganze Zahl $k \neq 0$ existiert $v_p(k) \in \mathbb{N}_0$ mit: $p^{v_p(k)}$ ist ein Teiler von k, aber $p^{v_p(k)+1}$ nicht.

- $k = \pm \prod_{p \in \mathbb{P}} p^{v_p(k)}$
- $v_p(k + l) \geq \min\{v_p(k), v_p(l)\}$
- $v_p(k \cdot l) = v_p(k) + v_p(l)$
- b teilt a genau dann, wenn $v_p(b) \leq v_p(a)$
- Der ggT von $a, b \in \mathbb{N}$ ist $g = \prod_{p \in \mathbb{P}} p^{e_p}$ mit $e_p = \min\{v_p(a), v_p(b)\}$
- Das kgV von $a, b \in \mathbb{N}$ ist $k = \prod_{p \in \mathbb{P}} p^{f_p}$ mit $f_p = \max\{v_p(a), v_p(b)\}$

Irreduzibilität von $m \in R$: $m \notin R^\times$ und $\forall\, a, b \in R:\ m = ab \Rightarrow a \in R^\times$ oder $b \in R^\times$

Primelement: $p \in R$ mit: p ist keine Einheit und $\forall\, a, b \in R$ gilt: p teilt $ab \Rightarrow p$ teilt a oder p teilt b

- Ein von 0 verschiedenes Primelement ist immer irreduzibel
- Wenn R ein Hauptidealring ist, dann ist ein irreduzibles Element in R immer auch prim

Primzerlegung in Hauptidealringen ($\cong$ Fundamentalsatz der Arithmetik für Hauptidealringe): Es sei R ein Hauptidealring. Weiter sei $\mathbb{P}_R$ ein Vertretersystem der Assoziiertenklassen von Primelementen $\neq 0$. Dann ist jedes $r \in R \setminus \{0\}$ assoziiert zu einem Produkt von endlich vielen Primelementen.
Sind weiter $s, t \in \mathbb{N}_0$ und $p_1, ..., p_s, q_1, ..., q_t \in \mathbb{P}_R$ derart, dass eine Einheit $e \in R^\times$ existiert mit $r = p_1 \cdot ... \cdot p_s = \varepsilon \cdot q_1 \cdot ... \cdot q_t$, so gelten $\varepsilon = 1,\ s = t$ und (bis auf Vertauschung de Reihenfolge der Faktoren $p_i = q_i$ für alle $1 \leq i \leq s$).

Hilfssatz: Es sei p eine Primzahl, die bei Division durch 4 Rest 1 lässt. Dann gibt es eine Zahl $u \in \{1, ..., p - 1\}$, sodass p ein Teiler von $u^2 + 1$ ist.

Summen zweier Quadrate: Eine natürliche Zahl n ist genau dann als Summe zweier Quadrate von ganzen Zahlen schreibbar, wenn für alle Primzahlen $p \in \mathbb{P}$, die bei Division durch 4 Rest 3 lassen, gilt, dass $v_p(n)$ gerade ist.

Zur Verteilung der Primzahlen

Euklid: Es gibt unendlich viele Primzahlen

Lücken: Es sei $k \in \mathbb{N}$. Dann gibt es eine natürliche Zahl M, so dass zwischen M und $M+k$ keine Primzahl liegt.

Eulerabschätzung: Für jede reelle Zahl $x > 1$ gilt $\sum_{x \geq p \in \mathbb{P}} \frac{1}{p} \geq \log(\log x) - \log 2$

Sieb des Erastothenes (erstellt Liste an Primzahlen)

1. Es sei $M \in \mathbb{N}$ eine natürliche Zahl. Betrachte $S_1 := \{n \in \mathbb{N} \mid 2 \leq n \leq M\}$
2. Die kleinste Zahl von S_1 ist $p_1 := 2$, eine Primzahl. Setze $S_2 := \{n \in S_1 \mid p_1 \text{ teilt nicht } n\}$
3. Das sind die Zahlen aus S_1, die keine Vielfachen von 2 oder 3 sind. Mache sukzessive so weiter: setze $p_i := \min(S_i)$, solange dies nicht leer ist. Dann ist p_i eine Primzahl, sonst wäre es vorher schon als Vielfaches einer kleinere Zahl gestrichen worden. Setze weiter $S_{i+1} := \{n \in S_i \mid p_i \text{ teilt nicht } n\}$
4. Wenn schließlich S_{i+1} leer ist, dann gilt: $\{p_1, p_2, ..., p_i\} = S_1 \cap \mathbb{P} = \{p \in \mathbb{P} \mid p \leq M\}$

Verteilungsfunktion (zählt alle Primzahlen unterhalb x): $\pi(x) := \#\{p \in \mathbb{P} \mid p \leq x\}$

Primzahlsatz: Es gilt $\lim_{x\to\infty} \pi(x) = \infty$, insbesondere $\lim_{x\to\infty} \pi(x) \cdot \frac{\log x}{x} = 1$

Arithmetische Funktion: Abbildung $\varphi : \mathbb{N} \to \mathbb{C}$

Faltung: $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A},\ (\varphi * \psi)(n) := \sum_{d|n} \varphi(d) \cdot \psi(n/d)$

Strikte Multiplikativität einer arithmetischen Funktion: $\varphi(1) = 1$ und $\forall\, m, n \in \mathbb{N} : \varphi(mn) = \varphi(m) \cdot \varphi(n)$

Multiplikativität einer arithmetischen Funktion: $\varphi(1) = 1$ und $\forall\, m, n \in \mathbb{N} :\ \mathrm{ggT}(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)$

Formale Dirichletreihe: $D(\varphi, s) := \sum_{n\in\mathbb{N}} \frac{\varphi(n)}{n^s}$

- Beispiel: Riemann'sche Zetafunktion $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$
- Für zwei arithemtische Funktionen φ, ψ gilt: $D(\varphi, s) \cdot D(\psi, s) = \sum_{m,n\in\mathbb{N}} \frac{\varphi(n)\cdot\psi(m)}{n^s m^s} = D(\varphi * \psi, s)$

p-Anteil von φ: $\varphi_p(n) = \begin{cases} \varphi(n) & \text{falls } n = p^k,\ k \in \mathbb{N}_0 \\ 0 & \text{sonst} \end{cases}$

Primzahlzwillingsvermutung: es gibt unendlich viele Primzahlen p, für die auch $p+2$ eine Primzahl ist

Goldbach-Vermutung: Jede gerade natürliche Zahl ≥ 4 lässt sich als Summe zweier Primzahlen schreiben

Gleichungssysteme

(ℤ-)Basis von A abelsche Gruppe: $B \subseteq A$ mit: jedes $a \in A$ lässt sich als $a = \sum_{b\in B} \lambda_b \cdot b$ schreiben

- $\lambda_b \in \mathbb{Z}$, fast alle $\lambda_b = 0$ (d.h. alle bis auf endlich viele)

Freie abelsche Gruppe über B: A abelsche Gruppe mit Basis B

Unimodulare Matrix: $M \in \mathbb{Z}^{n\times n}$, für die eine der folgenden äquivalenten Aussagen gilt:

- Die Spalten von M bilden eine Basis von $\mathbb{Z}^n$
- Es gibt eine zu M inverse Matrix mit ganzzahligen Einträgen
- $\det(M) = \pm 1$

Inhalt von $v \in \mathbb{Z}^n$: ggT der Einträge von v

Primitiver Vektor: Vektor mit Inhalt 1

Basisergänzung: Ein Vektor $v \in \mathbb{Z}^n$ ist genau dann ein Element einer Basis von $\mathbb{Z}^n$, wenn $\mathrm{Inh}(v) = 1$

Elementarteilersatz: Es seien F eine freie abelsche Gruppe vom Rang n und $U \subseteq F$ eine Untergruppe vom Rang n. Dann gibt es eine Basis $\{b_1, ..., b_n\}$ von F und natürliche Zahlen $e_1|e_2|...|e_r$, sodass $\{e_1 b_1, e_2 b_2, ..., e_r b_r\}$ eine Basis von U ist.

Matrixversion des Elementarteilersatzes: Es sei $M \in \mathbb{Z}^{n \times m}$ eine ganzzahlige Matrix. Dann gibt es unimodulare Matrizen $S \in GL_n(\mathbb{Z}),\ T \in GL_m(\mathbb{Z})$, sodass $S^{-1}MT = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix},\ D := diag(e_1, ..., e_r),\ e_1|e_2|...|e_r \neq 0$

Diophantische Gleichungen (Polynom-Gleichungssysteme): $P_i(x_1, ..., x_n) = 0,\ 1 \leq i \leq m,\ P_1, ..., P_m \in \mathbb{Z}[X_1, ..., X_n]$

Schinzels Hypothese: Sind $P_1, ..., P_m \in \mathbb{Z}[X]$ (nichtkonstante) irreduzible Polynome in einer Variablen mit positiven Leitkoeffizienten, sodass keine Primzahl p alle Werte $P_1(k) \cdot ... \cdot P_m(k),\ k \in \mathbb{Z}$ teilt, dann gibt es unendlich viele $k \in \mathbb{Z}$, sodass alle Werte $P_1(k), ..., P_m(k)$ Primzahlen sind.

Pythagoräisches Tripel: von $(0,0,0)$ verschiedenes Tripel $(a,b,c) \in \mathbb{Z}^3$ mit $a^2 + b^2 = c^2$

Kongruenzrechnung

Die Restklassenringe

Kongruenz modulo U von $a, b \in A$ (A abelsche Gruppe, $U \subseteq A$ Untergruppe): $a - b \in U$

- In Zeichen: $a \equiv b \mod U$

Addition von Restklassen: $(a + U) + (b + U) = (a + b) + U$

Homomorphiesatz: Wenn A, B zwei (abelsche) Gruppen sind und $\Phi : A \to B$ ein Homomorphismus, dann induziert Φ einen Isomorphismus zwischen $A/\text{Kern}(\Phi)$ und $\text{Bild}(\Phi)$. Dieser kommt durch $(\tilde{\Phi}(a + \text{Kern}(\Phi)) := \Phi(a)$ zustande.

Index von U in A ($U \subseteq A$ abelsche Gruppen): Kardinalität von U/A

Erzeugnis von $S \subseteq U$: U, wenn jedes Element von U eine ganzzahlige Linearkombination von Elementen aus S ist

- U heißt **endlich erzeugt**, wenn es ein endliches Erzeugendensystem gibt
- U heißt **zyklisch**, wenn sie von einem einzigen Element erzeugt wird

Ordnung von $a \in A$: kleinste natürliche Zahl d mit $da = 0$ (bzw. $a^d = 1$ in multiplik. Notation)

Elementarteilersatz: Es sei F eine frei abelsche Gruppe von Rang n und $U \subseteq F$ eine Untergruppe von endlichem Index. Dann hat U Rang n und $(F : U)$ ist das Produkt der Elementarteiler von U in F.

Lagrange-Satz für abelsche Gruppen

a) Es sei A eine (additiv geschriebene) endliche abelsche Gruppe und $a \in A$. Dann gilt: $|A| \cdot a = 0$

b) Die Ordnung d von a ist ein Teiler von $|A|$.

Kleiner Satz von Fermat (abstrakt): Wenn F ein endlicher Körper mit q Elementen ist, dann gilt für jedes $a \in F^\times :\ a^{q-1} = 1$

Restklassenring: R/I mit R kommutativer Ring, $I \subseteq R$ Ideal und $(a + I) \cdot (b + I) := (ab) + I$

Homomorphiesatz: Sind R, S zwei kommutative Ringe und ist $\Phi : R \to S$ ein Ringhomomorphismus, so liefert Φ einen Isomorphismus zwischen den Ringen $R/\text{Kern}(\Phi)$ und $\text{Bild}(\Phi)$.

Die Einheitengruppe - kleiner Fermat konkret

a) Es seien R ein kommutativer Ring und $I \subseteq R$. Dann ist $r + I$ genau dann eine Einheit von R/I, wenn es ein $s \in R$ gibt mit $rs - 1 \in I$.

b) Ist R ein Hauptidealring und $I = Rm,\ m \in R$, dann ist für $r \in R$ die Restklasse $r + 1$ genau dann in R/I invertierbar, wenn r und m teilerfremd sind.

c) Ist R ein Hauptidealring und $I = Rm,\ m \in R$, dann ist R/I genau dann ein Körper, wenn m irreduzibel ist.

d) Für $N \in \mathbb{N}$ ist $(\mathbb{Z}/N\mathbb{Z})^\times = \{r + N\mathbb{Z} \mid 0 \leq r \leq N - 1,\ \text{ggT}(r, N) = 1\}$. $\mathbb{Z}/N\mathbb{Z}$ ist genau dann ein Körper, wenn N eine Primzahl ist.

e) Ist $p \in \mathbb{P}$, so gilt für alle $a \in \mathbb{Z}$: $p | a^p - a$

Prime Restklassengruppe modulo $N \in \mathbb{N}$ = Einheitengruppe $(\mathbb{Z}/N\mathbb{Z})^\times$

$\mathbb{F}_p$: andere Schreibweise für $\mathbb{Z}/p\mathbb{Z}$, falls p eine Primzahl ist

Euler'sche φ-Funktion: $\varphi(N) := |(\mathbb{Z}/N\mathbb{Z})^\times|$

- $\varphi(N) = |\{x \in \mathbb{N} \mid x \leq N,\ \mathrm{ggT}(x, N) = 1\}|$
- Für eine Primzahl p gilt nach dem kleinen Fermat: $\varphi(p) = p - 1$
- Für Potenzen p^e (mit $e \geq 1$) von p gilt $\varphi(p^e) = p^{e-1}(p-1)$
- Man sieht schnell, dass $\varphi(N)$ genau die Anzahl der Elemente von Ordnung N in $\mathbb{Z}/N\mathbb{Z}$ ist.

Primzahltest: Kriterium dafür, dass eine gegebene Zahl n keine Primzahl ist: ist für eine Zahl $a \in \mathbb{Z}$, die zu n teilerfremd ist, die Kongruenz $a^{n-1} \equiv 1 \mod n$ nicht erfüllt, dann ist n sicher keine Primzahl.

Chinesischer Restsatz: Es seien N, M zwei teilerfremde Zahlen. Dann gelten die folgenden Aussagen:

a) Die Ringe $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ (mit komponentenweiser Addition und Multiplikation) und $\mathbb{Z}/(MN\mathbb{Z})$ sind isomorph.

b) Für je zwei Zahlen $a, b \in \mathbb{Z}$ gibt es eine ganze Zahl x, sodass simultan $x \equiv a \mod M$ und $x \equiv b \mod N$ gilt. Zwei Lösungen x und $\tilde{x}$ dieser Kongruenzbedingung sind kongruent modulo MN.

Folgerung: φ ist multiplikativ und für zwei Primzahlen $p \neq q$ und $k \in \mathbb{N}$: gilt: $\forall\, a \in \mathbb{Z} : a^{k(p-1)(q-1)+1} \equiv a \mod pq$

Endliche Körper

Endlicher Körper: Körper F mit $q = |F|$

- Die Ordnung von 1_F in der additiven Gruppe von F ist eine Primzahl p, und $\mathbb{Z}/p\mathbb{Z}$ ist ein Teilring von F.
- Die Kardinalität von F ist eine Potenz von p
- Die Einheitengruppe von F ist zyklisch
- F ist ein Restklassenkörper des Polynomrings $\mathbb{F}_p[X]$

Charakteristik von F = additive Ordnung von 1, wenn diese endlich (und damit eine Primzahl) ist, ansonsten 0

Primitives Element: $\xi \in F^\times$, das die Einheitengruppe erzeugt

Minimalpolynom von ξ über $\mathbb{F}_p$ = normierter Erzeuger m des Kerns von Φ

Zyklizität der Einheitengruppe von $R := \mathbb{Z}/p^m\mathbb{Z}$: $p \geq 3$ und $m \in \mathbb{N}$

Kreisteilungspolynom: $\Phi_N := \prod^*_{k \mod N}(X - c_k)$

- Das Produkt (mit Sternchen) läuft nur noch über die zu N teilerfremden k
- Hergeleitet aus dem Polynom $F_N = X^N - 1$, dessen komplexe Nullstellen $c_k := \cos\left(\frac{2\pi k}{N}\right) + i \sin\left(\frac{2\pi k}{N}\right)\big)$, $1 \leq k \leq N$ sind.
- rekursive Formel: $\Phi_1 = X - 1,\ \Phi_N = (X^N - 1) : (\prod_{d|N,\ d<N} \Phi_d)$

Nullstellen des Kreisteilungspolynoms: Es sei k ein Körper, dessen Charakteristik kein Teiler von $N \in \mathbb{N}$ ist. Dann sind äquivalent:

(i) In $K^\times$ liegt ein Element der Ordnung N

(ii) In K gibt es eine Nullstelle des Kreisteilungspolynoms Φ_N.

Spezialfall von Dirichlets Primzahlsatz: Es sei $N \in \mathbb{N}$ beliebig. Dann gibt es unendlich viele Primzahlen $p \equiv 1 \mod N$.

Alle endlichen Körper: Es sei p eine Primzahl und $e \in \mathbb{N}$. Dann gibt es einen Körper mit p^e Elementen und je zwei solche Körper sind zueinander isomorph.

Quadratische Reste

Quadrat: $a \in F^\times$ mit: $\exists\, b \in F :\ b^2 = a$

Menge der Quadrate: Bild von $Q : F^\times \to F^\times,\ b \mapsto b^2$ (Q ist ein Gruppenhom.)

Legendre-Symbol ($a \in \mathbb{Z},\ p \in \mathbb{P},\ p > 3$): $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p|a \\ 1 & \text{falls } \exists\, x \in \mathbb{Z}\backslash p\mathbb{Z} :\ a \equiv x^2 \mod p \\ -1 & \text{sonst} \end{cases}$

Legendre-Symbol für einen endlichen Körper F mit ungerader Charakteristik: $\left(\frac{a}{F}\right) = \begin{cases} 0 & \text{falls } a = 0 \\ 1 & \text{falls } a \in Q(F^\times) \\ -1 & \text{sonst} \end{cases}$

Satz von Euler

a) Es sei F ein endlicher Körper mit ungerader Charakteristik und q Elementen. Dann gilt für $a \in F$: $\left(\frac{a}{F}\right) = a^{\frac{q-1}{2}}$

b) Analog gilt für eine ungerade Primzahl p und $a \in \mathbb{Z}$: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$

c) Die Abbildung $\left(\frac{\cdot}{F}\right) : F^\times \to \{\pm 1\}$ ist ein Gruppenhomomorphismus

d) Die Abbildung $\left(\frac{\cdot}{F}\right) : \mathbb{Z} \to \{0, \pm 1\}$ ist strikt multiplikativ

Halbsystem: $H \subseteq F^\times$ mit $H \cap (-H) \neq \emptyset$ und $F^\times = H \cup (-H)$

- F: endlicher Körper von ungerade Charakteristik p mit q Elementen

Fehlstandszahl von a bezüglich H: $F(a, H) := \frac{q-1}{2} - |H \cap (aH)|$

Satz von Gauß: Es seien F ein endlicher Körper ungerader Charakteristik, $H \subset F^\times$ ein Halbsystem in F und $a \in F^\times$. Dann gilt: $\left(\frac{a}{F}\right) = (-1)^{F(a,H)}$

Quadratisches Reziprozitätsgesetz: Es seien $p \neq l$ zwei ungerade Primzahlen. Dann gilt: $\left(\frac{p}{l}\right) \cdot \left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}}$

- Ergänzung 1: $\forall\ 2 \neq p \in \mathbb{P} :\ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \mod 4 \\ -1 & \text{falls } p \equiv 3 \mod 4 \end{cases}$
- Ergänzung 2: für eine Primzahl $p \geq 3$ gilt: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \mod 8 \\ -1 & \text{falls } p \equiv \pm 3 \mod 8 \end{cases}$

Quadratische Zahlkörper

Der Ganzheitsring

Quadratischer Zahlkörper: Körper $K \subseteq \mathbb{C}$, wenn er als Vektorraum über $\mathbb{Q}$ Dimension 2 hat.

- Es gibt genau eine quadratfreie Zahl $d \in \mathbb{Z}$, sodass $K = \mathbb{Q}(\sqrt{d}) := \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\}$
- Ist umgekehrt $d \neq 1$ eine quadratfreie ganze Zahl, dann ist $\mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper

Reellquadratischer Zahlkörper: $K = \mathbb{Q}(\sqrt{d})$ mit $d > 0$

Imaginärquadratischer Zahlkörper: $K = \mathbb{Q}(\sqrt{d})$ mit $d \leq 0$

Automorphismus in $K = \mathbb{Q}(\sqrt{d})$: $\kappa : K \to K,\ \kappa(a + b\sqrt{d}) = a - b\sqrt{d}$

Norm $N(\alpha)$ ($\alpha \in K$): Determinante der Abbildung $\mu : K \to K,\ \mu(x) := \alpha \cdot x$

- $N(\alpha) = a^2 - db^2$ für $a\alpha = a + b\sqrt{d}$ bzw. $N(\alpha) = \alpha \cdot \kappa(\alpha)$

Spur $Sp(\alpha)$ ($\alpha \in K$): Spur der Abbildung $\mu : K \to K,\ \mu(x) := \alpha \cdot x$

- $Sp(\alpha) = 2a$ für $\alpha = a + b\sqrt{d}$ bzw. $Sp(\alpha) = \alpha + \kappa(\alpha)$

Ganzheit über $\mathbb{Z}$ von $\alpha \in \mathbb{C}$: $\alpha \in \mathbb{C}$, das Nullstelle eines ganzzahligen normierten Polynoms ist

Ganzheitsring $\mathcal{O}_K$ eines quadratischen Zahlkörpers $K \subseteq \mathbb{C}$: Menge aller über $\mathbb{Z}$ ganzen Elemente in K

- Für $K = \mathbb{Q}(\sqrt{d})$: $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}_{\omega_d}$ mit $\omega_d := \begin{cases} \sqrt{d} & d \not\equiv 1 \mod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \end{cases}$

Diskriminante von $K = \mathbb{Q}(\sqrt{d})$: $D_K := (\omega_d - \kappa(\omega_d))^2 = \begin{cases} 4d & d \not\equiv 1 \mod 4 \\ d & d \equiv 1 \mod 4 \end{cases}$

Primideal: $I \subseteq R$ Ideal mit $I \neq R$ und $\forall\, x, y \in R :\ x \cdot y \in I \Rightarrow x \in I$ oder $y \in I$

- Ist $P \subseteq \mathcal{O}_K$ ein von $\{0\}$ verschiedenes Primideal, so enthält P genau eine Primzahl
- Ist $p \in \mathbb{P}$ eine Primzahl, so liegt es in ein oder zwei Primidealen in $\mathcal{O}_K$.

Spektrum von R: Menge aller Primideale von R

Geometrie der Zahlen

Gitter: Untergruppe Γ eines reellen, endlichdimensionalen Vektorraums V, die von einer $\mathbb{R}$-Basis von V erzeugt wird

Fundamentalmasche von Γ in V: $\mathcal{F}_B := \{\sum_{i=1}^{n} a_i b_i \mid 0 \leq a_i \leq 1\}$

- $B = \{b_1, ..., b_n\}$: Basis, die das Gitter erzeugt

Kovolumen von Γ: Volumen von $\mathcal{F}_B$, falls V euklidisch

Gitterpunktsatz von Minkowski: Im euklidischen Vektorraum E sei ein Gitter Γ von Kovolumen V gegeben. Weiter sei $S \subseteq E$ eine konvexe, kompakte Menge mit $S = -S$ und Volumen $vol(S) > 2^n \cdot V$. Dann liegt in $S \cap \gamma$ mindestens ein Element $\neq 0$.

Vierquadratesatz von Lagrange: Jede natürliche Zahl lässt sich als Summe von vier Quadratzahlen schreiben

Spezialfall von Dirichlets Einheitensatz: Es sei K ein reellquadratischer Zahlkörper. Dann gibt es eine Einheit $\varepsilon \in \mathcal{O}_K^\times,\ \varepsilon \neq \pm 1$, so dass $\mathcal{O}_K^\times = \{\pm\varepsilon^a \mid a \in \mathbb{Z}\} \cong \{\pm 1\} \times \mathbb{Z}$

Pellsche Gleichung: Es sei $d \in \mathbb{N}$ keine Quadratzahl. Dann hat die Gleichung $x^2 - dy^2 = 1$ unendlich viele Lösungen $(x, y) \in \mathbb{Z}^2$.

Idealklassen

Äquivalenz zweier Ideale $I, J \subseteq \mathcal{O}_K$: $\exists\ \alpha \in K^\times$ mit $\alpha I = J$

Verknüpfung zweier Ideale $I, J \subseteq \mathcal{O}_K$: $I \cdot J$ ist definiert als das Ideal in $\mathcal{O}_K$, das von den Produkten $xy,\ x \in I, y \in J$ erzeugt wird

Erzeuger: Jedes von Null evrschiedene Ideal in $\mathcal{O}_K$ ist ein Produkt von Primidealen

Endlichkeit der Klassengruppe: Die Klassenkörper eines quadratischen Zahlkörpers K ist endlich

Kettenbrüche

Kettenbruch: $[a_0; a_1, a_2, ..., a_k]$ mit $a_0 := a_0,\ a_0 \in \mathbb{R}$ und $[a_0; a_1, a_2, ..., a_k] := a_0 + \frac{1}{[a_1; a_2, ..., a_k]}$

n-te Konvergente von $\alpha \in \mathbb{R}$ irrational: $\alpha = [a_0; a_1, ..., a_{n-1}, a_n, \beta_{n+1}]$

- $a_0 := \lfloor \alpha \rfloor,\ \beta_1 := \frac{1}{\alpha - a_0},\ \lfloor \cdot \rfloor$: Gaußklammer
- $a_n := \lfloor \beta_n \rfloor,\ \beta_{n+1} := \frac{1}{\beta_n - a_n}$

Rekursionsvorschrift: Es seien $a- =, a_1, ...$ reelle Zahlen, $a_i > 0$ für $i > 0$. Weiter seien p_i, q_i rekursiv definiert durch $p_{-2} = 0,\ q_{-2} = 1,\ p_{-1} = 1,\ q_{-1} = 0$ und $p_i := a_i p_{i-1} + p_{i-2},\ q_i := a_i q_{i-1} + q_{i-2}$. Dann gilt für $i \geq 0$ die Gleichung $[a_0; a_1, a_2, ..., a_i] := \frac{p_i}{q_i}$.

Satz zu Konvergenten: Es sei $\alpha \in \mathbb{R} \backslash \mathbb{Q}$. Dann konvergieren die Konvergenten der Kettenbruchentwicklung von α gegen α.

Satz: Es gibt ein $s \geq 1$, sodass $\sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor = \overline{[2a_0; a_1, a_2, ..., a_s]}$. Insbesondere ist also $\sqrt{d} = [a_0; \overline{a_1, a_2, ..., a_s, 2a_0}]$ und $\beta_{s+2} = \beta_1$.

Algebraische Zahl: Komplexe Zahl, die Nullstelle eines nichttrivialen rationalen Polynoms ist

- Die Menge der algebraischen Zahlen ist abzählbar

Transzendente Zahlen: nicht algebraische Zahlen

Satz von Liouville: Es sei α eine algebraische Zahl, die Nullstelle eines irreduziblen ganzen Polynoms vom Grad d ist. Dann gibt es nur endlich viele teilerfremde Zahlen p, q, sodass $|\alpha - \frac{p}{q}| < \frac{1}{q^{d+1}}$

- Dieser Satz zeigt z.B., dass $\alpha = \sum_{n \in \mathbb{N}} 10^{-n!}$ transzendent ist