# Protokoll zur Zahlentheorie (gymnasiales Lehramt)

W. Bley

2. Februar 2016

# 1 Ringtheorie

## 1.1 Ringe und Ringhomomorphismen

**Definition 1.1.1** Ein Ring ist eine nicht-leere Menge $R$ zusammen mit zwei binären Operationen $+$ und $\cdot$, so daß gilt:

$(i)$ $(R,+)$ ist eine abelsche Gruppe.
$(ii)$ $(R,\cdot)$ ist ein Monoid.
$(iii)$ $a\cdot(b+c)=a\cdot b+a\cdot c, \quad (a+b)\cdot c=a\cdot b+a\cdot c, \forall a,b,c\in R.$

Die Regeln unter (iii) sind die Distributivgesetze. Falls zusätzlich gilt:

$$(iv) a\cdot b=b\cdot a, \forall a,b\in R,$$

so heißt der Ring kommutativ.

**Definition 1.1.2** Sei $R$ ein Ring.
a) Elemente $x\neq 0, y\neq 0$ heißen Nullteiler, falls gilt: $xy=0$.
b) Ein Element $a\in R$ heißt invertierbar, falls es ein $b\in R$ gibt mit $ab=ba=1$. Man nennt dann $a$ auch eine Einheit. Die Menge der Einheiten von R bildet eine Gruppe und wird mit $R^\times$ bezeichnet.
c) Ein Integritätsbereich ist ein nullteilerfreier, kommutativer Ring.
d) Falls in $R$ jedes Element $a\neq 0$ invertierbar ist, so ist $R$ ein Schiefkörper. Falls $R$ zusätzlich auch kommutativ ist, so nennt man $R$ einen Körper.

Beispiele von Ringen sind allgegenwärtig in der Mathematik. Angesprochen wurden hier $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$, Matrizenringe und die Hamiltonschen Quaternionen.
Die folgende Tatsache setzen wir als bekannt voraus. Zu $a,b\in\mathbb{Z}, b\neq 0$, gibt es eindeutig bestimmte Zahlen $q,r\in\mathbb{Z}$, so dass gilt

$$a=qb+r, \quad 0\leq r<|b|.$$

**Definition 1.1.3** Seien $a,b\in\mathbb{Z}$. Dann heißt $d\in\mathbb{N}$ größter gemeinsamer Teiler von $a$ and $b$, wenn folgende Bedingungen erfüllt sind:

a) $d$ teilt $a$ und $b$.

b) Falls $d_1\in\mathbb{Z}$ ein gemeinsamer Teiler von $a$ und $b$ ist, so ist $d_1$ ein Teiler von $d$.

Die Existenz eines größten gemeinsamen Teilers haben wir mit dem erweiterten euklidischen Algorithmus nachgewiesen. Wir schreiben $\mathrm{ggT}(a,b)$ oder auch nur $(a,b)$. Der euklidische Algorithmus ist sehr wichtig, insbesondere in der algorithmischen Zahlentheorie. Er liefert auch den konstruktiven Beweis zu folgendem Satz.

**Satz 1.1.4** *Seien $a, b \in \mathbb{Z}$ und sei $d := \mathrm{ggT}(a, b)$. Dann gibt es $x, y \in \mathbb{Z}$, so dass*

$$d = xa + yb.$$

Sei nun $n \in \mathbb{N}$. Dann bezeichnet $\mathbb{Z}/n\mathbb{Z}$ die Menge der Äquivalenzklassen bezüglich der Äquivalenzrelation

$$a \sim b \iff n \text{ teilt } a - b.$$

Wir schreiben in der Regel $a \equiv b \pmod{n}$ anstatt $a \sim b$. Für $a \in \mathbb{Z}$ bezeichne $\bar{a}$ die Äquivalenzklasse von $a$, also

$$\bar{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = a + n\mathbb{Z}.$$

Es gilt also

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\},$$

aber natürlich kann man auch andere Vertretersysteme wählen, zum Beispiel

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{1}, \bar{2}, \ldots, \bar{n}\},$$

Die Addition und Multiplikation in $\mathbb{Z}$ induziert (oder vererbt) auf $\mathbb{Z}/n\mathbb{Z}$ die folgende Ringstruktur:

$$\bar{a} + \bar{b} := \overline{a+b}, \quad \bar{a}\bar{b} := \overline{ab}.$$

**Satz 1.1.5** *Sei $R = \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$. Dann gilt:*

$$\begin{array}{ll} (a) & \bar{k} \text{ ist Nullteiler} \iff (k, n) > 1. \\ (b) & \bar{k} \text{ ist Einheit} \iff (k, n) = 1. \end{array}$$

*Insbesondere gilt also:*

$$\mathbb{Z}/n\mathbb{Z} \text{ ist ein Körper} \iff n \text{ ist Primzahl.}$$

**Definition 1.1.6** a) Seien $R$ und $S$ Ringe. Eine Abbildung $f : R \to S$ ist ein Ringhomomorphismus, falls für alle $a, b \in R$ gilt:

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b).$$

b) Die Teilmenge $\ker(f) := \{r \in R \mid f(r) = 0\}$ heißt der Kern von $f$.

**Achtung:** Es gilt zwar stets $f(0) = 0$, jedoch i. a. nicht $f(1) = 1$.
**Es gilt:** $f$ injektiv $\iff \ker(f) = \{0\}$.

**Definition 1.1.7** Sei $R$ ein Ring. Falls es eine natürliche Zahl $n \in \mathbb{N}$ gibt mit $n \cdot 1 = 0$, so setzt man $char(R) := \min\{n \in \mathbb{N} \mid n \cdot 1 = 0\}$. Sonst definiert man $char(R) := 0$. $char(R)$ heißt die Charakteristik von $R$.

**Satz 1.1.8** *Sei $R$ ein Ring mit positiver Charakteristik $n$.*
*(a) Die Abbildung $\varphi : \mathbb{Z} \to R, m \mapsto m \cdot 1$ ist ein Ringhomomorphismus mit $\ker(\varphi) = n\mathbb{Z}$.*
*(b) Falls $R$ nullteilerfrei ist, so ist $n$ eine Primzahl.*

## 1.2 Ideale

Ideale spielen in der Ringtheorie die Rolle der Normalteiler in der Gruppentheorie.

**Definition 1.2.1** Sei $R$ ein Ring und $I$ eine Teilmenge von $R$. Dann heißt $I$ ein $R$-Linksideal (bzw. $R$-Rechtsideal), falls für alle $r, a, b \in R$ gilt:

$$\begin{array}{ll} (i) & a, b \in I \implies a + b \in I, \\ (ii) & a \in I, r \in R \implies ra \in I \quad (\text{bzw. } ar \in I). \end{array}$$

$I$ heißt (beidseitiges) Ideal, falls $I$ sowohl Rechts-, als auch Linksideal ist.

**Definition 1.2.2** Sei $R$ ein kommutativer Ring und $X \subseteq R$.
a) Die Menge

$$(X) := \left\{ \sum_{i \in I} r_i x_i \mid r_i \in R, x_i \in X \right\},$$

wobei $I$ eine beliebige endliche Indexmenge ist, heißt das von $X$ erzeugte Ideal. Falls $X = \{x_1, \ldots, x_n\}$ eine endliche Menge ist, so schreibt man auch $(x_1, \ldots, x_n)$ anstelle von $(X)$. Falls $X = \{x\}$, so heißt $(x)$ das von $x$ erzeugte Hauptideal.
b) Ein Hauptidealring ist ein nullteilerfreier, kommutativer Ring, in dem jedes Ideal ein Hauptideal ist.

**Satz 1.2.3** *Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ein Hauptidealring.*

**Beispiel:** Die Teilmenge $\mathbb{Q}(\sqrt{-5}) := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\}$ ist ein Teilkörper der komplexen Zahlen. Wir betrachten den Ring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ sowie $I := 3\mathbb{Z} + (1 + \sqrt{-5})\mathbb{Z}$. Dann ist $I$ ein Ideal in $R$. Durch Normbetrachtungen haben wir gezeigt, dass $I$ kein Hauptideal ist.

**Definition 1.2.4** Sei $R$ ein Ring und $I, J$ Ideale in $R$. Dann definiert man:

$$\begin{aligned} I + J &:= \{a + b \mid a \in I, b \in J\}, \\ IJ &:= \{ \sum_{\text{endlich}} a_i b_i \mid a_i \in I, b_i \in J\}. \end{aligned}$$

$IJ$ heißt das Produkt der Ideale $I$ und $J$, $I+J$ die Idealsumme oder oft auch der größte gemeinsame Teiler von $I$ und $J$.

**Bemerkung:** $IJ$ und $I + J$ sind Ideale von $R$. Offensichtlich ist auch der Durchschnitt $I \cap J$ ein Ideal.

Für einen Ring $R$ und ein Ideal $I$ in $R$ bezeichnen wir die Menge der Äquivalenzklassen bezüglich der additiven Struktur wie in der Gruppentheorie mit $R/I$. Sei $a \in R$. Dann schreiben wir $\bar{a} = a+I$ für die Restklasse von $a$ modulo $I$. $R/I$ ist durch vertreterweise Addition eine abelsche (additive) Gruppe.

**Satz 1.2.5** *Durch $(a + I) \cdot (b + I) := ab + I$ wird auf $R/I$ eine Ringstruktur definiert.*

**Satz 1.2.6** *Sei $R$ ein Ring. Dann sind die Ideale genau die Kerne von Ringhomomorphismen.*

Ersetzt man in den Isomorphiesätzen für Gruppen den Begriff “Gruppen” durch “Ringe” und “Normalteiler” durch “Ideale”, so ergeben sich mit demselben Beweis die entsprechenden Isomorphiesätze für Ringe. Wegen der offensichtlichen Analogie werden diese hier nicht noch einmal aufgeführt.

**Definition 1.2.7** Sei $R$ ein kommutativer Ring und $P \subseteq R, P \neq R$ ein Ideal. Dann heißt $P$ prim oder ein Primideal, falls für alle $a, b \in R$ gilt:

$$ab \in P \implies a \in P \text{ oder } b \in P.$$

Der folgende Satz liefert eine äquivalente Charakterisierung.

**Satz 1.2.8** *Sei $R$ ein kommutativer Ring und $P$ ein Ideal in $R$ mit $P \neq R$. Dann gilt:*

$$P \text{ ist Primideal} \iff R/P \text{ ist nullteilerfrei.}$$

**Definition 1.2.9** Sei $R$ ein kommutativer Ring und $M \subseteq R, M \neq R$ ein Ideal. Dann heißt $M$ maximal, falls für alle Ideale $I$ von $R$ gilt: $M \subseteq I, M \neq I \implies I = R$.

**Satz 1.2.10** *Sei $R$ ein kommutativer Ring und $I \subseteq R$, $I \neq R$, ein Ideal. Dann gilt:*

$$I \text{ ist maximal} \iff R/I \text{ ist ein Körper.}$$

*Insbesondere ist also jedes maximale Ideal ein Primideal.*

Um zu beweisen, daß maximale Ideale stets existieren, benötigen wir das Zornsche Lemma. Sei dazu $(A, \leq)$ eine partiell geordnete Menge (z.B. die Menge der natürlichen Zahlen mit der Teilbarkeitsrelation). Ein Element $a \in A$ heißt maximal, falls für alle mit $a$ vergleichbaren $b \in A$ gilt: $b \leq a$. Sei $B \subseteq A$. Dann heißt $d \in A$ eine obere Schranke für $B$, falls alle $b \in B$ mit $d$ vergleichbar sind und gilt: $b \leq d$. Eine Kette in $A$ ist eine linear geordnete Sequenz $a_0 \leq a_1 \leq a_2 \leq \ldots$ von Elementen $a_i \in A$.

**Zornsches Lemma:** Sei $A$ eine nicht-leere partiell geordnete Menge, so daß jede Kette in $A$ eine obere Schranke in $A$ hat. Dann existieren maximale Elemente in $A$.

Man kann zeigen, daß das Zornsche Lemma äquivalent ist zu

**Auswahlaxiom:** Sei $I$ ein nicht-leere Indexmenge und $\{S_i \mid i \in I\}$ eine Familie von nicht-leeren Mengen $S_i$. Dann gilt: $\prod_{i \in I} S_i \neq \emptyset$.

Als Anwendung erhalten wir

**Satz 1.2.11** *Sei $R$ ein kommutativer Ring und $I \subseteq R, I \neq R$, ein Ideal. Dann ist $I$ in einem maximalen Ideal enthalten. Insbesondere existieren also maximale Ideale.*

**Satz 1.2.12** *Sei $\{R_i \mid i \in I\}$ eine Familie von Ringen und $\prod_{i \in I} R_i$ das kartesische Produkt der $R_i$. Dann ist $\prod_{i \in I} R_i$ mit komponentenweiser Addition und Multiplikation ein Ring.*

**Satz 1.2.13** *(Chinesischer Restsatz) Sei $R$ ein Ring und seien $I_1, \ldots, I_n$ Ideale in $R$ mit $I_k + I_l = R$ für $k \neq l$. Seien weiter $b_1, \ldots, b_n \in R$ gegeben. Dann gibt es ein $b \in R$ mit $b \equiv b_k \pmod{I_k}, k = 1, \ldots, n$. $b$ ist dabei eindeutig bestimmt modulo $I_1 \cap \ldots \cap I_n$.*

**Folgerung 1.2.14** *Sei $R$ ein Ring und seien $I_1, \ldots, I_n$ Ideale in $R$ mit $I_k + I_l = R$ für $k \neq l$. Sei $I = I_1 \cap \ldots \cap I_n$. Dann ist*

$$\begin{aligned} R/I &\longrightarrow R/I_1 \times \ldots \times R/I_n, \\ a + I &\mapsto (a + I_1, \ldots, a + I_n) \end{aligned}$$

*ein Isomorphismus von Ringen.*

Die Folgerung ist tatsächlich äquivalent zum Chinesischen Restsatz. Die Surjektivität entspricht der Existenzaussage, die Injektivität der Eindeutigkeitsaussage im Chinesischen Restsatz.
Eine häufig verwendete Konsequenz aus dem Chinesischen Restsatz ist

**Folgerung 1.2.15** *Sei $m \in \mathbb{N}$ eine natürliche Zahl, $m \geq 2$. Sei*

$$m = p_1^{e_1} \cdots p_s^{e_s}$$

*die Primzahlzerlegung von $m$ mit paarweise verschiedenen Primzahlen $p_i$. Dann ist*

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_s^{e_s}\mathbb{Z}, \\ a + m\mathbb{Z} &\mapsto (a + p_1^{e_1}\mathbb{Z}, \ldots, a + p_s^{e_s}\mathbb{Z}) \end{aligned}$$

*ein Isomorphismus von Ringen.*

## 1.3 Faktorisierung in kommutativen Ringen

ZIEL: Satz von der eindeutigen Primzahlzerlegung in Hauptidealringen.

**Definition 1.3.1** Sei $R$ ein kommutativer Ring und $0 \neq a, b \in R$. Dann heißen $a$ und $b$ zueinander assoziiert, in Zeichen $a \sim b$, falls $a \mid b$ und $b \mid a$.

**Satz 1.3.2** *Sei $R$ ein komm. Ring und $a, b, u \in R$. Dann gilt:*

$$\begin{aligned}
(i) \quad & a \mid b \iff (b) \subseteq (a) \\
(ii) \quad & a \sim b \iff (a) = (b) \\
(iii) \quad & u \in R^\times \iff u \mid r, \forall r \in R \\
(iv) \quad & u \in R^\times \iff (u) = R \\
(v) \quad & a = bu, u \in R^\times \implies a \sim b.
\end{aligned}$$

*Falls $R$ nullteilerfrei ist, so gilt in $(v)$ auch die Rückrichtung.*

**Definition 1.3.3** Sei $R$ ein kommutativer Ring.
a) Ein Element $c \in R \setminus R^\times$ heißt irreduzibel, falls für alle $a, b \in R$ gilt:

$$c = ab \implies a \in R^\times \text{ oder } b \in R^\times.$$

b) Ein Element $p \in R \setminus R^\times$ heißt prim, falls für alle $a, b \in R$ gilt:

$$p \mid ab \implies p \mid a \text{ oder } p \mid b.$$

**Satz 1.3.4** *Sei $R$ ein nullteilerfreier, komm. Ring. Dann gilt:*

- *$p$ ist prim $\iff$ $(p)$ ist Primideal.*
- *$p$ prim $\implies$ $p$ irreduzibel.*
- *Falls $R$ ein Hauptidealring ist, so gilt:*

$$p \text{ prim} \iff p \text{ irreduzibel}$$

**Definition 1.3.5** Sei $R$ ein nullteilerfreier, komm. Ring. Dann heißt $R$ faktoriell oder ZPE-Ring, falls gilt:
(i) Jedes Element $a \neq 0, a \notin R^\times$ kann man als Produkt $a = c_1 \cdots c_n, c_i$ irreduzibel, schreiben.
(ii) Falls $a = d_1 \cdots d_m, d_j$ irreduzibel, eine weitere solche Darstellung ist, so gilt $n = m$ und (bis auf Numerierung) $d_i \sim c_i$.

**Bemerkung:** In einem faktoriellen Ring ist jedes irreduzible Element prim.

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

**Satz 1.3.6** *Jeder Hauptidealring ist faktoriell.*

**Definition 1.3.7** Ein euklidischer Ring ist ein nullteilerfreier, kommutativer Ring $R$ mit einer Funktion $\varphi : R \setminus \{0\} \to \mathbb{N}$, so daß es zu $a, b \in R, b \neq 0$, Elemente $v, r \in R$ gibt, so daß $a = vb + r$ mit $r = 0$ oder $r \neq 0$ und $\varphi(r) < \varphi(b)$.

Das Standardbeispiel hierfür ist $\mathbb{Z}$ zusammen mit dem Absolutbetrag. Wie für $\mathbb{Z}$ zeigt man

**Satz 1.3.8** *Jeder euklidische Ring ist ein Hauptidealring.*

**Definition 1.3.9** Sei $R$ ein Hauptidealring und $a, b \in R$. Dann heißt jeder Erzeuger $d$ von $(a)+(b)$ ein größter gemeinsamer Teiler von $a$ und $b$. Jeder Erzeuger $k$ von $(a) \cap (b)$ heißt ein kleinstes gemeinsames Vielfaches von $a$ und $b$.

In euklidischen Ringen hat man durch den euklidischen Algorithmus ein (schnelles) Verfahren zur Berechnung des ggT.

## 1.4 Polynomringe

**Satz 1.4.1** *Sei $R$ ein kommutativer Ring und $f, g \in R[x]$. Sei der führende Koeffizient von $g$ eine Einheit in $R$. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[x]$ mit der Eigenschaft:*

$$f = qg + r \text{ mit } r = 0 \text{ oder } deg(r) < deg(g).$$

**Folgerung 1.4.2** *Sei $K$ ein Körper. Dann ist $K[x]$ ein euklidischer Ring.*

**Satz 1.4.3** *Sei $R$ ein nullteilerfreier kommutativer Ring und $f \in R[x]$ ein Polynom vom Grad $n$. Dann hat $f$ höchstens $n$ Nullstellen in $R$.*

**Definition 1.4.4** Sei $R$ ein nullteilerfreier kommutativer Ring und $f \in R[x]$. Sei $c \in R$ eine Nullstelle von $f$. Dann heißt

$$max\{m \in \mathbb{N} \mid (x-c)^m \text{ teilt } f\}$$

die Vielfachheit der Nullstelle $c$.

**Satz 1.4.5** *Sei $R$ ein nullteilerfreier kommutativer Ring. Sei $R \subseteq S$ und $c \in S$, wobei $S$ ebenfalls ein nullteilerfreier kommutativer Ring ist. Dann gilt:*
*(i) $c$ ist mehrfache Nullstelle $\iff f(c) = f'(c) = 0$.*
*(ii) Sei $R$ ein Körper. Dann hat $f$ keine mehrfachen Nullstellen in $S$, falls $(f, f') = 1$.*
*(iii) Sei $R$ ein Körper und $f$ irreduzibel. Dann gilt:*

$$f \text{ hat mehrfache Nullstellen in } S \implies f' = 0.$$

**Definition 1.4.6** Sei $R$ ein faktorieller Ring. Sei $f = a_n x^n + a_{n-1}x^{n-1} + \dots a_1^x + a_0 \in R[x]$. Dann heißt $c(f) := (a_0, a_1, \dots, a_n)$ der Inhalt von $f$. Falls $c(f) \in R^\times$, so heißt $f$ primitiv.

**Bemerkungen:**
1) $c(f)$ ist nur bis auf Assoziiertheit bestimmt.
2) Jedes Polynom $g$ läßt sich in der Form $g = c(g)g_1$ mit primitivem $g_1$ schreiben.

**Satz 1.4.7** *(Gaußsches Lemma) Sei $R$ faktoriell und $f, g \in R[x]$. Dann gilt: $c(fg) \sim c(f)c(g)$. Insbesondere ist also das Produkt von primitiven Polynomen wieder primitiv.*

**Satz 1.4.8** *Sei $R$ faktoriell und $K = Quot(R)$ der Quotientenkörper. Sei $f \in R[x]$ ein nichtkonstantes, primitives Polynom. Dann gilt:*

$$f \text{ irreduzibel in } K[x] \iff f \text{ irreduzibel in } R[x]$$

**Bemerkung:** Der Quotientenkörper wurde bislang nur informell definiert. Dies wird noch nachgeholt.

**Satz 1.4.9** *(Eisensteinkriterium) Sei $R$ faktoriell und $K = Quot(R)$. Sei $f = a_n x^n + a_{n-1}x^{n-1} + \dots a_1 x + a_0 \in R[x]$, $deg(f) \geq 1$. Sei $p \in R$ irreduzibel und es gelte*

$$p \nmid a_n, \quad p \mid a_i,\ i = 0, \dots, n-1, \quad p^2 \nmid a_0.$$

*Dann ist $f$ irreduzibel in $K[x]$. Falls $f$ zusätzlich primitiv ist, so ist $f$ auch irreduzibel in $R[x]$.*

Im folgenden Einschub holen wir die Definition des Quotientenkörpers nach, gehen dabei aber etwas allgemeiner vor:

**Definition 1.4.10** Sei $R$ ein kommutativer Ring und $S \subseteq R$ eine nicht-leere Teilmenge. Dann heißt $S$ multiplikativ, falls gilt: $(i)$ $0 \notin S$, $(ii)$ $a, b \in S \implies ab \in S$.

**Satz 1.4.11** *Sei $S$ eine multiplikative Teilmenge eines kommutativen Rings $R$. Dann ist durch*

$$(r,s) \sim (r_1,s_1) :\Longleftrightarrow \exists t \in S : t(rs_1 - r_1 s) = 0$$

*eine Äquivalenzrelation auf $R \times S$ definiert.*

**Bemerkung:** Falls $R$ nullteilerfrei ist, so gilt einfacher:

$$(r,s) \sim (r_1,s_1) :\Longleftrightarrow rs_1 - r_1 s = 0$$

Die Äquivalenzklasse von $(r,s)$ bezeichnen wir suggestiv mit $\frac{r}{s}$; $S^{-1}R$ bezeichnet die Menge der Äquivalenzklassen.

**Satz 1.4.12** *Sei $S$ eine multiplikative Teilmenge des kommutativen Rings $R$. Dann gilt:*
*(i) $S^{-1}R$ ist ein kommutativer Ring mit den binären Operationen*

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1}, \quad \frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

*(ii) Falls $R$ nullteilerfrei ist, so auch $S^{-1}R$.*
*(iii) Falls $R$ nullteilerfrei ist und $S = R \setminus \{0\}$, so ist $S^{-1}R$ ein Körper.*

**Bemerkung:** Der Körper in (iii) heißt der Quotientenkörper von $R$ und wird im weiteren mit $Quot(R)$ bezeichnet.

**Satz 1.4.13** *Sei $S$ eine multiplikative Teilmenge des kommutativen Rings $R$. Dann gilt:*
*(i) Die Abbildung $\varphi_S : R \to S^{-1}R, r \mapsto \frac{rs}{s}$, $s \in S$ beliebig, ist ein wohldefinierter Ringhomomorphismus.*
*(ii) Falls $S$ keine Nullteiler enthält, so ist $\varphi_S$ injektiv. Insbesondere kann man also jeden kommutativen nullteilerfreien Ring in seinen Quotientenkörper einbetten.*

**Satz 1.4.14** *Sei $R$ faktoriell. Dann ist auch $R[x_1, \ldots, x_n]$ faktoriell.*

# 2 Die Struktur von $(\mathbb{Z}/m\mathbb{Z})^\times$

## 2.1 Die Eulersche $\varphi$-Funktion

**Definition 2.1.1** Sei $m \in \mathbb{N}$. Dann heißt $\varphi(m) := \left|(\mathbb{Z}/m\mathbb{Z})^\times\right|$ Eulersche $\varphi$-Funktion.

**Satz 2.1.2** *a) Die Eulersche $\varphi$-Funktion ist multiplikativ in folgendem Sinn:*

$$\varphi(mn) = \varphi(m)\varphi(n), \text{ falls } (m,n) = 1.$$

*Insbesondere gilt also:*

$$\varphi(m) = \prod_{i=1}^{t} \varphi(p_t^{\alpha_t})$$

*falls die eindeutige Primzahlzerlegung von $m$ durch $m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ gegeben ist.*
*b) Sei $p$ eine Primzahl. Dann gilt: $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.*

Eine direkte Folgerung aus der Definition der $\varphi$-Funktion ist der sogenannte "kleine Satz von Fermat":

**Satz 2.1.3** *Für $a \in \mathbb{Z}$ mit $(a,m) = 1$ gilt $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$.*

Eine einfache, aber im täglichen Leben sehr wichtige Anwendung des kleinen Satzes von Fermat, ist das sogenannte RSA-Kryptographie-Verfahren.

## 2.2 Primitivwurzeln

Um die Struktur der abelschen Gruppen $(\mathbb{Z}/m\mathbb{Z})^\times$ zu bestimmen, genügt es nach dem chinesischen Restsatz die Struktur der Gruppen $(\mathbb{Z}/p^\alpha)^\times$ für Primzahlen $p$ zu bestimmen.

**Satz 2.2.1** *Sei $p \neq 2$ eine Primzahl und $\alpha \in \mathbb{N}$. Dann ist $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ zyklisch von der Ordnung $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Die Gruppe $(\mathbb{Z}/2^\alpha)^\times$ ist für $\alpha > 2$ bizyklisch. Explizit hat man*

$$(\mathbb{Z}/2^\alpha)^\times \simeq \begin{cases} 1, & \text{falls } \alpha = 1, \\ \langle -1 \rangle, & \text{falls } \alpha = 2, \\ \langle -1 \rangle \times \langle 5 \rangle, & \text{falls } \alpha > 2. \end{cases}$$

Zum Beweis benötigen wir den

**Satz 2.2.2** *Sei $K$ ein Körper und $G \subseteq K^\times$ eine endliche Untergruppe. Dann ist $G$ zyklisch. Insbesondere ist also $(\mathbb{Z}/p\mathbb{Z})^\times$ für jede Primzahl $p$ eine zyklische Gruppe.*

Der Beweis des letzten Satzes beruht wesentlich auf

**Lemma 2.2.3** *Sei $G$ eine abelsche Gruppe und $x, y \in G$. Dann gibt es ein Element $z \in G$ mit $ord(z) = \mathrm{kgV}(ord(x), ord(y))$.*

# 3 Das quadratische Reziprozitätsgesetz

## 3.1 Das Legendre-Symbol

**Definition 3.1.1** Sei $p \neq 2$ eine Primzahl und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, p) = 1$. Dann definiert man das Legendresymbol durch

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{falls } a \equiv b^2 \pmod{p} \text{ für ein } b \in \mathbb{Z}, \\ -1, & \text{falls } a \not\equiv b^2 \pmod{p} \text{ für alle } b \in \mathbb{Z}. \end{cases}$$

Falls $\mathrm{ggT}(a, p) \neq 1$, so setzen wir $\left(\frac{a}{p}\right) := 0$.

**Remarks 3.1.2** a) $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$ für alle $k \in \mathbb{Z}$.
b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ für alle $a, b \in \mathbb{Z}$. Insbesondere ist

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$$

ein Gruppenhomomorphismus. Sein Kern sind genau die Quadrate.
c) Die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ ist zyklisch. Sei $w$ eine Primitivwurzel, also $(\mathbb{Z}/p\mathbb{Z})^\times = \langle w \rangle$. Dann gilt für $a \in (\mathbb{Z}/p\mathbb{Z})^\times$

$$\left(\frac{a}{p}\right) = (-1)^s, \text{ falls } a = w^s.$$

**Satz 3.1.3** *(Eulersches Kriterium) Sei $p \neq 2$ eine Primzahl und $a \in \mathbb{Z}$. Dann gilt:*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

**Folgerung 3.1.4** *(Ergänzungssätze) Sei $p \neq 2$ eine Primzahl. Dann gilt:*

$$a) \qquad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1, & \text{falls } p \equiv 1 \pmod 4, \\ -1, & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

$$b) \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1, & \text{falls } p \equiv \pm 1 \pmod 8, \\ -1, & \text{falls } p \equiv \pm 3 \pmod 8. \end{cases}$$

Im Folgenden rechnen wir im Ring

$$\mathbb{Z}[\zeta] := \{f(\zeta) \mid f \in \mathbb{Z}[x]\},$$

wobei hier $\zeta = \zeta_p := \exp(2\pi i/p)$. Da das Minimalpolynom von $\zeta$ durch $x^{p-1} + x^{p-2} + \ldots + x + 1$ gegeben ist, ist jedes Element $\alpha \in \mathbb{Z}[\zeta]$ von der Form

$$\alpha = a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{p-2}\zeta^{p-2}$$

mit eindeutig bestimmten $a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}$.

**Definition 3.1.5** Die Gaußsche Summe zu $p$ wird definiert durch

$$S(p) := \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k \in \mathbb{Z}[\zeta].$$

**Satz 3.1.6** *a) Für eine Primzahl $p \neq 2$ gilt:*

$$S(p)^2 = \left(\frac{-1}{p}\right) p.$$

*b) Seien $p \neq q$ zwei ungerade Primzahlen. Dann gilt:*

$$S(p)^q \equiv \left(\frac{q}{p}\right) S(p) \pmod{q\mathbb{Z}[\zeta]}.$$

Als Konsequenz aus diesem zahlentheoretischen Resultat erhalten wir das quadratische Reziprozitätsgesetz.

**Folgerung 3.1.7** *(Quadratisches Reziprozitätsgesetz) Seien $p \neq q$ zwei ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right) = \varepsilon \left(\frac{q}{p}\right)$$

*mit*

$$\varepsilon = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} +1, \text{ falls } p \equiv 1 \pmod 4 \text{ oder } q \equiv 1 \pmod 4, \\ -1, \text{ falls } p \equiv 3 \pmod 4 \text{ und } q \equiv 3 \pmod 4, \end{cases}$$

## 3.2 Das Jacobi-Symbol

Bei der Berechnung des Legendre-Symbols $\left(\frac{a}{p}\right)$ benötigt man die Primzahlzerlegung von $a$, deren Berechnung für große $a$ sehr problematisch oder gar unmöglich ist. Abhilfe schafft hier das sogenannte Jacobi-Symbol.

**Definition 3.2.1** Sei $m \geq 3$ eine ungerade ganze Zahl und $m = p_1 \cdots p_r$ die Primzahlzerlegung von $m$. Sei $a \in \mathbb{Z}$. Dann nennt man

$$\left(\frac{a}{m}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

das Jacobi-Symbol von $a$ über $m$.

**Remarks 3.2.2** a) Das Jacobi-Symbol ist multiplikativ, d.h. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.
b) Es gilt $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$, falls $a \equiv b \pmod{m}$.
c) $\left(\frac{a}{m}\right) = 1$ impliziert im Allgemeinen nicht, dass $a$ ein Quadrat modulo $m$ ist.

**Satz 3.2.3** *(Ergänzungssätze und quadratisches Reziprozitätsgestz für das Jacobi-Symbol) Seien $m, n \geq 3$ zwei ungerade ganze Zahlen. Dann gilt:*

$$a) \qquad \left(\frac{-1}{m}\right) = (-1)^{(m-1)/2} = \begin{cases} +1, & \text{falls } m \equiv 1 \pmod 4, \\ -1, & \text{falls } m \equiv 3 \pmod 4. \end{cases}$$

$$b) \qquad \left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8} = \begin{cases} +1, & \text{falls } m \equiv \pm 1 \pmod 8, \\ -1, & \text{falls } m \equiv \pm 3 \pmod 8. \end{cases}$$

$$c) \qquad \left(\frac{m}{n}\right) = \varepsilon \left(\frac{n}{m}\right)$$

*mit*

$$\varepsilon = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} = \begin{cases} +1, \text{ falls } m \equiv 1 \pmod 4 \text{ oder } n \equiv 1 \pmod 4, \\ -1, \text{ falls } m \equiv 3 \pmod 4 \text{ und } n \equiv 3 \pmod 4, \end{cases}$$

# 4 Kreisteilungskörper

## 4.1 Grundlegendes

**Definition 4.1.1** Sei $K$ ein Körper und $n \in \mathbb{N}$. Dann heißt

$$W_n(K) := \{\zeta \in K \mid \zeta^n = 1\}$$

Gruppe der $n$-ten Einheitswurzeln in $K$. Die Gruppe

$$W(K) := \bigcup_{n \in \mathbb{N}} W_n(K)$$

heißt Gruppe der Einheitswurzeln in $K$. Eine Einheitswurzel $\zeta \in W_n(K)$ nennt man primitiv (von der Ordnung $n$), falls $\mathrm{ord}(\zeta) = n$.

**Lemma 4.1.2** *Sei $K$ ein Körper und $n \in \mathbb{N}$. Dann ist $W_n(K)$ eine zyklische Gruppe mit*

$$|W_n(K)| \text{ teilt } n.$$

*Falls* $\mathrm{char}(K) = p > 0$, *so ist* $W_{np}(K) = W_n(K)$.

**Definition 4.1.3** Sei $K$ ein Körper und $n \in \mathbb{N}$. Dann heißt der Zerfällungskörper $E$ von $x^n - 1$ der Körper der $n$-ten Einheitswurzeln. Wir schreiben kurz $E = K(\sqrt[n]{1})$.

**Remark 4.1.4** Sei $C$ ein algebraischer Abschluß von $K$. Dann gilt: $K(\sqrt[n]{1}) = K(W_n(C))$.

## 4.2 Galoistheorie von Kreisteilungskörpern

Sei $E/K$ algebraisch. Wir erinnern an die Definition der Automorphismengruppe $G(E/K)$:

$$G(E/K) := \{\sigma \colon E \longrightarrow E \mid \sigma \text{ ist ein Homomorphismus mit } \sigma|_K = id\}.$$

**Satz 4.2.1** *Sei $E = K(\sqrt[n]{1})$. Dann ist $E/K$ eine endliche, normale und separable Erweiterung. Falls $\mathrm{char}(K) \nmid n$, so ist die Automorphismengruppe $G(E/K)$ isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$. Insbesondere ist $G(E/K)$ stets abelsch (auch im Fall $\mathrm{char}(K) \mid n$).*

**Satz 4.2.2** *Sei $E = \mathbb{Q}(\sqrt[n]{1})$. Dann gilt:*

$$G(E/K) \simeq (\mathbb{Z}/n\mathbb{Z})^\times .$$

*Insbesondere ist $[E : \mathbb{Q}] = \varphi(n)$ mit der Eulerschen phi-Funktion $\varphi$.*

**Remark 4.2.3** Sei $\zeta$ eine primitive $n$-te Einheitswurzel. Dann ist der Isomorphismus im Satz 4.2.2 gegeben durch

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow G(E/K), \quad \bar{k} \mapsto \sigma_k,$$

wobei $\sigma_k$ eindeutig festgelegt ist durch $\sigma_k(\zeta) = \zeta^k$. Entscheidend ist, dass man hier eine primitive Einheitswurzel $\zeta$ zugrunde legt.

## 4.3 Kreisteilungspolynome

Im Folgenden sei stets $C = \bar{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$.

**Definition 4.3.1** Sei $n \in \mathbb{N}$. Das Polynom

$$F_n(x) = \prod_{\zeta \in W_n(C), \mathrm{ord}(\zeta) = n} (x - \zeta)$$

nennt man das $n$-te Kreisteilungspolynom.

**Satz 4.3.2** *a) $F_n$ ist ein normiertes Polynom vom Grad $\varphi(n)$.*
*b) Es gilt:*

$$x^n - 1 = \prod_{d \mid n} F_d(x).$$

*c) $F_n(x) \in \mathbb{Z}[x]$.*

**Folgerung 4.3.3** *Das $n$-te Kreisteilungspolynom ist irreduzibel in $\mathbb{Q}[x]$. Sei $\zeta$ eine primitive $n$-te Einheitswurzel. Dann ist $F_n$ das Minimalpolynom von $\zeta$.*

# 5 Endliche Körper

## 5.1 Grundlegendes

**Lemma 5.1.1** *Sei $K$ ein endlicher Körper und $\mathrm{char}(K) = p > 0$. Dann ist $K$ in natürlicher Weise eine Körpererweiterung von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Sei $d = \dim_{\mathbb{F}_p}(K)$. Dann gilt: $|K| = p^d$.*

**Folgerung 5.1.2** *Sei $|K| = q = p^d$. Dann ist $K$ ein Zerfällungskörper von $x^q - x \in \mathbb{F}_p[x]$. Damit ist $K$ durch $p$ und $d$ bis auf Isomorphie eindeutig bestimmt.*

**Satz 5.1.3** *Sei $C$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dann gibt es zu jedem $d \in \mathbb{N}$ genau einen Körper $K \subseteq C$ mit $p^d$ Elementen, nämlich den Zerfällungskörper von $x^{p^d} - x$. Der Körper $K$ besteht genau aus den Nullstellen von $f$.*

**Folgerung 5.1.4** *Sei $K$ ein endlicher Körper. Dann gibt es zu jedem $d \in \mathbb{N}$ bis auf Isomorphie genau einen Erweiterungskörper $E$ von $K$ mit $[E : K] = d$.*

**Remark 5.1.5** Sei $K$ ein endlicher Körper und $d \in \mathbb{N}$. Dann gibt es in $K[x]$ irreduzible Polynome vom Grad $d$.

Schließlich untersuchen wir Erweiterungen endlicher Körper hinsichtlich ihrer Galoistheorie.

**Satz 5.1.6** *Sei $E/K$ eine Erweiterung von endlichen Körpern. Sei $|K| = q = p^d$. Dann ist $E/K$ galoissch mit zyklischer Galoisgruppe $G(E/K) = \langle \sigma_q \rangle$, wobei $\sigma_q(\alpha) = \alpha^q$ für alle $\alpha \in E$ ist.*

Der Automorphismus $\sigma_q$ heißt Frobenius-Automorphismus von $E/K$.

# 6 Die letzten 50 Minuten

Wir haben ansatzweise probabilistische Primzahltests besprochen und sind insbesondere auf die sogenannten Carmichael-Zahlen eingegangen. Dem interessierten Leser sei das Buch von Otto Forster, Algorithmische Zahlentheorie, und hier besonders die Kapitel 10 und 12, empfohlen.