Einführung in die Zahlentheorie und algebraische Strukturen

Wintersemester 2012/2013

Universität Bayreuth

Michael Stoll

Inhaltsverzeichnis

Druckversion vom 26. März 2013, 20:33 Uhr.

1. Wiederholung: Gruppen, Ringe, Körper

Diese Vorlesung ist eine erste Einführung in die Algebra (auch wenn etwas verwirrenderweise die *zweite* Algebra-Vorlesung „Einführung in die Algebra“ heißt).

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 anhand 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. Schließlich werden wir noch abelsche Gruppen diskutieren und den wichtigen Klassifikationssatz für endlich erzeugte abelsche Gruppen beweisen.

In der „Einführung in der Algebra“, die Sie sinnvollerweise dann im Sommersemester hören sollten, gibt es zwei Hauptthemen: Einerseits werden (insbesondere endliche) Gruppen genauer studiert; auf der anderen Seite geht es um algebraische Körpererweiterungen. Für die Konstruktion solcher Körpererweiterungen spielen die in diesem Semester genauer betrachteten Polynomringe eine wesentliche Rolle.

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.

Für die Zwecke dieser Vorlesung ist Null eine natürliche Zahl:

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

gelegentlich werden wir die Schreibweise

$$\mathbb{N}_+ = \{1, 2, 3, \ldots\}$$

für die Menge der positiven natürlichen (oder ganzen) Zahlen verwenden. Meistens werde ich zur Vermeidung von Unklarheiten aber $\mathbb{Z}_{\geq 0}$ und $\mathbb{Z}_{>0}$ für diese Mengen schreiben. Wie üblich steht $\mathbb{Z}$ für den Ring der ganzen Zahlen, $\mathbb{Q}$ für den Körper der rationalen Zahlen, $\mathbb{R}$ für den Körper der reellen Zahlen und $\mathbb{C}$ für den Körper der komplexen Zahlen.

Damit klar ist, wovon im Folgenden die Rede sein wird, wiederholen wir die Definitionen der wichtigsten algebraischen Strukturen (wie sie zum Beispiel bereits in der Linearen Algebra I eingeführt wurden).

Wir beginnen mit dem Minimum, das man für eine halbwegs interessante algebraische Struktur braucht.

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

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

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

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

Wenn die Verknüpfung $*$ aus dem Kontext klar ist, spricht man der Einfachheit halber meist von „der Halbgruppe H“. ♢

Das Assoziativgesetz bewirkt, dass es nicht darauf ankommt, wie Ausdrücke, die drei oder mehr Elemente miteinander verknüpfen, geklammert sind. Zum Beispiel gilt für beliebige Elemente a, b, c, d, e von H:

$$\begin{aligned} a * ((b * c) * d) &= a * (b * (c * d)) = (a * b) * (c * d) \\ &= ((a * b) * c) * d = (a * (b * c)) * d \qquad \text{und} \\ a * (b * (c * (d * e))) &= (a * b) * (c * (d * e)) = ((a * b) * (c * d)) * e = \dots . \end{aligned}$$

Man kann deswegen einfach $a * b * c * d$ bzw. $a * b * c * d * e$ schreiben.

Wenn die Halbgruppe kommutativ ist, dann kommt es auch nicht auf die Reihenfolge an:

$$a * b * c = b * a * c = b * c * a = c * b * a = c * a * b = a * c * b .$$

1.2. **Beispiele.** Das Trivialbeispiel einer Halbgruppe ist $(\emptyset, *)$, wobei $* : \emptyset \times \emptyset \to \emptyset$ die leere Abbildung ist (beachte: $\emptyset \times \emptyset = \emptyset$). **BSP** Halbgruppen

Beispiele von kommutativen Halbgruppen sind $(\mathbb{N}_+, +)$, $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{N}_+, \cdot)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$. Die Halbgruppe $(\mathrm{Abb}(X, X), \circ)$ der Abbildungen $X \to X$ für eine beliebige Menge X, mit der Komposition von Abbildungen als Verknüpfung, ist im Allgemeinen nicht kommutativ. ♣

Mit Halbgruppen kann man allerdings noch nicht allzu viel anfangen. Deshalb fordern wir zusätzliche Eigenschaften.

1.3. **Definition.** Ein *Monoid* ist ein Tripel $(M, *, e)$, bestehend aus einer Menge M, einer Abbildung $* : M \times M \to M$ und einem Element $e \in M$, sodass $(M, *)$ eine Halbgruppe mit *neutralem Element* e ist: **DEF** Monoid

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

Das Monoid heißt *kommutativ*, wenn die Halbgruppe $(M, *)$ kommutativ ist. ♢

Wenn es ein neutrales Element gibt, dann ist es eindeutig bestimmt. Aus diesem Grund lässt man meistens die Angabe des neutralen Elements weg und spricht vom „Monoid $(M, *)$“ oder auch nur vom „Monoid M“, wenn die Verknüpfung aus dem Kontext klar ist.

1.4. **Beispiele.** Da die Definition von „Monoid“ ein neutrales Element fordert, kann die leere Menge kein Monoid sein. Das triviale Monoid ist dann $(\{e\}, *, e)$, wobei $*$ die einzige Abbildung $\{e\} \times \{e\} \to \{e\}$ ist (es ist also $e * e = e$). **BSP** Monoide

Bis auf $(\mathbb{N}_+, +)$, wo es kein neutrales Element gibt, lassen sich alle Beispiele von Halbgruppen aus 1.2 als Monoide $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, +, 0)$, $(\mathbb{N}_+, \cdot, 1)$, $(\mathbb{N}, \cdot, 1)$, $(\mathbb{Z}, \cdot, 1)$ und $(\mathrm{Abb}(X, X), \circ, \mathrm{id}_X)$ betrachten. ♣

Noch schöner ist es, wenn sich die Verknüpfung mit einem Element durch die Verknüpfung mit einem (in der Regel) anderen Element wieder rückgängig machen lässt. Das führt auf den Begriff der Gruppe.

1.5. **Definition.** Eine *Gruppe* ist ein Quadrupel $(G, *, e, i)$, bestehend aus einer Menge G, einer Abbildung $* : G \times G \to G$, einem Element $e \in G$ und einer Abbildung $i : G \to G$, sodass $(G, *, e)$ ein Monoid ist und für jedes $g \in G$ das Element $i(g) \in G$ ein *Inverses* von g ist: **DEF** Gruppe

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

Die Gruppe heißt *kommutativ* oder *abelsch*, wenn das Monoid $(G, *, e)$ kommutativ ist. ♢

Die Bezeichnung „abelsch“ ehrt den norwegischen Mathematiker Niels Henrik Abel, nach dem auch der *Abelpreis* benannt ist, ein dem Nobelpreis vergleichbarer Preis für Mathematik, der seit 2003 jährlich verliehen wird.

Auch Inverse sind eindeutig bestimmt. Analog zu Monoiden spricht man deshalb auch einfach von „der Gruppe $(G, *)$“ oder auch von „der Gruppe G“, wenn die Verknüpfung aus dem Kontext klar ist.

Gruppen schreibt man gerne „multiplikativ“, dann ist die Verknüpfung $a \cdot b$ oder kurz ab, das neutrale Element heißt 1 und das Inverse von a wird a^{-1} geschrieben. Kommutative Gruppen schreibt man auch häufig „additiv“, dann ist die Verknüpfung $a + b$, das neutrale Element heißt 0 und das Inverse von a wird als das Negative von a geschrieben: $-a$. Dann schreibt man auch kurz $a - b$ für $a + (-b)$.

1.6. **Beispiele.** Das triviale Monoid lässt sich auch als Gruppe betrachten, denn das einzige Element e ist sein eigenes Inverses. **BSP** Gruppen

Von den übrigen Beispielen von Monoiden in 1.4 kann nur $(\mathbb{Z}, +, 0, -)$ auch als Gruppe betrachtet werden (und im letzten Beispiel $\mathrm{Abb}(X, X)$, wenn X höchstens ein Element hat; dann hat man eine triviale Gruppe). Ein weiteres Beispiel einer kommutativen Gruppe ist $(\mathbb{R}_{>0}, \cdot, 1, x \mapsto 1/x)$, wobei $\mathbb{R}_{>0}$ die Menge der positiven reellen Zahlen ist.

Wenn man sich bei den Abbildungen $X \to X$ auf die bijektiven Abbildungen beschränkt, dann erhält man eine Gruppe $(S(X), \circ, \mathrm{id}_X, f \mapsto f^{-1})$, die auch die *symmetrische Gruppe* von X heißt. Dabei ist

$$S(X) = \{f : X \to X \mid f \text{ bijektiv}\} \,.$$

Diese Gruppe ist genau dann kommutativ, wenn X höchstens zwei Elemente enthält.

Gruppen werden in der „Einführung in die Algebra“ genauer studiert. ♣

Als Nächstes betrachten wir Strukturen mit zwei Verknüpfungen.

* 1.7. **Definition.** Ein *Ring* ist ein Sextupel $(R, +, 0, -, \cdot, 1)$, bestehend aus einer Menge R, Abbildungen $+, \cdot : R \times R \to R$, Elementen $0, 1 \in R$ und einer Abbildung $- : R \to R$, sodass $(R, +, 0, -)$ eine kommutative Gruppe und $(R, \cdot, 1)$ ein Monoid ist und die *Distributivgesetze*

DEF Ring

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

gelten. Der Ring heißt *kommutativ*, wenn das Monoid $(R, \cdot, 1)$ kommutativ ist. ♢

Da die neutralen und inversen Elemente eindeutig bestimmt sind, spricht man oft nur vom „Ring $(R, +, \cdot)$“ oder sogar vom „Ring R“, wenn die Verknüpfungen aus dem Kontext klar sind. Ist der Ring kommutativ, dann genügt es, eines der beiden Distributivgesetze zu fordern. Für das Produkt $a \cdot b$ zweier Elemente schreibt man auch kurz ab.

In einem Ring kann man also addieren, subtrahieren und multiplizieren, und die üblichen Rechenregeln gelten, wie zum Beispiel $0 \cdot a = a \cdot 0 = 0$, $-(a+b) = -a-b$, $(-a) \cdot (-b) = a \cdot b$. Was aber im Allgemeinen *nicht* gelten muss, ist die Implikation $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$. Ringe, in denen diese Aussage gilt, werden in dieser Vorlesung eine wesentliche Rolle spielen; wir werden den entsprechenden Begriff bald definieren.

In einem Ring hat nicht unbedingt jedes (von null verschiedene) Element ein multiplikatives Inverses. Das motiviert folgende Definition.

1.8. **Definition.** Sei $(R, +, 0, -, \cdot, 1)$ ein Ring. Ein Element $u \in R$ heißt *Einheit* von R, wenn u in R *invertierbar* ist, wenn es also ein Element $u' \in R$ gibt mit $u \cdot u' = u' \cdot u = 1$. Man schreibt dann u^{-1} für u' (u' ist eindeutig bestimmt).

DEF Einheit

Einheitengruppe

Die Menge $R^\times$ aller Einheiten von R bildet mit der Multiplikation von R eine Gruppe $(R^\times, \cdot, 1)$, die *Einheitengruppe* von R. ♢

Der Beweis der Aussage, dass $R^\times$ eine Gruppe bildet, ist eine Übungsaufgabe.

1.9. **Beispiele.** Das Trivialbeispiel für einen Ring ist der sogenannte *Nullring* $(\{0\}, +, 0, -, \cdot, 0)$, in dem $0 = 1$ und $0 + 0 = -0 = 0 \cdot 0 = 0$ gelten. Jeder Ring R, in dem $0_R = 1_R$ gilt, ist so ein Nullring, denn für alle $r \in R$ gilt dann $r = 1_R \cdot r = 0_R \cdot r = 0_R$.

BSP Ringe

Das Standardbeispiel für einen (kommutativen) Ring ist der Ring $\mathbb{Z}$ der ganzen Zahlen mit der üblichen Addition und Multiplikation als Verknüpfungen. Es ist $\mathbb{Z}^\times = \{-1, 1\}$.

Aus der Linearen Algebra kennen wir den Matrizenring $\mathrm{Mat}(n, K)$ über einem Körper K. Dieser Ring ist nicht kommutativ, wenn $n \geq 2$ ist. Die Einheitengruppe von $\mathrm{Mat}(n, K)$ ist die „allgemeine lineare Gruppe“ $\mathrm{GL}(n, K)$ der invertierbaren $n \times n$-Matrizen. ♣

Schließlich kommen wir zu den Körpern.

1.10. **Definition.** Ein *Körper* ist ein Septupel $(K, +, 0, -, \cdot, 1, i)$, bestehend aus einer Menge K, Abbildungen $+, \cdot : K \times K \to K$, Elementen $0, 1 \in K$, einer Abbildung $- : K \to K$ und einer Abbildung $i : K \setminus \{0\} \to K \setminus \{0\}$, sodass $(K, +, 0, -, \cdot, 1)$ ein kommutativer Ring und $(K \setminus \{0\}, \cdot, 1, i)$ eine (kommutative) Gruppe ist. Für $i(a)$ schreibt man a^{-1}. ♢

DEF Körper

Wie üblich spricht man meistens einfach von dem „Körper $(K, +, \cdot)$“ oder von dem „Körper K“. Aus der Definition folgt, dass 0 und 1 in einem Körper verschieden sein müssen, denn 1 soll das neutrale Element der Gruppe $K \setminus \{0\}$ sein. Diese Gruppe $(K \setminus \{0\}, \cdot)$ ist die Einheitengruppe $K^\times$ von K (als Ring betrachtet); bei Körpern nennt man sie meist die *multiplikative Gruppe* von K. (Häufig findet man auch die Schreibweise K^* dafür.)

Für $a, b \in K$, $b \neq 0$, kann man die Division definieren durch $a/b = a \cdot b^{-1}$. Dann hat man die vier Grundrechenarten zur Verfügung und die üblichen Rechenregeln dafür gelten, denn man kann sie aus den Körperaxiomen ableiten. Zum Beispiel gilt in einem Körper stets, dass aus $a \cdot b = 0$ folgt, dass $a = 0$ oder $b = 0$ ist. (Denn ist $a \neq 0$, dann folgt $0 = a^{-1} \cdot 0 = a^{-1} \cdot a \cdot b = 1 \cdot b = b$.)

BSP Körper

1.11. **Beispiele.** Das kleinste Beispiel für einen Körper hat nur die beiden Elemente 0 und 1, die in der Definition gefordert werden. Für die Addition und Multiplikation folgt $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ und $1 \cdot 1 = 1$ direkt aus der Definition; für die verbleibende Summe $1 + 1$ bleibt nur der Wert 0, da die Gleichung $a + 1 = 0$ lösbar sein muss. Man kann (einfach, aber länglich) nachprüfen, dass dieser Körper, der mit $\mathbb{F}_2$ bezeichnet wird, die Axiome erfüllt.

Es gibt noch weitere endliche Körper: Zu jeder Potenz p^e einer Primzahl p (mit $e \geq 1$) gibt es im Wesentlichen genau einen Körper mit p^e Elementen, und es gibt keine anderen endlichen Körper. Das wird in der „Einführung in die Algebra“ genauer besprochen.

Standardbeispiele für Körper sind die Körper $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ der rationalen, reellen und komplexen Zahlen, jeweils mit der bekannten Addition und Multiplikation. ♣

Der Vollständigkeit halber folgt hier noch die Definition eines Schiefkörpers, auch wenn Schiefkörper in dieser Vorlesung und der „Einführung in die Algebra“ keine Rolle spielen werden.

DEF Schiefkörper

Definition. Ein *Schiefkörper* ist ein Septupel $(K, +, 0, -, \cdot, 1, i)$, bestehend aus einer Menge K, Abbildungen $+, \cdot : K \times K \to K$, Elementen $0, 1 \in K$, einer Abbildung $- : K \to K$ und einer Abbildung $i : K \setminus \{0\} \to K \setminus \{0\}$, sodass $(K, +, 0, -, \cdot, 1)$ ein nicht-kommutativer Ring und $(K \setminus \{0\}, \cdot, 1, i)$ eine Gruppe ist. Für $i(a)$ schreibt man a^{-1}. ♢

Der Unterschied zum Körper ist also, dass die Multiplikation nicht kommutativ ist. Das wichtigste Beispiel eines Schiefkörpers ist der Schiefkörper $\mathbb{H}$ der *Quaternionen*. Er ist definiert als ein vierdimensionaler Vektorraum über $\mathbb{R}$ mit Basis $1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$; für die Multiplikation der Basiselemente gilt

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1, \quad \boldsymbol{ij} = \boldsymbol{k} = -\boldsymbol{ji}, \quad \boldsymbol{jk} = \boldsymbol{i} = -\boldsymbol{kj}, \quad \boldsymbol{ki} = \boldsymbol{j} = -\boldsymbol{ik};$$

dadurch und durch das Distributivgesetz ist die Multiplikation eindeutig festgelegt. Es ist natürlich noch zu zeigen, dass $\mathbb{H} \setminus \{0\}$ unter der so definierten Multiplikation tatsächlich eine Gruppe bildet. Siehe § 29 im Skript „Lineare Algebra II“ (oder auch Definition 7.1 später in diesem Skript).

Endliche Schiefkörper gibt es nicht; das ist ein berühmter Satz von Joseph Wedderburn. (In der im hier verlinkten Wikipedia-Eintrag zu Grunde gelegten Definition von „Schiefkörper“ darf die Multiplikation auch kommutativ sein [das ist in der Literatur uneinheitlich], deshalb lautet die Aussage dort „Jeder endliche Schiefkörper ist ein Körper“.)

2. Teilbarkeitslehre in Integritätsbereichen

Wir wollen uns im Folgenden mit Teilbarkeit beschäftigen.

* 2.1. **Definition.** Seien R ein kommutativer Ring und $a, b \in R$. Wir sagen, a *teilt* b, a ist ein *Teiler* von b oder b ist ein *Vielfaches* von a, geschrieben $a \mid b$, wenn es ein $c \in R$ gibt mit $b = ac$. ♢ **DEF** Teiler

In nicht-kommutativen Ringen müsste man zwischen Teilbarkeit von rechts ($b = ca$) und von links ($b = ac$) unterscheiden.

Wir sind es gewöhnt, dass aus $ab = 0$ folgt, dass einer der Faktoren null ist. In allgemeinen Ringen gilt dies jedoch nicht unbedingt. Wir geben dieser unangenehmen Erscheinung einen Namen.

2.2. **Definition.** Seien R ein Ring und $a \in R$. Dann heißt a ein *Nullteiler* von R, wenn $a \neq 0$ ist und es $0 \neq b \in R$ gibt mit $ab = 0$ oder $ba = 0$. ♢ **DEF** Nullteiler

2.3. **Beispiele.** Man kann sich leicht überlegen, dass $\mathbb{Z} \times \mathbb{Z}$ mit komponentenweise definierter Addition und Multiplikation ein (kommutativer) Ring ist; das Nullelement ist $(0, 0)$ und das Einselement ist $(1, 1)$. In diesem Ring sind alle Elemente der Form $(a, 0)$ oder $(0, a)$ mit $a \neq 0$ Nullteiler, denn $(a, 0) \cdot (0, a) = (0, 0)$. (Das sind tatsächlich auch *alle* Nullteiler.) **BSP** Nullteiler

Ein anderes Beispiel ist der Ring $\mathbb{Z}/4\mathbb{Z}$, dessen Elemente man mit den Zahlen $0, 1, 2, 3$ identifizieren kann; die Addition und Multiplikation erfolgt dann „modulo 4“, man ersetzt also das Ergebnis der gewöhnlichen Addition bzw. Multiplikation durch seinen Rest bei Division durch 4. Es gilt also etwa $1 + 1 = 2$, $2 + 3 = 1$, $3 \cdot 3 = 1$ und $2 \cdot 2 = 0$. Letzteres zeigt, dass 2 ein Nullteiler in diesem Ring ist (tatsächlich auch der einzige Nullteiler). „Faktorringe“ wie $\mathbb{Z}/4\mathbb{Z}$ werden später in dieser Vorlesung noch genauer besprochen.

Ein in gewisser Weise ähnliches Beispiel ist der *Ring der dualen Zahlen* $K[\varepsilon]$ über einem Körper K. Seine Elemente haben die Form $a + b\varepsilon$ mit $a, b \in K$; sie werden gemäß

$$(a+b\varepsilon)+(a'+b'\varepsilon) = (a+a')+(b+b')\varepsilon \quad \text{und} \quad (a+b\varepsilon)\cdot(a'+b'\varepsilon) = aa'+(ab'+a'b)\varepsilon$$

addiert und multipliziert. Insbesondere ist $\varepsilon^2 = 0$; damit ist ε (und ebenso $b\varepsilon$ für alle $b \in K^\times$) ein Nullteiler.

Auch im Matrizenring $\mathrm{Mat}(n, K)$ gibt es Nullteiler, sobald $n \geq 2$ ist. Zum Beispiel ist

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

Für die Untersuchung von Teilbarkeit sind Nullteiler recht hinderlich. Darum zeichnen wir eine Klasse von Ringen aus, in denen sie nicht auftreten.

* 2.4. **Definition.** Ein *Integritätsring* ist ein Ring R, der nicht der Nullring ist und in dem es keine Nullteiler gibt. Ist R außerdem kommutativ, dann ist R ein *Integritätsbereich*. ♢ **DEF** Integritätsring Integritätsbereich

Die erste Bedingung ist zu $0 \neq 1$ in R äquivalent.

2.5. **Beispiele.** Das Standardbeispiel für einen Integritätsbereich ist der Ring $\mathbb{Z}$ der ganzen Zahlen. Daher kommt auch der Name: „integer“ heißt „ganz“. **BSP** Integritätsbereiche

Jeder Körper ist ein Integritätsbereich. ♣

Für das Folgende nicht unmittelbar wichtig, aber (nicht zuletzt wegen des im Beweis verwendeten Arguments) in diesem Zusammenhang interessant ist folgendes Resultat.

2.6. **Satz.** *Ist R ein endlicher Integritätsbereich, dann ist R bereits ein Körper (d.h., jedes Element $\neq 0$ von R ist invertierbar).* **SATZ** endl. IB ist Körper

Beweis. Sei $0 \neq a \in R$. Wir müssen zeigen, dass a invertierbar ist, dass es also ein $b \in R$ gibt mit $ab = 1$. Dazu betrachten wir folgende Abbildung:

$$m_a : R \longrightarrow R, \quad r \longmapsto ar$$

(„Multiplikation mit a“). Diese Abbildung m_a ist injektiv: Sind $r, r' \in R$ mit $m_a(r) = m_a(r')$, dann folgt $a(r-r') = 0$; weil $a \neq 0$ ist und R ein Integritätsbereich ist, muss $r = r'$ sein.

Da R endlich ist, ist eine injektive Abbildung $R \to R$ bereits bijektiv und damit insbesondere surjektiv. Es gibt also $b \in R$ mit $ab = m_a(b) = 1$. ❑

Analog zeigt man (unter Verwendung der beiden Abbildungen m_a und $m'_a : r \mapsto ra$), dass ein endlicher nicht-kommutativer Integritätsring ein Schiefkörper ist. Nach dem Satz von Wedderburn (siehe das Kleingedruckte auf Seite 6) gibt es keine endlichen Schiefkörper, also gilt: *Jeder endliche Integritätsring ist ein Körper.*

Bevor wir Eigenschaften der Teilbarkeitsrelation beweisen, führen wir noch einen Begriff ein.

∗ 2.7. **Definition.** Sei R ein kommutativer Ring. Zwei Elemente $a, b \in R$ heißen *(zueinander) assoziiert*, $a \sim b$, wenn es eine Einheit $u \in R^\times$ gibt mit $b = ua$. ♢ **DEF** assoziiert

Assoziiertheit ist eine Äquivalenzrelation; das kommt daher, dass $R^\times$ eine Gruppe ist. (Wenn Ihnen das nicht klar ist, sollten Sie es sich klar machen!)

Im Ring $\mathbb{Z}$ bedeutet $a \sim b$ nichts anderes als $a = \pm b$ oder auch $|a| = |b|$.

Nun zu den Eigenschaften der Teilbarkeitsrelation.

2.8. **Lemma.** *Seien R ein Integritätsbereich und $a, b, c \in R$. Dann gilt:* **LEMMA** Eigenschaften Teilbarkeit

(1) *Aus $a \mid b$ und $a \mid c$ folgt $a \mid b + c$ und $a \mid b - c$.*

(2) *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.*

(3) *Aus $a \mid b$ folgt $a \mid bc$.*

(4) $0 \mid a \iff a = 0 \quad$ *und* $\quad a \mid 1 \iff a \in R^\times$.

(5) $a \mid 0$, $1 \mid a$ *und* $a \mid a$.

(6) $a \mid b \quad$ *und* $\quad b \mid a \iff a \sim b$.

Beweis.

(1) Nach Definition bedeuten die Voraussetzungen, dass es $b', c' \in R$ gibt mit $b = ab'$ und $c = ac'$. Dann gilt $b \pm c = a(b' \pm c')$, also ist a auch ein Teiler von $b \pm c$.

(2) Übung.

(3) Übung.

(4) $0 \mid a$ bedeutet, dass es $b \in R$ gibt mit $a = b \cdot 0 = 0$, also muss $a = 0$ sein. Dass $0 \mid 0$ gilt, ist klar.

$a \mid 1$ bedeutet, dass es $b \in R$ gibt mit $1 = ab$; das ist aber genau die Bedingung dafür, dass a eine Einheit ist.

(5) Übung.

(6) Die links stehende Aussage besagt, dass es $c, c' \in R$ gibt mit $b = ac$, $a = bc'$. Es folgt $acc' = bc' = a$, also $a(cc' - 1) = 0$. Da R ein Integritätsbereich ist, muss $a = 0$ sein (dann folgt auch $b = 0$ und es gilt $a \sim b$) oder $cc' = 1$, dann ist c eine Einheit und damit gilt $a \sim b$.

Umgekehrt bedeutet $a \sim b$, dass es $u \in R^\times$ gibt mit $b = ua$; damit gilt jedenfalls $a \mid b$. Es gilt aber auch $a = u^{-1}b$ und damit $b \mid a$. ❑

Die Teilbarkeitsrelation ist also insbesondere reflexiv und transitiv, und sie hängt nur von der Assoziiertheitsklasse der beteiligten Elemente ab: Gilt $a \sim a'$ und $b \sim b'$, dann sind $a \mid b$ und $a' \mid b'$ äquivalent. (Die eine Richtung folgt so: Aus $a \sim a'$ folgt $a' \mid a$, aus $b \sim b'$ folgt $b \mid b'$, also folgt aus $a \mid b$ mit der Transitivität der Teilbarkeit auch $a' \mid b'$.) Auf den Assoziiertheitsklassen ist die Relation auch antisymmetrisch (das ist die letzte Eigenschaft in Lemma 2.8); wir erhalten eine (Teil-)Ordnung. In dieser Ordnung ist die Klasse der Einheiten das kleinste und die Klasse der Null das größte Element. Wir betrachten jetzt größte untere und kleinste obere Schranken von zwei Elementen in dieser Ordnung.

∗ 2.9. **Definition.** Seien R ein Integritätsbereich und $a, b \in R$. Wir sagen, $g \in R$ ist ein *größter gemeinsamer Teiler* (kurz: ggT) von a und b und schreiben dafür $g \sim \mathrm{ggT}(a, b)$, wenn g ein gemeinsamer Teiler von a und b ist (also $g \mid a$ und $g \mid b$) und für jeden weiteren gemeinsamen Teiler g' von a und b gilt $g' \mid g$. **DEF** ggT, kgV

Analog nennen wir $k \in R$ ein *kleinstes gemeinsames Vielfaches* (kurz: kgV) von a und b und schreiben $k \sim \mathrm{kgV}(a, b)$, wenn $a \mid k$ und $b \mid k$ gilt und für jedes $k' \in R$ mit $a \mid k'$ und $b \mid k'$ auch $k \mid k'$ gilt. ♢

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

Die Schreibweise mit dem Assoziiertheitssymbol erklärt sich aus dem folgenden Lemma.

2.10. **Lemma.** *Seien R ein Integritätsbereich und $a, b \in R$. Ist $g \in R$ ein ggT von a und b, dann gilt für $g' \in R$: g' ist ein ggT von a und b genau dann, wenn $g \sim g'$ ist. Die analoge Aussage gilt für kleinste gemeinsame Vielfache.* **LEMMA** ggT, kgV bis auf Ass. bestimmt

Beweis. Ist g' ein ggT von a und b, dann folgt aus der Definition von „ggT“, dass $g \mid g'$ und $g' \mid g$ gilt; damit sind g und g' assoziiert. Die Umkehrung folgt daraus, dass es für die Teilbarkeit nur auf die Assoziiertheitsklasse ankommt. ❑

Größte gemeinsame Teiler und kleinste gemeinsame Vielfache sind also nur bis auf Assoziiertheit bestimmt. Es ist also im Allgemeinen nicht sinnvoll, von „dem“ ggT oder kgV zu sprechen. In manchen Ringen kann man aber auf natürliche Weise

einen Repräsentanten einer Assoziiertheitsklasse auszeichnen. In diesem Fall kann man das Symbol „ggT(a,b)“ (oder „kgV(a,b)“) als diesen Repräsentanten der Klasse aller größten gemeinsamen Teiler (oder kleinsten gemeinsamen Vielfachen) definieren (wenn sie existieren). Im Ring der ganzen Zahlen wählt man dafür den nicht-negativen Vertreter der Klasse. Man hat dann also etwa

$$\mathrm{ggT}(12,18) = 6 \qquad \text{und} \qquad \mathrm{kgV}(12,18) = 36\,.$$

Wenn ein solches Repräsentantensystem nicht ausgezeichnet ist, dann bedeutet „ggT(a,b)“ (und analog „kgV(a,b)“) einen beliebigen ggT (bzw. ein beliebiges kgV) von a und b.

Eine wichtige Eigenschaft, die so ein „natürliches“ Repräsentantensystem der Assoziiertheitsklassen haben sollte, ist die Abgeschlossenheit unter Multiplikation: Aus $a \sim a'$ und $b \sim b'$ folgt $ab \sim a'b'$; wenn a und b die ausgewählten Vertreter ihrer Klassen sind, dann sollte das auch für ab gelten. Die nicht-negativen ganzen Zahlen erfüllen diese Bedingung.

Wir haben gesehen, inwieweit ein ggT oder kgV eindeutig bestimmt ist. Es bleibt die Frage, ob so ein ggT (oder kgV) stets existiert. Bevor wir an einem Beispiel sehen werden, dass das nicht so sein muss, beweisen wir noch einige Eigenschaften.

LEMMA
Eigenschaften des ggT

2.11. **Lemma.** *Seien R ein Integritätsbereich und $a, b, c \in R$.*

(1) *Existiert* $\mathrm{ggT}(a,b)$*, dann existiert auch* $\mathrm{ggT}(b,a)$*, und es gilt*
$$\mathrm{ggT}(a,b) \sim \mathrm{ggT}(b,a)\,.$$

(2) $a \sim \mathrm{ggT}(a,0)$ *und* $1 \sim \mathrm{ggT}(a,1)$.

(3) *Existiert* $\mathrm{ggT}(a,b)$*, dann existiert auch* $\mathrm{ggT}(a,b+ac)$*, und es gilt*
$$\mathrm{ggT}(a,b) \sim \mathrm{ggT}(a,b+ac)\,.$$

Beweis.

(1) Das folgt unmittelbar aus der Definition.

(2) $a \mid a$ und $a \mid 0$; jeder gemeinsame Teiler von a und 0 ist ein Teiler von a. $1 \mid a$ und $1 \mid 1$; jeder gemeinsame Teiler von a und 1 ist eine Einheit.

(3) Sei $g \sim \mathrm{ggT}(a,b)$, dann gilt $g \mid a$ und $g \mid b$ und damit auch $g \mid b+ac$. Ist g' ein weiterer gemeinsamer Teiler von a und $b+ac$, dann teilt g' auch $b = (b+ac) - ac$ und damit den ggT g von a und b. Das zeigt, dass g ein ggT von a und $b+ac$ ist. ❑

BSP
kein ggT

2.12. **Beispiel.** Wir betrachten den Ring

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}\,;$$

die Addition und Multiplikation sind die von $\mathbb{C}$ (mit $\sqrt{-5} = \sqrt{5}\boldsymbol{i}$), also konkret

$$(a + b\sqrt{-5}) + (a' + b'\sqrt{-5}) = (a+a') + (b+b')\sqrt{-5} \qquad \text{und}$$
$$(a + b\sqrt{-5}) \cdot (a' + b'\sqrt{-5}) = (aa' - 5bb') + (ab' + ba')\sqrt{-5}\,.$$

Als Unterring des Körpers $\mathbb{C}$ (der Begriff „Unterring“ wird später eingeführt) ist R ein Integritätsbereich. Wir schreiben

$$N(a + b\sqrt{-5}) = |a + b\sqrt{-5}|^2 = a^2 + 5b^2 \in \mathbb{Z}\,;$$

für Elemente $\alpha, \beta \in R$ gilt dann $N(\alpha\beta) = N(\alpha)N(\beta)$. Ist also α ein Teiler von β in R, dann ist $N(\alpha)$ ein Teiler von $N(\beta)$ in $\mathbb{Z}$ (aber nicht unbedingt umgekehrt). Daraus schließt man leicht, dass R nur die Einheiten ± 1 hat. Ebenso sieht man, dass 6 in R genau die Teiler

$$\pm 1, \pm 2, \pm 3, \pm(1+\sqrt{-5}), \pm(1-\sqrt{-5}), \pm 6$$

hat, während $3+3\sqrt{-5}$ genau die Teiler

$$\pm 1, \pm 3, \pm(1+\sqrt{-5}), \pm(1-\sqrt{-5}), \pm(2-\sqrt{-5}), \pm(3+3\sqrt{-5})$$

hat. Es sind also zum Beispiel 3 und $1+\sqrt{-5}$ gemeinsame Teiler, aber es gilt weder $3 \mid 1+\sqrt{-5}$ noch $1+\sqrt{-5} \mid 3$, wie man leicht an $N(3) = 9$ und $N(1+\sqrt{-5}) = 6$ sehen kann, und es gibt auch keine „größeren“ gemeinsamen Teiler d, die also sowohl von 3 als auch von $1+\sqrt{-5}$ geteilt werden. Das bedeutet, dass 6 und $3+3\sqrt{-5}$ in R keinen größten gemeinsamen Teiler haben. ♣

Ein Integritätsbereich R muss also zusätzliche Eigenschaften haben, damit stets größte gemeinsame Teiler existieren. Wie Sie sich sicher aus der Schule erinnern, gibt es zu zwei ganzen Zahlen stets den ggT in $\mathbb{Z}$. Was hat der Ring $\mathbb{Z}$, was der Ring $\mathbb{Z}[\sqrt{-5}]$ aus dem Beispiel nicht hat?

Es genügt offenbar, die Existenz des ggT für natürliche Zahlen zu zeigen. Dafür kann man Induktion verwenden: Man führt die Existenz von $\mathrm{ggT}(a,b)$ auf die Existenz des ggT von kleineren Zahlen zurück. Dafür benutzen wir, dass es im Ring $\mathbb{Z}$ die *Division mit Rest* gibt.

LEMMA Division mit Rest in $\mathbb{Z}$

2.13. **Lemma.** *Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gibt es (sogar eindeutig bestimmte) ganze Zahlen q („Quotient“) und r („Rest“) mit*

$$a = qb + r \qquad \textit{und} \qquad 0 \leq r < |b|\,.$$

Beweis. Wir betrachten zunächst $b > 0$ als fest und zeigen die Aussage durch Induktion nach $|a|$. Für $0 \leq a < b$ können wir $q = 0$ und $r = a$ nehmen. Ist $-b < a < 0$, dann nehmen wir $q = -1$ und $r = b + a$. Ist $|a| \geq b$, dann sei, falls $a > 0$ ist, $a' = a - b$, sonst $a' = a + b$; in jedem Fall ist $|a'| = |a| - b < |a|$, also gibt es nach Induktionsannahme $q', r \in \mathbb{Z}$ mit $a' = q'b + r$ und $0 \leq r < b$. Dann gilt aber auch

$$a = (q'+1)b + r \quad (\text{falls } a > 0), \qquad \text{bzw.} \qquad a = (q'-1)b + r \quad (\text{falls } a < 0).$$

Ist $b < 0$, dann gibt es nach dem gerade Gezeigten $q', r \in \mathbb{Z}$ mit $a = q'(-b) + r$ und $0 \leq r < -b = |b|$. Dann gilt $a = (-q')b + r$. Das zeigt die Existenz. Für die Eindeutigkeit nehmen wir an, dass $q', r' \in \mathbb{Z}$ ebenfalls $a = q'b + r'$, $0 \leq r' < |b|$ erfüllen. Dann folgt durch Gleichsetzen und Umordnen $(q - q')b = r' - r$; es gilt also $b \mid r' - r$ und $|r' - r| < |b|$, woraus $r' = r$ und dann $q = q'$ folgt. ❑

Damit und mit der Eigenschaft (3) aus Lemma 2.11 folgt die Existenz von größten gemeinsamen Teilern in $\mathbb{Z}$ relativ leicht.

SATZ Existenz des ggT in $\mathbb{Z}$

2.14. **Satz.** *Seien $a, b \in \mathbb{Z}$. Dann existiert der größte gemeinsame Teiler* $\mathrm{ggT}(a, b)$ *von a und b in $\mathbb{Z}$.*

Beweis. Induktion nach $|b|$. Genauer zeigen wir die Aussage „für alle $a \in \mathbb{Z}$ existiert $\mathrm{ggT}(a, b)$“ durch Induktion nach $|b|$. Im Fall $b = 0$ ist $|a| = \mathrm{ggT}(a, b) = \mathrm{ggT}(a, 0)$ (genauer ist a *ein* ggT; nach unserer Konvention ist dann $|a|$ *der* ggT). Ist $b \neq 0$, dann schreiben wir $a = qb + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < |b|$. Nach Induktionsannahme existiert $\mathrm{ggT}(b, r)$. Nach Lemma 2.11 existiert dann auch $\mathrm{ggT}(b, r + qb) = \mathrm{ggT}(b, a) = \mathrm{ggT}(a, b)$ (und stimmt mit $\mathrm{ggT}(b, r)$ überein). ❑

Aus dem Beweis ergibt sich unmittelbar der *Euklidische Algorithmus* zur Berechnung des größten gemeinsamen Teilers von a und b:

(1) Setze $a_0 := |a|$, $a_1 := |b|$ und $n := 1$.

(2) Solange $a_n \neq 0$ ist, setze $a_{n+1} :=$ Rest bei der Division von a_{n-1} durch a_n und dann $n := n + 1$.

(3) (Jetzt ist $a_n = 0$). Gib a_{n-1} aus.

BSP Berechnung des ggT

2.15. **Beispiel.** Wir berechnen den größten gemeinsamen Teiler von 345 und 567. Die Rechnung verläuft entsprechend der folgenden Tabelle:

n	0	1	2	3	4	5	6	7	8
a_n	345	567	345	222	123	99	24	3	0

Das Ergebnis ist $\mathrm{ggT}(345, 567) = 3$. ♣

Da im Algorithmus $a_1 > a_2 > a_3 > \ldots > a_{n-1} > a_n = 0$ gilt, muss man nach spätestens $|b| = a_1$ Schritten zum Ende kommen. Tatsächlich ist das Verfahren noch viel effizienter: Die Anzahl der Schleifendurchläufe kann durch ein Vielfaches von $\log |b|$ beschränkt werden (Übung).

Die beste Konstante C in einer oberen Schranke der Form $C \log |b| + C'$ für die Anzahl der Schleifendurchläufe im Euklidischen Algorithmus ist $C = 1/\log \phi = 2,078\ldots$, wobei $\phi = (1 + \sqrt{5})/2 = 1,618\ldots$ das Verhältnis des Goldenen Schnitts ist. Der Grund dafür liegt darin, dass aufeinander folgende Fibonacci-Zahlen den „worst case“ bilden; die Fibonacci-Zahlen F_n wachsen wie ϕ^n.

Wie kann man diesen Beweis der Existenz von ggTs verallgemeinern? Dazu brauchen wir eine geeignete Verallgemeinerung der Division mit Rest. Wichtig für den Beweis war, dass der Rest r „kleiner“ ist als der Divisor b, sodass wir Induktion verwenden konnten. Dafür muss die „Größe“ des Restes durch eine natürliche Zahl (in unserem Fall ist das $|r|$) gegeben sein. Das führt auf folgende Definition.

DEF euklidischer Ring

* 2.16. **Definition.** Sei R ein Integritätsbereich. Eine *euklidische Normfunktion* auf R ist eine Abbildung $N : R \to \mathbb{Z}_{\geq 0}$ mit folgenden Eigenschaften:

(1) $N(r) = 0 \iff r = 0$.

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

R heißt *euklidischer Ring*, wenn es eine euklidische Normfunktion auf R gibt. ♢

2.17. **Beispiel.** Die Abbildung $\mathbb{Z} \to \mathbb{Z}_{\geq 0}$, $a \mapsto |a|$, ist eine euklidische Normfunktion auf $\mathbb{Z}$; damit ist $\mathbb{Z}$ ein euklidischer Ring. ♣

BSP euklidischer Ring

Häufig wird der Begriff der euklidischen Normfunktion ein wenig anders definiert, nämlich als Abbildung $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$, sodass es für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ gibt mit $a = qb + r$ und entweder $r = 0$ oder $N(r) < N(b)$. Beide Versionen führen zum selben Begriff „euklidischer Ring“; manchmal ist die eine und manchmal die andere praktischer.

In der Definition wird nur die *Existenz* geeigneter Quotienten q und Reste r gefordert; *Eindeutigkeit* wird nicht verlangt.

Wir erhalten mit im Wesentlichen demselben Beweis wie für Satz 2.14 nun folgenden Satz:

2.18. **Satz.** *Sei R ein euklidischer Ring. Dann existiert zu je zwei Elementen $a, b \in R$ stets ein größter gemeinsamer Teiler von a und b in R.*

SATZ Existenz des ggT in euklidischen Ringen

Beweis. Sei $N : R \to \mathbb{Z}_{\geq 0}$ eine euklidische Normfunktion. Wir beweisen den Satz durch Induktion über $N(b)$. Im Fall $N(b) = 0$ ist $b = 0$, und a ist ein ggT. Anderenfalls gibt es $q, r \in R$ mit $a = qb + r$ und $N(r) < N(b)$. Nach Induktionsannahme existiert dann ein ggT g von b und r; wie im Beweis von Satz 2.14 folgt dann $g \sim \mathrm{ggT}(a, b)$. ❑

Ganz genauso wie in $\mathbb{Z}$ kann ein ggT in einem euklidischen Ring durch den Euklidischen Algorithmus bestimmt werden (daher auch der Name „euklidischer Ring“).

2.19. **Beispiel.** Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ aus Beispiel 2.12 ist ein Integritätsbereich, der kein euklidischer Ring ist. Denn sonst müssten je zwei Elemente einen ggT haben, was aber, wie wir gesehen haben, nicht der Fall ist. ♣

BSP nicht euklidischer Int.bereich

3. Unterringe, Ideale und Hauptidealringe

In diesem Abschnitt werden wir uns Ringe genauer anschauen. So wie es in Vektorräumen V Untervektorräume gibt, also Teilmengen, die mit den (eingeschränkten) Verknüpfungen von V selbst Vektorräume sind, gibt es auch in Ringen Unterstrukturen. Bei Ringen unterscheidet man aber zwei verschiedene Arten von Unterstrukturen: Unterringe und Ideale. Es wird sich herausstellen, dass die Bilder von Ringhomomorphismen (die wir später einführen werden) Unterringe und die Kerne Ideale sind.

Zuerst aber noch eine allgemeine Konstruktion von Ringen (analog zu Vektorräumen).

3.1. **Beispiel.** **BSP** Produktring

(1) Sind $R_1, R_2, \ldots, R_n$ Ringe, dann ist auch $R_1 \times R_2 \times \ldots \times R_n$ mit komponentenweise definierten Verknüpfungen ein Ring.

(2) Ist R ein Ring und X eine Menge, dann ist $R^X = \mathrm{Abb}(X, R)$ ein Ring mit punktweise definierten Verknüpfungen, also

$$(r_x)_{x\in X} + (r'_x)_{x\in X} = (r_x + r'_x)_{x\in X} \quad \text{und} \quad (r_x)_{x\in X} \cdot (r'_x)_{x\in X} = (r_x \cdot r'_x)_{x\in X}$$

bzw. (in Abbildungs-Schreibweise)

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

Zum Beispiel hat man den Ring $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ der reellen Funktionen (hier ist $X = \mathbb{R} = R$ sowohl die Menge als auch der Ring) oder den Ring $\mathbb{Q}^{\mathbb{N}}$ der Folgen rationaler Zahlen. ♣

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

Es ist leicht zu sehen, dass in diesem Fall $(S, +|_{S\times S}, 0, -|_S, \cdot|_{S\times S}, 1)$ ebenfalls ein Ring ist: Da alle Axiome die Form „für alle ...“ haben, gelten sie auch für die Elemente von S, solange alle Verknüpfungen definiert sind.

3.3. **Beispiele.** **BSP** Unterringe

(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 (mit punktweiser Addition und Multiplikation): Wir wissen aus der Analysis, dass Summe, Negation und Produkt stetiger Funktionen wieder stetig sind.

(4) Sei R ein Ring. Dann ist $R \times R$ ein Ring wie in Beispiel 3.1. 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.

(5) Im Ring $\mathbb{Q}^{\mathbb{N}}$ der Folgen rationaler Zahlen bilden die beschränkten Folgen und die Cauchy-Folgen Unterringe B und C (Übung). ♣

Für Integritätsringe bzw. -bereiche gilt dann Folgendes:

3.4. **Lemma.** *Ein Unterring eines Integritätsrings/bereichs ist wieder ein Integritätsring/bereich. Insbesondere ist jeder Unterring eines Körpers ein Integritätsbereich.*

LEMMA Unterringe von Int.ber.

Beweis. Sei S ein Unterring von R. Wenn $s \in S$ ein Nullteiler in S ist, dann auch in R. Es folgt, dass jeder Unterring eines Integritätsrings wieder ein Integritätsring ist. Da klar ist, dass Unterringe von kommutativen Ringen wieder kommutativ sind, folgt die entsprechende Aussage über Integritätsbereiche. Die letzte Aussage folgt daraus, dass jeder Körper ein Integritätsbereich ist. ❑

Tatsächlich gilt von der letzten Aussage auch eine Art Umkehrung: Jeder Integritätsbereich lässt sich als Unterring eines Körpers auffassen (so wie $\mathbb{Z} \subset \mathbb{Q}$). Das werden wir später in dieser Vorlesung sehen.

Analog wie für Untervektorräume gilt:

3.5. **Lemma.** *Sei R ein Ring.*

LEMMA Durchschnitt und aufst. Vereinigung von Unterringen

(1) *Ist $(R_i)_{i\in I}$ eine Familie von Unterringen von R mit $I \neq \emptyset$, dann ist auch der Durchschnitt $\bigcap_{i\in I} R_i$ wieder ein Unterring von R.*
(2) *Ist $(R_n)_{n\in\mathbb{N}}$ eine aufsteigende Folge (also mit $R_n \subset R_{n+1}$ für alle $n \in \mathbb{N}$) von Unterringen von R, dann ist auch die Vereinigung $\bigcup_{n\in\mathbb{N}} R_n$ wieder ein Unterring von R.*

Beweis.

(1) Sei $S = \bigcap_{i\in I} R_i$; es ist zu zeigen, dass S ein Unterring von R ist. Dazu müssen wir die Bedingungen aus der Definition nachprüfen. Da R_i für alle $i \in I$ ein Unterring ist, gilt $0, 1 \in R_i$ für alle i und damit auch $0, 1 \in S$. Seien $s, s' \in S$. Dann folgt $s, s' \in R_i$ für alle i; da R_i ein Unterring ist, folgt daraus $s + s', s \cdot s' \in R_i$ für alle i, also $s + s', s \cdot s' \in S$. Analog sieht man $-s \in S$.
(2) Sei jetzt $S = \bigcup_{n\in\mathbb{N}} R_n$. Es gilt $0, 1 \in R_0 \subset S$. Ist $s \in S$, dann gibt es $n \in \mathbb{N}$ mit $s \in R_n$; es folgt $-s \in R_n \subset S$. Sind $s, s' \in S$, dann gibt es $m, m' \in \mathbb{N}$ mit $s \in R_m$, $s' \in R_{m'}$. Sei $n = \max\{m, m'\}$, dann folgt (da die Folge der R_n aufsteigend ist) $R_m \subset R_n$, $R_{m'} \subset R_n$, also $s, s' \in R_n$. Weil R_n ein Unterring ist, haben wir dann auch $s + s', s \cdot s' \in R_n \subset S$. ❑

Beliebige Vereinigungen von Unterringen sind im Allgemeinen keine Unterringe.

Die erste Aussage in Lemma 3.5 zeigt, dass folgende Definition sinnvoll ist.

3.6. **Definition.** Seien R ein Ring, $R' \subset R$ ein Unterring und $A \subset R$ eine Teilmenge. Dann existiert der kleinste Unterring von R, der R' und A enthält (als Durchschnitt *aller* solcher Unterringe); wir schreiben dafür $R'[A]$ und nennen ihn den *von A über R' erzeugten Unterring von R*. Ist $A = \{a_1, a_2, \ldots, a_n\}$ endlich, dann schreiben wir auch $R'[a_1, a_2, \ldots, a_n]$ für $R'[A]$. ♢

DEF $R'[A] \subset R$

Das erklärt die Schreibweise $\mathbb{Z}[\sqrt{-5}]$, die wir bereits benutzt haben: Dieser Ring ist der von $\sqrt{-5}$ über $\mathbb{Z}$ erzeugte Unterring von $\mathbb{C}$ (denn es ist ein Unterring von $\mathbb{C}$,

und jeder Unterring von $\mathbb{C}$, der $\mathbb{Z}$ und $\sqrt{-5}$ enthält, muss alle Elemente $a+b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$ enthalten).

Mit $\sqrt{-2} = \sqrt{2}\boldsymbol{i}$ sind analog $\mathbb{Z}[\boldsymbol{i}]$ und $\mathbb{Z}[\sqrt{-2}]$ Unterringe von $\mathbb{C}$; ihre Vereinigung ist aber *kein* Unterring, da sie nicht unter der Addition abgeschlossen ist: $\boldsymbol{i} + \sqrt{2}\boldsymbol{i}$ ist weder in $\mathbb{Z}[\boldsymbol{i}]$ noch in $\mathbb{Z}[\sqrt{-2}]$ enthalten.

Achtung: Es gilt nicht immer (für $\alpha \in \mathbb{C}$), dass

$$\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$$

ist (das gilt nur dann, wenn $\alpha^2 = c + d\alpha$ ist mit geeigneten $c, d \in \mathbb{Z}$). Zum Beispiel ist

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \mid a, b, c \in \mathbb{Z}\}$$

(Übung).

Als nächstes wollen wir die Ideale einführen.

* 3.7. **Definition.** Sei R ein kommutativer Ring. Ein *Ideal* von R ist eine Teilmenge $I \subset R$ mit $0 \in I$, die unter der Addition abgeschlossen ist, und sodass für alle $r \in R$ und $a \in I$ auch $ra \in I$ gilt. ♢ **DEF** Ideal

In nicht-kommutativen Ringen muss man zwischen *Links-* und *Rechtsidealen* unterscheiden (je nachdem, ob man $ra \in I$ oder $ar \in I$ fordert); ein *Ideal* ist dann sowohl ein Links- als auch ein Rechtsideal.

Ein Ideal I ist auch unter der Negation abgeschlossen, denn $-a = (-1) \cdot a$. Außerdem ist I unter der Multiplikation abgeschlossen. Der Unterschied zum Unterring ist, dass *nicht* gefordert wird, dass $1 \in I$ ist, dafür aber *jedes* Vielfache (mit beliebigen Faktoren aus R) eines Elements von I wieder in I ist. Insofern ist die Definition formal wie die von Untervektorräumen, wobei der Ring R selbst die Rolle des Skalarkörpers spielt.

Tatsächlich kann man den Begriff „K-Vektorraum“ verallgemeinern zum Begriff „R-Modul“ (betont auf dem „Mo“) mit derselben Definition, nur dass R ein beliebiger Ring sein darf und nicht unbedingt ein Körper sein muss. Dann ist ein Ideal nichts anderes als ein Untermodul des R-Moduls R.

Da die Struktur von Ringen komplizierter ist als die von Körpern, ist die Theorie der R-Moduln auch komplizierter als die klassische lineare Algebra über Körpern. Zum Beispiel hat nicht jeder endlich erzeugte Modul eine Basis.

3.8. **Beispiele.** Sei R ein kommutativer Ring. **BSP** Ideale

(1) In jedem Ring gibt es die Ideale $\{0\}$ (das *Nullideal*) und R.

(2) Für $a \in R$ ist die Menge $Ra = \{ra \mid r \in R\}$ ein Ideal:

$$0a = 0, \quad ra + r'a = (r + r')a, \quad r'(ra) = (r'r)a\,.$$

(3) Im Ring $R \times R$ sind $R \times \{0\}$ und $\{0\} \times R$ Ideale.

(4) Im Ring $C \subset \mathbb{Q}^{\mathbb{N}}$ der Cauchy-Folgen bilden die Nullfolgen ein Ideal N (Übung). ♣

Wie für Unterringe auch haben wir die folgenden Eigenschaften:

LEMMA Durchschnitt und aufst. Vereinigung von Idealen

3.9. **Lemma.** *Sei R ein kommutativer Ring.*

(1) *Ist $(I_j)_{j\in J}$ eine Familie von Idealen von R mit $J \neq \emptyset$, dann ist auch der Durchschnitt $\bigcap_{j\in J} I_j$ wieder ein Ideal von R.*

(2) *Ist $(I_n)_{n\in\mathbb{N}}$ eine aufsteigende Folge (also mit $I_n \subset I_{n+1}$ für alle $n \in \mathbb{N}$) von Idealen von R, dann ist auch die Vereinigung $\bigcup_{n\in\mathbb{N}} I_n$ wieder ein Ideal von R.*

Beweis. Ganz analog wie für Lemma 3.5. ❑

Die erste Aussage in Lemma 3.9 zeigt (analog wie für Unterringe), dass folgende Definition sinnvoll ist.

DEF $\langle A\rangle_R \subset R$ Hauptideal Hauptidealring

3.10. **Definition.** Seien R ein kommutativer Ring und $A \subset R$ eine Teilmenge. Dann existiert das kleinste Ideal von R, das A enthält (als Durchschnitt *aller* solcher Ideale); wir schreiben dafür $\langle A\rangle_R$ (oder auch $\langle A\rangle$, wenn keine Verwechslung möglich ist) und nennen es das *von A erzeugte Ideal von R*. Ist $A = \{a_1, a_2, \ldots, a_n\}$ endlich, dann schreiben wir auch $\langle a_1, a_2, \ldots, a_n\rangle_R$ für $\langle A\rangle_R$. In diesem Fall heißt das Ideal *endlich erzeugt*.

Ein Ideal $I \subset R$ heißt *Hauptideal*, wenn es von einem Element erzeugt wird: $I = \langle a\rangle_R$ mit einem $a \in R$.

Ein Integritätsbereich R, in dem jedes Ideal ein Hauptideal ist, heißt ein *Hauptidealring* (bisweilen kurz HIR). ♢

Wie für Untervektorräume gilt auch für Ideale, dass ihre Elemente genau die (R-)Linearkombinationen der Erzeuger sind. Wir formulieren und beweisen das hier der Einfachheit halber nur für endlich viele Erzeuger.

LEMMA Linearkombinationen

3.11. **Lemma.** *Seien R ein kommutativer Ring und $a_1, a_2, \ldots, a_n \in R$. Dann gilt*

$$\langle a_1, a_2, \ldots, a_n\rangle_R = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_1, r_2, \ldots, r_n \in R\}\,.$$

Die Elemente von $\langle a_1, a_2, \ldots, a_n\rangle_R$ sind also gerade die Linearkombinationen der Erzeuger $a_1, a_2, \ldots, a_n$ mit Koeffizienten aus R.

Man schreibt deshalb auch $Ra_1 + Ra_2 + \ldots + Ra_n$ (oder $a_1R + a_2R + \ldots + a_nR$) für $\langle a_1, a_2, \ldots, a_n\rangle_R$. Für ein Hauptideal gilt demnach

$$\langle a\rangle_R = Ra = \{ra \mid r \in R\}\,.$$

Beweis. Sei $I = \langle a_1, a_2, \ldots, a_n\rangle_R$.

„$\supset$“: Da $a_1, a_2, \ldots, a_n \in I$ sind, folgt $r_1a_1, r_2a_2, \ldots, r_na_n \in I$ und damit auch $r_1a_1 + r_2a_2 + \ldots + r_na_n \in I$.

„$\subset$“: Die Menge auf der rechten Seite ist ein Ideal, denn

$$\begin{aligned} 0a_1 + 0a_2 + \ldots + 0a_n &= 0\,,\\ (r_1a_1 + r_2a_2 + \ldots + r_na_n) + (r'_1a_1 + r'_2a_2 + \ldots + r'_na_n)&\\ = (r_1 + r'_1)a_1 + (r_2 + r'_2)a_2 + \ldots + (r_n + r'_n)a_n &\quad \text{und}\\ r'(r_1a_1 + r_2a_2 + \ldots + r_na_n) = (r'r_1)a_1 + (r'r_2)a_2 + \ldots + (r'r_n)a_n\,.& \end{aligned}$$

Außerdem enthält sie $a_1, a_2, \ldots, a_n$. Da nach Definition I das *kleinste* solche Ideal ist, ist I in der rechten Seite enthalten. ❑

Für den Ring der ganzen Zahlen gilt:

3.12. **Satz.** *$\mathbb{Z}$ ist ein Hauptidealring.*

SATZ
$\mathbb{Z}$ ist HIR

Beweis. Sei $I \subset \mathbb{Z}$ ein Ideal mit $I \neq \{0\}$ (anderenfalls ist $I = \langle 0\rangle$ ein Hauptideal). Da mit a auch stets $-a = (-1)a$ in I liegt, hat I ein kleinstes positives Element n. Ich behaupte, dass $I = \langle n\rangle = n\mathbb{Z}$ ist. Sei dazu $a \in I$. Dann gibt es $q, r \in \mathbb{Z}$ mit $a = qn + r$ und $0 \leq r < n$. Es folgt, dass $r = a - qn \in I$ ist. Wäre $r \neq 0$, dann wäre r ein positives Element von I, das kleiner als n ist, ein Widerspruch. Also ist $r = 0$ und damit $a = qn \in n\mathbb{Z}$. ❑

Man sieht, dass hier wieder wesentlich die Division mit Rest eingeht. Es ist daher nicht überraschend, dass folgende Verallgemeinerung möglich ist:

* 3.13. **Satz.** *Ist R ein euklidischer Ring, dann ist R ein Hauptidealring.*

SATZ
eukl. Ring ist HIR

Beweis. Sei $I \subset R$ ein Ideal. Das Nullideal ist stets ein Hauptideal, also können wir $I \neq \{0\}$ annehmen. Sei N eine euklidische Normfunktion auf R und

$$n = \min\{N(r) \mid r \in I \setminus \{0\}\} > 0\,.$$

Sei $b \in I$ mit $N(b) = n$. Sei weiter $a \in I$ beliebig; wir müssen $a \in Rb$ zeigen. Da R euklidisch ist, gibt es $q, r \in R$ mit $a = qb + r$ und $N(r) < N(b) = n$. Wie eben folgt, dass $r \in I$ ist. Wäre $r \neq 0$, dann ergäbe sich ein Widerspruch zur Definition von n, also ist $r = 0$ und damit $a = qb \in Rb$. ❑

3.14. **Beispiel.** Der nicht euklidische Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist auch kein Hauptidealring. Tatsächlich ist das Ideal $I = \langle 2, 1 + \sqrt{-5}\rangle_R$ kein Hauptideal: Wäre $I = \langle\alpha\rangle_R$, dann müsste α ein gemeinsamer Teiler von 2 und $1 + \sqrt{-5}$ sein. Die einzigen gemeinsamen Teiler sind aber ± 1. Das Ideal $\langle 1\rangle_R$ ist aber ganz R und damit $\neq I$, denn $1 \notin I$ — für jedes $a + b\sqrt{-5} \in I$ gilt, dass $a + b$ gerade ist, wie man leicht nachprüft. ♣

BSP
kein HIR

Die Umkehrung von Satz 3.13 ist *falsch:* Es gibt Hauptidealringe, die nicht euklidisch sind. Ein Beispiel dafür ist der Ring $R = \mathbb{Z}[\alpha] \subset \mathbb{C}$ mit $\alpha = (1 + \sqrt{-19})/2$ (dann gilt $\alpha^2 = \alpha - 5$). Der Beweis ist allerdings nicht ganz einfach.

Dass R nicht euklidisch ist, kann man wie in der Bonus-Aufgabe auf dem zweiten Übungsblatt zeigen. Schwieriger ist der Beweis dafür, dass R ein Hauptidealring ist. Man kann dafür einen Satz aus der algebraischen Zahlentheorie verwenden (die unter anderem solche Ringe studiert), der in diesem Fall besagt, dass man nur nachprüfen muss, dass alle Ideale $I \neq \{0\}$ mit „Norm“

$$N(I) = \mathrm{ggT}\{|\gamma|^2 \mid \gamma \in I\} \leq 12$$

Hauptideale sind. Es gibt nur endlich viele solcher Ideale; man kann sie aufzählen und die Bedingung prüfen. Übrigens lässt sich auch zeigen, dass die Aussage daraus folgt, dass die ersten paar Werte des Polynoms $x^2 + x + 5$ für $x = 0, 1, 2, \ldots$ alles Primzahlen sind. (Vielleicht kennen Sie das Polynom $x^2 + x + 41$, das auf diese Weise sehr viele Primzahlen liefert. Das hat damit zu tun, dass der Ring $\mathbb{Z}\big[(1+\sqrt{-163})/2\big]$ ebenfalls ein Hauptidealring ist. Letzteres ist übrigens auch dafür verantwortlich, dass $e^{\pi\sqrt{163}}$ beinahe eine ganze Zahl ist.)

Auch in Hauptidealringen existieren größte gemeinsame Teiler. Bevor wir das beweisen, übersetzen wir die Teilbarkeitsrelation in die Sprache der Ideale.

LEMMA Ideale und Teilbarkeit

3.15. **Lemma.** *Sei R ein Integritätsbereich und seien $a, b \in R$. Dann gilt*

$$a \mid b \iff b \in \langle a \rangle_R \iff \langle b \rangle_R \subset \langle a \rangle_R .$$

Insbesondere sind a und b assoziiert genau dann, wenn sie dasselbe Hauptideal erzeugen.

Beweis. Es gilt

$$a \mid b \iff \exists r \in R : b = ra \iff b \in \langle a \rangle_R \iff \langle b \rangle_R \subset \langle a \rangle_R ;$$

die nicht völlig offensichtliche Richtung in der letzten Äquivalenz ergibt sich daraus, dass $\langle b \rangle_R$ das kleinste Ideal ist, das b enthält.

Der Zusatz folgt aus $a \sim b \iff a \mid b \wedge b \mid a$. ❑

SATZ ggT in HIR

∗ 3.16. **Satz.** *Sei R ein Hauptidealring. Dann haben je zwei Elemente $a, b \in R$ einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches in R. Genauer gilt für $r \in R$:*

$$r \sim \mathrm{ggT}(a, b) \iff \langle a, b \rangle_R = \langle r \rangle_R$$
$$r \sim \mathrm{kgV}(a, b) \iff \langle a \rangle_R \cap \langle b \rangle_R = \langle r \rangle_R$$

Beweis. Es genügt, die zweite Aussage („Genauer gilt ...“) zu zeigen, denn nach Voraussetzung ist jedes Ideal von einem Element erzeugbar, also gibt es Elemente r wie angegeben.

Nach Lemma 3.15 ist r ein gemeinsamer Teiler von a und b genau dann, wenn $a, b \in \langle r \rangle_R$ gilt, was mit $\langle a, b \rangle_R \subset \langle r \rangle_R$ gleichbedeutend ist. r ist ein ggT genau dann, wenn $\langle r \rangle_R$ das kleinste $\langle a, b \rangle_R$ umfassende Hauptideal ist. Da $\langle a, b \rangle_R$ selbst ein Hauptideal ist, muss $\langle a, b \rangle_R = \langle r \rangle_R$ sein.

Für das kgV gilt entsprechend, dass $\langle r \rangle_R$ das größte Hauptideal sein muss, das in $\langle a \rangle_R \cap \langle b \rangle_R$ enthalten ist. Auch $\langle a \rangle_R \cap \langle b \rangle_R$ ist ein Hauptideal, also muss auch hier Gleichheit gelten. ❑

FOLG ggT ist Linearkomb.

∗ 3.17. **Folgerung.** *Seien R ein Hauptidealring, $a, b \in R$ und $g \in R$ ein größter gemeinsamer Teiler von a und b. Dann gibt es $u, v \in R$ mit*

$$g = ua + vb .$$

Beweis. Nach Satz 3.16 gilt $Ra + Rb = Rg \ni g$, also ist g eine Linearkombination von a und b wie angegeben. ❑

In einem *euklidischen* Ring kann man Elemente u und v wie oben durch eine Erweiterung des Euklidischen Algorithmus berechnen. Sei N eine euklidische Normfunktion auf R und seien $a, b \in R$.

(1) Setze $(a_0, u_0, v_0) := (a, 1, 0)$, $(a_1, u_1, v_1) := (b, 0, 1)$ und $n := 1$.

(2) Solange $a_n \neq 0$ ist, schreibe $a_{n-1} = q_n a_n + a_{n+1}$ mit $N(a_{n+1}) < N(a_n)$; setze $(u_{n+1}, v_{n+1}) := (u_{n-1} - q_n u_n, v_{n-1} - q_n v_n)$ und dann $n := n + 1$.

(3) (Jetzt ist $a_n = 0$). Gib $(g, u, v) = (a_{n-1}, u_{n-1}, v_{n-1})$ aus.

Wir wissen bereits, dass $g = a_{n-1}$ ein ggT von a und b ist, und es ist leicht zu verifizieren, dass für alle n, die vorkommen, $a_n = u_n a + v_n b$ gilt. Damit ist auch $g = ua + vb$.

3.18. **Beispiel.** Wir berechnen wieder den ggT von 345 und 567 und zusätzlich eine ihn darstellende Linearkombination: **BSP** Erweiterter Eukl. Algo.

n	0	1	2	3	4	5	6	7	8
a_n	345	567	345	222	123	99	24	3	0
q_n		0	1	1	1	1	4	8	
u_n	1	0	1	-1	2	-3	5	-23	189
v_n	0	1	0	1	-1	2	-3	14	-115

Wir erhalten $-23 \cdot 345 + 14 \cdot 567 = 3$. ♣

Allgemein ist es so, dass man viele Aussagen für Hauptidealringe zeigen kann. Wenn man aber Dinge *berechnen* möchte, dann geht das effizient meist nur in euklidischen Ringen (vorausgesetzt, man hat ein effizientes Verfahren für die Division mit Rest).

* 3.19. **Definition.** Seien R ein kommutativer Ring und $a, b \in R$. Wir sagen, a und b sind *relativ* (oder *zueinander*) *prim*, wenn es $u, v \in R$ gibt mit $ua + vb = 1$, oder äquivalent, wenn $\langle a, b\rangle_R = R$ ist. In diesem Fall schreiben wir auch $a \perp b$. ♢ **DEF** relativ prim

In Hauptidealringen ist das dazu äquivalent, dass a und b *teilerfremd* sind, also $\mathrm{ggT}(a, b) \sim 1$ gilt.

Die Schreibweise $a \perp b$ ist (leider) nicht allgemein üblich, aber praktisch.

Das folgende wichtige Lemma zeigt die Nützlichkeit dieses Begriffs.

3.20. **Lemma.** *Seien R ein Integritätsbereich und $a, b, c \in R$ mit $a \perp b$. Ist a ein Teiler von bc, dann ist a auch ein Teiler von c.* **LEMMA** $a \perp b, a \mid bc \Rightarrow a \mid c$

Beweis. Nach Voraussetzung gibt es $u, v \in R$ mit $ua+vb = 1$. Multiplikation mit c liefert $c = a(uc) + v(bc)$; wegen $a \mid bc$ ist a ein Teiler der rechten Seite und damit auch von c. ❑

Auch folgende Aussage ist häufig nützlich. Dazu beachten wir, dass in einem Integritätsbereich Folgendes gilt: Ist $a \mid b$ und $a \neq 0$, dann ist c mit $b = ca$ eindeutig bestimmt. Wir schreiben dann auch b/a für c.

3.21. **Lemma.** *Seien R ein Hauptidealring und $a, b \in R$ nicht beide null. Sei weiter g ein größter gemeinsamer Teiler von a und b. Dann sind $a' = a/g$ und $b' = b/g$ relativ prim.* **LEMMA** Elemente relativ prim machen

Beweis. Unter der angegebenen Voraussetzung ist $g \neq 0$ (denn $\langle a, b\rangle_R$ ist nicht das Nullideal). Nach Folgerung 3.17 gibt es $u, v \in R$ mit $ua + vb = g$, also auch $(ua' + vb')g = g$. Da $g \neq 0$, folgt daraus (denn R ist ein Integritätsbereich) $ua' + vb' = 1$, also gilt $a' \perp b'$. ❑

Wir beenden diesen Abschnitt mit einer Aussage über kleinste gemeinsame Vielfache.

SATZ
kgV
durch ggT
in HIR

3.22. **Satz.** *Seien R ein Hauptidealring und $a, b \in R$. Dann gilt*

$$ab \sim \mathrm{ggT}(a,b)\,\mathrm{kgV}(a,b)\,.$$

Insbesondere gilt für $a \perp b$, dass $ab \sim \mathrm{kgV}(a,b)$ ist.

Beweis. Im Fall $a = 0$ oder $b = 0$ ist $\mathrm{kgV}(a,b) = 0$, sodass die Gleichung stimmt. Wir können also $a, b \neq 0$ voraussetzen. Es gelte nun zunächst $a \perp b$. Das Produkt ab ist in jedem Fall ein gemeinsames Vielfaches von a und b. Ist k irgendein gemeinsames Vielfaches, dann ist $k = ma$ mit $m \in R$; aus Lemma 3.20 folgt $b \mid m$ und damit $ab \mid k$. Also ist ab ein kgV von a und b. Im allgemeinen Fall sei $g \sim \mathrm{ggT}(a,b)$; wir setzen $a' = a/g$, $b' = b/g$. Dann gilt nach Lemma 3.21 $a' \perp b'$ und damit $a'b' \sim \mathrm{kgV}(a',b')$. Dann ist aber auch $a'b'g \sim \mathrm{kgV}(a'g, b'g) \sim \mathrm{kgV}(a,b)$ und demnach

$$ab = a'b'g^2 \sim g\,\mathrm{kgV}(a,b) \sim \mathrm{ggT}(a,b)\,\mathrm{kgV}(a,b)\,. \qquad \square$$

4. Primelemente und Faktorisierung

Wir wollen in diesem Abschnitt den Satz über die eindeutige Primzahlfaktorisierung von natürlichen Zahlen („Fundamentalsatz der Arithmetik“) beweisen und zeigen, dass die analoge Aussage in beliebigen Hauptidealringen gilt.

Wir beginnen mit einer bekannten Definition.

4.1. **Definition.** Eine *Primzahl* ist eine ganze Zahl $p > 1$, deren einzige positive Teiler 1 und p sind. ♢

DEF Primzahl

Die Zahl 1 ist laut dieser Definition keine Primzahl; der Grund dafür ist schlicht, dass das so praktischer ist: Sonst hätte man keine *eindeutige* Faktorisierung in Primzahlen, da man beliebig viele Faktoren 1 hinzufügen könnte.

4.2. **Beispiel.** Die Primzahlen unterhalb von 100 sind die folgenden 25 Zahlen:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\,.$$

♣

BSP Primzahlen bis 100

Um die *Existenz* einer Faktorisierung in Primzahlen zu zeigen, brauchen wir folgende wichtige Aussage:

4.3. **Lemma.** *Sei $n > 1$ eine natürliche Zahl. Dann gibt es eine Primzahl p mit $p \mid n$.*

So ein p heißt ein *Primteiler* von n.

LEMMA Existenz eines Primteilers

Beweis. Durch Induktion. Entweder ist $n = p$ prim (das deckt den „Induktionsanfang“ $n = 2$ ab) oder wir können $n = n_1 n_2$ schreiben mit $1 < n_1 < n$. Nach Induktionsannahme hat dann n_1 einen Primteiler p; es folgt $p \mid n$. ❑

Daraus folgt ziemlich unmittelbar:

4.4. **Lemma.** *Sei n eine positive ganze Zahl. Dann kann n als Produkt von Primzahlen geschrieben werden.*

LEMMA Existenz der Primfaktorisierung

Beweis. Durch Induktion. $n = 1$ ist das leere Produkt von Primzahlen (das leere Produkt hat den Wert 1, so wie die leere Summe den Wert 0 hat). Ist $n > 1$, dann gibt es (nach Lemma 4.3) eine Primzahl p_1 mit $n = p_1 n'$. Da $1 \leq n' < n$ ist, kann n' nach Induktionsannahme als Produkt $n' = p_2 p_3 \cdots p_k$ von Primzahlen geschrieben werden. Dann ist aber auch $n = p_1 p_2 p_3 \cdots p_k$ ein Produkt von Primzahlen. ❑

Um auch die *Eindeutigkeit* der Faktorisierung (bis auf Reihenfolge der Primfaktoren; die Multiplikation ist ja kommutativ) zeigen zu können, brauchen wir eine andere wichtige Eigenschaft von Primzahlen.

LEMMA Charakterisierung von Primzahlen

4.5. **Lemma.** *Eine natürliche Zahl $p > 1$ ist genau dann prim, wenn gilt:*

$$\forall a, b \in \mathbb{Z} : \big(p \mid ab \implies p \mid a \text{ oder } p \mid b\big) .$$

Beweis. „⇐“: Ist $p = d_1 d_2$ mit positiven ganzen Zahlen d_1 und d_2, dann folgt $p \mid d_1 d_2$; nach Voraussetzung gilt dann $p \mid d_1$ oder $p \mid d_2$. Im ersten Fall ist $d_1 = pc_1$; es folgt $p = pc_1 d_2$, also $c_1 d_2 = 1$ und damit $d_2 = 1$. Analog sieht man im zweiten Fall, dass $d_1 = 1$ ist. Damit hat p nur die Teiler 1 und p.

„⇒“: p sei eine Primzahl und es gelte $p \mid ab$ und $p \nmid a$. Wir müssen $p \mid b$ zeigen. Da p kein Teiler von a ist, muss $\mathrm{ggT}(p, a) = 1$ sein, es gilt also $p \perp a$. Nach Lemma 3.20 folgt die Behauptung. ❑

* **SATZ** Eindeutige Primfaktorisierung in $\mathbb{Z}$

4.6. **Satz.** *Sei $n > 0$ eine natürliche Zahl. Dann hat n eine bis auf die Reihenfolge der Faktoren eindeutige Darstellung als Produkt von Primzahlen.*

Beweis. Die Existenz wurde bereits in Lemma 4.4 gezeigt. Die Eindeutigkeit zeigen wir durch Induktion. Für $n = 1$ gibt es nur die Darstellung als leeres Produkt. Sei also $n > 1$ und seien $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ zwei Darstellungen von n als Produkt von Primzahlen. Wegen $n > 1$ gilt $k \geq 1$ und $l \geq 1$. Es folgt $p_1 \mid n = q_1 q_2 \cdots q_l$, also wegen Lemma 4.5 $p_1 \mid q_j$ für ein $j \in \{1, 2, \ldots, l\}$. Da q_j eine Primzahl ist und $p_1 \neq 1$, muss dann $q_j = p_1$ sein. Wir ordnen die Faktoren im zweiten Produkt um: $q_1' = q_j$, $q_j' = q_1$ und $q_i' = q_i$ für $i \neq 1, j$. Sei

$$n' = p_2 \cdots p_k = q_2' \cdots q_l' < n .$$

Nach Induktionsannahme ist die Primfaktorisierung von n' eindeutig; es folgt $l = k$ und die Existenz einer Umordnung $(q_2'', \ldots, q_k'')$ von $(q_2', \ldots, q_k')$ mit $q_i'' = p_i$ für alle $i \in \{2, 3, \ldots, k\}$. Mit $q_1'' = q_1'$ gilt dann $(p_1, p_2, \ldots, p_k) = (q_1'', q_2'', \ldots, q_k'')$; das ist die Behauptung. ❑

Für ganze Zahlen kann man das auch wie folgt formulieren. Wir schreiben $\mathbb{P}$ für die Menge der Primzahlen in $\mathbb{Z}$.

FOLG Standardform der Faktorisierung in $\mathbb{Z}$

4.7. **Folgerung.** *Für jede ganze Zahl $n \neq 0$ gibt es eindeutig bestimmte ganze Zahlen $e_p \geq 0$ für jede Primzahl p mit $e_p = 0$ für alle bis auf endlich viele p und $u \in \mathbb{Z}^\times = \{\pm 1\}$, sodass*

$$n = u \prod_{p \in \mathbb{P}} p^{e_p} .$$

Das formal unendliche Produkt ist so definiert, dass sein Wert $\prod_{p \in S} p^{e_p}$ ist, wobei $S \subset \mathbb{P}$ eine beliebige endliche Teilmenge ist, die alle p enthält mit $e_p > 0$.

Beweis. Für $n > 0$ ist das nur eine andere Formulierung von Satz 4.6: Wir fassen gleiche Faktoren zu Potenzen zusammen. In diesem Fall ist $u = 1$. Für $n < 0$ folgt es mit $u = -1$ aus dem Satz, angewandt auf $-n$. ❑

Wir wollen diese Aussage nun allgemeiner für Hauptidealringe beweisen. Dazu führen wir zwei Begriffe ein, die analog zur Definition und zur Charakterisierung von Primzahlen sind. Etwas fies dabei ist, dass die Definition von „Primelement“ unten *nicht* der Definition von „Primzahl“ entspricht, sondern der Charakterisierung in Lemma 4.5.

∗ 4.8. **Definition.** Sei R ein Integritätsbereich. Ein Element $r \in R$ heißt *irreduzibel*, wenn $r \neq 0$, $r \notin R^\times$ und für jede Faktorisierung $r = ab$ in R gilt $a \in R^\times$ oder $b \in R^\times$. ♢ **DEF** irreduzibel

Kurz gesagt: Es gibt keine nicht-triviale Faktorisierung von r; r ist multiplikativ unzerlegbar.

∗ 4.9. **Definition.** Sei R ein Integritätsbereich. Ein Element $r \in R$ heißt *prim* oder *Primelement*, wenn $r \neq 0$, $r \notin R^\times$ und wenn aus $r \mid ab$ in R stets folgt, dass r ein Teiler von a oder ein Teiler von b ist. ♢ **DEF** Primelement

Zwischen diesen Begriffen gibt es folgenden Zusammenhang:

4.10. **Lemma.** *Sei R ein Integritätsbereich. Jedes Primelement in R ist irreduzibel. Ist R ein Hauptidealring, so gilt auch die Umkehrung.* **LEMMA** prim und irreduzibel

Beweis. Der Beweis ist ganz analog zu dem von Lemma 4.5. Sei zunächst r ein Primelement. Dann gilt jedenfalls $r \neq 0$ und $r \notin R^\times$. Ist $r = ab$, dann gilt auch $r \mid ab$; weil r prim ist, folgt $r \mid a$ oder $r \mid b$, woraus wie vorher $b \in R^\times$ oder $a \in R^\times$ folgt.

Sei jetzt R ein Hauptidealring und r irreduzibel. Dann gilt jedenfalls $r \neq 0$ und $r \notin R^\times$. Ist r ein Teiler von ab, aber nicht von a, dann ist $\mathrm{ggT}(r, a) \sim 1$, also $r \perp a$. Nach Lemma 3.20 folgt dann $r \mid b$. ❑

4.11. **Beispiel.** In Integritätsbereichen, die keine Hauptidealringe sind, kann es irreduzible Elemente geben, die nicht prim sind. Im Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist zum Beispiel 2 irreduzibel (es gibt nur die Teiler ± 1 und ± 2). Auf der anderen Seite ist 2 ein Teiler von $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, teilt aber keinen der beiden Faktoren in R; damit ist 2 kein Primelement in R. ♣ **BSP** irreduzibel, nicht prim

Da die Begriffe „irreduzibel“ und „prim“ über Teilbarkeitseigenschaften definiert sind, ist klar, dass assoziierte Elemente stets gleichzeitig prim oder irreduzibel sind. Eine Faktorisierung in Primelemente kann also immer nur bis auf Reihenfolge und Multiplikation der Primelemente mit Einheiten eindeutig bestimmt sein. Wir formulieren die Eigenschaft eines Integritätsbereichs, eine solche eindeutige Faktorisierung zu erlauben, daher in Analogie zu Folgerung 4.7.

∗ 4.12. **Definition.** Ein Integritätsbereich R heißt *faktoriell* (oder ein *faktorieller Ring*), wenn Folgendes gilt: Sei $\mathbb{P}_R$ ein Repräsentantensystem der Primelemente von R bis auf Assoziierte. Dann gibt es für jedes $0 \neq r \in R$ eindeutig bestimmte $u \in R^\times$ und $(e_p)_{p \in \mathbb{P}_R} \in \mathbb{Z}_{\geq 0}^{\mathbb{P}_R}$ mit $e_p = 0$ für alle bis auf endlich viele $p \in \mathbb{P}_R$, sodass **DEF** faktorieller Ring

$$r = u \prod_{p \in \mathbb{P}_R} p^{e_p} .$$ ♢

BSP nicht faktoriell

4.13. **Beispiel.** Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell. Zum Beispiel hat $2 \in R$ keine Faktorisierung in Primelemente (weil 2 irreduzibel und nicht prim ist, siehe oben). Auf der anderen Seite gibt es Faktorisierungen in irreduzible Elemente; eine solche Faktorisierung ist in R aber nicht immer eindeutig. Es sind etwa 2, 3, $1 + \sqrt{-5}$ und $1 - \sqrt{-5}$ alle in R irreduzibel und man hat die beiden wesentlich verschiedenen Faktorisierungen

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

Wir wollen jetzt erst einmal faktorielle Ringe durch andere Eigenschaften charakterisieren und diese dann für Hauptidealringe nachweisen. Dazu erinnern wir uns an den Beweis der eindeutigen Faktorisierung für $\mathbb{Z}$: Für die *Existenz* einer Faktorisierung in *irreduzible* Elemente hatten wir Induktion benutzt. Letzten Endes diente sie dazu zu zeigen, dass wir ein Element nicht immer „feiner“ faktorisieren können, sondern irgendwann bei irreduziblen und somit nicht weiter zerlegbaren Elementen landen. Für die *Eindeutigkeit* wurde verwendet, dass die irreduziblen Elemente auch prim sind. Diese beiden Eigenschaften reichen aus, wie der folgende Satz zeigt.

SATZ Charakterisierung von „faktoriell“

4.14. **Satz.** *Ein Integritätsbereich R ist genau dann faktoriell, wenn er die folgenden beiden Eigenschaften hat:*

(1) *Es gibt keine Folge $(a_n)_{n\geq 0}$ von Elementen von R, sodass $a_{n+1} \mid a_n$ und $a_n \not\sim a_{n+1}$ für alle n.*

(2) *Jedes irreduzible Element von R ist prim.*

Die erste Eigenschaft ist äquivalent zu folgenden Aussagen:

- Es gibt keine unendliche echt aufsteigende Folge
$$\langle a_0 \rangle_R \subsetneq \langle a_1 \rangle_R \subsetneq \ldots \subsetneq \langle a_n \rangle_R \subsetneq \ldots$$
von Hauptidealen in R.
- Jede aufsteigende Folge
$$\langle a_0 \rangle_R \subset \langle a_1 \rangle_R \subset \ldots \subset \langle a_n \rangle_R \subset \ldots$$
von Hauptidealen in R wird stationär (also $\langle a_N \rangle_R = \langle a_{N+1} \rangle_R = \ldots$ für ein $N \in \mathbb{Z}_{\geq 0}$).

Beweis. Wir nehmen zunächst an, dass die beiden Bedingungen erfüllt sind, und zeigen, dass R faktoriell ist. Wir zeigen erst die Existenz der Faktorisierung durch einen Widerspruchsbeweis. Dazu nehmen wir an, es gäbe ein Element $0 \neq a_0 \in R$, das keine Darstellung in der Form $u \prod_p p^{e_p}$ hat. Dann ist a_0 keine Einheit (denn sonst hätte man diese Darstellung mit $u = a_0$ und $e_p = 0$ für alle p) und auch nicht prim (sonst gäbe es $p \in \mathbb{P}_R$ mit $a_0 \sim p$ und man hätte eine Darstellung mit $e_p = 1$, $e_q = 0$ für $q \neq p$ und $u = a_0/p$) und damit auch nicht irreduzibel. Also gibt es eine Faktorisierung $a_0 = rs$ mit Nicht-Einheiten r und s. Gäbe es für beide Faktoren eine Produktdarstellung, dann gälte dies auch für a_0, ein Widerspruch. Also hat einer der Faktoren, wir nennen ihn a_1, keine Produktdarstellung. Auf diese Weise konstruieren wir rekursiv 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 (1) nicht geben. Also gibt es a_0 nicht, was zu zeigen war.

Der Beweis der Eindeutigkeit geht analog wie für den Ring $\mathbb{Z}$. Gilt

$$u \prod_{p \in \mathbb{P}_R} p^{e_p} = r = u' \prod_{p \in \mathbb{P}_R} p^{e'_p},$$

und ist für ein p zum Beispiel $e_p > e'_p$, dann können wir beide Seiten durch $p^{e'_p}$ teilen. Die linke Seite ist immer noch durch p teilbar, also auch die rechte Seite; da p prim ist, würde $p \mid q$ folgen für ein $q \in \mathbb{P}_R$ mit $q \neq p$. Das ist aber nicht möglich, da zwei Primelemente, von denen das eine das andere teilt, assoziiert sein müssen. Dieser Widerspruch zeigt, dass $e_p = e'_p$ für alle $p \in \mathbb{P}_R$ gelten muss. Daraus folgt dann auch noch $u = u'$.

Für die Gegenrichtung nehmen wir jetzt an, dass R faktoriell ist. Sei r irreduzibel. Nach Annahme ist $r = u \prod_{p \in \mathbb{P}_R} p^{e_p}$. Da r irreduzibel ist, kann rechts nur ein Primelement p_0 tatsächlich (und dann mit Exponent 1) vorkommen, damit ist $r = up_0$ prim. Für den Beweis von Bedingung (1) definieren wir $\ell(r)$ für $r \in R$ durch $\ell(0) = +\infty$ und $\ell(r) = \sum_{p \in \mathbb{P}_R} e_p$ für $r \neq 0$, wenn $r = u \prod_{p \in \mathbb{P}_R} p^{e_p}$ die Primfaktorisierung von r ist. Aus der eindeutigen Primfaktorzerlegung folgt dann $\ell(rs) = \ell(r) + \ell(s)$ und $\ell(r) = 0 \iff r \in R^\times$. Ist (a_n) eine Folge wie in Bedingung (1), 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. ❑

* 4.15. **Satz.** *Ist R ein Hauptidealring, dann ist R faktoriell.*

SATZ HIR ist faktoriell

Beweis. Wir müssen die beiden Eigenschaften aus Satz 4.14 nachweisen. Eigenschaft (2) hatten wir schon in Lemma 4.10 bewiesen. Für Eigenschaft (1) verwenden wir die zweite äquivalente Formulierung, die unmittelbar nach dem Satz angegeben wurde. Sei also

$$\langle a_0 \rangle_R \subset \langle a_1 \rangle_R \subset \ldots \subset \langle a_n \rangle_R \subset \ldots$$

eine aufsteigende Folge von Hauptidealen von R. Nach Lemma 3.9 ist die Vereinigung $\bigcup_{n \geq 0} \langle a_n \rangle_R$ wieder ein Ideal von R; da R ein Hauptidealring ist, gibt es $a \in R$ mit $\bigcup_{n \geq 0} \langle a_n \rangle_R = \langle a \rangle_R$. Dann gibt es ein $N \geq 0$ mit $a \in \langle a_N \rangle_R$ und damit $a \in \langle a_n \rangle_R$ für alle $n \geq N$. Es folgt für diese n

$$\langle a \rangle_R \subset \langle a_n \rangle_R \subset \bigcup_{m \geq 0} \langle a_m \rangle_R = \langle a \rangle_R,$$

also $\langle a_n \rangle_R = \langle a \rangle_R$. ❑

4.16. **Beispiel.** Gibt es (bis auf Assoziierte) nur ein Primelement, dann ist die Struktur der Faktorisierung besonders einfach. Beispiele solcher Ringe kann man wie folgt konstruieren: Sei p eine Primzahl. Dann ist

BSP nur ein Primelement

$$\mathbb{Z}_{\langle p \rangle} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, p \nmid b \right\} \subset \mathbb{Q}$$

ein Unterring von $\mathbb{Q}$ (die Abgeschlossenheit unter Addition und Multiplikation ergibt sich aus $p \nmid b, p \nmid b' \Rightarrow p \nmid bb'$). Jedes von null verschiedene Element von $\mathbb{Z}_{\langle p \rangle}$ kann eindeutig geschrieben werden in der Form up^e mit $u \in \mathbb{Z}_{\langle p \rangle}^\times$ und $e \geq 0$: Ist a/b das Element (mit $p \nmid b$), dann ist $a = a'p^e$ mit $p \nmid a'$; damit ist a'/b eine Einheit. p selbst ist keine Einheit, da $1/p \notin \mathbb{Z}_{\langle p \rangle}$. Es folgt, dass $\mathbb{Z}_{\langle p \rangle}$ ein Hauptidealring

ist mit bis auf Assoziierte eindeutigem Primelement p: Sei I ein Ideal von $\mathbb{Z}_{\langle p\rangle}$. Das Nullideal ist stets ein Hauptideal, also können wir $I \neq \{0\}$ annehmen. Dann können wir e als das Minimum aller Exponenten n definieren, sodass I ein Element der Form up^n mit $u \in \mathbb{Z}_{\langle p\rangle}^\times$ enthält. Es folgt $I = \langle p^e\rangle$, denn mit up^e enthält I auch p^e, und jedes Element $\neq 0$ von I hat die Form $a = up^n$ mit $n \geq e$, also ist $a = up^{n-e} \cdot p^e \in \langle p^e\rangle$. ♣

Dass die zweite Bedingung in Satz 4.14 schiefgehen kann, haben wir schon an unserem üblichen Gegenbeispiel $\mathbb{Z}[\sqrt{-5}]$ gesehen. Ein Beispiel dafür zu finden, dass auch die erste Bedingung nicht immer erfüllt ist, ist schwieriger zu konstruieren. Wir beginnen mit dem Ring $R_0 = \mathbb{Z}_{\langle 2\rangle} \subset \mathbb{R}$ (statt 2 könnte man auch jede andere Primzahl nehmen) und setzen $w_0 = 2$. Ist R_n schon als Unterring von $\mathbb{R}$ konstruiert mit $w_n \in R_n$, dann setzen wir $w_{n+1} = \sqrt{w_n} \in \mathbb{R}$ und $R_{n+1} = R_n[w_{n+1}]$. Dann ist $(R_n)_{n\geq 0}$ eine aufsteigende Folge von Unterringen von $\mathbb{R}$, also ist $R = \bigcup_n R_n$ ebenfalls ein Unterring von $\mathbb{R}$ und damit ein Integritätsbereich. Ähnlich wie für $R_0 = \mathbb{Z}_{\langle 2\rangle}$ prüft man nach, dass w_n bis auf Assoziierte das einzige irreduzible (oder auch Prim-)Element von R_n ist. Es folgt, dass kein w_n eine Einheit in R sein kann (denn w_n ist stets Potenz mit positivem Exponenten des Primelements von R_m, für alle $m \geq n$). Damit erhalten wir die Folge $(w_n)_{n\geq 0}$ von Elementen von R mit $w_{n+1} \mid w_n = w_{n+1}^2$ und $w_n \not\sim w_{n+1}$. Tatsächlich gibt es in R gar keine irreduziblen (oder primen) Elemente; damit kann es natürlich auch keine Faktorisierung in solche Elemente geben.

In faktoriellen Ringen ist folgende Definition sinnvoll:

DEF *p*-adische Bewertung

4.17. **Definition.** Seien R ein faktorieller Ring, $p \in R$ ein Primelement und $a \in R$ beliebig. Ist $a = 0$, dann setzen wir $v_p(a) = +\infty$. Für $a \neq 0$ sei

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

Die Abbildung $v_p : R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ heißt die *p-adische Bewertung.* ♢

Ist $p \in \mathbb{P}_R$ und $a = u\prod_{p\in\mathbb{P}_R} p^{e_p}$ wie in Definition 4.12, dann ist $v_p(a) = e_p$. Man kann die Faktorisierung also in der Form

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

schreiben. Wir beweisen einige Eigenschaften der p-adischen Bewertung.

LEMMA Eigenschaften von v_p

4.18. **Lemma.** *Sei R ein faktorieller Ring und $\mathbb{P}_R$ ein Repräsentantensystem der Primelemente von R bis auf Assoziierte.*

(1) *Für alle $a, b \in R$ gilt $v_p(a \pm b) \geq \min\{v_p(a), v_p(b)\}$ mit Gleichheit im Fall $v_p(a) \neq v_p(b)$.*

(2) *Für alle $a, b \in R$ gilt $v_p(ab) = v_p(a) + v_p(b)$.*

(3) *Für alle $a, b \in R$ gilt $a \mid b \iff \forall p \in \mathbb{P}_R : v_p(a) \leq v_p(b)$.*

Dabei gelten die üblichen Rechenregeln $n \leq \infty$ und $n+\infty = \infty$ für $n \in \mathbb{Z}_{\geq 0}\cup\{\infty\}$.

Beweis.

(1) Die erste Aussage folgt aus der Implikation $p^n \mid a, p^n \mid b \Rightarrow p^n \mid a \pm b$. Für die zweite Aussage sei ohne Einschränkung $v_p(a) < v_p(b)$. Dann ist

$$v_p(b) > v_p(a) = v_p\big((a-b)+b\big) \geq \min\{v_p(a-b), v_p(b)\}\,;$$

es folgt $v_p(a) \geq v_p(a-b) \geq v_p(a)$ und damit Gleichheit. Für $a+b$ genauso (unter Verwendung von $v_p(-b) = v_p(b)$).

(2) Für $a = 0$ oder $b = 0$ ist das klar. Sonst folgt es aus der Eindeutigkeit der Primfaktorisierung.

(3) Die Fälle $a = 0$ bzw. $b = 0$ sind wieder klar. Für $a, b \neq 0$ ist „$\Rightarrow$“ eine Folgerung aus Teil (2); die Gegenrichtung folgt wieder aus der Primfaktorzerlegung. ❑

FOLG Existenz von ggT und kgV in faktoriellen Ringen

4.19. **Folgerung.** *Seien R ein faktorieller Ring und $\mathbb{P}_R$ ein Repräsentantensystem der Primelemente von R bis auf Assoziierte. Dann existieren zu je zwei Elementen $a, b \in R$ größte gemeinsame Teiler und kleinste gemeinsame Vielfache von a und b in R. Sind $a, b \neq 0$, dann ist*

$$\prod_{p \in \mathbb{P}_R} p^{\min\{v_p(a), v_p(b)\}} \sim \mathrm{ggT}(a, b) \quad \textit{und} \quad \prod_{p \in \mathbb{P}_R} p^{\max\{v_p(a), v_p(b)\}} \sim \mathrm{kgV}(a, b)\,.$$

Insbesondere gilt (für alle a, b) $\mathrm{ggT}(a, b)\,\mathrm{kgV}(a, b) \sim ab$.

Die letzte Aussage verallgemeinert Satz 3.22.

Beweis. Ist etwa $a = 0$, dann ist $b \sim \mathrm{ggT}(a, b)$ und $0 \sim \mathrm{kgV}(a, b)$ und damit auch $\mathrm{ggT}(a, b)\,\mathrm{kgV}(a, b) \sim ab$. Wir können also $a, b \neq 0$ annehmen. Die Produktformeln für ggT und kgV folgen in diesem Fall aus Teil (3) von Lemma 4.18. Die letzte Aussage ergibt sich dann aus der Relation

$$\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} = v_p(a) + v_p(b)\,. \qquad ❑$$

Diese *Eigenschaft* des ggT sollte man nicht mit seiner *Definition* verwechseln. Auch zur ggT-Berechnung (etwa in $\mathbb{Z}$) ist diese Eigenschaft nur mäßig gut geeignet, da man zuerst die beteiligten Zahlen faktorisieren muss, wofür kein wirklich effizientes Verfahren bekannt ist. Der Euklidische Algorithmus funktioniert sehr viel besser!

Wir hatten die Frage nach der Existenz von größten gemeinsamen Teilern als Motivation für die Entwicklung der Theorie bis hin zu den faktoriellen Ringen benutzt. Man kann sich nun fragen, ob jeder Ring, in dem je zwei Elemente einen ggT (und ein kgV) haben, auch schon faktoriell sein muss. Die Antwort lautet „Nein“. Ein Gegenbeispiel ist der Ring R aus dem Kleingedruckten auf Seite 27. Man kann zeigen, dass jedes $0 \neq r \in R$ eindeutig geschrieben werden kann als $r = u \cdot 2^{v_2(r)}$ mit $u \in R^\times$ und $v_2(r) \in \mathbb{Q}$, wobei der Nenner eine Potenz von 2 ist (es gilt dann $w_n = 2^{1/2^n}$, also $v_2(w_n) = 1/2^n$). Es folgt, dass $2^{\min\{v_2(a), v_2(b)\}}$ ein ggT und $2^{\max\{v_2(a), v_2(b)\}}$ ein kgV von $a, b \in R$ ist (für $a, b \neq 0$). Es existieren also größte gemeinsame Teiler und kleinste gemeinsame Vielfache, obwohl der Ring R nicht faktoriell ist.

5. Die gaussschen Zahlen und Summen von zwei Quadraten

Wir werden jetzt ein weiteres Beispiel für einen euklidischen Ring (der damit auch ein Hauptidealring und ein faktorieller Ring ist) betrachten. Die Kenntnisse, die wir uns bisher erarbeitet haben, werden uns dann erlauben genau zu beschreiben, wann eine natürliche Zahl Summe von zwei Quadratzahlen ist.

DEF Ring $\mathbb{Z}[\boldsymbol{i}]$ der gaußschen Zahlen

5.1. **Definition.** Der Ring $\mathbb{Z}[\boldsymbol{i}] = \{a+b\boldsymbol{i} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ heißt *Ring der (ganzen) gaußschen Zahlen.* ♢

Addition und Multiplikation in diesem Ring funktionieren also wie folgt:

$$(a+b\boldsymbol{i})+(a'+b'\boldsymbol{i}) = (a+a')+(b+b')\boldsymbol{i}, \quad (a+b\boldsymbol{i})\cdot(a'+b'\boldsymbol{i}) = (aa'-bb')+(ab'+ba')\boldsymbol{i}\,.$$

Daran sieht man auch, dass die Menge $\{a + b\boldsymbol{i} \mid a, b \in \mathbb{Z}\}$ einen Unterring von $\mathbb{C}$ bildet (was die Gleichheit mit dem von $\boldsymbol{i}$ über $\mathbb{Z}$ erzeugten Unterring $\mathbb{Z}[\boldsymbol{i}]$ begründet); insbesondere ist $\mathbb{Z}[\boldsymbol{i}]$ ein Integritätsbereich. Wir beweisen eine wichtige Eigenschaft.

SATZ $\mathbb{Z}[\boldsymbol{i}]$ ist euklidisch

5.2. **Satz.** *$\mathbb{Z}[\boldsymbol{i}]$ ist ein euklidischer Ring mit euklidischer Normfunktion*

$$N(a + b\boldsymbol{i}) = |a + b\boldsymbol{i}|^2 = (a + b\boldsymbol{i})(a - b\boldsymbol{i}) = a^2 + b^2\,.$$

Für $\alpha, \beta \in \mathbb{Z}[\boldsymbol{i}]$ gilt $N(\alpha\beta) = N(\alpha)N(\beta)$.

Beweis. Es ist klar, dass $N(\alpha) \in \mathbb{Z}_{\geq 0}$ ist für alle $\alpha \in \mathbb{Z}[\boldsymbol{i}]$ und $N(\alpha) = 0$ nur für $\alpha = 0$. Seien jetzt $\alpha, \beta \in \mathbb{Z}[\boldsymbol{i}]$ mit $\beta \neq 0$. Wir müssen die Existenz von $\gamma, \rho \in \mathbb{Z}[\boldsymbol{i}]$ zeigen mit $\alpha = \gamma\beta + \rho$ und $N(\rho) < N(\beta)$. Dazu bilden wir den Quotienten α/β in $\mathbb{C}$:

$$\frac{\alpha}{\beta} = u + v\boldsymbol{i} \qquad \text{mit } u, v \in \mathbb{R} \text{ (sogar in } \mathbb{Q}).$$

Dann gibt es ganze Zahlen a, b mit $|u - a| \leq 1/2$ und $|v - b| \leq 1/2$; wir setzen $\gamma = a + b\boldsymbol{i}$. Es folgt, dass

$$\rho := \alpha - \gamma\beta = \big((u + v\boldsymbol{i}) - (a + b\boldsymbol{i})\big)\beta$$

die Ungleichung

$$\begin{aligned} N(\rho) = |\rho|^2 &= \big|(u - a) + (v - b)\boldsymbol{i}\big|^2|\beta|^2 = \big((u - a)^2 + (v - b)^2\big)N(\beta) \\ &\leq \big(\tfrac{1}{4} + \tfrac{1}{4}\big)N(\beta) \leq \tfrac{1}{2}N(\beta) < N(\beta) \end{aligned}$$

erfüllt; die Gleichung $\alpha = \gamma\beta + \rho$ gilt nach Definition von ρ.

Die Multiplikativität von N folgt aus

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2\,|\beta|^2 = N(\alpha)N(\beta)\,.$$ ❑

FOLG $\mathbb{Z}[\boldsymbol{i}]$ ist HIR, faktoriell

5.3. **Folgerung.** *Der Ring $\mathbb{Z}[\boldsymbol{i}]$ ist ein Hauptidealring und daher faktoriell.*

Beweis. Das folgt aus Satz 3.13 und Satz 4.15. ❑

Da der Ring euklidisch ist, können wir größte gemeinsame Teiler mit dem Euklidischen Algorithmus berechnen.

5.4. **Beispiel.** Wir berechnen einen ggT von 41 und $32+\boldsymbol{i}$:

BSP
ggT in $\mathbb{Z}[\boldsymbol{i}]$

n	0	1	2	3	4
a_n	41	$32+\boldsymbol{i}$	$9-\boldsymbol{i}$	$5+4\boldsymbol{i}$	0
q_n		1	3	$1-\boldsymbol{i}$	

Der exakte Quotient der vorletzten Division ist $3+1/2+\boldsymbol{i}/2$, sodass das Runden nicht eindeutig ist. Ich habe 3 als Quotienten benutzt. Wir sehen, dass $5+4\boldsymbol{i}$ ein größter gemeinsamer Teiler ist. Man beachte $N(5+4\boldsymbol{i})=5^2+4^2=41$; die Primzahl 41 kann also als Summe von zwei Quadratzahlen geschrieben werden. ♣

Wir zeigen noch einige Eigenschaften von $\mathbb{Z}[\boldsymbol{i}]$.

5.5. **Lemma.**

LEMMA
Einheiten, Primel. in $\mathbb{Z}[\boldsymbol{i}]$

(1) *Für $\varepsilon\in\mathbb{Z}[\boldsymbol{i}]$ gilt $\varepsilon\in\mathbb{Z}[\boldsymbol{i}]^\times \iff N(\varepsilon)=1$. Insbesondere ist $\mathbb{Z}[\boldsymbol{i}]^\times=\{1,-1,\boldsymbol{i},-\boldsymbol{i}\}$.*

(2) *Ist $\pi\in\mathbb{Z}[\boldsymbol{i}]$ und $N(\pi)$ eine Primzahl, dann ist π ein Primelement.*

(3) *Ist $\pi\in\mathbb{Z}[\boldsymbol{i}]$ ein Primelement, dann gibt es eine Primzahl p mit $\pi\mid p$ und $N(\pi)=p$ oder $N(\pi)=p^2$. Im zweiten Fall gilt $\pi\sim p$ in $\mathbb{Z}[\boldsymbol{i}]$ und es gibt keine Elemente der Norm p in $\mathbb{Z}[\boldsymbol{i}]$.*

Beweis.

(1) Ist $\varepsilon\in\mathbb{Z}[\boldsymbol{i}]^\times$, dann folgt aus $\varepsilon\varepsilon^{-1}=1$, dass $N(\varepsilon)N(\varepsilon^{-1})=N(1)=1$ ist. Da die Werte von N natürliche Zahlen sind, folgt $N(\varepsilon)=1$. Ist $\varepsilon=a+b\boldsymbol{i}$ und gilt $N(\varepsilon)=1$, dann gilt mit $\bar\varepsilon=a-b\boldsymbol{i}$ die Gleichung $\varepsilon\bar\varepsilon=N(\varepsilon)=1$, also ist $\varepsilon\in\mathbb{Z}[\boldsymbol{i}]^\times$. Es ist dann leicht zu sehen, dass die einzigen Elemente mit Norm 1 die angegebenen vier Elemente sind.

(2) Wegen $N(\pi)>1$ ist $\pi\neq 0$ und keine Einheit. Im Hauptidealring $\mathbb{Z}[\boldsymbol{i}]$ sind irreduzible Elemente und Primelemente dasselbe; es genügt also zu zeigen, dass π irreduzibel ist. Sei also $\pi=\alpha\beta$ eine Faktorisierung in $\mathbb{Z}[\boldsymbol{i}]$. Dann folgt $N(\pi)=N(\alpha)N(\beta)$; weil $N(\pi)$ eine Primzahl ist, muss $N(\alpha)=1$ oder $N(\beta)=1$ gelten, damit ist ein Faktor eine Einheit.

(3) Da $\pi\neq 0$ und keine Einheit ist, folgt $n=\pi\bar\pi=N(\pi)>1$. Dann ist n ein nicht-leeres Produkt von Primzahlen in $\mathbb{Z}$; weil π ein Primelement ist, muss π einen der Primfaktoren von n teilen; sei p dieser Primteiler. Aus $\pi\mid p$ folgt $N(\pi)\mid N(p)=p^2$, also muss entweder $N(\pi)=p$ oder $N(\pi)=p^2$ sein. Im zweiten Fall sei $p=\pi\alpha$ mit $\alpha\in\mathbb{Z}[\boldsymbol{i}]$; es folgt $p^2=N(p)=N(\pi)N(\alpha)$ und damit $N(\alpha)=1$. Also ist $\alpha\in\mathbb{Z}[\boldsymbol{i}]^\times$ und damit $\pi\sim p$. Gäbe es $\pi'\in\mathbb{Z}[\boldsymbol{i}]$ mit $N(\pi')=p$, dann folgte $\pi'\mid p$ und p wäre nicht irreduzibel, ein Widerspruch. ❑

Bevor wir die Primelemente von $\mathbb{Z}[\boldsymbol{i}]$ genau beschreiben können, brauchen wir noch ein Resultat.

5.6. **Lemma.** *Ist p eine Primzahl der Form $p=4k+1$, dann gibt es $u\in\mathbb{Z}$ mit $p\mid u^2+1$.*

LEMMA
$p\mid u^2+1$ für $p=4k+1$

Beweis. Sei $u = (2k)! = 1 \cdot 2 \cdot 3 \cdots (2k-1) \cdot 2k$. Da $2k$ gerade ist, gilt dann $u^2 = 1 \cdot 2 \cdots (2k-1) \cdot 2k \cdot (-2k) \cdot (-2k+1) \cdots (-2) \cdot (-1)$. Dann ist

$$u^2 - (p-1)! = (2k)!\big((-2k) \cdot (-2k+1) \cdots (-1) - (p-2k) \cdot (p-2k+1) \cdots (p-1)\big)$$

durch p teilbar. Nun sagt der Satz von Wilson, dass p ein Teiler von $(p-1)!+1$ ist (wir werden diesen Satz später beweisen); damit gilt auch

$$p \mid u^2 + 1 = (u^2 - (p-1)!) + ((p-1)! + 1)\,. \qquad \square$$

Die *Berechnung* eines geeigneten $u \in \mathbb{Z}$ mit der Formel im Beweis ist fürchterlich ineffizient. Es gibt wesentlich bessere Möglichkeiten dafür.

* 5.7. **Satz.** *Ein Repräsentantensystem $\mathbb{P}_{\mathbb{Z}[i]}$ der Primelemente in $\mathbb{Z}[\boldsymbol{i}]$ bis auf Assoziierte ist gegeben durch folgende Elemente:*

SATZ Primelemente in $\mathbb{Z}[\boldsymbol{i}]$

(1) $1 + \boldsymbol{i}$,

(2) *q für jede Primzahl $q = 4k+3 \in \mathbb{Z}$,*

(3) *$\pi = a + b\boldsymbol{i}$ und $\bar\pi = a - b\boldsymbol{i}$ für jede Primzahl $p = 4k+1 \in \mathbb{Z}$, wobei $p = a^2 + b^2$ mit $0 < a < b$.*

Beweis. Wir wissen nach Lemma 5.5, dass jedes Primelement π von $\mathbb{Z}[\boldsymbol{i}]$ eine Primzahl p teilt und dass dann entweder $N(\pi) = p$ oder $\pi \sim p$ gilt. Wir betrachten die möglichen Primzahlen je nach ihrem Rest bei Division durch 4.

(1) $p = 2$: Es gibt Elemente der Norm 2, nämlich die vier Elemente $\pm 1 \pm \boldsymbol{i}$. Sie sind alle zueinander assoziiert.

(2) $q = 4k+3$: Es gibt keine Elemente der Norm q, denn das Quadrat einer geraden Zahl ist durch 4 teilbar und das Quadrat einer ungeraden Zahl $2m+1$ hat die Form $4(m^2+m)+1$, sodass eine Summe von zwei Quadraten niemals den Rest 3 bei Division durch 4 haben kann. Da ein nichttrivialer Teiler (also keine Einheit und nicht zu q assoziiert) von q in $\mathbb{Z}[\boldsymbol{i}]$ Norm q haben müsste, ist q irreduzibel und damit prim. Nach Lemma 5.5 sind alle Primteiler von q in $\mathbb{Z}[\boldsymbol{i}]$ zu q assoziiert.

(3) $p = 4k+1$: Nach Lemma 5.6 gibt es $u \in \mathbb{Z}$ mit $p \mid u^2+1$. Da p ein Teiler von $u^2+1 = (u+\boldsymbol{i})(u-\boldsymbol{i})$, aber nicht von $u \pm \boldsymbol{i}$ ist, kann p nicht prim in $\mathbb{Z}[\boldsymbol{i}]$ sein. Es gibt also $\pi = a + b\boldsymbol{i} \in \mathbb{Z}[\boldsymbol{i}]$ mit $N(\pi) = a^2 + b^2 = p$. Durch eventuelles Ändern der Vorzeichen oder/und Vertauschen von a und b können wir $0 < a < b$ erreichen. (Beachte $|a| \neq |b|$, da p nicht gerade ist.) Da die Norm von π (und von $\bar\pi$) die Primzahl p ist, sind π und $\bar\pi$ Primelemente; wegen $p = \pi\bar\pi$ sind alle Primteiler von p entweder zu π oder zu $\bar\pi$ assoziiert, die nicht zueinander assoziiert sind (die Assoziierten von π sind $a+b\boldsymbol{i}$, $-b+a\boldsymbol{i}$, $-a-b\boldsymbol{i}$ und $b-a\boldsymbol{i}$).

Ist also π ein Primelement, dann ist π Teiler einer Primzahl p; jeder Primteiler in $\mathbb{Z}[\boldsymbol{i}]$ einer Primzahl ist zu genau einem der aufgelisteten Primelemente assoziiert. Das ist die Behauptung. $\square$

Wir formulieren einen Teil der Aussage des Satzes noch einmal separat.

* 5.8. **Folgerung.** *Ist p eine Primzahl der Form $4k+1$, dann gibt es eindeutig bestimmte $a, b \in \mathbb{Z}$ mit $0 < a < b$ und $p = a^2 + b^2$.* **FOLG** 2-□-Satz für Primzahlen

Beweis. Die Existenz wurde als Teil von Satz 5.7 bewiesen. Für den Beweis der Eindeutigkeit seien $a', b' \in \mathbb{Z}$ mit $a'^2 + b'^2 = p$ und $0 < a' < b'$. Mit $\pi = a' + b'\boldsymbol{i}$ gilt dann $\pi \mid p$; es folgt (aus dem Beweis von Satz 5.7), dass $\pi \sim a + b\boldsymbol{i}$ oder $\pi \sim a - b\boldsymbol{i}$ ist. Das bedeutet, dass sich a' und b' von a und b nur durch Vorzeichen und Reihenfolge unterscheiden können. Durch die Bedingung $0 < a' < b'$ werden aber sowohl die Vorzeichen als auch die Reihenfolge eindeutig festgelegt, also folgt $(a', b') = (a, b)$. ❑

Dieser *Zwei-Quadrate-Satz für Primzahlen* wurde zuerst von Pierre de Fermat formuliert, dem Begründer der modernen Zahlentheorie.

Kennt man ein $u \in \mathbb{Z}$ mit $p \mid u^2+1$, dann kann man $\pi = a+b\boldsymbol{i}$ (bis auf Assoziierte und Übergang zu $\bar{\pi}$) als $\mathrm{ggT}(p, u + \boldsymbol{i})$ berechnen.

5.9. **Beispiel.** Es ist $22^2 + 1 = 484 + 1 = 485 = 5 \cdot 97$, also gilt $97 \mid 22^2 + 1$. Wir berechnen $\mathrm{ggT}(97, 22 + \boldsymbol{i})$: $97 = 4(22 + \boldsymbol{i}) + (9 - 4\boldsymbol{i})$ und $22 + \boldsymbol{i} = (2 + \boldsymbol{i})(9 - 4\boldsymbol{i})$, also ist $9 - 4\boldsymbol{i}$ ein ggT, und wir erhalten $97 = 4^2 + 9^2$. ♣ **BSP** p als □ + □

Aus Satz 5.7 folgt auch sehr direkt der allgemeine *Zwei-Quadrate-Satz.*

* 5.10. **Satz.** *Eine natürliche Zahl $n > 0$ ist genau dann Summe zweier Quadratzahlen, wenn in ihrer Primfaktorzerlegung jede Primzahl q der Form $4k + 3$ mit geradem Exponenten auftritt (d.h., $v_q(n)$ ist gerade).* **SATZ** 2-□-Satz

Beweis. Wegen $N(a + b\boldsymbol{i}) = a^2 + b^2$ ist die Menge der darstellbaren $n > 0$ gerade $\{N(\alpha) \mid 0 \neq \alpha \in \mathbb{Z}[\boldsymbol{i}]\}$. Wegen der Multiplikativität der Norm und weil $\mathbb{Z}[\boldsymbol{i}]$ faktoriell ist, erhalten wir als Werte gerade alle Produkte von Normen $N(\pi)$ von Primelementen. Diese Normen sind 2, p für Primzahlen $p = 4k + 1$ und q^2 für Primzahlen $q = 4k + 3$. n ist genau dann ein Produkt solcher Normen, wenn die Primzahlen q in der Primfaktorzerlegung von n mit geradem Exponenten vorkommen. ❑

6. 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*. Im Folgenden nehmen wir der Einfachheit halber an, dass die Ringe kommutativ sind (obwohl das in den meisten Fällen nicht nötig wäre).

* 6.1. **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 „·“ 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!)

DEF Ringhomomorphismus

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. ♢

6.2. **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.*

LEMMA Eigensch. von Ringhomomom.

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

6.3. **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).

DEF Ringisomorphismus

isomorph

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

Automorphismus

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

6.4. **Beispiele.** **BSP** Ringhomomorphismen

(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 $a \mapsto a + 0i$. In der anderen Richtung 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) Der Körper $\mathbb{R}$ besitzt außer der Identität keinen weiteren (Ring-)Automorphismus (Übung). ♣

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

Wie bei linearen Abbildungen sind Kern und Bild interessant.

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

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

Wir schreiben $\mathrm{im}(\phi)$ für das Bild von ϕ. ♢

6.6. **Lemma.** *Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus. Dann ist* $\mathrm{im}(\phi)$ *ein Unterring von R_2, und* $\ker(\phi)$ *ist ein Ideal von R_1. ϕ ist injektiv genau dann, wenn* $\ker(\phi) = \{0\}$ *ist.* **LEMMA** Kern ist Ideal

Beweis. Aus der Definition und Lemma 6.2 folgt, dass $\mathrm{im}(\phi)$ 0 und 1 enthält und unter Addition, Negation und Multiplikation abgeschlossen ist. Also ist $\mathrm{im}(\phi)$ ein Unterring von R_2.

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

$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0\,,$$

also ist $ra \in \ker(\phi)$. Damit ist gezeigt, dass $\ker(\phi) \subset R_1$ ein Ideal ist.

Ist ϕ injektiv, dann gilt

$$a \in \ker(\phi) \Rightarrow \phi(a) = 0 = \phi(0) \Rightarrow a = 0\,,$$

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. ❑

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

BSP Kern

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

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

LEMMA Homomorphismen und Ideale

(1) *Ist $I \subset R_1$ ein Ideal, dann ist $\phi(I)$ ein Ideal im Unterring* $\mathrm{im}(\phi)$ *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 $r \in \mathrm{im}(\phi)$ 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 $\mathrm{im}(\phi)$ zu sein.

(2) Wegen $\phi(0) = 0 \in J$ ist $0 \in \phi^{-1}(J)$. Seien $a, b \in \phi^{-1}(J)$, das bedeutet $\phi(a), \phi(b) \in J$. 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 $\phi(a) \in J$ und damit auch $\phi(ra) = \phi(r)\phi(a) \in J$, also $ra \in \phi^{-1}(J)$. Also ist $\phi^{-1}(J)$ 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 $a = b + (a-b) \in I$. ❑

6.9. **Beispiel.** Sei $\phi : \mathbb{Z} \to \mathbb{Q}$ der eindeutig bestimmte Ringhomomorphismus. Dann ist ϕ nicht surjektiv. Das Bild eines von null verschiedenen Ideals $n\mathbb{Z}$ 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 $\ker(\phi) = \{0\}$, sodass die Bedingung $\ker(\phi) \subset I$ leer ist): Sie liefert nur das Nullideal und $\mathbb{Z} = \phi^{-1}(\mathbb{Q})$ als Ideale von $\mathbb{Z}$. ♣

BSP ϕ(Ideal) kein Ideal

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.

6.10. **Definition.** Seien 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. $a \equiv b \bmod c$. ♢

DEF kongruent

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.

6.11. **Lemma.** *Seien R ein Ring und $I \subset R$ ein Ideal.*

LEMMA Eigensch. Kongruenz

(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: $a - a = 0 \in I \Rightarrow a \equiv a \bmod I$.
Symmetrie: $a \equiv b \bmod I \Rightarrow a - b \in I \Rightarrow -(a - b) = b - a \in I \Rightarrow b \equiv a \bmod I$.
Transitivität: $a \equiv b \equiv c \bmod I \Rightarrow a-b, b-c \in I \Rightarrow a-c = (a-b)+(b-c) \in I \Rightarrow a \equiv c \bmod I$.

(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. ❑

* 6.12. **Definition.** Seien 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. ♢

DEF Faktorring

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.

SATZ Faktorring ist Ring

6.13. **Satz.** *Seien R ein Ring und $I \subset R$ ein Ideal. Dann gibt es auf R/I genau eine Ringstruktur, sodass 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 6.11, (2). Die Ringaxiome übertragen sich dann sofort von R auf R/I. Schließlich gilt

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

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.

SATZ Homomorphiesatz für Ringe

* 6.14. **Satz.** *Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus. Dann induziert ϕ einen Isomorphismus $\varphi : R_1/\ker(\phi) \to \mathrm{im}(\phi)$, $[a] \mapsto \phi(a)$.*

Beweis. Wir müssen zeigen, dass φ wohldefiniert ist, also $[a] = [b] \Rightarrow \phi(a) = \phi(b)$. Es gilt aber

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

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

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

also ist $\ker(\varphi) = \{[0]\}$ wie gewünscht. $\square$

Wie sieht das mit den Faktorringen für den Ring $\mathbb{Z}$ aus? Wir wissen, dass die Ideale von $\mathbb{Z}$ gegeben sind durch $I = \langle n\rangle_{\mathbb{Z}} = n\mathbb{Z}$ 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:

LEMMA Faktorringe von $\mathbb{Z}$

6.15. **Lemma.** *Sei $n \in \mathbb{Z}_{>0}$. 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 gegeben durch $a \mapsto [r]$, wobei r der Rest bei der Division von a durch n ist.*

Alternativ kann man auch statt der Reste $0, 1, \ldots, n-1$ die „absolut kleinsten Reste“ $-\frac{n}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{n}{2}$ (für n gerade) bzw. $-\frac{n-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{n-1}{2}$ (für n ungerade) verwenden.

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 $a - r = qn \in n\mathbb{Z}$ 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. ❑

BSP Konstruktion von $\mathbb{R}$

6.16. **Beispiel.** Ein Beispiel für die Anwendung von Satz 6.14 tritt bei der Konstruktion des Körpers der reellen Zahlen mittels Cauchy-Folgen auf: Die Teilmenge $C \subset \mathbb{Q}^{\mathbb{N}}$ 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.) ♣

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.

BSP Summen von Potenzen

6.17. **Beispiel.** Wir zeigen noch einmal (wir hatten das bereits im Beweis von Satz 5.7 getan), 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.[1]) ♣

Wir wollen jetzt Lemma 6.8, (3) und Satz 6.14 kombinieren, um einen Zusammenhang herzustellen zwischen Eigenschaften des Bildes und des Kerns eines Ringhomomorphismus. Dazu definieren wir erst einmal die relevanten Eigenschaften von Idealen.

* 6.18. **Definition.** Seien R ein Ring und $I \subset R$ ein Ideal. **DEF** maximales Ideal Primideal

(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: Aus $ab \in I$ folgt $a \in I$ oder $b \in I$. ♢

6.19. **Beispiele.** **BSP** Primideale max. Ideale

(1) Ein Element $p \in R$ ist genau dann ein Primelement, wenn $p \neq 0$ ist und das von p erzeugte Hauptideal Rp ein Primideal ist.

(2) Aus den Definitionen folgt:

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

(3) Jedes maximale Ideal ist ein Primideal: 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. ♣

* 6.20. **Satz.** *Sei $\phi : R_1 \to R_2$ ein Ringhomomorphismus.* **SATZ** Bilder von Ringhom.

(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:

Seien R ein Ring und $I \subset R$ 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.*

Diese Version folgt aus der Version im Satz, indem man den Satz auf den kanonischen Epimorphismus $\phi : R \to R/I$ anwendet, denn dann ist $\ker(\phi) = I$ und $\operatorname{im}(\phi) = R/I$. Umgekehrt folgt die Version im Satz aus der zweiten Version mit $I = \ker(\phi)$ und dem Homomorphiesatz $R_1/\ker(\phi) \cong \operatorname{im}(\phi)$.

Beweis.

(1) Nach Lemma 6.8, (3) besteht 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“.

[1] Die kleinste Lösung ist $a = 2\,220\,422\,932$, $b = -2\,218\,888\,517$, $c = -283\,059\,965$.

(2) $\mathrm{im}(\phi)$ ist *kein* Integritätsbereich genau dann, wenn $\mathrm{im}(\phi)$ 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 $\mathrm{im}(\phi)$ aus, der definitionsgemäß kein Integritätsbereich ist.) ❑

6.21. **Beispiel.** Das Ideal N der Nullfolgen im Ring C der Cauchy-Folgen über $\mathbb{Q}$ ist ein maximales Ideal, denn es ist der Kern eines Ringhomomorphismus, dessen Bild der Körper $\mathbb{R}$ ist. **BSP** Konstruktion von $\mathbb{R}$

Umgekehrt kann man auch direkt zeigen, dass N ein maximales Ideal in C ist: Sei $(a_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge, die keine Nullfolge ist. Dann gibt es $n_0 \in \mathbb{N}$ und $c > 0$, sodass $|a_n| > c$ für alle $n > n_0$ gilt. Die Folge (b_n) mit $b_n = 0$ für $n \leq n_0$ und $b_n = 1/a_n$ für $n > n_0$ ist dann ebenfalls eine Cauchy-Folge. Die Folge (c_n) mit $c_n = 1$ für $n \leq n_0$ und $c_n = 0$ für $n > n_0$ ist eine Nullfolge. Es gilt dann $(a_n) \cdot (b_n) + (c_n) = (1)$, woraus $\langle N \cup \{(a_n)\}\rangle_C = C$ folgt. Das zeigt, dass N ein maximales Ideal ist. Es folgt, dass $\mathbb{R} := C/N$ ein Körper ist. Das ist eine Möglichkeit, die reellen Zahlen aus den rationalen Zahlen zu konstruieren. Man muss dann noch die relevanten Eigenschaften (wie das Supremumsaxiom) nachprüfen. ♣

6.22. **Beispiel.** Welche Faktorringe $\mathbb{Z}/n\mathbb{Z}$ (mit $n \geq 0$) sind Körper? **BSP** Faktorringe von $\mathbb{Z}$

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 dasselbe 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 $[a], [b] \neq [0]$, $[a] \cdot [b] = [ab] = [n] = [0]$.

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 $\mathrm{ggT}(a, p) = 1$. 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“.) ♣

Für einige Anwendungen in der Algebra ist es wichtig zu wissen, dass jedes echte Ideal eines Rings R in einem maximalen Ideal enthalten ist. Dafür braucht man das Zornsche Lemma. Man kann es recht allgemein für (halb-)geordnete Mengen formulieren; für unsere Zwecke genügt eine Version für durch Inklusion geordnete Teilmengen einer Menge.

Satz. *Sei X eine Menge und $\mathcal{T}$ eine Menge von Teilmengen von X. Eine Teilmenge $\mathcal{K}$ von $\mathcal{T}$ heißt eine Kette, wenn je zwei Elemente A, B von $\mathcal{K}$ miteinander vergleichbar sind, d.h., es gilt $A \subset B$ oder $B \subset A$. Wenn jede Kette $\mathcal{K} \subset \mathcal{T}$ eine obere Schranke S in $\mathcal{T}$ hat (d.h., $A \subset S$ für alle $A \in \mathcal{K}$), dann gibt es maximale Elemente T in $\mathcal{T}$ (d.h., für $A \in \mathcal{T}$ mit $T \subset A$ gilt $A = T$).* **SATZ** Zornsches Lemma

Man kann zeigen, dass diese Aussage (unter Annahme der übrigen Axiome der Mengenlehre) zum Auswahlaxiom äquivalent ist.

Wir können das hier folgendermaßen anwenden:

Satz. *Sei R ein Ring und $I \subsetneq R$ ein Ideal. Dann gibt es ein maximales Ideal M von R mit $I \subset M$.*

SATZ Existenz von max. Idealen

Beweis. Sei $\mathcal{T}$ die Menge aller Ideale J von R mit $I \subset J \subsetneq R$. Dann ist $I \in \mathcal{T}$; damit ist $\mathcal{T}$ nicht leer und die leere Kette hat eine obere Schranke (nämlich I). Ist $\mathcal{K}$ eine nicht-leere Kette, dann ist die Vereinigung $J = \bigcup \mathcal{K}$ aller Ideale in $\mathcal{K}$ wieder ein Ideal von R (das zeigt man wie in Lemma 3.9) und es gilt $I \subset J \subsetneq R$. Denn wäre $J = R$, dann wäre $1 \in J$, also gäbe es ein $J' \in \mathcal{K}$ mit $1 \in J'$ und es müsste $J' = R$ sein, ein Widerspruch. Damit ist $J \in \mathcal{T}$ eine obere Schranke von $\mathcal{K}$. Aus dem Zornschen Lemma folgt dann die Existenz (mindestens) eines maximalen Elements M von $\mathcal{T}$. Das ist dann aber gerade ein maximales Ideal von R, das I enthält. ❑

Insbesondere hat jeder Ring außer dem Nullring (für den ist die Voraussetzung $I \subsetneq R$ nicht erfüllbar) maximale Ideale und damit Faktorringe, die Körper sind.

Auf ähnliche Weise zeigt man, dass beliebige Vektorräume Basen besitzen; vgl. das Kleingedruckte auf den Seiten 51–52 des Skripts „Lineare Algebra I“.

7. Summen von vier Quadraten

Wir wollen jetzt 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. (Wenn Sie in einem der Fach-Studiengänge studieren, dann kennen Sie ihn bereits aus der Linearen Algebra II.)

DEF Quaternionen

7.1. **Definition.** 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 $1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ (damit sind Nullelement, Addition und Negation definiert). Die Multiplikation erfüllt die Distributivgesetze, ist $\mathbb{R}$-bilinear und ist auf der Basis gegeben durch

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1\,, \quad \boldsymbol{ij} = \boldsymbol{k}, \boldsymbol{jk} = \boldsymbol{i}, \boldsymbol{ki} = \boldsymbol{j}\,, \quad \boldsymbol{ji} = -\boldsymbol{k}, \boldsymbol{kj} = -\boldsymbol{i}, \boldsymbol{ik} = -\boldsymbol{j}$$

(und natürlich $1^2 = 1$, $1 \cdot \boldsymbol{i} = \boldsymbol{i}$ 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 $\alpha = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ (mit $a, b, c, d \in \mathbb{R}$) definiert man die *konjugierte Quaternion* $\bar\alpha = a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}$. 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.

Wir zeigen noch, 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.) ♢

Offenbar ist

$$\mathbb{Z}_{\mathbb{H}} = \{a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \mid a, b, c, d \in \mathbb{Z}\} \subset \mathbb{H}$$

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

7.2. **Lemma.** *Die Menge S_4 ist multiplikativ abgeschlossen: Sind $m, n \in S_4$, dann ist auch $mn \in S_4$.*

LEMMA
$4\square \cdot 4\square = 4\square$

Beweis. Seien $m, n \in S_4$. Wegen $S_4 = N(\mathbb{Z}_{\mathbb{H}})$ gibt es $\alpha, \beta \in \mathbb{Z}_{\mathbb{H}}$ mit $N(\alpha) = m$ und $N(\beta) = n$. Dann ist $mn = N(\alpha)N(\beta) = N(\alpha\beta) \in N(\mathbb{Z}_{\mathbb{H}}) = S_4$. ❑

Für die Aussage des Lemmas würde es genügen, einfach die explizite Darstellung eines Produkts von zwei Summen von vier Quadraten nachzurechnen, die man (z.B.) aus der Gleichung $N(\alpha\bar{\beta}) = N(\alpha)N(\beta)$ bekommt:

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) \\ = (aw + bx + cy + dz)^2 + (-ax + bw - cz + dy)^2 \\ + (-ay + bz + cw - dx)^2 + (-az - by + cx + dw)^2\end{aligned}$$

Es genügt also zu beweisen, dass jede *Primzahl* Summe von vier Quadraten ist. Als ersten Schritt dafür brauchen wir eine Hilfsaussage. Sie ist analog zur Aussage „$\exists u \in \mathbb{Z} : u^2 \equiv -1 \bmod p$“ für Primzahlen $p \equiv 1 \bmod 4$, die wir für den Beweis des Zwei-Quadrate-Satzes benötigt haben.

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

LEMMA
$u^2 + v^2$
$\equiv -1 \bmod p$

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, dass $x = a$ oder $x = -a$ ist, 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 das: 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. ❑

SATZ
4□-Satz für Primzahlen

7.4. **Satz.** *Sei p eine Primzahl. Dann ist $p \in S_4$.*

Beweis. Sei $M = \{m \in \mathbb{Z}_{>0} \mid mp \in S_4\}$. Wir zeigen zuerst, dass M nicht leer ist. Nach Lemma 7.3 gibt es $u, v \in \mathbb{Z}$ mit $|u|, |v| \le p/2$ und $p \mid 1^2 + u^2 + v^2$. Dann ist

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

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 $m_0 = \min M > 1$ ist und versuchen, daraus einen Widerspruch abzuleiten. Sei $\alpha = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \in \mathbb{Z}_{\mathbb{H}}$ mit $N(\alpha) = m_0 p$. Wir wählen $\beta = r + s\boldsymbol{i} + t\boldsymbol{j} + u\boldsymbol{k} \in \mathbb{Z}_{\mathbb{H}}$ mit $|r|, |s|, |t|, |u| \le m_0/2$ 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

$$N(\beta) = r^2 + s^2 + t^2 + u^2 \le 4(m_0/2)^2 = m_0^2 \tag{7.1}$$

und

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

also $N(\beta) = m_1 m_0$ mit $0 \le m_1 \le m_0$. Für unser Argument brauchen wir, dass $0 < m_1 < m_0$ ist. Wäre $m_1 = 0$, 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 $m_1 = m_0$, dann hätten wir in (7.1) Gleichheit, also wäre $m_0 = 2m'$ gerade und $|r| = |s| = |t| = |u| = m'$. Wegen $m' \equiv -m' \bmod m_0$ gilt dann $r \equiv -s \equiv -t \equiv -u \equiv m' \bmod m_0$. 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, sodass wir wie eben einen Widerspruch erhalten. Es gilt also $0 < m_1 < m_0$.

Wir zeigen nun, dass $m_1 \in M$ ist; das ist der gesuchte Widerspruch, denn m_0 sollte ja das kleinste Element von M sein. Dazu berechnen wir

$$N(\alpha\beta) = N(\alpha)N(\beta) = m_1 m_0^2 p$$

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

$$N(\gamma) = N\Big(\frac{\alpha\beta}{m_0}\Big) = \frac{m_1 m_0^2 p}{m_0^2} = m_1 p\,,$$

und damit ist $m_1 \in M$ wie gewünscht. ❑

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

Aus der multiplikativen Abgeschlossenheit von S_4 folgt jetzt:

* 7.5. **Satz.** *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.

SATZ
4□-Satz von Lagrange

Dieser Satz, der bereits von Bachet und Fermat in der ersten Hälfte des 17. Jahrhunderts vermutet wurde, wurde zuerst im Jahr 1770 von Joseph-Louis Lagrange bewiesen.

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

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

7.6. **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.*

SATZ
3□-Satz

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 die analog definierten Mengen S_2 und S_4: Zum Beispiel gilt $3, 5 \in S_3$, aber $3 \cdot 5 = 15 \notin S_3$.

Man kann den Drei-Quadrate-Satz recht einfach auf eine schwächere Aussage reduzieren.

Lemma. *Ist $n \in \mathbb{Z}$ Summe dreier Quadrate rationaler Zahlen, so ist n auch Summe dreier Quadrate ganzer Zahlen.*

LEMMA
Reduktion des 3□-Satzes

Beweis. (Siehe [Sch, S. 198f].) Sei $n = x_1^2 + x_2^2 + x_3^2$ mit $x_1, x_2, x_3 \in \mathbb{Q}$. Wir können annehmen, dass der Hauptnenner c von x_1, x_2, x_3 minimal gewählt ist. Wir müssen $c = 1$ zeigen, also nehmen wir $c > 1$ an. Seien y_1, y_2, y_3 die zu x_1, x_2, x_3 nächstgelegenen ganzen Zahlen (mit willkürlicher Auswahl, wenn es zwei Möglichkeiten gibt). Wir schreiben $x = (x_1, x_2, x_3)$ und $y = (y_1, y_2, y_3)$ und verwenden $\langle x, y\rangle = x_1y_1 + x_2y_2 + x_3y_3$ für das Skalarprodukt. Wir schreiben $|x| = \sqrt{\langle x, x\rangle}$ für die euklidische Länge eines Vektors. Es gilt dann $0 < |x - y|^2 \leq 3/4 < 1$. Außerdem ist

$$c > c' := c|x - y|^2 = cn - 2\langle cx, y\rangle + c|y|^2 \in \mathbb{Z}\,.$$

Der Punkt

$$x' = x + \frac{2\langle x, x - y\rangle}{|x - y|^2}\,(y - x) = \frac{1}{c'}\big((y^2 - n)\,cx + 2(cn - \langle cx, y\rangle)\,y\big)$$

erfüllt ebenfalls $|x'|^2 = n$ (x' ist der zweite Schnittpunkt der Geraden durch x und y mit der Kugeloberfläche $|x|^2 = n$) und hat einen Nenner, der $c' < c$ teilt. Das zeigt, dass c nicht minimal war, und ergibt den gesuchten Widerspruch. ❑

Es bleibt also noch zu zeigen, dass n, wenn es nicht die Form $4^k(8l + 7)$ hat, als Summe von drei Quadraten rationaler Zahlen geschrieben werden kann. Das folgt aus dem sogenannten *Hasse-Prinzip* für quadratische Formen:

Satz. *Sei $q(x_1, x_2, \ldots, x_m) = \sum_{1\le i,j\le m} a_{ij}x_ix_j$ eine quadratische Form mit $a_{ij} \in \mathbb{Z}$. Wenn es für alle $N \in \mathbb{Z}_{>0}$ jeweils $u_1, u_2, \ldots, u_m \in \mathbb{Z}$ gibt mit $\mathrm{ggT}(u_1, u_2, \ldots, u_m, N) = 1$ und $q(u_1, u_2, \ldots, u_m) \equiv 0 \bmod N$, dann gibt es $(u_1, u_2, \ldots, u_m) \in \mathbb{Z}^m \setminus \{(0, 0, \ldots, 0)\}$ mit $q(u_1, u_2, \ldots, u_m) = 0$.*

SATZ Hasse-Prinzip

Das können wir hier nicht beweisen. Man wendet es an auf die quadratische Form

$$q_n(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 - nx_4^2\,.$$

Hat n nicht die Form $4^k(8l+7)$, dann gibt es Lösungen modulo N für alle N, also gibt es eine nichttriviale ganzzahlige Lösung (u_1, u_2, u_3, u_4). Dabei kann u_4 nicht verschwinden, damit hat man in

$$\Big(\frac{u_1}{u_4}\Big)^2 + \Big(\frac{u_2}{u_4}\Big)^2 + \Big(\frac{u_3}{u_4}\Big)^2 = n$$

eine Darstellung von n als Summe dreier rationaler Quadrate gefunden.

Hier ist noch eine nette Konsequenz des Drei-Quadrate-Satzes. Eine *Dreieckszahl* ist eine ganze Zahl der Form $n(n+1)/2$, also eine Zahl aus der Folge $0, 1, 3, 6, 10, 15, 21, 28, \ldots$.

Satz. *Jede nichtnegative ganze Zahl ist Summe dreier Dreieckszahlen.*

SATZ $n = \triangle + \triangle + \triangle$

Beweis. Sei $m \ge 0$ eine ganze Zahl. Dann ist nach dem Drei-Quadrate-Satz 7.6 $8m + 3$ als Summe dreier Quadrate darstellbar: $8m + 3 = x^2 + y^2 + z^2$. Dabei müssen x, y, z ungerade sein (Betrachtung mod 4). Wir schreiben $x = 2u + 1$, $y = 2v + 1$, $z = 2w + 1$. Es folgt

$$\begin{aligned} m &= \frac{1}{8}\big((2u+1)^2 - 1\big) + \frac{1}{8}\big((2v+1)^2 - 1\big) + \frac{1}{8}\big((2w+1)^2 - 1\big) \\ &= \frac{u(u+1)}{2} + \frac{v(v+1)}{2} + \frac{w(w+1)}{2}\,. \end{aligned}$$

❑

Der Versuch der Verallgemeinerung des Vier-Quadrate-Satzes auf höhere Potenzen führt auf das Waringsche Problem:

Gibt es für jedes $k \ge 1$ eine Zahl $g(k)$, sodass jede natürliche Zahl Summe von höchstens $g(k)$ k-ten Potenzen natürlicher Zahlen ist?

Der Vier-Quadrate-Satz sagt, dass $g(2) = 4$ ist. Waring vermutete, dass $g(3) = 9$ und $g(4) = 19$ gilt. Hilbert bewies 1909, dass Warings Frage eine positive Antwort hat. Euler vermutete bereits, dass

$$g(k) = 2^k + \Big\lfloor \Big(\frac{3}{2}\Big)^k \Big\rfloor - 2$$

für alle k gilt. (In jedem Fall gilt hier „$\ge$“, da dies die Maximalzahl von k-ten Potenzen ist, die man für die Zahlen bis $3^k - 1$ braucht.) Heute ist bekannt, dass das zutrifft, falls

$$2^k\Big(\Big(\frac{3}{2}\Big)^k - \Big\lfloor \Big(\frac{3}{2}\Big)^k \Big\rfloor\Big) + \Big\lfloor \Big(\frac{3}{2}\Big)^k \Big\rfloor \le 2^k$$

gilt, was vermutungsweise immer der Fall ist. In jedem Fall kann es nur endlich viele Ausnahmen geben (und man hätte dann ebenfalls eine Formel für $g(k)$).

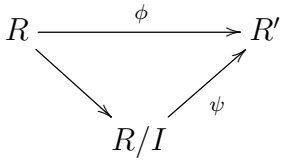
Weit schwieriger ist die Frage, was die kleinste Zahl $G(k)$ ist, so dass jede *hinreichend große* natürliche Zahl Summe von $G(k)$ k-ten Potenzen ist. Die einzigen bekannten Werte sind $G(2) = 4$ und $G(4) = 16$; sonst gibt es nur untere und obere Schranken, wie zum Beispiel $4 \le G(3) \le 7$ (mit der Vermutung $G(3) = 4$).

8. 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.

SATZ Homomorphismen von R/I

8.1. **Satz.** *Seien $\phi : R \to R'$ 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:

$$\begin{aligned} \psi([1]) &= \phi(1) = 1 \\ \psi([r_1] + [r_2]) = \psi([r_1 + r_2]) &= \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = \psi([r_1]) + \psi([r_2]) \end{aligned}$$

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

FOLG $R/I \to R/J$

8.2. **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 8.1 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. Für endliche Produkte und für Produkte R^X von Kopien desselben Rings haben wir das schon in Beispiel 3.1 gesehen.

DEF direktes Produkt von Ringen

8.3. **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

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

vergleiche Beispiel 3.1.

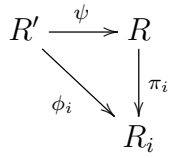
Für jedes $i \in I$ gibt es einen Ringhomomorphismus $\pi_i : R \to R_i$, der $(r_j)_{j\in I}$ auf die i-te Komponente r_i abbildet. Dieser (surjektive) Homomorphismus heißt die *i-te Projektion*.

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

Das Produkt von Ringen hat eine universelle Eigenschaft.

LEMMA Universelle Eigenschaft des Produktrings

8.4. **Lemma.** *Seien $(R_i)_{i\in I}$ 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 $\psi : R' \to R$, sodass 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. Nach Lemma 8.4 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

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

sodass 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 $b_1, b_2, \ldots, b_n \in R$, unter welchen Bedingungen gibt es stets ein Element $r \in R$ mit

$$r \equiv b_1 \bmod I_1\,, \quad r \equiv b_2 \bmod I_2\,, \quad \ldots, \quad r \equiv b_n \bmod I_n\,?$$

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

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

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

LEMMA Surjektivität von $\tilde{\psi}$

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 $\tilde{\psi}$ (oder äquivalent, ψ) surjektiv ist, dann können wir $b_j = 1$ und $b_k = 0$ für $k \neq j$ wählen, sodass wir die Elemente r_j bekommen. Umgekehrt ist $r = b_1 r_1 + \cdots + b_n r_n$ 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.

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

DEF komaximal

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

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

Das bleibt für beliebige Hauptidealringe richtig. Lässt es sich verallgemeinern?

8.7. **Lemma.** *Sei R ein Ring und seien $I_1, \ldots, I_n$ mit $n \geq 1$ paarweise komaximale Ideale von R. Dann gilt*

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

LEMMA Schnitt komaximaler Ideale

Dabei ist das Produkt der Ideale definiert durch

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

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

$$Ra_1 \cdot Ra_2 \cdots Ra_n = R(a_1 a_2 \cdots a_n)\,.$$

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 8.5 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.

SATZ Chinesischer Restsatz

∗ 8.8. **Satz.** *Sei R ein (kommutativer) Ring und seien $I_1, I_2, \ldots, I_n$ mit $n \geq 1$ paarweise komaximale Ideale von R. 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.

SATZ Chinesischer Restsatz für Hauptidealringe

∗ 8.9. **Satz.** *Sei R ein Hauptidealring und seien $a_1, a_2, \ldots, a_n \in R$ paarweise teilerfremd. Dann ist der kanonische Homomorphismus*

$$R/Ra_1a_2 \cdots a_n \longrightarrow R/Ra_1 \times R/Ra_2 \times \cdots \times R/Ra_n$$

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 mod $a_1a_2 \cdots a_n$ eindeutig bestimmt ist.

(In dieser Version darf n auch null sein. Dann steht links R/R, was ein Nullring ist, und rechts steht ein leeres Produkt von Ringen, also ebenfalls ein Nullring.)

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.

BSP simultane Kongruenzen

8.10. **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 8.5:

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

Die Lösung kommt aus dem Erweiterten Euklidischen Algorithmus (vgl. Beispiel 3.18), 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

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

Zum besseren Einprägen hier noch einmal der Algorithmus für die Lösung eines Systems von zwei Kongruenzen über $\mathbb{Z}$ (das funktioniert aber analog in jedem euklidischen Ring)

$$x \equiv b_1 \bmod a_1 \qquad \text{und} \qquad x \equiv b_2 \bmod a_2\,,$$

wobei $a_1 \perp a_2$.

(1) Berechne $u_1, u_2 \in \mathbb{Z}$ mit $u_1a_1 + u_2a_2 = 1$ mit dem Erweiterten Euklidischen Algorithmus.

(2) Setze $r_1 = u_2a_2$ und $r_2 = u_1a_1$; dann gilt $r_1 \equiv 1 \bmod a_1$, $r_1 \equiv 0 \bmod a_2$ und $r_2 \equiv 0 \bmod a_1$, $r_2 \equiv 1 \bmod a_2$.

(3) Dann ist $x_0 = b_1r_1 + b_2r_2 = b_1u_2a_2 + b_2u_1a_1$ eine Lösung. Die komplette Lösungsmenge ist die Restklasse $x_0 + a_1a_2\mathbb{Z}$.

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.

DEF direktes Produkt von Gruppen

8.11. **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 8.3) 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.

Ist $I = \{1, 2, \ldots, n\}$ endlich, dann schreiben wir auch $G_1 \times G_2 \times \cdots \times G_n$ für das direkte Produkt. $\diamondsuit$

Direkte Produkte von Gruppen haben die analoge universelle Eigenschaft wie direkte Produkte von Ringen (mit demselben Beweis).

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

8.12. **Lemma.** *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 $\prod_{i\in I} R_i$).

LEMMA Einheitengruppe im Produktring

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:

8.13. **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*. ♢

DEF Euler-ϕ

Der Name 'prime Restklassengruppe' kommt von der folgenden Tatsache:

8.14. **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.*

LEMMA prime Restklassen

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	6	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:

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

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 $0 \leq f \leq e$, 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 die Zahlen ap für $0 \leq a < p^{e-1}$), also bleiben

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

Zahlen übrig. ❑

Zusammen mit dem Chinesischen Restsatz und Lemma 8.12 erhalten wir daraus eine Formel für $\phi(n)$.

8.16. **Satz.** *Sei $n \in \mathbb{Z}_{>0}$. Dann gilt* **SATZ** Formel für $\phi(n)$

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

wobei die Produkte über die Primteiler von n laufen.

Beweis. Wir haben die Primfaktorzerlegung $n = \prod_{p|n} p^{v_p(n)}$; hierin sind die verschiedenen Primzahlpotenzen paarweise teilerfremd. Nach dem Chinesischen Restsatz gilt dann

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

und nach Lemma 8.12 dann auch

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

(Für unsere Zwecke können wir das als Bijektion lesen — ein Ringisomorphismus induziert eine Bijektion zwischen den Einheitengruppen — tatsächlich handelt es sich sogar um einen Gruppenisomorphismus. Gruppenhomomorphismen sind Abbildungen zwischen Gruppen, die mit der Verknüpfung auf beiden Seiten verträglich sind; ein Gruppenisomorphismus ist ein bijektiver Gruppenhomomorphismus.) Es folgt mit Lemma 8.15

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

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

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

LEMMA
Rekursion
für $\phi(n)$

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

wobei die Summe über alle positiven Teiler von n läuft.

Beweis. Übung. ❑

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

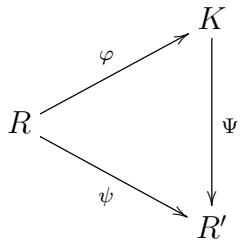
9. Der Quotientenkörper

Analog zur Konstruktion des Körpers $\mathbb{Q}$ der rationalen Zahlen aus dem Ring $\mathbb{Z}$ der ganzen Zahlen kann man jeden Integritätsbereich in einen „kleinsten“ Körper einbetten. Für $\mathbb{Q}$ führt man dazu 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 problemlos verallgemeinert werden.

* 9.1. **Satz.** *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:*

SATZ Quotientenkörper

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



Beweis. Wir konstruieren zuerst einen geeigneten Körper K zusammen mit einem 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 definieren, die Paare identifiziert, die den gleichen Quotienten repräsentieren:

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

Wir prüfen nach, dass es sich tatsächlich um eine Äquivalenzrelation handelt.

- Reflexivität: Aus $ab = ab$ folgt $(a, b) \sim (a, b)$.
- Symmetrie: $(a, b) \sim (a', b')$ bedeutet $ab' = a'b$, was zu $a'b = ab'$ und damit zu $(a', b') \sim (a, b)$ äquivalent ist.
- Transitivität: Es gelte $(a, b) \sim (a', b')$ und $(a', b') \sim (a'', b'')$. Das bedeutet $ab' = a'b$ und $a'b'' = a''b'$. Es folgt

  $$(a'b')(ab'') = (ab')(a'b'') = (a'b)(a''b') = (a'b')(a''b)$$

  (hier benutzen wir die Kommutativität von R). Ist $a' = 0$, dann folgt (wegen $b' \neq 0$) auch $a = 0$ und $a'' = 0$ und damit $ab'' = a''b$. Ist $a' \neq 0$, dann folgt (wiederum unter Verwendung von $b' \neq 0$) diese Relation ebenfalls. (Hier verwenden wir die Nullteilerfreiheit von R.) Nach Definition gilt dann auch $(a, b) \sim (a'', b'')$.

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, sodass $\psi(r)$ 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 $\psi(b)\in (R')^\times$, sodass $\psi(b)^{-1}$ existiert.) Das zeigt schon die Eindeutigkeit von Ψ. Die Existenz von Ψ als Abbildung folgt, wenn wir zeigen, dass uns die 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 $\Psi(a/b)$ dasselbe Ergebnis wie für $\Psi(a'/b')$. Es bleibt zu zeigen, dass Ψ ein Ringhomomorphismus ist. Das ist nicht schwer:

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

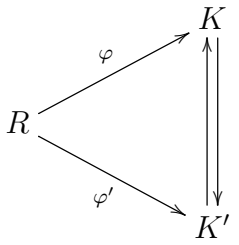
und

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

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 $K' \to K$, sodass



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. ❑

9.2. **Definition.** Der Körper K aus Satz 9.1 heißt der *Quotientenkörper* (engl. *field of fractions*) von R. ♢

DEF Quotientenkörper

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.

9.3. **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.

LEMMA Quotientenkörper von Unterringen eines Körpers

Beweis. Man zeigt das ganz genauso wie im Beweis von Satz 9.1. ❑

9.4. **Beispiel.** Als ein weiteres Beispiel können wir den Quotientenkörper von $\mathbb{Z}[\boldsymbol{i}]$ betrachten. Da $\mathbb{Z}[\boldsymbol{i}] \subset \mathbb{C}$ Unterring eines Körpers ist, kann man Lemma 9.3 anwenden und findet (Übung), dass der Quotientenkörper von $\mathbb{Z}[\boldsymbol{i}]$ gerade

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

ist. ♣

BSP Quotientenkörper von $\mathbb{Z}[\boldsymbol{i}]$

Die Schreibweise $\mathbb{Q}(\boldsymbol{i})$ ist das Analogon für Körper zur Schreibweise $\mathbb{Z}[\boldsymbol{i}]$ für Ringe: Ist K ein Körper, $K' \subset K$ ein Teilkörper (also ein Unterring, der ein Körper ist) und $A \subset K$ eine Teilmenge, dann bezeichnet $K'(A)$ den kleinsten Teilkörper von K, der sowohl K' als auch A enthält. Ist $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ endlich, dann schreiben wir wie üblich einfach $K'(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Körper werden ausführlicher in der „Einführung in die Algebra“ behandelt.

10. 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 $x \mapsto x^2$ dieselbe 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. Polynome in diesem Sinn kamen bereits in der Linearen Algebra vor; dort wurden sie gebraucht, um das charakteristische Polynom und das Minimalpolynom einer Matrix bzw. eines Endomorphismus zu definieren. Auch einige wichtige Eigenschaften von Polynomen wurden dort bereits gezeigt (und verwendet). Wir werden uns hier aber nicht darauf berufen, sondern diese Eigenschaften noch einmal beweisen.

Um zu einer sauberen Definition zu gelangen, 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.

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

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

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

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

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:

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

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

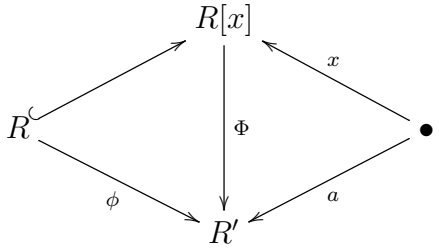
Die Idee hinter der Konstruktion des Polynomrings ist, dass man zum Ring R ein „neues“ Element x hinzufügen möchte, das von den Elementen von R vollkommen „unabhängig“ ist (außer dass es mit ihnen kommutiert). Diese Unabhängigkeit bedeutet, dass polynomiale Ausdrücke in x mit Koeffizienten in R verschieden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

* 10.2. **Satz.** *Seien R und R' Ringe, sei $a \in R'$ und sei $\phi : R \to R'$ ein Ringhomomorphismus, sodass 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 $\Phi(x) = a$:*

SATZ Universelle Eigenschaft des Polynomrings



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 $j > m$)

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

10.3. **Definition.** Wenn in der Situation von Satz 10.2 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'. $\diamondsuit$

DEF
Auswertungsabbildung
Nullstelle

Für das Rechnen mit Polynomen sind folgende Begriffe hilfreich:

10.4. **Definition.** Sei R ein Ring, $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$. 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 $f \in R \subset R[x]$. $\diamondsuit$

DEF
Grad
Leitkoeffizient
normiert
konstant

LEMMA Eigensch. des Grades

10.5. **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. Seien also $f, g \neq 0$; wir schreiben $f = \sum_{j=0}^{\infty} a_j x^j$ 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 wenigstens 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, also 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. ❑

FOLG R Int.ring $\Rightarrow R[x]$ Int.ring

10.6. **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 für $f, g \in R[x]$ die Beziehung $\deg(fg) = \deg(f) + \deg(g)$. Sind $f, g \neq 0$, dann folgt $\deg(fg) \geq 0$, also $fg \neq 0$. ❑

FOLG Einheiten in $R[x]$

10.7. **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 $f \in R^\times$. ❑

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

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

* 10.8. **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 $\deg(r) < \deg(b)$.* **SATZ** Polynomdivision

Beweis. Die Existenz beweisen wir durch Induktion nach dem Grad n von a. Ist $n < \deg(b)$, dann können wir $q = 0$ und $r = a$ wählen. Ist $n \geq \deg(b)$, dann sei $a' = a - \operatorname{lcf}(a)x^{\deg(a)-\deg(b)}b$. Nach Lemma 10.5 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 sodass $\deg(r), \deg(r') < \deg(b)$. Dann folgt $(q - q')b = r' - r$, und mit Lemma 10.5 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.

10.9. **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.* **FOLG** Nullstellen

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?)

Das Polynom $f = x^2 + 1 \in \mathbb{H}[x]$ vom Grad 2 hat mindestens die sechs verschiedenen Nullstellen $\pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}$ in $\mathbb{H}$. (Tatsächlich sind *alle* Quaternionen $\alpha = b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ mit $b^2 + c^2 + d^2 = 1$ Nullstellen, also hat f sogar überabzählbar viele Nullstellen!). Die Voraussetzung, dass R kommutativ ist, ist also auch wesentlich. (Wo geht der Beweis hier schief?)

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

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 $\beta = \operatorname{lcf}(b) \in K^\times$. Sei $b' = \beta^{-1}b$; $b' \in K[x]$ ist ein normiertes Polynom. Nach Satz 10.8 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.

10.11. **Definition.** Sei R ein faktorieller Ring und $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ ein Polynom. Dann heißt $\operatorname{cont}(f) = \operatorname{ggT}(a_0, a_1, \ldots, a_n)$ der *Inhalt* (engl. *content*) von f (der Inhalt ist 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 $\operatorname{cont}(f)$ und einem primitiven Polynom $\operatorname{pp}(f)$ (*primitive part*). Der Vollständigkeit halber setzen wir $\operatorname{pp}(0) = 1$. ♢

DEF
Inhalt
primitives Polynom

Den ggT und das kgV einer beliebigen Teilmenge A eines faktoriellen Rings R definiert man analog zu ggT und kgV von zwei Elementen (vergleiche Definition 2.9):

$g \in R$ heißt ein *größter gemeinsamer Teiler* von A, wenn $g \mid a$ gilt für alle $a \in A$ und wenn jedes $r \in R$ mit $r \mid a$ für alle $a \in A$ ein Teiler von g ist.

$k \in R$ heißt ein *kleinstes gemeinsames Vielfaches* von A, wenn $a \mid k$ gilt für alle $a \in A$ und wenn jedes $r \in R$ mit $a \mid r$ für alle $a \in A$ ein Vielfaches von k ist.

Wir schreiben dann wieder $g \sim \operatorname{ggT}(A)$, $k \sim \operatorname{kgV}(A)$, und falls $A = \{a_1, a_2, \ldots, a_n\}$ ist, auch $\operatorname{ggT}(a_1, a_2, \ldots, a_n)$ und $\operatorname{kgV}(a_1, a_2, \ldots, a_n)$.

Es gilt dann

$$\operatorname{ggT}(a_1, a_2, \ldots, a_n) \sim \operatorname{ggT}((\ldots \operatorname{ggT}(\operatorname{ggT}(a_1, a_2), a_3), \ldots), a_n)$$

und analog für das kgV. Außerdem hat man $\operatorname{ggT}(\emptyset) \sim 0$ und $\operatorname{kgV}(\emptyset) \sim 1$ (Übung).

10.12. **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 $\operatorname{cont}(f) \in K^\times$ und ein primitives Polynom $\operatorname{pp}(f) \in R[x]$ mit $f = \operatorname{cont}(f)\operatorname{pp}(f)$. Der Inhalt $\operatorname{cont}(f)$ (und damit auch $\operatorname{pp}(f)$) ist bis auf Multiplikation mit einer Einheit von R eindeutig bestimmt. Es gilt $f \in R[x]$ genau dann, wenn $\operatorname{cont}(f) \in R$.*

LEMMA
primitiver Anteil

Beweis. Sei $f = a_0 + a_1 x + \ldots + a_n x^n$ 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 $c = \operatorname{kgV}(c_0, c_1, \ldots, c_n)$, sodass $cf \in R[x]$. Wir setzen $\operatorname{cont}(f) = c^{-1}\operatorname{cont}(cf)$ und $\operatorname{pp}(f) = \operatorname{pp}(cf)$. (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 $\alpha \sim \operatorname{cont}(\alpha f) \sim \operatorname{cont}(\alpha' f') \sim \alpha'$, also $\alpha/\alpha' \in R^\times$.

Ist $\operatorname{cont}(f) \in R$, dann ist wegen $\operatorname{pp}(f) \in R[x]$ auch $f = \operatorname{cont}(f)\operatorname{pp}(f) \in R[x]$. Umgekehrt gilt natürlich (nach Definition) $\operatorname{cont}(f) \in R$ für $f \in R[x]$. ❑

* 10.13. **Lemma.** *Sei R ein faktorieller Ring und seien $f, g \in R[x]$ primitive Polynome. Dann ist fg ebenfalls primitiv.* **LEMMA** Lemma von Gauß

Wenn wir mit $\sim$ Gleichheit bis auf einen Faktor in $R^\times$ bezeichnen, folgt daraus leicht für beliebige Polynome $0 \neq f, g \in R[x]$:

$$\operatorname{cont}(fg) \sim \operatorname{cont}(f)\operatorname{cont}(g) \qquad \text{und} \qquad \operatorname{pp}(fg) \sim \operatorname{pp}(f)\operatorname{pp}(g)$$

(Übung).

Beweis. Nach Definition 10.11 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 $m, n \in \mathbb{Z}_{\geq 0}$, sodass $\pi \nmid a_m$, 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

$$(a_0 b_{m+n} + a_1 b_{m+n-1} + \ldots + a_{m-1} b_{n+1}) + a_m b_n + (a_{m+1} b_{n-1} + \ldots + a_{m+n-1} b_1 + a_{m+n} b_0)\,.$$

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.

10.14. **Lemma.** *Sei R ein faktorieller Ring mit Quotientenkörper K. Wir bezeichnen die Teilbarkeitsrelationen in R, $K[x]$ und $R[x]$ mit $|_R$, $|_{K[x]}$ und $|_{R[x]}$. Für Polynome $f, g \in R[x] \setminus \{0\}$ gilt dann* **LEMMA** Teilbarkeit in $R[x]$

$$f \mid_{R[x]} g \iff \operatorname{cont}(f) \mid_R \operatorname{cont}(g) \quad \textit{und} \quad \operatorname{pp}(f) \mid_{K[x]} \operatorname{pp}(g)\,.$$

Beweis. Es bezeichne $\sim$ Gleichheit bis auf einen Faktor in $R^\times$.

Sei $g = fh$ in $R[x]$. Aus dem Lemma von Gauß 10.13 folgt einerseits die Relation $\operatorname{cont}(g) \sim \operatorname{cont}(fh) \sim \operatorname{cont}(f)\operatorname{cont}(h)$, also $\operatorname{cont}(f) \mid_R \operatorname{cont}(g)$ und andererseits $\operatorname{pp}(g) \sim \operatorname{pp}(f)\operatorname{pp}(h)$, also $\operatorname{pp}(f) \mid_{R[x]} \operatorname{pp}(g)$ und damit auch $\operatorname{pp}(f) \mid_{K[x]} \operatorname{pp}(g)$.

Es 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 $f = \operatorname{cont}(f)\operatorname{pp}(f) \mid_{R[x]} \operatorname{cont}(g)\operatorname{pp}(g) = g$. ❑

Beachte, dass sich f und $\operatorname{pp}(f)$ nur um einen Faktor in $K^\times = K[x]^\times$ unterscheiden. Die Aussagen „$\operatorname{pp}(f) \mid_{K[x]} \operatorname{pp}(g)$“ und „$f \mid_{K[x]} g$“ sind also äquivalent. Die Aussage des Lemmas lässt sich also auch so formulieren: f teilt g in $R[x]$ genau dann, wenn f ein Teiler von g in $K[x]$ ist und zusätzlich der Inhalt von f den Inhalt von g teilt.

Lemma 10.14 liefert uns eine Beschreibung der irreduziblen Elemente von $R[x]$.

FOLG irreduzible Polynome

10.15. **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. Sei $0 \neq f \in R[x]$. Ist f konstant, dann sind die Teiler von f in $R[x]$ nach Lemma 10.14 genau die Teiler von f in R. Damit ist f genau dann irreduzibel in $R[x]$, wenn f irreduzibel in R ist. Da R faktoriell ist, ist das gleichbedeutend damit, dass f ein Primelement von R ist (vergleiche Satz 4.14).

Ist f nicht konstant, dann ist $f = \operatorname{cont}(f)\operatorname{pp}(f)$ eine Faktorisierung von f. Ist f irreduzibel, dann muss $\operatorname{cont}(f)$ eine Einheit sein, also ist f primitiv. Wir können uns im Folgenden also auf primitive Polynome beschränken.

Hat f einen nicht-trivialen Teiler g in $K[x]$ (also mit $1 \leq \deg(g) < \deg(f)$), dann gilt auch $\operatorname{pp}(g) \mid_{K[x]} f$; aus Lemma 10.14 folgt dann wegen $\operatorname{cont}(\operatorname{pp}(g)) \sim 1$ auch $\operatorname{pp}(g) \mid_{R[x]} f$, also ist f nicht irreduzibel in $R[x]$.

Ist andererseits f in $K[x]$ irreduzibel und ist g ein Teiler von f in $R[x]$, dann ist g auch ein Teiler von f in $K[x]$, also ist g konstant oder unterscheidet sich von f durch einen konstanten Faktor. Weil f primitiv ist, folgt im ersten Fall $g \in R^\times$ und im zweiten Fall $g \sim f$. Damit ist f irreduzibel in $R[x]$. ❑

Jetzt können wir den Satz beweisen.

SATZ R faktoriell $\Rightarrow R[x]$ faktoriell

* 10.16. **Satz.** *Sei R ein faktorieller Ring. Dann ist $R[x]$ ebenfalls faktoriell.*

Beweis. Wir müssen zwei Dinge zeigen (siehe Satz 4.14):

(1) 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 $N \geq 0$, sodass $f_n \sim f_N$ für alle $n \geq N$.

(2) Jedes irreduzible Element von $R[x]$ ist prim.

Wir beginnen mit (1). Wir können annehmen, dass die $f_n \neq 0$ sind, denn entweder gilt das ab irgendwann, und dann können wir die Folge einfach später beginnen lassen, oder *alle* f_n sind null, dann gilt die Behauptung trivialerweise. Aus Lemma 10.14 folgt dann, dass eine „Teilerkette“ $(f_n)_{n\geq 0}$ in $R[x]$ Teilerketten $\big(\operatorname{cont}(f_n)\big)_{n\geq 0}$ in R und $\big(\operatorname{pp}(f_n)\big)_{n\geq 0}$ in $K[x]$ ergibt. Sowohl R als auch $K[x]$ sind faktoriell, also gibt es $N \geq 0$ mit $\operatorname{cont}(f_n) \sim_R \operatorname{cont}(f_N)$ und $\operatorname{pp}(f_n) \sim_{K[x]} \operatorname{pp}(f_N)$ für alle $n \geq N$. Die Polynome $\operatorname{pp}(f_n)$ und $\operatorname{pp}(f_N)$ unterscheiden sich also um einen konstanten Faktor; da beide Polynome primitiv sind, muss der Faktor in $R^\times$ sein. Es folgt

$$f_n = \operatorname{cont}(f_n)\operatorname{pp}(f_n) \sim_{R[x]} \operatorname{cont}(f_N)\operatorname{pp}(f_N) = f_N$$

und die erste Eigenschaft ist bewiesen.

Wir zeigen jetzt die zweite Eigenschaft. Nach Folgerung 10.15 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:

$$\begin{aligned} p \mid fg &\Rightarrow p \mid \operatorname{cont}(fg) \sim \operatorname{cont}(f)\operatorname{cont}(g) \\ &\Rightarrow p \mid \operatorname{cont}(f) \mid f \quad \text{oder} \quad p \mid \operatorname{cont}(g) \mid g\,. \end{aligned}$$

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 $f = \operatorname{pp}(f) \mid_{K[x]} \operatorname{pp}(gh) \sim \operatorname{pp}(g)\operatorname{pp}(h)$, 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. ❑

10.17. **Folgerung.** *Sei R ein faktorieller Ring (zum Beispiel 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.*

FOLG
R faktoriell
$\Rightarrow$
$R[x_1, \ldots, x_n]$
faktoriell

Beweis. Induktion nach n unter Verwendung von Satz 10.16 und der rekursiven Definition $R[x_1, \ldots, x_n, x_{n+1}] = \big(R[x_1, \ldots, x_n]\big)[x_{n+1}]$. ❑

11. 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.

FOLG Irreduzibilität in $K[x]$ und $R[x]$

11.1. **Folgerung.** *Ein Polynom $0 \neq f \in K[x]$ ist genau dann irreduzibel, wenn $\operatorname{pp}(f)$ in $R[x]$ irreduzibel ist.*

Beweis. Das folgt aus Folgerung 10.15: In $K[x]$ sind alle Konstanten $\neq 0$ Einheiten, also ist f in $K[x]$ irreduzibel genau dann, wenn $\operatorname{pp}(f)$ in $K[x]$ irreduzibel ist. Das wiederum ist dazu äquivalent, dass $\operatorname{pp}(f)$ 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 $\operatorname{pp}(f) = 1$ eine Einheit in $R[x]$; beide sind daher nicht irreduzibel.) ❑

Für Polynome von niedrigem Grad haben wir folgendes Kriterium.

LEMMA Grad ≤ 3

11.2. **Lemma.** *Sei (nur für dieses Lemma) K ein beliebiger Körper und 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 genau dann irreduzibel, 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 10.9). ❑

BSP irreduzibles Polynom

11.3. **Beispiel.** Das Polynom $f = x^2 + x + 1$ ist in $\mathbb{Q}[x]$ irreduzibel, weil f keine Nullstelle in $\mathbb{Q}$ hat: $f(\xi) = \left(\xi + \frac{1}{2}\right)^2 + \frac{3}{4}$ ist für $\xi \in \mathbb{R}$ stets positiv, also hat f nicht einmal eine Nullstelle in $\mathbb{R}$. 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). ♣

BSP irreduzible Polynome über $\mathbb{R}$, $\mathbb{C}$

11.4. **Beispiel.** 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?

LEMMA rationale Nullstelle

11.5. **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 $r \mid a_0$. ❑

BSP Grad 3

11.6. **Beispiel.** Das Polynom $f = x^3 + \frac{1}{2}x^2 - x + \frac{3}{2} \in \mathbb{Q}[x]$ ist irreduzibel: Es ist $\operatorname{pp}(f) = 2x^3 + x^2 - 2x + 3 \in \mathbb{Z}[x]$. 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 $\pm\frac{3}{2}$; man rechnet nach, dass keine dieser acht Zahlen eine Nullstelle von f ist. Damit ist gezeigt, dass f keine Nullstelle in $\mathbb{Q}$ hat, also muss f irreduzibel sein. ♣

BSP Grad 4

11.7. **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. ♣

BSP Faktorisierung testen

11.8. **Beispiele.** Wenn man keine Kriterien anwenden kann, die einem direkt die Irreduzibilität liefern, dann kann man versuchen, explizit einen Teiler von $\operatorname{pp}(f)$ zu finden. Als Beispiel betrachten wir $f = x^4 + x^2 + 1 \in \mathbb{Q}[x]$. Dieses Polynom hat keine Nullstelle in $\mathbb{R}$, also auch nicht in $\mathbb{Q}$. Es bleibt die Möglichkeit einer Faktorisierung

$$\begin{aligned} f = \operatorname{pp}(f) = x^4 + x^2 + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a+c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd \end{aligned}$$

mit $a, b, c, d \in \mathbb{Z}$. Koeffizientenvergleich liefert die Bedingungen

$$a + c = 0, \qquad b + ac + d = 1, \qquad ad + bc = 0, \qquad bd = 1\,.$$

Die letzte Gleichung hat die beiden Lösungen $b = d = -1$ und $b = d = 1$. Mit $c = -a$ ergibt das

$$a^2 = -3 \qquad \text{bzw.} \qquad a^2 = 1\,.$$

Die erste Gleichung hat keine Lösung in $\mathbb{Z}$, während die zweite etwa von $a = 1$ gelöst wird. Tatsächlich ergibt $a = b = d = 1$, $c = -1$ die Faktorisierung

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)\,.$$

Für $x^4 + 8$, ebenfalls ohne rationale Nullstelle, bekommen wir analog die Bedingungen

$$a + c = 0, \qquad b + ac + d = 0, \qquad ad + bc = 0, \qquad bd = 8\,.$$

Mit $(b, d) = (1, 8), (-1, -8), (2, 4), (-2, -4)$ (das sind alle Möglichkeiten bis auf Vertauschen der Faktoren) und $c = -a$ erhalten wir aus der zweiten Gleichung

$$a^2 = b + d = 9, \quad -9, \quad 6, \quad -6\,.$$

Nur im ersten Fall gibt es Lösungen $a = \pm 3$. Eingesetzt in die dritte Gleichung liefert das $0 = \pm 3(d-b) = \pm 3{\cdot}7$, ein Widerspruch. Also gibt es keine Faktorisierung in Polynome vom Grad 2; damit ist $x^4 + 8 \in \mathbb{Q}[x]$ irreduzibel. ♣

Eine häufig erfolgreiche Methode arbeitet mit *Reduktion*. Wenn $p \in R$ ein Primelement ist, dann ist R/Rp ein Integritätsbereich (denn Rp ist ein Primideal, vergleiche Satz 6.20). Der Einsetzungshomomorphismus, der zum kanonischen Epimorphismus $R \to R/Rp$ und $x \mapsto x$ gehört (vergleiche Satz 10.2 und Definition 10.3) liefert einen kanonischen Homomorphismus $R[x] \to (R/Rp)[x]$. Um ihn anzuwenden, muss man die Koeffizienten „modulo p reduzieren“.

* 11.9. **Satz.** *Sei $p \in R$ prim und $f \in R[x]$ primitiv mit $p \nmid \operatorname{lcf}(f)$. Ist das Bild von f in $(R/Rp)[x]$ irreduzibel, so ist f in $R[x]$ irreduzibel.*

SATZ Reduktionskriterium

Beweis. Wir schreiben $\bar f$ für das Bild von f in $(R/Rp)[x]$; analog für andere Polynome. Ist $f = gh$ mit $1 \le \deg(g) < \deg(f)$, dann folgt $\bar f = \bar g\,\bar h$ in $(R/Rp)[x]$. Aus $p \nmid \operatorname{lcf}(f)$ folgt $p \nmid \operatorname{lcf}(g)$, $p \nmid \operatorname{lcf}(h)$, 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. ❑

11.10. **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)

BSP irred. Polynome über $\mathbb{F}_2$

$$x, \quad x+1, \qquad x^2+x+1, \qquad x^3+x+1, \quad x^3+x^2+1$$
$$x^4+x+1, \quad x^4+x^3+1, \quad x^4+x^3+x^2+x+1\,.$$

(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 11.2 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 $x^4 + x + 1$. ♣

BSP Reduktionskriterium nicht ausreichend

11.11. **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 das Polynom x^4+9. Ähnlich wie in Beispiel 11.8 zeigt man, dass es irreduzibel ist. Für den Nachweis, dass man stets eine Zerlegung mod p hat, braucht man die Theorie der quadratischen Reste (siehe später in dieser Vorlesung). Zum Beispiel gilt:

$$\begin{aligned}
x^4+9 &\equiv (x+1)^4 \bmod 2\\
x^4+9 &\equiv x^4 \bmod 3\\
x^4+9 &\equiv (x+1)(x+2)(x-2)(x-1) \bmod 5\\
x^4+9 &\equiv (x^2+x-3)(x^2-x-3) \bmod 7\\
x^4+9 &\equiv (x^2+4x-3)(x^2-4x-3) \bmod 11\\
&\vdots \quad \vdots \qquad\qquad \vdots
\end{aligned}$$

Demgegenüber funktioniert das Reduktionskriterium für x^4+8, denn die Reduktion modulo 5 ist irreduzibel. Allerdings erfordert der Nachweis, dass das so ist, eher mehr an Rechnung als die Methode von Beispiel 11.8. ♣

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 nichttrivialer 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.

Hinter der Aussage, dass x^4+9 modulo p stets reduzibel ist, stecken die Faktorisierungen

$$x^4+9 = (x^2+3\boldsymbol{i})(x^2-3\boldsymbol{i}) = (x^2+\sqrt{6}x+3)(x^2-\sqrt{6}x+3) = (x^2+\sqrt{6}\boldsymbol{i}x-3)(x^2-\sqrt{6}\boldsymbol{i}x-3)$$

über den Ringen $\mathbb{Z}[\boldsymbol{i}]$, $\mathbb{Z}[\sqrt{6}]$ und $\mathbb{Z}[\sqrt{6}\boldsymbol{i}]$. Aus der Theorie der quadratischen Reste folgt, dass für jede Primzahl p stets mindestens eine der Zahlen -1, 6 und -6 ein Quadrat modulo p ist (d.h., das Bild in $\mathbb{F}_p$ ist ein Quadrat). Damit lässt sich stets mindestens eine der obigen Faktorisierungen auch über $\mathbb{F}_p$ realisieren. Siehe das Kleingedruckte auf Seite 76.

Die Existenz der Faktorisierungen wiederum hängt mit der Darstellung der Nullstellen von x^4+n^2 in der Form $\frac{1}{2}(\pm\sqrt{2n} \pm \sqrt{2n}\boldsymbol{i})$ zusammen. Für x^4+8 hat man keine Darstellung der Nullstellen durch einfache (nicht verschachtelte) Quadratwurzeln. Eine genauere Analyse dieses Phänomens ist mithilfe der *Galois-Theorie* möglich, die wir eventuell am Ende der „Einführung in die Algebra“ kurz anreißen werden.

Ein weiteres wichtiges Kriterium ist das *Eisenstein-Kriterium*. Es basiert ebenfalls auf Reduktion, verwendet aber noch ein zusätzliches Argument.

LEMMA Teiler von ax^n

11.12. **Lemma.** *Sei R' ein Integritätsbereich, seien $a \in R' \setminus \{0\}$ und $n \geq 0$. Dann sind die Teiler von ax^n in $R'[x]$ genau die Polynome der Form bx^m mit $b \mid a$ (insbesondere $b \neq 0$) und $m \leq n$.*

Beweis. Es ist klar, dass die angegebenen Polynome Teiler sind. Sei umgekehrt $g \in R'[x]$ ein Teiler von ax^n. Dann gibt es $h \in R'[x]$ mit $ax^n = gh$; außerdem gilt $\deg(g) + \deg(h) = n$ (denn R' ist ein Integritätsring, vergleiche Lemma 10.5), also ist $m = \deg(g) \leq n$. Wir schreiben

$$g = b_0 + b_1 x + \ldots + b_m x^m \quad \text{und} \quad h = c_0 + c_1 x + \ldots + c_{n-m} x^{n-m} .$$

Sei $0 \leq k \leq m$ der kleinste Index mit $b_k \neq 0$ und $0 \leq l \leq n - m$ der kleinste Index mit $c_l \neq 0$. Analog zum Beweis des Lemmas von Gauß 10.13 folgt, dass der Koeffizient von x^{k+l} in gh nicht null ist (hier verwenden wir wieder, dass R' nullteilerfrei ist). Wegen $gh = ax^n$ muss $k + l = n$ sein, also $k = m$ und $l = n - m$. Damit haben g und h die Form $g = bx^m$, $h = cx^{n-m}$ mit $bc = a$; das war zu zeigen. ❑

* 11.13. **Satz.** *Sei $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ primitiv und nicht konstant und sei $p \in R$ ein Primelement mit $p \nmid a_n$, $p \mid a_j$ für $0 \leq j < n$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.*

SATZ Eisenstein-Kriterium

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 nach Lemma 11.12 (beachte, dass R/Rp ein Integritätsbereich ist, denn Rp ist ein Primideal, vergleiche Satz 6.20) $\bar{g} = u'x^m$, $\bar{h} = u''x^{n-m}$ mit $0 \neq u', u'' \in R/Rp$ und $1 \leq m \leq n - 1$. 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. ❑

11.14. **Beispiele.** Für jedes $n \geq 2$ ist das Polynom $x^n + 6x + 3$ in $\mathbb{Z}[x]$ irreduzibel, denn man kann das Eisenstein-Kriterium mit $p = 3$ anwenden.

BSP Eisenstein-Kriterium

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 genau dann irreduzibel ist, 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 $p = 2$. (Das funktioniert übrigens auch mit $x^4 + 9$.)

Ähnlich sieht man, dass für eine Primzahl p das Polynom $f_p = 1 + x + \ldots + x^{p-1}$ in $\mathbb{Z}[x]$ 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 $f_m \mid f_n$.

11.15. **Beispiel.** 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. ♣

BSP Eisenstein-Kriterium über $\mathbb{Q}[x]$

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.

11.16. **Definition.** Sei R ein kommutativer Ring, $f = a_0+a_1x+\ldots+a_nx^n \in R[x]$. Die *Ableitung* von f ist

$$f' = a_1 + 2a_2x + \ldots + na_nx^{n-1} = \sum_{j=1}^{n} ja_jx^{j-1}\,. \qquad \diamondsuit$$

DEF Ableitung

11.17. **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.*

LEMMA Ableitungsregeln

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. (Die *Charakteristik* eines Körpers K wurde in der Linearen Algebra definiert: Sie ist der nichtnegative Erzeuger des Ideals $\ker(\mathbb{Z} \to K)$ von $\mathbb{Z}$, wobei $\mathbb{Z} \to K$ der eindeutig bestimmte Ringhomomorphismus ist.)

Beweis. Die ersten beiden Punkte folgen leicht aus der Definition. Für die dritte Aussage genügt es, den Fall $f = x^m$, $g = x^n$ zu betrachten. Dann ist aber

$$(fg)' = (m+n)x^{m+n-1} = (mx^{m-1})x^n + x^m(nx^{n-1}) = f'g+fg'\,.$$

Der allgemeine Fall folgt aus dem Distributivgesetz und Teil (2).

Die Ungleichung in der vierten Aussage 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 null oder 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.

SATZ
Kriterium für quadratfrei

11.18. **Satz.** *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 $p^2 \mid f$. ❑

BSP
quadratfrei

11.19. **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 11.18 für beliebige Körper, wenn man „quadratfrei“ durch „quadratfrei über jedem Erweiterungskörper“ ersetzt.

12. Quadratische Reste und das Quadratische Reziprozitätsgesetz

Unser nächstes Ziel ist die Beantwortung der folgenden Frage:

Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Wie stellt man fest, ob die Kongruenz

$$x^2 \equiv a \bmod p$$

in $\mathbb{Z}$ lösbar ist?

Die Antwort wird durch das *Quadratische Reziprozitätsgesetz* geliefert.

Zunächst aber noch ein wichtiges Ergebnis über endliche Körper.

* 12.1. **Satz.** *Sei F ein endlicher Körper mit q Elementen. Dann gelten die folgenden beiden Aussagen:*

SATZ Kleiner Satz von Fermat

(1) *Für alle $a \in F^\times$ gilt $a^{q-1} = 1$.*

(2) *Für alle $a \in F$ gilt $a^q = a$.*

Beweis. Wir zeigen die erste Aussage; die zweite folgt durch Multiplikation mit a (der Fall $a = 0$ ist klar). Sei also $a \in F^\times$. Wir betrachten das Produkt

$$P = \prod_{b \in F^\times} b \in F^\times .$$

Die Abbildung $F^\times \to F^\times$, $b \mapsto ab$, ist eine Permutation (die inverse Abbildung ist $b \mapsto a^{-1}b$), also gilt

$$P = \prod_{b \in F^\times} b = \prod_{b \in F^\times} (ab) = a^{\#F^\times} \prod_{b \in F^\times} b = a^{q-1} P ,$$

und da $P \neq 0$ ist, folgt daraus $a^{q-1} = 1$. ❑

Wir erinnern uns an die endlichen Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für jede Primzahl p. Wenn man Satz 12.1 auf $\mathbb{F}_p$ anwendet, erhält man die Aussagen

(1) Für alle $a \in \mathbb{Z}$ mit $p \nmid a$ gilt $a^{p-1} \equiv 1 \bmod p$.

(2) Für alle $a \in \mathbb{Z}$ gilt $a^p \equiv a \bmod p$.

Wir führen jetzt die relevanten Begriffe ein.

* 12.2. **Definition.** Sei p eine ungerade Primzahl (also $p > 2$) und a eine nicht durch p teilbare ganze Zahl. Ist die Kongruenz $x^2 \equiv a \bmod p$ in $\mathbb{Z}$ lösbar, dann heißt a ein *quadratischer Rest* (QR) mod p. Anderenfalls heißt a ein *quadratischer Nichtrest* (QNR) mod p. Äquivalent kann man sagen, dass a ein QR (bzw. QNR) mod p ist, wenn $[a] \in \mathbb{F}_p^\times$ ein Quadrat (bzw. kein Quadrat) ist.

DEF quadratischer Rest bzw. Nichtrest

Legendre-Symbol

Für beliebiges $a \in \mathbb{Z}$ definieren wir das *Legendre-Symbol* wie folgt:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p \mid a \\ 1 & \text{falls } a \text{ quadratischer Rest mod } p \\ -1 & \text{falls } a \text{ quadratischer Nichtrest mod } p \end{cases} \qquad \diamondsuit$$

Aus der Definition folgt unmittelbar:

$$a \equiv b \bmod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) .$$

BSP QR, QNR für kleine p

12.3. **Beispiel.** Hier ist eine kleine Tabelle mit den quadratischen Resten bzw. Nichtresten zwischen 1 und $p-1$:

p	3	5	7	11	13	17
QR	1	1, 4	1, 2, 4	1, 3, 4, 5, 9	1, 3, 4, 9, 10, 12	1, 2, 4, 8, 9, 13, 15, 16
QNR	2	2, 3	3, 5, 6	2, 6, 7, 8, 10	2, 5, 6, 7, 8, 11	3, 5, 6, 7, 10, 11, 12, 14

Um alle quadratischen Reste mod p zu finden, bestimmt man die Restklassen der Quadrate 1^2, 2^2, …, $(\frac{p-1}{2})^2$. (Wegen $(-a)^2 = a^2$ ergeben die Quadrate von $(p+1)/2 \equiv -(p-1)/2, \ldots, p-2 \equiv -2, p-1 \equiv -1 \bmod p$ keine neuen Restklassen.) ♣

Es fällt auf, dass es stets genau so viele quadratische Reste wie Nichtreste gibt. Das ist kein Zufall:

LEMMA gleich viele QR wie QNR

12.4. **Lemma.** *Sei p eine ungerade Primzahl. Unter den Zahlen $1, 2, \ldots, p-1$ gibt es genau $(p-1)/2$ quadratische Reste und $(p-1)/2$ quadratische Nichtreste mod p.*

Beweis. Die Aussage ist äquivalent dazu, dass es in $\mathbb{F}_p^\times$ genauso viele Quadrate wie Nichtquadrate gibt. Wir betrachten die Abbildung

$$q : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times, \quad a \longmapsto a^2 \,.$$

Ihre Fasern $q^{-1}(\{c\})$ haben entweder null oder zwei Elemente: Da $\mathbb{F}_p$ ein Körper ist, gilt

$$b^2 = a^2 \iff (b-a)(b+a) = 0 \iff b = \pm a \,;$$

wegen $p \neq 2$ und $a \neq 0$ gilt $a \neq -a$, also haben die nichtleeren Fasern stets zwei Elemente a und $-a$. Es folgt, dass $\#\operatorname{im}(q) = \#\mathbb{F}_p^\times/2 = (p-1)/2$ ist. Es gibt also genau $(p-1)/2$ Quadrate in $\mathbb{F}_p^\times$ und demnach auch $(p-1)/2$ Nichtquadrate. ❑

Man kann die Aussage von Lemma 12.4 kurz und prägnant so ausdrücken:

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = 0 \,.$$

SATZ Euler-Kriterium

* 12.5. **Satz.** *Sei p eine ungerade Primzahl. Für $a \in \mathbb{Z}$ gilt*

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

Durch diese Kongruenz ist das Legendre-Symbol eindeutig festgelegt.

Beweis. Für $p \mid a$ ist das klar. Wir können also $p \nmid a$ annehmen. Nach dem kleinen Satz von Fermat 12.1 gilt dann $a^{p-1} \equiv 1 \bmod p$. Da p eine Primzahl ist, folgt aus

$$p \mid a^{p-1} - 1 = (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \,,$$

dass $a^{(p-1)/2} \equiv \pm 1 \bmod p$ sein muss. Ist a ein quadratischer Rest mod p, dann gibt es $b \in \mathbb{Z}$ mit $a \equiv b^2 \bmod p$, und es folgt $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \bmod p$. In diesem Fall stimmt die Behauptung also. Im Körper $\mathbb{F}_p$ kann das Polynom $x^{(p-1)/2} - 1$ höchstens $(p-1)/2$ Nullstellen haben; die Restklassen $[a]$ für quadratische Reste a tragen aber nach Lemma 12.4 bereits $(p-1)/2$ Nullstellen bei. Also folgt für jeden quadratischen Nichtrest a mod p, dass $a^{(p-1)/2} \not\equiv 1 \bmod p$ ist; es bleibt dann nur die Möglichkeit $a^{(p-1)/2} \equiv -1 \bmod p$.

Die Eindeutigkeit folgt daraus, dass 0, 1 und -1 mod p in verschiedenen Restklassen liegen, wenn $p > 2$ ist. ❑

12.6. **Folgerung.** *Sei p eine ungerade Primzahl. Für $a, b \in \mathbb{Z}$ gilt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

FOLG Legendre-Symbol ist multiplikativ

Beweis. Wir verwenden das Euler-Kriterium 12.5:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p\,.$$

Da beide Seiten in $\{-1, 0, 1\}$ liegen, folgt aus der Kongruenz die Gleichheit. ❑

Die Aussage der Folgerung lässt sich für $p \nmid a, b$ auch so zusammenfassen:

$$\begin{aligned} a \text{ QR und } b \text{ QR} &\implies ab \text{ QR} \\ a \text{ QR und } b \text{ QNR} &\implies ab \text{ QNR} \\ a \text{ QNR und } b \text{ QR} &\implies ab \text{ QNR} \\ a \text{ QNR und } b \text{ QNR} &\implies ab \text{ QR} \end{aligned}$$

Zum Beispiel gilt für jede Primzahl $p \geq 5$, dass mindestens eine der Zahlen $2, 3, 6$ ein quadratischer Rest mod p sein muss: Sind 2 und 3 QNR mod p, dann ist $6 = 2 \cdot 3$ ein QR mod p.

Ganz genauso zeigt man, dass für jede Primzahl $p \geq 5$ wenigstens eine der Zahlen -1, 6 und -6 ein QR mod p ist. Ist -1 ein QR mod p, dann gibt es $a \in \mathbb{Z}$ mit $a^2 \equiv -1$ mod p und man bekommt die Faktorisierung

$$x^4 + 9 \equiv (x^2 + 3a)(x^2 - 3a) \bmod p\,.$$

Ist 6 ein QR mod p, dann gibt es $b \in \mathbb{Z}$ mit $b^2 \equiv 6$ mod p und es gilt

$$x^4 + 9 \equiv (x^2 + bx + 3)(x^2 - bx + 3) \bmod p\,.$$

Ist schließlich -6 ein QR mod p und $c \in \mathbb{Z}$ mit $c^2 \equiv -6$ mod p, dann haben wir

$$x^4 + 9 \equiv (x^2 + cx - 3)(x^2 - cx - 3) \bmod p\,.$$

Da es auch für $p = 2$ und $p = 3$ Faktorisierungen gibt, haben wir die Behauptung aus Beispiel 11.11 bewiesen, dass man die Irreduzibilität von $x^4 + 9$ nicht mit dem Reduktionskriterium zeigen kann.

Aus dem Euler-Kriterium können wir auch schon einmal ableiten, wann -1 ein quadratischer Rest mod p ist und wann nicht.

* 12.7. **Folgerung.** *Sei p eine ungerade Primzahl. Dann gilt*

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

FOLG Erstes Ergänzungsgesetz zum QRG

Beweis. Es gilt

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

Da beide Seiten den Wert ± 1 haben, folgt Gleichheit. ❑

Also ist -1 quadratischer Rest mod p genau dann, wenn $p \equiv 1 \bmod 4$ ist. Die Aussage von Folgerung 12.7 wird auch als *Erstes Ergänzungsgesetz zum Quadratischen Reziprozitätsgesetz* bezeichnet. Der Grund dafür wird später klar werden.

In Lemma 5.6 hatten wir bereits auf andere Weise gezeigt, dass -1 quadratischer Rest mod p ist, wenn $p \equiv 1 \bmod 4$ ist. Wie dort versprochen, holen wir noch den Beweis des Satzes von Wilson nach.

SATZ Wilsonsche Kongruenz

12.8. **Satz.** *Eine Zahl $n \in \mathbb{Z}_{\geq 2}$ ist genau dann prim, wenn $(n-1)! \equiv -1 \bmod n$ ist.*

Beweis. Ist n keine Primzahl, dann sei $p < n$ ein Primteiler von n. Es folgt $p \mid (n-1)!$ und damit $p \mid \mathrm{ggT}(n, (n-1)!)$; dann kann $(n-1)!$ nicht kongruent zu $-1 \bmod n$ sein.

Ist $n = p$ eine Primzahl, dann ist die Behauptung äquivalent zu

$$P = \prod_{a \in \mathbb{F}_p^\times} a = -1\,,$$

wobei P das Produkt aus dem Beweis von Satz 12.1 ist. Für $p = 2$ ist das klar, deshalb können wir p ungerade annehmen. Die Abbildung $i : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $a \mapsto a^{-1}$, ist eine Involution (also $i \circ i = \mathrm{id}_{\mathbb{F}_p^\times}$), die genau die zwei Fixpunkte 1 und -1 hat (ein *Fixpunkt* von i ist ein Element a mit $i(a) = a$), denn $i(a) = a$ ist äquivalent zu $a^2 = 1$, und das Polynom $x^2 - 1$ hat im Körper $\mathbb{F}_p$ genau die beiden Nullstellen 1 und -1. Sei $S \subset \mathbb{F}_p^\times \setminus \{1, -1\}$ eine Teilmenge, die jeweils genau ein Element aus jeder zweielementigen Menge $\{a, i(a)\}$ enthält. Dann ist

$$P = 1 \cdot (-1) \cdot \prod_{a \in S} (a \cdot a^{-1}) = -1$$

wie behauptet. ❑

Wie sieht es damit aus, wann 2 quadratischer Rest mod p ist? Hier ist eine Tabelle mit Einträgen + für „ja“ und − für „nein“:

	$3:-$	$5:-$	$7:+$
	$11:-$	$13:-$	
$17:+$	$19:-$		$23:+$
		$29:-$	$31:+$
		$37:-$	
$41:+$	$43:-$		$47:+$

Es drängt sich folgende Vermutung auf:

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

Wir werden bald einen Beweis dafür geben. Erst brauchen wir aber noch einige Vorbereitungen.

Wir erinnern uns an die Definition von $R[a]$ als dem kleinsten Unterring eines Rings R' (wobei $R \subset R'$ und $a \in R'$), der sowohl R als auch a enthält. In ähnlicher Weise wie man die Elemente von Untervektorräumen oder Idealen als Linearkombinationen der Erzeuger darstellen kann, gibt es eine Beschreibung der Elemente von $R[a]$ mittels des Einsetzungshomomorphismus.

LEMMA Elemente von $R[a]$

12.9. **Lemma.** *Seien R' ein kommutativer Ring, $R \subset R'$ ein Unterring und $a \in R'$. Dann gilt*

$$R[a] = \{f(a) \mid f \in R[x]\}\,.$$

Beweis. Die rechte Seite ist das Bild des Einsetzungshomomorphismus $R[x] \to R'$, der x auf a abbildet; diese Menge ist also ein Unterring von R'. Auf der anderen Seite ist klar, dass jeder R und a enthaltende Unterring von R' auch alle $f(a)$ mit Polynomen $f \in R[x]$ enthalten muss. Die Menge rechts ist also der kleinste Unterring von R', der $R \cup \{a\}$ enthält, also definitionsgemäß gleich $R[a]$. ❑

Ringe wie $\mathbb{Z}[i]$ oder $\mathbb{Z}[\sqrt[3]{2}]$ sind Spezialfälle (für $R' = \mathbb{C}$, $R = \mathbb{Z}$ und $f = x^2 + 1$ bzw. $f = x^3 - 2$) des folgenden Sachverhalts.

LEMMA $R[a]$ für Nullstelle a eines irred. Polynoms

12.10. **Lemma.** *Seien R' ein Integritätsbereich, $R \subset R'$ ein Unterring und $a \in R'$ eine Nullstelle des normierten Polynoms $f \in R[x]$ vom Grad n. Wir nehmen an, dass f in $K[x]$ irreduzibel ist, wobei K der Quotientenkörper von R ist. Dann lassen sich die Elemente von $R[a]$ eindeutig in der Form*

$$r_0 + r_1 a + r_2 a^2 + \ldots + r_{n-1} a^{n-1}$$

schreiben, wobei $r_0, r_1, \ldots, r_{n-1} \in R$. Insbesondere gilt $(R[a])^\times \cap R = R^\times$.

Beweis. Nach Lemma 12.9 haben alle Elemente von $R[a]$ die Form $h(a)$ mit einem Polynom $h \in R[x]$. Nach Satz 11.8 (Division mit Rest für Polynome) gibt es Polynome $q, r \in R[x]$ mit $h = qf + r$ und $\deg(r) \le n - 1$, also

$$r = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1}\,.$$

Anwenden des Einsetzungshomomorphismus $x \mapsto a$ liefert

$$h(a) = q(a)f(a) + r(a) = r(a) = r_0 + r_1 a + \ldots + r_{n-1} a^{n-1}\,.$$

Damit ist gezeigt, dass sich jedes Element in der angegebenen Weise schreiben lässt. Es bleibt die Eindeutigkeit zu zeigen, d.h. die Injektivität der Abbildung

$$\phi : R^n \longrightarrow R[a]\,, \quad (r_0, r_1, \ldots, r_{n-1}) \longmapsto r_0 + r_1 a + \ldots + r_{n-1} a^{n-1}\,.$$

Diese Abbildung ist mit der Addition verträglich. Das übliche Argument zeigt, dass aus $\phi^{-1}(\{0\}) = \{\mathbf{0}\}$ die Injektivität folgt. Sei also $(r_0, \ldots, r_{n-1}) \in R^n$ mit $\phi(r_0, \ldots, r_{n-1}) = 0$. Das bedeutet für das Polynom

$$r = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} \in R[x]\,,$$

dass $r(a) = 0$ ist. Wir nehmen jetzt an, dass $r \neq 0$ ist und wollen daraus einen Widerspruch ableiten. Sei K der Quotientenkörper von R, dann ist $K[x]$ ein Hauptidealring, und wir können r und f auch als Elemente von $K[x]$ auffassen. Da f in $K[x]$ irreduzibel ist und $0 \le \deg(r) < \deg(f)$, sind r und f in $K[x]$ teilerfremd, also gibt es Polynome $u_1, v_1 \in K[x]$ mit $u_1 r + v_1 f = 1$. Durch Multiplikation mit einem gemeinsamen Nenner $d \in R \setminus \{0\}$ erhalten wir $u = du_1, v = dv_1 \in R[x]$ und $ur + vf = d$. Einsetzen von a liefert den Widerspruch

$$0 = u(a)r(a) + v(a)f(a) = d\,.$$

Also muss $r = 0$, sein; damit ist ϕ injektiv.

Für den Beweis des Zusatzes sei $u \in (R[a])^\times \cap R$. Dann gibt es

$$v = r_0 + r_1 a + \ldots + r_{n-1} a^{n-1} \in R[a] \qquad \text{mit} \quad uv = 1\,.$$

Wir erhalten die Relation

$$1 = uv = (ur_0) + (ur_1)a + \ldots + (ur_{n-1})a^{n-1}\,.$$

Da die Darstellung als R-Linearkombination von $1, a, \ldots, a^{n-1}$ eindeutig ist, folgt $ur_0 = 1$, also $u \in R^\times$. Die umgekehrte Inklusion ist trivial. ❑

* 12.11. **Lemma.** *Sei R ein kommutativer Ring und sei p eine Primzahl. Dann gilt in R:*

LEMMA „Freshman's Dream"

$$(r_1 + r_2 + \ldots + r_n)^p \equiv r_1^p + r_2^p + \ldots + r_n^p \bmod Rp\,.$$

Beweis. Es genügt der Fall $n = 2$ ($n < 2$ ist trivial, der allgemeine Fall folgt dann durch Induktion). Es gilt

$$(r_1 + r_2)^p = \sum_{j=0}^{p} \binom{p}{j} r_1^{p-j} r_2^j = r_1^p + \binom{p}{1} r_1^{p-1} r_2 + \ldots + \binom{p}{p-1} r_1 r_2^{p-1} + r_2^p\,,$$

wobei alle Terme außer dem ersten und letzten durch p teilbar sind, denn die entsprechenden Binomialkoeffizienten sind durch p teilbar (in $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ teilt p den Zähler, aber nicht den Nenner). Die Behauptung folgt. ❑

Äquivalent kann man Lemma 12.11 auch so formulieren (betrachte R/Rp):

Sei R ein kommutativer Ring und p eine Primzahl, sodass in R gilt $p \cdot 1 = 0$. Dann gilt für $r_1, \ldots, r_n$ in R stets $(r_1 + \ldots + r_n)^p = r_1^p + \ldots + r_n^p$.

Diese Aussage ist (vor allem in den USA) auch als „Freshman's Dream" bekannt (Freshman = Studienanfänger), weil sich damit Potenzen von Summen so schön vereinfachen lassen.

Jetzt können wir unsere Vermutung über $\left(\frac{2}{p}\right)$ beweisen.

* 12.12. **Satz.** *Ist p eine ungerade Primzahl, dann gilt*

SATZ Zweites Ergänzungsgesetz zum QRG

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

Beweis. Sei $\tau \in \mathbb{C}$ eine Zahl mit $\tau^4 = -1$, und sei $R = \mathbb{Z}[\tau]$. Dann gilt

$$(\tau + \tau^{-1})^2 = \tau^2 + 2 + \tau^{-2} = 2 + \tau^{-2}(\tau^4 + 1) = 2$$

und, für n ungerade,

$$\tau^n + \tau^{-n} = (-1)^{(n^2-1)/8}(\tau + \tau^{-1})\,,$$

denn $\tau^{1+8k} = \tau$, $\tau^{3+8k} = -\tau^{-1}$, $\tau^{5+8k} = -\tau$ und $\tau^{7+8k} = \tau^{-1}$ für $k \in \mathbb{Z}$. Wir haben dann mit Lemma 12.11 folgende Kongruenzen mod Rp:

$$(\tau + \tau^{-1})^p \equiv \tau^p + \tau^{-p} = (-1)^{(p^2-1)/8}(\tau + \tau^{-1})$$

und (unter Verwendung des Euler-Kriteriums 12.5)

$$(\tau + \tau^{-1})^p = \big((\tau + \tau^{-1})^2\big)^{(p-1)/2}(\tau + \tau^{-1}) = 2^{(p-1)/2}(\tau + \tau^{-1}) \equiv \left(\frac{2}{p}\right)(\tau + \tau^{-1})\,.$$

Durch Multiplikation mit $(\tau + \tau^{-1})$ ergibt sich

$$2(-1)^{(p^2-1)/8} \equiv 2\left(\frac{2}{p}\right) \bmod Rp\,,$$

und weil 2 mod p invertierbar ist (p ist ungerade), folgt

$$(-1)^{(p^2-1)/8} \equiv \left(\frac{2}{p}\right) \bmod Rp\,.$$

Nach Lemma 12.10 (beachte, dass $x^4+1 \in \mathbb{Z}[x]$ irreduzibel ist), ist p keine Einheit in $\mathbb{Z}[\tau]$. Wegen p ungerade gilt dann auch $2 \notin Rp$. Daher können wir aus der Kongruenz mod Rp oben auf Gleichheit schließen. ❑

Die Aussage von Satz 12.12 heißt auch das *Zweite Ergänzungsgesetz zum Quadratischen Reziprozitätsgesetz*.

Nachdem wir nun zwei „Ergänzungsgesetze“ kennen, stellt sich natürlich die Frage, was das *Quadratische Reziprozitätsgesetz* selbst aussagt. Wir bemerken dafür zunächst, dass ein Teil der Aussage der Ergänzungsgesetze sich auch wie folgt formulieren lässt:

- Ob -1 quadratischer Rest oder Nichtrest mod p ist, hängt nur von p mod 4 ab.
- Ob 2 quadratischer Rest oder Nichtrest mod p ist, hängt nur von p mod 8 ab.

Die Frage, die sich dann stellt, ist, ob sich das verallgemeinern lässt:

- Ob a QR oder QNR mod p ist, hängt nur von p mod $N(a)$ ab.

Dabei wäre noch ein geeigneter Wert für $N(a)$ zu bestimmen. Wegen der Multiplikativität des Legendre-Symbols genügt es, Primzahlen a zu betrachten. Wenn man sich ähnliche Tabellen macht wie oben für $a = 2$, findet man folgende wahrscheinliche Werte für $N(a)$:

a	3	5	7	11	13	17	19	23
$N(a)$	12	5	28	44	13	17	76	92

Man könnte also folgende Vermutung formulieren: Für eine ungerade Primzahl q gilt

$$N(q) = \begin{cases} q & \text{falls } q \equiv 1 \bmod 4, \\ 4q & \text{falls } q \equiv 3 \bmod 4. \end{cases}$$

Das Quadratische Reziprozitätsgesetz zeigt, dass diese Vermutung richtig ist, und sagt auch noch, wie man $\left(\frac{q}{p}\right)$ bestimmen kann. Zuerst noch eine Definition.

12.13. **Definition.** Sei p eine ungerade Primzahl. Dann sei **DEF** p^*

$$p^* = (-1)^{(p-1)/2} p = \begin{cases} p & \text{falls } p \equiv 1 \bmod 4, \\ -p & \text{falls } p \equiv 3 \bmod 4. \end{cases}$$

Es gilt dann stets $p^* \equiv 1 \bmod 4$. ♢

* 12.14. **Satz.** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt* **SATZ** Quadratisches Reziprozitätsgesetz

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

Das bedeutet: Für $p \equiv 1 \bmod 4$ oder $q \equiv 1 \bmod 4$ gilt $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. Im anderen Fall $p \equiv q \equiv 3 \bmod 4$ gilt dagegen $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Bevor wir uns über einen Beweis Gedanken machen, überlegen wir uns, dass daraus wirklich unsere Vermutung über $N(q)$ folgt:

- Ist $q \equiv 1 \bmod 4$, dann gilt stets $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, und das Symbol $\left(\frac{p}{q}\right)$ hängt nur von $p \bmod q$ ab.
- Ist $q \equiv 3 \bmod 4$, dann gilt $\left(\frac{q}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{q}\right)$. Der erste Faktor hängt nur von $p \bmod 4$ ab, der zweite nur von $p \bmod q$. Das Produkt hängt also nur von $p \bmod 4q$ ab.

Wir werden das Quadratische Reziprozitätsgesetz als „QRG“ abkürzen. Mit Hilfe des QRG und seiner Ergänzungsgesetze kann man nun Legendre-Symbole, die größere Zahlen enthalten, recht bequem auswerten. Zum Beispiel:

$$\begin{aligned}\left(\frac{67}{109}\right) = \left(\frac{109}{67}\right) = \left(\frac{42}{67}\right) &= \left(\frac{2}{67}\right)\left(\frac{3}{67}\right)\left(\frac{7}{67}\right)\\ &= (-1)(-\left(\frac{67}{3}\right))(-\left(\frac{67}{7}\right)) = -\left(\frac{1}{3}\right)\left(\frac{4}{7}\right) = -1\,.\end{aligned}$$

Oder alternativ:

$$\left(\frac{67}{109}\right) = \left(\frac{109}{67}\right) = \left(\frac{-25}{67}\right) = \left(\frac{-1}{67}\right)\left(\frac{5}{67}\right)^2 = -1\,.$$

Wir wollen das QRG auf ähnliche Weise beweisen wie das Zweite Ergänzungsgesetz. Dazu überlegen wir noch einmal, was wir dafür gebraucht haben:

- Einen geeigneten Ring R, in dem p keine Einheit ist;
- Ein Element $\gamma \in R$ mit $\gamma^2 = 2$ und $\gamma^p \equiv (-1)^{(p^2-1)/8}\gamma \bmod Rp$.

Wir wollen hier die 2 durch p^* und p durch q ersetzen. Wir brauchen dann ein $\gamma \in R$ mit

- $\gamma^2 = p^*$ und
- $\gamma^q \equiv \left(\frac{q}{p}\right)\gamma \bmod Rq$.

Gauß (der das QRG als Erster vollständig bewies, nachdem Legendre es vermutet und in Spezialfällen bewiesen hatte, und der in seinem Leben sieben verschiedene Beweise dafür fand) hat diese Elemente γ gefunden, deswegen werden sie heute nach ihm benannt.

* 12.15. **Definition.** Sei p eine ungerade Primzahl. Wir setzen $\zeta = e^{2\pi i/p} \in \mathbb{C}$ und $R = \mathbb{Z}[\zeta]$. Für $a \in \mathbb{Z}$ heißt

DEF Gaußsche Summe

$$g_a = \sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\zeta^{aj} \in R$$

eine *Gaußsche Summe* (zur Primzahl p). Für g_1 schreiben wir auch einfach g (die Primzahl p muss aus dem Kontext klar sein) und nennen es *die* Gaußsche Summe. ♢

12.16. **Lemma.** *Seien p eine ungerade Primzahl, $a \in \mathbb{Z}$ und ζ wie oben.*

LEMMA Eigensch. der Gaußschen Summe

(1) *Es gilt $\sum_{j=0}^{p-1}\zeta^{aj} = 0$, falls $p \nmid a$; im anderen Fall ist der Wert p.*

(2) $g_a = \left(\frac{a}{p}\right) g$.

(3) $g^2 = p^*$.

Beweis.

(1) Die Aussage für $p \mid a$ ist klar (dann gilt $\zeta^a = 1$). Es gelte also $p \nmid a$ und damit $\zeta^a \neq 1$. Es folgt

$$\sum_{j=0}^{p-1} \zeta^{aj} = \sum_{j=1}^{p} \zeta^{aj} = \zeta^a \sum_{j=0}^{p-1} \zeta^{aj} ,$$

also $(1-\zeta^a)\sum_{j=0}^{p-1} \zeta^{aj} = 0$. Wegen $\zeta^a \neq 1$ folgt die Behauptung.

(2) Für $p \mid a$ folgt die Behauptung aus Lemma 12.4. Es gelte also $p \nmid a$, dann gibt es $a' \in \mathbb{Z}$ mit $aa' \equiv 1 \bmod p$. Aus der Multiplikativität des Legendre-Symbols folgt $\left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right)$. Mit j durchläuft auch $a'j$ alle Restklassen mod p, also erhalten wir

$$g_a = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{aj} = \sum_{j=0}^{p-1} \left(\frac{a'j}{p}\right) \zeta^{j} = \left(\frac{a'}{p}\right) \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{j} = \left(\frac{a}{p}\right) g .$$

(3) Wir haben

$$\begin{aligned}(p-1)g^2 &\overset{(2)}{=} \sum_{a=0}^{p-1} g_a^2 = \sum_{a=0}^{p-1} \sum_{j,k=0}^{p-1} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) \zeta^{aj+ak} \\ &= \sum_{j,k=0}^{p-1} \left(\frac{jk}{p}\right) \sum_{a=0}^{p-1} \zeta^{a(j+k)} \overset{(1)}{=} \sum_{j,k=0}^{p-1} \left(\frac{jk}{p}\right) \begin{cases} 0 & \text{falls } p \nmid j+k \\ p & \text{falls } p \mid j+k \end{cases} \\ &= \sum_{j=0}^{p-1} \left(\frac{-j^2}{p}\right) p = \left(\frac{-1}{p}\right) p(p-1) ,\end{aligned}$$

also $g^2 = \left(\frac{-1}{p}\right) p = p^*$. ❑

Wir bemerken noch, dass $\zeta^p = 1$, aber $\zeta \neq 1$ ist, also ist ζ eine Nullstelle des Polynoms

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

Dieses Polynom ist irreduzibel in $\mathbb{Q}[x]$ (siehe Beispiel 11.14). Nach Lemma 12.10 ist also keine Primzahl q eine Einheit in $R = \mathbb{Z}[\zeta]$.

Der Beweis ist nun analog wie für das Zweite Ergänzungsgesetz.

Beweis von Satz 12.14. Sei $\zeta = e^{2\pi i/p}$ und $R = \mathbb{Z}[\zeta]$ wie oben. Sei $g \in R$ die Gaußsche Summe für p. Dann gilt modulo Rq:

$$g^q = (g^2)^{(q-1)/2} \cdot g = (p^*)^{(q-1)/2} g \equiv \left(\frac{p^*}{q}\right) g$$

und

$$g^q \equiv \sum_{j=0}^{p-1} \left(\frac{j}{p}\right)^q \zeta^{qj} = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{qj} = g_q = \left(\frac{q}{p}\right) g .$$

Es folgt $\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \bmod Rq$; nach Multiplikation mit g haben wir dann $\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \bmod Rq$. Wegen $p^* \perp q$ folgt $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \bmod Rq$. Da q in R keine Einheit und außerdem ungerade ist, folgt daraus die Gleichheit der Symbole wie im Beweis von Satz 12.12. ❑

Aus $g^2 = p^*$ folgt $g = \pm\sqrt{p}$, falls $p \equiv 1 \bmod 4$, und $g = \pm\boldsymbol{i}\sqrt{p}$, falls $p \equiv 3 \bmod 4$. Man kann sich nun fragen, welches Vorzeichen man bekommt. Rechnung zeigt in jedem konkreten Fall, dass das Vorzeichen jeweils das positive ist. Zum Beispiel ist für $p = 5$

$$g = \zeta - \zeta^2 - \zeta^{-2} + \zeta^{-1} = 2\cos\frac{2\pi}{5} - 2\cos\frac{4\pi}{5} = 4\sin\frac{\pi}{5}\sin\frac{3\pi}{5} > 0\,,$$

also $g = \sqrt{5}$. Gauß, der diese Vermutung im Jahr 1801 aufstellte, hat vier Jahre gebraucht, bis er das beweisen konnte (er schreibt dazu in einem Brief 1805 „Wie der Blitz einschlägt, hat sich das Räthsel gelöst"). Einen Beweis findet man zum Beispiel in dem schönen Buch von Ireland und Rosen, *A classical introduction to modern number theory*, Springer GTM 84, in § 6.4.

Ein Nachteil bei der oben angedeuteten Methode, ein Legendre-Symbol mit Hilfe des QRG und seiner Ergänzungsgesetze zu berechnen, besteht darin, dass man die obere Zahl, die in den während der Rechnung angetroffenen Symbolen auftritt, faktorisieren muss. Das ist aber nicht wirklich nötig. Dazu erweitert man die Definition des Legendre-Symbols: Ist $n > 0$ ungerade mit Primfaktorzerlegung $n = \prod_i p_i^{e_i}$, dann definiert man für $a \in \mathbb{Z}$

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i}\,;$$

man nennt das Symbol dann *Jacobi-Symbol*. Es ist in beiden Argumenten multiplikativ. Das QRG und die Ergänzungsgesetze gelten dann auch für das Jacobi-Symbol:

Seien m und n zwei positive ungerade Zahlen. Dann gilt:

(1) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$;

(2) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$;

(3) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Der Beweis ist eine Übungsaufgabe.

Damit lässt sich die Faktorisierung (abgesehen vom Abspalten des Vorzeichens und einer Potenz von 2) bei der Berechnung vermeiden:

$$\begin{aligned}\left(\frac{887}{1009}\right) = \left(\frac{1009}{887}\right) = \left(\frac{122}{887}\right) = \left(\frac{2}{887}\right)\left(\frac{61}{887}\right) = \left(\frac{887}{61}\right)\\ = \left(\frac{33}{61}\right) = \left(\frac{61}{33}\right) = \left(\frac{28}{33}\right) = \left(\frac{7}{33}\right)\\ = \left(\frac{33}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1\end{aligned}$$

Was jedoch im allgemeinen **nicht mehr** stimmt, ist die Implikation

$$\left(\frac{a}{n}\right) = 1 \implies a \text{ QR mod } n\,.$$

Zum Beispiel gilt $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, aber 2 ist *kein* Quadrat mod 15 (da kein Quadrat mod 3 und mod 5).

13. Normalform von Matrizen über Hauptidealringen

In der Linearen Algebra haben Sie folgenden wichtigen Satz kennengelernt:

SATZ Normalform von Matrizen über einem Körper

13.1. **Satz.** *Seien K ein Körper und $A \in \mathrm{Mat}(m \times n, K)$ eine $m \times n$-Matrix mit Einträgen in K. Dann gibt es invertierbare Matrizen $P \in \mathrm{GL}(m, K)$ und $Q \in \mathrm{GL}(n, K)$, sodass PAQ 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.

Wir verallgemeinern die „Diagonalform“ in Satz 13.1, indem wir auch von 1 verschiedene Elemente auf der Diagonalen zulassen.

DEF diag

13.2. **Definition.** Seien R ein Ring, $r, m, n \in \mathbb{Z}_{\geq 0}$ mit $r \leq \min\{m, n\}$ und $d_1, d_2, \ldots, d_r \in R$. Dann bezeichne $\mathrm{diag}_{m,n}(d_1, d_2, \ldots, d_r)$ die $m \times n$-Matrix (a_{ij}) über R mit $a_{ij} = 0$ für $i \neq j$, $a_{ii} = d_i$ für $1 \leq i \leq r$ und $a_{ii} = 0$ für $i > r$. ♢

Die Matrix PAQ aus Satz 13.1 lässt sich dann kurz als $\mathrm{diag}_{m,n}(1, 1, \ldots, 1)$ mit r Einsen schreiben.

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.

Wir verallgemeinern einige Begriffe aus der Linearen Algebra auf kommutative Ringe statt Körper.

DEF Matrizen über R

13.3. **Definition.** Seien R ein kommutativer Ring und $m, n \in \mathbb{Z}_{\geq 0}$. 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 $B = PAQ$. ♢

Die Multiplikativität der Determinante (die man über die Leibniz-Formel als Polynom in den Einträgen der Matrix definieren kann) auch über kommutativen Ringen folgt aus der Gleichheit der Polynome $\det\big((x_{ij}) \cdot (y_{kl})\big)$ und $\det(x_{ij}) \cdot \det(y_{kl})$, die wiederum ein Spezialfall der Multiplikativität der Determinante über einem

Körper ist, nämlich dem Quotientenkörper des Polynomrings $\mathbb{Z}[x_{ij}, y_{kl}]$ in $2n^2$ Unbestimmten (jeweils mit $i, j, k, l \in \{1, 2, \ldots, n\}$).

In ähnlicher Weise folgt die Invertierbarkeit von A in $\mathrm{Mat}(n, R)$ aus der von $\det(A)$ in R aus der Beziehung $A\tilde{A} = \det(A)I_n$, wo $\tilde{A}$ die adjungierte (oder adjunkte) Matrix ist.

Wir bemerken noch:

LEMMA Zeilen- und Spaltenumf.

13.4. **Lemma.** *Seien R ein kommutativer Ring und $A \in \mathrm{Mat}(m \times n, R)$. Eine elementare Zeilen- bzw. Spaltenumformung an A entspricht der Multiplikation von A mit einer invertierbaren Matrix von links bzw. von rechts.*

Dabei besteht eine elementare Zeilenumformung in der Multiplikation einer Zeile mit einer Einheit, der Addition eines Vielfachen einer Zeile zu einer anderen oder der Vertauschung zweier Zeilen; analog für Spaltenumformungen.

Beweis. Multiplikation von A von links mit der Diagonalmatrix

$$\mathrm{diag}_{m,m}(\underbrace{1, \ldots, 1, u, 1 \ldots, 1}_{m}) \in \mathrm{GL}(m, R)$$

(mit $u \in R^\times$ an der i-ten Position) multipliziert die i-te Zeile von A mit u. Sei $E_{i,j} \in \mathrm{Mat}(m, R)$ die Matrix, deren Einträge null sind außer einem Eintrag 1 an der Position (i, j). Dann hat Multiplikation von A von links mit $I_m + \lambda E_{i,j}$ den Effekt, das λ-fache der j-ten Zeile von A zur i-ten Zeile zu addieren. Die Vertauschung zweier Zeilen lässt sich auf die anderen beiden Arten von elementaren Zeilenumformungen zurückführen. Für Spaltenumformungen ist das Argument analog. ❑

Wir wollen nun folgendes Resultat beweisen:

SATZ Elementarteilersatz

∗ 13.5. **Satz.** *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 $d_r \neq 0$, sodass 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.

DEF Elementarteiler

13.6. **Definition.** Die Elemente $d_1, \ldots, d_r$ aus Satz 13.5 heißen die *Elementarteiler* der Matrix A. ♢

Wir zeigen erst einmal die behauptete Eindeutigkeit.

DEF $\mathrm{ggT}_r(A)$

13.7. **Definition.** Seien R ein Hauptidealring und $A \in \mathrm{Mat}(m \times n, R)$. Wir schreiben $\mathrm{ggT}(A)$ für einen größten gemeinsamen Teiler aller Einträge der Matrix A. Allgemeiner schreiben wir

$$\mathrm{ggT}_r(A) \sim \mathrm{ggT}\big(\{\det(SAT) \mid S \in \mathrm{Mat}(r \times m, R), T \in \mathrm{Mat}(n \times r, R)\}\big)\,. \quad \diamondsuit$$

$\mathrm{ggT}(A) = \mathrm{ggT}_1(A)$ ist ein Spezialfall, da die Einträge der 1×1-Matrizen SAT Linearkombinationen der Einträge von A sind und man die Einträge selbst auch auf diese Weise bekommt.

Größte gemeinsame Teiler einer beliebigen Menge von Elementen definiert man genauso wie für endlich viele Elemente. In faktoriellen Ringen existieren solche ggTs immer. In Hauptidealringen R gilt für Teilmengen $A \subset R$

$$g \sim \mathrm{ggT}(A) \iff \langle g \rangle_R = \langle A \rangle_R\,.$$

Die Eindeutigkeit beruht auf der folgenden Tatsache.

13.8. **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 $\mathrm{ggT}(A) \sim \mathrm{ggT}(B)$.)*

LEMMA Invarianz von ggT_r

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 dieselben Mengen von Determinanten gebildet, müssen also assoziiert sein. ❑

Für unsere Diagonalmatrizen gilt Folgendes.

13.9. **Lemma.** *Seien R ein Hauptidealring und $D = \mathrm{diag}_{m,n}(d_1, \ldots, d_r)$ eine Matrix über R mit $d_1 \mid d_2 \mid \cdots \mid d_r$ und $d_r \neq 0$. Dann gilt $\mathrm{ggT}_k(D) \sim d_1 d_2 \cdots d_k$ für alle $k \in \{1, 2, \ldots, r\}$ und $\mathrm{ggT}_k(D) = 0$ für $k > r$.*

LEMMA ggT_r für Diagonalmatrizen

Beweis. Wir können die Determinanten auch über dem Quotientenkörper K von R berechnen; daran sieht man, dass $\det(M) = 0$ ist, wenn $M \in \mathrm{Mat}(k, R)$ eine Matrix ist, die als Matrix über K Rang $< k$ hat. Daraus folgt die Aussage für $k > r$, denn der Rang von SDT ist durch den Rang r von D beschränkt. Wir können also $k \leq r$ annehmen.

Mit $S = (I_k \mid \mathbf{0}_{k,m-k})$ und $T = (I_k \mid \mathbf{0}_{k,n-k})^\top$ ist SDT die $k \times k$-Diagonalmatrix mit Einträgen $d_1, d_2, \ldots, d_k$, also ist $\det(SDT) = d_1 d_2 \cdots d_k$. Das zeigt die eine Richtung $\mathrm{ggT}_k(D) \mid d_1 d_2 \cdots d_k$.

Für die Gegenrichtung seien $S = (s_{ij})_{1 \leq i \leq k, 1 \leq j \leq m}$ und $T = (t_{hl})_{1 \leq h \leq n, 1 \leq l \leq k}$. Die Einträge von SDT haben dann die Form $\sum_{j=1}^{r} d_j s_{ij} t_{jl}$. Sei $M_j = (s_{ij} t_{jl})_{1 \leq i,l \leq k}$; dann ist $SDT = \sum_{j=1}^{r} d_j M_j$ und die Matrizen M_j haben Rang höchstens 1 (über K). Sei $M(j_1, \ldots, j_k)$ die Matrix, deren i-te Zeile die i-te Zeile von M_{j_i} ist. Aus der Multilinearität der Determinante als Funktion der Zeilen einer Matrix folgt dann

$$\det(SDT) = \det\Big(\sum_{j=1}^{r} d_j M_j\Big) = \sum_{j_1, \ldots, j_k \in \{1, \ldots, r\}} d_{j_1} \cdots d_{j_k} \det\big(M(j_1, \ldots, j_k)\big)\,.$$

Wenn zwei der j_i gleich sind, dann enthält $M(j_1, \ldots, j_k)$ zwei Zeilen derselben Matrix M_j. Da diese Zeilen linear abhängig sind, ist $\det\big(M(j_1, \ldots, j_k)\big)$ dann null. Also bleiben in der Summe oben nur Terme stehen, die durch ein Produkt $d_{j_1} \cdots d_{j_k}$ mit paarweise verschiedenen j_i teilbar sind. Da jedes solche Produkt durch $d_1 d_2 \cdots d_k$ teilbar ist, folgt $d_1 d_2 \cdots d_k \mid \mathrm{ggT}_k(D)$. ❑

Beweis der Eindeutigkeit in Satz 13.5.
Seien $D = \mathrm{diag}(d_1, \ldots, d_r)$ und $D' = \mathrm{diag}(d'_1, \ldots, d'_{r'})$ äquivalent; außerdem gelte $d_1 \mid d_2 \mid \cdots \mid d_r$ und $d'_1 \mid d'_2 \mid \cdots \mid d'_{r'}$, sowie $d_r, d'_{r'} \neq 0$. Nach Lemma 13.9 gilt $\mathrm{ggT}_k(D) = d_1 d_2 \cdots d_k \neq 0$ für $k \leq r$ und $\mathrm{ggT}_k(D) = 0$ für $k > r$, und analog für D'. Nach Lemma 13.8 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 3.16, der besagt, dass in einem Hauptidealring der größte gemeinsame Teiler zweier Elemente als Linearkombination dieser Elemente geschrieben werden kann.

13.10. **Lemma.** *Seien R ein Hauptidealring, $a, b \in R$ und $g \sim \mathrm{ggT}(a, b)$. Dann gibt es eine Matrix $Q \in \mathrm{GL}(2, R)$ mit $(a\ b)Q = (g\ 0)$.* **LEMMA**

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.

13.11. **Lemma.** *Seien R ein Hauptidealring, $n \in \mathbb{Z}_{>0}$, $a_1, a_2, \ldots, a_n \in R$ und sei $g \sim \mathrm{ggT}(a_1, \ldots, a_n)$. Dann gibt es eine Matrix $Q \in \mathrm{GL}(n, R)$ mit* **LEMMA**

$$(a_1\ a_2\ \ldots\ a_n)Q = (g\ 0\ \ldots\ 0)\,.$$

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 13.10 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

$$(a_1\ \ldots\ a_{n-2}\ a_{n-1}\ a_n)Q_1 = (a_1\ \ldots\ a_{n-2}\ g'\ 0)\,.$$

Nach Induktionsannahme gibt es eine Matrix $Q'' \in \mathrm{GL}(n-1, R)$ mit

$$(a_1\ \ldots\ a_{n-2}\ g')Q'' = (g\ 0\ \ldots\ 0\ 0)\,.$$

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:

13.12. **Folgerung.** *Sei R ein Hauptidealring und seien $a_1, a_2, \ldots, a_n \in R$ teilerfremd (d.h. $\mathrm{ggT}(a_1, a_2, \ldots, a_n) \sim 1$). Dann gibt es eine invertierbare Matrix $T \in \mathrm{GL}(n, R)$, deren erste Zeile $(a_1\ a_2\ \ldots\ a_n)$ ist.* **FOLG** Ergänzung zu inv.barer Matrix

Beweis. Nach Lemma 13.11 gibt es eine Matrix $Q \in \mathrm{GL}(n, R)$ mit

$$(a_1\ a_2\ \ldots\ a_n)Q = (1\ 0\ \ldots\ 0)\,.$$

Mit $T = Q^{-1}$ gilt dann

$$(a_1\ a_2\ \ldots\ a_n) = (1\ 0\ \ldots\ 0)T\,,$$

was genau die Behauptung ist. ❑

13.13. **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 **BSP**

$$(6\ \ 10\ \ 15)\begin{pmatrix}1&0&0\\0&-1&-3\\0&1&2\end{pmatrix} = (6\ \ 5\ \ 0)$$

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

$$T = Q^{-1} = \begin{pmatrix}6&10&15\\1&2&3\\0&-1&-1\end{pmatrix}\,. \qquad \clubsuit$$

Es gilt natürlich auch die transponierte Version von Lemma 13.11, bei der man eine Spalte von links mit einer invertierbaren Matrix multipliziert.

13.14. **Lemma.** *Sei R ein Hauptidealring, $m,n>0$, und $A \in \mathrm{Mat}(m\times n,R)$. Dann ist A äquivalent zu einer Matrix* **LEMMA**

$$B = \left(\begin{array}{c|c} d & 0_{1\times(n-1)} \\ \hline 0_{(m-1)\times 1} & A' \end{array}\right)$$

mit $d \sim \mathrm{ggT}(A)$ 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 13.8 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 13.11 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 $d \sim \mathrm{ggT}(B) \sim \mathrm{ggT}(A)$ ist 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 13.5 behauptete Existenz beweisen:

Beweis der Existenz in Satz 13.5.
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 13.14 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 $\mathrm{diag}_{m-1,n-1}(d_2,\dots,d_r)$ 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 $\mathrm{diag}_{m,n}(d_1,d_2,\dots,d_r)$. Da d_1 ein Teiler von $\mathrm{ggT}(A') \sim d_2$ ist, hat diese Matrix die verlangte Form. ❑

13.15. **Beispiel.** Als Beispiel bestimmen wir die Elementarteiler der „Telefonmatrix“

BSP
Elementarteiler

$$\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix} \in \mathrm{Mat}(3\times 3,\mathbb{Z})\,.$$

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 $d_1=1$, $d_2=3$. ♣

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 13.14 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 $N(b_{11})$ des Eintrags in der linken oberen Ecke. (Wir können natürlich $A\neq 0$ annehmen, sodass 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:

SATZ Erzeugung von $\mathrm{GL}(n, R)$

Satz. *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.)*

14. Endlich erzeugte abelsche Gruppen

Zum Abschluss dieser Vorlesung werden wir die Struktur endlich erzeugter abelscher Gruppen untersuchen und darüber einen Satz beweisen.

Wir erinnern uns:

DEF abelsche Gruppe

14.1. **Definition.** Eine *abelsche Gruppe* ist ein Quadrupel $(A, +, 0, -)$, bestehend aus einer Menge A, einer Verknüpfung $+ : A \times A \to A$, einem Element $0 \in A$ und einer Abbildung $- : A \to A$, mit folgenden Eigenschaften:

(1) (Assoziativität) $\forall a, b, c \in A : (a + b) + c = a + (b + c)$

(2) (Kommutativität) $\forall a, b \in A : a + b = b + a$

(3) (neutrales Element) $\forall a \in A : a + 0 = a$

(4) (inverses Element) $\forall a \in A : a + (-a) = 0$

Für $a + (-b)$ schreibt man auch $a - b$.

Ist die Menge A endlich, dann heißt die Gruppe *endlich*; die Anzahl ihrer Elemente ist die *Ordnung* der Gruppe. ♢

In jeder abelschen Gruppe gibt es eine *Skalarmultiplikation* oder *Vervielfachung* mit ganzen Zahlen, die man rekursiv so definieren kann:

$$0 \cdot a = 0\,, \qquad (n \pm 1) \cdot a = n \cdot a \pm a\,.$$

Dann gelten die üblichen Eigenschaften einer Skalarmultiplikation (wie für Vektorräume):

(1) $\forall a \in A : 1 \cdot a = a$

(2) $\forall m, n \in \mathbb{Z}\ \forall a \in A : (m + n) \cdot a = m \cdot a + n \cdot a$

(3) $\forall n \in \mathbb{Z}\ \forall a, b \in A : n \cdot (a + b) = n \cdot a + n \cdot b$

(4) $\forall m, n \in Z\ \forall a \in A : (mn) \cdot a = m \cdot (n \cdot a)$

(Beweis durch Induktion — Übung.) Es ist also sinnvoll, von (ganzzahligen) *Linearkombinationen* von Elementen von A zu sprechen. Meist schreibt man einfach na statt $n \cdot a$.

Für einen kommutativen Ring R definiert man einen *R-Modul* (Betonung auf dem „o“; Plural „die Moduln“) analog zu einem Vektorraum: Ein R-Modul ist ein Quintupel $(M, +, 0, -, \cdot)$, sodass $(M, +, 0, -)$ eine abelsche Gruppe ist und $\cdot : R \times M \to M$ die obigen Eigenschaften einer Skalarmultiplikation hat (mit R statt $\mathbb{Z}$). In diesem Sinne sind abelsche Gruppen auch $\mathbb{Z}$-Moduln. Die im Folgenden entwickelten Begriffe lassen sich allgemeiner für R-Moduln definieren.

Analog zu anderen Unterstrukturen (Untervektorräume, Unterringen), denen wir bereits begegnet sind, definieren wir Untergruppen.

DEF Untergruppe

14.2. **Definition.** Sei G eine Gruppe. Eine *Untergruppe* von G ist eine Teilmenge $H \subset G$, die das neutrale Element enthält und unter der Verknüpfung und Inversenabbildung von G abgeschlossen ist. ♢

Analog wie für Unterringe sieht man, dass eine Untergruppe mit den auf sie eingeschränkten Operationen der ursprünglichen Gruppe wieder eine Gruppe ist; jede Untergruppe einer abelschen Gruppe ist wieder abelsch.

14.3. **Lemma.** *Seien G eine Gruppe und $(G_i)_{i\in I}$ eine nichtleere (also $I \neq \emptyset$) Familie von Untergruppen von G. Dann ist $\bigcap_{i\in I} G_i$ ebenfalls eine Untergruppe von G.*

LEMMA Durchschnitt von Untergruppen

Beweis. Völlig analog wie für Untervektorräume, Unterringe, Ideale, ...; vergleiche etwa Lemma 3.5. ❑

Diese Durchschnitts-Eigenschaft erlaubt es uns, die von einer Teilmenge erzeugte Untergruppe zu definieren.

14.4. **Definition.** Sei G eine Gruppe und $T \subset G$ eine Teilmenge. Die *von T erzeugte Untergruppe* von G ist die kleinste Untergruppe von G, die T enthält. Wir schreiben dafür $\langle T\rangle$ (oder auch $\langle t_1, t_2, \ldots, t_n\rangle$, falls $T = \{t_1, t_2, \ldots, t_n\}$ endlich ist). Die Teilmenge T heißt ein *Erzeugendensystem* von G, falls $\langle T\rangle = G$ gilt. Gibt es ein endliches Erzeugendensystem von G, dann heißt G *endlich erzeugt*. Die Gruppe G heißt *zyklisch*, wenn sie von einem Element erzeugt wird. ♢

DEF $\langle T\rangle$ Erzeugendensystem endl. erzeugt zyklisch

Wie für Untervektorräume und Ideale gilt im Fall von abelschen Gruppen Folgendes:

14.5. **Lemma.** *Seien A eine abelsche Gruppe und $a_1, a_2, \ldots, a_n \in A$. Dann ist*

$$\langle a_1, a_2, \ldots, a_n\rangle = \{m_1a_1 + m_2a_2 + \ldots + m_na_n \mid m_1, m_2, \ldots, m_n \in \mathbb{Z}\}\,.$$

LEMMA Erzeugnis als Linearkomb.

Die Elemente der von einer Teilmenge erzeugten Untergruppe sind also gerade die ganzzahligen Linearkombinationen der Elemente der Teilmenge.

Beweis. Wie für Untervektorräume oder Ideale, vergleiche Lemma 3.11. ❑

Als Nächstes brauchen wir die passenden strukturverträglichen Abbildungen.

14.6. **Definition.** Seien A und B zwei abelsche Gruppen. Ein *Homomorphismus* abelscher Gruppen von A nach B ist eine Abbildung $\phi : A \to B$, die mit der Addition von A und B verträglich ist: $\forall a, a' \in A : \phi(a + a') = \phi(a) + \phi(a')$. Der *Kern* von ϕ, $\ker(\phi)$, besteht aus allen Elementen von A, die von ϕ auf 0 abgebildet werden. Die Begriffe *Monomorphismus*, *Epimorphismus*, *Isomorphismus*, *Endomorphismus* und *Automorphismus* sind analog wie für Vektorräume oder Ringe definiert. A und B heißen *isomorph*, wenn es einen Isomorphismus $A \to B$ gibt. ♢

DEF Homomorphismus isomorph

Wie üblich folgt $\phi(0) = 0$ und $\phi(-a) = -\phi(a)$. Außerdem gilt $\phi(na) = n\phi(a)$ für $n \in \mathbb{Z}$ und $a \in A$; so ein Homomorphismus ist also dasselbe wie eine $\mathbb{Z}$-lineare Abbildung. Der Kern von ϕ ist eine Untergruppe von A, das Bild von ϕ ist eine Untergruppe von B. Allgemeiner sind Bilder und Urbilder von Untergruppen unter Homomorphismen wieder Untergruppen (Beweis wie für Untervektorräume).

Beispiele. Die reelle Exponentialfunktion $\exp_{\mathbb{R}} : (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$, $x \mapsto e^x$, ist ein Homomorphismus abelscher Gruppen (denn $e^{x+y} = e^x \cdot e^y$). Der Kern ist trivial, also ist $\exp_{\mathbb{R}}$ injektiv; das Bild ist die Untergruppe $(\mathbb{R}^\times_{>0}, \cdot)$ der positiven reellen Zahlen. Wir bekommen also einen Isomorphismus $(\mathbb{R}, +) \cong (\mathbb{R}^\times_{>0}, \cdot)$. **BSP** Homomorphismen

Die komplexe Exponentialfunktion $\exp_{\mathbb{C}} : (\mathbb{C}, +) \to (\mathbb{C}^\times, \cdot)$, $z \mapsto e^z$, ist ebenfalls ein Homomorphismus abelscher Gruppen. Dieser Homomorphismus ist nicht injektiv, denn er hat Kern $2\pi i\mathbb{Z}$; dafür ist $\exp_{\mathbb{C}}$ surjektiv. Es folgt (siehe den Homomorphiesatz 14.14 unten), dass $(\mathbb{C}^\times, \cdot)$ isomorph zur additiven Gruppe $\mathbb{C}/2\pi i\mathbb{Z}$ ist. ♣

14.7. **Definition.** Eine endlich erzeugte abelsche Gruppe A heißt *frei* vom Rang r, wenn A isomorph zu $\mathbb{Z}^r$ (mit komponentenweise definierter Addition) ist. Wir schreiben $\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}^r$ mit der Eins an der j-ten Stelle; dann sind $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r$ die Standard-Erzeuger von $\mathbb{Z}^r$ ♢ **DEF** freie ab. Gruppe

Freie abelsche Gruppen zusammen mit ihren Standard-Erzeugern haben eine universelle Eigenschaft.

14.8. **Lemma.** *Seien A eine abelsche Gruppe und $a_1, a_2, \ldots, a_r \in A$. Dann gibt es einen eindeutig bestimmten Homomorphismus $\phi : \mathbb{Z}^r \to A$ mit $\phi(\mathbf{e}_j) = a_j$ für alle $j \in \{1, 2, \ldots, r\}$.* **LEMMA** Univ. Eig. einer freien ab. Gruppe

Beweis. Wenn ϕ existiert, dann muss jedenfalls gelten

$$\begin{aligned}\phi\big((m_1, m_2, \ldots, m_r)\big) &= \phi(m_1\mathbf{e}_1 + m_2\mathbf{e}_2 + \ldots + m_r\mathbf{e}_r)\\ &= m_1\phi(\mathbf{e}_1) + m_2\phi(\mathbf{e}_2) + \ldots + m_r\phi(\mathbf{e}_r)\\ &= m_1a_1 + m_2a_2 + \ldots + m_ra_r\,;\end{aligned}$$

damit ist ϕ eindeutig bestimmt. Andererseits können wir ϕ so auch wenigstens als Abbildung definieren; es ist dann leicht nachzurechnen, dass ϕ ein Homomorphismus ist. ❑

Das nächste Resultat ist wichtig.

* 14.9. **Satz.** *Jede Untergruppe von $\mathbb{Z}^r$ kann von höchstens r Elementen erzeugt werden.* **SATZ** Untergruppen von $\mathbb{Z}^r$

Beweis. Induktion über r. Der Fall $r = 0$ ist trivial ($\mathbb{Z}^0$ ist die triviale Gruppe und wird von der leeren Menge erzeugt). Im Fall $r = 1$ ist $\mathbb{Z}^r = \mathbb{Z}$. Die Existenz der Skalarmultiplikation bewirkt, dass die Untergruppen von $\mathbb{Z}$ dieselben sind wie die Ideale des Rings $\mathbb{Z}$. Da $\mathbb{Z}$ ein Hauptidealring ist, sind die Ideale alle von einem Element erzeugt; dasselbe gilt dann auch für die Untergruppen.

Sei jetzt $r > 1$ und $A \subset \mathbb{Z}^r$ eine Untergruppe. Sei weiter $\phi : \mathbb{Z}^r \to \mathbb{Z}^{r-1}$ der Homomorphismus, der die letzte Koordinate entfernt. Dann ist $\phi(A)$ eine Untergruppe von $\mathbb{Z}^{r-1}$. Nach Induktionsvoraussetzung ist $\phi(A)$ von höchstens $r-1$ Elementen erzeugt; es gibt also $a_1, a_2, \ldots, a_k \in A$ mit $k \le r-1$ und

$$\phi(A) = \langle \phi(a_1), \phi(a_2), \ldots, \phi(a_k) \rangle\,.$$

Sei $B \subset \mathbb{Z}$ die Menge der $n \in \mathbb{Z}$ mit $(0, \ldots, 0, n) \in A$. Dann ist B eine Untergruppe; es folgt, dass $B = n_0\mathbb{Z}$ ist für ein n_0. Wir zeigen, dass A von $a_1, a_2, \ldots, a_k$ und

$b = (0, \ldots, 0, n_0)$ erzeugt wird: Sei $a \in A$, dann können wir $\phi(a)$ als Linearkombination $m_1\phi(a_1) + m_2\phi(a_2) + \ldots + m_k\phi(a_k)$ schreiben. Es folgt

$$\phi(a - m_1a_1 - m_2a_2 - \ldots - m_ka_k) = 0\,,$$

also ist (mit geeignetem $n \in \mathbb{Z}$)

$$a - m_1a_1 - m_2a_2 - \ldots - m_ka_k = (0, \ldots, 0, n) \in A$$

und damit $n \in B$. Es ist also $n = mn_0$ und damit

$$a = m_1a_1 + m_2a_2 + \ldots + m_ka_k + mb\,.$$

Wir sehen also, dass $A = \langle a_1, a_2, \ldots, a_k, b\rangle$ ist. Das zeigt, dass A von $k + 1 \leq r$ Elementen erzeugt werden kann. ❑

Wir können charakterisieren, wann eine abelsche Gruppe endlich erzeugt ist:

LEMMA wann ist A endl. erz.?

14.10. **Lemma.** *Eine abelsche Gruppe A ist genau dann endlich erzeugt, wenn es $r \in \mathbb{Z}_{\geq 0}$ und einen Epimorphismus $\mathbb{Z}^r \to A$ gibt.*

Beweis. Ist $\phi : \mathbb{Z}^r \to A$ ein surjektiver Homomorphismus, dann ist jedes Element von A von der Form $\phi\big((m_1, m_2, \ldots, m_r)\big) = m_1\phi(\mathbf{e}_1) + m_2\phi(\mathbf{e}_2) + \ldots + m_r\phi(\mathbf{e}_r)$. Also ist $A = \langle\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_r)\rangle$ endlich erzeugt.

Ist $A = \langle a_1, a_2, \ldots, a_r\rangle$ endlich erzeugt, dann sei $\phi : \mathbb{Z}^r \to A$ der nach Lemma 14.8 existierende Homomorphismus mit $\phi(\mathbf{e}_j) = a_j$. Es bleibt zu zeigen, dass ϕ surjektiv ist. Sei $a \in A$; weil $\{a_1, a_2, \ldots, a_r\}$ ein Erzeugendensystem von A ist, kann man a als Linearkombination $a = m_1a_1 + m_2a_2 + \ldots + m_ra_r$ (mit $m_1, m_2, \ldots, m_r \in \mathbb{Z}$) schreiben. Dann ist aber $a = \phi\big((m_1, m_2, \ldots, m_r)\big)$ auch im Bild von ϕ. ❑

Man sieht, dass man r als Anzahl der Erzeuger wählen kann.

* **FOLG** Untergruppen von endl. erz. ab. Gruppen sind endl. erz.

14.11. **Folgerung.** *Ist A eine endlich erzeugte abelsche Gruppe und $B \subset A$ eine Untergruppe, dann ist auch B endlich erzeugt.*

Beweis. Nach Lemma 14.10 gibt es einen Epimorphismus $\phi : \mathbb{Z}^r \to A$. Dann ist $\phi^{-1}(B)$ als Untergruppe von $\mathbb{Z}^r$ nach Satz 14.9 endlich erzeugt:

$$\phi^{-1}(B) = \langle v_1, v_2, \ldots, v_m\rangle\,.$$

Es folgt

$$B = \phi\big(\phi^{-1}(B)\big) = \langle\phi(v_1), \phi(v_2), \ldots, \phi(v_m)\rangle\,;$$

also ist B endlich erzeugt. ❑

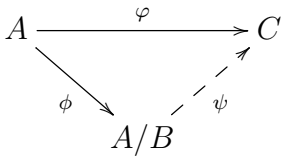
Daraus ergibt sich auch, dass B von höchstens so vielen Elementen erzeugt werden kann, wie man braucht, um A zu erzeugen. (Nach Satz 14.9 kann man $m \leq r$ wählen.)

Für nicht-abelsche Gruppen ist die Aussage von Folgerung 14.11 falsch: Es gibt endlich erzeugte Gruppen mit nicht endlich erzeugten Untergruppen.

Analog zur Situation bei Vektorräumen kann man zu jeder Untergruppe einer abelschen Gruppe eine *Faktorgruppe* oder *Quotientengruppe* konstruieren:

* 14.12. **Satz.** *Sei A eine abelsche Gruppe und sei $B \subset A$ eine Untergruppe. Dann gibt es eine Gruppe A/B und einen Epimorphismus $\phi : A \to A/B$ mit folgender universeller Eigenschaft: Ist C eine weitere abelsche Gruppe und $\varphi : A \to C$ ein Homomorphismus mit $B \subset \ker(\varphi)$, dann gibt es einen eindeutig bestimmten Homomorphismus $\psi : A/B \to C$ mit $\psi \circ \phi = \varphi$.*

SATZ Faktorgruppe



14.13. **Definition.** Die Gruppe A/B in Satz 14.12 heißt *Faktorgruppe* oder *Quotientengruppe* von A modulo B; der Homomorphismus ϕ heißt *kanonischer Epimorphismus*. ♢

DEF Faktorgruppe

Man kann A/B als Menge der *Nebenklassen* $[a] = a + B$ von B in A realisieren; die Gruppenstruktur ist durch $[a] + [a'] = [a + a']$ gegeben und ϕ durch $a \mapsto [a]$.

Es gilt der übliche Homomorphiesatz, der wie für Vektorräume bewiesen werden kann.

* 14.14. **Satz.** *Sei $\phi : A \to B$ ein Homomorphismus von abelschen Gruppen. Dann induziert ϕ einen Isomorphismus $\tilde{\phi} : A/\ker(\phi) \to \mathrm{im}(\phi)$, $[a] \mapsto \phi(a)$.*

SATZ Homomorphiesatz für ab. Gruppen

14.15. **Folgerung.** *Eine zyklische Gruppe ist entweder isomorph zu $\mathbb{Z}$ oder zu einer Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ mit einem $n \in \mathbb{Z}_{>0}$. Im letzteren Fall hat die Gruppe Ordnung n.*

FOLG zyklische Gruppen

Beweis. Ist A zyklisch, dann kann A von einem Element erzeugt werden. Es gibt also einen Epimorphismus $\phi : \mathbb{Z} \to A$. Nach Satz 14.14 folgt $A \cong \mathbb{Z}/\ker(\phi)$. Der Kern von ϕ ist entweder trivial, dann ist $A \cong \mathbb{Z}$, oder von der Form $n\mathbb{Z}$ mit $n \in \mathbb{Z}_{>0}$, dann ist $A \cong \mathbb{Z}/n\mathbb{Z}$. ❑

Schließlich erinnern wir uns daran, dass wir *direkte Produkte* von Gruppen definiert haben (Definition 8.11 im Zusammenhang mit dem Chinesischen Restsatz).

Damit können wir den Klassifikationssatz formulieren.

* 14.16. **Satz.** *Sei A eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte Zahlen $k, r \in \mathbb{Z}_{\geq 0}$, sowie $d_1, d_2, \ldots, d_k \in \mathbb{Z}_{\geq 2}$ mit $d_1 \mid d_2 \mid \cdots \mid d_k$, sodass A isomorph ist zum direkten Produkt $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^r$. A ist genau dann endlich, wenn $r = 0$ ist. In diesem Fall ist $\#A = d_1 d_2 \cdots d_k$.*

SATZ Klassifikationssatz für endl. erz. ab. Gruppen

Beweis. Wir zeigen zunächst die Existenz der behaupteten Darstellung. Da A endlich erzeugt ist, gibt es einen surjektiven Homomorphismus $\phi : \mathbb{Z}^n \to A$ für ein geeignetes $n \in \mathbb{Z}_{\geq 0}$ (Lemma 14.10). Nach dem Homomorphiesatz 14.14 ist dann $A \cong \mathbb{Z}^n/\ker(\phi)$. Der Kern von ϕ ist eine Untergruppe von $\mathbb{Z}^n$, also nach Satz 14.9 ebenfalls endlich erzeugt. Seien $v_1, v_2, \ldots, v_m \in \mathbb{Z}^n$ Erzeuger von $\ker(\phi)$. Sei weiter $M \in \mathrm{Mat}(m \times n, \mathbb{Z})$ die Matrix, deren Zeilen durch die Einträge von $v_1, v_2, \ldots, v_m$ gegeben sind. Wenn wir M von links mit einer invertierbaren Matrix P multiplizieren, dann hat das den Effekt, dass wir $v_1, v_2, \ldots, v_m$ durch andere Erzeuger von $\ker(\phi)$ ersetzen; die neue Matrix beschreibt also immer noch

dieselbe Untergruppe. Wenn wir M von rechts mit einer invertierbaren Matrix Q multiplizieren, dann ersetzen wir ϕ durch $\phi \circ \psi$ mit dem durch Q gegebenen Isomorphismus ψ von $\mathbb{Z}^n$. In jedem Fall ist A auch isomorph zu $\mathbb{Z}^n/B$, wobei B die von den Zeilen von PMQ erzeugte Untergruppe ist. Nach dem Elementarteilersatz 13.5 können wir P und Q so wählen, dass $PMQ = \operatorname{diag}_{m,n}(d'_1, d'_2, \ldots, d'_l)$ ist mit positiven ganzen Zahlen $d'_1 \mid d'_2 \mid \cdots \mid d'_l$. Die von den Zeilen dieser Matrix erzeugte Untergruppe B besteht dann aus allen n-Tupeln, deren j-te Komponente durch d'_j teilbar ist (für alle $j \in \{1, 2, \ldots, l\}$). Es ist dann leicht zu sehen, dass $\mathbb{Z}^n/B \cong \mathbb{Z}/d'_1\mathbb{Z} \times \mathbb{Z}/d'_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d'_l\mathbb{Z} \times \mathbb{Z}^{n-l}$ ist. Sei j der kleinste Index mit $d'_j > 1$. Wir setzen $k = l - j + 1$, $r = n - l$ und $d_i = d'_{i+j-1}$. Dann gilt

$$A \cong \mathbb{Z}^n/B \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^r$$

wie gewünscht (denn für $d'_i = 1$ ist $\mathbb{Z}/d'_i\mathbb{Z}$ die triviale Gruppe, kann also im Produkt weggelassen werden).

Für die Eindeutigkeit bemerken wir zunächst, dass A von $n = k + r$ Elementen erzeugt werden kann, aber nicht von weniger. Sei dazu p ein Primteiler von d_1 (falls $k > 0$) oder irgendeine Primzahl (falls $k = 0$). Kann A von $m < n$ Elementen erzeugt werden, dann auch $A/pA \cong \mathbb{F}_p^n$; für diesen n-dimensionalen Vektorraum ist das aber nicht möglich. Damit ist $k + r$ eindeutig bestimmt.

Wir definieren nun für $j = 0, 1, 2, \ldots, n$

$$I_j(A) = \{m \in \mathbb{Z} \mid mA \text{ kann von höchstens } n - j \text{ Elementen erzeugt werden}\}.$$

Es ist $m \cdot \mathbb{Z}/d\mathbb{Z} = \{0\}$ genau dann, wenn $d \mid m$. Für ein Produkt

$$A' = \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^r$$

gilt dann also $I_j(A') = d_j\mathbb{Z}$ für $j \in \{1, 2, \ldots, k\}$, denn genau wenn m durch d_j (und damit auch durch $d_1, d_2, \ldots, d_{j-1}$) teilbar ist, fallen in mA' die ersten j Faktoren weg. Für $j > k$ ist $I_j(A') = \{0\}$, denn es bleibt immer mindestens ein Anteil $m\mathbb{Z}^r$ übrig, der für $m \neq 0$ nicht von weniger als $r = n - k$ Elementen erzeugt werden kann. Da die Ideale $I_j(A)$ offenbar nur von der Isomorphieklasse von A abhängen, sind k und r und die Zahlen $d_1, d_2, \ldots, d_k$ durch A eindeutig bestimmt. ❑

Der Satz zeigt, dass eine endlich erzeugte abelsche Gruppe ein direktes Produkt von (endlich vielen) zyklischen Gruppen ist; er gibt die Darstellung mit der *minimalen* Anzahl von zyklischen Faktoren.

Es kann mehrere Möglichkeiten geben, eine Gruppe als Produkt von zyklischen Gruppen zu schreiben. Zum Beispiel ist $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Allgemeiner habe n die Primfaktorzerlegung $p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$. Dann ist nach dem Chinesischen Restsatz (als Ring und damit auch als abelsche Gruppe)

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}.$$

* 14.17. **Folgerung.** *Jede endliche abelsche Gruppe ist isomorph zu einem Produkt von zyklischen Gruppen der Form $\mathbb{Z}/p^e\mathbb{Z}$ mit einer Primzahl p und $e \in \mathbb{Z}_{>0}$. Die Primzahlpotenzen sind bis auf ihre Reihenfolge eindeutig bestimmt.*

FOLG Klassifikationssatz für endliche ab. Gruppen

Diese Version des Klassifikationssatzes gibt die Darstellung mit der *maximalen* Anzahl von (nichttrivialen) zyklischen Faktoren.

Beweis. Sei A eine endliche abelsche Gruppe. Dann ist A endlich erzeugt. Nach Satz 14.16 ist $A \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ mit $d_j \in \mathbb{Z}_{\geq 2}$, $d_1 \mid d_2 \mid \cdots \mid d_k$. Nach dem Chinesischen Restsatz können wir jeden Faktor $\mathbb{Z}/d_j\mathbb{Z}$ als Produkt von zyklischen Gruppen von Primpotenzordnung schreiben; das zeigt die Existenz. Für die Eindeutigkeit überlegt man sich, dass die minimale Anzahl der Erzeuger von p^eA genau der Anzahl Faktoren $\mathbb{Z}/p^f\mathbb{Z}$ mit $f > e$ entspricht. ❑

BSP Isomorphieklassen von ab. Gruppen

14.18. **Beispiel.** Die Klassifikationssätze 14.16 und 14.17 lassen sich zum Beispiel dazu verwenden, die Anzahl der Isomorphieklassen von endlichen abelschen Gruppen gegebener Ordnung zu bestimmen. Wenn wir etwa diese Anzahl für die Ordnung 72 bestimmen wollen, dann können wir entweder alle Tupel $(d_1, d_2, \ldots, d_k)$ mit $2 \leq d_1 \mid d_2 \mid \cdots \mid d_k$ und $d_1 d_2 \cdots d_k = 72$ bestimmen, oder wir verwenden die zweite Version des Satzes und finden alle Möglichkeiten, 72 als Produkt von Primzahlpotenzen zu schreiben. Dieser Ansatz liefert

$$72 = 2^3 \cdot 3^2 = 2 \cdot 2^2 \cdot 3^2 = 2 \cdot 2 \cdot 2 \cdot 3^2 = 2^3 \cdot 3 \cdot 3 = 2 \cdot 2^2 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$$

und damit sechs Isomorphieklassen. Sie entsprechen den Zerlegungen

$$72 = 72 = 2 \cdot 36 = 2 \cdot 2 \cdot 18 = 3 \cdot 24 = 6 \cdot 12 = 2 \cdot 6 \cdot 6$$

in der ersten Version; die Gruppen können also als

$$\mathbb{Z}/72\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z},$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

gewählt werden.

Sei $I(n)$ die Anzahl der Isomorphieklassen abelscher Gruppen der Ordnung n. An dem Ansatz mit den Primzahlpotenzen sieht man, dass für $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ sich diese Zahl als Produkt $I(n) = I(p_1^{e_1}) I(p_2^{e_2}) \cdots I(p_k^{e_k})$ zerlegt. Weiter sieht man, dass $I(p^e)$ nur von e und nicht von p abhängt: Man muss alle Möglichkeiten finden, e als (ungeordnete) Summe von positiven ganzen Zahlen zu schreiben: $2 = 1 + 1$, $3 = 2 + 1 = 1 + 1 + 1$. Wenn wir $p(e)$ für diese *Partitionszahl* schreiben, dann ist also $I(n) = p(e_1)p_(e_2) \cdots p(e_k)$. ♣

Da der Satz 13.5, auf dem der Klassifikationssatz 14.16 basiert, allgemeiner für Matrizen über Hauptidealringen gilt, lässt sich der Klassifikationssatz entsprechend verallgemeinern:

SATZ Klassifikationssatz für endl. erz. Moduln über Hauptidealringen

Satz. *Seien R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es eindeutig bestimmte Zahlen $k, r \in \mathbb{Z}_{\geq 0}$, sowie bis auf Assoziierte eindeutig bestimmte Elemente $d_1, d_2, \ldots, d_k \in R \setminus R^\times$ mit $d_1 \mid d_2 \mid \cdots \mid d_k$, sodass M isomorph ist zum direkten Produkt $R/Rd_1 \times R/Rd_2 \times \cdots \times R/Rd_k \times R^r$.*

Analog gibt es auch die Version, bei der man statt der d_j Potenzen von Primelementen hat. Ist $R = K[x]$ der Polynomring über einem Körper, dann ist ein R-Modul nichts anderes als ein K-Vektorraum V zusammen mit einem Endomorphismus $T : V \to V$; dabei gilt dann $x \cdot v = T(v)$. Ist V endlich-dimensional, dann ist im Klassifikationssatz $r = 0$ und das Produkt der d_j (wenn man sie normiert wählt) ist gerade das charakteristische Polynom von T. Zerfällt es in Linearfaktoren, dann lässt sich der Modul schreiben als ein Produkt von zyklischen Moduln der Form $K[x]/\langle (x-\lambda)^e \rangle$. Wählt man als Basis dieses K-Vektorraums die Restklassen von 1, $x - \lambda$, $(x-\lambda)^2$, …, $(x-\lambda)^{e-1}$ (in umgekehrter Reihenfolge), dann ist die Operation von T (also die Multiplikation mit x) genau durch den Jordan-Block der Größe e mit dem Eigenwert λ gegeben. Das liefert einen durchsichtigeren und weniger mühsamen Beweis des Satzes über die Jordan-Normalform (wenn man erst einmal die relevante Theorie aufgebaut hat).

Literatur

[Fi] Gerd Fischer: *Lehrbuch der Algebra,* Vieweg, 2008. Signatur 80/SK 200 F529 L5. Online-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.