Einführung in die Zahlentheorie und algebraische Strukturen

Wintersemester 2010/2011

Universität Bayreuth

Michael Stoll

Inhaltsverzeichnis

0. Einführung

Dies ist die erste einer Reihe aufeinander aufbauender Vorlesungen:

(1) **Einführung in die Zahlentheorie und algebraische Strukturen:**
- Elementare Zahlentheorie
- Ringe

(2) **Einführung in die Algebra:**
- Gruppen
- Körpererweiterungen

(3) **Vertiefung der Algebra:**
- Galoistheorie

Die ersten beiden sollte eigentlich jeder Mathematik Studierende hören, denn sie bilden die Grundlage für alle weiter führenden Veranstaltungen im Bereich Algebra. Im Studiengang Lehramt Gymnasium sind alle drei verpflichtend, aus gutem Grund: Die Beherrschung des dort vermittelten Stoffs ist notwendig, um die Aufgaben der Staatsexamensklausur in Algebra lösen zu können. Es sei gleich darauf hingewiesen, dass vieles von dem, was in einer der Vorlesungen besprochen wird, später in einer der anderen wieder benötigt wird. So sind zum Beispiel die Polynomringe, die in dieser Vorlesung diskutiert werden, ein wesentliches Hilfsmittel für die Konstruktion von Körpererweiterungen, und die Galoistheorie, die das Thema der „Vertiefung der Algebra“ bildet, verknüpft die Gruppentheorie mit der Theorie der Körpererweiterungen, die beide in der „Einführung in die Algebra“ besprochen werden. Es ist also keine gute Idee, nach dem Bestehen der Klausur das Gelernte schnell wieder zu vergessen. Aus dem gleichen Grund ist es sinnvoll, die drei Vorlesungen möglichst in auf einander folgenden Semestern zu hören.

Die „Einführung in die Zahlentheorie und algebraische Strukturen“ hat zwei Hauptthemen (wie der längliche Titel andeutet). Einerseits geht es darum, grundlegende Techniken und Ergebnisse der (elementaren) Zahlentheorie kennen zu lernen. Das beginnt mit der Teilbarkeitslehre mit Themen wie Primzahlen, größte gemeinsame Teiler, Euklidischer Algorithmus und eindeutige Primfaktorzerlegung und führt weiter zu quadratischen Resten und dem Quadratischen Reziprozitätsgesetz und zu Sätzen über die Darstellbarkeit natürlicher Zahlen als Summen von zwei oder vier Quadratzahlen. Andererseits soll auch ein Einstieg in die Algebra gegeben werden. Dies erfolgt exemplarisch an Hand der Ringe, die ein gutes Beispiel für eine „algebraische Struktur“ darstellen. Diese im Vergleich mit dem üblicheren Aufbau in der Reihenfolge „Gruppen, Ringe, Körper“ vielleicht ungewohnte Wahl ist auch dadurch motiviert, dass der Ring $\mathbb{Z}$ der ganzen Zahlen, der in der elementaren Zahlentheorie die Hauptrolle spielt, ein prototypisches Beispiel für einen Ring ist. Von diesem Beispiel ausgehend lässt sich die Theorie der Ringe gut aufbauen. Themen aus der Ringtheorie sind euklidische Ringe, Hauptidealringe und faktorielle Ringe (letztere sind Ringe, in denen die eindeutige Primfaktorzerlegung gilt), dann als wichtige Beispiele und weil sie auch für sich genommen wichtig sind, Polynomringe. Noethersche Ringe sind eine große Klasse von Ringen (zum Beispiel sind Polynomringe in mehreren Variablen über einem Körper noethersch). Schließlich werden wir noch Moduln diskutieren (das sind gewissermaßen Vektorräume über einem Ring) und den wichtigen Klassifikationssatz für endlich erzeugte Moduln über Hauptidealringen (mit Anwendungen auf abelsche Gruppen) beweisen.

Einige Abschnitte in diesem Skript sind kleiner gedruckt. Dabei kann es sich um ergänzende Bemerkungen zur Vorlesung handeln, die nicht zum eigentlichen Stoff gehören, die Sie aber vielleicht trotzdem interessant finden. Manchmal handelt es sich auch um Beweise, die in der Vorlesung nicht ausgeführt werden, zum Beispiel weil sie relativ lang sind und fürs Verständnis nicht unbedingt benötigt werden, die aber doch der Vollständigkeit halber oder auch als Anregung etwa für Übungsaufgaben im Skript stehen sollten.

1. Die natürlichen und die ganzen Zahlen

In diesem Kapitel werden wir die natürlichen und die ganzen Zahlen aus mathematischer Sicht besprechen. Dabei werden wir uns auch schon dem Thema „algebraische Strukturen“ ein wenig nähern. Zum Teil wird Ihnen das vielleicht etwas abstrakt erscheinen, aber wenn Sie sich mit der Herangehensweise anfreunden, dann wird Ihnen das später in der Vorlesung helfen. Im nächsten Kapitel geht es dann aber erst einmal ganz konkret mit ganzen Zahlen und Teilbarkeit weiter.

Sie haben sicher ein ganz gutes Gefühl dafür, was die natürlichen und die ganzen Zahlen „sind“. Trotzdem wird es nicht schaden, sich noch einmal kurz zu vergegenwärtigen, wie man sie aus mathematischer Sicht einführen kann (auch wenn Sie das schon einmal zu Beginn der Anfängervorlesungen gesehen haben).

Zuerst müssen wir uns aber festlegen, was die kleinste natürliche Zahl sein soll. Es gibt zwei Lager: Die einen lassen $\mathbb{N}$ mit der Zahl 1 anfangen, und für die anderen ist 0 die kleinste natürliche Zahl. Es gibt dabei kein Richtig oder Falsch, höchstens kann die getroffene Festlegung mehr oder weniger zweckmäßig sein. Ich persönlich finde es „natürlicher“, die natürlichen Zahlen mit 0 beginnen zu lassen und führe dafür folgende Gründe an:

- Die natürlichen Zahlen sollten etwas „zählen“, nämlich die Anzahlen von Elementen endlicher Mengen. Die leere Menge ist nun sicher eine endliche Menge, also sollte $0 = \#\emptyset$ auch eine natürliche Zahl sein.
- Mit der Null wird $\mathbb{N}$ unter der Addition ein Monoid (also eine Halbgruppe mit neutralem Element); ohne die Null haben wir nur eine Halbgruppe.

Dagegen spricht vielleicht die kulturgeschichtliche Tatsache, dass die Zahl null (und die leere Menge) vergleichsweise viel jüngere Errungenschaften des menschlichen Geistes sind als die Zahlenreihe $1, 2, 3, \ldots$. In jedem Fall definieren wir:

1.1. **Definition.** Die *Menge der natürlichen Zahlen* ist

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}\,.$$

Um bezüglich der Frage „$0 \in \mathbb{N}$?“ keine Verwirrung aufkommen zu lassen, werde ich mich aber bemühen, von „positiven“ oder „nichtnegativen ganzen Zahlen“ zu sprechen und

$$\mathbb{Z}_{>0} = \{1, 2, 3, \ldots\} \quad \text{bzw.} \quad \mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, \ldots\}$$

zu schreiben.

Obige Definition 1.1 sagt uns im übrigen nicht wirklich, was die natürlichen Zahlen sind, denn es ist erst einmal überhaupt nicht klar, was die Pünktchen „…“ darin bedeuten. Das kann zum Beispiel durch die *Peanoschen Axiome* präzisiert werden:

1.2. **Peano-Axiome für die natürlichen Zahlen.**

(1) 0 ist eine natürliche Zahl.
(2) Ist n eine natürliche Zahl, so ist der *Nachfolger* $S(n)$ von n ebenfalls eine natürliche Zahl.
(3) 0 ist nicht Nachfolger einer natürlichen Zahl.
(4) Haben zwei natürliche Zahlen den selben Nachfolger, dann sind sie gleich.
(5) Ist M eine Menge natürlicher Zahlen, so dass $0 \in M$ und mit $n \in M$ auch stets $S(n) \in M$ gilt, so enthält M alle natürlichen Zahlen.

Das letzte Axiom ist das *Induktionsaxiom*, das uns sagt, dass wir alle natürlichen Zahlen ausgehend von 0 durch iterierte Bildung des Nachfolgers bekommen. In diesem Sinne definiert es die Bedeutung der Pünktchen oben.

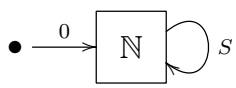
In etwas konziserer Form und unter Verwendung von weiteren Begriffen aus der Mengenlehre können wir $\mathbb{N}$ auch wie folgt beschreiben.

1.3. **Definition.** $\mathbb{N}$ ist eine Menge mit einem ausgezeichneten Element $0 \in \mathbb{N}$ und einer injektiven Abbildung $S : \mathbb{N} \to \mathbb{N}\setminus\{0\} \subset \mathbb{N}$. Zusätzlich gilt für jede Teilmenge $M \subset \mathbb{N}$:[1]

$$\text{Aus} \quad 0 \in M \quad \text{und} \quad n \in M \Rightarrow S(n) \in M \qquad \text{folgt} \qquad M = \mathbb{N}\,.$$

1.4. **Exkurs.** Vom Standpunkt der Logik ist das Induktionsaxiom in der Form oben unbefriedigend, weil es von „allen Teilmengen“ von $\mathbb{N}$ spricht und damit der Bereich der Logik erster Stufe verlässt. Man ersetzt es durch ein „Axiomschema“, also eine Familie von Axiomen, in denen die Teilmenge M durch eine sie definierende Eigenschaft (die sich als logische Formel hinschreiben lässt) ersetzt ist. Es ist klar, dass man ein schwächeres System erhält, denn es gibt überabzählbar viele Teilmengen von $\mathbb{N}$, aber nur abzählbar viele verschiedene formulierbare Eigenschaften. Tatsächlich gibt es dann außer dem „Standardmodell“ der natürlichen Zahlen auch noch andere Strukturen, die diesen Axiomen genügen. Der berühmte Gödelsche Unvollständigkeitssatz, der besagt, dass es wahre Aussagen über natürliche Zahlen gibt, die sich nicht beweisen lassen, hängt mit diesem Phänomen zusammen. Arbeitet man innerhalb der Mengenlehre, dann kann man natürlich über Teilmengen quantifizieren und damit $\mathbb{N}$ wie oben definieren. Man kann dann (wenn man 0 und S geeignet definiert, etwa $0 := \emptyset$ und $S(n) := n \cup \{n\}$) innerhalb der Mengenlehre zeigen, dass $\mathbb{N}$ (existiert und) eindeutig bestimmt ist. Allerdings ist diese Behauptung ein wenig geschummelt: Man muss die Existenz einer „induktiven Menge“ M (also einer Menge mit $\emptyset \in M$ und $x \in M \implies x \cup \{x\} \in M$) als Axiom fordern, sonst kann man die Existenz von $\mathbb{N}$ nicht beweisen.

Man kann sich $\mathbb{N}$ also etwa so vorstellen:



Das ist ein einfaches Beispiel einer „algebraischen Struktur“: Wir haben eine unterliegende *Menge* mit einem ausgezeichneten *Element* und einer *Abbildung* der Menge in sich. Dazu kommen dann im allgemeinen *Axiome*, die erfüllt werden müssen.

[1] Ich verwende die Notation „$A \subset B$“ für „$a \in A \Rightarrow a \in B$“; $A = B$ ist also erlaubt.

1.5. **Beispiel.** Als weiteres Beispiel einer algebraischen Struktur, das wir in dieser Vorlesung noch ausführlich behandeln werden, sei der *Ring* (mit 1) genannt. Hier haben wir

- eine unterliegende Menge R;
- zwei ausgezeichnete Elemente $0 \in R$ und $1 \in R$;
- zwei Abbildungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$ und eine Abbildung $- : R \to R$;
- eine Reihe von Axiomen, die den üblichen Rechenregeln entsprechen.

Die formale Definition sieht so aus:

1.6. **Definition.** Ein *Ring* ist ein Sextupel $(R, 0, 1, +, -, \cdot)$, wobei R eine Menge ist, $0, 1 \in R$ und $+ : R \times R \to R$ (Addition), $- : R \to R$ (Negation) und $\cdot : R \times R \to R$ (Multiplikation) drei Abbildungen sind, die folgende Axiome erfüllen. Für alle $r, s, t \in R$ gilt

(1) (Nullelement, Kommutativität und Assoziativität der Addition, Negation)
$r + 0 = r, \quad r + s = s + r, \quad (r + s) + t = r + (s + t), \quad r + (-r) = 0;$
(2) (Einselement, Assoziativität der Multiplikation)
$r \cdot 1 = r = 1 \cdot r, \quad (r \cdot s) \cdot t = r \cdot (s \cdot t);$
(3) (Distributivgesetze)
$r \cdot (s + t) = r \cdot s + r \cdot t, \quad (r + s) \cdot t = r \cdot t + s \cdot t.$

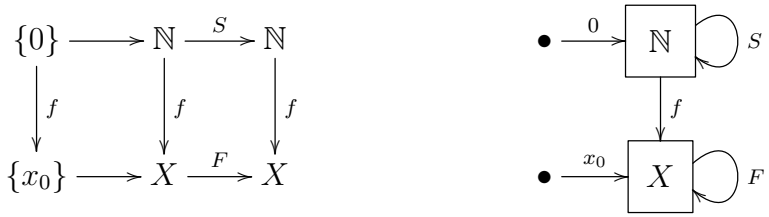
Der Ring heißt *kommutativ*, wenn zusätzlich $r \cdot s = s \cdot r$ für alle $r, s \in R$ gilt.

Man kann zeigen, dass, wenn die Addition und die Multiplikation gegeben sind, das Null- und das Einselement und die Negationsabbildung eindeutig bestimmt sind. Deswegen kürzt man $(R, 0, 1, +, -, \cdot)$ gerne zu $(R, +, \cdot)$ ab. Normalerweise ist auch klar, was die Addition und Multiplikation ist, und man spricht dann einfach vom „Ring R“.

In vielen Lehrbüchern wird von $(R, +, \cdot)$ ausgegangen und dann die Existenz von 0, 1, $-$ in den betreffenden Axiomen gefordert. Beide Versionen sind äquivalent, und welche man bevorzugt, ist Geschmackssache. Mein Standpunkt ist, dass man sowieso wissen muss, was das Null- und das Einselement ist und wie man das Negative eines Elements bestimmt, so dass man die relevanten Daten auch gleich als Teil der Struktur auffassen kann.

Dem Induktionsaxiom entspricht das *Rekursionsprinzip*, dass Sie sicher schon häufig verwendet haben.

1.7. **Satz.** *Sei X eine Menge, $x_0 \in X$, und sei $F : X \to X$ eine Abbildung. Dann gibt es eine eindeutig bestimmte Abbildung $f : \mathbb{N} \to X$ mit $f(0) = x_0$ und $f\big(S(n)\big) = F\big(f(n)\big)$.*



Beweis. Wir beginnen mit der Eindeutigkeit. Seien also f_1 und f_2 zwei Abbildungen $\mathbb{N} \to X$ mit den geforderten Eigenschaften. Wir setzen

$$M = \{n \in \mathbb{N} \mid f_1(n) = f_2(n)\}\,.$$

Dann gilt $0 \in M$ wegen $f_1(0) = x_0 = f_2(0)$, und wenn $n \in M$ ist, dann folgt $f_1\big(S(n)\big) = F\big(f_1(n)\big) = F\big(f_2(n)\big) = f_2\big(S(n)\big)$, also gilt auch $S(n) \in M$. Aus dem Induktionsaxiom folgt $M = \mathbb{N}$, und das heißt $f_1 = f_2$.

Für die Existenz verwenden wir eine ähnliche Idee. Sei $M \subset \mathbb{N}$ die Teilmenge, so dass $f(n)$ für $n \in M$ eindeutig festgelegt ist (insbesondere ist f auf M definiert). Da $f(0) = x_0$ sein muss, ist $0 \in M$. Und ist $f(n)$ eindeutig festgelegt, so folgt, dass auch $f\big(S(n)\big) = F\big(f(n)\big)$ eindeutig festgelegt ist: Es ist weder $S(n) = 0$ noch kann $S(n) = S(m)$ sein mit einem $m \neq n$, so dass es keinen Konflikt geben kann. Aus $n \in M$ folgt also $S(n) \in M$ und damit wieder $M = \mathbb{N}$. □

Man beachte, dass wir für den Existenzbeweis die Peano-Axiome (3) und (4) benutzen mussten, während für die Eindeutigkeit das Induktionsaxiom ausreicht.

1.8. **Universelle Eigenschaft.** Wie oben angedeutet, können wir $(\mathbb{N}, 0, S)$ (mit $0 \in \mathbb{N}$, $S : \mathbb{N} \to \mathbb{N}$) als einfaches Beispiel einer algebraischen Struktur betrachten. Dann ist (X, x_0, F) eine Struktur der gleichen Art, und Satz 1.7 sagt, dass *es genau eine Struktur erhaltende Abbildung $f : \mathbb{N} \to X$ gibt.* „Struktur erhaltend“ bedeutet hier konkret $f(0) = x_0$ und $f \circ S = F \circ f$. Dies ist ein erstes Beispiel einer *universellen Eigenschaft*. Wir werden noch einigen anderen begegnen. Solche Eigenschaften charakterisieren gewisse algebraische Strukturen eindeutig und können daher als Definition angesehen werden:

1.9. **Lemma.** *Ist $(\mathbb{N}', 0', S')$ ein Tripel mit einer Menge $\mathbb{N}'$, $0' \in \mathbb{N}'$ und einer Abbildung $S' : \mathbb{N}' \to \mathbb{N}'$, das anstelle von $(\mathbb{N}, 0, S)$ Satz 1.7 erfüllt, dann gibt es eine eindeutig bestimmte Bijektion $h : \mathbb{N} \to \mathbb{N}'$ mit $h(0) = 0'$ und $h\big(S(n)\big) = S'\big(h(n)\big)$.*

Beweis. Nach Satz 1.7 gibt es jedenfalls eine eindeutig bestimmte Abbildung h mit den letzten beiden Eigenschaften; es ist nur noch nicht klar, ob h auch bijektiv ist. Wir können den Satz auch mit vertauschten Rollen anwenden (da auch $(\mathbb{N}', 0', S')$ den Satz erfüllt und wir $(X, x_0, F) = (\mathbb{N}, 0, F)$ setzen können). Es gibt also eine eindeutig bestimmte Abbildung $h' : \mathbb{N}' \to \mathbb{N}$ mit $h'(0') = 0$ und $h' \circ S' = S \circ h'$. Dann sind $h' \circ h$ und $\mathrm{id}_{\mathbb{N}}$ zwei Abbildungen, die 0 auf 0 abbilden und mit S kommutieren. Nach dem Satz müssen sie gleich sein: $h' \circ h = \mathrm{id}_{\mathbb{N}}$. Ebenso gilt $h \circ h' = \mathrm{id}_{\mathbb{N}'}$. Also ist h tatsächlich eine Bijektion. □

1.10. **Isomorphismen.** Eine bijektive Struktur erhaltende Abbildung, deren Inverses ebenfalls Struktur erhaltend ist (was in vielen Fällen automatisch ist), wird *Isomorphismus* genannt. Strukturen, die *isomorph* sind, zwischen denen es also einen Isomorphismus gibt, haben die selben algebraischen Eigenschaften und werden deshalb als im wesentlichen gleich betrachtet. Zwei Strukturen mit der selben universellen Eigenschaft sind analog zu der Argumentation in Lemma 1.9 stets *eindeutig isomorph* zueinander: Es gibt genau einen Isomorphismus zwischen ihnen.

Wir können das Rekursionsprinzip dazu benutzen, Addition und Multiplikation auf $\mathbb{N}$ zu definieren.

1.11. **Definition.** Wir definieren die *Addition* $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ und die *Multiplikation* $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ wie folgt:

(1) $m + 0 := m$ und $m + S(n) := S(m + n)$.
(2) $m \cdot 0 := 0$ und $m \cdot S(n) := (m \cdot n) + m$.

Mit $1 := S(0)$ haben wir dann insbesondere $S(n) = S(n + 0) = n + S(0) = n + 1$.

Nach dem Rekursionsprinzip sind die Funktionen $n \mapsto m + n$ und $n \mapsto m \cdot n$ wohldefiniert (es ist jeweils $X = \mathbb{N}$; im ersten Fall nehmen wir $x_0 = m$ und $F = S$, im zweiten Fall $x_0 = 0$ und $F(n) = n + m$).

Man kann jetzt daran gehen, die bekannten Rechengesetze zu beweisen.

1.12. **Satz.** Für alle $k, m, n \in \mathbb{N}$ gelten folgende Aussagen:

(1) $m + 0 = m, \quad m + n = n + m, \quad (k + m) + n = k + (m + n)$;
(2) $m \cdot 1 = m, \quad m \cdot n = n \cdot m, \quad (k \cdot m) \cdot n = k \cdot (m \cdot n)$;
(3) $k \cdot (m + n) = k \cdot m + k \cdot n, \quad (m + n) \cdot k = m \cdot k + n \cdot k$.

Beweis. Das ist eine gute, wenn auch langwierige Übungsaufgabe. Als Beispiel zeigen wir hier die Kommutativität der Addition: $m + n = n + m$. Zuerst zeigen wir durch Induktion, dass $0 + m = m = m + 0$ gilt:

$$0 + 0 = 0 + 0 \qquad \text{und}$$
$$m + 0 = 0 + m \implies S(m) + 0 = S(m) = S(m + 0) = S(0 + m) = 0 + S(m)$$

Jetzt zeigen wir $S(m) + n = S(m + n) = m + S(n)$ durch Induktion nach m. Der Induktionsanfang $m = 0$ wird durch Induktion nach n erledigt:

$$S(0) + 0 = S(0) = S(0 + 0) \quad \text{und}$$
$$S(0) + n = S(n) \implies S(0) + S(n) = S(S(0) + n) = S(S(n))$$

Auch der Induktionsschritt $m \to S(m)$ benötigt eine „innere“ Induktion nach n:

$$S(S(m)) + 0 = S(S(m)) = S(S(m) + 0) \quad \text{und}$$
$$S(S(m)) + n = S(S(m) + n)$$
$$\implies S(S(m)) + S(n) = S(S(S(m)) + n) = S(S(S(m) + n)) = S(S(m) + S(n)) .$$

Sei jetzt $n \in \mathbb{N}$ fixiert. Wir zeigen durch Induktion, dass $m + n = n + m$ für alle $m \in \mathbb{N}$. Das haben wir für $m = 0$ bereits gezeigt. Außerdem gilt

$$m + n = n + m \implies S(m) + n = S(m + n) = S(n + m) = n + S(m) .$$

□

Wie sieht es mit den ganzen Zahlen aus? Die Motivation für ihre Einführung ist der Wunsch, beliebig Zahlen voneinander subtrahieren zu können. (In $\mathbb{N}$ existiert etwa die Differenz $0 - 1$ nicht, denn 0 ist kein Nachfolger.)

Das Vorgehen bei der Konstruktion der ganzen aus den natürlichen Zahlen ist recht typisch:

(1) Man konstruiert die gewünschten Objekte formal;
(2) Man identifiziert formale Darstellungen, die das selbe Objekt repräsentieren (Äquivalenzrelation/Bildung von Äquivalenzklassen);
(3) Man definiert die gewünschten Abbildung auf der Menge der Äquivalenzklassen;
(4) Man zeigt, dass die resultierende Struktur die gewünschten Eigenschaften hat.

1.13. **Konstruktion der ganzen Zahlen.** Wir werden das jetzt für die Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$ durchführen.

Erster Schritt. Wir hätten gerne beliebige Differenzen zur Verfügung. Wir denken uns also $\mathbb{Z}$ als Menge aller möglichen Differenzen von natürlichen Zahlen. Formal betrachten wir $Z = \mathbb{N} \times \mathbb{N}$ und interpretieren $(n, m) \in Z$ als Repräsentant für die Differenz $n - m$.

Zweiter Schritt. Die selbe Zahl kann in vielen verschiedenen Weisen als Differenz geschrieben werden: Es gilt

$$n - m = n' - m' \iff n + m' = n' + m\,.$$

Wir führen also eine Äquivalenzrelation $\sim$ auf Z ein durch die Festlegung

$$(n, m) \sim (n', m') \iff n + m' = n' + m\,.$$

Es ist hier natürlich noch zu zeigen, dass $\sim$ tatsächlich eine Äquivalenzrelation ist (Übung)! Wir setzen $\mathbb{Z} = Z/\!\sim$, das ist die Menge der Äquivalenzklassen bezüglich $\sim$ in Z. Wir schreiben $[n, m]$ für die Äquivalenzklasse, die (n, m) enthält.

Dritter Schritt. Die neue Struktur $\mathbb{Z}$ soll ein Ring werden. Wir müssen also jetzt das Null- und das Einselement und die Additions- und Multiplikationsabbildung definieren. Die Beziehungen

$$0 = 0 - 0, \quad 1 = 1 - 0 \quad \text{und} \quad (n - m) + (n' - m') = (n + n') - (m + m')$$

motivieren die folgenden Definitionen:

$$0_{\mathbb{Z}} = [0, 0], \quad 1_{\mathbb{Z}} = [1, 0] \quad \text{und} \quad [n, m] +_{\mathbb{Z}} [n', m'] = [n + n', m + m']\,.$$

Wie immer, wenn man eine Abbildung auf Äquivalenzklassen mit Hilfe von Repräsentanten definiert, muss man zeigen, dass die Abbildung wohldefiniert ist, also nicht von den gewählten Repräsentanten abhängt. Für die Addition heißt das hier konkret:

$$[n, m] = [k, l], \quad [n', m'] = [k', l'] \implies [n + n', m + m'] = [k + k', l + l']\,.$$

Nach Definition der Äquivalenzrelation bedeutet das

$$n + l = m + k, \quad n' + l' = m' + k' \implies (n + n') + (l + l') = (m + m') + (k + k')\,,$$

was leicht aus den Rechenregeln in Satz 1.12 folgt. Für die Negation lassen wir uns von $-(n - m) = m - n$ inspirieren:

$$-_{\mathbb{Z}}[n, m] = [m, n]\,.$$

Man prüft wieder leicht nach, dass dies wohldefiniert ist.

Für die Definition der Multiplikation lassen wir uns von

$$(n - m) \cdot (n' - m') = nn' - nm' - mn' + mm' = (nn' + mm') - (nm' + mn')$$

leiten und setzen

$$[n, m] \cdot_{\mathbb{Z}} [n', m'] = [nn' + mm', nm' + mn']\,.$$

Wie vorher ist nachzuweisen, dass diese Abbildung wohldefiniert ist, was ebenfalls nicht schwer fällt (Übung).

Schließlich soll $\mathbb{Z}$ eine Erweiterung von $\mathbb{N}$ sein. Wir müssen also noch eine *Einbettung* von $\mathbb{N}$ in $\mathbb{Z}$ definieren (also eine injektive Abbildung, die mit der Struktur (Null, Eins, Addition, Multiplikation) verträglich ist. Es ist klar, dass man dafür

$$i : \mathbb{N} \longrightarrow \mathbb{Z}, \quad n \longmapsto [n, 0]$$

wählen wird. Es ist dann nicht schwer nachzuprüfen, dass

$$i(0) = 0_{\mathbb{Z}}, \quad i(1) = 1_{\mathbb{Z}}, \quad i(n+m) = i(n) +_{\mathbb{Z}} i(m) \quad \text{und} \quad i(n \cdot m) = i(n) \cdot_{\mathbb{Z}} i(m)$$

gilt.

Vierter Schritt. Schließlich bleibt nachzuweisen, dass $\mathbb{Z}$ tatsächlich ein kommutativer Ring ist. Dafür stützt man sich auf die in $\mathbb{N}$ geltenden Rechenregeln 1.12. Das macht keine Schwierigkeiten, auch wenn es etwas langwierig ist.

Es gilt nun

$$[n,m] = \begin{cases} i(n-m) & \text{wenn } n \geq m \\ -_{\mathbb{Z}}[m,n] = -_{\mathbb{Z}} i(m-n) & \text{wenn } n \leq m \end{cases}$$

Wir identifizieren $\mathbb{N}$ mit $i(\mathbb{N}) \subset \mathbb{Z}$ und schreiben n für $i(n)$, $-n$ für $-_{\mathbb{Z}} n$, $m+n$ für $m +_{\mathbb{Z}} n$, mn oder $m \cdot n$ für $m \cdot_{\mathbb{Z}} n$. Dann haben wir wie gewohnt

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Nach diesem ersten Ausflug in abstraktere Gefilde können wir annehmen, dass wir wissen, was die ganzen Zahlen sind, und uns konkreteren Fragestellungen zuwenden. Insbesondere werden wir die folgenden Eigenschaften von $\mathbb{Z}$ verwenden:

(1) $(\mathbb{Z}, 0, 1, +, -, \cdot)$ ist ein kommutativer Ring *ohne Nullteiler*, d.h. aus $ab = 0$ folgt $a = 0$ oder $b = 0$.
(2) $(\mathbb{Z}_{\geq 0}, \leq)$ ist *wohlgeordnet*, d.h. jede nichtleere Teilmenge hat ein kleinstes Element.
(3) Die Relation $a < b$ bleibt unter Addition von ganzen Zahlen und unter Multiplikation mit positiven ganzen Zahlen erhalten.

Aus der Tatsache, dass $\mathbb{Z}_{\geq 0}$ wohlgeordnet ist, folgt folgendes allgemeinere Induktionsprinzip:

1.14. **Allgemeines Induktionsprinzip.** *Sei $A(n)$ eine Aussage, die für Zahlen $n \in \mathbb{Z}_{\geq 0}$ richtig oder falsch sein kann. Wenn für jedes $n \in \mathbb{Z}_{\geq 0}$ gilt:*

$$\textit{Aus } A(m) \textit{ für alle } 0 \leq m < n \textit{ folgt } A(n),$$

dann gilt $A(n)$ für alle $n \in \mathbb{Z}_{\geq 0}$.

Beweis. Der Beweis verwendet das *Prinzip des kleinsten Verbrechers:* Wir nehmen an, $A(n)$ gilt nicht für alle $n \geq 0$. Dann ist die Menge der „Verbrecher“

$$M = \{n \in \mathbb{Z}_{\geq 0} \mid A(n) \text{ ist falsch}\} \subset \mathbb{Z}_{\geq 0}$$

nicht leer, hat also nach (2) oben ein kleinstes Element $n_{\min}$. Nach Definition von M heißt das, dass $A(m)$ für alle $0 \leq m < n_{\min}$ gilt. Dann gilt nach Voraussetzung aber auch $A(n_{\min})$, im Widerspruch zu $n_{\min} \in M$. Die Annahme muss also falsch sein: Es gibt keine Verbrecher, und $A(n)$ gilt für alle $n \geq 0$. □

Sie werden bei dem Induktionsprinzip vielleicht den Induktionsanfang vermissen. Er versteckt sich im Fall $n = 0$: Die Voraussetzung lautet dann „$A(m)$ gilt für alle $m \in \emptyset$“, und so eine Aussage ist immer wahr (weil es keine Gegenbeispiele gibt). Es ist also de facto $A(0)$ zu zeigen.

2. Grösste gemeinsame Teiler

In diesem Kapitel untersuchen wir die Eigenschaften der Teilbarkeitsrelation. Wir beginnen mit einer Definition.

2.1. **Definition.** Seien $a, b \in \mathbb{Z}$ ganze Zahlen. Wir sagen, *a teilt b*, *a ist ein Teiler von b* oder *b ist ein Vielfaches von a* und schreiben $a \mid b$, wenn es eine ganze Zahl c gibt, so dass $b = a \cdot c$ gilt. Wenn a kein Teiler von b ist, schreiben wir $a \nmid b$.

Diese Relation hat folgende Eigenschaften:

2.2. **Proposition.** *Seien $a, b, c \in \mathbb{Z}$. Es gilt:*

(1) *Aus $a \mid b$ und $a \mid c$ folgt $a \mid b \pm c$.*
(2) *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.*
(3) *Aus $a \mid b$ folgt $a \mid bc$.*
(4) $0 \mid a \iff a = 0$ *und* $a \mid 1 \iff a = \pm 1$.
(5) $a \mid 0$, $1 \mid a$ *und* $a \mid a$.
(6) *Aus $a \mid b$ und $b \mid a$ folgt $a = \pm b$.*
(7) *Aus $a \mid b$ und $|b| < |a|$ folgt $b = 0$.*

Beweis. (1), (2), (6), (7): Übung.
(3) $a \mid b$ heißt, dass es $n \in \mathbb{Z}$ gibt mit $b = an$. Dann folgt $bc = a \cdot (nc)$, also gilt $a \mid bc$.
(4) $0 \mid a \iff a = 0 \cdot n$ für ein $n \in \mathbb{Z}$, aber $0 \cdot n = 0$. Die zweite Aussage ist äquivalent zu $ab = 1 \implies a = \pm 1$. Das folgt aus $|ab| > |b|$ für $|a| > 1$ und $b \neq 0$.
(5) $0 = a \cdot 0$, $a = 1 \cdot a$, $a = a \cdot 1$. □

2.3. **Bemerkung.** Aus (5) (Reflexivität), (6) (Antisymmetrie) und (2) (Transitivität) ergibt sich, dass $(\mathbb{Z}_{\geq 0}, |)$ eine *teilweise geordnete Menge* ist; aus (4) und (5) folgt noch, dass 1 das kleinste und 0 das größte(!) Element dieser Ordnung ist.

Die Ordnung durch Teilbarkeit ist keine Totalordnung, da zum Beispiel weder $2 \mid 3$ noch $3 \mid 2$ gilt: Divisionen in $\mathbb{Z}$ gehen nicht immer auf. Deswegen sind die folgenden Begriffe interessant.

2.4. **Definition.** Seien $a, b \in Z$ ganze Zahlen. Wir sagen, eine ganze Zahl $g \in \mathbb{Z}$ sei *ein größter gemeinsamer Teiler von a und b*, wenn $g \mid a$ und $g \mid b$ (d.h., g ist ein gemeinsamer Teiler), und wenn für alle $n \in \mathbb{Z}$ mit $n \mid a$ und $n \mid b$ gilt, dass $n \mid g$ (d.h. g ist unter allen gemeinsamen Teilern ein größter im Sinne der Ordnung durch Teilbarkeit).

Analog sagen wir, eine ganze Zahl $k \in \mathbb{Z}$ sei *ein kleinstes gemeinsames Vielfaches von a und b*, wenn $a \mid k$ und $b \mid k$, und wenn für alle $n \in \mathbb{Z}$ mit $a \mid n$ und $b \mid n$ gilt, dass $k \mid n$.

(Auf englisch sagt man *greatest common divisor*, gcd [in England bisweilen auch noch *highest common factor*, hcf] und *least common multiple*, lcm.)

Es ist erst einmal gar nicht klar, ob es zu je zwei ganzen Zahlen immer einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches gibt. (Man beachte, das „größter“ hier im Sinne der Teilbarkeit zu verstehen ist und nicht im Sinne der üblichen (Total-)Ordnung.) Immerhin können wir leicht zeigen, dass größte gemeinsame Teiler und kleinste gemeinsame Vielfache (wenn sie existieren) im wesentlichen eindeutig bestimmt sind.

2.5. **Lemma.** *Seien $a, b \in \mathbb{Z}$. Sind $g, g' \in \mathbb{Z}$ zwei größte gemeinsame Teiler von a und b, dann gilt $g = \pm g'$. Sind $k, k' \in \mathbb{Z}$ zwei kleinste gemeinsame Vielfache von a und b, dann gilt $k = \pm k'$.*

Beweis. Nach Definition 2.4 gilt (weil g' ein größter gemeinsamer Teiler von a und b ist) $g' \mid a$, $g' \mid b$, woraus (weil auch g ein größter gemeinsamer Teiler von a und b ist) folgt, dass $g' \mid g$. Ganz genauso sieht man $g \mid g'$. Prop. 2.2, (6) folgt dann $g = \pm g'$. Die Behauptung über kleinste gemeinsame Vielfache beweist man im wesentlichen genauso. □

2.6. **Folgerung.** *Zu $a, b \in \mathbb{Z}$ gibt es höchstens einen größten gemeinsamen Teiler $g \geq 0$ und höchstens ein kleinstes gemeinsames Vielfaches $k \geq 0$.*

Wir schreiben dann kurz

$$g = \mathrm{ggT}(a, b) \qquad \text{und} \qquad k = \mathrm{kgV}(a, b)\,.$$

Dann ist natürlich auch $g = \mathrm{ggT}(b, a)$ bzw. $k = \mathrm{kgV}(b, a)$.

Wie können wir uns davon überzeugen, dass es immer einen größten gemeinsamen Teiler gibt? Die Idee ist, dafür Induktion zu benutzen, die Existenz von $\mathrm{ggT}(a, b)$ also auf den Fall von „kleineren“ a und b zurückzuführen. Dazu brauchen wir als wichtiges Hilfsmittel die *Division mit Rest*.

2.7. **Lemma.** *Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gibt es eindeutig bestimmte ganze Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < |b|$ und $a = qb + r$.*

Beweis. Wir können $b > 0$ annehmen (wende sonst das Lemma auf a und $b' = -b$ an, das liefert q' und r; setze $q = -q'$).

Wir zeigen die Existenz erst einmal für $a \geq 0$ durch Induktion. Für $0 \leq a < b$ können wir $q = 0$, $r = a$ setzen. Ist $a \geq b$, dann sei $a > a' = a - b \geq 0$. Nach Induktionsvoraussetzung gibt es $q', r \in \mathbb{Z}$ mit $0 \leq r < b$ und $a' = q'b + r$. Dann können wir $q = q' + 1$ setzen, und q, r erfüllen die verlangten Bedingungen.

Sei jetzt $a < 0$. Dann ist $a' = -1 - a \geq 0$; es gibt nach dem eben Bewiesenen also $q', r' \in \mathbb{Z}$ mit $0 \leq r' < b$ und $a' = q'b + r'$. Wir setzen $q = -1 - q'$ und $r = b - 1 - r'$, dann gilt $0 \leq r < b$ und $a = -1 - a' = -q'b - 1 - r' = qb + r$.

Es bleibt noch die Eindeutigkeit zu zeigen. Seien dazu also q, r und q', r' zwei Paare ganzer Zahlen mit

$$a = qb + r = q'b + r' \qquad \text{und} \qquad 0 \leq r, r' < b\,.$$

Es folgt $(q - q')b = r' - r$, also $|(q - q')b| = |r' - r| < b$. Nach Prop. 2.2, (7) gilt dann $r' - r = 0$, also $r' = r$ und damit dann auch $q' = q$. □

2.8. **Bemerkung.** Aus dem obigen Beweis ergibt sich ein (nicht besonders effizienter) Algorithmus zur Berechnung von q und r. Wir nehmen an, dass $a \geq 0$ und $b > 0$ ist (die anderen Fälle lassen sich ja leicht darauf zurückführen).

(1) Setze $q := 0$ und $r := a$.
(2) Solange $r \geq b$ ist, wiederhole $q := q + 1$, $r := r - b$.

Bevor wir die Division mit Rest für den Beweis der Existenz des ggT nutzen können, brauchen wir noch ein paar Eigenschaften des ggT.

2.9. **Lemma.** *Seien $a, b, c \in \mathbb{Z}$. Dann gilt*

(1) $\mathrm{ggT}(a, 0) = \mathrm{ggT}(a, \pm a) = |a|$.
(2) $\mathrm{ggT}(a, \pm 1) = 1$.
(3) *Existiert* $g = \mathrm{ggT}(a, b)$, *dann gilt* $g = \mathrm{ggT}(a, b + ac)$.

Beweis.

(1) $|a|$ ist sicher ein gemeinsamer Teiler von a, $\pm a$ und 0. Andererseits gilt für jeden gemeinsamen Teiler g auch $g \mid |a|$, wegen $|a| \geq 0$ ist dann $|a|$ der ggT von a und 0 und von a und $\pm a$.
(2) Das folgt aus Prop. 2.2, (4).
(3) Wir zeigen, dass a, b und $a, b + ac$ die selben gemeinsamen Teiler haben. Daraus folgt dann unmittelbar die Behauptung. Es gilt

$$n \mid a,\ n \mid b \implies n \mid a,\ n \mid b,\ n \mid ac \implies n \mid a,\ n \mid b + ac$$

(verwende Prop. 2.2, (1) und (3)) und ebenso

$$n \mid a,\ n \mid b + ac \implies n \mid a,\ n \mid b + ac,\ n \mid ac \implies n \mid a,\ n \mid b\,.$$

□

Jetzt können wir die Existenz des ggT beweisen.

2.10. **Satz.** *Seien $a, b \in \mathbb{Z}$. Dann existiert $g = \mathrm{ggT}(a, b)$.*

Beweis. Der Beweis geht durch Induktion nach $m = \min\{|a|, |b|\}$. Für $m = 0$ folgt die Existenz aus Lemma 2.9, (1). Anderenfalls sei ohne Einschränkung $m = |b| > 0$. Nach Lemma 2.7 gibt es $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$. Nach Induktionsvoraussetzung existiert $g = \mathrm{ggT}(b, r)$ (denn $\min\{|b|, |r|\} = r < |b| = m$). Dann folgt aber aus Lemma 2.9, (3), dass auch $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r + qb) = g$ existiert. □

2.11. **Bemerkung.** Aus diesem Beweis ergibt sich unmittelbar der *Euklidische Algorithmus* zur Berechnung des größten gemeinsamen Teilers. Man beachte, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$. Der Algorithmus ist dann wie folgt.

(1) Setze $a_0 := |a|$, $a_1 := |b|$, $n := 1$.
(2) Solange $a_n > 0$ ist, wiederhole die folgenden Schritte:
   (a) Schreibe $a_{n-1} = q_n a_n + a_{n+1}$ mit $0 \leq a_{n+1} < a_n$.
   (b) Setze $n := n + 1$.
(3) (Jetzt ist $a_n = 0$.)
   Der ggT von a und b ist a_{n-1}.

Aus dem obigen Beweis können wir sogar noch mehr herausziehen:

2.12. **Satz.** *Seien $a, b \in \mathbb{Z}$. Dann gibt es $x, y \in \mathbb{Z}$ mit $xa + yb = \mathrm{ggT}(a, b)$.*

Beweis. Wir verwenden wieder Induktion nach $m = \min\{|a|, |b|\}$. Ist $m = b = 0$, dann gilt $\mathrm{ggT}(a, b) = |a| = xa + yb$ mit $x = \pm 1$ und $y = 0$. Ist $m = |b| > 0$, dann sei wie oben $a = qb + r$ mit $0 \leq r < |b|$. Es gilt dann nach Induktionsannahme

$$g = \mathrm{ggT}(a, b) = \mathrm{ggT}(b, r) = x'b + y'r$$

mit geeigneten $x', y' \in \mathbb{Z}$. Wegen $r = a - qb$ folgt

$$g = x'b + y'(a - qb) = y'a + (x' - qy')b = xa + yb\,,$$

wenn wir $x = y'$ und $y = x' - qy'$ setzen. □

Die Zahlen x und y in diesem Satz sind nicht eindeutig bestimmt, denn für jedes $t \in \mathbb{Z}$ gilt auch $(x - tb)a + (y + ta)b = xa + yb = \mathrm{ggT}(a, b)$.

2.13. **Bemerkung.** Man kann den Euklidischen Algorithmus leicht erweitern, so dass er auch geeignete Zahlen x und y liefert. Dazu führt man Zahlen x_n, y_n mit, die die Relation $a_n = x_n a + y_n b$ erfüllen. Das sieht dann so aus:

(1) Setze $a_0 := |a|$, $a_1 := |b|$, $x_0 = \mathrm{sign}(a)$, $y_0 = 0$, $x_1 = 0$, $y_1 = \mathrm{sign}(b)$, $n := 1$.
(2) Solange $a_n > 0$ ist, wiederhole die folgenden Schritte:
  (a) Schreibe $a_{n-1} = q_n a_n + a_{n+1}$ mit $0 \le a_{n+1} < a_n$.
  (b) Setze $x_{n+1} := x_{n-1} - q_n x_n$, $y_{n+1} := y_{n-1} - q_n y_n$.
  (c) Setze $n := n + 1$.
(3) (Jetzt ist $a_n = 0$.)
  Mit $(g, x, y) := (a_{n-1}, x_{n-1}, y_{n-1})$ gilt $\mathrm{ggT}(a, b) = g = xa + yb$.

Folgende Anwendung ist wichtig:

2.14. **Folgerung.** *Seien $a, b, c \in \mathbb{Z}$. Dann gilt*

$$\mathrm{ggT}(a, b) \mid c \iff c \in \mathbb{Z}a + \mathbb{Z}b = \{xa + yb \mid x, y \in \mathbb{Z}\}\,.$$

Die ganzzahligen Linearkombinationen von a und b sind also genau die Vielfachen des ggT von a und b.

Beweis. Sei $g = \mathrm{ggT}(a, b)$. Wenn $c = xa + yb$ ist, dann folgt aus $g \mid a$ und $g \mid b$ sofort $g \mid c$. Sei umgekehrt c ein Vielfaches von g, also $c = gn$ mit einem $n \in \mathbb{Z}$. Nach Satz 2.12 gibt es $u, v \in \mathbb{Z}$ mit $g = ua + vb$. Dann ist auch $c = gn = un \cdot a + vn \cdot b \in \mathbb{Z}a + \mathbb{Z}b$. □

Der Fall, dass sich *jede* ganze Zahl als Linearkombination von a und b schreiben lässt, ist besonders wichtig.

2.15. **Definition.** Zwei ganze Zahlen a und b heißen *teilerfremd* oder *relativ prim* (engl. *coprime*), wenn $\mathrm{ggT}(a, b) = 1$. Wir schreiben dafür $a \perp b$. (Diese Schreibweise hat sich leider (noch?) nicht allgemein durchgesetzt, ist aber praktisch.)

Es gilt also:

$$a \perp b \iff \exists x, y \in \mathbb{Z} : xa + yb = 1\,.$$

Der Beweis des folgenden Lemmas ist recht typisch dafür, wie man das ausnutzt.

2.16. **Lemma.** *Seien $a, b, c \in \mathbb{Z}$ mit $a \perp b$ und $a \mid bc$. Dann gilt $a \mid c$.*

Beweis. Wegen $a \perp b$ gibt es $x, y \in \mathbb{Z}$ mit $xa + yb = 1$. Wir multiplizieren mit c, das ergibt $c = cxa + cyb = (cx)a + y(bc)$. Beide Terme rechts werden von a geteilt, also auch c. □

Auf ganz ähnliche Weise kann man die erste Aussage im nächsten Lemma zeigen.

2.17. **Lemma.**

(1) *Seien $a, b \in \mathbb{Z}$ teilerfremd. Dann ist $|ab|$ das kleinste gemeinsame Vielfache von a und b.*
(2) *Seien $a, b \in \mathbb{Z}$, $g = \mathrm{ggT}(a, b)$. Dann ist $a = a'g$, $b = b'g$ mit $a' \perp b'$.*
(3) *Seien $a, b \in \mathbb{Z}$. Gilt $a \neq 0$ oder $b \neq 0$, dann ist $|ab|/\mathrm{ggT}(a, b)$ das kleinste gemeinsame Vielfache von a und b. Außerdem ist $\mathrm{kgV}(0, 0) = 0$.*

Kleinste gemeinsame Vielfache existieren also auch, und es gilt stets

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = |ab| .$$

Beweis. Übung. □

3. Primzahlen und Faktorisierung

Unser nächstes Ziel ist der „Fundamentalsatz der Arithmetik“, der besagt, dass sich jede positive ganze Zahl im wesentlichen eindeutig als Produkt von Primzahlen schreiben lässt. Wir beginnen mit einer bekannten Definition.

3.1. **Definition.** Eine positive ganze Zahl p heißt *Primzahl* oder *prim*, wenn $p > 1$ und in jeder Faktorisierung $p = ab$ mit $a, b \in \mathbb{Z}$ entweder $a = \pm 1$ oder $b = \pm 1$ gilt. („p ist nur durch 1 und sich selbst teilbar.“)

Warum ist 1 keine Primzahl? Einfach deshalb, weil es unpraktisch wäre: Der Satz von der *eindeutigen* Primfaktorzerlegung wäre falsch, wenn man beliebig viele Faktoren 1 hinzufügen könnte. Die Eins als Teiler einer Zahl trägt schlicht keine Information.

Die folgende Eigenschaft ist grundlegend.

3.2. **Satz.** *Jede ganze Zahl $n > 1$ hat einen* Primteiler*, d.h. es gibt eine Primzahl p mit $p \mid n$.*

Beweis. Wir beweisen die Aussage durch Induktion. Wir nehmen an, die Aussage sei für alle $1 < m < n$ richtig. Ist n selbst eine Primzahl, so gilt die Behauptung mit $p = n$. Anderenfalls gibt es nach Definition ganze Zahlen a und b mit $n = ab$ und $a, b \neq \pm 1$. Wir können $a, b > 0$ annehmen (eventuell muss man bei a und b das Vorzeichen ändern), dann gilt $a, b > 1$ und damit auch $a, b < n$. Nach Induktionsannahme gibt es dann einen Primteiler p von a; wegen $a \mid n$ gilt dann auch $p \mid n$. □

Bemerkung. Aus dem Beweis ergibt sich wieder ein Algorithmus zum Auffinden eines Primteilers. In der Praxis kann es aber sehr schwierig sein, dies tatsächlich durchzuführen. Das Problem liegt darin, dass man, wenn n nicht prim ist, eine Faktorisierung von n finden muss. Dafür gibt es bisher kein effizientes Verfahren (technisch gesprochen: ein Verfahren, das in polynomial durch die Anzahl der Ziffern von n beschränkter Zeit fertig wird). Dies macht man sich sogar zu Nutze: Die Sicherheit des bekannten RSA-Verschlüsselungsverfahrens (dazu später in dieser Vorlesung mehr) beruht genau auf dieser Schwierigkeit. Wenn einmal ein schneller Faktorisierungsalgorithmus gefunden werden sollte (es ist nicht bewiesen, dass es so etwas nicht geben kann), dann ist das RSA-Verfahren gestorben. Auf der anderen Seite gibt es effiziente Algorithmen, die feststellen, ob n eine Primzahl ist oder nicht.

Es ist nun plausibel, dass man jede positive ganze Zahl als Produkt von Primzahlen schreiben kann.

3.3. **Satz.** *Jede positive ganze Zahl n ist Produkt von Primzahlen.*

Beweis. Induktion nach n. Hier ist $n = 1$ der Induktionsanfang. Wie kann man 1 als Produkt von Primzahlen schreiben? Ganz einfach: Wir nehmen das *leere Produkt*:

$$\prod_{p\in\emptyset} p = 1\,.$$

Sei jetzt $n > 1$. Dann hat n nach Satz 3.2 einen Primteiler p; wir können also schreiben $n = pm$. Wegen $p > 1$ ist $m < n$ (und positiv). Nach Induktionsannahme ist m ein Produkt von Primzahlen: $m = p_1 \cdots p_k$ (hier ist $k = 0$ erlaubt, wenn $m = 1$ ist). Also ist

$$n = pm = pp_1 \cdots p_k$$

ebenfalls ein Produkt von Primzahlen. □

Wie sieht es mit der Eindeutigkeit dieser Faktorisierung in Primzahlen aus? Wir können natürlich die Reihenfolge der Faktoren ändern. Das Beste, was wir erwarten können, ist also, dass die Faktorisierung bis auf die Reihenfolge der Faktoren eindeutig ist. Um das zu zeigen, müssen wir erst eine andere Charakterisierung der Primzahlen beweisen.

3.4. **Satz.** *Eine ganze Zahl $p > 1$ ist genau dann Primzahl, wenn für alle ganzen Zahlen a und b Folgendes gilt:*

$$p \mid ab \implies p \mid a \quad \textit{oder} \quad p \mid b\,.$$

Beweis. Wir beweisen zunächst, dass Primzahlen die angegebene Eigenschaft haben. Wir nehmen also an, dass p das Produkt ab teilt. Wir können zusätzlich annehmen, dass $p \nmid a$ (sonst wären wir ja fertig) und müssen dann zeigen, dass $p \mid b$. Wir erinnern uns an Lemma 2.16, das eine Aussage wie die gewünschte liefert. Um es anwenden zu können, müssen wir $p \perp a$ zeigen. Das folgt aber daraus, dass p eine Primzahl ist und a nicht teilt: $\mathrm{ggT}(p, a)$ muss ein positiver Teiler von p sein, also kommen nur 1 und p in Frage, aber p ist kein Teiler von a, also ist $\mathrm{ggT}(p, a) \neq p$ und damit $\mathrm{ggT}(p, a) = 1$.

Sei jetzt umgekehrt $p > 1$ eine ganze Zahl, die die angegebene Eigenschaft hat. Wir müssen zeigen, dass p eine Primzahl ist. Sei also $p = ab$ mit $a, b \in \mathbb{Z}$. Dann gilt natürlich $p \mid ab$, aus der Voraussetzung folgt also $p \mid a$ oder $p \mid b$. Da auch $a \mid p$ und $b \mid p$, folgt $a = \pm p$ oder $b = \pm p$ und damit $b = \pm 1$ oder $a = \pm 1$. Damit ist die definierende Eigenschaft einer Primzahl nachgewiesen. □

Es ergibt sich sofort folgende Verallgemeinerung.

3.5. **Folgerung.** *Sei p eine Primzahl. Teilt p ein Produkt $a_1 a_2 \cdots a_k$, so teilt p einen der Faktoren a_j.*

(Eine Primzahl, die ein Produkt teilt, teilt auch einen der Faktoren.)

Diese Eigenschaft der Primzahlen erlaubt es uns jetzt, zwei Faktorisierungen einer ganzen Zahl miteinander zu vergleichen. Wir schieben noch ein leichtes Lemma ein.

3.6. **Lemma.** *Sind p und q Primzahlen, und gilt $p \mid q$, so folgt $p = q$.*

Beweis. Wegen $p \mid q$ gilt $q = pr$ mit $r \in \mathbb{Z}$. Da p und q positiv sind, ist $r > 0$. Da q prim ist, folgt $p = \pm 1$ oder $r = \pm 1$; mit $p > 1$ und $r > 0$ bleibt $r = 1$ als einzige Möglichkeit. Damit ist $q = pr = p$. □

3.7. **Satz von der eindeutigen Primfaktorzerlegung.** *Sei n eine positive ganze Zahl. Dann lässt sich n bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen schreiben. Sind also*

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

zwei Darstellungen von n als Produkt von Primzahlen, dann gibt es gibt eine Bijektion $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, l\}$, so dass $q_{\sigma(j)} = p_j$ für alle $1 \leq j \leq k$; insbesondere gilt $k = l$.

Beweis. Die Existenz der Primfaktorzerlegung wurde schon in Satz 3.3 bewiesen. Es bleibt also noch die Eindeutigkeit zu zeigen. Sei also

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

wie oben im Satz (dabei ist $k = 0$ und/oder $l = 0$ erlaubt). Wir können $k \geq l$ annehmen. Für den Beweis verwenden wir Induktion nach k. Ist $k = 0$, dann gilt auch $l = 0$ und $n = 1$, und die Behauptung ist trivialerweise richtig (denn es gibt eine Bijektion $\sigma : \emptyset \to \emptyset$). Sei also jetzt $k > 0$. Dann ist p_1 ein Faktor im ersten Produkt, und $p_1 \mid n = q_1 q_2 \cdots q_l$. Nach Folgerung 3.5 gibt es dann $1 \leq i_1 \leq l$ mit $p_1 \mid q_{i_1}$. Nach Lemma 3.6 folgt $q_{i_1} = p_1$. Sei jetzt

$$n' = \frac{n}{p_1} = \frac{n}{q_{i_1}} = p_2 p_3 \cdots p_k = q_1 q_2 \cdots q_{i_1 - 1} q_{i_1 + 1} \cdots q_l \,.$$

Dann hat das erste Produkt $k - 1$, das zweite $l - 1$ Faktoren. Nach Induktionsannahme gibt es eine Bijektion $\tau : \{2, 3, \ldots, k\} \to \{1, 2, \ldots, l\} \setminus \{i_1\}$, so dass $q_{\tau(j)} = p_j$ für alle $2 \leq j \leq k$. Wir definieren $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, l\}$ durch $\sigma(1) = i_1$, $\sigma(j) = \tau(j)$ für $j > 1$. Dann ist σ eine Bijektion mit $q_{\sigma(j)} = p_j$ für alle $1 \leq j \leq k$. □

Wir werden bald sehen, dass dieser Satz keine Selbstverständlichkeit ist: Es gibt Ringe, die dem Ring $\mathbb{Z}$ sehr ähnlich sind, in denen der Satz aber nicht gilt.

Wir können die Produktdarstellung eindeutig machen, indem wir die Faktoren der Größe nach anordnen:

3.8. **Folgerung.** *Jede positive ganze Zahl n kann eindeutig geschrieben werden als*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

mit Primzahlen $p_1 < p_2 < \ldots < p_k$ und Exponenten $e_j \geq 1$.

Dabei kann $k = 0$ sein; dann ist $n = 1$.

Die Häufigkeit, mit der eine Primzahl p in der Primfaktorzerlegung von n vorkommt, ist eine wichtige Größe. Wir führen dafür eine Bezeichnung ein.

3.9. **Definition.** Sei $n \in \mathbb{Z} \setminus \{0\}$ und p eine Primzahl. Wir setzen

$$v_p(n) = \max\{m \in \mathbb{Z}_{\geq 0} \mid p^m \text{ teilt } n\}\,.$$

Dann ist $v_p(n)$ eine nichtnegative ganze Zahl (denn $p^0 \mid n$, also ist die Menge oben nicht leer, und $p^m \mid n$ impliziert $p^m \leq |n|$, also ist die Menge beschränkt, und das Maximum existiert). Wir setzen noch $v_p(0) = +\infty$ in Analogie mit der Definition oben ($+\infty$ wird als Supremum der unbeschränkten Menge $\mathbb{Z}_{\geq 0}$ betrachtet). Die Zahl $v_p(n)$ wird die *p-adische Bewertung* von n genannt.

Für $n \neq 0$ folgt, dass $n = p^{v_p(n)} r$ ist mit $p \nmid r$.

3.10. **Lemma.** *Sei $n \in \mathbb{Z}_{>0}$, $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ wie in Folgerung 3.8. Dann gilt $v_{p_j}(n) = e_j$ für alle $1 \leq j \leq k$ und $v_p(n) = 0$ für alle Primzahlen $p \notin \{p_1, p_2, \ldots, p_k\}$.*

Beweis. Sei p eine beliebige Primzahl. Gilt $v_p(n) > 0$, dann muss p ein Teiler von $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ sein. Nach Folgerung 3.5 gilt dann $p \mid p_j$ für ein $1 \leq j \leq k$, nach Lemma 3.6 folgt $p = p_j$. Damit ist die Behauptung für $p \notin \{p_1, p_2, \ldots, p_k\}$ gezeigt. Sei jetzt also $p = p_j$. Dann gilt offenbar $p^{e_j} \mid n$, also $v_{p_j}(n) \geq e_j$. Sei $n' = n/p^{e_j} = \prod_{i \neq j} p_i^{e_i}$. Wäre $v_{p_j}(n) > e_j$, dann würde $p \mid n'$ folgen, aber nach dem Argument oben kann das nicht gelten. Also gilt $v_{p_j}(n) = e_j$. □

3.11. **Satz.** *Sei $n \in \mathbb{Z}$, $n \neq 0$. Dann gilt*

$$n = \operatorname{sign}(n) \prod_p p^{v_p(n)}\,.$$

Das Produkt läuft dabei über alle Primzahlen. Alle bis auf endliche viele Faktoren haben den Wert 1, so dass das Produkt definiert ist.

Beweis. Wir können offenbar annehmen, dass $n > 0$ ist. Aus Lemma 3.10 folgt, dass $v_p(n) = 0$ ist für alle bis auf endlich viele Primzahlen p; damit ist $p^{v_p(n)} = 1$ für diese p. Das Produkt ist also definiert und stimmt mit $p_1^{v_{p_1}(n)} \cdots p_k^{v_{p_k}(n)}$ überein, wobei $p_1 < p_2 < \ldots < p_k$ die Primzahlen p sind mit $v_p(n) > 0$. Aus Lemma 3.10 folgt dann die Behauptung. □

Die p-adische Bewertung hat folgende Eigenschaften.

3.12. **Proposition.** *Seien $m, n \in \mathbb{Z}$ und p eine Primzahl. Dann gilt*

(1) $v_p(mn) = v_p(m) + v_p(n)$.
(2) $v_p(m+n) \geq \min\{v_p(m), v_p(n)\}$ *mit Gleichheit, falls* $v_p(m) \neq v_p(n)$.

Dabei setzen wir $e + \infty = +\infty$ und $\min\{e, +\infty\} = e$ für $e \in \mathbb{Z} \cup \{+\infty\}$.

Beweis.

(1) Für $m = 0$ oder $n = 0$ ist die Aussage klar. Seien also $m, n \neq 0$. Dann können wir $m = p^{v_p(m)} s$, $n = p^{v_p(n)} t$ schreiben mit $s, t \in \mathbb{Z}$, $p \nmid s$, $p \nmid t$. Aus Satz 3.4 folgt, dass $p \nmid st$. Wegen $mn = p^{v_p(m)+v_p(n)} \cdot st$ folgt die Behauptung.

(2) Sei $e = \min\{v_p(m), v_p(n)\}$. Ist $e = +\infty$, dann gilt $m = n = 0$, und die Behauptung ist klar. Sei also $e < +\infty$. Dann gilt $p^e \mid m$ und $p^e \mid n$, also $p^e \mid m+n$, was gerade $v_p(m+n) \geq e$ bedeutet. Das beweist den ersten Teil der Behauptung. Für den zweiten Teil können wir annehmen, dass $v_p(m) = e < v_p(n)$. Nach dem ersten Teil ergibt sich

$$\begin{aligned} e = v_p(m) &= v_p\big((m+n)+(-n)\big) \\ &\geq \min\{v_p(m+n), v_p(-n)\} = \min\{v_p(m+n), v_p(n)\}\,, \end{aligned}$$

und weil $v_p(n) > e$, sehen wir, dass

$$e \geq v_p(m+n) \geq e\,,$$

was die gewünschte Gleichheit liefert.

□

3.13. **Folgerung.** *Seien $m, n \in \mathbb{Z}$. Dann gilt*

(1) $m \mid n \iff v_p(m) \leq v_p(n)$ *für alle Primzahlen p.*
(2) *für alle Primzahlen p:* $v_p\big(\mathrm{ggT}(m,n)\big) = \min\{v_p(m), v_p(n)\}$.
(3) $m \perp n \iff \min\{v_p(m), v_p(n)\} = 0$ *für alle Primzahlen p.*
(4) *für alle Primzahlen p:* $v_p\big(\mathrm{kgV}(m,n)\big) = \max\{v_p(m), v_p(n)\}$.

Beweis.

(1) $m \mid n$ bedeutet $n = mk$ mit einem $k \in \mathbb{Z}$, also nach Proposition 3.12 $v_p(n) = v_p(m) + v_p(v) \geq v_p(m)$ für alle Primzahlen p. Gilt umgekehrt $v_p(n) \geq v_p(m)$ für alle Primzahlen p und $n \neq 0$, dann folgt $n = \pm mk$ mit $k = \prod_p p^{v_p(n)-v_p(m)}$ (das Produkt ist definiert, da $v_p(n) = v_p(m) = 0$ für alle bis auf endlich viele p), also gilt $m \mid n$. Für $n = 0$ gilt $m \mid n$ sowieso immer.
(2) Sei $g = \mathrm{ggT}(m,n)$. Der Fall $m = 0$ oder $n = 0$ ist klar; seien also $m, n \neq 0$. nach Teil (1) gilt $v_p(g) \leq \min\{v_p(m), v_p(n)\}$. Sei auf der anderen Seite $g' = \prod_p p^{\min\{v_p(m), v_p(n)\}}$ (wie oben sind alle bis auf endlich viele Exponenten null), dann gilt nach Teil (1), dass g' ein gemeinsamer Teiler von m und n ist. Es folgt $g' \mid g$, also $v_p(g) \geq \min\{v_p(m), v_p(n)\}$ (und gleichzeitig $g = g'$).
(3) Das ist ein Spezialfall von Teil (2).
(4) Das geht völlig analog zu Teil (2).

□

Man kann das Resultat von Teil (3) auch so formulieren:

$$m \perp n \iff \sum_p v_p(m) \cdot v_p(n) = 0\,.$$

Rechts steht so etwas wie das „Skalarprodukt“ der „Vektoren“ $(v_p(m))_p$ und $(v_p(n))_p$. Das kann man als Motivation für die Schreibweise „$m \perp n$“ betrachten.

3.14. **Bemerkung.** Sind $m, n \neq 0$, dann gilt also

$$\mathrm{ggT}(m,n) = \prod_p p^{\min\{v_p(m), v_p(n)\}} \qquad \text{und} \qquad \mathrm{kgV}(m,n) = \prod_p p^{\max\{v_p(m), v_p(n)\}}\,.$$

Diese Methode zur Berechnung des größten gemeinsamen Teilers wird bisweilen in der Schule gelehrt. Sie ist aber extrem ineffizient, wenn m und n groß sind, weil die Zahlen erst faktorisiert werden müssen. Der Euklidische Algorithmus ist die viel bessere Methode!

4. Gruppen, Ringe und Integritätsbereiche

Nachdem wir uns den Satz über die eindeutige Primfaktorzerlegung in $\mathbb{Z}$ erarbeitet haben, wollen wir nun untersuchen, in wie weit dieser Satz auch in allgemeineren Ringen noch gilt. Dazu führen wir erst einmal (neben den Ringen, die wir schon kurz gesehen haben) einige Typen von algebraischen Strukturen ein.

4.1. **Definition.** Eine *Halbgruppe* ist ein Paar $(H, *)$, bestehend aus einer Menge H und einer Abbildung („Verknüpfung“) $* : H \times H \to H$, $(a, b) \mapsto a * b$, die das *Assoziativgesetz* erfüllt:

$$\forall a, b, c \in H : (a * b) * c = a * (b * c) .$$

Die Halbgruppe heißt *kommutativ*, wenn zusätzlich das *Kommutativgesetz* gilt:

$$\forall a, b \in H : a * b = b * a .$$

Meistens spricht man kurz von der „Halbgruppe H“; die Verknüpfung ist dann aus dem Zusammenhang ersichtlich. Analoge Bemerkungen gelten für die nachfolgend definierten Strukturen.

Die „einfachste“ Halbgruppe ist die leere Menge (in der Definition wird nicht die Existenz von irgendwelchen Elementen verlangt).

4.2. **Beispiel.** $(\mathbb{Z}_{>0}, +)$ ist eine kommutative Halbgruppe.

4.3. **Definition.** Ein *Monoid* ist ein Tripel $(M, e, *)$, bestehend aus einer Menge M, einem Element $e \in M$ und einer Verknüpfung $* : M \times M \to M$, so dass $(M, *)$ eine Halbgruppe ist und zusätzlich e ein *neutrales Element* ist:

$$\forall a \in M : e * a = a = a * e .$$

Das Monoid ist *kommutativ*, wenn die unterliegende Halbgruppe kommutativ ist.

Es kann in einer Halbgruppe höchstens ein neutrales Element geben: Sind e und e' zwei neutrale Elemente, dann folgt $e = e * e' = e'$.

Das „einfachste“ Monoid ist $\{e\}$: Wir brauchen ein neutrales Element, und mit der zwangsläufigen Definition $e * e = e$ sind alle Bedingungen erfüllt.

4.4. **Beispiel.** Sei X eine Menge und $\mathrm{Abb}(X, X)$ die Menge der Abbildungen $f : X \to X$. Dann ist $(\mathrm{Abb}(X, X), \mathrm{id}_X, \circ)$ ein Monoid, das nicht kommutativ ist, wenn X mehr als ein Element hat. ($f \circ g$ ist die Hintereinanderausführung von f und g: $(f \circ g)(x) = f(g(x))$.)

4.5. **Definition.** Eine *Gruppe* ist ein Quadrupel $(G, e, *, i)$, bestehend aus einer Menge G, einem Element $e \in G$, einer Verknüpfung $* : G \times G \to G$ und einer Abbildung $i : G \to G$, so dass $(G, e, *)$ ein Monoid ist und zusätzlich folgendes gilt:

$$\forall a \in G : a * i(a) = e = i(a) * a .$$

Das Element $i(a) \in G$ heißt das *Inverse* von a. Die Gruppe heißt *kommutativ* oder *abelsch*, wenn das unterliegende Monoid kommutativ ist. Häufige Schreibweisen sind $(G, 1, \cdot, g \mapsto g^{-1})$ für allgemeine Gruppen und $(G, 0, +, g \mapsto -g)$ für abelsche Gruppen.

In einem Monoid gibt es zu einem Element a höchstens ein Inverses: Sind b und c zwei Inverse von a, so folgt $b = b * e = b * (a * c) = (b * a) * c = e * c = c$.

Genauer zeigt dieses Argument, dass Links- und Rechtsinverse übereinstimmen, wenn beide existieren. Gibt es nur (z.B.) Linksinverse eines Elements, kann es mehrere verschiedene geben. Nimmt man im Beispiel 4.4 etwa $X = \mathbb{N}$, dann hat die Nachfolgerabbildung unendlich viele verschiedene Linksinverse (jede Abbildung, die $S(n)$ auf n und 0 irgendwo hin abbildet), aber kein Rechtsinverses.

4.6. **Beispiele.**

(1) Die „einfachste“ Gruppe ist die *triviale Gruppe* $\{e\}$ (mit der offensichtlichen Verknüpfung und Inversenabbildung).
(2) $(\mathbb{Z}, 0, +, -)$ ist eine abelsche Gruppe.
(3) Sei X eine Menge und G die Menge der Bijektionen $X \to X$ (Permutationen von X). Dann ist $(G, \mathrm{id}_X, \circ, f \mapsto f^{-1})$ eine Gruppe, die nicht abelsch ist, wenn X mehr als zwei Elemente enthält.
(4) Die Menge $\mathrm{GL}_n(\mathbb{R})$ der reellen invertierbaren $n \times n$-Matrizen trägt eine Gruppenstruktur: $(\mathrm{GL}_n(\mathbb{R}), I_n, \cdot, A \mapsto A^{-1})$ (dabei ist I_n die Einheitsmatrix und $\cdot$ die Matrizenmultiplikation). Diese Gruppe ist nicht abelsch für $n \geq 2$.

Man kann aus einem Monoid eine Gruppe extrahieren (das verallgemeinert das Beispiel (3) oben):

4.7. **Lemma.** *Sei $(M, e, *)$ ein Monoid, und sei $G \subset M$ die Teilmenge der invertierbaren Elemente von M, also*

$$G = \{m \in M \mid \exists m' \in M : m * m' = e = m' * m\}.$$

Dann gibt es eine eindeutig bestimmte Abbildung $i : G \to G$, so dass $(G, e, *|_{G\times G}, i)$ eine Gruppe ist.

Beweis. Übung. □

Gruppen sind die „schönsten“ algebraischen Strukturen mit *einer* Verknüpfung. Sie sind wichtig, weil sie als „Symmetriegruppen“ oder „Automorphismengruppen“ in vielen Zusammenhängen auftreten. Wir werden sie im nächsten Semester in der „Einführung in die Algebra“ genauer studieren. Wir wenden uns jetzt Strukturen mit *zwei* Verknüpfungen zu.

4.8. **Definition.** (Vergleiche Definition 1.6.)
Ein *Ring* ist ein Sextupel $(R, 0, 1, +, -, \cdot)$, bestehend aus einer Menge R, Elementen $0, 1 \in R$, Verknüpfungen $+$ (Addition) und $\cdot$ (Multiplikation) : $R \times R \to R$ und einer Abbildung $-$ (Negation) : $R \to R$, so dass $(R, 0, +, -)$ eine abelsche Gruppe und $(R, 1, \cdot)$ ein Monoid ist, und außerdem folgende *Distributivgesetze* gelten:

$$\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Der Ring heißt *kommutativ*, wenn das Monoid $(R, 1, \cdot)$ kommutativ ist. Die nach Lemma 4.7 existierende Gruppe der invertierbaren Elemente des Monoids $(R, 1, \cdot)$ heißt die *Einheitengruppe* von R und wird $R^\times$ geschrieben. Ihre Elemente heißen die *Einheiten* von R.

Wenn mehrere Ringe (oder Strukturen) im Spiel sind, schreiben wir manchmal 0_R, 1_R, $+_R$ usw., um zu verdeutlichen, welche Struktur gemeint ist.

4.9. **Beispiele.**

(1) Der „einfachste“ Ring ist der *Nullring* $R = \{0\}$ mit der einzig möglichen Struktur. In diesem Fall gilt $0_R = 1_R$. Umgekehrt gilt: Stimmen Null- und Einselement in einem Ring überein, so ist der Ring der Nullring (d.h., er hat nur das eine Element $0_R = 1_R$): $a = 1 \cdot a = 0 \cdot a = 0$, siehe Proposition 4.13 unten.

(1′) Der einfachste Ring, der nicht der Nullring ist, ist $\mathbb{F}_2 = \{0, 1\}$; es gibt nur eine mögliche Wahl der Verknüpfungen, so dass die Ringaxiome erfüllt sind. In $\mathbb{F}_2$ gilt $1 + 1 = 0$, da $-1 = 1$ sein muss (denn $-1 \neq 0$). $\mathbb{F}_2$ ist sogar ein Körper (Definition siehe unten).

(2) $(\mathbb{Z}, 0, 1, +, -, \cdot)$ ist ein kommutativer Ring; es gilt $\mathbb{Z}^\times = \{\pm 1\}$.

(3) Sei $\mathrm{Mat}_n(\mathbb{R})$ die Menge der reellen $n \times n$-Matrizen.
Dann ist $(\mathrm{Mat}_n(\mathbb{R}), 0_n, I_n, +, -, \cdot)$ ein Ring (dabei ist 0_n die $n \times n$-Nullmatrix; die Abbildungen sind Addition, Negation und Multiplikation von Matrizen). Dieser Ring ist nicht kommutativ, wenn $n \geq 2$ ist (Übung).
Die Einheitengruppe ist $\mathrm{Mat}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$.

(4) Sei X eine Menge und $P(X)$ die Potenzmenge von X (also die Menge aller Teilmengen von X). Dann ist $(P(X), \emptyset, X, \triangle, \mathrm{id}_{P(X)}, \cap)$ ein kommutativer Ring; dabei bezeichnet

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

die *symmetrische Differenz* von A und B. (Übung.)

(5) Sei X eine Menge und R ein Ring. Dann ist die Menge R^X der Abbildungen von X nach R in natürlicher Weise ein Ring, wenn man Addition und Multiplikation „punktweise“ definiert:

$$(f + g)(x) = f(x) + g(x) \quad \text{und} \quad (f \cdot g)(x) = f(x) \cdot g(x)\,.$$

Zum Beispiel bilden die reellen Funktionen $f : \mathbb{R} \to \mathbb{R}$ auf diese Weise einen Ring.

Beispiel (4) oben kann als Spezialfall von Beispiel (5) verstanden werden, wenn man $R = \mathbb{F}_2$ nimmt ($\mathbb{F}_2$ ist der Körper mit zwei Elementen aus Beispiel (1′)).

Wie Sie das in der Linearen Algebra mit Untervektorräumen bereits kennen gelernt haben, betrachtet man generell in algebraischen Strukturen Unterstrukturen. Wir formulieren das am Beispiel der Ringe (analog definiert man Untermonoide, Untergruppen usw.).

4.10. **Definition.** Sei $(R, 0, 1, +, -, \cdot)$ ein Ring. Eine Teilmenge $S \subset R$ ist ein *Unterring* (engl. *subring*) von R, wenn $0 \in S$, $1 \in S$ und S unter $+$, $-$ und $\cdot$ abgeschlossen ist (d.h., aus $s, s' \in S$ folgt $s + s', -s, s \cdot s' \in S$).

Es ist leicht zu sehen, dass in diesem Fall $(S, 0, 1, +|_{S\times S}, -|_S, \cdot|_{S\times S})$ ebenfalls ein Ring ist.

4.11. **Beispiele.**

(1) $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$.

(2) $\mathbb{Z}_{\geq 0}$ ist kein Unterring von $\mathbb{Z}$, weil $\mathbb{Z}_{\geq 0}$ nicht unter der Negation abgeschlossen ist.

(3) Die *stetigen* Funktionen $f : \mathbb{R} \to \mathbb{R}$ bilden einen Unterring des Rings der reellen Funktionen (wir wissen aus der Analysis, dass Summe, Negation und Produkt stetiger Funktionen wieder stetig sind).

(4) Sei R ein Ring. Dann ist $R^2 = R \times R$ ein Ring wie in Beispiel 4.9, (5). Die Teilmenge $R \times \{0\}$ ist *kein* Unterring, obwohl sie unter Addition, Negation und Multiplikation abgeschlossen ist, das Nullelement enthält, und die Multiplikation auf $R \times \{0\}$ das neutrale Element $(1, 0)$ hat. Der Grund ist, dass die Teilmenge nicht das Einselement $(1, 1)$ von $R \times R$ enthält.

Es gibt noch eine „schönere“ Variante von Ringen, die Sie bereits kennen, und die für uns in dieser Vorlesung erst einmal weniger von Interesse sein wird.

4.12. **Definition.** Ein *Schiefkörper* (engl. *skew field* oder *division ring*) beziehungsweise *Körper* (engl. *field*) ist ein Septupel $(K, 0, 1, +, -, \cdot, a \mapsto a^{-1})$, bestehend aus einer Menge K, Elementen $0, 1 \in K$, zwei Verknüpfungen $+, \cdot : K \times K \to K$ und Abbildungen $- : K \to K$ und $a \mapsto a^{-1} : K \setminus \{0\} \to K \setminus \{0\}$, so dass $(K, 0, 1, +, -, \cdot)$ ein nichtkommutativer bzw. kommutativer Ring und $(K \setminus \{0\}, 1, \cdot, a \mapsto a^{-1})$ eine Gruppe ist. (Insbesondere muss $0 \neq 1$ gelten.)

Für K als Ring gilt dann also $K^\times = K \setminus \{0\}$; wir behalten dies als Schreibweise für die *multiplikative Gruppe* eines (Schief)Körpers bei. Ist umgekehrt R ein Ring mit $R^\times = R \setminus \{0\}$, dann „ist“ R ein Schiefkörper oder Körper (d.h., die eindeutig bestimmte Inversenabbildung der Gruppe $R^\times$ ergänzt die Struktur von R zu der eines Körpers).

Wir schreiben ein paar einfache Aussagen auf, die in allen Ringen gelten:

4.13. **Proposition.** *Sei R ein Ring, und seien $a, b \in R$. Dann gilt:*

(1) $0 \cdot a = a \cdot 0 = 0$.
(2) $(-1) \cdot a = a \cdot (-1) = -a$.
(3) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ *und* $(-a) \cdot (-b) = a \cdot b$.

Beweis. Übung. □

Eine Aussage, die nicht in allen Ringen gilt, ist die *Kürzungsregel:*

$$\forall a, b, c \in R : a \neq 0,\ ab = ac \implies b = c\,.$$

Durch Subtraktion können wir das auf den Fall $c = 0$ zurückführen.

4.14. **Definition.** Sei R ein Ring. Ein Element $a \in R$ heißt *Nullteiler*, wenn $a \neq 0$ und es $0 \neq b \in R$ gibt mit $ab = 0$. Ein Ring mit $0 \neq 1$, der keine Nullteiler besitzt, heißt *nullteilerfrei* oder *Integritätsring*. Ein kommutativer Integritätsring heißt *Integritätsbereich* (engl. *integral domain*).

4.15. **Beispiele.**

(1) Der Ring der ganzen Zahlen ist ein Integritätsbereich. (Daher kommt der Name *Integritäts*bereich: integer = ganz.)
(2) Jeder Schiefkörper ist ein Integritätsring, jeder Körper ein Integritätsbereich.
(3) Der Matrizenring $\mathrm{Mat}_2(\mathbb{R})$ ist kein Integritätsring, denn es gilt zum Beispiel

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(4) Die Ringe aus Beispiel 4.9, (5), sind keine Integritätsringe, wenn X mindestens zwei Elemente hat: Für $x \in X$ sei $\delta_x : X \to R$ die Abbildung mit $\delta_x(x) = 1$ und $\delta_x(y) = 0$ für alle $y \neq x$. Sind x_0 und x_1 zwei verschiedene Elemente von X (und ist R nicht der Nullring), dann gilt $\delta_{x_0} \neq 0$, $\delta_{x_1} \neq 0$, aber $\delta_{x_0} \cdot \delta_{x_1} = 0$ in R^X.
(5) Der Ring der stetigen reellen Funktionen ist kein Integritätsbereich (denn wir haben etwa mit $f(x) = \max\{0, x\}$ und $g(x) = \max\{0, -x\}$, dass $f \cdot g$ die Nullfunktion ist).
(6) Demgegenüber ist der Ring der holomorphen Funktionen auf einem Gebiet (zusammenhängende offene Menge) $U \subset \mathbb{C}$ ein Integritätsbereich: Ist f holomorph auf U und nicht die Nullfunktion, dann liegen die Nullstellen von f isoliert. Das selbe gilt für das Produkt von zwei von der Nullfunktion verschiedenen holomorphen Funktionen, so dass das Produkt nicht die Nullfunktion sein kann (siehe Funktionentheorie).

4.16. **Bemerkung.** *Ein Unterring eines Integritätsrings ist wieder ein Integritätsring. Insbesondere ist ein Unterring eines Körpers stets ein Integritätsbereich.*

Beweis. Klar. □

Die Frage, ob jeder Integritätsbereich als Unterring eines Körpers aufgefasst werden kann, werden wir später in dieser Vorlesung beantworten.

5. Faktorisierung in Integritätsbereichen

Wir wollen jetzt die Faktorisierung in allgemeineren Ringen studieren. Es ist ziemlich klar, dass man keine schöne Theorie erwarten kann, wenn es Nullteiler gibt, also arbeiten wir mit Integritätsringen. Außerdem beschränken wir uns auf kommutative Ringe; sonst geht zu viel von dem verloren, was wir vom Arbeiten mit dem Ring der ganzen Zahlen gewohnt sind. Wir nehmen daher in diesem Kapitel generell an, dass jeder Ring ein **Integritätsbereich** ist, sofern nicht explizit etwas anderes gesagt wird.

Als erstes verallgemeinern wir den Begriff der Teilbarkeit.

5.1. **Definition.** Sei R ein Integritätsbereich, und seien $a, b \in R$. Wir sagen, *a teilt b*, *a ist ein Teiler von b*, *b ist ein Vielfaches von a* und schreiben $a \mid b$, wenn es ein $c \in R$ gibt mit $b = ac$.

Zwei Elemente $a, b \in R$ heißen *assoziiert*, und wir schreiben $a \sim b$, wenn es eine Einheit $u \in R^\times$ gibt mit $b = au$. (Übung: Das definiert eine Äquivalenzrelation, wie die Schreibweise suggeriert.)

Die Eigenschaften der Teilbarkeitsrelation gelten dann analog (außer der letzten Eigenschaft in Proposition 2.2, die auf die Anordnung von $\mathbb{Z}$ Bezug nimmt).

5.2. **Proposition.** *Seien $a, b, c \in R$. Es gilt:*

(1) *Aus $a \mid b$ und $a \mid c$ folgt $a \mid b \pm c$.*
(2) *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.*
(3) *Aus $a \mid b$ folgt $a \mid bc$.*
(4) $0 \mid a \iff a = 0$ *und* $a \mid 1 \iff a \in R^\times$.
(5) $a \mid 0$, $1 \mid a$ *und* $a \mid a$.
(6) $a \mid b$ *und* $b \mid a$ *ist äquivalent zu* $a \sim b$.

Beweis. Leicht und analog zu Proposition 2.2. □

Als nächstes wollen wir Analoga zu Primzahlen definieren. Hier tritt eine Schwierigkeit auf: Primzahlen sind durch zwei verschiedene Eigenschaften charakterisiert. Wir geben ihnen hier verschiedene Namen.

5.3. **Definition.** Ein Element $r \in R$ heißt *irreduzibel*, wenn $r \neq 0$, $r \notin R^\times$, und wenn für jede Faktorisierung $r = st$ in R gilt, dass $s \in R^\times$ oder $t \in R^\times$.

Irreduzible Elemente können also nicht multiplikativ zerlegt werden.

5.4. **Definition.** Ein Element $p \in R$ heißt *prim* oder *Primelement*, wenn $p \neq 0$, $p \notin R^\times$, und wenn für $r, s \in R$ aus $p \mid rs$ stets $p \mid r$ oder $p \mid s$ folgt.

Wir haben gesehen, dass im Ring $\mathbb{Z}$ beide Definitionen äquivalent sind. Allgemein gilt immerhin noch eine Implikation:

5.5. **Lemma.** *Jedes Primelement in einem Integritätsbereich ist auch irreduzibel.*

Beweis. Der Beweis ist der selbe wie für Primzahlen: Sei $p \in R$ ein Primelement. Gilt $p = rs$ mit $r, s \in R$, dann erst recht $p \mid rs$, nach Definition also $p \mid r$ oder $p \mid s$. Da aber auch $r \mid p$ und $s \mid p$, folgt $r \sim p$ oder $s \sim p$ und damit $s \in R^\times$ oder $r \in R^\times$. □

5.6. **Beispiel.** Die Umkehrung der Aussage von Lemma 5.5 gilt nicht. Zum Beispiel können wir $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ betrachten (wobei $\sqrt{-5} = \sqrt{5}\,i$ eine der Quadratwurzeln von -5 in $\mathbb{C}$ ist). Es ist leicht zu sehen, dass R ein Unterring von $\mathbb{C}$ ist; damit ist R ein Integritätsbereich. Man kann sich davon überzeugen, dass $2 \in R$ irreduzibel ist. Andererseits gilt $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, aber 2 teilt keinen der beiden Faktoren, also ist $2 \in R$ kein Primelement. Man kann auch zeigen, dass die beiden Zerlegungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

als Produkt irreduzibler Elemente wesentlich verschieden sind (Übung).

Es ist auch keineswegs garantiert, dass jedes Element ($\neq 0$ und keine Einheit) eines Integritätsrings sich als Produkt von irreduziblen Elementen schreiben lassen muss. Beispiele dafür sind etwas schwieriger zu konstruieren. Wir beginnen mit einem Beispiel für einen Ring, der (bis auf Assoziierte) genau ein irreduzibles Element besitzt.

5.7. **Beispiel.** Sei $R = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, 2 \nmid b\} \subset \mathbb{Q}$. Dann ist R ein Unterring von $\mathbb{Q}$, also ein Integritätsbereich. Die Einheitengruppe ist $R^\times = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, 2 \nmid a, 2 \nmid b\}$, und jedes Element $0 \neq r \in R$ kann eindeutig geschrieben werden in der Form $r = u2^n$ mit $u \in R^\times$ und $n \in \mathbb{Z}_{\geq 0}$ (Übung). Daraus folgt, dass $2 \in R$ bis auf Assoziierte das einzige irreduzible Element von R ist; gleichzeitig ist $2 \in R$ ein Primelement, und der Satz von der eindeutigen Primfaktorzerlegung gilt in R in einer sehr einfachen Form.

Im nächsten Beispiel gibt es gar keine irreduziblen Elemente.

5.8. **Beispiel.** Sei $R_0 = R \subset \mathbb{Q} \subset \mathbb{R}$ wie in Beispiel 5.7. Wir definieren induktiv für $n \geq 1$

$$R_n = \{a + b2^{1/2^n} \mid a, b \in R_{n-1}\} \subset \mathbb{R}\,.$$

Dann gilt, dass $R_0 \subset R_1 \subset R_2 \subset \ldots \subset \mathbb{R}$ eine aufsteigende Folge von Unterringen von $\mathbb{R}$ ist, und

$$S = R_0 \cup R_1 \cup R_2 \cup \ldots = \bigcup_{n\geq 0} R_n \subset \mathbb{R}$$

ist ebenfalls ein Unterring von $\mathbb{R}$, also ein Integritätsbereich (Übung).

Um die Schreibweise zu vereinfachen, setzen wir $w_n = 2^{1/2^n}$. Dann gilt also $w_0 = 2$ und $w_{n+1}^2 = w_n$.

Für $r = a + bw_n \in R_n$ mit $a, b \in R_{n-1}$ gilt: $r = 0 \iff a = b = 0$. Für $n = 1$ folgt das aus $w_1 = \sqrt{2} \notin \mathbb{Q}$. Allgemein hätte man sonst $w_n = -a/b$ und damit $w_{n-1} = a^2/b^2$, also $a^2 - b^2 w_{n-1} = 0$, und man kann Induktion anwenden und auf $a = b = 0$ schließen.

Wir definieren Abbildungen $N_n : R_n \to R_{n-1}$ (für $n \geq 1$) durch $N_n(a + bw_n) = a^2 - b^2 w_{n-1}$ (mit $a, b \in R_{n-1}$). Dann ist N_n *multiplikativ:*

$$\begin{aligned} N_n\big((a + bw_n)(c + dw_n)\big) &= N_n\big((ac + bdw_{n-1}) + (ad + bc)w_n\big) \\ &= (ac + bdw_{n-1})^2 - (ad + bc)^2 w_{n-1} \\ &= (a^2c^2 + b^2d^2w_{n-2}) - (a^2d^2 + b^2c^2)w_{n-1} \\ &= (a^2 - b^2w_{n-1})(c^2 - d^2w_{n-1}) \\ &= N_n(a + bw_n)N_n(c + dw_n) \end{aligned}$$

Ist $r \in R_n^\times$ eine Einheit, dann gibt es $s \in R_n$ mit $rs = 1$, und es folgt

$$1 = N_n(1) = N_n(rs) = N_n(r)N_n(s)\,,$$

also ist $N_n(r) \in R_{n-1}^\times$. Da (nachrechnen!) $N_n(a + bw_n) = (a + bw_n)(a - bw_n)$, folgt aus $N_n(r) \in R_{n-1}^\times \subset R_n^\times$ auch $r \in R_n^\times$.

Wir schreiben dies und weitere Folgerungen auf:

(1) $r \in R_n$ ist genau dann Einheit, wenn $N_n(r) \in R_{n-1}$ Einheit ist.
(2) $r \in R_n$ ist irreduzibel, wenn $N_n(r) \in R_{n-1}$ irreduzibel ist.
(3) Für jedes $n \geq 0$ ist w_n in R_n irreduzibel.

Die erste Aussage haben wir gerade bewiesen. Für die zweite Aussage bemerken wir erst einmal, dass $N_n(r) \in R_{n-1}$ irreduzibel insbesondere heißt $N_n(r) \notin \{0\} \cup R_{n-1}^\times$, woraus mit Aussage (1) $r \notin \{0\} \cup R_n^\times$ folgt. Sei nun $r = st$ eine Faktorisierung in R_n. Dann folgt $N_n(r) = N_n(s)N_n(t)$, und da $N_n(r)$ irreduzibel ist, muss $N_n(s)$ oder $N_n(t)$ eine Einheit sein. Nach Aussage (1) folgt dann, dass s oder t eine Einheit in R_n ist. Also ist r irreduzibel. Der Beweis der dritten Aussage geht durch Induktion. Für $n = 0$ folgt die Aussage aus Beispiel 5.7. Für $n \geq 1$ haben wir $N_n(w_n) = -w_{n-1}$, was nach Induktionsvoraussetzung in R_{n-1} irreduzibel ist. Nach Aussage (2) folgt dann, dass w_n in R_n irreduzibel ist.

Wir beweisen jetzt, dass folgende Aussagen für ein Element $r = a + bw_n \in R_n$ (mit $a, b \in R_{n-1}$) äquivalent sind:

(1) $w_n \mid r$;
(2) $w_{n-1} \mid a$;
(3) $r \notin R_n^\times$.

Die erste Aussage bedeutet, dass es $c, d \in R_{n-1}$ gibt mit $w_n(c + dw_n) = a + bw_n$; die linke Seite schreibt sich als $dw_{n-1} + cw_n$. Durch Koeffizientenvergleich sehen wir $w_{n-1} \mid a$. Umgekehrt funktioniert das Argument genauso; damit ist die Äquivalenz der ersten beiden Aussagen gezeigt. Der Beweis der Äquivalenz mit der dritten Aussage geht

wieder durch Induktion nach n. Für $n = 0$ sind (1) und (3) sinnvoll und äquivalent nach Beispiel 5.7. Für $n \geq 1$ haben wir

$$\begin{aligned} r \notin R_n^\times &\iff N_n(r) = a^2 - b^2 w_{n-1} \notin R_{n-1}^\times \\ &\overset{\text{IV}}{\iff} w_{n-1} \mid N_n(r) \iff w_{n-1} \mid a^2 \iff w_{n-1} \mid a\,. \end{aligned}$$

Für die letzte Äquivalenz haben wir benutzt, dass w_{n-1} sogar ein Primelement von R_{n-1} ist. Das sieht man auch durch Induktion: Sei $s = c + dw_n \in R_n$ mit $c, d \in R_{n-1}$ und r wie oben. Dann gilt (wegen der Äquivalenz von (1) und (2))

$$\begin{aligned} w_n \mid rs = (ac + bdw_{n-1}) + (ac + bd)w_n \\ \iff w_{n-1} \mid ac + bdw_{n-1} \iff w_{n-1} \mid ac \iff w_{n-1} \mid a \text{ oder } w_{n-1} \mid c \\ \iff w_n \mid r \text{ oder } w_n \mid s\,. \end{aligned}$$

Es folgt, dass es in R_n im wesentlichen nur ein irreduzibles Element gibt, nämlich w_n:

$$\text{Ist } r \in R_n \text{ irreduzibel, dann gilt } r \sim w_n.$$

Zum Beweis sei $r \in R_n$ irreduzibel, dann gilt $r \neq 0$ und $r \notin R_n^\times$, also folgt $w_n \mid r$. Aus $r = w_n s$ und r irreduzibel (und $w_n \notin R_n^\times$) folgt dann $s \in R_n^\times$, also $r \sim w_n$.

Jetzt aber zum eigentlichen Ziel:

S ist kein Körper (d.h. $S^\times \neq S \setminus \{0\}$), hat aber auch keine irreduziblen Elemente.

Für die erste Aussage bemerken wir, dass $2 \notin S^\times$ (denn sonst gäbe es $s \in S$ mit $2s = 1$; dann wäre aber $s \in R_n$ für ein geeignetes n, also auch $2 \in R_n^\times$, was aber wegen $w_n \mid 2$ nicht sein kann). Für die zweite Aussage sei $s \in S$ irreduzibel. Dann ist $s \neq 0$ und $s \notin S^\times$. Es gibt n mit $s \in R_n$; s ist keine Einheit in R_n (sonst wäre $s \in S^\times$), also folgt $w_n \mid s$, also $s = w_n t$. Dann gilt aber (in R_{n+1}), dass $s = w_{n+1} \cdot (w_{n+1} t)$ ein Produkt von zwei Nicht-Einheiten ist, also kann s nicht irreduzibel sein.

Wir haben jetzt an diesen Beispielen gesehen, dass beide Teile des Satzes über die eindeutige Primfaktorzerlegung schief gehen können: Es kann von null verschiedene Elemente geben, die keine Einheiten sind und sich nicht als Produkt von Irreduziblen schreiben lassen. Es ist aber auch möglich, dass ein Element zwei wesentlich verschiedene Produktzerlegungen hat.

Im ersten Fall (Existenz gilt nicht) haben wir das Problem, dass es eine unendliche Kette $\ldots w_{n+1} \mid w_n \mid w_{n-1} \ldots w_2 \mid w_1 \mid w_0$ gibt, so dass je zwei aufeinander folgende Elemente nicht assoziiert sind. Dann kann man immer „feiner“ unterteilen (im Beispiel $2 = w_0 = w_1^2 = w_2^4 = \ldots = w_n^{2^n} = \ldots$), ohne dass man an ein (irreduzibles) Ende kommt. Im zweiten Fall (Eindeutigkeit geht schief) scheint das Problem damit zu tun zu haben, dass es irreduzible Elemente gibt, die nicht prim sind.

Wir geben jetzt erst einmal den „guten“ Ringen einen Namen, und dann zeigen wir, dass die beiden oben angesprochenen Schwierigkeiten tatsächlich die einzigen Hindernisse gegen die Gültigkeit der eindeutigen Primfaktorzerlegung sind.

5.9. **Definition.** Ein Integritätsbereich R heißt *faktoriell* (engl. meistens *unique factorisation domain* oder kurz *UFD*), wenn in R der Satz von der eindeutigen Primfaktorzerlegung gilt:

Jedes Element $0 \neq r \in R$, das keine Einheit ist, kann als Produkt von Primelementen geschrieben werden. Sind

$$r = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

zwei solche Darstellungen, dann gibt es eine Bijektion $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, l\}$ *mit* $p_j \sim q_{\sigma(j)}$ *für alle* $1 \leq j \leq k$.

(Mehr Eindeutigkeit können wir nicht erwarten, weil wir die Faktoren immer mit Einheiten, deren Produkt 1 ist, multiplizieren können.)

5.10. **Satz.** *Sei* R *ein Integritätsbereich. Dann ist* R *faktoriell genau dann, wenn folgende zwei Bedingungen erfüllt sind:*

(1) *Jedes irreduzible Element von* R *ist prim.*
(2) *Es gibt keine Folge* $(a_n)_{n\geq 0}$ *von Elementen von* R*, so dass* $a_{n+1} \mid a_n$ *und* $a_{n+1} \not\sim a_n$ *für alle* $n \geq 0$.

Beweis. Wir nehmen zunächst an, dass die beiden Bedingungen erfüllt sind, und zeigen, dass R faktoriell ist. Wir zeigen erst die Existenz der Faktorisierung. Dazu nehmen wir an, es gäbe ein Element $a_0 \neq 0$, das keine Einheit ist und sich nicht als Produkt von Irreduziblen schreiben lässt. Dann ist a_0 jedenfalls nicht irreduzibel, also gibt es eine Faktorisierung $a_0 = rs$ mit Nicht-Einheiten r und s. Wären beide Faktoren Produkte von Irreduziblen, dann gälte dies auch für a_0, ein Widerspruch. Also ist einer der Faktoren, wir nennen ihn a_1, kein Produkt von Irreduziblen. Auf diese Weise konstruieren wir eine Folge $(a_n)_{n\geq 0}$ von Elementen von R, so dass jeweils a_{n+1} ein echter Teiler von a_n ist („echter Teiler“ heißt $a_{n+1} \not\sim a_n$). So eine Folge kann es aber nach Bedingung (2) nicht geben. Also gibt es a_0 nicht, und jede Nicht-Einheit $r \neq 0$ ist Produkt von irreduziblen (und damit wegen Bedingung (1) auch primen) Elementen.

Der Beweis der Eindeutigkeit geht genau wie für den Ring $\mathbb{Z}$ (Satz 3.7): Wir nehmen ein Primelement der einen Faktorisierung, dann finden wir es (weil es ein Primelement ist) bis auf Assoziierte als Faktor auf der anderen Seite. Wir können den Faktor abdividieren und per Induktion weiter machen. Der einzige Unterschied ist, dass zusätzlich Einheiten auftreten, die beim Dividieren übrig bleiben. Damit geht man am einfachsten um, wenn man von der etwas allgemeineren Gleichheit $p_1 \cdots p_k = uq_1 \cdots q_l$ mit einer Einheit $u \in R^\times$ ausgeht.

Für die Gegenrichtung nehmen wir jetzt an, dass R faktoriell ist. Sei r irreduzibel. Nach Annahme ist $r = p_1 \cdots p_k$ ein Produkt von Primelementen. Da r irreduzibel ist, kann das Produkt nur einen Faktor haben (Primelemente sind keine Einheiten), also ist $r = p_1$ prim. Für den Beweis der zweiten Bedingung definieren wir $\ell(r)$ für $r \in R$ durch $\ell(0) = +\infty$, $\ell(r) = 0$ für Einheiten r, und sonst $\ell(r) = k$, wenn $r = p_1 p_2 \cdots p_k$ Produkt von k Primelementen ist. Aus der eindeutigen Primfaktorzerlegung folgt dann $\ell(rs) = \ell(r) + \ell(s)$. Ist (a_n) eine Folge wie in Bedingung (2), dann erhalten wir also mit

$$\infty \geq \ell(a_0) > \ell(a_1) > \ell(a_2) > \ldots \geq 0$$

eine unendliche strikt absteigende Folge nichtnegativer ganzer Zahlen (ab $\ell(a_1)$), was es nicht geben kann. □

Analog wie wir das für $R = \mathbb{Z}$ getan haben, kann man sich ein Repräsentantensystem $\mathbb{P}_R$ der Primelemente bis auf Assoziiertheit wählen (d.h. man wählt aus jeder Assoziiertheitsklasse von Primelementen eines aus — für $R = \mathbb{Z}$ hatten wir den positiven Repräsentanten genommen) und den Satz dann wie folgt formulieren.

5.11. **Satz.** *Sei R ein faktorieller Ring und $\mathbb{P}_R$ ein Repräsentantensystem der Primelemente von R bis auf Assoziiertheit. Dann kann jedes Element $0 \neq r \in R$ eindeutig geschrieben werden in der Form*

$$r = u \prod_{p \in \mathbb{P}_R} p^{v_p(r)}$$

mit $u \in R^\times$ und $v_p(r) \in \mathbb{Z}_{\geq 0}$, so dass $v_p(r) = 0$ ist für alle bis auf endlich viele $p \in \mathbb{P}_R$.

Beweis. Wie für $R = \mathbb{Z}$. □

Wir hatten das für den Ring aus Beispiel 5.7 gesehen; dort können wir $\mathbb{P}_R = \{2\}$ wählen, und jedes Element $r \neq 0$ hat die Form $r = u2^n$ mit $u \in R^\times$.

6. Hauptidealringe und euklidische Ringe

Wir wollen jetzt etwas handlichere Kriterien beweisen, die hinreichend dafür sind, dass ein Integritätsbereich faktoriell ist. Dafür müssen wir erst einmal einen neuen Begriff einführen.

6.1. **Definition.** Sei R ein (beliebiger) Ring. Eine Teilmenge $I \subset R$ heißt *Linksideal* von R, wenn $0 \in I$, I unter der Addition von R abgeschlossen ist, und für jedes $a \in I$ und $r \in R$ gilt $r \cdot a \in I$. I heißt *Rechtsideal* von R, wenn in der letzten Bedingung $a \cdot r \in I$ gilt (statt $ra \in I$). I heißt *Ideal* von R, wenn I gleichzeitig Rechts- und Linksideal von R ist.

(Man vergleiche mit der Definition eines Untervektorraums!)

Ist R kommutativ, fallen alle drei Begriffe zusammen, und man spricht einfach von Idealen von R. Wir beschränken uns im Folgenden auf diesen Fall. (D.h., alle Ringe sind ab jetzt **kommutativ**. Für den allgemeinen Fall gibt es analoge Aussagen und Begriffsbildungen für Links-/Rechtsideale und Ideale.)

Es gibt immer die beiden trivialen Ideale R und $0 := \{0\}$.

6.2. **Bemerkung.** Man beachte die Unterschiede zur Definition eines *Unterrings* S:

$$1 \in S \quad \text{und} \quad rs \in S \text{ für } r, s \in S$$

gegenüber

$$ra \in I \text{ für } r \in R,\, a \in I\,.$$

Hier sind zwei einfache Eigenschaften:

6.3. **Lemma.** *Sei R ein Ring.*

(1) *Sei $(I_j)_{j \in J}$ eine Familie von Idealen von R mit $J \neq \emptyset$. Dann ist der Durchschnitt $\bigcap_{j \in J} I_j$ ebenfalls ein Ideal von R.*
(2) *Sei $I_1 \subset I_2 \subset I_3 \subset \ldots$ eine aufsteigende Kette von Idealen von R. Dann ist die Vereinigung $\bigcup_{n \geq 1} I_n$ ebenfalls ein Ideal von R.*

Die erste Aussage kann man analog statt mit Familien von Idealen mit Mengen von Idealen formulieren: Sei $\mathcal{I}$ eine nichtleere Menge von Idealen von R. Dann ist der Durchschnitt $\bigcap \mathcal{I} = \bigcap_{I \in \mathcal{I}} I$ wieder ein Ideal von R.

Beweis. Wir müssen jeweils die drei Bedingungen der Definition nachprüfen.

(1) Sei $I = \bigcap_{j\in J} I_j$. Wegen $0 \in I_j$ für alle j gilt auch $0 \in I$. Seien $a, b \in I$. Dann gilt $a, b \in I_j$ für alle j. Es folgt $a + b \in I_j$ für alle j, also $a + b \in I$. Seien schließlich $a \in I$ und $r \in R$. Dann gilt $a \in I_j$ für alle j, also $ra \in I_j$ für alle j, und damit $ra \in I$.
(2) Sei jetzt $I = \bigcup_{n\geq 1} I_n$. Es ist $0 \in I_1 \subset I$. Seien $a, b \in I$. Dann gibt es $m, n \geq 1$ mit $a \in I_m$, $b \in I_n$. Sei $N = \max\{m, n\}$, dann haben wir $I_m \subset I_N$ und $I_n \subset I_N$. Es folgt $a, b \in I_N$, also $a + b \in I_N \subset I$. Seien $a \in I$ und $r \in R$. Dann gibt es $n \geq 1$ mit $a \in I_n$, Es folgt $ra \in I_n \subset I$.

□

Die erste Eigenschaft zeigt, dass die folgende Definition sinnvoll ist.

6.4. **Definition.** Sei R ein Ring, $A \subset R$ eine Teilmenge. Das Ideal

$$\langle A\rangle_R = \bigcap\{I \subset R \mid I \text{ Ideal und } A \subset I\}$$

heißt das *von A erzeugte Ideal* von R. Ist $A = \{a_1, \ldots, a_n\}$ endlich, schreiben wir für $\langle A\rangle_R$ auch $\langle a_1, \ldots, a_n\rangle_R$.

Ist $I \subset R$ ein Ideal und $A \subset R$ eine Teilmenge mit $I = \langle A\rangle_R$, so heißt A ein *Erzeugendensystem* von I. Hat I ein endliches Erzeugendensystem, so heißt I *endlich erzeugt*. Gilt $I = \langle a\rangle_R$ für ein $a \in R$, so heißt I ein *Hauptideal* (engl. *principal ideal*).

Eine recht konkrete Beschreibung von $\langle A\rangle_R$ wird im folgenden Lemma gegeben.

6.5. **Lemma.** *Sei R ein Ring und $A \subset R$ eine Teilmenge. Dann gilt*

$$\langle A\rangle_R = \{r_1a_1 + \cdots + r_na_n \mid n \geq 0, r_j \in R, a_j \in A\}\,.$$

Beweis. Aus Definition 6.1 folgt, dass jedes A enthaltende Ideal von R auch die rechte Seite enthalten muss. Das zeigt die Inklusion „$\supset$“. Für die andere Richtung zeigt man, dass die rechte Seite bereits ein Ideal ist. □

(Die analoge Aussage gilt für Untervektorräume.)

Aus diesem Grund schreibt man auch gerne $Ra_1+\cdots+Ra_n$ für das Ideal $\langle a_1, \ldots, a_n\rangle_R$.

Wir können jetzt sagen, was ein Hauptidealring ist.

6.6. **Definition.** Ein Integritätsbereich R heißt *Hauptidealring* (engl. *principal ideal domain* oder kurz *PID*), wenn jedes Ideal von R ein Hauptideal ist.

6.7. **Beispiele.** Jeder Körper K ist trivialerweise ein Hauptidealring, denn es gibt nur die beiden Ideale 0 und K, die von 0 bzw. 1 erzeugt werden.

Der Ring $\mathbb{Z}$ der ganzen Zahlen ist auch ein Hauptidealring. Das sieht man so: Sei $I \subset \mathbb{Z}$ ein Ideal. Dann ist $I = 0$, oder I enthält positive Elemente (wegen $n \in I \implies -n \in I$). Sei im zweiten Fall n das kleinste positive Element in I. Dann gilt $I = \langle n\rangle_{\mathbb{Z}}$ („$\supset$“ ist klar wegen $n \in I$; für „$\subset$“ sei $a \in I$, und wir schreiben $a = qn + r$ mit $0 \leq r < n$, dann ist $r = a - qn \in I$, und wegen der Wahl von n muss $r = 0$ sein, also $a = qn \in \langle n\rangle_{\mathbb{Z}}$).

Das hier verwendete Argument werden wir später in diesem Abschnitt in allgemeinerer Form wiedersehen.

Bevor wir zu einem der Hauptergebnisse dieser Vorlesung kommen, stellen wir noch ein paar einfache Eigenschaften des Idealbegriffs bereit.

6.8. **Lemma.** *Sei R ein Integritätsbereich.*

(1) *Seien $a, b \in R$. Dann gilt $a \mid b \iff b \in Ra \iff Rb \subset Ra$. Insbesondere gilt $a \sim b \iff Ra = Rb$ und $a \in R^\times \iff Ra = R$.*
(2) *Ein Element $r \in R$ ist irreduzibel genau dann, wenn Rr nicht das Nullideal und gleichzeitig ein **maximales Hauptideal** ist, d.h. $Rr \subsetneq R$, und für jedes Hauptideal I von R mit $Rr \subset I$ gilt $I = Rr$ oder $I = R$.*
(3) *Ein Element $p \in R$ ist prim genau dann, wenn $p \neq 0$ und Rp ein **Primideal** ist, d.h. $Rp \neq R$, und für $a, b \in R$ mit $ab \in Rp$ gilt $a \in Rp$ oder $b \in Rp$.*

Beweis.

(1) Die erste Äquivalenz ist genau die Definition der Teilbarkeitsrelation. Die zweite Äquivalenz folgt daraus, dass Rb das kleinste Ideal ist, das b enthält (daher muss Rb in Ra enthalten sein, denn Ra ist ein Ideal, das b enthält). Der zweite Teil ist dann klar.
(2) Ist $r \in R$ irreduzibel, so ist $r \neq 0$ und $r \notin R^\times$, also ist $Rr \neq 0, R$. Sei $I = Rs \supset Rr$ ein Hauptideal. Dann gilt (nach Teil (1)) $s \mid r$, also ist entweder $s \in R^\times$ und damit $I = R$, oder $s \sim r$ und damit $I = Rr$. Die Gegenrichtung zeigt man genauso.
(3) Das folgt direkt aus der Definition von „Primelement“ und Teil (1).

□

Die Bedeutung von Hauptidealringen zeigt sich im folgenden Resultat.

6.9. **Satz.** *Sei R ein Hauptidealring. Dann ist R faktoriell.*

Beweis. Wir müssen die beiden Eigenschaften aus Satz 5.10 nachweisen. Sei dazu $r \in R$ irreduzibel; wir müssen zeigen, dass r prim ist. Nach Lemma 6.8 ist $0 \neq Rr$ ein maximales Hauptideal von R. Seien jetzt $a, b \in R$ mit $r \nmid a$, $r \nmid b$, also $a, b \notin Rr$. Es folgt $Ra + Rr, Rb + Rr \supsetneq Rr$, also (wegen der Maximalität von Rr und weil die beiden Ideale nach Voraussetzung Hauptideale sein müssen) $Ra + Rr = R = Rb + Rr$. Das bedeutet, dass es $u, v, x, y \in R$ gibt mit $ua + xr = 1 = vb + yr$. Durch Multiplikation der Gleichungen erhalten wir $(uv)(ab) + (uya + vxb + xyr)r = 1$, also $Rab + Rr = R$. Daraus folgt $ab \notin Rr$ (sonst wäre $Rab + Rr = Rr \subsetneq R$), also $r \nmid ab$. Wir haben die Implikation $r \nmid a, r \nmid b \implies r \nmid ab$ gezeigt; das bedeutet gerade, dass r ein Primelement ist.

Für die zweite Eigenschaft nehmen wir an, es gäbe eine Folge (a_n) in R, so dass $a_{n+1} \mid a_n$ und $a_{n+1} \not\sim a_n$ für alle $n \geq 0$. Nach Lemma 6.8 übersetzt sich das in eine strikt aufsteigende Kette von Hauptidealen $Ra_0 \subsetneq Ra_1 \subsetneq Ra_2 \subsetneq \ldots$. Nach Lemma 6.3 ist die Vereinigung $I = \bigcup_{n \geq 0} Ra_n$ wieder ein Ideal von R. Da R ein Hauptidealring ist, ist $I = Ra$ mit einem $a \in R$. Es gilt $a \in I = \bigcup_{n \geq 0} Ra_n$, also gibt es ein $n \geq 0$ mit $a \in Ra_n$. Dann folgt aber

$$I = Ra \subset Ra_n \subsetneq Ra_{n+1} \subsetneq \ldots \subset I\,,$$

ein Widerspruch. Also kann es eine Folge (a_n) wie angenommen nicht geben, und Eigenschaft (2) ist nachgewiesen. □

Die Umkehrung von Satz 6.9 gilt nicht: Es gibt faktorielle Ringe, die keine Hauptidealringe sind. Wir werden später Beispiele dafür sehen.

6.10. **Beispiel.** Der Ring $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ aus Beispiel 5.6 ist kein Hauptidealring, da er nicht faktoriell ist. Tatsächlich ist etwa das Ideal $I = \langle 2, 1+\sqrt{-5}\rangle_R$ kein Hauptideal. Das sieht man zum Beispiel so: Wäre $I = \langle r\rangle$, dann würde gelten $r \mid 2$ und $r \mid 1+\sqrt{-5}$, und daraus würde folgen $N(r) \mid N(2) = 4$ und $N(r) \mid N(1+\sqrt{-5}) = 6$, also $N(r) = 1$ oder $N(r) = 2$. Elemente mit Norm 2 gibt es aber nicht in R, also bleibt nur $N(r) = 1$, und das heißt $r \in R^\times = \{\pm 1\}$. Dann wäre $1 \in I$, also gäbe es $a, b, c, d \in \mathbb{Z}$ mit

$$1 = (a + b\sqrt{-5}) \cdot 2 + (c + d\sqrt{-5})(1 + \sqrt{-5}) = (2a + c - 5d) + (2b + c + d)\sqrt{-5}\,.$$

Koeffizientenvergleich ergibt $1 = 2a + c - 5d$ und $0 = 2b + c + d$, also $1 = 1 - 0 = 2(a - b - 3d)$, was nicht geht, da 1 nicht gerade ist.

Ein Hauptidealring verhält sich in vielen Aspekten so wie der Ring $\mathbb{Z}$.

6.11. **Satz.** *Sei R ein Hauptidealring. Dann hat jede Teilmenge $A \subset R$ einen größten gemeinsamen Teiler g in R (in dem Sinne, dass $g \mid a$ für alle $a \in A$, und für jedes $r \in R$ mit $r \mid a$ für alle $a \in A$ gilt $r \mid g$), und g kann als Linearkombination von endlich vielen Elementen von A geschrieben werden:*

$$g = r_1 a_1 + r_2 a_2 + \ldots + r_n a_n$$

mit $r_1, \ldots, r_n \in R$ und $a_1, \ldots, a_n \in A$.

Beweis. Wir betrachten das Ideal $I = \langle A\rangle_R$. Da R ein Hauptidealring ist, gilt $I = Rg$ für ein $g \in R$. Wegen $a \in I = Rg$ für alle $a \in A$ folgt $g \mid a$. Gilt $r \mid a$ für alle $a \in A$, so folgt $A \subset Rr$ und daher $Rg = I \subset Rr$, also $r \mid g$. Damit ist gezeigt, dass g ein größter gemeinsamer Teiler von A ist. Da $g \in \langle A\rangle_R$, ist g als Linearkombination von (endlich vielen) Elementen von A darstellbar, siehe Lemma 6.5. □

Man beachte den Spezialfall $A = \emptyset$: Hier ist $\langle A\rangle_R = 0$ das Nullideal, also $g = 0$.

Wie kann man jetzt aber sehen, dass ein Integritätsbereich ein Hauptidealring ist? Wir erinnern uns an den Beweis für den Ring $\mathbb{Z}$. Dort war der wesentliche Punkt, dass wir die *Division mit Rest* zur Verfügung haben:

$$a, b \in \mathbb{Z}, b \neq 0 \quad \Longrightarrow \quad \exists q, r \in \mathbb{Z} : 0 \leq r < |b| \text{ und } a = qb + r\,.$$

Hier wird auf die Anordnung Bezug genommen, allerdings nur über den Absolutbetrag. Schreiben wir $N : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ für die Betragsabbildung $b \mapsto |b|$, dann haben wir einen Spezialfall der folgenden allgemeinen Definition.

6.12. **Definition.** Ein Integritätsbereich R heißt *euklidischer Ring* oder einfach *euklidisch*, wenn er eine *euklidische Normfunktion* besitzt. Das ist eine Abbildung $N : R \to \mathbb{Z}_{\geq 0}$ mit folgenden Eigenschaften:

(1) Für alle $r \in R$ gilt $N(r) = 0 \iff r = 0$.
(2) Für alle $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$ mit $N(r) < N(b)$ und $a = qb + r$.

In der Literatur findet man häufig eine leicht unterschiedliche Definition. Dort wird $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ betrachtet mit der Eigenschaft, dass es für $a, b \in R$ mit $b \neq 0$ immer $q, r \in R$ gibt mit $r = 0$ oder $r \neq 0$ und $N(r) < N(b)$, so dass $a = qb + r$. Man kann sich leicht überlegen, dass beide Definitionen äquivalent sind (d.h., es gibt genau dann eine euklidische Normfunktion im Sinne von Def. 6.12, wenn es eine euklidische Normfunktion im hier beschriebenen Sinne gibt).

Man beachte, dass in obiger Definition keinerlei Eindeutigkeit von q und r gefordert wird.

6.13. **Beispiel.** Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein euklidischer Ring.

6.14. **Beispiel.** Sei $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$ der Unterring von $\mathbb{C}$, bestehend aus den komplexen Zahlen mit ganzzahligem Real- und Imaginärteil (dass $\mathbb{Z}[i]$ ein Unterring von $\mathbb{C}$ ist sieht man analog wie für $\mathbb{Z}[\sqrt{-5}]$). Dann ist $\mathbb{Z}[i]$ als Unterring eines Körpers automatisch ein Integritätsbereich. Der Ring ist sogar euklidisch. Dazu sei $N(a+bi) = |a+bi|^2 = a^2+b^2$. Wir müssen zeigen, dass $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ eine euklidische Normfunktion ist. Es ist klar, dass

$$N(a+bi) = 0 \iff a^2+b^2 = 0 \iff a = b = 0 \iff a+bi = 0\,.$$

Seien jetzt $a, b \in \mathbb{Z}[i]$ mit $b \neq 0$. Wir müssen geeignete $q, r \in \mathbb{Z}[i]$ finden. Dabei lassen wir uns von der Idee leiten, dass der „Quotient“ q nahe beim wahren Quotienten in $\mathbb{C}$ liegen sollte. Wir schreiben also $a/b = \xi + \eta i \in \mathbb{C}$. Dann gibt es ganze Zahlen x, y mit $|x-\xi|, |y-\eta| \leq \frac{1}{2}$. Wir setzen $q = x+yi$. Dann folgt $|(a/b)-q|^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2} < 1$. Mit $r = a - qb$ gilt dann

$$N(r) = |r|^2 = |a-qb|^2 = \left|\frac{a}{b} - q\right|^2 \cdot |b|^2 < |b|^2 = N(b)\,.$$

Damit erfüllt N die Eigenschaften einer euklidischen Normfunktion.

Der Ring $\mathbb{Z}[i]$ heißt auch der *Ring der (ganzen) Gaußschen Zahlen.*

Die Bedeutung dieser Begriffsbildung zeigt sich in den nächsten beiden Resultaten. Der Beweis des ersten verläuft analog zu dem Beweis, dass $\mathbb{Z}$ ein Hauptidealring ist.

6.15. **Satz.** *Sei R ein Integritätsbereich. Ist R euklidisch, dann ist R ein Hauptidealring (und damit faktoriell).*

Beweis. Sei $I \subset R$ ein Ideal, und sei $N : R \to \mathbb{Z}_{\geq 0}$ eine euklidische Normfunktion. Wir können $I \neq 0$ annehmen (denn das Nullideal ist ein Hauptideal). Dann ist $N(I \setminus \{0\}) = \{N(r) \mid 0 \neq r \in I\}$ eine nichtleere Teilmenge von $\mathbb{Z}_{\geq 0}$ und hat demzufolge ein kleinstes Element n. Sei $a \in I \setminus \{0\}$ mit $N(a) = n$. Dann gilt $I = Ra$: Wegen $a \in I$ ist klar, dass $Ra \subset I$ ist. Für die umgekehrte Inklusion sei $b \in I$. Dann gibt es $q, r \in R$ mit $N(r) < N(a)$ und $b = qa + r$. Es folgt $r = b - qa \in I$, und wegen $N(r) < N(a)$ muss dann $r = 0$ sein (a ist das Element mit kleinster Norm in $I \setminus \{0\}$). Also gilt $b = qa \in Ra$. □

Auch die Umkehrung dieses Satzes ist falsch: Es gibt Hauptidealringe, die nicht euklidisch sind. Solche Beispiele sind relativ schwierig zu konstruieren, da der Nachweis der Nicht-Existenz einer euklidischen Normfunktion nicht so einfach ist.

6.16. **Beispiel.** Nach Beispiel 6.14 und Satz 6.15 ist der Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen ein faktorieller Ring. Man kann Folgendes zeigen (das werden wir bald tun):

6.17. **Satz.** *Die Primelemente des Rings $\mathbb{Z}[i]$ sind gegeben bis auf Assoziiertheit durch $1+i$, Primzahlen q der Form $4k+3$, und für jede Primzahl p der Form $4k+1$ zwei Elemente $a+bi$ und $a-bi$ mit $a^2+b^2 = p$. Insbesondere ist jede Primzahl $p = 4k+1$ Summe von zwei Quadraten.*

Das nächste Resultat zeigt, dass man in euklidischen Ringen größte gemeinsame Teiler berechnen kann. Das erklärt auch die Namensgebung, denn man verwendet dafür den Euklidischen Algorithmus.

6.18. **Satz.** *Sei R ein euklidischer Ring. Dann kann man zu je zwei Elementen $a, b \in R$ einen größten gemeinsamen Teiler berechnen, indem man den Euklidischen Algorithmus anwendet: Man setzt $a_0 = a$, $a_1 = b$, und solange $a_n \neq 0$ ist, $a_{n+1} = r$, wobei $a_{n-1} = qa_n + r$ und $N(r) < N(a_n)$. Nach endlich vielen Schritten bricht die Folge ab; wenn $a_n = 0$, dann ist a_{n-1} ein ggT von a und b.*

Beweis. Sei g ein ggT von a und b (g existiert nach Satz 6.11, weil R nach Satz 6.15 ein Hauptidealring ist). Für jedes n mit $a_n \neq 0$ gilt die Äquivalenz

$$g \sim \mathrm{ggT}(a_{n-1}, a_n) \iff g \sim \mathrm{ggT}(a_n, a_{n+1})$$

(das sieht man wie früher für $R = \mathbb{Z}$). Wegen $g \sim \mathrm{ggT}(a_0, a_1)$ ist also g ein ggT jedes Paars aufeinander folgender Glieder der Folge (a_n). Gilt $a_n = 0$, dann folgt $\mathrm{ggT}(a, b) \sim g \sim \mathrm{ggT}(a_{n-1}, 0) \sim a_{n-1}$.

Es bleibt zu zeigen, dass die Folge abbricht. Das folgt aus $N(a_1) > N(a_2) > \ldots \geq 0$ und daraus, dass die Werte der Normfunktion ganze Zahlen sind. Da die Folge fortgesetzt wird, solange $N(a_n) > 0$ ist, muss schließlich der Wert null erreicht werden, und dann ist $a_n = 0$ für das letzte Folgenglied. □

Wie früher für $R = \mathbb{Z}$ kann man den Euklidischen Algorithmus erweitern, so dass er Koeffizienten $x, y \in R$ liefert mit $g = xa + yb$.

6.19. **Beispiel.** Wir bestimmen einen ggT von 41 und $9 + i$ in $\mathbb{Z}[i]$. Wir setzen also $a_0 = 41$, $a_1 = 9 + i$. Als nächstes müssen wir a_0 mit Rest durch a_1 teilen. Der exakte Quotient ist $41/(9 + i) = 9/2 - i/2$; wir können also zum Beispiel $q = 4$ nehmen, dann ist $a_2 = r = 41 - 4(9 + i) = 5 - 4i$. Jetzt teilen wir a_1 durch a_2:

$$\frac{9+i}{5-4i} = \frac{(9+i)(5+4i)}{5^2+4^2} = \frac{(45-4)+(36+5)i}{41} = 1 + i \in \mathbb{Z}[i]\,.$$

Diese Division geht auf, also ist $a_3 = 0$, und $a_2 = 5 - 4i$ ist ein ggT.

Allgemein kann man sagen, dass Hauptidealringe schöne mathematische Eigenschaften haben; wenn man aber rechnen möchte, dann sollte man besser einen euklidischen Ring haben.

Wir stellen die bewiesenen Implikationen noch einmal zusammen: Für einen Integritätsbereich R gilt

$$\boxed{R \text{ euklidisch} \implies R \text{ Hauptidealring} \implies R \text{ faktoriell.}}$$

Die Umkehrungen dieser Implikationen gelten i.a. nicht.

7. Ringhomomorphismen und Faktorringe

Wir haben bisher immer nur einen Ring betrachtet. Es ist aber, wie in vielen anderen Gebieten der Mathematik auch, wichtig, auch die Beziehungen zwischen verschiedenen Ringen zu verstehen. Diese werden hergestellt durch geeignete *strukturerhaltende Abbildungen.*

7.1. **Definition.** Seien R_1, R_2 zwei Ringe. Ein *Ringhomomorphismus* von R_1 nach R_2 ist eine Abbildung $\phi : R_1 \to R_2$ mit $\phi(1) = 1$ und $\phi(a+b) = \phi(a) + \phi(b)$, $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ für alle $a, b \in R_1$. (Beachte, dass „1“, „+“ und „$\cdot$“ jeweils *zwei verschiedene* Bedeutungen haben: Auf der linken Seite sind Einselement, Addition und Multiplikation von R_1 gemeint, auf der rechten Seite die von R_2!)

Analog zur Begriffsbildung in der Linearen Algebra heißt ein injektiver Ringhomomorphismus ein *(Ring-)Monomorphismus* und ein surjektiver Ringhomomorphismus ein *(Ring-)Epimorphismus*. Ein Ringhomomorphismus $R \to R$ heißt ein *Endomorphismus* von R.

7.2. **Lemma.** *Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus. Dann gilt $\phi(0) = 0$ und $\phi(-a) = -\phi(a)$ für alle $a \in R$. Ist ϕ bijektiv, dann ist ϕ^{-1} ebenfalls ein Ringhomomorphismus.*

Die erste Aussage zeigt, dass ein Ringhomomorphismus wirklich *alle* Bestandteile der Struktur $(R, 0, 1, +, -, \cdot)$ erhält.

Beweis. Es gilt $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$, woraus $\phi(0) = 0$ folgt. Für $a \in R_1$ gilt $0 = \phi(0) = \phi(a + (-a)) = \phi(a) + \phi(-a)$, was $\phi(-a) = -\phi(a)$ impliziert.

Sei jetzt ϕ bijektiv, und seien $a', b' \in R_2$. Wir können dann $a' = \phi(a)$, $b' = \phi(b)$ schreiben mit geeigneten $a = \phi^{-1}(a')$, $b = \phi^{-1}(b')$. Dann gilt

$$\phi^{-1}(a' + b') = \phi^{-1}(\phi(a) + \phi(b)) = \phi^{-1}(\phi(a+b)) = a + b = \phi^{-1}(a') + \phi^{-1}(b')\,.$$

Die Aussage $\phi^{-1}(a' \cdot b') = \phi^{-1}(a') \cdot \phi^{-1}(b')$ zeigt man genauso. Schließlich folgt $\phi^{-1}(1) = 1$ aus $\phi(1) = 1$. □

7.3. **Definition.** Ein bijektiver Ringhomomorphismus heißt *(Ring-)Isomorphismus*. Gibt es einen Isomorphismus $\phi : R_1 \to R_2$, dann heißen die Ringe R_1 und R_2 (zueinander) *isomorph*, und man schreibt $R_1 \cong R_2$. Das definiert eine Äquivalenzrelation zwischen Ringen (Übung).

Ein Isomorphismus ist also ein Ringhomomorphismus, zu dem es einen inversen Ringhomomorphismus gibt.

Ein Isomorphismus $R \to R$ heißt ein *Automorphismus* von R.

7.4. **Beispiele.**

(1) Für jeden Ring R ist die identische Abbildung $\mathrm{id}_R : R \to R$ ein Automorphismus.
(2) Sei $\mathbb{F}_2 = \{0, 1\}$ der Körper mit zwei Elementen. Die Abbildung

$$\phi : \mathbb{Z} \longrightarrow \mathbb{F}_2\,, \quad n \longmapsto \begin{cases} 0 & \text{wenn } n \text{ gerade} \\ 1 & \text{wenn } n \text{ ungerade} \end{cases}$$

ist ein (surjektiver) Ringhomomorphismus: $\phi(1) = 1$ ist klar; für die anderen Bedingungen muss man Aussagen wie „ungerade + ungerade = gerade“ nachprüfen.
(3) Für jeden Ring R gibt es *genau einen* Ringhomomorphismus $\phi : \mathbb{Z} \to R$: Wir müssen $\phi(1) = 1_R$ setzen, dann gilt für $n \in \mathbb{Z}_{>0}$ zwangsläufig

$$\phi(n) = \phi(\underbrace{1 + 1 + \ldots + 1}_{n \text{ Summanden}}) = \underbrace{\phi(1) + \phi(1) + \ldots + \phi(1)}_{n \text{ Summanden}} = \underbrace{1_R + 1_R + \ldots + 1_R}_{n \text{ Summanden}};$$

außerdem natürlich $\phi(0) = 0_R$ und $\phi(-n) = -\phi(n)$. Wir schreiben $m \cdot 1_R$ für $\phi(m)$ (für $m \in \mathbb{Z}$), und allgemeiner $m \cdot r$ für $\phi(m)r \in R$. Man prüft nach (Fallunterscheidung nach Vorzeichen, Induktion), dass

$$(m + m') \cdot 1_R = m \cdot 1_R + m' \cdot 1_R \quad \text{und} \quad (mm') \cdot 1_R = (m \cdot 1_R)(m' \cdot 1_R)$$

gelten; ϕ ist also tatsächlich ein Ringhomomorphismus.

(4) Der (eindeutig bestimmte) Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}[i]$ ist gegeben durch $a \mapsto a + 0i$. Umgekehrt gibt es keinen Ringhomomorphismus $\phi : \mathbb{Z}[i] \to \mathbb{Z}$: Angenommen, so ein ϕ existiert. Dann ist $a = \phi(i)$ eine ganze Zahl, und es würde folgen $a^2 = \phi(i)^2 = \phi(i^2) = \phi(-1) = -1$, was nicht möglich ist.

(5) Der Ring $\mathbb{Z}[i]$ hat außer der Identität noch genau einen nichttrivialen Automorphismus, nämlich $a + bi \mapsto a - bi$ (Übung).

(6) Die Ringe $\mathbb{F}_2^X$ und $P(X)$ aus Beispiel 4.9, (4) und (5), sind isomorph (Übung). Dabei ist $\mathbb{F}_2$ der Körper mit zwei Elementen.

Beispiel (3) beschreibt eine *universelle Eigenschaft* des Rings $\mathbb{Z}$.

Wie bei linearen Abbildungen sind Kern und Bild interessant.

7.5. **Definition.** Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus. Der *Kern* von ϕ ist definiert als

$$\ker \phi = \{r \in R_1 \mid \phi(r) = 0\}.$$

Wir schreiben $\operatorname{im} \phi$ für das Bild von ϕ.

7.6. **Lemma.** *Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus. Dann ist $\operatorname{im} \phi$ ein Unterring von R_2, und $\ker \phi$ ist ein Ideal von R_1. ϕ ist injektiv genau dann, wenn $\ker \phi = 0$ ist.*

Beweis. Aus der Definition und Lemma 7.2 folgt, dass $\operatorname{im} \phi$ 0 und 1 enthält und unter Addition, Negation und Multiplikation abgeschlossen ist. Also ist $\operatorname{im} \phi \subset R_2$ ein Unterring.

Es gilt $0 \in \ker \phi$, da $\phi(0) = 0$. Seien $a, b \in \ker \phi$. Dann ist $\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$, also ist $a + b \in \ker \phi$. Seien $a \in \ker \phi$, $r \in R_1$. Dann ist $\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0$, analog $\phi(ar) = 0$, also sind $ra, ar \in \ker \phi$. Damit ist gezeigt, dass $\ker \phi \subset R_1$ ein Ideal ist.

Ist ϕ injektiv, dann gilt $a \in \ker \phi \implies \phi(a) = 0 = \phi(0) \implies a = 0$, also ist $\ker \phi = 0$. Ist umgekehrt $\ker \phi$ das Nullideal, und sind $a, b \in R_1$ mit $\phi(a) = \phi(b)$, dann folgt $0 = \phi(a) - \phi(b) = \phi(a - b)$, also $a - b \in \ker \phi = \{0\}$ und damit $a = b$. Damit ist gezeigt, dass ϕ injektiv ist. □

7.7. **Beispiel.** Für den Ringhomomorphismus $\mathbb{Z} \to \mathbb{F}_2$ aus dem vorigen Beispiel gilt $\ker \phi = \mathbb{Z}2$.

Wir zeigen jetzt, dass Ringhomomorphismen sich gut mit Idealen vertragen.

7.8. **Lemma.** *Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus.*

(1) *Ist $I \subset R_1$ ein Ideal, dann ist $\phi(I)$ ein Ideal im Unterring* $\operatorname{im}\phi$ *von R_2 (aber nicht unbedingt in R_2 selbst!).*
(2) *Ist $J \subset R_2$ ein Ideal, dann ist $\phi^{-1}(J)$ ein Ideal von R_1.*
(3) *Ist ϕ surjektiv, dann induziert ϕ eine Bijektion:*

$$\begin{aligned} \{I \subset R_1 \mid I \text{ Ideal und } \ker\phi \subset I\} &\longleftrightarrow \{J \subset R_2 \mid J \text{ Ideal}\} \\ I &\longmapsto \phi(I) \\ \phi^{-1}(J) &\longmapsfrom J \end{aligned}$$

Beweis.

(1) Wegen $\phi(0) = 0$ und $\phi(a+b) = \phi(a)+\phi(b)$ gilt $0 \in \phi(I)$, und aus $r, s \in \phi(I)$ folgt $r + s \in \phi(I)$. Ist $r \in \operatorname{im}\phi$ und $s \in \phi(I)$, dann gibt es $a \in R_1$ und $b \in I$ mit $r = \phi(a)$ und $s = \phi(b)$; es folgt wegen $ab \in I$, dass auch $rs = \phi(a)\phi(b) = \phi(ab) \in \phi(I)$ ist. Damit erfüllt $\phi(I)$ die Bedingungen dafür, ein Ideal von $\operatorname{im}\phi$ zu sein.
(2) Wegen $\phi(0) = 0 \in J$ ist $0 \in \phi^{-1}(J)$. Seien $a, b \in \phi^{-1}(J)$, d.h. $\phi(a), \phi(b) \in J$. Dann ist $\phi(a + b) = \phi(a) + \phi(b) \in J$, also $a + b \in \phi^{-1}(J)$. Seien jetzt $r \in R_1$ und $a \in \phi^{-1}(J)$. Dann ist $\phi(a) \in J$, also auch $\phi(ra) = \phi(r)\phi(a) \in J$ und damit $ra \in \phi^{-1}(J)$. Also ist J ein Ideal von R_1.
(3) Nach Teil (1) und (2) sind die beiden Abbildungen wohldefiniert (es ist klar, dass $\phi^{-1}(J) \supset \ker\phi = \phi^{-1}(0)$). Es bleibt zu zeigen, dass sie zueinander invers sind. Weil ϕ surjektiv ist, gilt $\phi(\phi^{-1}(J)) = J$ für jede Teilmenge $J \subset R_2$, insbesondere für jedes Ideal. Sei jetzt $I \subset R_1$ ein Ideal, $\ker\phi \subset I$. Dann gilt in jedem Fall $\phi^{-1}(\phi(I)) \supset I$, und es ist noch die umgekehrte Inklusion zu zeigen. Sei also $a \in \phi^{-1}(\phi(I))$, d.h. $\phi(a) \in \phi(I)$. Dann gibt es $b \in I$ mit $\phi(a) = \phi(b)$. Es folgt $\phi(a - b) = \phi(a) - \phi(b) = 0$, also ist $a - b \in \ker\phi \subset I$ und damit ist auch $a = b + (a - b) \in I$.

□

7.9. **Beispiel.** Sei $\phi : \mathbb{Z} \to \mathbb{Q}$ der eindeutig bestimmte Ringhomomorphismus. Dann ist ϕ nicht surjektiv. Das Bild eines von null verschiedenen Ideals $\mathbb{Z}n$ von $\mathbb{Z}$ ist *kein* Ideal von $\mathbb{Q}$ (denn $\mathbb{Q}$ hat als Körper nur die beiden trivialen Ideale 0 und $\mathbb{Q}$). Auch ist die Abbildung $J \mapsto \phi^{-1}(J)$ weit davon entfernt, surjektiv zu sein (ϕ ist injektiv, also $\ker\phi = 0$, so dass die Bedingung $\ker\phi \subset I$ leer ist): Sie liefert nur das Nullideal und $\mathbb{Z} = \phi^{-1}(\mathbb{Q})$ als Ideale von $\mathbb{Z}$.

Wir haben gesehen, dass jeder Kern eines Ringhomomorphismus ein Ideal ist. Gilt das auch umgekehrt? Ist jedes Ideal auch der Kern eines Ringhomomorphismus? Die Antwort lautet „Ja“; sie ist eng mit dem Begriff der Kongruenz verbunden.

7.10. **Definition.** Sei R ein Ring und $I \subset R$ ein Ideal. Wir sagen, zwei Elemente $a, b \in R$ sind *kongruent modulo I* und schreiben $a \equiv b \bmod I$, wenn $a - b \in I$. Ist $I = Rc$ ein Hauptideal, dann sagen und schreiben wir auch „modulo c“ bzw. $a \equiv b \bmod c$.

Zum Beispiel ist in $R = \mathbb{Z}$ die Aussage „$a \equiv 1 \bmod 2$“ äquivalent dazu, dass a ungerade ist.

Wir beweisen einige wichtige Eigenschaften.

7.11. **Lemma.** *Sei R ein Ring und $I \subset R$ ein Ideal.*

(1) *Die Relation $a \equiv b \bmod I$ ist eine Äquivalenzrelation auf R.*
(2) *Sie ist mit Addition und Multiplikation verträglich: Aus $a \equiv a' \bmod I$ und $b \equiv b' \bmod I$ folgt $a + b \equiv a' + b' \bmod I$ und $ab \equiv a'b' \bmod I$ (und insbesondere $-a \equiv -a' \bmod I$).*
(3) *Für $a, b \in R$ gilt*

$$a \equiv b \bmod I \iff a - b \in I \iff b \in a + I = \{a + r \mid r \in I\}\,.$$

Beweis.

(1) Reflexivität: $a - a = 0 \in I \implies a \equiv a \bmod I$.
Symmetrie: $a \equiv b \bmod I \implies a - b \in I \implies -(a - b) = b - a \in I \implies b \equiv a \bmod I$.
Transitivität: $a \equiv b \equiv c \bmod I \implies a - b, b - c \in I \implies a - c = (a - b) + (b - c) \in I \implies a \equiv c \bmod I$.
(2) Seien $a, a', b, b' \in R$ mit $a \equiv a'$, $b \equiv b' \bmod I$. Es gilt also $a - a', b - b' \in I$. Es folgt $(a+b)-(a'+b') = (a-a')+(b-b') \in I$, also $a+b \equiv a'+b' \bmod I$. Ebenso gilt $ab - a'b' = a(b-b')+(a-a')b' \in I$ und damit $ab \equiv a'b' \bmod I$.
(3) Die erste Äquivalenz ist die Definition, die zweite ist klar.

□

7.12. **Definition.** Sei R ein Ring und $I \subset R$ ein Ideal. Wir schreiben R/I für die Menge der Äquivalenzklassen unter „Kongruenz modulo I“; für die durch $a \in R$ repräsentierte Äquivalenzklasse schreiben wir $a + I$ oder $[a]$, wenn das Ideal I aus dem Kontext klar ist. So eine Äquivalenzklasse heißt auch *Restklasse* modulo I (oder modulo c, wenn $I = Rc$ ist). Die Menge R/I trägt eine natürliche Ringstruktur (siehe unten); R/I heißt der *Faktorring* von R modulo I.

Es ist auch die Bezeichnung *Quotientenring* gebräuchlich. Die möchte ich hier aber lieber vermeiden, um Verwechslungen mit dem *Quotientenkörper* eines Integritätsrings zu vermeiden, den wir bald konstruieren werden.

7.13. **Satz.** *Sei R ein Ring und $I \subset R$ ein Ideal. Dann gibt es auf R/I genau eine Ringstruktur, so dass die natürliche Abbildung $\phi : R \to R/I$, $a \mapsto [a] = a + I$, ein (surjektiver) Ringhomomorphismus ist. Es gilt* $\ker \phi = I$.

Der Homomorphismus ϕ heißt auch der *kanonische Epimorphismus* von R auf R/I.

Beweis. Da die Abbildung vorgegeben ist, muss die Ringstruktur so definiert werden, dass $[a]+[b] = [a+b]$ und $[a]\cdot[b] = [ab]$ gelten. Es ist nachzuprüfen, dass diese Verknüpfungen wohldefiniert sind (also nicht von den gewählten Repräsentanten abhängen). Dies ist aber gerade die Aussage von Lemma 7.11, (2). Die Ringaxiome übertragen sich dann sofort von R auf R/I. Schließlich gilt

$$\ker \phi = \phi^{-1}([0]) = \{a \in R \mid [a] = [0]\} = \{a \in R \mid a \in I\} = I\,.$$

□

Wir sehen also, dass tatsächlich jedes Ideal als Kern eines (sogar surjektiven) Ringhomomorphismus auftritt.

Wir beweisen hier gleich noch eine sehr wichtige und nützliche Aussage.

7.14. **Satz.** *Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus. Dann ist der Faktorring $R_1/\ker\phi$ isomorph zum Unterring $\operatorname{im}\phi$ von R_2.*

Beweis. Wir müssen einen Isomorphismus $R_1/\ker\phi \to \operatorname{im}\phi$ konstruieren. Die einzige sinnvolle Möglichkeit dafür ist $\varphi : [a] \mapsto \phi(a)$. Wir müssen zeigen, dass φ wohldefiniert ist. Das bedeutet gerade $[a] = [b] \implies \phi(a) = \phi(b)$. Es gilt aber

$$[a] = [b] \implies [a-b] = [0] \implies a - b \in \ker\phi \implies \phi(a) = \phi(a-b) + \phi(b) = \phi(b)\,.$$

Dass φ dann ein Ringhomomorphismus ist, folgt aus der entsprechenden Eigenschaft von ϕ: $\varphi([1]) = \phi(1) = 1$, sowie

$$\varphi([a] + [b]) = \varphi([a+b]) = \phi(a+b) = \phi(a) + \phi(b) = \varphi([a]) + \varphi([b])\,,$$

und analog für das Produkt. Es bleibt zu zeigen, dass $\varphi : R_1/\ker\phi \to \operatorname{im}\phi$ bijektiv ist. φ ist aber surjektiv nach Definition (denn $\phi(a) = \varphi([a])$, also ist $\operatorname{im}\varphi = \operatorname{im}\phi$). Um zu zeigen, dass φ auch injektiv ist, genügt es, $\ker\varphi = 0$ nachzuweisen. Es gilt

$$[a] \in \ker\varphi \implies \phi(a) = \varphi([a]) = 0 \implies a \in \ker\phi \implies [a] = [0]\,,$$

also ist $\ker\varphi = \{[0]\}$ wie gewünscht. □

7.15. **Beispiel.** Wie sieht das mit den Faktorringen für den Ring $\mathbb{Z}$ aus? Wir wissen, dass die Ideale von $\mathbb{Z}$ gegeben sind durch $I = \mathbb{Z}n$ mit $n \geq 0$. Für $I = 0$ (also $n = 0$) gilt (wie für jeden Ring) $\mathbb{Z}/I \cong \mathbb{Z}$: Die Äquivalenzklassen sind einelementig und können mit ihren Elementen identifiziert werden. Für $n > 0$ haben wir folgende Aussage:

Der Faktorring $\mathbb{Z}/n\mathbb{Z}$ hat n Elemente (ist also endlich), die repräsentiert werden durch $0, 1, \ldots, n-1$. Der kanonische Epimorphismus $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ist dann gegeben durch $a \mapsto [r]$, wo r der Rest bei der Division von a durch n ist.

Beweis. Es gilt $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$, denn für $a \in \mathbb{Z}$ können wir schreiben $a = qn + r$ mit $0 \leq r < n$, und $a - r = qn \in \mathbb{Z}n$ bedeutet $[a] = [r]$. Die Restklassen $[0], [1], \ldots, [n-1]$ sind alle verschieden, denn die Differenz der Repräsentanten hat Betrag $< n$, kann also nur dann durch n teilbar sein, wenn die Repräsentanten gleich sind. □

7.16. **Beispiel.** Ein Beispiel für die Anwendung von Satz 7.14 tritt bei der Konstruktion des Körpers der reellen Zahlen mittels Cauchy-Folgen auf: Die Menge $C \subset \mathbb{Q}^{\mathbb{N}}$ der Cauchy-Folgen rationaler Zahlen ist ein Unterring von $\mathbb{Q}^{\mathbb{N}}$, und die Menge $N \subset C$ der Nullfolgen bildet darin ein Ideal. Wir nehmen an, dass wir die reellen Zahlen bereits kennen. Dann haben wir in $\lim : C \to \mathbb{R}$, $(a_n) \mapsto \lim_{n\to\infty} a_n$ einen surjektiven Ringhomomorphismus mit Kern N, also ist $C/N \cong \mathbb{R}$. (Übung.)

7.17. **Anwendungen von Faktorringen.** Wozu sind Faktorringe (bzw. das Rechnen mit Kongruenzen) nützlich? Ein Faktorring R/I ist ein „vergröbertes“ Abbild des Rings R. Man kann auf diese Weise also Teile der Struktur, auf die es im Moment nicht ankommt, vernachlässigen und sich auf das Wesentliche konzentrieren. Oder man erhält durch die Abbildung eines Problems von R nach R/I eine einfachere Version, deren Lösbarkeit sich leichter prüfen lässt. Ist das Problem in R/I nicht lösbar, dann folgt daraus häufig, dass es auch in R nicht lösbar ist.

7.18. **Beispiel.** Wir zeigen, dass eine ganze Zahl der Form $n = 4k + 3$ nicht Summe von zwei Quadratzahlen sein kann. Dazu rechnen wir „modulo 4“, also im Faktorring $\mathbb{Z}/4\mathbb{Z}$. Das Bild von n ist $[n] = [3]$. Gilt $n = a^2 + b^2$, dann haben wir auch $[3] = [n] = [a]^2 + [b]^2$. Nun ist aber $[0]^2 = [2]^2 = [0]$ und $[1]^2 = [3]^2 = [1]$, also gibt es für $[a]^2 + [b]^2$ nur die Möglichkeiten $[0]$, $[1]$, oder $[2]$, ein Widerspruch.

Ähnlich sieht man, dass zum Beispiel 31 nicht Summe von drei Kuben sein kann, d.h. die Gleichung $a^3 + b^3 + c^3 = 31$ hat keine Lösung in ganzen Zahlen. (Man beachte, dass man hier, im Gegensatz zu $a^2 + b^2 = 31$, keine Schranken für a, b, c angeben kann, da die Zahlen auch negativ sein können.) Dazu betrachten wir das Problem in $\mathbb{Z}/9\mathbb{Z}$. Man findet, dass $[a]^3 \in \{[0], [1], [8]\}$ ist; daraus folgt, dass eine Summe von drei Kuben in $\mathbb{Z}/9\mathbb{Z}$ niemals $[4]$ oder $[5]$ sein kann. Es ist aber $[31] = [4]$, also gibt es keine Lösung.

Was wir hier entscheidend benutzen, ist die *Endlichkeit* der Ringe $\mathbb{Z}/n\mathbb{Z}$. Dadurch lässt sich die Lösbarkeit jeder Gleichung in so einem Ring in endlich vielen Schritten überprüfen. Für den Ring $\mathbb{Z}$ gilt das nicht. Zum Beispiel ist immer noch unbekannt, ob die Gleichung $a^3 + b^3 + c^3 = 33$ in ganzen Zahlen lösbar ist. (Wer Lust und Zeit hat, kann versuchen, eine Lösung von $a^3 + b^3 + c^3 = 30$ zu finden. Von dieser Gleichung weiß man, dass sie lösbar ist.)

Wir wollen jetzt Lemma 7.8, (3) und Satz 7.14 kombinieren, um einen Zusammenhang herzustellen zwischen Eigenschaften des Bildes und des Kerns eines Ringhomomorphismus. Dazu definieren wir erst einmal die relevanten Eigenschaften von Idealen.

7.19. **Definition.** Sei R ein Ring und $I \subset R$ ein Ideal.

(1) I heißt *maximales Ideal* von R, wenn $I \neq R$ ist und für alle Ideale J von R mit $I \subset J$ gilt $J = I$ oder $J = R$. (D.h., I ist ein maximales Element bezüglich Inklusion in der Menge aller *echten* Ideale von R.)
(2) I heißt *Primideal* von R, wenn $I \neq R$ ist und für je zwei Elemente $a, b \in R$ gilt, dass aus $ab \in I$ folgt, dass $a \in I$ oder $b \in I$ ist.

7.20. **Bemerkungen.**

(1) Man sieht, dass ein Element $p \in R$ genau dann Primelement ist, wenn $p \neq 0$ ist und das von p erzeugte Hauptideal Rp ein Primideal ist.
(2) Aus den Definitionen folgt:

$$R \text{ Integritätsbereich} \iff 0 \subset R \text{ Primideal}$$

(3) Im Beweis von Satz 6.9 haben wir eigentlich auch bewiesen, dass jedes maximale Ideal ein Primideal ist: Sei $M \subset R$ ein maximales Ideal, und seien $a, b \in R \setminus M$. Wir müssen zeigen, dass $ab \notin M$ ist. Da $a \notin M$ und M maximal ist, folgt $Ra + M = \langle M \cup \{a\}\rangle_R = R$, ebenso $Rb + M = R$. Es gibt also $r, r' \in R$, $m, m \in M$ mit $ra + m = 1 = r'b + m'$. Wir erhalten $(rr')(ab) + (ram' + r'bm + mm') = 1$, was zeigt, dass $Rab + M = R$ ist, also kann ab nicht in M sein.

7.21. **Proposition.** *Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus.*

(1) $\operatorname{im}\phi$ *ist genau dann ein Körper, wenn* $\ker\phi \subset R_1$ *ein maximales Ideal ist.*
(2) $\operatorname{im}\phi$ *ist genau dann ein Integritätsbereich, wenn* $\ker\phi$ *ein Primideal ist.*

Wegen $R_1/\ker\phi \cong \operatorname{im}\phi$ kann man das auch wie folgt formulieren, ohne auf einen Ringhomomorphismus Bezug zu nehmen:

Sei R ein Ring, $I \subset R$ ein Ideal.

(1) *R/I ist genau dann ein Körper, wenn I ein maximales Ideal ist.*
(2) *R/I ist genau dann ein Integritätsbereich, wenn I ein Primideal ist.*

Beweis.

(1) Nach Lemma 7.8, (3) haben wir eine Bijektion zwischen den Idealen von $\operatorname{im}\phi$ und den $\ker\phi$ enthaltenden Idealen von R_1. Nun ist ein (kommutativer) Ring ein Körper genau dann, wenn er *genau zwei* Ideale hat. Die Aussage „$\operatorname{im}\phi$ ist ein Körper“ ist also äquivalent zu „es gibt genau zwei Ideale I von R_1 mit $\ker\phi \subset I$“. Das ist aber genau die Definition von „$\ker\phi$ ist maximales Ideal von R_1“.
(2) $\operatorname{im}\phi$ ist *kein* Integritätsbereich genau dann, wenn $\operatorname{im}\phi$ Nullteiler hat. Das bedeutet, es gibt $a, b \in R_1$ mit $\phi(a), \phi(b) \neq 0$ und $\phi(a)\phi(b) = 0$. Zurückübersetzt nach R_1 heißt das, $a, b \notin \ker\phi$, aber $ab \in \ker\phi$. Solche Elemente gibt es genau dann, wenn $\ker\phi$ kein Primideal ist. (Beachte: Die Bedingung $\ker\phi \neq R_1$ schließt den Nullring als $\operatorname{im}\phi$ aus, der definitionsgemäß kein Integritätsbereich ist.)

□

7.22. **Beispiel.** Wir sehen etwa, dass das Ideal N der Nullfolgen im Ring C der Cauchy-Folgen über $\mathbb{Q}$ ein maximales Ideal ist, denn es ist der Kern eines Ringhomomorphismus, dessen Bild ein Körper ist.

7.23. **Faktorringe von $\mathbb{Z}$.** Welche Faktorringe $\mathbb{Z}/n\mathbb{Z}$ (mit $n \geq 0$) sind Körper? Das ist dazu äquivalent, dass $n\mathbb{Z}$ ein maximales Ideal von $\mathbb{Z}$ ist. Da $\mathbb{Z}$ ein Hauptidealring ist, ist ein maximales Ideal das selbe wie ein maximales *Hauptideal*. Ein Hauptideal ist genau dann ein maximales Hauptideal, wenn sein Erzeuger irreduzibel ist. Es folgt:

$\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.

Dass n eine Primzahl sein muss, sieht man auch so recht leicht: Ist $n = ab$ nämlich eine echte Faktorisierung, dann ist (zum Beispiel) $[a] \in \mathbb{Z}/n\mathbb{Z}$ ein Nullteiler wegen $[a] \neq [0]$, $[a] \cdot [b] = [ab] = [n] = [0]$.

Wenn $n = p$ eine Primzahl ist und $[0] \neq [a] \in \mathbb{Z}/p\mathbb{Z}$, dann ist p kein Teiler von a, also gilt $\operatorname{ggT}(a, p) = 1$. Es gibt also $x, y \in \mathbb{Z}$ mit $xa + yp = 1$, und man sieht $[a] \cdot [x] = [1]$. Damit ist $[a]$ invertierbar, also ($[a] \neq [0]$ war beliebig) ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Wir schreiben oft $\mathbb{F}_p$ für den Körper $\mathbb{Z}/p\mathbb{Z}$. („$\mathbb{F}$“ wegen *field*, der englischen Bezeichnung für „Körper“.)

Man sieht, dass der Ring $\mathbb{Z}/n\mathbb{Z}$ schon dann ein Körper ist, wenn er ein Integritätsbereich ist. Allgemeiner gilt:

7.24. **Satz.** *Ein endlicher Integritätsbereich ist bereits ein Körper.*

Beweis. Sei R ein endlicher Integritätsbereich. Dann gilt jedenfalls $1 \neq 0$, und es ist nur zu zeigen, dass jedes Element $0 \neq a \in R$ invertierbar ist. Wir betrachten die Abbildung $m_a : R \to R$, $x \mapsto ax$. Da R ein Integritätsbereich ist, ist a kein Nullteiler, also ist m_a injektiv ($ax = ay \implies a(x - y) = 0 \implies x = y$). Da R

endlich ist, ist m_a auch surjektiv, also gibt es $x \in R$ mit $1 = m_a(x) = ax$; damit ist a invertierbar. □

Ganz genauso sieht man, dass in einem endlichen nicht notwendig kommutativen Integritätsring jedes von null verschiedene Element (links- und rechts-)invertierbar ist. Andererseits gibt es ein (schwieriger zu beweisendes) Resultat von Wedderburn, das besagt, dass es keine endlichen Schiefkörper gibt. Es folgt, dass jeder endliche (nicht notwendig kommutative) Integritätsring schon ein Körper (und damit tatsächlich kommutativ) ist.

8. Summen von zwei und vier Quadraten

Wir wollen unsere neuen Erkenntnisse anwenden, um herauszufinden, welche natürlichen Zahlen sich als Summe von zwei Quadratzahlen schreiben lassen. Wir werden dazu den Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen und seine Normfunktion $N(a+bi) = a^2 + b^2$ verwenden. Es ist klar, dass genau die natürlichen Zahlen Summen von zwei Quadratzahlen sind, die als Wert von N vorkommen. Wir setzen

$$S_2 = \{a^2 + b^2 \mid a, b \in \mathbb{Z}\} = N\big(\mathbb{Z}[i]\big)\,.$$

Da N multiplikativ und $\mathbb{Z}[i]$ faktoriell ist, muss folgendes gelten:

8.1. **Lemma.** *Sei $\mathbb{P}_{\mathbb{Z}[i]}$ ein Repräsentantensystem der Primelelemente von $\mathbb{Z}[i]$ bis aus Assoziiertheit. Die Menge S_2 besteht genau aus der Null und allen Produkten (einschließlich des leeren Produkts) von Zahlen der Form $N(\pi)$ mit $\pi \in \mathbb{P}_{\mathbb{Z}[i]}$.*

Beweis. Sei $0 \neq n \in S_2$. Dann gibt es ein Element $\alpha \in \mathbb{Z}[i]$ mit $N(\alpha) = n$. Wir können α schreiben als eine Einheit mal ein Produkt von Elementen von $\mathbb{P}_{\mathbb{Z}[i]}$: $\alpha = u\prod_j \pi_j$. Dann gilt $n = N(\alpha) = \prod_j N(\pi_j)$ (denn $N(u) = 1$ und N ist multiplikativ). Umgekehrt ist jedes Produkt n von Zahlen der Form $N(\pi)$ mit $\pi \in \mathbb{P}_{\mathbb{Z}[i]}$ die Norm eines geeigneten Elements von $\mathbb{Z}[i]$, also ist n ein Element von S_2. □

Wir müssen also noch herausfinden, was die Primelemente von $\mathbb{Z}[i]$ sind. Wir haben das Ergebnis schon als Satz 6.17 formuliert.

8.2. **Satz.** *Ein Repräsentantensystem der Primelemente von $\mathbb{Z}[i]$ bis auf Assoziiertheit ist gegeben durch*

(1) $1 + i$,
(2) *q für Primzahlen $q \equiv 3 \bmod 4$,*
(3) *$a + bi$ und $a - bi$ mit $a^2 + b^2 = p$ für Primzahlen $p \equiv 1 \bmod 4$.*

Beweis. Wir zeigen zuerst, dass jedes Primelement π von $\mathbb{Z}[i]$ eine Primzahl p teilt (Teilbarkeit im Ring $\mathbb{Z}[i]$). Dazu bemerken wir, dass π ein Teiler von $n = \pi\bar{\pi} = N(\pi) \in \mathbb{Z}$ ist. Wir können n in $\mathbb{Z}$ faktorisieren: $n = p_1 p_2 \cdots p_k$ mit Primzahlen $p_1, p_2, \ldots, p_k$. Da π ein Primelement ist, muss π einen der Faktoren teilen (das Produkt kann nicht leer sein, sonst wäre $N(\pi) = 1$ und π eine Einheit), also teilt π eine Primzahl p.

Da die Normfunktion multiplikativ ist, folgt $N(\pi) \mid N(p) = p^2$. Damit gilt entweder $N(\pi) = p^2$, dann ist π zu p assoziiert, oder es gilt $N(\pi) = p$. Wiederum wegen der Multiplikativität der Norm ist jedes Element, dessen Norm eine Primzahl ist, irreduzibel und damit ein Primelement. Wir stellen fest, dass $N(1+i) = 2$, also ist $1 + i$ ein Primelement. Alle Elemente der Norm 2 haben die Form $\pm 1 \pm i$; man prüft nach, dass sie zu $1 + i$ assoziiert sind.

Sei jetzt $q \equiv 3 \bmod 4$ eine Primzahl. Gäbe es $\pi = a + bi \in \mathbb{Z}[i]$ mit $N(\pi) = q$, so würde $a^2 + b^2 = q \equiv 3 \bmod 4$ folgen, im Widerspruch zur Aussage, die wir in Beispiel 7.18 oben bewiesen haben. Also bleibt q selbst prim; jedes andere Primelement der Norm q^2 ist zu q assoziiert.

Sei schließlich $p \equiv 1 \bmod 4$ eine Primzahl. Wir müssen noch zeigen, dass p als Produkt $p = \pi\bar{\pi}$ zerlegt werden kann. Nach Lemma 8.4 unten gibt es $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \bmod p$ und $|x| < p/2$. Dann gilt $p \mid x^2 + 1 < p^2/4 + 1 < p^2$, also ist $N(x + i) = pm$ mit $p \nmid m$. Dann muss es in der Primfaktorzerlegung von $x + i$ ein Primelement $\pi = a + bi$ geben mit $N(\pi) = p$. Es bleibt noch zu zeigen, dass $a + bi$ und $a - bi$ nicht assoziiert sind, und dass jedes Primelement der Norm p entweder zu $a + bi$ oder zu $a - bi$ assoziiert ist. Zum ersten Punkt: Die Assoziierten von $a + bi$ sind $\pm(a + bi)$ und $\pm(-b + ai)$; wegen $a, b \neq 0$ und $a \neq \pm b$ sind sie von $a - bi$ verschieden (die Norm $p = a^2 + b^2$ ist nicht von der Form x^2 oder $2x^2$). Zum zweiten Punkt: Jedes Primelement der Norm p ist ein Teiler von $p = \pi\bar{\pi}$, muss also zu $\pi = a + bi$ oder $\bar{\pi} = a - bi$ assoziiert sein. □

Wir halten als Spezialfall fest:

8.3. **Zwei-Quadrate-Satz für Primzahlen.**
Sei $p \equiv 1 \bmod 4$ eine Primzahl. Dann gibt es $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$ (und diese Darstellung ist bis auf Reihenfolge und Vorzeichen eindeutig).

Dieser Satz wurde zuerst von Pierre de Fermat im 17. Jahrhundert (auf andere Weise) bewiesen.

Um den Beweis abzuschließen, müssen wir noch folgendes Lemma zeigen.

8.4. **Lemma.** *Sei $p \equiv 1 \bmod 4$ eine Primzahl. Dann gibt es $x \in \mathbb{Z}$ mit $|x| < p/2$ und $p \mid x^2 + 1$.*

Beweis. Wir zeigen zuerst die *Wilsonsche Kongruenz* $(p-1)! \equiv -1 \bmod p$ (sie gilt für jede Primzahl p). Dazu erinnern wir uns daran, dass $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper ist. Die Aussage ist äquivalent dazu, dass in $\mathbb{F}_p$ gilt $[(p-1)!] = \prod_{[a]\neq[0]}[a] = -[1]$. Nun sind $[1]$ und $-[1]$ die beiden einzigen Elemente von $\mathbb{F}_p$, die mit ihrem Inversen übereinstimmen (in einem Körper folgt aus $x^2 = 1$, also $0 = x^2 - 1 = (x-1)(x+1)$, dass $x = \pm 1$ ist). Die anderen kann man mit ihrem Inversen zusammenfassen, ihr Produkt ist also gleich $[1]$. Es bleiben nur die Faktoren $[1]$ und $-[1]$, und die Behauptung ist klar.

Sei jetzt $p = 2m + 1$. Es gilt ($\bmod p$)

$$\begin{aligned}
(m!)^2 &= 1 \cdot 2 \cdots (m-1) \cdot m \cdot m \cdot (m-1) \cdots 2 \cdot 1 \\
&\equiv 1 \cdot 2 \cdots (m-1) \cdot m \cdot (m-p) \cdot (m-1-p) \cdots (2-p) \cdot (1-p) \\
&= 1 \cdot 2 \cdots (m-1) \cdot m \cdot (-m-1) \cdot (-m-2) \cdots (-(p-2)) \cdots (-(p-1)) \\
&= (-1)^m \cdot 1 \cdot 2 \cdots m \cdot (m+1) \cdots (p-2) \cdot (p-1) \\
&= (-1)^m (p-1)! \equiv -(-1)^m
\end{aligned}$$

Wegen $p \equiv 1 \bmod 4$ ist in unserem Fall m gerade, also gilt $(m!)^2 \equiv -1 \bmod p$. Es gibt $q, x \in \mathbb{Z}$ mit $|x| < p/2$ und $m! = qp + x$ (Division mit „absolut kleinstem Rest“); es folgt $x^2 \equiv (m!)^2 \equiv -1 \bmod p$. □

Die sich aus dem Lemma ergebende Methode, ein x wie angegeben zu finden, ist ausgesprochen ineffizient. Es gibt wesentlich bessere Algorithmen dafür.

Wir können jetzt die Menge S_2 genau beschreiben:

8.5. **Folgerung.** *Sei $n \in \mathbb{Z}_{>0}$. Dann ist n Summe zweier Quadratzahlen genau dann, wenn $v_q(n)$ gerade ist für alle Primzahlen $q \equiv 3 \bmod 4$.*

Beweis. Nach Lemma 8.1 ist $n \in S_2$ genau dann, wenn n ein Produkt von Zahlen der Form $N(\pi)$ ist, wo π ein Primelement von $\mathbb{Z}[i]$ ist. Nach Satz 8.2 sind diese Zahlen $N(\pi)$ genau 2, q^2 für Primzahlen $q \equiv 3 \bmod 4$ und p für Primzahlen $p \equiv 1 \bmod 4$. Erfüllt n die angegebene Bedingung, dann kann man n offensichtlich als Produkt solcher Zahlen schreiben, und umgekehrt erfüllt jede dieser Zahlen die Bedingung, also auch jedes Produkt von solchen Zahlen. □

8.6. **Bemerkung.** Auf analoge Weise und unter Zuhilfenahme des Rings $\mathbb{Z}[\sqrt{-2}]$ lässt sich zeigen, dass $n > 0$ genau dann in der Form $x^2 + 2y^2$ geschrieben werden kann, wenn $v_q(n)$ gerade ist für alle Primzahlen $q \equiv 5$ oder $7 \bmod 8$. Allerdings setzt sich das nicht in der Weise fort, wie man vielleicht vermuten könnte: Es gibt zum Beispiel kein vergleichbar einfaches Kriterium dafür, wann sich n in der Form $x^2 + 23y^2$ schreiben lässt.

Als nächstes wollen wir herausfinden, welche (nichtnegativen) ganzen Zahlen sich als Summe von vier Quadraten schreiben lassen. Wir definieren dafür

$$S_4 = \{a^2 + b^2 + c^2 + d^2 \mid a, b, c, d \in \mathbb{Z}\}\,.$$

Wenn man ein wenig herumprobiert, stellt man fest, dass man offenbar für *jede* nichtnegative ganze Zahl eine solche Darstellung finden kann. Bevor wir das beweisen, lernen wir erst einmal einen Schiefkörper kennen.

8.7. **Der Schiefkörper der Quaternionen.** Man kann zeigen, dass der Körper der komplexen Zahlen der einzige Körper ist, der die reellen Zahlen echt enthält und ein endlich-dimensionaler $\mathbb{R}$-Vektorraum ist. Es gibt aber noch einen etwas größeren *Schiefkörper*. Er wurde von Hamilton entdeckt; seine Elemente wurden von ihm *Quaternionen* getauft (Singular: die Quaternion). Man bezeichnet ihn zu Ehren Hamiltons mit $\mathbb{H}$ (denn $\mathbb{Q}$ ist ja schon belegt). $\mathbb{H}$ ist ein vierdimensionaler $\mathbb{R}$-Vektorraum mit Basis $1, i, j, k$ (damit sind Nullelement, Addition und Negation definiert). Die Multiplikation erfüllt die Distributivgesetze, ist verträglich mit der $\mathbb{R}$-Vektorraumstruktur und ist auf der Basis gegeben durch

$$i^2 = j^2 = k^2 = -1\,, \qquad ij = k, jk = i, ki = j\,, \qquad ji = -k, kj = -i, ik = -j$$

(und natürlich $1^2 = 1$, $1 \cdot i = i$ und so weiter). Man kann dann nachprüfen, dass die so definierte Multiplikation assoziativ ist, so dass $\mathbb{H}$ zu einem (nichtkommutativen) Ring wird. Die reellen Zahlen sitzen in natürlicher Weise in $\mathbb{H}$; sie vertauschen mit allen Quaternionen: $r\alpha = \alpha r$ für alle $r \in \mathbb{R}$ und $\alpha \in \mathbb{H}$.

Für eine Quaternion $\alpha = a + bi + cj + dk$ (mit $a, b, c, d \in \mathbb{R}$) definiert man die *konjugierte Quaternion* $\bar\alpha = a - bi - cj - dk$. Dann findet man

$$N(\alpha) := \alpha\bar\alpha = a^2 + b^2 + c^2 + d^2 = \bar\alpha\alpha \in \mathbb{R}_{\geq 0}\,.$$

Diese *Norm* $N(\alpha)$ ist also nichts anderes als die quadrierte euklidische Länge des entsprechenden Vektors.

Weiter findet man, dass die Konjugationsabbildung $\alpha \mapsto \bar\alpha$ zwar kein Ringhomomorphismus ist, aber ein *Anti-Automorphismus* von $\mathbb{H}$. Das bedeutet, dass alle Eigenschaften eines Ringautomorphismus erfüllt sind, nur dass die Anwendung auf ein Produkt die Reihenfolge der Faktoren vertauscht: $\overline{\alpha\beta} = \bar\beta\,\bar\alpha$. Es folgt

$$N(\alpha\beta) = \alpha\beta\,\overline{\alpha\beta} = \alpha\,\beta\bar\beta\,\bar\alpha = \alpha\,N(\beta)\,\bar\alpha = \alpha\bar\alpha\,N(\beta) = N(\alpha)N(\beta)\,,$$

also ist die Norm multiplikativ.

Offenbar ist

$$\mathbb{Z}_{\mathbb{H}} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\} \subset \mathbb{H}$$

ein Unterring, und es gilt $S_4 = N(\mathbb{Z}_{\mathbb{H}})$. Aus der Multiplikativität der Norm folgt dann analog wie für S_2:

8.8. **Lemma.** *Die Menge S_4 ist multiplikativ abgeschlossen.*

Es genügt also zu beweisen, dass jede *Primzahl* Summe von vier Quadraten ist. Dazu kommen wir gleich. Erst einmal wollen wir uns davon überzeugen, dass $\mathbb{H}$ tatsächlich ein Schiefkörper ist, dass also alle von null verschiedenen Elemente invertierbar sind. Dazu stellen wir erst einmal fest, dass die Norm $N(\alpha)$ genau dann verschwindet, wenn $\alpha = 0$ ist. Für $\alpha \neq 0$ ist also $N(\alpha) \neq 0$, und wir haben

$$\alpha \cdot \frac{1}{N(\alpha)}\bar{\alpha} = \frac{1}{N(\alpha)} \cdot \alpha\bar{\alpha} = \frac{1}{N(\alpha)} \cdot N(\alpha) = 1$$

und ebenso $\frac{1}{N(\alpha)}\bar{\alpha} \cdot \alpha = 1$. Also ist

$$\alpha^{-1} = \frac{1}{N(\alpha)}\bar{\alpha}$$

das Inverse von α. (Man sieht, dass vieles sehr ähnlich funktioniert wie bei den komplexen Zahlen.)

Als ersten Schritt für den Beweis, dass jede Primzahl in S_4 ist, brauchen wir eine Hilfsaussage.

8.9. **Lemma.** *Sei p eine Primzahl. Dann gibt es $u, v \in \mathbb{Z}$ mit $u^2 + v^2 \equiv -1 \bmod p$ und $|u|, |v| \leq p/2$.*

Beweis. Für $p = 2$ ist die Behauptung leicht nachzuprüfen. Sei also jetzt p ungerade. Wir betrachten den Körper $\mathbb{F}_p$; es ist zu zeigen, dass es $[u], [v] \in \mathbb{F}_p$ gibt mit $[u]^2 + [v]^2 = -[1]$ oder äquivalent, $[u]^2 = -[1] - [v]^2$. Ich behaupte, dass die Menge $\{[u]^2 \mid [u] \in \mathbb{F}_p\}$ genau $(p+1)/2$ Elemente hat. Dazu betrachten wir die Abbildung $q : \mathbb{F}_p \to \mathbb{F}_p$, $[u] \mapsto [u]^2$. Ihre Fasern sind entweder leer, haben ein Element (genau für $[0]$) oder zwei Elemente $[u]$ und $-[u]$. (Letzteres, weil in einem Körper aus $x^2 = a^2$ folgt $x = a$ oder $x = -a$, und für $[u] \neq [0]$ die beiden Elemente $[u]$ und $-[u]$ verschieden sind, denn $p \neq 2$.) Es folgt, dass die $p - 1$ von null verschiedenen Elemente auf $(p-1)/2$ Werte abgebildet werden und damit die Behauptung.

Damit gilt auch, dass die Menge $\{-[1] - [v]^2 \mid [v] \in \mathbb{F}_p\}$ genau $(p+1)/2$ Elemente hat (denn $[a] \mapsto -[1] - [a]$ ist eine Bijektion). Die beiden Mengen können nicht disjunkt sein, denn $\mathbb{F}_p$ hat nur $p < p+1 = (p+1)/2 + (p+1)/2$ Elemente. Deshalb ist die Gleichung $[u]^2 + [v]^2 = -[1]$ in $\mathbb{F}_p$ lösbar. Übersetzt bedeutet, dass, es gibt ganze Zahlen u und v mit $u^2 + v^2 \equiv -1 \bmod p$. Wir können u und v durch ihre betragsmäßig kleinsten Reste modulo p ersetzen (dann haben wir $|u|, |v| < p/2$), ohne die Kongruenz zu stören. □

8.10. **Vier-Quadrate-Satz für Primzahlen.** *Sei p eine Primzahl. Dann gibt es $a, b, c, d \in \mathbb{Z}$ mit $p = a^2 + b^2 + c^2 + d^2$.*

Beweis. Sei $M = \{m \in \mathbb{Z}_{>0} \mid mp \in S_4\}$. Wir zeigen zuerst, dass M nicht leer ist. Nach Lemma 8.9 gibt es $u, v \in \mathbb{Z}$ mit $|u|, |v| \leq p/2$ und $p \mid 1^2 + u^2 + v^2$. Dann ist

$$S_4 \ni 1^2 + u^2 + v^2 = mp \quad \text{mit} \quad m \leq (1 + (p/2)^2 + (p/2)^2)/p < p\,,$$

also gibt es Elemente in M, und $\min M < p$. Wenn wir zeigen können, dass $\min M = 1$ ist, dann sind wir fertig. Also nehmen wir an, dass $m_0 = \min M > 1$ und versuchen, daraus einen Widerspruch abzuleiten. Sei $\alpha = a + bi + cj + dk \in \mathbb{Z}_{\mathbb{H}}$ mit $N(\alpha) = m_0 p$. Wir wählen $\beta = r + si + tj + uk \in \mathbb{Z}_{\mathbb{H}}$ mit $|r|, |s|, |t|, |u| \leq m_0/2$ und $\beta \equiv \bar{\alpha} \bmod m_0$ (d.h., $r \equiv a$, $s \equiv -b$, $t \equiv -c$, $u \equiv -d \bmod m_0$). Dann ist $N(\beta) = r^2 + s^2 + t^2 + u^2 \leq 4(m_0/2)^2 \leq m_0^2$, und

$$N(\beta) \equiv a^2 + b^2 + c^2 + d^2 = N(\alpha) \equiv 0 \bmod m_0\,,$$

also $N(\beta) = mm_0$ mit $0 \leq m \leq m_0$. Für unser Argument brauchen wir, dass $0 < m < m_0$ ist. Wäre $m = 0$, dann wäre auch $\beta = 0$, also α durch m_0 teilbar und damit $m_0 p = N(\alpha)$ durch m_0^2 teilbar, was wegen $1 < m_0 < p$ und p prim nicht möglich ist. Wäre $m = m_0$, dann hätten wir oben überall Gleichheit, also wäre $m_0 = 2m'$ gerade und $|r| = |s| = |t| = |u| = m'$. Es folgte

$$a \equiv b \equiv c \equiv d \equiv m' \bmod m_0\,,$$

das heißt, $a = a'm'$, $b = b'm'$, $c = c'm'$, $d = d'm'$ mit a', b', c', d' ungerade. Damit ist

$$(a')^2 + (b')^2 + (c')^2 + (d')^2 \equiv 1 + 1 + 1 + 1 \equiv 0 \bmod 4\,,$$

und wir hätten, dass

$$m_0 p = N(\alpha) = a^2 + b^2 + c^2 + d^2 = \big((a')^2 + (b')^2 + (c')^2 + (d')^2\big)(m')^2$$

durch $4(m')^2 = m_0^2$ teilbar ist, so dass wir wie eben einen Widerspruch erhalten. Es gilt also $0 < m < m_0$.

Wir zeigen nun, dass $m \in M$ ist; das ist der gesuchte Widerspruch, denn m_0 sollte ja das kleinste Element von M sein. Dazu berechnen wir

$$N(\alpha\beta) = N(\alpha)N(\beta) = mm_0^2 p$$

und (Kongruenz bedeutet koeffizientenweise Kongruenz)

$$\alpha\beta \equiv \alpha\bar{\alpha} = N(\alpha) \equiv 0 \bmod m_0\,.$$

Letzteres bedeutet, dass alle Koeffizienten von $\alpha\beta$ durch m_0 teilbar sind, d.h. $\gamma = \alpha\beta/m_0 \in \mathbb{Z}_{\mathbb{H}}$. Außerdem gilt

$$N(\gamma) = \mathbb{N}\Big(\frac{\alpha\beta}{m_0}\Big) = \frac{mm_0^2 p}{m_0^2} = mp\,,$$

und damit ist $m \in M$ wie gewünscht. □

Aus der multiplikativen Abgeschlossenheit von S_4 folgt jetzt:

8.11. **Vier-Quadrate-Satz von Lagrange.** *Jede nichtnegative ganze Zahl n kann man in der Form $n = a^2 + b^2 + c^2 + d^2$ mit $a, b, c, d \in \mathbb{Z}$ schreiben.*

8.12. **Bemerkung.** Ein analoger Beweis durch „Abstieg“ ist auch für den Zwei-Quadrate-Satz möglich (Übung).

Wie sieht es mit Summen von *drei* Quadraten aus?

Es gilt folgender Satz, der zuerst von Gauß bewiesen wurde:

8.13. **Drei-Quadrate-Satz.** *Eine nichtnegative ganze Zahl n lässt sich genau dann in der Form $n = a^2+b^2+c^2$ mit $a, b, c \in \mathbb{Z}$ schreiben, wenn n nicht die Form $4^m(8k+7)$ mit $k, m \in \mathbb{Z}_{\geq 0}$ hat.*

Dass die Bedingung notwendig ist (sich also Zahlen der angegebenen Form *nicht* als Summen dreier Quadrate schreiben lassen), ist nicht schwer zu sehen (Betrachtung modulo 8, Übung). Die Umkehrung verlangt tiefere Hilfsmittel, die wir hier nicht zur Verfügung haben. Einen Hinweis darauf, dass dieser Fall schwieriger ist, gibt die Tatsache, dass die Menge

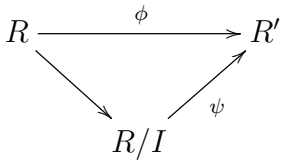
$$S_3 = \{a^2 + b^2 + c^2 \mid a, b, c \in \mathbb{Z}\}$$

keine multiplikative Struktur besitzt wie S_2 und S_4: Zum Beispiel gilt $3, 5 \in S_3$, aber $3 \cdot 5 = 15 \notin S_3$.

9. Der Chinesische Restsatz

Nach unserem Ausflug in die Zahlentheorie kehren wir zurück zu Ringen, speziell Faktorringen. Wir beginnen mit einem Resultat darüber, wann ein Ringhomomorphismus $R \to R'$ einen Ringhomomorphismus $R/I \to R'$ induziert. Es sind wieder alle Ringe *kommutativ*, wenn nichts anderes gesagt wird.

9.1. **Satz.** *Sei $\phi : R \to R'$ ein Ringhomomorphismus und $I \subset R$ ein Ideal. Es gibt genau dann einen Ringhomomorphismus $\psi : R/I \to R'$, der das Diagramm*



kommutativ macht, wenn $I \subset \ker \phi$ ist. (Dabei ist die Abbildung $R \to R/I$ der kanonische Epimorphismus.) In diesem Fall ist ψ eindeutig bestimmt.

Wir sagen, dass ψ von ϕ *induziert* wird.

Beweis. Wir nehmen zunächst an, dass es einen solchen Homomorphismus ψ gibt. Dann gilt für $r \in I$

$$\phi(r) = \psi([r]) = \psi([0]) = 0\,,$$

also ist $r \in \ker \phi$. Da $r \in I$ beliebig war, folgt $I \subset \ker \phi$.

Umgekehrt nehmen wir an, dass I in $\ker \phi$ enthalten ist. Für $r_1, r_2 \in R$ mit $[r_1] = [r_2]$ gilt dann

$$\phi(r_1) = \phi\big((r_1 - r_2) + r_2\big) = \phi(r_1 - r_2) + \phi(r_2) = \phi(r_2)\,,$$

weil $r_1 - r_2 \in \ker \phi$ ist. Damit ist die Abbildung

$$\psi : R/I \longrightarrow R'\,, \qquad [r] \longmapsto \phi(r)$$

wohldefiniert; es ist klar, dass ψ das Diagramm kommutativ macht. Man rechnet nach, dass ψ ein Ringhomomorphismus ist:

$$\psi([1]) = \phi(1) = 1$$
$$\psi([r_1] + [r_2]) = \psi([r_1 + r_2]) = \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = \psi([r_1]) + \psi([r_2])$$

und ebenso für das Produkt. Der Homomorphismus ψ ist eindeutig bestimmt, denn es muss $\psi([r]) = \phi(r)$ gelten, damit das Diagramm kommutiert. □

9.2. **Folgerung.** *Sei R ein Ring, und seien $I \subset J$ Ideale von R. Dann definiert*

$$R/I \longrightarrow R/J\,, \qquad r + I \longmapsto r + J$$

einen surjektiven Ringhomomorphismus.

Da dieser Homomorphismus vom kanonischen Epimorphismus $R \to R/J$ induziert wird, wird auch er als ein *kanonischer Ringhomomorphismus* bezeichnet.

Beweis. Wir wenden Satz 9.1 auf den kanonischen Epimorphismus $\pi : R \to R/J$ an. Da $I \subset J = \ker \pi$, folgt die Existenz und Eindeutigkeit des angegebenen Homomorphismus. Da jedes Element von R/J sich in der Form $r + J$ schreiben lässt, ist der Homomorphismus surjektiv. □

Als nächstes betrachten wir Produkte von Ringen. Einen Spezialfall davon haben wir schon in Gestalt der Ringe R^X gesehen.

9.3. **Definition.** Sei $(R_i)_{i\in I}$ eine Familie von Ringen. Sei $R = \prod_{i\in I} R_i$ ihr cartesisches Produkt. Dann ist R ein Ring, wenn wir Addition und Multiplikation komponentenweise definieren:

$$(r_i)_{i\in I} + (s_i)_{i\in I} = (r_i + s_i)_{i\in I}\,, \qquad (r_i)_{i\in I} \cdot (s_i)_{i\in I} = (r_i s_i)_{i\in I}$$

Der Ring R heißt das *direkte Produkt* der Ringe R_i. Ist $I = \{1, 2, 3, \ldots, n\}$ endlich, dann schreiben wir auch

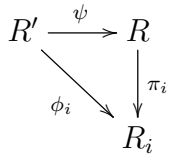
$$R = R_1 \times R_2 \times \cdots \times R_n\,.$$

Für jedes $i \in I$ gibt es einen Ringhomomorphismus $\pi_i : R \to R_i$, der $(r_j)_{j\in I}$ auf die i-te Komponente r_i abbildet. Dieser (surjektive) Homomorphismus heißt die *i-te Projektion.*

Ist die Indexmenge I leer, dann ist R der Nullring.

Das Produkt von Ringen hat eine universelle Eigenschaft.

9.4. **Proposition (Universelle Eigenschaft des Produkts von Ringen).** *Sei $(R_i)_{i\in I}$ eine Familie von Ringen und R ihr direktes Produkt. Sei R' ein weiterer Ring, und seien (für $i \in I$) $\phi_i : R' \to R_i$ Ringhomomorphismen. Wenn $\pi_i : R \to R_i$ die i-te Projektion bezeichnet, dann gibt es genau einen Ringhomomorphismus $\psi : R' \to R$, so dass alle Diagramme*



kommutativ sind.

Beweis. Dass ψ als Abbildung existiert und eindeutig ist, ist eine Aussage der Mengentheorie: Es muss gelten $\psi(r) = \big(\phi_i(r)\big)_{i\in I}$. Man prüft sofort nach, dass ψ auch ein Ringhomomorphismus ist. □

Wir betrachten nun folgende Situation: R ist ein Ring, und wir haben Ideale $I_1, I_2, \ldots, I_n$ von R. Dann induzieren die kanonischen Epimorphismen $\phi_j : R \to R/I_j$ einen Ringhomomorphismus

$$\psi : R \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n\,.$$

Der Kern von ψ ist offensichtlich

$$\ker\psi = \ker\phi_1 \cap \ker\phi_2 \cap \ldots \cap \ker\phi_n = I_1 \cap I_2 \cap \ldots \cap I_n\,,$$

so dass wir einen injektiven Ringhomomorphismus

$$\tilde{\psi} : R/(I_1 \cap \ldots \cap I_n) \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

erhalten. Jetzt stellt sich die Frage: Wann ist $\tilde{\psi}$ auch surjektiv und damit ein Isomorphismus? Anders formuliert: Gegeben $a_1, a_2, \ldots, a_n \in R$, unter welchen Bedingungen gibt es stets ein Element $r \in R$ mit

$$r \equiv a_1 \bmod I_1\,, \quad r \equiv a_2 \bmod I_2\,, \quad \ldots, \quad r \equiv a_n \bmod I_n\,?$$

9.5. **Lemma.** *Der Homomorphismus $\tilde{\psi}$ ist genau dann surjektiv, wenn es Elemente $r_1, \ldots, r_n \in R$ gibt, so dass*

$$r_j \equiv 1 \bmod I_j \quad \textit{und} \quad r_j \in I_k \textit{ für alle } k \neq j$$

gilt. Das ist genau dann der Fall, wenn $I_j + I_k = R$ für alle $1 \leq j < k \leq n$.

Hier steht für Ideale I, J von R die Summe $I + J$ für

$$I + J = \langle I \cup J\rangle_R = \{r + s \mid r \in I, s \in J\}\,.$$

Beweis. Wenn $\tilde{\psi}$ surjektiv ist, dann können wir $a_j = 1$ und $a_k = 0$ für $k \neq j$ wählen, so dass wir die Elemente r_j bekommen. Umgekehrt ist $r = a_1r_1 + \cdots + a_nr_n$ ein Element, das die verlangten Kongruenzen erfüllt, also ist die Existenz der r_j auch hinreichend für die Surjektivität von $\tilde{\psi}$.

Zur zweiten behaupteten Äquivalenz: Wir nehmen zuerst an, dass die r_j existieren. Wegen $1 = (1 - r_j) + r_j \in I_j + I_k$ für $k \neq j$ folgt, dass $I_j + I_k = R$ ist. Sei nun umgekehrt vorausgesetzt, dass $I_j + I_k = R$ ist für alle $j \neq k$. Dann gibt es $a_{jk} \in I_j$, $b_{jk} \in I_k$ mit $a_{jk} + b_{jk} = 1$. Es gilt also $b_{jk} \equiv 1 \bmod I_j$. Wir setzen $r_j = \prod_{k\neq j} b_{jk}$, dann gilt $r_j \equiv 1 \bmod I_j$ und $r_j \in I_k$ für alle $k \neq j$ wie gewünscht. □

Wir geben der relevanten Eigenschaft von Paaren von Idealen einen Namen.

9.6. **Definition.** Zwei Ideale I und J eines Ringes R heißen *komaximal* oder *zueinander prim*, wenn gilt $I + J = R$.

Sind zwei ganze Zahlen m und n teilerfremd, dann gilt $\mathrm{ggT}(m, n) = 1$, also $\mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}$, d.h., die von m und n erzeugten Hauptideale sind komaximal. Dann gilt auch

$$\mathbb{Z}m \cap \mathbb{Z}n = \mathbb{Z}\,\mathrm{kgV}(m, n) = \mathbb{Z}mn\,.$$

Lässt sich das verallgemeinern?

9.7. **Lemma.** *Sei R ein Ring, und seien $I_1, \ldots, I_n$ Ideale von R, die paarweise komaximal sind. Dann gilt*

$$I_1 \cap \ldots \cap I_n = I_1 \cdots I_n\,.$$

Dabei ist das Produkt der Ideale definiert durch

$$I_1 \cdots I_n = \langle\{a_1 \cdots a_n \mid a_1 \in I_1, \ldots, a_n \in I_n\}\rangle_R\,;$$

es ist also das von allen Produkten $a_1 \cdots a_n$ erzeugte Ideal, wo der Faktor a_j aus I_j ist. Es besteht aus allen endlichen Summen solcher Produkte. Als Spezialfall haben wir für Hauptideale

$$Ra_1 \cdot Ra_2 \cdots Ra_n = R(a_1a_2 \cdots a_n)\,.$$

Beweis. Es gilt stets die Inklusion „$\supset$“, denn jedes Produkt $a_1 \cdots a_n$ wie oben ist in allen Idealen I_j enthalten. Es ist noch die umgekehrte Inklusion zu zeigen. Dies geschieht durch Induktion über die Anzahl n der Ideale. Für $n = 1$ ist nichts zu zeigen. Sei also jetzt $n = 2$. Nach Voraussetzung sind die beiden Ideale I_1 und I_2 komaximal, es gibt also $a_1 \in I_1$ und $a_2 \in I_2$ mit $a_1 + a_2 = 1$. Sei $r \in I_1 \cap I_2$. Dann gilt

$$r = r \cdot 1 = r(a_1 + a_2) = a_1 r + r a_2 \in I_1 \cdot I_2 \,,$$

denn im ersten Produkt ist $r \in I_2$, im zweiten Produkt ist $r \in I_1$, also sind beide Produkte in $I_1 \cdot I_2$. Das zeigt die Behauptung für $n = 2$. Sei jetzt $n > 2$. Nach Induktionsannahme gilt $I_1 \cap \ldots \cap I_{n-1} = I_1 \cdots I_{n-1}$. Das Argument im Beweis des zweiten Teils von Lemma 9.5 zeigt, dass $I_1 \cap \ldots \cap I_{n-1}$ und I_n komaximal sind. Dann folgt mit dem Fall $n = 2$:

$$I_1 \cap \ldots \cap I_{n-1} \cap I_n = (I_1 \cap \ldots \cap I_{n-1}) \cdot I_n = I_1 \cdots I_{n-1} \cdot I_n \,.$$

(Man beachte, dass wir in diesem Beweis tatsächlich verwendet haben, dass R kommutativ ist!) □

Wir fassen unsere Ergebnisse zusammen.

9.8. **Chinesischer Restsatz.** *Sei R ein (kommutativer) Ring, und seien $I_1, \ldots, I_n$ Ideale von R, die paarweise komaximal sind. Dann gilt*

$$I_1 \cap I_2 \cap \ldots \cap I_n = I_1 \cdot I_2 \cdots I_n \,,$$

und der kanonische Homomorphismus

$$R/I_1 I_2 \cdots I_n \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

ist ein Isomorphismus.

In einem Hauptidealring sind die von zwei Elementen a und b erzeugten Ideale genau dann komaximal, wenn a und b teilerfremd sind, also ggT 1 haben. Wir erhalten folgenden Spezialfall.

9.9. **Chinesischer Restsatz für Hauptidealringe.** *Sei R ein Hauptidealring, und seien $a_1, \ldots, a_n \in R$ paarweise teilerfremd. Dann ist der kanonische Homomorphismus*

$$R/Ra_1 a_2 \cdots a_n \longrightarrow R/Ra_1 \times R/Ra_2 \times \cdots \times R/Ra_n$$

ein Isomorphismus. Anders ausgedrückt bedeutet das, dass jedes System von Kongruenzen

$$x \equiv b_1 \bmod a_1 \,, \quad x \equiv b_2 \bmod a_2 \,, \quad \ldots \,, \quad x \equiv b_n \bmod a_n$$

eine Lösung $x \in R$ besitzt, und dass die Restklasse von $x \bmod a_1 \cdots a_n$ eindeutig bestimmt ist.

Das lässt sich natürlich insbesondere auf den Ring $\mathbb{Z}$ der ganzen Zahlen anwenden. Dabei erhebt sich die Frage, wie man eine Lösung x des Systems von Kongruenzen in der Praxis berechnen kann. Dazu betrachten wir ein Beispiel.

9.10. **Beispiel.** Wir wollen das System von Kongruenzen

$$x \equiv 3 \bmod 5\,, \qquad x \equiv 4 \bmod 7\,, \qquad x \equiv 6 \bmod 11$$

lösen. Es gibt im wesentlichen zwei Möglichkeiten.

(1) Wir bestimmen die r_j wie in Lemma 9.5:

$$r_1 \equiv 1 \bmod 5\,, \qquad r_1 \equiv 0 \bmod 7 \cdot 11 = 77$$

Die Lösung kommt aus dem Erweiterten Euklidischen Algorithmus, der die Linearkombination $1 = 31 \cdot 5 - 2 \cdot 77$ liefert, also können wir $r_1 = -2 \cdot 77 = -154$ nehmen. Analog finden wir $r_2 = -55$ und $r_3 = -175$. Eine Lösung ergibt sich dann als

$$x = 3r_1 + 4r_2 + 6r_3 = -1732\,.$$

Diese Lösung ist modulo $5 \cdot 7 \cdot 11 = 385$ eindeutig bestimmt; die kleinste nichtnegative Lösung ist somit $x = 193$.

(2) Wir lösen das System iterativ. Zuerst bestimmen wir die Lösungen der ersten beiden Kongruenzen. Es ist $1 = 3 \cdot 5 - 2 \cdot 7$, also ist die Lösung gegeben durch

$$x \equiv 3 \cdot (-14) + 4 \cdot 15 = 18 \bmod 5 \cdot 7 = 35\,.$$

Jetzt müssen wir das System

$$x \equiv 18 \bmod 35\,, \qquad x \equiv 6 \bmod 11$$

lösen. Analog finden wir $1 = -5 \cdot 35 + 16 \cdot 11$ und damit

$$x \equiv 18 \cdot 176 + 6 \cdot (-175) = 2118 \equiv 193 \bmod 385\,.$$

Als Anwendung des Chinesischen Restsatzes für $\mathbb{Z}$ wollen wir uns die Einheitengruppen der Ringe $\mathbb{Z}/n\mathbb{Z}$ etwas näher betrachten. Dazu schauen wir uns erst einmal allgemein die Einheitengruppe eines Produkts von Ringen an.

9.11. **Definition.** Sei $(G_i)_{i\in I}$ eine Familie von Gruppen mit cartesischem Produkt $G = \prod_{i\in I} G_i$. Analog zur Situation bei Ringen (siehe Definition 9.3 wird G zu einer Gruppe, wenn wir die Verknüpfung komponentenweise definieren:

$$(g_i)_{i\in I} \cdot (h_i)_{i\in I} = (g_i \cdot h_i)_{i\in I}$$

Die Gruppe G mit dieser Verknüpfung heißt das *direkte Produkt* der Gruppen G_i.

Die Schreibweise $G_1 \times G_2 \times \cdots \times G_n$ für ein Produkt endlich vieler Gruppen $G_1, G_2, \ldots, G_n$ ist analog wie bei Ringen (und Produkten von Mengen). Direkte Produkte von Gruppen haben die analoge universelle Eigenschaft wie direkte Produkte von Ringen (mit dem selben Beweis).

Der Zusammenhang zwischen direkten Produkten von Ringen und Gruppen ist wie folgt.

9.12. **Proposition.** *Sei $(R_i)_{i\in I}$ eine Familie von Ringen. Dann gilt*

$$\Big(\prod_{i\in I} R_i\Big)^\times = \prod_{i\in I} R_i^\times$$

(als Teilmengen von $\prod_{i\in I} R_i$).

Die Einheitengruppe eines direkten Produkts von Ringen ist also das direkte Produkt der Einheitengruppen.

Beweis. Übung. □

Uns interessiert nun die Mächtigkeit der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ für $n \in \mathbb{Z}_{>0}$. Dafür gibt es einen Namen:

9.13. **Definition.** Sei $n \in \mathbb{Z}_{>0}$. Dann setzen wir $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. Die Funktion $\phi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ heißt *Eulersche Phi-Funktion*. Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ heißt die *prime Restklassengruppe modulo n*. Dieser Name kommt von der folgenden Tatsache:

9.14. **Lemma.** *Sei $n \in \mathbb{Z}_{>0}$. Eine Restklasse $[a] = a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ ist invertierbar genau dann, wenn $a \perp n$ ist.*

Beweis. Sei $a \in \mathbb{Z}$. Dann gilt

$$\begin{aligned} [a] \in (\mathbb{Z}/n\mathbb{Z})^\times &\iff \exists b \in \mathbb{Z} : [a] \cdot [b] = [1] \\ &\iff \exists b \in \mathbb{Z} : ab \equiv 1 \bmod n \\ &\iff \exists b, c \in \mathbb{Z} : ab + cn = 1 \\ &\iff a \perp n\,. \end{aligned}$$

□

Die invertierbaren Restklassen sind also genau die, die durch Zahlen repräsentiert werden, die prim zu n sind. Da die Restklassen eindeutig durch die Zahlen von 0 bis $n-1$ (oder von 1 bis n) repräsentiert werden, können wir $\phi(n)$ auch wie folgt beschreiben:

$$\phi(n) = \#\{0 \le a < n \mid a \perp n\} = \#\{1 \le a \le n \mid a \perp n\}\,.$$

Die Werte von ϕ für kleine Werte von n sind dann also:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	12	8	8

Es ist ziemlich klar, dass gilt

$$\phi(n) = n - 1 \iff n \text{ Primzahl}\,,$$

denn genau dann gilt

$$\{0 \le a < n \mid a \perp n\} = \{1, 2, \ldots, n-1\}\,.$$

Dies lässt sich zu einer einfachen Formel für Primzahlpotenzen verallgemeinern:

9.15. **Lemma.** *Sei p eine Primzahl und $e \in \mathbb{Z}_{>0}$. Dann gilt $\phi(p^e) = (p-1)p^{e-1}$.*

Beweis. Wir zählen die Zahlen zwischen 0 und $p^e - 1$, die zu p^e teilerfremd sind. Da alle (positiven) Teiler von p^e die Form p^f haben mit $0 \le f \le e$, gilt

$$\mathrm{ggT}(a, p^e) \neq 1 \iff p \mid a\,.$$

Wir müssen also genau die Zahlen zählen, die nicht durch p teilbar sind. Es gibt genau p^{e-1} Zahlen von 0 bis $p^e - 1$, die durch p teilbar sind (nämlich ap für $0 \le a < p^{e-1}$), also bleiben

$$\phi(p^e) = p^e - p^{e-1} = (p-1)p^{e-1}$$

Zahlen übrig. □

Zusammen mit dem Chinesischen Restsatz und Proposition 9.12 erhalten wir daraus eine Formel für $\phi(n)$.

9.16. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$. Dann gilt*

$$\phi(n) = \prod_{p|n} (p-1)p^{v_p(n)-1} = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big)\,,$$

wobei die Produkte über die Primteiler von n laufen.

Beweis. Wir haben die Primfaktorzerlegung $n = \prod_{p|n} p^{v_p(n)}$. Nach dem Chinesischen Restsatz gilt dann (Übung)

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{p|n} \mathbb{Z}/p^{v_p(n)}\mathbb{Z}$$

und nach Proposition 9.12 dann auch

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{p|n} (\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^\times\,.$$

Es folgt mit Lemma 9.15

$$\begin{aligned}\phi(n) &= \#(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{p|n} \#(\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^\times = \prod_{p|n} \phi(p^{v_p(n)}) \\ &= \prod_{p|n} (p-1)p^{v_p(n)-1} = \prod_{p|n} \Big(1-\frac{1}{p}\Big)p^{v_p(n)} = n\prod_{p|n}\Big(1-\frac{1}{p}\Big)\,.\end{aligned}$$

□

Eine weitere Möglichkeit zur rekursiven Berechnung von $\phi(n)$ liefert folgende Aussage.

9.17. **Lemma.** *Sei $n \in \mathbb{Z}_{>0}$. Dann gilt*

$$\sum_{d|n} \phi(d) = n\,,$$

wobei die Summe über alle positiven Teiler von n läuft.

Beweis. Übung. □

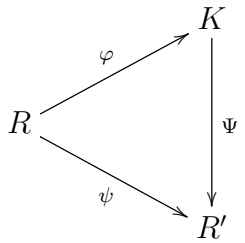
So hat man zum Beispiel $\phi(6) = 6 - \phi(3) - \phi(2) - \phi(1) = 6 - 2 - 1 - 1 = 2$.

10. Der Quotientenkörper

Sie werden sich an die Konstruktion des Körpers $\mathbb{Q}$ der rationalen Zahlen aus dem Ring $\mathbb{Z}$ der ganzen Zahlen erinnern: Man führt Quotienten a/b ein (mit $a, b \in \mathbb{Z}$, $b \neq 0$; formal sind das Äquivalenzklassen von Paaren) und definiert darauf Addition und Multiplikation durch die bekannten Formeln. Diese Konstruktion kann ohne weiteres auf beliebige Integritätsbereiche verallgemeinert werden.

10.1. **Satz und Definition.** *Sei R ein Integritätsbereich. Dann gibt es (bis auf eindeutige Isomorphie) genau einen Körper K und einen Ringhomomorphismus $\varphi : R \to K$ mit der folgenden universellen Eigenschaft:*

Zu jedem Ringhomomorphismus $\psi : R \to R'$ in einen kommutativen Ring R', so dass $\psi(R \setminus \{0\}) \subset (R')^\times$, gibt es genau einen Ringhomomorphismus $\Psi : K \to R'$, so dass das folgende Diagramm kommutiert:



Der Körper K heißt der *Quotientenkörper* (engl. *field of fractions*) von R.

Beweis. Wir konstruieren zuerst einen geeigneten Körper K und Homomorphismus φ, dann zeigen wir die universelle Eigenschaft; die Eindeutigkeit bis auf eindeutige Isomorphie folgt daraus.

Die Vorgehensweise für die Konstruktion von K ist analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ (und ähnlich zur Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$). Wir wollen die Elemente (a, b) von $M = R \times (R \setminus \{0\})$ als Repräsentanten von Quotienten a/b betrachten. Diese Darstellung ist nicht eindeutig, also müssen wir eine Äquivalenzrelation (Reflexivität, Symmetrie und Transitivität sind nachzuprüfen; für die Transitivität braucht man die Nullteilerfreiheit von R) definieren, die Paare identifiziert, die den gleichen Quotienten repräsentieren:

$$(a, b) \sim (a', b') \iff ab' = a'b\,.$$

Wir schreiben a/b für die durch (a, b) repräsentierte Äquivalenzklasse und K für die Menge $M/\sim$ der Äquivalenzklassen. Dann definieren wir Addition und Multiplikation auf K wie üblich:

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

(man beachte, dass $bd \neq 0$ wegen $b, d \neq 0$ und weil R ein Integritätsbereich ist, also liegen die Paare $(*, bd)$ wieder in M). Es ist nachzuprüfen, dass diese Verknüpfungen wohldefiniert sind, dass also der Wert nicht von der Wahl der Repräsentanten abhängt. Wir zeigen das hier für die Multiplikation; die Addition lassen wir als Übungsaufgabe. Seien also $a, b, c, d,\ a', b', c', d' \in R$ mit $b, d,\ b', d' \neq 0$ und $ab' = a'b$, $cd' = c'd$. Es ist zu zeigen, dass dann

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}\,, \qquad \text{also} \quad (ac)(b'd') = (a'c')(bd)$$

gilt. Das folgt so (unter Verwendung von Kommutativität und Assoziativität der Multiplikation):

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd)\,.$$

Dann müssen die Körperaxiome nachgerechnet werden (mit $0/1$ als Nullelement und $1/1$ als Einselement; das Inverse von a/b (mit $a \neq 0$) ist natürlich b/a). Das ist langwierig und -weilig; die Axiome für K folgen aus den Ringaxiomen, der

Kommutativität und der Nullteilerfreiheit von R. Wir müssen noch den Homomorphismus $\varphi : R \to K$ definieren. Wir setzen natürlich $\varphi(r) = r/1$; dass φ tatsächlich ein Ringhomomorphismus ist, ist leicht nachzurechnen.

Jetzt zeigen wir die universelle Eigenschaft. Sei also $\psi : R \to R'$ ein Ringhomomorphismus, so dass $\psi(r)$ invertierbar ist für alle $0 \neq r \in R$. Wenn es einen Homomorphismus $\Psi : K \to R'$ wie im Satz gibt, dann muss gelten

$$\Psi(a/b) = \Psi(\varphi(a)\varphi(b)^{-1}) = \Psi(\varphi(a))\Psi(\varphi(b))^{-1} = \psi(a)\psi(b)^{-1}\,.$$

(Beachte, dass $b \neq 0$, also $\psi(b) \in (R')^\times$, so dass $\psi(b)^{-1}$ existiert.) Das zeigt schon die Eindeutigkeit von Ψ. Die Existenz von Ψ als Abbildung folgt, wenn wir zeigen, dass uns obige Relation etwas Wohldefiniertes liefert. Sei also $a/b = a'/b'$, das bedeutet $ab' = a'b$. Dann folgt

$$\psi(ab') = \psi(a'b) \implies \psi(a)\psi(b') = \psi(a')\psi(b) \implies \psi(a)\psi(b)^{-1} = \psi(a')\psi(b')^{-1}\,,$$

also erhalten wir für $\Psi(a/b)$ das selbe Ergebnis wie für $\Psi(a'/b')$. Es bleibt zu zeigen, dass Ψ ein Ringhomomorphismus ist. Das ist nicht schwer:

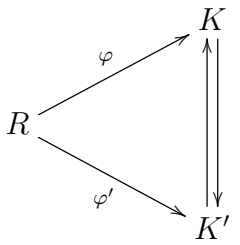
$$\Psi(1) = \Psi(1/1) = \psi(1)\psi(1)^{-1} = 1$$

und

$$\begin{aligned}\Psi\Big(\frac{a}{b} + \frac{c}{d}\Big) &= \Psi\Big(\frac{ad+bc}{bd}\Big) = \psi(ad+bc)\psi(bd)^{-1} \\ &= (\psi(a)\psi(d) + \psi(b)\psi(c))\psi(b)^{-1}\psi(d)^{-1} \\ &= \psi(a)\psi(b)^{-1} + \psi(c)\psi(d)^{-1} = \Psi\Big(\frac{a}{b}\Big) + \Psi\Big(\frac{c}{d}\Big)\,;\end{aligned}$$

für die Multiplikation geht es ähnlich.

Wie üblich folgt aus der universellen Eigenschaft die Eindeutigkeit bis auf eindeutigen Isomorphismus: Sind K', $\varphi' : R \to K'$ ein Körper und Ringhomomorphismus mit der gleichen Eigenschaft, dann gibt es eindeutig bestimmte Homomorphismen $K \to K'$ und $K' \to K$, so dass



kommutiert. (Man wende die universelle Eigenschaft einmal für K (mit K' in der Rolle von R') und einmal für K' (mit K in der Rolle von R') an.) Aus der Eindeutigkeit folgt dann, dass diese Homomorphismen zueinander invers sind, also hat man einen eindeutig bestimmten Isomorphismus von K nach K', der mit φ und φ' verträglich ist. □

In diesem Sinne ist $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$. Ist R bereits ein Körper, dann kann man $K = R$, $\varphi = \mathrm{id}_R$ nehmen.

In jedem Fall ist $\varphi : R \to K$ injektiv, denn es gilt

$$\varphi(r) = 0 \iff \frac{r}{1} = \frac{0}{1} \iff r \cdot 1 = 0 \cdot 1 \iff r = 0\,,$$

also hat φ trivialen Kern. Man identifiziert deshalb gerne R mit seinem Bild unter φ in K, betrachtet also R als Unterring von K (analog zu $\mathbb{Z} \subset \mathbb{Q}$). Die universelle Eigenschaft sagt dann, dass man den Ringhomomorphismus $R \to R'$ eindeutig

auf K fortsetzen kann, wenn er alle von null verschiedenen Elemente auf invertierbare Elemente von R' abbildet.

10.2. **Lemma.** *Ist R Unterring eines Körpers K, dann ist*

$$K' = \left\{ \frac{a}{b} \;\middle|\; a, b \in R, b \neq 0 \right\} \subset K$$

(mit der Inklusionsabbildung $\varphi : R \to K'$) der Quotientenkörper von R.

Beweis. Man zeigt das ganz genauso wie im Beweis von Satz 10.1. □

10.3. **Beispiel.** Als ein weiteres Beispiel können wir den Quotientenkörper von $\mathbb{Z}[i]$ betrachten. Da $\mathbb{Z}[i] \subset \mathbb{C}$ Unterring eines Körpers ist, kann man Lemma 10.2 anwenden und findet (Übung), dass der Quotientenkörper von $\mathbb{Z}[i]$ gerade

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

ist.

11. Polynomringe

Wir kommen zu einem zentralen Thema dieser Vorlesung: Polynomringe sind wichtig für viele algebraische Konstruktionen (etwa bei der Konstruktion von Erweiterungskörpern, siehe nächstes Semester). Aus der Analysis kennen sie sicher *Polynomfunktionen*, etwa auf $\mathbb{R}$. Das sind Funktionen der Form

$$f : x \mapsto a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \,.$$

Es ist nicht schwer zu sehen, dass diese Funktionen einen Unterring des Rings aller reellen Funktionen bilden. In diesem Fall erhält man tatsächlich (bis auf Isomorphie) den Polynomring über $\mathbb{R}$. Im allgemeinen jedoch bekommt man nicht das Richtige, wenn man Funktionen betrachtet. Zum Beispiel können wir Polynomfunktionen $f : \mathbb{F}_2 \to \mathbb{F}_2$ betrachten ($\mathbb{F}_2 = \{0, 1\}$ ist der Körper mit zwei Elementen) und stellen fest, dass $x \mapsto x$ und $x \mapsto x^2$ die selbe Funktion ergeben. Wir möchten aber gerne die „Polynome“ x und x^2 als verschiedene Objekte betrachten. Um das zu erreichen, konstruieren wir einen Ring, dessen Elemente formale Ausdrücke der Form $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ sind; dabei kommen $a_0, a_1, \ldots, a_n$ aus einem gegebenen Ring R, und x steht für ein „neues“ Element, gern *Unbestimmte* genannt. Um das Ganze wirklich auf saubere Füße zu stellen, repräsentieren wir das Polynom $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ durch die Folge $(a_0, a_1, \ldots, a_{n-1}, a_n, 0, 0, \ldots) \in R^{\mathbb{N}}$. Die Ringstruktur, die wir definieren wollen, ist aber nicht die komponentenweise Struktur vom Ring $R^{\mathbb{N}}$ der Folgen, sondern hat eine andere Multiplikation.

11.1. **Definition.** Sei R ein (nicht notwendig kommutativer) Ring. Wir konstruieren einen Ring $R[x]$ wie folgt. Die unterliegende Menge ist die Menge

$$\{(a_0, a_1, \ldots) \in R^{\mathbb{N}} \mid a_n = 0 \text{ für alle bis auf endlich viele } n\}$$

der endlichen (oder abbrechenden) Folgen von Elementen von R. Wir definieren die Addition komponentenweise. Wir setzen

$$x := (0, 1, 0, 0, 0, \ldots)$$

und definieren Multiplikation mit Elementen $r \in R$ und mit x wie folgt:

$$r \cdot (a_0, a_1, a_2, \ldots) = (ra_0, ra_1, ra_2, \ldots) \quad \text{und} \quad x \cdot (a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots) \,.$$

Dann gilt $x^n = (\underbrace{0, \ldots, 0}_{n}, 1, 0, 0, 0, \ldots)$ (bzw. wir definieren x^0 so), und

$$(a_0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n \,.$$

Das Element $a_j \in R$ heißt der *Koeffizient von* x^j oder der *j-te Koeffizient* im *Polynom* $a_0 x^0 + \ldots + a_n x^n$. Wir identifizieren R mit seinem Bild in $R[x]$ unter

$$\varphi : r \mapsto (r, 0, 0, \ldots) = r x^0 \,.$$

Damit $R[x]$ ein Ring wird, muss die Multiplikation das Distributivgesetz erfüllen. Das zwingt uns zu der Festlegung

$$\begin{aligned}(a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n) \cdot (b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m) \\ = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \ldots + (a_n b_m) x^{n+m} \,.\end{aligned}$$

Der k-te Koeffizient des Produkts ist also $\sum_{j=0}^{k} a_j b_{k-j}$. Mit den offensichtlichen Definitionen

$$0 = \varphi(0) = (0, 0, 0, \ldots) \,, \quad 1 = \varphi(1) = (1, 0, 0, \ldots)$$
$$\text{und} \quad -(a_0, a_1, \ldots) = (-a_0, -a_1, \ldots)$$

müssen wir uns noch davon überzeugen, dass $R[x]$ tatsächlich ein Ring ist. Es ist ziemlich klar, dass $(R[x], 0, +, -)$ eine abelsche Gruppe ist (denn wir haben offensichtlich eine Untergruppe der additiven Gruppe des Folgenrings $R^{\mathbb{N}}$). Es ist auch klar, dass 1 neutrales Element bezüglich der Multiplikation ist. Die weiteren Axiome (Assoziativität der Multiplikation, Distributivgesetze) verifiziert man ohne große Probleme unter Verwendung der entsprechenden Eigenschaften von R. Und natürlich ist die Einbettung $\varphi : R \to R[x]$ ein Ringhomomorphismus.

Der so konstruierte Ring $R[x]$ heißt der *Polynomring über R* in der *Unbestimmten x*. Analog kann man Polynomringe $R[X]$, $R[y]$ usw. definieren; es unterscheidet sich dabei lediglich der Name der Unbestimmten. Polynomringe in mehreren Unbestimmten erhält man durch Iteration der Konstruktion: $R[x, y] = (R[x])[y]$, $R[x, y, z] = (R[x, y])[z]$ usw.

Man beachte, dass in $R[x]$ für $r \in R \subset R[x]$ stets $rx = xr$ gilt (auch wenn R selbst nicht kommutativ ist). Es folgt:

$$R \text{ kommutativ} \implies R[x] \text{ kommutativ.}$$

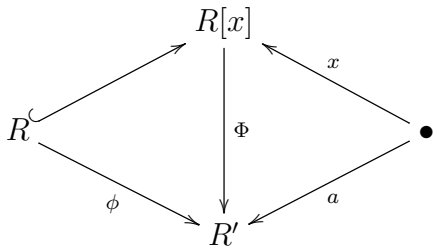
Wir werden sehen, dass sich auch andere Eigenschaften von R auf $R[x]$ vererben.

Die Idee hinter der Konstruktion des Polynomrings ist, dass man zum Ring R ein „neues“ Element x hinzufügen möchte, das von den Elementen von R vollkommen „unabhängig“ ist (außer dass es mit ihnen kommutiert). Diese Unabhängigkeit bedeutet, dass polynomiale Ausdrücke in x mit Koeffizienten in R verschieden sind, wenn nicht alle ihre Koeffizienten übereinstimmen:

$$a_0 + a_1 x + \ldots + a_n x^n = b_0 + b_1 x + \ldots + b_n x^n \iff a_0 = b_0,\ a_1 = b_1,\ \ldots,\ a_n = b_n$$

(„Koeffizientenvergleich“). In der Konstruktion wird dies dadurch erreicht, dass man ein Polynom mit der Folge seiner Koeffizienten identifiziert; damit umgeht man die Probleme beim Betrachten von Polynom*funktionen*. Auf der anderen Seite bewirkt diese Unabhängigkeit aber auch, dass man aus Polynomen Funktionen machen kann. Formal wird das ausgedrückt durch eine universelle Eigenschaft.

11.2. **Satz (Universelle Eigenschaft des Polynomrings).** *Seien R und R' Ringe, sei $a \in R'$, und sei $\phi : R \to R'$ ein Ringhomomorphismus, so dass für alle $r \in R$ gilt $\phi(r)a = a\phi(r)$ (das ist automatisch, wenn R' kommutativ ist). Dann gibt es einen eindeutig bestimmten Ringhomomorphismus $\Phi : R[x] \to R'$ mit $\Phi|_R = \phi$ und $\Phi(x) = a$:*



Beweis. Wir beginnen mit der Eindeutigkeit. Wenn Φ existiert, dann muss gelten

$$\begin{aligned}\Phi(a_0 + a_1x + \ldots + a_nx^n) &= \Phi(a_0) + \Phi(a_1)\Phi(x) + \ldots + \Phi(a_n)\Phi(x)^n \\ &= \phi(a_0) + \phi(a_1)a + \ldots + \phi(a_n)a^n\,;\end{aligned}$$

damit sind die Werte von Φ durch die Daten ϕ und a eindeutig festgelegt. Die Existenz von Φ als Abbildung mit den obigen Werten folgt daraus, dass Polynome eindeutig ihren Koeffizientenfolgen entsprechen — es gibt keine Äquivalenzklassen und damit kein Problem mit der Wohldefiniertheit. Es bleibt zu zeigen, dass Φ ein Ringhomomorphismus ist. Wir haben $\Phi(1) = \phi(1) = 1$,

$$\begin{aligned}&\Phi(a_0 + a_1x + \ldots + a_nx^n) + \Phi(b_0 + b_1x + \ldots + b_nx^n) \\ &\quad= \big(\phi(a_0) + \phi(a_1)a + \ldots + \phi(a_n)a^n\big) + \big(\phi(b_0) + \phi(b_1)a + \ldots + \phi(b_n)a^n\big) \\ &\quad= \big(\phi(a_0) + \phi(b_0)\big) + \big(\phi(a_1) + \phi(b_1)\big)a + \ldots + \big(\phi(a_n) + \phi(b_n)\big)a^n \\ &\quad= \phi(a_0 + b_0) + \phi(a_1 + b_1)a + \ldots + \phi(a_n + b_n)a^n \\ &\quad= \Phi\big((a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n\big) \\ &\quad= \Phi\big((a_0 + a_1x + \ldots + a_nx^n) + (b_0 + b_1x + \ldots + b_nx^n)\big)\end{aligned}$$

und mit $f = \sum_{i=0}^n a_ix^i$, $g = \sum_{j=0}^m b_jx^j$:

$$\Phi(f) \cdot \Phi(g) = \Big(\sum_{i=0}^n \phi(a_i)a^i\Big) \cdot \Big(\sum_{j=0}^m \phi(b_j)a^j\Big) = \sum_{i=0}^n \sum_{j=0}^m \phi(a_i)\phi(b_j)a^{i+j}$$

(hier haben wir benutzt, dass $a\phi(b_j) = \phi(b_j)a$!)

$$= \sum_{i=0}^n \sum_{j=0}^m \phi(a_ib_j)a^{i+j} = \sum_{k=0}^{n+m} \Big(\sum_{i=0}^k \phi(a_ib_{k-i})\Big)a^k$$

(wir setzen $a_i = 0$ für $i > n$ und $b_j = 0$ für $j > m$)

$$= \sum_{k=0}^{n+m} \phi\Big(\sum_{i=0}^k a_ib_{k-i}\Big)a^k = \Phi\Big(\sum_{k=0}^{n+m} \Big(\sum_{i=0}^k a_ib_{k-i}\Big)x^k\Big) = \Phi(fg)\,.$$

□

11.3. **Definition.** Wenn in der Situation von Satz 11.2 der Homomorphismus ϕ kanonisch ist (zum Beispiel im Fall $R \subset R'$), dann heißt Φ *Auswertungsabbildung in a* oder *Einsetzungshomomorphismus*, und man schreibt suggestiv $f(a)$ für $\Phi(f)$.

Ist R' kommutativ, dann induziert ein Polynom $f \in R[x]$ also eine *Polynomfunktion* $R' \to R'$, $a \mapsto f(a)$. Gilt $f(a) = 0$, so heißt a eine *Nullstelle* von f in R'.

Für das Rechnen mit Polynomen sind folgende Begriffe hilfreich:

11.4. **Definition.** Sei R ein Ring, $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$. Ist $a_n \neq 0$, dann heißt $\deg(f) = n$ der *Grad* (*degree*) und $\operatorname{lcf}(f) = a_n$ der *Leitkoeffizient* (*leading coefficient*) des Polynoms f. Für das Nullpolynom $0 \in R[x]$ setzen wir $\deg(0) = -\infty$; das Nullpolynom hat keinen Leitkoeffizienten. Ein Polynom mit Leitkoeffizient 1 heißt *normiert*. (Das Wort „normiert“ hat in der Mathematik leider sehr viele verschiedene Bedeutungen. Im Englischen gibt es für diesen speziellen Fall ein eigenes Wort: *monic*.) Ein Polynom f heißt *konstant*, wenn $f = 0$ oder $\deg(f) = 0$, also wenn $f \in R \subset R[x]$.

11.5. **Lemma.** *Sei R ein Ring, und seien $f, g \in R[x]$ Polynome. Dann gilt:*

(1) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ *mit Gleichheit, falls* $\deg(f) \neq \deg(g)$.
(2) $\deg(fg) \leq \deg(f) + \deg(g)$ *mit Gleichheit, falls R ein Integritätsring oder eines der Polynome normiert ist. Gilt Gleichheit und $fg \neq 0$, so gilt auch* $\operatorname{lcf}(fg) = \operatorname{lcf}(f)\operatorname{lcf}(g)$.

Beweis. Ist $f = 0$ oder $g = 0$, dann sind die Aussagen klar. Sonst seien $f = \sum_{j=0}^{\infty} a_j x^j$ und $g = \sum_{j=0}^{\infty} b_j x_j$ (mit $a_j, b_j = 0$ für j groß genug). Dann ist $a_j = 0$ für $j > \deg(f)$ und $b_j = 0$ für $j > \deg(g)$, also $a_j + b_j = 0$ für $j > \max\{\deg(f), \deg(g)\}$. Das zeigt $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$. Sind die Grade verschieden, etwa $\deg(f) < \deg(g) = n$, dann ist $a_n + b_n = b_n \neq 0$, also $\deg(f+g) = \deg(g) = \max\{\deg(f), \deg(g)\}$.

In der Summe $\sum_{j=0}^{m} a_j b_{m_j}$ ist in jedem Term ein Faktor null, wenn $m > \deg(f) + \deg(g)$ ist, also ist der entsprechende Koeffizient von fg ebenfalls null. Das zeigt $\deg(fg) \leq \deg(f) + \deg(g)$. Ist $m = \deg(f) + \deg(g)$, dann ergibt sich für den entsprechenden Koeffizienten des Produkts $a_{\deg(f)} b_{\deg(g)}$. Ist R ein Integritätsring oder einer der Faktoren gleich 1, so ist dieses Produkt von null verschieden, und es gilt $\deg(fg) = \deg(f) + \deg(g)$. Umgekehrt bedeutet Gleichheit in dieser Relation genau $a_{\deg(f)} b_{\deg(g)} \neq 0$; die Formel für den Leitkoeffizienten von fg folgt. □

11.6. **Folgerung.** *Sei R ein Ring. Ist R ein Integritätsring, so ist $R[x]$ ebenfalls ein Integritätsring. Ist R ein Integritätsbereich, so gilt das auch für $R[x]$.*

Beweis. Wir haben bereits gesehen, dass $R[x]$ kommutativ ist, wenn R kommutativ ist. Es ist also nur zu zeigen, dass $R[x]$ nullteilerfrei ist, wenn das für R gilt. In diesem Fall haben wir aber die Beziehung $\deg(fg) = \deg(f) + \deg(g)$ für $f, g \in R[x]$. Sind $f, g \neq 0$, dann folgt $\deg(fg) \geq 0$, also $fg \neq 0$. □

11.7. **Folgerung.** *Sei R ein Integritätsring. Dann gilt $R[x]^\times = R^\times$, d.h., alle Einheiten sind konstant.*

Beweis. Die Inklusion „$\supset$“ ist klar. Sei umgekehrt $f \in R[x]$ invertierbar; es gebe also $g \in R[x]$ mit $fg = 1$. Dann folgt $0 = \deg(1) = \deg(f) + \deg(g)$, und das ist nur möglich, wenn $\deg(f) = \deg(g) = 0$ ist, also $f, g \in R$. Es folgt $p \in R^\times$. □

Ist R kein Integritätsring, dann gilt das nicht. In $\mathbb{Z}/4\mathbb{Z}[x]$ zum Beispiel haben wir $(1+2x)^2 = 1$, also ist $1+2x$ eine Einheit, aber nicht konstant.

Eine wichtige Eigenschaft von Polynomen ist, dass man eine Version der Division mit Rest hat („Polynomdivision“, aus der Schule bekannt).

11.8. **Satz.** *Sei R ein Ring und seien $a, b \in R[x]$ Polynome mit b normiert. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[x]$ mit $a = qb + r$ und $\deg(r) < \deg(b)$.*

Beweis. Die Existenz beweisen wir durch Induktion nach dem Grad von a. Ist $\deg(a) < \deg(b)$, dann können wir $q = 0$ und $r = a$ wählen. Ist $n = \deg(a) \geq \deg(b)$, dann sei $a' = a - \operatorname{lcf}(a)x^{\deg(a)-\deg(b)}b$. Nach Lemma 11.5 gilt $\deg(a') \leq \deg(a)$, und man sieht, dass der Koeffizient von x^n in a' gerade $a_n - a_n = 0$ ist, also gilt sogar $\deg(a') < \deg(a)$. Nach Induktionsannahme gibt es $q', r \in R[x]$ mit $a' = q'b + r$ und $\deg(r) < \deg(b)$. Mit $q = q' + \operatorname{lcf}(a)x^{\deg(a)-\deg(b)}$ folgt $a = qb + r$.

Zur Eindeutigkeit: Seien $q, q', r, r' \in R[x]$ mit $qb+r = q'b+r'$ und $\deg(r), \deg(r') < \deg(b)$. Dann folgt $(q-q')b = r' - r$, und mit Lemma 11.5 erhalten wir

$$\deg(q-q') + \deg(b) = \deg(r'-r) \leq \max\{\deg(r'), \deg(r)\} < \deg(b)\,.$$

Dies ist nur dann möglich, wenn $\deg(q-q') = -\infty$ ist, also $q = q'$ und damit auch $r = r'$. □

Aus diesem Beweis ergibt sich unmittelbar der bekannte Algorithmus für die Polynomdivision.

11.9. **Folgerung.** *Sei R ein kommutativer Ring, $f \in R[x]$ und $a \in R$. Dann gilt: a ist Nullstelle von f genau dann, wenn $x - a$ ein Teiler von f ist. Insbesondere kann ein Polynom vom Grad $n \geq 0$ über einem Integritätsbereich R höchstens n verschiedene Nullstellen in R haben.*

Beweis. In jedem Fall gibt es (eindeutige) $q, r \in R[x]$ mit $\deg(r) < \deg(x-a) = 1$, also r konstant, und $f = q(x-a) + r$. Wir wenden den Einsetzungshomomorphismus (bzgl. a) an und erhalten $f(a) = q(a)(a-a) + r = r$. Also gilt $f(a) = 0$ genau dann, wenn $r = 0$. Die zweite Aussage zeigt man leicht durch Induktion (Übung). □

Das Polynom $f = x^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[x]$ vom Grad 2 hat die vier verschiedenen Nullstellen $1, 3, 5, 7 \in \mathbb{Z}/8\mathbb{Z}$. Die Voraussetzung, dass R ein Integritätsbereich ist, ist also notwendig. (Wo geht der Beweis für dieses Beispiel schief?)

11.10. **Folgerung.** *Sei K ein Körper. Dann ist $K[x]$ ein euklidischer Ring mit der euklidischen Normfunktion $N : f \mapsto \max\{0, \deg(f) + 1\}$.*

Beweis. Es ist nur zu zeigen, dass die angegebene Funktion eine euklidische Normfunktion ist. Es ist klar, dass $N(f) = 0$ genau für $f = 0$ gilt. Seien $a, b \in K[x]$ mit $b \neq 0$. Dann ist $\beta = \mathrm{lcf}(b) \in K^\times$. Sei $b' = \beta^{-1}b$; $b' \in K[x]$ ist ein normiertes Polynom. Nach Satz 11.8 gibt es $q', r \in K[x]$ mit

$$a = q'b' + r \quad \text{und} \quad \deg(r) < \deg(b') = \deg(b)\,, \quad \text{also } N(r) < N(b)\,.$$

Wir setzen $q = \beta^{-1}q'$, dann gilt $a = qb + r$. Damit erfüllt N auch die zweite Eigenschaft einer euklidischen Normfunktion. □

Insbesondere ist $K[x]$ also ein *Hauptidealring* und damit *faktoriell*.

Auf der anderen Seite ist etwa der Ring $\mathbb{Z}[x]$ *kein* Hauptidealring. Zum Beispiel ist das Ideal $\langle 2, x\rangle_{\mathbb{Z}[x]}$ kein Hauptideal. (Wäre es eines, etwa erzeugt von $a \in \mathbb{Z}[x]$, dann müsste a konstant sein, denn a ist ein Teiler von 2. Damit a ein Teiler von x ist, müsste $a = \pm 1$ sein, aber ± 1 sind nicht im Ideal enthalten.) Allerdings ist $\mathbb{Z}[x]$ immer noch faktoriell. Das ist ein Spezialfall des nächsten Satzes. Dafür brauchen wir aber noch ein wenig Vorbereitung.

11.11. **Definition.** Sei R ein faktorieller Ring und $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ ein Polynom. Dann heißt $\mathrm{cont}(f) = \mathrm{ggT}(a_0, a_1, \ldots, a_n)$ der *Inhalt* (engl. *content*) von f (der Inhalt ist i.a. nur bis auf Assoziierte eindeutig bestimmt). Hat f den Inhalt 1, dann heißt f *primitiv*. Offenbar kann man jedes Polynom f schreiben als ein Produkt aus seinem Inhalt $\mathrm{cont}(f)$ und einem primitiven Polynom $\mathrm{pp}(f)$ (*primitive part*). Der Vollständigkeit halber setzen wir $\mathrm{pp}(0) = 1$.

11.12. **Lemma.** *Sei R ein faktorieller Ring und K der Quotientenkörper von R. Wir betrachten $R[x]$ als Unterring von $K[x]$. Sei $0 \neq f \in K[x]$. Dann gibt es $\mathrm{cont}(f) \in K^\times$ und ein primitives Polynom $\mathrm{pp}(f) \in R[x]$ mit $f = \mathrm{cont}(f)\,\mathrm{pp}(f)$. Der Inhalt $\mathrm{cont}(f)$ (und damit auch $\mathrm{pp}(f)$) ist bis auf Multiplikation mit einer Einheit von R eindeutig bestimmt. Es gilt $f \in R[x]$ genau dann, wenn $\mathrm{cont}(f) \in R$.*

Beweis. Sei $f = a_0 + a_1x + \ldots + a_nx^n$ mit $a_j = b_j/c_j$ und $b_j, c_j \in R$, $c_j \neq 0$. Da R faktoriell ist, gibt es einen gemeinsamen Nenner $c = \mathrm{kgV}(c_0, c_1, \ldots, c_n)$, so dass $cf \in R[x]$. Wir setzen $\mathrm{cont}(f) = c^{-1}\,\mathrm{cont}(cf)$ und $\mathrm{pp}(f) = \mathrm{pp}(cf)$. (Dies erweitert die für $f \in R[x]$ definierten Begriffe, da wir für $f \in R[x]$ den gemeinsamen Nenner $c = 1$ nehmen können.)

Gilt $\alpha f = \alpha' f'$ mit $\alpha, \alpha' \in K^\times$ und primitiven Polynomen $f, f' \in R[x]$, dann können wir (nach Multiplikation mit einem gemeinsamen Nenner) annehmen, dass $\alpha, \alpha' \in R$. Es folgt $\alpha \sim \mathrm{cont}(\alpha f) \sim \mathrm{cont}(\alpha' f') \sim \alpha'$, also $\alpha/\alpha' \in R^\times$.

Ist $\mathrm{cont}(f) \in R$, so auch $f = \mathrm{cont}(f)\,\mathrm{pp}(f)$. Umgekehrt gilt natürlich (nach Definition) $\mathrm{cont}(f) \in R$ für $f \in R[x]$. □

11.13. **Lemma von Gauß.** *Sei R ein faktorieller Ring, und seien $f, g \in R[x]$ primitive Polynome. Dann ist fg ebenfalls primitiv.*

Wenn wir mit $\sim$ Gleichheit bis auf einen Faktor in $R^\times$ bezeichnen, folgt daraus leicht für beliebige Polynome $0 \neq f, g \in R[x]$:

$$\mathrm{cont}(fg) \sim \mathrm{cont}(f)\,\mathrm{cont}(g) \qquad \text{und} \qquad \mathrm{pp}(fg) \sim \mathrm{pp}(f)\,\mathrm{pp}(g)$$

(Übung).

Beweis. Nach Definition 11.11 ist fg genau dann primitiv, wenn es kein Primelement π von R gibt, das alle Koeffizienten von fg teilt. Sei also π ein Primelement von R. Wir schreiben a_j für die Koeffizienten von f und b_j für die Koeffizienten von g. Da f und g beide primitiv sind, gibt es $m, n \in \mathbb{Z}_{\geq 0}$, so dass $\pi \nmid a_m$, aber $\pi \mid a_j$ für alle $j > m$, und $\pi \nmid b_n$, aber $\pi \mid b_j$ für alle $j > n$. Wir betrachten den $(m+n)$-ten Koeffizienten von fg. Er ist gegeben durch

$$(a_0 b_{m+n} + a_1 b_{m+n-1} + \ldots + a_{n-1} b_{m+1}) + a_m b_n + (a_{n+1} b_{m-1} + \ldots + a_{m+n-1} b_1 + a_{m+n} b_0)\,.$$

In der ersten Teilsumme sind alle b_j durch π teilbar, in der letzten Teilsumme sind alle a_j durch π teilbar, also sind beide Teilsummen durch π teilbar. Auf der anderen Seite ist aber der mittlere Term $a_m b_n$ nicht durch π teilbar. Also ist auch die gesamte Summe nicht durch π teilbar, und wir sehen, dass π nicht alle Koeffizienten von fg teilt. □

Wir wollen jetzt beweisen, dass mit R auch $R[x]$ wieder faktoriell ist. Die Idee dazu kommt aus den vorigen beiden Lemmata, die es uns erlauben, die Behauptung darauf zurückzuführen, dass sowohl R als auch $K[x]$ faktoriell sind. Das wollen wir zuerst noch präzisieren.

11.14. **Lemma.** *Sei R ein faktorieller Ring mit Quotientenkörper K. Wir bezeichnen die Teilbarkeitsrelation in R, $K[x]$ und $R[x]$ mit $|_R$, $|_{K[x]}$ und $|_{R[x]}$. Für Polynome $f, g \in R[x]$ gilt dann*

$$f \mid_{R[x]} g \iff \operatorname{cont}(f) \mid_R \operatorname{cont}(g) \quad \textit{und} \quad \operatorname{pp}(f) \mid_{K[x]} \operatorname{pp}(g)\,.$$

Beweis. Es bezeichne $\sim$ Gleichheit bis auf einen Faktor in $R^\times$.

Sei $g = fh$ in $R[x]$. Aus dem Lemma von Gauß 11.13 folgt $\operatorname{cont}(g) = \operatorname{cont}(fh) \sim \operatorname{cont}(f)\operatorname{cont}(h)$, also $\operatorname{cont}(f) \mid_R \operatorname{cont}(g)$, und $\operatorname{pp}(g) \sim \operatorname{pp}(f)\operatorname{pp}(h)$, also $\operatorname{pp}(f) \mid_{R[x]} \operatorname{pp}(g)$ und damit auch $\operatorname{pp}(f) \mid_{K[x]} \operatorname{pp}(g)$.

Gelte jetzt umgekehrt $\operatorname{cont}(f) \mid_R \operatorname{cont}(g)$ und $\operatorname{pp}(f) \mid_{K[x]} \operatorname{pp}(g)$. Dann gibt es $h \in K[x]$ mit $\operatorname{pp}(g) = \operatorname{pp}(f)h$. Es folgt $\operatorname{cont}(h) \sim \operatorname{cont}(\operatorname{pp}(f)h) \sim \operatorname{cont}(\operatorname{pp}(g)) \sim 1$, also ist $h \in R[x]$ (sogar primitiv), und wir haben $\operatorname{pp}(f) \mid_{R[x]} \operatorname{pp}(g)$. Es folgt $f = \operatorname{cont}(f)\operatorname{pp}(f) \mid_{R[x]} \operatorname{cont}(g)\operatorname{pp}(g) = g$. □

Daraus können wir schon einmal ableiten, was die irreduziblen Elemente von $R[x]$ sind.

11.15. **Folgerung.** *Sei R ein faktorieller Ring mit Quotientenkörper K, und sei $f \in R[x]$. Dann ist f irreduzibel genau dann, wenn entweder $f \in R$ ein Primelement ist oder f nicht konstant, primitiv und in $K[x]$ irreduzibel ist.*

Beweis. Aus Lemma 11.14 folgt, dass f genau dann irreduzibel ist, wenn entweder $\operatorname{cont}(f)$ in R irreduzibel und $\operatorname{pp}(f) \in K[x]^\times \cap R[x] = R^\times$ ist, oder wenn $\operatorname{cont}(f) \in R^\times$ und $\operatorname{pp}(f)$ in $K[x]$ irreduzibel ist. Im ersten Fall können wir $\operatorname{pp}(f) = 1$ und $\operatorname{cont}(f) = f$ wählen, im zweiten Fall entsprechend $\operatorname{pp}(f) = f$ und $\operatorname{cont}(f) = 1$. □

Jetzt können wir den Satz beweisen.

11.16. **Satz.** *Sei R ein faktorieller Ring. Das ist $R[x]$ ebenfalls faktoriell.*

Beweis. Wir müssen zwei Dinge zeigen (siehe Satz 5.10):

(1) Jedes irreduzible Element von $R[x]$ ist prim.
(2) Für jede Folge $(f_n)_{n\geq 0}$ von Elementen von $R[x]$ mit $f_{n+1} \mid f_n$ für alle $n \geq 0$ gibt es ein $N \geq 0$, so dass $f_n \sim f_N$ für alle $n \geq N$.

Wir beginnen mit der zweiten Eigenschaft. Aus Lemma 11.14 folgt, dass eine „Teilerkette“ $(f_n)_{n\geq 0}$ in $R[x]$ Teilerketten $\big(\mathrm{cont}(f_n)\big)_{n\geq 0}$ in R und $\big(\mathrm{pp}(f_n)\big)_{n\geq 0}$ in $K[x]$ ergibt. Sowohl R als auch $K[x]$ sind faktoriell, also gibt es $N \geq 0$ mit $\mathrm{cont}(f_n) \sim_R \mathrm{cont}(f_N)$ und $\mathrm{pp}(f_n) \sim_{K[x]} \mathrm{pp}(f_N)$ für alle $n \geq N$. Die Polynome $\mathrm{pp}(f_n)$ und $\mathrm{pp}(f_N)$ unterscheiden sich also um einen konstanten Faktor; da beide Polynome primitiv sind, muss der Faktor in $R^\times$ sein. Es folgt

$$f_n = \mathrm{cont}(f_n)\,\mathrm{pp}(f_n) \sim_{R[x]} \mathrm{cont}(f_N)\,\mathrm{pp}(f_N) = f_N\,,$$

und die zweite Eigenschaft ist bewiesen.

Wir zeigen jetzt die erste Eigenschaft. Nach Folgerung 11.15 sind die irreduziblen Elemente von $R[x]$ entweder Primelemente von $R \subset R[x]$ oder nicht konstante primitive Polynome $f \in R[x]$, die in $K[x]$ irreduzibel sind. Wir zeigen, dass diese Elemente auch prim in $R[x]$ sind. Für Primelemente $p \in R$ ist das klar:

$$\begin{aligned} p \mid fg &\implies p \mid \mathrm{cont}(fg) \sim \mathrm{cont}(f)\,\mathrm{cont}(g) \\ &\implies p \mid \mathrm{cont}(f) \mid f \quad \text{oder} \quad p \mid \mathrm{cont}(g) \mid g \end{aligned}$$

Sei jetzt also $f \in R[x]$ ein nicht konstantes, primitives Polynom, das in $K[x]$ irreduzibel ist, und seien $g, h \in R[x]$ mit $f \mid_{R[x]} gh$. Dann folgt $f = \mathrm{pp}(f) \mid_{K[x]} \mathrm{pp}(gh) \sim \mathrm{pp}(g)\,\mathrm{pp}(h)$, also (da $K[x]$ faktoriell und f in $K[x]$ irreduzibel, also prim ist) $f \mid_{K[x]} \mathrm{pp}(g)$ oder $f \mid_{K[x]} \mathrm{pp}(h)$. Da $\mathrm{cont}(f) = 1$ ein Teiler von $\mathrm{cont}(g)$ und von $\mathrm{cont}(h)$ ist, folgt $f \mid_{R[x]} g$ oder $f \mid_{R[x]} h$ wie gewünscht. □

11.17. **Folgerung.** *Sei R ein faktorieller Ring oder ein Körper. Dann ist der Polynomring $R[x_1, x_2, \ldots, x_n]$ in n Unbestimmten über R für jedes $n \geq 0$ faktoriell.*

Beweis. Triviale Induktion nach n unter Verwendung von Satz 11.16 und von $R[x_1, \ldots, x_n, x_{n+1}] = \big(R[x_1, \ldots, x_n]\big)[x_{n+1}]$. □

12. Irreduzibilitätskriterien für Polynome

Sei R ein faktorieller Ring mit Quotientenkörper K. (Das Standardbeispiel ist $R = \mathbb{Z}$ und $K = \mathbb{Q}$.) In diesem Abschnitt geht es darum, wie man zeigen kann, dass ein gegebenes Polynom aus $K[x]$ irreduzibel ist. Eine erste Aussage in dieser Richtung setzt Irreduzibilität in $K[x]$ und in $R[x]$ zueinander in Beziehung.

12.1. **Folgerung.** *Ein Polynom $0 \neq f \in K[x]$ ist irreduzibel genau dann, wenn $\mathrm{pp}(f)$ in $R[x]$ irreduzibel ist.*

Beweis. Das folgt aus Folgerung 11.15: In $K[x]$ sind alle Konstanten $\neq 0$ Einheiten, also ist f in $K[x]$ irreduzibel genau dann, wenn $\mathrm{pp}(f)$ in $K[x]$ irreduzibel ist. Das wiederum ist dazu äquivalent, dass $\mathrm{pp}(f)$ in $R[x]$ irreduzibel ist. (Beachte, dass die Äquivalenz auch für f konstant gilt: In diesem Fall ist f eine Einheit in $K[x]$ und $\mathrm{pp}(f) = 1$ eine Einheit in $R[x]$; beide sind daher nicht irreduzibel.) □

Für Polynome von niedrigem Grad haben wir folgendes Kriterium.

12.2. **Lemma.** *Sei (nur für dieses Lemma) K ein beliebiger Körper, sei $f \in K[x]$ nicht konstant. Dann ist f genau dann irreduzibel, wenn es kein normiertes Polynom $g \in K[x]$ gibt mit $1 \leq \deg(g) \leq \deg(f)/2$ und $g \mid f$. Insbesondere gilt:*

(1) *Ist $\deg(f) = 1$, dann ist f irreduzibel.*
(2) *Ist $\deg(f) \in \{2, 3\}$, dann ist f irreduzibel genau dann, wenn f keine Nullstelle in K hat.*

Beweis. f ist reduzibel genau dann, wenn $f = gh$ mit $g, h \in K[x]$ beide nicht konstant. Es folgt $\deg(g), \deg(h) \geq 1$ und $\deg(g) + \deg(h) = \deg(f)$. Wir können ohne Einschränkung annehmen, dass $\deg(g) \leq \deg(h)$; dann folgt $\deg(g) \leq \deg(f)/2$. Der Leitkoeffizient von g ist eine Einheit; mit g ist also auch das normierte Polynom $\operatorname{lcf}(g)^{-1}g$ vom selben Grad ein Teiler von f.

Gilt $\deg(f) = 1$, dann ist das Kriterium trivialerweise erfüllt. Im Fall $\deg(f) \in \{2, 3\}$ darf es keinen normierten Teiler vom Grad 1 geben. Das Polynom $x - a$ ist aber genau dann ein Teiler von f, wenn a eine Nullstelle von f ist (siehe Folgerung 11.9). □

12.3. **Beispiele.** Das Polynom $f = x^2 + x + 1$ ist in $\mathbb{Q}[x]$ irreduzibel, weil f keine Nullstelle in $\mathbb{Q}$ hat — f hat nicht einmal eine Nullstelle in $\mathbb{R}$, denn $f(\xi) = \left(\xi + \frac{1}{2}\right)^2 + \frac{3}{4}$ ist für $\xi \in \mathbb{R}$ stets positiv. Man sieht, dass x^2+x+1 auch in $\mathbb{R}[x]$ irreduzibel ist. Es gibt auch Polynome, die in $\mathbb{Q}[x]$ irreduzibel sind, aber in $\mathbb{R}[x]$ reduzibel, zum Beispiel $x^2 - 2$. Auf der anderen Seite ist kein Polynom von ungeradem Grad > 1 in $\mathbb{R}[x]$ irreduzibel, denn es hat stets eine reelle Nullstelle (nach dem Zwischenwertsatz).

Der *Fundamentalsatz der Algebra* besagt, dass jedes nicht konstante Polynom in $\mathbb{C}[x]$ eine Nullstelle in $\mathbb{C}$ hat. Daraus folgt, dass die einzigen normierten irreduziblen Polynome in $\mathbb{C}[x]$ die der Form $x - \alpha$ sind. Daraus folgt auch, dass ein Polynom in $\mathbb{R}[x]$ reduzibel sein muss, sobald sein Grad größer als 2 ist: Sei $f \in \mathbb{R}[x]$ mit $\deg(f) \geq 3$. Dann hat f eine Nullstelle $\alpha \in \mathbb{C}$. Ist α sogar reell, dann ist f offensichtlich reduzibel. Ist α nicht reell, dann ist $\bar{\alpha}$ eine weitere Nullstelle von f, und f ist durch $(x-\alpha)(x-\bar{\alpha}) = x^2 - 2\operatorname{Re}\alpha\, x + |\alpha|^2 \in \mathbb{R}[x]$ teilbar. Wegen $\deg(f) \geq 3$ ist dies ein echter Teiler, also ist f reduzibel. Insgesamt sieht man, dass die normierten irreduziblen Polynome in $\mathbb{R}[x]$ genau die Polynome $x - a$ mit $a \in \mathbb{R}$ und die Polynome $x^2 + bx + c$ mit $b^2 < 4c$ sind (letztere sind die normierten quadratischen Polynome ohne reelle Nullstelle).

Wie kann man nun feststellen, ob ein Polynom in $\mathbb{Q}[x]$ eine Nullstelle in $\mathbb{Q}$ hat?

12.4. **Lemma.** *Sei $f \in R[x]$ primitiv und nicht konstant, $f = a_0 + a_1 x + \ldots + a_n x^n$ mit $a_n \neq 0$. Ist $\alpha \in K$ eine Nullstelle von f, dann kann man α schreiben als $\alpha = r/s$ mit $r, s \in R$, $r \mid a_0$, $s \mid a_n$.*

Beweis. Sei $\alpha = r/s$ mit $r, s \in R$, $r \perp s$ (da R faktoriell ist, kann man den Bruch stets kürzen). Aus $x - \alpha \mid_{K[x]} f$ folgt $\operatorname{pp}(x - \alpha) \mid_{R[x]} \operatorname{pp}(f) = f$, und es ist $\operatorname{pp}(x - \alpha) = sx - r$. Daraus folgt (durch Betrachten der Leitkoeffizienten und der Koeffizienten von x^0), dass $s \mid a_n$ und $r \mid a_0$. □

12.5. **Beispiel.** Das Polynom $f = x^3 + \frac{1}{2}x^2 - x + \frac{3}{2} \in \mathbb{Q}[x]$ ist irreduzibel: Es ist $\mathrm{pp}(f) = 2x^3 + x^2 - 2x + 3 \in \mathbb{Z}[x]$. Ist $r/s \in \mathbb{Q}$ eine Nullstelle von f in gekürzter Form, dann gilt $r \mid 3$ und $s \mid 2$. Es gibt also die Möglichkeiten ± 1, ± 3, $\pm\frac{1}{2}$ und $\pm\frac{3}{2}$, und man rechnet nach, dass keine dieser acht Zahlen eine Nullstelle von f ist. Damit ist gezeigt, dass f keine Nullstelle in $\mathbb{Q}$ hat, und f muss irreduzibel sein.

12.6. **Beispiel.** Demgegenüber hat $x^4 + 4 \in \mathbb{Q}[x]$ ebenfalls keine Nullstelle in $\mathbb{Q}$ (denn der Wert ist stets positiv), ist aber reduzibel:

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

Für Polynome vom Grad ≥ 4 braucht man also andere Methoden.

Eine häufig erfolgreiche Methode ist das folgende *Reduktionskriterium*. Wenn $p \in R$ ein Primelement ist, dann ist R/Rp ein Körper (denn Rp ist ein maximales Ideal), und wir erhalten einen kanonischen Homomorphismus $R[x] \to R/Rp[x]$ (Einsetzungshomomorphismus mit $R \to R/pR$ und $x \mapsto x$). Um ihn anzuwenden, muss man die Koeffizienten „modulo p reduzieren“.

12.7. **Satz (Reduktionskriterium).** *Sei $p \in R$ prim und $f \in R[x]$ primitiv mit $p \nmid \mathrm{lcf}(f)$. Ist das Bild von f in $R/Rp[x]$ irreduzibel, so ist f in $R[x]$ irreduzibel.*

Beweis. Wir schreiben $\bar{f}$ für das Bild von f in $R/Rp[x]$; analog für andere Polynome. Ist $f = gh$ mit $1 \leq \deg(g) < \deg(f)$, dann folgt $\bar{f} = \bar{g}\,\bar{h}$ in $R/Rp[x]$. Aus $p \nmid \mathrm{lcf}(f)$ folgt $p \nmid \mathrm{lcf}(g)$, $p \nmid \mathrm{lcf}(h)$, und damit $\deg(\bar{f}) = \deg(f)$, $\deg(\bar{g}) = \deg(g)$, $\deg(\bar{h}) = \deg(h)$. Wir erhalten also eine echte Zerlegung von $\bar{f}$, im Widerspruch dazu, dass $\bar{f}$ irreduzibel ist. Also kann f auch nicht reduzibel sein. □

12.8. **Beispiel.** Wir betrachten $R = \mathbb{Z}$ und $p = 2$, dann ist $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ der Körper mit zwei Elementen. Die irreduziblen Polynome vom Grad höchstens 4 in $\mathbb{F}_2[x]$ sind (alle sind normiert, da 1 der einzig mögliche Leitkoeffizient ist)

$$x, \quad x+1, \qquad x^2+x+1, \qquad x^3+x+1, \quad x^3+x^2+1$$
$$x^4+x+1, \quad x^4+x^3+1, \quad x^4+x^3+x^2+x+1\,.$$

(Um diese Liste zu bekommen, beginnt man mit den (normierten) irreduziblen Polynomen vom Grad 1; das sind alle der Form $x - a$, hier mit $a \in \{0, 1\} = \mathbb{F}_2$. Dann bildet man alle Produkte von zwei solchen Polynomen — hier x^2, $x(x+1) = x^2 + x$, $(x+1)^2 = x^2 + 1$ — das sind die *reduziblen* Polynome vom Grad 2. Die verbleibenden sind dann die irreduziblen Polynome vom Grad 2, das ist hier nur $x^2 + x + 1$. Dann bildet man alle möglichen Produkte vom Grad 3 aus den irreduziblen Polynomen vom Grad ≤ 2, um die reduziblen Polynome vom Grad 3 zu finden, usw. Für Polynome von kleinem Grad kann man das natürlich unter Verwendung von Lemma 12.2 abkürzen.)

Daraus folgt zum Beispiel, dass $3x^4 + 2x^3 - 4x^2 - 5x + 7 \in \mathbb{Z}[x]$ irreduzibel ist, denn die Reduktion modulo 2 ist das irreduzible Polynom $x^4 + x + 1$.

12.9. **Beispiel.** Es gibt aber auch Polynome, die irreduzibel sind, aber gleichzeitig die Eigenschaft haben, dass sie modulo jeder Primzahl reduzibel werden. Ein Beispiel dafür ist $x^4 - 10x^2 + 1$. Das Polynom ist irreduzibel, weil es keine Nullstelle in $\mathbb{Q}$ hat (nur ± 1 kommen in Frage) und es keine Zerlegung

$$x^4 - 10x^2 + 1 = (x^2 + ax \pm 1)(x^2 + bx \pm 1)$$

gibt. Für den Nachweis, dass man stets eine Zerlegung mod p hat, braucht man die Theorie der quadratischen Reste (siehe später in diesem Vorlesungszyklus). Zum Beispiel gilt:

$$\begin{aligned}
x^4 - 10x^2 + 1 &\equiv (x+1)^4 \bmod 2\\
x^4 - 10x^2 + 1 &\equiv (x^2+1)^2 \bmod 3\\
x^4 - 10x^2 + 1 &\equiv (x^2+2)(x^2-2) \bmod 5\\
x^4 - 10x^2 + 1 &\equiv (x^2+x-1)(x^2-x-1) \bmod 7\\
&\vdots \qquad\quad \vdots \qquad\qquad \vdots\\
x^4 - 10x^2 + 1 &\equiv (x+2)(x+11)(x-11)(x-2) \bmod 23\\
&\vdots \qquad\quad \vdots \qquad\qquad \vdots
\end{aligned}$$

Man kann das Reduktionskriterium verfeinern, indem man die Faktorisierungen in irreduzible Faktoren modulo verschiedener Primzahlen vergleicht. Für das Polynom $f = x^4 - x^3 + 3x^2 + 2x - 1 \in \mathbb{Z}[x]$ gilt zum Beispiel

$$f \equiv (x+1)(x^3+x+1) \bmod 2 \qquad \text{und} \qquad f \equiv (x^2+1)(x^2-x-1) \bmod 3\,,$$

und die angegebenen Faktoren sind irreduzibel in $\mathbb{F}_2[x]$ bzw. $\mathbb{F}_3[x]$. Ein Teiler g von f in $\mathbb{Z}[x]$ müsste sich mod 2 und mod 3 jeweils auf einen der Faktoren reduzieren (allgemein: auf ein Produkt irreduzibler Faktoren), was $\deg(g) \in \{1,3\} \cap \{2\} = \emptyset$ zur Folge hätte. Also kann es keinen nichttrivialen Teiler geben, und f ist irreduzibel.

Ein weiteres wichtiges Kriterium ist das *Eisenstein-Kriterium*.

12.10. **Satz (Eisenstein-Kriterium).** *Sei $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ primitiv und nicht konstant und $p \in R$ ein Primelement mit $p \nmid a_n$, $p \mid a_j$ für $0 \le j < n$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.*

Beweis. Wir betrachten wieder die Reduktion $\bar f$ von f modulo p. Die Voraussetzungen implizieren, dass $\bar f = ux^n$ ist mit einem Element $0 \neq u \in R/Rp$. Ist $f = gh$ eine echte Zerlegung, dann folgt $\bar g = u'x^m$, $\bar h = u''x^{n-m}$ mit $0 \neq u', u'' \in R/Rp$ und $1 \le m \le n-1$. (Hier benutzen wir, dass R/Rp ein Integritätsbereich ist: Rp ist ein Primideal, vergleiche Proposition 7.21.) Dann müssen die konstanten Terme von g und h durch p teilbar sein: $p \mid g(0)$, $p \mid h(0)$, woraus folgt $p^2 \mid g(0)h(0) = f(0) = a_0$, ein Widerspruch zur Voraussetzung. Also kann f keine echte Zerlegung haben. □

12.11. **Beispiele.** Für jedes $n \ge 2$ ist das Polynom $x^n + 6x + 3$ in $\mathbb{Z}[x]$ irreduzibel, denn man kann das Eisenstein-Kriterium mit $p = 3$ anwenden.

Manchmal muss man einen kleinen Trick anwenden: Ist $a \in R$, dann haben wir den Einsetzungshomomorphismus $R[x] \to R[x]$, $f \mapsto f(x+a)$, der ein Automorphismus von $R[x]$ ist ($f \mapsto f(x-a)$ ist der inverse Homomorphismus). Daher gilt, dass f irreduzibel ist genau dann, wenn $f(x+a)$ irreduzibel ist. Zum Beispiel ist $f = x^4 + 1 \in \mathbb{Z}[x]$ irreduzibel, denn $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ ist irreduzibel nach Eisenstein mit $p = 2$.

Ähnlich sieht man, dass für eine Primzahl p das Polynom $f = 1 + x + \ldots + x^{p-1}$ irreduzibel ist: Es gilt $f_p = (x^p - 1)/(x - 1)$ (im Quotientenkörper von $\mathbb{Q}[x]$), also ist

$$f_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{j=1}^{p} \binom{p}{j} x^{j-1}\,.$$

Die Binomialkoeffizienten $\binom{p}{j}$ sind für $1 \leq j < p$ durch p teilbar (denn p teilt den Zähler $p!$, aber nicht den Nenner $j!(p-j)!$), und der konstante Term ist $\binom{p}{1} = p$, also ist das Eisenstein-Kriterium mit der Primzahl p anwendbar.

Ist n keine Primzahl, dann ist $f_n = 1 + x + \ldots + x^{n-1}$ nicht irreduzibel, denn für $m \mid n$ gilt $f_m \mid f_n$.

Ein weiteres Beispiel ist $f = x^n + y^n - 1 \in \mathbb{Q}[x, y]$ mit $n \geq 1$. Hier ist $R = \mathbb{Q}[x]$; wir betrachten also f als Polynom $y^n + (x^n - 1)$ in y mit Koeffizienten aus R. Das Element $p = x - 1$ ist ein Primelement von R, das alle Koeffizienten von f bis auf den Leitkoeffizienten teilt, und es gilt $p^2 = (x-1)^2 \nmid x^n - 1$ (denn $(x^n - 1)/(x - 1) = x^{n-1} + \ldots + x + 1$ hat den Wert $n \neq 0$ an der Stelle 1). Nach dem Eisenstein-Kriterium ist f also irreduzibel.

Zum Abschluss werden wir noch ein Kriterium herleiten, das es uns erlaubt zu entscheiden, ob ein Polynom über einem Körper *quadratfrei* ist, also keine Primfaktoren mehrfach enthält. Dazu definieren wir die Ableitung eines Polynoms. Wir können natürlich keine Grenzwerte verwenden; deswegen nehmen wir einfach die üblichen Formeln.

12.12. **Definition.** Sei R ein kommutativer Ring und $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$. Die *Ableitung* von f ist

$$f' = a_1 + 2a_2 x + \ldots + (n-1)a_n x^{n-1} = \sum_{j=1}^{n} j a_j x^{j-1} .$$

12.13. **Lemma.** *Sei R ein kommutativer Ring. Dann gilt für $a \in R$, $f, g \in R[x]$:*

(1) $a' = 0$.
(2) $(af)' = af'$ *und* $(f+g)' = f' + g'$.
(3) $(fg)' = f'g + fg'$.
(4) $\deg(f') \leq \deg(f) - 1$ *mit Gleichheit wenn* $\deg(f) \cdot 1_R \neq 0$ *und kein Nullteiler in R ist, also insbesondere dann, wenn f nicht konstant und R in einem Körper der Charakteristik* 0 *enthalten ist.*

Ein Körper K hat *Charakteristik 0*, wenn für alle $n \in \mathbb{Z}_{>0}$ gilt $n \cdot 1_K \neq 0$. Das ist äquivalent dazu, dass $\mathbb{Q}$ in K enthalten ist.

Beweis. Die ersten drei Punkte rechnet man leicht nach. Die Ungleichung ist klar; ist $\deg(f) = n$ und $\operatorname{lcf}(f) = a_n$, dann gilt $\deg(f') = n - 1$ genau dann, wenn $na_n = (n \cdot 1_R)a_n \neq 0$ ist; das ist sicher dann erfüllt, wenn $n \cdot 1_R$ nicht null und kein Nullteiler ist. Ist f nicht konstant, dann ist $\deg(f) > 0$; in einem Körper der Charakteristik 0 ist $n \cdot 1$ nur dann ein Nullteiler, wenn $n = 0$ ist. □

Jetzt können wir das Kriterium formulieren. Es ist analog zu der aus der Analysis bekannten Tatsache, dass eine (hinreichend glatte) Funktion genau dann eine mehrfache Nullstelle in einem Punkt hat, wenn sowohl sie selbst als auch ihre Ableitung dort verschwinden.

12.14. **Proposition.** *Sei K ein Körper der Charakteristik 0. Dann ist $f \in K[x]$ quadratfrei genau dann, wenn f und f' teilerfremd sind.*

Beweis. Eine Richtung ist leicht: Ist f nicht quadratfrei, also etwa $f = g^2h$ mit $\deg(g) > 0$, dann ist $f' = g(2g'h + gh')$, also ist g ein Teiler sowohl von f als auch von f'.

Umgekehrt nehmen wir an, es gebe ein irreduzibles Polynom $p \in K[x]$ mit $p \mid f$ und $p \mid f'$. Dann ist $f = ph$, also $f' = p'h + ph'$, und es folgt $p \mid p'h$. Da p ein Primelement in $K[x]$ ist, muss dann $p \mid p'$ oder $p \mid h$ gelten. Da $p' \neq 0$ (denn p ist nicht konstant, also ist $\deg(p') = \deg(p) - 1 \geq 0$ — hier verwenden wir, dass K Charakteristik 0 hat) und $\deg(p') < \deg(p)$, kann p kein Teiler von p' sein. Es folgt $p \mid h$ und damit $p^2 \mid f$. □

12.15. **Beispiele.** Ist K ein Körper der Charakteristik 0, dann ist für jedes $n \geq 1$ das Polynom $f = x^n - 1 \in K[x]$ quadratfrei, denn $f' = nx^{n-1}$ ist offensichtlich teilerfremd zu f.

Sei p Primzahl und $K = \mathbb{F}_p(t)$ der Quotientenkörper von $\mathbb{F}_p[t]$. Dann ist das Polynom $f = x^p - t \in K[x]$ irreduzibel (Eisenstein-Kriterium mit dem Primelement t von $\mathbb{F}_p[t]$), aber $f' = px^{p-1} = 0$. Die Voraussetzung, dass K Charakteristik 0 hat, ist also wichtig.

Wenn wir den Körper $L = \mathbb{F}_p(u)$ betrachten, in den wir K einbetten können, indem wir t auf u^p abbilden (der Einsetzungshomomorphismus $\mathbb{F}_p[t] \to L$, der durch $t \mapsto u^p$ gegeben ist, setzt sich auf den Quotientenkörper K von $\mathbb{F}_p[t]$ fort), dann gilt allerdings $f = x^p - u^p = (x - u)^p$ in $L[x]$; über dem größeren Körper ist f also nicht mehr quadratfrei. Tatsächlich gilt das Kriterium in Proposition 12.14 für beliebige Körper, wenn man „quadratfrei“ durch „quadratfrei über jedem Erweiterungskörper“ ersetzt.

13. Normalform für Matrizen über Hauptidealringen

In der Linearen Algebra haben Sie folgenden wichtigen Satz kennengelernt:

13.1. **Satz.** *Sei K ein Körper, $A \in \mathrm{Mat}_{m\times n}(K)$ eine $m \times n$-Matrix mit Einträgen in K. Dann gibt es invertierbare Matrizen $P \in \mathrm{GL}_m(K)$ und $Q \in \mathrm{GL}_n(K)$, so dass $PAQ = \mathrm{diag}_{m,n}(\underbrace{1, \ldots, 1}_{r})$ die Form*

$$\left(\begin{array}{cccc|ccc} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right) = \left(\begin{array}{c|c} I_r & 0_{r\times(n-r)} \\ \hline 0_{(m-r)\times r} & 0_{(m-r)\times(n-r)} \end{array}\right)$$

hat. Dabei ist r der Rang von A.

Allgemeiner sei $\mathrm{diag}_{m,n}(d_1, d_2, \ldots, d_r)$ (mit $r \leq \min\{m, n\}$) die $m \times n$-Matrix (a_{ij}) mit $a_{ij} = 0$ für $i \neq j$, $a_{ii} = d_i$ für $1 \leq i \leq r$ und $a_{ii} = 0$ für $i > r$.

Satz 13.1 ist äquivalent zu der Aussage, dass man eine beliebige Matrix über K durch elementare Zeilen- und Spaltenumformungen auf die angegebene Diagonalform bringen kann. Wir wollen jetzt das entsprechende Problem studieren, wenn

man K durch einen Hauptidealring ersetzt. Das Ergebnis wird es uns dann erlauben, zum Beispiel den *Klassifikationssatz für endlich erzeugte abelsche Gruppen* zu beweisen. Auch den Satz über die Jordan-Normalform kann man daraus ableiten.

Der Vollständigkeit halber beginnen wir mit einer Definition.

13.2. **Definition.** Sei R ein kommutativer Ring, $m, n \in \mathbb{Z}_{\geq 0}$. Wir bezeichnen die Menge der $m \times n$-Matrizen mit Einträgen in R mit $\mathrm{Mat}_{m\times n}(R)$. Im Fall $m = n$ schreiben wir auch $\mathrm{Mat}_n(R)$; dies ist in natürlicher Weise ein Ring (mit Matrizenaddition und -multiplikation).

Wie über einem Körper haben wir die *Determinante* $\det : \mathrm{Mat}_n(R) \to R$; sie ist multiplikativ. Eine Matrix $A \in \mathrm{Mat}_n(R)$ ist invertierbar genau dann, wenn $\det(A) \in R^\times$ ist. Die Gruppe der invertierbaren $n \times n$-Matrizen über R wird mit $\mathrm{GL}_n(R)$ bezeichnet.

Zwei Matrizen $A, B \in \mathrm{Mat}_{m\times n}(R)$ heißen *äquivalent*, wenn es invertierbare Matrizen $P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ gibt mit $B = PAQ$.

Wir wollen nun folgendes Resultat beweisen:

13.3. **Satz und Definition.** *Sei R ein Hauptidealring, seien $m, n \geq 0$, und sei $A \in \mathrm{Mat}_{m\times n}(R)$. Dann gibt es $r \in \mathbb{Z}_{\geq 0}$ und Elemente $d_1, d_2, \ldots, d_r \in R$ mit $d_j \mid d_{j+1}$ für $1 \leq j < r$ und $d_r \neq 0$, so dass A zu $\mathrm{diag}_{m,n}(d_1, d_2, \ldots, d_r)$ äquivalent ist.*

Die Elemente $d_1, \ldots, d_r$ sind bis auf Assoziierte eindeutig bestimmt.

Diese Elemente $d_1, \ldots, d_r$ heißen die *Elementarteiler* der Matrix A.

Wir zeigen erst einmal die behauptete Eindeutigkeit. Wir schreiben $\mathrm{ggT}(A)$ für einen größten gemeinsamen Teiler aller Einträge der Matrix A. Allgemeiner schreiben wir $\mathrm{ggT}_r(A)$ für einen größten gemeinsamen Teiler aller $r \times r$-Minoren von A (also aller Determinanten von $r \times r$-Matrizen, die durch Auswahl von r Zeilen und Spalten in A entstehen). Das ist äquivalent zu

$$\mathrm{ggT}_r(A) = \mathrm{ggT}\big(\{\det(SAT) \mid S \in \mathrm{Mat}_{r\times m}(R), T \in \mathrm{Mat}_{n\times r}(R)\}\big)$$

(wegen der Multilinearität der Determinante lässt sich $\det(SAT)$ als Linearkombination von Minoren schreiben, und die Minoren selbst treten für geeignete Matrizen S und T in der Menge auf). $\mathrm{ggT}(A) = \mathrm{ggT}_1(A)$ ist ein Spezialfall.

Die Eindeutigkeit beruht auf der folgenden Tatsache.

13.4. **Lemma.** *Sei R ein Hauptidealring, $m, n \geq 0$ und $A, B \in \mathrm{Mat}_{m\times n}(R)$. Sind A und B äquivalent, dann gilt $\mathrm{ggT}_r(A) \sim \mathrm{ggT}_r(B)$ für alle $r \geq 1$. (Insbesondere gilt $\mathrm{ggT}(A) \sim \mathrm{ggT}(B)$.)*

Beweis. Seien $P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ mit $B = PAQ$. Dann gilt

$$\begin{aligned}\{SBT \mid S \in \mathrm{Mat}_{r\times m}(R), T \in \mathrm{Mat}_{n\times r}(R)\}& \\ = \{(SP)A(QT) \mid S \in \mathrm{Mat}_{r\times m}(R), T \in \mathrm{Mat}_{n\times r}(R)\}& \\ = \{S'AT' \mid S' \in \mathrm{Mat}_{r\times m}(R), T' \in \mathrm{Mat}_{n\times r}(R)\}\,,&\end{aligned}$$

denn $S \mapsto SP$ und $T \mapsto QT$ sind Bijektionen. Damit werden die ggTs oben über die selben Mengen von Determinanten gebildet, müssen also assoziiert sein. □

Seien nun $D = \operatorname{diag}(d_1, \dots, d_r)$ und $D' = \operatorname{diag}(d'_1, \dots, d'_{r'})$ äquivalent, und es gelte $d_1 \mid d_2 \mid \cdots \mid d_r$ und $d'_1 \mid d'_2 \mid \cdots \mid d'_{r'}$, sowie $d_r, d'_{r'} \neq 0$. Dann ist $d_1 = \operatorname{ggT}(D) \sim \operatorname{ggT}(D') = d'_1$, und allgemeiner gilt $\operatorname{ggT}_k(D) = d_1 d_2 \cdots d_k$ für $k \leq r$ und $\operatorname{ggT}_k(D) = 0$ für $k > r$, und analog für D'. Nach Lemma 13.4 erhalten wir $r = r'$ und $d_1 \cdots d_k \sim d'_1 \cdots d'_k$ für $k \leq r$, woraus die Behauptung $d_j \sim d'_j$ für alle $1 \leq j \leq r$ folgt.

Jetzt wenden wir uns der Existenz zu. Wir beginnen mit einem einfachen Spezialfall. Dazu erinnern wir uns an Satz 6.11, der besagt, dass in einem Hauptidealring der größte gemeinsame Teiler zweier Elemente als Linearkombination dieser Elemente geschrieben werden kann.

13.5. **Lemma.** *Sei R ein Hauptidealring, $a, b \in R$ und $g = \operatorname{ggT}(a, b)$. Dann gibt es eine Matrix $Q \in \mathrm{GL}_2(R)$ mit $(a\ b)Q = (g\ 0)$.*

Beweis. Es gibt $u, v \in R$ mit $ua + vb = g$. Wir schreiben $a = a'g$, $b = b'g$ und setzen

$$Q = \begin{pmatrix} u & -b' \\ v & a' \end{pmatrix}; \qquad \text{dann rechnet man nach, dass} \qquad (a\ b)Q = (g\ 0)\,.$$

Außerdem ist $\det(Q) = ua' + vb' = (ua + vb)/g = 1$, also ist Q invertierbar. □

Wir dehnen das jetzt auf beliebige $1 \times n$-Matrizen aus.

13.6. **Lemma.** *Sei R ein Hauptidealring, $n \in \mathbb{Z}_{>0}$, $a_1, a_2, \dots, a_n \in R$, und sei $g = \operatorname{ggT}(a_1, \dots, a_n)$. Dann gibt es eine Matrix $Q \in \mathrm{GL}_n(R)$ mit*

$$(a_1\ a_2\ \dots\ a_n)Q = (g\ 0\ \dots\ 0)\,.$$

Beweis. Der Beweis geht durch Induktion nach n. Im Fall $n = 1$ gilt $g = a_1 u$ mit einer Einheit $u \in R^\times$; man kann dann $Q = (u)$ nehmen. Sei also $n \geq 2$. Nach Lemma 13.5 gibt es $Q' \in \mathrm{GL}_2(R)$ mit $(a_{n-1}\ a_n)Q' = (g'\ 0)$, dabei ist g' ein ggT von a_{n-1} und a_n. Wir bilden die Blockdiagonalmatrix $Q_1 \in \mathrm{GL}_n(R)$ aus den Blöcken I_{n-2} und Q'; dann gilt

$$(a_1\ \dots\ a_{n-2}\ a_{n-1}\ a_n)Q_1 = (a_1\ \dots\ a_{n-2}\ g'\ 0)\,.$$

Nach Induktionsannahme gibt es eine Matrix $Q'' \in \mathrm{GL}_{n-1}(R)$ mit

$$(a_1\ \dots\ a_{n-2}\ g')Q'' = (g\ 0\ \dots\ 0\ 0)\,.$$

Wir ergänzen Q'' zu einer Matrix $Q_2 \in \mathrm{GL}_n(R)$, indem wir eine 1 in der rechten unteren Ecke (und sonst Nullen) hinzufügen. Mit $Q = Q_1 Q_2$ erhalten wir dann das gewünschte Resultat. □

Eine Anwendung ist von unabhängigem Interesse:

13.7. **Folgerung.** *Sei R ein Hauptidealring, und seien $a_1, a_2, \dots, a_n \in R$ teilerfremd (d.h. $\operatorname{ggT}(a_1, a_2, \dots, a_n) = 1$). Dann gibt es eine invertierbare Matrix $T \in \mathrm{GL}_n(R)$, deren erste Zeile $(a_1\ a_2\ \dots\ a_n)$ ist.*

Beweis. Nach Lemma 13.6 gibt es eine Matrix $Q \in \mathrm{GL}_n(R)$ mit

$$(a_1\ a_2\ \dots\ a_n)Q = (1\ 0\ \dots\ 0)\,.$$

Mit $T = Q^{-1}$ gilt dann

$$(a_1\ a_2\ \dots\ a_n) = (1\ 0\ \dots\ 0)T\,,$$

was genau die Behauptung ist. □

13.8. **Beispiel.** Es muss also etwa eine Matrix $T \in \mathrm{GL}_3(\mathbb{Z})$ geben mit erster Zeile $(6\ \ 10\ \ 15)$. Wenn man dem Beweis oben folgt, dann erhält man

$$(6\ \ 10\ \ 15)\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & -3\\ 0 & 1 & 2\end{pmatrix} = (6\ \ 5\ \ 0)$$

und

$$(6\ \ 5\ \ 0)\begin{pmatrix}1 & -5 & 0\\ -1 & 6 & 0\\ 0 & 0 & 1\end{pmatrix} = (1\ \ 0\ \ 0)\,,$$

also

$$Q = \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & -3\\ 0 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & -5 & 0\\ -1 & 6 & 0\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & -5 & 0\\ 1 & -6 & -3\\ -1 & 6 & 2\end{pmatrix}$$

und

$$T = Q^{-1} = \begin{pmatrix}6 & 10 & 15\\ 1 & 2 & 3\\ 0 & -1 & -1\end{pmatrix}.$$

Es gilt natürlich auch die transponierte Version von Lemma 13.6, bei der man eine Spalte von links mit einer invertierbaren Matrix multipliziert.

13.9. **Lemma.** *Sei R ein Hauptidealring, $m, n > 0$, und $A \in \mathrm{Mat}_{m\times n}(R)$. Dann ist A äquivalent zu einer Matrix*

$$B = \left(\begin{array}{c|c} d & 0_{1\times(n-1)} \\ \hline 0_{(m-1)\times 1} & A' \end{array}\right)$$

mit $d = \mathrm{ggT}(A)$ und $A' \in \mathrm{Mat}_{(m-1)\times(n-1)}(R)$.

Beweis. Wir betrachten alle zu A äquivalenten Matrizen; sei darunter B' eine, deren linke obere Ecke d bezüglich Teilbarkeit minimal ist (das gibt es, da es in R keine unendlich absteigenden Teilerketten gibt). Ich behaupte, dass d ein ggT von A ist. Nach Lemma 13.4 gilt $\mathrm{ggT}(A) \sim \mathrm{ggT}(B') \mid d$. Angenommen, es gibt einen Eintrag in B', der nicht von d geteilt wird. Ist dieser Eintrag in der ersten Zeile oder Spalte von B', dann können wir Lemma 13.6 oder seine transponierte Version anwenden, um d durch den ggT d' der ersten Zeile oder Spalte zu ersetzen. Dann hätten wir aber eine äquivalente Matrix, deren linke obere Ecke ein echter Teiler von d wäre im Widerspruch zur Wahl von B'. Also können wir annehmen, dass d alle Einträge der ersten Zeile und Spalte teilt. Wir können diese Einträge dann durch geeignete elementare Spalten- und Zeilenumformungen zu null machen und die resultierende Matrix als B' betrachten. Gibt es jetzt einen Eintrag, der nicht von d geteilt wird, etwa in der $k$ten Zeile, dann addieren wir die $k$te Zeile zur ersten Zeile (das lässt die linke obere Ecke unverändert, da der erste Eintrag in der $k$ten Zeile null ist) und sind dann im gerade schon behandelten Fall. Wir bekommen also in jedem Fall einen Widerspruch, wenn $d \nmid \mathrm{ggT}(B)$. Es folgt, dass $d = \mathrm{ggT}(B) \sim \mathrm{ggT}(A)$ wie behauptet. Wie gerade schon im Beweis der Behauptung können wir die erste Zeile und Spalte von B' „ausräumen“ und erhalten so eine äquivalente Matrix der angegebenen Form. □

Damit können wir die im Satz 13.3 behauptete Existenz beweisen, und zwar durch Induktion nach $\min\{m, n\}$. Gilt $m = 0$ oder $n = 0$, so ist nichts zu zeigen. Seien also $m, n \geq 1$. Nach Lemma 13.9 ist A äquivalent zu einer Matrix B der dort

angegebenen Form, und es gilt $d_1 := d \mid \mathrm{ggT}(A')$. Ist $d = 0$, dann sind wir fertig, denn $A = 0$ hat bereits die richtige Form (mit $r = 0$). Im anderen Fall ist nach Induktionsannahme A' äquivalent zu einer Matrix $\mathrm{diag}_{m-1,n-1}(d_2, \ldots, d_r)$ mit $d_2 \mid d_3 \mid \cdots \mid d_r$ und $d_r \neq 0$. Die betreffenden Matrizen P und Q können (durch Erweitern nach links oben mit Eckeintrag 1 und weiteren Einträgen 0) zu invertierbaren Matrizen in $\mathrm{GL}_m(R)$ bzw. $\mathrm{GL}_n(R)$ erweitert werden und liefern die Äquivalenz von B mit $\mathrm{diag}_{m,n}(d_1, d_2, \ldots, d_r)$. Da d_1 ein Teiler von $\mathrm{ggT}(A') = d_2$ ist, hat diese Matrix die verlangte Form.

13.10. **Beispiel.** Als Beispiel bestimmen wir die Elementarteiler der „Telefonmatrix“

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(\mathbb{Z})\,.$$

Dabei halten wir uns nicht sklavisch an den Beweis, sondern führen geeignete Zeilen- und Spaltenumformungen durch, bis die Matrix die richtige Form hat:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \overset{\text{S1}\to 23}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 4 & -3 & -6 \\ 7 & -6 & -12 \end{pmatrix} \overset{\text{Z1}\to 23}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}$$

$$\overset{\text{Z2}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 6 \\ 0 & -6 & -12 \end{pmatrix} \overset{\text{S2}\to 3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & -6 & 0 \end{pmatrix} \overset{\text{Z2}\to 3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Damit gilt $r = 2$ und $d_1 = 1$, $d_2 = 3$.

13.11. **Bemerkung.** Der Satz über die Normalform gilt über jedem Hauptidealring R. Wenn man die Normalform aber *berechnen* will, dann muss man in der Lage sein, einen größten gemeinsamen Teiler von $a, b \in R$ explizit als Linearkombination von a und b zu schreiben. Ist R ein *euklidischer* Ring, dann geht das mit dem erweiterten Euklidischen Algorithmus. Für euklidische Ringe kann man auch zeigen, dass man bei der Umformung in die Normalform immer mit *elementaren* Zeilen- und Spaltenumformungen auskommt (also Multiplikation einer Zeile oder Spalte mit einer Einheit, Addition eines Vielfachen einer Zeile oder Spalte zu einer anderen; das Vertauschen zweier Zeilen oder Spalten lässt sich darauf zurückführen).

Sei dazu N die euklidische Normfunktion von R. Um Lemma 13.9 für den Fall zu beweisen, dass nur elementare Umformungen erlaubt sind, betrachten wir unter allen Matrizen, die sich aus A auf diese Weise erzeugen lassen und einen von null verschiedenen Eintrag in der linken oberen Ecke haben, eine, sie heiße B, mit minimaler Norm $N(b_{11}) > 0$ des Eintrags in der linken oberen Ecke. (Wir können natürlich $A \neq 0$ annehmen, so dass so eine Matrix B existiert.) Wir müssen zeigen, dass dann b_{11} alle Einträge von B teilt. Gibt es einen Eintrag in der ersten Zeile, der nicht von b_{11} geteilt wird, dann kann man ihn durch eine geeignete elementare Spaltenumformung durch seinen Rest bei Division durch b_{11} ersetzen und bekommt ein Element $\neq 0$ kleinerer Norm, das durch einen Spaltentausch in die linke obere Ecke kommt, Widerspruch. Ebenso für die erste Spalte. Also sind jedenfalls die Einträge in der ersten Zeile und ersten Spalte durch b_{11} teilbar; durch geeignete elementare Zeilen- und Spaltenumformungen können diese Einträge zu null gemacht werden. Ist jetzt b_{ij} (mit $i, j > 1$) nicht durch b_{11} teilbar, addieren wir die i-te zur ersten Zeile und sind im bereits ausgeschlossenen Fall. Aus diesem Beweis lässt sich ein Algorithmus extrahieren.

Schreibt man E_{ij} für die $n \times n$-Matrix, deren einziger von null verschiedener Eintrag eine 1 in Zeile i und Spalte j ist, dann folgt:

Sei R ein euklidischer Ring. Dann wird die Gruppe $\mathrm{GL}_n(R)$ erzeugt von den Matrizen $I + \lambda E_{ij}$ für $i \neq j$ und $\lambda \in R$ und $I + (u-1)E_{ii}$ für alle $1 \leq i \leq n$ und $u \in R^\times$. (Dabei sei I die $n \times n$-Einheitsmatrix.)

13.12. **Ausblick.** Wir skizzieren noch kurz, wie man aus Satz 13.3 den *Klassifikationssatz für endlich erzeugte abelsche Gruppen* herleitet:

Sei G eine endlich erzeugte abelsche Gruppe. Dann ist G isomorph zu einem direkten Produkt

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^r$$

mit eindeutig bestimmten ganzen Zahlen $r \geq 0$ und $d_j > 1$, so dass $d_1 \mid d_2 \mid \cdots \mid d_k$.

Sei n die Zahl der Erzeuger von G. Dann gibt es einen surjektiven Homomorphismus $\varphi : \mathbb{Z}^n \to G$ von abelschen Gruppen. Nach dem üblichen Isomorphiesatz folgt $G \cong \mathbb{Z}^n/\ker(\varphi)$. Nun kann man zeigen, dass jede Untergruppe von $\mathbb{Z}^n$ endlich erzeugt ist; insbesondere gilt das für $\ker(\varphi)$; sei dieser Kern erzeugt von $(a_{11}, a_{12}, \ldots, a_{1n}),\ \ldots,\ (a_{m1}, a_{m2}, \ldots, a_{mn})$. Wir bilden aus diesen m Zeilen eine $m \times n$-Matrix $A \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$. Auf diese Matrix wenden wir Satz 13.3 an: $PAQ = \mathrm{diag}_{m,n}(d_1, d_2, \ldots, d_l)$. Die Zeilen von PA erzeugen ebenfalls die Untergruppe $\ker(\varphi)$; die Multiplikation von rechts mit Q entspricht einem Isomorphismus $\mathbb{Z}^n \to \mathbb{Z}^n$, den wir mit dem Homomorphismus $\varphi : \mathbb{Z}^n \to G$ verknüpfen können. Wir können also annehmen, dass $\ker(\varphi)$ von den Zeilen $d_1\vec{e}_1, d_2\vec{e}_2, \ldots, d_l\vec{e}_l$ der neuen Matrix erzeugt wird. Daraus folgt sofort, dass

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_l\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n-l}$$

ist. Wir können die d_j positiv wählen und alle $d_j = 1$ weglassen. Dann bekommen wir die Darstellung wie im Satz behauptet; die Eindeutigkeit folgt aus der Eindeutigkeit der Elementarteiler.

Wir werden dies zu Beginn des kommenden Semesters in der *Einführung in die Algebra* im Detail durchführen.

Literatur

[Fi] Gerd Fischer: *Lehrbuch der Algebra,* Vieweg, 2008. Signatur 80/SK 200 F529 L5. Onlie-Zugriff unter
http://dx.doi.org/10.1007/978-3-8348-9455-7

- Ein Standard-Lehrbuch. Das Buch folgt dem üblichen Aufbau Gruppen-Ringe-Körper, so dass für diese Vorlesung hauptsächlich der mittlere Teil (Kapitel II) interessant ist, wo aber natürlich gelegentlich auf Resultate über Gruppen zurückgegriffen wird.

[KM] Christian Karpfinger und Kurt Meyberg: *Algebra. Gruppen - Ringe - Körper,* Spektrum Akademischer Verlag, 2010. Online-Zugriff unter
http://dx.doi.org/10.1007/978-3-8274-2601-7.

- Kapitel 12–18 und 10. Das Buch folgt dem üblichen Aufbau Gruppen-Ringe-Körper, so dass für diese Vorlesung hauptsächlich der mittlere Teil interessant ist, wo aber natürlich gelegentlich auf Resultate über Gruppen zurückgegriffen wird.

[MP] Stefan Müller-Stach und Jens Piontkowski: *Elementare und algebraische Zahlentheorie,* Vieweg, 2006. Signatur 82/SK 180 M947. Online-Zugriff unter
http://dx.doi.org/10.1007/978-3-8348-9064-1.

- Die ersten neun Kapitel sind relevant für den Zahlentheorie-Teil der Vorlesung.

[Sch] Alexander Schmidt: *Einführung in die algebraische Zahlentheorie,* Springer-Verlag 2007. Signatur 82/SK 180 S349. Online-Zugriff unter
http://dx.doi.org/10.1007/978-3-540-45974-3.

- Kapitel 1, 2 und 4 sind relevant für den Zahlentheorie-Teil der Vorlesung.