Ralf Gerkmann

Mathematisches Institut

Ludwig-Maximilians-Universität München

Zahlentheorie

(Version 11. Juli 2019)

Inhaltsverzeichnis

§ 1. *Motivation*

Bevor wir mit dem regulären Stoff beginnen, soll zunächst an zwei Beispielen gezeigt werden, wie die in dieser Vorlesung entwickelte Theorie in konkrete Anwendungen eingeht. Im ersten Beispiel geht es um eine einfach zu formulierende Fragestellung der elementaren Zahlentheorie, wie sie zum Beispiel auch Schülern im Mathematikuntterricht präsentiert werden könnte. Im zweiten Teil betrachten wir ein auf Zahlentheorie basierendes Verfahren der Kryptographie.

(a) Primzahlen als Summe von Quadraten

Die Frage, mit der wir uns hier befassen, lautet: „Welche Primzahlen lassen sich als Summe von zwei Quadraten darstellen ?“ Anders formuliert: Für welche Primzahlen p besitzt die Gleichung $x^2 + y^2 = p$ eine Lösung mit $x, y \in \mathbb{Z}$? Durch Einsetzen findet man für die kleinsten Primzahlen

2	$=$	$1^2 + 1^2$	11		keine Darstellung
3		keine Darstellung	13	$=$	$2^2 + 3^2$
5	$=$	$1^2 + 2^2$	17	$=$	$1^2 + 4^2$
7		keine Darstellung	19		keine Darstellung

Probiert man dies für weitere Primzahlen durch, so merkt man, dass die Darstellbarkeit von p als Summe von zwei Quadraten offenbar von der Restklasse von p modulo 4 abhängt. Man sagt, zwei Zahlen $a, b \in \mathbb{Z}$ sind ***kongruent*** modulo einer natürlichen Zahl n und schreibt $a \equiv b \bmod n$, wenn n ein Teiler von $a - b$ ist. Eine äquivalente Bedingung lautet, dass bei a und b nach Division durch n derselbe Rest übrig bleibt, weshalb man modulo n kongruente Zahlen auch zu einer ***Restklasse*** zusammenfasst. Man stellt nun fest, dass eine Primzahl $p > 2$ offenbar genau dann als Summe von zwei Quadraten geschrieben werden kann, wenn $p \equiv 1 \bmod 4$ gilt. In der Tabelle oben sind dies genau die Primzahlen 5, 13 und 17. Dementsprechend sind die Primzahlen p mit $p \equiv 3 \bmod 4$ nicht als Summe zweier Quadrate darstellbar, darunter fallen die Primzahlen 3, 7, 11 und 19 von oben. Die einzige gerade Primzahl 2 spielt eine Sonderrolle und wird deshalb bei der Betrachtung ausgeklammert.

Unser Ziel besteht nun darin, diese (experimentell gefundene) Vermutung zu beweisen. Dafür sind zwei Teilaussagen zu zeigen: dass die Bedingung $p \equiv 1 \bmod 4$ sowohl *notwendig* als auch *hinreichend* für die Darstellbarkeit einer ungeraden Primzahl p als Summe von Quadraten ist. Befassen wir uns zunächst mit der Notwendigkeit. Diese ist, ebenfalls mit Hilfe der Kongruenzrechnung, sehr einfach einzusehen. Das Quadrat einer beliebigen geraden Zahl ist immer durch 4 teilbar, also $\equiv 0 \bmod 4$, denn jede gerade Zahl ist von der Form $2k$ für ein $k \in \mathbb{Z}$, und es gilt $(2k)^2 = 4k^2 \equiv 0 \bmod 4$. Eine ungerade Zahl hat die Form $2k + 1$ für ein $k \in \mathbb{Z}$, und es gilt

$$(2k + 1)^2 \equiv 4k^2 + 4k + 1 \equiv 1 \bmod 4.$$

Also ist jede Quadratzahl $\equiv 0 \bmod 4$ oder $\equiv 1 \bmod 4$. Ist nun die ungerade Primzahl p als Summe von zwei Quadraten darstellbar, also $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$, dann kann die Quadratsumme nur kongruent zu 0, 1 oder 2 modulo 4 sein. Weil p ungerade ist, scheiden die Restklassen 0 und 2 als Möglichkeit aus, und es bleibt nur $p \equiv 1 \bmod 4$ übrig.

Es gibt noch eine andere Möglichkeit, die Notwendigkeit der Bedingung $p \equiv 1 \bmod 4$ einzusehen. Diese erfordert zwar etwas mehr theoretischen Hintergrund, liefert uns aber dafür auch einen brauchbaren Ansatz zum Beweis der Rückrichtung. Wie wir später sehen werden, gibt es zu jeder natürlichen Zahl n einen ***endlichen Ring*** bestehend aus n Elementen $\bar{0}$, $\bar{1}$, $\bar{2}$, ..., $\overline{n-1}$, der mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet wird. Ferner gibt es eine surjektive Abbildung $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \bar{a}$ mit

$$\overline{a+b} = \bar{a} + \bar{b} \qquad \text{und} \qquad \overline{ab} = \bar{a} \cdot \bar{b}.$$

Für zwei Zahlen $a, b \in \mathbb{Z}$ gilt $\bar{a} = \bar{b}$ genau dann, wenn $a \equiv b \bmod n$ erfüllt ist. Ist p eine Primzahl, dann ist $\mathbb{Z}/p\mathbb{Z}$ sogar ein ***Körper***, d.h. jedes Element ungleich $\bar{0}$ besitzt bezüglich der Multiplikation ein Inverses. Man bezeichnet den Ring in diesem Fall auch mit $\mathbb{F}_p$ ($\mathbb{F}$ für „field"). Die Elemente von $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\bar{0}\}$ bilden eine zyklische Gruppe mit $p-1$ Elementen. Man bezeichnet $p-1$ auch als die ***Ordnung*** der Gruppe $\mathbb{F}_p^\times$.

Ist nun die ungerade Primzahl p als Quadratsumme darstellbar, $x^2 + y^2 = p$ mit $x, y \in \mathbb{Z}$, dann gilt $x^2 + y^2 \equiv 0 \bmod p$, und dies kann in $\mathbb{F}_p$ als Gleichung der Form $\bar{x}^2 + \bar{y}^2 = \bar{0}$ interpretiert werden. Wegen $\bar{x}, \bar{y} \neq \bar{0}$ kann die Gleichung zu $(\bar{y}/\bar{x})^2 = -\bar{1}$ umgestellt werden. Dies bedeutet, dass in $\mathbb{F}_p$ eine Quadratwurzel von $-\bar{1}$ existiert. Wir wissen bereits, dass dies eine Eigenschaft ist, die nicht jeder Körper besitzt: Während in $\mathbb{C}$ eine Quadratwurzel aus -1 existiert, trifft dies für den Körper $\mathbb{R}$ nicht zu.

Wie wir in der Gruppentheorie sehen werden, kannjedem Element $\bar{z}$ der multiplikativen Gruppe $\mathbb{F}_p^\times$ unseres Körpers eine natürliche Zahl n zugeordnet werden, die man als ***Ordnung*** von $\bar{z}$ bezeichnet. Es handelt sich dabei um die kleinste Zahl $n \in \mathbb{N}$ mit $\bar{z}^n = \bar{1}$. Ist $i \in \mathbb{F}_p$ eine Quadratwurzel aus $-\bar{1}$, dann ist dieses Element von Ordnung 4, denn es gilt $i^4 = \bar{1}$, während $i^1 = i$, $i^2 = -\bar{1}$ und $i^3 = -i$ ungleich $\bar{1}$ sind. Ein elementarer Satz aus der Gruppentheorie besagt, dass in einer Gruppe der Ordnung $p-1$ nur dann ein Element der Ordnung 4 existieren kann, wenn 4 ein Teiler von $p-1$ ist. Dies wiederum ist äquivalent zu $p \equiv 1 \bmod 4$. Dait haben wir also einen zweiten Beweis für die Notwendigkeit unserer Bedingung gefunden.

Setzen wir nun voraus, dass $p \equiv 1 \bmod 4$ ist und zeigen, dass diese Bedingung auch ***hinreichend*** für die Darstellbarkeit als Quadratsumme ist. Nach Voraussetzung ist 4 ein Teiler von $p-1$. Weil $\mathbb{F}_p^\times$ eine ***zyklische*** Gruppe der Ordnung $p-1$ ist, folgt daraus, dass in $\mathbb{F}_p^\times$ ein Element $\bar{a}$ der Ordnung 4 existiert. Weil $-\bar{1}$ in $\mathbb{F}_p^\times$ das einzige Element der Ordnung 2 ist, gilt $\bar{a}^2 = -\bar{1}$. Dies bedeutet wiederum, dass ein $a \in \mathbb{Z}$ mit $a^2 + 1 \equiv 0 \bmod p$ existiert. Um nun von dieser Kongruenz auf die Lösbarkeit der Gleichung $x^2 + y^2 = p$ in $\mathbb{Z}$ zu schließen, benötigen wir als weiteres Hilfsmittel den Ring

$$\mathbb{Z}[i] \quad = \quad \{a + bi \mid a, b \in \mathbb{Z}\}$$

der ***Gaußschen Zahlen***. Es handelt sich dabei um einen Teilring von $\mathbb{C}$, dem Körper der komplexen Zahlen, und $i \in \mathbb{C}$ bezeichnet die imaginäre Einheit mit $i^2 = -1$. Wir werden den Ring $\mathbb{Z}[i]$ in der Vorlesung eingehend studieren und dabei feststellen, dass dieser mit dem Ring $\mathbb{Z}$ der ganzen Zahlen vielen gemeinsame Eigenschaften besitzt. Eine wichtige solche Eigenschaft ist die ***eindeutige Primfaktorzerlegung***. Genau wie sich jede ganze Zahl $\neq 0$ bis auf Vorzeichen und Reihenfolge eindeutig als Produkt von Primzahlen darstellen lässt, besitzt jede Zahl $\neq 0$ in $\mathbb{Z}[i]$ eine im wesentlichen eindeutige Darstellung als Produkt von ***Primelementen***, die sich nicht weiter in „kleinere" Elemente zerlegen lassen. Ein Unterschied zwischen $\mathbb{Z}$ und $\mathbb{Z}[i]$ liegt in der Anzahl der ***Einheiten***, also der Elemente, die im Ring selbst einen Kehrwert besitzen. In $\mathbb{Z}$ sind ± 1 die einzigen Einheiten, während $\mathbb{Z}[i]$ mit ± 1, $\pm i$ genau vier Einheiten besitzt.

Die Kongruenz $a^2 + 1 \equiv 0 \bmod p$ lässt sich nun in $\mathbb{Z}[i]$ so interpretieren, dass das Produkt

$$(a - i)(a + i) \quad = \quad a^2 + 1$$

von p geteilt wird. Nehmen wir nun an, p wäre in $\mathbb{Z}[i]$ ein Primelement. Allgemein gilt für ein Primelement π in einem Ring R, dass aus der Teilbarkeit $\pi|(cd)$ eines Produkts von Elementen $c, d \in R$ stets $\pi|c$ oder $\pi|d$ folgt. In unserem Fall wäre p also ein Teiler von $a-i$ oder $a+i$. Weil aber die Elemente $\frac{a}{p} - \frac{i}{p}$ und $\frac{a}{p} + \frac{i}{p}$ beide nicht in $\mathbb{Z}[i]$ liegen, wird tatsächlich keines der beiden Elemente von p geteilt. Damit kann p in $\mathbb{Z}[i]$ kein Primelement sein. Auf Grund der eindeutigen Primfaktorzerlegung lässt sich p in $\mathbb{Z}[i]$ also weiter zerlegen. Mit Hilfe der sog. ***Normfunktion*** auf $\mathbb{Z}[i]$ lässt sich zeigen, dass eine solche Zerlegung von der Form $p = (x + iy)(x - iy)$ mit $x, y \in \mathbb{Z}$ sein muss. Wegen $(x + iy)(x - iy) = x^2 + y^2$ ist p dann als Quadratsumme darstellbar.

(b) Verschlüsselung mit dem RSA-Verfahren

Das 1977 entwickelte, nach seinen Erfindern Rivest, Shamir und Adleman entwickelte RSA-Kryptosystem ist ein Beispiel für ein sog. ***Public-Key-Kryptographieverfahren***. Das Grundprinzip von solchen Verfahren besteht darin, dass eine Person X auf ihrem Rechner ein Paar bestehend aus einem ***öffentlichen*** und einem ***geheimen*** Schlüssel erzeugt. Der öffentliche Schlüssel wird jedem zugegänglich gemacht, der die Möglichkeit haben soll, der Person X eine verschlüsselte Nachricht zukommen zu lassen. Mit Hilfe des öffentlichen Schlüssels wird eine Nachricht m codiert und die so erhaltene Chiffre c der Person X zugestellt. Mit ihrem geheimen Schlüssel kann X aus c die Nachricht m zurückgewinnen. Fängt jemand die Chiffre c unterwegs ab, so ist diese ohne den geheimen Schlüssel wertlos.

Der erste Schritt ist also die Generierung eines öffentlichen und eines geheimen Schlüssels. Dazu wählt man beim RSA-Verfahren zwei große Primzahlen p und q und bildet das Produkt $N = p \cdot q$. Außerdem berechnet man noch die Zahl $\varphi(N) = (p-1)(q-1)$. (Dabei steht φ für die sog. ***Eulersche φ-Funktion***.) Die Sicherheit des RSA-Verfahrens beruht darauf, dass kein effizienter Algorithmus bekannt ist, mit dem sich die Zahl N in die Faktoren p und q zerlegen oder die Zahl $\varphi(N)$ ohne Kenntnis von p und q berechnen lässt. In einem weiteren Schritt bestimmt man zufällig eine Zahl e mit $1 < e < \varphi(N)$, die zu $\varphi(N)$ teilerfremd ist, und eine Zahl d mit $1 < d < \varphi(N)$ und $de \equiv 1 \bmod \varphi(N)$. Das Paar (e, N) ist dann der ***öffentliche***, das Paar (d, N) der ***geheime Schlüssel***.

Kommen wir nun zur Verschlüsselung einer Nachricht m mit Hilfe des öffentlichen Schlüssels. Wir gehen davon aus, dass die Nachricht m eine Zahl mit $0 \leq m < N$ ist. Handelt es sich bei m nicht um eine Zahl, sondern um einen Text, so muss dieser zunächst in Blöcke geeigneter Größe zerlegt und jeder einzelne Block in eine Zahl der passenden Größe umgewandelt werden. Im Beispiel unten werden wir sehen, wie sich dies konkret bewerkstelligen lässt. Die Verschlüsselung c von m ist nun die eindeutig bestimmte Zahl $c \in \mathbb{Z}$ mit $0 \leq c < N$ und

$$c \equiv m^e \bmod N.$$

Die Berechnung der Potenz m^d modulo N ist auf einem Rechner auch bei sehr großen Exponenten d in kurzer Zeit möglich. Um aus c die Nachricht m zurückzuerhalten, berechnet man die eindeutig bestimmte Zahl $m' \in \mathbb{Z}$ mit $0 \leq m' < N$ und

$$m' \equiv c^d \bmod N.$$

Eventuell muss die Zahl m' dann noch in einen Textblock zurückverwandelt werden. Dass die Entschlüsselung die Nachricht m zurückliefert, dass also $m = m'$ gilt, ist darauf zurückzuführen, dass jedes $a \in \mathbb{Z}$ der Kongruenz $a^{de} \equiv a \bmod N$ genügt. Dies wiederum hat mit der Struktur des Rings $\mathbb{Z}/N\mathbb{Z}$ und seiner ***primen Restklassengruppe*** $(\mathbb{Z}/N\mathbb{Z})^\times$ zu tun. Eine wesentliche Rolle spielt hierbei der ***Chinesische Restsatz***, ein weiterer wichtiger Satz, den wir in der Vorlesung kennenlernen werden.

Schauen wir uns nun an einem konkreten Beispiel an, wie das RSA-Verfahren funktioniert. Dazu stellen wir uns die Aufgabe, den Namen **RIVEST** von einem der RSA-Entwickler zu chiffrieren. Wir unterteilen unseren „Text" in Blöcke zu je einem Buchstaben und wandeln jeden Buchstaben in eine Zahl zwischen 0 und 25 um, wobei der Buchstabe **A** der Null, **B** der Eins usw. entspricht. Als Primzahlen wählen wir $p = 7$ und $q = 11$. Dann ist $N = 77$ und $\varphi(N) = 6 \cdot 10 = 60$. Weiter sei $e = 13$ und $d = 37$. Die Bedingung $13 \cdot 37 = 481 \equiv 1 \bmod 60$ ist dann erfüllt. Das Paar $(13, 77)$ ist dann der öffentliche, das Paar $(37, 77)$ der geheime Schlüssel.

Die Buchstabenfolge **RIVEST** entspricht den Zahlen $17, 8, 21, 4, 18, 19$. Für die Verschlüsselung bildet man

$$\begin{aligned} 17^{13} \equiv 73 \bmod 77 \quad , \quad 8^{13} \equiv 50 \bmod 77 \quad , \quad 21^{13} \equiv 21 \bmod 77 \quad , \\ 4^{13} \equiv 53 \bmod 77 \quad , \quad 18^{13} \equiv 46 \bmod 77 \quad , \quad 19^{13} \equiv 61 \bmod 77. \end{aligned}$$

Unsere Chiffre besteht also aus den Zahlen 73, 50, 21, 53, 46, 61. Durch Potenzierung mit $d = 37$ erhält man die ursprüngliche Zahlenfolge zurück:

$$\begin{aligned} 73^{37} \equiv 17 \bmod 77 \quad , \quad 50^{37} \equiv 8 \bmod 77 \quad , \quad 21^{37} \equiv 21 \bmod 77 \quad , \\ 53^{37} \equiv 4 \bmod 77 \quad , \quad 46^{37} \equiv 18 \bmod 77 \quad , \quad 61^{37} \equiv 19 \bmod 77. \end{aligned}$$

Die Verschlüsselung einzelner Buchstaben ist kein besonders sicheres Verfahren. In vielen Fällen kann man den Originaltext beispielsweise durch ***Häufigkeitsanalyse*** gewinnen. Man nutzt dabei aus, dass einige Buchstaben, wie z.B. das „e" in einem deutschsprachigen Text, häufiger vorkommen als andere Buchstaben. Ein höheres Maß an Sicherheit gewinnt man, indem man Blöcke bestehend aus zwei oder mehr Buchstaben gleichzeitig verschlüsselt. Allerdings benötigt man dafür dann eine größere Schlüssellänge. Entscheiden wir uns beispielsweise dafür, Zweierblöcke zu verschüsseln, dann gibt es $26 \cdot 26$ Möglichkeiten für eine Buchstabenkombination. Entsprechend müssen die Primzahlen p und q so groß gewählt werden, dass $N = p \cdot q \geq 26^2$ ist.

Sehen wir uns auch dies noch einmal an einem konkreten Beispiel an. Wählen wir etwa die Primzahlen $p = 29$ und $q = 31$, dann ist mit $N = 29 \cdot 31 = 899$ die Bedingung $N \geq 26 \cdot 26 = 416$ erfüllt. Wir erhalten $\varphi(N) = 28 \cdot 30 = 840$. Außerdem wählen wir $e = 17$ und erhalten durch $d = 593$ (welche die Bedinung $d \cdot e \equiv 1 \bmod 840$ erfüllt). Damit ist $(17, 899)$ der öffentliche und $(593, 899)$ der private Schlüssel.

Verwenden wir nun den öffentlichen Schlüssel, um die drei Blöcke **RI**, **VE** und **ST** des Originaltexts **RIVEST** zu chiffrieren. Die Buchstabenkombination **RI** entspricht der Zahl $17 + 8 \cdot 26 = 225$, für **VE** erhält man $21 + 4 \cdot 26 = 125$, und **ST** ergibt $18 + 19 \cdot 26 = 512$. Die drei Zahlen $225, 125, 512$ werden nun mit $(17, 899)$ verschlüsselt zu

$$225^{17} \equiv 498 \bmod 899 \quad , \quad 125^{17} \equiv 497 \bmod 899 \quad , \quad 512^{17} \equiv 101 \bmod 899$$

Mit dem privaten Schlüssel $(593, 899)$ erhält man durch

$$498^{593} \equiv 225 \bmod 899 \quad , \quad 497^{593} \equiv 125 \bmod 899 \quad , \quad 101^{593} \equiv 512 \bmod 899$$

die zuvor verschlüsselten Zahlen zurück. Aus den drei Zahlen 225, 125 und 512 lässt sich auch die Buchstabenkombination leicht wiederherstellen: Dividiert man 225 durch 26, so erhält man $225 = 17 + 8 \cdot 26$. Die Zahl 17 entspricht dem Buchstaben **R**, die Zahl 8 dem Buchstaben **I**. Genauso verfährt man mit den anderen beiden Blöcken.

§ 2. *Die Kategorie der Ringe*

Überblick

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 Zahlbreiche $\mathbb{Q}$, $\mathbb{R}$ 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 $1_R + ... + 1_R = 0_R$ gelten kann, das man aber in den gewohnten Zahlbereichen ebenfalls nicht antrifft.

Wichtige Begriffe und Sätze

- Ringe und Ringhomomorphismen
- Für jeden Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to R$.
- Einheiten und Nullteiler
- wichtige Ringtypen: Nullringe, Integritätsbereiche, Körper
- Charakteristik eines Rings

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

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.
(ii) Das Paar $(R, \cdot)$ ist ein kommutatives Monoid.
(iii) 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*** $\mathbb{Z}/n\mathbb{Z}$ kennnenlernen. 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

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

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

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

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

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

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

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 $\pi_1 : R \times S \to R$, $(r,s) \mapsto r$ und $\pi_2 : R \times S \to S$, $(r,s) \mapsto s$ 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

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

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 $\phi : R \to S$ ein ***Gruppenhomomorphismus*** $(R, +_R) \to (S, +_S)$ und ein ***Monoid-Homomorphismus*** $(R, \cdot_R) \to (S, \cdot_S)$ 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

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

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.

(2.3) Satz Für jeden Ring R existiert ein eindeutig bestimmter Homomorphismus $\mathbb{Z} \to R$ 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

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

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

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

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. Ingesamt ist somit gezeigt, dass es sich bei ϕ um einen Ringhomomorphismus handelt.

Zum Nachweis der *Eindeutigkeit* sei ein weiterer Ringhomomorphismus $\psi : \mathbb{Z} \to R$ vorgegeben. Dann gilt $\phi(1) = 1_R = \psi(1)$. Weil ϕ und ψ insbesondere Gruppenhomorphismen 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. □

(2.4) Definition 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***.

(2.5) Definition 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.

(2.6) Lemma

(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. □

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

(2.7) Proposition Ein Körperhomomorphismus $\phi : K \to L$ 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. □

(2.8) Definition Sei R ein Ring. Die ***Charakteristik*** eines Rings R ist definiert durch

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

Bei positiver Charakteristik ist $\operatorname{char}(R)$ 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.

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

Beweis: Wäre $\mathrm{char}(R) = 1$, dann wäre der Ring R, wie wir soeben bemerkt haben, ein Nullring und damit kein Integritätsbereich. Nehmen wir nun an, dass $n = \mathrm{char}(R) > 1$, 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. □

Nach (2.9) ist also insbesondere $\mathrm{char}(K)$ für einen Körper gleich Null oder eine Primzahl. Es gibt beispielsweise keinen Körper der Charakteristik 4.

§ 3. *Teilringe und Erzeugendensysteme*

Überblick

Häufig ist bei der Untersuchung einer algebraischen Struktur daran interessiert, gleichartige Unterstrukturen zu finden. Bei den Ringen sind dies die ***Teilringe***, also Teilmengen die (mit entsprechend eingeschränkter Addition und Multiplikation) selbst einen Ring bilden. Fast noch wichtiger ist in der Ringtheorie der umgekehrte Gesichtspunkt, nämlich die ***Erweiterung*** eines Rings zu einer größeren Struktur. So ist es beispielsweise für arithmetische Anwendungen interessant, wie der kleinste Erweiterungsring von $\mathbb{Z}$ aussieht, der eine irrationale Zahl wie etwa $\sqrt{2}$ enthält (den man dann mit $\mathbb{Z}[\sqrt{2}]$ bezeichnet). Wir werden in diesem Abschnitt sehen, wie man die Elemente eines solchen Rings bestimmt.

Wichtige Begriffe und Sätze

- Teilring eines Rings R, Erweiterungsring, Ringerweiterung
- Definition des von einer Menge A erzeugten Erweiterungsrings $R[A]$, Existenz und Eindeutigkeit
- Die Elemente des Rings $\mathbb{Z}[\sqrt{d}]$ sind die Elemente der Form $a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$.
- Allgemein sind die Elemente eines Erweiterungsrings $R[c]$ die Polynomausdrücke in c mit Koeffizienten aus R.
- Teilkörper und Primkörper; jeder Primkörper ist isomorph zu $\mathbb{Q}$ oder $\mathbb{F}_p$, für eine Primzahl p

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

(3.2) Satz 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 Verknüpfungen, die durch Einschränkung von $+$ und $\cdot$ auf S zu Stande kommen, 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

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

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. □

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.

> **(3.3) Lemma** 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 $a - b \in S_i$ iund $ab \in S_i$ 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. □

> **(3.4) Satz** 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 (3.3) 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 $R[A] = S$. □

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 gelegentlich 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

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

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 $a \equiv b \bmod n$, 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 § 6 beschäftigen. Als konkrete Anwendung von (3.4) zeigen wir nun

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

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

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

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 $\alpha \in M$ vorgeben, $\alpha = r + s\sqrt{d}$ 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. Zunächst liegt $1 = \frac{1}{2} \cdot 2 + \frac{1}{2} \cdot 0 \cdot \sqrt{d}$ in M, denn es gilt $2 \equiv 0 \bmod 2$. 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 $r \equiv s \bmod 2$ und $t \equiv u \bmod 2$ gilt. Das Element

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

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

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

mit $v = \frac{1}{2}\left(rt + dsu\right)$ und $w = \frac{1}{2}\left(st + ru\right)\sqrt{d}$ 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 $v \equiv w \bmod 2$ erfüllen. Auf Grund der Voraussetzung $d \equiv 1 \bmod 4$ gilt $rt + dsu + st + ru \equiv rt + su + st + ru \equiv (r+s)(t+u) \bmod 4$, 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 $a = \frac{1}{2}(2a) + \frac{1}{2} \cdot 0\sqrt{d}$ und $2a \equiv 0 \bmod 2$ 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 $1 \equiv 1 \bmod 2$.

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 $r, s \in \mathbb{Z}$, $r \equiv s \bmod 2$. 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'. □

Allgemeiner kann man zeigen

(3.6) Proposition Sei $\tilde{R}|R$ eine Ringerweiterung und $c \in \tilde{R}$. Dann gilt

$$R[c] \quad = \quad \left\{ \sum_{i=0}^{n} a_i c^i \;\mid\; n \in \mathbb{N}_0,\ a_0, ..., a_n \in R \right\}.$$

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 (setze $n = 0$ und $a_0 = 1_R$). Seien $f, g \in S$ vorgegeben. Dann gibt es $m, n \in \mathbb{N}_0$ und $a_i, b_j \in R$ für $0 \le i \le m$ und $0 \le j \le n$, so dass

$$f = \sum_{i=0}^{m} a_i c^i \qquad \text{und} \qquad g = \sum_{j=0}^{n} b_j c^j$$

erfüllt ist. O.B.d.A. können wir $m \le n$ annehmen (sonst vertauschen wir die Rolle von f und g). Indem wir $a_{m+1}, ..., a_n$ auf Null setzen, können wir sogar $m = n$ voraussetzen. Es gilt dann

$$f - g \quad = \quad \sum_{j=0}^{n} (a_j - b_j) c^j \in S \quad \text{und} \quad fg \quad = \quad \sum_{i=0}^{m} \left(\sum_{j=0}^{i} a_{i-j} b_j \right) c^i \in S.$$

Dies zeigt, dass es sich bei S um einen Teilring von $\tilde{R}$ handelt. Jedes $a \in R$ ist in S enthalten (setze $n = 0$, $a_0 = a$). Auch das Element c liegt in S (setze $n = 1$, $a_0 = 0_R$, $a_1 = 1_R$). Also ist $R \cup \{c\}$ in S enthalten.

Sei nun R' ein beliebiger Teilring von R mit $R' \supseteq R \cup \{c\}$. Zu zeigen ist, dass $R' \supseteq S$ gilt. Wir beweisen durch vollständige Induktion über $n \in \mathbb{N}_0$, dass sämtliche Elemente der Form $\sum_{i=0}^{n} a_i c^i$ mit $a_0, ..., a_n \in R$ in R' enthalten sind. Für $n = 0$ folgt dies direkt aus der Voraussetzung für $R \subseteq R'$. Sei nun $n \in \mathbb{N}_0$, und setzen wir die Behauptung für n voraus. Sei $f = \sum_{i=0}^{n+1} a_i c^i$ vorgegeben, mit $a_0, ..., a_n, a_{n+1} \in R$. Nach Induktionsvoraussetzung ist $g = \sum_{i=0}^{n} a_i c^i$ in R' enthalten. Wegen $a_{n+1}, c \in R'$ und auf Grund der Teilring-Eigenschaft von R' ist dann auch $f = g + a_{n+1} c^{n+1}$ in R' enthalten. Damit haben wir die Eigenschaften (i),(ii) aus (3.4) für S nachgewiesen, und es folgt $R[c] = S$. □

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

(3.7) Definition 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 (3.2) 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. Genau wie in (3.3) beweist man

(3.8) Proposition 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.

Insbesondere gibt es bezüglich Inklusion einen kleinsten Teilkörper von K, den man als ***Primkörper*** von K bezeichnet. Dieser Körper wird im zweiten Teil der Algebra-Vorlesung eine wichtige Rolle spielen. Dort werden wir sehen, dass jeder Primkörper entweder isomorph zum Körper $\mathbb{Q}$ der rationalen Zahlen oder zum Körper $\mathbb{F}_p$ mit p Elementen ist, für eine geeignete Primzahl p.

§ 4. *Konstruktion der Quotientenkörper und Polynomringe*

Überblick

In diesem Abschnitt lernen wir ein allgemeines Verfahren zur Konstruktion von Ringerweiterungen kennen. Mit diesem Verfahren werden wir für jeden Integritätsbereich R einen Quotienenkörper K konstruieren, dessen Elemente genau die „Brüche "der Form ab^{-1} mit $a, b \in R$ und $b \neq 0_R$ sind, und für die in der Regel auch die gewohnte Bruchschreibweise $\frac{a}{b}$ verwendet wird. Außerdem werden wir mit diesem Verfahren jedem Ring R einen Polynomring $R[x]$ zuordnen, der genau die Rechenregeln erfüllt, die man vom Ring $\mathbb{R}[x]$ der reellen Polynome her gewohnt ist. Neben der Konstruktion leiten wir in diesem Abschnitt für $R[x]$ auch einige algebraische Eigenschaften her, zum Beispiel die Beschreibung der Einheiten und Nullteiler sowie Rechenregeln für die Gradfunktion.

Wichtige Begriffe und Konzepte

- Übertragung von Verknüfpungen durch Bijektionen, „Vererbung "der Verknüpfungseigenschaften
- Anwendung dieses Prinzips zur Konstruktion von Ringerweiterungen
- Definition des Quotientenkörpers eines Integritätsbereichs R
- Definition des Polynomrings $R[x]$ über einem Ring R
- Für den Grad von Polynomen gelten die Rechenregeln $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$ und $\operatorname{grad}(fg) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$. Für die zweite Regel gilt bei Integritätsbereichen sogar Gleichheit.
- Ist R ein Integritätsbereich, dann auch $R[x]$. Die Einheitengruppe von $R[x]$ ist in diesem Fall gegeben durch $R[x]^\times = R^\times$.

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

(4.1) Lemma Seien X und Y Mengen, $\phi : Y \to X$ eine Bijektion und $\cdot$ eine Verknüpfung auf X. Wir definieren auf Y eine Vernüpfung $\odot$, 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 $\cdot$ kommuativ 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 Neutralelement 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 $d \odot c = e_Y$. □

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.

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

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

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

Beweis: Es genügt, mit Hilfe von (4.1) 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 (4.1) dasselbe für die Verknüpfung $\oplus$ auf S. Weil 0_R in der Halbgruppe $(R, +)$ ein Neutralelement ist, handelt es sich bei $0_S = \phi^{-1}(0_R)$ nach (4.1) (ii) um ein Neutralelement in $(S, \oplus)$. Schließlich besitzt jedes Element $a \in S$ bezüglich $\oplus$ ein Inverses, nämlich nach (4.1) (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

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

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

(4.3) Satz *(Konstruktion von Ringerweiterungen)*
Sei $\phi : R \to S$ ein Monomorphismus von Ringen. Dann gibt es einen Erweiterungsring $\hat{R} \supseteq R$ und einen Isomorphismus $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}|_R = \phi$.

Beweis: Allgemein gilt: Sind A, B, C, D Mengen mit $A \cap B = C \cap D = \varnothing$, und $\phi_1 : A \to C$, $\phi_2 : B \to D$ bijektive Abbildungen, dann gibt es eine eindeutig bestimmte Abbildung $\phi : A \cup B \to C \cup D$ 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 $\hat{\phi} : \hat{R} \to S$ mit $\hat{\phi}|_R = \phi$ und $\hat{\phi}|_{S \setminus \phi(R)} = \mathrm{id}_{S \setminus \phi(R)}$.

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 (4.2) 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 (4.1) 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 erstes verwenden wir diesen Satz nun für die Konstruktion der Quotientenkörper.

(4.4) Definition 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 $\mathbb{Z}$. Der Nachweis der Eindeutigkeit ist auf Grund der Definition zwar etwas langwierig, aber einfach.

(4.5) Proposition Ist R ein Integritätsbereich und sind K und K' Quotientenkörper von R, dann gibt es einen Isomorphismus $\phi : K \to K'$ mit $\phi|_R = \mathrm{id}_R$.

Beweis: Zunächst beweisen wir die zweite Teilaussage. Seien K, K' wie angegeben. Wir definieren $\phi : K \to K'$, indem wir für $a, b \in R$ mit $b \neq 0_R$ jeweils $\phi(ab^{-1}) = ab^{-1}$ setzen (wobei das Inverse b^{-1} und die Verknüpfung ab^{-1} einmal in K und einmal in K' gebildet wird. Es muss nun zuerst gezeigt werden, dass diese Abbildung wohldefiniert, das Bild von $ab^{-1} \in K$ also unabhängig von der Darstellung des Elements durch die Ringelemente a, b ist. Nehmem wir also an, dass $c, d \in R$ Elemente mit $d \neq 0_R$ existieren, so dass in K die Gleichung $ab^{-1} = cd^{-1}$ gilt. Es ist dann $ad = bc$ in R. Dementsprechend muss die Gleichung $ab^{-1} = cd^{-1}$ auch im Erweiterungsring K' von K gelten, wodurch die Wohldefiniertheit von ϕ bewiesen ist. Dass $\phi|_R = \mathrm{id}_R$ gilt, ist wegen $\phi(a) = \phi(a \cdot 1_R^{-1}) = a \cdot 1_R^{-1} = a$ für alle $a \in R$ offensichtlich. Die Abbildung ϕ ist surjektiv,

denn jedes $\beta \in K'$ kann in der Form $\beta = ab^{-1}$ mit $a, b \in R$ und $b \neq 0_R$ dargestellt werden, und es gilt $\phi(ab^{-1}) = ab^{-1} = \beta$. Schließlich ist die Abbildung auch injektiv. Sind nämlich $a, b, c, d \in R$ vorgegeben, mit $c, d \neq 0_R$ und $\phi(ab^{-1}) = \phi(cd^{-1})$, dann folgt $ab^{-1} = cd^{-1}$ in K' nach Definition von ϕ, damit $ad = bc$ in R, und damit wiederum $ab^{-1} = cd^{-1}$ in K.

Es bleibt zu zeigen, dass es sich bei ϕ um einen Homomorphismus von Ringen handelt. Wegen $\phi(a) = a$ für alle $a \in R$ und $1_R \in R$ gilt insbesondere $\phi(1_R) = 1_R = 1_{K'}$, wobei die letzte Gleichung dadurch zu Stande kommt, dass R ein Teilring von K' ist. Seien nun $\alpha, \beta \in K$ vorgegeben und $a, b, c, d \in R$ mit $b, d \neq 0_R$ und $\alpha = ab^{-1}$ und $\beta = cd^{-1}$. Dann gilt $\alpha + \beta = (ad + bc)(bd)^{-1}$ und $\alpha\beta = (ac)(bd)^{-1}$. Nach Definition von ϕ folgt dann

$$\phi(\alpha +_K \beta) \quad = \quad \phi((ad +_R bc)(bd)^{-1}) \quad = \quad (ad +_R bc)(bd)^{-1} \quad = \quad ab^{-1} +_{K'} cd^{-1} \quad = \quad \phi(\alpha) +_{K'} \phi(\beta)$$

und ebenso $\phi(\alpha \cdot_K beta) = \phi((ac)(bd)^{-1}) = (ac)(bd)^{-1} = \alpha \cdot_{K'} \beta$. □

Interessanter ist der Nachweis der *Existenz* eines Quotientenkörpers, wozu nun zum ersten Mal der Satz (4.3) zum Einsatz kommt.

(4.6) Satz Zu jedem Integritätsbereich R existiert ein Quotientenkörper.

Beweis: Wir definieren auf der Menge $X_R = R \times (R \setminus \{0_R\})$ eine Relation $\sim$ durch $(a, b) \sim (c, d) \Leftrightarrow ad = bc$. Zunächst überprüfen wir, dass $\sim$ eine Äquivalenzrelation ist. Wegen $ab = ab$ gilt $(a, b) \sim (a, b)$, also ist die Relation reflexiv. Die Äquivalenz

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

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 $cf = de$. $adf = bcf = bde$. Weil R ein Integritätsbereich ist, dürfen wir nach (2.6) die Kürzungsregel anwenden und erhalten $af = be$, also $(a, b) \sim (e, f)$. Also ist $\sim$ tatsächlich eine Äquivalenzrelation auf X_R.

Sei nun $\hat{R} = X_R/\sim$ die Menge der Äquivalenzklassen von $\sim$. Für jedes Paar (a, b) sei $[a, b]$ jeweils die zugehörige Äquivalenzklasse. Wir definieren auf $\hat{R}$ zwei Verknüpfungen $\oplus$ und $\odot$, indem wir

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

setzen. (Die Verknüpfungen sind so gewählt, dass sie den bekannten Regeln $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ und $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ der Bruchrechnung entsprechen.) Wir müssen zeigen, dass diese Verknüpfungen wohldefiniert sind, also nicht von der Wahl der jeweiligen Äquivalenzklassenvertreter abhängen. Seien dazu $(a', b'), (c', d') \in X_R$ Elemente mit $(a, b) \sim (a', b')$ und $(c, d) \sim (c', d')$. Dann gilt $ab' = a'b$ und $cd' = c'd$. Es folgt $(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd)$, also $(ac, bd) \sim (a'c', b'd')$. Ebenso gilt

$$(ad + bc)(b'd') \quad = \quad adb'd' + bcb'd' \quad = \quad a'dbd' + bc'b'd \quad = \quad (a'd' + b'c')(bd)$$

und somit $(ab + cd, bd) \sim (a'b' + c'd', b'd')$. 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 ergibt sich aus der Rechnung

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

Damit ist der Beweis der Ringeigenschaften abgeschlossen. Darüber hinaus ist $(\hat{R}, \oplus, \odot)$ sogar ein Körper. Ist nämlich $\alpha \in \hat{R} \setminus \{0_{\hat{R}}\}$, $\alpha = [a,b]$ mit $a, b \in R$, dann ist $[b,a]$ ein Kehrwert von α, denn wegen $(ab, ab) \sim (1_R, 1_R)$ gilt $[a,b] \odot [b,a] = [1_R, 1_R] = 1_{\hat{R}}$.

Also sind sämtliche Elemente der Menge $\hat{R} \setminus \{0_{\hat{R}}\}$ Einheiten. Außerdem ist $\hat{R}$ kein Nullring. Denn andernfalls würde $0_{\hat{R}} = 1_{\hat{R}}$ 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 R als Integritätsbereich kein Nullring ist.

Durch die Abbildung $\phi_R : R \to \hat{R}$, $a \mapsto [a, 1_R]$ ist ein Monomorphismus von Ringen definiert. (...) Nach Satz (4.3) existiert nun ein Erweiterungsring K von R und ein Isomorphismus $\hat{\phi}_R : K \to \hat{R}$ von Ringen mit $\hat{\phi}_R|_R = \phi_R$. Für jedes Element $\alpha \in K$ gibt es $a, b \in R$ mit $b = 0_R$ und

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

wobei das Element ab^{-1} im letzten Schritt im Körper K gebildet wird. Auf Grund der Injektivität von $\hat{\phi}_R$ folgt $\alpha = ab^{-1}$. Dies zeigt, dass es sich bei K um einen Quotientenkörper handelt. □

Nun kommen wir zur Konstruktion der Polynomringe. Ausdrücke wie zum Beispiel $x^2 - 3x + 5$, die aus Zahlen und einer „Unbekannten“ x zusammengesetzt sind, begegnen uns schon im Mathematikuntericht der Mittelstufe. Wir werden nun die Ringe, die aus solchen Elementen bestehen, zunächst durch ihre algebraischen Eigenschaften charakterisieren und zeigen, dass sie durch diese Eigenschaften bis auf Isomorphie eindeutig bestimmt sind. Am Ende des Abschnitts wird dann die Existenz solcher Ringe mit derselben Methode wie bei den Quotientenkörpern formal nachgewiesen.

(4.7) Satz *(Existenz von Polynomringen)*
Sei R ein Ring. Dann gibt es einen Erweiterungsring $R[x] \supseteq R$ und ein Element $x \in R[x]$ 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 $a_0, ..., a_n \in R$ existieren, so dass $a_n \neq 0$ ist und f in der Form

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

Ein Ring $R[x]$ mit der in (4.7) beschriebenen Eigenschaften wird ***Polynomring*** über R genannt, die Elemente von $R[x]$ heißen ***Polynome***. Man bezeichnet die Zahl $n = \deg(f)$ in (4.7) als ***Grad*** des Polynoms f. Das Polynom $a_n x^n$ ist der ***Leitterm***, das Element $a_n \in R$ der ***Leitkoeffizient*** des Polynoms.

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 $a_1 = 1_R$). Ein wichtiges Merkmal der Polynomringe ist die folgende universelle Eigenschaft.

(4.8) Satz *(universelle Eigenschaft des Polynomrings)*
Für jeden Ringhomomorphismus $\phi : R \to S$ und jedes $a \in S$ gibt es einen eindeutig bestimmten Ringhomomorphismus $\hat{\phi} : R[x] \to S$ 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

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

und diese ist eindeutig bestimmt. Wir definieren eine Abbildung $\hat{\phi} : R[x] \to S$, 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

$$f = \sum_{k=0}^{m} a_k x^k \qquad \text{und} \qquad g = \sum_{k=0}^{n} b_k x^k$$

besitzen, mit $m, n \in \mathbb{N}_0$, $a_k, b_k \in R$ und $a_m, b_n \neq 0_R$. Wir setzen $a_i = 0_R$ für $i > m$ und $b_j = 0$ für $j > n$. Es gilt dann

$$f + g = \sum_{k \in \mathbb{N}_0} (a_k + b_k) x^k \qquad \text{und} \qquad fg = \left(\sum_{k \in \mathbb{N}_0} a_k x^k \right) \left(\sum_{k \in \mathbb{N}_0} b_k x^k \right) = \sum_{k \in \mathbb{N}_0} \left(\sum_{i=0}^{k} a_{k-i} b_i \right) x^k \quad ,$$

und es folgt

$$\hat{\phi}(f+g) \quad = \quad \sum_{k\in\mathbb{N}_0} \phi(a_k+b_k)a^k \quad = \quad \sum_{k\in\mathbb{N}_0} \phi(a_k)a^k + \sum_{k\in\mathbb{N}_0} \phi(b_k)a^k \quad = \quad \hat{\phi}(f)+\hat{\phi}(g)$$

sowie

$$\hat{\phi}(fg) \quad = \quad \sum_{k\in\mathbb{N}_0} \phi\left(\sum_{i=0}^{k} a_{k-i}b_i\right)a^k \quad = \quad \sum_{k\in\mathbb{N}_0}\sum_{i=0}^{k} \phi(a_{k-i})\phi(b_i)a^k \quad =$$

$$\left(\sum_{k\in\mathbb{N}_0} \phi(a_k)a^k\right)\left(\sum_{k\in\mathbb{N}_0} \phi(b_k)b^k\right) \quad = \quad \hat{\phi}(f)\hat{\phi}(g).$$

Für den Beweis der *Eindeutigkeit* nehmen wir an, dass neben $\hat{\phi}$ durch ψ ein weiterer Ringhomomorphismus $R[x] \to S$ 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 $a_0, ..., a_n \in R$ und $a_n \neq 0_R$. Es gilt dann

$$\hat{\phi}(f) \quad = \quad \hat{\phi}\left(\sum_{k=0}^{n} a_k x^k\right) \quad = \quad \sum_{k=0}^{n} \hat{\phi}(a_k x^k) \quad = \quad \sum_{k=0}^{n} \phi(a_k)a^k \quad =$$

$$\sum_{k=0}^{n} \psi(a_k x^k) \quad = \quad \psi\left(\sum_{k=0}^{n} a_k x^k\right) \quad = \quad \psi(f).$$

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

Ist $S = R$ oder ein Erweiterungsring von R, dann bezeichnet man den eindeutig bestimmten Homorphismus $\hat{\phi}$ aus (4.8) als ***Auswertungshomomorphismus*** an der Stelle a.

(4.9) Folgerung 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 (4.8) gibt es eindeutig bestimmte Homomorphismen $\phi : R[x] \to \tilde{R}[y]$ und $\psi : \tilde{R}[y] \to R[x]$ mit $\phi|_R = \psi|_R = \mathrm{id}_R$ sowie $\phi(x) = y$ und $\psi(y) = x$. Damit ist $\psi \circ \phi$ ein Ringhomomorphismus $R[x] \to R[x]$ mit $(\psi \circ \phi)|_R = \mathrm{id}_R$ und $(\psi \circ \phi)(x) = x$. Aber nach (4.8) ist $\mathrm{id}_{R[x]}$ der eindeutig bestimmte Homomorphismus mit dieser Eigenschaft. Es folgt $\psi \circ \phi = \mathrm{id}_{R[x]}$. Genauso beweist man die Gleichung $\phi \circ \psi = \mathrm{id}_{\tilde{R}[y]}$. Also ist ϕ ein Isomorphismus von Ringen. □

(4.10) Proposition 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

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

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

Beweis: zu (i) Sei $m = \deg(f)$ und $n = \deg(g)$. Dann können wir f und g in der Form $f = \sum_{k=0}^{m} a_k x^m$ und $g = \sum_{\ell=0}^{n} b_\ell x^\ell$ darstellen, mit geeigneten $a_k, b_\ell \in R$. Für $k > m$ setzen wir $a_k = 0_R$, ebenso $b_\ell = 0_R$ für $\ell > n$. Es gilt nun

$$f + g \quad = \quad \sum_{k=0}^{m} a_k x^k + \sum_{\ell=0}^{n} b_\ell x^\ell \quad = \quad \sum_{k \in \mathbb{N}_0} a_k x^k + \sum_{\ell \in \mathbb{N}_0}^{m+n} b_\ell x^\ell \quad = \quad \sum_{k \in \mathbb{N}_0} (a_k + b_k) x^\ell .$$

Dabei ist $a_k + b_k \neq 0_R$ nur möglich, wenn $a_k \neq 0_R$ oder $b_k \neq 0_R$ gilt, also wenn $k \leq m$ oder $k \leq n$ ist, was mit $k \leq \max\{m, n\}$ gleichbedeutend ist. Daraus folgt $\deg(f + g) \leq \max\{m, n\} = \max\{\deg(f), \deg(g)\}$. Ebenso zeigt die Rechnung

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

dass $\deg(fg) \leq m + n = \deg(f) + \deg(g)$ 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 $b_n = 0_R$, 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 $a_m b_n \neq 0_R$. Inbesondere 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. □

(4.11) Folgerung 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 $b \in R$ it $ab = 1_R = 1_{R[x]}$. 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 (4.10) (ii) erhalten wir $\operatorname{grad}(f) + \operatorname{grad}(g) = \operatorname{grad}(fg) = \operatorname{grad}(1_R) = 0$, und wegen $\operatorname{grad}(f), \operatorname{grad}(g) \geq 0$ folgt daraus $\operatorname{grad}(f) = \operatorname{grad}(g) = 0$. Also sind f und g beides Elemente des Grundrings R. Aus der Gleichung $fg = 1$ folgt nun, dass f in $R^\times$ enthalten ist. □

Man beachte, dass die Folgerung für Nicht-Integritätsbereiche im Allgemeinen falsch ist. Hier kann es in $R[x]^\times$ auch Einheiten mit Polynomgrad ≥ 1 geben. Beispielsweise werden wir in Kürze den Restklassenring $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ kennenlernen, in dem das Element $\bar{2}$ der wegen $\bar{2} \cdot \bar{2} = \bar{0}$ ein Nullteiler ist. Im Polynomring $\mathbb{Z}/4\mathbb{Z}[x]$ ist das Polynom $f = \bar{2}x + \bar{1}$ eine Einheit, denn es gilt $f \cdot f = (\bar{2}x + \bar{1})(\bar{2}x + \bar{1}) = (\bar{2} \cdot \bar{2})x^2 + (\bar{2} + \bar{2})x + \bar{1} = \bar{0} \cdot x^2 + \bar{0} \cdot x + \bar{1} = \bar{1}$.

Kommen wir nun zur Konstruktion der Polynomringe. Es sei P_R die Menge aller Abbildungen $f : \mathbb{N}_0 \to R$ mit der Eigenschaft, dass $f(k) = 0_R$ für alle bis auf endlich viele $k \in \mathbb{N}_0$ gilt. Wir definieren auf P_R zwei Verknüpfungen $\oplus$ und $\odot$ durch

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

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 $n \geq 1$. Außerdem definieren wir ein Element $\tilde{x} \in P_R$ durch $\tilde{x}(1) = 1_R$ und $\tilde{x}(n) = 0_R$ für $n \neq 1$.

(4.12) Lemma 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.

$$((f \oplus g) \oplus h)(n) \quad = \quad (f \oplus g)(n) + h(n) \quad = \quad (f(n) + g(n)) + h(n) \quad = \quad f(n) + (g(n) + h(n)) \quad =$$
$$f(n) + (g \oplus h)(n) \quad = \quad (f \oplus (g \oplus h))(n)$$

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 $(-f) : \mathbb{N}_0 \to R$ 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

$$((f \odot g) \odot h)(n) \quad = \quad \sum_{k+\ell=n} (f \odot g)(k)h(\ell) \quad = \quad \sum_{k+\ell=n} \left(\sum_{i+j=k} f(i)g(j) \right) h(\ell) \quad =$$
$$\sum_{k+\ell=n} \sum_{i+j=k} f(i)g(j)h(\ell) \quad = \quad \sum_{i+j+\ell=n} f(i)g(j)h(\ell).$$

Ebenso erhalten wir

$$(f \odot (g \odot h))(n) \quad = \quad \sum_{i+k=n} f(i)(g \odot h)(k) \quad = \quad \sum_{i+k=n} f(i) \left(\sum_{j+\ell=k} g(j)h(\ell) \right) \quad =$$
$$\sum_{i+k=n} \sum_{j+\ell=k} f(i)g(j)h(\ell) \quad = \quad \sum_{i+j+k=n} f(i)g(j)h(\ell).$$

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

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

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

$$(f \odot (g \oplus h))(n) \quad = \quad \sum_{k=0}^{n} f(n-k)(g \oplus h)(k) \quad = \quad \sum_{k=0}^{n} f(n-k)\,(g(k) + h(k)) \quad =$$

$$\sum_{k=0}^{n} f(n-k)g(k) + \sum_{k=0}^{n} f(n-k)h(k) \quad = \quad (f \odot g)(n) + (f \odot h)(n) \quad = \quad ((f \odot g) \oplus (f \odot h))(n)$$

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

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

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

$$\tilde{x}^{m+1}(m+1) \quad = \quad (\tilde{x}^m \odot \tilde{x})(m+1) \quad = \quad \sum_{k=0}^{m+1} (\tilde{x}^m)(m+1-k)\tilde{x}(k) \quad = \quad \tilde{x}^m(m+1-1)\tilde{x}(1)$$

$$= \quad \tilde{x}^m(m)\tilde{x}(1) \quad = \quad 1_R \cdot 1_R \quad = \quad 1_R \quad ,$$

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

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

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

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

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 $n \neq m$. □

(4.14) Lemma Für jedes $f \in P_R \setminus \{\tilde{0}_{PR}\}$ gilt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, a_1, ..., a_n \in R$, so dass $a_n \neq 0_R$ und $f = \tilde{a}_n\tilde{x}^n \oplus ... \oplus \tilde{a}_1\tilde{x} \oplus \tilde{a}_0$ ist.

Beweis: Zum Nachweis der *Existenz* sei $f \in P_R \setminus \{\tilde{0}_{PR}\}$ 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 $g = \tilde{a}_n\tilde{x}^n \oplus ... \oplus \tilde{a}_1\tilde{x} \oplus \tilde{a}_0$. Dann gilt für $0 \leq k \leq n$ jeweils

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

wobei im zweiten Schritt (4.13) 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 $b_0, ..., b_m \in R$, so dass $b_m \neq 0_R$ und

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

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 $0 \leq k \leq n$. □

Beweis von Satz (4.7):

Sei $\phi : R \to P_R$ 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 1_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 $n > 0$ 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 $a = \phi(a)(0) = \tilde{0}(0) = 0_R$.

Wir können nun (4.3) auf den Monomorphismus ϕ anwenden. Wir erhalten einen Erweiterungsring von R, den wir mit $R[x]$ bezeichnen, und einen Isomorphismus $\hat{\phi} : R[x] \to P_R$ 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 (4.14) gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte $a_0, ..., a_n \in R$ mit $a_n \neq 0_R$, so dass

$$\tilde{f} \quad = \quad \tilde{a}_n\tilde{x}^n \oplus \ ... \ \oplus \tilde{a}_1\tilde{x} \oplus \tilde{a}_0 \qquad \text{gilt.}$$

Durch Anwendung von $\hat{\phi}^{-1}$ auf beide Seiten der Gleichung erhalten wir auf Grund der Homomorphismus-Eigenschaft die Gleichung $f = a_nx^n + ... + a_1x + a_0$. Aus der Eindeutigkeit von n und $a_0, ..., a_n$ für das Element $\tilde{f}$ folgt auch die Eindeutigkeit für das Element f. □

§ 5. *Euklidische Ringe*

Überblick

Bereits aus der Schulmathematik ist das Konzept der *Division mit Rest* bekannt: Gibt man zwei natürliche Zahlen a, b vor, so lassen sich immer Zahlen $q, r \in \mathbb{N}_0$ mit $a = qb + r$ und $0 \leq r < b$ finden. Der Rest r ist also stets kleiner als die Zahl b, durch die dividiert wurde. Ist $r = 0$, dann sagt man, dass die Division „glatt aufgeht“ . Ebenso ist aus der Schulmathematik bekannt, dass sich durch wiederholte Division mit Rest der größte gemeinsame Teiler zweier natürlicher Zahlen bestimmen lässt. Dieses Verfahren wird *Euklidischer Algorithmus* genannt.

Bei den *euklidischen Ringe* handelt es sich um eine Klasse von Ringen, auf die das Konzept der Division mit Rest übertragen werden kann. Um dieses für allgemeine Ringe formulieren zu können, ist es erforderlich, je zwei Ringelemente der „Größe“ nach vergleichbar zu machen. Nur dann ist gewährleistet, dass die Forderung, der Rest solle nach der Division kleiner sein als das Element, durch das geteilt wurde, überhaupt einen Sinn ergibt. Zu diesem Zweck stattet man euklidische Ringe mit einer sog. *Höhenfunktion* aus. Unter anderem auf Grund des Eukldischen Algorithmus sind eukldische Ringe expliziten Berechnungen besser zugänglich als andere Ringe. Dies ist ein Grund, weshalb wir sie zu einem so frühen Zeitpunkt behandeln. Außerdem besitzen euklidische Ringe algebraische Eigenschaften, mit denen wir uns später ausführlich beschäftigen werden: Sie sind Hauptidealringe und damit insbesondere auch faktoriell.

In diesem Abschnitt definieren wir zunächst Teiler und auch das Konzept des ggT und kgV für allgemeine Ringe. Dann werden die euklidischen Ringe definiert und eine Reihe konkreter Beispiele betrachtet. Anschließend formulieren wir den Euklidischen Algorithmus in diesem allgemeinen Kontext, beweisen seine Korrektheit und behandeln auch hierzu einige Beispiele.

Wichtige Begriffe und Konzepte:

- Teilerrelation | auf beliebigen Ringen, assoziierte Elemente
- Definition von ggT und kgV in beliebigen Ringen
- Höhenfunktion auf einem Ring, Definition euklidischer Ringe
- Beispiele für euklidische Ringe:
  Ring $\mathbb{Z}$ der ganzen Zahlen, Polynomring $K[x]$ für beliebige Körper K, Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen
- Euklidischer Algorithmus

(5.1) Definition 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.

In Integritätsbereichen lässt sich die Relation „assoziiert“ auch folgendermaßen beschreiben.

(5.2) Lemma 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: „⇐“ Aus $b = \varepsilon a$ folgt $a|b$, und wegen $a = \varepsilon^{-1} b$ gilt auch $b|a$.

„⇒“ 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.□ □

(5.3) Definition Sei R ein Ring mit $a_1, ..., a_n \in R$. Wir sagen, ein Element $d \in R$ ist ein ***größter gemeinsamer Teiler*** (kurz ggT) von $a_1, ..., a_n$, 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 $a_1, ..., a_n$ ***teilerfremd***, wenn 1_R ein ggT der Elemente ist.

(5.4) Definition Sei R ein Ring mit $a_1, ..., a_n \in R$. Ein Element $e \in R$ heißt ***kleinstes gemeinsames Vielfaches*** (kurz kgV) von $a_1, ..., a_n$, 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 $d = \mathrm{ggT}(a_1, ..., a_n)$, um auszudrücken, dass d ein ggT von $a_1, ..., a_n$ ist. Dabei handelt es sich aber um keine Gleichung im herkömmlichen Sinn, weil der ggT im allgemeinen nicht eindeutig bestimmt ist. Statt dessen gilt

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

Beweis: Sei d' ein weiterer ggT von $a_1, ..., a_n$. Nach Voraussetzung gilt $d'|a_i$ für $1 \leq i \leq n$. Weil nach Voraussetzung $d = \mathrm{ggT}(a_1, ..., a_n)$ 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 $d = \mathrm{ggT}(a_1, ..., a_n)$, 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 $a_1, ..., a_n$ handelt. Für das kleinste gemeinsame Vielfache verläuft der Beweis völlig analog. □

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.

(5.6) Definition Eine ***Höhenfunktion*** auf einem Integritätsbereich R ist eine Abbildung $h : R \setminus \{0_R\} \to \mathbb{N}$ 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 $R \setminus \{0_R\} \to \mathbb{N}_0$, 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.

Beipiel 1: Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein euklidischer Ring. Die Abbildung $h : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ 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. (Für jedes $x \in \mathbb{R}$ ist $\langle x \rangle$ die kleinste ganze Zahl z mit $z \leq x < z + 1$.) Auf Grund der Definition der unteren Gaußklammer $\lfloor\ \rfloor$ 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 $q_1, r_1 \in R$ 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 $h(r) = h(r_1) < h(b_1) = h(b)$. □

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

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

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

Durch vollständige Induktion über $n \in \mathbb{N}_0$ zeigen wir: Ist $f \in K[x]$ mit $n = \mathrm{grad}(f)$, dann gibt es ein $q \in K[x]$, so dass für $r = f - qg$ entweder $r = 0$ oder $\mathrm{grad}(r) < m$ 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

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

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 $\mathrm{grad}(r) < m$ 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 $\mathrm{grad}(r) < \mathrm{grad}(g)$. □

(5.7) Definition 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.

(5.8) Folgerung 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 geeignetes Polynom $g \in K[x]$.

(ii) Ist $\mathrm{grad}(f) = n$ 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 $\mathrm{grad}(r) < \mathrm{grad}(x-a) = 1$. 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 $a_1, ..., a_r$ die verschiedenen Nullstellen von f, wobei $r \in \mathbb{N}_0$ ist. Im Fall $r = 0$ ist die Aussage $r \leq \mathrm{grad}(f)$ 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 $\mathrm{grad}(g) = n$ 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. □

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

$$d \quad = \quad xa + yb.$$

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

(5.9) Lemma Sei R ein Ring, und seien $a, b, q \in R$ mit $b \neq 0$. Dann gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(a - qb, b)$. Genauer ausformuliert: 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: „⇒“ Sei d ein größter gemeinsamer Teiler von a und b. Dann gibt es $c_1, c_2 \in R$ mit $a = c_1 d$ und $b = c_2 d$. Es folgt $a - qb = c_1 d - q c_2 d$, 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 $a - qb = c_3 e$ und $b = c_4 e$. Man erhält $a = (a - qb) + qb = c_3 e + c_4 e = (c_3 + c_4)e$. Also ist e ein gemeinsamer Teiler von a und b, und aus $d = \mathrm{ggT}(a, b)$ folgt $e|d$. Damit haben wir gezeigt, dass d ein größter gemeinsamer Teiler von $a - qb$ und b ist. Die Beweisrichtung „⇐“ funktioniert analog. □

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 $d = \mathrm{ggT}(a, b)$ 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
$a_{n-1} = q a_n + r$ und $r = 0$ oder $h(r) < h(a_n)$.
Definere $(a_{n+1}, x_{n+1}, y_{n+1}) = (r, x_{n-1} - q x_n, y_{n-1} - q y_n)$.
Wiederhole Schritt 2.

(5.10) Satz 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 $d = \mathrm{ggT}(a, b)$ 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 $a_{n-1} = q a_n + r$ sind. Wir erhalten also eine unendliche absteigende Folge

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

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

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

erfüllt ist. Für $k = 2$ haben wir nach Definition $a_1 = a$ und $a_2 = b$, also ist die Gleichung $\mathrm{ggT}(a_1, a_2) = \mathrm{ggT}(a, b)$ 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

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

wobei wir im zweiten Schritt (5.9) und im letzten Schritt die Induktionsvoraussetzung angwendet haben. Nun beweisen wir noch durch vollständige Induktion die Gleichung

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

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 $a_{k+1} - qa_k$, $x_{k+1} = x_{k-1} - qx_k$ und $y_{k+1} = y_{k-1} - qy_k$ erfüllt sind. Es folgt

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

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

Als Anwendungbeispiel 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 $\mathrm{ggT}(a, b) = 6 = 36a + (-439)b$. (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

$$\mathrm{ggT}(f,g) \quad = \quad 2x - 6 \quad = \quad (\tfrac{1}{2}x - \tfrac{1}{2})f + (-\tfrac{1}{2}x^2 - \tfrac{1}{2}x + 1)g.$$

Wir haben in (3.5) 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 $N : \mathbb{C} \to \mathbb{R}$ 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 $h : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$.

(5.11) Proposition 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

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

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

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

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

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

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

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 sezten $q = r_0 + s_0 i$.

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

Zum Schluss 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 allerdings noch die Grundlagen, um dies zu beweisen.

§ 6. *Ideale*

Überblick

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; bei Letzterem ist zu beachten, dass es sich *nicht* um das elementweise Produkt der Ideale handelt, sondern um das von den elementweisen Produkten erzeugte Ideal. Als besonders wichtige Idealtypen lernen wir die ***Primideale*** und die ***maximalen Ideale*** kennen. Zum Schluss betrachten wir das Verhalten von Idealen unter Ringhomomorphismen.

Wichtige Begriffe und Konzepte

- Definition der Ideale eines Rings (wichtiger Spezialfall: Hauptideale)
- Erzeugendensysteme eines Ideals
- Rechenoperationen für Ideale (Summen, Produkte)
- Primideale und maximale Ideale
- Urbilder von Idealen unter Ringhomomorphismen sind Ideale
  (Bilder von Idealen im Allgemeinen nicht)

(6.1) Definition 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 $ra \in I$.

Für jede natürliche Zahl ist die Menge $n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\}$ ein Ideal in $\mathbb{Z}$. Allgemeiner gilt: Ist R ein Ring und $b \in R$, dann ist die Menge der Vielfachen $\{ab \mid b \in R\}$ von b ein Ideal in R. Man nennt solche Ideale ***Hauptideale*** und bezeichnet sie mit (a). Ein Integritätsbereich wird ***Hauptidealring*** genannt, wenn jedes Ideal in R 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. Ähnlich wie für Untergruppen, Normalteiler und Teilringe gilt auch für die Ideale

> **(6.2) Proposition** 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 $ra \in I$. □

Wie die Ringelemente können auch Ideale addiert und multipliziert werden.

> **(6.3) Proposition** 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 $ra = ra' + ra'' \in I + J$. □

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 (3.4).

> **(6.4) Definition** 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

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

die Bedingungen (i) und (ii) aus (6.4) 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, $S = \{a_1, ..., a_n\}$, dann verwendet man an Stelle von (S) auch die Schreibweise $(a_1, ..., a_n)$ für das erzeugte Ideal. Der folgende Satz gibt an, wie die Elemente eines solchen Ideals konkret aussehen.

(6.5) Proposition Sei R ein Ring, und seien $a_1, ..., a_n \in R$. Dann gilt

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

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

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

gilt. Wir erhalten

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

Damit ist die Idealeigenschaft von I bewiesen. Außerdem enthält I die Menge S. Ist nämlich $j \in \{1, ..., n\}$, 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 $r_1, ..., r_n \in R$ beliebig gewählt, dann enthält J auf Grund der Idealeigenschaft die Elemente $r_1 a_1, ..., r_n a_n$, 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. □

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

(6.6) Lemma 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 $(T) \subseteq (S)$. □

Nun können wir definieren

(6.7) Definition 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.

(6.8) Proposition Sei R ein Ring, und seien I, J von endlichen vielen Ringelementen erzeugte Ideale, $I = (a_1, ..., a_m)$ und $J = (b_1, ..., b_n)$ 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

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

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 (6.6) 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 $b = J$ mit $c = ab$. Wegen $I = (a_1, ..., a_m)$ gibt es Ringelemente $r_1, ..., r_m \in R$, so dass a in der Form $\sum_{i=1}^{m} r_i a_i$ geschrieben werden kann. Ebenso finden wir $s_1, ..., s_n \in R$ mit $b = \sum_{j=1}^{n} s_j b_j$. Es gilt also

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

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 (6.5) 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 $\mathrm{grad}(f) + \mathrm{grad}(g) = \mathrm{grad}(fg) = \mathrm{grad}(x) = 1$ jeweils $\mathrm{grad}(f), \mathrm{grad}(g) \leq 1$ folgen. Es gäbe also $a, b, c, d \in \mathbb{Z}$ mit $f = ax + b$ und $g = cx + d$. Wir würden dann

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

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 (6.8) ist das Produktideal IJ gegeben durch $IJ = (6, 2x, 3x, x^2)$. Mit (6.6) 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

> **(6.9) Lemma** Für Ideale I, J, K ein einem Ring R gilt das Distributivgesetz $I(J + K) = IJ + IK$, außerdem gilt $IJ \subseteq I$ und $IJ \subseteq J$.

Beweis: „⊆" 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. □

(6.10) Definition 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

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

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.

(6.11) Proposition 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 $a \in I$ oder $b \in J$. 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 $ab \in IJ \in \mathfrak{p}$. Wir haben also Elemente $a, b \in R$ mit $ab \in \mathfrak{p}$ und $a, b \notin \mathfrak{p}$ gefunden, im Widerspruch zur Primidealeigenschaft. □

An dieser Stelle kommen wir auf die zu Anfang erwähnte Beziehung zwischen Idealen und Teilbarkeitslehre zurück. Für viele wichtige zahlentheoretische Problem (etwa Fermats letzten 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

$$21 \quad = \quad 3 \cdot 7 \quad = \quad (1+2\sqrt{-5})(1-2\sqrt{-5}). \tag{6.1}$$

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 (6.1) irreduzibel sind, lassen sich die entsprechenden Hauptideale weiter zerlegen Mit Hilfe von (6.6) und (6.8) berechnet man zum Beispiel

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

Dabei gilt die Gleichung im vierten Schritt wegen (6.6) 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

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

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

(6.12) Definition Sei $\phi : R \to S$ Ringhomomorphismus. Dann nennt man $\ker(\phi) = \phi^{-1}(\{0_S\})$ den ***Kern*** und $\mathrm{im}(\phi) = \phi(R)$ 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.

(6.13) Proposition Seien R, S Ringe und $\phi : R \to S$ 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 $\iota : \mathbb{Z} \to \mathbb{Q}$, $a \mapsto a$, 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 $\mathrm{im}(\phi)$ eines Ringhomomorphismus $\phi : R \to S$ zwar im allgemeinen kein Ideal, aber immer ein Teilring von S ist. Wie bei den Gruppen oder den linearen Abbildungen zeigt man, dass ein Homomorphismus $\phi : R \to S$ genau dann injektiv ist, wenn $\ker(\phi) = \{0_R\}$ gilt.

§ 7. *Faktorringe und Restklassenringe*

Überblick

In der Gruppentheorie haben wir aus einer Gruppe G und einem Normalteiler $N \trianglelefteq G$ 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 $n \in \mathbb{N}$ einen Ring $\mathbb{Z}/n\mathbb{Z}$ mit n Elementen, den sog. ***Restklassenring*** modulo n, von deren Nützlichkeit wir uns schon im Einführungskapitel überzeugen konnten. 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 Definitionen und Sätze

- Konstruktion des Faktorrings R/I für einen Ring R und ein Ideal I
- Definition des kanonischen Epimorphismus $\pi_I : R \to R/I$
- Homomorphie- und Korrespondenzsatz für Ringe
- Faktorringe von Primidealen sind Integritätsbereiche, Faktorringe von maximalen Idealen 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.

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

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

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.

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

$$a \equiv b \bmod I \quad \Leftrightarrow \quad b - a \in I$$

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

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

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

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

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

$$a \equiv b \bmod I \quad \Leftrightarrow \quad b - a \in I \quad \Leftrightarrow \quad a + I = b + I \quad \Leftrightarrow \quad b \in a + I. \tag{7.2}$$

Ein wichtiger Speziallfall 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.

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

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

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 $0 \le a < n$. Es gilt also $b - a = nq \in (n)$, und auf Grund der Äquivalenz (7.2) 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 $0 \le a < n$ verschieden sind, seien $a_1, a_2 \in \mathbb{Z}$ mit $0 \le a_1, a_2 < n$ und $\bar{a}_1 = \bar{a}_2$ vorgegeben. Nach (7.2) 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 $a_1 = a_2$. □

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

(7.4) Definition Sei R ein Ring und $I \subseteq R$ ein Ideal. Eine Teilmenge $S \subseteq R$ wird ***Repräsentantensystem*** von R/I genannt, wenn die Abbildung $S \to R/I$, $r \mapsto r + I$ bijektiv ist. Jede Nebenklasse in R/I enthält also genau ein Element aus S.

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

> **(7.5) Proposition** Sei K ein Körper, $R = K[x]$ und $f \in K[x]$ ein Polynom vom Grad $n \geq 1$. Dann ist die Teilmenge $S = \{g \in K[x] \mid g \neq 0, \mathrm{grad}(g) < n\} \cup \{0\}$ von $K[x]$ ein Repräsentantensystem von $R/(f)$.

Beweis: Sei $\phi : S \to K[x]/(f)$ gegeben durch $g \mapsto g + (f)$. 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 $\mathrm{grad}(f) < n$. 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 $\mathrm{grad}(g_i) < n$ für $i = 1, 2$ ist das jedoch ausgeschlossen. Also muss $g_1 = g_2$ gelten. □

> **(7.6) Proposition** Sei R ein Ring und I ein Ideal. Dann gibt es (eindeutig bestimmte) Verknüpfungen $+$ und $\cdot$ auf R/I mit der Eigenschaft
>
> $$(a + I) + (b + I) = (a + b) + I \quad \text{und} \quad (a + I) \cdot (b + I) = ab + I \qquad \text{für alle} \quad a, b \in R.$$

Beweis: Die Eindeutigkeit der Verknüpfungen ist offensichtlich, denn durch die beiden Gleichungen sind die Abbildungen $+$ und $\cdot$ auf allen Paaren in $(R/I) \times (R/I)$ festgelegt. Zum Nachweis der Existenz sei $S \subseteq R$ ein Repräsentantensystem von R/I. Sind $\bar{a}, \bar{b} \in R/I$ vorgegeben, dann gibt es eindeutig bestimmte Elemente $a_0, b_0 \in S$ mit $\bar{a} = a_0 + I$ und $\bar{b} = b_0 + I$. Wir definieren dann die Verknüpfungen $+$ und $\cdot$ auf R/I durch

$$\bar{a} + \bar{b} = (a_0 + b_0) + I \qquad \text{und} \qquad \bar{a} \cdot \bar{b} = a_0 b_0 + I.$$

Seien nun $a, b \in R$. Zunächst beweisen wir die Gleichung $(a + I) + (b + I) = (a + b) + I$. Seien $a_0, b_0 \in S$ die eindeutig bestimmten Elemente mit $a_0 \in a+I$ und $b_0 \in b+I$. Es folgt $a+I = a_0+I$, $b+I = b_0+I$, insbesondere gibt es Elemente $i, j \in I$ mit $a = a_0 + i$ und $b = b_0 + j$. Nach Definition ist $(a + I) + (b + I) = (a_0 + b_0) + I$, wir müssen also $(a_0+b_0)+I = (a+b)+I$ zeigen. Nun gilt $a+b = (a_0+i)+(b_0+j) = (a_0+b_0)+(i+j) \in (a_0+b_0)+I$, also ist die Gleichung $(a_0 + b_0) + I = (a + b) + I$ tatsächlich erfüllt.

Nun zeigen wir noch, dass auch $(a + I) \cdot (b + I) = ab + I$ gilt. Nach Definition ist $(a + I) \cdot (b + I) = a_0 b_0 + I$, wir müssen also $a_0 b_0 + I = ab + I$ zeigen. Die Rechnung

$$ab - a_0 b_0 \quad = \quad ab - ab_0 + ab_0 - a_0 b_0 \quad = \quad a(b - b_0) + (a - a_0)b_0 \quad = \quad aj + ib_0 \in I$$

zeigt, dass dies tatsächlich der Fall ist. □

> **(7.7) Satz** 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 $\pi_I : R \to R/I$ 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. □

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 Verknüpfungstafeln gegeben.

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

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

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.

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

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

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 $\bar{3}\cdot\bar{4} = \overline{12} = \bar{4}$, 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.

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

Beweis: „⇒“ 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 $\bar{r}, \bar{s} \neq 0$ und $\bar{r}\bar{s} = \bar{n} = \bar{0}$. Dies zeigt, dass $\mathbb{Z}/n\mathbb{Z}$ kein Integritätsbereich ist. Nach (2.4) ist $\mathbb{Z}/n\mathbb{Z}$ damit auch kein Körper.

„⇐“ 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. □

Ist p eine Primzahl, dann verwendet man für den Körper $\mathbb{Z}/p\mathbb{Z}$ auch die Bezeichung $\mathbb{F}_p$. (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.

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

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

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

wobei im zweiten Schritt verwendet wurde, dass $(-1)(x^2 + 1)$ in I liegt. Man überprüft leicht, dass durch $\phi : \mathbb{R} \to R/I$, $a \mapsto a + I$ 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 $\deg(x^2 + 1)$ ist dies nur für $a = 0$ möglich. Mit Hilfe von (4.3) erhält nun man einen Erweiterungsring C von $\mathbb{R}$ und einen Isomorphismus $\hat{\phi} : C \to R/I$ mit $\hat{\phi}|_{\mathbb{R}} = \phi$. Für das Element $i = \hat{\phi}^{-1}(x+I)$ gilt

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

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.

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

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

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

Beweis: Die Eindeutigkeit von $\bar{\phi}$ ist offensichtlich, da durch die Gleichung $\bar{\phi}(a+I) = \phi(a)$ die Bilder sämtlicher Elemente in R/I unter $\bar{\phi}$ eindeutig festgelegt sind. Zum Beweis der Existenz wählen wir ein Repräsentantensystem $S \subseteq R$ von R/I. Ist nun ein Element $\bar{a} \in R/I$ vorgegeben und a das eindeutig bestimmte Element in S mit $\bar{a} = a + I$, dann definieren wir $\bar{\phi}(\bar{a}) = \phi(a)$.

Zu zeigen ist nun, dass für alle $a' \in R$ die Gleichung $\bar{\phi}(a' + I) = \phi(a')$ erfüllt ist. Sei $a' \in R$ beliebig und $a \in S$ das eindeutig bestimmte Element mit $a + I = a' + I$. Dann gilt nach Definition $\bar{\phi}(a' + I) = \phi(a)$, wir müssen also $\phi(a) = \phi(a')$ zeigen. Wegen $a + I = a' + I$ ist $a' - a$ in $I \subseteq \ker(\phi)$ enthalten. Also gilt $\phi(a') = \phi(a + a' - a) = \phi(a) + \phi(a' - a) = \phi(a) + 0 = \phi(a)$.

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. □

(7.10) Satz *(Homomorphiesatz für Ringe)*

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

Beweis: Auf Grund der Proposition existiert ein Homomorphismus $\bar{\phi} : R/I \to R'$ mit $\bar{\phi}(a + I) = \phi(a)$ für alle $a \in R$. Insbesondere gilt $\mathrm{im}(\phi) = \mathrm{im}(\bar{\phi})$, so dass durch $\bar{\phi}$ ein surjektiver Homomorphismus auf $\mathrm{im}(\phi)$ 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. □

(7.11) Satz *(Korrespondenzsatz für Ideale)*

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

(i) Die Zuordnungen $\phi : \mathscr{I}_I \to \bar{\mathscr{I}}$, $J \mapsto \pi(J)$ und $\psi : \bar{\mathscr{I}} \to \mathscr{I}_I$, $\bar{J} \mapsto \pi^{-1}(J)$ sind bijektiv und zueinander invers.

(ii) Für alle Ideale $J, K \in \mathscr{I}_I$ gilt $J \subseteq K \Leftrightarrow \pi(J) \subseteq \pi(K)$.

Beweis: zu (i) Zum Nachweis von $\psi \circ \phi = \mathrm{id}_{\mathscr{I}_I}$ muss für jedes $J \in \mathscr{I}_I$ 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 $\phi \circ \psi = \mathrm{id}_{\mathscr{I}}$ 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) $J = \pi^{-1}(\pi(J)) \subseteq \pi^{-1}(\pi(K)) = K$. □

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

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

Beweis: „⇒“ 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 $(0) \neq (1)$.

„⇐“ 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. □

(7.13) Satz 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: „⇒“ 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 $\bar{b} = 0 + \mathfrak{p}$.

„⇐“ 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. □

(7.14) Folgerung Jedes maximale Ideal ist ein Primideal.

Beweis: Dies folgt direkt aus (7.13), da jeder Körper ein Integritätsbereich ist. □

§ 8. *Der Chinesische Restsatz*

Überblick

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 $x \equiv 3 \bmod 5$ und $x \equiv 4 \bmod 7$ die Lösung $x =$. 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 (5.8) ausgeschlossen ist.

(8.1) Definition Zwei Ideale I, J in einem Ring R werden ***teilerfremd*** genannt, wenn $I + J = (1)$ gilt.

Diese Bezeichnung wird durch das folgende Lemma gerechtfertigt.

(8.2) Lemma 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. □

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

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

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

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

Beweis: Wir beweisen die Aussage durch vollständige Induktion über R und beginnen mit dem Fall $m = 2$. Nach (6.9) 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

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

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 $I_1, ..., I_{m+1}$ paarweise teilerfremde Ideale. Sei $J = I_1 \cdot ... \cdot I_m$. Nach (8.3) sind J und I_{m+1} teierfremd. Die Induktionsvoraussetzung liefert also

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

(8.5) Satz *(Chinesischer Restsatz)*

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

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

Beweis: Sei $\phi : R \to (R/I_1) \times ... \times (R/I_m)$ gegeben durch $\phi(a) = (a + I_1, ..., a + I_m)$. Nach (8.4) gilt $I = I_1 \cap ... \cap I_m$. 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 (7.9) gibt es einen Homomorphismus

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

mit $\bar{\phi}(a + I) = (a + I_1, ..., a + I_m)$, 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

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

und ebenso

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

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 $I_1, ..., I_{m+1}$ teilerfremde Ideale und das Element

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

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 $J = I_1 \cdot ... \cdot I_m$ und I_{m+1} sind nach (8.3) 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 $\phi(a) = (a_1 + I_1, ..., a_{m+1} + I_{m+1})$. $\square$

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

$$a \equiv 0 \bmod 2 \quad , \quad a \equiv 2 \bmod 3 \quad , \quad a \equiv 4 \bmod 5$$

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

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

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

$$x \equiv 15 \bmod 59 \quad , \quad x \equiv 20 \bmod 73.$$

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

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

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

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

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

$$-929 \equiv 15 \bmod 59 \qquad \text{und} \qquad -929 \equiv 20 \bmod 73. \qquad \square$$

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

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

Sei $a \in \mathbb{Z}$ und $\bar{a} = a + 35\mathbb{Z} \in \mathbb{Z}/35\mathbb{Z}$. Ist $\phi : \mathbb{Z}/35\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ der Isomomorphismus 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

$$f(\bar{a}) = 0 \quad \Leftrightarrow \quad \bar{a}^2 - \bar{a} = \bar{0} \quad \Leftrightarrow \quad \phi(\bar{a})^2 - \phi(\bar{a}) = \phi(\bar{0}) \quad \Leftrightarrow$$

$$(a + 5\mathbb{Z}, a + 7\mathbb{Z})^2 - (a + 5\mathbb{Z}, a + 7\mathbb{Z}) = (0 + 5\mathbb{Z}, 0 + 7\mathbb{Z})$$

$$\Leftrightarrow \quad (a + 5\mathbb{Z})^2 - (a + 5\mathbb{Z}) = 0 + 5\mathbb{Z} \ \wedge \ (a + 7\mathbb{Z})^2 - (a + 7\mathbb{Z}) = 0 + 7\mathbb{Z}.$$

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

$$(a + 5\mathbb{Z})^2 - (a + 5\mathbb{Z}) = 0 + 5\mathbb{Z} \ \wedge \ (a + 7\mathbb{Z})^2 - (a + 7\mathbb{Z}) = 0 + 7\mathbb{Z} \quad \Leftrightarrow$$

$$a + 5\mathbb{Z} \in \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}\} \ \wedge \ a + 7\mathbb{Z} \in \{0 + 7\mathbb{Z}, 1 + 7\mathbb{Z}\}$$

$$\Leftrightarrow \quad (a + 5\mathbb{Z}, a + 7\mathbb{Z}) \ \in \ \{ \, (0 + 5\mathbb{Z}, 0 + 7\mathbb{Z}) \, , \, (1 + 5\mathbb{Z}, 0 + 7\mathbb{Z}) \, , \, (0 + 5\mathbb{Z}, 1 + 7\mathbb{Z}) \, , \, (1 + 5\mathbb{Z}, 1 + 7\mathbb{Z}) \} \, .$$

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 $\phi(\overline{21}) = (1 + 5\mathbb{Z}, 0 + 7\mathbb{Z})$ und $\phi(\overline{15}) = (0 + 5\mathbb{Z}, 1 + 7\mathbb{Z})$. Daraus folgt

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

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

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

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

§ 9. *Die Struktur der primen Restklassengruppen*

Überblick

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. Unter anderem kann mit den Strukturaussagen dieses Kapitels die Korrektheit des RSA-Verfahrens nachgewiesen werden (siehe § 1).

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 $C_1 \times ... \times C_r$ 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.

Wichtige 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 allgmeinen Bemerkung zu den Einheiten in beliebigen Ringen.

(9.1) Lemma Seien R und S Ringe. Dann gilt

(i) $(R \times S)^\times = R^\times \times S^\times$

(ii) Ist $\phi : R \to S$ 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 Elememte $c \in R$ 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 $\phi(R^\times) = S^\times$. □

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 $n \in \mathbb{N}$.

(9.2) Proposition 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 $m_1, ..., m_r \in \mathbb{N}$ mit

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

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 $\ell = \mathrm{kgV}(m_1, ..., m_r)$ übereinstimmt. Nach Definition des Exponenten gilt $mg = 0_G$ für $g \in G$. Insbesondere gilt

$$m(1 + m_1\mathbb{Z}, ..., 1 + m_r\mathbb{Z}) = 0_G \quad \Leftrightarrow \quad (m + m_1\mathbb{Z}, ..., m + m_r\mathbb{Z}) = (m_1\mathbb{Z}, ..., m_r\mathbb{Z}) \quad \Leftrightarrow$$

$$m + m_k\mathbb{Z} = m_k\mathbb{Z} \text{ für } 1 \leq k \leq r \quad \Leftrightarrow \quad m_k | m \text{ für } 1 \leq k \leq r.$$

Also ist m jedenfalls ein gemeinsames Vielfaches von $m_1, ..., m_r$ und damit auch ein Vielfaches von ℓ. Weil ℓ ein Vielfaches von $m_1, ..., m_r$ ist, gilt andererseits für alle $a_1, ..., a_r \in \mathbb{Z}$ 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

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

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

(9.3) Satz Sei K ein Körper und U eine endliche Untergruppe der multiplikativen Gruppe $K^\times$. Dann ist U zyklisch. Inbesondere 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 $\mathrm{ord}(a)$ 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 (5.8) höchstens d Nullstellen besitzen. Daraus folgt $n \leq d$, insgesamt $n = d$. Nach (9.2) gibt es in U ein Element der Ordnung n. Also ist U zyklisch. □

(9.4) Proposition 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 $\mathrm{ggT}(a, n) = 1$ 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: „⇒“ 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.

„⇐“ 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. □

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

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

Für eine Primzahl p ist $\varphi(p) = p - 1$, denn in diesem Fall ist $\mathbb{Z}/p\mathbb{Z}$ nach (7.8) 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.

(9.5) Folgerung 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 (9.3) zyklisch, damit isomorph zu $\mathbb{Z}/(p - 1)\mathbb{Z}$. □

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 $\bar{3}^{21} = \overline{42}$, $\bar{3}^{14} = \overline{36}$ und $\bar{3}^6 = \overline{41}$, also haben wir mit $\bar{a} = \bar{3}$ eine Primitivwurzel modulo 43 gefunden. Tatsächlich erhält man, wenn man die Potenzen $\bar{a}^1$, $\bar{a}^2$, $\bar{a}^3$, ... der Reihe nach aufschreibt, die Elemente

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

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

$$\bar{3}^1 = \bar{3} \quad , \quad \bar{3}^2 = \bar{9} \quad , \quad \bar{3}^4 = (\bar{3}^2)^2 = \bar{9}^2 = \overline{81} = \overline{38} \quad , \quad \bar{3}^8 = (\bar{3}^4)^2 = (\overline{38})^2 = (-\bar{5})^2 = \overline{25} \quad ,$$

$$\bar{3}^{16} = (\bar{3}^8)^2 = (\overline{25})^2 = \overline{625} = \overline{195} = \overline{23}$$

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

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

(9.6) Proposition 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 (9.1) gilt

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

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

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

und somit insbesondere $\varphi(15) = 8$. Denn nach dem Chinesischen Restsatz und (9.1) gilt zunächst $(\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$. 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 (9.5).

(9.7) Lemma

(i) Sei p eine ungerade Primzahl und $m \in \mathbb{N}$. Dann gilt $(1+p)^{p^{m-1}} \equiv 1 \bmod p^m$ und $(1+p)^{p^{m-1}} \not\equiv 1 \bmod p^{m+1}$.

(ii) Für alle $m \in \mathbb{N}$, $m \geq 2$ gilt $5^{2^{m-2}} \equiv 1 \bmod 2^m$ und $5^{2^{m-2}} \not\equiv 1 \bmod 2^{m+1}$.

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

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

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 $\sum_{j=2}^{p} \binom{p}{j} k^j p^{mj}$ also durch p^{m+2} teilbar, und wir erhalten $(1+p)^{p^m} \equiv 1 + kp^{m+1} \bmod p^{m+2}$. Es folgt $(1+p)^{p^m} \equiv 1 \bmod p^{m+1}$ und $(1+p)^{p^m} \not\equiv 1 \bmod p^{m+2}$.

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

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

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

(9.8) Satz

(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 $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$ für alle $m \geq 3$.

Beweis: zu (i) Wegen (9.5) 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 $r = \operatorname{ord}(\bar{a})$, dann gilt $\bar{a}^r = \bar{1}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$, also $a^r \equiv 1 \bmod p^m$ und erst recht $a^r \equiv 1 \bmod p$. 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 (9.7) (i) gilt $\bar{c}^{p^{m-2}} \neq \bar{1}$ und $\bar{c}^{p^{m-1}} = \bar{1}$ in $\bar{c}$ 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 (2.17) aus der Gruppentheorie und dem Chinesischen Restsatz folgt

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

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 (9.7) (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 $\operatorname{ord}(\bar{5}) = 2^{m-2}$. 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 $-1 \equiv 5^k \bmod 2^m$ für ein $k \in \mathbb{Z}$ gelten. Daraus wiederum würde wegen $5 \equiv 1 \bmod 4$ dann $-1 \equiv 5^k \equiv 1^k \equiv 1 \bmod 4$ folgen, im Widerspruch zu $-1 \not\equiv 1 \bmod 4$. 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 $(\mathbb{Z}/2^m\mathbb{Z})^\times = UV$. □

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 Rechung $\bar{2}^9 = \overline{26} \neq \bar{1}$ und $\bar{2}^6 = \overline{10} \neq \bar{1}$. Die Potenzen $\bar{a}^1, \bar{a}^2, \bar{a}^3, ...$ sind der Reihe nach gegeben durch

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

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

§ 10. Hauptidealringe und die Teilbarkeitsrelation

Überblick

Der Begriff des ***Hauptidealrings*** ist uns bereits aus § 6 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 das 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 Hauptidealringen 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 Definitionen, Konzepte und Sätze:

- idealtheoretische Interpretation der Teilbarkeitsrelation
- Euklidische Ringe sind Hauptidealringe.
- irreduzible Elemente und Primelemente eines Rings
- Jedes Primelement in einem Integritatsbereich ist ein irreduzibles Element.
  (Die Umkehrung ist im Allgemeinen falsch, für Hauptidealringe und allgemeiner faktorielle Ringe aber richtig.)
- In einem Hauptidealring entsprechen die Primelemente den maximalen Idealen. Die Primideale sind die maximalen Ideale zusammen mit dem Nullideal.

Bereits in § 6 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 ein Hauptidealring, denn nach (7.12) sind (0) und (1) die einzigen Ideale eines Körpers.

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

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

Beweis: Um zu sehen, dass $\mathfrak{p}$ kein Hauptideal ist, betrachten wir die ***Normfunktion*** $N : R \to \mathbb{N}_0$ 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 $N : \mathbb{C} \to \mathbb{R}_+$ aus Kapitel §3, es gilt also insbesondere $N(\alpha\beta) = N(\alpha)N(\beta)$ 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 $\mathrm{ggT}(9, 21) = 3$. Es folgt $N(\alpha) \in \{1, 3\}$. Betrachten wir zunächst den Fall $N(\alpha) = 3$. Schreibe 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

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

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.

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

(10.1) Satz 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) „⇒“ 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 $b \mid a$. „⇐“ Nach Voraussetzung gibt es ein $r \in R$ mit $a = rb$, also gilt $a \in (b)$. Also ist (b) ein Ideal, dass 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 $(e) = (e') = (a) \cap (b)$. □

(10.2) Satz 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 $I = (a)$. □

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.

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

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

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

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

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

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

(10.5) Satz In einem Integritätsbereich ist jedes Primelment 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. □

(10.6) Proposition 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. □

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

Beweis: „⇒“ 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 $\mathbb{Z}$.

„⇐“ 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. □

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 $N : \mathbb{C} \to \mathbb{R}_+$, 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.

(10.8) Proposition 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) „⇒“ 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. „⇐“ Sei $\alpha = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$. Nach Voraussetzung gilt

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

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. □

(10.9) Folgerung 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 (10.8). □

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 (10.8) (iii) irreduzibel, denn es gilt

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

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

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

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

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

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

(10.10) Proposition 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: „⇒“ 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 $b \in (p)$.

„⇐“ 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. □

(10.11) Satz Sei R ein Hauptidealring, aber kein Körper, und $p \in R$. Dann sind die folgenden Aussagen äquvialent.

(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) ⇒ (ii)“ Nach (10.5) ist jedes Primelment in einem Integritätsbereich irreduzibel.

„(ii) ⇒ (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) ⇒ (iv)“ Nach (7.14) 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 (7.12) würde das bedeuten, dass R ein Körper ist. Aber dies ist nach Voraussetzung ausgeschlossen.

“(iv) ⇒ (i)“ Das folgt aus (10.10). □

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 $R = \mathbb{Z}[\frac{1}{2}\sqrt{-19}]$ 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.

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

Beweis: In Satz (3.5) wurde gezeigt, dass die Elemente von R durch $R = \{\frac{1}{2}a+\frac{1}{2}b\sqrt{-19} \mid a, b \in \mathbb{Z}\,,\ a \equiv b \bmod 2\}$ 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 $a \equiv b \bmod 2$ ist

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

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 $a^2 \equiv b^2 \equiv 1 \bmod 4$ (wie wir bereits im Einführungsbeispiel aus § 1 festgestellt haben), und wegen $19 \equiv 3 \bmod 4$ folgt $a^2 + 19b^2 \equiv 1 + 3 \cdot 1 \equiv 4 \equiv 0 \bmod 4$.

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 $|\mathrm{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$ erfüllt ist. Dazu setzen wir $r = \frac{1}{\sqrt{19}}\mathrm{Im}(\rho)$ 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

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

und somit $\mathrm{Im}(\frac{\beta'}{\alpha}) = \sqrt{19}(r - \frac{1}{2}s)$ und $|\mathrm{Im}(\frac{\beta'}{\alpha})| \leq \frac{1}{4}\sqrt{19}$. Ersetzen wir also β durch β', dann ist $|\mathrm{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$ 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 $|\mathrm{Im}(\rho)| < \frac{1}{2}\sqrt{3}$ erfüllt ist. Wählen wir $a \in \mathbb{Z}$ so, das $|\mathrm{Re}(\rho) - a| \leq \frac{1}{2}$ 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 $\frac{1}{2}\sqrt{3} \leq |\mathrm{Im}(\rho)| \leq \frac{1}{4}\sqrt{19}$. 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 $\frac{1}{2}\sqrt{3} \leq \mathrm{Im}(\rho) \leq \frac{1}{4}\sqrt{19}$ annehmen. Es folgt dann $\sqrt{3} \leq \mathrm{Im}(2\rho) \leq \frac{1}{2}\sqrt{19}$ und $\sqrt{3} - \frac{1}{2}\sqrt{19} \leq \mathrm{Im}(2\rho - \frac{1}{2}(1 + \sqrt{-19})) = \mathrm{Im}(\frac{\delta}{\alpha}) \leq 0$. Wir wählen nun $a \in \mathbb{Z}$ so, dass $|\mathrm{Re}(2\rho - \frac{1}{2}(1 + \sqrt{-19})) - a| \leq \frac{1}{2}$ erfüllt ist und definieren $\gamma = \delta - a\alpha$. Dann gilt

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

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 $(\sqrt{3} - \frac{1}{2}\sqrt{19})^2 < \frac{3}{4}$. □

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

Beweis: Mit ähnlichen Argumenten wie in Prop. (10.8) 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 $a \equiv b \bmod 2$, 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 $a \equiv b \bmod 2$, 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 $h : R \setminus \{0\} \to \mathbb{N}$ 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

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

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. □

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 $N(a^2 + b\sqrt{d}) = |a^2 - db^2|$ zu tun hat. In [Ha] wird dies zum Beispiel für den Ring $\mathbb{Z}[\sqrt{14}]$ bewiesen.

§ 11. *Faktorielle Ringe*

Überblick

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 Begriffe und Konzepte:

- Definition der faktoriellen Ringe
- Eindeutigkeit der Primfaktorzerlegung bis auf Einheiten und Reihenfolge
- Definition einer eindeutigen Produktdarstellung
- Hauptidealringe sind faktoriell

(11.1) Definition 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 $p_1, ..., p_n \in R$, so dass

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

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 (5.1)).

(11.2) Lemma Sei R ein Integritätsbereich.

(i) Seien $a, a', b, b' \in R$, wobei $a \sim a'$, $b \sim b'$ und $a|b$ gilt. Dann gilt auch $a'|b'$.

(ii) Jedes Element in R, das eine Einheit teilt, ist selbst eine Einheit.

(iii) 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. □

(11.3) Proposition 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 $p = p_1 \cdot ... \cdot p_n$ von p als Produkt von Primlementen. Im Fall $n > 1$ könnten wir p damit als Produkt $p = p_1 \cdot (p_2 \cdot ... \cdot p_n)$ schreiben. Dabei ist p_1 eine Nicht-Einheit, ebenso das Produkt $p_2 \cdot ... \cdot p_n$ nach (11.2) (iii). Aber dies widerspricht der Irreduzibilität von p. Also ist $n = 1$ und $p = p_1$ ein Primelement. □

(11.4) Satz 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

$$p_1 \cdot ... \cdot p_m \quad = \quad r \quad = \quad q_1 \cdot ... \cdot q_n$$

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) ⇒ (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 (11.2) (i) $p|a$ 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 $a = p_1 \cdot ... \cdot p_m$ und $b = q_1 \cdot ... \cdot q_n$ erfüllt ist. Das Element c kann keine Einheit sein, denn sonst hätten wir eine Gleichung der Form

$(p_1 \cdot ... \cdot p_m)(q_1 \cdot ... \cdot q_n) = pc$, 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 $r_1 \cdot ... \cdot r_k$ mit irreduziblen Elementen r_i. Wir erhalten also eine Gleichung der Form

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

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 $i \in \{1, ..., m\}$, dann ist p ein Teiler von a. Gilt $p \sim q_j$ für ein $j \in \{1, ..., n\}$, 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

$$p_1 \cdot ... \cdot p_m \quad = \quad r \quad = \quad q_1 \cdot ... \cdot q_n$$

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 Umnummerierung p_i zu q_i assoziiert ist, für $1 \leq i \leq n$. Im Fall $n = 1$ gilt

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

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 $p_2 \cdot ... \cdot p_m$.

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

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

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

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

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

(11.5) Definition 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 $K[x]$.

(11.6) Folgerung 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

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

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 $f = q_1 \cdot ... \cdot q_m$ 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 $\varepsilon = \varepsilon_1 \cdot ... \cdot \varepsilon_m$, dann gilt also

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

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

$$v_p(f) \quad = \quad \big|\{i \in \{1, ..., m\} \;\big|\; p_i = p\}\big| \quad ,$$

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

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

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

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

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.

(11.7) Lemma 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

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

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

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

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

(11.8) Folgerung 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. □

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

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

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 $f_1, ..., f_m$. 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 (11.7) ein gemeinsamer Teiler von $f_1, ..., f_m$. 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. □

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

(11.10) Satz Jeder Hauptidealring R ist faktoriell.

Beweis: Wir wissen bereits, dass jedes irreduzible Element in einem Hauptidealring R auch ein Primelement ist ((10.11)). 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 $a_{n+1} = \varepsilon a_n = \varepsilon rs = \varepsilon a_{n+1} s$ 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 (10.1) (i) die Beziehung

$$(a_1) \quad \subsetneq \quad (a_2) \quad \subsetneq \quad (a_3) \quad \subsetneq \quad (a_4) \quad \subsetneq \quad \ldots$$

Wir zeigen, dass auch die Vereinigung $I = \bigcup_{n=1}^{\infty} (a_n)$ ein Ideal im Ring R ist. Wegen $0_R \in (a)$ 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 $ra_n \in (a_n)$, 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. In der Höheren Algebra beweist man den ***Hilbertschen Basissatz***, welcher besagt, dass für jeden faktoriellen Ring R auch der Polynomring $R[x]$ faktoriell ist. Daraus folgt dann 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 $(f) = I$, $f = a_n x^n + \ldots + a_1 x + a_0$ mit $a_0, \ldots, a_n \in \mathbb{Z}$. 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.

§ 12. *Irreduzibilitätskriterien und Gaußsches Lemma*

Überblick

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 Verfüfung stellen, wobei wir für die Herleitung auf die Theorie insbesondere der letzten beiden Kapitel zurückgreifen werden. Von besonderem Interesse ist für uns die Situtation, 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 Begriffe und Konzepte:

- Kriterium für die Nullstellen eines Polynoms $R[x]$ in K, wobei R einen faktoriellen Ring und K seinen Quotientenkörper bezeichnet
- Definition der primitiven Polynome über einem faktoriellen Ring R
- Formulierung und Beweis des Gaußschen Lemmas
- Irreduzibilität eines Polynoms über dem Ring R und seinem Quotientenkörper
- Eisenstein-Kriterium
- 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 $\operatorname{grad}(f) \in \{2, 3\}$ 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 weitere Verlauf des Kapitels vorstellen werden.

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

(i) Ist $\alpha \in K$ eine Nulstelle 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

$$f(\alpha) = 0 \quad \Leftrightarrow \quad a_n \alpha^n + \sum_{k=0}^{n-1} a_k \alpha^k = 0 \quad \Leftrightarrow \quad a_n \alpha^n = -\sum_{k=0}^{n-1} a_k \alpha^k \quad \Leftrightarrow \quad a_n (\tfrac{p}{q})^n = -\sum_{k=0}^{n-1} a_k (\tfrac{p}{q})^k$$

$$\Leftrightarrow \quad a_n p^n = -\sum_{k=0}^{n-1} a_k p^k q^{n-k} = q \left(-\sum_{k=0}^{n-1} a_k p^k q^{n-1-k} \right).$$

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

$$f(\alpha) = 0 \quad \Leftrightarrow \quad \sum_{k=1}^{n} a_k \alpha^k + a_0 = 0 \quad \Leftrightarrow \quad a_0 = -\sum_{k=1}^{n} a_k \alpha^k \quad \Leftrightarrow \quad a_0 = -\sum_{k=1}^{n} a_k (\tfrac{p}{q})^k$$
$$\Leftrightarrow \quad a_0 q^n = -\sum_{k=1}^{n} a_k p^k q^{n-k} = p\left(-\sum_{k=1}^{n} a_k p^{k-1} q^{n-k}\right).$$

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 $\mathrm{grad}(f) = 3$ 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, dass 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.

> **(12.2) Lemma** Sei R ein faktorieller Ring und K sein Quotientenkörper. Sind $a_1, ..., a_n \in K^\times$ beliebig vorgegeben, dann gibt ein $\alpha \in K^\times$, so dass die Elemente $a_i' = \alpha a_i$ in R liegen und $\mathrm{ggT}(a_1', ..., a_n') = 1$ 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 $\alpha = s_1 ... s_n$, dann liegt α in $K^\times$, und es gilt

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

Wir können also o.B.d.A. voraussetzen, das $a_i \in R$ für $1 \leq i \leq n$ gilt Sei nun $d = \mathrm{ggT}(a_1, ..., a_n)$, $\alpha = d^{-1}$ und $a_i' = \alpha a_i$ für $1 \leq i \leq n$. Angenommen, die Elemente $a_1', ..., a_n'$ sind nicht teilerfremd. Dann gibt es ein Primelement p mit $p | a_i'$ für $1 \leq i \leq n$. Es folgt $pd | a_i$ für $1 \leq i \leq n$ und somit $pd | d$ 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 $\mathrm{ggT}(a_1', ..., a_n') = 1$ erfüllt. □

> **(12.3) Definition** 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 $a_0, ..., a_n$ keinen gemeinsamen Primteiler besitzen.

Wir betrachten einige Beispiele.

(i) Normierte Polynome in $R[x]$, also Polynome der Form $x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ mit höchstem Koeffizienten 1 und ansonsten beliebigen Koeffizienten $a_0, ..., a_{n-1} \in R$, sind immer primitiv.

(ii) Das Polynom $2x^2 + 4x + 6$ ist nicht primitiv, denn es gilt $\mathrm{ggT}(2, 4, 6) = 2$.

(iii) Ist R ein Integritiätsbereich 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.

(12.4) Folgerung 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 (12.2), 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 $\pi : R \to \bar{R}$. 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.

(12.5) Lemma Der Homomorphismus $\phi : R[x] \to \bar{R}[x]$ 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 $\pi : R \to \bar{R}$ surjektiv ist, gilt dasselbe für ϕ. Außerdem ist $\mathfrak{p}[x]$ ist der Kern von ϕ. Also folgt die Aussage aus dem Homomorphiesatz. □

(12.6) Folgerung 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 (7.13) 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 (7.13) folgt daraus, dass $\mathfrak{p}[x]$ ein Primideal ist. □

(12.7) Satz *(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 (10.10) ist (p) in R ein Primideal, und nach (12.6) 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. □

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

(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 (12.4) 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 $\mathrm{ggT}(a, b) = 1$. Dann erhalten wir aus $f = g(\alpha^{-1}\tilde{h})$ Gleichung $af = bg\tilde{h}$. 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 $\tilde{g} = ag$ 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 $\tilde{g} = ag$ 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. □

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. Wir formulieren noch zwei Kriterien für die Irreduzibilität von Polynomen über Ringen.

(12.9) Satz *(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 $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ mit $a_0, ..., a_n \in R$, 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 $u \in \{1, ..., r\}$ mit $p \nmid b_u$. Nun gilt

$$a_u \quad = \quad \sum_{i=0}^{u} b_{u-i} c_i \quad ,$$

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 $\mathrm{grad}(g) = n = \mathrm{grad}(f)$ und $\mathrm{grad}(h) = 0$. Weil f primitiv ist, muss h in $R^\times$ liegen. Damit ist die Irreduzibilität von f in $R[x]$ bewiesen. □

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 (12.8) auch in $\mathbb{Q}[x]$ irreduzibel.

(12.10) Satz *(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 $\mathrm{grad}(f) = \mathrm{grad}(\bar{f})$, und damit muss auch $\mathrm{grad}(g) = \mathrm{grad}(\bar{g})$ und $\mathrm{grad}(h) = \mathrm{grad}(\bar{h})$ gelten.

Insbesondere sind $\bar{g}$ und $\bar{h}$ nicht konstant. Nun ist (p) wegen (10.10) ein Primideal in R und $\bar{R} = R/(p)$ damit nach Satz (7.13) (i) ein Integritätsbereich. Daraus folgt, dass die Einheiten im Polynomring $\bar{R}[x]$ genau die Einheiten in $\bar{R}$ sind, siehe (4.11). 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. □

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

$$\bar{f} \quad = \quad x^3 + x + \bar{1} \in \mathbb{F}_2[x]$$

hat in $\mathbb{F}_2$ keine Nullstelle (es gilt $\bar{f}(\bar{0}) = \bar{f}(\bar{1}) = \bar{1}$), wegen $\mathrm{grad}(\bar{f}) = 3$ ist es also irreduzibel. Auf Grund des Reduktionskriteriums ist f also in $\mathbb{Z}[x]$ irreduzibel, und mit Satz (12.8) erhalten wir die Irreduzibilität in $\mathbb{Q}[x]$.

§ 13. *Kreisteilungspolynome*

Überblick

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. Besonderen 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 § 12 zur Anwendung.

Wichtige Definitionen und Sätze:

- n-te Einheitswurzel, primitive n-Einheitswurzel
- Gruppe μ_n der Einheitswurzeln
- n-tes Kreisteilungspolynom
- Rekursionsformel zur Berechnung der Kreisteilungspolynome
- Irreduzibilität der Kreisteilungspolynome über $\mathbb{Q}$

(13.1) Definition Sei $n \in \mathbb{N}$. Eine (komplexe) ***n-te Einheitswurzel*** 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

$$\mu_n \quad = \quad \left\{ e^{2\pi i k/n} \;\middle|\; 0 \leq k < n \right\} \quad ,$$

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

$$\left(e^{2\pi i k/n} \right)^n \quad = \quad e^{2\pi i k} \quad = \quad 1$$

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 $\mu_n = \langle \zeta_n \rangle$.

(13.2) Lemma Sei $k \in \mathbb{Z}$. Genau dann gilt $\mu_n = \langle \zeta_n^k \rangle$, wenn $\mathrm{ggT}(k, n) = 1$ 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 $\mathrm{ggT}(k, n) = 1$. Das Lemma ist ein Spezialfall dieser Aussage. □

(13.3) Definition 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

$$\Phi_n \quad = \quad \prod_{\zeta \in \mu_n^\times} (x - \zeta)$$

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 (13.2) gilt für alle $n \geq 2$ jeweils

$$|\mu_n^\times| \quad = \quad |\{k \in \mathbb{Z} \mid 0 \leq k < n, \mathrm{ggT}(k, n) = 1\}| \quad = \quad \varphi(n) \quad ,$$

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.

(13.4) Lemma 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 $d = \mathrm{ord}(\zeta)$ von ζ in $\mathbb{C}^\times$ ist dann ein Teiler von n. Also erzeugt ζ erzeugt 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. □

(13.5) Satz 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 (13.4) gilt

$$x^n - 1 \quad = \quad \prod_{d|n} \Phi_d \quad .$$

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 $\mathrm{grad}(r) < \mathrm{grad}(g)$. 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 (12.8) 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 $\Phi_n = h \in \mathbb{Z}[x]$. □

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

$$x^p - 1 \quad = \quad \Phi_1 \Phi_p \quad = \quad (x-1)\Phi_p$$

und somit

$$\Phi_p \quad = \quad \frac{x^p - 1}{x - 1} \quad = \quad x^{p-1} + x^{p-2} + ... + x + 1.$$

Ist $q \in \mathbb{N}$ eine Primzahlpotenz, $q = p^r$ mit einer Primzahl p und $r \in \mathbb{N}$, $r \geq 2$, dann gilt

$$x^{p^r} - 1 \quad = \quad \prod_{d|p^r} \Phi_d \quad = \quad \left(\prod_{d|p^{r-1}} \Phi_d \right) \Phi_{p^r} \quad = \quad \left(x^{p^{r-1}} - 1 \right) \Phi_{p^r}$$

also

$$\begin{aligned} \Phi_{p^r} \quad = \quad \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} \quad = \quad \frac{(x^{p^{r-1}})^p - 1}{x^{p^{r-1}} - 1} \quad = \quad & \left(x^{p^{r-1}} \right)^{p-1} + \left(x^{p^{r-1}} \right)^{p-2} + \ ... \ + \left(x^{p^{r-1}} \right)^1 + \left(x^{p^{r-1}} \right)^0 \\ = \quad & x^{p^{r-1}(p-1)} + x^{p^{r-1}(p-2)} + \ ... \ + x^{p^{r-1}} + 1. \end{aligned}$$

Das sechste Kreisteilungspolynom berechnet man durch

$$\Phi_6 \quad = \quad \frac{x^6 - 1}{\Phi_1 \Phi_2 \Phi_3} \quad = \quad \frac{x^6 - 1}{(x-1)(x+1)(x^2 + x + 1)} \quad = \quad x^2 - x + 1 \quad ,$$

und das zwölfte Kreisteilungspolynom erhält man durch die Rechnung

$$\Phi_{12} \quad = \quad \frac{x^{12} - 1}{\Phi_1 \Phi_2 \Phi_3 \Phi_4 \Phi_6} \quad = \quad \frac{x^{12} - 1}{(x-1)(x+1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)} \quad = \quad x^4 - x^2 + 1.$$

Wir zeigen nun, dass die Kreisteilungspolynome über $\mathbb{Q}$ irreduzibel sind. Zur Vorbereitung bemerken wir

(13.6) Lemma 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 $a_0, ..., a_n \in \mathbb{F}_p$. 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

$$f^p \quad = \quad \left(\sum_{k=0}^{n} a_i x^p \right)^p \quad = \quad \sum_{k=0}^{n} a_i^p x^{ip} \quad = \quad \sum_{k=0}^{n} a_i x^{ip} \quad = \quad f(x^p). \qquad \square$$

(13.7) Satz 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 (12.8) (ii) auch in $\mathbb{Z}[x]$. Es gibt dann normierte Polynome $f, g \in \mathbb{Z}[x]$ mit $\Phi_n = fg$ und $\mathrm{grad}(f), \mathrm{grad}(g) > 1$, 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 (12.8) (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 (13.6) 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 $\Phi_n \mid (x^n - 1)$ 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 $\mathbb{F}_p^{\mathrm{alg}}$ von $\mathbb{F}_p$ mehrfache Nullstellen. Andererseits zeigt die Gleichung

$$\mathrm{ggT}(x^n - \bar{1}, (x^n - \bar{1})') \quad = \quad \mathrm{ggT}(x^n - \bar{1}, n x^{n-1}) \quad = \quad \bar{1} \quad ,$$

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 ζ^{p_1}, $\zeta^{p_1 p_2}$, $\zeta^{p_1 p_2 p_3}$, ..., ζ^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. $\square$

§ 14. *Das Quadratische Reziprozitätsgesetz*

Überblick

Mit dem Quadratische Reziprozitätsgesetz lässt sich die Lösbarkeit von Kongruenzen der Form $x^2 \equiv a \bmod p$ für eine vorgegebene Primzahl p und vorgegebenes $a \in \mathbb{Z}$ schnell entscheiden. Allgemeiner lassen sich damit auch quadratische Kongruenzen der Form $ax^2 + bx + c \equiv 0 \bmod p$ systematisch untersuchen. Das Gesetz gilt als einer der Meilensteine beim Aufbau der Algebraischen Zahlentheorie als eigenständigem Teilgebiet der Mathematik. Die Bemühungen, dieses Gesetz auf höhere Potenzen zu verallgemeinern, hatten eine starken Einfluss auf die weitere Entwicklung, und haben in den 1950er Jahren mit der Vollendung der *Klassenkörpertheorie* einen befriedigenden Abschluss gefunden. Für die Formulierung der meisten Aussagen benötigen wir aber nicht mehr als einfache Kongruenzrechnung. Der Beweis kann zum Beispiel mit Hilfe der Einheitswurzeln aus dem vorherigen Kapitel geführt werden.

Wichtige Definitionen und Sätze:

- quadratische Reste und quadratische Nichtreste modulo p
- Legendre- und Jacobi-Symbol
- Quadratisches Reziprozitätsgesetz und Ergänzungssätze

(14.1) Definition Sei p eine Primzahl und $a \in \mathbb{Z}$. Man nennt a einen ***quadratischen Rest*** modulo p, wenn eine Zahl $c \in \mathbb{Z}$ mit $a \equiv c^2 \bmod p$ existiert. Andernfalls spricht man von einem ***quadratischen Nichtrest***.

Eine alternative Formulierung lautet: Die Zahl a ist quadratischer Rest modulo p genau dann, wenn das Bild $\bar{a} = a + p\mathbb{Z}$ in $\mathbb{F}_p$ ein Quadrat ist. Anhand diese Formulierung sieht man, dass die Eigenschaft einer Zahl, quadratischer (Nicht-)Rest zu sein, nur von ihrer Restklasse modulo p abhängt. Für die Formulierung der nachfolgenden Aussagen ist die Einführung der folgenden Notation sinnvoll.

(14.2) Definition Sei p eine ungerade Primzahl und $a \in Z$. Das ***Legendre-Symbol*** modulo p ist definiert durch

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

Man beachte, dass durch p teilbare Zahlen a auf jeden Fall quadratische Reste sind, denn für sie gilt jeweils $a \equiv 0^2 \bmod p$. Für die Primzahl 2 wäre die Definition des Legendre-Symbols zwar auch möglich, aber wenig sinnvoll, denn jede ganze Zahl (gerade oder ungerade) ist wegen $0^2 \equiv 0 \bmod 2$ und $1^2 \equiv 1 \bmod 2$ ein quadratischer Rest modulo 2.

(14.3) Lemma Sei p eine ungerade Primzahl, und seien $a, b \in \mathbb{Z}$. Dann gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad \text{und} \qquad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ falls } a \equiv b \bmod p.$$

Beweis: Zunächst beweisen wir die zweite Gleichung. Aus $a \equiv b \bmod p$ folgt, dass die Bilder $\bar{a}, \bar{b}$ von a, b in $\mathbb{F}_p$ übereinstimmen. Das Element $\bar{a}$ ist also genau dann gleich $\bar{0}$, wenn dies auf $\bar{b}$ zutrifft. Daraus folgt die Äquivalenz $(\frac{a}{p}) = 0 \Leftrightarrow (\frac{b}{p}) = 0$. Das Element $\bar{a}$ ist genau dann ungleich $\bar{0}$ und ein Quadrat in $\mathbb{F}_p$, wenn dies für $\bar{b}$ gilt. Also ist $(\frac{a}{p}) = 1$ äquivalent zu $(\frac{b}{p}) = 1$. Weil das Legendre-Symbol nur die drei Werte $-1, 0, 1$ annehmen kann, folgt aus den bereits bewiesenen Äquivalenzen auch $(\frac{a}{p}) = -1 \Leftrightarrow (\frac{b}{p}) = -1$.

Die Gleichung $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ ist offenbar erfüllt, wenn $p \mid a$ oder $p \mid b$ gilt, denn dann ist p auch ein Teiler von ab, und beide Seiten der Gleichung sind null. Setzen wir nun $p \nmid a$ und $p \nmid b$ voraus. Dann sind die Bilder $\bar{a}, \bar{b}$ in $\mathbb{F}_p$ beide ungleich Null. Gilt $(\frac{a}{p}) = (\frac{b}{p}) = 1$, dann sind $\bar{a}$ und $\bar{b}$ beides Quadrate in $\mathbb{F}_p^\times$. Es gilt also $c, d \in \mathbb{F}_p^\times$ mit $\bar{a} = \bar{c}^2$ und $\bar{b} = \bar{d}^2$. Wegen $\bar{a}\bar{b} = (\bar{c}\bar{d})^2$ ist dann auch das Bild von ab in $\mathbb{F}_p^\times$ ein Quadrat, und es folgt $(\frac{ab}{p}) = 1$.

Ist genau eines der beiden Legendre-Symbole gleich 1 und das andere gleich -1, dann muss auch $(\frac{ab}{p}) = -1$ gelten. Denn nehmen wir an, es wäre o.B.d.A. $(\frac{a}{p}) = 1$ und $(\frac{b}{p}) = -1$, aber $(\frac{ab}{p}) = 1$. Dann wären $\bar{a}$ und $\bar{a}\bar{b}$ beides Quadrate in $\mathbb{F}_p^\times$. Es gäbe also $\bar{c}, \bar{d} \in \mathbb{F}_p^\times$ mit $\bar{a} = \bar{c}^2$ und $\bar{a}\bar{b} = \bar{d}^2$. Wegen $\bar{b} = (\bar{a}\bar{b})\bar{a}^{-1} = \bar{d}^2(\bar{c}^2)^{-1} = (\bar{d}\bar{c}^{-1})^2$ wäre auch $\bar{b}$ ein Quadrat in $\mathbb{F}_p^\times$, was aber zu $(\frac{b}{p}) = -1$ im Widerspruch steht.

Betrachten wir nun noch den Fall $(\frac{a}{p}) = (\frac{b}{p}) = -1$; zu zeigen ist $(\frac{ab}{p}) = 1$. Sei $c \in \mathbb{Z}$ eine Primitivwurzel modulo p. Dann gilt $\langle \bar{c} \rangle = \mathbb{F}_p^\times$, es gibt also $m, n \in \mathbb{Z}$ mit $\bar{c}^m = \bar{a}$ und $\bar{c}^n = \bar{b}$. Dabei sind m und n ungerade, denn andernfalls wären $\bar{a}$ oder $\bar{b}$ Quadrate in $\mathbb{F}_p^\times$ und folglich $(\frac{a}{p}) = 1$ oder $(\frac{b}{p}) = 1$, im Widerspruch zur Voraussetzung. Die Summe $m + n$ ist dann gerade, also $m + n = 2\ell$ für ein $\ell \in \mathbb{Z}$. Es folgt $\bar{a}\bar{b} = c^{m+n} = (c^\ell)^2$ und somit $(\frac{ab}{p}) = 1$. □

(14.4) Satz *(Eulersches Kriterium)*
Sei p eine ungerade Primzahl. Dann gilt $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$ für alle $a \in \mathbb{Z}$ mit $p \nmid a$.

Beweis: Sei c eine Primitivwurzel modulo p, und seien $\bar{a}, \bar{c}$ die Bilder von a, c in $\mathbb{F}_p^\times$. Wegen $\langle \bar{c} \rangle = \mathbb{F}_p^\times$ gibt es ein $m \in \mathbb{Z}$ mit $\bar{a} = \bar{c}^m$. Ist m gerade, $m = 2k$ für ein $k \in \mathbb{Z}$, dann ist $\bar{a}$ ein Quadrat in $\mathbb{F}_p^\times$ und folglich $(\frac{a}{p}) = 1$. Wegen $\bar{c}^{p-1} = \bar{1}$ gilt außerdem $\bar{a}^{(p-1)/2} = \bar{c}^{m(p-1)/2} = \bar{c}^{k(p-1)} = \bar{1}$. Damit ist die Kongruenz in diesem Fall bewiesen.

Ist m ungerade, $m = 2k+1$ für ein $k \in \mathbb{Z}$, dann ist $\bar{a}$ kein Quadrat in $\mathbb{F}_p^\times$. Denn andernfalls wäre $\bar{a} = \bar{b}^2$ für ein $\bar{b} \in \mathbb{F}_p^\times$. Schreiben wir $\bar{b} = \bar{c}^\ell$ mit $\ell \in \mathbb{Z}$, dann erhalten wir insgesamt $\bar{c}^{2\ell} = \bar{b}^2 = \bar{a} = \bar{c}^{2k+1}$ und somit $\bar{c}^{2\ell-2k-1} = \bar{1}$. Wegen $\operatorname{ord}(p) = p-1$ folgt $(p-1) \mid 2\ell - 2k - 1$. Aber dies ist unmöglich, weil $p-1$ gerade und $2\ell - 2k - 1$ ungerade ist. Also ist $\bar{a}$ tatsächlich ein Nichtquadrat, und es folgt $(\frac{a}{p}) = -1$. Andererseits gilt auch $\bar{a}^{(p-1)/2} = \bar{c}^{m(p-1)/2} = \bar{c}^{(2k+1)(p-1)/2} = \bar{c}^{k(p-1)}\bar{c}^{(p-1)/2} = \bar{1} \cdot \bar{c}^{(p-1)/2} = \bar{c}^{(p-1)/2}$. Wegen $\bar{a}^{(p-1)} = \bar{1}$ ist $\bar{a}^{(p-1)/2}$ eine Nullstelle von $x^2 - \bar{1}$. Andererseits ist $\bar{a}^{(p-1)/2} = \bar{c}^{(p-1)/2} \neq \bar{1}$ wegen $\operatorname{ord}(\bar{c}) = p-1$. Weil $\pm\bar{1}$ die einzigen beiden Nullstellen von $x^2 - \bar{1}$ in $\mathbb{F}_p$ sind, folgt $\bar{a}^{(p-1)/2} = -\bar{1}$. Also ist die Kongruenz auch in diesem Fall nachgewiesen. □

(14.5) Satz *(Ergänzungssätze zum Quadratischen Reziprozitätsgesetz)*
Für jede ungerade Primzahl p gilt

$$\left(\frac{-1}{p}\right) \quad = \quad (-1)^{(p-1)/2} \quad = \quad \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases}$$

und

$$\left(\frac{2}{p}\right) \quad = \quad (-1)^{(p^2-1)/8} \quad = \quad \begin{cases} 1 & \text{falls } p \equiv 1, 7 \bmod 8 \\ -1 & \text{falls } p \equiv 3, 5 \bmod 8 \end{cases}$$

Beweis: Den zweiten Teil jeder der beiden Gleichungen überprüft man unmittelbar dadurch, dass man die Fälle einzeln durchgeht. Ist $p \equiv 1 \bmod 4$, dann ist $\frac{1}{2}(p-1)$ gerade und folglich $(-1)^{(p-1)/2} = 1$. Ist dagegen $p \equiv 3 \bmod 4$, dann ist $\frac{1}{2}(p-1)$ ungerade, und wir erhalten $(-1)^{(p-1)/2} = -1$. Ist $p \equiv 1 \bmod 8$ oder $p \equiv 7 \bmod 8$, dann ist p modulo 16 kongruent zu einer der Zahlen $-7, -1, 1$ oder 7. In jedem Fall gilt dann $p^2 \equiv 1 \bmod 16$, also ist $\frac{1}{8}(p^2-1)$ gerade und $(-1)^{(p^2-1)/8} = 1$. Ist $p \equiv 3 \bmod 8$ oder $p \equiv 5 \bmod 8$, dann gilt $p \equiv a \bmod 16$ für ein $a \in \{-5, -3, 3, 5\}$ und $p^2 \equiv 9 \bmod 16$. In diesem Fall ist $\frac{1}{8}(p^2-1)$ ungerade und $(-1)^{(p^2-1)/8} = -1$.

Auf Grund der Eulerschen Gleichung gilt $(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} \bmod p$. Weil auf beiden Seiten der Kongruenz nur die Werte ± 1 möglich sind und wegen $p > 2$ folgt aus der Kongruenz modulo p Gleichheit. Zum Beweis des ersten Teils der zweiten Gleichung rechnen wir im Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen. Weil der Faktorring $Z[i]/(p)$ ein Ring der Charakteristik p ist, gilt $(\alpha+\beta)^p \equiv \alpha^p + \beta^p \bmod p$; siehe § 15 der Algebra-Vorlesung. Auf Grund der Eulerschen Gleichung und wegen $2 = (-i)(1+i)^2$ erhalten wir

$$\left(\frac{2}{p}\right) \quad \equiv \quad 2^{(p-1)/2} \quad \equiv \quad (-i)^{(p-1)/2}(1+i)^{p-1} \quad \equiv \quad \frac{(-i)^{(p-1)/2}}{1+i}(1+i)^p \quad \equiv$$

$$\frac{(-i)^{(p-1)/2}(1-i)}{(1+i)(1-i)}(1+i^p) \quad \equiv \quad \left(\tfrac{1}{2}(-i)^{(p-1)/2} + \tfrac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p)$$

Gehen wir nun die einzelnen möglichen Fälle durch. Weil p ungerade ist, gilt $p \equiv 1, 3, 5$ oder $7 \bmod 8$. Im Fall $p \equiv 1 \bmod 8$ gilt $\left(\frac{1}{2}(-i)^{(p-1)/2} + \frac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) = (\frac{1}{2} - \frac{1}{2}i)(1+i) = 1$. Im Fall $p \equiv 3 \bmod 8$ ist $\left(\frac{1}{2}(-i)^{(p-1)/2} + \frac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) = (\frac{1}{2}(-i) - \frac{1}{2})(1-i) = -1$. Ist $p \equiv 5 \bmod 8$, dann erhalten wir $\left(\frac{1}{2}(-i)^{(p-1)/2} + \frac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) = (-\frac{1}{2} + \frac{1}{2}i)(1+i) = -1$, und im letzten Fall $p \equiv 7 \bmod 8$ gilt $\left(\frac{1}{2}(-i)^{(p-1)/2} + \frac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) = (\frac{1}{2}i + \frac{1}{2})(1-i) = 1$. Also ist die Kongruenz $(\frac{2}{p}) \equiv (-1)^{(p^2-1)/8} \bmod p$ in jedem der vier Fälle erfüllt. Da auf beiden Seite der Kongruenz nur die Werte ± 1, folgt aus der Kongruenz modulo p wiederum Gleichheit. □

Das entscheidende Hilfsmittel zur Berechnung des Legendre-Symbol ist nun das berühmte, auf *C.F. Gauß* zurückgehende

(14.6) Satz *(Quadratisches Reziprozitätsgesetz)*

Für zwei beliebige voeinander verschiedene ungerade Primzahlen p, q gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \quad = \quad (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \quad = \quad \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Am Ende dieses Kapitels werden wir zwei Beweise für diesen Satz angeben, einen elementaren und einen weiteren, der auf einer Rechnung mit Einheitswurzeln basiert. Wir zeigen nun anhand eines Beispiels, wie das Quadratische Reziprozitätsgesetz zur Berechnung des Legendre-Symbols verwendet werden kann. Die Zahl 5209 ist eine Primzahl. Mit Hilfe der uns zur Verfüng stehenden Rechenregeln erhalten wir

$$\left(\frac{8498}{5209}\right) \overset{(1)}{=} \left(\frac{3289}{5209}\right) \overset{(2)}{=} \left(\frac{11\cdot 13\cdot 13}{5209}\right) \overset{(3)}{=} \left(\frac{11}{5209}\right)\left(\frac{13}{5209}\right)\left(\frac{23}{5209}\right) \overset{(4)}{=}$$

$$\left(\frac{5209}{11}\right)\left(\frac{5209}{13}\right)\left(\frac{5209}{23}\right) \overset{(5)}{=} \left(\frac{6}{11}\right)\left(\frac{9}{13}\right)\left(\frac{11}{23}\right) \overset{(6)}{=} \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)\left(\frac{3}{13}\right)^2\left(\frac{11}{23}\right) \overset{(7)}{=}$$

$$(-1)\cdot\left(\frac{3}{11}\right)\cdot 1\cdot\left(\frac{11}{23}\right) \overset{(8)}{=} -\left(\frac{3}{11}\right)\left(\frac{11}{23}\right) \overset{(9)}{=} -(-1)\left(\frac{11}{3}\right)\cdot(-1)\left(\frac{23}{11}\right)$$

$$\overset{(10)}{=} -\left(\frac{2}{3}\right)\left(\frac{1}{11}\right) \overset{(11)}{=} -\left(\frac{2}{3}\right) \overset{(12)}{=} -(-1) \quad = \quad 1.$$

Dabei kommt die Gleichung (1) durch $8498 \equiv 3289 \bmod 5209$ zu Stande. In Schritt (4) wird zum ersten Mal das Quadratische Reziprozitätsgesetz angewendet, und zwar auf jeden der drei Faktoren. Wegen $5209 \equiv 1 \bmod 4$ kommt es dabei zu keinem Vorzeichenwechsel. Gleichung (5) ist wegen $5209 \equiv 6 \bmod 11$, $5209 \equiv 9 \bmod 13$ und $5209 \equiv 11 \bmod 23$ erfüllt. In Schritt (7) wurde auf den ersten Faktor der Zweite Ergänzungssatz angewendet; wegen $11 \equiv 3 \bmod 8$ gilt $\left(\frac{2}{11}\right) = -1$. Außerdem ist zu beachten, dass das Legendre-Symbol $\left(\frac{3}{13}\right)$ wegen $13 \nmid 3$ gleich 1 oder -1, das Quadrat also gleich 1 ist. In Schritt (9) wird noch das Quadratische Reziprozitätsgesetz angewendet, auf beide Faktoren. Wegen $3 \equiv 3 \bmod 4$, $11 \equiv 3 \bmod 4$ und $23 \equiv 3 \bmod 4$ entsteht dabei jeweils ein Vorzeichenwechsel. Gleichung (10) gilt wegen $11 \equiv 2 \bmod 3$ und $23 \equiv 1 \bmod 11$. Schließlich wird Schritt (12) noch einmal der Zweite Ergänzungssatz angewendet. Insgesamt ergibt unsere Rechnung, dass 8498 ein quadratischer Rest modulo der Primzahl 5209 ist. Durch aufwändiges Probieren findet man tatsächlich die Kongruenz $8498 \equiv 2046^2 \bmod 5209$.

Man beachte, dass die erste Anwendung des Quadratischen Reziprozitätsgesetzes unter (4) nur möglich war, weil wir zuvor die Zahl 3289 in das Produkt $11\cdot 13\cdot 23$ von Primzahlen zerlegt haben. Die Berechnung einer solchen Primfaktorzerlegung ist natürlich bei großen Zahlen sehr aufwändig (sogar so aufwändig, dass die unter anderem die Sicherheit der RSA-Verschlüsselung darauf beruht). Um das Quadratische Reziprozitätsgesetz in dieser Hinsicht praktikabler zu machen, wird es auf geeignete Weise verallgemeinert.

(14.7) Definition Sei $n \in \mathbb{N}$ ungerade und $n = p_1 \cdot \ldots \cdot p_r$ die Primfaktorzerlegung von n, wobei wir auch das mehrfache Auftreten derselben Primzahl zulassen (und die Anzahl r der Faktoren im Fall $n = 1$ gleich Null ist). Sei $a \in \mathbb{Z}$. Dann ist das ***Jacobi-Symbol*** von a modulo n definiert durch

$$\left(\frac{a}{n}\right) \quad = \quad \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_r}\right)$$

Unmittelbar aus der Definition folgt $(\frac{a}{mn}) = (\frac{a}{m})(\frac{a}{n})$ für alle $a \in \mathbb{Z}$ und ungerade $m, n \in \mathbb{N}$. Aus (14.3) kann leicht $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$ für alle $a, b \in \mathbb{Z}$ und ungerades $n \in \mathbb{N}$ abgeleitet werden, und $(\frac{a}{n}) = (\frac{b}{n})$ falls $a \equiv b \bmod n$. Ist nämlich $n = p_1 \cdot \ldots \cdot p_r$ die Primfaktorzerlegung von n, dann gilt

$$\left(\frac{ab}{n}\right) \quad = \quad \prod_{i=1}^{r}\left(\frac{ab}{p_i}\right) \quad = \quad \prod_{i=1}^{r}\left(\frac{a}{p_i}\right)\prod_{i=1}^{r}\left(\frac{b}{p_i}\right) \quad = \quad \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

Aus $a \equiv b \bmod n$ folgt $a \equiv b \bmod p_i$ für $1 \leq i \leq r$ und somit

$$\left(\frac{a}{n}\right) \quad = \quad \prod_{i=1}^{r}\left(\frac{a}{p_i}\right) \quad = \quad \prod_{i=1}^{r}\left(\frac{b}{p_i}\right) \quad = \quad \left(\frac{b}{n}\right).$$

Darüber hinaus gilt

(14.8) Satz Der Erste und Zweite Ergänzungssatz sowie das Quadratische Reziprozitätsgesetz gelten unverändert auch für das Jacobi-Symbol.

Beweis: Da das Jacobi-Symbol, wie wir bereits festgestellt haben, in der unteren Komponente multiplikativ ist, müssen wir zeigen, dass sich auch die „rechten Seiten" unserer drei Rechenregeln multiplikativ verhalten. Wir beweisen für alle ungeraden $m_1, m_2, n_1, n_2 \in \mathbb{N}$ die Gleichungen

$$(-1)^{\frac{n_1-1}{2}} \cdot (-1)^{\frac{n_2-1}{2}} = (-1)^{\frac{n_1 n_2 - 1}{2}} \qquad , \qquad (-1)^{\frac{n_1^2-1}{8}} \cdot (-1)^{\frac{n_2^2-1}{8}} = (-1)^{\frac{(n_1 n_2)^2-1}{8}}$$

und

$$(-1)^{\frac{m_1-1}{2}\cdot\frac{n_1-1}{2}} \cdot (-1)^{\frac{m_2-1}{2}\cdot\frac{n_2-1}{2}} \quad = \quad (-1)^{\frac{m_1 m_2-1}{2}\cdot\frac{n_1 n_2-1}{2}}.$$

Die erste Gleichung ist äquivalent zu $(-1)^{\frac{n_1-1}{2}+\frac{n_2-1}{2}} = (-1)^{\frac{n_1 n_2-1}{2}}$. Weil allgemein $(-1)^a$ für $a \in \mathbb{Z}$ nur von der Restklasse von a modulo 2 abhängt, ist dies wiederum äquivalent zu

$$\frac{n_1-1}{2} + \frac{n_2-1}{2} \equiv \frac{n_1 n_2 - 1}{2} \bmod 2 \quad \Leftrightarrow \quad (n_1-1) + (n_2-1) \equiv n_1 n_2 - 1 \bmod 4 \quad \Leftrightarrow$$
$$n_1 n_2 - n_1 - n_2 + 1 \equiv 0 \bmod 4 \quad \Leftrightarrow \quad (n_1-1)(n_2-1) \equiv 0 \bmod 4.$$

Die letzte Äquivalenz ist offenbar erfüllt, weil die Faktoren $n_1 - 1$ und $n_2 - 1$ beide durch 2 teilbar sind. Entsprechend beweist man die zweite Gleichung durch die Äquivalenzumformung

$$(-1)^{\frac{n_1^2-1}{8}} \cdot (-1)^{\frac{n_2^2-1}{8}} = (-1)^{\frac{(n_1 n_2)^2-1}{8}} \quad \Leftrightarrow \quad \tfrac{1}{8}(n_1^2-1) + \tfrac{1}{8}(n_2^2-1) \equiv \tfrac{1}{8}((n_1 n_2)^2 - 1) \bmod 8 \quad \Leftrightarrow$$

$$(n_1^2-1) + (n_2^2-1) \equiv (n_1 n_2)^2 - 1 \bmod 16 \quad \Leftrightarrow \quad (n_1 n_2)^2 - n_1^2 - n_2^2 + 1 \equiv 0 \bmod 16 \quad \Leftrightarrow$$

$$(n_1^2-1)(n_2^2-1) \equiv 0 \bmod 16 \quad \Leftrightarrow \quad (n_1-1)(n_1+1)(n_2-1)(n_2+1) \equiv 0 \bmod 16.$$

Wieder sind alle vier Faktoren durch 2 teilbar und die letzte Kongrenz somit erfüllt. Die dritte Gleichung folgt schließlich aus den ersten beiden durch die Rechnung

$$(-1)^{\frac{m_1 m_2 - 1}{2} \cdot \frac{n_1 n_2 - 1}{2}} \quad = \quad (-1)^{\frac{m_1 - 1}{2}} (-1)^{\frac{m_2 - 1}{2}} (-1)^{\frac{n_1 - 1}{2}} (-1)^{\frac{n_2 - 1}{2}} \quad =$$

$$(-1)^{\frac{m_1 - 1}{2}} (-1)^{\frac{n_1 - 1}{2}} (-1)^{\frac{m_2 - 1}{2}} (-1)^{\frac{n_2 - 1}{2}} \quad = \quad (-1)^{\frac{m_1 - 1}{2} \cdot \frac{m_2 - 1}{2}} (-1)^{\frac{n_1 - 1}{2} \cdot \frac{n_2 - 1}{2}}.$$

Seien nun ungerade natürliche Zahlen $m, n \in \mathbb{N}$ vorgegeben, mit zugehörigen Primfaktorzerlegungen $m = p_1 \cdot \ldots \cdot p_r$ und $n = q_1 \cdot \ldots \cdot q_s$. Den Ersten Ergänzungssatz erhält man durch die Rechnung

$$\left(\frac{-1}{m}\right) \quad = \quad \prod_{i=1}^{m} \left(\frac{-1}{p_i}\right) \quad = \quad \prod_{i=1}^{m} (-1)^{(p_i - 1)/2} \quad = \quad (-1)^{(p_1 \cdot \ldots \cdot p_r - 1)/2} \quad = \quad (-1)^{(m-1)/2} \quad ,$$

den Zweiten Ergänzungssatz durch

$$\left(\frac{2}{m}\right) \quad = \quad \prod_{i=1}^{m} \left(\frac{2}{p_i}\right) \quad = \quad \prod_{i=1}^{m} (-1)^{(p_i^2 - 1)/8} \quad = \quad (-1)^{(p_1 \cdot \ldots \cdot p_r - 1)/8} \quad = \quad (-1)^{(m^2 - 1)/8}$$

und das Quadratische Reziprozitätsgesetz für das Jacobi-Symbol schließlich durch

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) \quad = \quad \prod_{i=1}^{r} \left(\frac{p_i}{n}\right)\left(\frac{n}{p_i}\right) \quad = \quad \prod_{i=1}^{r} \prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right)\left(\frac{p_i}{q_j}\right)$$

$$= \quad \prod_{i=1}^{r} \prod_{j=1}^{s} (-1)^{\frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2}} \quad = \quad (-1)^{\frac{p_1 \cdot \ldots \cdot p_r - 1}{2} \cdot \frac{q_1 \cdot \ldots \cdot q_s - 1}{2}} \quad = \quad (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \, . \qquad \square$$

Man beachte, dass am Jacobi-Symbol $\left(\frac{a}{n}\right)$, im Gegensatz zum Legendre-Symbol, *nicht* abgelesen werden kann, ob a ein quadratischer Rest modulo n ist. Beispielsweise ist 2 kein quadratischer Rest modulo 15, denn wäre dies der Fall, dann müsste 2 sowohl ein quadratischer Rest modulo 3 als auch ein quadratischer Rest modulo 5 sein. Ist nämlich $2 \equiv c^2 \bmod 15$ für ein $c \in \mathbb{Z}$ erfüllt, dann folgt daraus auch $2 \equiv c^2 \bmod 3$ und $2 \equiv c^2 \bmod 5$. Aber wie durch Ausprobieren leicht überprüft, ist 2 weder modulo 3 noch modulo 5 ein quadratischer Rest, also erst recht kein quadratischer Rest moduldo 15. Es gilt aber

$$\left(\frac{2}{15}\right) \quad = \quad \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) \quad = \quad (-1)(-1) \quad = \quad 1.$$

Das Jacobi-Symbol ermöglicht aber eine effizientere Berechnung von Legendre-Symbolen, weil es vor der Anwendung des Reziprozitätsgesetzes nicht mehr nötig ist, die obere Zahl in ihre Primfaktoren zu zerlegen. So vereinfacht sich zum Beispiel die Rechnung von oben zu

$$\left(\frac{8498}{5209}\right) \quad = \quad \left(\frac{3289}{5209}\right) \quad = \quad \left(\frac{5209}{3289}\right) \quad = \quad \left(\frac{1920}{3298}\right) \quad = \quad \left(\frac{2^7 \cdot 15}{3298}\right) \quad = \quad \left(\frac{2}{3289}\right)^7 \left(\frac{15}{3289}\right)$$

$$= \quad 1^7 \cdot \left(\frac{15}{3289}\right) \quad = \quad \left(\frac{3289}{15}\right) \quad = \quad \left(\frac{4}{15}\right) \quad = \quad \left(\frac{2}{15}\right)^2 \quad = \quad 1.$$

Literaturverzeichnis

[Bo] S. Bosch, *Algebra*. Springer-Verlag.

[Ca] O. Cámpoli, *A principal ideal domain that is not a Euclidean domain*. American Math. Monthly, vol. 95 no. 9 (Nov. 1988), 868-871.

[Ge] W. Geyer, *Algebra*. Vorlesung Uni Erlangen-Nürnberg, WS 03/04.

[Ha] M. Harper, $\mathbb{Z}[\sqrt{14}]$ *is Euclidean*. Canad. J. Math. Vol. **56** (1), pp. 55-70, 2004.

[LL] F. Lorenz, F. Lemmermeyer, *Algebra 1*. Spektrum Akad. Verlag.

[Me] K. Meyberg, *Algebra, Teil 1 und 2*. Hanser-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.