

Ralf Gerkmann

Mathematisches Institut

Ludwig-Maximilians-Universität München

Vorlesung im Wintersemester 2022-23

Zahlentheorie

Zusammenfassung

Gegenstand dieser Vorlesung ist die Ringtheorie, mit einem Schwerpunkt auf Anwendungen in der Zahlentheorie. Wir beginnen mit der Definition der Ringe, der Ringhomomorphismen, der Teil- und Erweiterungsringe, samt ihrer Beschreibung durch Erzeugendensysteme. Um genügend Beispielmateriale für die weiteren Kapitel zur Verfügung zu haben, behandeln wir anschließend die Konstruktion von Ringweiterungen, aus der die Quotientenkörper und die Polynomringe hervorgehen. Weitere wichtige Beispiele für Ringe liefert uns das Kapitel über Ideale und Faktorringe.

Ein Teil der Vorlesung widmet sich der Klassifizierung der Ringe, wozu wir (in aufsteigender Allgemeinheit) die euklidischen Ringe, die Hauptidealringe und die faktoriellen Ringe betrachten. Eine besonders wichtige Eigenschaft dieser Ringe ist dabei die Eindeutigkeit der Primfaktorzerlegung. Diese spielt auch bei der Faktorisierung von Polynomen eine zentrale Rolle. Als zahlentheoretische Anwendungen behandeln wir verschiedene Aspekte der Kongruenzrechnung, zum Beispiel den Chinesischen Restsatz, die Struktur der primen Restklassengruppen und das Quadratische Reziprozitätsgesetz.

Inhaltsverzeichnis

§ 1. Die Kategorie der Ringe	3
§ 2. Teilringe und Erzeugendensysteme	8
§ 3. Quotientenkörper und Polynomringe	17
§ 4. Euklidische Ringe	27
§ 5. Ideale	34
§ 6. Faktorringe und Restklassenringe	41
§ 7. Der Chinesische Restsatz	48
§ 8. Die Struktur der primen Restklassengruppen	52
§ 9. Hauptidealringe und die Teilbarkeitsrelation	57
§ 10. Faktorielle Ringe	66
§ 11. Irreduzibilitätskriterien und Gauß'sches Lemma	72
§ 12. Kreisteilungspolynome	78
Literaturverzeichnis	82

§ 1. Die Kategorie der Ringe

Zusammenfassung. Ein Ring ist eine algebraische Struktur, in der die arithmetischen Operationen Addition, Subtraktion und Multiplikation zur Verfügung stehen, im Allgemeinen aber keine Division. Eine präzise Definition der Ringe basiert auf den Begriffen der Gruppe und des Monoids, die wir aus der Algebravorlesung kennen. Ein wichtiges Standardbeispiel ist der Ring \mathbb{Z} der ganzen Zahlen, ebenso die Zahlbereiche \mathbb{Q} , \mathbb{R} und \mathbb{C} . Ein etwas ungewohnteres Beispiel ist $\mathbb{Z} \times \mathbb{Z}$ mit der komponentenweisen Addition und Multiplikation.

Wichtige spezielle Elementen in Ringen sind *Einheiten* und *Nullteiler*. Die Einheiten eines Rings sind die Elemente, die in R bezüglich der Multiplikation invertierbar sind, in \mathbb{Z} zum Beispiel die Elemente ± 1 . Nullteiler kommen abgesehen von 0 selbst in den gewohnten Zahlbereichen (s.o.) nicht vor, in „exotischeren“ Ringen wie $\mathbb{Z} \times \mathbb{Z}$ aber schon. Die *Charakteristik* eines Rings beschreibt das Phänomen, dass in einem allgemeinen Ring R durchaus $1_R + \dots + 1_R = 0_R$ gelten kann, das man aber in den gewohnten Zahlbereichen ebenfalls nicht antrifft.

Wichtige Grundbegriffe

- Ringe und Ringhomomorphismen
- Einheiten und Nullteiler
- Nullringe, Integritätsbereiche, Körper
- Charakteristik eines Rings

Zentrale Sätze

- Für jeden Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \rightarrow R$.

Definition 1.1 Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+: R \times R \rightarrow R$ und $\cdot: R \times R \rightarrow R$, genannt **Addition** und **Multiplikation**, so dass die folgenden Bedingungen erfüllt sind:

- Das Paar $(R, +)$ ist eine abelsche Gruppe.
- Das Paar (R, \cdot) ist ein kommutatives Monoid.
- Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Das Neutralelement der Gruppe $(R, +)$ bezeichnet man mit 0_R und nennt es das **Nullelement** des Rings. Ist $a \in R$, dann schreibt man $-a$ für das Inverse von a in der Gruppe $(R, +)$ und nennt es das **Negative** von a . Das Neutralelement von (R, \cdot) wird **Einselement** von R genannt und mit 1_R bezeichnet. An Stelle von $a + (-b)$ schreiben wir auch kürzer $a - b$. Die Rechenregeln für Inverse aus der Algebra-Vorlesung sind natürlich auch in der Gruppe $(R, +)$ gültig, es gilt also $-(a + b) = (-a) + (-b)$ und $-(-a) = a$ für alle $a, b \in R$. Darüber hinaus gilt auch

$$0_R \cdot a = 0_R \quad , \quad (-a)b = a(-b) = -(ab) \quad \text{und} \quad (-a)(-b) = ab \quad \text{für alle} \quad a, b \in R.$$

Ähnliche Rechenregeln wurden in der Linearen Algebra für die Elemente eines Vektorraums bewiesen. Die erste Gleichung erhält man, indem man in der Gleichung $0_R \cdot a = (0_R + 0_R) \cdot a = 0_R \cdot a + 0_R \cdot a$ auf beiden Seiten das Element

$-(0_R \cdot a)$ addiert. Die Gleichung $(-a)b + ab = ((-a) + a)b = 0_R \cdot b = 0_R$ zeigt, dass $(-a)b$ das additive Inverse von ab ist, also $(-a)b = -(ab)$ gilt, und genauso zeigt man $a(-b) = -(ab)$. Die letzte Gleichung kann schließlich durch $(-a)(-b) = -(a(-b)) = -(-ab) = ab$ auf die bereits bekannten Regeln zurückgeführt werden.

Die Zahlbereiche \mathbb{Z} , \mathbb{Q} , \mathbb{R} und \mathbb{C} bilden mit ihrer herkömmlichen Addition und Multiplikation jeweils Ringe. Als weitere wichtige Beispiele von Ringen werden wir später noch die **Polynomringe** $R[x]$ und die **Restklassenringe** $\mathbb{Z}/n\mathbb{Z}$ kennenlernen. Dagegen ist der Zahlbereich \mathbb{N}_0 mit der gewöhnlichen Addition und Multiplikation *kein* Ring, weil $(\mathbb{N}_0, +)$ keine Gruppe ist. Beispielsweise besitzt das Element 1 in $(\mathbb{N}_0, +)$ kein Inverses. Ein solches Inverses $a \in \mathbb{N}_0$ von 1 müsste nämlich die Gleichung $a + 1 = 0$ erfüllen, aber durch Addition von -1 auf beiden Seiten erhält man $a = -1$, im Widerspruch zu $a \in \mathbb{N}_0$.

Man beachte, dass Null- und Einselement eines Rings R auch zusammenfallen können, also $0_R = 1_R$ gelten kann. Allerdings kann dies nur passieren, wenn der gesamte Ring nur aus einem einzigen Element besteht, also $R = \{0_R\} = \{1_R\}$ gilt. Ist nämlich R ein Ring mit $0_R = 1_R$ und $a \in R$ beliebig, dann erhält man $a = a \cdot 1_R = a \cdot 0_R = 0_R$. Ringe mit nur einem Element bezeichnet man als **Nullringe**.

Wie in der Kategorie der Gruppen lassen sich aus gegebenen Ringen neue Ringe konstruieren. Sind $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ zwei vorgegebene Ringe, und definiert man auf dem kartesischen Produkt $R \times S$ eine Addition und eine Multiplikation durch

$$(r_1, s_1) + (r_2, s_2) = (r_1 +_R r_2, s_1 +_S s_2) \quad \text{und} \quad (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot_R r_2, s_1 \cdot_S s_2) \quad ,$$

so ist $(R \times S, +, \cdot)$ ein Ring. Denn wie in der Algebra-Vorlesung gezeigt wurde, ist $(R \times S, +)$ als äußeres direktes Produkt der abelschen Gruppen $(R, +)$ und $(S, +)$ selbst eine abelsche Gruppe, und wie dort zeigt man, dass $(R \times S, \cdot)$ ein abelsches Monoid ist. Auch das Distributivgesetz kann auf die Distributivgesetze in $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ zurückgeführt werden, denn für beliebig vorgegebene Elemente $(r_1, s_1), (r_2, s_2), (r_3, s_3) \in R \times S$ gilt

$$\begin{aligned} (r_1, s_1) \cdot ((r_2, s_2) + (r_3, s_3)) &= (r_1, s_1) \cdot (r_2 +_R r_3, s_2 +_S s_3) = (r_1 \cdot_R (r_2 +_R r_3), s_1 \cdot_S (s_2 +_S s_3)) \\ &= (r_1 \cdot_R r_2 +_R r_1 \cdot_R r_3, s_1 \cdot_S s_2 +_S s_1 \cdot_S s_3) = (r_1 \cdot_R r_2, s_1 \cdot_S s_2) + (r_1 \cdot_R r_3, s_1 \cdot_S s_3) \\ &= (r_1, s_1) \cdot (r_2, s_2) + (r_1, s_1) \cdot (r_3, s_3). \end{aligned}$$

Man bezeichnet $R \times S$ als **direktes Produkt** der Ringe R und S .

Definition 1.2 Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe. Eine Abbildung $\phi : R \rightarrow S$ heißt **Ringhomomorphismus** von $(R, +_R, \cdot_R)$ nach $(S, +_S, \cdot_S)$, wenn die Gleichung $\phi(1_R) = 1_S$ gilt und außerdem

$$\phi(a +_R b) = \phi(a) +_S \phi(b) \quad \text{und} \quad \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$$

für alle $a, b \in R$ erfüllt ist.

Sind beispielsweise R und S Ringe, und betrachten wir den oben konstruierten Ring $R \times S$, dann sind die Abbildungen $\pi_1 : R \times S \rightarrow R, (r, s) \mapsto r$ und $\pi_2 : R \times S \rightarrow S, (r, s) \mapsto s$ beides Ringhomomorphismen. Dies rechnet man durch Einsetzen unmittelbar nach.

Man beachte, dass die Bedingung $\phi(1_R) = 1_S$ für Ringhomomorphismen im Allgemeinen **nicht redundant** ist, sie ergibt sich also nicht automatisch aus den beiden anderen Eigenschaften der Abbildung ϕ . Beispielsweise erfüllt der Homomorphismus

$$\phi : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z} \quad , \quad a \mapsto (a, 0)$$

die beiden Bedingungen $\phi(a + b) = \phi(a) + \phi(b)$ und $\phi(ab) = \phi(a)\phi(b)$ für alle $a, b \in \mathbb{Z}$. Es gilt aber nicht $\phi(1) = 1_{\mathbb{Z} \times \mathbb{Z}}$, denn das Einselement von $\mathbb{Z} \times \mathbb{Z}$ ist $(1, 1)$ und nicht $(1, 0)$.

Aus der Definition folgt unmittelbar, dass ein Ringhomomorphismus $\phi : R \rightarrow S$ ein **Gruppenhomomorphismus** $(R, +_R) \rightarrow (S, +_S)$ und ein **Monoid-Homomorphismus** $(R, \cdot_R) \rightarrow (S, \cdot_S)$ ist. Also gelten alle Rechenregeln, die wir in der Algebra für solche Homomorphismen bewiesen haben, insbesondere $\phi(0_R) = 0_S$ und $\phi(-a) = -\phi(a)$ für alle $a \in R$.

Die Begriffe Mono-, Epi-, Iso-, Endo- und Automorphismus von Ringen sind wie in der Kategorie der Gruppen definiert. (Ein Monomorphismus von Ringen ist also ein injektiver Ringhomomorphismus usw.) Wie dort zeigt man auch hier, dass die Komposition zweier Ringhomomorphismen ein Ringhomomorphismus und die Umkehrabbildung eines Isomorphismus von Ringen wiederum ein Isomorphismus ist.

In der Gruppentheorie wurde für jedes $n \in \mathbb{N}_0$ die n -te Potenz eines Monoidelements g definiert. Diese wurde in additiver Schreibweise mit $n \cdot g$ und in multiplikativer Schreibweise g^n bezeichnet. Bei invertierbaren Elementen wurde die Definition sogar auf alle $n \in \mathbb{Z}$ ausgedehnt. Wir behalten diese Notation für die Gruppe $(R, +)$ und das Monoid (R, \cdot) bei, falls $(R, +, \cdot)$ einen Ring bezeichnet. Für jedes $n \in \mathbb{N}$ und jedes $a \in R$ gilt also

$$n \cdot a = \underbrace{a + \dots + a}_{n\text{-mal}} \quad \text{und} \quad a^n = \underbrace{a \cdot \dots \cdot a}_{n\text{-mal}}$$

Außerdem gilt $0 \cdot a = 0_R$, $a^0 = 1_R$ sowie $(-n) \cdot a = -n \cdot a$ und $a^{-n} = (a^n)^{-1}$ für alle $n \in \mathbb{N}$.

Der folgende Satz zeigt, dass der Ring \mathbb{Z} der ganzen Zahlen in der Ringtheorie eine besondere Rolle spielt.

Satz 1.3 Für jeden Ring R existiert ein eindeutig bestimmter Homomorphismus $\mathbb{Z} \rightarrow R$ von Ringen.

Beweis: Zum Nachweis der *Existenz* definieren wir $\phi(n) = n \cdot 1_R$ für alle $n \in \mathbb{Z}$. Zu überprüfen ist, dass es sich um einen Ringhomomorphismus handelt. Zunächst gilt $\phi(1) = 1 \cdot 1_R = 1_R$. Auf Grund der Potenzgesetze in $(R, +)$ gilt außerdem $\phi(m + n) = (m + n) \cdot 1_R = m \cdot 1_R + n \cdot 1_R = \phi(m) + \phi(n)$ für alle $m, n \in \mathbb{Z}$; somit ist ϕ jedenfalls ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(R, +)$. Als nächstes beweisen wir die Gleichung $\phi(mn) = \phi(m)\phi(n)$ für alle $m \in \mathbb{Z}$ und $n \in \mathbb{N}_0$, durch vollständige Induktion über n . Für $n = 0$ ist die Gleichung wegen

$$\phi(m \cdot 0) = \phi(0) = 0 \cdot 1_R = 0_R = (m \cdot 1_R) \cdot (0 \cdot 1_R) = \phi(m)\phi(0)$$

erfüllt. Setzen wir die Gleichung nun für n voraus, dann erhalten wir

$$\begin{aligned} \phi(m(n+1)) &= \phi(mn + m) = \phi(mn) + \phi(m) = \phi(m)\phi(n) + \phi(m) \cdot 1_R = \\ &= \phi(m)\phi(n) + \phi(m)\phi(1) = \phi(m)(\phi(n) + \phi(1)) = \phi(m)\phi(n+1). \end{aligned}$$

Schließlich gilt noch $\phi(m(-n)) = \phi(-mn) = -\phi(mn) = -\phi(m)\phi(n) = \phi(m)(-\phi(n)) = \phi(m)\phi(-n)$ für alle $m \in \mathbb{Z}$ und $n \in \mathbb{N}$, so dass die Gleichung $\phi(mn) = \phi(m)\phi(n)$ damit für alle $m, n \in \mathbb{Z}$ bewiesen ist. Insgesamt ist somit gezeigt, dass es sich bei ϕ um einen Ringhomomorphismus handelt.

Zum Nachweis der *Eindeutigkeit* sei ein weiterer Ringhomomorphismus $\psi : \mathbb{Z} \rightarrow R$ vorgegeben. Dann gilt $\phi(1) = 1_R = \psi(1)$. Weil ϕ und ψ insbesondere Gruppenhomomorphismen von $(\mathbb{Z}, +)$ nach $(R, +)$ sind, gilt für alle $n \in \mathbb{Z}$ außerdem jeweils $\phi(n) = \phi(n \cdot 1) = n \cdot \phi(1) = n \cdot 1_R = n \cdot \psi(1) = \psi(n \cdot 1) = \psi(n)$. Damit ist die Eindeutigkeit nachgewiesen. \square

Definition 1.4 Sei R ein Ring.

- (i) Ein Element $a \in R$ heißt **Einheit**, wenn ein $b \in R$ mit $ab = 1_R$ existiert. Die Menge der Einheiten von R bezeichnen wir mit R^\times .
- (ii) Man nennt es **Nullteiler**, wenn ein Element $b \in R$, $b \neq 0_R$ mit $ab = 0_R$ existiert.

Die Einheiten sind genau die invertierbaren Elemente im Monoid (R, \cdot) . Das multiplikative Inverse eines Elements $a \in R^\times$ wird auch der **Kehrwert** von a genannt und mit a^{-1} bezeichnet. Auch hier gelten die bekannten Rechenregeln für Inverse, also $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ und $(a^{-1})^{-1} = a$ für alle $a, b \in R^\times$. Aus der Gruppentheorie ist bekannt, dass die invertierbaren Elemente in einem Monoid eine Gruppe bilden. Damit ist auch R^\times eine Gruppe, die sog. **Einheitengruppe**.

Definition 1.5 Ein Ring R mit 0_R als einzigem Nullteiler heißt **Integritätsbereich**. Gilt $R^\times = R \setminus \{0_R\}$, dann ist R ein **Körper**.

Die Zahlbereiche \mathbb{Q} , \mathbb{R} und \mathbb{C} sind Körper, denn jedes Element ungleich Null in diesen Bereichen besitzt ein multiplikatives Inverses. Im Ring \mathbb{Z} die Elemente ± 1 die einzigen beiden Einheiten. Es gibt also außer der Null weitere Nicht-Einheiten, und damit ist \mathbb{Z} kein Körper. Man überprüft aber leicht, dass \mathbb{Z} ein Integritätsbereich ist. Denn das Element 0 ist ein Nullteiler, denn es gilt $1 \neq 0$ und $0 \cdot 1 = 0$. Andererseits ist 0 der einzige Nullteiler. Sind nämlich $a, b \neq 0$, dann ist auch das Produkt ab ungleich Null. Wäre $ab = 0$, dann würden wir durch $b = a^{-1}ab = a^{-1}0 = 0$ einen Widerspruch zur Voraussetzung erhalten. Mit demselben Argument kann gezeigt werden, dass jeder Teilring (s.u.) eines Körpers ein Integritätsbereich ist.

Im Ring $\mathbb{Z} \times \mathbb{Z}$ gibt es vier Einheiten, die Elemente $(\pm 1, \pm 1)$. Es ist aber kein Integritätsbereich, denn das Element $(1, 0)$ ist wegen $(1, 0)(0, 1) = (0, 0)$ und $(0, 1) \neq (0, 0)$ ein Nullteiler des Rings. Nullringe der Form $R = \{0_R\}$ sind generell keine Integritätsbereiche, weil das Nullelement 0_R nach Definition kein Nullteiler ist.

Lemma 1.6

- (i) Ein Element a in einem Ring R kann nicht zugleich Nullteiler und Einheit sein.
- (ii) Jeder Körper ist ein Integritätsbereich.
- (iii) In jedem Integritätsbereich R gilt die **Kürzungsregel**: Sind $a, b, c \in R$ mit $c \neq 0_R$, dann folgt aus $ac = bc$ die Gleichung $a = b$.

Beweis: zu (i) Angenommen, a ist zugleich Nullteiler und Einheit. Dann gibt es ein Element $b \neq 0_R$ mit $ab = 0_R$ und ein $c \in R$ mit $ca = 1_R$. Wir erhalten den Widerspruch $b = 1_R \cdot b = (ca)b = c(ab) = c0_R = 0_R$.

zu (ii) Nehmen wir an, dass R ein Körper, aber kein Integritätsbereich ist. Dann ist 0_R kein Nullteiler in R , oder es gibt einen Nullteiler $a \neq 0_R$. Die erste Möglichkeit ist ausgeschlossen, denn 1_R ist in jedem Ring stets eine Einheit, und aus $R^\times = R \setminus \{0_R\}$ folgt $1_R \neq 0_R$. Die Gleichung $1_R \cdot 0_R = 0_R$ zeigt also, dass 0_R ein Nullteiler ist. Aber auch die zweite Möglichkeit kann nicht eintreten, denn wegen $R^\times = R \setminus \{0_R\}$ wäre a zugleich Nullteiler und Einheit, was zu (i) im Widerspruch steht.

zu (iii) Aus $ac = bc$ folgt $(a - b)c = ac - bc = 0_R$. Wäre $a - b \neq 0_R$, dann wäre das Element ein Nullteiler ungleich 0_R . Weil R aber ein Integritätsbereich ist, muss $a - b = 0_R$ gelten. \square

Einen Ringhomomorphismus zwischen Körpern bezeichnet man als **Körperhomomorphismus**. Wir bemerken

Proposition 1.7 Ein Körperhomomorphismus $\phi : K \rightarrow L$ ist stets injektiv.

Beweis: Sei $a \in K$ ein Element im Kern, also ein Element mit $\phi(a) = 0_L$, und nehmen wir an, dass $a \neq 0_K$ ist. Dann folgt $1_L = \phi(1_K) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = 0_L\phi(a^{-1}) = 0_L$. Aber dies ist unmöglich, da L kein Nullring ist. \square

Definition 1.8 Sei R ein Ring. Die **Charakteristik** eines Rings R ist definiert durch

$$\text{char}(R) = \begin{cases} n & \text{falls } n \in \mathbb{N} \text{ minimal mit } n \cdot 1_R = 0_R \text{ ist,} \\ 0 & \text{falls } n \cdot 1_R \neq 0_R \text{ für alle } n \in \mathbb{N} \text{ gilt.} \end{cases}$$

Bei positiver Charakteristik ist $\text{char}(R)$ also die Ordnung des Elements 1_R in der Gruppe $(R, +)$. Die Charakteristik kann auch den Wert 1 annehmen. Dies ist genau dann der Fall, wenn Null- und Einselement von R zusammenfallen, also $0_R = 1_R$ gilt. Wir untersuchen nun die Charakteristik von Integritätsbereichen. Wie allgemein üblich, bezeichnen wir eine natürliche Zahl n als **Primzahl**, wenn $n > 1$ ist und keine Zahlen $r, s \in \mathbb{N}$ mit $1 < r, s < n$ und $n = rs$ existieren.

Proposition 1.9 Sei R ein Integritätsbereich. Dann ist die Charakteristik $\text{char}(R)$ entweder gleich Null oder eine Primzahl.

Beweis: Wäre $\text{char}(R) = 1$, dann wäre der Ring R , wie wir soeben bemerkt haben, ein Nullring und damit kein Integritätsbereich. Nehmen wir nun an, dass $n = \text{char}(R) > 1$, aber keine Primzahl ist. Dann gibt es natürliche Zahlen r, s mit $1 < r, s < n$ und $n = rs$. Nach Definition der Charakteristik gilt $r \cdot 1_R, s \cdot 1_R \neq 0_R$, aber $n \cdot 1_R = 0_R$. Die Gleichung $(r \cdot 1_R)(s \cdot 1_R) = (rs) \cdot 1_R = n \cdot 1_R = 0_R$ zeigt dann, dass die Elemente r_R und s_R des Rings R Nullteiler ungleich Null sind. Aber dies widerspricht der Voraussetzung, dass es sich bei R um einen Integritätsbereich handelt. \square

Nach 1.9 ist also insbesondere $\text{char}(K)$ für einen Körper gleich Null oder eine Primzahl. Es gibt beispielsweise keinen Körper der Charakteristik 4.

§ 2. Teilringe und Erzeugendensysteme

Zusammenfassung. Häufig ist man bei der Untersuchung einer algebraischen Struktur daran interessiert, gleichartige Unterstrukturen zu finden. Bei den Ringen sind dies die *Teilringe*. In der Ringtheorie noch wichtiger ist der umgekehrte Gesichtspunkt, nämlich die *Erweiterung* eines Rings zu einer größeren Struktur. Zum Beispiel lassen sich viele arithmetische Probleme einfacher lösen, wenn man den Ring \mathbb{Z} der ganzen Zahlen um geeignete komplexe Zahlen erweitert. In diesem Kapitel werden wir sehen, wie solche Erweiterungen definiert werden können, wie man die Elemente einer solchen Erweiterung bestimmt, und wie Ringerweiterungen mit Hilfe geeigneter Homomorphismen konstruiert werden können.

Wichtige Grundbegriffe und Konzepte

- Teilring eines Rings R
- Erweiterungsring, Ringerweiterung
- Teilkörper und Primkörper
- Definition des von einer Menge A erzeugten Erweiterungsringes $R[A]$
- quadratische Zahlringe, Gauß'sche Zahlen und Eisenstein-Zahlen
- Übertragung von Verknüpfungen auf andere Mengen durch Bijektionen

Zentrale Sätze

- Teilringe von Ringen sind Ringe.
- Existenz und Eindeutigkeit von $R[A]$
- Die Elemente einer einfachen Erweiterung $R[c]$ sind Polynomausdrücke in c .
- Konstruktion des Körpers \mathbb{C} der komplexen Zahlen

Definition 2.1 Sei R ein Ring. Eine Teilmenge $S \subseteq R$ wird **Teilring** von R genannt, wenn $1_R \in S$ gilt und mit $a, b \in S$ jeweils auch die Elemente $a - b$ und ab in S liegen.

Umgekehrt bezeichnet man einen Ring R als **Erweiterungsring** eines anderen Rings S , wenn R ein Teilring von S ist. Das Paar (S, R) bezeichnet man in diesem Fall als **Ringerweiterung**. Allgemein wird die Schreibweise $R|S$ verwendet, um ausdrücken, dass durch (S, R) eine Ringerweiterung gegeben ist.

Satz 2.2 Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$ ein Teilring. Dann ist die Menge S unter den Verknüpfungen $+$ und \cdot abgeschlossen. Bezeichnen wir mit $+_S$ und \cdot_S die auf S eingeschränkten Verknüpfungen, dann ist $(S, +_S, \cdot_S)$ ein Ring.

Beweis: Als erstes beweisen wir die Abgeschlossenheit. Aus $1_R \in S$ folgt zunächst $0_R = 1_R - 1_R \in S$, denn auf Grund der Teilring-Eigenschaft liegt Differenz zweier Elemente aus S wieder in S . Wegen $-a = 0_R - a$ ist mit jedem $a \in S$

auch das Negative $-a$ in S enthalten. Seien nun $a, b \in S$ vorgegeben. Dann gilt $-b \in S$ und somit $a + b = a - (-b) \in S$. Aus der Teilring-Eigenschaft folgt auch $ab \in S$. Also ist S tatsächlich unter $+$ und \cdot abgeschlossen.

Nun überprüfen wir die Ringeigenschaften von $(S, +_S, \cdot_S)$. Wie bereits gezeigt wurde, gilt $0_R \in S$, und mit $a, b \in S$ liegen auch die Elemente $a + b$ und $-a$ in S . Also ist S eine Untergruppe von $(R, +)$, und wie in der Algebra-Vorlesung gezeigt wurde, ist $(S, +_S)$ damit eine Gruppe. Wegen

$$a +_S b = a + b = b + a = b +_S a \text{ für alle } a, b \in S$$

ist diese auch kommutativ. Ebenso kann das Assoziativ- und Kommutativitätsgesetz von \cdot_S auf die Assoziativität und Kommutativität von \cdot zurückgeführt werden. Wegen $a \cdot_S 1_R = a \cdot 1_R = a$ und $1_R \cdot_S a = 1_R \cdot a = a$ ist 1_R das Neutralelement von (S, \cdot_S) . Schließlich leitet man auch das Distributivgesetz für $+_S$ und \cdot_S aus dem entsprechenden Gesetz für $+_R$ und \cdot_R ab. \square

Beispielsweise ist \mathbb{Z} ein Teilring von \mathbb{Q} , \mathbb{Q} ein Teilring von \mathbb{R} und \mathbb{R} ein Teilring von \mathbb{C} . Die Menge $\mathbb{Z} \times \{0\}$ ist mit den Verknüpfungen $(a, 0) + (b, 0) = (a + b, 0)$ und $(a, 0) \cdot (b, 0) = (ab, 0)$ zwar ein Ring, aber *kein* Teilring von $\mathbb{Z} \times \mathbb{Z}$, denn das Einselement $1_{\mathbb{Z} \times \mathbb{Z}} = (1, 1)$ ist nicht in $\mathbb{Z} \times \{0\}$ enthalten.

Der soeben durchgeführte Beweis zeigt, dass für die Teilring-Eigenschaft $a - b \in S$ für $a, b \in S$ gefordert werden muss, um die Existenz von Negativen in S sicherzustellen. Würde man statt dessen $a + b \in S$ fordern, dann wäre die Unterstruktur S im allgemeinen kein Ring. Die Teilmenge $\mathbb{N} \subseteq \mathbb{Z}$ genügt beispielsweise den Bedingungen $1 \in \mathbb{N}$ und $a, b \in \mathbb{N} \Rightarrow a + b, ab \in \mathbb{N}$, ohne dass $(\mathbb{N}, +, \cdot)$ selbst ein Ring ist.

Lemma 2.3 Sei $(R, +, \cdot)$ ein Ring, und sei $(S_i)_{i \in I}$ eine Familie von Teilringen. Dann ist auch $S = \bigcap_{i \in I} S_i$ ein Teilring von R .

Beweis: Weil S_i für jedes $i \in I$ ein Teilring von R ist, gilt $1_R \in S_i$ für alle $i \in I$ und damit $1_R \in S$. Seien nun $a, b \in S$ vorgegeben. Dann folgt $a, b \in S_i$ für alle $i \in I$. Weil jedes S_i ein Teilring von R ist, gilt damit auch $a - b \in S_i$ und $ab \in S_i$ für alle $i \in I$. Dies wiederum bedeutet $a - b \in S$ und $ab \in S$. Damit ist der Nachweis der Teilring-Eigenschaft von S abgeschlossen. \square

Das Analogon zum Teilring in der Kategorie der Körper ist durch folgende Definition gegeben.

Definition 2.4 Sei K ein Körper. Eine Teilmenge $F \subseteq K$ wird **Teilkörper** von K genannt, wenn $1_K \in F$ gilt, für alle $a, b \in F$ auch die Elemente $a - b$ und ab in F liegen und für jedes $a \in F$, $a \neq 0_K$ auch $a^{-1} \in F$ gilt.

Wir haben in Lemma 2.2 gesehen, dass man durch Einschränkung von Addition und Multiplikation von K auf die Teilmenge F einen Ring erhält. Durch Bedingung, dass für jedes $a \in F \setminus \{0_K\}$ auch a^{-1} in F liegt, wird F darüber hinaus zu einem Körper. Die Begriffe „**Erweiterungskörper**“ und „**Körpererweiterung**“ sind in genauer Analogie zu den Ringen definiert.

Lemma 2.5 Sei K ein Körper und $(F_i)_{i \in I}$ eine beliebige Familie von Teilkörpern. Dann ist auch $F = \bigcap_{i \in I} F_i$ ein Teilkörper von K .

Beweis: Nach Lemma 2.3 ist F jedenfalls ein Teilring von K . Ist außerdem $a \in F^\times$, dann liegt a auch in F_i^\times für jedes $i \in I$, und somit liegt auch a^{-1} jeweils in F_i . Daraus wiederum folgt $a^{-1} \in F$. Damit ist die Teilkörper-Eigenschaft von F nachgewiesen. \square

Folgerung 2.6 Ist K ein Körper und ist $(F_i)_{i \in I}$ die Familie *aller* Teilkörper von K , dann nennt man $P = \bigcap_{i \in I} F_i$ den **Primkörper** von K . Es handelt sich um den bezüglich Inklusion kleinsten Teilkörper von K .

Beispielsweise ist \mathbb{Q} der gemeinsame Primkörper von \mathbb{Q} , \mathbb{R} und \mathbb{C} , und für jede Primzahl ist \mathbb{F}_p sein eigener Primkörper. Im Körpertheorie-Teil der Vorlesung werden wir sehen, dass der Primkörper jedes Körpers isomorph zu \mathbb{Q} oder zu \mathbb{F}_p für eine Primzahl p ist.

Satz 2.7 Sei $\tilde{R}|R$ eine Ringerweiterung und $A \subseteq \tilde{R}$ eine beliebige Teilmenge. Dann gibt es einen eindeutig bestimmten Teilring $R[A]$ von \tilde{R} mit den folgenden beiden Eigenschaften.

- (i) Es gilt $R[A] \supseteq R \cup A$.
- (ii) Ist R' ein weiterer Teilring von \tilde{R} mit $R' \supseteq R \cup A$, dann folgt $R' \supseteq R[A]$.

Damit ist $R[A]$ also der **kleinste** Teilring von \tilde{R} , der $R \cup A$ enthält. Man nennt ihn den von A über R **erzeugten** Teilring.

Beweis: *Existenz:* Sei $(S_i)_{i \in I}$ die Menge *aller* Teilringe von \tilde{R} mit $S_i \subseteq R \cup A$. Nach Lemma 2.3 ist $R[A] = \bigcap_{i \in I} S_i$ ein Teilring von \tilde{R} . Wegen $R \cup A \subseteq S_i$ für alle $i \in I$ gilt auch $R \cup A \subseteq R[A]$. Ist nun R' ein beliebiger Teilring von \tilde{R} mit $R' \supseteq R \cup A$, dann gilt $R' = S_i$ für ein $i \in I$ nach Definition der Familie $(S_i)_{i \in I}$. Weil $R[A]$ nach Definition der Durchschnitt aller Ringe in der Familie $(S_i)_{i \in I}$ ist, gilt $R[A] \subseteq R_i = R'$.

Eindeutigkeit: Sei S ein weiterer Teilring mit den Eigenschaften (i) und (ii). Dann ist S jedenfalls ein Teilring von \tilde{R} mit $S \supseteq R \cup A$, und $R[A]$ ist der **kleinste** Teilring mit dieser Eigenschaft. Daraus folgt $R[A] \subseteq S$. Umgekehrt ist auch $R[A]$ ein Teilring von \tilde{R} mit $R[A] \supseteq R \cup A$, und S ist der kleinste Teilring mit dieser Eigenschaft. Somit gilt auch $S \subseteq R[A]$, insgesamt $R[A] = S$. \square

Ist $S = \{s\}$ einelementig, dann schreibt man an Stelle von $R[\{s\}]$ auch einfach $R[s]$ für den erzeugten Teilring. Auch bei mehreren Elementen werden die Mengenklammern oft weggelassen, man schreibt also statt $R[\{s_1, s_2\}]$ den Ausdruck $R[s_1, s_2]$ usw.

Als wichtiges Beispiel für erzeugte Teilringe sehen wir uns die **quadratischen Zahlringe** an. Dazu verabreden wir für die Bezeichnung von Quadratwurzeln reeller Zahlen die folgende Konvention. Ist $d \in \mathbb{R}$ positiv, dann sei \sqrt{d} ein eindeutig bestimmte positive Quadratwurzel von d . Im Fall $d < 0$ sei $d \in \mathbb{C}$ die eindeutig bestimmte komplexe Quadratwurzel mit positivem Imaginärteil, also $\sqrt{d} = i\sqrt{|d|}$. Zu beachten ist, dass bei dieser Schreibweise die Gleichung

$$\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}$$

im allgemeinen nicht erfüllt ist, nämlich dann nicht, wenn a und b beide negativ sind. Zum Beispiel ist $\sqrt{(-3)(-5)} \neq \sqrt{-3}\sqrt{-5}$, denn es gilt $\sqrt{-3}\sqrt{-5} = (i\sqrt{3})(i\sqrt{5}) = i^2\sqrt{15} = -\sqrt{15} \neq \sqrt{15} = \sqrt{(-3)(-5)}$.

Außerdem verwenden wir im Folgenden die **Kongruenzschreibweise**. Sind $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$, so bedeutet der Ausdruck $a \equiv b \pmod{n}$, dass n ein Teiler von $b - a$ ist. Man sagt „Die Zahlen a und b sind kongruent modulo n .“ Ausführlicher werden wir uns mit den Kongruenzen in § 5 beschäftigen. Als konkrete Anwendung von Satz 2.7 zeigen wir nun

Satz 2.8 Sei $d \in \mathbb{Z}$ und $\sqrt{d} \in \mathbb{C}$ wie oben definiert.

(i) Es gilt $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

(ii) Ist $d \equiv 1 \pmod{4}$, dann gilt $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})] = \{\frac{1}{2}a + \frac{1}{2}b\sqrt{d} \mid a, b \in \mathbb{Z}, a \equiv b \pmod{2}\}$.

Die Ringe dieser Form bezeichnen wir als **quadratische Zahlringe**.

Beweis: zu (i) Sei M die Teilmenge auf der rechten Seite der Gleichung. Wir überprüfen, dass M ein Teilring von \mathbb{C} ist. Wegen $1 = 1 + 0\sqrt{d}$ gilt $1 \in M$. Seien nun $\alpha, \beta \in M$ vorgegeben. Dann gibt es $r, s, t, u \in \mathbb{Z}$ mit $\alpha = r + s\sqrt{d}$ und $\beta = t + u\sqrt{d}$. Es folgt $\alpha - \beta = (r - t) + (s - u)\sqrt{d} \in M$ und

$$\alpha\beta = (r + s\sqrt{d})(t + u\sqrt{d}) = (rt + sud) + (ru + st)\sqrt{d} \in M.$$

Außerdem gilt $M \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$, denn für jedes $a \in \mathbb{Z}$ gilt $a = a + 0 \cdot \sqrt{d} \in M$ und $\sqrt{d} = 0 + 1 \cdot \sqrt{d} \in M$.

Sei nun R' ein beliebiger Teilring von \mathbb{C} mit $R' \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$. Zu zeigen ist $R' \supseteq M$. Sei dazu $\alpha \in M$ vorgegeben, $\alpha = r + s\sqrt{d}$ mit $r, s \in \mathbb{Z}$. Aus $r, s \in \mathbb{Z}$ folgt $r, s \in R'$. Ebenso ist \sqrt{d} nach Voraussetzung in R' enthalten. Da es sich bei R' um einen Teilring von \mathbb{C} handelt, der als solcher unter Addition und Multiplikation abgeschlossen ist, folgt daraus zunächst $s\sqrt{d} \in R'$ und dann $r + s\sqrt{d} \in R'$.

zu (ii) Zunächst überprüfen wir wieder, dass die Menge M auf der rechten Seite ein Teilring von \mathbb{C} ist. Es gilt $1 = \frac{1}{2} \cdot 2 + \frac{1}{2} \cdot 0 \cdot \sqrt{d}$ in M , denn es gilt $2 \equiv 0 \pmod{2}$. Seien nun $\alpha, \beta \in M$ vorgegeben. Dann gibt es $r, s, t, u \in \mathbb{Z}$ mit $\alpha = \frac{1}{2}r + \frac{1}{2}s\sqrt{d}$, $\beta = \frac{1}{2}t + \frac{1}{2}u\sqrt{d}$, wobei $r \equiv s \pmod{2}$ und $t \equiv u \pmod{2}$ gilt. Das Element

$$\alpha - \beta = \left(\frac{1}{2}r + \frac{1}{2}s\sqrt{d}\right) - \left(\frac{1}{2}t + \frac{1}{2}u\sqrt{d}\right) = \frac{1}{2}(r - t) + \frac{1}{2}(s - u)\sqrt{d}$$

liegt ebenfalls in M , denn aus $r \equiv s \pmod{2}$ und $t \equiv u \pmod{2}$ folgt $r - t \equiv s - u \pmod{2}$. Um zu sehen, dass auch das Element

$$\alpha\beta = \left(\frac{1}{2}r + \frac{1}{2}s\sqrt{d}\right)\left(\frac{1}{2}t + \frac{1}{2}u\sqrt{d}\right) = \frac{1}{4}(rt + dsu) + \frac{1}{4}(st + ru)\sqrt{d} = \frac{1}{2}v + \frac{1}{2}w\sqrt{d}$$

mit $v = \frac{1}{2}(rt + dsu)$ und $w = \frac{1}{2}(st + ru)\sqrt{d}$ in M enthalten ist, müssen wir überprüfen, dass $2v + 2w = rt + dsu + st + ru$ durch 4 teilbar ist. Denn daraus folgt, dass $v + w$ gerade ist, was wiederum äquivalent dazu ist dass v und w beide gerade oder ungerade sind, also $v \equiv w \pmod{2}$ erfüllen. Auf Grund der Voraussetzung $d \equiv 1 \pmod{4}$ gilt $rt + dsu + st + ru \equiv rt + su + st + ru \equiv (r + s)(t + u) \pmod{4}$, und die Zahl $(r + s)(t + u)$ ist durch 4 teilbar, weil $r + s$ und $t + u$ gerade sind. Insgesamt ist M also tatsächlich ein Teilring von \mathbb{C} . Außerdem gilt $M \supseteq \mathbb{Z} \cup \{\frac{1}{2}(1 + \sqrt{d})\}$. Denn jedes $a \in \mathbb{Z}$ ist wegen $a = \frac{1}{2}(2a) + \frac{1}{2} \cdot 0 \cdot \sqrt{d}$ und $2a \equiv 0 \pmod{2}$ in M enthalten, und ebenso gilt $\frac{1}{2}(1 + \sqrt{d}) = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 \cdot \sqrt{d} \in M$ wegen $1 \equiv 1 \pmod{2}$.

Sei nun R' ein weiterer Teilring von \mathbb{C} mit $R' \supseteq \mathbb{Z} \cup \{\frac{1}{2}(1 + \sqrt{d})\}$. Zu zeigen ist $R' \supseteq M$. Sei dazu $\alpha \in M$ vorgegeben, $\alpha = \frac{1}{2}r + \frac{1}{2}s\sqrt{d}$ mit $r, s \in \mathbb{Z}$, $r \equiv s \pmod{2}$. Dann gilt $\alpha - s \cdot \frac{1}{2}(1 + \sqrt{d}) = \frac{1}{2}(r - s)$. Wegen $\frac{1}{2}(r - s) \in \mathbb{Z}$ und $\mathbb{Z} \subseteq R'$ folgt $\frac{1}{2}(r - s) \in R'$. Aus $\frac{1}{2}(1 + \sqrt{d}) \in R'$ folgt ebenso $s \cdot \frac{1}{2}(1 + \sqrt{d}) \in R'$. Da R' unter Addition abgeschlossen ist, liegt damit auch α in R' . \square

Zwei Zahlringe spielen in der Zahlentheorie eine besonders wichtige Rolle: der Ring $\mathbb{Z}[i]$ der **Gauß'schen Zahlen** und der Ring $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})]$ der **Eisenstein-Zahlen**.

Wir betrachten nun allgemeine Ringerweiterungen, die von nur einem Element erzeugt werden. Bereits in der Linearen Algebra haben wir den Polynomring $R[x]$ über einem Ring R eingeführt; in § 3 werden wir diese Ringe genauer studieren.

Proposition 2.9 Sei $\tilde{R} | R$ eine Ringerweiterung und $c \in \tilde{R}$. Dann gilt $R[c] = \{f(c) \mid f \in R[x]\}$.

Beweis: Sei S die Teilmenge auf der rechten Seite der Gleichung. Wir zeigen, dass S ein Teilring von \tilde{R} ist. Das Einselement $1_{\tilde{R}} = 1_R$ von \tilde{R} ist in $R[c]$ enthalten, denn betrachten wir 1_R als konstantes Polynom, also als Element von $R[x]$, dann gilt $1_R = 1_R(c) \in S$. Seien nun $\alpha, \beta \in S$ vorgegeben. Dann gibt es Polynome $f, g \in R[x]$ mit $\alpha = f(c)$ und $\beta = g(c)$. Es folgt $\alpha - \beta = f(c) - g(c) = (f - g)(c) \in S$ und $\alpha\beta = f(c)g(c) = (fg)(c) \in S$. Dies zeigt, dass S tatsächlich ein Teilring von \tilde{R} ist.

Um zu zeigen, dass S mit $R[c]$ übereinstimmt, müssen wir noch überprüfen, dass S in jedem Teilring R' von \tilde{R} mit $R' \supseteq R \cup \{c\}$ enthalten ist. Sei also R' ein solcher Teilring und $\alpha \in S$. Zu zeigen ist $\alpha \in R'$. Nach Definition von S gibt es ein $f \in R[x]$ mit $\alpha = f(c)$. Schreiben wir $f = \sum_{k=0}^n a_k x^k$ mit $n \in \mathbb{N}_0$ und $a_0, \dots, a_n \in R$, dann gilt $\alpha = \sum_{k=0}^n a_k c^k$. Weil die Elemente a_0, \dots, a_n, c nach Voraussetzung in R' liegen, gilt auch $a_k c^k \in R'$ für $0 \leq k \leq n$, auf Grund der Abgeschlossenheit von R' unter der Multiplikation von \tilde{R} . Aus der Abgeschlossenheit von R' unter Addition (und vollständiger Induktion über n) folgt dann auch, dass $\alpha = \sum_{k=0}^n a_k c^k$ in R' liegt. \square

Ein wesentliches Hilfsmittel bei der Konstruktion von Ringen ist die Übertragung von Verknüpfungen auf andere Mengen mittels Bijektionen.

Lemma 2.10 Seien X und Y Mengen, $\phi : Y \rightarrow X$ eine Bijektion und \cdot eine Verknüpfung auf X . Wir definieren auf Y eine Verknüpfung \odot , indem wir $a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b))$ für alle $a, b \in Y$ definieren. Die neue Verknüpfung \odot hängt dann mit \cdot auf folgende Weise zusammen.

- (i) Ist die Verknüpfung \cdot auf X assoziativ bzw. kommutativ, dann gilt dasselbe jeweils für die Verknüpfung \odot auf Y .
- (ii) Ist $e_X \in X$ ein Neutralelement in X bezüglich \cdot , dann ist $e_Y = \phi^{-1}(e_X)$ ein Neutralelement in Y bezüglich \odot .
- (iii) Seien e_X und e_Y wie in (ii) und $a, b \in X$. Ist b ein Inverses von a bezüglich \cdot , dann ist $\phi^{-1}(b)$ ein Inverses von $\phi^{-1}(a)$ bezüglich \odot .

Man sagt, dass die Verknüpfung \cdot durch die Bijektion ϕ von X auf Y **übertragen** wird.

Beweis: zu (i) Seien $a, b, c \in Y$ vorgegeben. Zunächst bemerken wir, dass auf Grund der Definition von ϕ jeweils $\phi(a \odot b) = \phi(a) \cdot \phi(b)$ gilt. Setzen wir nun voraus, dass die Verknüpfung \cdot assoziativ ist. Dann gilt

$$\begin{aligned}\phi((a \odot b) \odot c) &= \phi(a \odot b) \cdot \phi(c) = (\phi(a) \cdot \phi(b)) \cdot \phi(c) = \phi(a) \cdot (\phi(b) \cdot \phi(c)) \\ &= \phi(a) \cdot \phi(b \odot c) = \phi(a \odot (b \odot c)).\end{aligned}$$

Auf Grund der Bijektivität von ϕ folgt daraus $(a \odot b) \odot c = a \odot (b \odot c)$. Nehmen wir nun an, dass \cdot kommutativ ist. Dann gilt $\phi(a \odot b) = \phi(a) \cdot \phi(b) = \phi(b) \cdot \phi(a) = \phi(b \odot a)$, und es folgt $a \odot b = b \odot a$.

zu (ii) Sei $a \in Y$ vorgegeben. Dann gilt $\phi(e_Y \odot a) = \phi(e_Y) \cdot \phi(a) = e_X \cdot \phi(a) = \phi(a)$, weil e_X ein Neutralement bezüglich \cdot ist. Auf Grund der Bijektivität von ϕ folgt $e_Y \odot a = a$. Ebenso beweist man die Gleichung $a \odot e_Y = a$.

zu (iii) Sei $a \in X$ und $b \in X$ bezüglich der Verknüpfung \cdot ein Inverses von a . Sei $c = \phi^{-1}(a)$ und $d = \phi^{-1}(b)$; zu zeigen ist $c \odot d = d \odot c = e_Y$. Nun gilt $\phi(c \odot d) = \phi(c) \cdot \phi(d) = a \cdot b = e_X = \phi(e_Y)$, und durch Anwendung von ϕ^{-1} auf beide Seiten der Gleichung erhalten wir $c \odot d = e_Y$. Genauso zeigt man $d \odot c = e_Y$. \square

Aus dem Lemma ergibt sich unmittelbar, dass ϕ auch zur Übertragung einer kompletten algebraischen Struktur von X auf die Menge Y genutzt werden kann. In dieser Vorlesung sind wir vor allem an Ringstrukturen interessiert.

Satz 2.11 Sei $(R, +, \cdot)$ ein Ring, S eine Menge und $\phi : S \rightarrow R$ eine bijektive Abbildung. Seien die Verknüpfungen \oplus und \odot auf S definiert durch

$$a \oplus b = \phi^{-1}(\phi(a) + \phi(b)) \quad \text{und} \quad a \odot b = \phi^{-1}(\phi(a) \cdot \phi(b)).$$

Dann ist (S, \oplus, \odot) ein Ring, und ϕ ist ein Isomorphismus von Ringen.

Beweis: Es genügt, mit Hilfe von Lemma 2.10 die einzelnen Ringaxiome für (S, \oplus, \odot) durchzugehen. Zunächst ist zu überprüfen, dass (S, \oplus) eine abelsche Gruppe ist. Weil die Verknüpfung $+$ auf R assoziativ und kommutativ ist, gilt nach Lemma 2.10 dasselbe für die Verknüpfung \oplus auf S . Weil 0_R in der Halbgruppe $(R, +)$ ein Neutralement ist, handelt es sich bei $0_S = \phi^{-1}(0_R)$ nach Lemma 2.10 (ii) um ein Neutralement in (S, \oplus) . Schließlich besitzt jedes Element $a \in S$ bezüglich \oplus ein Inverses, nämlich nach Lemma 2.10 (iii) das Element $\phi^{-1}(-\phi(a))$. Insgesamt ist (S, \oplus) also tatsächlich eine abelsche Gruppe.

Nach dem gleichen Muster zeigt man, dass (S, \odot) ein abelsches Monoid ist. Das Distributivgesetz kann direkt nachgerechnet werden. Seien dazu $a, b, c \in S$ vorgegeben. Nach Definition der Verknüpfungen \oplus und \odot auf S gilt $\phi(r \oplus s) = \phi(r) + \phi(s)$ und $\phi(r \odot s) = \phi(r) \cdot \phi(s)$ für alle $r, s \in S$. Damit erhalten wir

$$\begin{aligned}a \odot (b \oplus c) &= \phi^{-1}(\phi(a) \cdot \phi(b \oplus c)) = \phi^{-1}(\phi(a) \cdot (\phi(b) + \phi(c))) = \phi^{-1}(\phi(a) \cdot \phi(b) + \phi(a) \cdot \phi(c)) \\ &= \phi^{-1}(\phi(a \odot b) + \phi(a \odot c)) = \phi^{-1}(\phi(a \odot b \oplus a \odot c)) = (a \odot b) \oplus (a \odot c).\end{aligned} \quad \square$$

Das Prinzip der Übertragung von Verknüpfungen kann nun auch für die **Konstruktion von Ringerweiterungen** genutzt werden.

Satz 2.12 Sei $\phi : R \rightarrow S$ ein Monomorphismus von Ringen. Dann gibt es einen Erweiterungsring $\hat{R} \supseteq R$ und einen Isomorphismus $\hat{\phi} : \hat{R} \rightarrow S$ mit $\hat{\phi}|_R = \phi$.

Beweis: Allgemein gilt: Sind A, B, C, D Mengen mit $A \cap B = C \cap D = \emptyset$, und $\phi_1 : A \rightarrow C$, $\phi_2 : B \rightarrow D$ bijektive Abbildungen, dann gibt es eine eindeutig bestimmte Abbildung $\phi : A \cup B \rightarrow C \cup D$ mit $\phi|_A = \phi_1$ und $\phi|_B = \phi_2$, und diese Abbildung ist bijektiv (Beweis als Übung). Setzen wir $\hat{R} = R \cup (S \setminus \phi(R))$, und wenden wir die soeben formulierte Aussage auf $A = R$, $C = \phi(R)$ und $B = D = S \setminus \phi(R)$ an, so existiert dementsprechend eine eindeutig bestimmte bijektive Abbildung $\hat{\phi} : \hat{R} \rightarrow S$ mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}|_{S \setminus \phi(R)} = \text{id}_{S \setminus \phi(R)}$.

Wir nutzen diese bijektive Abbildung zur Definition von Verknüpfungen \oplus und \odot auf \hat{R} , indem wir $a \oplus b = \hat{\phi}^{-1}(\phi(a) + \phi(b))$ und $a \odot b = \hat{\phi}^{-1}(\phi(a)\phi(b))$ für alle $a, b \in \hat{R}$ setzen. Nach Satz 2.11 ist (\hat{R}, \oplus, \odot) dann ein Ring, und $\hat{\phi}$ ist ein Isomorphismus von Ringen. Nach Definition gilt $\hat{\phi}|_R = \phi$, es bleibt also nur zu zeigen, dass R ein Teilring von \hat{R} ist. Nach Lemma 2.10 ist wegen $\phi(1_R) = 1_S$ das Element $1_R = \phi^{-1}(1_S)$ das Einselement von \hat{R} , und dieses ist in R enthalten. Für alle $a, b \in R$ gilt nach Definition $a \oplus b = \hat{\phi}^{-1}(\phi(a) + \phi(b)) = \hat{\phi}^{-1}(\phi(a+b)) = \hat{\phi}^{-1}(\hat{\phi}(a+b)) = a+b$, also insbesondere $a \oplus b \in R$ für alle $a, b \in R$. Genauso sieht man, dass R auch unter der Multiplikation \odot abgeschlossen ist. □

Als Anwendungsbeispiel zeigen wir, wie mit den soeben eingeführten Konzepten der Körper \mathbb{C} der komplexen Zahlen konstruiert werden kann. Weitere Anwendungen folgen in den Kapiteln § 3 und § 6 sowie im Körpertheorie-Teil der Algebra-Vorlesung.

Proposition 2.13 Wir definieren auf der Menge \mathbb{R}^2 die beiden Verknüpfungen \oplus und \odot durch

$$(a, b) \oplus (c, d) = (a + c, b + d) \quad \text{und} \quad (a, b) \odot (c, d) = (ac - bd, bc + ad)$$

für alle $a, b, c, d \in \mathbb{R}$. Dann ist $(\mathbb{R}^2, \oplus, \odot)$ ein Körper, und die Abbildung $\phi : \mathbb{R} \rightarrow \mathbb{R}^2$, $a \mapsto (a, 0)$ ist ein Monomorphismus von Ringen.

Beweis: Dass es sich bei \mathbb{R}^2 mit der komponentenweisen Addition um eine abelsche Gruppe handelt, ist bereits aus der Algebra-Vorlesung bekannt. Wir zeigen nun, dass (\mathbb{R}^2, \odot) ein Monoid ist, mit $(1, 0)$ als Neutralement. Für beliebige $a, b, c, d, e, f \in \mathbb{R}$ gilt sowohl

$$\begin{aligned} (a, b) \odot ((c, d) \odot (e, f)) &= (a, b) \odot (ce - df, de + cf) = (a(ce - df) - b(de + cf), b(ce - df) + a(de + cf)) \\ &= (ace - adf - bde - bcf, bce - bdf + ade + acf) \end{aligned}$$

als auch

$$\begin{aligned} ((a, b) \odot (c, d)) \odot (e, f) &= (ac - bd, bc + ad) \odot (e, f) = ((ac - bd)e - (bc + ad)f, (bc + ad)e + (ac - bd)f) \\ &= (ace - bde - bcf - adf, bce + ade + acf - bdf) = (ace - adf - bde - bcf, bce - bdf + ade + acf). \end{aligned}$$

Damit ist das Assoziativgesetz nachgewiesen. Ebenso gilt wegen $(a, b) \odot (c, d) = (ac - bd, bc + ad) = (ca - db, da + cb) = (c, d) \odot (a, b)$ auch das Kommutativgesetz. Ferner gilt $(1, 0) \odot (a, b) = (1 \cdot a - 0 \cdot b, 0 \cdot a + 1 \cdot b) = (a, b)$ und auf Grund der Kommutativität auch $(a, b) \odot (1, 0) = (a, b)$.

Das Distributivgesetz ist ebenfalls erfüllt, denn für beliebige $a, b, c, d, e, f \in \mathbb{R}$ gilt

$$\begin{aligned} (a, b) \odot (c, d) \oplus (a, b) \odot (e, f) &= (ac - bd, bc + ad) \oplus (ae - bf, be + af) = \\ (ac + ae - bd - bf, bc + be + ad + af) &= (a(c + e) - b(d + f), b(c + e) + a(d + f)) = \\ (a, b) \odot (c + e, d + f) &= (a, b) \odot ((c, d) \oplus (e, f)). \end{aligned}$$

Damit ist insgesamt gezeigt, dass es sich bei $(\mathbb{R}^2, \oplus, \odot)$ um einen Ring handelt. Für jedes $(a, b) \in \mathbb{R}^2$ mit $(a, b) \neq (0, 0)$ gilt $a^2 + b^2 \neq 0$. Setzen wir $c = \frac{a}{a^2 + b^2}$ und $d = -\frac{b}{a^2 + b^2}$, so zeigen die Rechnungen

$$\begin{aligned} (a, b) \odot (c, d) &= (ac - bd, bc + ad) = \left(a \cdot \frac{a}{a^2 + b^2} - b \cdot \left(-\frac{b}{a^2 + b^2} \right), b \cdot \frac{a}{a^2 + b^2} + a \cdot \left(-\frac{b}{a^2 + b^2} \right) \right) \\ &= \left(\frac{a^2 + b^2}{a^2 + b^2}, \frac{ba - ab}{a^2 + b^2} \right) = (1, 0) \end{aligned}$$

und $(c, d) \odot (a, b) = (a, b) \odot (c, d) = (1, 0)$, dass (a, b) im Monoid (\mathbb{R}^2, \odot) ein invertierbares Element ist, mit Kehrwert $(a, b)^{-1} = (c, d)$. Dies zeigt, dass es sich bei $(\mathbb{R}^2, \oplus, \odot)$ um einen Körper handelt.

Zum Schluss zeigen wir noch, dass durch $\phi : \mathbb{R} \rightarrow \mathbb{R}^2, a \mapsto (a, 0)$ ein Monomorphismus von Ringen gegeben ist. Die Injektivität von ϕ ist offensichtlich, denn für $a, b \in \mathbb{R}$ folgt aus $\phi(a) = \phi(b)$ jeweils $(a, 0) = (b, 0)$ und damit $a = b$. Darüber hinaus gilt $\phi(1_{\mathbb{R}}) = \phi(1) = (1, 0) = 1_{\mathbb{R}^2}$ und für alle $a, b \in \mathbb{R}$ jeweils $\phi(a + b) = (a + b, 0) = (a, 0) \oplus (b, 0) = \phi(a) \oplus \phi(b)$ sowie $\phi(ab) = (ab, 0) = (a \cdot b - 0 \cdot 0, 0 \cdot b + a \cdot 0) = (a, 0) \odot (b, 0) = \phi(a) \odot \phi(b)$. \square

Folgerung 2.14 Es existiert ein Erweiterungskörper \mathbb{C} von \mathbb{R} mit einem Element $i \in \mathbb{C}$, so dass $i^2 = -1$ gilt und jedes Element $z \in \mathbb{C}$ auf eindeutige Weise in der Form $z = a + ib$ mit $a, b \in \mathbb{R}$ dargestellt werden kann. (Mit anderen Worten, wir haben den Körper \mathbb{C} der komplexen Zahlen konstruiert.)

Beweis: Wir wenden Satz 2.12 auf den Monomorphismus ϕ aus Proposition 2.13 an. Demnach existiert ein Erweiterungsring von \mathbb{R} , den wir mit \mathbb{C} bezeichnen, und ein Isomorphismus $\hat{\phi} : \mathbb{C} \rightarrow \mathbb{R}^2$ von Ringen, der $\phi : \mathbb{R} \rightarrow \mathbb{R}^2$ auf \mathbb{C} fortsetzt. Weil der Ring \mathbb{C} zum Körper $(\mathbb{R}^2, \oplus, \odot)$ isomorph ist, handelt es sich auch bei \mathbb{C} um einen Körper.

Sei nun $i = \hat{\phi}^{-1}((0, 1)) \in \mathbb{C}$. Aus der Injektivität von $\hat{\phi}$ und

$$\begin{aligned} \hat{\phi}(i^2) &= \hat{\phi}(i)^2 = (0, 1)^2 = (0, 1) \odot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) \\ &= (-1, 0) = \phi(-1) = \hat{\phi}(-1) \end{aligned}$$

folgt $i^2 = -1$. Sei nun $z \in \mathbb{C}$ vorgegeben und $\hat{\phi}(z) = (a, b)$ mit $a, b \in \mathbb{R}$. Dann gilt

$$\begin{aligned} \hat{\phi}(a + ib) &= \hat{\phi}(a) \oplus \hat{\phi}(i) \odot \hat{\phi}(b) = \phi(a) \oplus \hat{\phi}(i) \odot \phi(b) = (a, 0) \oplus (0, 1) \odot (b, 0) \\ &= (a, 0) \oplus (0 \cdot b - 1 \cdot 0, 1 \cdot b + 0 \cdot 0) = (a, 0) \oplus (0, b) = (a, b) = \hat{\phi}(z) \end{aligned}$$

und somit $z = a + ib$, wiederum auf Grund der Injektivität von $\hat{\phi}$. Ist $z = c + id$ eine weitere Darstellung des Elements z mit $c, d \in \mathbb{R}$, dann zeigt die soeben durchgeführte Berechnung, dass $(a, b) = \hat{\phi}(a + ib) = \hat{\phi}(c + id) = (c, d)$ und somit $a = c$ und $b = d$ gilt. Damit ist die Eindeutigkeit der Darstellung nachgewiesen. \square

In § 6 werden wir mit Hilfe der dort eingeführten Faktorringe sehen, dass man sich die langwierigen Rechnungen im Beweis von Proposition 2.13 sparen kann. Darüber hinaus ermöglicht der dort vorgestellte Ansatz eine Vielzahl anderer Ringkonstruktionen. Aber auch dort ist Satz 2.12 ein wichtiger Bestandteil der Argumentation.

§ 3. Quotientenkörper und Polynomringe

Zusammenfassung. Ein Quotientenkörper eines Integritätsbereichs R ist ein Körper K , dessen Elemente die Form ab^{-1} mit $a \in R$ und $b \in R \setminus \{0_R\}$ haben. Beispielsweise ist \mathbb{Q} der Quotientenkörper von \mathbb{Z} . Die Quotientenkörper werden vor allem im hinteren Teil der Vorlesung, im Zusammenhang mit den faktoriellen Ringen und den Irreduzibilitätskriterien, eine wichtige Rolle spielen. Ein zentraler Aspekt des aktuellen Kapitels wird die Konstruktion der Quotientenkörper sein, durch Anwendung der in § 2 bereitgestellten Hilfsmittel.

Diese Konzepte werden uns auch dabei helfen, zu jedem Ring R einen zugehörigen Polynomring $R[x]$ zu konstruieren. Wir zeigen, dass sowohl Quotientenkörper als auch Polynomringe bis auf Isomorphie eindeutig bestimmt sind. Darüber hinaus werden die algebraischen Eigenschaften der Polynomringe untersucht, beispielsweise im Hinblick auf Einheiten und das Auftreten von Nullteilern. Diese Untersuchungen basieren in erster Linie auf dem Polynomgrad, einem wichtigen Merkmal der Elemente des Polynomrings.

Wichtige Grundbegriffe

- Quotientenkörper eines Integritätsbereichs
- Polynomring $R[x]$ über einem Ring R
- Grad eines Polynoms

Zentrale Sätze

- universelle Eigenschaft des Quotientenkörpers
- universelle Eigenschaft des Polynomrings
- Rechenregeln für den Polynomgrad
- für Integritätsbereiche R :
Polynomring $R[x]$ ist ebenfalls Integritätsbereich,
Einheitengruppe ist gegeben durch $R[x]^\times = R^\times$

Definition 3.1 Sei R ein Integritätsbereich. Ein Erweiterungsring $K \supseteq R$ wird **Quotientenkörper** von R genannt, wenn K ein Körper ist und $K = \{ab^{-1} \mid a, b \in R, b \neq 0_R\}$ gilt.

Beispielsweise ist der Körper \mathbb{Q} der rationalen Zahlen ein Quotientenkörper von \mathbb{Z} . Zunächst befassen wir uns mit der Frage, in welchem Sinne der Quotientenkörper eines Integritätsbereichs eindeutig ist.

Satz 3.2 (universelle Eigenschaft des Quotientenkörpers)

Sei R ein Integritätsbereich, und sei K ein Quotientenkörper von R .

- Ist $\phi : R \rightarrow S$ ein Ringhomomorphismus mit $\phi(r) \in S^\times$ für alle $r \in R \setminus \{0_R\}$, dann gibt es eine eindeutig bestimmte Fortsetzung von ϕ auf K , also einen eindeutig bestimmten Ringhomomorphismus $\hat{\phi} : K \rightarrow S$ mit $\hat{\phi}|_R = \phi$.
- Je zwei Quotientenkörper von R sind isomorph.

Beweis: zu (i) Zur Definition von $\hat{\phi}$ wählen wir für jedes Element $\alpha \in K$ ein Paar (a_α, b_α) von Elementen $a_\alpha \in R$ und $b_\alpha \in R \setminus \{0_R\}$ mit $\alpha = a_\alpha b_\alpha^{-1}$ und definieren $\hat{\phi}(\alpha) = \phi(a_\alpha)\phi(b_\alpha)^{-1}$. Zunächst zeigen wir, dass $\hat{\phi}(ab^{-1}) = \phi(a)\phi(b)^{-1}$ für alle $a \in R$ und $b \in R \setminus \{0_R\}$ gilt. Ist ein solches Paar (a, b) vorgegeben und setzen wir $\alpha = ab^{-1}$, dann gilt $ab^{-1} = a_\alpha b_\alpha^{-1}$, woraus $ab_\alpha = a_\alpha b$ und $\phi(a)\phi(b_\alpha) = \phi(a_\alpha)\phi(b)$ folgt. Multiplikation dieser Gleichung mit $\phi(b_\alpha)^{-1}\phi(b)^{-1}$ liefert

$$\hat{\phi}(\alpha) = \phi(a_\alpha)\phi(b_\alpha)^{-1} = \phi(a)\phi(b)^{-1}$$

wie gewünscht. Um nun zu zeigen, dass $\hat{\phi}$ ein Ringhomomorphismus ist, seien $\alpha, \beta \in K$ vorgegeben. Zu zeigen ist $\hat{\phi}(1_R) = 1_S$ sowie $\hat{\phi}(\alpha + \beta) = \hat{\phi}(\alpha) + \hat{\phi}(\beta)$ und $\hat{\phi}(\alpha\beta) = \hat{\phi}(\alpha)\hat{\phi}(\beta)$. Nach Definition des Quotientenkörpers K gibt es $a, c \in R$ und $b, d \in R \setminus \{0_R\}$ mit $\alpha = ab^{-1}$ und $\beta = cd^{-1}$. Es gilt $\hat{\phi}(1_R) = \hat{\phi}(1_R \cdot 1_R^{-1}) = \phi(1_R)\phi(1_R)^{-1} = 1_S \cdot 1_S^{-1} = 1_S$, weil ϕ ein Ringhomomorphismus ist. Die Verträglichkeit mit der Addition erhalten wir wegen $\alpha + \beta = ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1}$ durch die Rechnung

$$\begin{aligned} \hat{\phi}(\alpha + \beta) &= \phi(ad + bc)\phi(bd)^{-1} = \phi(ad)\phi(bd)^{-1} + \phi(bc)\phi(bd)^{-1} \\ &= \phi(a)\phi(d)\phi(b)^{-1}\phi(d)^{-1} + \phi(b)\phi(c)\phi(b)^{-1}\phi(d)^{-1} = \phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1} = \hat{\phi}(\alpha) + \hat{\phi}(\beta), \end{aligned}$$

und die Verträglichkeit mit der Multiplikation wegen $\alpha\beta = (ac)(bd)^{-1}$

$$\hat{\phi}(\alpha\beta) = \phi(ac)\phi(bd)^{-1} = \phi(a)\phi(b)^{-1}\phi(c)\phi(d)^{-1} = \hat{\phi}(\alpha)\hat{\phi}(\beta).$$

Also ist $\hat{\phi}$ tatsächlich ein Ringhomomorphismus. Wegen $\hat{\phi}(a) = \hat{\phi}(a \cdot 1_R^{-1}) = \phi(a)\phi(1_R)^{-1} = \phi(a) \cdot 1_S^{-1} = \phi(a)$ für alle $a \in R$ gilt $\hat{\phi}|_R = \phi$, also ist $\hat{\phi}$ tatsächlich eine Fortsetzung von ϕ . Die Eindeutigkeit von $\hat{\phi}$ als Fortsetzung von ϕ ist unmittelbar klar, denn für jede Fortsetzung ψ von ϕ und jedes Paar (a, b) mit $a \in R$ und $b \in R \setminus \{0_R\}$ muss $\psi(ab^{-1})\psi(b) = \psi(ab^{-1}b) = \psi(a)$ gelten, was zu $\psi(ab^{-1}) = \psi(a)\psi(b)^{-1} = \hat{\phi}(ab^{-1})$ äquivalent ist.

zu (ii) Sei K' ein weiterer Quotientenkörper von R . Dann ist die Abbildung $\phi : R \rightarrow K', a \mapsto a$ offenbar ein Ringhomomorphismus mit $\phi(a) \in (K')^\times$ für alle $a \in R \setminus \{0_R\}$, denn weil K' ein Körper ist, sind alle Element ungleich $0_R = 0_{K'}$ invertierbar. Es gibt also einen eindeutig bestimmte Fortsetzung $\hat{\phi} : K \rightarrow K'$ von ϕ . Ebenso gibt es eine eindeutig bestimmte Fortsetzung $\hat{\psi} : K' \rightarrow K$ des Homomorphismus $\psi : R \rightarrow K, a \mapsto a$ auf den Körper K' . Es ist dann $\hat{\psi} \circ \hat{\phi} : K \rightarrow K$ eine Fortsetzung von $R \rightarrow K, a \mapsto a$ auf K . Weil die Identität id_K ebenfalls eine solche Fortsetzung ist, muss auf Grund der Eindeutigkeit $\hat{\psi} \circ \hat{\phi} = \text{id}_K$ gelten. Ebenso zeigt man $\hat{\phi} \circ \hat{\psi} = \text{id}_{K'}$. Insgesamt ist damit nachgewiesen, dass $\hat{\phi}$ ein Isomorphismus und die Körper K und K' folglich isomorph sind. \square

Als nächstes werden wir nun die Existenz eines Quotientenkörpers für jeden Integritätsbereichs nachweisen. Dabei verwenden wir die am Ende von § 2 zur Verfügung gestellten Hilfsmittel. In der Linearen Algebra wurde der Begriff der *Äquivalenzrelation* eingeführt. Dabei handelt es sich um eine Relation \equiv auf einer Menge X , die reflexiv, symmetrisch und transitiv ist. Für jedes $x \in X$ nennt man $[x] = \{y \in X \mid x \equiv y\}$ die *Äquivalenzklasse* von x . Eine Teilmenge $R \subseteq X$, die aus jeder Äquivalenzklasse genau ein Element enthält, nennt man ein *Repräsentantensystem* der Äquivalenzklassen.

Sei nun R ein Integritätsbereich. Wir definieren auf der Menge $X_R = R \times (R \setminus \{0_R\})$ eine Relation \sim durch die Festlegung $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ für alle $(a, b), (c, d) \in X_R$.

Lemma 3.3 Die Relation \sim ist eine Äquivalenzrelation auf $R \times (R \setminus \{0_R\})$.

Beweis: Für jedes Paar $(a, b) \in X_R$ gilt $ab = ab$ und somit $(a, b) \sim (a, b)$. Deshalb ist die Relation reflexiv. Die Äquivalenz

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c, d) \sim (a, b)$$

für beliebige Paare $(a, b), (c, d) \in X_R$ zeigt, dass die Relation auch symmetrisch ist. Zum Nachweis der Transitivität seien $(a, b), (c, d)$ und (e, f) aus X_R mit $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$ vorgegeben. Dann gilt $ad = bc$ und $cf = de$. Es folgt $adf = bcf = bde$, und mit der Kürzungsregel für Integritätsbereiche folgt $af = be$, also $(a, b) \sim (e, f)$. Dies zeigt, dass die Relation auch transitiv ist. \square

Für jedes Paar $(a, b) \in X_R$ bezeichnen wir mit $[a, b]$ die zugehörige Äquivalenzklasse, und die Menge der Äquivalenzklassen mit X_R/\sim . Bei der Konstruktion des Quotientenkörpers orientieren wir uns nun an den herkömmlichen Regeln

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{und} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

für das Bruchrechnen.

Proposition 3.4 Auf der Menge $\hat{R} = X_R/\sim$ der Äquivalenzklassen der Relation \sim auf X_R gibt es eindeutig bestimmte Verknüpfungen \oplus und \odot mit

$$[a, b] \oplus [c, d] = [ad + bc, bd] \quad \text{und} \quad [a, b] \odot [c, d] = [ac, bd]$$

für alle $(a, b), (c, d) \in X_R$, und \hat{R} bildet mit diesen Verknüpfungen einen Körper.

Beweis: Wie in der Algebra-Vorlesung wurde, genügt es für die Existenz und Eindeutigkeit der Verknüpfungen nachzuweisen, dass für alle $(a, b), (a', b'), (c, d)$ und (c', d') aus $(a, b) \sim (a', b')$ und $(c, d) \sim (c', d')$ jeweils $[ad + bc, bd] = [a'd' + b'c', b'd']$ und $[ac, bd] = [a'c', b'd']$ folgt. Beides ist erfüllt, denn wegen $(a, b) \sim (a', b')$ und $(c, d) \sim (c', d')$ gilt $ab' = a'b$ und $cd' = c'd$, und somit auch

$$(ad + bc)(b'd') = ab'dd' + bb'cd' = a'bdd' + bb'c'd = (a'd' + b'c')(bd)$$

und $(ac)(b'd') = ab'cd' = a'bc'd = (a'c')(bd)$, was zu $[ad + bc, bd] = [a'd' + b'c', b'd']$ und $[ac, bd] = [a'c', b'd']$ äquivalent ist. Im nächsten Schritt zeigen wir, dass (\hat{R}, \oplus, \odot) ein Ring ist, mit $0_{\hat{R}} = [0_R, 1_R]$ als Null- und $1_{\hat{R}} = [1_R, 1_R]$ als Einselement. Wir beginnen mit dem Nachweis, dass (\hat{R}, \oplus) eine abelsche Gruppe ist. Seien dazu $[a, b], [c, d]$ und $[e, f]$ in \hat{R} vorgegeben. Wegen $[a, b] \oplus [c, d] = [ad + bc, bd] = [cb + da, db] = [c, d] \oplus [a, b]$ ist die Verknüpfung kommutativ, und wegen

$$\begin{aligned} [a, b] \oplus ([c, d] \oplus [e, f]) &= [a, b] \oplus [cf + de, df] = [adf + bcf + bde, bdf] = \\ &[ad + bc, bd] \oplus [e, f] = ([a, b] \oplus [c, d]) \oplus [e, f]. \end{aligned}$$

ist sie auch assoziativ. Die Rechnung $[a, b] \oplus 0_{\hat{R}} = [a, b] \oplus [0_R, 1_R] = [a \cdot 1_R + b \cdot 0_R, b \cdot 1_R] = [a, b]$ zeigt, dass $0_{\hat{R}} = [0_R, 1_R]$ tatsächlich ein Neutralelement von (\hat{R}, \oplus) ist. Schließlich gilt noch $[a, b] \oplus [-a, b] = [ab + b(-a), b^2] = [0_R, b] = [0_R, 1_R] = 0_{\hat{R}}$, wobei im vorletzten Schritt verwendet wurde, dass $(0_R, b) \sim (0, 1_R)$ gilt. Also ist $[-a, b]$ in (\hat{R}, \oplus) jeweils das Inverse von $[a, b]$.

Nun zeigen wir, dass (\hat{R}, \odot) ein Monoid ist. Wegen $[a, b] \odot [c, d] = [ac, bd] = [ca, db] = [c, d] \odot [a, b]$ ist die Verknüpfung \odot kommutativ, und die Assoziativität ergibt sich aus der Rechnung $[a, b] \odot ([c, d] \odot [e, f]) = [a, b] \odot [ce, df] = [a(ce), b(df)] = [(ac)e, (bd)f] = [ac, bd] \odot [e, f] = ([a, b] \odot [c, d]) \odot [e, f]$. Dass $1_{\hat{R}} = [1_R, 1_R]$ in (\hat{R}, \odot) ein Neutralelement ist, ergibt sich aus der Rechnung $[a, b] \cdot [1_R, 1_R] = [a \cdot 1_R, b \cdot 1_R] = [a, b]$. Es fehlt noch der Nachweis des Distributivgesetzes. Dieses erhält man durch

$$\begin{aligned} [a, b] \odot ([c, d] \oplus [e, f]) &= [a, b] \odot [cf + de, df] = [acf + ade, bdf] = \\ [acbf + bdae, b^2df] &= [ac, bd] \oplus [ae, bf] = [a, b] \odot [c, d] \oplus [a, b] \odot [e, f]. \end{aligned}$$

Damit ist der Beweis der Ringeigenschaften abgeschlossen. Darüber hinaus ist (\hat{R}, \oplus, \odot) sogar ein Körper. Ist nämlich $\alpha = [a, b]$ ein Element von \hat{R} mit $[a, b] \neq [0_R, 1_R]$, dann ist $[b, a]$ wegen $b_R \neq 0_R$ ein Kehrwert von α , denn wegen $(ab, ab) \sim (1_R, 1_R)$ gilt $[a, b] \odot [b, a] = [ab, ba] = [1_R, 1_R]$. Also sind sämtliche Elemente der Menge $\hat{R} \setminus \{0_{\hat{R}}\}$ Einheiten. Außerdem ist \hat{R} kein Nullring. Denn andernfalls würde $[0_R, 1_R] = 0_{\hat{R}} = 1_{\hat{R}} = [1_R, 1_R]$ gelten, woraus $(0_R, 1_R) \sim (1_R, 1_R)$ und $0_R \cdot 1_R = 1_R \cdot 1_R$, also $0_R = 1_R$ folgen würde, im Widerspruch dazu, dass der Ring R als Integritätsbereich kein Nullring ist. \square

Nach diesen Vorbereitungen können wir nun zeigen

Satz 3.5 Zu jedem Integritätsbereich existiert ein Quotientenkörper.

Beweis: Sei (\hat{R}, \oplus, \odot) der in Satz 3.4 definierte Körper. Durch die Abbildung $\phi_R : R \rightarrow \hat{R}, a \mapsto [a, 1_R]$ ist ein Monomorphismus von Ringen definiert. Denn es gilt $\phi_R(1_R) = [1_R, 1_R] = 1_{\hat{R}}$, und für alle $a, b \in R$ ist $\phi_R(a + b) = [a + b, 1_R] = [a, 1_R] \oplus [b, 1_R] = \phi_R(a) \oplus \phi_R(b)$ und $\phi_R(ab) = [ab, 1_R] = [a, 1_R] \odot [b, 1_R] = \phi_R(a) \odot \phi_R(b)$. Außerdem ist ϕ injektiv. Ist nämlich $a \in R$ mit $\phi_R(a) = 0_{\hat{R}}$, dann folgt $[a, 1_R] = \phi_R(a) = [0_R, 1_R]$ und somit $a \cdot 1_R = 0_R \cdot 1_R$, also $a = 0_R$. Nach Satz 2.12 existiert nun ein Erweiterungsring K von R und ein Isomorphismus $\hat{\phi}_R : K \rightarrow \hat{R}$ von Ringen mit $\hat{\phi}_R|_R = \phi_R$. Um zu zeigen, dass K nun ein Quotientenkörper von R ist, müssen wir für ein beliebig vorgegebenes Element $\alpha \in K$ zeigen, dass ein Paar $(a, b) \in X_R$ mit $\alpha = ab^{-1}$ existiert. Wegen $\hat{\phi}_R(\alpha) \in \hat{K}$ gibt es ein Paar (a, b) in X_R mit $\hat{\phi}_R(\alpha) = [a, b]$. Auf Grund der Eigenschaft $\hat{\phi}_R|_R = \phi_R$ von $\hat{\phi}_R$ erhalten wir

$$\hat{\phi}_R(\alpha) = [a, b] = [a, 1_R] \odot [b, 1_R]^{-1} = \phi_R(a) \phi_R(b)^{-1} = \hat{\phi}_R(a) \hat{\phi}_R(b)^{-1} = \hat{\phi}_R(ab^{-1})$$

wobei das Element ab^{-1} im letzten Schritt im Körper K gebildet wird. Auf Grund der Injektivität von $\hat{\phi}_R$ folgt $\alpha = ab^{-1}$, wie gewünscht. \square

Kommen wir nun zum zweiten Thema dieses Kapitels, den Polynomringen. Die folgende Definition ist bereits aus der Linearen Algebra bekannt.

Definition 3.6 Sei R ein Ring. Ein Erweiterungsring S von R wird **Polynomring** über R genannt, wenn es ein ausgezeichnetes Element $x \in S$ gibt mit der Eigenschaft, dass für jedes Element $f \in R[x] \setminus \{0_R\}$ ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, \dots, a_n \in R$ existieren, so dass $a_n \neq 0$ ist und f in der Form

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \text{dargestellt werden kann.}$$

Das ausgezeichnete Element x nennt man die **Variable** (oder Unbestimmte) des Polynomrings. Für einen Polynomring S über einem Ring R mit der Variablen x wird in der Regel die Bezeichnung $R[x]$ verwendet. Die Elemente von $R[x]$ heißen **Polynome** über dem Ring R . Man bezeichnet die Zahl n in der Definition als den Grad $\text{grad}(f)$ des Polynoms f . Das Polynom $a_n x^n$ ist der **Leitterm**, das Element $a_n \in R$ der **Leitkoeffizient** von f .

Es sei ausdrücklich darauf hingewiesen, dass das Element x im Polynomring $R[x]$ kein Element von R ist, sofern es sich bei R nicht um einen Nullring handelt. Wäre $x = 0_R$, dann würde $1_R = x + 1_R$ gelten, was im Widerspruch dazu steht, dass jedes Element von $R[x]$ ungleich Null *genau eine* Darstellung als Polynomausdruck besitzt. Im Fall $x \in R \setminus \{0_R\}$ erhalten wir ebenfalls einen Widerspruch zu dieser Eindeutigkeit, denn dann könnte x sowohl als Polynom vom Grad 0 (mit $a_0 = x$) als auch als Polynom vom Grad 1 aufgefasst werden (in der Form $1_R \cdot x + 0_R$, also mit $a_0 = 0_R$ und $a_1 = 1_R$).

Für die folgenden Ausführungen ist es wichtig, sich noch einmal ins Gedächtnis zu rufen, wie Polynome addiert und multipliziert werden. Seien $f, g \in R[x]$ mit $f = \sum_{k=0}^m a_k x^k$ und $g = \sum_{\ell=0}^n b_\ell x^\ell$. Bei der Addition bietet es sich an, die Koeffizienten a_k und b_ℓ auch für $k > m$ und $\ell > n$ zu definieren, indem man $a_k = 0$ und $b_\ell = 0$ setzt. Die Polynome können dann in der Form

$$f = \sum_{k \in \mathbb{N}_0} a_k x^k \quad \text{und} \quad g = \sum_{\ell \in \mathbb{N}_0} b_\ell x^\ell$$

dargestellt werden, und die Summe hat dann die Form

$$f + g = \sum_{r \in \mathbb{N}_0} (a_r + b_r) x^r.$$

Das Produkt von f und g erhält man durch die Rechnung

$$fg = \left(\sum_{k=0}^m a_k x^k \right) \left(\sum_{\ell=0}^n b_\ell x^\ell \right) = \sum_{k=0}^m \sum_{\ell=0}^n a_k b_\ell x^{k+\ell} = \sum_{r=0}^{m+n} \left(\sum_{\substack{k, \ell \geq 0 \\ k+\ell=r}} a_k b_\ell \right) x^r = \sum_{r=0}^{m+n} \left(\sum_{\ell=0}^r a_{r-\ell} b_\ell \right) x^r.$$

Wie bei den Quotientenkörpern beschäftigen wir uns zunächst mit der Frage der Eindeutigkeit.

Satz 3.7 (universelle Eigenschaft des Polynomrings)

Für jeden Ringhomomorphismus $\phi : R \rightarrow S$ und jedes $a \in S$ gibt es einen eindeutig bestimmten Ringhomomorphismus $\hat{\phi} : R[x] \rightarrow S$ mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}(x) = a$.

Beweis: Zunächst beweisen wir die Existenz des Homomorphismus $\hat{\phi}$. Jedes Element $0_R \neq f \in R[x]$ besitzt eine Darstellung der Form

$$f = \sum_{k=0}^n a_k x^k \quad \text{mit} \quad n \in \mathbb{N}_0, \quad a_0, \dots, a_n \in R \quad \text{und} \quad a_n \neq 0_R,$$

und diese ist eindeutig bestimmt. Wir definieren eine Abbildung $\hat{\phi} : R[x] \rightarrow S$, indem wir $\hat{\phi}(0_R) = 0_S$ und $\hat{\phi}(f) = \sum_{k=0}^n \phi(a_k) a^k$ setzen. Zu zeigen ist, dass wir auf diese Weise einen Ringhomomorphismus definiert haben. Da das Element 1_R als Polynom in $R[x]$ vom Grad Null aufgefasst werden kann, gilt zunächst $\hat{\phi}(1_R) = \phi(1_R) = 1_S$ nach Definition von $\hat{\phi}$. Seien nun $f, g \in R[x]$ vorgegeben. Ist eines dieser Elemente gleich Null, dann sind die Gleichungen $\hat{\phi}(f + g) = \hat{\phi}(f) + \hat{\phi}(g)$ und $\hat{\phi}(fg) = \hat{\phi}(f)\hat{\phi}(g)$ wegen $\hat{\phi}(0_R) = 0_S$ offensichtlich erfüllt. Wir können also $f, g \neq 0_R$ annehmen und damit voraussetzen, dass f und g Darstellungen der Form

$$f = \sum_{k=0}^m a_k x^k \quad \text{und} \quad g = \sum_{\ell=0}^n b_\ell x^\ell$$

besitzen, mit $m, n \in \mathbb{N}_0$, $a_k, b_\ell \in R$ und $a_m, b_n \neq 0_R$. Wie oben setzen wir $a_k = 0_R$ für $k > m$ und $b_\ell = 0$ für $\ell > n$. Auf Grund der Rechenregeln für die Addition und Multiplikation von Polynomen gilt dann

$$\begin{aligned}\hat{\phi}(f+g) &= \hat{\phi}\left(\sum_{r \in \mathbb{N}_0} (a_r + b_r)x^r\right) = \sum_{r \in \mathbb{N}_0} \phi(a_r + b_r)a^r = \sum_{r \in \mathbb{N}_0} (\phi(a_r) + \phi(b_r))a^r \\ &= \sum_{k \in \mathbb{N}_0} \phi(a_k)a^k + \sum_{\ell \in \mathbb{N}_0} \phi(b_\ell)a^\ell = \hat{\phi}\left(\sum_{k \in \mathbb{N}_0} a_k x^k\right) + \hat{\phi}\left(\sum_{\ell \in \mathbb{N}_0} b_\ell x^\ell\right) = \hat{\phi}(f) + \hat{\phi}(g)\end{aligned}$$

sowie

$$\hat{\phi}(fg) = \hat{\phi}\left(\sum_{r=0}^{m+n} \left(\sum_{\ell=0}^r a_{r-\ell} b_\ell\right) x^r\right) = \sum_{r=0}^{m+n} \left(\sum_{\ell=0}^r \phi(a_{r-\ell})\phi(b_\ell)\right) a^r = \left(\sum_{k=0}^m \phi(a_k)a^k\right) \left(\sum_{\ell=0}^n \phi(b_\ell)a^\ell\right) = \hat{\phi}(f)\hat{\phi}(g).$$

Für den Beweis der *Eindeutigkeit* nehmen wir an, dass neben $\hat{\phi}$ durch ψ ein weiterer Ringhomomorphismus $R[x] \rightarrow S$ mit $\psi(x) = a$ und $\psi|_R = \phi$ gegeben ist. Auf Grund der Homomorphismus-Eigenschaft gilt $\hat{\phi}(0_R) = 0_S = \psi(0_R)$. Sei nun $f \in R[x]$ ein Element mit $f \neq 0_{R[x]}$, also $f = \sum_{k=0}^n a_k x^k$ mit $a_0, \dots, a_n \in R$ und $a_n \neq 0_R$. Es gilt dann

$$\hat{\phi}(f) = \hat{\phi}\left(\sum_{k=0}^m a_k x^k\right) = \sum_{k=0}^m \hat{\phi}(a_k x^k) = \sum_{k=0}^m \phi(a_k)a^k = \sum_{k=0}^m \psi(a_k x^k) = \psi\left(\sum_{k=0}^m a_k x^k\right) = \psi(f).$$

Damit ist die Eindeutigkeit von $\hat{\phi}$ bewiesen. □

Ist $S = R$ oder ein Erweiterungsring von R , dann bezeichnet man den eindeutig bestimmten Homomorphismus $\hat{\phi}$ aus 3.7 als den **Auswertungshomomorphismus** an der Stelle a .

Folgerung 3.8 Je zwei Polynomringe über einem Ring R sind isomorph.

Beweis: Nehmen wir an, dass $R[x] \supseteq R$ und $\tilde{R}[y] \supseteq R$ beides Polynomringe über R sind. Nach Satz 3.7 gibt es eindeutig bestimmte Homomorphismen $\phi : R[x] \rightarrow \tilde{R}[y]$ und $\psi : \tilde{R}[y] \rightarrow R[x]$ mit $\phi|_R = \psi|_R = \text{id}_R$ sowie $\phi(x) = y$ und $\psi(y) = x$. Damit ist $\psi \circ \phi$ ein Ringhomomorphismus $R[x] \rightarrow R[x]$ mit $(\psi \circ \phi)|_R = \text{id}_R$ und $(\psi \circ \phi)(x) = x$. Aber auch der Homomorphismus $\text{id}_{R[x]}$ besitzt diese Eigenschaft. Auf Grund der Eindeutigkeit muss also $\psi \circ \phi = \text{id}_{R[x]}$ gelten. Genauso beweist man die Gleichung $\phi \circ \psi = \text{id}_{\tilde{R}[y]}$. Also ist ϕ ein Isomorphismus von Ringen. □

Kommen wir nun zum Beweis der Existenz eines Polynomrings über jedem Ring R . Ein Polynom der Form $a_0 + a_1 x + \dots + a_n x^n$ ist bestimmt durch die Folge a_0, a_1, \dots, a_n seiner Koeffizienten, also durch die Abbildung $k \mapsto a_k$ (wobei k für $k > n$ auf 0_R abgebildet wird). Diese Beobachtung führt uns auf die Idee, Polynome durch Abbildungen darzustellen.

Es sei P_R die Menge aller Abbildungen $f : \mathbb{N}_0 \rightarrow R$ mit der Eigenschaft, dass $f(k) = 0_R$ für alle bis auf endlich viele $k \in \mathbb{N}_0$ gilt. Zur Definition geeigneter Verknüpfungen orientieren wir uns an den Rechenregeln zur Addition und Multiplikation von Polynomen. Dementsprechend definieren wir auf P_R zwei Verknüpfungen \oplus und \odot durch

$$(f \oplus g)(n) = f(n) + g(n) \quad \text{und} \quad (f \odot g)(n) = \sum_{k=0}^n f(n-k)g(k) = \sum_{k+\ell=n} f(\ell)g(k).$$

Für jedes $a \in R$ sei $\tilde{a} \in P_R$ das Element gegeben durch $\tilde{a}(0) = a$ und $\tilde{a}(n) = 0_R$ für alle $n \geq 1$. Diese Elemente sollen den konstanten Polynomen $a \in R$ entsprechen. Außerdem definieren wir ein Element $\tilde{x} \in P_R$ durch $\tilde{x}(1) = 1_R$ und $\tilde{x}(n) = 0_R$ für $n \neq 1$. Dieses Element übernimmt die Rolle der Variablen x im Polynomring $R[x]$.

Lemma 3.9 Das Tripel (P_R, \oplus, \odot) ist ein Ring, mit $\tilde{0}$ als Null- und $\tilde{1}$ als Einselement.

Beweis: Zunächst überprüfen wir, dass (P_R, \oplus) eine abelsche Gruppe ist. Seien $f, g, h \in P_R$ vorgegeben. Es gilt

$$\begin{aligned} ((f \oplus g) \oplus h)(n) &= (f \oplus g)(n) + h(n) = (f(n) + g(n)) + h(n) = f(n) + (g(n) + h(n)) = \\ &= f(n) + (g \oplus h)(n) = (f \oplus (g \oplus h))(n) \end{aligned}$$

für jedes $n \in \mathbb{N}_0$ und somit $(f \oplus g) \oplus h = f \oplus (g \oplus h)$ für alle $f, g, h \in P_R$. Ebenso gilt $(f \oplus g)(n) = f(n) + g(n) = g(n) + f(n) = (g \oplus f)(n)$ für alle $n \in \mathbb{N}_0$ und somit $f \oplus g = g \oplus f$.

Für jedes $n \in \mathbb{N}_0$ gilt $(f \oplus \tilde{0})(n) = f(n) + \tilde{0}(n) = f(n) + 0_R = f(n)$, also $f \oplus \tilde{0} = f$. Sei nun die Abbildung $(-f) : \mathbb{N}_0 \rightarrow R$ definiert durch $(-f)(n) = -f(n)$ für alle $n \in \mathbb{N}_0$. Dann gilt $-f \in P_R$, und für alle $n \in \mathbb{N}_0$ ist $(f \oplus (-f))(n) = f(n) + (-f)(n) = f(n) + (-f(n)) = 0_R = \tilde{0}(n)$. Wir erhalten $f \oplus (-f) = \tilde{0}$. Insgesamt ist (P_R, \oplus) also tatsächlich eine abelsche Gruppe.

Als nächstes beweisen wir für die Verknüpfung \odot das Assoziativgesetz. Seien dazu $f, g, h \in P_R$ vorgegeben. Für alle $n \in \mathbb{N}_0$ gilt

$$\begin{aligned} ((f \odot g) \odot h)(n) &= \sum_{k+l=n} (f \odot g)(k)h(\ell) = \sum_{k+l=n} \left(\sum_{i+j=k} f(i)g(j) \right) h(\ell) = \\ &= \sum_{k+l=n} \sum_{i+j=k} f(i)g(j)h(\ell) = \sum_{i+j+l=n} f(i)g(j)h(\ell). \end{aligned}$$

Ebenso erhalten wir

$$\begin{aligned} (f \odot (g \odot h))(n) &= \sum_{i+k=n} f(i)(g \odot h)(k) = \sum_{i+k=n} f(i) \left(\sum_{j+l=k} g(j)h(\ell) \right) = \\ &= \sum_{i+k=n} \sum_{j+l=k} f(i)g(j)h(\ell) = \sum_{i+j+k=n} f(i)g(j)h(\ell). \end{aligned}$$

Insgesamt gilt also $(f \odot g) \odot h = f \odot (g \odot h)$. Nun überprüfen wir, dass $\tilde{1}$ in (P_R, \odot) das Neutralelement ist. Wegen $\tilde{1}(k) = 0_R$ für $k > 0$ gilt für alle $n \in \mathbb{N}_0$ jeweils

$$(f \odot \tilde{1})(n) = \sum_{k=0}^n f(n-k)\tilde{1}(k) = f(n-0) \cdot 1 = f(n)$$

und somit $f \odot \tilde{1} = f$. Zum Schluss müssen wir noch das Distributivgesetz überprüfen. Wieder seien $f, g, h \in P_R$ vorgegeben. Für jedes $n \in \mathbb{N}_0$ gilt

$$\begin{aligned} (f \odot (g \oplus h))(n) &= \sum_{k=0}^n f(n-k)(g \oplus h)(k) = \sum_{k=0}^n f(n-k)(g(k) + h(k)) = \\ &= \sum_{k=0}^n f(n-k)g(k) + \sum_{k=0}^n f(n-k)h(k) = (f \odot g)(n) + (f \odot h)(n) = ((f \odot g) \oplus (f \odot h))(n) \end{aligned}$$

also tatsächlich $f \odot (g \oplus h) = (f \odot g) \oplus (f \odot h)$. □

Lemma 3.10 Sei $a \in R$ und $m \in \mathbb{N}_0$. Dann gilt $(\tilde{a} \odot \tilde{x}^m)(m) = a$, und $(\tilde{a} \odot \tilde{x}^m)(n) = 0_R$ für alle $n \in \mathbb{N}_0 \setminus \{m\}$.

Beweis: Wir beweisen durch vollständige Induktion über $m \in \mathbb{N}_0$, dass $x^m(m) = 1_R$ und für alle $n \neq \mathbb{N}_0 \setminus \{m\}$ jeweils $\tilde{x}^m(n) = 0_R$ gilt. Für $m = 0$ ist $\tilde{x}^0 = \tilde{1}$, und es gilt $\tilde{1}(0) = 1_R$ und $\tilde{1}(n) = 0_R$ für alle $n > 0$. Sei nun $m \in \mathbb{N}_0$ vorgegeben, und setzen wir die Aussage für dieses m voraus. Zunächst gilt

$$\begin{aligned} \tilde{x}^{m+1}(m+1) &= (\tilde{x}^m \odot \tilde{x})(m+1) = \sum_{k=0}^{m+1} (\tilde{x}^m)(m+1-k) \tilde{x}(k) = \tilde{x}^m(m+1-1) \tilde{x}(1) \\ &= \tilde{x}^m(m) \tilde{x}(1) = 1_R \cdot 1_R = 1_R, \end{aligned}$$

wobei wir im dritten und fünften Schritt die definierende Eigenschaft von \tilde{x} und im fünften Schritt außerdem die Induktionsvoraussetzung angewendet haben. Für jedes $n \in \mathbb{N}_0 \setminus \{m+1\}$ gilt dagegen $n-1 \neq m$ und somit

$$\tilde{x}^{m+1}(n) = (\tilde{x}^m \odot \tilde{x})(n) = \sum_{k=0}^{m+1} (\tilde{x}^m)(n-k) \tilde{x}(k) = \tilde{x}^m(n-1) \tilde{x}(1) = 0_R \cdot 1_R = 0_R.$$

Damit ist der Induktionsbeweis abgeschlossen. Für jedes $m \in \mathbb{N}$ gilt nun außerdem

$$(\tilde{a} \odot x^m)(n) = \sum_{k=0}^n \tilde{a}(n-k) x^m(k) = \tilde{a}(0) x^m(n) = a \cdot x^m(n),$$

also $(\tilde{a} \odot x^m)(n) = a \cdot 1_R = a$ im Fall $n = m$ und $(\tilde{a} \odot x^m)(n) = a \cdot 0_R = 0_R$ im Fall $n \neq m$. \square

Lemma 3.11 Für jedes $f \in P_R \setminus \{\tilde{0}\}$ gilt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, a_1, \dots, a_n \in R$, so dass $a_n \neq 0_R$ und

$$f = (\tilde{a}_n \odot \tilde{x}^n) \oplus \dots \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0 \quad \text{gilt.}$$

Beweis: Zum Nachweis der Existenz sei $f \in P_R \setminus \{\tilde{0}\}$ vorgegeben und $n \in \mathbb{N}_0$ maximal mit der Eigenschaft $f(n) \neq 0_R$. Sei $a_k = f(k)$ für $0 \leq k \leq n$ und $g = (\tilde{a}_n \odot \tilde{x}^n) \oplus \dots \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0$. Dann gilt für $0 \leq k \leq n$ jeweils

$$g(k) = \sum_{\ell=0}^n (\tilde{a}_\ell \odot \tilde{x}^\ell)(k) = a_k = f(k),$$

wobei im zweiten Schritt Lemma 3.10 angewendet wurde. Für $k > n$ gilt $g(k) = 0_R = f(k)$, insgesamt also $f = g$. Für den Nachweis der Eindeutigkeit seien $m \in \mathbb{N}_0$ und $b_0, \dots, b_m \in R$, so dass $b_m \neq 0_R$ und

$$f = (\tilde{b}_m \odot \tilde{x}^m) \oplus \dots \oplus (\tilde{b}_1 \odot \tilde{x}) \oplus \tilde{b}_0 \quad \text{erfüllt ist.}$$

Wie im letzten Absatz überprüft man, dass $f(k) = b_k$ für $0 \leq k \leq m$ und $f(k) = 0_R$ für $k > m$ gilt. Somit ist m die maximale Zahl mit der Eigenschaft $f(m) \neq 0_R$, und es folgt $m = n$. Außerdem gilt $b_k = f(k) = a_k$ für $0 \leq k \leq n$. \square

Satz 3.12 Zu jedem Ring R existiert ein Polynomring über R .

Beweis: Sei $\phi : R \rightarrow P_R$ definiert durch $\phi(a) = \tilde{a}$ für alle $a \in R$. Diese Abbildung ist ein Homomorphismus von Ringen. Denn ϕ bildet 1_R auf das Einselement $\tilde{1}$ von P_R ab. Für beliebige $a, b \in R$ gilt außerdem $\phi(a+b) = \phi(a) \oplus \phi(b)$ und $\phi(ab) = \phi(a) \odot \phi(b)$. Denn es gilt $\phi(a+b)(0) = a+b = \phi(a)(0) + \phi(b)(0) = (\phi(a) \oplus \phi(b))(0)$ und $\phi(ab)(0) = ab = \phi(a)(0)\phi(b)(0) = (\phi(a) \odot \phi(b))(0)$, und für jedes $n \in \mathbb{N}$ gilt $\phi(a+b)(n) = 0_R = (\phi(a) \oplus \phi(b))(n)$ sowie $\phi(ab)(n) = \phi(a)(n) \cdot \phi(b)(n) = (\phi(a) \odot \phi(b))(n)$. Außerdem ist ϕ injektiv. Ist nämlich $\phi(a) = \tilde{0}$ für ein $a \in R$, dann folgt $a = \tilde{a}(0) = \phi(a)(0) = \tilde{0}(0) = 0_R$.

Wir können nun Satz 2.12 auf den Monomorphismus ϕ anwenden. Wir erhalten einen Erweiterungsring von R , den wir mit $R[x]$ bezeichnen, und einen Isomorphismus $\hat{\phi} : R[x] \rightarrow P_R$ mit $\hat{\phi}|_R = \phi$. Außerdem setzen wir $x = \hat{\phi}^{-1}(\tilde{x})$. Wegen $\hat{\phi}|_R = \phi$ gilt $\hat{\phi}(a) = \phi(a) = \tilde{a}$ für alle $a \in R$. Sei nun $f \in R[x] \setminus \{0\}$ beliebig vorgeben und $\tilde{f} = \hat{\phi}(f)$. Nach Lemma 3.11 gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, \dots, a_n \in R$ mit $a_n \neq 0_R$, so dass

$$\tilde{f} = (\tilde{a}_n \odot \tilde{x}^n) \oplus \dots \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0 \quad \text{gilt.}$$

Durch Anwendung von $\hat{\phi}^{-1}$ auf beide Seiten der Gleichung erhalten wir auf Grund der Homomorphismus-Eigenschaft die Gleichung $f = a_n x^n + \dots + a_1 x + a_0$. Aus der Eindeutigkeit von n und a_0, \dots, a_n für das Element \tilde{f} folgt auch die Eindeutigkeit für das Element f . Nehmen wir nämlich an, dass auch $f = b_m x^m + \dots + b_1 x + b_0$ erfüllt ist, mit $m \in \mathbb{N}_0$ und b_0, b_1, \dots, b_m . Dann folgt

$$(\tilde{a}_n \odot \tilde{x}^n) \oplus \dots \oplus (\tilde{a}_1 \odot \tilde{x}) \oplus \tilde{a}_0 = \tilde{f} = \hat{\phi}(f) = (\tilde{b}_m \odot \tilde{x}^m) \oplus \dots \oplus (\tilde{b}_1 \odot \tilde{x}) \oplus \tilde{b}_0,$$

und die Eindeutigkeitsaussage in 3.11, angewendet auf das Element $\tilde{f} \in P_R \setminus \{\tilde{0}\}$, liefert die Gleichungen $m = n$ und $a_k = b_k$ für $0 \leq k \leq n$. \square

Zum Abschluss des Kapitels befassen wir uns noch mit den algebraischen Eigenschaften der Polynomringe.

Proposition 3.13 Sei R ein Ring und $R[x]$ ein Polynomring über R .

(i) Sind $0_R \neq f, g \in R[x]$ und gilt auch $f + g \neq 0_R$ und $fg \neq 0_R$, dann folgt

$$\text{grad}(f + g) \leq \max\{\text{grad}(f), \text{grad}(g)\} \quad \text{und} \quad \text{grad}(fg) \leq \text{grad}(f) + \text{grad}(g).$$

(ii) Ist R ein Integritätsbereich, dann gilt dasselbe auch für den Ring $R[x]$. In diesem Fall gilt sogar $\text{grad}(fg) = \text{grad}(f) + \text{grad}(g)$ für alle $f, g \in R[x]$ mit $f, g \neq 0_R$.

Beweis: zu (i) Sei $m = \text{grad}(f)$ und $n = \text{grad}(g)$. Dann können wir f und g in der Form $f = \sum_{k=0}^m a_k x^k$ und $g = \sum_{\ell=0}^n b_\ell x^\ell$ darstellen, mit geeigneten $a_k, b_\ell \in R$. Wie zuvor definieren wir die Koeffizienten von a_k und b_ℓ auch für $k > m$ und $\ell > n$, indem wir sie auf Null setzen. Wie wir oben festgestellt haben, gilt $f + g = \sum_{r \in \mathbb{N}_0} (a_r + b_r) x^r$. Dabei ist $a_r + b_r \neq 0_R$ nur möglich, wenn $a_r \neq 0_R$ oder $b_r \neq 0_R$ gilt, also wenn $r \leq m$ oder $r \leq n$ ist, was mit $r \leq \max\{m, n\}$ gleichbedeutend ist. Daraus folgt $\text{grad}(f + g) \leq \max\{m, n\} = \max\{\text{grad}(f), \text{grad}(g)\}$. Ebenso zeigt die Gleichung $fg = \sum_{r=0}^{m+n} (\sum_{\ell=0}^r a_{r-\ell} b_\ell) x^r$, dass $\text{grad}(fg) \leq m + n = \text{grad}(f) + \text{grad}(g)$ gilt.

zu (ii) Der Koeffizient von x^{m+n} des Polynoms fg ist gegeben durch $\sum_{\ell=0}^{m+n} a_{m+n-\ell} b_\ell = a_m b_n$, denn für $\ell > n$ ist $b_\ell = 0_R$, und für $\ell < n$ ist $m + n - \ell > m$ und somit $a_{m+n-\ell} = 0_R$. Ist R ein Integritätsbereich, dann folgt aus $a_m \neq 0_R$ und $b_n \neq 0_R$ auch $a_m b_n \neq 0_R$. Insbesondere ist das Produkt zweier Polynome ungleich Null wiederum ungleich Null; außerdem ist mit R auch der Polynomring $R[x]$ kein Nullring. Dies zeigt, dass auch $R[x]$ ein Integritätsbereich ist. \square

Folgerung 3.14 Sei R ein Integritätsbereich. Dann gilt $R[x]^\times = R^\times$, d.h. die Einheitengruppe des Polynomrings $R[x]$ stimmt mit der Einheitengruppe des Grundrings R überein.

Beweis: Sei $a \in R^\times$. Dann gibt es ein $b \in R$ mit $ab = 1_R = 1_{R[x]}$. Dies zeigt, dass jede Einheit in R auch eine Einheit in $R[x]$ ist. Sei nun umgekehrt f eine Einheit in $R[x]$. Dann gibt es ein Element $g \in R[x]$ mit $fg = 1_{R[x]} = 1_R$. Mit Proposition 3.13 (ii) erhalten wir $\text{grad}(f) + \text{grad}(g) = \text{grad}(fg) = \text{grad}(1_R) = 0$, und wegen $\text{grad}(f), \text{grad}(g) \geq 0$ folgt daraus $\text{grad}(f) = \text{grad}(g) = 0$. Also sind f und g beides Elemente des Grundrings R . Aus der Gleichung $fg = 1$ folgt nun, dass f in R^\times enthalten ist. \square

Man beachte, dass die Folgerung für Nicht-Integritätsbereiche im Allgemeinen falsch ist. Hier kann es in $R[x]^\times$ auch Elemente mit Polynomgrad ≥ 1 geben. Im Restklassenring $\mathbb{Z}/4\mathbb{Z}$ gilt beispielsweise $\bar{2} \cdot \bar{2} = \bar{0}$, das Element $\bar{2}$ ist also ein Nullteiler. Daraus folgt, dass das Polynom $f = \bar{2}x + \bar{1}$ im Polynomring $\mathbb{Z}/4\mathbb{Z}[x]$ eine Einheit ist, denn es gilt $f \cdot f = (\bar{2}x + \bar{1})(\bar{2}x + \bar{1}) = (\bar{2} \cdot \bar{2})x^2 + (\bar{2} + \bar{2})x + \bar{1} = \bar{0} \cdot x^2 + \bar{0} \cdot x + \bar{1} = \bar{1}$.

§ 4. Euklidische Ringe

Zusammenfassung. Bei den *euklidischen Ringen* handelt es sich um Integritätsbereiche, in denen das Konzept der Division mit Rest auf sinnvolle Weise definiert ist. Da der Rest in einem geeigneten Sinn stets „kleiner“ sein soll als das Element, durch das geteilt wurde, sind solche Ringe mit einer *Höhenfunktion* ausgestattet, die es ermöglicht, die „Größe“ von Elementen miteinander zu vergleichen.

Je zwei Elementen in einem euklidischen Ring kann ein *größter gemeinsamer Teiler* (ggT) zugeordnet werden, und dieser lässt sich mit dem sog. *Euklidischen Algorithmus* berechnen. Um den ggT (und ebenso das kleinste gemeinsame Vielfache, kgV) definieren zu können, müssen wir die Teilerrelation von \mathbb{Z} auf beliebige Ringe verallgemeinern.

Wichtige Grundbegriffe

- Teilerrelation | auf beliebigen Ringen
- assoziierte Elemente in einem Ring
- Definition von ggT und kgV in beliebigen Ringen
- Höhenfunktion auf einem Ring
- euklidische Ringe

Zentrale Sätze

- Eindeutigkeit von ggT und kgV bis auf Assoziierte
- Der Ring \mathbb{Z} und Polynomringe über Körpern sind euklidisch.
- Korrektheit des Euklidischen Algorithmus

Definition 4.1 Seien R ein Ring und $a, b \in R$. Wir sagen, dass a ein **Teiler** von b ist und schreiben $a|b$, wenn ein $c \in R$ mit $b = ac$ existiert. Gilt sowohl $a|b$ als auch $b|a$, dann sagt man, die Elemente a und b sind **assoziiert** zueinander.

Es ist leicht zu sehen, dass es sich bei der Relation „assoziiert“ um eine Äquivalenzrelation handelt. In Integritätsbereichen lässt sich die Relation auch folgendermaßen beschreiben.

Lemma 4.2 Ist R ein Integritätsbereich, so sind $a, b \in R$ genau dann zueinander assoziiert, wenn ein $\varepsilon \in R^\times$ mit $b = \varepsilon a$ existiert.

Beweis: „ \Leftarrow “ Aus $b = \varepsilon a$ folgt $a|b$, und wegen $a = \varepsilon^{-1}b$ gilt auch $b|a$.

„ \Rightarrow “ Nach Voraussetzung gilt $a|b$ und $b|a$, es gibt also Elemente $c, d \in R$ mit $b = ac$ und $a = bd$. Es folgt $a = acd$. Ist $a = 0$, dann gibt dasselbe für b , und die Gleichung $b = \varepsilon a$ ist mit der Einheit $\varepsilon = 1$ erfüllt. Ansonsten können wir auf $a \cdot 1 = acd$ die Kürzungsregel anwenden und erhalten $cd = 1$. Dies zeigt, dass $\varepsilon = c$ ein Einheit ist, also ist auch hier $b = \varepsilon a$ für ein geeignetes Element $\varepsilon \in R^\times$ erfüllt. \square

Definition 4.3 Sei R ein Ring mit $a_1, \dots, a_n \in R$. Wir sagen, ein Element $d \in R$ ist ein **größter gemeinsamer Teiler** (kurz ggT) von a_1, \dots, a_n , wenn gilt

- (i) $d|a_i$ für $1 \leq i \leq n$
- (ii) Ist $b \in R$ mit $b|a_i$ für $1 \leq i \leq n$, dann folgt $b|d$.

Wir nennen die Elemente a_1, \dots, a_n **teilerfremd**, wenn 1_R ein ggT der Elemente ist.

Definition 4.4 Sei R ein Ring mit $a_1, \dots, a_n \in R$. Ein Element $e \in R$ heißt **kleinstes gemeinsames Vielfaches** (kurz kgV) von a_1, \dots, a_n , wenn gilt

- (i) $a_i|e$ für $1 \leq i \leq n$
- (ii) Ist $b \in R$ mit $a_i|b$ für $1 \leq i \leq n$, dann folgt $e|b$.

Häufig schreibt man der Einfachheit halber $d = \text{ggT}(a_1, \dots, a_n)$, um auszudrücken, dass d ein ggT von a_1, \dots, a_n ist. Dabei handelt es sich aber um keine Gleichung im herkömmlichen Sinn, weil der ggT im Allgemeinen nicht eindeutig bestimmt ist. Statt dessen gilt

Lemma 4.5 Sei R ein Ring und $d \in R$ ein größter gemeinsamer Teiler der Ringelemente a_1, \dots, a_n . Ein weiteres Element $d' \in R$ ist genau dann ein ggT von a_1, \dots, a_n , wenn d und d' zueinander assoziiert sind. Dieselbe Aussage gilt auch für das kleinste gemeinsame Vielfache.

Beweis: Sei d' ein weiterer ggT von a_1, \dots, a_n . Nach Voraussetzung gilt $d'|a_i$ für $1 \leq i \leq n$. Weil nach Voraussetzung $d = \text{ggT}(a_1, \dots, a_n)$ ist, folgt daraus $d'|d$. Genauso zeigt man $d|d'$, also sind d und d' assoziiert.

Sind umgekehrt d, d' zueinander assoziierte Elemente und ist $d = \text{ggT}(a_1, \dots, a_n)$, dann folgt aus $d'|d$ und $d|a_i$ jeweils $d'|a_i$ für $1 \leq i \leq n$. Ist $b \in R$ ein Element mit $b|a_i$ für alle i , dann gilt $b|d$ auf Grund der ggT-Eigenschaft von d . Aus $b|d$ und $d|d'$ folgt $b|d'$. Damit ist insgesamt bewiesen, dass es sich bei d' um einen ggT der Elemente a_1, \dots, a_n handelt. Für das kleinste gemeinsame Vielfache verläuft der Beweis völlig analog. \square

Nach diesen Vorbereitungen definieren wir nun einen neuen Ringtyp, der dadurch gekennzeichnet ist, dass in ihm eine „Division mit Rest“ ausgeführt werden kann (und sinnvoll definiert ist). Wie wir sehen werden, hat dies unter anderem zur Folge, dass je zwei Ringelemente a, b einen ggT besitzen, sofern sie nicht beide Null sind.

Definition 4.6 Eine **Höhenfunktion** auf einem Integritätsbereich R ist eine Abbildung $h : R \setminus \{0_R\} \rightarrow \mathbb{N}$ mit der folgenden Eigenschaft: Sind $a, b \in R$, $b \neq 0_R$, dann gibt es Elemente $q, r \in R$, so dass die Gleichung $a = qb + r$ erfüllt ist und außerdem entweder $r = 0_R$ oder $h(r) < h(b)$ gilt. Ein **euklidischer Ring** ist ein Integritätsbereich, auf dem eine Höhenfunktion existiert.

Gelegentlich bietet es sich an, für die Höhenfunktion eine Abbildung $R \setminus \{0_R\} \rightarrow \mathbb{N}_0$, also mit Wertebereich \mathbb{N}_0 statt \mathbb{N} zu verwenden. Der Begriff des euklidischen Rings ändert sich dadurch nicht. Ist nämlich h eine Höhenfunktion mit Wertebereich \mathbb{N}_0 , dann ist durch $\tilde{h}(a) = h(a) + 1$ eine Höhenfunktion mit Wertebereich \mathbb{N} definiert.

Wir werden nun zwei konkrete Beispiele für euklidische Ringe angeben. Im Hinblick auf das erste Beispiel erinnern wir an die Definition der untern Gaußklammer: Nach Definition ist $\lfloor x \rfloor$ für $x \in \mathbb{R}$ jeweils die größte ganze Zahl a mit $a \leq x$. Es ist also beispielsweise $\lfloor \frac{6}{5} \rfloor = 1$ und $\lfloor -\frac{3}{2} \rfloor = -2$.

Beispiel 1: Der Ring \mathbb{Z} der ganzen Zahlen ist ein euklidischer Ring. Die Abbildung $h : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ gegeben durch $h(a) = |a|$ ist eine Höhenfunktion.

Beweis: Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Wir betrachten zunächst den Fall $b > 0$. Setzen wir $q = \lfloor \frac{a}{b} \rfloor$ und $r = a - qb$, dann ist die Gleichung $a = qb + r$ nach Definition erfüllt. Auf Grund der Definition der unteren Gaußklammer gilt $q \leq \frac{a}{b} < q + 1$. Multiplikation mit b liefert $qb \leq a < (q + 1)b$, und durch Subtraktion von qb erhalten wir schließlich $0 \leq r < b$. Also gilt entweder $r = 0$ oder $h(r) < h(b)$.

Betrachten wir nun den Fall $b < 0$. Dann ist $b_1 = -b > 0$, und wie wir bereits gezeigt haben, gibt es $q_1, r_1 \in \mathbb{Z}$ mit $a = q_1 b_1 + r_1$ und $r_1 = 0$ oder $h(r_1) < h(b_1)$. Setzen wir $q = -q_1$ und $r = r_1$, dann gilt $a = qb + r$ und entweder $r = 0$ oder $h(r) = h(r_1) < h(b_1) = h(b)$. \square

Beispiel 2: Sei K ein Körper. Dann ist der Polynomring $K[x]$ ein euklidischer Ring mit der Höhenfunktion gegeben durch die Gradabbildung, also $h(f) = \text{grad}(f)$.

Beweis: Sei $0 \neq g \in K[x]$ vorgegeben, mit $m = \text{grad}(g)$ und

$$g = \sum_{i=0}^m b_i x^i \quad , \quad b_0, \dots, b_m \in R, \quad b_m \neq 0.$$

Durch vollständige Induktion über $n \in \mathbb{N}_0$ zeigen wir: Ist $f \in K[x]$ mit $n = \text{grad}(f)$, dann gibt es ein $q \in K[x]$, so dass für $r = f - qg$ entweder $r = 0$ oder $\text{grad}(r) < m$ gilt. Im Fall $n < m$ können wir einfach $q = 0$, $r = f$ setzen, und es ist nichts zu zeigen. Sei nun $n \in \mathbb{N}_0$, $n \geq m$, und setzen wir die Aussage für die Polynomgrade $< n$ als gültig voraus. Sei f ein Polynom vom Grad n , also

$$f = \sum_{i=0}^n a_i x^i \quad \text{mit} \quad a_0, \dots, a_n \in K, \quad a_n \neq 0.$$

Setzen wir $q_0 = \frac{a_n}{b_m} x^{n-m}$, dann ist $f_0 = f - q_0 g$ ein Polynom vom Grad $< n$, und wir können die Induktionsvoraussetzung auf f_0 anwenden. Wir erhalten ein $q_1 \in K[x]$, so dass $r = f_0 - q_1 g$ entweder gleich Null oder $\text{grad}(r) < m$ erfüllt ist. Wegen $r = f - (q_0 + q_1)g$ erhalten wir durch $q = q_0 + q_1$ ein Element mit den gewünschten Eigenschaften. Insgesamt haben wir damit gezeigt: Sind $f, g \in K[x]$ mit $g \neq 0$, dann gibt es $q, r \in K[x]$ mit $f = qg + r$ und $r = 0$ oder $\text{grad}(r) < \text{grad}(g)$. \square

Definition 4.7 Sei R ein Ring und $f \in R[x]$. Ein Element $a \in R$ mit $f(a) = 0$ wird **Nullstelle** des Polynoms genannt.

Die folgenden Regeln für die Nullstellen von Polynomen über Körpern sind im Prinzip bereits aus der Schulmathematik bekannt. Ihre Gültigkeit beruht letztlich darauf, dass Polynomringe über Körpern euklidische Ringe sind.

Folgerung 4.8 Sei K ein Körper und $0 \neq f \in K[x]$.

- (i) Ist $a \in K$ eine Nullstelle von f , dann gilt $f = (x - a)g$ für ein Polynom $g \in K[x]$.
- (ii) Ist $\text{grad}(f) = n$ mit $n \in \mathbb{N}_0$, dann hat f höchstens n Nullstellen in K .

Beweis: zu (i) Da $K[x]$ ein euklidischer Ring ist, gibt es Polynome $g, r \in K[x]$ mit $f = (x - a)g + r$ mit $r = 0$ oder $\text{grad}(r) < \text{grad}(x - a) = 1$. Es gilt also $r \in K$. Daraus folgt $r = r(a) = f(a) - (a - a)g(a) = 0 - 0 = 0$ und somit $f = (x - a)g$.

zu (ii) Diese Aussage beweisen wir durch vollständige Induktion über n . Ist $n = 0$, dann handelt es sich bei f um eine Konstante in K^\times , und f besitzt dann offensichtlich keine Nullstellen. Setzen wir nun die Aussage für n voraus, und sei f ein Polynom vom Grad $n + 1$. Seien a_1, \dots, a_r die verschiedenen Nullstellen von f , wobei $r \in \mathbb{N}_0$ ist. Im Fall $r = 0$ ist die Aussage $r \leq \text{grad}(f)$ offenbar erfüllt. Andernfalls gibt es nach (i) gibt es ein Polynom $g \in K[x]$ mit $f = (x - a_1)g$, und für $2 \leq i \leq r$ ist a_i wegen $(a_i - a_1)g(a_i) = f(a_i) = 0$ und $a_i - a_1 \neq 0$ eine Nullstelle von g . Die Gleichung $f = (x - a_i)g$ zeigt, dass $\text{grad}(g) = n$ ist. Wir können also die Induktionsvoraussetzung auf g anwenden und erhalten die Abschätzung $r - 1 \leq n$. Daraus folgt $r \leq n + 1$ wie gewünscht. \square

In einem euklidischen Ring R kann durch wiederholte Division mit Rest ein größter gemeinsamer Teiler d zweier Ringelemente $a, b \in R$ in endlich vielen Schritten ermittelt werden. Man bezeichnet dieses Verfahren als **euklidischen Algorithmus**. Zugleich liefert dieses Verfahren Elemente $x, y \in R$ mit der Eigenschaft

$$d = xa + yb.$$

Somit zeigt der Algorithmus, dass das **Lemma von Bézout** nicht nur in \mathbb{Z} , sondern in beliebigen euklidischen Ringen gültig ist.

Lemma 4.9 Sei R ein Ring, und seien $a, b, q \in R$ mit $b \neq 0$. Dann gilt die Gleichung $\text{ggT}(a, b) = \text{ggT}(a - qb, b)$. Genauer ausformuliert bedeutet das: Ein Ringelement d ist genau dann ein größter gemeinsamer Teiler von a und b , wenn d ein größter gemeinsamer Teiler von $a - qb$ und b ist.

Beweis: „ \Rightarrow “ Sei d ein größter gemeinsamer Teiler von a und b . Dann gibt es $c_1, c_2 \in R$ mit $a = c_1d$ und $b = c_2d$. Es folgt $a - qb = c_1d - qc_2d$, also ist d ein gemeinsamer Teiler von $a - qb$ und b . Ist $e \in R$ ein weiterer gemeinsamer Teiler dieser beiden Zahlen, dann gibt es $c_3, c_4 \in R$ mit $a - qb = c_3e$ und $b = c_4e$. Man erhält $a = (a - qb) + qb = c_3e + c_4e = (c_3 + c_4)e$. Also ist e ein gemeinsamer Teiler von a und b , und aus $d = \text{ggT}(a, b)$ folgt $e|d$. Damit ist gezeigt, dass d ein größter gemeinsamer Teiler von $a - qb$ und b ist. Die Beweisrichtung „ \Leftarrow “ läuft analog. \square

EUKLIDISCHER ALGORITHMUS

Eingabe: ein euklidischer Ring R mit Höhenfunktion h
Elemente $a, b \in R$ mit $b \neq 0$

Ausgabe: Elemente $d, x, y \in R$ mit $d = \text{ggT}(a, b)$ und $d = xa + yb$

Ablauf: (1) definiere $(a_1, x_1, y_1) = (a, 1, 0)$ und $(a_2, x_2, y_2) = (b, 0, 1)$

(2) Sei das Tupel (a_n, x_n, y_n) bereits definiert.

Wenn $a_n = 0$ ist,

dann setze $d = a_{n-1}$, $x = x_{n-1}$, $y = y_{n-1}$ und gib d, x, y
als Ergebnis aus. (STOP)

Ansonsten

bestimme $q, r \in R$ mit

$a_{n-1} = qa_n + r$ und $r = 0$ oder $h(r) < h(a_n)$.

Definiere $(a_{n+1}, x_{n+1}, y_{n+1}) = (r, x_{n-1} - qx_n, y_{n-1} - qy_n)$.

Wiederhole Schritt 2.

Satz 4.10 Sei R ein euklidischer Ring mit Höhenfunktion h . Der euklidische Algorithmus hält für jedes Paar (a, b) mit $a, b \in R$ und $b \neq 0$ nach einer endlichen Zahl von Wiederholungen. Er liefert als Ausgabe tatsächlich $d = \text{ggT}(a, b)$ und Ringelemente $x, y \in R$ mit $d = xa + yb$.

Beweis: Gehen wir zunächst davon aus, dass der zweite Schritt unendlich oft wiederholt wird. Dann ist das Tupel (a_n, x_n, y_n) für alle $n \in \mathbb{N}$ definiert. Nach Definition gilt für jedes $n \in \mathbb{N}$ aber jeweils aber $r = a_{n+1}$ und $h(a_{n+1}) = h(r) < h(a_n)$, wobei $q, r \in \mathbb{Z}$ die in Schritt 2 definierten Elemente in der Gleichung $a_{n-1} = qa_n + r$ sind. Wir erhalten also eine unendliche absteigende Folge

$$h(a_2) > h(a_3) > h(a_4) > h(a_5) > \dots \quad \text{von Zahlen in } \mathbb{N}_0.$$

Aber eine solche Folge existiert nicht: Eine absteigende Folge in \mathbb{N}_0 , die bei einer Zahl $b \in \mathbb{N}_0$ beginnt, kann höchstens $b+1$ Schritte lang sein. Damit ist gezeigt, dass der euklidische Algorithmus nach einer endlichen Anzahl von Schritten abbricht.

Sei nun $n \geq 2$ und $(a_n, x_n, y_n) = (0, x_n, y_n)$ das letzte Tupel, das vom euklidischen Algorithmus berechnet wird. Wir beweisen durch vollständige Induktion über k , dass für $2 \leq k \leq n$ die Gleichung

$$\text{ggT}(a_{k-1}, a_k) = \text{ggT}(a, b)$$

erfüllt ist. Für $k = 2$ haben wir nach Definition $a_1 = a$ und $a_2 = b$, also ist die Gleichung $\text{ggT}(a_1, a_2) = \text{ggT}(a, b)$ offensichtlich erfüllt. Nehmen wir nun an, dass die Gleichung für k bereits bewiesen ist. Nach Definition gibt es ein $q \in \mathbb{Z}$ mit $a_{k-1} = qa_k + a_{k+1}$, und es folgt

$$\text{ggT}(a_k, a_{k+1}) = \text{ggT}(a_k, a_{k-1} - qa_k) = \text{ggT}(a_k, a_{k-1}) = \text{ggT}(a_{k-1}, a_k) = \text{ggT}(a, b),$$

wobei wir im zweiten Schritt 4.9 und im letzten Schritt die Induktionsvoraussetzung angewendet haben. Nun beweisen wir noch durch vollständige Induktion die Gleichung

$$x_k a + y_k b = a_k \quad \text{für } 1 \leq k \leq n.$$

Es gilt $x_1 a + y_1 b = 1 \cdot a + 0 \cdot b = a = a_1$ und $x_2 a + y_2 b = 0 \cdot a + 1 \cdot b = b = a_2$. Nehmen wir nun an, dass die Gleichung für k bereits bewiesen ist. Nach Definition existiert ein q , für das die Gleichungen $a_{k+1} - q a_k$, $x_{k+1} = x_k - q x_k$ und $y_{k+1} = y_k - q y_k$ erfüllt sind. Es folgt

$$\begin{aligned} x_{k+1} a + y_{k+1} b &= (x_k - q x_k) a + (y_k - q y_k) b = (x_k a + y_k b) - q(x_k a + y_k b) \\ &= a_k - q a_k = a_{k+1}. \end{aligned}$$

Der Algorithmus liefert $d = a_{n-1}$, $x = x_{n-1}$ und $y = y_{n-1}$ als Ergebnis. Nun gilt allgemein $\text{ggT}(c, 0) = c$ für jedes Ringelement c ungleich Null. Aus dem bereits Bewiesenen folgt $\text{ggT}(a, b) = \text{ggT}(a_{n-1}, a_n) = \text{ggT}(a_{n-1}, 0) = a_{n-1} = d$ und $x a + y b = x_{n-1} a + y_{n-1} b = d$. \square

Als Anwendungsbeispiel berechnen wir den ggT der Zahlen $a = 16170$ und $b = 1326$.

q	a_n	x_n	y_n
–	16170	1	0
–	1326	0	1
12	258	1	–12
5	36	–5	61
7	6	36	–439
6	0	(–221)	(2695)

Wir erhalten $\text{ggT}(a, b) = 6 = 36a + (-439)b$. (Die Zahlen in Klammern werden für das Ergebnis nicht mehr benötigt.)

Wie wir gesehen haben, sind auch Polynomringe über Körpern Beispiele für euklidische Ringe. Folglich kann der euklidische Algorithmus auch auf diese Ring angewendet werden. Als Beispiel berechnen wir den ggT der beiden Polynome $f = x^4 - 3x^3 - x^2 + 5x - 6$ und $g = x^3 - 3x^2 + x - 3$ in $\mathbb{Q}[x]$.

q	a_n	x_n	y_n
–	$x^4 - 3x^3 - x^2 + 5x - 6$	1	0
–	$x^3 - 3x^2 + x - 3$	0	1
x	$-2x^2 + 8x - 6$	1	$-x$
$-\frac{1}{2}x - \frac{1}{2}$	$2x - 6$	$\frac{1}{2}x + \frac{1}{2}$	$-\frac{1}{2}x^2 - \frac{1}{2}x + 1$
$-x + 1$	0	$(\frac{1}{2}x^2 + \frac{1}{2})$	$(-\frac{1}{2}x^3 + \frac{1}{2}x - 1)$

Als Ergebnis erhalten wir

$$\text{ggT}(f, g) = 2x - 6 = (\frac{1}{2}x - \frac{1}{2})f + (-\frac{1}{2}x^2 - \frac{1}{2}x + 1)g.$$

Wir haben in Satz 2.8 die Teilringe von \mathbb{C} der Form $\mathbb{Z}[\sqrt{d}]$ betrachtet, wobei d eine beliebige ganze Zahl bezeichnet. Den Ring $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ bezeichnet man speziell als Ring der **Gaußschen Zahlen**. Um zu zeigen, dass dies ein

euklidischer Ring ist, definieren wir eine Abbildung $N : \mathbb{C} \rightarrow \mathbb{R}$ durch $N(z) = z\bar{z} = |z|^2$, wobei \bar{z} die zu z konjugierte komplexe Zahl und $|z|$ den Absolutbetrag von $z \in \mathbb{C}$ bezeichnet. Offenbar ist die Funktion N **multiplikativ**, das heißt für alle $z, w \in \mathbb{C}$ gilt $N(zw) = |zw|^2 = |z|^2|w|^2 = N(z)N(w)$. Für die Gaußschen Zahlen der Form $a + ib$ mit $a, b \in \mathbb{Z}$ gilt $N(a + ib) = a^2 + b^2$. Durch Einschränkung von N erhalten wir also eine Abbildung $h : \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}$.

Proposition 4.11 Der Ring $\mathbb{Z}[i]$ ist ein euklidischer Ring, und die soeben definierte Abbildung h ist eine Höhenfunktion auf diesem Ring.

Beweis: Als Körper ist \mathbb{C} ein Integritätsbereich, also ist 0 der einzige Nullteiler in \mathbb{C} . Damit ist 0 auch der einzige Nullteiler in $\mathbb{Z}[i] \subseteq \mathbb{C}$, d.h. auch $\mathbb{Z}[i]$ ist ein Integritätsbereich. Zum Nachweis, dass h eine Höhenfunktion ist, seien $\alpha, \beta \in \mathbb{Z}[i]$ vorgegeben, wobei wir $\beta \neq 0$ voraussetzen. Wir müssen zeigen, dass ein $q \in \mathbb{Z}[i]$ mit $\alpha - q\beta = 0$ oder $h(\alpha - q\beta) < h(\beta)$ existiert. Sei $\alpha = a + ib$ und $\beta = c + id$ mit $a, b, c, d \in \mathbb{Z}$. Wegen $\beta \neq 0$ ist $(c, d) \neq (0, 0)$. Es gilt

$$\frac{\alpha}{\beta} = \frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{(c + id)(c - id)} = \frac{ac + bd}{c^2 + d^2} + i \frac{bc - ad}{c^2 + d^2} = r + is,$$

wenn wir die Zahlen $r, s \in \mathbb{Q}$ durch

$$r = \frac{ac + bd}{c^2 + d^2} \quad \text{und} \quad s = \frac{bc - ad}{c^2 + d^2}$$

definieren. Seien nun $r_0, s_0 \in \mathbb{Z}$ so gewählt, dass $|r - r_0| \leq \frac{1}{2}$ und $|s - s_0| \leq \frac{1}{2}$ gilt, und setzen wir $q = r_0 + is_0$. Dann folgt

$$h\left(\frac{\alpha}{\beta} - q\right) = (r - r_0)^2 + (s - s_0)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

Es gilt dann $\alpha - q\beta = 0$ oder zumindest $h(\alpha - q\beta) = h\left(\frac{\alpha}{\beta} - q\right)h(\beta) \leq \frac{1}{2}h(\beta) < h(\beta)$. □

Wir berechnen den ggT der Elemente $\alpha = 12 + 14i$ und $\beta = 32 - 6i$. Um den Teiler q in jedem Schritt zu bestimmen, gehen wir folgendermaßen vor. Zunächst berechnen wir den Quotienten $\frac{a_{n-1}}{a_n}$ in der Form $r + si$ mit $r, s \in \mathbb{Q}$. Anschließend wählen wir $r_0, s_0 \in \mathbb{Z}$ mit $|r - r_0| \leq \frac{1}{2}$ und $|s - s_0| \leq \frac{1}{2}$ und setzen $q = r_0 + s_0i$.

a_{n-1}/a_n	q	a_n	x_n	y_n
—	—	$12 + 14i$	1	0
—	—	$32 - 6i$	0	1
$\frac{15}{53} + \frac{26}{53}i$	0	$12 + 14i$	1	0
$\frac{15}{17} - \frac{26}{17}i$	$1 - 2i$	$-8 + 4i$	$-1 + 2i$	1
$-\frac{1}{2} - 2i$	$-1 - 2i$	$-4 + 2i$	-4	$1 + 2i$
2	2	0	$(7 + 2i)$	$(-1 - 4i)$

Also ist $\text{ggT}(\alpha, \beta) = -4 + 2i = (-4)\alpha + (1 + 2i)\beta$.

Zum Abschluss sei noch darauf hingewiesen, dass $\mathbb{Z}[\sqrt{d}]$ keineswegs für jedes $d \in \mathbb{Z}$ ein euklidischer Ring ist. Beispielsweise kann man zeigen, dass $\mathbb{Z}[\sqrt{-3}]$ und $\mathbb{Z}[\sqrt{-5}]$ nicht euklidisch sind; auf diesen Ringen kann also keine Höhenfunktion definiert werden. Momentan fehlen uns noch die Grundlagen, um dies zu beweisen, aber wir werden darauf zurückkommen.

§ 5. Ideale

Zusammenfassung. Ideale sind Teilmengen von Ringen, mit denen in gewissen Grenzen auf ähnliche Weise gerechnet werden kann wie mit Ringelementen. Beispielsweise können auch Ideale addiert und multipliziert werden. Ursprünglich eingeführt wurden sie in Mathematik, um einen Ersatz für die eindeutige Primfaktorzerlegung zu erhalten, die in vielen Ringen wie beispielsweise $\mathbb{Z}[\sqrt{-5}]$ nicht mehr gültig ist. Inzwischen aber hat sich der Anwendungsbereich der Idealtheorie von der Zahlentheorie auf viele andere Gebiete der Mathematik ausgeweitet, darunter die Algebraische Geometrie und die Funktionalanalysis.

Im nächsten Kapitel werden wir sehen, dass die Ideale das natürliche Analogon der Normalteiler in der Gruppentheorie sind, weil sie wie diese zur Definition von Faktorstrukturen genutzt werden können. Nachdem wir die Ideale eines Rings definiert haben, beschäftigen wir uns zunächst, wie schon bei den Untergruppen und den Ringerweiterungen, mit der Beschreibung der Ideale durch Erzeugendensysteme. Wir definieren die Summe und das Produkt von Idealen. Als besonders wichtige Idealtypen lernen wir die **Primideale** und die **maximalen Ideale** kennen.

Wichtige Grundbegriffe

- Ideale eines Rings
- Hauptideal
- Erzeugendensysteme eines Ideals
- Rechenoperationen für Ideale (Summen, Produkte)
- Primideale und maximale Ideale

Zentrale Sätze

- Urbilder von Idealen unter Ringhomomorphismen sind Ideale
- Bilder von Idealen unter surjektiven Ringhomomorphismen sind Ideale

Definition 5.1 Sei R ein Ring. Ein **Ideal** in R ist eine Teilmenge $I \subseteq R$ mit den Eigenschaften

- (i) $0_R \in I$
- (ii) Für alle $a, b \in I$ und $r \in R$ gilt $a + b \in I$ und $ra \in I$.

Eine wichtige Rolle spielen die Ideale der folgenden Form.

Proposition 5.2 Ist R ein Ring und $b \in R$, dann ist die Menge der Vielfachen $\{ab \mid a \in R\}$ von b ein Ideal in R . Man nennt ein solches Ideal ein **Hauptideal** und bezeichnet es mit (b) . Ein **Hauptidealring** ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist. In jedem Ring R ist das **Nullideal** $(0_R) = \{0_R\}$ das kleinste und das **Einheitsideal** $(1_R) = R$ das bezüglich Inklusion größte Ideal.

Beweis: Sei $b \in R$. Wir überprüfen, dass die Teilmenge (b) von R die in Definition 5.1 genannten Eigenschaften hat. Wegen $0_R = 0_R \cdot b$ ist 0_R in (b) enthalten. Seien nun $c, d \in (b)$ und $r \in R$ vorgegeben. Wegen $c, d \in (b)$ gibt es $a_1, a_2 \in R$ mit $c = a_1 b$ und $d = a_2 b$. Es folgt $c + d = (a_1 + a_2)b \in (b)$. Ebenso gilt $rc = r(a_1 b) = (ra_1)b \in (b)$. Also ist (b) tatsächlich ein Ideal.

Für alle $a \in R$ gilt $a \cdot 0_R = 0_R$. Dies zeigt, dass das Nullideal (0_R) tatsächlich als einziges Element 0_R enthält und damit das bezüglich Inklusion kleinste Ideal ist. Wegen $a \cdot 1_R = a$ für alle $a \in R$ enthält das Einheitsideal (1_R) alle Ringelemente und ist damit das bezüglich Inklusion größte Ideal. \square

Ähnlich wie für Untergruppen, Normalteiler und Teilringe gilt auch für die Ideale

Proposition 5.3 Sei R ein Ring und $(I_j)_{j \in A}$ eine Familie von Idealen in R . Dann ist $I = \bigcap_{j \in A} I_j$ ein Ideal in R .

Beweis: Weil jedes I_j ein Ideal ist, gilt $0_R \in I_j$ für alle $j \in A$ und somit $0_R \in I$. Seien nun $a, b \in I$ und $r \in R$ vorgegeben. Dann gilt $a, b \in I_j$ für alle $j \in A$. Aus der Idealeigenschaft folgt $a + b \in I_j$ und $ra \in I_j$ für alle $j \in A$. Dies wiederum bedeutet $a + b \in I$ und $ra \in I$. \square

Wie die Ringelemente können auch Ideale addiert und multipliziert werden.

Proposition 5.4 Sei ein Ring, und seien I, J Ideale in R . Dann ist auch die Teilmenge $I + J = \{ a + b \mid a \in I, b \in J \}$ von R ein Ideal in R .

Beweis: Aus $0_R \in I$ und $0_R \in J$ folgt $0_R = 0_R + 0_R \in I + J$. Seien nun $a, b \in I + J$ und $r \in R$ vorgegeben. Dann gibt es Elemente $a', b' \in I$ und $a'', b'' \in J$ mit $a = a' + a''$ und $b = b' + b''$. Weil I und J Ideale sind, gilt $a' + b' \in I$ und $a'' + b'' \in J$. Es folgt $a + b = (a' + b') + (a'' + b'') \in I + J$. Die Idealeigenschaft von I und J liefert auch $ra' \in I$ und $ra'' \in J$. Es folgt $ra = ra' + ra'' \in I + J$. \square

Leider ist die Definition des *Produkts* zweier Ideale I und J nicht ganz so einfach. Man ist versucht, dass Produkt durch $IJ = \{ ab \mid a \in I, b \in J \}$ zu definieren, aber leider ist eine solche Menge im allgemeinen kein Ideal mehr. (Weiter unten werden wir dies durch ein Gegenbeispiel belegen.) Statt dessen müssen wir das von dieser Produktmenge *erzeugte* Ideal betrachten. Das Konzept der Erzeugendensysteme ist uns bereits aus der Linearen Algebra und der Gruppentheorie bekannt. Auch Teilringe, die von einer Menge erzeugt werden, haben wir bereits definiert, siehe dazu Satz 2.7.

Definition 5.5 Sei R ein Ring und $S \subseteq R$ eine Teilmenge. Man sagt, ein Ideal I in R wird von S *erzeugt* und schreibt $I = (S)$, wenn folgende Bedingungen erfüllt sind.

- (i) $I \supseteq S$
- (ii) Ist J ein Ideal in R mit $J \supseteq S$, dann folgt $J \supseteq I$.

Insgesamt ist I also das *kleinste* Ideal mit der Eigenschaft $I \supseteq S$.

Existenz und Eindeutigkeit des Ideals (S) beweist man wie bei den Teilringen. Für die Existenz bildet man die Familie $(I_j)_{j \in A}$ aller Ideale in R , die S enthalten und überprüft dann, dass

$$I = \bigcap_{j \in A} I_j$$

die Bedingungen (i) und (ii) aus Definition 5.5 erfüllt. Nehmen wir nun an, dass J ein weiteres Ideal ist, dass diese Bedingungen erfüllt. Dann liefert die Anwendung von (ii) sowohl $J \supseteq I$ als auch $I \supseteq J$, insgesamt also $I = J$. Ist S endlich, $S = \{a_1, \dots, a_n\}$, dann verwendet man an Stelle von (S) auch die Schreibweise (a_1, \dots, a_n) für das erzeugte Ideal. Der folgende Satz gibt an, wie die Elemente eines solchen Ideals konkret aussehen.

Proposition 5.6 Sei R ein Ring, und seien $a_1, \dots, a_n \in R$. Dann gilt

$$(a_1, \dots, a_n) = \left\{ \sum_{i=1}^n r_i a_i \mid r_1, \dots, r_n \in R \right\}.$$

Beweis: Sei I die Menge auf der rechten Seite der Gleichung. Wir überprüfen, dass I die definierenden Eigenschaften des von $\{a_1, \dots, a_n\}$ erzeugten Ideals besitzt. Zunächst zeigen wir, dass I ein Ideal ist. Das Element 0_R ist in I enthalten, denn es gilt $0_R = 0_R a_1 + \dots + 0_R a_n$. Seien nun $a, b \in I$ und $r \in R$ vorgegeben. Dann existieren nach Definition von I Elemente $r_1, \dots, r_n, r'_1, \dots, r'_n \in R$, so dass

$$a = \sum_{i=1}^n r_i a_i \quad \text{und} \quad b = \sum_{i=1}^n r'_i a_i$$

gilt. Wir erhalten

$$a + b = \sum_{i=1}^n (r_i + r'_i) a_i \in I \quad \text{und} \quad ra = \sum_{i=1}^n (r r_i) a_i \in I.$$

Damit ist die Idealeigenschaft von I bewiesen. Außerdem enthält I die Menge S . Ist nämlich $j \in \{1, \dots, n\}$, dann gilt $a_j = \sum_{i=1}^n \delta_{ij} a_i \in I$, wobei $\delta_{ij} \in \{0_R, 1_R\}$ jeweils das Kronecker-Delta bezeichnet. Sei nun J ein weiteres Ideal mit $J \supseteq I$. Sind $r_1, \dots, r_n \in R$ beliebig gewählt, dann enthält J auf Grund der Idealeigenschaft die Elemente $r_1 a_1, \dots, r_n a_n$, und durch einen einfachen Induktionsbeweis zeigt man, dass auch die Summe $\sum_{i=1}^n r_i a_i$ in J enthalten ist. Damit ist die Inklusion $J \supseteq I$ nachgewiesen. \square

Die folgende Regel wird häufig beim Rechnen mit Idealen verwendet, die durch Erzeugendensysteme definiert sind.

Lemma 5.7 Sei R ein Ring, und seien $S, T \subseteq R$ beliebige Teilmengen. Gilt für die erzeugten Ideale $S \subseteq (T)$ und $T \subseteq (S)$, dann folgt $(S) = (T)$.

Beweis: Nach Definition ist (S) das *kleinste* Ideal, das S als Teilmenge enthält, und wegen $S \subseteq (T)$ ist (T) jedenfalls ein Ideal mit dieser Eigenschaft. Daraus folgt $(S) \subseteq (T)$, und ebenso erhält man $(T) \subseteq (S)$. \square

Nun können wir definieren

Definition 5.8 Sei R ein Ring, und seien I, J Ideale in R . Dann ist das **Produktideal** IJ das von der Menge $\{ab \mid a \in I, b \in J\}$ erzeugte Ideal in R .

Die folgende Proposition ist für die Berechnung von Produktidealen hilfreich.

Proposition 5.9 Sei R ein Ring, und seien I, J von endlichen vielen Ringelementen erzeugte Ideale, $I = (a_1, \dots, a_m)$ und $J = (b_1, \dots, b_n)$ mit $m, n \in \mathbb{N}$, $a_i, b_j \in R$ für $1 \leq i \leq m$, $1 \leq j \leq n$. Dann wird IJ von der Menge

$$S = \{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$

erzeugt, es gilt also $IJ = (S)$.

Beweis: Nach Definition des Produktideals gilt $IJ = (T)$ mit $T = \{ab \mid a \in I, b \in J\}$. Nach Lemma 5.7 genügt es also, $S \subseteq (T)$ und $T \subseteq (S)$ nachzuweisen. Die Inklusion $S \subseteq (T)$ ist offenbar erfüllt, weil für alle i, j mit $1 \leq i \leq m$ und $1 \leq j \leq n$ jeweils $a_i \in I$, $b_j \in J$ und damit $a_i b_j \in T$ gilt. Zum Beweis von $T \subseteq (S)$ sei $c \in T$ vorgegeben. Dann gibt es $a \in I$ und $b \in J$ mit $c = ab$. Wegen $I = (a_1, \dots, a_m)$ gibt es Ringelemente $r_1, \dots, r_m \in R$, so dass a in der Form $\sum_{i=1}^m r_i a_i$ geschrieben werden kann. Ebenso finden wir $s_1, \dots, s_n \in R$ mit $b = \sum_{j=1}^n s_j b_j$. Es gilt also

$$c = ab = \left(\sum_{i=1}^m r_i a_i \right) \left(\sum_{j=1}^n s_j b_j \right) = \sum_{i=1}^m \sum_{j=1}^n r_i s_j (a_i b_j).$$

Die Gleichung zeigt, dass c in (S) enthalten ist. □

Wir zeigen nun anhand eines Gegenbeispiels, dass das elementweise Produkt zweier Ideale im allgemeinen kein Ideal ist. Sei $R = \mathbb{Z}[x]$, und seien die Ideale I und J definiert durch $I = (2, x)$ und $J = (3, x)$. Nach Proposition 5.6 sind die Elemente aus $I = (2, x)$ die Polynome der Form $2u + xv$ mit $u, v \in \mathbb{Z}[x]$. Wie man sich leicht überlegt, sind es genau die Polynome $f \in \mathbb{Z}[x]$ mit durch 2 teilbarem konstanten Term $f(0)$, die auf diese Weise zu Stande kommen, zum Beispiel $x^2 + 5x - 10 = 2(-5) + x(x + 5)$ mit dem konstanten Term -10 . Ebenso besteht J genau aus den Polynomen $g \in \mathbb{Z}[x]$ mit der Eigenschaft, dass $g(0)$ durch 3 teilbar ist.

Wegen $-2, x \in I$ und $3, x \in J$ sind $3x$ und $(-2)x$ in M enthalten. Nehmen wir nun an, dass die Menge gegeben durch $M = \{fg \mid f \in I, g \in J\}$ ein Ideal in $\mathbb{Z}[x]$ ist, dann wäre auch $x = 3x + (-2)x \in M$. Aber andererseits kann x nicht in der Form $x = fg$ mit $f \in I$ und $g \in J$ geschrieben werden. Wäre dies so, dann würde wegen $\text{grad}(f) + \text{grad}(g) = \text{grad}(fg) = \text{grad}(x) = 1$ jeweils $\text{grad}(f), \text{grad}(g) \leq 1$ folgen. Es gäbe also $a, b, c, d \in \mathbb{Z}$ mit $f = ax + b$ und $g = cx + d$. Wir würden dann

$$x = fg = (ax + b)(cx + d) = acx^2 + (bc + ad)x + bd$$

erhalten, also insbesondere $ac = 0$. Ist nun $a = 0$, dann folgt $x = bcx + bd$ und somit $bc = 1$. Wie oben bemerkt, ist $b = f(0)$ aber durch 2 teilbar, was zu $bc = 1$ im Widerspruch steht. Ebenso führt $c = 0$ auf die Gleichung $x = adx + bd$, und wir erhalten $ad = 1$ im Widerspruch zu $3 \mid g(0) \Leftrightarrow 3 \mid d$.

Die Annahme, dass M ein Ideal in $\mathbb{Z}[x]$ ist, war also falsch. Nach Proposition 5.9 ist das Produktideal IJ gegeben durch $IJ = (6, 2x, 3x, x^2)$. Mit Lemma 5.7 lässt sich dies zu $IJ = (6, x)$ vereinfachen, denn einerseits sind die Elemente $6, 2x, 3x, x^2$ offenbar alle in $(6, x)$ enthalten, andererseits liegen 6 und x wegen $x = (-1)(2x) + 3x$ auch in $(6, 2x, 3x, x^2)$.

Im Hinblick auf spätere Anwendungen zeigen wir noch

Lemma 5.10 Für Ideale I, J, K in einem Ring R gilt das Distributivgesetz $I(J + K) = IJ + IK$, außerdem gilt $IJ \subseteq I$ und $IJ \subseteq J$.

Beweis: „ \subseteq “ Die Elemente der Form ab mit $a \in I$ und $b \in J + K$ bilden ein Erzeugendensystem von $I(J + K)$. Es genügt also zu zeigen, dass alle Elemente dieser Bauart in $IJ + IK$ enthalten sind. Das Element b kann in der Form $b = c + d$ mit $c \in J$ und $d \in K$ geschrieben werden. Es gilt $ab = a(c + d) = ac + ad$, mit $ac \in IJ$ und $ad \in IK$. Also ist ab in $IJ + IK$ enthalten.

„ \supseteq “ Hier genügt es zu zeigen, dass $IJ \subseteq I(J + K)$ und $IK \subseteq I(J + K)$ gilt. Das Ideal IJ wird erzeugt von den Elementen der Form ab mit $a \in I$ und $b \in J$, und es reicht zu zeigen, dass diese Produkte in $I(J + K)$ enthalten sind. Aus $b \in J$ folgt $b \in J + K$, also ist $ab \in I(J + K)$ erfüllt. Die Inklusion $IK \subseteq I(J + K)$ beweist man genauso.

Auch für die Inklusion $IJ \subseteq I$ brauchen wir nur zu zeigen, dass $\{ab \mid a \in I, b \in J\}$ eine Teilmenge von I ist. Dies ist auf Grund der Idealeigenschaft offensichtlich. Die Inklusion $IJ \subseteq J$ ist damit auch klar. \square

Definition 5.11 Ein Ideal \mathfrak{p} in einem Ring R wird **Primideal** genannt, wenn $\mathfrak{p} \neq (1)$ gilt und für alle $a, b \in R$ die Implikation

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$$

erfüllt ist. Man nennt \mathfrak{p} ein **maximales** Ideal, wenn $\mathfrak{p} \neq (1)$ ist und kein Ideal I mit der Eigenschaft $\mathfrak{p} \subsetneq I \subsetneq (1)$ existiert, das Ideal also abgesehen vom Einheitsideal bezüglich Inklusion maximal ist.

Gelegentlich wird die Primideal-Bedingung nicht mit Elementen, sondern mit Idealen formuliert.

Proposition 5.12 Ein Ideal \mathfrak{p} in einem Ring R ist genau dann ein Primideal in R , wenn $\mathfrak{p} \neq (1)$ ist und für beliebige Ideale I, J mit $IJ \subseteq \mathfrak{p}$ eine der Bedingungen $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$ erfüllt ist.

Beweis: „ \Leftarrow “ Nehmen wir an, dass die Idealbedingung für R erfüllt ist, und seien $a, b \in R$ mit $ab \in \mathfrak{p}$ vorgegeben. Dann betrachten wir die Ideale $I = (a)$ und $J = (b)$. Das Produktideal IJ wird auf Grund der Bemerkung von oben durch das Element ab erzeugt, und mit ab ist auch das Ideal IJ in \mathfrak{p} enthalten. Auf Grund unserer Voraussetzung folgt $(a) = I \subseteq \mathfrak{p}$ oder $(b) = J \subseteq \mathfrak{p}$, insbesondere $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Da außerdem $\mathfrak{p} \neq (1)$ gilt, handelt es sich bei \mathfrak{p} tatsächlich um ein Primideal.

„ \Rightarrow “ Sei \mathfrak{p} ein Primideal. Dann ist $\mathfrak{p} \neq (1)$. Seien nun I und J Ideale in R , und nehmen wir an, dass zwar $IJ \subseteq \mathfrak{p}$, aber weder $I \subseteq \mathfrak{p}$ noch $J \subseteq \mathfrak{p}$ erfüllt ist. Dann gibt es Elemente $a \in I \setminus \mathfrak{p}$ und $b \in J \setminus \mathfrak{p}$. Weiter gilt $ab \in IJ \subseteq \mathfrak{p}$. Wir haben also Elemente $a, b \in R$ mit $ab \in \mathfrak{p}$ und $a, b \notin \mathfrak{p}$ gefunden, im Widerspruch zur Primidealeigenschaft. \square

An dieser Stelle kommen wir auf die zu Anfang erwähnte Beziehung zwischen Idealen und Teilbarkeitslehre zurück. Für viele wichtige zahlentheoretische Problem (etwa Fermats letzter Satz oder Verallgemeinerungen des quadratischen Reziprozitätsgesetzes, das wir später noch kennenlernen werden) hat es sich als nützlich herausgestellt, Fragen

der Teilbarkeit in allgemeinen Ringen wie z.B. dem Ring $\mathbb{Z}[\sqrt{-5}]$ zu studieren. Insbesondere lassen sich in solchen Ringen Elemente definieren, die ähnlich wie die bekannten Primzahlen nicht weiter zerlegt werden können. Wir werden für solche Elemente später die Bezeichnung *irreduzibel* einführen. Im Ring $\mathbb{Z}[\sqrt{-5}]$ ist zum Beispiel $1 - 2\sqrt{-5}$ ein irreduzibles Element, ebenso die Primzahl 3. Es kann aber auch vorkommen, dass eine Primzahl p im Ring $\mathbb{Z}[\sqrt{-5}]$ zerlegbar wird, zum Beispiel $41 = (6 + \sqrt{-5})(6 - \sqrt{-5})$.

Der Mathematiker *Eduard Kummer* beschäftigte sich im 19. Jahrhundert mit dem Problem, dass die Zerlegung von Zahlen in irreduzible Elemente in Ringen wie $\mathbb{Z}[\sqrt{-5}]$ im Allgemeinen nicht mehr eindeutig ist. Zum Beispiel gilt

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}). \quad (*)$$

Kummer gelang es, die Eindeutigkeit der Zerlegung wieder herzustellen, indem er an Stelle der Zerlegung der Zahl 21 die Zerlegung des Hauptideals (21) in *Primideale* betrachtete. So kann man zum Beispiel zeigen, dass die Ideale in $\mathbb{Z}[\sqrt{-5}]$ gegeben durch

$$\mathfrak{p}_1 = (3, 1 + 2\sqrt{-5}) \quad , \quad \mathfrak{p}_2 = (3, 1 - 2\sqrt{-5}) \quad , \quad \mathfrak{p}_3 = (7, 1 + 2\sqrt{-5}) \quad \text{und} \quad \mathfrak{p}_4 = (7, 1 - 2\sqrt{-5})$$

Primideale sind. Obwohl die Faktoren in der Produktdarstellung (*) irreduzibel sind, lassen sich die entsprechenden Hauptideale weiter zerlegen. Mit Hilfe von Lemma 5.7 und Proposition 5.9 berechnet man zum Beispiel

$$\begin{aligned} \mathfrak{p}_1 \mathfrak{p}_3 &= (3, 1 + 2\sqrt{-5})(7, 1 + 2\sqrt{-5}) = (3 \cdot 7, (1 + 2\sqrt{-5}) \cdot 7, 3 \cdot (1 + 2\sqrt{-5}), (1 + 2\sqrt{-5})(1 + 2\sqrt{-5})) \\ &= (21, 7 + 14\sqrt{-5}, 3 + 6\sqrt{-5}, -19 + 4\sqrt{-5}) = (21, 1 + 2\sqrt{-5}, 3 + 6\sqrt{-5}, -19 + 4\sqrt{-5}) = \\ &= (21, 1 + 2\sqrt{-5}, 3 + 6\sqrt{-5}, 2 + 4\sqrt{-5}) = (21, 1 + 2\sqrt{-5}) = (1 + 2\sqrt{-5}). \end{aligned}$$

Dabei gilt die Gleichung im vierten Schritt wegen 5.7 und $7 + 14\sqrt{-5} = (1 + 2\sqrt{-5}) + 2(3 + 6\sqrt{-5})$, im fünften wegen $-19 + 4\sqrt{-5} + 21 = 2 + 4\sqrt{-5}$. Im vorletzten Schritt wurde verwendet, dass die Elemente $3 + 6\sqrt{-5}$ und $2 + 4\sqrt{-5}$ beides Vielfache von $1 + 2\sqrt{-5}$ sind und im letzten die Gleichung $21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. Die Rechnung zeigt also, dass das Hauptideal $(1 + 2\sqrt{-5})$ in die Faktoren \mathfrak{p}_1 und \mathfrak{p}_3 zerfällt.

Durch ähnliche Rechnungen erhält man die Gleichungen $\mathfrak{p}_1 \mathfrak{p}_2 = (3)$, $\mathfrak{p}_2 \mathfrak{p}_4 = (1 - 2\sqrt{-5})$ und $\mathfrak{p}_3 \mathfrak{p}_4 = (7)$. Insgesamt gilt also

$$(21) = (3) \cdot (7) = (\mathfrak{p}_1 \mathfrak{p}_2)(\mathfrak{p}_3 \mathfrak{p}_4) \quad , \quad \text{ebenso} \quad (21) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (\mathfrak{p}_1 \mathfrak{p}_3)(\mathfrak{p}_2 \mathfrak{p}_4).$$

Bis auf die Reihenfolge der „Primfaktoren“ \mathfrak{p}_i stimmen die Zerlegungen also überein.

Definition 5.13 Sei $\phi : R \rightarrow S$ Ringhomomorphismus. Dann nennt man $\ker(\phi) = \phi^{-1}(\{0_S\})$ den **Kern** und $\text{im}(\phi) = \phi(R)$ das **Bild** von ϕ .

Teil (i) der folgenden Proposition zeigt, dass Kerne von Ringhomomorphismen stets Ideale sind, in Analogie zur Aussage aus der Gruppentheorie, dass es sich bei Kernen von Gruppenhomomorphismen stets um Normalteiler handelt.

Proposition 5.14 Seien R, S Ringe und $\phi : R \rightarrow S$ ein Ringhomomorphismus.

- (i) Ist J ein Ideal in S , dann ist $\phi^{-1}(J)$ ein Ideal in R .
- (ii) Ist I ein Ideal in R und ϕ surjektiv, dann ist $\phi(I)$ ein Ideal in S .

Beweis: zu (i) Wegen $\phi(0_R) = 0_S$ und $0_S \in J$ ist $0_R \in \phi^{-1}(J)$ enthalten. Seien nun $a, b \in \phi^{-1}(J)$ und $r \in R$ vorgegeben. Dann gilt $\phi(a), \phi(b) \in J$, somit auch $\phi(a+b) \in J$ und $a+b \in \phi^{-1}(J)$. Ebenso ist $\phi(ra) = \phi(r)\phi(a) \in J$ und folglich $ra \in \phi^{-1}(J)$.

zu (ii) Wegen $0_R \in I$ gilt $0_S = \phi(0_R) \in \phi(I)$. Seien nun $a, b \in \phi(I)$ und $s \in S$ vorgegeben. Wegen $a, b \in \phi(I)$ gibt es $a', b' \in I$ mit $a = \phi(a')$ und $b = \phi(b')$. Es folgt $a' + b' \in I$ und $a + b = \phi(a') + \phi(b') = \phi(a' + b') \in \phi(I)$. Auf Grund der Surjektivität gibt es ein $r \in R$ mit $\phi(r) = s$, und mit a' ist auch ra' in I enthalten. Es folgt $sa = \phi(r)\phi(a') \in \phi(I)$.
□

Ohne die Voraussetzung der Surjektivität ist Teil (ii) der Proposition im allgemeinen falsch. Betrachtet man z.B. die Inklusionsabbildung $\iota : \mathbb{Z} \rightarrow \mathbb{Q}$, $a \mapsto a$, dann ist $(2) = \{2a \mid a \in \mathbb{Z}\}$ ein Ideal in \mathbb{Z} , aber die Menge $M = \{2a \mid a \in \mathbb{Z}\}$ ist kein Ideal in \mathbb{Q} : Es gilt $\frac{1}{2} \in \mathbb{Q}$, $2 \in M$, aber $\frac{1}{2} \cdot 2 \notin M$.

Man überprüft leicht, dass das Bild $\text{im}(\phi)$ eines Ringhomomorphismus $\phi : R \rightarrow S$ zwar im allgemeinen kein Ideal, aber immer ein Teiling von S ist. Wie bei den Gruppen oder den linearen Abbildungen zeigt man, dass ein Homomorphismus $\phi : R \rightarrow S$ genau dann injektiv ist, wenn $\ker(\phi) = \{0_R\}$ gilt.

§ 6. Faktorringe und Restklassenringe

Zusammenfassung. In der Gruppentheorie haben wir aus einer Gruppe G und einem Normalteiler $N \triangleleft G$ eine neue Gruppe G/N konstruiert, die sog. Faktorgruppe von G modulo N . Mit dem gleichen Ansatz werden wir in diesem Abschnitt einem Ring R und einem Ideal I den **Faktorring** R/I zuordnen. Auf diesem Weg erhält man zum Beispiel für jedes $n \in \mathbb{N}$ den bereits aus der Linearen Algebra bekannten Restklassenring $\mathbb{Z}/n\mathbb{Z}$. In der Körpertheorie werden wir sehen, dass die Faktorringe eine wichtige Rolle bei der Konstruktion von algebraischen Erweiterungen spielen.

Das Ziel dieses Abschnitts besteht, neben der Konstruktion der Faktorringe und der Betrachtung von Beispielen, im Wesentlichen darin, die Sätze, die uns für Faktorgruppen bereits aus der Algebra-Vorlesung bekannt sind, auf die Faktorringe zu übertragen. Für konkrete Anwendungen ist es von Bedeutung, und welchen Bedingungen ein Faktorring R/I ein Integritätsbereich oder sogar ein Körper ist. Dieser Frage gehen wir am Ende des Kapitels nach.

Wichtige Grundbegriffe

- Definition des Faktorring R/I (für einen Ring R und ein Ideal I)
- kanonischer Epimorphismus $\pi_I : R \rightarrow R/I$

Zentrale Sätze

- Homomorphiesatz für Ringe
- Korrespondenzsatz für Ringe
- Faktorringe von Primidealen sind Integritätsbereiche
- Faktorringe von maximalen Idealen sind Körper

In der Gruppentheorie haben wir gesehen, wie die Normalteiler einer Gruppe zur Definition von neuen Gruppen genutzt werden können. Eine ähnliche Rolle spielen die Ideale in der Ringtheorie.

Definition 6.1 Sei R ein Ring, I ein Ideal und $a \in R$. Dann nennen wir die Menge

$$a + I = \{a + i \mid i \in I\}$$

die **Nebenklasse** von a modulo I . Die Menge $\{a + I \mid a \in R\}$ aller Nebenklassen von Elementen aus R bezeichnen wir mit R/I .

Proposition 6.2 Sei R ein Ring und I ein Ideal. Dann ist die Relation auf R gegeben durch

$$a \equiv b \pmod{I} \iff b - a \in I$$

eine Äquivalenzrelation, und die Elemente von R/I sind genau die Äquivalenzklassen dieser Relation. Man spricht in diesem Zusammenhang von einer **Kongruenzrelation** und bezeichnet zwei Elemente a, b in derselben Äquivalenzklasse als **kongruent modulo I** .

Beweis: Für alle $a \in R$ gilt $a - a = 0 \in I$ und somit $a \equiv a \pmod I$. Also ist die Relation reflexiv. Für alle $a, b \in R$ gilt die Implikation

$$a \equiv b \pmod I \Rightarrow b - a \in I \Rightarrow (-1)(b - a) \in I \Rightarrow a - b \in I \Rightarrow b \equiv a \pmod I,$$

also ist die Relation symmetrisch. Zum Nachweis der Transitivität seien $a, b, c \in R$ mit $a \equiv b \pmod I$ und $b \equiv c \pmod I$ vorgegeben. Dann gilt $b - a \in I$ und $c - b \in I$. Es folgt $c - a = (c - b) + (b - a) \in I$ und damit $a \equiv c \pmod I$.

Nun zeigen wir noch, dass für ein beliebig vorgegebenes $a \in R$ die Nebenklasse $a + I$ mit der Äquivalenzklasse von a übereinstimmt. Nach Definition liegt $b \in I$ genau dann in der Äquivalenzklasse von a , wenn $a \equiv b \pmod I$ gilt, was nach Definition $b - a \in I$ bedeutet. Dies wiederum ist gleichbedeutend mit $b = a + (b - a) \in a + I$. \square

Nach Definition sind zwei Elemente $a, b \in R$ also genau dann kongruent modulo I , wenn ihre Kongruenzklassen übereinstimmen. Aus der Algebra ist bekannt, dass zwei Äquivalenzklassen entweder disjunkt oder gleich sind. Es gilt also die Äquivalenz

$$a \equiv b \pmod I \Leftrightarrow b - a \in I \Leftrightarrow a + I = b + I \Leftrightarrow b \in a + I. \quad (6.1)$$

Ein wichtiger Spezialfall ist der Ring $R = \mathbb{Z}$ mit den Idealen der Form $I = n\mathbb{Z}$, wobei $n \in \mathbb{N}$ ist. Hier wird die Nebenklasse $a + n\mathbb{Z}$ einer Zahl $a \in \mathbb{Z}$ häufig nur mit \bar{a} bezeichnet. Ein Problem bei dieser Notation besteht darin, dass sie die natürliche Zahl n nicht beinhaltet; so kann $\bar{1}$ für $1 + 2\mathbb{Z}$, $1 + 3\mathbb{Z}$ oder für $1 + n\mathbb{Z}$ mit irgendeinem anderen n stehen. Bei Verwendung der Notation muss also darauf geachtet werden, dass sich das n aus dem Kontext heraus ergibt.

Proposition 6.3 Die Menge $\mathbb{Z}/n\mathbb{Z}$ der Kongruenzklassen ist n -elementig, es gilt

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}, 0 \leq a < n\}.$$

Beweis: Nach Definition gilt $\mathbb{Z}/n\mathbb{Z} = \{\bar{b} \mid b \in \mathbb{Z}\}$. Ist nun $b \in \mathbb{Z}$ beliebig vorgegeben, dann erhält man nach Division mit Rest Elemente $q, a \in \mathbb{Z}$ mit $b = qn + a$ und $0 \leq a < n$. Es gilt also $b - a = nq \in (n)$, und auf Grund der Äquivalenz (6.1) folgt $\bar{a} = \bar{b}$. Dies zeigt, dass $\mathbb{Z}/n\mathbb{Z}$ aus den angegebenen Klassen besteht.

Um zu sehen, dass die Klassen \bar{a} mit $0 \leq a < n$ verschieden sind, seien $a_1, a_2 \in \mathbb{Z}$ mit $0 \leq a_1, a_2 < n$ und $\bar{a}_1 = \bar{a}_2$ vorgegeben. Nach (6.1) gilt dann $a_1 - a_2 \in (n)$, es existiert also ein $q \in \mathbb{Z}$ mit $a_1 - a_2 = qn$. Wegen $|a_1 - a_2| < n$ ist dies nur für $q = 0$ möglich. Es gilt somit $a_1 = a_2$. \square

Für die Kongruenzklasse modulo (n) eines Elements $a \in \mathbb{Z}$ verwendet man häufig die Schreibweise \bar{a} , und man schreibt $a \equiv b \pmod n$, wenn zwei Elemente kongruent modulo (n) sind.

In der Algebra hatten wir den Begriff des Repräsentantensystems für eine Menge von Äquivalenzklassen eingeführt. Dieser Begriff lässt sich auch hier verwenden. Wie wir gerade gesehen haben, ist für jedes $n \in \mathbb{N}$ die Menge $\{a \in \mathbb{Z} \mid 0 \leq a < n\}$ ein Repräsentantensystem von $\mathbb{Z}/n\mathbb{Z}$. Für Ideale in Polynomringen gilt

Proposition 6.4 Sei K ein Körper, $R = K[x]$ und $f \in K[x]$ ein Polynom vom Grad $n \geq 1$. Dann ist die Teilmenge $S = \{g \in K[x] \mid g \neq 0, \text{grad}(g) < n\} \cup \{0\}$ von $K[x]$ ein Repräsentantensystem von $R/(f)$.

Beweis: Sei $\phi : S \rightarrow K[x]/(f)$ gegeben durch $g \mapsto g + (f)$. Ein Repräsentantensystem liegt vor, wenn die Abbildung ϕ bijektiv ist. Zunächst beweisen wir die Surjektivität von ϕ . Sei $\bar{g} \in K[x]/(f)$ vorgegeben und $g \in K[x]$ mit $\bar{g} = g + (f)$. Durch Division mit Rest erhalten wir Polynome $q, r \in K[x]$ mit $g = qf + r$ mit $r = 0$ oder $\text{grad}(f) < n$. Nach Definition ist r in S enthalten. Außerdem gilt $g - r \in (f)$ und somit $\phi(r) = r + (f) = g + (f) = \bar{g}$.

Seien nun $g_1, g_2 \in S$ mit $\phi(g_1) = \phi(g_2)$ vorgegeben. Dann folgt $g_1 + (f) = g_2 + (f)$, also $g_1 - g_2 \in (f)$. Es gibt also ein $q \in K[x]$ mit $g_1 - g_2 = qf$. Im Fall $q \neq 0$ wäre $g_1 - g_2 = qf$ vom Grad $\geq n$. Wegen $g_i = 0$ oder $\text{grad}(g_i) < n$ für $i = 1, 2$ ist das jedoch ausgeschlossen. Also muss $g_1 = g_2$ gelten. \square

Proposition 6.5 Sei R ein Ring und I ein Ideal. Dann gibt es (eindeutig bestimmte) Verknüpfungen $+$ und \cdot auf R/I mit der Eigenschaft

$$(a + I) + (b + I) = (a + b) + I \quad \text{und} \quad (a + I) \cdot (b + I) = ab + I \quad \text{für alle } a, b \in R.$$

Beweis: Nach Satz 4.10 aus der Algebra-Vorlesung genügt es zu zeigen, dass für alle $a_0, a, b_0, b \in I$ aus $a_0 \equiv a \pmod I$ und $b_0 \equiv b \pmod I$ jeweils $(a_0 + b_0) + I = (a + b) + I$ und $a_0 b_0 + I = ab + I$ folgt. Auf Grund der Voraussetzung gilt $i = a - a_0 \in I$ und $j = b - b_0 \in I$. Es folgt $(a + b) - (a_0 + b_0) = (a - a_0) + (b - b_0) = i + j \in I$, also $(a + b) \in (a_0 + b_0) + I$ und somit $(a + b) + I = (a_0 + b_0) + I$. Auf Grund der Rechnung

$$ab - a_0 b_0 = ab - ab_0 + ab_0 - a_0 b_0 = a(b - b_0) + (a - a_0)b_0 = aj + b_0 i$$

gilt ebenso $ab - a_0 b_0 \in I$, also $ab \in a_0 b_0 + I$ und somit $ab + I = a_0 b_0 + I$. \square

Satz 6.6 Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann ist R/I mit den beiden soeben definierten Verknüpfungen ein Ring, den man als **Faktorring** bezeichnet. Die Abbildung $\pi_I : R \rightarrow R/I$ gegeben $a \mapsto a + I$ ist ein Epimorphismus von Ringen, der sog. **kanonische Epimorphismus**.

Beweis: Wir verwenden die für alle $a, b \in R$ geltenden Gleichungen $(a + I) + (b + I) = (a + b) + I$ und $(a + I) \cdot (b + I) = (ab) + I$, um die Gültigkeit der Ringaxiome in R/I auf die Ringeigenschaften von R zurückzuführen. Beginnen wir mit den Axiomen der Addition. Sind $a, b, c \in R$ vorgegeben, dann gilt

$$\begin{aligned} ((a + I) + (b + I)) + (c + I) &= ((a + b) + I) + (c + I) = ((a + b) + c) + I = \\ (a + (b + c)) + I &= (a + I) + ((b + c) + I) = (a + I) + ((b + I) + (c + I)). \end{aligned}$$

Also ist das Assoziativgesetz in R/I erfüllt. Ferner gilt $(a + I) + (0 + I) = ((a + 0) + I) = a + I$ und ebenso $(0 + I) + (a + I) = (0 + a) + I = a + I$, somit besitzt $0 + I$ in R/I die Eigenschaften des Nullelements. Aus $(a + I) + ((-a) + I) = (a + (-a)) + I = 0 + I$ und $((-a) + I) + (a + I) = ((-a) + a) + I = 0 + I$ folgt, dass die Nebenklasse $(-a) + I$ bezüglich der Addition ein zu $a + I$ inverses Element ist. Also hat jedes Element in R/I ein Negatives. Schließlich gilt wegen $(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I)$ auch das Kommutativgesetz. Die Axiome der Multiplikation und das Distributivgesetz verifiziert man nach dem gleichen Schema. Die Nebenklasse $1 + I$ übernimmt in R/I die Rolle des Einselements.

Zum Schluss überprüfen wir die Homomorphismus-Eigenschaft der Abbildung π_I . Sind $a, b \in R$, dann gilt $\pi_I(a + b) = (a + b) + I = (a + I) + (b + I) = \pi_I(a) + \pi_I(b)$, ebenso $\pi_I(ab) = (ab) + I = (a + I)(b + I) = \pi_I(a)\pi_I(b)$ und $\pi_I(1) = 1 + I$.

Offenbar ist π_I surjektiv, denn jedes Element in R/I hat die Form $a + I$ für ein $a \in R$, es liegt also wegen $\pi_I(a) = a + I$ im Bild von π_I . \square

Als Beispiel betrachten wir den Ring $\mathbb{Z}/4\mathbb{Z}$. Es sei noch einmal daran erinnert, dass $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ Kurzschreibweisen für die Elemente $0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}$ sind. Die Addition und Multiplikation des Rings $\mathbb{Z}/4\mathbb{Z}$ sind durch die folgenden Verknüpfungstabellen gegeben.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{1}$	$\bar{2}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Beispielsweise gilt $\bar{2} + \bar{3} = \bar{5} = \bar{1}$, wobei die Gleichung $5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$ durch $5 - 1 = 4 \in 4\mathbb{Z}$ zu Stande kommt. Auf dieselbe Weise überprüft man $\bar{2} \cdot \bar{3} = \bar{6} = \bar{2}$, denn es ist $6 + 4\mathbb{Z} = 2 + 4\mathbb{Z}$ wegen $6 - 2 = 4 \in 4\mathbb{Z}$. Man beachte, dass $\mathbb{Z}/4\mathbb{Z}$ kein Integritätsbereich ist: Es gilt $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$, obwohl $\bar{2} \neq \bar{0}$ ist.

Neben $\{0, 1, 2, 3\}$ ist auch $\{1, 2, 3, 4\}$ ein Repräsentantensystem von $\mathbb{Z}/4\mathbb{Z}$. Es gilt also auch $\mathbb{Z}/4\mathbb{Z} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Mit dieser Darstellung der Elemente sehen die Verknüpfungstabellen folgendermaßen aus.

+	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$
$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{4}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

·	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{4}$

Auch hier überprüfen in jeder Tabelle exemplarisch je einen Eintrag. Es gilt $\bar{4} + \bar{3} = \bar{7} = \bar{3}$, denn wegen $7 - 3 = 4 \in 4\mathbb{Z}$ ist $7 + 4\mathbb{Z} = 3 + 4\mathbb{Z}$. Ebenso findet man $\bar{3} \cdot \bar{4} = \bar{12} = \bar{4}$, denn wegen $12 - 4 = 8 \in 4\mathbb{Z}$ ist $12 + 4\mathbb{Z} = 4 + 4\mathbb{Z}$. Man beachten, dass $\bar{4}$ das Null- und $\bar{1}$ das Einselement von $\mathbb{Z}/4\mathbb{Z} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ ist.

Satz 6.7 Sei $n \in \mathbb{N}$. Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n eine Primzahl ist.

Beweis: „ \Rightarrow “ Im Fall $n = 1$ ist $\mathbb{Z}/n\mathbb{Z}$ ein Nullring und damit kein Körper. Ist $n > 1$ keine Primzahl, dann gibt es $r, s \in \mathbb{N}$ mit $1 < r, s < n$ und $n = rs$. Es folgt dann $\bar{r}, \bar{s} \neq \bar{0}$ und $\bar{r}\bar{s} = \bar{n} = \bar{0}$. Dies zeigt, dass $\mathbb{Z}/n\mathbb{Z}$ kein Integritätsbereich ist. Nach Definition 1.4 ist $\mathbb{Z}/n\mathbb{Z}$ damit auch kein Körper.

„ \Leftarrow “ Sei $p = n$ eine Primzahl. Dann enthält $\mathbb{Z}/p\mathbb{Z}$ jedenfalls mehr als ein Element und ist damit kein Nullring. Sei nun $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ ein Element ungleich Null und $a \in \mathbb{Z}$ mit $\bar{a} = a + p\mathbb{Z}$. Wegen $a + p\mathbb{Z} \neq \bar{0}$ ist a kein Vielfaches von p , und weil p eine Primzahl ist, muss der größte gemeinsame Teiler von a und p gleich 1 sein. Nach dem Lemma von Bézout gibt es $x, y \in \mathbb{Z}$ mit $xa + yp = 1$. Es folgt $\bar{x}\bar{a} = xa + p\mathbb{Z} = (xa + p\mathbb{Z}) + (0 + p\mathbb{Z}) = (xa + p\mathbb{Z}) + (yp + p\mathbb{Z}) = (xa + yp) + p\mathbb{Z} = 1 + p\mathbb{Z} = \bar{1}$. Also ist \bar{a} in $\mathbb{Z}/p\mathbb{Z}$ invertierbar. Somit haben wir gezeigt, dass jedes Element $\bar{a} \neq \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$ ein Inverses besitzt, und folglich ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. \square

Ist p eine Primzahl, dann verwendet man für den Körper $\mathbb{Z}/p\mathbb{Z}$ auch die Bezeichnung \mathbb{F}_p . (Dabei steht der Buchstabe \mathbb{F} für „field“, engl. „Körper“.)

Der euklidische Algorithmus kann verwendet werden, um die multiplikativen Inversen von Elementen der Körper \mathbb{F}_p zu bestimmen. Sei beispielsweise $p = 43$ und $\bar{a} = \overline{37} \in \mathbb{F}_{43}$. Der euklidische Algorithmus liefert für die Gleichung $37x + 43y = 1$ die Lösung $x = 7, y = -6$. In \mathbb{F}_{43} gilt also $\overline{37} \cdot \bar{7} = \bar{1}$ und $\overline{37}^{-1} = \bar{7}$.

Als weiteres Beispiel betrachten wir den Körper \mathbb{F}_{13} . Mit dem soeben beschriebenen Verfahren findet man hier für die Elemente $\neq \bar{0}$ die folgenden multiplikativen Inversen.

\bar{a}	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$	$\bar{11}$	$\bar{12}$
\bar{a}^{-1}	$\bar{1}$	$\bar{7}$	$\bar{9}$	$\bar{10}$	$\bar{8}$	$\bar{11}$	$\bar{2}$	$\bar{5}$	$\bar{3}$	$\bar{4}$	$\bar{6}$	$\bar{12}$

Auch mit Polynomringen lassen sich Restklassenringe bilden. Sei zum Beispiel $R = \mathbb{R}[x]$ und $I = (f)$ mit $f = x^2 + 1$. Dann gilt in R/I die Gleichung

$$(x + I) \cdot (x + I) = x^2 + I = (x^2 + (-1)(x^2 + 1)) + I = (-1) + I$$

wobei im zweiten Schritt verwendet wurde, dass $(-1)(x^2 + 1)$ in I liegt. Man überprüft leicht, dass durch $\phi : \mathbb{R} \rightarrow R/I, a \mapsto a + I$ ein Monomorphismus von Ringen definiert ist. Die Homomorphismus-Eigenschaft ist offensichtlich, und ist $a \in \mathbb{R}$ ein Element im Kern, dann folgt aus $a + I = 0 + I$, dass a in I liegt, also von $x^2 + 1$ geteilt wird. Wegen $\text{grad}(x^2 + 1) = 2$ ist dies nur für $a = 0$ möglich. Mit Hilfe von Satz 2.12 erhält nun man einen Erweiterungsring C von \mathbb{R} und einen Isomorphismus $\hat{\phi} : C \rightarrow R/I$ mit $\hat{\phi}|_{\mathbb{R}} = \phi$. Für das Element $i = \hat{\phi}^{-1}(x + I)$ gilt

$$i^2 = \hat{\phi}^{-1}((x + I)^2) = \hat{\phi}^{-1}(x^2 + I) = \hat{\phi}^{-1}((-1) + I) = -1.$$

Wir werden in Kürze noch sehen, dass C ein Körper ist. Es handelt sich dabei um den Körper \mathbb{C} der komplexen Zahlen!

Wie in der Gruppen- gibt es auch in der Ringtheorie induzierte Homomorphismen und einen Homomorphiesatz.

Proposition 6.8 Sei $\phi : R \rightarrow R'$ ein Ringhomomorphismus und $I \subseteq R$ ein Ideal mit $I \subseteq \ker(\phi)$. Dann gibt es einen eindeutig bestimmten Homomorphismus

$$\bar{\phi} : R/I \longrightarrow R' \quad \text{mit} \quad \bar{\phi}(a + I) = \phi(a) \quad \text{für alle} \quad a \in R.$$

Man bezeichnet ihn als den von ϕ **induzierten** Homomorphismus.

Beweis: Für die Existenz der Abbildung $\bar{\phi}$ genügt es nach Satz 4.10 aus der Algebra-Vorlesung zu zeigen, dass für alle $a_0, a \in I$ aus $a_0 \equiv a \pmod{I}$ jeweils $\phi(a) = \phi(a_0)$ folgt. Auf Grund der Voraussetzung gilt $a - a_0 \in I$ und damit auch $a - a_0 \in \ker(\phi)$. Es folgt $\phi(a) = \phi(a - a_0 + a_0) = \phi(a - a_0) + \phi(a_0) = 0_{R'} + \phi(a_0) = \phi(a_0)$.

Dass $\bar{\phi}$ ein Homomorphismus von Ringen ist, folgt unmittelbar aus der bewiesenen Gleichung und der Homomorphismus-Eigenschaft von ϕ . Zunächst gilt $\bar{\phi}(1 + I) = \phi(1) = 1_{R'}$. Seien $\bar{a}, \bar{b} \in R/I$ vorgegeben und $a, b \in R$ mit $\bar{a} = a + I, \bar{b} = b + I$. Dann gilt $\bar{\phi}(\bar{a} + \bar{b}) = \bar{\phi}((a + I) + (b + I)) = \bar{\phi}((a + b) + I) = \phi(a + b) = \phi(a) + \phi(b) = \bar{\phi}(a + I) + \bar{\phi}(b + I) = \bar{\phi}(\bar{a}) + \bar{\phi}(\bar{b})$. Der Beweis der Gleichung $\bar{\phi}(\bar{a}\bar{b}) = \bar{\phi}(\bar{a})\bar{\phi}(\bar{b})$ läuft analog. \square

Satz 6.9 (Homomorphiesatz für Ringe)

Sei $\phi : R \rightarrow R'$ ein Homomorphismus von Ringen und $I = \ker(\phi)$. Dann induziert ϕ einen Isomorphismus $\bar{\phi} : R/I \xrightarrow{\sim} \text{im}(\phi)$ von Ringen.

Beweis: Auf Grund der Proposition existiert ein Homomorphismus $\bar{\phi} : R/I \rightarrow R'$ mit $\bar{\phi}(a + I) = \phi(a)$ für alle $a \in R$. Insbesondere gilt $\text{im}(\phi) = \text{im}(\bar{\phi})$, so dass durch $\bar{\phi}$ ein surjektiver Homomorphismus auf $\text{im}(\phi)$ gegeben ist. Zum Nachweis der Injektivität sei $\bar{a} \in \ker(\bar{\phi})$ vorgegeben. Ist $a \in R$ mit $a + I = \bar{a}$, dann gilt $\phi(a) = \bar{\phi}(\bar{a}) = 0_{R'}$ und somit $a \in I$. Es folgt $\bar{a} = a + I = 0 + I$. Der Kern von $\bar{\phi}$ ist somit gleich $\{0 + I\}$, und folglich ist $\bar{\phi}$ injektiv. \square

Satz 6.10 (Korrespondenzsatz für Ideale)

Sei R ein Ring, I ein Ideal und $\pi : R \rightarrow R/I$ der kanonische Epimorphismus. Sei $\bar{\mathcal{J}}$ die Menge der Ideale von R/I und \mathcal{J}_I die Menge der Ideale J von R mit $J \supseteq I$.

- (i) Die Zuordnungen $\phi : \mathcal{J}_I \rightarrow \bar{\mathcal{J}}, J \mapsto \pi(J)$ und $\psi : \bar{\mathcal{J}} \rightarrow \mathcal{J}_I, \bar{J} \mapsto \pi^{-1}(\bar{J})$ sind bijektiv und zueinander invers.
- (ii) Für alle Ideale $J, K \in \mathcal{J}_I$ gilt $J \subseteq K \Leftrightarrow \pi(J) \subseteq \pi(K)$.

Beweis: zu (i) Zum Nachweis von $\psi \circ \phi = \text{id}_{\mathcal{J}_I}$ muss für jedes $J \in \mathcal{J}_I$ gezeigt werden, dass $\pi^{-1}(\pi(J)) = J$ gilt. Ist $a \in J$, dann gilt $\pi(a) \in \pi(J)$ und damit auch $a \in \pi^{-1}(\pi(J))$. Sei umgekehrt $a \in \pi^{-1}(\pi(J))$ vorgegeben. Dann gilt $\pi(a) \in \pi(J)$, es gibt also ein $b \in J$ mit $\pi(a) = \pi(b)$. Wegen $\pi(a - b) = \pi(a) - \pi(b) = 0$ folgt $a - b \in I$, denn I ist offenbar genau der Kern des kanonischen Epimorphismus. Damit liegt auch $a = (a - b) + b \in J$.

Nun beweisen wir $\phi \circ \psi = \text{id}_{\bar{\mathcal{J}}}$ und zeigen dafür, dass $\pi(\pi^{-1}(\bar{J})) = \bar{J}$ für jedes Ideal \bar{J} von R/I erfüllt ist. Sei zunächst $\bar{a} \in \bar{J}$ vorgegeben und $a \in R$ mit $a + I = \bar{a}$. Dann gilt $\pi(a) = \bar{a} \in \bar{J}$ und somit $a \in \pi^{-1}(\bar{J})$. Dies wiederum bedeutet $\pi(a) \in \pi(\pi^{-1}(\bar{J}))$. Die Inklusion $\pi(\pi^{-1}(\bar{J})) \subseteq \bar{J}$ ist nach Definition von Bild- und Urbildmenge klar.

zu (ii) Aus $J \subseteq K$ folgt offenbar $\pi(J) \subseteq \pi(K)$. Ist umgekehrt $\pi(J) \subseteq \pi(K)$ vorausgesetzt, dann folgt unter Anwendung des Ergebnisses aus Teil (i) $J = \pi^{-1}(\pi(J)) \subseteq \pi^{-1}(\pi(K)) = K$. \square

Wir werden den Korrespondenzsatz nun anwenden, um die Primideale und die maximalen Ideale über ihre Restklassenringe zu charakterisieren.

Lemma 6.11 Ein Ring ist genau dann ein Körper, wenn (0) und (1) die einzigen Ideale des Rings sind und $(0) \neq (1)$ gilt.

Beweis: „ \Rightarrow “ Sei R ein Körper und $I \subseteq R$ ein Ideal. Im Fall $I \neq (0)$ sei $a \in I$ ein beliebiges Element ungleich Null. Dann liegt auch $1 = a^{-1}a$ in I , und es folgt $I = (1)$. Auf Grund der Körpereigenschaft gilt auch $0 \neq 1$ und somit $(0) \neq (1)$.

„ \Leftarrow “ Sei R ein Ring mit der Eigenschaft, dass $(0) \neq (1)$ die einzigen Ideale in R sind. Ist $a \in R$ ein beliebiges Element, dann gilt entweder $(a) = (0)$ oder $(a) = (1)$. Im ersten Fall ist $a = 0$, im zweiten liegt 1 in (a) , und es gibt somit ein $r \in R$ mit $ra = 1$. Also ist a in diesem Fall eine Einheit. Wir haben somit gezeigt, dass jedes Element ungleich Null in R invertierbar ist. Dies zeigt, dass R entweder ein Nullring oder ein Körper ist. Aber wegen $(0) \neq (1)$ gilt $0 \neq 1$, und folglich ist R kein Nullring. \square

Satz 6.12 Sei R ein Ring, $\mathfrak{p} \subseteq R$ ein Ideal und $\bar{R} = R/\mathfrak{p}$.

- (i) Genau dann ist \mathfrak{p} ein Primideal, wenn \bar{R} ein Integritätsbereich ist.
- (ii) Genau dann ist \mathfrak{p} ein maximales Ideal, wenn \bar{R} ein Körper ist.

Beweis: „ \Rightarrow “ Wegen $\mathfrak{p} \neq (1)$ besteht \bar{R} aus mehr als einem Element, ist also kein Nullring. Seien nun $\bar{a}, \bar{b} \in \bar{R}$ mit $\bar{a}\bar{b} = 0 + \mathfrak{p}$ vorgegeben. Sind $a, b \in R$ mit $\bar{a} = a + \mathfrak{p}$ und $\bar{b} = b + \mathfrak{p}$, dann gilt $(ab) + \mathfrak{p} = (a + \mathfrak{p})(b + \mathfrak{p}) = \bar{a}\bar{b} = 0 + \mathfrak{p}$ und folglich $ab \in \mathfrak{p}$. Aus der Primideal-Eigenschaft erhalten wir $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ und somit $\bar{a} = 0 + \mathfrak{p}$ oder $\bar{b} = 0 + \mathfrak{p}$.

„ \Leftarrow “ Ist \bar{R} ein Integritätsbereich, dann ist \bar{R} insbesondere kein Nullring. Deshalb muss $\mathfrak{p} \neq (1)$ gelten. Seien nun $a, b \in R$ mit $ab \in \mathfrak{p}$ vorgegeben. Dann gilt $(a + \mathfrak{p})(b + \mathfrak{p}) = (ab) + \mathfrak{p} = 0 + \mathfrak{p}$. Weil \bar{R} ein Integritätsbereich ist, folgt daraus $a + \mathfrak{p} = 0 + \mathfrak{p}$ oder $b + \mathfrak{p} = 0 + \mathfrak{p}$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

zu (ii) Auf Grund des Korrespondenzsatzes gibt es eine Bijektion zwischen den Idealen J von R mit $\mathfrak{p} \subseteq J \subseteq (1)$ und den Idealen von \bar{R} . Ist \mathfrak{p} ein maximales Ideal, dann ist $\mathfrak{p} \subsetneq (1)$, und für jedes Ideal J mit $\mathfrak{p} \subseteq J \subseteq (1)$ gilt $\mathfrak{p} = J$ oder $J = (1)$. Dies bedeutet, dass der Faktorring R/\mathfrak{p} genau zwei Ideale besitzt, nämlich (0) oder (1) . Also ist R/\mathfrak{p} ein Körper. Setzen wir dies umgekehrt voraus, dann sind $(0) \neq (1)$ die einzigen beiden Ideale im Faktorring. Es gilt dann $\mathfrak{p} \subsetneq (1)$ in R , denn ansonsten gäbe es im Faktorring nur ein einziges Ideal. Zugleich ist \mathfrak{p} maximal, denn jedes Ideal J mit $\mathfrak{p} \subsetneq J \subsetneq (1)$ würde ein Ideal \bar{J} mit $(0) \subsetneq \bar{J} \subsetneq (1)$ im Faktorring liefern. \square

Folgerung 6.13 Jedes maximale Ideal ist ein Primideal.

Beweis: Dies folgt direkt aus Satz 6.12, da jeder Körper ein Integritätsbereich ist. \square

Aus den Sätzen 6.12 und 6.7 folgt zum Beispiel, dass im Ring \mathbb{Z} die Hauptideale (p) von Primzahlen p alle maximale Ideale sind. Nach Folgerung 6.13 sind dies auch alle Primideale. Dass umgekehrt nicht jedes Primideal ein maximales Ideal ist, sieht man am Nullideal (0) von \mathbb{Z} . Wie man an Hand der Definition unmittelbar überprüft, ist (0) ein Primideal. Andererseits ist es z.B. wegen $(0) \subsetneq (2) \subsetneq (1)$ kein maximales Ideal.

§ 7. Der Chinesische Restsatz

Zusammenfassung. In diesem Abschnitt lernen wir eine erste wichtige Anwendung der Faktorringe kennen, den *Chinesischen Restsatz*. In seiner klassischen Form besagt er, dass jedes System von Kongruenzen zu paarweise teilerfremden Zahlen eine Lösung besitzt. Beispielsweise besitzt das System $x \equiv 3 \pmod{5}$ und $x \equiv 4 \pmod{7}$ die Lösung $x = 18$. Wir formulieren und beweisen aber eine allgemeinere Fassung, in der \mathbb{Z} durch einen beliebigen Ring R und die teilerfremden Zahlen durch teilerfremde Ideale ersetzt werden. Anschließend diskutieren wir einige Anwendungen. Unter anderem werden wir sehen, dass der Chinesische Restsatz auch bei der Lösung von Polynomgleichungen verwendet werden kann. Nebenbei stellt sich heraus, dass die Nullstellenzahl von Polynomen über Nicht-Integritätsarbeiten auch höher als der Polynomgrad sein kann, was für Körper nach Folgerung 4.8 ausgeschlossen ist.

Wichtige Grundbegriffe

– Teilerfremdheit bei Idealen

Zentrale Sätze

– Chinesischer Restsatz für Ringe

Definition 7.1 Sei R ein Ring. Zwei Ideale I, J in R werden **teilerfremd** genannt, wenn $I + J = (1)$ gilt, wobei (1) wie üblich das Einheitsideal in R bezeichnet.

Diese Bezeichnung wird durch das folgende Lemma gerechtfertigt.

Lemma 7.2 Sei $R = \mathbb{Z}$, und seien $m, n \in \mathbb{N}$. Genau dann sind die Ideale $I = (m)$ und $J = (n)$ teilerfremd, wenn m, n als natürliche Zahlen teilerfremd sind.

Beweis: Sind m und n teilerfremd, dann gibt es nach dem Lemma von Bézout $a, b \in \mathbb{Z}$ mit $am + bn = 1$. Es folgt $1 \in (m) + (n) = I + J$, also $I + J = (1)$. Setzen wir umgekehrt $I + J = (1)$ voraus. Dann liegt 1 in $I + J$, es gibt also $a, b \in \mathbb{Z}$ mit $1 = am + bn$. Ist d ein gemeinsamer Teiler von m und n , dann teilt d auf Grund der Gleichung auch 1 . Dies zeigt, dass m und n teilerfremd sind. \square

Lemma 7.3 Sei R ein Ring, und seien I_1, \dots, I_m, J Ideale in R , wobei I_1, \dots, I_m jeweils teilerfremd zu J sind. Dann ist auch das Produkt $I_1 \cdot \dots \cdot I_m$ teilerfremd zu J .

Beweis: Wir beweisen die Aussage durch vollständige Induktion über m . Sei zunächst $m = 2$. Dann ist die Gleichung $I_1 I_2 + J = (1)$ zu zeigen. Nun gilt

$$(1) = (1)(1) = (I_1 + J)(I_2 + J) = I_1 I_2 + J I_2 + I_1 J + J J \subseteq I_1 I_2 + J$$

und somit $I_1 I_2 + J = (1)$. Sei nun die Behauptung für m bereits bewiesen, und seien I_1, \dots, I_{m+1}, J Ideale, welche die Voraussetzung des Lemmas erfüllen. Nach Induktionsannahme sind die Ideale $I = I_1 \cdot \dots \cdot I_m$ und I_{m+1} beide teilerfremd zu J . Auf Grund des bereits bewiesenen Falls $m = 2$ ist auch $I I_{m+1} = I_1 \cdot \dots \cdot I_m \cdot I_{m+1}$ teilerfremd zu J . \square

Proposition 7.4 Sei R ein Ring, und seien I_1, \dots, I_m Ideale in R , die paarweise teilerfremd sind. Dann gilt $I_1 \cdot \dots \cdot I_m = I_1 \cap \dots \cap I_m$.

Beweis: Wir beweisen die Aussage durch vollständige Induktion über R und beginnen mit dem Fall $m = 2$. Nach Lemma 5.10 gilt $I_1 I_2 \subseteq I_1$ und $I_1 I_2 \subseteq I_2$, insgesamt also $I_1 I_2 \subseteq I_1 \cap I_2$. Sei nun umgekehrt $r \in I_1 \cap I_2$ vorgegeben. Wegen $I_1 + I_2 = (1)$ gibt es Elemente $a_1 \in I_1$ und $a_2 \in I_2$ mit $a_1 + a_2 = 1$. Es folgt

$$r = r \cdot 1 = r(a_1 + a_2) = ra_1 + ra_2.$$

Die Elemente ra_1 und ra_2 liegen beide in $I_1 I_2$, also gilt dasselbe auch für die Summe. Sei nun die Behauptung für m bereits bewiesen, und seien I_1, \dots, I_{m+1} paarweise teilerfremde Ideale. Sei $J = I_1 \cdot \dots \cdot I_m$. Nach 7.3 sind J und I_{m+1} teilerfremd. Die Induktionsvoraussetzung liefert also

$$(I_1 \cap \dots \cap I_m) \cap I_{m+1} = J \cap I_{m+1} = J I_{m+1} = I_1 \cdot \dots \cdot I_m \cdot I_{m+1}. \quad \square$$

Satz 7.5 (Chinesischer Restsatz)

Sei R ein Ring, I_1, \dots, I_m paarweise teilerfremde Ideale in R und $I = I_1 \cdot \dots \cdot I_m$. Dann gibt es einen Isomorphismus von Ringen

$$\bar{\phi} : R/I \longrightarrow (R/I_1) \times \dots \times (R/I_m) \quad \text{mit} \quad \bar{\phi}(a + I) = (a + I_1, \dots, a + I_m) \quad \text{für alle} \quad a \in R.$$

Beweis: Sei $\phi : R \rightarrow (R/I_1) \times \dots \times (R/I_m)$ gegeben durch $\phi(a) = (a + I_1, \dots, a + I_m)$. Nach 7.4 gilt $I = I_1 \cap \dots \cap I_m$. Ein Element $a \in R$ liegt genau dann im Kern von ϕ , wenn $a + I_k = I_k \Leftrightarrow a \in I_k$ für $1 \leq k \leq m$ gilt. Dies wiederum ist äquivalent zu $a \in I$. Es gilt also $I = \ker(\phi)$. Nach Proposition 6.8 gibt es einen Homomorphismus

$$\bar{\phi} : R/I \longrightarrow (R/I_1) \times \dots \times (R/I_m)$$

mit $\bar{\phi}(a + I) = (a + I_1, \dots, a + I_m)$, und nach dem Homomorphiesatz für Ringe ist $\bar{\phi}$ ein Isomorphismus, wenn ϕ surjektiv ist. Dies beweisen wir nun durch vollständige Induktion über m .

Sei zunächst $m = 2$ und $(a_1 + I_1, a_2 + I_2) \in (R/I_1) \times (R/I_2)$ vorgegeben. Weil I_1 und I_2 teilerfremd sind, gibt es Elemente $s_1 \in I_1, s_2 \in I_2$ mit $s_1 + s_2 = 1$. Es gilt dann $s_1 + I_1 = I_1, s_1 + I_2 = (1 - s_2) + I_2 = 1 + I_2, s_2 + I_1 = (1 - s_1) + I_1 = 1 + I_1$ und $s_2 + I_2 = I_2$. Bilden wir nun das Element $a = s_2 a_1 + s_1 a_2$, dann folgt

$$a + I_1 = (s_2 + I_1)(a_1 + I_1) + (s_1 + I_1)(a_2 + I_2) = (1 + I_1)(a_1 + I_1) + (0 + I_1)(a_2 + I_2) = a_1 + I_1$$

und ebenso

$$a + I_2 = (s_2 + I_2)(a_1 + I_2) + (s_1 + I_2)(a_2 + I_2) = (0 + I_2)(a_1 + I_2) + (1 + I_2)(a_2 + I_2) = a_2 + I_2$$

insgesamt also $\phi(a) = (a + I_1, a + I_2) = (a_1 + I_1, a_2 + I_2)$. Sei nun $m \in \mathbb{N}$, und setzen wir die Aussage für dieses m voraus. Seien I_1, \dots, I_{m+1} teilerfremde Ideale und das Element

$$(a_1 + I_1, \dots, a_m + I_m, a_{m+1} + I_{m+1}) \in (R/I_1) \times \dots \times (R/I_m) \times (R/I_{m+1})$$

vorgegeben. Nach Induktionsvoraussetzung finden wir ein Element $a' \in R$ mit $a' + I_k = a_k + I_k$ für $1 \leq k \leq m$. Die Ideale $J = I_1 \cdot \dots \cdot I_m$ und I_{m+1} sind nach 7.3 teilerfremd. Wiederum auf Grund der Induktionsvoraussetzung finden wir ein $a \in R$ mit $a + J = a' + J$ und $a + I_{m+1} = a_{m+1} + I_{m+1}$. Die Gleichung $a + J = a' + J$ ist äquivalent zu $a - a' \in J$, und aus $J \subseteq I_k$ für $1 \leq k \leq m$ folgt $a - a' \in I_k$, also $a + I_k = a' + I_k = a_k + I_k$ für $1 \leq k \leq m$. Insgesamt gilt also $a + I_k = a_k + I_k$ für $1 \leq k \leq m + 1$ und $\phi(a) = (a_1 + I_1, \dots, a_{m+1} + I_{m+1})$. \square

Wir behandeln eine Reihe von Anwendungsbeispielen für den Chinesischen Restsatz.

Beispiel 1: Gesucht wird die Menge A aller ganzen Zahlen $a \in \mathbb{Z}$, welche die Kongruenzbedingungen

$$a \equiv 0 \pmod{2}, \quad a \equiv 2 \pmod{3}, \quad a \equiv 4 \pmod{5}$$

erfüllen. Wir werden mit Hilfe des Chinesischen Restsatzes zeigen, dass die Menge dieser Zahlen durch $A = 14 + 30\mathbb{Z} = \{14 + 30k \mid k \in \mathbb{Z}\} = \{14, 44, 74, 104, \dots\} \cup \{-16, -46, -76, -106, \dots\}$ gegeben ist.

Nach Definition der Kongruenzen liegt ein $a \in \mathbb{Z}$ genau dann in der Lösungsmenge A des Systems, wenn die Gleichung $(a + 2\mathbb{Z}, a + 3\mathbb{Z}, a + 5\mathbb{Z}) = (0 + 2\mathbb{Z}, 2 + 3\mathbb{Z}, 4 + 5\mathbb{Z})$ im Ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ erfüllt ist. Wir zeigen mit dem Chinesischen Restsatz, dass dies genau auf die Elemente $a \in 14 + 30\mathbb{Z}$ zutrifft.

Als erstes überprüfen wir, dass der Chinesische Restsatz in dieser Situation anwendbar ist. Die Zahlen 2, 3, 5 sind paarweise teilerfremd, also gilt dasselbe für die Ideale $I_2 = (2)$, $I_3 = (3)$ und $I_5 = (5)$ des Rings \mathbb{Z} der ganzen Zahlen. Das Produktideal $I_2 I_3 I_5$ ist gleich $(2 \cdot 3 \cdot 5) = (30)$. Nach dem Chinesischen Restsatz gibt es also einen Ringisomorphismus

$$\bar{\phi} : \mathbb{Z}/30\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \quad \text{mit} \quad \bar{\phi}(a + 30\mathbb{Z}) = (a + 2\mathbb{Z}, a + 3\mathbb{Z}, a + 5\mathbb{Z})$$

für alle $a \in \mathbb{Z}$. Wir suchen nun ein Urbild von $(0 + 2\mathbb{Z}, 2 + 3\mathbb{Z}, 4 + 5\mathbb{Z})$ unter diesem Isomorphismus. Jedes Element in $\mathbb{Z}/30\mathbb{Z}$ wird durch ein $a \in \mathbb{Z}$ mit $0 \leq a < 30$ repräsentiert. Gilt $a + 5\mathbb{Z} = 4 + 5\mathbb{Z}$, dann ist a in der Menge $\{4, 9, 14, 19, 24, 29\}$ enthalten. Unter diesen sechs Elementen $a + 3\mathbb{Z} = 2 + 3\mathbb{Z}$, nämlich 14 und 29. Dabei ist 14 das einzige Element a , das zusätzlich noch die Bedingung $a + 2\mathbb{Z} = 0 + 2\mathbb{Z}$ Damit haben wir das Urbild von $(0 + 2\mathbb{Z}, 2 + 3\mathbb{Z}, 4 + 5\mathbb{Z})$ im Ring $\mathbb{Z}/30\mathbb{Z}$ gefunden: Es gilt

$$\bar{\phi}(14 + 30\mathbb{Z}) = (14 + 2\mathbb{Z}, 14 + 3\mathbb{Z}, 14 + 5\mathbb{Z}) = (0 + 2\mathbb{Z}, 2 + 3\mathbb{Z}, 4 + 5\mathbb{Z}).$$

Nun beweisen wir die Gleichung $A = 14 + 30\mathbb{Z}$. „ \subseteq “ Ist $a \in A$, dann gilt $(a + 2\mathbb{Z}, a + 3\mathbb{Z}, a + 5\mathbb{Z}) = \bar{\phi}(a + 30\mathbb{Z}) = (0 + 2\mathbb{Z}, 2 + 3\mathbb{Z}, 4 + 5\mathbb{Z})$. Auf Grund der Injektivität von $\bar{\phi}$ folgt $a + 30\mathbb{Z} = 14 + 30\mathbb{Z}$, also $a \in 14 + 30\mathbb{Z}$. „ \supseteq “ Liegt a in $14 + 30\mathbb{Z}$, dann gilt $a + 30\mathbb{Z} = 14 + 30\mathbb{Z}$ und somit $(a + 2\mathbb{Z}, a + 3\mathbb{Z}, a + 5\mathbb{Z}) = \bar{\phi}(a + 30\mathbb{Z}) = \bar{\phi}(14 + 30\mathbb{Z}) = (0 + 2\mathbb{Z}, 2 + 3\mathbb{Z}, 4 + 5\mathbb{Z})$. Daraus folgt $a \in A$.

Bei größeren Zahlen bietet es sich an, mit dem Euklidischen Algorithmus zu arbeiten.

Beispiel 2: Wir suchen eine Lösung $x \in \mathbb{Z}$ des Kongruenzsystems

$$x \equiv 15 \pmod{59}, \quad x \equiv 20 \pmod{73}.$$

Da 59 und 73 Primzahlen sind, gilt $\text{ggT}(59, 73) = 1$. Damit ist der Chinesische Restsatz anwendbar. Es ist $59 \cdot 73 = 4307$, und auf Grund des Satzes ist

$$\phi : \mathbb{Z}/4307\mathbb{Z} \rightarrow \mathbb{Z}/59\mathbb{Z} \times \mathbb{Z}/73\mathbb{Z}, \quad a + 4307\mathbb{Z} \mapsto (a + 59\mathbb{Z}, a + 73\mathbb{Z})$$

ein Ringisomorphismus. Um eine Lösung des Kongruenzsystems zu finden, müssen wir ein Urbild des Elements $(15 + 59\mathbb{Z}, 20 + 73\mathbb{Z})$ unter diesem Isomorphismus bestimmen. Mit Hilfe des Euklidischen Algorithmus finden wir zunächst die Darstellung $26 \cdot 59 + (-21) \cdot 73 = 1$ des größten gemeinsamen Teilers von 59 und 73. Diese Gleichung liefert uns

$$\phi(-1533 + 4307\mathbb{Z}) = \phi((-21) \cdot 73 + 4307\mathbb{Z}) = (1 + (-26) \cdot 59 + 59\mathbb{Z}, (-21) \cdot 73 + 73\mathbb{Z}) = (1 + 59\mathbb{Z}, 0 + 73\mathbb{Z})$$

und

$$\phi(1534 + 4307\mathbb{Z}) = \phi(26 \cdot 59 + 4307\mathbb{Z}) = (26 \cdot 59 + 59\mathbb{Z}, 1 + 21 \cdot 73 + 73\mathbb{Z}) = (0 + 59\mathbb{Z}, 1 + 73\mathbb{Z}).$$

Wir berechnen $15 \cdot (-1533) + 20 \cdot 1534 = 7685$ und $7685 + 4307\mathbb{Z} = -929 + 4307\mathbb{Z}$. Dieses Element wird auf $(15 + 59\mathbb{Z}, 20 + 73\mathbb{Z})$ abgebildet. Damit haben wir eine Lösung des Kongruenzsystems gefunden, denn tatsächlich gilt

$$-929 \equiv 15 \pmod{59} \quad \text{und} \quad -929 \equiv 20 \pmod{73}. \quad \square$$

Der Chinesische Restsatz kann auch verwendet werden, um Lösungen von Polynomgleichungen in Restklassenringen zu bestimmen.

Beispiel 3: Wir zeigen, dass das Polynom $f = x^2 - x \in R[x]$ über dem Ring $R = \mathbb{Z}/35\mathbb{Z}$ genau vier Nullstellen besitzt, nämlich

$$\bar{0}, \quad \bar{1}, \quad \bar{15} \quad \text{und} \quad \bar{21}.$$

Sei $a \in \mathbb{Z}$ und $\bar{a} = a + 35\mathbb{Z} \in \mathbb{Z}/35\mathbb{Z}$. Ist $\phi : \mathbb{Z}/35\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ der Isomorphismus aus dem Chinesischen Restsatz, dann gilt also $\phi(\bar{a}) = (a + 5\mathbb{Z}, a + 7\mathbb{Z})$. Da ϕ ein Ringisomorphismus ist, gilt die Äquivalenz

$$\begin{aligned} f(\bar{a}) = 0 &\iff \bar{a}^2 - \bar{a} = \bar{0} \iff \phi(\bar{a})^2 - \phi(\bar{a}) = \phi(\bar{0}) \iff \\ &(a + 5\mathbb{Z}, a + 7\mathbb{Z})^2 - (a + 5\mathbb{Z}, a + 7\mathbb{Z}) = (0 + 5\mathbb{Z}, 0 + 7\mathbb{Z}) \\ \iff &(a + 5\mathbb{Z})^2 - (a + 5\mathbb{Z}) = 0 + 5\mathbb{Z} \wedge (a + 7\mathbb{Z})^2 - (a + 7\mathbb{Z}) = 0 + 7\mathbb{Z}. \end{aligned}$$

Da $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ und $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ Körper sind, besitzt die Gleichung $x^2 - x = \bar{0}$ dort jeweils genau zwei Lösungen, nämlich $a + 5\mathbb{Z} \in \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}\}$ bzw. $a + 7\mathbb{Z} \in \{0 + 7\mathbb{Z}, 1 + 7\mathbb{Z}\}$. Es gilt also

$$\begin{aligned} (a + 5\mathbb{Z})^2 - (a + 5\mathbb{Z}) = 0 + 5\mathbb{Z} \wedge (a + 7\mathbb{Z})^2 - (a + 7\mathbb{Z}) = 0 + 7\mathbb{Z} &\iff \\ a + 5\mathbb{Z} \in \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}\} \wedge a + 7\mathbb{Z} \in \{0 + 7\mathbb{Z}, 1 + 7\mathbb{Z}\} & \\ \iff (a + 5\mathbb{Z}, a + 7\mathbb{Z}) \in \{(0 + 5\mathbb{Z}, 0 + 7\mathbb{Z}), (1 + 5\mathbb{Z}, 0 + 7\mathbb{Z}), (0 + 5\mathbb{Z}, 1 + 7\mathbb{Z}), (1 + 5\mathbb{Z}, 1 + 7\mathbb{Z})\}. & \end{aligned}$$

Die Gleichung $(a + 5\mathbb{Z}, a + 7\mathbb{Z}) = (0 + 5\mathbb{Z}, 0 + 7\mathbb{Z})$ ist äquivalent zu $\phi(\bar{a}) = (0 + 5\mathbb{Z}, 0 + 7\mathbb{Z}) = \phi(\bar{0})$, auf Grund der Injektivität von ϕ also zu $\bar{a} = \bar{0}$. Mit dem Verfahren aus Anwendungsbeispiel 1 findet man $\phi(\bar{21}) = (1 + 5\mathbb{Z}, 0 + 7\mathbb{Z})$ und $\phi(\bar{15}) = (0 + 5\mathbb{Z}, 1 + 7\mathbb{Z})$. Daraus folgt

$$(a + 5\mathbb{Z}, a + 7\mathbb{Z}) = (1 + 5\mathbb{Z}, 0 + 7\mathbb{Z}) \iff \bar{a} = \bar{21}, \quad (a + 5\mathbb{Z}, a + 7\mathbb{Z}) = (0 + 5\mathbb{Z}, 1 + 7\mathbb{Z}) \iff \bar{a} = \bar{15}$$

und schließlich $(a + 5\mathbb{Z}, a + 7\mathbb{Z}) = (1 + 5\mathbb{Z}, 1 + 7\mathbb{Z}) \iff \bar{a} = \bar{1}$. Insgesamt haben wir damit die Äquivalenz

$$f(\bar{a}) = \bar{0} \iff \bar{a} \in \{\bar{0}, \bar{1}, \bar{15}, \bar{21}\}$$

für alle $\bar{a} \in \mathbb{Z}/35\mathbb{Z}$ bewiesen.

§ 8. Die Struktur der primen Restklassengruppen

Zusammenfassung. In diesem Abschnitt setzen wir den Chinesischen Restsatz ein, um die Struktur der Einheitengruppen $(\mathbb{Z}/m\mathbb{Z})^\times$ der Restklassenringe zu klären, die auch *prime Restklassengruppen* genannt werden. In vielen Bereichen der Elementaren Zahlentheorie und Kryptographie spielen diese Gruppen eine wichtige Rolle.

Für die Untersuchung der Struktur stellen wir zunächst fest, dass $(\mathbb{Z}/m\mathbb{Z})^\times$ eine endliche abelsche Gruppe ist. Aus der Algebra-Vorlesung wissen wir bereits, dass jede solche Gruppe isomorph zu einem Produkt $C_1 \times \dots \times C_r$ von zyklischen Gruppen C_j ist. Mit dem Chinesischen Restsatz kann die Untersuchung auf den Fall zurückgeführt werden, dass m eine Primzahlpotenz ist. Ist m eine Primzahl, dann handelt es sich bei $\mathbb{Z}/m\mathbb{Z}$ um einen Körper; auf Grund eines allgemeinen Satzes ist dessen multiplikative Gruppe zyklisch. Im Fall, dass m Potenz einer ungeraden Primzahl p ist, kann nun durch ein Induktionsargument gezeigt werden, dass $(\mathbb{Z}/m\mathbb{Z})^\times$ ebenfalls zyklisch ist. Bei Potenzen der Primzahl 2 ist die Sache komplizierter. Hier ist die prime Restklassengruppe in der Regel ein direktes Produkt von zwei zyklischen Gruppen.

Zentrale Sätze

- Für teilerfremde $m, n \in \mathbb{N}$ gilt $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.
- Für jede ungerade Primzahl p und alle $r \in \mathbb{N}$ gilt $(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \mathbb{Z}/p^{r-1}(p-1)\mathbb{Z}$.
- Ist K ein Körper und U eine endliche Untergruppe von K^\times , dann ist U zyklisch.
- Es gilt $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ für $r \geq 3$.

Im folgenden werden wir mit Hilfe des Chinesischen Restsatzes die Einheitengruppen der Ringe $\mathbb{Z}/n\mathbb{Z}$ näher untersuchen. Wir beginnen mit einer allgemeinen Bemerkung zu den Einheiten in beliebigen Ringen.

Lemma 8.1 Seien R und S Ringe. Dann gilt

- $(R \times S)^\times = R^\times \times S^\times$
- Ist $\phi : R \rightarrow S$ ein Isomorphismus von Ringen, dann gilt $\phi(R^\times) = S^\times$. Insbesondere sind die Einheitengruppen R^\times und S^\times also isomorph.

Beweis: zu (i) „ \subseteq “ Das Einselement des Rings $R \times S$ ist $(1_R, 1_S)$. Ist $(a, b) \in (R \times S)^\times$, dann gibt es nach Definition ein Paar $(c, d) \in R \times S$ mit $(ac, bd) = (a, b)(c, d) = (1_R, 1_S)$. Es gilt also $ac = 1_R$, $bd = 1_S$ und damit $a \in R^\times$, $b \in S^\times$. „ \supseteq “ Sei $(a, b) \in R^\times \times S^\times$. Dann gibt es Elemente $c \in R$ und $d \in S$ mit $ac = 1_R$ und $bd = 1_S$. Insgesamt erhalten wir $(a, b)(c, d) = (ac, bd) = (1_R, 1_S) = 1_{R \times S}$, also $(a, b) \in (R \times S)^\times$.

zu (ii) Wir beweisen zunächst die Inklusion $\phi(R^\times) \subseteq S^\times$. Sei $a \in \phi(R^\times)$. Dann gibt es ein $b \in R^\times$ mit $\phi(b) = a$. Weil b eine Einheit ist, existiert ein $c \in R^\times$ mit $bc = 1_R$, und es folgt $a\phi(c) = \phi(b)\phi(c) = \phi(bc) = \phi(1_R) = 1_S$. Dies zeigt,

dass a eine Einheit in S ist. Wir können nun dasselbe Argument auf den Ringhomomorphismus ϕ^{-1} anwenden und erhalten $\phi^{-1}(S^\times) \subseteq R^\times$. Anwendung von ϕ auf beide Seiten liefert $S^\times \subseteq \phi(R^\times)$. Insgesamt gilt also $\phi(R^\times) = S^\times$. \square

In der Gruppentheorie haben wir den **Exponenten** einer Gruppe G definiert. Es handelt sich um die kleinste Zahl $n \in \mathbb{N}$ mit der Eigenschaft $g^n = e$ für alle $n \in \mathbb{N}$.

Proposition 8.2 Sei G eine endliche abelsche Gruppe vom Exponenten n . Dann gibt es in G ein Element der Ordnung n .

Beweis: Aus der Gruppentheorie ist bekannt, dass G als endliche abelsche Gruppe isomorph zu einem direkten Produkt endlicher zyklischer Gruppen ist. Es gibt also $m_1, \dots, m_r \in \mathbb{N}$ mit

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}.$$

Der Einfachheit halber können wir annehmen, dass G zu dem Produkt auf der rechten Seite nicht nur isomorph ist, sondern damit übereinstimmt. Sei nun m der Exponent von G . Wir zeigen, dass m mit $\ell = \text{kgV}(m_1, \dots, m_r)$ übereinstimmt. Nach Definition des Exponenten gilt $mg = 0_G$ für $g \in G$. Insbesondere gilt

$$\begin{aligned} m(1 + m_1\mathbb{Z}, \dots, 1 + m_r\mathbb{Z}) = 0_G &\iff (m + m_1\mathbb{Z}, \dots, m + m_r\mathbb{Z}) = (m_1\mathbb{Z}, \dots, m_r\mathbb{Z}) \iff \\ m + m_k\mathbb{Z} = m_k\mathbb{Z} \text{ für } 1 \leq k \leq r &\iff m_k | m \text{ für } 1 \leq k \leq r. \end{aligned}$$

Also ist m jedenfalls ein gemeinsames Vielfaches von m_1, \dots, m_r und damit auch ein Vielfaches von ℓ . Weil ℓ ein Vielfaches von m_1, \dots, m_r ist, gilt andererseits für alle $a_1, \dots, a_r \in \mathbb{Z}$ und $1 \leq k \leq r$ jeweils $m_k | (\ell a_k)$, also $\ell a_k + m_k\mathbb{Z} = m_k\mathbb{Z}$ und somit

$$\ell(a_1 + m_1\mathbb{Z}, \dots, a_r + m_r\mathbb{Z}) = (\ell a_1 + m_1\mathbb{Z}, \dots, \ell a_r + m_r\mathbb{Z}) = (m_1\mathbb{Z}, \dots, m_r\mathbb{Z}) = 0_G.$$

Nach Definition des Exponenten folgt daraus $\ell \geq m$. Aus $\ell | m$ und $\ell \geq m$ folgt $\ell = m$. Die Rechnung von oben zeigt darüber hinaus, dass $(1 + m_1\mathbb{Z}, \dots, 1 + m_r\mathbb{Z})$ ein Element der maximalen Ordnung m ist. \square

Satz 8.3 Sei K ein Körper und U eine endliche Untergruppe der multiplikativen Gruppe K^\times . Dann ist U zyklisch. Insbesondere ist die multiplikative Gruppe eines endlichen Körpers immer eine zyklische Gruppe.

Beweis: Sei $n = |U|$ und d der Exponent von U . Nach dem Satz von Lagrange ist $\text{ord}(a)$ für jedes $a \in U$ jeweils ein Teiler von n , also gilt $a^n = 1$ für alle $a \in U$. Dies zeigt, dass $d \leq n$ gilt. Andererseits gilt nach Definition des Exponenten auch $a^d = 1$ für alle $a \in U$. Damit sind alle Elemente aus U Nullstellen des Polynoms $f = x^d - 1 \in K[x]$. Aber ein Polynom vom Grad d über einem Körper kann nach Folgerung 4.8 höchstens d Nullstellen besitzen. Daraus folgt $n \leq d$, insgesamt $n = d$. Nach Prop. 8.2 gibt es in U ein Element der Ordnung n . Also ist U zyklisch. \square

Proposition 8.4 Sei $n \in \mathbb{N}$, $n \geq 2$, $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ und $a \in \mathbb{Z}$ mit $\bar{a} = a + n\mathbb{Z}$. Genau dann ist \bar{a} eine Einheit in $\mathbb{Z}/n\mathbb{Z}$, wenn $\text{ggT}(a, n) = 1$ gilt. Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$ bezeichnet man auch als **prime Restklassengruppe** modulo n .

Beweis: „ \Rightarrow “ Ist $a+n\mathbb{Z}$ eine Einheit, dann gibt es ein $b \in \mathbb{Z}$ mit $(a+n\mathbb{Z})(b+n\mathbb{Z}) = 1+n\mathbb{Z}$. Daraus folgt $ab = 1+n\mathbb{Z}$. Es gibt also ein $k \in \mathbb{Z}$ mit $ab = 1+kn$. Ist nun d ein gemeinsamer Teiler von a und n , dann teilt d auch $ab+(-k)n = 1$. Dies zeigt, dass a und n teilerfremd sind.

„ \Leftarrow “ Sind a und n teilerfremd, dann gibt es nach dem Lemma von Bézout ganze Zahlen k, ℓ mit $ak + n\ell = 1$. Es folgt $(a+n\mathbb{Z})(k+n\mathbb{Z}) = ak + n\mathbb{Z} = (ak + n\ell) + n\mathbb{Z} = 1 + n\mathbb{Z}$, also ist $a+n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ invertierbar und damit eine Einheit. \square

Die Anzahl der Elemente in $(\mathbb{Z}/n\mathbb{Z})^\times$ wird durch die sogenannte **Eulersche φ -Funktion** beschrieben, die durch

$$\varphi(n) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq n, \text{ggT}(k, n) = 1\}| \quad \text{gegeben ist.}$$

Für eine Primzahl p ist $\varphi(p) = p - 1$, denn in diesem Fall ist $\mathbb{Z}/p\mathbb{Z}$ nach Satz 6.7 ein Körper und damit jedes Element außer der Null invertierbar. Ist n eine Primzahlpotenz, $n = p^r$ für eine Primzahl p und ein $r \in \mathbb{N}$, dann gilt $\varphi(n) = p^{r-1}(p-1) = p^r - p^{r-1}$. Die einzigen Zahlen zwischen 1 und p^r , die *nicht* teilerfremd zu p^r sind, sind die Vielfachen von p , und von denen gibt es in diesem Bereich $\frac{p^r}{p} = p^{r-1}$ Stück. Es bleiben also $p^r - p^{r-1}$ Zahlen übrig.

Folgerung 8.5 Ist p eine Primzahl, dann gilt $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Beweis: Wie wir bereits festgestellt haben, gilt $|(\mathbb{Z}/p\mathbb{Z})^\times| = \varphi(p) = p - 1$. Außerdem ist $(\mathbb{Z}/p\mathbb{Z})^\times$ nach Satz 8.3 zyklisch, damit isomorph zu $\mathbb{Z}/(p-1)\mathbb{Z}$. \square

Eine Zahl $a \in \mathbb{Z}$ mit der Eigenschaft $(\mathbb{Z}/p\mathbb{Z})^\times = \langle a + p\mathbb{Z} \rangle$ wird **Primitivwurzel modulo p** genannt. Es ist zwar keine Formel bekannt, mit der sich ein solches a bestimmen lässt, aber man kann folgenden Satz aus der Gruppentheorie zur Hilfe nehmen, um es zu finden: Ist G eine zyklische Gruppe der Ordnung n und gilt $g^{\frac{n}{p}} \neq e_G$ für alle Primteiler p von n , dann ist g ein erzeugendes Element, es gilt also $G = \langle g \rangle$.

Beispiel: Wir bestimmen eine Primitivwurzel modulo 43. Die Gruppenordnung von $(\mathbb{Z}/43\mathbb{Z})^\times$ ist $42 = 2 \cdot 3 \cdot 7$, ein Element $\bar{a} \in (\mathbb{Z}/43\mathbb{Z})^\times$ ist also genau dann eine Primitivwurzel, wenn $\bar{a}^m \neq \bar{1}$ für alle $m \in \{\frac{42}{2}, \frac{42}{3}, \frac{42}{7}\} = \{21, 14, 6\}$ gilt. Wegen $\bar{2}^{14} = \bar{1}$ ist $\bar{2}$ keine Primitivwurzel. Es gilt aber $\bar{3}^{21} = \bar{42}$, $\bar{3}^{14} = \bar{36}$ und $\bar{3}^6 = \bar{41}$, also haben wir mit $\bar{a} = \bar{3}$ eine Primitivwurzel modulo 43 gefunden. Tatsächlich erhält man, wenn man die Potenzen $\bar{a}^1, \bar{a}^2, \bar{a}^3, \dots$ der Reihe nach aufschreibt, die Elemente

$$\begin{aligned} &\bar{3}, \bar{9}, \bar{27}, \bar{38}, \bar{28}, \bar{41}, \bar{37}, \bar{25}, \bar{32}, \bar{10}, \bar{30}, \bar{4}, \bar{12}, \bar{36}, \bar{22}, \bar{23}, \bar{26}, \bar{35}, \bar{19}, \bar{14}, \bar{42}, \bar{40}, \bar{34}, \bar{16}, \\ &\bar{5}, \bar{15}, \bar{2}, \bar{6}, \bar{18}, \bar{11}, \bar{33}, \bar{13}, \bar{39}, \bar{31}, \bar{7}, \bar{21}, \bar{20}, \bar{17}, \bar{8}, \bar{24}, \bar{29}, \bar{1} \end{aligned}$$

und somit die gesamte Gruppe $(\mathbb{Z}/43\mathbb{Z})^\times$.

Das Rechenbeispiel wirft die Frage auf, wie hohe Potenzen von Elementen $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ effizient ausgerechnet werden können. Es gibt hierzu das Verfahren der *schnellen Exponentiation*, dass wir hier kurz am Beispiel der Potenz $\bar{3}^{21}$ im Restklassenring $\mathbb{Z}/43\mathbb{Z}$ erläutern wollen. Zunächst schreibt man den Exponenten als Summe von Zweierpotenzen, in unserem Fall also $21 = 16 + 4 + 1$. Anschließend berechnet man die Elemente $\bar{3}^{2^d}$ für hinreichend großes d . In unserem Fall ist

$$\begin{aligned} \bar{3}^1 &= \bar{3} \quad , \quad \bar{3}^2 = \bar{9} \quad , \quad \bar{3}^4 = (\bar{3}^2)^2 = \bar{9}^2 = \bar{81} = \bar{38} \quad , \quad \bar{3}^8 = (\bar{3}^4)^2 = (\bar{38})^2 = (-\bar{5})^2 = \bar{25} \quad , \\ \bar{3}^{16} &= (\bar{3}^8)^2 = (\bar{25})^2 = \bar{625} = \bar{195} = \bar{23} \end{aligned}$$

weiter $\overline{38} \cdot \overline{23} = \overline{874} = \overline{14}$ und schließlich $\overline{3^{21}} = \overline{3^{16}} \cdot \overline{3^4} \cdot \overline{3^1} = \overline{23} \cdot \overline{38} \cdot \overline{3} = \overline{14} \cdot \overline{3} = \overline{42}$.

Die folgende Rechenregel haben wir bereits in der Gruppentheorie formuliert. Sie lässt sich aber ringtheoretisch besser beweisen, wie der folgende extrem kurze Beweis zeigt.

Proposition 8.6 Sind m, n teilerfremd und $m, n \geq 2$. Dann gilt für die Eulersche φ -Funktion die Rechenregel $\varphi(mn) = \varphi(m)\varphi(n)$.

Beweis: Auf Grund des Chinesischen Restsatzes und Lemma 8.1 gilt

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Die Menge links enthält $\varphi(mn)$, die Menge rechts $\varphi(m)\varphi(n)$ Elemente. □

Mit den bisherigen Ergebnissen können wir die Struktur der primen Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ bereits in vielen Fällen bestimmen. Beispielsweise gilt

$$(\mathbb{Z}/15\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

und somit insbesondere $\varphi(15) = 8$. Denn nach dem Chinesischen Restsatz und Lemma 8.1 existiert ein Isomorphismus $(\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$. Außerdem gilt $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ nach Folgerung 8.5.

Lemma 8.7

- (i) Sei p eine ungerade Primzahl und $m \in \mathbb{N}$. Dann gilt $(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}$ und $(1+p)^{p^{m-1}} \not\equiv 1 \pmod{p^{m+1}}$.
- (ii) Für alle $m \in \mathbb{N}$, $m \geq 2$ gilt $5^{2^{m-2}} \equiv 1 \pmod{2^m}$ und $5^{2^{m-2}} \not\equiv 1 \pmod{2^{m+1}}$.

Beweis: zu (i) Wir beweisen die Aussage durch vollständige Induktion über m . Für $m = 1$ lautet die Aussage $1+p \equiv 1 \pmod{p}$ und $1+p \not\equiv 1 \pmod{p^2}$, und sie ist offenbar erfüllt. Sei nun $m \in \mathbb{N}$, und setzen wir die Aussage für m voraus. Dann gilt $(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}$. Es gilt also $(1+p)^{p^{m-1}} = 1+kp^m$ für ein $k \in \mathbb{Z}$, aber wegen $(1+p)^{p^{m-1}} \not\equiv 1 \pmod{p^{m+1}}$ ist p kein Teiler von k . Durch Anwendung des Binomischen Lehrsatzes erhalten wir

$$\begin{aligned} (1+p)^{p^m} &= ((1+p)^{p^{m-1}})^p = (1+kp^m)^p = \\ &= \sum_{j=0}^p \binom{p}{j} (kp^m)^j = 1 + kp^{m+1} + \sum_{j=2}^p \binom{p}{j} k^j p^{jm}. \end{aligned}$$

Für $2 \leq j \leq p-1$ ist $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ durch p teilbar. Also ist der j -te Summand $\binom{p}{j} k^j p^{jm}$ durch p^{mj+1} teilbar, und es gilt $mj+1 \geq 2m+1 \geq m+2$. Der letzte Summand $\binom{p}{p} k^p p^{mp}$ ist durch p^{mp} teilbar, und es gilt $mp \geq 3m \geq m+2$. Insgesamt ist $\sum_{j=2}^p \binom{p}{j} k^j p^{jm}$ also durch p^{m+2} teilbar, und wir erhalten $(1+p)^{p^m} \equiv 1+kp^{m+1} \pmod{p^{m+2}}$. Es folgt $(1+p)^{p^m} \equiv 1 \pmod{p^{m+1}}$ und $(1+p)^{p^m} \not\equiv 1 \pmod{p^{m+2}}$.

zu (ii) Auch hier beweisen wir die Aussage durch vollständige Induktion über m . Für den Startwert $m = 2$ ist die Aussage wegen $5 \equiv 1 \pmod{4}$ und $5 \not\equiv 1 \pmod{8}$ erfüllt. Sei nun $m \geq 2$ und die Aussage für dieses m vorausgesetzt. Dann gilt $5^{2^{m-2}} \equiv 1 \pmod{2^m}$ und $5^{2^{m-2}} \not\equiv 1 \pmod{2^{m+1}}$. Es gibt also ein ungerades $k \in \mathbb{Z}$ mit $5^{2^{m-2}} = 1+k2^m$. Durch Einsetzen erhalten wir

$$5^{2^{m-1}} = (5^{2^{m-2}})^2 = (1+k2^m)^2 = 1+k2^{m+1} + k^2 2^{2m}.$$

Wegen $2m \geq m+2$ folgt $5^{2^{m-1}} \equiv 1+k2^{m+1} \pmod{2^{m+2}}$. Wir erhalten $5^{2^{m-1}} \equiv 1 \pmod{2^{m+1}}$ und $5^{2^{m-1}} \not\equiv 1 \pmod{2^{m+2}}$. □

Satz 8.8

- (i) Für jede ungerade Primzahl p und jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}/p^m\mathbb{Z})^\times$ eine zyklische Gruppe der Ordnung $p^{m-1}(p-1)$.
- (ii) Es gilt $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$. Für alle $m \geq 3$ existiert jeweils ein Isomorphismus $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Beweis: zu (i) Wegen Folgerung 8.5 können wir $m \geq 2$ voraussetzen; außerdem gibt es auf Grund dieses Satzes ein $a \in \mathbb{Z}$ mit $\langle a + p\mathbb{Z} \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$. Setzen wir $\bar{a} = a + p^m\mathbb{Z}$ und $r = \text{ord}(\bar{a})$, dann gilt $\bar{a}^r = \bar{1}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$, also $a^r \equiv 1 \pmod{p^m}$ und erst recht $a^r \equiv 1 \pmod{p}$. Weil $a + p\mathbb{Z}$ in der Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ die Ordnung $p-1$ hat, folgt aus $(a + p\mathbb{Z})^r = 1 + p\mathbb{Z}$, dass $p-1$ ein Teiler von r ist. Sei $k \in \mathbb{N}$ mit $k(p-1) = r$. Auf Grund der Rechenregeln für Elementordnungen aus der Gruppentheorie ist $\bar{b} = \bar{a}^k$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ ein Element der Ordnung $p-1$.

Sei nun außerdem $\bar{c} = \overline{1+p} = (1+p) + p^m\mathbb{Z}$. Nach Lemma 8.7 (i) gilt $\bar{c}^{p^{m-2}} \neq \bar{1}$ und $\bar{c}^{p^{m-1}} = \bar{1}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Dies zeigt, dass \bar{c} in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ ein Element der Ordnung p^{m-1} ist. Sei nun die Untergruppen U und V von $G = (\mathbb{Z}/p^m\mathbb{Z})^\times$ gegeben durch $U = \langle \bar{b} \rangle$ und $V = \langle \bar{c} \rangle$. Als Untergruppen einer abelschen Gruppe sind U und V Normalteiler von G . Weil die Ordnungen $|U| = p-1$ und $|V| = p^{m-1}$ der zyklischen Gruppen $U \cong \mathbb{Z}/(p-1)\mathbb{Z}$ und $V \cong \mathbb{Z}/p^{m-1}\mathbb{Z}$ teilerfremd sind, gilt außerdem $U \cap V = \{\bar{1}\}$. Insgesamt ist das Komplexprodukt UV ein inneres direktes Produkt von U und V . Nach Proposition (5.7) aus der Gruppentheorie und dem Chinesischen Restsatz folgt

$$UV \cong U \times V \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \cong \mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}.$$

Wegen $|G| = \varphi(p^m) = p^{m-1}(p-1)$ folgt $G = UV \cong \mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}$, also ist $G = (\mathbb{Z}/p^m\mathbb{Z})^\times$ zyklisch von Ordnung $p^{m-1}(p-1)$.

zu (ii) Die ersten beiden Aussagen sind unmittelbar klar, denn nach Definition gilt $(\mathbb{Z}/2\mathbb{Z})^\times = \{1 + 2\mathbb{Z}\}$ und $(\mathbb{Z}/4\mathbb{Z})^\times = \{1 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\} = \langle 3 + 4\mathbb{Z} \rangle$. Sei nun $m \in \mathbb{N}$ mit $m \geq 3$. Nach Lemma 8.7 (ii) gilt $\bar{5}^{2^{m-2}} = \bar{1}$ und $\bar{5}^{2^{m-3}} \neq \bar{1}$ in $(\mathbb{Z}/2^m\mathbb{Z})^\times$. Daraus folgt $\text{ord}(\bar{5}) = 2^{m-2}$. Außerdem ist $-\bar{1}$ ein Element der Ordnung 2 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$, denn es gilt $-\bar{1} \neq \bar{1}$ und $(-\bar{1})^2 = \bar{1}$. Außerdem gilt $-\bar{1} \notin \langle \bar{5} \rangle$. Denn andernfalls würde $-\bar{1} = \bar{5}^k$ und damit $-1 \equiv 5^k \pmod{2^m}$ für ein $k \in \mathbb{Z}$ gelten. Daraus wiederum würde wegen $5 \equiv 1 \pmod{4}$ dann $-1 \equiv 5^k \equiv 1^k \equiv 1 \pmod{4}$ folgen, im Widerspruch zu $-1 \not\equiv 1 \pmod{4}$. Wegen $-\bar{1} \notin \langle \bar{5} \rangle$ gilt $\langle \bar{5} \rangle \cap \langle -\bar{1} \rangle = \{\bar{1}\}$, also bilden die Untergruppen $U = \langle \bar{5} \rangle$ und $V = \langle -\bar{1} \rangle$ ein inneres direktes Produkt UV . Wie in Teil (i) liefert der Satz über innere direkte Produkte aus der Gruppentheorie einen Isomorphismus $UV \cong U \times V \cong \mathbb{Z}/2^{m-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Aus $|UV| = |U \times V| = 2^{m-2} \cdot 2 = 2^{m-1} = \varphi(2^m) = |(\mathbb{Z}/2^m\mathbb{Z})^\times|$ gilt außerdem $(\mathbb{Z}/2^m\mathbb{Z})^\times = UV$. \square

Beispiel: Das Element $\bar{a} = \bar{2}$ ein Erzeuger der 18-elementigen Gruppe $(\mathbb{Z}/27\mathbb{Z})^\times$. Dies überprüft man mit dem oben angegebenen Kriterium aus der Gruppentheorie durch die Rechnung $\bar{2}^9 = \bar{26} \neq \bar{1}$ und $\bar{2}^6 = \bar{10} \neq \bar{1}$. Die Potenzen $\bar{a}^1, \bar{a}^2, \bar{a}^3, \dots$ sind der Reihe nach gegeben durch

$$\bar{2}, \bar{4}, \bar{8}, \bar{16}, \bar{5}, \bar{10}, \bar{20}, \bar{13}, \bar{26}, \bar{25}, \bar{23}, \bar{19}, \bar{11}, \bar{22}, \bar{17}, \bar{7}, \bar{14}, \bar{1} \quad ,$$

also genau die Elemente der 18-elementigen Gruppe $(\mathbb{Z}/27\mathbb{Z})^\times$.

§ 9. Hauptidealringe und die Teilbarkeitsrelation

Zusammenfassung. Der Begriff des **Hauptidealrings** ist uns bereits aus § 5 bekannt. Diese Ringe sind für viele Anwendungen interessant, weil sich in diesen Ringen die Teilbarkeitsrelation weitgehend analog zur Teilbarkeit ganzer Zahlen verhält. Beispielsweise gilt, wie wir im nächsten Abschnitt sehen werden, in Hauptidealringen ein Analogon zum Fundamentalsatz der Algebra, welcher besagt, dass jede natürliche Zahl > 1 auf eindeutige Weise als Produkt von Primzahlen darstellbar ist. Eine erste Schwierigkeit besteht darin, für das Konzept der Primzahl einen geeigneten Ersatz zu finden. Es zeigt sich, dass es hier zwei Möglichkeiten gibt: Primzahlen sind dadurch charakterisiert, dass sie nicht weiter zerlegt werden können. Dies führt in allgemeinen Ringen zur Definition der **irreduziblen** Elemente. Wir werden sehen, wie man mit Hilfe der Normfunktionen irreduzible Elemente in Ringen der Form $\mathbb{Z}[\sqrt{d}]$ erkennen kann.

Andererseits kann auch folgende Beobachtung zur Verallgemeinerung der Primzahlen genutzt werden: Kommt ein Primfaktor in der Primfaktorzerlegung eines Produkts ab ganzer Zahlen a, b vor, dann muss er bereits in a oder in b vorkommen. Dies führt in beliebigen Ringen zur Definition der **Primelemente**. Wir werden sehen, dass Primelemente in Integritätsbereichen stets irreduzible Elemente sind, und dass in Hauptidealringen die beiden Begriffe zusammenfallen. In beliebigen Integritätsbereichen kann es aber irreduzible Elemente geben, die nicht prim sind.

Neben der Verallgemeinerung des Primzahlbegriffs geht es in diesem Abschnitt auch darum, die Hauptidealringe in die allgemeine Ringtheorie einzuordnen. Wir zeigen, dass alle euklidischen Ringe Hauptidealringe sind. Somit sind \mathbb{Z} , $\mathbb{Z}[i]$ und Polynomringe über beliebigen Körpern Hauptidealringe. Im Anhang zu diesem Kapitel geben wir ein konkretes Beispiel für einen Hauptidealring an, der kein euklidischer Ring ist. Dies zeigt, dass die Hauptidealringe eine echte Verallgemeinerung der euklidischen Ringe darstellen. Im nächsten Kapitel zeigen wir dann, dass die Hauptidealringe ihrerseits durch die sog. **faktoriellen Ringe** verallgemeinert werden. Dies sind Ringe mit einer eindeutigen Primfaktorzerlegung, von der schon zu Beginn die Rede war.

Wichtige Grundbegriffe

- Normfunktion auf einem quadratischen Zahlring
- irreduzibles Element
- Primelement

Zentrale Sätze

- Identifikation von irreduziblen Elementen in quadratischen Zahlringen mit der Normfunktion
- Interpretation der Teilbarkeitsrelation durch Ideale
- Euklidische Ringe sind Hauptidealringe.
- Primelemente in Integritätsbereichen sind irreduzibel.
- Beziehung zwischen Primelementen, irreduziblen Elementen, maximalen Idealen und Primidealen in einem Hauptidealring

Bereits in § 5 haben wir die **Hauptideale** in einem Ring R definiert. Dies waren genau die Ideale mit einer Darstellung der Form $(a) = \{ra \mid r \in R\}$, die aus den Vielfachen eines festgewählten Elements $a \in R$ bestehen. Einen Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, hatten wir **Hauptidealring** genannt. Jeder Körper ist ein Hauptidealring, denn nach Lemma 6.11 sind (0) und (1) die einzigen Ideale eines Körpers.

Dagegen ist $R = \mathbb{Z}[\sqrt{-5}]$ **kein** Hauptidealring, denn beispielsweise ist das Ideal

$$\mathfrak{p} = (3, 1 + 2\sqrt{-5}) \quad \text{kein Hauptideal.}$$

Beweis: Um zu sehen, dass \mathfrak{p} kein Hauptideal ist, betrachten wir die **Normfunktion** $N : R \rightarrow \mathbb{N}_0$ gegeben durch $N(\alpha) = \alpha\bar{\alpha}$ für $\alpha \in R$, wobei $\bar{\alpha}$ wie immer das zu α konjugiert-komplexe Element bezeichnet. Dabei handelt es sich um die Einschränkung der multiplikativen Funktion $N : \mathbb{C} \rightarrow \mathbb{R}_+$, die wir in Kapitel § 4 verwendet hatten um zu zeigen, dass $\mathbb{Z}[i]$ ein euklidischer Ring ist. Diese Funktion erfüllt also insbesondere die Gleichung $N(\alpha\beta) = N(\alpha)N(\beta)$ für alle $\alpha, \beta \in R$.

Nehmen wir nun an, dass \mathfrak{p} ein Hauptideal ist. Dann gibt es ein $\alpha \in R$ mit $\mathfrak{p} = (\alpha)$. Da die Elemente 3 und $1 + 2\sqrt{-5}$ in \mathfrak{p} liegen, gibt es $\beta, \gamma \in R$ mit $3 = \alpha\beta$ und $1 + 2\sqrt{-5} = \alpha\gamma$. Die Multiplikativität der Normfunktion liefert $9 = N(3) = N(\alpha)N(\beta)$ und $21 = N(1 + 2\sqrt{-5}) = N(\alpha)N(\gamma)$. Also ist $N(\alpha)$ ein gemeinsamer Teiler von 9 und 21, damit auch ein Teiler vom ggT(9, 21) = 3. Es folgt $N(\alpha) \in \{1, 3\}$. Betrachten wir zunächst den Fall $N(\alpha) = 3$. Schreiben wir $\alpha = a + b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$, dann gilt $a^2 + 5b^2 = N(\alpha) = 3$. Aber die Gleichung $a^2 + 5b^2 = 3$ besitzt keine Lösung mit $a, b \in \mathbb{Z}$, also ist dieser Fall ausgeschlossen.

Also gilt $N(\alpha) = 1$. Aus $a^2 + 5b^2 = 1$ folgt $b = 0$ und $a \in \{\pm 1\}$, damit $\alpha \in \{\pm 1\}$. Es folgt $\mathfrak{p} = (\alpha) = (1)$. Wir zeigen nun, dass auch dies unmöglich ist. Ein beliebiges Element ρ in $\mathfrak{p} = (3, 1 + 2\sqrt{-5})$ hat die Form $3\beta + (1 + 2\sqrt{-5})\gamma$ mit $\beta, \gamma \in R$. Schreiben wir $\beta = a + b\sqrt{-5}$ und $\gamma = c + d\sqrt{-5}$ mit $a, b, c, d \in \mathbb{Z}$, dann folgt

$$\begin{aligned} \rho &= 3(a + b\sqrt{-5}) + (1 + 2\sqrt{-5})(c + d\sqrt{-5}) = 3a + 3b\sqrt{-5} + (c - 10d) + (2c + d)\sqrt{-5} \\ &= (3a + c - 10d) + (3b + 2c + d)\sqrt{-5}. \end{aligned}$$

Addiert man die beiden Koeffizienten, dann erhält man den Wert $3a + 3b + 3c - 9d$, ein Vielfaches von 3. Ist also $\rho \in \mathfrak{p}$, $\rho = m + n\sqrt{-5}$, dann ist $m + n$ stets durch 3 teilbar. Dies zeigt, dass beispielsweise das Element $1 = 1 + 0\sqrt{-5}$ nicht in \mathfrak{p} liegt, weshalb $\mathfrak{p} \neq (1)$ gilt. Die Annahme, dass \mathfrak{p} ein Hauptideal ist, hat also insgesamt zu einem Widerspruch geführt. \square

Der folgende Satz zeigt, wie sich die Teilbarkeitsrelation auf den Elementen eines Rings rein idealtheoretisch beschreiben lässt.

Satz 9.1 Sei R ein Ring, und seien $a, b \in R$.

- (i) Es gilt $(a) \subseteq (b)$ genau dann, wenn b ein Teiler von a ist.
- (ii) Ist $d \in R$ mit $(d) = (a, b)$, dann ist d ein ggT von a und b .
- (iii) Ist $e \in R$ mit $(e) = (a) \cap (b)$, dann ist e ein kgV von a und b .

Ist R ein Hauptidealring, dann gilt auch von (ii) und (iii) die Umkehrung.

Beweis: zu (i) „ \Rightarrow “ Aus $(a) \subseteq (b)$ folgt insbesondere $a \in (b)$. Da das Hauptideal (b) aus den Vielfachen von b besteht, bedeutet dies, dass ein $r \in R$ mit $a = rb$ existiert. Daraus folgt $b \mid a$. „ \Leftarrow “ Nach Voraussetzung gibt es ein $r \in R$ mit $a = rb$, also gilt $a \in (b)$. Also ist (b) ein Ideal, das a enthält, und nach Definition des von a erzeugten Ideals folgt $(a) \subseteq (b)$.

zu (ii) Aus $(d) = (a, b)$ folgt insbesondere $a \in (d)$ und $b \in (d)$. Es gibt also $r, s \in R$ mit $a = rd$ und $b = sd$. Dies zeigt, dass d ein gemeinsamer Teiler von a und b ist. Sei nun d' ein weiteres Ringelement mit $d' \mid a$ und $d' \mid b$. Dann gibt es $r', s' \in R$ mit $a = r'd'$ und $b = s'd'$. Also enthält das Hauptideal (d') die zweielementige Menge $\{a, b\}$. Nach Definition des erzeugten Ideals folgt $(a, b) \subseteq (d')$ und somit $(d) \subseteq (d')$. Nach Teil (i) ist d' damit ein Teiler von d . Insgesamt haben wir damit die ggT-Eigenschaft von d nachgerechnet.

zu (iii) Aus $(e) = (a) \cap (b)$ folgt $e \in (a)$ und $e \in (b)$. Es gibt also Ringelemente $r, s \in R$ mit $e = ra$ und $e = sb$. Damit ist e ein gemeinsames Vielfaches von a und b . Sei nun $e' \in R$ ein weiteres gemeinsames Vielfaches von a und b . Dann gibt es $r', s' \in R$ mit $e' = r'a$ und $e' = s'b$, und wir erhalten $e' \in (a) \cap (b)$. Es folgt $(e') \subseteq (a) \cap (b) = (e)$ und somit $e' \in (e)$. Dies zeigt, dass e' ein Vielfaches von e ist. Insgesamt ist e also ein kgV von a und b .

Setzen wir nun voraus, dass R ein Hauptidealring ist, und beweisen wir die Umkehrung von (ii). Sei d ein ggT der Elemente a und b . Das Ideal (a, b) ist ein Hauptideal, es gibt also ein $d' \in R$ mit $(a, b) = (d')$. Auf Grund von Teil (ii) ist d' ebenfalls ein ggT von a und b , also sind d und d' assoziiert. Aus $d \mid d'$ und $d' \mid d$ folgt nach Teil (i), dass $(d) = (d') = (a, b)$ gilt.

Zum Schluss beweisen wir die Umkehrung von (iii) unter der Voraussetzung, dass R ein Hauptidealring ist. Sei e ein kgV der Elemente a und b . Weil $(a) \cap (b)$ ein Hauptideal ist, gilt $(a) \cap (b) = (e')$ für ein $e' \in R$. Nach Teil (iii) ist e' damit ebenfalls ein kgV von a und b , also sind e und e' assoziiert. Wie im vorherigen Absatz folgt daraus $(e) = (e') = (a) \cap (b)$. \square

Satz 9.2 Jeder euklidische Ring R ist ein Hauptidealring.

Beweis: Sei I ein Ideal in R . Zu zeigen ist, dass es sich bei I um ein Hauptideal handelt, wozu wir $I \neq (0)$ voraussetzen können. Sei nun h eine Höhenfunktion auf R und $a \in I \setminus \{0\}$ ein Element mit $h(a) \leq h(b)$ für alle $b \in I$. Wir zeigen, dass dann $I = (a)$ gilt.

Ist $b \in I$ beliebig vorgegeben, dann liefert Division mit Rest Elemente $q, r \in R$ mit $b = qa + r$, wobei $r = 0$ oder $h(r) < h(a)$ gilt. Im ersten Fall ist b in (a) enthalten. Ansonsten ist mit $a, b \in I$ auch $r = b - qa$ ein Element aus I . Aber die Ungleichung $h(r) < h(a)$ widerspricht der Bedingung, die wir an das Element a gestellt haben. Es folgt $I \subseteq (a)$, und zusammen mit $a \in I$ erhalten wir $I = (a)$. \square

Aus dem Satz folgt, dass der Ring \mathbb{Z} der ganzen Zahlen ein Hauptidealring ist. Dasselbe gilt für die Polynomringe $K[x]$ über beliebigen Körpern K und für den Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen.

Definition 9.3 Sei R ein Ring. Ein Element $p \in R$ wird *irreduzibel* genannt, wenn p weder eine Einheit noch Null ist und die Implikation

$$p = ab \Rightarrow a \in R^\times \text{ oder } b \in R^\times$$

für alle $a, b \in R$ erfüllt ist. Nichteinheiten ungleich Null, die nicht irreduzibel sind, bezeichnen wir als *reduzible* Ringelemente.

Definition 9.4 Sei R ein Ring. Ein Element $p \in R$ heißt **Primelement**, wenn p weder eine Einheit noch Null ist und außerdem die Implikation

$$p \mid (ab) \Rightarrow p \mid a \text{ oder } p \mid b \quad \text{für alle } a, b \in R \text{ erfüllt ist.}$$

Der folgende Satz stellt einen Zusammenhang zwischen den beiden neuen Begriffen her.

Satz 9.5 In einem Integritätsbereich ist jedes Primelement irreduzibel.

Beweis: Sei p ein Primelement. Dann ist p jedenfalls ungleich Null und keine Einheit. Seien nun $a, b \in R$ mit $p = ab$ vorgegeben. Dann gilt insbesondere $p \mid (ab)$, und auf Grund der Primelement-Eigenschaft gilt $p \mid a$ oder $p \mid b$. Setzen wir o.B.d.A. voraus, dass $p \mid a$ der Fall ist. Dann gibt es ein $c \in R$ mit $a = cp$, und wir erhalten $p = ab = cpb$. Die Kürzungsregel liefert $cb = 1$, also ist b eine Einheit. Damit ist die Irreduzibilität von p nachgewiesen. \square

Proposition 9.6 Sei R ein Integritätsbereich, und seien $p, q \in R$ assoziiert.

- (i) Ist p irreduzibel, dann gilt dasselbe für q .
- (ii) Ist p ein Primelement, dann ist auch q ein Primelement.

Beweis: Nach Voraussetzung gibt es ein $\varepsilon \in R^\times$ mit $q = \varepsilon p$.

zu (i) Sei p irreduzibel. Wäre q eine Einheit, dann würde $p = \varepsilon^{-1}q$ als Produkt zweier Einheiten ebenfalls in R^\times liegen. Wäre $q = 0$, dann würde auch $p = \varepsilon^{-1}0 = 0$ folgen. Seien nun $a, b \in R$ Ringelemente mit $q = ab$. Dann folgt $p = \varepsilon^{-1}q = (\varepsilon^{-1}a)b$. Weil p irreduzibel ist, erhalten wir $\varepsilon^{-1}a \in R^\times$ oder $b \in R^\times$. Es folgt $a = \varepsilon(\varepsilon^{-1}a) \in R^\times$ oder $b \in R^\times$.

zu (ii) Sei p ein Primelement. Wie unter (i) folgt daraus zunächst, dass q dann weder eine Einheit noch Null ist. Seien nun $a, b \in R$ mit $q \mid (ab)$ vorgegeben. Dann gibt es ein $c \in R$ mit $ab = cq$. Es folgt $ab = c\varepsilon p$, also $p \mid (ab)$. Weil p ein Primelement ist, gilt $p \mid a$ oder $p \mid b$. Ohne Beschränkung der Allgemeinheit können wir $p \mid a$ annehmen. Dies bedeutet, dass ein $c' \in R$ mit $a = c'p = c'\varepsilon^{-1}q$ existiert. Daraus wiederum folgt $q \mid a$. Die Implikation $q \mid (ab) \Rightarrow q \mid a$ oder $q \mid b$ ist damit bewiesen. \square

Proposition 9.7 Im Ring \mathbb{Z} der ganzen Zahlen sind die irreduziblen Elemente genau die Zahlen der Form $\pm p$, wobei p die Primzahlen durchläuft.

Beweis: „ \Rightarrow “ Sei p eine Primzahl. Dann gilt nach Definition $p \neq 0$. Außerdem ist p keine Einheit, denn die beiden Einheiten ± 1 im Ring \mathbb{Z} sind keine Primzahlen. Wäre p nicht irreduzibel, dann gäbe es nach Definition Zahlen $r, s \in \mathbb{Z}$ mit $p = rs$, wobei r und s beides keine Einheiten, also ungleich ± 1 sind. Indem wir gegebenenfalls r durch $-r$ und s durch $-s$ ersetzen, können wir $r, s \in \mathbb{N}$ annehmen. Aus $r, s > 1$ folgt dann $1 < r, s < p$. Aber dies zusammen mit der Gleichung $p = rs$ widerspricht der definierenden Eigenschaft der Primzahlen. Da sich die Eigenschaft eines Elements,

irreduzibel zu sein, durch Multiplikation mit Einheiten nicht ändert, ist auch $-p$ für jede Primzahl p ein irreduzibles Element in \mathbb{Z} .

„ \Leftarrow “ Sei umgekehrt $n \in \mathbb{Z}$ ein irreduzibles Element, und nehmen wir an, dass $\pm n$ beides keine Primzahlen sind. Da Multiplikation mit Einheiten an der Irreduzibilitäts-Eigenschaft nichts ändert, können wir $n > 0$ annehmen. Da n keine Primzahl ist, gilt entweder $n = 1$, oder es gibt $r, s \in \mathbb{N}$ mit $n = rs$ und $1 < r, s < n$. Im ersten Fall wäre n eine Einheit, was aber der Voraussetzung an n , ein irreduzibles Element zu sein, widerspricht. Im zweiten Fall haben wir n als Produkt von Nicht-Einheiten dargestellt, was ebenfalls einen Widerspruch zur Voraussetzung bedeutet. \square

Wir werden im nächsten Abschnitt zeigen, dass in einer allgemeinen Klasse von Ringen, welche die Hauptidealringe umfasst, die irreduziblen Elemente genau mit den Primelementen zusammenfallen. Also sind in \mathbb{Z} auch die Primelemente genau die Zahlen $\pm p$, wobei p die Primzahlen durchläuft.

In beliebigen Integritätsbereichen sind irreduzible Elemente dagegen im allgemeinen nicht prim. Um dies zu sehen, formulieren wir ein Kriterium, mit dem sich leicht feststellen lässt, ob Elemente in Ringen der Form $\mathbb{Z}[\sqrt{-d}]$ (mit $d \in \mathbb{N}$) irreduzibel sind. Wieder verwenden wir dazu die multiplikative Funktion $N : \mathbb{C} \rightarrow \mathbb{R}_+$, die auf $\mathbb{Z}[\sqrt{-d}]$ wegen $N(a + b\sqrt{-d}) = a^2 + db^2$ für $a, b \in \mathbb{Z}$ nur die natürlichen Zahlen und Null als Werte annimmt.

Proposition 9.8 Sei $d \in \mathbb{N}$, $R = \mathbb{Z}[\sqrt{-d}]$ und $\alpha \in R$ beliebig.

- (i) Das Element α ist genau dann eine Einheit in R , wenn $N(\alpha) = 1$ ist.
- (ii) Ist $N(\alpha)$ eine Primzahl, dann ist α in R irreduzibel.
- (iii) Gilt $N(\alpha) = p^2$ mit einer Primzahl p , und besitzt die Gleichung $a^2 + db^2 = p$ keine Lösung mit $a, b \in \mathbb{Z}$, dann ist α ebenfalls ein irreduzibles Element.

Beweis: zu (i) „ \Rightarrow “ Ist α eine Einheit, dann gibt es ein $\beta \in R$ mit $\alpha\beta = 1$. Auf Grund der Multiplikativität von N gilt $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Weil $N(\alpha)$ und $N(\beta)$ beides natürliche Zahlen sind, muss $N(\alpha) = N(\beta) = 1$ gelten. „ \Leftarrow “ Sei $\alpha = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$. Nach Voraussetzung gilt

$$a^2 + db^2 = N(\alpha) = 1.$$

Da a^2 und b^2 natürliche Zahlen sind, muss $a = 0$ oder $b = 0$ gelten, darüber hinaus $a = \pm 1$ oder $d = -1$, $b = \pm 1$. Es folgt $\alpha = \pm 1$ oder $\alpha = \pm\sqrt{-1}$, wobei letzteres nur im Fall $d = -1$ auftreten kann. Alle vier Elemente sind Einheiten in R , denn es gilt $1 \cdot 1 = 1$, $(-1)(-1) = 1$ und $\sqrt{-1} \cdot (-\sqrt{-1}) = 1$.

zu (ii) Sei $\alpha \in R$ und $p = N(\alpha)$ eine Primzahl. Dann kann α keine Einheit sein, denn nach (i) ist dafür $N(\alpha) = 1$ erforderlich. Sei nun $\alpha = \beta\gamma$ eine Zerlegung von α mit $\beta, \gamma \in R$. Dann folgt $p = N(\alpha) = N(\beta)N(\gamma)$. Da $N(\beta), N(\gamma)$ natürliche Zahlen und p eine Primzahl ist, folgt $N(\beta) = 1$ oder $N(\gamma) = 1$. Nach (i) ist damit β oder γ eine Einheit. Damit ist die Irreduzibilität von α bewiesen.

zu (iii) Nehmen wir an, dass $\alpha \in R$ die angegebenen Voraussetzungen erfüllt, aber nicht irreduzibel ist. Wegen $N(\alpha) = p^2$ kann α keine Einheit sein. Ist $\alpha = \beta\gamma$ mit $\beta, \gamma \in R$, und sind β, γ beides keine Einheiten, dann ist wegen $N(\beta)N(\gamma) = p^2$ nur $N(\beta) = N(\gamma) = p$ möglich. Schreiben wir $\beta = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, dann gilt $p = N(\beta) = a^2 + db^2$. Aber dies ist unmöglich, da die Gleichung nach Voraussetzung mit $a, b \in \mathbb{Z}$ nicht lösbar ist. Also ist α irreduzibel. \square

Folgerung 9.9 Sei $d \in \mathbb{N}$. Für die Einheitengruppe von $R = \mathbb{Z}[\sqrt{-d}]$ gilt $R^\times = \{\pm 1, \pm\sqrt{-1}\}$, falls $d = 1$ ist, ansonsten $R^\times = \{\pm 1\}$.

Beweis: Dies ist ein Nebenergebnis des Beweises von Proposition 9.8. □

Als Anwendung der bisherigen Ergebnisse zeigen wir, dass die Elemente 2 und $1 + \sqrt{-3}$ im Ring $R = \mathbb{Z}[\sqrt{-3}]$ irreduzibel, aber keine Primelemente sind. Beide Elemente sind nach Proposition 9.8 (iii) irreduzibel, denn es gilt

$$N(2) = N(1 + \sqrt{-3}) = 4 = 2^2,$$

aber die Gleichung $a^2 + 3b^2 = 2$ ist mit $a, b \in \mathbb{Z}$ nicht lösbar. Um zu zeigen, dass 2 und $1 + \sqrt{-3}$ keine Primelemente sind, betrachten wir in R die Gleichung

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Die Zahl 2 ist ein Teiler des Produkts $(1 + \sqrt{-3})(1 - \sqrt{-3})$. Andererseits teilt 2 keine der beiden Elemente $1 \pm \sqrt{-3}$. Wäre dies der Fall, dann gäbe es ein $\gamma \in R$ mit $1 \pm \sqrt{-3} = 2\gamma$, und diese γ wäre eines der beiden Elemente $\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$. Insbesondere läge eine dieser beiden Zahlen in R . Dies würde bedeuten, dass $a, b \in \mathbb{Z}$ existieren, so dass eine der beiden Gleichungen

$$\frac{1}{2} \pm \frac{1}{2}\sqrt{-3} = a + b\sqrt{-3}$$

erfüllt ist. Vergleichen wir aber den Realteil auf beiden Seiten, dann erhalten wir $a = \frac{1}{2}$ im Widerspruch zu $a \in \mathbb{Z}$. Also ist 2 in R tatsächlich kein Primelement. Genauso zeigt man, dass auch das Element $1 + \sqrt{-3}$ nicht prim ist.

Die Primelemente hängen mit den bereits früher definierten Primidealen eng zusammen. Es gilt nämlich

Proposition 9.10 Sei R ein Integritätsbereich und $p \in R$, $p \neq 0_R$. Genau dann ist p ein Primelement in R , wenn das Hauptideal (p) ein Primideal ist.

Beweis: „ \Rightarrow “ Wäre $(p) = (1)$, dann wäre die 1 in (p) enthalten, und folglich gäbe es ein $r \in R$ mit $rp = 1$. Dies würde bedeuten, dass p eine Einheit ist, was aber nach Voraussetzung nicht der Fall ist. Seien nun $a, b \in R$ mit $ab \in (p)$. Dann gibt es ein $r \in R$ mit $ab = rp$, also ist p ein Teiler von ab . Weil p ein Primelement ist, folgt $p|a$ oder $p|b$. Im ersten Fall gilt $a \in (p)$, im zweiten $b \in (p)$.

„ \Leftarrow “ Wäre p eine Einheit, dann gäbe es ein $r \in R$ mit $rp = 1$. Daraus würde dann $1 \in (p)$ und $(p) = (1)$ folgen, was aber der Voraussetzung widerspricht. Seien nun $a, b \in R$, so dass $p|(ab)$ gilt. Dann folgt $ab \in (p)$, und aus der Primidealeigenschaft von (p) folgt $a \in (p)$ oder $b \in (p)$. Im ersten Fall wäre $p|a$, im zweiten $p|b$ erfüllt. □

Satz 9.11 Sei R ein Hauptidealring, aber kein Körper, und $p \in R$. Dann sind die folgenden Aussagen äquivalent.

- (i) Das Element p ist prim.
- (ii) Das Element p ist irreduzibel.
- (iii) Das Ideal (p) ist maximal.
- (iv) Das Ideal (p) ist ein Primideal, und es gilt $p \neq 0_R$.

Beweis: „(i) \Rightarrow (ii)“ Nach Satz 9.5 ist jedes Primelment in einem Integritätsbereich irreduzibel.

„(ii) \Rightarrow (iii)“ Zunächst ist $(p) = (1)$ unmöglich, denn sonst wäre p eine Einheit und damit kein irreduzibles Element. Sei nun \mathfrak{m} ein Ideal mit $(p) \subseteq \mathfrak{m} \subseteq (1)$ und $a \in R$ mit $\mathfrak{m} = (a)$. Wegen $(p) \subseteq (a)$ gilt $a|p$, es gibt also ein $b \in R$ mit $p = ab$. Weil p irreduzibel ist, muss a oder b eine Einheit sein. Im ersten Fall ist $\mathfrak{m} = (a) = (1)$, im zweiten $\mathfrak{m} = (p)$. Also ist (p) in der Tat ein maximales Ideal.

„(iii) \Rightarrow (iv)“ Nach Folgerung 6.13 ist jedes maximale Ideal in einem Ring ein Primideal. Nehmen wir nun an, es gilt $(p) = (0_R)$. Auf Grund der Maximalität von (p) sind dann (0_R) und (1_R) die einzigen Ideale in R . Nach Lemma 6.11 würde das bedeuten, dass R ein Körper ist. Aber dies ist nach Voraussetzung ausgeschlossen.

„(iv) \Rightarrow (i)“ Das folgt aus Proposition 9.10. □

Anhang: Beispiel für einen Hauptidealring, der kein euklidischer Ring ist

Die naheliegende Frage, ob solche Ringe existieren, wird in der aktuellen Lehrbuchliteratur übergangen, so dass unklar bleibt, ob die Hauptidealringe überhaupt eine echte Verallgemeinerung der euklidischen Ringe darstellen. Wir zeigen, dass der Ring $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ zwar ein Hauptidealring, aber kein euklidischer Ring ist. Dabei folgen wir im Wesentlichen der Darstellung von [Wi], der einen zuvor erbrachten Beweis in der Veröffentlichung [Ca] weiter vereinfachen konnte.

Satz 9.12 Der Ring $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ ist ein Hauptidealring.

Beweis: In Satz 2.8 wurde gezeigt, dass die Elemente von R durch $R = \{\frac{1}{2}a + \frac{1}{2}b\sqrt{-19} \mid a, b \in \mathbb{Z}, a \equiv b \pmod{2}\}$ gegeben sind. Sei nun I ein Ideal in R ungleich (0) . Zu zeigen ist, dass es sich bei I um ein Hauptideal handelt. Die Normfunktion $N(z) = |z|^2$ nimmt auf $R \setminus \{0\}$ nur Werte aus \mathbb{N} an, denn für alle $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ und $a \equiv b \pmod{2}$ ist

$$N(\frac{1}{2}a + \frac{1}{2}b\sqrt{-19}) = \frac{1}{4}(a^2 + 19b^2)$$

positiv und ganzzahlig. Sind nämlich a und b beide gerade, dann sind die Zahlen a^2 und $19b^2$ beide durch vier teilbar. Sind a und b beide ungerade, dann gilt $a^2 \equiv b^2 \equiv 1 \pmod{4}$, und wegen $19 \equiv 3 \pmod{4}$ folgt $a^2 + 19b^2 \equiv 1 + 3 \cdot 1 \equiv 4 \equiv 0 \pmod{4}$.

Auf Grund dieser Eigenschaft der Normfunktion gibt es ein $\alpha \in I \setminus \{0\}$, so dass $|\alpha|$ minimal ist. Nehmen wir nun an, I ist kein Hauptideal. Dann gibt es ein $\beta \in I \setminus (\alpha)$. Sei $\rho = \frac{\beta}{\alpha}$. In einem ersten Schritt zeigen wir, dass β so gewählt werden kann, dass $|\operatorname{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$ erfüllt ist. Dazu setzen wir $r = \frac{1}{\sqrt{19}}\operatorname{Im}(\rho)$ und wählen $s \in \mathbb{Z}$ so, dass $|2r - s| \leq \frac{1}{2}$ erfüllt ist. Definieren wir dann $\beta' = \beta - \frac{1}{2}s(1 + \sqrt{-19})\alpha$, dann folgt

$$\frac{\beta'}{\alpha} = \frac{\beta}{\alpha} - \frac{1}{2}s(1 + \sqrt{-19}) = \operatorname{Re}(\rho) + i\operatorname{Im}(\rho) - \frac{1}{2}s - i \cdot \frac{1}{2}s\sqrt{19}$$

und somit $\operatorname{Im}(\frac{\beta'}{\alpha}) = \sqrt{19}(r - \frac{1}{2}s)$ und $|\operatorname{Im}(\frac{\beta'}{\alpha})| \leq \frac{1}{4}\sqrt{19}$. Ersetzen wir also β durch β' , dann ist $|\operatorname{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$ also erfüllt. Außerdem gilt weiterhin $\beta \in I \setminus (\alpha)$, wenn wir β durch β' ersetzen. Denn mit β liegt auch $\beta' = \beta - \frac{1}{2}s(1 + \sqrt{-19})\alpha$ in I , und wäre β' ein Element des Hauptideals (α) , dann würde dies auch für β gelten.

In einem zweiten Schritt zeigen wir, dass ein $\gamma \in I \setminus \{0\}$ mit $|\gamma| < |\alpha|$ existiert und führen damit die Minimalität von α zum Widerspruch. Zunächst betrachten wir den Fall, dass sogar $|\operatorname{Im}(\rho)| < \frac{1}{2}\sqrt{3}$ erfüllt ist. Wählen wir $a \in \mathbb{Z}$ so, dass $|\operatorname{Re}(\rho) - a| \leq \frac{1}{2}$ gilt, dann folgt $|\rho - a|^2 < (\frac{1}{2})^2 + (\frac{1}{2}\sqrt{3})^2 = 1$. Sei nun $\gamma = \beta - a\alpha$. Dann liegt γ in I , das Element ist wegen $\beta \notin (\alpha)$ ungleich Null, und es gilt $|\beta - a\alpha| = |\alpha||\rho - a| < |\alpha|$, wie gewünscht.

Nun betrachten wir noch den Fall $\frac{1}{2}\sqrt{3} \leq |\operatorname{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$. Sei $\delta = 2\beta - \frac{1}{2}(1 + \sqrt{-19})\alpha$. Dann gilt $\frac{\delta}{\alpha} = 2\rho - \frac{1}{2}(1 + \sqrt{-19})$. Ersetzen wir nötigenfalls β durch $-\beta$ und ρ durch $-\rho$, dann können wir $\frac{1}{2}\sqrt{3} \leq \operatorname{Im}(\rho) \leq \frac{1}{4}\sqrt{19}$ annehmen. Es folgt dann $\sqrt{3} \leq \operatorname{Im}(2\rho) \leq \frac{1}{2}\sqrt{19}$ und $\sqrt{3} - \frac{1}{2}\sqrt{19} \leq \operatorname{Im}(2\rho - \frac{1}{2}(1 + \sqrt{-19})) = \operatorname{Im}(\frac{\delta}{\alpha}) \leq 0$. Wir wählen nun $a \in \mathbb{Z}$ so, dass $|\operatorname{Re}(2\rho - \frac{1}{2}(1 + \sqrt{-19})) - a| \leq \frac{1}{2}$ erfüllt ist und definieren $\gamma = \delta - a\alpha$. Dann gilt

$$\left|\frac{\gamma}{\alpha}\right|^2 = \left|\frac{\delta}{\alpha} - a\right|^2 = |\operatorname{Re}(\frac{\delta}{\alpha} - a) + i\operatorname{Im}(\frac{\delta}{\alpha})|^2 = |\operatorname{Re}(\frac{\delta}{\alpha} - a)|^2 + |\operatorname{Im}(\frac{\delta}{\alpha})|^2 \leq \frac{1}{4} + (\sqrt{3} - \frac{1}{2}\sqrt{19})^2.$$

Wir zeigen, dass $(\sqrt{3} - \frac{1}{2}\sqrt{19})^2 < \frac{3}{4}$ ist. Daraus folgt dann $|\frac{\gamma}{\alpha}|^2 < 1$ und $|\gamma| < |\alpha|$, so dass wir auch in diesem Fall am Ziel sind. Aus $\sqrt{19} < \sqrt{27} = 3\sqrt{3}$ folgt $\frac{1}{2}\sqrt{19} < \frac{3}{2}\sqrt{3}$. Durch Subtraktion von $\sqrt{3}$ auf beiden Seiten erhalten wir $\frac{1}{2}\sqrt{3} > \frac{1}{2}\sqrt{19} - \sqrt{3}$, und $\frac{1}{2}\sqrt{19} - \sqrt{3}$ ist positiv wegen $3 < \frac{19}{4} \Leftrightarrow 12 < 19$. Durch Quadrieren erhalten wir nun die gewünschte Abschätzung $(\sqrt{3} - \frac{1}{2}\sqrt{19})^2 < \frac{3}{4}$. \square

Satz 9.13 Der Ring $R = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$ ist kein euklidischer Ring.

Beweis: Mit ähnlichen Argumenten wie in Prop. 9.8 zeigen wir zunächst, dass die Einheitengruppe von R durch $R^\times = \{\pm 1\}$ gegeben ist, und dass die Elemente 2 und 3 in R irreduzibel sind. Wegen $1 \cdot 1 = 1$ und $(-1)(-1) = 1$ sind ± 1 jedenfalls Einheiten. Ist umgekehrt $\varepsilon \in R^\times$, dann gilt $N(\varepsilon)N(\varepsilon^{-1}) = N(\varepsilon\varepsilon^{-1}) = N(1) = 1$. Aus $N(\varepsilon), N(\varepsilon^{-1}) \in \mathbb{N}$ und $N(\varepsilon)N(\varepsilon^{-1}) = 1$ folgt $N(\varepsilon) = 1$. Schreiben wir $\varepsilon = \frac{1}{2}a + \frac{1}{2}b\sqrt{-19}$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \pmod{2}$, dann folgt $\frac{1}{4}a^2 + \frac{19}{4}b^2 = N(\varepsilon) = 1$ und $a^2 + 19b^2 = 4$. Die einzigen ganzzahligen Lösungen dieser Gleichung sind $(a, b) = (\pm 2, 0)$. Es folgt $\varepsilon \in \{\pm 1\}$. Die Einheitengruppe von R also gegeben durch $R^\times = \{\pm 1\}$ und besteht genau aus den Elementen mit Norm 1.

Wegen $N(2) = 4 > 1$ und $N(3) = 9 > 1$ sind 2 und 3 jedenfalls keine Einheiten. Wäre 2 reduzibel, dann gäbe es Elemente $\alpha, \beta \in R$, die keine Einheiten in R sind und $\alpha\beta = 2$ erfüllen. Es wäre dann $N(\alpha)N(\beta) = N(\alpha\beta) = N(2) = 4$. Wegen $\alpha, \beta \notin R^\times$ gilt außerdem $N(\alpha), N(\beta) > 1$. Damit bleibt $N(\alpha) = N(\beta) = 2$ als einzige Möglichkeit. Schreiben wir $\alpha = \frac{1}{2}a + \frac{1}{2}b\sqrt{-19}$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \pmod{2}$, dann ist $N(\alpha) = 2$ äquivalent zu $\frac{1}{4}a^2 + \frac{19}{4}b^2 = 2 \Leftrightarrow a^2 + 19b^2 = 8$. Aber diese Gleichung besitzt offenbar keine Lösung mit $(a, b) \in \mathbb{Z}^2$. Ebenso zeigt die Unlösbarkeit der Gleichung $a^2 + 19b^2 = 12$, dass 3 im Ring R irreduzibel ist.

Nach diesen Vorbereitungen nehmen wir nun an, dass R euklidisch und $h : R \setminus \{0\} \rightarrow \mathbb{N}$ eine Höhenfunktion auf R ist. Weiter sei $\pi \in R$ eine Nichteinheit mit der Eigenschaft, dass $h(\pi)$ für alle Nicht-Einheiten aus $R \setminus \{0\}$ ein minimaler Wert ist. Wir zeigen, dass π dann in der Menge $\{\pm 2, \pm 3\}$ enthalten sein muss. Durch Division mit Rest erhalten wir Elemente $\gamma, \rho \in R$ mit $2 = \gamma\pi + \rho$, wobei $\rho = 0$ oder $\rho \neq 0$ und $h(\rho) < h(\pi)$ gelten muss. Auf Grund der Minimalität von $h(\pi)$ gibt es nur die beiden Möglichkeiten, dass $\rho = 0$ oder eine Einheit ist. Es gilt also $\rho \in \{-1, 0, 1\}$. Im Fall $\rho = 0$ wäre π ein Teiler von 2. Auf Grund der Irreduzibilität von 2 sind 2 und π dann assoziiert, und daraus folgt $\pi \in \{\pm 2\}$.

Betrachten wir nun den Fall $\rho = 1$. Die Gleichung $2 = \gamma\pi + 1$ liefert dann $\gamma\pi = 1$. Aber dies steht im Widerspruch dazu, dass π keine Einheit ist. Als letzte Möglichkeit betrachten wir den Fall $\rho = -1$. Dann gilt $2 = \gamma\pi - 1$. Dann gilt $\gamma\pi = 3$. Weil 3 irreduzibel ist, sind π und 3 assoziiert, also $\pi \in \{\pm 3\}$. Damit haben wir insgesamt gezeigt, dass in jedem möglichen Fall $\pi \in \{\pm 2, \pm 3\}$ gilt.

Sei nun $\theta = \frac{1}{2}(1 + \sqrt{-19})$. Wiederum wenden wir Division mit Rest an und erhalten Elemente $\gamma, \rho \in R$ mit $\theta = \gamma\pi + \rho$, wobei $\rho = 0$ oder $\rho \neq 0$ und $h(\rho) < h(\pi)$ gilt. Wie zuvor schließen wir daraus $\rho \in \{-1, 0, 1\}$. Im Fall $\rho = 0$ gilt $\theta = \gamma\pi$. Im Fall $\rho = 1$ ist $\theta - 1 = \gamma\pi$, und im Fall $\rho = -1$ ist $\theta + 1 = \gamma\pi$. Also ist eines der Elemente $\theta - 1, \theta, \theta + 1$ auf jeden Fall durch π teilbar. Es gilt aber $\pi \in \{\pm 2, \pm 3\}$, und wie man sich leicht überzeugt, ist keines der sechs Elemente

$$\frac{1}{2}(\theta - 1), \frac{1}{2}\theta, \frac{1}{2}(\theta + 1), \frac{1}{3}(\theta - 1), \frac{1}{3}\theta, \frac{1}{3}(\theta + 1)$$

in R enthalten. Die Annahme, dass eine Höhenfunktion h auf R existiert, hat also insgesamt zu einem Widerspruch geführt. Also ist R kein euklidischer Ring. \square

Zum Schluss sei noch erwähnt, dass es Beispiele für quadratische Zahlringe $\mathbb{Z}[\sqrt{d}]$ gibt, die zwar euklidisch sind, bei denen aber die Höhenfunktion nichts mit der in der Vorlesung eingeführten Normfunktion der Form $N(a + b\sqrt{d}) = |a^2 - db^2|$ zu tun hat. In [Ha] wird dies zum Beispiel für den Ring $\mathbb{Z}[\sqrt{14}]$ bewiesen.

§ 10. Faktorielle Ringe

Zusammenfassung. Aus der Schulmathematik ist der **Fundamentalsatz der Algebra** bekannt, welcher besagt, dass sich jede natürliche Zahl > 1 auf eindeutige Weise als Produkt von Primzahlen schreiben lässt. Im letzten Kapitel wurden die Primelemente als Analoga der Primzahlen für beliebige Ringe definiert. Deshalb ist es eine naheliegende Frage, in welchen Ringen Elemente auf eindeutige Weise als Produkte von Primelementen darstellbar sind. Ringe mit dieser Eigenschaft werden wir als **faktorielle Ringe** bezeichnen. Natürlich gibt es bei der Eindeutigkeit ein paar offensichtliche Einschränkungen: Die Reihenfolge der Faktoren kann beliebig gewählt werden (auf Grund der Kommutativität der Multiplikation), und auch Produktzerlegungen wie $2 \cdot 3 \cdot 5$ und $2 \cdot (-3) \cdot (-5)$, die sich also nur um Einheiten des Rings (hier \mathbb{Z}) unterscheiden, sieht man als „im Wesentlichen gleich“ an. Fixiert man ein Repräsentantensystem der Primelemente des Rings, dann lässt sich aber eine vollkommen eindeutige Produktdarstellung der Ringelemente definieren; in \mathbb{Z} bilden zum Beispiel die (positiven) Primzahlen ein solches System. Zum Schluss des Kapitels wird noch gezeigt, dass alle Hauptidealringe, und damit erst recht alle euklidischen Ringe, faktoriell sind.

Wichtige Grundbegriffe

- faktorieller Ring
- Repräsentantensystem der Primelemente

Zentrale Sätze

- Eindeutigkeit der Primfaktorzerlegung bis auf Einheiten und Reihenfolge
- Eindeutigkeit der Primfaktorzerlegung bis auf Reihenfolge (nach Wahl eines Repräsentantensystems der Primelemente)
- Hauptidealringe sind faktoriell.

Definition 10.1 Ein **faktorieller Ring** ist ein Integritätsbereich R mit der Eigenschaft, dass jedes Element $r \in R$, das weder gleich Null noch eine Einheit ist, als Produkt von Primelementen dargestellt werden kann. Dies bedeutet: Es gibt ein $n \in \mathbb{N}$ und Primelemente $p_1, \dots, p_n \in R$, so dass

$$r = p_1 \cdot p_2 \cdot \dots \cdot p_n \quad \text{gilt.}$$

Im folgenden verwenden wir für zwei Ringelemente a, a' in einem Ring R die Notation $a \sim a'$, um zu kennzeichnen, dass a und a' zueinander assoziiert sind, siehe Definition 4.1.

Lemma 10.2 Sei R ein Integritätsbereich.

- Seien $a, a', b, b' \in R$, wobei $a \sim a'$, $b \sim b'$ und $a|b$ gilt. Dann gilt auch $a'|b'$.
- Jedes Element in R , das eine Einheit teilt, ist selbst eine Einheit.
- Ein Element, das von einem Primelement geteilt wird, ist keine Einheit.

Beweis: zu (i) Wegen $a \sim a'$ und $b \sim b'$ gibt es Einheiten ε, μ in R mit $a' = \varepsilon a$ und $b' = \mu b$. Aus $a|b$ folgt, dass ein $c \in R$ mit $b = ac$ existiert. Wir erhalten $b' = \mu ac = \mu \varepsilon^{-1} a' c$ und somit $a'|b'$.

zu (ii) Sei $\varepsilon \in R^\times$ und $a \in R$ mit $a|\varepsilon$. Weil die Elemente ε und 1_R assoziiert sind, gilt $a|1_R$ nach Teil (i). Umgekehrt ist 1_R das Einselement ein Teiler von a , denn es gilt $a = 1_R \cdot a$. Also sind a und 1_R assoziiert. Dies bedeutet, dass ein $\mu \in R^\times$ mit $a = \mu \cdot 1_R = \mu$ existiert.

zu (iii) Wäre $\varepsilon \in R^\times$ und p ein Primelement mit $p|\varepsilon$, dann wäre p nach (ii) eine Einheit. Ein Ringelement kann nach Definition aber nicht zugleich Einheit und Primelement sein. \square

Proposition 10.3 In einem faktoriellen Ring R ist jedes irreduzible Element ein Primelement.

Beweis: Sei $p \in R$ irreduzibel. Da R faktoriell und p weder gleich Null noch eine Einheit ist, gibt es eine Darstellung $p = p_1 \cdot \dots \cdot p_n$ von p als Produkt von Primementen. Im Fall $n > 1$ könnten wir p damit als Produkt $p = p_1 \cdot (p_2 \cdot \dots \cdot p_n)$ schreiben. Dabei ist p_1 eine Nicht-Einheit, ebenso das Produkt $p_2 \cdot \dots \cdot p_n$ nach Teil (iii) von Lemma 10.2. Aber dies widerspricht der Irreduzibilität von p . Also ist $n = 1$ und $p = p_1$ ein Primelement. \square

Satz 10.4 Sei R ein Integritätsbereich. Dann sind äquivalent

- (i) R ist ein faktorieller Ring.
- (ii) Jedes Element $r \in R$, dass weder gleich Null noch eine Einheit ist, kann als Produkt von irreduziblen Elementen dargestellt werden, und diese Darstellung ist im wesentlichen eindeutig. Dies bedeutet genau: Sind $m, n \in \mathbb{N}$ und

$$p_1 \cdot \dots \cdot p_m = r = q_1 \cdot \dots \cdot q_n$$

zwei Darstellungen von r als Produkt irreduzibler Elemente p_i, q_j , dann ist $m = n$, und nach eventueller Umnummerierung der Elemente ist p_i assoziiert zu q_i für $1 \leq i \leq m$.

Beweis: „(ii) \Rightarrow (i)“ Hier genügt es zu zeigen, dass unter der gegebenen Voraussetzung jedes irreduzible Element in R ein Primelement ist. Sei $p \in R$ irreduzibel. Dann ist p weder gleich Null noch eine Einheit. Seien nun $a, b \in R$ mit $p|(ab)$ vorgegeben. Zu zeigen ist, dass p ein Teiler von a oder ein Teiler von b ist.

Nehmen wir zunächst an, dass $a = 0_R$ oder $b = 0_R$ gilt. Weil das Nullelement 0_R von jedem Ringelement geteilt wird, folgt daraus sofort $p|a$ oder $p|b$. Nehmen wir nun an, dass eines der Elemente a, b eine Einheit ist, o.B.d.A. das Element b . Dann wären a und ab assoziiert, und aus $p|(ab)$ würde nach Teil (i) von Lemma 10.2 $p|a$ folgen. Also können wir auch $a, b \notin R^\times$ annehmen. Wegen $p|(ab)$ gibt es ein $c \in R$ mit $ab = pc$. Wäre $c = 0_R$, dann würde daraus $ab = 0_R$ und somit $a = 0_R$ oder $b = 0_R$ folgen. Aber dies haben wir bereits ausgeschlossen.

Weil a und b beide weder gleich Null noch Einheiten sind, besitzen sie jeweils eine Darstellung als Produkt von irreduziblen Elementen. Seien also $p_i, q_j \in R$ irreduzible Elemente, so dass $a = p_1 \cdot \dots \cdot p_m$ und $b = q_1 \cdot \dots \cdot q_n$ erfüllt ist. Das Element c kann keine Einheit sein, denn sonst hätten wir eine Gleichung der Form $(p_1 \cdot \dots \cdot p_m)(q_1 \cdot \dots \cdot q_n) = pc$, wobei rechts ein einziges irreduzibles Element, auf der linken Seite aber ein Produkt von mindestens zwei irreduziblen

Elementen steht. Dies widerspricht der vorausgesetzten Eindeutigkeit. Weil also auch c weder gleich Null noch eine Einheit ist, besitzt auch c eine Zerlegung der Form $r_1 \cdot \dots \cdot r_k$ mit irreduziblen Elementen r_i . Wir erhalten also eine Gleichung der Form

$$(p_1 \cdot \dots \cdot p_m) \cdot (q_1 \cdot q_n) = (r_1 \cdot \dots \cdot r_k) \cdot p.$$

Auf Grund der Eindeutigkeit der Produktzerlegung ist p zu einem Faktor auf der linken Seite der Gleichung assoziiert. Gilt $p \sim p_i$ für ein $i \in \{1, \dots, m\}$, dann ist p ein Teiler von a . Gilt $p \sim q_j$ für ein $j \in \{1, \dots, n\}$, dann ist p ein Teiler von b .

“(i) \Rightarrow (ii)“ Nach Voraussetzung besitzt jede Nicht-Einheit $r \in R$, $r \neq 0_R$ eine Darstellung als Produkt von Primelementen, damit insbesondere als Produkt von irreduziblen Elementen. Zu zeigen bleibt, dass diese Produktdarstellung im Wesentlichen eindeutig ist. Seien also

$$p_1 \cdot \dots \cdot p_m = r = q_1 \cdot \dots \cdot q_n$$

zwei Darstellungen von r also Produkt von irreduziblen Elementen p_i, q_j . Wie wir bereits gezeigt haben, sind die p_i und q_j zugleich Primelemente. Wir beweisen nun durch vollständige Induktion über n , dass $n = m$ gilt und nach Ummummerierung p_i zu q_i assoziiert ist, für $1 \leq i \leq n$. Im Fall $n = 1$ gilt

$$p_1 \cdot \dots \cdot p_m = q_1.$$

Weil q_1 irreduzibel ist, muss auch das Element auf der linken Seite der Gleichung irreduzibel sein. Dies ist nur dann der Fall, wenn $m = 1$ gilt, denn ansonsten wäre das Element links ein Produkt der beiden Nicht-Einheiten p_1 und $p_2 \cdot \dots \cdot p_m$.

Setzen wir nun die Aussage für n als gültig voraus, und nehmen wir an, dass eine Gleichung der Form

$$p_1 \cdot \dots \cdot p_m = q_1 \cdot \dots \cdot q_n \cdot q_{n+1}$$

mit $m \in \mathbb{N}$ und irreduziblen Elementen p_i, q_j besteht (wobei diese Elemente wiederum zugleich auch prim sind). Weil das Element auf der rechten Seite der Gleichung nicht irreduzibel ist, kann auch das Element links nicht irreduzibel sein, es muss also $m \geq 2$ gelten. Wiederum teilt q_1 als Primelement einen der Faktoren p_i , zum Beispiel p_1 . Es gilt also wiederum $q_1 = p_1 \varepsilon$ für ein $\varepsilon \in R^\times$, und wir erhalten

$$p_1 \cdot p_2 \cdot \dots \cdot p_m = (p_1 \varepsilon) \cdot q_2 \cdot \dots \cdot q_{n+1}.$$

Durch Kürzung erhalten wir $p_2 \cdot \dots \cdot p_m = (\varepsilon q_2) \cdot \dots \cdot q_{n+1}$. Nach Induktionsvoraussetzung gilt $m - 1 = n \Leftrightarrow m = n + 1$. Außerdem ist nach Ummummerierung das Element p_2 assoziiert zu εq_2 (also auch zu q_2), und es gilt $p_i \sim q_i$ für $3 \leq i \leq m$. \square

Definition 10.5 Sei R ein Integritätsbereich und $P \subseteq R$ eine Teilmenge bestehend aus Primelementen. Wir nennen P ein **Repräsentantensystem der Primelemente** in R , wenn jedes Primelement $q \in R$ zu genau einem $p \in P$ assoziiert ist.

Beispielsweise bilden die Primzahlen $p \in \mathbb{N}$ ein Repräsentantensystem der Primelmente in \mathbb{Z} . Ist K ein Körper, dann bilden die *normierten* irreduziblen Polynome (also die irreduziblen Polynome mit dem Leitkoeffizienten 1_K) ein Repräsentantensystem in $K[x]$.

Folgerung 10.6 Sei R ein faktorieller Ring und $P \subseteq R$ ein Repräsentantensystem der Primelemente. Dann gibt es für jedes Element $0_R \neq f \in R$ eine eindeutig bestimmte Familie $(v_p(f))_{p \in P}$ von Zahlen $v_p(f) \in \mathbb{N}_0$ und eine eindeutig bestimmte Einheit $\varepsilon \in R^\times$, so dass

$$f = \varepsilon \prod_{p \in P} p^{v_p(f)} \quad \text{erfüllt ist.}$$

Dabei gilt $v_p(f) = 0$ für alle bis auf endlich viele Elemente $p \in P$.

Da R ein faktorieller Ring ist, besitzt f eine Darstellung $f = q_1 \cdot \dots \cdot q_m$ als Produkt von Primelementen. Für jedes i gibt es ein $p_i \in P$ und eine Einheit $\varepsilon_i \in R^\times$, so dass $q_i = \varepsilon_i p_i$ gilt. Setzen wir $\varepsilon = \varepsilon_1 \cdot \dots \cdot \varepsilon_m$, dann gilt also

$$f = \varepsilon \cdot p_1 \cdot \dots \cdot p_m.$$

Definieren wir nun für jedes $p \in P$ die Zahl $v_p(f) \in \mathbb{N}_0$ durch

$$v_p(f) = |\{i \in \{1, \dots, m\} \mid p_i = p\}|,$$

dann ist die Gleichung $f = \varepsilon \prod_{p \in P} p^{v_p(f)}$ erfüllt, und für alle bis auf endlich viele $p \in P$ gilt $v_p(f) = 0$. Die Eindeutigkeit der Zahlen $v_p(f)$ folgt direkt aus der Eindeutigkeit der Zerlegung von f als Produkt irreduzibler Elemente, und mit den Zahlen $v_p(f)$ ist auch die Einheit ε eindeutig bestimmt.

Für alle $a, b \in R \setminus \{0_R\}$ gilt offenbar $v_p(ab) = v_p(a) + v_p(b)$. Seien nämlich

$$a = \varepsilon \prod_{p \in P} p^{v_p(a)} \quad \text{und} \quad b = \varepsilon' \prod_{p \in P} p^{v_p(b)}$$

die Darstellungen von $a, b \in R$ wie im Satz angegeben. Dann gilt

$$ab = \varepsilon \varepsilon' \prod_{p \in P} p^{v_p(a) + v_p(b)},$$

und aus der Eindeutigkeit der Exponenten $v_p(ab)$ folgt $v_p(ab) = v_p(a) + v_p(b)$. Die Teilbarkeitsrelation lässt sich mit Hilfe der Zahlen $v_p(a)$ also folgendermaßen umformulieren.

Lemma 10.7 Sei R ein faktorieller Ring, $P \subseteq R$ ein Repräsentantensystem der Primelemente, und seien $f, g \in R$ mit $f, g \neq 0_R$. Dann gilt $f | g$ genau dann, wenn $v_p(f) \leq v_p(g)$ für alle $p \in P$ erfüllt ist.

Beweis: Ist f ein Teiler von g , dann gibt es ein $h \in R, h \neq 0$ mit $g = fh$. Es folgt $v_p(g) = v_p(fh) = v_p(f) + v_p(h) \geq v_p(f)$ für alle $p \in P$. Gilt umgekehrt

$$f = \varepsilon \prod_{p \in P} p^{v_p(f)} \quad \text{und} \quad g = \varepsilon' \prod_{p \in P} p^{v_p(g)}$$

mit $\varepsilon, \varepsilon' \in R^\times$ und $v_p(f) \leq v_p(g)$ für alle $p \in P$, dann erhalten wir durch

$$h = \varepsilon' \varepsilon^{-1} \prod_{p \in P} p^{v_p(g) - v_p(f)}$$

ein Element $h \in R$ mit $g = fh$. Es folgt $f | g$. □

Folgerung 10.8 Sei R ein faktorieller Ring, und seien $a, b \in R \setminus \{0_R\}$ teilerfremd. Ist $0_R \neq c \in R$ ein Element mit $a|(bc)$, dann folgt $a|c$.

Beweis: Nehmen wir an, dass $a \nmid c$ gilt. Dann gibt es ein Primelement $p \in P$ mit $v_p(a) > v_p(c)$. Andererseits gilt $v_p(a) \leq v_p(bc) = v_p(b) + v_p(c)$ und somit $v_p(b) > 0$. Damit wäre dann p ein Primteiler von b , was aber der Teilerfremdheit von a und b widerspricht. \square

Satz 10.9 Sei R ein faktorieller Ring, und sei $P \subseteq R$ ein Repräsentantensystem der Primelemente in R . Seien $f_1, \dots, f_n \in R$ beliebige Elemente ungleich Null. Für jedes $p \in P$ definieren wir

$$u_p = \min\{v_p(f_i) \mid 1 \leq i \leq m\} \quad \text{und} \quad w_p = \max\{v_p(f_i) \mid 1 \leq i \leq m\}.$$

Dann ist $f = \prod_{p \in P} p^{u_p}$ ein ggT und $g = \prod_{p \in P} p^{w_p}$ ein kgV der Elemente f_1, \dots, f_m . Dies zeigt also insbesondere, dass in einem faktoriellen Ring für beliebige endliche Mengen von Elementen jeweils ein kgV und ein ggT existiert.

Beweis: Wegen $v_p(f) = u_p \leq v_p(f_i)$ für alle $p \in P$ und $1 \leq i \leq m$ ist f nach Lemma 10.7 ein gemeinsamer Teiler von f_1, \dots, f_m . Ist $h \in R$ ein weiteres Element mit $h|f_i$ für $1 \leq i \leq m$, dann folgt ebenfalls auf Grund des Lemmas jeweils $v_p(h) \leq v_p(f_i)$ für alle $p \in P$ und $1 \leq i \leq m$. Damit gilt $v_p(h) \leq u_p = v_p(f)$ für alle $p \in P$, und folglich ist h ein Teiler von f . Der entsprechende Beweis für das kgV läuft analog. \square

Wir beenden den Abschnitt mit einem Satz, der die faktoriellen Ringe in die bisher definierten Ringtypen einordnet.

Satz 10.10 Jeder Hauptidealring R ist faktoriell.

Beweis: Wir wissen bereits, dass jedes irreduzible Element in einem Hauptidealring R auch ein Primelement ist, nach Proposition 9.11. Daher genügt es zu zeigen, dass für jede Nichteinheit $a \in R$, $a \neq 0_R$ eine Zerlegung in irreduzible Elemente existiert. Nehmen wir nun an, dass $a \in R$ wäre eine Nichteinheit ungleich Null, die keine solche Zerlegung besitzt. Wir zeigen, dass dann eine Folge $(a_n)_{n \in \mathbb{N}}$ von Ringelementen existiert, so dass gilt

- (i) $a_n \neq 0_R$ und $a_n \notin R^\times$
- (ii) Das Element a_n ist nicht als Produkt irreduzibler Elemente darstellbar.
- (iii) $a_{n+1}|a_n$ und $a_n \nmid a_{n+1}$

Nach Voraussetzung besitzt das Element $a_1 = a$ die Eigenschaften (i) und (ii). Zu zeigen ist nun, dass für ein vorgegebenes a_n mit den Eigenschaften (i) und (ii) ein Element a_{n+1} existiert, so dass (iii) gilt und die Bedingungen (i), (ii) auch für a_{n+1} erfüllt sind. Das Element a_n ist nicht irreduzibel, weil die Irreduzibilität der Bedingung (ii) widersprechen würde. Sei $a_n = rs$ eine Darstellung von a_n als Produkt von Nicht-Einheiten. Dann ist eines der Elemente r, s

nicht als Produkt von irreduziblen Elementen darstellbar, denn ansonsten würde sich erneut ein Widerspruch zu (ii) ergeben. Wir können annehmen, dass das Element $a_{n+1} = r$ keine solche Darstellung besitzt. Wäre $a_{n+1} = 0_R$, dann würde $a_n = 0_R$ folgen, im Widerspruch zu (i). So aber sind die Bedingungen (i) und (ii) für a_{n+1} erfüllt. Offenbar gilt auch $a_{n+1} | a_n$. Würde $a_n | a_{n+1}$ gelten, dann gäbe es ein $\varepsilon \in R$ mit $a_{n+1} = \varepsilon a_n$, und aus $a_{n+1} = \varepsilon a_n = \varepsilon r s = \varepsilon a_{n+1} s$ würde mit der Kürzungsregel $\varepsilon s = 1_R$ folgen, im Widerspruch dazu, dass s keine Einheit ist. So aber ist die Bedingung (iii) für a_n und a_{n+1} erfüllt.

Sei nun $(a_n)_{n \in \mathbb{N}}$ eine Folge mit den Eigenschaften (i), (ii) und (iii). Aus der Bedingung (iii) folgt für die Hauptideale (a_n) nach Satz 9.1 (i) die Beziehung

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq (a_4) \subsetneq \dots$$

Wir zeigen, dass auch die Vereinigung $I = \bigcup_{n=1}^{\infty} (a_n)$ ein Ideal im Ring R ist. Wegen $0_R \in (a_1)$ liegt 0_R auch in I . Seien nun $a, b \in I$ und $r \in R$ vorgegeben. Dann gibt es $m, n \in \mathbb{N}$ mit $a \in (a_m)$ und $b \in (a_n)$. Setzen wir o.B.d.A. die Ungleichung $m \leq n$ voraus, dann liegen a und b wegen $(a_m) \subseteq (a_n)$ also beide in (a_n) . Weil (a_n) ein Ideal ist, folgt $a + b \in (a_n)$ und $ra \in (a_n)$, damit auch $a + b \in I$ und $ra \in I$.

Da R nun ein Hauptidealring ist, gibt es ein $b \in R$ mit $I = (b)$. Insbesondere gilt dann $(a_n) \subseteq (b)$ für alle $n \in \mathbb{N}$. Nach Definition von I gibt es andererseits ein $m \in \mathbb{N}$ mit $b \in (a_m)$, also $b \in (a_n)$ für alle $n \geq m$. Es folgt $(b) \subseteq (a_n)$ und damit $(a_n) = (b)$ für alle $n \geq m$. Aber dies widerspricht der vorherigen Feststellung $(a_m) \subsetneq (a_{m+1})$. Die Annahme, dass es ein Element gibt, das sich nicht in irreduzible Elemente zerlegen lässt, hat also zu einem Widerspruch geführt.

□

Die Umkehrung dieses Satzes ist falsch: Es gibt faktorielle Ringe, die keine Hauptidealringe sind. Im nächsten Kapitel werden wir sehen, dass für jeden faktoriellen Ring R auch der Polynomring $R[x]$ faktoriell ist. Daraus folgt unter anderem, dass $\mathbb{Z}[x]$ ein faktorieller Ring ist. Aber R ist kein Hauptidealring, denn das Ideal $I = (2, x)$ ist kein Hauptideal.

Zum Beweis nehmen wir an, es gibt ein $f \in \mathbb{Z}[x]$ mit $(f) = I$, $f = a_n x^n + \dots + a_1 x + a_0$ mit $a_0, \dots, a_n \in \mathbb{Z}$. Wegen $f \in (2, x)$ gibt es Polynome $g, h \in \mathbb{Z}[x]$ mit $f = 2g + xh$. Dies zeigt, dass der konstante Term a_0 eine gerade ganze Zahl sein muss. Aber aus $(f) = (2, x)$ folgt auch $2 \in (f)$, also $2 = uf$ für ein weiteres Polynom $u \in \mathbb{Z}[x]$. Dies ist nur möglich, wenn f eine Konstante ist. Wegen $x \in (f)$, also $x = vf$ für ein $v \in \mathbb{Z}[x]$ muss diese Konstante gleich 1 sein. Aber dies steht im Widerspruch dazu, dass a_0 gerade ist.

§ 11. Irreduzibilitätskriterien und Gauß'sches Lemma

Zusammenfassung. Wie wir bereits in der Körpertheorie festgestellt haben, ist es für verschiedene Anwendungen notwendig, die Irreduzibilität eines Polynoms $f \in K[x]$ über einem Körper K nachzuweisen. In diesem Abschnitt werden wir mehrere solche Kriterien zur Verfügung stellen, wobei wir für die Herleitung auf die Theorie insbesondere der letzten beiden Kapitel zurückgreifen werden. Von besonderem Interesse ist für uns die Situation, in der K Quotientenkörper eines faktoriellen Rings R ist, wie sie z.B. für $K = \mathbb{Q}$ und $R = \mathbb{Z}$ vorliegt. Hier werden wir unter anderem zeigen, dass für die Irreduzibilität eines Polynoms $f \in R[x]$ über dem Körper K bereits die Irreduzibilität in $R[x]$ hinreichend ist.

Wichtige Grundbegriffe

- primitives Polynom über einem faktoriellen Ring

Zentrale Sätze

- Kriterium für die Nullstellen eines Polynoms $R[x]$ im Quotientenkörper K von R
- Gauß'schen Lemmas, Zusammenhang zwischen Irreduzibilität über R und K
- Polynomringe über faktoriellen Ringen sind faktoriell.
- Eisenstein-Kriterium und Reduktionskriterium

Wir beginnen mit einem einfachen Kriterium für die Existenz von Nullstellen eines Polynoms $f \in R[x]$ über einem faktoriellen Ring R über seinem Quotientenkörper K . Wie wir wissen, ist im Fall $\text{grad}(f) \in \{2, 3\}$ die Nicht-Existenz von Nullstellen für die Irreduzibilität von f in $K[x]$ bereits hinreichend. Bei höheren Polynomgraden kann man häufig auf andere Irreduzibilitätskriterien zurückgreifen, von denen wir einige im weiteren Verlauf des Kapitels vorstellen werden.

Satz 11.1 Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in R[x]$ ein Polynom vom Grad $n \geq 1$. Sei $f = a_n x^n + \dots + a_1 x + a_0$ mit $a_0, \dots, a_n \in R$.

- (i) Ist $\alpha \in K$ eine Nullstelle von f , $\alpha = \frac{p}{q}$ mit $p, q \in R$ und $q \neq 0$, wobei p und q teilerfremd sind, dann gilt $q \mid a_n$ und $p \mid a_0$.
- (ii) Ist insbesondere f normiert, also $a_n = 1$, dann liegt α in R und ist ein Teiler von a_0 .

Beweis: Offenbar ist die Aussage (ii) eine direkte Folgerung von (i). Zum Beweis von (i) sei $\alpha = \frac{p}{q}$ wie angegeben. Es gilt

$$\begin{aligned} f(\alpha) = 0 &\Leftrightarrow a_n \alpha^n + \sum_{k=0}^{n-1} a_k \alpha^k = 0 \Leftrightarrow a_n \alpha^n = -\sum_{k=0}^{n-1} a_k \alpha^k \Leftrightarrow a_n \left(\frac{p}{q}\right)^n = -\sum_{k=0}^{n-1} a_k \left(\frac{p}{q}\right)^k \\ &\Leftrightarrow a_n p^n = -\sum_{k=0}^{n-1} a_k p^k q^{n-k} = q \left(-\sum_{k=0}^{n-1} a_k p^k q^{n-1-k} \right). \end{aligned}$$

Dies zeigt, dass $a_n p^n$ durch q teilbar ist. Weil mit p und q auch p^n und q teilerfremd sind, muss $q \mid a_n$ gelten. Nun gilt ebenso

$$\begin{aligned} f(\alpha) = 0 &\Leftrightarrow \sum_{k=1}^n a_k \alpha^k + a_0 = 0 \Leftrightarrow a_0 = -\sum_{k=1}^n a_k \alpha^k \Leftrightarrow a_0 = -\sum_{k=1}^n a_k \left(\frac{p}{q}\right)^k \\ &\Leftrightarrow a_0 q^n = -\sum_{k=1}^n a_k p^k q^{n-k} = p \left(-\sum_{k=1}^n a_k p^{k-1} q^{n-k} \right). \end{aligned}$$

Dies zeigt, dass $a_0 q^n$ von p geteilt wird. Weil p und q^n teilerfremd sind, folgt daraus $p \mid a_0$. □

Mit Hilfe dieses Kriteriums kann beispielsweise leicht gezeigt werden, dass Polynom $f = x^3 - x + 2$ in $\mathbb{Q}[x]$ irreduzibel ist. Wäre es reduzibel, dann hätte es wegen $\text{grad}(f) = 3$ eine rationale Nullstelle. Weil aber \mathbb{Z} faktoriell und \mathbb{Q} der Quotientenkörper von \mathbb{Z} ist, und weil f in $\mathbb{Z}[x]$ liegt und normiert ist, muss jede rationale Nullstelle von f ein ganzzahliger Teiler von 2 sein. Die einzigen möglichen Nullstellen von f in \mathbb{Q} sind damit $\pm 1, \pm 2$. Es gilt aber $f(1) = f(-1) = 2$, $f(2) = 4$ und $f(-2) = -4$. Somit besitzt f in \mathbb{Q} keine Nullstelle.

Unser nächstes Ziel ist die Formulierung und der Beweis des Gaußschen Lemmas, das einen Zusammenhang zwischen der Irreduzibilität über einem faktoriellen Ring R und über dessen Quotientenkörper K herstellt. In den Anwendungen ist man meistens am Spezialfall $R = \mathbb{Z}$ und $K = \mathbb{Q}$ interessiert.

Lemma 11.2 Sei R ein faktorieller Ring und K sein Quotientenkörper. Sind $a_1, \dots, a_n \in K^\times$ beliebig vorgegeben, dann gibt ein $\alpha \in K^\times$, so dass die Elemente $a'_i = \alpha a_i$ in R liegen und $\text{ggT}(a'_1, \dots, a'_n) = 1$ gilt.

Beweis: Nach Definition des Quotientenkörpers gibt es Elemente $r_i, s_i \in K$ mit $s_i \neq 0$, so dass $a_i = r_i/s_i$ für $1 \leq i \leq n$ gilt. Setzen wir $\alpha = s_1 \dots s_n$, dann liegt α in K^\times , und es gilt

$$\alpha a_i = r_i \left(\prod_{k=1}^{i-1} s_k \right) \left(\prod_{k=i+1}^n s_k \right) \in R.$$

Wir können also o.B.d.A. voraussetzen, dass $a_i \in R$ für $1 \leq i \leq n$ gilt. Sei nun $d = \text{ggT}(a_1, \dots, a_n)$, $\alpha = d^{-1}$ und $a'_i = \alpha a_i$ für $1 \leq i \leq n$. Angenommen, die Elemente a'_1, \dots, a'_n sind nicht teilerfremd. Dann gibt es ein Primelement p mit $p \mid a'_i$ für $1 \leq i \leq n$. Es folgt $pd \mid a_i$ für $1 \leq i \leq n$ und somit $pd \mid d$ nach Definition des ggT. Dies bedeutet, dass ein $a \in R$ mit $pda = d$ existiert, und die Kürzungsregel liefert $pa = 1$. Aber dies ist unmöglich, denn ein Primelement kann nicht zugleich Einheit sein. Also ist $\text{ggT}(a'_1, \dots, a'_n) = 1$ erfüllt. □

Definition 11.3 Sei R ein faktorieller Ring und $f = \sum_{k=0}^n a_k x^k \in R[x]$. Wir nennen das Polynom f **primitiv**, wenn $f \neq 0$ ist und die Koeffizienten a_0, \dots, a_n keinen gemeinsamen Primteiler besitzen.

Wir betrachten einige Beispiele.

- (i) Normierte Polynome in $R[x]$, also Polynome der Form $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ mit höchstem Koeffizienten 1 und ansonsten beliebigen Koeffizienten $a_0, \dots, a_{n-1} \in R$, sind immer primitiv.
- (ii) Das Polynom $2x^2 + 4x + 6$ ist nicht primitiv, denn es gilt $\text{ggT}(2, 4, 6) = 2$.
- (iii) Ist R ein Integritätsbereich und $f \in R[x]$ ein irreduzibles Element vom Grad ≥ 1 , dann ist f primitiv. Ansonsten hätten die Koeffizienten von f einen gemeinsamen Primteiler $p \in R$, und es würde ein Polynom $\tilde{f} \in R[x]$ mit $f = p\tilde{f}$ existieren. Dies aber bedeutet, dass f als Produkt von Nichteinheiten dargestellt werden kann und somit reduzibel ist.

Folgerung 11.4 Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in K[x]$ ein Polynom mit $f \neq 0$. Dann gibt es ein $\alpha \in K^\times$, so dass αf in $R[x]$ liegt und primitiv ist.

Beweis: Das folgt unmittelbar aus Lemma 11.2, angewendet auf die Koeffizienten des Polynoms f . □

Sei nun R ein Integritätsbereich, $\mathfrak{p} \subseteq R$ ein Primideal und $\bar{R} = R/\mathfrak{p}$ der zugehörige Restklassenring, mit dem kanonischen Epimorphismus $\pi : R \rightarrow \bar{R}$. Wir bezeichnen mit $\mathfrak{p}[x] = \mathfrak{p}R[x]$ die Menge aller Polynome, deren Koeffizienten im Primideal \mathfrak{p} enthalten sind. Es handelt sich um das von der Teilmenge \mathfrak{p} in $R[x]$ erzeugte Ideal.

Lemma 11.5 Der Homomorphismus $\phi : R[x] \rightarrow \bar{R}[x]$ gegeben durch $\sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \pi(a_i) x^i$ induziert einen Isomorphismus $R[x]/\mathfrak{p}[x] \cong \bar{R}[x]$ von Ringen.

Beweis: Weil der kanonische Epimorphismus $\pi : R \rightarrow \bar{R}$ surjektiv ist, gilt dasselbe für ϕ . Außerdem ist $\mathfrak{p}[x]$ der Kern von ϕ . Also folgt die Aussage aus dem Homomorphiesatz. □

Folgerung 11.6 Das Ideal $\mathfrak{p}[x]$ ist ein Primideal in $R[x]$.

Beweis: Weil \mathfrak{p} in R ein Primideal ist, handelt es sich beim Faktorring \bar{R} nach Satz 6.12 um einen Integritätsbereich. Damit ist auch der Polynomring $\bar{R}[x]$ ein Integritätsbereich, auf Grund der Isomorphie also auch $R[x]/\mathfrak{p}[x]$. Wiederum nach Satz 6.12 folgt daraus, dass $\mathfrak{p}[x]$ ein Primideal ist. □

Satz 11.7 (Lemma von Gauß)

Sei R ein faktorieller Ring, und seien $f, g \in R[x]$ primitive Polynome. Dann ist auch fg primitiv.

Beweis: Angenommen, das Produkt fg ist nicht primitiv und das Primelement $p \in R$ ein gemeinsamer Teiler der Koeffizienten. Nach Proposition 9.10 ist (p) in R ein Primideal, und nach Folgerung 11.6 erzeugt p auch ein Primideal in $R[x]$, das wir ebenfalls mit (p) bezeichnen. Nun sind fg nach Voraussetzung in (p) enthalten, es folgt $f \in (p)$ oder $g \in (p)$. Setzen wir o.B.d.A. den ersten Fall voraus, dann ist p ein gemeinsamer Teiler der Koeffizienten von f , im Widerspruch dazu, dass f primitiv ist. □

Satz 11.8 Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in R[x]$ ein Polynom mit $\text{grad}(f) \geq 1$.

- (i) Ist $g \in R[x]$ ein primitives Polynom mit der Eigenschaft, dass g ein Teiler von f in $K[x]$ ist, so ist g bereits ein Teiler von f in $R[x]$.
- (ii) Ist f irreduzibel in $R[x]$, dann auch in $K[x]$.

Beweis: zu (i) Nach Voraussetzung gibt es ein $h \in K[x]$ mit $f = gh$, und Folgerung 11.4 liefert uns ein Element $\alpha \in K^\times$, so dass $\tilde{h} = \alpha h$ in $R[x]$ liegt und primitiv ist. Nach dem Lemma von Gauß ist $g\tilde{h}$ primitiv, und es gilt $f = g(\alpha^{-1}\tilde{h})$.

Sei $\alpha = a/b$ eine Darstellung von α als gekürzter Bruch, also mit $a, b \in R$, $b \neq 0$ und $\text{ggT}(a, b) = 1$. Dann erhalten wir aus $f = g(\alpha^{-1}\tilde{h})$ Gleichung $af = b\tilde{h}$. Angenommen, p ist ein Primteiler von a . Dann wäre p auch ein gemeinsamer Primteiler der Koeffizienten von $g\tilde{h}$. Aber das ist unmöglich, weil $g\tilde{h}$ primitiv ist. Es folgt $\alpha^{-1} = b/a \in R$, und die Gleichung $f = g(\alpha^{-1}\tilde{h})$ zeigt, dass g auch in $R[x]$ ein Teiler von f ist.

zu (ii) Sei $f = gh$ mit $g, h \in K[x]$. Ferner sei $\alpha \in K^\times$ ein Element mit der Eigenschaft, dass $\tilde{g} = \alpha g$ in $R[x]$ liegt und primitiv ist. Wegen $f = \tilde{g}(a^{-1}h)$ ist auch \tilde{g} ein Teiler von f in $K[x]$. Weil aber \tilde{g} außerdem primitiv ist, ist \tilde{g} nach Teil (i) sogar ein Teiler von f in $R[x]$. Es gibt also ein $\tilde{h} \in R[x]$ mit $f = \tilde{g}\tilde{h}$. Wegen $\tilde{g}\tilde{h} = f = \tilde{g}(a^{-1}h)$ gilt $\tilde{h} = a^{-1}h$. Weil f nach Voraussetzung in $R[x]$ irreduzibel ist, ist \tilde{g} oder \tilde{h} eine Einheit in $R[x]$, also ein Element aus R^\times . Wegen $\tilde{g} = \alpha g$ und $\tilde{h} = a^{-1}h$ folgt daraus $g \in K^\times$ oder $h \in K^\times$. Also ist g oder h eine Einheit in K^\times , und folglich ist f auch in $K[x]$ irreduzibel. \square

Um also beispielsweise zu zeigen, dass ein normiertes Polynom $f \in \mathbb{Z}[x]$ im Polynomring $\mathbb{Q}[x]$ irreduzibel ist, genügt es, die Irreduzibilität in $\mathbb{Z}[x]$ nachzuweisen. In vielen Fällen ist dies bedeutend einfacher.

Satz 11.9 Ist R ein faktorieller Ring, dann ist auch $R[x]$ faktoriell.

Beweis: Sei $f \in R[x]$ ungleich 0_R und keine Einheit in $R[x]$. Wir zeigen zunächst, dass f in $R[x]$ eine Zerlegung in irreduzible Elemente besitzt. Sei c ein ggT der Koeffizienten von f im Ring R . Dann können wir f in der Form $f = cg$ schreiben, mit einem primitiven Polynom g . Weil R faktoriell ist, kann c in R als Produkt irreduzibler Elemente dargestellt werden.

Wir zeigen nun durch vollständige Induktion über $m = \text{grad}(g)$, dass auch g ein Produkt irreduzibler Elemente ist. Im Fall $m = 0$ ist g in $R[x]$ eine Einheit und nichts zu zeigen. Setzen wir nun $m \geq 1$ voraus. Besitzt g keine Zerlegung in Nicht-Einheiten, so ist g nach Definition irreduzibel. Nehmen wir nun an, es gilt $g = h_1h_2$, wobei h_1 und h_2 in $R[x]$ keine Einheiten sind. Wäre $\text{grad}(h_1) = 0$ oder $\text{grad}(h_2) = 0$, dann wäre h_1 oder h_2 eine Nicht-Einheit in R und würde somit von einem Primelement p des Rings R geteilt. Somit wäre dann p ein Teiler von g , im Widerspruch dazu, dass g primitiv ist. So aber gilt $0 < \text{grad}(g_1), \text{grad}(g_2) < m$. Wir können auf g_1 und g_2 die Induktionsvoraussetzung anwenden und erhalten Darstellungen beider Polynome als Produkte irreduzibler Elemente von $R[x]$. Daraus ergibt sich eine ebensolche Darstellung für g , womit der Induktionsschritt abgeschlossen ist.

Nun müssen wir noch zeigen, dass die Darstellung von unserem Polynom f im Wesentlichen eindeutig ist. Wieder stellen wir f als Produkt cg mit einem Element $c \in R$ und einem primitiven Polynom $g \in R[x]$ dar. In jeder Darstellung von f als Produkt irreduzibler Elemente bilden die Faktoren vom Grad 0 (bis auf Einheiten) eine Zerlegung von c , und die übrigen Faktoren eine Zerlegung von g . Da die Eindeutigkeit der Faktorzerlegung in R bereits bekannt ist, können wir uns auf den Fall $f = g$ beschränken. Nehmen wir nun an, dass durch

$$g_1 \cdot \dots \cdot g_r = f = h_1 \cdot \dots \cdot h_s$$

zwei Zerlegungen des primitiven Polynoms $f \in R[x]$ in irreduzible Elemente g_i, h_j des Rings $R[x]$ gegeben sind, alle von positivem Grad. Nach Satz 11.8 (ii) sind die Elemente g_i, h_j auch alle irreduzibel in $K[x]$, wobei K den Quotientenkörper von R bezeichnet. Auf Grund der Eindeutigkeit der Primfaktorzerlegung in $K[x]$ muss $r = s$ gelten, und nach eventueller Umnummerierung ist g_i in $K[x]$ assoziiert zu h_i , für $1 \leq i \leq r$. Wegen Satz 11.8 (i) g_i auch in $R[x]$ jeweils assoziiert zu h_i . Damit ist die Eindeutigkeit der Zerlegung nachgewiesen. \square

Wir formulieren noch zwei Kriterien für die Irreduzibilität von Polynomen über Ringen.

Satz 11.10 (Eisenstein-Kriterium)

Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $f \in R[x]$ ein primitives Polynom vom Grad $n > 0$. Es sei $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ mit $a_0, \dots, a_n \in R$, und wir setzen voraus, dass die Koeffizienten von f folgende Bedingungen erfüllen.

- (i) $p|a_i$ für $0 \leq i < n$ (ii) $p \nmid a_n$ (iii) $p^2 \nmid a_0$

Dann ist f in $R[x]$ irreduzibel.

Beweis: Angenommen, es gibt Polynome $g, h \in R[x]$ mit $f = gh$. Wir schreiben

$$g = \sum_{i=0}^r b_i x^i \quad \text{und} \quad h = \sum_{k=0}^s c_k x^k \quad \text{mit} \quad b_i, c_k \in R, \quad b_r, c_s \neq 0.$$

Dann gilt $a_0 = b_0 c_0$, und wegen Bedingung (iii) gilt $p|a_0, p^2 \nmid a_0$. Nach eventueller Vertauschung von g und h können wir annehmen, dass $p|b_0$ und $p \nmid c_0$ gilt. Wäre p ein Teiler sämtlicher Koeffizienten von g , dann wäre p auch ein Teiler von $a_n = b_r c_s$, im Widerspruch zur Bedingung (ii). Es gibt also ein minimales $u \in \{1, \dots, r\}$ mit $p \nmid b_u$. Nun gilt

$$a_u = \sum_{i=0}^u b_{u-i} c_i,$$

und p ist ein Teiler von $b_{u-i} c_i$ für $1 \leq i \leq u$, aber kein Teiler von $b_u c_0$. Folglich ist p auch kein Teiler von a_u , und wegen Bedingung (i) muss $u = n$ gelten. Damit ist $\text{grad}(g) = n = \text{grad}(f)$ und $\text{grad}(h) = 0$. Weil f primitiv ist, muss h in R^\times liegen. Damit ist die Irreduzibilität von f in $R[x]$ bewiesen. \square

Beispielsweise sind die Polynome $x^2 - 5$ und $x^3 + 2x + 6$ beide primitiv, weil sie normiert sind. Beim ersten Polynom kann das Eisenstein-Kriterium auf die Primzahl $p = 5$, beim zweiten auf $p = 2$ angewendet werden. Also sind beide Polynome in $\mathbb{Z}[x]$ und nach Satz 11.8 auch in $\mathbb{Q}[x]$ irreduzibel.

Satz 11.11 (Reduktionskriterium)

Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $\bar{R} = R/(p)$. Es sei $f = \sum_{i=0}^n a_i x^i \in R[x]$ ein primitives Polynom mit $a_n \notin (p)$ und \bar{f} das Bild von f in $\bar{R}[x]$. Ist \bar{f} in $\bar{R}[x]$ irreduzibel, dann auch das Polynom f in $R[x]$.

Beweis: Nehmen wir an, es gibt eine Zerlegung $f = gh$ von f mit $g, h \in R[x]$, wobei wir annehmen, dass weder g noch h eine Einheit in $R[x]$ ist. Weil f primitiv ist, sind dann g und h auch keine konstanten Polynome. Es gilt dann $\bar{f} = \bar{g}\bar{h}$ in $\bar{R}[x]$, wobei \bar{g}, \bar{h} die Bilder von g, h in $\bar{R}[x]$ bezeichnen. Wegen $a_n \notin (p)$ gilt $\text{grad}(f) = \text{grad}(\bar{f})$, und damit muss auch $\text{grad}(g) = \text{grad}(\bar{g})$ und $\text{grad}(h) = \text{grad}(\bar{h})$ gelten.

Insbesondere sind \bar{g} und \bar{h} nicht konstant. Nun ist (p) wegen Proposition 9.10 ein Primideal in R und $\bar{R} = R/(p)$ damit nach Satz 6.12 (i) ein Integritätsbereich. Daraus folgt, dass die Einheiten im Polynomring $\bar{R}[x]$ genau die Einheiten in \bar{R} sind, siehe Folgerung 3.14. Somit sind \bar{g} und \bar{h} keine Einheiten in $\bar{R}[x]$. Aber dann zeigt die Gleichung $\bar{f} = \bar{g}\bar{h}$, dass \bar{f} in $\bar{R}[x]$ nicht irreduzibel ist. \square

Als Anwendung des Reduktionskriteriums zeigen wir, dass $f = x^3 + x + 1$ in $\mathbb{Q}[x]$ irreduzibel ist. Offenbar ist f in $\mathbb{Z}[x]$ ein primitives Polynom. Setzen wir $\mathfrak{p} = (2)$, dann ist $R/\mathfrak{p} \cong \mathbb{F}_2$. Der Leitkoeffizient von f ist gleich 1 und liegt somit nicht in \mathfrak{p} . Das Bildpolynom

$$\bar{f} = x^3 + x + \bar{1} \in \mathbb{F}_2[x]$$

hat in \mathbb{F}_2 keine Nullstelle (es gilt $\bar{f}(\bar{0}) = \bar{f}(\bar{1}) = \bar{1}$), wegen $\text{grad}(\bar{f}) = 3$ ist es also irreduzibel. Auf Grund des Reduktionskriteriums ist f also in $\mathbb{Z}[x]$ irreduzibel, und mit Satz 11.8 erhalten wir die Irreduzibilität in $\mathbb{Q}[x]$.

§ 12. Kreisteilungspolynome

Zusammenfassung. Die Kreisteilungskörper spielen in der Algebra eine wichtige Rolle, da einerseits viele ihrer strukturellen Merkmale, zum Beispiel ihre Galoisgruppen, leicht zu beschreiben sind, sie andererseits aber auch die Grundlage für viele fortgeschrittene Aufgabenstellungen bilden. Unter anderem werden sie benötigt, um die Auflösbarkeit algebraischer Gleichungen zu studieren, und auch bei der Frage nach der Konstruierbarkeit regelmäßiger n -Ecke durch Zirkel und Lineal spielen sie eine wichtige Rolle. Sie treten sowohl beim Beweis des Dirichletschen Primzahlsatzes in Erscheinung wie auch beim Satz von Kronecker-Weber, der die Galois-Erweiterungen von \mathbb{Q} mit abelscher Galoisgruppe klassifiziert. In der Algebra-Vorlesung verwenden wir sie als konkretes weiteres Beispiel für den Hauptsatz der Galois-Theorie.

Die Bezeichnung der Kreisteilungskörper ergibt sich aus der Tatsache, dass sie von **Einheitswurzeln** erzeugt werden, die (aufgefasst als Punkte in der komplexen Ebene) den Einheitskreis gleichmäßig unterteilen. Die Minimalpolynome der Einheitswurzeln bezeichnet man als **Kreisteilungspolynome**. Die Nullstellen des n -ten Kreisteilungspolynom sind dabei gerade die **primitiven** n -ten Einheitswurzeln. Wir werden zeigen, dass es sich dabei um ganzzahlige Polynome handelt, und geben eine Rekursionsformel für ihre Berechnung an. Besonders Aufwand erfordert der Beweis, dass die Polynome, die durch die Formel definiert werden, tatsächlich über \mathbb{Q} irreduzibel sind. Hier kommen unter anderem die Ergebnisse aus § 11 zur Anwendung.

Wichtige Grundbegriffe

- n -te Einheitswurzel, primitive n -Einheitswurzel
- Gruppe μ_n der Einheitswurzeln
- n -tes Kreisteilungspolynom

Zentrale Sätze

- Rekursionsformel zur Berechnung der Kreisteilungspolynome
- Irreduzibilität der Kreisteilungspolynome über \mathbb{Q}

Definition 12.1 Sei $n \in \mathbb{N}$. Eine n -te **Einheitswurzel** in \mathbb{C} ist ein Element $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$.

Wie man leicht nachrechnet, bilden die n -ten Einheitswurzeln eine Untergruppe von \mathbb{C}^\times , die wir mit μ_n bezeichnen. Es gilt

$$\mu_n = \{e^{2\pi ik/n} \mid 0 \leq k < n\},$$

denn nach Definition sind die n -ten Einheitswurzeln genau die Nullstellen von $x^n - 1 \in \mathbb{Z}[x]$ in \mathbb{C} , und da $x^n - 1$ ein Polynom vom Grad n ist, kann es höchstens n verschiedene Nullstellen in \mathbb{C} geben. Andererseits sind durch die Elemente auf der rechten Seite der Gleichung wegen

$$(e^{2\pi ik/n})^n = e^{2\pi ik} = 1$$

offenbar n verschiedene Nullstellen des Polynoms gegeben. Das Element $\zeta_n = e^{2\pi i/n}$ ist ein Erzeuger der Gruppe μ_n , es gilt also $\mu_n = \langle \zeta_n \rangle$.

Lemma 12.2 Sei $k \in \mathbb{Z}$. Genau dann gilt $\mu_n = \langle \zeta_n^k \rangle$, wenn $\text{ggT}(k, n) = 1$ ist.

Beweis: In der Gruppentheorie wurde gezeigt: Ist G eine zyklische Gruppe der Ordnung n und g ein Erzeuger von G , dann ist $G = \langle g^k \rangle$ äquivalent zu $\text{ggT}(k, n) = 1$. Das Lemma ist ein Spezialfall dieser Aussage. \square

Definition 12.3 Sei $n \in \mathbb{N}$, $n \geq 2$. Eine **primitive** n -te Einheitswurzel ist ein Element $\zeta \in \mu_n$ mit $\mu_n = \langle \zeta \rangle$. Wir bezeichnen mit $\mu_n^\times \subseteq \mu_n$ die Menge der primitiven n -ten Einheitswurzeln. Das Polynom $\Phi_n \in \mathbb{C}[x]$ gegeben durch

$$\Phi_n = \prod_{\zeta \in \mu_n^\times} (x - \zeta)$$

wird das n -te **Kreisteilungspolynom** genannt.

Aus technischen Gründen setzen wir $\Phi_1 = x - 1$, obwohl wir für $n = 1$ keine primitiven n -ten Einheitswurzeln definiert haben.

Nach Lemma 12.2 gilt für alle $n \geq 2$ jeweils

$$|\mu_n^\times| = |\{k \in \mathbb{Z} \mid 0 \leq k < n, \text{ggT}(k, n) = 1\}| = \varphi(n) \quad ,$$

also ist $\varphi(n)$ auch der Grad des Polynoms Φ_n . Unser nächstes Ziel besteht in dem Nachweis, dass jedes Kreisteilungspolynom nicht nur über \mathbb{C} , sondern über den ganzen Zahlen definiert ist.

Lemma 12.4 Für alle $n \in \mathbb{N}$ gilt $x^n - 1 = \prod_{d|n} \Phi_d$, wobei d die natürlichen Teiler von n durchläuft.

Beweis: Nach Definition sind die Nullstellen von $x^n - 1$ genau die Elemente $\zeta \in \mathbb{C}^\times$ mit $\zeta^n = 1$. Die Ordnung $d = \text{ord}(\zeta)$ von ζ in \mathbb{C}^\times ist dann ein Teiler von n . Also erzeugt ζ in diesem Fall die Gruppe μ_d , ist also eine primitive d -te Einheitswurzel und somit eine Nullstelle von Φ_d . Sei umgekehrt ζ eine Nullstelle von Φ_d für einen Teiler d von n . Ist $k \in \mathbb{N}$ mit $n = kd$, dann gilt $\zeta^n = (\zeta^d)^k = 1^k = 1$, also ist ζ eine Nullstelle von $x^n - 1$.

Somit haben wir gezeigt, dass die Nullstellenmengen der beiden Polynome auf der linken und rechten Seite der Gleichung übereinstimmen. Beide Polynome haben darüber hinaus nur einfache Nullstellen, also sind sie gleich. \square

Satz 12.5 Es gilt $\Phi_n \in \mathbb{Z}[x]$ für alle $n \in \mathbb{N}$.

Beweis: Erneut führen wir den Beweis durch vollständige Induktion über n . Für $n = 1$ ist die Aussage wegen $\Phi_1 = x - 1$ klar. Sei nun $n > 1$, und setzen wir $\Phi_d \in \mathbb{Z}[x]$ für alle $d < n$ voraus. Nach Lemma 12.4 gilt

$$x^n - 1 = \prod_{d|n} \Phi_d \quad .$$

Sei nun $S = \{d \in \mathbb{N} \mid d|n, d < n\}$ und $g = \prod_{d \in S} \Phi_d$. Dann gilt also $x^n - 1 = g \cdot \Phi_n$, wobei das Polynom g nach Induktionsvoraussetzung in $\mathbb{Z}[x]$ liegt; darüber hinaus ist es normiert. Wir zeigen nun zunächst, dass Φ_n in $\mathbb{Q}[x]$ enthalten ist. Weil $\mathbb{Q}[x]$ ein euklidischer Ring ist, gibt es Polynome $q, r \in \mathbb{Q}[x]$ mit $g \cdot \Phi_n = x^n - 1 = qg + r$ und $r = 0$ der $\text{grad}(r) < \text{grad}(g)$. Durch Umformen erhalten wir $(\Phi_n - q)g = r$, und auf Grund des Grades von g bleibt $r = 0$ als einzige Möglichkeit. Es gilt also $g \cdot \Phi_n = gq$ und somit $\Phi_n = q \in \mathbb{Q}[x]$, da \mathbb{Q} ein Integritätsbereich ist, in dem die Kürzungsregel angewendet werden kann.

Also ist g ein normierter Teiler von $x^n - 1$ im Ring $\mathbb{Q}[x]$, wobei g und $x^n - 1$ beide in $\mathbb{Z}[x]$ liegen. Nach 11.8 folgt daraus, dass g auch ein Teiler von $x^n - 1$ im Ring $\mathbb{Z}[x]$ ist. Es gibt also ein eindeutig bestimmtes, normiertes Polynom $h \in \mathbb{Z}[x]$ mit $x^n - 1 = gh$. Aus $gh = x^n - 1 = g \cdot \Phi_n$ folgt $\Phi_n = h \in \mathbb{Z}[x]$. \square

Die Produktformel $x^n - 1 = \prod_{d|n} \Phi_d$ kann verwendet werden, um die Kreisteilungspolynome für die einzelnen natürlichen Zahlen n rekursiv zu berechnen. Ist p zum Beispiel eine Primzahl, dann gilt

$$x^p - 1 = \Phi_1 \Phi_p = (x - 1) \Phi_p$$

und somit

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1.$$

Ist $q \in \mathbb{N}$ eine Primzahlpotenz, $q = p^r$ mit einer Primzahl p und $r \in \mathbb{N}$, $r \geq 2$, dann gilt

$$x^{p^r} - 1 = \prod_{d|p^r} \Phi_d = \left(\prod_{d|p^{r-1}} \Phi_d \right) \Phi_{p^r} = (x^{p^{r-1}} - 1) \Phi_{p^r}$$

also

$$\begin{aligned} \Phi_{p^r} &= \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = \frac{(x^{p^{r-1}})^p - 1}{x^{p^{r-1}} - 1} = (x^{p^{r-1}})^{p-1} + (x^{p^{r-1}})^{p-2} + \dots + (x^{p^{r-1}})^1 + (x^{p^{r-1}})^0 \\ &= x^{p^{r-1}(p-1)} + x^{p^{r-1}(p-2)} + \dots + x^{p^{r-1}} + 1. \end{aligned}$$

Das sechste Kreisteilungspolynom berechnet man durch

$$\Phi_6 = \frac{x^6 - 1}{\Phi_1 \Phi_2 \Phi_3} = \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)} = x^2 - x + 1,$$

und das zwölfte Kreisteilungspolynom erhält man durch die Rechnung

$$\Phi_{12} = \frac{x^{12} - 1}{\Phi_1 \Phi_2 \Phi_3 \Phi_4 \Phi_6} = \frac{x^{12} - 1}{(x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)} = x^4 - x^2 + 1.$$

Wir zeigen nun, dass die Kreisteilungspolynome über \mathbb{Q} irreduzibel sind. Zur Vorbereitung bemerken wir

Lemma 12.6 Für jedes Polynom $f \in \mathbb{F}_p[x]$ gilt $f^p = f(x^p)$.

Beweis: Wir können $f \neq 0$ voraussetzen. Sei $f = \sum_{k=0}^n a_k x^k$ mit $n \in \mathbb{N}$ und $a_0, \dots, a_n \in \mathbb{F}_p$. Auf Grund der allgemeinen Rechenregel $(a + b)^p = a^p + b^p$ in Ringen der Charakteristik p und der Gleichung $a^p = a$ für alle $a \in \mathbb{F}_p$ (siehe Algebra-Skript, Abschnitt endliche Körper) gilt

$$f^p = \left(\sum_{k=0}^n a_k x^k \right)^p = \sum_{k=0}^n a_k^p x^{kp} = \sum_{k=0}^n a_k x^{kp} = f(x^p). \quad \square$$

Satz 12.7 Für jedes $n \in \mathbb{N}$ ist das Kreisteilungspolynom Φ_n in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ irreduzibel.

Beweis: Wir gehen davon aus, dass $n > 1$ ist, denn für $n = 1$ ist die Aussage offensichtlich. Wäre das Kreisteilungspolynom in $\mathbb{Q}[x]$ reduzibel, dann nach Satz 11.8 (ii) auch in $\mathbb{Z}[x]$. Es gibt dann normierte Polynome $f, g \in \mathbb{Z}[x]$ mit $\Phi_n = fg$ und $\text{grad}(f), \text{grad}(g) > 1$, wobei wir voraussetzen, dass f in $\mathbb{Z}[x]$ (und damit auch in $\mathbb{Q}[x]$) irreduzibel ist. Wir zeigen nun:

Ist p eine Primzahl mit $p \nmid n$ und $\zeta \in \mathbb{C}$ eine Nullstelle von f , dann gilt auch $f(\zeta^p) = 0$.

Angenommen, es gilt $f(\zeta^p) \neq 0$. Wegen $\Phi_n(\zeta) = 0$ und $\Phi_n = fg$ muss dann $g(\zeta^p) = 0$ gelten. Dies bedeutet, dass ζ eine Nullstelle des Polynoms $g(x^p)$ ist. Weil aber f das Minimalpolynom von ζ ist, teilt f das Polynom $g(x^p)$ in $\mathbb{Q}[x]$. Darüber hinaus ist f normiert, insbesondere primitiv, und nach Satz 11.8 (i) ist f damit auch im Ring $\mathbb{Z}[x]$ ein Teiler von $g(x^p)$.

Seien nun \bar{f}, \bar{g} die Bilder von f, g im Polynomring $\mathbb{F}_p[x]$. Dann ist \bar{f} ein Teiler von $\bar{g}(x^p)$, nach Lemma 12.6 also ein Teiler von \bar{g}^p . Sei \bar{f}_1 ein irreduzibler Teiler von \bar{f} . Dann ist \bar{f}_1 wegen $\bar{f} | \bar{g}^p$ auch ein Teiler von \bar{g} . Wegen $\Phi_n = fg$ und $\Phi_n | (x^n - 1)$ ist $\bar{f}\bar{g}$ ein Teiler von $x^n - \bar{1}$, und wegen $\bar{f}_1 | \bar{f}$ und $\bar{f}_1 | \bar{g}$ folgt daraus $\bar{f}_1^2 | (x^n - \bar{1})$. Insbesondere hat $x^n - \bar{1}$ im algebraischen Abschluss $\mathbb{F}_p^{\text{alg}}$ von \mathbb{F}_p mehrfache Nullstellen. Andererseits zeigt die Gleichung

$$\text{ggT}(x^n - \bar{1}, (x^n - \bar{1})') = \text{ggT}(x^n - \bar{1}, nx^{n-1}) = \bar{1},$$

dass dies *nicht* der Fall ist. Auf Grund dieses Widerspruchs ist die Annahme falsch und die Behauptung bewiesen.

Jede Nullstelle von Φ_n , also jede primitive n -te Einheitswurzel, kann in der Form ζ^m dargestellt werden, wobei $m \in \mathbb{N}$ eine zu n teilerfremde Zahl bezeichnet. Ist $m > 1$, dann ist m ein Produkt $p_1 \cdots p_r$ bestehend aus Primzahlen p_k mit $p_k \nmid n$ für $1 \leq k \leq r$. Durch mehrfache Anwendung der soeben bewiesenen Behauptung erkennt man, dass mit ζ auch die Elemente $\zeta^{p_1}, \zeta^{p_1 p_2}, \zeta^{p_1 p_2 p_3}, \dots, \zeta^m$ Nullstellen von f sind. Insgesamt sind also alle $\varphi(m)$ verschiedenen Linearfaktoren von Φ_n Teiler von f . Daraus folgt $\Phi_n | f$ und $f = \Phi_n$, insgesamt also die Irreduzibilität von Φ_n . \square

Literaturverzeichnis

[Bö] J. Böhm, *Grundlagen der Algebra und Zahlentheorie*. Springer-Verlag.

[Ca] O. Cápoli, *A principal ideal domain that is not a Euclidean domain*. American Math. Monthly, vol. 95 no. 9 (Nov. 1988), 868-871.

[Ha] M. Harper, $\mathbb{Z}[\sqrt{14}]$ is Euclidean. Canad. J. Math. Vol. 56 (1), pp. 55-70, 2004.

[KM] C. Karpfinger, K. Meyberg, *Algebra*. Spektrum Akademischer Verlag.

[LL] F. Lorenz, F. Lemmermeyer, *Algebra 1*. Spektrum Akademischer Verlag.

[Me] H. Menzer, *Zahlentheorie*. Oldenbourg-Verlag.

[MP] S. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie*. vieweg-Verlag.

[Wi] R. Wilson, *An example of a PID which is not a Euclidean domain*. Veröffentlicht im WWW unter der URL-Adresse <http://www.maths.qmul.ac.uk/~raw/MTH5100/PIDnotED.pdf>, abgerufen am 22. November 2018.