MASTERARBEIT | MASTER'S THESIS

Titel | Title

Das Reziprozitätsgesetz in Polynombereichen

verfasst von | submitted by

Alexandra Vallant BEd

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Education (MEd)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 199 502 520 02
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Masterstudium Lehramt Sek (AB) Unterrichtsfach Biologie und Umweltbildung Unterrichtsfach Mathematik
Betreut von | Supervisor:	ao. Univ.-Prof. Dr. Joachim Mahnkopf

Abstract

Das quadratische Reziprozitätsgesetz zählt zu den zentralen Sätzen der Zahlentheorie und beschreibt die Lösbarkeit von quadratischen Kongruenzen im Ring der ganzen Zahlen $\mathbb{Z}$. Ziel dieser Arbeit ist es, ein Analogon dieses Gesetzes im Polynomring $\mathbb{F}_q[T]$ über einem endlichen Körper $\mathbb{F}_q$ zu beschreiben. Ausgehend von den algebraischen Grundlagen - insbesondere den Eigenschaften faktorieller Ringe, Hauptidealringe und euklidischer Ringe - wird gezeigt, dass $\mathbb{F}_q[T]$ in vielerlei Hinsicht mit $\mathbb{Z}$ zu vergleichen ist. Dies ermöglicht die Übertragung der Definition des Legendresymbols als Potenzrestsymbol und es stellt sich die Frage nach einem Analogon des quadratischen Reziprozitätsgesetz für $\mathbb{F}_q[T]$. In der Tat gilt im Polynombereich ein Reziprozitätsgesetz sogar für d-te Potenzreste, wobei d ein Teiler von $q-1$ ist. Im Mittelpunkt steht dabei die Frage, wie sich das Reziprozitätsgesetz für $\mathbb{F}_q[T]$ beweisen lässt. Die Beweismethode profitiert erheblich von den algebraischen Eigenschaften von $\mathbb{F}_q[T]$: Polynome zerfallen vollständig in Linearfaktoren in der Koeffizientenerweiterung $\overline{\mathbb{F}}_q[T]$ von $\mathbb{F}_q[T]$ und in Verbindung mit der Wirkung des Frobeniusautomorphismus ist eine technisch einfache Beweisführung möglich. Im Gegensatz dazu fehlen im Ring der ganzen Zahlen analoge Strukturen, die eine solche Beweisführung unmöglich machen. Abschließend werden die Unterschiede zwischen $\mathbb{Z}$ und $\mathbb{F}_q[T]$ tabellarisch gegenübergestellt.

Abstract

The quadratic reciprocity law is one of the central theorems of number theory and describes the solvability of quadratic congruences in the ring of integers $\mathbb{Z}$. The aim of this work is to describe an analogue of this law in the polynomial ring $\mathbb{F}_q[T]$ over a finite field $\mathbb{F}_q$. Starting from the algebraic foundation - in particular the properties of factorial rings, principal ideal rings and euclidean rings - it is shown that $\mathbb{F}_q[T]$ can be compared with $\mathbb{Z}$ in many aspects. This makes it possible to transfer the definition of the Legendre symbol as a power residue symbole and the question of an analogue of the quadratic reciprocity law for $\mathbb{F}_q[T]$ arises. In fact, a reciprocity law applies in the polynomial domain even for d-th power residues, where d is a divisor of $q-1$. The central question here is how to prove the reciprocity law for $\mathbb{F}_q[T]$: Polynomials decompose completely into linear factors in the coefficient extension and, in conjunction with the effect of the Frobenius automorphism, a technically simple proof is possible. In contrast, analogue structures are missing in the ring of integers, which make this kind of proof impossible. Finally, the differences between $\mathbb{Z}$ and $\mathbb{F}_q[T]$ are compared in a table.

Inhaltsverzeichnis

1 Einleitung

Im Allgemeinen beschäftigt sich die Zahlentheorie mit den arithmetischen Eigenschaften des Rings der ganzen Zahlen, in dem auch das quadratische Reziprozitätsgesetz seine Anwendung findet und eine zentrale Rolle spielt [13, S. vii].

Das quadratische Reziprozitätsgesetz wird benötigt, um zu bestimmen, ob eine Primzahl ein quadratischer Rest modulo einer anderen Primzahl ist [3, S. 306]. Diesen genannten Zusammenhang beschreibt das Legendresymbol: Wir definieren das Legendresymbol wie folgt: $(\frac{a}{p}) = 1$ genau dann, wenn die Zahl a ein quadratischer Rest modulo der Primzahl p ist, wobei $p \nmid a$, also genau dann, wenn die Kongruenz $x^2 \equiv a \mod p$ lösbar ist. Andernfalls ist $(\frac{a}{p}) = -1$ [3, S. 303]. Der Mathematiker Adrien-Marie Legendre führte das nach ihm benannte Legendresymbol ein [15, S.128]. Das Gesetz wurde allerdings erstmals von Carl Friedrich Gauß bewiesen. Insgesamt fand Gauß im Laufe seines Lebens neun verschiedene Beweise für das quadratische Reziprozitätsgesetz [13, S. 23].

Der Polynomring $\mathbb{F}_q[T]$ über einem endlichen Körper $\mathbb{F}_q$ weist ähnliche algebraische Eigenschaften wie der Ring der ganzen Zahlen auf. Zu nennen ist hier insbesondere, dass $\mathbb{F}_q[T]$ ein euklidischer Ring, damit auch Hauptidealring und faktorieller Ring, ist [13, S. 2]. In dieser Analogie entsprechen den Primzahlen in $\mathbb{Z}$ die irreduziblen Polynome in $\mathbb{F}_q[T]$. Kongruenzen modulo (Prim-)Zahlen in $\mathbb{Z}$ entsprechen demnach Kongruenzen modulo (Prim-)Polynomen in $\mathbb{F}_q[T]$. Während in $\mathbb{Z}$ die Fragestellung lautet, ob es ein $n \in \mathbb{Z}$ gibt, sodass $n^2 \equiv a \mod p$ gilt, also ob a ein quadratischer Rest modulo einer Primzahl ist, fragen wir im Polynomring nach höheren Potenzresten, das heißt, wann ein Polynom $f \in \mathbb{F}_q[T]$ existiert, sodass $f^d \equiv a \mod P$ gilt, wobei $d|q-1$. Zur Beantwortung dieser Frage stellen wir in der vorliegenden Arbeit das höhere Reziprozitätsgesetz im Polynomring $\mathbb{F}_q[T]$ dar, das an die Stelle des quadratischen Reziprozitätsgesetz im Ring der ganzen Zahlen $\mathbb{Z}$ tritt [13, S. 23].

Wird das quadratische Reziprozitätsgesetz auf den Polynombereich der Form $\mathbb{F}_q[T]$ übertragen, also als höheres Reziprozitätsgesetz formuliert, so ist es weniger aufwendig zu beweisen [13, S. 23]. Ein Ziel der Arbeit ist, einen Beweis des Reziprozitätsgesetz darzustellen.

Wer das höhere Reziprozitätsgesetz im Polynombereich erstmals bewiesen hat, ist historisch gesehen interessant. Der Mathematiker Richard Dedekind lieferte Beiträge zum Analogon des quadratischen Reziprozitätsgesetz in $\mathbb{F}_q[T]$, also für den Fall $d = 2$ [14, S. 167]. Später formulierte Emil Artin den Beweis des Reziprozitätsgesetzes für $d = 2$ [1, S. 153 f]. Für den allgemeinen Fall, also für $d|q-1$, galt eine Zeit lang der Mathematiker Leonard Carlitz als Erster, der einen Beweis fand. Allerdings stellte sich später heraus, dass Friedrich Karl Schmidt schon vor Carlitz im Jahr 1928 einen gültigen Beweis publiziert hatte [13, S. 23]. Vergleicht man die Beweismethoden ist, hervorzuheben,

dass Artins Beweis des quadratischen Reziprozitätsgesetz für $\mathbb{F}_q[T]$ auf der Betrachtung von quadratischen Erweiterungen von $\mathbb{F}_q[T]$ beruht, während der Beweis des höheren Reziprozitätsgesetzes von Schmidt und der Beweis von Carliz auf die Koeffizientenerweiterung von $\mathbb{F}_q[T]$ zurückgreifen [14, S. 168].
In der vorliegenden Arbeit wird der Beweis für das allgemeine Reziprozitätsgesetz in Polynombereichen nach Carlitz geführt. Dieser Beweis wurde in der Literatur von Michael Rosen beschrieben, nach der sich diese Arbeit orientiert. Schlussendlich werden die Ringe $\mathbb{Z}$ und $\mathbb{F}_q[T]$ gegenübergestellt. Damit wird insgesamt die folgende Fragestellung beantwortet:

Existiert ein Analogon des quadratischen Reziprozitätsgesetz im Polynomring $\mathbb{F}_q[T]$ über einem endlichen Körper $\mathbb{F}_q$, das dem quadratischen Reziprozitätsgesetz im Ring der ganzen Zahlen $\mathbb{Z}$ entspricht und lässt sich die Beweismethode auf $\mathbb{Z}$ übertragen bzw. nicht übertragen und was ist der Grund dafür?

2 Grundlegende Algebra

2.1 Grundlegende Eigenschaften von Ringen

2.1.1 Monoide und Gruppen

Gruppen und Monoide dienen als eine grundlegende Struktur, die etwa für Ringe und Körper bei der Verknüpfung der Addition gegeben ist. Die Verknüpfung einer Gruppe G ordnet zwei Elementen $g, h \in G$ ein weiteres Element $g \circ h \in G$ zu. Ein einfaches Beispiel dafür sind Rechnungen in verschiedenen Zahlenbereichen. Die Eigenschaften der Verknüpfung gelten aber auch bei Objekten, die nicht als Zahlenbereich interpretiert werden können [4, S. 10].

Definition. Ein Monoid ist eine Menge M mit einer Verknüpfung auf M als Abbildung $M \times M \to M$ mit $(a, b) \mapsto a \cdot b$. Die Verknüpfung ist assoziativ, daher gilt für alle $a, b, c \in M$, dass $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Außerdem besitzt M ein Einselement e, für das $e \cdot a = a = a \cdot e$ gilt [4, S. 11].

Monoide begegnen uns in der Mathematik etwa bei den natürlichen Zahlen mit der Verknüpfung der herkömmlichen Addition. Das neutrale Element respektive Einselement ist dabei die Null. Dafür schreibt man $(\mathbb{N}, +, 0)$. Ein anderes Beispiel für ein Monoid sind wieder die natürlichen Zahlen $\mathbb{N}$ mit der herkömmlichen Multiplikation und dem Einselement der Eins $(\mathbb{N}, \cdot, 1)$. Weitere Beispiele mit der Menge der ganzen Zahlen sind etwa $(\mathbb{Z}, +, 0)$ und $(\mathbb{Z}, \cdot, 1)$ [8, S. 29].

Definition. Eine Gruppe sei eine Menge G mit der Verknüpfung auf G als eine Abbildung $G \times G \to G$ mit $(a, b) \mapsto a \cdot b$, die die folgenden Eigenschaften erfüllt:

1. Assoziativität: Für alle $a, b, c \in G$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. Einselement: Für alle $a \in G$ gibt es ein Element $e \in G$, sodass $e \cdot a = a = a \cdot e$ gilt.
3. Inverses: Für jedes Element $a \in G$ existiert ein inverses Element $a^{-1} \in G$, damit gilt $a \cdot a^{-1} = e = a^{-1} \cdot a$.

[4, S. 11]
Demzufolge ist eine Gruppe ein Monoid G, das für jedes Element ein Inverses besitzt [8, S. 26].

Ist die Verknüpfung der Gruppe zusätzlich kommutativ, also gilt für alle $a, b \in G$ $a \cdot b = b \cdot a$, so heißt die Gruppe abelsch [4, S. 11].

Beispiele für abelsche Gruppen sind $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ mit der gewöhnlichen Addition. Genauso sind die Mengen ohne der Null $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ mit der Verknüpfung der herkömmlichen Multiplikation abelsche Gruppen. Nicht unter den Gruppenbegriff fallen allerdings die natürlichen Zahlen $\mathbb{N}$ mit der Addition oder der Multiplikation und die ganzen Zahlen $\mathbb{Z}$ mit der Multiplikation, da innerhalb dieser Mengen kein Inverses für jedes Element existiert [4, S. 12].

2.1.2 Ringe und Körper

Neben dem Monoid und der Gruppe gibt es noch weitere wichtige algebraische Strukturen, wie Ringe und Körper, auf die im Folgenden eingegangen wird. Das wahrscheinlich naheliegendste Beispiel für einen Ring ist der Ring der ganzen Zahlen $\mathbb{Z}$. Dieser Ring besteht aus zwei Monoiden $(\mathbb{Z}, +, 0)$ und $(\mathbb{Z}, \cdot, 1)$, die mit der Grundlage des Distributivgesetzes miteinander verbunden werden [8, S. 85]. Im allgemeinen Sinne handelt es sich hierbei um eine abelsche Gruppe gemeinsam mit der Definition der Multiplikation. Wie bereits im Beispiel erwähnt, erfüllen innerhalb des Rings die Addition und die Multiplikation das Distributivgesetz [4, S. 28].

Definition. Ein Ring ist eine nicht-leere Menge R mit den Verknüpfungen der Addition $+$ und der Multiplikation $\cdot$. Die Verknüpfungen erfüllen folgende Eigenschaften:

1. $(R, +, 0)$ ist eine kommutative Gruppe.
2. $(R, \cdot, 1)$ ist ein Monoid, die Multiplikation in R ist assoziativ und bezüglich der Multiplikation gibt es ein Einselement.
3. Die Distributivgesetze gelten. Demnach ist für alle $a, b, c \in R$
   a) $(a + b) \cdot c = a \cdot c + b \cdot c$
   b) $c \cdot (a + b) = c \cdot a + c \cdot b$

[4, 8, S. 28, 86]
Sollte die Multiplikation ebenfalls kommutativ sein, so heißt der Ring kommutativ [4, S. 28].

Bemerkung. In allgemeinen Ringen wird das Einselemet der Multiplikation mit 1 bezeichnet und das Nullelement bezüglich der Addition mit 0. Es ist möglich, dass das Einselement und das Nullelement übereinstimmen: $0 = 1$. Dieser Fall tritt allerdings nur im Nullring, bestehend aus einem einzigen Element, der Null, ein [4, S. 28].

Definition. Eine Teilmenge S eines Rings R nennt man Unterring von R, wenn die Teilmenge eine Untergruppe der additiven Gruppe $(R, +, 0)$ und ein Untermonoid des multiplikativen Monoids $(R, \cdot, 1)$ ist [8, S. 87]. Damit ist S mit den Verknüpfungen des Rings R wiederum ein Ring. $S \subset R$ ist eine Ringerweiterung [4, S. 28].

Beispiel. Neben dem Ring der ganzen Zahlen $\mathbb{Z}$ handelt es sich auch bei den rationalen Zahlen $\mathbb{Q}$ mit der gewöhnlichen Addition und Multiplikation um einen Ring. Selbiges

gilt für die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$. Dabei sind $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ Teilringe von $\mathbb{C}$ [8, S. 87]. Da für diese Ringe außerdem die Kommutativität der Multiplikation gilt, handelt es sich um kommutative Ringe [6, S. 43].

Beispiel. Ein weiteres Beispiel für einen Ring ist der Restklassenring $\mathbb{Z}_n$ der ganzen Zahlen modulo n mit der Verknüpfung der Addition und Multiplikation. Im Restklassenring $\mathbb{Z}_n$ beschreibt eine Restklasse alle Zahlen mit demselben Rest bei der Division durch n [6, S. 8]. Der Restklassenring $\mathbb{Z}_n$ wird im Kapitel 2.1.5 Teilbarkeit genauer betrachtet.

Definition. Ein Körper ist ein kommutativer Ring K mit Einselement, wobei jedes Element $x \in K - \{0\}$ ein multiplikatives Inverses besitzt [3, S. 119].

Beispiele für Körper sind $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Die ganzen Zahlen $\mathbb{Z}$ bilden keinen Körper, da sie nicht für jedes Element ein zugehöriges Inverses bezüglich der Multiplikation besitzen [4, S. 29].

Bemerkung. Das Konzept eines Rings ist gegenüber dem eines Körpers weniger streng, da keine Division, sondern lediglich die Addition, die Subtraktion und die Multiplikation verlangt werden [11, S. 3]. Aus diesem Grund wird in weiterer Folge der Fokus auf die Struktur eines Rings gesetzt.

Rechenregeln und Eigenschaften von Ringen

Die nachfolgenden Eigenschaften und Rechenregeln innerhalb eines Rings wirken bereits durch das Rechnen mit gewöhnlichen Zahlen sehr vertraut [6, S. 45].

Lemma 2.1.1. *Das additive Nullelement eines Rings R ist eindeutig bestimmt [6, S. 45].*

Beweis. Angenommen es existieren innerhalb von R die Elemente 0 und $0'$ mit der Eigenschaft $a + 0 = a$ und $a + 0' = a$ für alle $a \in R$. Da die Addition innerhalb von R kommutativ ist, gilt jedoch $a + 0 = 0 + a = a$ und $a + 0' = 0' + a = a$ für jedes a. Sei nun $a = 0'$, so folgt $0' + 0 = 0'$. Setzt man allerdings für $a = 0$, so erhält man $0' + 0 = 0$ und damit $0 = 0'$. Demnach gibt es nur ein additives Nullelement in R [6, S. 45]. □

Ebenfalls gilt innerhalb eines Rings die Eindeutigkeit des additiven Inversen $-a$ für a. Durch das additive Inverse ist die Subtraktion im gewöhnlichen Sinne möglich [6, S. 46].

Lemma 2.1.2. *Es gilt für den Ring R mit $a, b \in R$*

1. $-(-a) = a$
2. $-(a + b) = -a + (-b)$
3. $-(a - b) = -a + b$ *[6, S. 46].*

Beweis.

1. Sei $a \in R$. Für a gilt:

$$a + (-a) = (-a) + a = 0$$

   a ist damit das additive Inverse von $-a$. Es folgt:

$$a = -(-a) \text{ [6, S. 46]}.$$

2. Sei $a, b \in R$. Das additive Inverse von $(a + b)$ ist $-(a + b)$ und umgekehrt. Nun wird gezeigt, dass $-a + (-b)$ ebenfalls additives Inverses ist:

$$(a + b) + (-a + (-b)) = ((a + b) + (-a)) + (-b)$$

   Aufgrund der Assoziativität der Addition, kann umgeklammert werden:

$$= (a + (b + (-a))) + (-b)$$

   Da die Addition kommutativ ist, ist folgender Schritt möglich:

$$= (a + ((-a) + b)) + (-b)$$

   Durch wiederum Umklammern ergibt sich:

$$= ((a + (-a)) + b) + (-b) = (0 + b) + (-b) = b + (-b) = 0.$$

   Daraus folgt, dass $-a + (-b)$ das additive Inverse von $a + b$ ist. Damit folgt außerdem, dass $-(a + b) = -a + (-b)$ gilt [6, S. 46].

3. Um die dritte Eigenschaft zu zeigen, sei wiederum $a, b \in R$. Die folgenden Schritte zeigen, dass $a - b$ das additive Inverse von $-a + b$ ist:

$$\begin{gathered}(a - b) + (-a + b) = (a + (-b)) + (-a + b) \\ = (a + (-b) + (-a)) + b = (a + (-a) + (-b)) + b \\ = 0 + (-b) + b = (-b) + b = 0.\end{gathered}$$

   Daraus folgt nun, dass $-a + b = -(a - b)$ ist [6, S. 46].

□

Durch die eben beschriebene Subtraktion, gilt innerhalb eines Rings das Kürzungsgesetz der Addition, das in weiterer Folge beschrieben wird [6, S. 46].

Proposition 2.1.3. *Seien $a, b, c \in R$. Wenn $a + b = a + c$ gilt, so ist $b = c$ [6, S. 46].*

Beweis. Seien $a, b, c \in R$ und angenommen es gilt $a + b = a + c$. Durch die Addition von $-a$ auf beiden Seiten der Gleichung ergibt sich Folgendes:

$$\begin{aligned} a + b &= a + c \\ -a + (a + b) &= -a + (a + c) \\ (-a + a) + b &= (-a + a) + c \\ 0 + b &= 0 + c \\ b &= c \end{aligned}$$

[6, S. 47] □

Bemerkung. Des Weiteren gilt für $a, b \in R$ $(-a) \cdot b = -(ab) = a \cdot (-b)$ [4, S. 28].

Lemma 2.1.4. *Sei R ein Ring und $a \in R$. Es gilt:*

$$a \cdot 0 = 0 \cdot a = 0 \text{ [6, S. 47].}$$

Beweis. Sei $a \in R$. Zunächst wird zu $a \cdot 0$ ein a addiert:

$$a \cdot 0 + a$$

Anschließend wird mit dem addierten a das neutrale Element multipliziert.

$$= a \cdot 0 + a \cdot 1$$

Da innerhalb des Rings die Distributivgesetze gelten, ist der folgende Schritt möglich

$$= a \cdot (0 + 1)$$

Wenn nun verwendet wird, dass 0 das neutrale Element bezüglich Addition ist, folgt

$$= a \cdot 1 = a = 0 + a.$$

Damit ist gezeigt, dass $a \cdot 0 = 0$ gilt. Der Beweis erfolgt analog für die Gegenrichtung [6, S. 47]. □

2.1.3 Nullteiler und Einheiten

Die zuvor beschriebenen Rechenregeln gelten für die gewöhnlichen ganzen Zahlen. Umgekehrt ist zu beachten, dass einige Eigenschaften, die innerhalb der ganzen Zahlen gelten, nicht für allgemeine Ringe verwendet werden dürfen. Aus $a \cdot (b - c) = 0$ mit $a \neq 0$ folgt etwa nicht automatisch $b = c$ [4, S. 28].

Diese Eigenschaft wird häufig beim Lösen von quadratischen Gleichungen genutzt [6, S. 47]:

Beispiel. Um eine quadratische Gleichung wie beispielsweise $x^2 + 5x - 6 = 0$ zu lösen, wird durch Faktorisieren Folgendes erhalten:

$$(x + 1) \cdot (x - 6) = 0$$

Da innerhalb der reellen Zahlen der Produkt-Null-Satz gilt, zerfällt die quadratische Gleichung in zwei lineare Gleichungen:

$$x + 1 = 0 \text{ und } x - 6 = 0.$$

Daraus ergeben sich für x zwei Lösungen $x = -1$ und $x = 6$ [6, S. 47].

Dass diese Eigenschaft nicht in allen Ringen gilt, zeigt das folgende Beispiel: [6, S. 47].

Beispiel. Das Beispiel des Restklassenrings $\mathbb{Z}_n$ zeigt etwa, dass das Produkt von zwei Elementen, die nicht der Null entsprechen, dennoch Null ergeben kann. In $\mathbb{Z}_6$ ergibt $\overline{2} \cdot \overline{3} = \overline{0}$ [6, S. 47].

Aus diesem Grund ist es essentiell zu wissen, ob das Produkt von Nicht-Null-Elementen Null ergeben kann, wenn Gleichungen in einem Ring gelöst werden sollen [6, S. 47]. Diese Erkenntnis führt zur Definition des Nullteilers.

Definition. Ein Nullteiler ist ein Element a eines Rings R, wenn es dazu ein $b \in R - \{0\}$ gibt, sodass $a \cdot b = 0$ oder $b \cdot a = 0$ [4, S. 29].

Bemerkung. Ein Körper besitzt neben der 0 keine anderen Nullteiler [4, S. 29].

Definition. Sollte es innerhalb eines kommutativen Rings $R \neq 0$ neben der 0 keine weiteren Nullteiler geben, so nennt man R Integritätsring beziehungsweise Integritätsbereich [4, S. 29].

Ein weiteres wichtiges algebraisches Konstrukt ist das der Einheit:

Definition. Die Einheiten eines Rings sind die Menge der durch Multiplikation invertierbaren Elemente von R. Man schreibt:

$$R^* = \{a \in R; \text{ existiert } b \in R \text{ mit } ab = ba = 1\} \text{ [4, S. 29].}$$

Beispiel. Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ein Integritätsring mit den Einheiten $\{-1, 1\}$ [4, S. 29].

Bemerkung. In einem Körper K gilt $K^* = K - \{0\}$. Das heißt jedes Element in K ausgenommen 0 besitzt ein multiplikatives Inverses [3, S. 239].

2.1.4 Vektorraum

Nachfolgend werden die Grundbegriffe des Vektorraums definiert. Später wird die Verallgemeinerung von Vektorräumen für die Körpererweiterung verwendet.

Definition. Man betrachtet einen Körper K und eine Menge V mit den Verknüpfungen der Addition + und Multiplikation $\cdot$. Die Addition ist dabei eine innere Verknüpfung. Für die Verknüpfungen gilt:

$$+ : V \times V \to V, (v, w) \mapsto v + w$$

Die Multiplikation stellt eine äußere Verknüpfung dar:

$$\cdot : K \times V \to V, (\lambda, v) \mapsto \lambda \cdot v$$

Die Menge V mit den eben beschriebenen Verknüpfungen heißt K-Vektorraum, wenn die folgenden Eigenschaften erfüllt sind.

1. V ist mit der Verknüpfung der Addition eine abelsche Gruppe. Hierbei ist der Nullvektor das neutrale Element.
2. Die Skalarmultiplikation ist mit den Verknüpfungen verträglich. Für alle $\lambda, \mu \in K$ und $v, w \in V$ gilt:

$$\begin{gathered}(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v \\ \lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w \\ \lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v \\ 1 \cdot v = v \text{ [7, S. 76]}\end{gathered}$$

Beispiel. Multipliziert man im Körper der komplexen Zahlen $\mathbb{C}$ diese mit reellen Zahlen, so erhält man die folgende Abbildung: $\mathbb{R} \times \mathbb{C} \to \mathbb{C}, (\lambda, a + ib) \mapsto \lambda a + i\lambda b$. Damit ist $\mathbb{C}$ ein $\mathbb{R}$-Vektorraum [7, S. 75, 77].

Die Dimension ist ein wichtiges Instrument, um einem Vektorraum das Maß für seine Größe zuzuordnen. Bevor diese definiert wird, beschreiben wir zunächst das Erzeugendensystem eines Vektorraums [7, S. 86].

Definition. In einem Vektorraum V heißt $(v_i)_{i \in I}$ Erzeugendensystem von V, wenn Folgendes gilt:

$$V = span(v_i)_{i \in I}$$

In anderen Worten: Wenn der Vektorraum durch die Familie der $(v_i)_{i \in I}$ aufgespannt wird, beziehungsweise, wenn jedes $v \in V$ als Linearkombination von endlich vielen v_i geschrieben werden kann, dann ist $(v_i)_{i \in I}$ Erzeugendensystem von V [7, S. 80, 86].

Definition. Die Familie $(v_i)_{i \in I}$ wird linear unabhängig genannt, wenn aus $\sum_{i \in I} a_i v_i = 0$ mit $a_i \in K$ als Koeffizienten sofort für alle $a_i = 0$ folgt [4, S. 71].

Definition. Wenn $(v_i)_{i \in I} \in V$ ein linear unabhängiges Erzeugendensystem ist, so handelt es sich um die Basis von V [7, S. 86].

Definition. Für V einen K-Vektorraum wird die Dimension von V über K folgendermaßen definiert:

$$dim_K V := \begin{cases} \infty, \text{ wenn } V \text{ über keine endliche Basis verfügt.} \\ r, \text{ wenn } V \text{ eine Basis mit der Länge } r \text{ aufweist.} \end{cases} \quad \text{[7, S. 91]}$$

Bemerkung. Die Dimension des K-Vektorraums ist wohldefiniert. Das heißt, jede Basis eines endlich-dimensionalen Vektorraums besitzt dieselbe Länge. Damit ist r unabhängig von der Wahl der Basis [2, S. 44].

2.1.5 Teilbarkeit, ggT, kgV

In diesem Kapitel wird zunächst die Division mit Rest als Basis vieler Algorithmen etwa innerhalb der ganzen Zahlen betrachtet [3, S. 8]. Die wichtigsten Eigenschaften innerhalb des Rings der ganzen Zahlen $\mathbb{Z}$, des Restklassenrings $\mathbb{Z}_n$ oder des Polynomrings $F[T]$ über einem Körper F, auf den im Kapitel 2.3 näher eingegangen wird, gehen auf die Division mit Rest zurück [4, S. 44].

Lemma 2.1.5. *Division mit Rest: Sind $a, b \in \mathbb{Z}$ und $b \neq 0$, so existieren eindeutig bestimmte $q, r \in \mathbb{Z}$, sodass $a = bq + r$ und $0 \leq r < b$ [3, S. 8].*

Beweis. Die Menge $\{w \in \mathbb{Z} | bw > a\}$ ist nicht leer und hat ein kleinstes Element. Sei nun $q := w - 1$ und $r := a - qb$. Woraus die Existenz folgt. Die Eindeutigkeit von q und r ergibt sich aus folgender Überlegung:
Gäbe es für a zwei solcher Darstellungen $bq_1 + r_1 = bq_2 + r_2$, so folgt $r_2 \leq r_1$ und es gilt $0 \leq r_1 - r_2 < b(q_2 - q_1) < |b|$. Damit folgt $r_1 = r_2$ und $q_1 = q_2$ [3, S. 8]. □

In weiterer Folge wird mithilfe der Division mit Rest die Teilbarkeit definiert.

Definition. Die Zahl b teilt a, mit $a, b \in \mathbb{Z}$, wenn $q \in \mathbb{Z}$ existiert, sodass $a = bq$. Man schreibt $a|b$. Die beiden Zahlen sind zueinander teilerfremd beziehungsweise relativ prim, wenn für alle $t \in \mathbb{N}$, die sowohl a als auch b teilen, gilt, dass $t = 1$ ist [3, S. 9].

Definition. Die Zahl $a \in \mathbb{Z}$ ist kongruent zu $b \in \mathbb{Z}$ modulo $m \in \mathbb{N}$, wenn $m|(a - b)$. Dafür schreibt man: $a \equiv b \bmod m$ [3, S. 9].

Bemerkung. Kongruenz ist eine Äquivalenzrelation [3, S. 9].

Da die Bildung des Restklassenrings $\mathbb{Z}_n$ auf die Division mit Rest zurückgeht, wird dieser nun genauer betrachtet. Grundlegend kann $\mathbb{Z}_n$ als abelsche Gruppe gebildet werden. Dabei ist n eine Untergruppe und Normalteiler der additiven Gruppe $\mathbb{Z}$. Damit besteht $\mathbb{Z}_n$ aus Restklassen der Form $x + n$ mit $x \in \mathbb{Z}$ [4, S. 38]. Es gilt, dass n eine ganze Zahl ist und $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ...\overline{n-1}\}$. Für die Kardinalität bedeutet das $|\mathbb{Z}_n| = n$ [6, S. 8].
Die Addition und Multiplikation in den Restklassen modulo n, also in $\mathbb{Z}_n$, sind folgendermaßen definiert:

$$a + b \equiv (a + b) \bmod n$$
$$a \cdot b \equiv (a \cdot b) \bmod n$$

Da hier auch die Kommutativität der Multiplikation gilt $\overline{a \cdot b} = \overline{b \cdot a}$, ist $\mathbb{Z}_n$ ein kommutativer Ring [6, S. 8, 44].

Definition. $(\mathbb{Z}_n, +, \cdot)$ heißt Restklassenring $\mathbb{Z}$ modulo n [7, S. 50].

Betrachten wir nun als Beispiel einfache Rechenbeispiele im Restklassenring $\mathbb{Z}_6$.

$$\overline{5} + \overline{3} = \overline{8} = \overline{2}$$
$$\overline{2} \cdot \overline{5} = \overline{10} = \overline{4}$$
$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$$

Die Addition und Multiplikation im Restklassenring können als Addition beziehungsweise Multiplikation von Äquivalenzklassen gesehen werden. Betrachtet man beispielsweise auch im Restklassenring $\mathbb{Z}_6$ die Rechnung $\overline{5} + \overline{3}$, so ergibt sich durch die Addition von zwei Elementen des Restklassenrings eine Menge von ganzen Zahlen, die bei der Division durch 6 den Rest 2 besitzt: $\{..., -8, 2, 8, 14, 20, 26, 32, ...\}$ [6, S. 9].
Dass die Restklasse als Äquivalenzklasse wohldefiniert ist und Elemente davon eindeutig gewählt werden, folgt aus dem nächsten Lemma:

Lemma 2.1.6. *Gilt für eine positive ganze Zahl n mit $a, b, c, d \in \mathbb{Z}$, dass $a \equiv c$ mod n und $b \equiv d$ mod n, dann gilt ebenfalls $a + b \equiv c + d$ mod n. Des Weiteren gilt $a \cdot b \equiv c \cdot d$ mod n [6, S. 9]. Das heißt, die Addition $+$ und die Multiplikation $\cdot$ sind wohldefiniert, also unabhängig von der Wahl des Vertreters [6, S. 10].*

Beweis. Sei n eine ganze Zahl und angenommen es gilt $a \equiv c$ mod n und $b \equiv d$ mod n, so folgt aus der Definition der Kongruenz, dass n sowohl $c - a$ als auch $d - b$ teilt. Demzufolge existieren $s, t \in \mathbb{Z}$, für die $a - c = sn$ und $b - d = tn$ gilt. Durch Umstellen der Gleichungen folgt $a = c + sn$ und $b = d + tn$. Werden nun die Gleichungen addiert, erhält man

$$a + b = (c + sn) + (d + tn) = (c + d) + (s + t)n.$$

Stellt man diese Gleichung wiederum um, so zeigt sich, dass $(a + b) - (c + d)$ durch n teilbar ist und damit ist $a + b \equiv c + d$ mod n.
Multipliziert man die Gleichungen, so zeigt sich

$$a \cdot b = (c + sn) \cdot (d + tn) = cd + ctn + snd + sntn = cd + (ct + sd + snt)n.$$

Auch hier ist zu sehen, dass $ab - cd$ ein Vielfaches von n ist. Demzufolge gilt $a \cdot b \equiv c \cdot d$ mod n [6, S. 9 f]. □

Trotz einiger Gemeinsamkeiten gibt es auch Unterschiede in der Arithmetik von $\mathbb{Z}_n$ und der gewöhnlichen Arithmetik in $\mathbb{Z}$. Wenn im Ring der ganzen Zahlen $\mathbb{Z}$ für zwei ganze Zahlen a und b gilt, dass $ab = 0$, dann ist $a = 0$ oder $b = 0$ (Produkt-Null-Satz). Innerhalb von $\mathbb{Z}_n$ ist diese Eigenschaft allerdings nicht erfüllt, wie bereits das Beispiel zuvor aus dem Restklassenring $\mathbb{Z}_6$ zeigt [6, S. 10]. Auf diese Besonderheit wurde im Kapitel Nullteiler und Einheiten näher eingegangen.
Als Nächstes wird unter Verwendung der Teilbarkeit der größte gemeinsame Teiler sowie das kleinste gemeinsame Vielfaches definiert.

Definition. Die Zahl $d \in \mathbb{N}$ ist größter gemeinsamer Teiler von $a_1, a_2, ...a_t \in \mathbb{Z}$, wenn ...

1. die Zahl d Teiler für alle a_j, also $d|a_j$ für $j = 1, 2, ...t$ ist.
2. $\tilde{d} \in \mathbb{Z}$ auch alle a_j teilt, so muss $\tilde{d}$ auch d teilen.

Man schreibt $d = \mathrm{ggT}(a_1, a_2, ...a_t)$ [3, S. 13].

Bemerkung. Zwei ganze Zahlen a und b sind zueinander relativ prim, wenn ggT(a,b) $= 1$ [6, S. 12].

Theorem 2.1.7. *Für zwei ganze Zahlen a und b kann der größte gemeinsame Teiler d als Linearkombination von a und b ausgedrückt werden. Damit existieren die ganzen Zahlen x und y mit $d = ax + by$ [6, S. 11].*

Beweis. Sei $S = \{as + bt : s, t \in \mathbb{Z}, as + bs > 0\}$.
Für diesen Beweis wird erst gezeigt, dass die wohlgeordnete Menge S nicht leer ist und anschließend wird für ihr kleinstes Element belegt, dass dieses der größte gemeinsame Teiler von a und b ist.
Um zu zeigen, dass S nicht leer ist, wird $a^2 + b^2$ betrachtet. Hierbei handelt es sich um eine Linearkombination von a und b, die positiv und damit ein Element von S ist.
Sei nun e das kleinste Element von S und d der größte gemeinsame Teiler von a und b. Nach den Eigenschaften von S gibt es ganze Zahlen x und y mit $e = ax + by$. Nachdem d die Zahlen a und b teilt, ist d auch ein Teiler von $e = ax + by$. Aus diesem Grund und da sowohl d als auch e positiv sind, gilt $d \leq e$.
Mittels Divisionsalgorithmus kann folgende Gleichheit beschrieben werden:

$$a = qe + r \text{ mit den ganzen Zahlen } q, r \text{ und } 0 \leq r < e$$

Aus Umformungen der Gleichung folgt:

$$r = a - qe = a - (ax + by) = a - qx - qbx = a(1 - qx) + b(-qy)$$

Für $r < 0$ wurde nun gezeigt, dass $r \in S$. Das ist allerdings nicht möglich, da $r < e$ und e das kleinste Element von S ist. Damit muss $r = 0$ gelten und demnach $a = qe$, also ist a ein Teiler von e. Analog kann für b gezeigt werden, dass es ein Teiler von e ist. Dies impliziert, dass $e \leq d$ gilt, da d der größte gemeinsame Teiler von a und b ist.
Zuvor wurde bereits $d \leq e$ gezeigt und demnach erhält man $e = d = ax + by$ [6, S. 12]. □

Ebenso kann das kleinste gemeinsame Vielfaches definiert werden:

Definition. Die Zahl m ist ein kleinstes gemeinsames Vielfaches von $a_1, a_2, ...a_t \in \mathbb{Z}$, wenn ...

1. die Zahl m ein Vielfaches aller a_j ist, also $a_j | m$ für $j = 1, 2, ...t$.
2. $\tilde{m}$ auch ein Vielfaches aller a_j ist, so muss das kleinste gemeinsame Vielfache m die Zahl $\tilde{m}$ teilen.

Man schreibt $m = \text{kgV}(a_1, a_2, ...a_t)$ [3, S. 14].

Eigenschaften der Teilbarkeit

Korollar: Für zwei ganze Zahlen a und b mit dem größten gemeinsamen Teiler d gilt: Wenn c ein Teiler von a und b ist, dann teilt c auch d [6, S. 12].

Beweis. Wie bereits beschrieben, gilt für den größten gemeinsamen Teiler $d = ax + by$ mit ganzen Zahlen x, y. Wenn c ein gemeinsamer Teiler von a und b ist, dann teilt c auch ihren größten gemeinsamen Teiler d [6, S. 12]. □

2.1.6 Ideale und Faktorringe

Ideale sind für Ringe von großer Bedeutung [4, S. 34].

Definition. Eine Teilmenge I eines Rings R heißt Ideal in R, wenn I eine additive Untergruppe von R ist und, wenn für $r \in R, a \in I \Rightarrow ra \in I$. Demzufolge sind im Ideal Addition sowie Multiplikation abgeschlossen [4, 6, S. 35, S. 77].

Bemerkung. Die Forderung der Abgeschlossenheit der Addition ist weniger streng, als die der Multiplikation für ein Ideal: Ein Produkt aus zwei Elementen des Ideals I muss in I liegen, zusätzlich muss das Produkt aus einem Element von I und einem Element von R wiederum in I liegen [6, S. 77].

Beispiel. Für den Ring der ganzen Zahlen $\mathbb{Z}$ und einer ganzen Zahl n ist die Menge $n\mathbb{Z}$ ein Ideal. Die Abgeschlossenheit bezüglich der Addition ist erfüllt, da für $x, y \in n\mathbb{Z}$ mit $a, b \in \mathbb{Z}$ und $x = na$ und $y = nb$ folgende Eigenschaft gilt: $x + y = na + nb = n(a + b)$. Genauso gilt für die Multiplikation und ein Element $r \in \mathbb{Z}$, dass das Produkt mit einem Element des Ideals wiederum im Ideal liegt: $rx = xr = r(na) = n(ra) \in n\mathbb{Z}$ [6, S. 77].

Bemerkung. Innerhalb eines jeglichen kommutativen Rings R mit $a \in R$ ist die Menge $aR = \{ar : r \in R\}$ Ideal von R [6, S. 77].

Bemerkung. Ein Ideal eines Rings ist nicht zwingend ein Unterring, da Ideale nicht das Einselement der Multiplikation als Element führen müssen. In jedem Ring R sind aber die trivialen Ideale, wie das Nullideal $\{0\}$ und das Einheitsideal R enthalten. Sollte R ein Körper sein, dann sind das Einheitsideal und das Nullideal die einzigen Ideale von R [4, S. 35].

Theorem 2.1.8. *Für einen kommutativen Ring $R \neq 0$ gilt: R ist ein Körper, genau dann, wenn die einzigen Ideale von R das Nullideal $= 0$ und das Einheitsideal, also R selbst, sind [8, S. 102].*

Beweis. Um diese Aussage zu beweisen, werden beide Implikationen getrennt voneinander betrachtet: Sei zum einen R ein Quotientenring und I ein Nicht-Null-Ideal von R. Wenn $a \neq 0$ und $a \in I$ ist, dann gilt $a \cdot a^{-1} = 1$. Das heißt, a besitzt ein multiplikatives Inverses in R. Es gilt, dass das einzige Ideal eines Rings, das das Einselement 1 enthält, der Ring selbst ist. Das folgt daraus, dass I dann jedes Element $x = x \cdot 1$ des Rings enthalten muss. Es folgt $I = R$ [8, S. 103].
Sei nun zum anderen R ein kommutativer Ring, dessen einzige Ideale 0 und R sind. Für $a \neq 0$ und $a \in R$ folgt $(a) \neq 0$ und $(a) = R$. Weiters muss das Einselement $1 \in (a)$ und damit auch ein $c \in R$ sein, sodass $a \cdot x = 1$. Damit ist jedes Nicht-Null-Element von R invertierbar und R ist ein Körper [8, S. 103]. □

Definition. Sei R ein Ring und I ein Ideal von R. Wenn $a \in R$ ist, dann ist die Nebenklasse $a + I$ folgendermaßen definiert: $a + I = \{a + x : x \in I\}$ [6, S. 78].

Beispiel. Die Nebenklassen für das Ideal $5\mathbb{Z}$ entsprechen den Restklassen modulo 5.

$$\overline{0} = 0 + 5\mathbb{Z}$$
$$\overline{1} = 1 + 5\mathbb{Z}$$
$$\overline{2} = 2 + 5\mathbb{Z}$$
$$\overline{3} = 3 + 5\mathbb{Z}$$
$$\overline{4} = 4 + 5\mathbb{Z} \text{ [6, S. 79]}$$

Lemma 2.1.9. *Sei I ein Ideal eines Rings R, so gilt für $a, b \in R$ die folgende Eigenschaft:*

$$a + I = b + I \text{ genau dann, wenn } a - b \in I \text{ [6, S. 80].}$$

Beweis. Für $a, b \in R$ wird angenommen, dass $a + I = b + I$ gilt. Da $0 \in I$, erhält man $a = a + 0 \in a + I$ und durch die zuvor angenommene Gleichheit auch $a \in b + I$. Damit gibt es ein x aus dem Ideal I mit der Eigenschaft $a = b + x$. Durch Umstellen der Gleichung erhält man $a - b = x \in I$. Sei nun x ein Element des Ideals mit $x = a - b$, so gilt $a = b + x$ und damit $a \in b + I$ [6, S. 80].
Demzufolge ist für jedes $y \in I$ die folgende Gleichheit gültig, da das Ideal I abgeschlossen bezüglich der Addition ist: $a + y = b + (x + y) \in I$. Daraus folgt, $a + I \subseteq b + I$. Genauso kann die Gegenrichtung gezeigt werden, wenn $-x = b - a \in I$ verwendet wird und daraus folgt, dass $b + I \subseteq a + I$. In der Schlussfolgerung gilt demnach: $a + I = b + I$ [6, S. 80]. □

Beispiel. Im Allgemeinen können Äquivalenzklassen modulo n mit Nebenklassen von $n\mathbb{Z}$ gleichgesetzt werden. Insofern gilt $a \equiv b \pmod{n}$ genau dann, wenn $a - b$ ein Vielfaches von n ist, oder anders ausgedrückt $a - b \in n\mathbb{Z}$. Genauso gilt für ein Ideal I eines Rings R, dass $x \equiv y \pmod{I}$ genau dann gilt, wenn $x - y \in I$. Damit ist für jedes $a \in R$ die Nebenklasse $a + I$ eine Äquivalenzklasse von a [6, S. 80].

Allgemein gilt für jede positive ganze Zahl n, dass die Restklasse $\overline{a}$ einer ganzen Zahl a modulo n der Nebenklasse $a + n\mathbb{Z}$ des Ideals $n\mathbb{Z}$ entspricht [6, S. 79].

Definition. Für ein Ideal I eines Rings R definieren wir nun R/I als Menge der Nebenklassen mit $R/I = \{a + I : a \in R\}$ [6, S. 79].
Dabei sind $+$ und $\cdot$ wohldefiniert:

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = (ab) \cdot I \text{ [6, S. 79]}$$

Lemma 2.1.10. *Die Rechenoperationen der Nebenklassen sind bezüglich $+$ und $\cdot$ wohldefiniert. Seien $a, b, c, d \in R$ eines Rings R und I das Ideal des Rings. Wenn $a + I = c + I$ und $b + I = d + I$ gilt, dann gilt auch:*

1. $(a + b) + I = (c + d) + I$
2. $ab + I = cd + I$ *[6, S. 80].*

Beweis. Seien $a, b, c, d \in R$ und $a + I = c + I$ und $b + I = d + I$. Weiters werden zwei Elemente x, y des Ideals I folgendermaßen definiert: $x = a - c$ und $y = b - d$. Dann gilt:

$$(a + b) - (c + d) = a + b - c - d = (a - c) + (b - d) = x + y \in I$$

Damit folgt $(a + b) + I = (c + d) + I$.
Für die zweite Aussage des Lemmas wird die Gleichung umgestellt: $a = c + x$ und $b = d + y$.

$$ab = (c + x)(d + y) = c(d + y) + x(d + y) = cd + (cy + xd + xy)$$

Alle Summanden der Klammer sind Elemente des Ideals, da x und y Elemente des Ideals sind. Damit ist auch die Summe Teil des Ideals und es folgt $ab+I = cd+I$ [6, S. 80]. □

Durch die Wohldefiniertheit der Addition und Multiplikation kann das nächste Theorem formuliert werden:

Theorem 2.1.11. *Sei I das Ideal eines Rings R. Die Menge der Nebenklassen R/I bildet mit der Addition und Multiplikation einen Ring [6, S. 80].*

Beweis. Um zu zeigen, dass R/I einen Ring bildet, müssen mehrere Eigenschaften überprüft werden. Die meisten Eigenschaften folgen sofort aus den Eigenschaften von R. Um zu zeigen, dass die Addition von Nebenklassen kommutativ ist, wird die Eigenschaft der Kommutativität der Addition des Rings R verwendet:
Sei $a, b \in R$, so gilt

$$(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I).$$

Das neutrale Element bezüglich der Addition ist $0+I$ für den Ring R/I, da 0 das neutrale Element aus R ist. Sei $a + I \in R/I$, so folgt

$$(a + I) + (0 + I) = (a + 0) + I = a + I.$$

Analog zur Addition folgt, dass $(1+I)$ das neutrale Element bezüglich der Multiplikation ist, da

$$(a + I) \cdot (1 + I) = (a \cdot 1) + I = a + I \text{ und}$$
$$(1 + I) \cdot (a + I) = (1 \cdot a) + I = a + I \text{ ist.}$$

Das inverse Element bezüglich der Addition ist $-a + I$, weil

$$(a + I) + (-a + I) = (a + (-a)) + I = 1 + I \text{ gilt.}$$

Daraus folgt die Aussage, dass R/I ein Ring ist [6, S. 81]. □

Definition. Der Ring R/I wird Faktorring von R genannt [6, S. 81].

Beispiel. Das wichtigste Beispiel für einen Faktorring ist $\mathbb{Z}/n\mathbb{Z}$ und es gilt $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ der Restklassenring, der im Kapitel 2.1.5 definiert wurde [6, S. 81].

Die nachfolgenden Definitionen sind für die weiteren Aussagen relevant.

Definition. Ein Ideal P eines Rings R ist ein Primideal, wenn $P \neq R$ ist und wenn für zwei Elemente $a, b \in R$ mit $a \cdot b \in P$ folgt, dass $a \in P$ oder $b \in P$ [4, S. 41].

Definition. Ein Ideal m eines Rings R heißt maximal, wenn $m \neq R$ und wenn kein anderes Ideal a in R, das m als echte Teilmenge ohne Gleichheit besitzt, existiert: $m \subsetneq a \subsetneq R$ [9, S. 87].

Beispiel. Betrachtet man nun das Ideal $n\mathbb{Z}$, wobei n aus den natürlichen Zahlen stammt und keine Primzahl ist, so kann n als Produkt zweier ganzer Zahlen $r, s > 1$ geschrieben werden. Es gilt jedoch $r \notin n\mathbb{Z}$ und $s \notin n\mathbb{Z}$. Damit folgt, dass $n\mathbb{Z}$ weder Primideal noch maximales Ideal im Ring der ganzen Zahlen $\mathbb{Z}$ darstellt [9, S. 87].

Beispiel. Das Ideal $0\mathbb{Z} = \{0\}$ erfüllt die Bedingungen für ein Primideal, es ist aber nicht maximal [9, S. 87].

Theorem 2.1.12. *Ist R ein kommutativer Ring mit Eins und I ein Ideal, so gelten die beiden folgenden Aussagen:*

1. *Das Ideal I ist prim $\iff$ R/I ist ein Integritätsring.*
2. *Das Ideal I ist maximal $\iff$ R/I ist ein Körper [3, S. 133].*

Beweis. Zunächst wird die erste Äquivalenz gezeigt: Vorausgesetzt das Ideal I ist prim, dann gilt

$$ab + I = (a + I)(b + I) = 0_{R/I} = I \iff a \cdot b \in I.$$

Damit ist $a \in I$ oder $b \in I$ und somit folgt auch

$$a + I = I = 0_{R/I} \text{ oder } b + I = I = 0_{R/I}.$$

Ergo existieren in R/I keine Nullteiler und R/I ist ein Integritätsring. Für die Gegenrichtung wird angenommen, dass R/I ein Integritätsring ist. Infolgedessen gilt:

$$a \cdot b \in I \iff (a + I)(b + I) = I = 0_{R/I}.$$

Weiterhin folgt

$$a + I = 0_{R/I} = I \text{ oder } b + I = 0_{R/I} = I \text{ dies impliziert, dass } a \in I \text{ oder } b \in I.$$

Damit ist die Definition eines primen Ideals erfüllt [3, S. 133].

Um die zweite Äquivalenz zu zeigen, nehmen wir an, dass $m \subset R$ maximal ist und $a + m \neq 0_{R/m} = m$ ist. Dementsprechend ist $a \notin m$. Es gilt:

$$R = m + (a) = \{w + ba | w \in m, b \in R\}.$$

Dies ist äquivalent dazu, dass ein $b \in R$ und $w \in m$ existiert mit $a \cdot b + w = 1$. Weiters ist äquivalent, dass es ein $b \in R$ mit $(a + m)(b + m) = 1 + m = 1_{R/m}$ gibt. Daraus folgt, dass R/m ein Körper ist und es gilt $(a + m)^{-1} = b + m$.
Für die Umkehrung sei R/m ein Körper und $a \notin m$. Dann gibt es ein $b \in R$ mit $(a+m)(b+m) = 1_{R/m}$. Dazu ist die folgende Aussage äquivalent: $m+(a) = R$. Es folgt, dass $m \subsetneq I$ und $I = R$ [3, S. 133 f]. □

Korollar 2.1.13. *Zusammenfassend ist ein Ideal I maximal genau dann, wenn der Faktorring R/I ein Körper ist und ein Ideal I ist prim, wenn R/I ein Integritätsbereich ist. Aus Theorem 2.1.12 folgt, dass jedes maximale Ideal zwangsweise auch ein Primideal ist [9, S. 87].*

Zum Abschluss des Kapitels wird der Chinesische Restsatz formuliert und ein Beispiel gerechnet. Zuvor betrachten wir eine Definition, die dafür benötigt wird:

Definition. Seien I_1 und I_2 zwei Ideale eines kommutativen Rings R. Diese Ideale heißen teilerfremd, wenn $I_1 + I_2 = R$ gilt. Das ist äquivalent zu der Bedingung, dass es Elemente $a \in I_1$ und $b \in I_2$ mit $a + b = 1$ gibt [9, S. 89].

Theorem 2.1.14. *Sei R ein kommutativer Ring und $I_1, ...I_n$ die Ideale in R, die zueinander paarweise teilerfremd sind, dann gilt:*

1. *Jedes Ideal I_j mit $1 \leq j \leq n$ ist teilerfremd zum Produkt $\prod_{i \neq j} I_i$.*
2. *Das Produktideal und das Schnittideal sind ident.*

$$\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$$

3. *(Chinesischer Restsatz)*
   Bei der folgenden Abbildung handelt es sich um einen Ringhomomorphismus:

$$x \mapsto (x + I_1, ..., x + I_n)$$
$$\varphi : R \to \prod(R/I_j)$$

   Dieser Ringhomomorphismus führt zu einem Isomorphismus zwischen den folgenden Quotientenringen $R/\bigcap_j I_j \to \prod_j (R/I_j)$.

[9, S. 90]

Beweis. Für den Beweis des Theorems werden die Teilaussagen separat betrachtet:

1. Durch die Teilerfremdheit gilt für alle $i \neq j$, dass es Elemente $x_i \in I_i$ und $y_j \in I_j$ gibt, sodass

$$x_i + y_i = 1.$$

   Das heißt, das Einselement des Rings kann als Summe von einem Element aus I_i und einem Element aus I_j geschrieben werden. In weiterer Folge betrachten wir das Produkt der Gleichungen $x_i + y_i = 1$ für alle $i \neq j$. Es folgt, dass das Einselement folgendermaßen ausgedrückt werden kann:

$$1 = \prod_{i \neq j}(x_i + y_i) = y_1 \cdot ... \cdot y_n + I \text{ mit } I \in I_j.$$

   Das heißt, das Ideal I_j ist teilerfremd zum Produkt der anderen Ideale $\prod_{i \neq j} I_i$.

2. Diese Aussage wird durch die Induktion über n gezeigt. Im ersten Abschnitt wurde bereits der Fall $n = 2$ betrachtet. Sei nun $n > 2$. Als Induktionsvoraussetzung sei das Ergebnis für $I_1, ...I_{n-1}$ richtig. Dieses Produkt wird J genannt.

$$\prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i =: J$$

Wird nun die Aussage aus 1. verwendet, folgt

$$\prod_{i=1}^{n} I_i = \prod_{i=1}^{n-1} I_i \cdot I_n = J \cdot I_n = J \cap I_n = \bigcap_{i=1}^{n} I_i.$$

Damit ist der Induktionsschritt abgeschlossen und die Aussage für n Ideale gezeigt.

3. Sei nun wiederum $n > 2$ und $x_1, ..., x_n \in R$. Wie bereits gezeigt, sind die Ideale I_j mit $j = 1, ..., n$ und $\prod_{i \neq j} I_i$ zueinander teilerfremd. Aus diesem Grund gibt es Elemente $u_j \in I_j$ und $v_j \in \prod_{i \neq j} I_i$, für die $u_j + v_j = 1$ gilt. Somit gilt auch

$$v_j \equiv \delta_{ij} \bmod I_i.$$

In weiterer Folge wird ein Element x konstruiert. Dazu setzen wir $x = \sum_{j=1}^{n} v_j x_j$. Dieses Element stimmt modulo jedem Ideal I_j mit x_j überein: $x \equiv x_j \bmod I_j$. Die Abbildung $\varphi : R \to \prod(R/I_j)$ mit $\varphi(x) = (x \bmod I_1, ..., x \bmod I_n)$ ist surjektiv. Dies gilt, weil für jede Restklasse $x_j \in R/I_j$ ein Element x gefunden werden kann, dass diese Restklasse repräsentiert. Der Kern der Abbildung φ ist $\bigcap I_j$, da x dafür in allen Idealen I_j liegen muss. Wendet man nun die zweite Teilaussage an, so folgt

$$\bigcap I_j = \prod I_j.$$

Damit ist die Aussage gezeigt [9, S. 90].

□

Wendet man das Theorem 2.1.14 an, so wird dies der Chinesischer Restsatz genannt. Der Satz sagt aus, dass für paarweise teilerfremde Ideale $I_1, ..., I_n$ in R und $x_1, ..., x_n \in R$ das System von Kongruenzen

$$X \equiv x_j \bmod I_j$$

immer lösbar ist [9, S. 90].

Bemerkung. Die Anwendung des Chinesischen Restsatzes in den ganzen Zahlen ist wahrscheinlich die bekannteste. Hierfür sind $m_1, ..., m_n$ relativ prime natürliche Zahlen. Weiter definieren wir das Produkt dieser Zahlen mit $m := m_1 \cdot ... \cdot m_n$. Dann ist der Quotientenring $\mathbb{Z}/m\mathbb{Z}$ isomorph zum Produkt der Quotientenringe $\prod_i(\mathbb{Z}/m_i\mathbb{Z})$, denn die Ideale (m_j) sind zueinander relativ prim, also ist $am_i + bm_i = 1$ und es folgt $(m_i) + (m_j) = \mathbb{Z}$, weil $\bigcap_{i=1}^{n}(m_i) = (m)$ [9, S. 90].

Beispiel. Durch den Chinesischen Restsatz können Systeme von Kongruenzen wie das Folgende gelöst werden.

$$\begin{aligned} X &\equiv 1 \bmod 2 \\ X &\equiv 2 \bmod 3 \\ X &\equiv 3 \bmod 5 \end{aligned}$$

Erst berechnen wir das Produkt $m = 2 \cdot 3 \cdot 5 = 30$. Das heißt, X wird eine Lösung in $\mathbb{Z}/30\mathbb{Z}$ sein. Nun werden die Teilprodukte von m berechnet.

$$\begin{aligned} m_1 &= \tfrac{m}{2} = 15 \\ m_2 &= 10 \\ m_3 &= 6 \end{aligned}$$

In weiterer Folge werden die multiplikativen Inversen der Teilprodukte m_i mithilfe des Euklidischen Algorithmus bestimmt.

$$\begin{aligned} y_1 \cdot 15 \equiv 1 \bmod 2 \quad &\Rightarrow (-7) \cdot 2 + 1 \cdot 15 = 1 \quad \Rightarrow y_1 = 1 \\ y_2 \cdot 10 \equiv 1 \bmod 3 \quad &\Rightarrow 7 \cdot 3 + (-2) \cdot 10 = 1 \quad \Rightarrow y_2 = -2 \\ y_3 \cdot 6 \equiv 1 \bmod 5 \quad &\Rightarrow (-1) \cdot 5 + 1 \cdot 6 = 1 \quad \Rightarrow y_3 = 1 \end{aligned}$$

Die berechneten Werte werden in die Formel $X = a_1 \cdot y_1 \cdot m_1 + a_2 \cdot y_2 \cdot m_2 + a_3 \cdot y_3 \cdot m_3$ eingesetzt. Dann zeigt sich, dass $x = 1 \cdot 1 \cdot 15 + 2 \cdot (-2) \cdot 10 + 3 \cdot 1 \cdot 6 = -7$ eine Lösung ist [9, S. 90 f].

2.2 Faktorielle Ringe, Hauptidealringe und Euklidische Ringe

Nachdem nun die Struktur von allgemeinen Ringen bekannt ist, werden im folgenden Kapitel Ringe mit speziellen Eigenschaften beschrieben. Dazu zählen etwa faktorielle Ringe, in denen die Möglichkeit der Primfaktorisierung besteht [3, S. 149].
Zunächst werden essentielle Begriffe in allgemeinen Ringen ohne Nullteiler definiert:

Definition. Wir betrachten einen Integritätsbereich R. Für ein Element $a \in R$ ist $(a) = aR$ das Hauptideal [9, S. 92].

1. Für $a, b \in R$ ist a ein Teiler von b (man schreibt: $a|b$), wenn es ein $c \in R$ gibt, sodass $ac = b$. Es gilt $(b) \subset (a)$ [9, S. 92].

2. Die beiden Elemente $a, b \in R$ sind assoziiert (man schreibt: $a \sim b$), wenn $a|b$ und $b|a$. Das heißt $(a) = (b)$ [9, S. 92].

3. Ein Element $p \in R$ ist ein Primelement, wenn (p) ein Primideal in R ist und $p \neq 0$ [9, S. 93].

4. Ein Element $i \in R$ heißt irreduzibel, wenn $i \neq 0$ und keine Einheit ist (also $i \notin R^*$) und wenn aus $i = ab$ folgt, dass a oder b eine Einheit ist. Das heißt, dass das Element nicht weiter in Faktoren zerlegbar ist [9, S. 93].

Theorem 2.2.1. *Für einen Integritätsbereich R und ein Element $p \in R$ gelten, dass wenn p prim ist, so impliziert dies, dass p irreduzibel ist [3, S. 150].*

Beweis. Sei p ein Primelement und $p = (a \cdot b)$. Dann gilt $p|(a \cdot b)$. Aus der Definition folgt, dass $p|a$ oder $p|b$ gilt. Angenommen $p|a$, dann kann $a = p \cdot r$ geschrieben werden. Durch Einsetzen in die Gleichung erhält man $p = p \cdot r \cdot b$. Wird nun die Kürzungsregel angewendet, folgt $1 = r \cdot b$ und somit $b \in R^*$. Das heißt, b ist eine Einheit und damit ist p irreduzibel [3, S. 150]. Der Beweis erfolgt analog im Fall $p|b$. □

Das folgende Beispiel zeigt, dass diese Aussage nicht gültig ist, wenn die Eigenschaften des Integritätsbereichs nicht erfüllt sind:

Beispiel. Betrachten wir den Restklassenring $\mathbb{Z}_6$. Das Element $\overline{2}$ ist prim, jedoch nicht irreduzibel. $\overline{2}$ ist keine Einheit, weil es kein multiplikatives Inverses in $\mathbb{Z}_6$ besitzt. Es gilt $\overline{2} \cdot \overline{4} = \overline{2}$, wobei auch $\overline{4}$ keine Einheit ist. Damit ist gezeigt, dass $\overline{2}$ nicht irreduzibel ist [3, S. 150].

2.2.1 Faktorielle Ringe

Definition. Gilt innerhalb eines Integritätsbereichs R, dass jedes Element a des Integritätsbereichs, das nicht Null und keine Einheit ist, sich als Produkt von Primelementen $p \in A$ schreiben lässt, so ist R ein faktorieller Ring.

$$a = p_1 \cdot ... \cdot p_n \text{ [9, 3, S. 95, S. 151]}$$

Beispiel. Hierfür kann wiederum der Ring der ganzen Zahlen als Beispiel genannt werden. [3, S. 152].

Bemerkung. Weiters gilt, dass alle Körper faktorielle Ringe sind [4, S. 49].

Theorem 2.2.2. *Sei R ein faktorieller Ring und a ein Element von R. Es gilt ein Element a ist prim genau dann, wenn a irreduzibel ist [3, S. 151].*

Beweis. Die Implikation a ist prim $\Longrightarrow$ a ist irreduzibel wurde bereits im Theorem zuvor gezeigt. Für die Umkehrung betrachten wir a in folgender Darstellung

$$a = p_1 \cdot ... \cdot p_n.$$

Wäre $n \geq 2$, so widerspricht dies der Definition der Unzerlegbarkeit. Das heißt, a wäre nicht irreduzibel. Damit muss $n = 1$ und $a = p_1$ gelten und die Aussage, dass a prim ist, ist gezeigt [3, S. 151]. □

Nun wird die Primfaktorzerlegung genauer betrachtet. Das folgende Theorem zeigt die Eindeutigkeit dieser:

Theorem 2.2.3. *Ein Integritätsbereich R ist genau dann ein faktorieller Ring, wenn jedes Element $a \in R$ das nicht Null und keine Einheit ist, als eindeutiges Produkt von irreduziblen Elementen geschrieben werden kann. Das heißt, die Darstellung ist eindeutig bis auf die Einheiten und die Reihenfolge der Elemente [3, S. 151].*

Beweis. Sei R ein faktorieller Ring, das heißt es existiert eine Zerlegung in prime Elemente. Wir betrachten zwei solcher Zerlegungen:

$$p_1 \cdot ... \cdot p_r = q_1 \cdot ... \cdot q_s$$

Durch die prime Eigenschaft eines jeden Elements gilt $p_1 | q_j$. Für den Fall $j = 1$ gilt dementsprechend $q_1 = w \cdot p_1$. Da q_1 nach Voraussetzung irreduzibel ist, muss w eine Einheit sein. Setzt man diese Gleichung in die erste ein, folgt der nächste Schritt aus der Kürzungsregel:

$$p_1 \cdot ... \cdot p_r = w \cdot p_1 \cdot q_2 \cdot ... \cdot q_s$$
$$p_2 \cdot ... \cdot p_r = (w \cdot q_2) \cdot q_3 \cdot ... \cdot q_s$$

Wird dieser Schritt bis r wiederholt, folgt die Eindeutigkeit der Primfaktorzerlegung.
Nun ist noch zu zeigen, dass jedes $a \in R$ mit a irreduzibel $\Longrightarrow$ a prim gilt. Dafür betrachten wir ein irreduzibles Element q mit $q | a \cdot b$. Für den Fall, dass a eine Einheit ist, teilt q das Element b. Sollte $a = 0$ sein, dann ist q ein Teiler von a. Im Fall, dass a und b keine Einheiten und nicht Null sind, kann das Produkt der beiden Elemente auch folgendermaßen geschrieben werden (mit $w \notin R^*$)

$$a \cdot b = q \cdot w.$$

Zuvor wurde vorausgesetzt, dass a, b und w in irreduzible Elemente zerlegt werden können. Wird diese Zerlegung eingesetzt und verwenden wir die bereits gezeigte Eindeutigkeit, so folgt, dass q einer der irreduziblen Faktoren von a oder b ist. Damit ist q ein Teiler von a oder b und dies zeigt, dass q prim ist [3, S. 152]. □

Bemerkung. Aus der Eindeutigkeit der Primfaktorzerlegung lässt sich in faktoriellen Ringen die Existenz des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen zeigen [4, S. 50]. Festzuhalten ist:

1. Innerhalb eines faktoriellen Rings R besitzt jedes Element $a \in R - \{0\}$ eine Primfaktorzerlegung in folgender Gestalt: $a = \epsilon p_1^{v_1} \ ... \ \epsilon p_r^{v_r}$. Dabei ist ϵ eine Einheit. Sollte bereits a eine Einheit sein, so gilt für die Exponenten $v_i = 0$ [4, S. 49]. Für die Primfaktorzerlegung wird ein Vertretersystem P bezüglich Assoziiertheit von Primelementen festgelegt. Dabei gilt in der Teilmenge P, die aus den Primelementen besteht, dass P aus jeder Klasse zueinander assoziierter Primelemente exakt eines enthält [4, S. 50].

2. Wir betrachten wiederum einen faktoriellen Ring R mit P, dem Vertretersystem der Primelemente von R. Dabei ist für die Elemente $x_1, ...x_n \in R - \{0\}$ die Primfaktorzerlegung gegeben durch

$$x_i = \epsilon \prod_{p \in P} p^{v_p(x_i)} \text{ mit } i = 1, ..., n.$$

   Es existiert der $ggT(x_1, ..., x_n)$ und das $kgV(x_1, ..., x_n)$ und es gilt bis auf Assoziiertheit:

$$ggT(x_1, ..., x_n) = \prod_{p \in P} p^{min(v_p(x_1), ..., v_p(x_n))}$$
$$kgV(x_1, ..., x_n) = \prod_{p \in P} p^{max(v_p(x_1), ..., v_p(x_n))}$$

   [4, S. 50].

2.2.2 Hauptidealringe

Definition. Ein Ideal I, das nur von einem einzigen Element erzeugt wird, ist ein Hauptideal [6, S. 78]. Das heißt, I ist von der Form

$$I = (a) := \{xa, x \in R\} \text{ [9, S. 88].}$$

Die trivialen Ideale eines Rings, das Nullideal $\{0\} = (0)$ und das Einheitsideal $R = (1)$ bilden auch Hauptideale [4, S. 33, 35].

Definition. Ein Integritätsbereich, der die Eigenschaft besitzt, dass jedes Ideal aus einem einzigen Element erzeugt werden kann, heißt Hauptidealring [6, S. 78]. Das Hauptideal, das von dem Element a entsteht, weist demnach die nachstehende Form auf: $I = (a)$ [3, S. 156].

Beispiel. Beim Ring der ganzen Zahlen $\mathbb{Z}$ handelt es sich ebenfalls um einen Hauptidealring [4, S. 35]. Dabei haben die Ideale, wie bereits erwähnt, die folgende Gestalt: $n\mathbb{Z} = (n)$ wobei $n \in \mathbb{N}$ ist [9, S. 87].

Betrachtet man die beschriebenen Theoreme aus dem Kapitel zuvor jedoch innerhalb eines Hauptidealrings, so führen sie zu stärkeren Aussagen [4, S. 47].

Theorem 2.2.4. *Sei R ein Hauptidealring und $I = (f) \neq 0$ ein Ideal in R. Die folgenden Aussagen sind zueinander äquivalent:*

i) I ist Primideal.

ii) f ist irreduzibel $\iff$ f ist prim.

iii) I ist Maximalideal.

[4, S. 47], [9, S. 93]

Beweis. Sei $I = (f)$ ein Hauptideal im Hauptidealring R.
Erst wird die Implikation i) $\implies$ ii) gezeigt. Wenn $I = (f)$ prim ist, dann folgt aus Theorem 2.1.12., dass $R/(f)$ ein Integritätsbereich ist, also nullteilerfrei. Angenommen f wäre reduzibel, also wenn $f = g \cdot h$ mit g, h keine Einheiten gelte, würde folgen, dass

$$\overline{g} \cdot \overline{h} = \overline{g \cdot h} = \overline{f} = \overline{0} \text{ mit } g, h \in R/I.$$

Da aber g und h keine Einheiten sind, folgt, dass $\overline{g}, \overline{h} \neq 0$ in R/I. Dies führt zum Widerspruch der Annahme, dass R/I Integritätsbereich ist, denn er wäre nicht nullteilerfrei, wenn f reduzibel ist. Demnach folgt, dass f irreduzibel ist.
Nun betrachten wir die nächste Implikation ii) $\implies$ iii). Sei (f) irreduzibel. Angenommen (f) ist nicht maximal, das heißt, es existiert ein Ideal I, sodass $(f) \subsetneqq I \subsetneqq R$. Da R ein Hauptidealring ist, gilt $I = (g)$ und wir erhalten $(f) \subset (g)$ und damit $f \in (g)$. Daraus folgt $f = g \cdot h$ mit $h \in R$. Dies widerspricht der Behauptung, dass h keine Einheit ist, da sonst $(f) = I = (g)$ gelte und dass h keine Einheit ist, da sonst $I = (g) = R$. Damit liefert das Resultat einen Widerspruch zur Irreduzibilität von (f). Dementsprechend folgt, dass (f) maximal ist.
Zuletzt wird die Implikation iii) $\implies$ i) gezeigt: Sei dafür (f) maximal. Verwendet man wiederum die Aussage aus Theorem 2.1.12., so folgt, dass $R/(f)$ ein Körper ist. Da Körper immer nullteilerfrei sind, folgt, dass $R/(f)$ auch ein Integritätsbereich ist. Dies impliziert, dass (f) prim ist. Damit ist die Implikationskette geschlossen und die Äquivalenz der Aussagen gezeigt [4, S. 47], [9, S. 93].

□

Beispiel. Wie bereits in einem Beispiel beschrieben, haben die Ideale des Rings der ganzen Zahlen $\mathbb{Z}$ die Form $n\mathbb{Z}$. Wird für n eine Primzahl p gesetzt, so erhält man ein maximales Ideal $p\mathbb{Z}$. Das Ideal ist maximal, weil, wenn nun $p\mathbb{Z}$ als eine Teilmenge von $m\mathbb{Z}$ betrachtet wird, muss $p = mk$ für $k \in \mathbb{N}$ gelten. Berücksichtigt man nun die Eigenschaften von Primzahlen, kommt für k oder m keine andere Zahl als die 1 in Frage. Insofern gilt $m\mathbb{Z} = p\mathbb{Z}$ oder $m\mathbb{Z} = \mathbb{Z}$ [9, S. 87].

Theorem 2.2.5. *Für jeden Hauptidealring A gilt, dass A auch faktoriell ist [9, S. 97]. In anderen Worten: In einem Hauptidealring A kann jedes $a \in A - (A^* \cup \{0\})$ als Produkt von Primelementen ausgedrückt werden [4, S. 47].*

Beweis. Nun ist zu zeigen, dass sich jedes $a \in A-(A^* \cup \{0\})$ als Produkt von irreduziblen Elementen zerlegen lässt. Wir betrachten dazu die Menge S aller Hauptideale von A, die von $a \in A - (A^* \cup \{0\})$ erzeugt werden, wobei a keine endliche Zerlegung in irreduzible Elemente besitzen soll, also gilt es $S = \emptyset$ zu zeigen [4, S. 47 f].
Angenommen $S \neq \emptyset$, dann muss nach dem Zornschen Lemma ein maximales Element in S existieren. Für dieses Element $\mathbf{a}$ gilt dann, dass aus $\mathbf{a} \subsetneq \mathbf{b}$ in A folgt, dass $\mathbf{b} \notin S$ ist. Wir setzen für das maximale Element $\mathbf{a} = (a)$. Damit ist a reduzibel und kann als Produkt von Nichteinheiten $a_1, a_2 \in A$ geschrieben werden: $a = a_1 \cdot a_2$. Nun folgt $(a) \subsetneq (a_1)$ und $(a) \subsetneq (a_2)$, sodass (a_1) und (a_2) nicht Element von S sein können. Dies führt wiederum dazu, dass a_1 und a_2 in irreduzible Elemente zerlegt werden können und demzufolge genauso ihr Produkt $a = a_1 \cdot a_2$. Somit stößt man auf einen Widerspruch zu $(a) \in S$ und es folgt $S = \emptyset$. Da in Hauptidealringen irreduzible Elemente prim sind, haben wir eine Zerlegung in Primelemente gefunden [4, S. 47 f]. □

Bemerkung. Das Theorem zuvor ist allgemein in Hauptidealringen gültig. Für den Beweis betrachtet man ein Element $a \in A - (A^* \cup \{0\})$. Für den Fall, dass dieses Element prim ist, folgt sofort die Aussage. Ist a nicht prim, so zerlegt man es in ein Produkt von Nichteinheiten $b \cdot c$ des Hauptidealrings A. Diese Zerlegung wird anschließend endlich oft wiederholt. Der Beweis gestaltet sich einfacher, wenn man die Aussage lediglich für die ganzen Zahlen zeigt. (Bei $\mathbb{Z}$ handelt es sich, wie bereits erwähnt, ebenfalls um einen Hauptidealring.) Grund dafür ist, dass in $\mathbb{Z}$ das Faktorisieren von zwei Nichteinheiten die folgende Eigenschaft erfüllt: $|b|, |c| < |a|$. Der Betrag von a nimmt stetig ab, weshalb das Verfahren nach endlich vielen Schritten abbricht [4, S. 47].

2.2.3 Euklidische Ringe

Definition. Ein euklidischer Ring ist ein Integritätsring R mit einer Abbildung $\delta : R - \{0\} \longrightarrow \mathbb{N}$, sodass es zu den Elementen $f, g \in R, g \neq 0$ immer Elemente $q, r \in R$ gibt, die die folgende Bedingung erfüllen:

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

Dabei ist die Abbildung δ die Normalabbildung des euklidischen Rings R, außerdem heißt r Rest der Division von f durch g [4, S. 44].

Beispiel. Körper sind euklidische Ringe. Auch der Ring der ganzen Zahlen $\mathbb{Z}$ ist mit der gewöhnlichen Division mit Rest und der Betragsabbildung $\delta(n) = |n|$ ein euklidischer Ring [4, 3, S. 45, S. 160].

Theorem 2.2.6. *Ist R ein euklidischer Ring, so ist R ebenfalls ein Hauptidealring [4, S. 46].*

Beweis. Sei I ein Ideal eines euklidischen Rings D. Für den Fall, dass $I = 0$ ist, erhält man $I = (0)$. Für $I \neq 0$ wählen wir ein Element $a \in I - \{0\}$ wobei $\delta(a)$ minimal unter den Nicht-Null-Elementen von I ist. Damit gilt bereits $I = (a)$, da für ein $f \in I$ mit

$f = qa + r$ und $\delta(r) < \delta(a)$ folgt, dass $r = f - qa \in I$ und aufgrund der zuvor geforderten Eigenschaft, dass $\delta(a)$ minimal ist, gilt $r = 0$. Damit ist $f = qa \in (a)$ und es folgt, dass $I = (a)$ das Hauptideal ist [4, 8, S. 46, S. 149]. □

Aus den beiden Behauptungen folgt nun auch, dass euklidische Ringe ebenso faktorielle Ringe sind [8, S. 149].

Bemerkung. Zusammenfassend folgt nun, dass $\mathbb{Z}$ als euklidischer Ring auch Hauptidealring und ein faktorieller Ring ist [4, S. 49]. Insbesondere ist das Ideal in $\mathbb{Z}$ von der Form $I = (a), a \in \mathbb{Z}$ [9, S. 87].

Euklidischer Algorithmus

Für beliebige euklidische Ringe ist der euklidische Algorithmus anwendbar. Durch dieses Berechnungsverfahren ist es möglich, den größten gemeinsamen Teiler von zwei Elementen des euklidischen Rings zu ermitteln [9, S. 94]. Ebenso erhält man durch den euklidischen Algorithmus die explizite Darstellung des größten gemeinsamen Teilers d der Elementen a und b als Linearkombination mit $d = ax + by$ [4, 6, S. 52, S. 15].

Bemerkung. Mit diesen Eigenschaften bildet der Algorithmus die Basis für weitere Verfahren wie etwa die RSA-Verschlüsselung [6, S. 13].

Theorem 2.2.7. *In einem euklidischen Ring R sei für die beiden Elemente x und y aus $R - \{0\}$ die nachstehende Folge $z_0, z_1, z_2, ...$ definiert durch:*

$$\begin{aligned} z_0 &:= x, \\ z_1 &:= y, \\ z_{i+1} &:= \textit{der Rest bei der Division von } z_{i-1} \textit{ durch } z_i \end{aligned}$$

(sofern $z_i \neq 0$).
Führt man diesen Algorithmus durch, so gibt es einen Index n, für den $z_{n+1} = 0$ gilt. Dabei stellt z_n den größten gemeinsamen Teiler der Elemente x und y dar. Man schreibt:

$$z_n = ggT(x, y)$$

[4, S. 52]

Bemerkung. Im Zuge dieser Rechenvorschrift wird mithilfe des Divisionsalgorithmus immerzu der verbleibende Rest berechnet. Gilt $x > y$, so wird der Rest bei der Division von $\frac{x}{y}$ ermittelt. Anschließend wird y durch den zuvor ermittelten Rest dividiert und wiederum ein zweiter Rest gefunden. Nun wird der erste Rest durch den zweiten Rest geteilt und man erhält damit den dritten Rest. Durch die Eigenschaft des Divisionsalgorithmus ist jeder Rest kleiner als sein Vorgänger. Der Algorithmus endet, wenn der verbleibende Rest gleich 0 ist. Der letzte Rest ungleich 0 ist der größte gemeinsame Teiler [6, S. 13].

Beweis. Sei R ein euklidischer Ring mit der Gradabbildung $\delta : R - \{0\} \longrightarrow \mathbb{N}$. Ein Element der zuvor beschriebenen Folge des euklidischen Algorithmus besitzt die nachstehende Gestalt:

$$z_{i-1} = q_i \cdot z_i + z_{i+1}$$

Die Folge der Grade ist streng monoton fallend, es gilt: $\delta(z : i+1) < \delta(z_i)$. Damit folgt, dass es nur endlich viele i mit $z_i \neq 0$ und ein n mit $z_{n+1} = 0$ gibt.

$z_0 = q_1 \cdot z_1 + z_2$
...
$z_{n-2} = q_{n-1} \cdot z_{n-1} + z_n$
$z_{n-1} = q_n \cdot z_n + 0$

Betrachtet man nun die Teilerrelationen, folgt $z_n | z_{n-1}$ und damit auch, dass $z_n | z_{n-2}$. Führt man diese Argumentationskette weiter, so erhält man schlussendlich $z_n | z_1$ und $z_n | z_0$. Dementsprechend ist z_n der gemeinsame Teiler von x und y.
Außerdem ist z_n der größte gemeinsame Teiler, denn wenn $a \in R$ ein anderer Teiler von x und y ist, muss a genauso z_2 und z_3 teilen sowie letztlich auch z_n. Da $a | z_n$ gilt, muss $a < z_n$ sein und damit ist $z_n = ggT(x, y)$ [4, S. 52]. □

Beispiel. Nun wird der euklidische Algorithmus im Ring der ganzen Zahlen für ein Beispiel angewendet. Es werden die ganzen Zahlen 10 und 14 betrachtet, für die der größte gemeinsame Teiler ermittelt wird.

$$14 = 1 \cdot 10 + 4$$
$$10 = 2 \cdot 4 + 2$$
$$4 = 2 \cdot 2 + 0$$

Der letzte Rest ungleich Null ist 2 und damit erhält man $ggT(10, 14) = 2$ [6, S. 13].

Bemerkung. Der größte gemeinsame Teiler kann in einem beliebigen Ring R durch Ideale beschrieben werden. Seien f und $g \in R$. Wenn $ggT(f, g) = d$ ist, dann gilt $d = fh + gk$ für $h, k \in R$. Demnach ist d ein Element des Ideals $I = \{fs + gt : s, t \in R\}$. Die Elemente f und g sind durch d teilbar und damit teilt d auch jedes Element des Ideals. Demzufolge ist $I = (d)$. Das Hauptideal wird durch den größten gemeinsamen Teiler der Elemente f und g erzeugt [6, S. 78] [4, S. 51].

Theorem 2.2.8. *In einem euklidischen Ring R mit $m \in R$ gilt für die Gruppe der Einheiten die folgende Eigenschaft*

$$(R/mR)^* = \{r + mR | ggT(r, m) = 1\} \text{ [3, S. 214].}$$

Der folgende Beweis des Theorems richtet sich nach der mündlichen Erläuterung von ao. Univ.-Prof. Dr. Joachim Mahnkopf im persönlichen Gespräch.

Beweis. Für den Beweis dieses Theorems wird die Aussage in beide Richtungen betrachtet: Zunächst sind nach Definition die Einheiten von R/mR diejenigen Elemente, die ein multiplikatives Inverses besitzen. Das heißt, es existiert ein $s + mR \in R/mR$, sodass

$$(r + mR) \cdot (s + mR) = 1 + mR.$$

Damit folgt, dass $rs - 1 \in mR$ ist, also ist $rs - 1 = mt$ für $t \in R$.
Das wiederum heißt, es existiert eine Linearkombination in der folgenden Gestalt

$$rs + mt = 1 \text{ mit } s, t \in R.$$

Dies ist die Bedingung der Teilerfremdheit von r und m: $\mathrm{ggT}(r, m) = 1$.
Ist umgekehrt der $ggT(r, m) = 1$, dann existiert nach dem euklidischen Algorithmus eine Darstellung

$$rs + tm = 1$$
$$(r + mR) \cdot (s + mR) = sr + mR = 1 - tm + mR = 1 + mR.$$

Das heißt, $s + mR$ ist das Inverse zu $r + mR$. Infolgedessen sind die Einheiten in R/mR genau die Restklassen $r + mR$ mit $\mathrm{ggT}(r, m) = 1$. □

Bemerkung. Das Theorem 2.2.8 gilt nicht nur in euklidischen Ringen, sondern auch in allen Hauptidealringen. In euklidischen Ringen steht aber der euklidische Algorithmus zur Verfügung, der eine geeignete Rechenvorschrift liefert, um den größten gemeinsamen Teiler von zwei Elementen zu ermitteln [4, S. 51].

2.3 Polynomringe

In weiterer Folge werden Polynomringe über Körpern betrachtet. Dafür wird zunächst das Element eines Polynomrings definiert:

Definition. Ein Polynom ist ein Ausdruck der folgenden Form:

$$\alpha_n x^n + ... + \alpha_2 x^2 + \alpha_1 x + \alpha_0,$$

wobei die Koeffizienten α_i Elemente eines Rings R sind. Die Veränderliche x des Polynoms kann auf unterschiedliche Weisen interpretiert werden. Zum einen kann die Interpretation zum Konzept der Polynomform, zum anderen zur Polynomfunktion führen [11, S. 6].

Bemerkung. Um nicht alle Koeffizienten anzugeben, werden Polynome mit einem Namen, wie beispielsweise $f(x)$ oder $g(x)$ versehen [11, S. 7].

Definition. Wenn der führende Koeffizient $\alpha_n \neq 0$ ist, bestimmt dieser den Grad des Polynoms - das Polynom besitzt den Grad n [11, S. 7]. Man schreibt:

$$deg(f) := max\{n; \alpha_n \neq 0\} \text{ [4, S. 31]}$$

Des Weiteren schreibt man $sgn(f) = \alpha_n$ für den führenden Koeffizienten von f[13, S. 1].

Bemerkung. Jedes konstante Polynom weist die Form $g(x) = a$ mit $a \in F$ auf und besitzt den Grad 0 und ist, ausgenommen des Nullpolynoms, eine Einheit [6, S. 81].

Ein Polynom, dessen Koeffizienten alle Null sind, wird Nullpolynom genannt. Wir definieren für das Nullpolynom den führenden Koeffizienten und den Grad folgendermaßen:

$$sgn(0) := 0 \quad deg(0) := -\infty$$

Mit dieser Definition bleiben getroffene Aussagen zum Grad der Polynome ohne Ausnahme gültig [13, S. 1].
Sind f und g zwei Nicht-Null-Polynome gelten wiederum die folgenden Eigenschaften:

i) $deg(fg) = deg(f) + deg(g)$

ii) $sgn(fg) = sgn(f) \cdot sgn(g)$

iii) $deg(f + g) \leq max(deg(f), deg(g))$ [13, S. 1].

Definition. Der Polynomring $R[T]$ stellt die Menge aller Polynome über dem Ring R mit der Variablen x dar [4, S. 30]. Da die Addition und Multiplikation wohldefiniert sind, bildet diese Menge einen Ring [11, S. 7]. Die Addition und Multiplikation sind wie folgt definiert: Seien $f(x)$ und $g(x)$ in $R[T]$ mit $f(x) = \sum_{i=1}^{n} \alpha_i x^i$ und $g(x) = \sum_{i=1}^{m} \beta_i x^i$. Wenn Null-Koeffizienten hinzugefügt werden, um $m = n$ vorauszusetzen, gilt:

$$(f + g)(x) = \sum_{i=1}^{n} \alpha_i x^i + \sum_{i=1}^{n} \beta_i x^i = \sum_{i=1}^{n} (\alpha_i + \beta_i) x^i$$
$$(f \cdot g)(x) = \sum_{i=0}^{n} \alpha_i x^i \cdot \sum_{i=0}^{m} \beta_i x^i = \sum_{i=1}^{n+m} (\sum_{j=0}^{j} \alpha_j \cdot \beta_{j-i} x^i) \text{ [6, S. 44]}$$

Ist R sogar ein Körper, so handelt es sich um einen Polynomring über einem Körper. Der Polynomring selbst bildet allerdings keinen Körper, da die Elemente des Polynomrings kein Inverses bezüglich der Multiplikation besitzen. Dies folgt aus der Eigenschaft der i) der Gradfunktion *deg*. [11, S. 7].

Beispiel. Ein konkretes Beispiel ist etwa die Menge $\mathbb{R}[T]$ aller Polynome mit reellen Zahlen als Koeffizienten gemeinsam mit den Verknüpfungen der Addition und Multiplikation, die einen kommutativen Ring bilden [6, S. 44].

Theorem 2.3.1. *Sei K ein Körper. Für $f(x)$ und $g(x) \in K[T]$ und $g(x) \neq 0$ gibt es Polynome $q(x)$ und $r(x)$ in $K[T]$, sodass $f(x) = g(x)q(x) + r(x)$ gilt. Dabei ist entweder $r(x) = 0$ oder es gilt $deg(r) < deg(g)$. Außerdem sind q und r eindeutig bestimmt [11, 13, S. 11, S. 2].*

Beweis. Sei n der Grad von f, α sein führender Koeffizient und m der Grad von g mit dem führenden Koeffizienten β: $n = deg(f)$, $\alpha = sgn(f)$, $m = deg(g)$, $\beta = sgn(g)$.
Für $n < m$ muss $q = 0$ gesetzt werden und für den Rest gilt $r = f$.
Wenn $n \geqslant m$ gilt, dass $f_1 = f - \alpha\beta^{-1}T^{n-m}g$ einen kleineren Grad als f besitzt. Nun wird mit Induktion gezeigt, dass $q_1, r_1 \in K[T]$ mit $f_1 = q_1 g + r_1$ und $r_1 = 0$ oder $deg(r_1) < deg(g)$ existieren. Für diesen Fall setzen wir $q = \alpha\beta^{-1}T^{n-m} + q_1$ und $r = r + 1$.
Um die Eindeutigkeit zu zeigen, sei $f = qg + r = q'g + r'$. Gelte dies, würde g auch $r - r'$ teilen. Wenn nun der Grad der Polynome betrachtet wird, so folgt, dass $r = r'$ gilt und damit auch $qg = q'g$. Somit folgt $q = q'$ [13, S. 2]. □

Bemerkung. Nun ergibt sich aus Theorem 2.3.1 für einen Körper K, dass der Polynomring $K[T]$ ein euklidischer Ring mit der Normabbildung $\delta : K[T] - \{0\} \longrightarrow \mathbb{N}$, $f \longmapsto \deg f$ ist [4, S. 44]. Insbesondere ist der euklidische Algorithmus in $K[T]$ gültig [4, S. 45]. In weiterer Folge wird ein Beispiel der Polynomdivision mit Rest berechnet. Des Weiteren folgt, dass $K[T]$ auch Hauptidealring ist [4, S. 46].

Beispiel. Im Ring $R = K[T]$ der Polynome über dem Körper K mit einem Element $f \in K[T]$ sei $I = \{gf : g \in K[T]\}$ die Menge aller Produkte mit f. Diese Menge ist ein Ideal von $K[T]$, nämlich das von f erzeugte Hauptideal (f) [6, S. 77].

Als Nächstes wird der Divisionsalgorithmus für Polynome auf der Menge des Polynomrings über einem Körper $K[T]$ beschrieben:
Der Divisionsalgorithmus für Polynome funktioniert analog zu der Division mit Rest innerhalb der ganzen Zahlen $\mathbb{Z}$. Wird ein Polynom (Dividend) durch ein weiteres Polynom (Divisor) dividiert, so erhält man den Quotient mit dem zugehörigen Rest [11, S. 10 f].

Beispiel. Im folgenden Beispiel wird das Polynom $x^3 + 2x^2 + 3x + 4$ durch das Polynom $x + 1$ dividiert.

$$\begin{array}{rl}
\big(& x^3 + 2x^2 + 3x + 4 \big) \div \big(x + 1\big) = x^2 + x + 2 + \dfrac{2}{x+1} \\
\underline{-x^3 \;\; -x^2} & \\
x^2 + 3x & \\
\underline{-x^2 \;\; -x} & \\
2x + 4 & \\
\underline{-2x - 2} & \\
2 &
\end{array}$$

Hierbei bleibt 2 als Rest. Dieser wurde im Beispiel dem Quotienten als Bruch $\frac{2}{x+1}$ addiert. Ob die Division richtig durchgeführt wurde, kann durch folgende Rechnung überprüft werden:

$$\textit{Quotient} \cdot \textit{Divisor} + \textit{Rest} = \textit{Dividend} \text{ [11, S. 10]}$$

Um den Divisionsalgorithmus näher zu beleuchten, werden nachfolgend die Zwischenschritte des Beispiels zuvor beschrieben. Dabei wird der momentane Dividend in folgende Form umgestellt:

$$(x + 1)\cdot \text{ Polynom der Form } cx^n + \text{ Rest}$$

[11, S. 10]

$$\begin{aligned}
x^3 + 2x^2 + 3x + 4 &= (x + 1) \cdot x^2 + (x^2 + 3x + 4) \\
x^2 + 3x + 4 &= (x + 1) \cdot x + (2x + 4) \\
2x + 4 &= (x + 1) \cdot 2 + 2
\end{aligned}$$

Im ersten Schritt ist der Dividend der tatsächliche Dividend der ursprünglichen Division. Anschließend ist das Ziel, das Polynom der Form cx^n so zu wählen, dass es den höchstmöglichen Grad von x aus dem Dividenden aufweist. Damit ist der Grad des Restes kleiner als der Grad des Dividenden. Im nächsten Schritt wird der Rest des vorherigen Schritts zum neuen Dividenden und der erste Schritt wiederholt sich. Der Algorithmus stoppt, wenn der Grad des Restes kleiner ist, als der Grad des Divisors. Schlussendlich können die Ergebnisse folgendermaßen zusammengefasst werden:

$$x^3 + 2x^2 + 3x + 4 = (x + 1)(x^2 + x + 2) + 2 \text{ [11, S. 10]}$$

Definition. Ein Polynom $f(x) = \alpha_n x^n + ... + \alpha_2 x^2 + \alpha_1 x + \alpha_0$ aus dem Polynomring über einem Körper $K[T]$ heißt normiert, wenn der führende Koeffizient $\alpha_n = 1$ ist [11, S. 25]. Das heißt, es gilt $sgn(f) = 1$ [13, S. 1].

Beispiel. Das Polynom $x^2 - 2$ ist normiert, während diese Eigenschaft nicht auf das Polynom $3x^2 - 6$ zutrifft. Dennoch besitzen die beiden Polynome dieselbe Nullstelle: $\sqrt{2}$ [11, S. 25].

Definition. Für einen Körper K ist ein nicht-konstantes Polynom $f \in K[T]$ irreduzibel über K, wenn aus $f = gh$ folgt, dass g oder h konstante Polynome, das heißt, sie haben den Grad 0 [6, S. 81].

Beispiel. Ein Polynom mit dem Grad 1, wie etwa das Polynom x ist irreduzibel, denn gäbe es eine Faktorisierung mit $x = gh$, so müsste der Grad der Polynome g und h addiert den Grad des Polynom x ergeben. Dafür schreibt man: $deg(x) = 1 = deg(g) + deg(h)$. Eines der Polynome g oder h besitzt den Grad 1 und das andere Polynom den Grad 0. Damit ist das andere Polynom konstant. Daraus folgt, dass Polynome ersten Grades, wie beispielsweise das Polynom x, irreduzibel sind [6, S. 82].

Beispiel. Das Polynom $x^2 + 1$ ist in $\mathbb{R}$ irreduzibel, weil die Zerlegung in Linearfaktoren wie etwa $x^2 + 1 = (ax + b) \cdot (cx + d)$ mit $a, b, c, d \in \mathbb{R}$ nicht möglich ist. Diese Zerlegung würde zeigen, dass $x^2 + 1$ eine Nullstelle besitzt, das ist allerdings ein Widerspruch zu $x^2 + 1 \geq 1$ für alle x [6, S. 82]. Betrachtet man selbiges Polynom in $\mathbb{C}$, ist es sehr wohl reduzibel, da $x^2 + 1$ als Produkt mit $(x - i) \cdot (x + i)$ geschrieben werden kann [6, S. 81].

Bemerkung. (Normierte Darstellung im Restklassenring) Im Faktorring $K[T]/I$ kann der Divisionsalgorithmus verwendet werden, um Elemente in normierter Form zu schreiben. Dafür setzt man $I = (f)$ und für ein $g \in K[T]$ wird der Divisionsalgorithmus angewandt. Man schreibt $g = qf + r$, wobei $g, r \in K[T]$ und für den Grad der Polynome $\deg(r) < \deg(f)$ gilt. Durch Umstellen erhält man $g - r = qf \in I$ und damit $g + I = r + I$. Dies zeigt, dass die Nebenklasse $g + I$ äquivalent zur Nebenklasse $r + I$ ist, wobei $\deg(r) < \deg(f)$ gilt. Mit dieser Bedingung ist r eindeutig bestimmt. Diese Darstellung nennt man normierte Darstellung. Man erhält

$$K[T]/(f) = \{r + I : r \in K[T], \deg(r) < \deg(f)\}.$$

Dieses Resultat erinnert an die Beschreibung des Restklassenrings mit $\mathbb{Z}_n = \{\overline{a} : 0 \leq a < n\} = \{a + (n) : 0 \leq a < n\}$ [6, S. 82].

Bemerkung. Letztlich bleibt noch zu erwähnen, dass in Polynomringen die Erzeuger von maximalen Idealen irreduzible Polynome sind. Wie bereits beschrieben, handelt es sich beim Polynomring $K[T]$ um einen Hauptidealring [4, S. 46]. Dies folgt aus Theorem 2.2.4.

Zusammenfassend wurde in diesem Abschnitt gezeigt, dass Polynomringe euklidische Ringe und Hauptidealringe sind. Aus der Implikationskette des letzten Kapitels folgt nun, dass Polynomringe ebenfalls faktorielle Ringe sind [13, S. 2].

2.4 Endliche Körpererweiterung

In diesem Kapitel werden die Eigenschaften von endlichen Körpererweiterungen untersucht. Eine endliche Körpererweiterung kann etwa mit einem irreduziblen Polynom durchgeführt werden, wie das folgende Beispiel zeigt [6, S. 83].

Beispiel. Die reellen Zahlen werden mittels des irreduziblen Polynoms $f = x^2 + 1$ auf die komplexen Zahlen erweitert. Dazu wird der Quotientenkörper $\mathbb{R}[T]/(x^2+1)$ mit dem Körper der komplexen Zahlen $\mathbb{C}$ verknüpft. Die Rechenoperationen in $\mathbb{R}[T]/(x^2+1)$ weisen Ähnlichkeit mit den Operationen in $\mathbb{C}$ auf. Aufgrund des Divisionsalgorithmus im Quotientenring gilt, dass jedes Element in der Form $a + bx + I$ geschrieben werden kann, wenn $I = (x^2+1)$. Diese Eigenschaft wurde bereits in Kapitel 2.3 mit der Bemerkung für die normierte Darstellung im Restklassenring beschrieben. Damit gilt für die Addition

$$(a + bx + I) + (c + dx + I) = (a + c) + (b + d)x + I.$$

Für die Multiplikation gilt

$$(a + bx + I)(c + dx + I) = ac + bdx^2 + (ad + bc)x + I = (ac - bd) + (ad + bc)x + I.$$

Die letzte Umformung gilt, da $bdx^2 + I = -bd + I$. Zum Vergleich lauten die Rechenoperationen der komplexen Zahlen wie folgt

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \text{ [6, S. 82].}$$

Definition. Ist K ein Körper, dann ist eine Körpererweiterung von K ein Körper L, der K enthält. Des Weiteren gilt, dass die Körperoperationen von L sich auf die des Körpers K beschränken. Damit ist K ein Unterkörper von L [6, S. 83].

Proposition 2.4.1. *Sei K ein Körper und sei $f \in K[T]$ ein Polynom. Wenn $I = (f)$ das Ideal erzeugt von dem irreduziblen Polynom f ist, dann ist $K[T]/I$ eine Körpererweiterung von K [6, S. 83].*

Beweis. Sei K ein Körper, $f \in K[T]$ irreduzibel und $I = (f)$. Um zu zeigen, dass $K[T]/I$ ein Körper ist, genügt es nachzuweisen, dass jedes Nicht-Null-Element ein multiplikatives Inverses besitzt, da bereits bekannt ist, dass es sich bei $K[T]/I$ um einen kommutativen Ring handelt.
Sei $g + I \in K[T]/I$ und nicht Null. Dann gilt $g + I \neq 0 + I$ und damit $g \notin I$. Das heißt, f teilt nicht g. Da f allerdings irreduzibel ist, muss der größte gemeinsame Teiler von f und g gleich 1 sein. Dementsprechend existieren h und k in $K[T]$, für die $1 = hf + kg$ gilt. Da $hf \in I$ und $kg - 1 \in I$ gilt, ist $kg + I = 1 + I$ ebenfalls gültig. Die Multiplikation kann umgestellt werden und damit erhält man die folgende Gleichung: $(k - I)(g + I) = 1 + I$. Dies führt wiederum zum multiplikativen Inversen von $(k + I)$, nämlich $(g + I)$. Nachdem nun gezeigt wurde, dass ein beliebiges Element ungleich Null aus $K[T]/I$ ein multiplikatives Inverses besitzt, handelt es sich nicht nur um einen kommutativen Ring, sondern auch um einen Körper.

Die Elemente $a+I$ mit $a \in K$ bilden einen Unterkörper von $K[T]/I$, der dem Körper K zugeordnet ist. Es folgt, dass $K[T]/I$ eine Körpererweiterung von K ist [6, S. 83 f]. □

Bemerkung. Dass $K[T]/I$ ein Körper ist, folgt bereits aus Theorem 2.1.12, das besagt, dass für einen kommutativen Ring R mit Ideal I gilt: Der Faktorring R/I ist ein Körper, genau dann, wenn das Ideal maximal ist [3, S. 133]. Hierbei ist das Ideal $I = (f)$ maximal, da f ein irreduzibles Polynom ist [4, S. 47].

Durch diesen Beweis ist umgekehrt ersichtlich, dass, wenn $K[T]/(f)$ ein Körper ist, so ist f ein irreduzibles Polynom [6, S. 84].

2.4.1 Dimensionsformel

Definition. Sei L eine Körpererweiterung von K. Man bezeichnet die Dimension von L als K-Vektorraum mit $[L : K]$ [6, S. 86]. Die Dimension wird auch Grad der Körpererweiterung genannt [3, S. 242].

Bemerkung. Sollte $[L : K] = 1$ gelten, so stimmen K und L überein [3, S. 243].

Proposition 2.4.2. *Sei K ein Körper und $f \in K[T]$ ein irreduzibles Polynom. Es gilt für die Dimension die folgende Gleichheit:*

$$[K[T]/(f) : F] = deg(f)$$

[6, S. 86]

Beweis. Setze für $deg(f) = n$ und für eine einfache Schreibweise wird statt $a + (f)$ mit $a \in K$ lediglich a und für $x^i + (f)$ nur $\overline{x}^i$ geschrieben. Die normierte Darstellung eines jeden Elements aus $F[T]/(f)$ ist $\sum_{i=0}^{n-1} a_i \overline{x}^i$ für $a_i \in K$. Die Menge $\{1, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}\}$ ist linear unabhängig und spannt $K[T]/(f)$ als einen K-Vektorraum auf [6, S. 86].
Die lineare Unabhängigkeit ergibt sich wie folgt: für $\sum_{i=0}^{n-1} a_i \overline{x}^i = 0$ mit $a_i \in K$, dass das Polynom f mit dem Grad n das Polynom $\sum_{i=0}^{n-1} a_i \overline{x}^i$ mit geringerem Grad teilt. Also gilt dann $\sum_{i=0}^{n-1} a_i \overline{x}^i \in (f)$. Das impliziert wiederum, dass das letzte Polynom dem Nullpolynom entspricht - Für jedes i ist $a_i = 0$ [6, S. 86]. □

Theorem 2.4.3. *(Dimensionsformel / Gradsatz) Sei K ein Körper und L die Körpererweiterung von K. Sei außerdem M eine Körpererweiterung von L. Damit ist L ein Zwischenkörper von K und M. Man schreibt auch $K \subset L \subset M$. Es gilt:*

$$[M : K] = [M : L] \cdot [L : K].$$

[3, 6, S. 243, S. 87]

Beweis. Ist der Grad der Körpererweiterung $[M : L]$ oder $[L : K]$ unendlich, so ist $[M : K]$ ebenfalls unendlich und die Aussage folgt.
Für den Fall, dass die Dimensionen $[M : L]$ und $[L : K]$ endlich sind, ist mehr zu zeigen. Angenommen $[L : K] = m$ und $[M : L] = n$ und eine Basis für L über K ist $\{a_1, ..., a_m\}$

und für M über L ist eine Basis $\{b_1, ..., b_n\}$. Es gilt zu zeigen, dass die Elemente $a_i b_j \in M$ mit $1 \leq i \leq m$ und $1 \leq j \leq n$ die Basis für den Vektorraum von M über K bilden.
Für die lineare Unabhängigkeit wird vorausgesetzt, dass $\sum_{1 \leq i \leq m, 1 \leq j \leq n} \gamma_{ij} a_i b_j = 0$ für $\gamma_{ij} \in K$ ist. Schreibt man diese Gleichheit als Linearkombination in den b_j mit den Koeffizienten in L, so erhält man

$$\sum_{1 \leq j \leq n} (\sum_{1 \leq i \leq m} \gamma_{ij} a_i) b_j = 0.$$

Aufgrund der zuvor geforderten linearen Unabhängigkeit muss es einen Koeffizienten für jedes b_j gleich Null geben. Dadurch gilt für jedes j

$$\sum_{1 \leq i \leq m} \gamma_{ij} a_i = 0.$$

Die lineare Unabhängigkeit von a_i fordert wiederum $\gamma_{i,j} = 0$. Das zeigt, dass aus der linearen Unabhängigkeit von a_i über K und von b_j über L die lineare Unabhängigkeit von $a_i b_j$ über K folgt.
Um noch zu zeigen, dass die Menge $\{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ eine Basis von M über K bildet, sei $c \in M$. Da $\{b_1, ..., b_n\}$ das Erzeugendensystem von M über L ist, kann c wie folgt ausgedrückt werden:

$$c = \sum_{1 \leq j \leq n} \alpha_j b_j \text{ mit } \alpha_j \in L.$$

Jedes α_j kann als Linearkombination mit den Koeffizienten $a_i \in K$ geschrieben werden:

$$\alpha_j = \sum_{1 \leq i \leq m} \beta_{ij} a_i$$

Kombiniert man diese beiden Ausdrücke, so erhält man die folgende Gleichheit:

$$c = \sum_{1 \leq j \leq n} \alpha_j b_j = \sum_{1 \leq j \leq n} \sum_{1 \leq i \leq m} \beta_{ij} a_i b_j$$

Damit folgt, dass $a_i b_j$ ein Erzeugendensystem von M über K bildet [6, 4, S. 87, S. 90]. □

2.4.2 Algebraische Elemente, Minimalpolynom

Algebraische Elemente und Minimalpolynome dienen der Untersuchung der Struktur von Körpererweiterungen.

Lemma 2.4.4. *Sei L eine Körpererweiterung von K und $\alpha \in L$. Dann ist $I = \{g \in K[T] : g(\alpha) = 0\}$ ein Ideal von $K[T]$. Ist I nicht das Nullideal, dann gilt $I = (f)$ für ein irreduzibles f aus $K[T]$ [6, S. 88].*

Beweis. I ist ein Ideal, da es abgeschlossen bezüglich Addition und Multiplikation von Elementen aus $K[T]$ ist [6, S. 80]. Sei $I \neq (0)$, so muss $I = (f)$ für ein $f \in I$ mit positiven Grad gelten. Der Grad von f ist minimal unter den Nicht-Null-Elementen des Ideals, da f der Erzeuger des Ideals ist. Wenn für $g, h \in K[T]$ gilt, dass $f = gh$, dann folgt $0 = f(\alpha) = (gh)(\alpha) = g(\alpha)h(\alpha)$. Da wir diese Gleichung innerhalb des Körpers L betrachten, muss eine der beiden Gleichungen zutreffen: $g(\alpha) = 0$ oder $h(\alpha) = 0$, also $g \in I$ oder $h \in I$. Nachdem f unter allen Nicht-Null-Elementen aus I den geringsten

Grad besitzt, muss entweder g oder h den Grad 0 aufweisen und ist damit eine Einheit. Somit folgt, dass f irreduzibel ist [6, S. 88]. □

Definition. Sei L eine Körpererweiterung von K. Außerdem sei $\alpha \in L$ und $I = \{g \in K[T] : g(\alpha) = 0\}$. Entspricht I nicht dem Nullideal, so heißt α algebraisch abhängig über K. In anderen Worten: Das Element α ist algebraisch abhängig über K, wenn α eine Nullstelle eines Polynom positiven Grades mit Koeffizienten aus K ist [6, S. 88].

Beispiel. Eine Zahl $\alpha \in \mathbb{C}$ heißt algebraisch über einem Körper $K \subseteq \mathbb{C}$, wenn es ein Nicht-Null-Polynom $f(x) \in K[T]$ mit α als Nullstelle von $f(x)$ gibt [11, S. 20].

Definition. Ist α nicht algebraisch, also gilt $I = (0)$, so heißt α transzendent über K [6, 3, S. 88, S. 284].

Beispiel. Für die komplexen Zahlen $\mathbb{C}$ eine Körpererweiterung der reellen Zahlen $\mathbb{R}$ ist $\alpha = i = \sqrt{-1}$, die imaginäre Einheit, algebraisch über $\mathbb{R}$, weil es ein Polynom gibt, für das $g(\alpha) = 0$ gilt. Damit gilt für das Ideal $I = (x^2 + 1)$ [6, S. 88].

Beispiel. Betrachten wir nun die reellen Zahlen $\mathbb{R}$ als Körpererweiterung der rationalen Zahlen $\mathbb{Q}$ mit $q \in \mathbb{Q}$ und $n \in \mathbb{N}^*$. Dann ist $\sqrt[n]{q} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$, da die Wurzel eine Nullstelle des Polynoms $x^n - q$ ist [4, S. 91].

Beispiel. Ein Beispiel für die Transzendenz wäre etwa für $\alpha = \pi$ in $\mathbb{R}$ als Körpererweiterung von $\mathbb{Q}$. Die Zahl π ist keine Nullstelle eines nicht-trivialen Polynoms mit rationalen Koeffizienten. Der Beweis dazu, die Unmöglichkeit der Quadratur des Kreises, wurde von Ferdinand von Lindemann im Jahr 1882 geführt [3, 6, S. 249, S. 88].

Für eine Körpererweiterung L des Körpers K wird angenommen, dass $\alpha \in L$ algebraisch über K ist. Sei $f = \sum_{i=0}^{n} a_i x^i$ mit $a_i \in K$ und $a_n \neq 0$ der Erzeuger des Ideals $I = \{g \in K[T] : g(\alpha) = 0\}$. Dann gilt, dass $a^{-1}f$ monisch ist und denselben Grad wie f besitzt. Da f den kleinsten positiven Grad unter den Nicht-Null-Elementen aus I aufweist, ist das Polynom $a^{-1}f$ eindeutig in I [6, S. 88].

Definition. Das Polynom $a^{-1}f$ wird Minimalpolynom von α über K genannt. Dafür schreibt man $min_K(\alpha)$ [6, S. 88]. Dabei ist $min_K(\alpha)$ das eindeutig bestimmte normierte Polynom kleinsten Grades, das α annulliert. Weiters ist das Minimalpolynom prim und damit irreduzibel [4, S. 91].

Beispiel. Die reelle Zahl $\sqrt{2}$ ist algebraisch über den rationalen Zahlen $\mathbb{Q}$, da es ein Polynom mit raionalen Koeffizienten gibt, das $\sqrt{2}$ als Nullstelle besitzt. Für $f = x^2 - 2$ gilt $f(\sqrt{2}) = 0$. Da f normiert ist und der Grad von f nicht kleiner als 2 sein kann, gilt $min_{\mathbb{Q}}(\sqrt{2}) = x^2 - 2$ [6, S. 88].

Definition. Für zwei Körper K und L ist ein Homomorphismus eine Funktion $\varphi : K \longrightarrow L$, für die mit $a, b \in K$ die folgenden Eigenschaften gelten:

$$f(1_K) = 1_L$$
$$f(a + b) = f(a) + f(b)$$
$$f(ab) = f(a)f(b)$$

Ein Körper-Homomorphismus ist immer injektiv. Erfüllt die Abbildung zusätzlich die Eigenschaften der Surjektivität, so handelt es sich um einen Isomorphismus [6, S. 88].

Theorem 2.4.5. *Sei K ein Körper und $f \in K[T]$ ein irreduzibles Polynom mit α als Nullstelle von f. Dann gibt es einen Isomorphismus $K[T]/(f) \longrightarrow K[\alpha]$. Dieser Isomorphismus ist auch ein Isomorphismus von K-Vektorräumen [6, S. 89].*

Beweis. Sei $g = \sum_{i=0}^{m} a_i x^i \in K[T]$ und es sei $\varphi(g + (f)) := \sum_{i=0}^{m} a_i \alpha^i = g(\alpha) \in K[\alpha]$. Nun ist zu zeigen, dass φ wohldefiniert ist und das Bild ein Körper ist. Wenn das Bild $K(\alpha)$ ein Körper ist, so ist das Bild auch die kleinste Körpererweiterung von K, die α enthält.
Im ersten Schritt wird die Wohldefiniertheit überprüft: Angenommen es gilt

$$g + (f) = h + (f).$$

Dann gilt auch $h = g + fk$ für $k \in K[T]$, sodass

$$\varphi(h + (f)) = h(\alpha) = g(\alpha) + (fk)(\alpha) = g(\alpha) + (f)(\alpha)(k)(\alpha).$$

Da α eine Wurzel des Polynoms f ist, gilt $f(\alpha) = 0$ und damit kann die Gleicheitskette folgendermaßen weitergeführt werden:

$$\varphi(h + (f)) = g(\alpha) = \varphi(g + (f)).$$

Im folgenden Schritt wird gezeigt, dass das Bild von φ ein Körper ist. Diese Aussage folgt, wenn gezeigt wird, dass die Abbildung φ injektiv ist. Sei dafür $g + (f), h + (f) \in K[T]/(f)$ in Normalform geschrieben und damit ist $deg(g), deg(h) < deg(f)$. Gilt die Gleichheit $\varphi(h + (f)) = \varphi(g + (f))$, so folgt, dass $g(\alpha) = h(\alpha)$ und damit $(h - g)(\alpha) = 0$. Aus dem Lemma 2.4.4 folgt, dass die Differenz $h - g \in (f)$ ist. Aufgrund dessen, dass die Grade von g und h kleiner als der Grad des Minimalpolynoms f sind, muss $g - h$ das Nullpolynom sein [6, S. 89]. □

Bemerkung. Das Bild des Isomorphismus φ ist der Ring $K[\alpha]$ der über K durch α gebildet wird. Dieser Ring ist ein Körper und stimmt mit $K(\alpha)$ überein. Außerdem handelt es sich hierbei um die kleinste Körpererweiterung von K, die α enthält. Die Eigenschaften für das algebraische Element α werden im nachfolgenden Theorem beschrieben [6, S. 90].

Korollar 2.4.6. *Sei L eine Körpererweiterung von K und $\alpha \in L$ algebraisch über K. Es gilt: $[K(\alpha) : K] = deg(min_K(\alpha))$. Das heißt, der Grad der Körpererweiterung entspricht dem Grad des Minimalpolynoms [6, S. 89].*

Beweis. Da $K(\alpha)$ und $K[T]/(f)$ isomorph als Körper sind, sind sie auch als K Vektorräume isomporph. Damit sind ihre Dimensionen über K gleich [6, S. 89]. □

Beispiel. Die reelle Zahl $\sqrt[3]{2}$ ist die Wurzel des Polynoms $x^3 - 2 \in \mathbb{Q}[T]$. Mithilfe des Satzes über rationale Nullstellen, der nachfolgend beschrieben wird, kann überprüft werden, dass dieses Polynom keine rationalen Nullstellen besitzt und lediglich die reelle Nullstelle $\sqrt[3]{2}$ aufweist. Es folgt, dass $x^3 - 2 = min_{\mathbb{Q}}(\sqrt[3]{2})$ also das Minimalpolynom mit dieser Nullstelle ist und dass $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = deg(x^3 - 2) = 3$ der Grad der Körpererweiterung mit dem des Minimalpolynoms übereinstimmt [6, S. 89].

Theorem 2.4.7. *(Satz über rationale Nullstellen) Sei $f(x) \in \mathbb{Z}[T]$ ein Polynom mit dem Grad n, sodass $f(x) = a_n x^n + ... + a_2 x^2 + a_1 x + a_0$. Wenn $x_0 = \frac{p}{q}$ eine gekürzte rationale Zahl ist und eine Nullstelle von $f(x)$, so gilt*

i) p ist ein Faktor von a_0 und

ii) q ist ein Faktor von a_n

[11, S. 12 f].

Beweis. Sei $f(\beta) = 0$, sodass

$$a_0 + a_1(\tfrac{p}{q}) + a_2(\tfrac{p}{q})^2 + ... + a_n(\tfrac{p}{q})^n = 0.$$

Durch die Multiplikation von q^n ergibt sich

$$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + ... + a_n p^n = 0.$$

Weitere Umformungen ergeben

$$a_0 q^n + p(a_1 q^{n-1} + a_2 p q^{n-2} + ... + a_n p^{n-1}) = 0$$

und

$$a_0 s^n = -p(a_1 q^{n-1} + a_2 p q^{n-2} + ... + a_n p^{n-1}).$$

Nach Voraussetzung sind p und q zueinander teilerfremd, somit existiert keine gemeinsame Primzahl bei der Primfaktorzerlegung von p und q. Das wiederum führt zu dem Schluss, dass p ein Teiler von a_0 ist. Analog kann argumentiert werden, dass q auch $a_n p^n$ teilt, denn

$$a_n p^n = -q(a_0 q^{n-1} + a_1 p q^{n-2} + ... + a_{n-1} r^{n-1})$$

und q damit ein Teiler von a_n ist. Damit sind beide Aussagen gezeigt [11, S. 13]. □

Das folgende Theorem stellt eine Zusammenfassung der wichtigsten Resultate dieses Kapitels dar:

Theorem 2.4.8. *Für eine Körpererweiterung L eines Körpers K und $\alpha \in L$ sind die folgenden Aussagen zueinander äquivalent.*

i) Das Element α ist algebraisch über K.

ii) Die kleinste Ringerweiterung von K, die α enthält, stimmt mit der kleinsten Körpererweiterung von K, die α enthält, überein.

iii) Das Element α ist die Nullstelle eines irreduziblen Polynoms aus $K[T]$.

iv) Die Elemente $1, \alpha, \alpha^2, ... \in L$ sind über K linear abhängig [6, S. 90].

Bemerkung. Diese vier Aussagen charakterisieren eine algebraische Struktur von α bezüglich K. Ad i) Es gibt ein Polynom $f \in K[T]$, sodass $f(\alpha) = 0$. Hierbei handelt es sich um das Minimalpolynom [4, S. 91]. Des Weiteren folgt diese Aussage - genauso wie iii) und vi) aus der jeweiligen Definition.

Nun ist bekannt, dass α algebraisch über K ist, wenn die oben genannten Aussagen zutreffen. In weiterer Folge konzentrieren wir uns auf die Beziehung zwischen α und Polynomen in $K[T]$: Da die Division mit Rest hier auch gilt, ist ein Element α einer Körpererweiterung L von K genau dann eine Nullstelle von f, wenn $x - \alpha$ ein Teiler von f in $L[T]$ ist. In anderen Worten: Das Element α ist eine Nullstelle von f, wenn $f = (x - \alpha)g$ mit $g \in L[T]$. Damit folgt, dass alle Nullstellen von f genau dann in L liegen, wenn sich f in Linearfaktoren aus $L[T]$ zerlegen lässt [6, S. 90].

Beispiel. Das Polynom $x^4 + 2x^2 + 1 \in \mathbb{Q}[T]$ lässt sich folgendermaßen faktorisieren

$$(x + i)^2(x - i)^2 \in \mathbb{Q}(i)[T].$$

Das zeigt, dass das gegebene Polynom 4 Nullstellen in $\mathbb{Q}(i)$ aufweist [6, S. 90].

2.5 Endliche Körper

Für die folgende Konstruktion von endlichen Körpern betrachten wir zunächst die Definitionen des Primkörpers und der Charakteristik.

Definition. Für einen Körper K heißt der von $\{1_K\}$ erzeugte Unterkörper der Primkörper von K [10, S. 13]. Der Primkörper ist der kleinste Teilkörper in K [9, S. 129]. Damit besitzt er keinen echten Unterkörper [3, S. 245].

Um einen solchen kleinsten Unterkörper über eine Zahl zu charakterisieren, wird die nächste Definition benötigt [3, S. 244]:

Definition. Für einen Körper K wird

$$\begin{aligned} \chi : \mathbb{Z} &\longrightarrow K \\ n &\longmapsto n \cdot 1_K \end{aligned}$$

als charakteristische Abbildung definiert [3, S. 131]. Aufgrund dessen, dass der Kern $ker\chi$ ein Ideal in $\mathbb{Z}$ ist, gibt es eine Zahl $char(R)$ mit der folgenden Eigenschaft

$$ker\chi = (char(K)).$$

Weiter heißt $char(K)$ die Charakteristik des Körpers K [10, S. 9]. Genauso kann die Charakteristik für beliebige Ringe definiert werden [3, S. 132]. Für einen Ring R mit Einselement 1_R kann die Charakteristik folgendermaßen definiert werden:

$$\begin{aligned} \chi : \mathbb{Z} &\longrightarrow R \\ n &\longmapsto n \cdot 1_R \end{aligned}$$

und

$$char(R) := \begin{cases} 0, \text{ wenn } n \cdot 1_R \neq 0 \text{ für alle } n. \\ min\{n \in \mathbb{N} - \{0\} : n \cdot 1_R = 0\}, \text{ sonst.} \end{cases} \qquad [7, \text{S. } 61]$$

Lemma 2.5.1. *Für einen Körper K gilt für die Charakteristik $char(K) = 0$ oder $char(K)$ ist eine Primzahl [7, S. 61].*

Beweis. Es wird indirekt angenommen, dass die Charakteristik keine Primzahl und ungleich Null ist.

$$char(K) = m = k \cdot l \neq 0 \text{ wobei } 1 < k, l < m$$

Aus der Definition der Charakteristik folgt

$$0 = m \cdot 1_K = k \cdot l \cdot 1_K = (k \cdot 1)(l \cdot 1).$$

Da jeder Körper nullteilerfrei ist, muss $k \cdot 1 = 0$ oder $l \cdot 1 = 0$ gelten. Dies führt jedoch zu einem Widerspruch der Minimalität der Charakteristik. Damit ist die Aussage gezeigt [7, S. 61]. □

Nun können endliche Körper betrachtet werden:

Definition. Ein Körper F heißt endlich, genau dann, wenn er eine endliche Anzahl von Elementen besitzt [11, S. 3]. Das heißt, die Ordnung $|F|$ ist endlich [10, S. 45].

Beispiel. Für jede Primzahl p ist der Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ endlich [10, S. 45]. Das heißt, $\mathbb{Z}/p\mathbb{Z}$ wird Primkörper der Charakteristik p genannt [7, S. 61].

Bemerkung. Für einen endlichen Körper F ist der Primkörper in F isomorph zu $\mathbb{F}_p$ für eine Primzahl p. Also gilt für die Charakteristik von F: $char(F) > 0$. Außerdem ist F ein $\mathbb{F}_p$-Vektorraum mit endlicher Basis. Es gilt daher $|F| = p^n$ mit $p \in \mathbb{N}$, wobei $p = char(F)$ und $n = dim_{\mathbb{F}_p} F$ [10, S. 45].
Somit gibt es zu jedem endlichen Körper F eine Primzahl p, sodass $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Unterkörper von F ist und die Anzahl der Elemente von F einer Potenz von p entspricht [7, S. 61].

Definition. Sei K ein Körper und das Polynom $f \in K[T]$ mit einem Grad ≥ 1, also keine Einheit und ungleich Null. Weiters sei $K \subset L$ eine Körpererweiterung. Wir definieren L als zerfällenden Oberkörper für f, wenn f in dem faktoriellen Ring $L[T]$ in Linearfaktoren zerfällt mit $c \in K, \alpha_i \in L, n_i \geq 1$

$$f = c \cdot (x - \alpha_1)^{n_1} \cdot ... \cdot (x - \alpha_r)^{n_r} \text{ [3, S. 252].}$$

Definition. Der minimale Zerfällungskörper von f ist der Zerfällungskörper L von f, der von den Nullstellen von f erzeugt wird [10, S. 29]. Das heißt $L = K(\alpha_1, ..., \alpha_r)$, wobei α_i die Nullstellen des Polynoms f über K sind [3, S. 252].

Beispiel. Der Körper $\mathbb{C}$ stellt einen Zerfällungskörper von $x^2+1 \in \mathbb{R}[T]$ dar. Das Polynom zerfällt in die folgenden Linearfaktoren:

$$x^2 + 1 = (x + i)(x - i)$$

Es gilt $\mathbb{C} = \mathbb{R}[i]$ [3, S. 252].

2.5.1 Existenzsatz für endliche Körper

Lemma 2.5.2. *Sei F ein endlicher Körper und $|F| = q = p^n$. Dann gilt, dass jedes α aus F eine Nullstelle des Polynoms $P(x) := x^q - x \in \mathbb{F}_p[T]$ ist. Außerdem ist F ein minimaler Zerfällungskörper von P über $\mathbb{F}_p$. Daher ist F bis auf $\mathbb{F}_p$-Isomorphie eindeutig [10, S. 45].*

Beweis. Die Anzahl der Elemente der multiplikativen Gruppe F^* ist $q - 1$, da F die Kardinalität von q hat und die multiplikative Gruppe F^* das Nullelement exkludiert. Für jedes $\alpha \in F^*$ gilt nach dem Satz von Lagrange $\alpha^{q-1} = 1$. Damit ist jedes $\alpha \in F^*$ eine Nullstelle des Polynoms $x^{q-1} - 1$. Weiterhin sind alle $\alpha \in F$ Nullstellen von $x^q - x$. Dementsprechend existieren q Nullstellen des Polynoms P in F. Aufgrund des Grades von P mit $deg(P) = q$ zerfällt P vollständig innerhalb von $F[T]$. Somit gilt

$$\mathbb{F}_p(\text{Nullstelle von } P \text{ in } F) = F.$$

Zusammenfassend kann man schlussfolgern, dass F alle Nullstellen von $P(x)$ enthält und P vollständig in Linearfaktoren zerfällt. Damit ist F minimaler Zerfällungskörper von P über $\mathbb{F}_p$ [10, S. 46]. □

Lemma 2.5.3. *Sei wiederum F ein endlicher Körper und $|F| = q = p^n$. Wenn L/F ein Erweiterungskörper ist, in dem $P(x) := x^q - x$ vollständig in Linearfaktoren zerfällt, dann ist F die Menge der Nullstellen von P in L [10, S. 46].*

Beweis. Aus dem letzten Lemma folgt, dass die Elemente $\alpha \in F \subseteq L$ die Nullstellen von P sind. Insgesamt sind das q Nullstellen. Aufgrund dessen, dass P den Grad q besitzt, müssen dies bereits alle möglichen Nullstellen von P in L sein. Damit ist die Aussage gezeigt [10, S. 46]. □

In weiterer Folge wird gezeigt, dass zu jeder Primzahlpotenz p^n genau ein endlicher Körper existiert mit $|F| = q = p^n$. Durch die beiden Lemmata kann dieser Körper mithilfe des Zerfällungskörpers von $P = x^q - x$ oder als Nullstellenmenge von P in einem Körper, in dem P vollständig in Linearfaktoren zerfällt, konstruiert werden. Schwierigkeiten birgt diese Vorgehensweise allerdings darin, zu zeigen, dass dieser Körper die Kardinalität von q besitzt. Dafür wird als Hilfsmittel die folgende Abbildung definiert [10, S. 46].

Definition. Sei K ein Körper der Charakteristik $p > 0$. Die Abbildung

$$Fr_K = Fr_p : K \to K,\ \alpha \mapsto \alpha^p$$

heißt Frobeniusmorphismus [10, S. 46].

Bemerkung. Die eben definierte Abbildung ist verträglich mit der Addition und Multiplikation auf K [4, 10, S. 89, S. 46]. Für die Addition gilt

$$Fr_p(x+y) = (x+y)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} + y^p = x^p + y^p = Fr_p(x) + Fr_p(y),$$

denn aufgrund der Charakteristik p und der Teilbarkeit des Binomialkoeffizienten $\binom{p}{i}$ durch p für $i = 1, ..., p-1$ ist $\binom{p}{i} = 0$. Weiters gilt für die Multiplikation

$$Fr_p(x \cdot y) = x^p \cdot y^p = Fr_p(x) \cdot Fr_p(y).$$

Es folgt, dass die Abbildung ein Körpermorphismus ist [10, S. 46].

Bemerkung. Sei F ein Körper der Charakteristik p, dann gilt:

i) Die Abbildung $(Fr_p)^n : F \to F,\ x \mapsto x^{p^n}$ ist auch ein Körpermorphismus.

ii) Für einen endlichen Körper F ist der Frobeniusmorphismus ein Automorphismus. Dies gilt aufgrund der Injektivität jedes Körpermorphismus [10, S. 47].

In weiterer Folge wird gezeigt, dass zu jeder Primzahlpotenz $p^n = q$ ein Erweiterungskörper $\mathbb{F}_q/\mathbb{F}_p$ mit der Kardinalität $|\mathbb{F}_q| = q$ existiert [10, S. 48].

Lemma 2.5.4. *Sei $q = p^n$ mit $n \in \mathbb{N}$ und einer Primzahl p. Sei weiters L ein Körper der Charakteristik p und das Polynom $P(x) = x^q - x$ zerfällt in $L[T]$ vollständig in $P \in \mathbb{F}_p$ Linearfaktoren. Es gilt, dass die Menge L' der Nullstellen des Polynoms P in L einen Teilkörper von L mit der Kardinalität $|L'| = q$ bildet [10, S. 47].*

Beweis. Für den Beweis betrachten wir ein Element α aus der Nullstellenmenge von P. Es folgt

$$\alpha \in L' \iff P(\alpha) = 0 \iff \alpha^q = \alpha \iff (Fr_p)^n(\alpha) = \alpha.$$

Wie bereits bemerkt, ist $(Fr_p)^n$ ein Körpermorphismus. Aufgrund dessen ist sowohl die Addition, die Multiplikation als auch die Inversenbildung in L' abgeschlossen. Es folgt, dass $L' \subseteq L$ ein Teilkörper ist. Nun ist noch zu zeigen, dass L' insgesamt q Elemente besitzt. Dafür betrachtet man die Nullstellen des Polynoms P. Nach Voraussetzung zerfällt P vollständig in L. Die Nullstellen müssen allesamt einfach sein, um die Aussage zu beweisen. Man betrachte eine beliebige Nullstelle des Polynoms $\alpha \in L'$. Es gilt:

$$\begin{aligned} x^q - x &= x^q - x + (\alpha - \alpha^q) = x^q - \alpha^q - x + \alpha \\ &= (x - \alpha)^q - (x - \alpha) = (x - \alpha)[(x - \alpha)^{q-1} - 1] \end{aligned}$$

Es folgt, dass α keine Nullstelle von $(x - \alpha)^{q-1} - 1$ ist, da $(\alpha - \alpha)^{q-1} - 1 = -1$. Damit handelt es sich bei α um eine einfache Nullstelle des Polynoms. Demnach besitzt P nur einfache Nullstellen und $|L'| = q$ folgt [10, S. 47]. □

Lemma 2.5.5. *Sei F ein Zerfällungskörper von $x^q - x$ über $\mathbb{F}_p$ mit einer Primzahl p und $q = p^n$, so hat F insgesamt q Elemente: $|F| = q$ [10, S. 47].*

Beweis. Wie im Lemma zuvor sei L' die Nullstellenmenge von $x^q - x$ in F. Es folgt, dass L' ein Teilkörper von F ist. Außerdem folgt die Gleichheit $L' = F$, da L' die gesamten Nullstellen von $x^q - x$ enthält. Für die Kardinalität gilt demnach $|F| = |L'| = q$. Das heißt, $L' = F$ [10, S. 47]. □

Nun kann zusammenfassend für dieses Kapitel der folgende Satz formuliert werden:

Theorem 2.5.6. *Zu jeder Primzahlpotenz p^r mit $r \in \mathbb{N}$ gibt es genau einen Körper $\mathbb{F}_{p^r}$, der p^r Elemente besitzt. Es handelt sich um den Zerfällungskörper von $x^{p^r} - x \in \mathbb{F}_p[T]$ [3, S. 265].*

Beweis. Zuerst wird die Existenz des Körpers mit p^r Elementen gezeigt: Sei L der Zerfällungskörper von P. Das heißt, P zerfällt in L in Linearfaktoren. Aus Lemma 2.5.4 folgt, die Menge der Nullstellen von P in L ist Körper $\mathbb{F}$ mit einer Anzahl von $q = p^r$ Elementen.
Dass $\mathbb{F}_{p^r}$ eindeutig bestimmt ist, wird im nächsten Schritt gezeigt. Sei nun F ein Körper mit p^r Elementen. Aus dem Lemma 2.5.2 folgt, dass jedes $\alpha \in F$ eine Nullstelle von $P = x^q - x \in \mathbb{F}_p[T]$ mit $q = p^r$ ist. Nach Definition ist $F \subset L$ der Zerfällungskörper von P, wobei L eindeutig bestimmt ist. Aus dem Lemma 2.5.3 folgt, dass F die Menge der Nullstellen von P in L ist. Demnach ist F bis auf Isomorphie eindeutig bestimmt [3, S. 265]. □

2.5.2 Multiplikative Gruppe eines Körpers ist zyklisch

Eine wichtige Eigenschaft von endlichen Körpern betrifft die multiplikative Gruppe. Bevor diese Aussage der Kapitelüberschrift formuliert wird, betrachten wir zunächst die Definition des Begriffs zyklisch.

Definition. Eine Gruppe G heißt zyklisch, wenn es ein Element $g \in G$ gibt, sodass $G = \langle g \rangle$ gilt [3, S. 34]. Das heißt, die Gruppe wird von einem Element erzeugt [3, S. 217].

Beispiel. Ein Beispiel für eine Gruppe, die zyklisch erzeugt wird, ist etwa $n\mathbb{Z}$ als Untergruppe von $(\mathbb{Z}, +)$. Es gilt $n\mathbb{Z} = \langle n \rangle$ [3, S. 35].

Definition. Für ein Element $g \in G$ einer Gruppe G ist $|\langle g \rangle|$ die Ordnung von g [3, S. 35].

Theorem 2.5.7. *Sei $q = p^n$ eine Primzahlpotenz. Die multiplikative Gruppe $\mathbb{F}_q$ ist zyklisch und von der Ordnung $q - 1$ [4, S. 128].*

Um dieses Theorem zu zeigen, wird eine allgemeinere Aussage betrachtet:

Theorem 2.5.8. *Sei K ein Körper und K^* die multiplikative Gruppe. Jede endliche Untergruppe H von K^* ist zyklisch [4, S. 121].*

Beweis. Sei a ein Element der Untergruppe H von maximaler Ordnung m. Weiters sei H_m eine Untergruppe von H, die alle Elemente, deren Ordnung ein Teiler von m ist, enthält. Demzufolge sind alle diese Elemente Nullstellen des Polynoms $x^m - 1$ und H_m kann maximal m Elemente enthalten. Demgegenüber besteht die Untergruppe H_m auch aus der von a erzeugten zyklischen Gruppe, deren Ordnung m ist. Folglich gilt, H_m ist zyklisch und $H_m = \langle a \rangle$. Nun bleibt die folgende Gleichheit zu zeigen: $H = H_m$. Angenommen es gäbe ein Element $b \in H$ und $b \notin H_m$, dann besitzt dieses Element eine Ordnung n, die nicht m teilt [4, S. 121]. Es müsste aber ein Element in der Gruppe existieren, das die Ordnung $kgV(m, n) > m$ besitzt [4, S. 120]. Dies widerspricht der Bedingung für die Wahl des Elements a. Damit ist $H = H_m$ und die Untergruppe H zyklisch [4, S. 121]. □

Bemerkung. Der Beweis zeigt, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist. Diese Eigenschaft kann nun auch auf $\mathbb{F}_q$ angewendet werden, bei dem es sich ebenfalls um eine multiplikative Gruppe eines endlichen Körper handelt. Die Ordnung ist $q-1$, da $|\mathbb{F}_q^*| = q-1$ gilt. Dies begründet die Aussage des Theorems 2.5.7. [4, S. 128].

Da nun endliche Körper konstruiert wurden, ihre Existenz gezeigt und die zyklische Eigenschaft der multiplikativen Gruppe $\mathbb{F}_q^*$ beleuchtet wurde, kann sich das folgende Kapitel den Polynomringen über endlichen Körpern widmen.

2.6 Polynomringe über endlichen Körpern

In diesem Abschnitt sei $\mathbb{F} = \mathbb{F}_q$ der endliche Körper mit q Elementen. Nach Kapitel 2.5. gilt $q = p^f$ und p ist die Charakteristik von $\mathbb{F}$. Weiter sei $\mathbb{F}[T]$ der Polynomring über $\mathbb{F}$. Der Polynomring $\mathbb{F}[T]$ und der Ring der ganzen Zahlen $\mathbb{Z}$ weisen einige gemeinsame Eigenschaften auf: Beide sind etwa Hauptidealringe, haben eine endliche Einheitengruppe und die Eigenschaft, dass jeder Restklassenring modulo eines Nicht-Null-Ideals endlich viele Elemente besitzt. Aus diesem Grund können viele Fragen der Zahlentheorie zu den ganzen Zahlen $\mathbb{Z}$ als Analogon in dem Ring $\mathbb{F}[T]$ betrachtet werden. Etwa sind dabei normierte Polynome ein Analogon zu positiven ganzen Zahlen [13, S. 1].

Proposition 2.6.1. *Sei $g \in \mathbb{F}[T]$ und $g \neq 0$, dann ist $\mathbb{F}[T]/g\mathbb{F}[T]$ ein endlicher Ring mit $q^{deg(g)}$ Elementen [13, S. 2].*

Beweis. Sei m der Grad des Polynoms $m = deg(g)$. Aufgrund der Division mit Rest gilt, dass die Menge $\{r \in \mathbb{F}[T] | deg(r) < m\}$ die Restklassen von Polynomen $\mathbb{F}[T]/g\mathbb{F}[T]$ repräsentiert. Die Elemente dieser Menge besitzen die folgende Gestalt:

$$r = \alpha_{m-1}x^{m-1} + \alpha_{m-2}x^{m-2} ... + \alpha_0 \text{ wobei } \alpha_i \in \mathbb{F}.$$

Da die Koeffizienten α_i unabhängig voneinander im endlichen Körper $\mathbb{F}$ gewählt werden können und $|\mathbb{F}| = q$ gilt, gibt es q^m solcher Polynome. Der Ring hat damit q^m Elemente und die Aussage folgt [13, S. 2]. □

Definition. Für ein Polynom $g \in \mathbb{F}[T]$ mit $g \neq 0$ ist der Betrag definiert durch

$$|g| = q^{deg(g)},$$

wobei $q = |\mathbb{F}|$. Für das Nullpolynom $g = 0$ setzen wir den Betrag $|g| = 0$ [13, S. 2].

Bemerkung.

i) Der Betrag dient als Instrument zur Bestimmung der Größe des Polynoms g. Für eine ganze Zahl n ist der Absolutbetrag $|n|$ die Anzahl der Elemente von $\mathbb{Z}/n\mathbb{Z}$. Genauso gilt für $|g|$, dass er der Anzahl der Elemente von $\mathbb{F}[T]/g\mathbb{F}[T]$ entspricht [13, S. 2].

ii) Für die Polynome f und g gilt

$$|f \cdot g| = |f| \cdot |g|.$$

iii) Für zwei Polynome f und g, deren Beträge nicht übereinstimmen, also $|f| \neq |g|$, folgt die Gleichung

$$|f + g| = max(|f|, |g|) \text{ [13, S. 2].}$$

In weiterer Folge wird die Einheitengruppe $\mathbb{F}[T]^*$ beschrieben. Wie eingangs definiert, gilt, wenn g eine Einheit ist, dann existiert ein Polynom f mit $f \cdot g = 1$. Da aber $0 = deg(1) = deg(f) + deg(g)$ gilt, muss für die Polynome f und g folgen, dass $deg(f) = deg(g) = 0$. Wie bereits im Kapitel 2.3 bemerkt, sind die einzigen Einheiten demnach die Nicht-Null-Konstanten [13, S. 2].

Proposition 2.6.2. *Die Einheitengruppe in $\mathbb{F}[T]$ ist $\mathbb{F}^*$, eine endliche zyklische Gruppe mit $q-1$ Elementen [13, S. 2].*

Beweis. Es bleibt lediglich die Eigenschaft zu zeigen, dass $\mathbb{F}^*$ zyklisch ist, die aus dem Theorem 2.5.7. (bzw. 2.5.8.) folgt, wonach jede endliche Untergruppe einer multiplikativen Gruppe eines Körpers zyklisch ist [13, S. 2]. □

Nun wird die Struktur des Rings $\mathbb{F}[T]/f\mathbb{F}[T]$ und die der Einheitengruppe $(\mathbb{F}[T]/f\mathbb{F}[T])^*$ untersucht.

Proposition 2.6.3. *Seien $m_1, m_2, m_3, ..., m_t$ Elemente von $\mathbb{F}[T]$ und zueinander paarweise teilerfremd. Sei $m = m_1 \cdot m_2 \cdot ... \cdot m_t$ und ϕ_i der natürliche Homomorphismus von $\mathbb{F}[T]/m\mathbb{F}[T]$ zu $\mathbb{F}[T]/m_i\mathbb{F}[T]$ mit $a + m\mathbb{F}[T] \mapsto a + m_i\mathbb{F}[T]$. Die Abbildung*

$$\phi : \mathbb{F}[T]/m\mathbb{F}[T] \to \mathbb{F}[T]/m_1\mathbb{F}[T] \oplus \mathbb{F}[T]/m_2\mathbb{F}[T] \oplus ... \oplus \mathbb{F}[T]/m_t\mathbb{F}[T],$$

die gegeben ist durch

$$\phi(a) = (\phi_1(a), \phi_2(a), ...\phi_t(a)),$$

ist ein Ringisomorphismus [13, S. 3].

Beweis. Der chinesische Restsatz für den Ring $R = \mathbb{F}[T]$ beweist dieses Theorem. Er wurde bereits am Ende des Kapitel 2.1. bewiesen [13, S. 3]. □

Korollar 2.6.4. *Dieselbe Abbildung ϕ eingeschränkt auf die Einheiten von $\mathbb{F}[T], \mathbb{F}[T]^*$ führt zu einem Gruppenisomorphismus*

$$(\mathbb{F}[T]/m\mathbb{F}[T])^* \simeq (\mathbb{F}[T]/m_1\mathbb{F}[T])^* \times (\mathbb{F}[T]/m_2\mathbb{F}[T])^* \times ... \times (\mathbb{F}[T]/m_t\mathbb{F}[T])^* \text{ [13, S. 3].}$$

Sei nun $f \in \mathbb{F}[T]$ ein Nicht-Null-Polynom und keine Einheit. Außerdem wird angenommen, dass f die die folgende Primfaktorzerlegung besitzt

$$f = \alpha \cdot P_1^{e_1} \cdot P_2^{e_2} \cdot ... \cdot P_t^{e_t},$$

wobei P_i irreduzible Polynome und die Exponenten e_i ganze, nicht negative Zahlen sind und $\alpha \in \mathbb{F}^*$. Aus dem Korollar zuvor folgt, dass die Einheitengruppe des Quotientenrings $(\mathbb{F}[T]/f\mathbb{F}[T])$ isomorph zu dem Produkt der Einheitenguppen der Quotientenringe $(\mathbb{F}[T]/P_i^{e_i}\mathbb{F}[T])$ ist.
Demnach gilt

$$(\mathbb{F}[T]/f\mathbb{F}[T])^* \simeq (\mathbb{F}[T]/P_1^{e_1}\mathbb{F}[T])^* \times (\mathbb{F}[T]/P_2^{e_2}\mathbb{F}[T])^* \times ... \times (\mathbb{F}[T]/P_t^{e_t}\mathbb{F}[T])^* \text{ [13, S. 3].}$$

Den speziellen Fall, dass $f = P$ irreduzibel ist, beschreibt die folgende Proposition:

Proposition 2.6.5. *Sei $P \in \mathbb{F}[T]$ ein irreduzibles Polynom. Dann ist $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ eine zyklische Gruppe mit $|P| - 1$ Elementen [13, S. 4].*

Beweis. Da $\mathbb{F}[T]$ ein Hauptidealring ist, ist $P\mathbb{F}[T] = (P)$ nach Theorem 2.2.4. ein Maximalideal. Außerdem ist nach Theorem 2.6.1. $\mathbb{F}[T]/P\mathbb{F}[T]$ ein endlicher Körper. Die endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch. Also ist $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ zyklisch nach Theorem 2.5.8. des vorherigen Kapitels. Genauso folgt aus 2.6.1., dass die Gruppe $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ insgesamt $|P| - 1$ Elemente besitzt, da $|\mathbb{F}[T]/P\mathbb{F}[T]| = q^{deg(P)} = |P|$. [13, S. 4]. □

In nachfolgender Proposition wird die Struktur der Einheiten im Faktorring $(\mathbb{F}[T]/P^e\mathbb{F}[T])^*$ beschrieben, wobei $e > 1$ gilt. Nun unterscheidet sich die Struktur grundlegend zu der der ganzen Zahlen [13, S. 4].

Proposition 2.6.6. *Für ein irreduzibles Polynom $P \in \mathbb{F}[T]$ und e eine positive ganze Zahl, ist die Anzahl der Elemente der Einheitengruppe $(\mathbb{F}[T]/P^e\mathbb{F}[T])^*$ die folgende:*

$$|P|^{e-1} \cdot (|P| - 1)$$

Sei außerdem $(\mathbb{F}[T]/P^e\mathbb{F}[T])^{(1)}$ der Kern der natürlichen Abbildung von $(\mathbb{F}[T]/P^e\mathbb{F}[T])^*$ zu $(\mathbb{F}[T]/P\mathbb{F}[T])^*$. Hierbei handelt es sich um eine p-Gruppe der Ordnung $|P|^{e-1}$. Wenn e gegen Unendlich strebt, strebt die kleinste Zahl der Erzeuger von $(\mathbb{F}[T]/P^e\mathbb{F}[T])^{(1)}$ ebenfalls gegen Unendlich [13, S. 4].

Beweis. Um diese Proposition zu beweisen, wird zunächst die Größe von $(\mathbb{F}[T]/P^e\mathbb{F}[T])^{(1)}$ gezeigt. Der Ring $\mathbb{F}[T]/P^e\mathbb{F}[T]$ besitzt nach Theorem 2.2.4. das Maximalideal $P\mathbb{F}[T]/P^e\mathbb{F}[T]$ mit der Anzahl von $|P|^{e-1}$ Elementen. Demnach hat $(\mathbb{F}[T]/P^e\mathbb{F}[T])^* = \mathbb{F}[T]/P^e\mathbb{F}[T] - P\mathbb{F}[T]/P^e\mathbb{F}[T]$ eine Anzahl von $|P|^e - |P|^{e-1} = |P|^{e-1} \cdot (|P| - 1)$ Elementen. Da die Abbildung von $(\mathbb{F}[T]/P^e\mathbb{F}[T])^* \longrightarrow (\mathbb{F}[T]/P\mathbb{F}[T])^*$ surjektiv ist (denn f ist eine Einheit genau dann, wenn Teilerfremdheit gilt, das heißt, wenn $ggT(f, P) = 1$ bzw. $ggT(f, P^e) = 1$) und die Gruppe $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ insgesamt $|P| - 1$ Elemente besitzt, folgt die Behauptung zur Größe von $(\mathbb{F}[T]/P^e\mathbb{F}[T])^{(1)}$:

$$|(\mathbb{F}[T]/P^e\mathbb{F}[T])^{(1)}| = |P|^{e-1} \text{ [13, S. 4]}$$

Diese Folgerung kann gezogen werden, wenn die folgende Kette von Abbildungen, sogar exakte Sequenz, betrachtet wird:

$$1 \longrightarrow (\mathbb{F}[T]/P^e)^{(1)} \longrightarrow (\mathbb{F}[T]/P^e)^* \longrightarrow (\mathbb{F}[T]/P)^* \longrightarrow 1$$

Die Kardinalität von $(\mathbb{F}[T]/P^e)^*$ ist $|P|^e - |P|^{e-1} = |P|^{e-1}(|P| - 1)$ und die Kardinalität von $(\mathbb{F}[T]/P)^*$ ist $|P| - 1$. Für die Kardinalität des Kerns $(\mathbb{F}[T]/P^e\mathbb{F}[T])^{(1)}$ heißt das demnach

$$|(\mathbb{F}[T]/P^e\mathbb{F}[T])^{(1)}| = \tfrac{|P|^{e-1}(|P|-1)}{|P|-1} = |P|^{e-1}.$$

Nun bleibt noch die Aussage der minimalen Zahl der Erzeuger zu zeigen. Betrachten wir hierfür zunächst den Fall $e = 2$. Jedes Element von $(\mathbb{F}[T]/P^2\mathbb{F}[T])^{(1)}$ kann als Polynom der Form $a = 1 + bP$ geschrieben werden. Da die Charakteristik p ist, gilt

$$a^p = 1 + b^p \cdot P^p \equiv 1(modP^2).$$

Damit ist $(\mathbb{F}[T]/P^2\mathbb{F}[T])^{(1)}$ eine Gruppe der Ordnung $|P| = q^{degp} = p^{fdegp}$ vom Exponent p. Es folgt, dass $(\mathbb{F}[T]/P^2\mathbb{F}[T])^{(1)}$ als eine direkte Summe von insgesamt $fdeg(P)$ Kopien der zyklischen Gruppe $\mathbb{Z}/p\mathbb{Z}$ geschrieben werden kann. Dies ist eine zyklische Gruppe unter der sehr restriktiven Bedingung, sodass $q = p$ und $deg(P) = 1$ gilt.
Für den allgemeinen Fall wird angenommen, dass s die kleinste ganze Zahl ist, sodass $p^s \geq e$. Es gilt $(1 + bP)^{p^s} = 1 + (bP)^{p^s} \equiv 1(modP^e)$. Damit hat die Gruppe $G = (\mathbb{F}[T]/P^e\mathbb{F}[T])^{(1)}$ den Exponenten p^s. Es folgt, dass es eine surjektive Abbildung von $(\mathbb{Z}/p^s\mathbb{Z})^d$ zu G gibt, für ein gewisses $d \in \mathbb{N}$. In weiterer Folge wird die Größe von d abgeschätzt: Es gilt

$$p^{ds} = (p^s)^d = |(\mathbb{Z}/p^s\mathbb{Z})^d| \quad \geq \quad |G| = |P|^{e-1} = q^{deg(P)(e-1)} = p^{fdeg(P)(e-1)}$$

und daher

$$p^{ds} \geq p^{fdeg(P)(e-1)}.$$

Weiter folgt

$$d \geq \frac{fdeg(P)(e-1)}{s}.$$

Da s die kleinste ganze Zahl größer oder gleich als $log_p(e)$ ist, folgt, dass wenn $e \to \infty$ auch $d \to \infty$ [13, S. 4]. □

Nun wurden genügend Eigenschaften der Einheitengruppe $(\mathbb{F}[T]/P^e\mathbb{F}[T])^*$ beschrieben, um im Anschluss Analogien zur Eulerschen Phi-Funktion und dem Kleinen Satz von Euler und Fermat zu ziehen [13, S. 5].
Sei f ein Nicht-Null-Polynom und sei $\phi(f)$ die Anzahl der Elemente der Gruppe $(\mathbb{F}[T]/f\mathbb{F}[T])^*$. Diese Zahl kann auch auf eine andere Weise definiert werden: Die Menge $\{r \in \mathbb{F}[T] | deg(r) < deg(f)\}$ beschreibt die Vertreter der Menge $\mathbb{F}[T]/f\mathbb{F}[T]$. Weiter ist r genau dann eine Einheit in $\mathbb{F}[T]/f\mathbb{F}[T]$, wenn es teilerfremd zu f ist. Damit ist $\phi(f)$ die Anzahl der Polynome (die nicht Null sind), deren Grad kleiner als der Grad von f ist und die relativ prim zu f sind [13, S. 5]. Dies folgt aus Theorem 2.2.9.

Proposition 2.6.7. *Für die Euler'sche ϕ-Funktion für Polynomringe gilt*

$$\phi(f) = |f| \cdot \prod_{P|f} (1 - \tfrac{1}{|P|}) \text{ [13, S. 5].}$$

Beweis. Sei $f = \alpha \cdot P_1^{e_1} \cdot ... \cdot P_t^{e_t}$ die Primfaktorzerlegung von f. Aus dem Korollar 2.6.4 folgt bezüglich Anzahl der Einheiten

$$\phi(f) = \prod_{i=1}^{t} \phi(P_i^{e_i}).$$

Weiter folgt aus Proposition 2.6.6.

$$\prod_{i=1}^{t} \phi(P_i^{e_i}) = \prod_{i=1}^{t} (|P_i|^{e_i} - |P_i|^{e_i-1}).$$

Damit ist die Aussage gezeigt [13, S. 5]. □

Nun betrachten wir die direkte Analogie des kleinen Satzes von Euler und Fermat [13, S. 5].

Proposition 2.6.8. *Für ein Polynom $f \in \mathbb{F}[T]$ mit $f \neq 0$ und ein Element $a \in \mathbb{F}[T]$, das teilerfremd zu f ist, gilt*

$$a^{\phi(f)} \equiv 1 \pmod{f} \text{ [13, S. 5].}$$

Beweis. Nach Definition hat die Gruppe $(\mathbb{F}[T]/f\mathbb{F}[T])^*$ insgesamt $\phi(f)$ Elemente. Die Restklasse von a modulo f liegt in dieser Gruppe. Damit gilt $\overline{a}^{\phi(f)} = \overline{1}$. Diese Gleichheit ist äquivalent zur Aussage der Proposition [13, S. 5]. □

Korollar 2.6.9. *Sei $P \in \mathbb{F}[T]$ ein irreduzibles Polynom und $a \in \mathbb{F}[T]$ ein Polynom, das nicht durch P teilbar ist. Dann gilt*

$$a^{|P|-1} \equiv 1 \pmod{P} \text{ [13, S. 5].}$$

Beweis. Da P irreduzibel ist, ist es relativ prim zu a genau dann, wenn es a nicht teilt. Die Aussage folgt aus der Proposition zuvor und aus der Proposition 2.6.5. Wonach für ein irreduzibles Polynom P Folgendes gilt, dass $\phi(P) = |P| - 1$ [13, S. 5]. □

In weiterer Folge betrachten wir die Polynom-Version des Wilson's Theorems [13, S. 6].

Proposition 2.6.10. *Sei wiederum $P \in \mathbb{F}[T]$ ein irreduzibles Polynom mit dem Grad d. Sei außerdem X Unbestimmte über dem Polynomring $\mathbb{F}[T]$. Dann gilt*

$$X^{|P|-1} - 1 \equiv \prod_{0 \leq deg(f) < d} (X - f) \pmod{P} \text{ [13, S. 6].}$$

Das Nullpolynom ist hier ausgenommen, da $deg(0) = -\infty$ gilt [13, S. 1, 6].

Beweis. Um die Aussage zu zeigen, betrachten wir die Menge $\{f \in \mathbb{F}[T] | deg(f) < d\}$ der Repräsentanten der Restklassen von $\mathbb{F}[T]/P\mathbb{F}[T]$. Wenn das Nullelement $f = 0$ exkludiert wird, erhält man die Menge der Elemente von $(\mathbb{F}[T]/P\mathbb{F}[T])^*$. Der nächste Schritt folgt aus dem Korollar 2.6.9: Demnach gilt (wobei hier $\overline{1}$ und $\overline{f}$ für die Restklassen modulo P stehen)

$$X^{|P|-1} - \overline{1} = \prod_{0 \leq deg(f) < d} (X - \overline{f}).$$

Dies gilt, da beide Seiten der Gleichung normierte Polynome mit derselben Menge von Nullstellen im Körper $\mathbb{F}[T]/P\mathbb{F}[T]$ darstellen:
Aus Korollar 2.6.9. folgt, dass alle Restklassen $\overline{f}$, mit f nicht durch P teilbar, Nullstellen des Polynoms $X^{|P|-1} - \overline{1}$ sind. Das bedeutet, dass die Elemente $\overline{f}$ alle Elemente der multiplikativen Einheitengruppe $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ durchlaufen. Da es $|P| - 1$ dieser Elemente gibt, hat das Polynom $X^{|P|-1} - \overline{1}$ auch $|P| - 1$ Nullstellen. Weil der Grad des Polynoms $|P| - 1$ ist, besitzt es daher genau alle diese Nullstellen. Da beide Seiten der Gleichung normierte Polynome mit denselben Nullstellen sind, muss die Differenz dieser das Nullpolynom sein. Die behauptete Kongruenz aus der Proposition ist äquivalent zu dieser Aussage [13, S. 6]. □

Ähnliche Strukturen findet man im folgenden Korollar:

Korollar 2.6.11. *Sei d ein Teiler von $|P| - 1$. Die Kongruenz $X^d \equiv 1$ (mod P) hat genau d Lösungen. Äquivalent dazu besitzt die Gleichung $X^d = \overline{1}$ genau d Lösungen in $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ [13, S. 6].*

Beweis. In diesem Beweis wird die zweite Aussage gezeigt: Aufgrund dessen, dass d die Zahl $|P| - 1$ teilt, folgt, dass $X^d - 1$ ein Teiler von $X^{|P|-1} - 1$ ist. Das letztere Polynom zerfällt in verschiedene Linearfaktoren. Dies folgt aus dem Kapitel 2.5. Genauso zerfällt das erste Polynom $X^d - 1$ in verschiedene Linearfaktoren. Damit ist die Aussage gezeigt [13, S. 6]. □

Korollar 2.6.12. *Sei $P \in \mathbb{F}[T]$ wiederum ein irreduzibles Polynom und $f \neq 0$. Es gilt:*

$$\prod_{0 \leq deg(f) < deg(P)} f \equiv -1 \text{ (mod } P\text{) [13, S. 6].}$$

Beweis. Für den Beweis setzen wir in Propositon 2.6.10 für $X = 0$.

$$-1 \equiv \prod_{0 \leq deg(f) < deg(P)} -f \quad (mod \text{ P})$$

Da $|P| = q^{degp} = p^{f degP}$ und p eine ungerade Primzahl ist, folgt, dass $|P| - 1$ eine gerade Zahl ist, wenn die Charakteristik von $\mathbb{F}$ ungerade ist. Da das Produkt von einer geraden Anzahl von Elementen zu -1 führt, folgt das Resultat. Ist die Charakteristik 2, so gilt $-1 = 1$, da $-1 \equiv 1 \pmod 2$ ist und das Resultat folgt ebenfalls [13, S. 6]. □

Um im nächsten Kapitel das Reziprozitätsgesetz für $\mathbb{F}[T]$ zu beschreiben, wird die folgende Definition in der nächsten Proposition benötigt:

Definition. Ein Polynom $a \in \mathbb{F}[T]$ heißt d-ter Potenzrest modulo f für ein Polynom f mit positivem Grad, das teilerfremd zu a ist, wenn die Gleichung

$$x^d \equiv a \pmod f$$

in $\mathbb{F}[T]$ lösbar ist. Äquivalent dazu ist, dass die Restklasse $\overline{a} \in (\mathbb{F}[T]/f\mathbb{F}[T])^*$ eine d-te Potenz in der multiplikativen Gruppe ist, das heißt, es gibt ein $\overline{x} \in (\mathbb{F}[T]/f\mathbb{F}[T])^*$ mit $\overline{x}^d = \overline{a}$ [13, S. 7].

Angenommen $f = \alpha \cdot P_1^{e_1} \cdot P_2^{e_2} \cdot ... \cdot P_t^{e_t}$ ist die Primfaktorzerlegung von f. Nun ist nach Korollar 2.6.4 a der d-te Potenzrest modulo f genau dann, wenn a ein d-te Potenzrest modulo $P_i^{e_i}$ für $1 \leq i \leq t$ ist. Diese Eigenschaft vereinfacht das Problem zu dem Fall, in dem der Modul eine Primfaktorpotenz ist [13, S. 7]. Dieser Fall wird nun beschrieben:

Proposition 2.6.13. *Sei P ein irreduzibles Polynom und $a \in \mathbb{F}[T]$ nicht teilbar durch P. Wenn d ein Teiler von $|P| - 1$ ist, dann ist die Kongruenz $X^d \equiv a \pmod{P^e}$ genau dann lösbar, wenn die folgende Kongruenz gilt:*

$$a^{\frac{|P|-1}{d}} \equiv 1 \pmod{P}.$$

Insgesamt gibt es $\frac{\phi(P^e)}{d}$ d-te Potenzreste modulo P^e [13, S. 7].

Beweis. Erst wird der Fall $e = 1$ betrachtet. Wenn die folgende Kongruenz gilt

$$b^d \equiv a \pmod{P},$$

dann folgt aus der Korollar 2.6.9., dass

$$a^{\frac{|P|-1}{d}} \equiv b^{|P|-1} \equiv 1 \pmod{P}.$$

Das wiederum zeigt, dass die Bedingung aus der Proposition notwendig ist.
Um zu zeigen, dass die Bedingung hinreichend ist, erinnern wir uns an das Wilson'sche Theorem, das explizit aus Korollar 2.6.11 folgt. Demnach sind alle d-ten Einheitswurzeln im Körper $\mathbb{F}[T]/P\mathbb{F}[T]$ enthalten. Betrachtet man den Homomorphismus von $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ mit $x \mapsto x^d$, so hat sein Kern also die Ordnung d und das Bild sind die d-ten Potenzen. Daher gibt es genau $\frac{|P|-1}{d} = \frac{\phi(P)}{d}$ viele d-te Potenzen in $(\mathbb{F}[T]/P\mathbb{F}[T])^*$. Nun ist ersichtlich, dass alle diese Potenzen die Gleichung $X^{\frac{|P|-1}{d}} - 1 = 0$ erfüllen. Sie sind die Nullstellen dieser Gleichung. Dies zeigt den Fall $e = 1$ [13, S. 7].

Für den Fall $e > 1$ benötigt man ein wenig Gruppentheorie. Die natürliche Abbildung (also die Reduktion auf modulo P) ist ein Homomorphismus von $(\mathbb{F}[T]/P^e\mathbb{F}[T])^*$ auf $(\mathbb{F}[T]/P\mathbb{F}[T])^*$. Dabei ist nach 2.6.6. der Kern dieser Abbildung eine p-Gruppe. Da die Ordnung von $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ gleich $|P| - 1$ prim zu p ist, folgt, dass die Struktur von $(\mathbb{F}[T]/P^e\mathbb{F}[T])^*$ als das Produkt einer p-Gruppe und einer Kopie von $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ geschrieben werden kann. Weil $(d, p) = 1$ gilt, ist das Erheben zur d-ten Potenz in einer abelschen p-Gruppe ein Automorphismus. Infolgedessen ist $a \in \mathbb{F}[T]$ genau dann ein d-ter Potenzrest modulo P^e, wenn a ein d-ter Potenzrest modulo P ist. Dies ist erfüllt, wenn $a^{\frac{|P|-1}{d}} \equiv 1 \pmod{P}$ gilt, wie oben im Fall $e = 1$ gezeigt. Nun betrachten wir den Automorphismus von $(\mathbb{F}[T]/P^e\mathbb{F}[T])^*$ gegeben durch $x \mapsto x^d$. Es folgt, dass der Kern dieser Abbildung d Elemente besitzt und das Bild der Untergruppe der d-ten Potenzen entspricht. Demnach hat diese Gruppe die Ordnung $\frac{\phi(P^e)}{d}$. Dies schließt den Beweis ab [13, S. 7]. □

3 Reziprozitätsgesetz

3.1 Potenzrestsymbol

3.1.1 Definition des Potenzrestsymbols

Da alle nötigen algebraischen Grundlagen beschrieben wurden, kann sich das folgende Kapitel dem Reziprozitätsgesetz widmen. Das Reziprozitätsgesetz wird nun in der allgemeinen Form für $\mathbb{F}_q[T]$ mit $q = p^f$ bewiesen. Im Vergleich zu diesem Beweis, ist der Nachweis der Gültigkeit der höheren Reziprozitätsgesetze im Ring der ganzen Zahlen deutlich aufwändiger - dafür werden viele fortgeschrittene Konzepte der algebraischen Zahlentheorie und der Klassenkörpertheorie benötigt. Carl Friedrich Gauß war der erste, der das quadratische Reziprozitätsgesetz in $\mathbb{Z}$ bewies. Er nannte es das „Goldene Theorem". Das Analogon des quadratischen Reziprozitätsgesetzes für $\mathbb{F}[T]$ zeigte Richard Dedekind. Der Beweis, der in diesem Kapitel präsentiert wird, ist der von Leonard Carlitz und orientiert sich an der Literatur von Michael Rosen [13, S. 23].

Zunächst wird das Potenzrestsymbol definiert, dazu betrachten wir ein irreduzibles Polynom P und d als einen Teiler von $q-1$, wobei q die Kardinalität von $\mathbb{F}_q$ ist. Wenn das Polynom $a \in \mathbb{F}[T]$ nicht durch P teilbar ist, das heißt, $\overline{a} \in (\mathbb{F}[T]/(P))^*$ hat nach Proposition 2.6.5 die Kardinalität $|P|-1$, dann ist die Kongruenz $X^d \equiv a \bmod P$ mit $X \in \mathbb{F}[T]$ genau dann lösbar, wenn

$$a^{\frac{|P|-1}{d}} \equiv 1 \bmod P \text{ [13, S. 23].}$$

Diese Aussage wurde bereits in Proposition 2.6.13 gezeigt. Die linke Seite der Kongruenz ist ein Element, dessen Ordnung in der Einheitengruppe $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ die Zahl d teilt, da $d|(q-1)$ und $(q-1)||P|-1$, wobei $|P| = q^{deg(P)}$ gilt, ist $|P|-1$ teilbar durch d. Demnach folgt, dass

$$(a^{\frac{|P|-1}{d}})^d = a^{|P|-1} \equiv 1 \bmod P,$$

weil $X^d \equiv 1 \bmod P$. Da die Abbildung $\mathbb{F}^* \longrightarrow (\mathbb{F}[T]/P\mathbb{F}[T])^*$ injektiv ist und die Kongruenz $x^d \equiv 1$ in $\mathbb{F}^*$ schon d Lösungen hat, sind das bereits alle Lösungen. Damit gibt es ein eindeutig bestimmtes $\alpha \in \mathbb{F}^*$, sodass

$$a^{\frac{|P|-1}{d}} \equiv \alpha \bmod P \text{ [13, S. 23].}$$

Nun wird mithilfe der Aussagen über die Lösbarkeit von Kongruenzen das Potenzrestsymbol definiert:

Definition. Sei d ein Teiler von $q-1$ und P ein irreduzibles Polynom, das $a \in \mathbb{F}[T]$ nicht teilt. Das Element $(a/P)_d \in \mathbb{F}^*$ ist das eindeutig bestimmte Element, für das gilt

$$a^{\frac{|P|-1}{d}} \equiv (\tfrac{a}{P})_d \bmod P.$$

Für den Fall, dass a durch P teilbar ist, definieren wir $(a/P)_d = 0$. Dieses Symbol wird das d-te Potenzrestsymbol genannt [13, S. 24].

Bemerkung. Unmittelbar aus der Definition des Potenzrestsymbols folgt

$$(\tfrac{a}{P})_d = (\tfrac{a}{P})_{q-1}^{\frac{q-1}{d}}.$$

Das heißt, des genügt das Potenzrestsymbol zur $(q-1)$-ten Potenz zu betrachten [13, S. 24 f].

3.1.2 Eigenschaften

Nun werden die grundlegenden Eigenschaften des d-ten Potenzrestsymbols beschrieben. Setzt man für $d = 2$, so entspricht das Symbol dem Legendresymbol der elementaren Zahlentheorie [13, S. 24]. Hierbei gibt das Legendresymbol an, ob eine Zahl ein quadratischer Rest modulo einer Primzahl ist [3, S. 302].

Die Situation in $\mathbb{F}[T]$ ist etwas flexibler, da es sich um einen endlichen Körper handelt und damit die multiplikative Gruppe $\mathbb{F}[T]^* = \mathbb{F}^*$ eine zyklische Gruppe mit der Ordnung $q-1$ aufweist. Vergleicht man dazu die Einheitengruppe von $\mathbb{Z}$, bemerkt man, dass diese nur aus zwei Elementen besteht: $\mathbb{Z}^* = \{-1, +1\}$ [13, S. 24].
Letztlich ist noch ein weiterer Unterschied zum klassischen Legendresymbol anzumerken. In der elementaren Zahlentheorie ist das Symbol in $\mathbb{Z}$ mit den Werten $\{-1, 0, 1\}$ definiert. In $\mathbb{F}$ nimmt das Potenzrestsymbol Werte des endlichen Körpers $\mathbb{F}$ an [13, S. 24].

Proposition 3.1.1. *Das d-te Potenzrestsymbol besitzt die folgenden Eigenschaften:*

i) $(\frac{a}{P})_d = (\frac{b}{P})_d$, *wenn* $a \equiv b \bmod P$.

ii) $(\frac{ab}{P})_d = (\frac{a}{P})_d(\frac{b}{P})_d$.

iii) $(\frac{a}{P})_d = 1$ *genau dann, wenn die Gleichung* $X^d \equiv a \bmod P$ *lösbar ist.*

iv) Sei $\zeta \in \mathbb{F}^*$, *dessen Ordnung d teilt. Dann existiert ein* $a \in \mathbb{F}[T]$, *sodass* $(\frac{a}{P})_d = \zeta$.

[13, S. 24]

Beweis. Sei P ein irreduzibles Polynom und $\mathbb{F}$ ein endlicher Körper. Für den Beweis betrachten wir die Aussagen abschnittsweise:

i) Die erste Aussage folgt direkt aus der Definition. Das d-te Potenzrestsymbol ist nur abhängig von der Restklasse von a modulo P.

ii) Die Multiplikationseigenschaft folgt auch direkt aus der Definition. Essentiell ist hierbei der Fakt, dass, wenn zwei Konstanten kongruent modulo P sind, sofort die Gleichheit der Konstanten folgt.

iii) Die Eigenschaft, dass das Potenzrestsymbol genau dann den Wert 1 besitzt, wenn a als d-te Potenz einer anderen Zahl geschrieben werden kann, folgt wiederum aus der Definition und aus Proposition 2.6.13.

iv) Für die letzte Eigenschaft, die aussagt, dass jedes Element ζ, dessen Ordnung d teilt, als Wert des Potenzrestsymbols geschrieben werden kann, betrachten wir die Abbildung, die jedem Polynom $a \in \mathbb{F}[T]$ das d-te Potenzrestsymbol aus $\mathbb{F}^*$ zuweist. Das heißt, die Abbildung ist von $(\mathbb{F}[T]/P\mathbb{F}[T])^* \to \mathbb{F}^*$ und gegeben durch $a \to (a/P)_d$. Bei dieser Abbildung handelt es sich um einen Homomorphismus nach der zweiten Eigenschaft, dessen Kern die d-ten Potenzen in $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ sind, da nach der dritten Eigenschaft das Potenzrestsymbol dieser Elemente die 1 ist. Dies folgt auch aus der dritten Aussage. Da es sich bei $(\mathbb{F}[T]/P\mathbb{F}[T])^*$ um eine zyklische Gruppe der Ordnung $|P|-1$ handelt, ist die Ordnung des Kerns $(|P|-1)/d$. Das heißt, das Bild besteht aus allen Elementen in $\mathbb{F}^*$, deren Ordnung d teilt. Daraus folgt, dass das Bild von der Ordnung d ist.

[13, S. 24] □

Wenn das Potenzrestsymbol auf einer Konstante angewendet wird, stellt sich die Berechnung besonders simpel dar [13, S. 24].

Proposition 3.1.2. *Sei α eine Konstante in $\mathbb{F}$, dann gilt*

$$(\tfrac{\alpha}{P})_d = \alpha^{\frac{q-1}{d}degP} \text{ [13, S. 24].}$$

Beweis. Für den Beweis sei $deg(P) = \delta$. Dann gilt aufgrund der geometrischen Summe

$$(*) \qquad \frac{|P|-1}{d} = \frac{q^\delta - 1}{d} = (1 + q + q^2 ... + q^{\delta-1})\frac{q-1}{d}.$$

Im ersten Schritt wird als Produkt von Potenzen von α geschrieben.

$$\alpha^{\frac{|P-1|}{d}} = (\alpha^1 \cdot \alpha^q \cdot ... \cdot \alpha^{q^{\delta-1}})^{\frac{q-1}{d}}$$

Die Aussage folgt nun, da für alle Konstanten im endlichen Körper die folgende Eigenschaft gilt $\alpha^q = \alpha$:

$$(\alpha^1 \cdot \alpha^q \cdot ... \cdot \alpha^{q^{\delta-1}})^{\frac{q-1}{d}} = (\alpha \cdot \alpha \cdot ... \cdot \alpha)^{\frac{q-1}{d}} = (\alpha^\delta)^{\frac{q-1}{d}} = \alpha^{degP \cdot \frac{q-1}{d}}$$

[13, S. 24 f]. □

Bemerkung. Sollte d ein Teiler des Grads des Polynoms P sein, so ist die Konstante automatisch ein d-ter Potenzrest modulo P [13, S. 25].

3.2 Reziprozitätsgesetz

In weiterer Folge wird das Reziprozitätsgesetz formuliert:

Theorem 3.2.1. *(d-te Potenz Reziprozitätsgesetz) Es seien P und Q normierte irreduzible Polynome mit dem Grad δ und ν, dann gilt*

$$(\frac{Q}{P})_d = (-1)^{\frac{q-1}{d}\delta\nu}(\frac{P}{Q})_d \text{ [13, S. 25].}$$

Beweis. Für den Beweis definieren wir $(\frac{a}{P}) = (\frac{a}{P})_{q-1}$. Somit gilt nach der Definition des Potenzrestsybols $(\frac{a}{P})_d = (\frac{a}{P})^{\frac{q-1}{d}}$. Um das Theorem zu beweisen, ist zu zeigen, dass

$$(\frac{Q}{P}) = (-1)^{\delta\nu}(\frac{P}{Q}),$$

da das allgemeine Resultat folgt, wenn beide Seiten mit $\frac{q-1}{d}$ potenziert werden. Sei nun α eine Nullstelle von P und β eine Nullstelle von Q in $\overline{\mathbb{F}}$. Sei außerdem $\mathbb{F}'$ ein endlicher Körper, der den Körper $\mathbb{F}$ sowie α und β enthält. Aus der Theorie der endlichen Körper folgt:

$$P(T) = (T-\alpha)(T-\alpha^q)...(T-\alpha^{q^{\delta-1}})$$

und

$$(**) \qquad Q(T) = (T-\beta)(T-\beta^q)...(T-\beta^{q^{\nu-1}}).$$

Da $P(\alpha) = 0$, folgt durch Anwenden der q-ten Potenz $P(\alpha)^q = 0$. Die Frobenius Eigenschaft $P(\alpha)^q \equiv P(\alpha^q)$ gilt, weil $P \in \mathbb{F}[T]$.
Betrachtet man diese Eigenschaft nun für das Polynom $P(\alpha) = \sum a_i\alpha^i$, folgt

$$P(\alpha)^q = (\sum a_i\alpha^i)^q = \sum a_i^q(\alpha^q)^i.$$

Aufgrund dessen, dass die Koeffizienten a_i in $\mathbb{F}_q$ liegen, ist $a_i^q = a_i$ und damit gilt

$$P(\alpha)^q = P(\alpha^q).$$

Wir betrachten nun Kongruenzen im Ring $\mathbb{F}'[T]$. Zu beachten ist, dass wenn $f(T) \in \mathbb{F}'[T]$ gilt, dann ist $f(T) \equiv f(\alpha) \bmod (T-\alpha)$. Weiter folgt wegen $g(T)^q = g(T^q)$, dass das Potenzrestsymbol $(\frac{Q}{P}) = Q^{\frac{|P|-1}{q-1}}$ mit $d = q-1$ nach $(*)$ kongruent zu

$$Q(T)^{1+q+...+q^{\delta-1}} \equiv Q(T)Q(T^q)...Q(T^{q^{\delta-1}}) \equiv Q(\alpha)Q(\alpha^q)...Q(\alpha^{q^{\delta-1}}) \bmod (T-\alpha)$$

ist. Im letzten Schritt wird die Eigenschaft $f(T) \equiv f(\alpha) \bmod (T-\alpha)$ verwendet. Das bedeutet, dass in dieser Kongruenz $T \mapsto \alpha$ und $(T \mapsto \alpha^{q^i})$ eingesetzt werden kann.
Aufgrund der Symmetrieeigenschaft dieser Kongruenz gilt diese auch modulo $(T-\alpha^{q^i})$ für alle i. Damit folgt, dass die Kongruenz auch modulo P gilt. Das heißt:

$$(\frac{Q}{P}) \equiv Q(\alpha)Q(\alpha^q)....Q(\alpha^{q^{\delta-1}}) \bmod \text{P.}$$

Für jedes Q wird nun, wie bei $(**)$ beschrieben, eingesetzt - etwa für $Q(\alpha)$ schreiben wir $\prod_{i=0} \alpha - \beta^{qi}$ und so weiter. Wenn nun dieses Resultat mit der Gleichung, die zuvor beschrieben wurde, kombiniert wird, führt dies zu der folgenden Kongruenz:

$$(\tfrac{Q}{P}) \equiv \prod_{i=0}^{\delta-1} \prod_{j=0}^{\nu-1} (\alpha^{q^i} - \beta^{q^j}) \bmod P,$$

mit $(\frac{Q}{P}) \in \mathbb{F}$ und $\prod_{i=0}^{\delta-1} \prod_{j=0}^{\nu-1} (\alpha^{q^i} - \beta^{q^j}) \in \mathbb{F}'$, weil es die Nullstellen α und β enthält. Da beide Seiten der Kongruenz in $\mathbb{F}'$ liegen, müssen sie gleich sein. Das heißt $(\frac{Q}{P}) = \prod_{i=0}^{\delta-1} \prod_{j=0}^{\nu-1} (\alpha^{q^i} - \beta^{q^j})$. Folglich ist

$$(\tfrac{Q}{P}) = \prod_{i=0}^{\delta-1} \prod_{j=0}^{\nu-1} (\alpha^{q^i} - \beta^{q^j}) = (-1)^{\delta\nu} \prod_{j=0}^{\nu-1} \prod_{i=0}^{\delta-1} (\beta^{q^j} - \alpha^{q^i}) = (-1)^{\delta\nu} (\tfrac{P}{Q}).$$

Damit ist das d-te Potenz Reziprozitätsgesetz gezeigt [13, S. 25]. □

In weiterer Folge wird die Definition des d-ten Restsymbols auf den Fall erweitert, in dem das Primelement P durch ein beliebiges Nicht-Null-Element $b \in \mathbb{F}[T]$ ersetzt wird [13, S. 26].

Definition. Sei $b \in \mathbb{F}[T]$, $b \neq 0$ und $b = \beta Q_1^{f_1} Q_2^{f_2} ... Q_s^{f_s}$ sei die Primfaktorzerlegung von b. Ist $a \in \mathbb{F}[T]$, dann definieren wir das erweiterte d-te Potenzrestsymbol folgendermaßen:

$$(\tfrac{a}{b})_d = \prod_{j=1}^{s} (\tfrac{a}{Q_j})_d^{f_j}.$$

[13, S. 26]

Nach dieser Definition ist das Potenzrestsymbol lediglich abhängig von dem von b erzeugten Hauptideal $b\mathbb{F}[T]$. Das heißt, es ist nicht von β abhängig. Das erweiterte d-te Potenzrestsymbol ist im Fall $d = 2$ das Analogon des Jacobi-Symbols [13, S. 26].
Die Eigenschaften für das erweiterte d-te Potenzrestsymbol können von den Eigenschaften des d-ten Potenzrestsymbols übertragen werden:

Proposition 3.2.2. *Für das Symbol $(\frac{a}{b})_d$ gelten die folgenden Eigenschaften:*

i) *Wenn $a_1 \equiv a_2$ mod b, dann $(\frac{a_1}{b})_d = (\frac{a_2}{b})_d$.*

ii) $(\frac{a_1 a_2}{b})_d = (\frac{a_1}{b})_d (\frac{a_2}{b})_d$.

iii) $(\frac{a}{b_1 b_2})_d = (\frac{a}{b_1})_d (\frac{a}{b_2})_d$.

iv) *Das Restsymbol $(\frac{a}{b})_d \neq 0$ genau dann, wenn a und b relativ prim zueinander sind.*

v) *Wenn die Kongruenz $x^d \equiv a$ mod b lösbar ist, dann ist $(\frac{a}{b})_d = 1$. Dabei sei $ggT(a, b) = 1$ vorausgesetzt.*

[13, S. 26]

Beweis. Die Eigenschaften i) bis iv) folgen aus der Definition und den Eigenschaften des d-ten Potenzrestsymbols. Um die letzte Eigenschaft zu zeigen, sei $c^d \equiv a \bmod b$. Wird die multiplikative Eigenschaft auf c^d angewendet, folgt:

$$(\tfrac{a}{b})_d = (\tfrac{c^d}{b})_d = 1$$

Da eine d-te Potenz stets ein d-Potenzrest ist, gilt $(\frac{c}{d})_d^d = 1$. Für den Nachweis der Implikation ($\Leftarrow$) betrachten wir Proposition 3.1.3 iii). Damit folgt die Aussage [13, S. 26]. □

Bemerkung. Die Umkehrung der fünften Eigenschaft der Proposition 3.2.2 ist nicht im Allgemeinen gültig. Dafür wird angenommen, dass Q ein normiertes, irreduzibles Polynom ist, das a nicht teilt. Weiter sei $b = Q^d$. Nach der dritten Eigenschaft gilt

$$(\tfrac{a}{b})_d = (\tfrac{a}{Q^d})_d = (\tfrac{a}{Q})_d^d = (\tfrac{a^d}{Q})_d = 1.$$

Allerdings ist nicht jedes Element von $(\mathbb{F}[T]/b\mathbb{F}[T])^* = (\mathbb{F}[T]/Q^d\mathbb{F}[T])^*$ eine d-te Potenz [13, S. 26].

Es ist von Vorteil das Reziprozitätsgesetz in allgemeiner Form zu formulieren, sodass es für beliebige Elemente von $\mathbb{F}[T]$ gilt, die nicht zwingend normiert oder irreduzibel sein müssen. Für $f \in \mathbb{F}[T]$ und $f \neq 0$ sei in weiterer Folge der führende Koeffizient von f versehen mit der $\frac{q-1}{d}$ Potenz, das heißt, wir definieren

$$sgn(a)_d := a^{\frac{(q-1)}{d}} \text{ [13, S. 26].}$$

Theorem 3.2.3. *(Allgemeines Reziprozitätsgesetz) Seien $a, b \in \mathbb{F}[T]$ zueinander relativ prim und Nicht-Null-Elemente und $sgn_d(a) = sgn(a)^{\frac{q-1}{d}}$. Dann gilt*

$$(\tfrac{a}{b})_d(\tfrac{b}{a})_d^{-1} = (-1)^{\frac{q-1}{d}deg(a)deg(b)} sgn_d(a)^{deg(b)} sgn_d(b)^{-deg(a)}$$

[13, S. 27].

Beweis. Sind a und b normiert und irreduzibel, so zeigt der Beweis des Theorems 3.2.1 die Aussage. Im Allgemeinen wird der Beweis durchgeführt, indem man sich auf Proposition 3.1.2 - für den führenden Koeffizienten d.h. für das Signum von a und b - und Theorem 3.2.1, das Reziprozitätsgesetz für normierte Teiler von a und b, sowie die Definitionen bezieht. Weiters wird der Fakt verwendet, dass der Grad des Produkts von zwei Polynomen mit der Summe der Grade beider Polynome übereinstimmt [13, S. 27]. □

3.3 Beispiel

In diesem Kapitel wird ein Beispiel zur Bestimmung des Potenzrestsymbols $(\frac{Q}{P})_d$ berechnet. Gegeben sind dafür die Polynome $P, Q \in \mathbb{F}_7[T]$ mit

$$Q(x) = x^5 + 1 \text{ und } P(x) = x^5 + 5x^4 + 2x^2 + 6x + 3.$$

Für d setzen wir $d = 3$ und untersuchen, ob das Polynom Q eine dritte Potenz modulo P ist, also ob die folgende Kongruenz erfüllt ist:

$$X^d - Q \equiv 0 \bmod P \iff X^d \equiv Q \bmod P.$$

Ist diese Kongruenz erfüllt, so gilt für das Potenzrestsymbol $(\frac{Q}{P})_d = 1$ (siehe Proposition 3.2.2 (v)).
Wir wollen im Folgenden $(\frac{Q}{P})_d$ berechnen. Dazu wenden wir das allgemeine Reziprozitätsgesetz, das zuvor im Theorem 3.2.3 gezeigt wurde, an:

$$(\tfrac{a}{b})_d = (-1)^{\frac{q-1}{d} deg(a) deg(b)} sgn_d(a)^{deg(b)} sgn_d(b)^{-deg(a)} (\tfrac{b}{a})_d \ .$$

Dabei war $sgn_d(a)$ der führende Koeffizient von a zur Potenz $\frac{q-1}{d}$ [13, S. 26 f].
Neben dem allgemeinen Reziprozitätsgesetz verwenden wir die folgende Eigenschaft, die in Proposition 3.2.2 i) beschrieben wurde:

$$(\tfrac{Q}{P})_d \equiv (\tfrac{Q' = Q mod P}{P})_d$$

(siehe Proposition 3.2.2 (i)). Um $Q' = Q \bmod P$ zu berechnen, wird die Polynomdivision angewendet:

$$\begin{array}{r} (\ x^5 + 1\ ) \\ \underline{-\,x^5 - 5x^4 - 2x^2 - 6x - 3\ } \\ -\,5x^4 - 2x^2 - 6x - 2 \end{array} \div \left(x^5 + 5x^4 + 2x^2 + 6x + 3\right) = 1 + \frac{-5x^4 - 2x^2 - 6x - 2}{x^5 + 5x^4 + 2x^2 + 6x + 3}$$

Der verbleibenden Rest ist demnach $-5x^4 - 2x^2 - 6x - 2$. Da die Division in $\mathbb{F}_7$ berechnet wird, ist jeder Koeffizient ein Element aus $\mathbb{F}_7$. Jedes Element hat daher einen Vertreter in der Menge $\{0, 1, 2, 3, 4, 5, 6\}$. Die Koeffizienten werden nun auf ihren Vertreter in $\mathbb{F}_7$ reduziert, um diese für die weitere Berechnung klein zu halten:

$$-5x^4 - 2x^2 - 6x - 2 \equiv 2x^4 + 5x^2 + x + 5 \bmod 7$$

Wir setzen nun

$$Q' = 2x^4 + 5x^2 + x + 5.$$

Folglich ist:

$$(\tfrac{Q}{P})_3 = (\tfrac{Q'}{P})_3$$

In weiterer Folge wird das Potenzrestsymbol unter Anwendung des allgemeinen Reziprozitätsgesetzes „umgedreht“:

$$(\tfrac{Q'}{P})_3 = (-1)^{\frac{7-1}{3}\cdot 4\cdot 5}\cdot sgn_3(Q')^{deg(P)}\cdot sgn_3(P)^{-deg(Q')}(\tfrac{P}{Q'})_3 = 1\cdot 2^{2\cdot 5}\cdot 1^{2\cdot(-4)}(\tfrac{P}{Q'})_3 = 2\cdot(\tfrac{P}{Q'})_3$$

Das heißt:

$$(\tfrac{Q'}{P})_3 = (\tfrac{2x^4+5x^2+x+5}{x^5+5x^4+2x^2+6x+3})_3 = 2\cdot(\tfrac{x^5+5x^4+2x^2+6x+3}{2x^4+5x^2+x+5})_3 = 2\cdot(\tfrac{P}{Q'})_3$$

Nun berechnen wir $P' = P \bmod Q'$ wiederum mittels Polynomdivision:

$$\begin{array}{rrrrr}
\big(& x^5 + 5x^4 & + 2x^2 & + 6x & + 3\big) \div \big(2x^4 + 5x^2 + x + 5\big) = \frac{1}{2}x + \frac{5}{2} + \frac{-\frac{5}{2}x^3 - 11x^2 + x - \frac{19}{2}}{2x^4 + 5x^2 + x + 5} \\
 & -x^5 & -\frac{5}{2}x^3 & -\frac{1}{2}x^2 - \frac{5}{2}x & \\
\hline
 & 5x^4 & -\frac{5}{2}x^3 & +\frac{3}{2}x^2 + \frac{7}{2}x & +3 \\
 & -5x^4 & & -\frac{25}{2}x^2 - \frac{5}{2}x - \frac{25}{2} & \\
\hline
 & & -\frac{5}{2}x^3 - 11x^2 & +x - \frac{19}{2} &
\end{array}$$

Der verbleibende Rest der Division ist $-\frac{5}{2}x^3 - 11x^2 + x - \frac{19}{2}$. Die Koeffizienten werden modulo 7 gerechnet und damit reduziert.

$$\begin{aligned}
-\tfrac{5}{2} &\equiv 1 \bmod 7 \\
-11 &\equiv 3 \bmod 7 \\
-\tfrac{19}{2} &\equiv 1 \bmod 7
\end{aligned}$$

Damit erhält man für P' das folgende Polynom:

$$P' = x^3 + 3x^2 + x + 1$$

Nun wird statt P das Polynom P' eingesetzt:

$$(\tfrac{Q}{P})_3 = (\tfrac{Q'}{P})_3 = 2\cdot(\tfrac{P}{Q'})_3 = 2\cdot(\tfrac{P'}{Q'})_3$$

Erneut wird das allgemeine Reziprozitätsgesetz angewendet:

$$2\cdot(\tfrac{P'}{Q'})_3 = 2\cdot 1\cdot 1^{2\cdot 4}\cdot 2^{2\cdot(-3)}(\tfrac{Q'}{P'})_3 = \tfrac{1}{32}(\tfrac{Q'}{P'})_3 = 2\cdot(\tfrac{Q'}{P'})_3$$

Daran anschließend berechnen wir $Q'' = Q' \bmod P'$.

$$\begin{array}{rrrrr}
\big(& 2x^4 & + 5x^2 & + x & + 5\big) \div \big(x^3 + 3x^2 + x + 1\big) = 2x - 6 + \frac{21x^2 + 5x + 11}{x^3 + 3x^2 + x + 1} \\
 & -2x^4 - 6x^3 & -2x^2 - 2x & & \\
\hline
 & -6x^3 & +3x^2 & -x & +5 \\
 & 6x^3 + 18x^2 & +6x & & +6 \\
\hline
 & & 21x^2 + 5x + 11 & &
\end{array}$$

Nachdem die Koeffizienten des Rests abermals reduziert wurden, erhalten wir für Q'' das folgende Polynom:

$$Q'' = 0x^2 + 5x + 4 = 5x + 4$$

Wiederum setzen wir dieses Polynom ein und wenden das Reziprozitätsgesetz an:

$$2 \cdot (\tfrac{Q'}{P'})_3 = 2 \cdot (\tfrac{Q''}{P'})_3 = 2 \cdot 1 \cdot 5^{2\cdot 3} \cdot 1^{2\cdot(-1)} (\tfrac{P'}{Q''})_3 = 2 \cdot (\tfrac{P'}{Q''})_3$$

Anschließend wird ein weiteres Mal P' auf $P'' = P' \bmod Q''$ reduziert:

$$\begin{array}{rrrr|l}
\multicolumn{4}{l|}{\big(\quad x^3 \quad + 3x^2 \quad + x \quad + 1\big) \div \big(5x + 4\big) = \tfrac{1}{5}x^2 + \tfrac{11}{25}x - \tfrac{19}{125} + \dfrac{\frac{201}{125}}{5x+4}} \\
-x^3 & -\tfrac{4}{5}x^2 & & & \\
\hline
 & \tfrac{11}{5}x^2 & + x & & \\
 & -\tfrac{11}{5}x^2 & -\tfrac{44}{25}x & & \\
\hline
 & & -\tfrac{19}{25}x & + 1 & \\
 & & \tfrac{19}{25}x & + \tfrac{76}{125} & \\
\hline
 & & & \tfrac{201}{125} &
\end{array}$$

Weil der verbleibende Rest $\frac{201}{125} \equiv 2 \bmod 7$ ist, setzen wir:

$$P'' = 2$$

mit

$$2 \cdot (\tfrac{P'}{Q''})_3 = 2 \cdot (\tfrac{P''}{Q''})_3.$$

Da mit P'' nun eine Konstante gefunden ist, kommt nun Proposition 3.1.2 zur Anwendung. Demnach gilt:

$$2 \cdot (\tfrac{P''}{Q''})_3 = 2 \cdot (\tfrac{2}{5x+4})_3 = 2 \cdot 2^{2\cdot 1} = 2 \cdot 4 = 8 = 1 \bmod 7$$

Aufgrund der Irreduzibilität von P folgt aus $(\frac{Q}{P})_3 = 1$ schließlich, dass Q eine 3. Potenz modulo P ist. Diese Aussage folgt aus Proposition 3.1.1 (iii).
Zusammenfassend wurde in diesem Beispiel die folgende Rechnung durchgeführt:

$$(\tfrac{Q}{P})_3 = (\tfrac{Q'}{P})_3 = 2 \cdot (\tfrac{P}{Q'})_3 = 2 \cdot (\tfrac{P'}{Q'})_3 = 2 \cdot (\tfrac{Q'}{P'})_3 = 2 \cdot (\tfrac{Q''}{P'})_3 = 2 \cdot (\tfrac{P'}{Q''})_3 = 2 \cdot (\tfrac{P''}{Q''})_3 = 1.$$

Bemerkung. (Konstruktion des Beispiels)
Im Anschluss wird die Konstruktion des zuvor berechneten Beispiels skizziert.
Wir suchen ein Polynom Q und ein irreduzibles Polynom P, sodass Q eine d-Potenz modulo P ist, das heißt $(\frac{Q}{P})_d = 1$.
Sei $\mathbb{F}' = \mathbb{F}_q$ und $d|q-1$. Für das Beispiel wählen wir $q = 7$ und $d = 3$, da $3|(7-1)$.
Nun wählen wir zwei Polynome P und $Q \in \mathbb{F}[T]$.
Das Polynom Q ist vom fünften Grad.

$$Q(x) = x^5 + 1 \in \mathbb{F}_7[T]$$

Wir wählen weiter ein Polynom $X \in \mathbb{F}[T]$ vom Grad 6.

$$X(x) = x^6 + 1$$

In weiterer Folge bilden wir $X^d - Q$:

$$X^3 - Q = (x^6 + 1)^3 - (x^5 + 1) = x^{18} + 3x^{12} + 3x^6 - x^5$$

Wir faktorisieren $X^d - Q$ in $\mathbb{F}[T]$: Zunächst berechnen wir in der folgenden Kongruenz positive Koeffizienten:

$$x^{18} + 3x^{12} + 3x^6 - x^5 \equiv x^{18} + 3x^{12} + 3x^6 + 6x^5 \bmod 7$$

Mithilfe der Anwendung der Primfaktorisierung nach Cantor-Zassenhaus schreiben wir das Polynom in einzelnen Faktoren:

$$x^{18}+3x^{12}+3x^6+6x^5 = x^5(x^5+5x^4+2x^2+6x+3)(x^8+2x^7+4x^6+6x^5+2x^4+2x^3+4x+2)$$

[12]
Als Nächstes wählen wir einen irreduziblen Teiler P von $X^d - Q$ von Grad 5

$$P(x) = x^5 + 5x^4 + 2x^2 + 6x + 3$$

Damit wurden zwei Polynome P und Q gefunden, für die gilt, dass das Polynom Q dritte Potenz von X modulo P ist. Also

$$Q = (x^6 + 1)^3 \bmod P.$$

Insbesondere wissen wir daher, dass $(\frac{Q}{P})_3 = 1$.

3.4 Vergleich von $\mathbb{Z}$ und $\mathbb{F}_q[T]$

In diesem abschließenden Kapitel werden $\mathbb{F}[T]$ und $\mathbb{Z}$ verglichen. Wie bereits erwähnt, handelt es sich bei beiden um Hauptidealringe und Euklidische Ringe [13, S. 1].

$\mathbb{Q}$	$F_q(T)$ mit $q = p^e$
$\mathbb{Z}$	$F_q[T]$
$\mathbb{Z}^* = \{\pm 1\}$	$F_q[T]^* = F_q^* =$ konstante Polynome $\neq 0$
sgn	$sgn(f) := \alpha_n$ führende Koeffizient von $f = \sum_{i=0}^{n} \alpha_i T^i$
Absolutbetrag $\lvert n \rvert$	$\lvert f \rvert := q^{deg(f)}$
Primelement p	irreduzibles Polynom P
$\mathbb{Z}/p^e\mathbb{Z}$	$\mathbb{F}_q[T]/p^e\mathbb{F}_q[T]$
$(\mathbb{Z}/p^e\mathbb{Z})^*$	$(\mathbb{F}_q[T]/p^e\mathbb{F}_q[T])^*$
Euler $\varphi(m) = \lvert(\mathbb{Z}/m\mathbb{Z})^*\rvert$	$\varphi(f) = \lvert(\mathbb{F}_q[T]/f\mathbb{F}_q[T])^*\rvert$
$(\mathbb{Z}/p^e\mathbb{Z})^*$ ist endlich erzeugt für p prim und sogar zyklisch für $p \neq 2$	Anzahl der Erzeuger von $(\mathbb{F}_q[T]/P^e\mathbb{F}_q[T])^* \to \infty$ für $e \to \infty$ (P irreduzibel)
Legendre-Symbol $(\frac{a}{p})$ für $p \nmid a$, p prim	$(\frac{a}{P})_d$, P irreduzibel und $P \nmid a$
Jacobi-Symbol $(\frac{a}{b})$ mit $ggT(a,b) = 1$	d-tes Potenzrestsymbol $(\frac{a}{b})_d$ mit $d \mid q-1$ und $ggT(a,b) = 1$
Quadratisches Reziprozitätsgesetz für $(\frac{a}{b})$	Höheres Reziprozitätsgesetz für $(\frac{a}{b})_d$ mit $d \mid q-1 \Longrightarrow$ quadratisches Reziprozitätsgesetz für alle $p \neq 2$
1. Ergänzungssatz: $(\frac{-1}{a})$	$(\frac{a}{P})_d$ und a ist ein konstantes Polynom
2. Ergänzungssatz $(\frac{2}{a})$	nicht nötig, da das Reziprozitätsgesetz für alle Primpolynome gilt
-	Koeffizientenerweiterung $\bar{\mathbb{F}}_q[T]$
-	Frobeniusmorphismus $a \mapsto a^q$
-	Derivation $\frac{d}{dx}$

Die Tabelle liefert einen groben Überblick zur Gegenüberstellung der Ringe $\mathbb{Z}$ und $\mathbb{F}[T]$: Etwa entsprechen den Elementen aus dem Ring der ganzen Zahlen im Polynomring die Polynome mit Koeffizienten aus $\mathbb{F}_q$ [6, S. 73]. Betrachtet man jeweils die Einheitengruppe

dieser beiden Ringe, so besteht diese in $\mathbb{Z}$ aus den Elementen $\{-1, +1\}$, während die Einheitengruppe von $\mathbb{F}_q$ aus den konstanten Nicht-Null-Polynomen besteht [4, 6, S. 29, S. 81]. Das Analogon des Signums *sgn* (bzw. des Vorzeichens) einer Zahl aus dem Ring der ganzen Zahlen entspricht in $\mathbb{F}_q[T]$ dem führenden Koeffizienten α_n eines Polynoms [13, S. 1]. Genauso weist der Betrag $|n|$ im Ring der ganzen Zahlen ein Äquivalent in $\mathbb{F}_q[T]$ auf: Hierbei handelt es sich um $q^{deg(f)}$, wobei $deg(f)$ der Grad des Polynoms f ist. Der Betrag einer ganzen Zahl respektive der Grad eines Polynoms sind Instrumente, um das Größenmaß von Elementen anzugeben. Außerdem sind sie wichtige Konzepte, die die Anwendung des Divisionsalgorithmus in beiden Ringen ermöglichen [6, S. 74].
Des Weiteren stellen irreduzible Polynome in $\mathbb{F}_q[T]$ das Pendant zu Primzahlen aus $\mathbb{Z}$ dar. Das Gegenstück des Restklassenrings $\mathbb{Z}/p^e\mathbb{Z}$ ist der Polynomring modulo eines irreduziblen Polynoms $\mathbb{F}_q[T]/P^e\mathbb{F}_q[T]$. Diese beiden Ringe sind endlich [5, S. 1].
Die multiplikative Gruppe des zuvor genannten Restklassenrings $(\mathbb{Z}/p^e\mathbb{Z})^*$ enthält alle Elemente, die teilerfremd zu p^e sind. Dem entgegen steht $(\mathbb{F}_q[T]/P^e\mathbb{F}_q[T])^*$ die Gruppe der Polynome modulo P^e, die zu P teilerfremd sind. Wie in dieser Arbeit beschrieben, ist die Anzahl der Einheiten der Ringe $(\mathbb{Z}/p^e\mathbb{Z})^*$ und $(\mathbb{F}_q[T]/P^e\mathbb{F}_q[T])^*$ endlich [5, S. 1]. Die Größen dieser endlichen Gruppen definiert die Euler'schen φ-Funktion [4, S. 183]. Die Gruppen unterscheiden sich allerdings in ihrer Struktur: Während im Zahlenbereich $(\mathbb{Z}/p^e\mathbb{Z})^*$ für $p \neq 2$ zyklisch ist, trifft dies auf $(\mathbb{F}_q[T]/P^e\mathbb{F}_q[T])^*$ für $e > 1$ dagegen nicht zu. Die Anzahl der Erzeuger von $(\mathbb{F}_q[T]/P^e\mathbb{F}_q[T])^*$ nimmt mit wachsendem e zu und strebt für $e \to \infty$ gegen Unendlich [13, S. 4].
Nennenswert ist auch, dass bekannte Begriffe aus der Zahlentheorie, wie etwa das Legendre-Symbol $(\frac{a}{p})$ oder Jacobi-Symbol $(\frac{a}{b})$, die zur Beschreibung von quadratischen Resten dienen, mit $(\frac{a}{b})_d$ eine Entsprechung in $\mathbb{F}_q[T]$ haben [13, S. 24]. Wie in dieser Arbeit dargestellt, gibt es zum Reziprozitätsgesetz in $\mathbb{Z}$ eine Analogie im Kontext der Polynome für höhere d-te Potenzreste modulo einem Polynom in $\mathbb{F}_q[T]$. Der erste Ergänzungssatz gibt spezifische Aussagen darüber, unter welchen Umständen -1 ein quadratischer Rest modulo a ist [3, S. 307]. Überträgt man diesen Satz auf den Polynomring, so liefert der Ergänzungssatz Aussagen, ob konstante Polynome Reste modulo P d-te Potenzen sind [13, S. 25]. Der 2. Ergänzungssatz hat keine Entsprechung für Polynome, denn das Reziprozitätsgesetz in $\mathbb{F}_q[T]$ gilt im Unterschied zum quadratischen Reziprozitätsgesetz in $\mathbb{Z}$ für alle irreduziblen Polynome. Das heißt, man muss kein irreduzibles Element, wie die 2 ausschließen.
Ferner treten im Polynomring drei wichtige Werkzeuge auf, die im Ring der ganzen Zahlen keine Analogie haben: Die Koeffizientenerweiterung $\overline{\mathbb{F}}_q[T]$ von $\mathbb{F}_q[T]$ und der Frobeniusmorphismus in $\mathbb{F}_q[T]$, der Elemente auf die q-te Potenz hebt, sind zentral beim Beweis des Reziprozitätsgesetzes für Polynome. Darüber hinaus gibt es für Polynome die Derivation $\frac{d}{dx}$ [4, S. 60]. In dieser Arbeit ist sie nicht relevant - jedoch ist die Ableitung ein wichtiges Instrument in anderen Thematiken.

4 Fazit

Um die in der Einleitung formulierte Fragestellung zu beantworten, nämlich ob ein Analogon des Quadratischen Reziprozitätsgesetz im Polynomring $\mathbb{F}_q[T]$ über einem endlichen Körper existiert und ob sich der Beweis übertragen lässt, ist Folgendes festzuhalten:

i) Im Vergleich zeigt sich, dass beide Ringe - sowohl $\mathbb{Z}$ und $\mathbb{F}_q[T]$ - Euklidische Ringe, Hauptidealringe und faktorielle Ringe sind. Dies bildet die entsprechende algebraische Grundlage für das Reziprozitätsgesetz in $\mathbb{Z}$. Aus diesem Grund stellt sich die Frage, ob es ein Analogon in $\mathbb{F}_q[T]$ gibt. Das Quadratische Reziprozitätsgesetz, das in $\mathbb{Z}$ seine Anwendung findet, kann tatsächlich auf den Polynombereich $\mathbb{F}_q[T]$ für höhere d-te Potenzreste modulo eines Polynoms P, wobei d ein Teiler von $(q-1)$ ist, übertragen werden.

ii) Trotz der vielen Gemeinsamkeiten der beiden Ringe gibt es spezifische Unterschiede, die die Komplexität des Beweises des Reziprozitätsgesetzes in $\mathbb{Z}$ im Vergleich zum Beweis für $\mathbb{F}_q[T]$ bedingen:

   Entscheidend für den Beweis im Polynomring $\mathbb{F}_q[T]$ ist die Existenz der Koeffizientenerweiterung $\overline{\mathbb{F}}_q[T]$ von $\mathbb{F}_q[T]$, in der jedes Polynom vollständig in Linearfaktoren zerfällt. Außerdem ist die Galoisgruppe $\overline{\mathbb{F}}_q(T)/\mathbb{F}_q(T)$ sehr einfach strukturiert, da sie vom Frobeniusmorphismus erzeugt wird [10, S.85]. Damit ist eine einfache Bestimmung der Faktorisierung eines Polynoms möglich. Diese Eigenschaft wurde in der Gleichung $(**)$ für den Beweis des Reziprozitätsgesetzes in $\mathbb{F}_q[T]$ zentral angewendet.

   Der Beweis lässt sich nicht auf $\mathbb{Z}$ übertragen, da für $\mathbb{Z}$ kein Analogon zur Koeffizientenerweiterung existiert und die Galoisgruppe von $\overline{\mathbb{Q}}/\mathbb{Q}$ komplizierter aufgebaut ist.

iii) Diese Arbeit zeigt, dass sich ein klassisches zahlentheoretisches Prinzip, wie das Reziprozitätsgesetz, auf den Polynomring $\mathbb{F}_q[T]$ übertragen lässt, aber die relativ einfache Beweisführung auf $\mathbb{Z}$ nicht übertragbar ist.

Literaturverzeichnis

[1] Emil Artin. Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Mathematische Zeitschrift*, 19:153–246, 1924.

[2] Sheldon Axler. *Linear Algebra Done Right*. Undergraduate Texts in Mathematics. Springer International Publishing : Imprint: Springer, 4. edition, 2024.

[3] Janko Böhm. *Grundlagen der Algebra und Zahlentheorie*. Springer-Lehrbuch. Springer Berlin Heidelberg, 2016.

[4] Siegfried Bosch. *Algebra*. Springer-Lehrbuch. Springer-Verlag Berlin Heidelberg, Berlin, Heidelberg, 2009.

[5] Keith Conrad. Carlitz extensions. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/carlitz.pdf`, 2009. [Online; aufgerufen am 28. April 2025].

[6] David R. Finston and Patrick J. Morandi. *Abstract Algebra: Structure and Application*. Springer Undergraduate Texts in Mathematics and Technology. Springer International Publishing, 2014.

[7] Gerd Fischer. *Lineare Algebra : Eine Einführung für Studienanfänger*. Vieweg+Teubner Verlag / GWV Fachverlage GmbH, Wiesbaden, Wiesbaden, 17., aktualisierte Auflage edition, 2010.

[8] Nathan Jacobson. *Basic algebra. 1 (1996)*. Freeman, San Francisco, Calif., 2. ed., 9. print. edition, 1996.

[9] Jens Carsten Jantzen and Joachim Schwermer. *Algebra*. Springer-Lehrbuch. Springer, Berlin, Heidelberg :, 2nd ed. 2014. edition, 2014.

[10] Joachim Mahnkopf. Algebra 2. Vorlesungsskript, Universität Wien, 2023.

[11] Sidney A. Morris, Arthur Jones, and Kenneth R. Pearson. *Abstract Algebra and Famous Impossibilities: Squaring the Circle, Doubling the Cube, Trisecting an Angle, and Solving Quintic Equations*. Undergraduate Texts in Mathematics. Springer International Publishing, 2022.

[12] o.V. Polynomfaktorisierung in einem endlichen Körper nach Cantor-Zassenhaus. `https://de.planetcalc.com/8372/`, 2021. [Online; aufgerufen am 22. Februar 2025].

[13] Michael Rosen. *Number Theory in Function Fields*. Graduate Texts in Mathematics. Springer New York, 2013.

[14] Friedrich Karl Schmidt. Zur Zahlentheorie in Körpern von der Charakteristik p (Vorläufige Mitteilung). *Sitzungsberichte der Physikalisch-Medizinischen Sozietät zu Erlangen*, 58–59:159–172, 1926–1927.

[15] Friedrich Schwarz. *Einführung in die elementare Zahlentheorie*. MuPAD lectures. Teubner, Stuttgart [u.a.], 1998.