Einführung in die Zahlentheorie und algebraische Strukturen

Wintersemester 2017/2018

Universität Bayreuth

Michael Stoll

Inhaltsverzeichnis

Bildschirmversion vom 19. Februar 2018, 15:51 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 zum Satz über die Darstellbarkeit natürlicher Zahlen als Summe von zwei Quadratzahlen. (Weitere zahlentheoretische Inhalte wie quadratische Reste und den Satz von Lagrange über die Darstellbarkeit von natürlichen Zahlen als Summe von vier Quadraten werden wir (leider) nur eher kurz abhandeln, um mehr Zeit für den Stoff zu haben, den Sie, falls Sie auf Lehramt studieren, für das Staatsexamen in Algebra beherrschen müssen.) 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. Gegen Ende des Semesters werden wir in die Gruppentheorie einsteigen und unter anderem 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 weiter 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 der einfachsten halbwegs interessanten algebraischen Struktur.

DEF Monoid

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

$$\forall a, b, c \in M\colon (a * b) * c = a * (b * c)\,;$$
$$\forall a \in M\colon e * a = a = a * e\,.$$

Das Monoid heißt *kommutativ*, wenn zusätzlich

$$\forall a, b \in M\colon a * b = b * a$$

gilt. ♢

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.

BSP Monoide

1.2. **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 $e * e = e$).

Weitere Beispiele von Monoiden sind $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, +, 0)$, $(\mathbb{N}_+, \cdot, 1)$, $(\mathbb{N}, \cdot, 1)$, $(\mathbb{Z}, \cdot, 1)$ und $(\mathrm{Abb}(X, X), \circ, \mathrm{id}_X)$. ♣

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.

DEF Gruppe

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

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

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

N.H. Abel
1802–1829

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 (oder auch 1_G) 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 $a + (-b)$.

1.4. **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 1.2 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

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

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

Als Nächstes betrachten wir Strukturen mit zwei Verknüpfungen.

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

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

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 $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$. Rings, 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.

1.6. **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

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

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

1.7. **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.

1.8. **Definition.** Ein *Körper* ist ein Septupel $(K, +, 0, -, \cdot, 1, i)$, bestehend aus einer Menge K, Abbildungen $+, \cdot\colon K \times K \to K$, Elementen $0, 1 \in K$, einer Abbildung $-\colon K \to K$ und einer Abbildung $i\colon K\backslash\{0\} \to K\backslash\{0\}$, 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.) **DEF** multiplikative Gruppe von K

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 $0 = a^{-1} \cdot 0 = a^{-1} \cdot a \cdot b = 1 \cdot b = b$.)

1.9. **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. **BSP** Körper

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.

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

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 Seite 75ff im Skript „Lineare Algebra II“ vom Sommersemester 2017.

Endliche Schiefkörper gibt es nicht; das ist ein berühmter Satz von Joseph Wedderburn. (In der im hier verlinkten Wikipedia-Eintrag zugrunde 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 (R ist nicht der Nullring) 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:

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

(„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 $m'_a \colon r \mapsto ra$), 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 $a, b, c, a', b' \in R$. 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) $0 \mid a \iff a = 0$ *und* $a \mid 1 \iff a \in R^\times$.

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

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

(7) *Aus $a \sim a'$ und $b \sim b'$ folgt die Äquivalenz $a \mid b \iff a' \mid b'$.*

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) Die Voraussetzungen bedeuten, dass es $s, t \in R$ gibt mit $b = as$ und $c = bt$. Einsetzen der ersten Gleichung in die zweite ergibt $c = (as)t = a(st)$ und damit $a \mid c$,

(3) Nach Voraussetzung gibt es $s \in R$ mit $b = as$. Dann gilt $bc = (as)c = a(sc)$, also ist a ein Teiler von bc.

(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) Es ist $0 = a \cdot 0$, $a = 1 \cdot a$, $a = a \cdot 1$. Die Aussagen folgen damit aus der Definition der Teilbarkeitsrelation.

(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 $b \mid a$.

(7) Wir zeigen „$\Rightarrow$“; die andere Richtung zeigt man analog. Aus $a \sim a'$ folgt mit (6) $a' \mid a$; aus $b \sim b'$ folgt $b \mid b'$. Zusammen mit $a \mid b$ ergibt sich (durch zweimaliges Anwenden von (2)) wie gewünscht $a' \mid b'$. ❑

Die Teilbarkeitsrelation ist also insbesondere reflexiv (das ist die letzte Aussage in (5)) und transitiv (das ist (2)), und sie hängt nur von der Assoziiertheitsklasse der beteiligten Elemente ab (das ist (7)). Auf den Assoziiertheitsklassen ist die Relation auch antisymmetrisch (das ist (6)); wir erhalten also eine (Teil-)Ordnung auf den Assoziiertheitsklassen. In dieser Ordnung ist die Klasse der Einheiten das kleinste und die Klasse der Null das größte Element (das sind die ersten beiden Aussagen in (5)).

Wir betrachten jetzt größte untere und kleinste obere Schranken von zwei Elementen in dieser Ordnung.

DEF Ordnungsrelation

Allgemein nennt man eine Relation „$\leq$“ auf einer Menge X eine *Ordnungsrelation* oder kurz *Ordnung*, wenn „$\leq$“ die folgenden Eigenschaften hat:

(1) (Reflexivität) $\forall x \in X : x \leq x$.

(2) (Transitivität) $\forall x, y, z \in X : x \leq y \wedge y \leq z \Longrightarrow x \leq z$.

(3) (Antisymmetrie) $\forall x, y \in X : x \leq y \wedge y \leq x \Longrightarrow x = y$.

$(X, \leq)$ ist dann eine *geordnete Menge*. Gilt zusätzlich $\forall x, y \in X : x \leq y \vee y \leq x$ (Vergleichbarkeit), dann heißt die Ordnung *total* oder *linear*. Beispiele für total geordnete Mengen sind $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ mit der üblichen Anordnung. Beispiele für geordnete Mengen, die im Allgemeinen nicht total geordnet sind, sind $(\mathcal{P}(X), \subset)$ für eine beliebige Menge X ($\mathcal{P}(X)$ ist die Potenzmenge von X, also die Menge aller Teilmengen von X.) Nach den obigen Überlegungen ist für einen Integritätsbereich R auch

$(R/\sim, |)$ eine geordnete Menge; dabei bezeichnet $R/\sim$ die Menge der Assoziiertheitsklassen von R. Ist Y eine Teilmenge von X, dann ist $(Y, \leq|_{Y\times Y})$ (also mit der auf Y eingeschränkten Relation) ebenfalls eine geordnete Menge.

Ein Element g in einer geordneten Menge $(X, \leq)$ ist das *größte Element* der Ordnung, wenn gilt $\forall x \in X : x \leq g$. Entsprechend ist ein Element k das *kleinste Element*, wenn gilt $\forall x \in X : k \leq x$. Für eine Teilmenge $Y \subset X$ heißt $s \in X$ eine *obere* bzw. *untere Schranke* von Y, wenn gilt $\forall y \in Y : y \leq s$ bzw. $s \leq y$. (Beachte: s muss nicht in Y liegen!) $s \in X$ heißt *kleinste obere* bzw. *größte untere Schranke* von Y, wenn s das kleinste Element in der Menge aller oberen Schranken von Y bzw. das größte Element in der Menge aller unteren Schranken von Y ist. Die Existenz von kleinsten oberen und größten unteren Schranken (Supremum und Infimum) von beliebigen nichtleeren beschränkten Teilmengen von $\mathbb{R}$ ist zum Beispiel eine wichtige definierende Eigenschaft der reellen Zahlen.

Die nachfolgende Definition von ggT und kgV besagt, dass sie (als Assoziiertheitsklassen) nichts anderes sind als die größte untere bzw. die kleinste obere Schranke der Teilmenge $\{[a], [b]\}$ von $R/\sim$ bezüglich der Teilbarkeitsordnung.

* 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 „$\mathrm{ggT}(a, b)$“ (oder „$\mathrm{kgV}(a, b)$“) 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 bezeichnet „$\mathrm{ggT}(a, b)$“ (und analog „$\mathrm{kgV}(a, b)$“) 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* $\operatorname{ggT}(a,b)$, *dann existiert auch* $\operatorname{ggT}(b,a)$, *und es gilt*
$$\operatorname{ggT}(a,b) \sim \operatorname{ggT}(b,a)\,.$$

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

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

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 $g \sim \operatorname{ggT}(a,b)$, 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?

Für die Existenz des ggT in $\mathbb{Z}$ genügt es, die Existenz eines ggT in $\mathbb{Z}$ für natürliche Zahlen zu zeigen (denn jede ganze Zahl ist assoziiert zu einer natürlichen Zahl). 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*

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

Beweis. Wir betrachten zunächst $b>0$ als fest und zeigen die Aussage durch Induktion nach $|a|$. Für $0\le a<b$ können wir $q=0$ und $r=a$ nehmen. Ist $-b<a<0$, dann nehmen wir $q=-1$ und $r=b+a$. Ist $|a|\ge b$, 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 $0\le r<b$. 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 $0\le r<-b=|b|$. Dann gilt $a=(-q')b+r$. Das zeigt die Existenz. Für die Eindeutigkeit nehmen wir an, dass $q',r'\in\mathbb{Z}$ ebenfalls $a=q'b+r'$, $0\le r'<|b|$ 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 $0\le r<|b|$. 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). ❑

DEF euklidischer Algorithmus

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, schreibe $a_{n-1}=q_na_n+a_{n+1}$ mit $0\le a_{n+1}<a_n$ und setze $n:=n+1$.

(3) (Jetzt ist $a_n=0$). Gib a_{n-1} aus, das ist der ggT von a und b.

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

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	

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.

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

(1) Für alle $r \in R$ gilt $N(r) = 0 \iff r = 0$.

(2) Für alle $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$ mit $a = qb + r$ 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 $N\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$, 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 $N\colon R \to \mathbb{Z}_{\geq 0}$ 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. Das ist ein Unterschied zu Vektorräumen, wo ja sowohl Bild als auch Kern einer linearen Abbildung ein Untervektorraum ist. Später, wenn wir Gruppen genauer studieren, werden wir auch dort einen Unterschied zwischen Bildern (Untergruppen) und Kernen (Normalteilern) von Gruppenhomomorphismen sehen.

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

BSP Produktring

3.1. **Beispiele.**

(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. ♣

DEF Unterring

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

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

BSP Unterringe

3.3. **Beispiele.**

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

(2) $\mathbb{Z}_{\geq 0}$ ist kein Unterring von $\mathbb{Z}$, weil $\mathbb{Z}_{\geq 0}$ nicht unter der Negation abgeschlossen ist. Tatsächlich hat $\mathbb{Z}$ keinen echten (also $\neq \mathbb{Z}$) Unterring, da man aus 1 durch wiederholtes Addieren und durch Negieren alle ganzen Zahlen bekommt.

(3) Die *stetigen* Funktionen $f\colon \mathbb{R} \to \mathbb{R}$ 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. (Und natürlich sind die konstanten Funktionen 0 und 1 stetig.)

(4) Sei R ein Ring mit $0 \neq 1$. 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 R ein Integritätsring und S ein Unterring von R. Dann gilt $0 \neq 1$ in R und damit auch in S, also ist S kein Nullring. 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 $A = \{a_1, a_2, \dots, a_n\}$ endlich, dann schreiben wir auch $R'[a_1, a_2, \dots, a_n]$ 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:

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

LEMMA Durchschnitt und aufst. Vereinigung von Idealen

(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.

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*.

DEF $\langle A\rangle_R \subset R$ Hauptideal Hauptideal-ring

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). ♢

DEF noethersch

Ein kommutativer Ring heißt *noethersch* (zu Ehren der Mathematikerin Emmy Noether), wenn jedes Ideal endlich erzeugt ist. Das ist eine Abschwächung des Begriffs „Hauptidealring“, die aber für viele Anwendungen ausreicht.

Statt $\langle a_1, a_2, \ldots, a_n\rangle$ findet man in der Literatur auch häufig die Schreibweise $(a_1, a_2, \ldots, a_n)$ für das von $a_1, a_2, \ldots, a_n$ erzeugte Ideal von R.

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.

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

LEMMA Linear-kombinationen

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

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

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

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. ❑

Es gilt nun folgender wichtiger Satz:

* 3.12. **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

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

(Wegen $I \neq \{0\}$ ist die Menge nicht-leer, also existiert das Minimum.) Sei $b \in I$ mit $N(b) = n$. Wir zeigen $I = Rb$. Die Inklusion $Rb \subset I$ ist wegen $b \in I$ klar. Sei nun $a \in I$ beliebig; wir wollen $a \in Rb$ zeigen. Da R euklidisch ist, gibt es $q, r \in R$ mit $a = qb + r$ und $N(r) < N(b) = n$. Es ist $r = a - qb \in I$. Wäre $r \neq 0$, dann ergäbe sich ein Widerspruch zur Definition von n, also ist $r = 0$ und damit $a = qb \in Rb$. ❑

Insbesondere ist also der Ring $\mathbb{Z}$ der ganzen Zahlen ein Hauptidealring.

3.13. **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 3.12 ist *falsch:* Es gibt Hauptidealringe, die nicht euklidisch sind. Ein Beispiel dafür ist der Ring $R = \mathbb{Z}[\alpha] \subset \mathbb{C}$ mit $\alpha = \frac{1}{2}(1 + \sqrt{-19})$ (dann gilt $\alpha^2 = \alpha - 5$). Der Beweis ist allerdings nicht ganz einfach.

Dass R nicht euklidisch ist, kann man wie folgt zeigen: Angenommen, R wäre doch euklidisch. Dann ist die Menge

$$\mathcal{N} = \{N\colon R \to \mathbb{Z}_{\geq 0} \mid N \text{ ist euklidische Normfunktion}\}$$

nicht leer. Wir definieren

$$N_{\min}\colon R \longrightarrow \mathbb{Z}_{\geq 0}, \qquad r \longmapsto \min\{N(r) \mid N \in \mathcal{N}\}\,.$$

Dann prüft man nach, dass $N_{\min}$ ebenfalls eine euklidische Normfunktion ist (Übung). Außerdem gilt $N_{\min}(r) = 1 \iff r \in R^\times = \{\pm 1\}$, und $N_{\min}$ ist surjektiv (Übung). Es gibt also $a \in R$ mit $N_{\min}(a) = 2$; es muss dann gelten, dass jedes $r \in R$ entweder ein Vielfaches von a ist oder sich von einem Vielfachen von a um ± 1 unterscheidet. Man kann aber relativ leicht nachprüfen, dass es kein $a \in R$ mit dieser Eigenschaft gibt.

Schwieriger ist der Beweis dafür, dass R ein Hauptidealring ist. Man kann dafür einen Satz aus der algebraischen Zahlentheorie verwenden (die unter anderem Ringe wie den hier betrachteten studiert), der in diesem Fall besagt, dass man nur nachprüfen muss, dass alle Ideale $I \neq \{0\}$ mit „Norm“

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

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

3.14. **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 genau dann assoziiert, wenn sie dasselbe Hauptideal erzeugen.

Beweis. Es gilt

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

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

3.15. **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 $r \in R$:*

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

Beweis. Es genügt, die beiden Äquivalenzen zu zeigen. Da R ein Hauptidealring ist, sind die beiden Ideale $\langle a, b\rangle_R$ und $\langle a\rangle_R \cap \langle b\rangle_R$ beide von einem Element erzeugbar, also gibt es Elemente r wie angegeben, und die Existenz von ggT und kgV folgt.

Nach Lemma 3.14 ist r genau dann ein gemeinsamer Teiler von a und b, 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 genau dann ein ggT, 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 dafür $\langle a, b\rangle_R = \langle r\rangle_R$ 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. ❑

Da wir gesehen haben, dass es in $\mathbb{Z}[\sqrt{-5}]$ nicht zu jedem Paar von Elementen einen ggT gibt, liefert das einen anderen Beweis dafür, dass dieser Ring kein Hauptidealring ist (vergleiche Beispiel 3.13 oben).

FOLG ggT ist Linearkombination

✳ 3.16. **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 3.15 gilt $Ra + Rb = Rg \ni g$, also ist g eine Linearkombination von a und b wie angegeben. ❑

In Ringen, die keine Hauptidealringe sind, in denen aber größte gemeinsame Teiler existieren, muss die Aussage der Folgerung nicht gelten. Zum Beispiel werden wir später sehen, dass der Polynomring $\mathbb{Z}[X]$ „faktoriell“ ist, woraus die Existenz von größten gemeinsamen Teilern folgt. Es ist etwa 1 ein ggT von 2 und X in $\mathbb{Z}[X]$, aber 1 kann nicht als $\mathbb{Z}[X]$-Linearkombination von 2 und X geschrieben werden.

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 $g = ua + vb$.

BSP Erweiterter Eukl. Algo.

3.17. **Beispiel.** Wir berechnen wieder den ggT von 345 und 567 und zusätzlich eine ihn darstellende Linearkombination:

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).

DEF relativ prim teilerfremd

✳ 3.18. **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 $ua + vb = 1$ (das ist äquivalent dazu, dass $\langle a, b\rangle_R = R$ ist). In diesem Fall schreiben wir auch $a \perp b$. Ist R ein Integritätsbereich, dann sagen wir, a und b sind *teilerfremd*, wenn $\mathrm{ggT}(a, b) \sim 1$ in R gilt. ♢

In Hauptidealringen sind nach Folgerung 3.16 beide Begriffe äquivalent.

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

Das folgende wichtige Lemma zeigt die Nützlichkeit des Begriffs „relativ prim“.

3.19. **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 die 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. (Denn aus $ca = b = c'a$ folgt $(c - c')a = 0$; wegen $a \neq 0$ folgt dann $c = c'$.) Wir schreiben dann auch b/a (oder $\frac{b}{a}$) für c.

DEF
b/a

3.20. **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 3.16 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.

3.21. **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.

SATZ
kgV durch ggT in HIR

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. Sei dann $g \sim \mathrm{ggT}(a, b)$. Wir schreiben $a' = a/g$, $b' = b/g$; dann gilt $a' \perp b'$ nach Lemma 3.20. Es ist $ab = g \cdot ga'b'$, also müssen wir $ga'b' \sim \mathrm{kgV}(a, b)$ zeigen. Wegen $ga'b' = ab' = a'b$ ist $ga'b'$ jedenfalls ein gemeinsames Vielfaches von a und b. Sei k ein weiteres gemeinsames Vielfaches. Dann gibt es $r, s \in R$ mit $k = ar = ga'r = bs = gb's$; insbesondere ist b' ein Teiler von $k/g = a'r$. Da a' und b' relativ prim sind, folgt mit Lemma 3.19, dass b' ein Teiler von r sein muss. Damit folgt $ga'b' \mid ga'r = k$, was zu zeigen war. ❑

4. Primelemente und Faktorisierung

Wir wollen in diesem Abschnitt zeigen, dass es in jedem Hauptidealring eine „eindeutige Primfaktorzerlegung“ gibt, wie wir sie für die ganzen Zahlen kennen. Dazu müssen wir erst einige Begriffe einführen.

∗ 4.1. **Definition.** Sei R ein Integritätsbereich. Ein Element $r \in R$ heißt *irreduzibel*, wenn $r \neq 0$, $r \notin R^\times$ ist und für alle $a, b \in R$ mit $r = ab$ gilt $a \in R^\times$ oder $b \in R^\times$. ♢

DEF irreduzibel

Kurz gesagt: Es gibt keine nichttriviale Faktorisierung von r; r ist multiplikativ unzerlegbar.

∗ 4.2. **Definition.** Sei R ein Integritätsbereich. Ein Element $r \in R$ heißt *prim* oder ein *Primelement* von R, wenn $r \neq 0$, $r \notin R^\times$ ist und wenn für alle $a, b \in R$ gilt:

$$r \mid ab \implies r \mid a \quad \text{oder} \quad r \mid b\,. \qquad ♢$$

DEF Primelement

Durch Induktion folgt dann: Ist $p \in R$ prim und teilt p ein Produkt $a_1 a_2 \cdots a_n$, dann muss p einen Faktor a_j teilen.

Zwischen diesen Begriffen gibt es folgenden Zusammenhang:

4.3. **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. 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 $r \mid b$. Wir können annehmen, dass $r \mid a$ gilt (sonst vertauschen wir die Rollen von a und b). Es gilt aber auch $a \mid ab = r$, also sind a und r assoziiert; dann muss $b \in R^\times$ sein, also ist r irreduzibel.

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 $r \perp a$ (hier benutzen wir, dass R ein Hauptidealring ist). Nach Lemma 3.19 folgt dann $r \mid b$. ❑

Im Hauptidealring $\mathbb{Z}$ heißen die positiven primen Elemente *Primzahlen*. Die übliche Definition sagt, dass sie irreduzibel sind; nach Lemma 4.3 sind sie dann auch prim.

DEF Primzahl

4.4. **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

4.5. **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

Folgende Beobachtung ist nützlich.

4.6. **Lemma.** *Seien R ein Integritätsbereich und $p, q \in R$ zwei Primelemente. Gilt $p \mid q$, dann sind p und q assoziiert.*

LEMMA assoziierte Primelemente

Beweis. Nach Voraussetzung gibt es $r \in R$ mit $q = rp$. Da q als Primelement nach Lemma 4.3 auch irreduzibel ist und p keine Einheit ist, muss r eine Einheit sein; damit gilt $q \sim p$. ❑

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 einer Weise, die diese trivialen Uneindeutigkeiten gewissermaßen „ausblendet“.

∗ 4.7. **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

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

DEF faktorieller Ring

Dabei ist das formal möglicherweise unendliche Produkt so definiert, dass es gleich dem Produkt der endlich vielen Faktoren $\neq 1$ ist. (Beachte, dass $r^0 = 1$ ist für alle $r \in R$. Das leere Produkt hat den Wert 1.)

4.8. **Beispiel.** Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell. Zum Beispiel hat das Element $2 \in R$ keine Faktorisierung in Primelemente (weil 2 irreduzibel und nicht prim ist; siehe Beispiel 4.5). 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, aber paarweise nicht assoziiert, und man hat die beiden wesentlich verschiedenen Faktorisierungen

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

BSP nicht faktoriell

Jetzt formulieren und beweisen wir das Hauptergebnis dieses Abschnitts.

∗ 4.9. **Satz.** *Ist R ein Hauptidealring, dann ist R faktoriell.*

SATZ HIR ist faktoriell

Beweis. Sei $\mathbb{P}_R$ ein Repräsentantensystem der Primelemente von R bis auf Assoziierte. Wir zeigen zunächst die Existenz der Faktorisierung. Sei $M \subset R \setminus \{0\}$ die Menge der Elemente, die nicht in der Form $u \prod_{p\in\mathbb{P}_R} p^{e_p}$ geschrieben werden können. Wir wollen zeigen, dass $M = \emptyset$ ist. Das geht über einen Widerspruchsbeweis. Sei $a \in M$. Dann kann a keine Einheit sein (sonst könnten wir $u = a$ und alle $e_p = 0$ wählen). a kann auch nicht irreduzibel sein, denn dann wäre a auch prim, also gäbe es $p \in \mathbb{P}_R$ mit $a \sim p$, und wir könnten $u = a/p \in R^\times$, $e_p = 1$ und $e_{p'} = 0$ für alle $p' \in \mathbb{P}_R \setminus \{p\}$ wählen. Also gibt es $r, s \in R$ mit $a = rs$ und $r, s \notin R^\times$. Wären r und s beide nicht in M, dann auch ihr Produkt a (denn das Produkt zweier Faktorisierungen wie oben lässt sich wieder in dieser Form schreiben). Also ist $r \in M$ oder $s \in M$. Das zeigt: Zu jedem $a \in M$ gibt es ein $a' \in M$, sodass a'

ein echter Teiler von a ist (also $a' \mid a$, aber $a' \not\sim a$). Wir führen jetzt die Annahme $M \neq \emptyset$ wie folgt auf einen Widerspruch. Sei $a_0 \in M$. Wir konstruieren eine Folge von Elementen von M mittels $a_{n+1} = a'_n$. Dann ist jeweils a_{n+1} ein echter Teiler von a_n, also $\langle a_n \rangle_R \subsetneq \langle a_{n+1} \rangle_R$ für alle $n \geq 0$. Die aufsteigende Vereinigung $I = \bigcup_{n \geq 0} \langle a_n \rangle_R$ ist nach Lemma 3.9 ein Ideal von R. Da R ein Hauptidealring ist, gibt es $a \in R$ mit $I = \langle a \rangle_R$. Dann muss es $n \geq 0$ geben mit $a \in \langle a_n \rangle_R$, also

$$\langle a \rangle_R \subset \langle a_n \rangle_R \subsetneq \langle a_{n+1} \rangle_R \subset I = \langle a \rangle_R ,$$

was den gewünschten Widerspruch liefert.

Für den Beweis der Eindeutigkeit sei

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

mit $u, u' \in R^\times$ und $e_p, e'_p \in \mathbb{Z}_{\geq 0}$ für alle $p \in \mathbb{P}_R$ mit $e_p = e'_p = 0$ für alle bis auf endlich viele p. Wir zeigen zunächst $e_p = e'_p$ für alle p. Anderenfalls wäre etwa $e_p > e'_p$. Wir können beide Seiten der Gleichung durch $p^{e'_p}$ teilen; so können wir ohne Einschränkung $e_p > e'_p = 0$ annehmen. Dann teilt p das linke Produkt, muss (als Primelement) also auch einen Faktor des rechten Produkts teilen. Das ist aber nicht der Fall, da p keine Einheit teilt und da ein Primelement q, das von p geteilt wird, zu p assoziiert sein muss (Lemma 4.6). Dieser Widerspruch zeigt, dass $e_p = e'_p$ sein muss für alle $p \in \mathbb{P}_R$. Dann folgt aber auch $u = u'$. ❑

Auch bei diesem Satz gilt die Umkehrung nicht. Ein Beispiel für einen faktoriellen Ring, der kein Hauptidealring ist, ist der Polynomring $\mathbb{Z}[x]$ über dem Ring $\mathbb{Z}$ der ganzen Zahlen (Polynomringe werden später in dieser Vorlesung noch ausführlich besprochen): Man kann ganz allgemein zeigen, dass für einen faktoriellen Ring R auch der Polynomring $R[x]$ wieder faktoriell ist. Auf der anderen Seite ist zum Beispiel $\langle 2, x \rangle_{\mathbb{Z}[x]}$ kein Hauptideal (2 und x haben 1 als ggT, aber das Ideal ist nicht ganz $\mathbb{Z}[x]$).

Wir schreiben $\mathbb{P}$ für die Menge der Primzahlen in $\mathbb{Z}$. Dann ist $\mathbb{P}$ ein Repräsentantensystem der Primelemente von $\mathbb{Z}$ bis auf Assoziierte.

DEF $\mathbb{P}$

4.10. **Folgerung.** *Der Ring $\mathbb{Z}$ ist faktoriell: Jede ganze Zahl $n \neq 0$ kann eindeutig geschrieben werden als*

$$n = \pm \prod_{p \in \mathbb{P}} p^{e_p} \qquad \text{mit } e_p \in \mathbb{Z}_{\geq 0} \text{ und } e_p = 0 \text{ für alle bis auf endlich viele } p.$$

FOLG Primfaktorzerlegung in $\mathbb{Z}$

Insbesondere hat jede natürliche Zahl $n \geq 2$ einen Primteiler, also eine Primzahl p mit $p \mid n$.

DEF Primteiler

Beweis. $\mathbb{Z}$ ist ein Hauptidealring; die Aussage folgt somit aus Satz 4.9.

Ist $n \geq 2$, dann muss wenigstens ein e_p positiv sein; damit ist p ein Primteiler von n. ❑

Die Existenz und Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ kann man auch direkter und „konstruktiver“ beweisen.

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

SATZ Eindeutige Primfaktorisierung in $\mathbb{Z}$

Beweis. Die Existenz zeigen wir durch Induktion. $n = 1$ kann als das leere Produkt von Primzahlen geschrieben werden. Sei nun $n > 1$. Dann ist entweder n eine Primzahl und somit trivialerweise ein Produkt von Primzahlen, oder n ist keine Primzahl und damit nicht irreduzibel; es gibt also $n_1, n_2 \in \mathbb{Z}_{\geq 2}$ mit $n = n_1 n_2$. Insbesondere sind n_1 und n_2 echt kleiner als n. Nach Induktionsannahme können also n_1 und n_2 als Produkte von Primzahlen geschrieben werden, was eine Darstellung von $n = n_1 n_2$ als Produkt von Primzahlen liefert.

Die Eindeutigkeit zeigen wir ebenfalls 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 $p_1 \mid q_j$ für ein $j \in \{1, 2, \ldots, l\}$. Da p_1 und q_j Primzahlen sind, 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. ❑

4.11. **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 $1/p \notin \mathbb{Z}_{\langle p \rangle}$. Jeder faktorielle Ring mit bis auf Assoziierte genau einem Primelement ist ein Hauptidealring (Übung), also ist $\mathbb{Z}_{\langle p \rangle}$ ein Hauptidealring. ♣

Allgemeiner kann man zeigen: Ist R ein faktorieller Ring mit nur endlich vielen Primelementen bis auf Assoziierte, dann ist R ein Hauptidealring. Das liefert eine teilweise Umkehrung von Satz 4.9.

Man kann faktorielle Ringe durch die zwei Eigenschaften charakterisieren, die wesentlich für den Beweis von Satz 4.9 waren, wie der folgende Satz zeigt.

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

SATZ Charakterisierung von „faktoriell“

(1) *(„Teilerkettenbedingung“) 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 gilt.*

(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. Die Existenz der Faktorisierung ergibt sich analog wie im Beweis von Satz 4.9; dort haben wir genau die Eigenschaft (1) benutzt. Der Beweis der Eindeutigkeit geht ebenso analog wie für Satz 4.9.

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, was Eigenschaft (2) zeigt. Für den Beweis von (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. ❑

Die Richtung „⇐“ in Satz 4.12 werden wir später brauchen, um zu zeigen, dass Polynomringe über faktoriellen Ringen wieder faktoriell sind.

Dass die zweite Bedingung in Satz 4.12 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. Wir beginnen mit dem Ring $R_0 = \mathbb{Z}_{\langle 2\rangle} \subset \mathbb{R}$ aus Beispiel 4.11 (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

4.13. **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 $v_p\colon R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ 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 4.7, 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

4.14. **Lemma.** *Seien R ein faktorieller Ring und $\mathbb{P}_R$ ein Repräsentantensystem der Primelemente von R bis auf Assoziierte. Dann gilt für $a, b \in R$ und $p \in \mathbb{P}_R$:*

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

(2) $v_p(ab) = v_p(a) + v_p(b)$.

(3) $a \mid b \iff \forall p \in \mathbb{P}_R\colon v_p(a) \leq v_p(b)$.
Insbesondere gilt $a \sim b \iff \forall p \in \mathbb{P}_R\colon v_p(a) = v_p(b)$.

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

(2) Für $a = 0$ oder $b = 0$ ist das klar. Sonst folgt es aus der Eindeutigkeit der Primfaktorisierung: Multiplikation der Primfaktorisierungen von a und b führt zur Addition der Exponenten.

(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. Die zweite Aussage folgt aus $a \sim b \iff a \mid b$ und $b \mid a$. ❑

FOLG Existenz von ggT und kgV in faktoriellen Ringen

4.15. **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 $a, b \in R$: $\mathrm{ggT}(a,b)\,\mathrm{kgV}(a,b) \sim ab$.

Die letzte Aussage verallgemeinert Satz 3.21.

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 4.14: Zum Beispiel ist $g \in R$ genau dann ein gemeinsamer Teiler von a und b, wenn

$$\forall p \in \mathbb{P}_R\colon v_p(g) \leq \min\{v_p(a), v_p(b)\}$$

gilt. Die letzte Aussage ergibt sich dann (mit Lemma 4.14, (2)) aus der Relation

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

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 von $v_2(r)$ 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 $\mathbb{Z}[i]$ 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 formulieren eine wichtige Eigenschaft.

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

5.2. **Satz.** *$\mathbb{Z}[\boldsymbol{i}]$ ist ein euklidischer Ring mit der euklidischen 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. Siehe Aufgabe (4) auf Übungsblatt 2.

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

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

Beweis. Das folgt aus Satz 3.12 und Satz 4.9. ❑

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

(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 $N(\varepsilon) = a^2+b^2 = 1$, dann muss $(a,b) = (\pm 1, 0)$ oder $(0,\pm 1)$ sein; damit ist $\varepsilon \in \{1,-1,\boldsymbol{i},-\boldsymbol{i}\}$. Umgekehrt sind alle Elemente dieser Menge Einheiten (denn $\boldsymbol{i}\cdot(-\boldsymbol{i}) = 1$).

(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 nach Teil (1) 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 (denn mit π ist auch p prim in $\mathbb{Z}[\boldsymbol{i}]$). ❑

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

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 $p = 4k+1$

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

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

(1) $1+i$,

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

(3) $\pi = a+bi$ *und* $\bar{\pi} = a-bi$ *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 $\mathbb{Z}[i]$ 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 $\pm 1 \pm i$. 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 $\mathbb{Z}[i]$ Norm q haben müsste, ist q irreduzibel und damit prim. Nach Lemma 5.5 sind alle Primteiler von q in $\mathbb{Z}[i]$ 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 $u^2+1 = (u+i)(u-i)$, aber nicht von $u \pm i$ ist, kann p nicht prim in $\mathbb{Z}[i]$ sein. Es gibt also $\pi = a+bi \in \mathbb{Z}[i]$ 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 wiederum nicht zueinander assoziiert sind (die Assoziierten von π sind $a+bi$, $-b+ai$, $-a-bi$ und $b-ai$).

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

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

FOLG 2-□-Satz für Primzahlen

* 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 $p = a^2+b^2$.*

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 $\pi = a'+b'i$ gilt dann $\pi \mid p$; es folgt (aus dem Beweis von Satz 5.7), dass $\pi \sim a+bi$ oder $\pi \sim a-bi$ 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 $(a', b') = (a, b)$. ❑

P. de Fermat 1607–1665

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

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

5.9. **Beispiel.** Es ist $22^2+1 = 484+1 = 485 = 5\cdot 97$, also gilt $97 \mid 22^2+1$. Wir berechnen $\operatorname{ggT}(97, 22+\boldsymbol{i})$: $97 = 4(22+\boldsymbol{i}) + (9-4\boldsymbol{i})$ 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 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. ❑

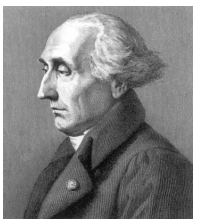
Wir formulieren hier noch ohne Beweis entsprechende Aussagen über Summen von mehr als zwei Quadraten.

5.11. **Satz.** *Jede ganze Zahl $n\geq 0$ 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



J.-L. Lagrange 1736–1813

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.

Man zeigt zuerst relativ einfach, dass die Menge der natürlichen Zahlen, die Summen von vier Quadraten sind, multiplikativ abgeschlossen ist. Das folgt aus der Formel

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

Dann muss man noch zeigen, dass jede Primzahl Summe von vier Quadraten ist. Das lässt sich mit den Mitteln dieser Vorlesung eigentlich gut machen (siehe zum Beispiel §7 in meinem Skript dieser Vorlesung vom Wintersemester 2012), würde aber leider zu viel Zeit brauchen.

C.F. Gauß 1777–1855

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

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

5.12. **Satz.** *Eine ganze Zahl $n\geq 0$ lässt sich genau dann in der Form*

$$n = a^2+b^2+c^2 \qquad \text{mit } a,b,c\in\mathbb{Z}$$

schreiben, wenn n nicht die Form $4^m(8k+7)$ mit $k,m\in\mathbb{Z}_{\geq 0}$ hat.

SATZ 3-□-Satz von Gauß

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 allerdings tiefere Hilfsmittel.

6. Ringhomomorphismen und Faktorringe

Wir haben bisher immer nur einen Ring betrachtet. Es ist aber wie in vielen anderen Gebieten der Mathematik 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).

DEF Ringhomomorphismus

∗ 6.1. **Definition.** Seien R_1, R_2 zwei Ringe. Ein *Ringhomomorphismus* von R_1 nach R_2 ist eine Abbildung $\phi\colon R_1 \to R_2$ 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!)

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. ♢

LEMMA Eigensch. von Ringhomomorphismen

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

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 $\phi(1) = 1$. ❑

DEF Ringisomorphismus
isomorph
Automorphismus

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

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

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 $\mathrm{id}_R\colon R \to R$ ein Automorphismus.

(2) Sei $\mathbb{F}_2 = \{0, 1\}$ der Körper mit zwei Elementen. Die Abbildung

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

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 $\phi\colon \mathbb{Z} \to R$: 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 $\phi(m)$ (mit $m \in \mathbb{Z}$), 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 $\mathbb{Z} \to \mathbb{Z}[\boldsymbol{i}]$ ist gegeben durch $a \mapsto a + 0\boldsymbol{i}$. In der anderen Richtung gibt es keinen Ringhomomorphismus $\phi\colon \mathbb{Z}[\boldsymbol{i}] \to \mathbb{Z}$: Angenommen, so ein ϕ existiert. Dann ist $a = \phi(\boldsymbol{i})$ eine ganze Zahl, und es würde folgen $a^2 = \phi(\boldsymbol{i})^2 = \phi(\boldsymbol{i}^2) = \phi(-1) = -1$, was nicht möglich ist.

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

(6) Der Körper $\mathbb{R}$ besitzt außer der Identität keinen weiteren (Ring-)Automorphismus (Übung).

(7) Seien $R_1, \ldots, R_n$ Ringe. Die j-te Projektion $\mathrm{pr}_j\colon R_1 \times \cdots \times R_n \to R_j$ (für $j \in \{1, 2, \ldots, n\}$) ist ein Ringhomomorphismus. Das liegt daran, dass die Struktur des Produktrings komponentenweise definiert ist. ♣

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

Wie bei linearen Abbildungen sind Kern und Bild interessant.

6.5. **Definition.** Sei $\phi\colon R_1 \to R_2$ 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. **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 Unterringen und Idealen vertragen. Das ist im Wesentlichen analog zu den entsprechenden Aussagen über lineare Abbildungen und Untervektorräume. Der Hauptunterschied ist, dass es hier zwei verschiedene Arten von Unterstrukturen gibt.

LEMMA
Homomorphismen und Unterringe bzw. Ideale

6.7. **Lemma.** *Sei $\phi\colon R_1 \to R_2$ ein Ringhomomorphismus.*

(1) *Ist $S_1 \subset R_1$ ein Unterring, dann ist $\phi(S_1) \subset R_2$ ein Unterring. Insbesondere ist $\operatorname{im}(\phi) = \phi(R_1)$ ein Unterring von R_2.*

(2) *Ist $S_2 \subset R_2$ ein Unterring, dann ist $\phi^{-1}(S_2) \subset R_1$ ein Unterring.*

(3) *Ist $I_1 \subset R_1$ ein Ideal, dann ist $\phi(I_1)$ ein Ideal im Unterring $\operatorname{im}(\phi)$ von R_2 (aber nicht unbedingt in R_2 selbst!).*

(4) *Ist $I_2 \subset R_2$ ein Ideal, dann ist $\phi^{-1}(I_2)$ ein Ideal von R_1. Insbesondere ist $\ker(\phi) = \phi^{-1}(\{0\})$ ein Ideal von R_1.*

(5) *ϕ ist genau dann injektiv, wenn $\ker(\phi) = \{0\}$ ist.*

(6) *Ist ϕ surjektiv, dann erhalten wir zueinander inverse inklusionserhaltende Bijektionen*

$$\begin{aligned} \{I_1 \subset R_1 \mid I_1 \text{ Ideal und } \ker(\phi) \subset I_1\} &\longleftrightarrow \{I_2 \subset R_2 \mid I_2 \text{ Ideal}\} \\ I_1 &\longmapsto \phi(I_1) \\ \phi^{-1}(I_2) &\longmapsfrom I_2\,. \end{aligned}$$

Beweis.

(1) Es gilt $0 = \phi(0) \in \phi(S_1)$ und $1 = \phi(1) \in \phi(S_1)$. Sind $s, s' \in \phi(S_1)$, dann gibt es $r, r' \in S_1$ mit $\phi(r) = s$, $\phi(r') = s'$. Es folgt

$$\begin{aligned} s + s' = \phi(r) + \phi(r') = \phi(r + r') \in \phi(S_1), \\ -s = -\phi(r) = \phi(-r) \in \phi(S_1), \\ ss' = \phi(r)\phi(r') = \phi(rr') \in \phi(S_1)\,. \end{aligned}$$

Damit erfüllt $\phi(S_1)$ die Bedingungen für einen Unterring von R_2.

(2) Wegen $\phi(0) = 0 \in S_2$, $\phi(1) = 1 \in S_2$ gilt $0, 1 \in \phi^{-1}(S_2)$. Sind $r, r' \in \phi^{-1}(S_2)$, dann sind $s = \phi(r) \in S_2$, $s' = \phi(r') \in S_2$. Es folgt

$$\begin{aligned} \phi(r + r') = \phi(r) + \phi(r') = s + s' \in S_2 \Longrightarrow r + r' \in \phi^{-1}(S_2), \\ \phi(-r) = -\phi(r) = -s \in S_2 \Longrightarrow -r \in \phi^{-1}(S_2), \\ \phi(rr') = \phi(r)\phi(r') = ss' \in S_2 \Longrightarrow rr' \in \phi^{-1}(S_2)\,. \end{aligned}$$

Damit erfüllt $\phi^{-1}(S_2)$ die Bedingungen für einen Unterring von R_1.

(3) Es gilt $0 = \phi(0) \in \phi(I_1)$. Sind $s, s' \in \phi(I_1)$, dann gibt es $r, r' \in I_1$ mit $s = \phi(r)$, $s' = \phi(r')$. Es folgt $s + s' = \phi(r) + \phi(r') = \phi(r + r') \in \phi(I_1)$. Ist außerdem $b \in \operatorname{im}(\phi)$, dann gibt es $a \in R_1$ mit $\phi(a) = b$, und es folgt $bs = \phi(a)\phi(r) = \phi(ar) \in \phi(I_1)$. Damit erfüllt $\phi(I_1)$ die Bedingungen dafür, ein Ideal von $\operatorname{im}(\phi)$ zu sein.

(4) Wegen $\phi(0) = 0 \in I_2$ ist $0 \in \phi^{-1}(I_2)$. Sind $r, r' \in \phi^{-1}(I_2)$, dann sind $s = \phi(r) \in I_2$, $s' = \phi(r') \in I_2$. Es folgt $\phi(r+r') = \phi(r)+\phi(r') = s+s' \in I_2$, also $r + r' \in \phi^{-1}(I_2)$. Sei jetzt zusätzlich $a \in R_1$. Dann ist $b = \phi(a) \in R_2$ und es folgt $\phi(ar) = \phi(a)\phi(r) = bs \in I_2$, also $ar \in \phi^{-1}(I_2)$. Also ist $\phi^{-1}(I_2)$ ein Ideal von R_1.

(5) Ist ϕ injektiv, dann gilt

$$r \in \ker(\phi) \implies \phi(r) = 0 = \phi(0) \implies r = 0\,,$$

also ist $\ker(\phi) = \{0\}$. Ist umgekehrt $\ker(\phi) = \{0\}$, und sind $r, r' \in R_1$ mit $\phi(r) = \phi(r')$, dann folgt $0 = \phi(r) - \phi(r') = \phi(r - r')$, also $r - r' \in \ker(\phi) = \{0\}$ und damit $r = r'$. Damit ist gezeigt, dass ϕ injektiv ist.

(6) Nach Teil (3) und (4) sind die beiden Abbildungen wohldefiniert (es ist klar, dass $\phi^{-1}(I_2) \supset \ker(\phi) = \phi^{-1}(\{0\})$). Es ist auch klar, dass sie inklusionserhaltend sind. Es bleibt zu zeigen, dass sie zueinander invers sind. Weil ϕ surjektiv ist, gilt $\phi(\phi^{-1}(I_2)) = I_2$ für jede Teilmenge $I_2 \subset R_2$, insbesondere für jedes Ideal. Sei jetzt $I_1 \subset R_1$ ein Ideal mit $\ker(\phi) \subset I_1$. Dann gilt in jedem Fall $\phi^{-1}(\phi(I_1)) \supset I_1$, und es ist noch die umgekehrte Inklusion zu zeigen. Sei also $r \in \phi^{-1}(\phi(I_1))$, d.h. $\phi(r) \in \phi(I_1)$. Dann gibt es $r' \in I_1$ mit $\phi(r) = \phi(r')$. Es folgt $\phi(r - r') = \phi(r) - \phi(r') = 0$, also ist $r - r' \in \ker(\phi) \subset I_1$ und damit ist auch $r = r' + (r - r') \in I_1$. ❑

6.8. **Beispiel.** Sei $\phi\colon \mathbb{Z} \to \mathbb{Q}$ 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 $I_2 \mapsto \phi^{-1}(I_2)$ weit davon entfernt, surjektiv zu sein (ϕ ist injektiv, also $\ker(\phi) = \{0\}$, sodass die Bedingung $\ker(\phi) \subset I_1$ 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. Die Definition ist analog zu $v \equiv v' \bmod U$ für einen Untervektorraum U eines Vektorraums V.

6.9. **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. Ist $I = Rc$ ein Hauptideal, dann sagen und schreiben wir auch „modulo c“ bzw. $a \equiv b \bmod c$. ♢

DEF
kongruent
modulo I

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.

6.10. **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: $a \equiv b \bmod I \Rightarrow a - b \in I \Rightarrow -(a - b) = b - a \in I$, also $b \equiv a \bmod I$.
Transitivität: $a \equiv b \bmod I$, $b \equiv c \bmod I \Rightarrow a - b,\ b - c \in I$; damit ist auch $a - c = (a - b) + (b - c) \in I$, also $a \equiv c \bmod I$.

(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. ❑

* 6.11. **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* oder *Restklassenring* von R modulo I. ♢

DEF Faktorring

Wie immer bei Äquivalenzklassen gilt $[a] = [b] \iff a \equiv b \bmod I$.

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

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

SATZ Faktorring ist Ring

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

DEF kanon. Epimorphismus

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 6.10, (2). Die Ringaxiome übertragen sich dann sofort von R auf R/I. Schließlich gilt

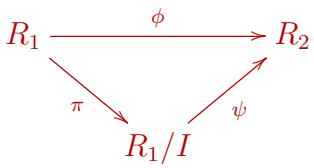
$$\ker(\phi) = \phi^{-1}(\{[0]\}) = \{a \in R \mid [a] = [0]\} = \{a \in R \mid a \in I\} = I\,. \qquad ❑$$

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.

* 6.13. **Satz.** *Sei $\phi\colon R_1 \to R_2$ ein Ringhomomorphismus und $I \subset R_1$ ein Ideal. Sei weiter $\pi\colon R_1 \to R_1/I$ der kanonische Epimorphismus. Es gibt genau dann einen Ringhomomorphismus $\psi\colon R_1/I \to R_2$, der das Diagramm*

SATZ Homomorphiesatz für Ringe



kommutativ macht, wenn $I \subset \ker(\phi)$ ist. In diesem Fall ist ψ eindeutig bestimmt. ψ ist genau dann injektiv, wenn $I = \ker(\phi)$ ist. Damit ist

$$\varphi\colon R_1/\ker(\phi) \longrightarrow \operatorname{im}(\phi), \quad [a] \longmapsto \phi(a)$$

ein Isomorphismus; insbesondere sind $R_1/\ker(\phi)$ und $\operatorname{im}(\phi)$ isomorph.

Wir sagen, dass ψ und φ von ϕ *induziert* werden.

Beweis. Wir nehmen zunächst an, dass ψ wie angegeben existiert. Für $r \in R_1$ muss dann gelten, dass $\psi([r]) = \psi(\pi(r)) = \phi(r)$ ist. Das zeigt schon einmal die Eindeutigkeit von ψ. Ist $r \in I$, dann ist

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

also ist $r \in \ker(\phi)$; es folgt $I \subset \ker(\phi)$.

Umgekehrt gelte $I \subset \ker(\phi)$. Nach dem eben Gezeigten müssen wir $\psi([r]) = \phi(r)$ definieren, wenn ψ existiert. Es bleibt zu zeigen, dass ψ wohldefiniert und ein Ringhomomorphismus ist. ψ ist wohldefiniert, denn für $r, r' \in R_1$ mit $[r] = [r']$ gilt $r - r' \in I \subset \ker(\phi)$, und es folgt

$$\phi(r) = \phi((r - r') + r') = \phi(r - r') + \phi(r') = 0 + \phi(r') = \phi(r')\,.$$

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

$$\psi([r] + [r']) = \psi([r + r']) = \phi(r + r') = \phi(r) + \phi(r') = \psi([r]) + \psi([r'])\,,$$

und analog für das Produkt.

In jedem Fall gilt dann für $r \in R_1$:

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

also ist $\ker(\psi) = \pi(\ker(\phi))$, und $\ker(\psi) = \{[0]\}$ ist äquivalent zu $[r] = [0]$ für alle $r \in \ker(\phi)$, also $\ker(\phi) \subset I$. Da ja $I \subset \ker(\phi)$ gilt, folgt, dass ψ genau dann injektiv ist, wenn $I = \ker(\phi)$ ist.

Wir erhalten φ, indem wir $I = \ker(\phi)$ betrachten und den daraus erhaltenen Homomorphismus $\psi\colon R_1/\ker(\phi) \to R_2$ im Ziel auf sein Bild $\operatorname{im}(\psi) = \operatorname{im}(\phi)$ einschränken. Damit ist φ jedenfalls surjektiv; nach dem eben Bewiesenen ist φ auch injektiv und somit ein Isomorphismus. ❑

Beispiel. Ein Beispiel für die Anwendung von Satz 6.13 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 $\lim\colon C \to \mathbb{R}$, $(a_n) \mapsto \lim_{n\to\infty} a_n$ einen surjektiven Ringhomomorphismus mit Kern N, also ist $C/N \cong \mathbb{R}$. ♣

BSP
Konstruktion von $\mathbb{R}$

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:

6.14. **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.*

LEMMA
Faktorringe von $\mathbb{Z}$

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

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

6.15. **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]) ♣

Man kann sich jetzt fragen, wie man den „richtigen“ Faktorring findet, in dem man am ehesten einen Widerspruch bekommt. Die wesentliche Überlegung dabei ist, dass man möglichst wenige Quadrate, dritte Potenzen, oder was auch immer in dem jeweiligen Problem auftritt, haben möchte, weil man dann die besten Chancen hat, einen Widerspruch zu finden. Für Quadrate sind häufig $\mathbb{Z}/4\mathbb{Z}$ oder $\mathbb{Z}/8\mathbb{Z}$ gut geeignet, für dritte Potenzen $\mathbb{Z}/9\mathbb{Z}$ oder auch $\mathbb{Z}/7\mathbb{Z}$. Ein anderes Kriterium ist, dass man möglichst Terme zum Verschwinden bringen möchte; dann wird man modulo einem Teiler eines (oder mehrerer) Koeffizienten rechnen. Eine Garantie, dass dieser Ansatz funktioniert, gibt es aber nicht: Es gibt Gleichungen, die Lösungen modulo n haben für alle $n \in \mathbb{Z}_{>0}$, aber keine Lösungen in $\mathbb{Z}$.

Wir wollen jetzt Lemma 6.7, (6) und Satz 6.13 kombinieren, um einen Zusammenhang herzustellen zwischen Eigenschaften des Bildes und des Kerns eines Ringhomomorphismus. Dazu definieren wir erst einmal die relevanten Eigenschaften von Idealen.

* 6.16. **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 $b \in I$. ♢

6.17. **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. ♣

* 6.18. **Satz.** *Sei $\phi\colon R_1 \to R_2$ 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 $R_1/\ker(\phi) \cong \operatorname{im}(\phi)$ nach Satz 6.13 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 $\phi\colon R \to R/I$ 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 6.7, (6) besteht eine Bijektion zwischen den Idealen von $\operatorname{im}(\phi)$ und den $\ker(\phi)$ enthaltenden Idealen von R_1. Nun ist ein (kommutativer) Ring genau dann ein Körper, wenn er *genau zwei* Ideale hat (siehe Aufgabe (4) auf Übungsblatt 3). 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 genau dann *kein* Integritätsbereich, 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.) ❑

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. ♣

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

Dass $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist, ist nach Satz 6.18 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.

Man kann das auch direkt leicht sehen: 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 dagegen $n = p$ 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“.) ♣ **DEF** $\mathbb{F}_p$

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. *Seien 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 57–58 des Skripts „Lineare Algebra I“ vom Wintersemester 2016/17.

7. Der Chinesische Restsatz

In diesem Abschnitt sind wieder alle Ringe *kommutativ*, wenn nichts anderes gesagt wird.

Wir erinnern uns an den Produktring $R_1 \times \cdots \times R_n$ aus Beispiel 3.1 (1). Dabei sind $R_1, \ldots, R_n$ Ringe, und die Verknüpfungen sind komponentenweise definiert. Ist $n = 0$, dann ist das Produkt ein Nullring.

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

$$\psi \colon R \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n\,, \qquad r \longmapsto (r + I_1, r + I_2, \ldots, r + I_n)$$

kombinieren. 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 nach Satz 6.13 einen injektiven Ringhomomorphismus

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

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

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

DEF Summe von Idealen

7.1. **Definition.** Seien R ein Ring und I, J Ideale von R. Die *Summe* von I und J ist (analog wie bei Untervektorräumen) definiert als

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

Analog definiert man die Summe von mehr als zwei Idealen. ♢

LEMMA Surjektivität von $\tilde{\psi}$

7.2. **Lemma.** *Der Homomorphismus $\tilde{\psi}$ ist genau dann surjektiv, wenn es Elemente $r_1, \ldots, r_n \in R$ gibt, sodass für alle $1 \le j \le n$ gilt*

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

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

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.

DEF komaximal

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

Sind zwei ganze Zahlen m und n teilerfremd, dann gilt $\mathrm{ggT}(m,n) = 1$ 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?

DEF Produkt von Idealen

7.4. **Definition.** Seien R ein Ring und $I_1, \ldots, I_n$ Ideale von R. Das *Produkt* von $I_1, \ldots, I_n$ ist 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, wobei der Faktor a_j aus I_j ist, und besteht aus allen endlichen Summen solcher Produkte. Als Spezialfall haben wir für Hauptideale

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

LEMMA Schnitt komaximaler Ideale

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

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

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 $I_1 \cap \ldots \cap I_{n-1} = I_1 \cdots I_{n-1}$. Wir zeigen, dass I_n und $I_1 \cdots I_{n-1} = I_1 \cap \ldots \cap I_{n-1}$ komaximal sind. Nach Voraussetzung sind I_n und I_j komaximal für alle $j \leq n-1$, also gibt es $a_j \in I_j$, $b_j \in I_n$ mit $a_j + b_j = 1$. Das Produkt dieser Gleichungen liefert

$$1 = \prod_{j=1}^{n-1}(a_j + b_j) = \prod_{j=1}^{n-1} a_j + (r_1 b_1 + r_2 b_2 + \ldots + r_{n-1} b_{n-1})$$

mit geeigneten $r_1, \ldots, r_{n-1} \in R$. Dabei ist das Produkt der a_j in $I_1 \cdots I_{n-1}$ und die Summe der $r_j b_j$ in I_n; das zeigt die behauptete Komaximalität. Nun 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.

* 7.6. **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*

SATZ Chinesischer Restsatz

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

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.

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

SATZ Chinesischer Restsatz für Hauptidealringe

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

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.)

Anders ausgedrückt:

In einem Hauptidealring ist ein System von Kongruenzen

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

mit paarweise teilerfremden $a_1, \ldots, a_n$ äquivalent zu einer einzigen Kongruenz

$$x \equiv b \bmod a_1 \cdots a_n\,.$$

Warum heißt der Chinesische Restsatz so? Laut der englischen Wikipedia-Seite dazu taucht er erstmalig in Form einer Aufgabenstellung in einer chinesischen Quelle aus dem 3. Jahrhundert auf. Der allgemeine Satz (über $\mathbb{Z}$) und ein Lösungsalgorithmus findet sich in einer weiteren chinesischen Quelle etwa 1000 Jahre später.

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.

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

BSP simultane 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 7.2:

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

Die Lösung kommt aus dem Erweiterten Euklidischen Algorithmus (vgl. Beispiel 3.17), 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 $x_0 + a_1a_2\mathbb{Z}$.

Was passiert, wenn die „Moduln“ a_j im Chinesischen Restsatz 7.7 nicht paarweise teilerfremd sind? Dann ist die Abbildung in das Produkt der Restklassenringe nicht mehr surjektiv, und man kann fragen, wann ein Tupel $(b_1 + Ra_1, \dots, b_n + Ra_n)$ im Bild liegt, also wann das System

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

lösbar ist. Da für jeden Teiler d von a aus $x \equiv b \bmod a$ auch $x \equiv b \bmod d$ folgt (denn $d \mid a \mid x - b$), ist für die Lösbarkeit jedenfalls notwendig, dass

$$b_i \equiv b_j \bmod \operatorname{ggT}(a_i, a_j) \quad \text{für alle } 1 \le i, j \le n$$

gilt. Umgekehrt kann man ohne große Schwierigkeiten zeigen, dass diese Bedingung auch hinreichend für die Lösbarkeit ist. Die Lösung ist dann bis auf Addition von Vielfachen von $\operatorname{kgV}(a_1, a_2, \dots, a_n)$ eindeutig bestimmt.

Man kann den Chinesischen Restsatz dazu verwenden, Rechnungen zu beschleunigen. Er besagt nämlich zum Beispiel, dass wir eine ganze Zahl a mit $|a| \le M$ aus ihren Restklassen modulo verschiedener Primzahlen $p_1, \dots, p_n$ eindeutig rekonstruieren können,

wenn $p_1 \cdots p_n > 2M$ ist. Wenn wir zum Beispiel die Determinante einer $n \times n$-Matrix A mit Einträgen in $\mathbb{Z}$ berechnen wollen, dann könnten wir dafür den üblichen Algorithmus (mittels Gauß-Elimination) über $\mathbb{Q}$ benutzen. Dann hat man aber mit zunehmend komplizierteren rationalen Zahlen zu tun (in dem Sinn, dass die Zähler und Nenner im Vergleich zu den Einträgen der ursprünglichen Matrix ziemlich groß werden können). Alternativ können wir Folgendes überlegen: Die Determinante ist gegeben durch eine Summe von vorzeichenbehafteten Produkten von Einträgen der Matrix (Leibniz-Formel, vgl. Lineare Algebra I); es folgt für jeden Homomorphismus ϕ von kommutativen Ringen, dass $\det\big(\phi(a_{ij})\big) = \phi\big(\det(a_{ij})\big)$ ist. Insbesondere können wir $\det(A) + p\mathbb{Z} \in \mathbb{F}_p$ als Determinante der Matrix berechnen, deren Einträge die Restklassen mod p der Einträge von A sind. Dafür verwenden wir wieder den üblichen Algorithmus. Wir können $|\det(A)| \leq M$ abschätzen (mit der Hadamardschen Ungleichung); wir wählen dann Primzahlen $p_1, \ldots, p_m$ mit $p_1 \cdots p_m > 2M$. Dann berechnen wir $\det(A) + p_j\mathbb{Z}$ für alle $1 \leq j \leq m$ und rekonstruieren $\det(A) \in \mathbb{Z}$ aus diesen Restklassen. Auf diese Weise müssen wir nur mit den kleinen ganzen Zahlen rechnen, die die Elemente von $\mathbb{F}_{p_j}$ repräsentieren, was zu einem deutlich schnelleren Verfahren führt.

Als Anwendung des Chinesischen Restsatzes für $\mathbb{Z}$ wollen wir 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.

LEMMA Einheitengruppe im Produktring

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

Die Einheitengruppe eines direkten Produkts von Ringen ist also das direkte Produkt der Einheitengruppen (das, analog zu Ringen, wieder eine Gruppe ist, wenn man die Verknüpfung komponentenweise definiert).

Beweis. Sei $(r_i)_{i\in I} \in R = \prod_{i\in I} R_i$. Dann gilt

$$\begin{aligned}
(r_i)_{i\in I} \in R^\times &\iff \exists (s_i)_{i\in I} \in R\colon (r_i)_{i\in I} \cdot (s_i)_{i\in I} = 1 = (s_i)_{i\in I} \cdot (r_i)_{i\in I} \\
&\iff \forall i \in I\ \exists s_i \in R_i\colon r_i s_i = 1 = s_i r_i \\
&\iff \forall i \in I\colon r_i \in R_i^\times \\
&\iff (r_i)_{i\in I} \in \prod_{i\in I} R_i^\times .
\end{aligned}$$

❑

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

DEF Euler-φ

prime Restklassengruppe

7.10. **Definition.** Sei $n \in \mathbb{Z}_{>0}$. Dann setzen wir $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. Die Funktion $\varphi\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ heißt *Eulersche Phi-Funktion*. Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ heißt die *prime Restklassengruppe modulo n*. ♢

Der Name ‘prime Restklassengruppe’ kommt von der folgenden Tatsache:

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

LEMMA
prime Restklassen

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

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

❑

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 $\varphi(n)$ auch wie folgt beschreiben:

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

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
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

Es ist ziemlich klar, dass gilt

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

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:

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

LEMMA
$\varphi(p^e)$

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 $0 \le f \le e$, gilt

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

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 $0 \le a < p^{e-1}$), also bleiben

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

Zahlen übrig. ❑

Zusammen mit dem Chinesischen Restsatz und Lemma 7.9 erhalten wir daraus eine Formel für $\varphi(n)$.

SATZ Formel für $\varphi(n)$

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

$$\varphi(n) = \prod_{p|n} (p-1)p^{v_p(n)-1} = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

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 7.9 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 7.12

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

Man kann also $\varphi(n)$ leicht berechnen, *wenn* man die Primfaktorisierung von n kennt. Für die Berechnung der Letzteren gibt es allerdings bisher keinen wirklich effizienten Algorithmus. Das wird zum Beispiel beim bekannten RSA-Kryptosystem ausgenutzt. Die Verschlüsselung geschieht dabei durch eine Berechnung modulo n, wobei $n = pq$ ein Produkt von zwei großen Primzahlen ist. Man kann das System knacken, wenn man $\varphi(n) = (p-1)(q-1)$ kennt. In diesem Fall ist die Kenntnis von $\varphi(n)$ tatsächlich äquivalent zur Kenntnis von p und q, denn man erhält p und q als die beiden Lösungen der quadratischen Gleichung $x^2 + (\varphi(n) - n - 1)x + n = 0$.

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

LEMMA Rekursion für $\varphi(n)$

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

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

wobei die Summe über alle positiven Teiler von n läuft.

Beweis. Wir betrachten die Menge $M = \{1, 2, \ldots, n\}$. Für jeden Teiler d von n sei $M_d = \{m \in M \mid \mathrm{ggT}(m, n) = d\}$. Da jedes Element von M einen eindeutigen ggT mit n hat, der ein Teiler von n sein muss, ist M die disjunkte Vereinigung

der Mengen M_d. Weiterhin gilt $M_d = \{md \mid 1 \leq m \leq n/d, m \perp n/d\}$ und damit $\#M_d = \varphi(n/d)$. Es folgt

$$n = \#M = \sum_{d|n} \#M_d = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)\,;$$

für die letzte Gleichheit nutzen wir aus, dass $d \mapsto n/d$ die Teiler von n permutiert; die beiden letzten Summen sind also nur Umordnungen voneinander. ❑

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

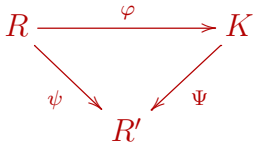
8. Der Quotientenkörper

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.

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

SATZ Quotientenkörper

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



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 $(a', b') \sim (a'', b'')$, also $ab' = a'b$ und $a'b'' = a''b'$. Es folgt

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

  (hier benutzen wir die Kommutativität von R). Da $b' \neq 0$ ist und R keine Nullteiler hat, können wir b' „kürzen“; es folgt $ab'' = a''b$, also $(a, b) \sim (a'', b'')$.

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 $\varphi\colon R \to K$ 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 $\psi\colon R \to R'$ ein Ringhomomorphismus, sodass $\psi(r)$ invertierbar ist für alle $0 \neq r \in R$. Wenn es einen Homomorphismus $\Psi\colon K \to R'$ 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:

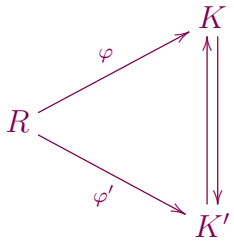
$$\Psi(1) = \Psi(1/1) = \psi(1)\psi(1)^{-1} = 1$$

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', $\varphi'\colon R \to K'$ 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. ❑

8.2. **Definition.** Der Körper K aus Satz 8.1 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 $\varphi\colon R \to K$ 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 einen Ringhomomorphismus $R \to R'$ eindeutig auf K fortsetzen kann, wenn er alle von null verschiedenen Elemente auf invertierbare Elemente von R' abbildet.

8.3. **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 8.1. ❑

8.4. **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 8.3 anwenden und findet, dass der Quotientenkörper von $\mathbb{Z}[\boldsymbol{i}]$ gerade

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

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

ist. Das ergibt sich aus

$$\frac{a + b\boldsymbol{i}}{c + d\boldsymbol{i}} = \frac{(a + b\boldsymbol{i})(c - d\boldsymbol{i})}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}\boldsymbol{i}\,. \qquad ♣$$

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.

9. Polynomringe

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

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

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 $f\colon \mathbb{F}_2 \to \mathbb{F}_2$ 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.

* 9.1. **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

$$(a_0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots) = a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n\,.$$

Das Element $a_j \in R$ heißt der *Koeffizient von x^j* oder der *j-te Koeffizient* im *Polynom* $a_0x^0 + \ldots + a_nx^n$. Wir identifizieren R mit seinem Bild in $R[x]$ unter

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

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

$$\begin{aligned}(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n)\cdot(b_0 + b_1x + b_2x^2 + \ldots + b_mx^m)\\ = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots + (a_nb_m)x^{n+m}\,.\end{aligned}$$

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 $\varphi\colon R \to R[x]$ 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. ♢

Die Schreibweise „$R[x]$“ deutet an, dass der Polynomring von R und x erzeugt wird (d.h., alle Elemente können aus Elementen von R und aus x durch Addition und Multiplikation erzeugt werden), analog dazu wie $R'[\alpha]$ den von R' und α erzeugten Unterring eines Rings R bezeichnet. Der Unterschied ist, dass wir $R[x]$ nicht als Unterring eines „vorher schon vorhandenen“ Rings konstruiert haben.

Man könnte $R[x]$ tatsächlich als Unterring des Endomorphismenrings $\mathrm{End}(M)$ des R-Moduls $M = R^{\mathbb{N}}$ konstruieren (ein *R-Modul* ist wie ein Vektorraum definiert, aber mit dem Ring R statt einem Körper als Heimat der Skalare). $\mathrm{End}(M)$ besteht aus allen R-linearen Abbildungen $M \to M$; die Addition ist die punktweise Addition von Abbildungen und die Multiplikation ist die Verknüpfung von Abbildungen. Die Abbildung $r \mapsto (v \mapsto r \cdot v)$ liefert eine Einbettung von R in $\mathrm{End}(M)$; wir identifizieren ihr Bild mit R. Wir bezeichnen mit x die „Verschiebung“ $(a_0,a_1,a_2,\ldots) \mapsto (0,a_0,a_1,\ldots)$; dann ist $x \in \mathrm{End}(M)$, und wir können den Polynomring dann tatsächlich als den Unterring $R[x]$ von $\mathrm{End}(M)$ definieren.

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.

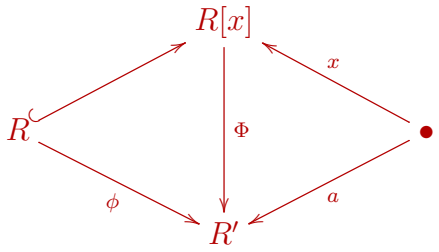
Die Idee hinter der Konstruktion des Polynomrings ist, dass man zum Ring R ein „neues“ Element x hinzufügen möchte, das von den Elementen von R vollkommen „unabhängig“ ist (außer dass es mit ihnen kommutiert). Diese Unabhängigkeit bedeutet, dass polynomiale Ausdrücke in x mit Koeffizienten in R verschieden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

∗ 9.2. **Satz.** *Seien R und R' Ringe, sei $a \in R'$ und sei $\phi\colon R \to R'$ 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 $\Phi\colon R[x] \to R'$ 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 $a\phi(b_j) = \phi(b_j)a$ ist!)

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

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

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

Die analoge universelle Eigenschaft gilt für Polynomringe in mehreren Variablen: Ist $\phi\colon R \to R'$ gegeben und sind $a_1, \ldots, a_n \in R'$ mit $\phi(r)a_j = a_j\phi(r)$ für alle $r \in R$ und $1 \le j \le n$ und zusätzlich $a_ia_j = a_ja_i$ für alle $1 \le i, j \le n$ (beides ist automatisch erfüllt, wenn R' kommutativ ist), dann gibt es eine eindeutig bestimmte Fortsetzung $\Phi\colon R[x_1, \ldots, x_n] \to R'$ von ϕ mit $\Phi(x_j) = a_j$ für alle $1 \le j \le n$.

DEF Auswertungsabbildung Polynomfunktion Nullstelle

9.3. **Definition.** Wenn in der Situation von Satz 9.2 der Homomorphismus ϕ kanonisch ist (zum Beispiel im Fall $R \subset R'$), dann heißt Φ *Auswertungsabbildung in a* oder *Einsetzungshomomorphismus*, und man schreibt suggestiv $f(a)$ für $\Phi(f)$.

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

Für das Rechnen mit Polynomen sind folgende Begriffe hilfreich:

DEF Grad Leitkoeffizient normiert konstant

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

LEMMA Eigensch. des Grades

9.5. **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

9.6. **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 $R[x]$

9.7. **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 $fg = gf = 1$. 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 im Allgemeinen 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“, aus der Linearen Algebra bekannt).

* **SATZ** Polynomdivision

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

Beweis. Die Existenz beweisen wir durch Induktion nach dem Grad 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 9.5 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 9.5 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.

FOLG Nullstellen

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

Beweis. In jedem Fall gibt es (eindeutige) $q, r \in R[x]$ mit $\deg(r) < \deg(x - a) = 1$, also r konstant, und $f = q(x - a) + r$. Wir wenden den Einsetzungshomomorphismus (bzgl. a) an und erhalten $f(a) = q(a)(a - a) + r = r$. Also gilt $f(a) = 0$ genau dann, wenn $r = 0$ ist. Die zweite Aussage zeigt man leicht durch Induktion: Sie ist klar für $n = 0$. Sei f ein Polynom vom Grad $n > 0$. Entweder hat f keine Nullstelle in R, dann ist nichts zu zeigen. Oder $a \in R$ ist eine Nullstelle, dann ist $f = (x - a)g$ mit $\deg(g) = n - 1$. Für $a \neq b \in R$ gilt dann $f(b) = (b - a)g(b)$, also $f(b) = 0 \iff g(b) = 0$. Nach Induktionsannahme hat g höchstens $n - 1$ Nullstellen in R; damit hat f höchstens n Nullstellen. ❑

9.10. **Beispiel.** 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?) ♣

BSP zu viele Nullstellen

Sei $\mathbb{H}$ der Schiefkörper der Quaternionen (vgl. das Kleingedruckte auf Seite 6). 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?)

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

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 $\beta = \mathrm{lcf}(b) \in K^\times$. Sei $b' = \beta^{-1}b$; $b' \in K[x]$ ist ein normiertes Polynom. Nach Satz 9.8 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*.

9.12. **Beispiel.** 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. ♣

BSP $\mathbb{Z}[x]$ kein HIR

Tatsächlich gilt sogar:

Ist $R[x]$ ein Hauptidealring, dann ist R ein Körper.

Folgerung 9.11 ist hier also das bestmögliche Ergebnis.

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

9.13. **Definition.** Seien R ein Integritätsbereich und $A \subset R$ eine Teilmenge. $g \in R$ 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.

DEF ggT, kgV von Teilmengen

$k \in R$ 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 $g \sim \mathrm{ggT}(A)$, $k \sim \mathrm{kgV}(A)$, und falls $A = \{a_1, a_2, \ldots, a_n\}$ ist, auch $\mathrm{ggT}(a_1, a_2, \ldots, a_n)$ und $\mathrm{kgV}(a_1, a_2, \ldots, a_n)$. ♢

Es gilt dann

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

und analog für das kgV. Außerdem hat man $\mathrm{ggT}(\emptyset) \sim 0$ und $\mathrm{kgV}(\emptyset) \sim 1$ (Übung). Ist R faktoriell, dann existieren also ggT und kgV von beliebigen endlichen Teilmengen von R.

DEF Inhalt, primitives Polynom

9.14. **Definition.** Seien R ein faktorieller Ring und $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ 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 $\operatorname{pp}(0) = 1$. ♢

LEMMA primitiver Anteil

9.15. **Lemma.** *Seien 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 $\operatorname{cont}(f) \in R$.*

Beweis. Sei $f = a_0 + a_1x + \ldots + a_nx^n$ mit $a_j = b_j/c_j$ und $b_j, c_j \in R$, $c_j \neq 0$. Es gibt einen gemeinsamen Nenner $c \in R$ (z.B. $c = c_0c_1 \cdots c_n$), 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 $\alpha g = \alpha' g'$ mit $\alpha, \alpha' \in K^\times$ und primitiven Polynomen $g, g' \in R[x]$, dann können wir (nach Multiplikation mit einem gemeinsamen Nenner) annehmen, dass $\alpha, \alpha' \in R$. Es folgt $\alpha \sim \operatorname{cont}(\alpha g) \sim \operatorname{cont}(\alpha' g') \sim \alpha'$, also $\alpha/\alpha' \in R^\times$ (und analog für g und g'). Daraus folgt die Eindeutigkeitsaussage, wenn wir für α (bzw. α') einen Inhalt von f und für g (bzw. g') den zugehörigen primitiven Anteil nehmen.

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 $f \in R[x]$. ❑

* **LEMMA** Lemma von Gauß

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

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

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

Beweis. Nach Definition 9.14 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

$$(a_0b_{m+n} + a_1b_{m+n-1} + \ldots + a_{m-1}b_{n+1}) + a_mb_n + (a_{m+1}b_{n-1} + \ldots + a_{m+n-1}b_1 + a_{m+n}b_0)\,.$$

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_mb_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 Lemmas, die es uns erlauben, die Behauptung darauf zurückzuführen, dass sowohl R als auch $K[x]$ faktoriell sind. Das wollen wir zuerst noch präzisieren.

LEMMA Teilbarkeit in $R[x]$

9.17. **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*

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

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

Sei $g = fh$ in $R[x]$. Aus dem Lemma von Gauß 9.16 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.

FOLG Primelemente in $R[x]$

9.18. **Folgerung.** *Sei R ein faktorieller Ring mit Quotientenkörper K und sei $f \in R[x]$. f ist genau dann ein Primelement von $R[x]$, wenn entweder $f \in R$ ein Primelement ist oder f nicht konstant, primitiv und in $K[x]$ prim ist.*

Da R und $K[x]$ beide faktoriell sind, bedeutet „prim“ und „irreduzibel“ in beiden Ringen jeweils dasselbe.

Beweis. Sei zunächst $f \in R \subset R[x]$. Wir haben schon gesehen, dass $R[x]^\times = R^\times$ ist. Die Bedingung „$f \neq 0$ und keine Einheit“ ist daher in R und $R[x]$ dieselbe. Ist f prim in $R[x]$, dann auch in R, da die Bedingung für Letzteres schwächer ist. Umgekehrt folgt aus $f \mid_{R[x]} gh$ nach Lemma 9.17 auch $f \sim \operatorname{cont}(f) \mid_R \operatorname{cont}(gh) \sim \operatorname{cont}(g)\operatorname{cont}(h)$; wenn f in R prim ist, dann gilt also $f \mid_{R[x]} \operatorname{cont}(g) \mid_{R[x]} g$ oder $f \mid_{R[x]} \operatorname{cont}(h) \mid_{R[x]} h$, und f ist auch in $R[x]$ prim.

Sei jetzt f nicht konstant. Dann ist $f \neq 0$ und keine Einheit (auch keine Einheit in $K[x]$). Ist f prim in $R[x]$, dann folgt aus $f \sim \operatorname{cont}(f)\operatorname{pp}(f)$, dass $f \mid_{R[x]} \operatorname{pp}(f)$ gelten muss (denn $f \nmid_{R[x]} \operatorname{cont}(f)$, wenn f nicht konstant ist); das bedeutet aber, dass schon $f \sim \operatorname{pp}(f)$ gilt, also ist f primitiv. Gilt dann $f \mid_{K[x]} gh$ mit $g, h \in K[x]$, dann folgt wieder mit Lemma 9.17 $f \sim \operatorname{pp}(f) \mid_{K[x]} \operatorname{pp}(g)\operatorname{pp}(h)$; diese Teilbarkeit gilt auch in $R[x]$, und aus f prim folgt dann $f \mid_{R[x]} \operatorname{pp}(g) \mid_{R[x]} g$ oder $f \mid_{R[x]} \operatorname{pp}(h) \mid_{R[x]} h$; diese Teilbarkeit gilt dann auch in $K[x]$, und damit ist f auch prim in $K[x]$.

Ist umgekehrt f primitiv und prim in $K[x]$, dann folgt aus $f \mid_{R[x]} gh$ auch $f \mid_{K[x]} gh$, also $f \mid_{K[x]} g$ oder $f \mid_{K[x]} h$. Zusammen mit der trivialen Relation $1 \sim \operatorname{cont}(f) \mid_R \operatorname{cont}(g), \operatorname{cont}(h)$ folgt mit Lemma 9.17 dann $f \mid_{R[x]} g$ oder $f \mid_{R[x]} h$ gelten muss. Damit ist f prim in $R[x]$. ❑

Jetzt können wir den Satz beweisen.

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

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

Beweis. Sei $\mathbb{P}_R$ ein Repräsentantensystem der Primelemente von R bis auf Assoziierte und sei $\mathbb{P}_{K[x]}$ ein Repräsentantensystem der Primelemente von $K[x]$ bis auf Assoziierte, das aus primitiven Polynomen in $R[x]$ besteht. Nach Lemma 9.18 ist dann $\mathbb{P}_{R[x]} = \mathbb{P}_R \cup \mathbb{P}_{K[x]}$ ein Repräsentantensystem der Primelemente von $R[x]$ bis auf Assoziierte.

Sei $0 \neq f \in R[x]$. Da $K[x]$ faktoriell ist, gibt es eindeutig bestimmte $e_p \in \mathbb{Z}_{\geq 0}$ für $p \in \mathbb{P}_{K[x]}$ mit $e_p = 0$ für alle bis auf endlich viele p und $c \in K[x]^\times = K^\times$ mit

$$f = c \prod_{p \in \mathbb{P}_{K[x]}} p^{e_p} .$$

Da alle $p \in \mathbb{P}_{K[x]}$ primitiv sind, ist das Produkt auf der rechten Seite auch primitiv (Lemma 9.16 von Gauß), und es folgt $\operatorname{cont}(f) \sim c \in R$. Da R faktoriell ist, gibt es eindeutig bestimmte $e_p \in \mathbb{Z}_{\geq 0}$ für $p \in \mathbb{P}_R$ mit $e_p = 0$ für alle bis auf endlich viele p und $u \in R^\times = R[x]^\times$ mit

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

Insgesamt bekommen wir die gewünschte eindeutige Darstellung

$$f = u \prod_{p \in \mathbb{P}_{R[x]}} p^{e_p} .$$

❑

9.20. **Folgerung.** *Sei R ein faktorieller Ring. Ein Polynom $f \in R[x]$ ist genau dann irreduzibel, wenn entweder f konstant und irreduzibel in R oder f nicht konstant, primitiv und irreduzibel in $K[x]$ ist.*

FOLG
irreduzibel
in $R[x]$

Beweis. Das folgt aus Lemma 9.18 und Satz 9.19, da in jedem faktoriellen Ring die Primelemente und die irreduziblen Elemente übereinstimmen. ❑

9.21. **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 9.19 und der rekursiven Definition $R[x_1, \ldots, x_n, x_{n+1}] = \big(R[x_1, \ldots, x_n]\big)[x_{n+1}]$. ❑

10. 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 $R[x]$

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

Beweis. Das folgt aus Folgerung 9.20: In $K[x]$ sind alle Konstanten $\neq 0$ Einheiten, also ist f in $K[x]$ irreduzibel genau dann, wenn $\mathrm{pp}(f)$ in $K[x]$ irreduzibel ist. Das wiederum ist dazu äquivalent, dass $\mathrm{pp}(f)$ in $R[x]$ irreduzibel ist. (Beachte, dass die Äquivalenz auch für f konstant gilt: In diesem Fall ist f eine Einheit in $K[x]$ und $\mathrm{pp}(f) = 1$ eine Einheit in $R[x]$; beide sind daher nicht irreduzibel.) ❑

Für Polynome von niedrigem Grad haben wir folgendes Kriterium.

LEMMA Grad ≤ 3

10.2. **Lemma.** *Sei (nur für dieses Lemma) K ein beliebiger Körper und sei $f \in K[x]$ nicht konstant. f ist 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 genau dann reduzibel, 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 $\deg(g) \leq \deg(h)$ ist; dann folgt $\deg(g) \leq \deg(f)/2$. Der Leitkoeffizient von g ist eine Einheit; mit g ist also auch das normierte Polynom $\mathrm{lcf}(g)^{-1}g$ 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 9.9). ❑

BSP irreduzibles Polynom

10.3. **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, aber in $\mathbb{R}[x]$ reduzibel sind, 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 $\mathbb{R}$, $\mathbb{C}$

10.4. **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

10.5. **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 $\operatorname{pp}(x-\alpha) \sim sx - r$. 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

10.6. **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

10.7. **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

10.8. **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 6.18). Der Einsetzungshomomorphismus, der zum kanonischen Epimorphismus $R \to R/Rp$ und $x \mapsto x$ gehört (vergleiche Satz 9.2 und Definition 9.3), liefert einen kanonischen Homomorphismus $R[x] \to (R/Rp)[x]$. Um ihn anzuwenden, muss man die Koeffizienten „modulo p reduzieren“.

* 10.9. **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. ❑

10.10. **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 10.2 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

10.11. **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 10.8 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 10.8. ♣

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.

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 am Ende der „Einführung in die Algebra“ diskutieren 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

10.12. **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 $\deg(g) + \deg(h) = n$ (vergleiche Lemma 9.5), 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 9.16 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. ❑

* 10.13. **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

G. Eisenstein
1823–1852

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 10.12 (beachte, dass R/Rp ein Integritätsbereich ist, denn Rp ist ein Primideal, vergleiche Satz 6.18) $\bar{g} = u'x^m$, $\bar{h} = u''x^{n-m}$ 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. ❑

Ein häufiger Fehler bei der Anwendung des Kriteriums ist, dass die Bedingung $p \mid a_0$ vergessen wird und nur $p^2 \nmid a_0$ geprüft wird. (Und natürlich muss p prim sein...)

10.14. **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 $f_m \mid f_n$.

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

10.15. **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. ♣

Zum Abschluss werden wir noch ein Kriterium herleiten, das es uns erlaubt zu entscheiden, ob ein Polynom über einem Körper *quadratfrei* ist, also keine irreduziblen Faktoren mehrfach enthält. Dazu definieren wir die Ableitung eines Polynoms. Wir können natürlich keine Grenzwerte verwenden; deswegen nehmen wir einfach die üblichen Formeln.

DEF Ableitung

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

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

LEMMA Ableitungsregeln

10.17. **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.*

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

10.18. **Satz.** *Sei K ein Körper der Charakteristik 0. $f \in K[x]$ ist genau dann quadratfrei, 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

10.19. **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 Satz 10.18 für beliebige Körper, wenn man „quadratfrei“ durch „quadratfrei über jedem Erweiterungskörper“ ersetzt.

Wir definieren die Vielfachheit einer Nullstelle in der offensichtlichen Weise, so wie wir das schon in der Linearen Algebra für die algebraische Vielfachheit eines Eigenwerts getan haben:

DEF Vielfachheit einer Nullstelle

10.20. **Definition.** Seien K ein Körper, $0 \neq f \in K[x]$ und $a \in K$. Die *Vielfachheit* von a als Nullstelle von f ist der Exponent von $x - a$ in der Primfaktorzerlegung von f (im faktoriellen Ring $K[x]$). ♢

Wenn n die Vielfachheit ist, dann kann man also $f = (x - a)^n g$ schreiben mit $g \in K[x]$ und $g(a) \neq 0$.

Hat K Charakteristik 0, dann kann man die Vielfachheit einer Nullstelle mithilfe der höheren Ableitungen bestimmen.

LEMMA Vielfachheit durch Ableitungen

10.21. **Lemma.** *Sei K ein Körper der Charakteristik 0 und seien $0 \neq f \in K[x]$ und $a \in K$. Die Vielfachheit von a als Nullstelle von f ist das (eindeutig bestimmte) $n \in \mathbb{Z}_{\geq 0}$, sodass $f^{(k)}(a) = 0$ ist für alle $0 \leq k < n$, aber $f^{(n)}(a) \neq 0$.*

Dabei ist $f^{(k)}$ die k-te Ableitung von f, also $f^{(0)} = f$ und $f^{(k+1)} = (f^{(k)})'$.

Beweis. Übung. ❑

11. 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. Leider haben wir nicht genug Zeit dafür, dieses Ergebnis vollständig zu beweisen (obwohl das mit den Mitteln der Vorlesung durchaus möglich wäre; siehe den klein gedruckten Text in diesem Abschnitt). Auf der anderen Seite ist das Quadratische Reziprozitätsgesetz ein Highlight der Zahlentheorie, das ich Ihnen nicht vorenthalten will.

Wir brauchen dafür ein wichtiges Ergebnis über endliche Körper.

* 11.1. **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 $a^q = a$.*

P. de Fermat
1607–1665

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 11.1 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.

* 11.2. **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:

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

A.-M. Legendre
1752–1833

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

11.3. **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 $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. (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

11.4. **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

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

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 11.4 kurz und prägnant so ausdrücken:

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

SATZ
Euler-
Kriterium

* 11.5. **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.


L. Euler
1707–1783

Beweis. Für $p \mid a$ ist das klar. Wir können also $p \nmid a$ annehmen. Nach dem kleinen Satz von Fermat 11.1 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 11.4 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 in verschiedenen Restklassen modulo p liegen, wenn $p > 2$ ist. ❑

11.6. **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 11.5:

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

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:

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

11.7. **Beispiel.** Für jede Primzahl $p \geq 5$ gilt, 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. ♣

BSP 2, 3 oder 6 ist QR

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 $a^2 \equiv -1 \bmod p$ 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 $b^2 \equiv 6 \bmod p$ 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 $c^2 \equiv -6 \bmod p$, 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 10.11 bewiesen, dass man die Irreduzibilität von $x^4 + 9$ nicht mit dem Reduktionskriterium zeigen kann.

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

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

FOLG Erstes Ergänzungsgesetz zum QRG

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

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 genau dann quadratischer Rest mod p, wenn $p \equiv 1 \bmod 4$ ist. Diese Aussage haben wir bereits als Lemma 5.6 formuliert; sie war wichtig für unseren Beweis des Zwei-Quadrate-Satzes für Primzahlen (Folgerung 5.8), der damit nun also vollständig bewiesen ist.

Die Aussage von Folgerung 11.8 wird auch als *Erstes Ergänzungsgesetz zum Quadratischen Reziprozitätsgesetz* bezeichnet. Der Grund dafür wird später klar werden.

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

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

Die sich hier aufdrängende Vermutung stimmt tatsächlich:

* 11.9. **Satz.** *Ist p eine ungerade Primzahl, dann gilt*

SATZ Zweites Ergänzungsgesetz zum QRG

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

Die Aussage von Satz 11.9 heißt auch das *Zweite Ergänzungsgesetz zum Quadratischen Reziprozitätsgesetz.*

Für den Beweis dieses Ergänzungsgesetzes wie auch des eigentlichen Quadratischen Reziprozitätsgesetzes haben wir leider in der Vorlesung keine Zeit, da dafür noch Einiges an Arbeit nötig ist. Im Kleingedruckten hier und später finden Sie aber die relevanten Ergebnisse.

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

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

LEMMA Elemente von $R[a]$

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

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

Beweis. Nach dem vorigen Lemma haben alle Elemente von $R[a]$ die Form $h(a)$ mit einem Polynom $h \in R[x]$. Nach Satz 9.8 (Division mit Rest für Polynome; hier benutzen wir, dass f normiert ist) 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

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

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. ❑

Lemma. *Sei R ein kommutativer Ring und sei p eine Primzahl. Dann gilt in R:*

$$(r_1 + r_2 + \ldots + r_n)^p \equiv r_1^p + r_2^p + \ldots + r_n^p \bmod Rp\,.$$

LEMMA „Freshman's Dream“

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 das 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.

Beweis von Satz 11.9. 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 dem „Freshman's Dream“ 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 11.5)

$$(\tau + \tau^{-1})^p = \big((\tau + \tau^{-1})^2\big)^{(p-1)/2}(\tau + \tau^{-1}) = 2^{(p-1)/2}(\tau + \tau^{-1}) \equiv \left(\frac{2}{p}\right)(\tau + \tau^{-1})\,.$$

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 dem Lemma über $R[a]$ oben (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. ❑

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.

* 11.10. **Satz.** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt*

SATZ Quadratisches Reziprozitäts-gesetz

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

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 $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Wir überlegen 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.

11.11. **Beispiel.** Mithilfe des QRG und seiner Ergänzungsgesetze kann man nun Legendre-Symbole, die größere Zahlen enthalten, recht bequem auswerten. Zum Beispiel:

BSP Anwendung QRG

$$\begin{aligned}\left(\frac{67}{109}\right) &= \left(\frac{109}{67}\right) = \left(\frac{42}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{3}{67}\right)\left(\frac{7}{67}\right) \\ &= (-1)(-\left(\frac{67}{3}\right))(-\left(\frac{67}{7}\right)) = -\left(\frac{1}{3}\right)\left(\frac{4}{7}\right) = -1\,.\end{aligned}$$

Oder alternativ:

$$\left(\frac{67}{109}\right) = \left(\frac{109}{67}\right) = \left(\frac{-25}{67}\right) = \left(\frac{-1}{67}\right)\left(\frac{5}{67}\right)^2 = -1\,. \qquad \clubsuit$$

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 2 durch p^* und p durch q ersetzen. Wir brauchen dann ein $\gamma \in R$ mit

- $\gamma^2 = p^*$ und
- $\gamma^q \equiv \left(\frac{q}{p}\right)\gamma \bmod Rq$.

Dabei setzen wir für eine ungerade Primzahl 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 $p^* \equiv 1 \bmod 4$. Das QRG kann man dann auch in der Form

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

formulieren. Gauß (der das QRG als Erster vollständig bewies, nachdem Legendre es vermutet und in Spezialfällen bewiesen hatte, und der in seinem Leben sieben oder acht verschiedene Beweise dafür fand) hat diese Elemente γ gefunden, deswegen werden sie heute nach ihm benannt.

C.F. Gauß
1777–1855

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. ♢

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 11.4. 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 10.14). Nach dem Lemma über $R[a]$ 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 11.10. 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 11.9. ❑

Aus $g^2 = p^*$ folgt $g = \pm\sqrt{p}$, falls $p \equiv 1 \bmod 4$, und $g = \pm i\sqrt{p}$, 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).

12. Gruppen und Untergruppen

Wir erinnern uns daran, was eine Gruppe ist; vergleiche Definition 1.3.

∗ 12.1. **Definition.** Eine *Gruppe* ist ein Quadrupel $(G, *, e, i)$, bestehend aus einer Menge G, einer Abbildung $*\colon G \times G \to G$, einem Element $e \in G$ und einer Abbildung $i\colon G \to G$ mit den folgenden Eigenschaften:

(1) (Assoziativität) $\forall a, b, c \in G\colon (a * b) * c = a * (b * c)$.

(2) (Neutrales Element) $\forall a \in G\colon a * e = a = e * a$.

(3) (Inverses Element) $\forall a \in G\colon a * i(a) = e = i(a) * a$.

Die Gruppe heißt *kommutativ* oder *abelsch*, wenn zusätzlich gilt

(4) (Kommutativität) $\forall a, b \in G\colon a * b = b * a$.

Ist die Menge G endlich, dann heißt die Gruppe *endlich*, und ihre Kardinalität $\#G$ heißt die *Ordnung* der Gruppe. ♢

DEF Gruppe

DEF abelsche Gruppe

DEF endliche Gruppe

DEF Ordnung

Da, wie wir uns früher schon überlegt haben, sowohl das neutrale Element (wenn es existiert) als auch das zu a inverse Element (wenn es existiert) eindeutig bestimmt sind, lässt man diese Daten häufig weg und spricht deshalb einfach von „der Gruppe $(G, *)$“ oder auch von „der Gruppe G“, wenn die Verknüpfung aus dem Kontext klar ist. Für das Inverse $i(a)$ schreibt man meist a^{-1}.

Gruppen schreibt man gerne „multiplikativ“, dann ist die Verknüpfung $a \cdot b$ oder kurz ab und das neutrale Element heißt 1 (oder 1_G).

Abelsche (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 $a + (-b)$.

12.2. **Beispiel.** Das einfachste Beispiel einer Gruppe ist $G = \{e\}$ (mit $e * e = e$ und $i(e) = e$). Eine Gruppe, die nur aus dem neutralen Element besteht, heißt auch *triviale Gruppe*. ♣

BSP triviale Gruppe

DEF triviale Gruppe

12.3. **Beispiel.** Ein wichtiges und grundlegendes Beispiel einer Gruppe ist die Gruppe $S(X)$ der Permutationen einer Menge X. Die unterliegende Menge besteht hier aus allen bijektiven Abbildungen $X \to X$, die Verknüpfung ist die Verknüpfung von Abbildungen, das neutrale Element ist die identische Abbildung id_X und das Inverse $i(f)$ ist die Umkehrabbildung f^{-1}. Die in Definition 12.1 geforderten Eigenschaften sind elementare Eigenschaften von Mengen und Abbildungen.

BSP Permutationsgruppe

Für $\#X \leq 1$ ist die Gruppe $S(X) = \{\mathrm{id}_X\}$ trivial. Für $\#X \geq 3$ ist $S(X)$ nicht abelsch.

Für $S\big(\{1, 2, \ldots, n\}\big)$ schreibt man auch S_n (in der Literatur auch häufig in Fraktur: $\mathfrak{S}_n$) und nennt S_n die *symmetrische Gruppe* auf n Elementen. Ihre Ordnung ist $\#S_n = n!$. ♣

DEF symmetrische Gruppe

Diese Gruppe S_n ist uns bereits in der Linearen Algebra im Zusammenhang mit der Determinante und der „Leibniz-Formel“

$$\det\big((a_{ij})_{1\leq i,j\leq n}\big) = \sum_{\sigma\in S_n} \varepsilon(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

begegnet. Die Abbildung $\varepsilon\colon S_n \to \{\pm 1\}$ ist übrigens ein Beispiel für einen *Gruppenhomomorphismus*; diesen Begriff werden wir bald einführen.

Gruppen treten innerhalb der Mathematik natürlicherweise als „Symmetriegruppen“ (in einem weiten Sinn) auf: Mathematische Objekte haben „Symmetrien“ (häufig sind das invertierbare strukturerhaltende Abbildungen des Objekts in sich), die hintereinander ausgeführt werden können und dann eine neue Symmetrieoperation ergeben; außerdem kann man sie rückgängig machen, und es gibt die Operation, die gar nichts tut (üblicherweise die identische Abbildung). Die Symmetrien bilden also eine Gruppe. Zum Beispiel ist S_n die Symmetriegruppe der Menge $\{1, 2, \dots, n\}$ ohne weitere Struktur.

In der Algebra heißen die Symmetrien „Automorphismen“; sie bilden die *Automorphismengruppe* der Struktur. Für einen K-Vektorraum V ist das zum Beispiel die Gruppe der invertierbaren K-linearen Abbildungen $V \to V$. Für diese Gruppe schreibt man üblicherweise $\mathrm{GL}(V)$; im Fall $V = K^n$ auch $\mathrm{GL}(n, K)$ (oder $\mathrm{GL}_n(K)$). Das ist gerade die Gruppe der invertierbaren $n \times n$-Matrizen über K (siehe die Vorlesungen zur Linearen Algebra).

DEF Automorphismengruppe

12.4. **Beispiele.** Weitere Beispiele von Symmetriegruppen oder Automorphismengruppen sind: **BSP** Gruppen

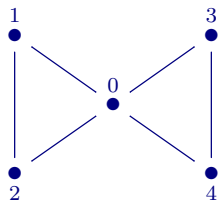
(1) Die Symmetriegruppe eines geometrischen Objekts, also die Menge der (eventuell auch nur der orientierungserhaltenden) Bewegungen, die das Objekt in sich überführen. Die Symmetriegruppe des Einheitskreises in der Ebene ist zum Beispiel die orthogonale Gruppe $\mathrm{O}(2)$, während sich für reguläre Polygone endliche Gruppen ergeben, die sogenannten *Diedergruppen*, die wir später noch genauer betrachten werden.

(2) Die Isometriegruppe eines metrischen Raums X, also die Menge der bijektiven Abbildungen $f\colon X \to X$, die die Metrik erhalten:

$$\forall x, y \in X\colon d\big(f(x), f(y)\big) = d(x, y)\,.$$

(3) Ein (einfacher, schlingenloser, ungerichteter) *Graph* $\Gamma = (V, E)$ ist gegeben durch eine Menge V von „Ecken“ (engl. *vertex/vertices*) und eine Menge E von zweielementigen Teilmengen von V, den „Kanten“ (engl. *edges*); die Idee dabei ist, dass jede Kante zwei Ecken verbindet. Ein Automorphismus von Γ ist eine Permutation von V, die Kanten auf Kanten abbildet. Die Automorphismen von Γ bilden eine Gruppe. Zum Beispiel ist $\#\operatorname{Aut}(\Gamma) = 8$ für den folgenden Graphen

$$\Gamma = \big(\{0,1,2,3,4\}, \{\{0,1\},\{0,2\},\{0,3\},\{0,4\},\{1,2\},\{3,4\}\}\big)\ :$$



♣

Wie wir das für andere algebraische Strukturen auch getan haben, betrachten wir in Gruppen Unterstrukturen.

∗ 12.5. **Definition.** Sei $(G, *, e, i)$ eine Gruppe und $H \subset G$ eine Teilmenge. Dann ist H eine *Untergruppe* von G, wenn H die folgenden Bedingungen erfüllt: **DEF** Untergruppe

(1) $e \in H$.

(2) $\forall a, b \in H\colon a * b \in H$.

(3) $\forall a \in H\colon i(a) \in H$.

H muss also das neutrale Element enthalten und unter der Verknüpfung und Inversenbildung abgeschlossen sein. Man schreibt häufig $H \leq G$ für „H ist Untergruppe von G“. ♢

Natürlich ist die Definition gerade so gemacht, dass $(H, *|_{H\times H}, e, i|_H)$ (also mit den von G auf H eingeschränkten Abbildungen) wieder eine Gruppe ist. Das folgt daraus, dass alle Axiome in Definition 12.1 die Form „für alle . . . “ haben — wenn sie für alle Elemente von G gelten, dann auch für alle Elemente von H, solange die vorkommenden Ausdrücke Sinn haben. Das ist aber durch die Abgeschlossenheit von H sichergestellt.

Wie üblich haben Untergruppen die folgende Durchschnittseigenschaft.

12.6. **Lemma.** *Seien G eine Gruppe und $(H_i)_{i\in I}$ eine Familie von Untergruppen von G mit nichtleerer Indexmenge I. Dann ist auch $\bigcap_{i\in I} H_i$ wieder eine Untergruppe von G.* **LEMMA** Durchschnitt von Untergruppen

Beweis. Analog wie für Untervektorräume, Unterringe, Ideale, . . .

Der Vollständigkeit halber sei der Beweis hier ausgeführt. Wir müssen die drei Bedingungen aus Definition 12.5 nachweisen. Sei $H = \bigcap_{i\in I} H_i$; die Gruppe sei $(G, *, e, i)$.

(1) Da $e \in H_i$ ist für alle $i \in I$, ist auch $e \in H$.
(2) Seien $a, b \in H$. Dann gilt $a, b \in H_i$ für alle $i \in I$. Da die H_i Untergruppen sind, folgt $a * b \in H_i$ für alle $i \in I$ und damit auch $a * b \in H$.
(3) Sei $a \in H$. Dann ist $a \in H_i$ für alle $i \in I$. Da die H_i Untergruppen sind, folgt $i(a) \in H_i$ für alle $i \in I$ und damit auch $i(a) \in H$. ❑

Die Durchschnittseigenschaft aus Lemma 12.6 ermöglicht folgende Definitionen, die wir in analoger Weise schon aus anderen Zusammenhängen kennen.

12.7. **Definition.** Seien G eine Gruppe und sei $T \subset G$ eine Teilmenge. Dann gibt es die kleinste Untergruppe von G, die T enthält; wir bezeichnen sie mit **DEF** Erzeugendensystem

$$\langle T\rangle = \langle T\rangle_G = \bigcap\{H \leq G \mid T \subset H\}$$

und nennen sie die *von T erzeugte Untergruppe* von G. Ist $T = \{t_1, t_2, \ldots, t_n\}$ endlich, dann schreiben wir statt $\langle T\rangle$ auch $\langle t_1, t_2, \ldots, t_n\rangle$. endlich erzeugt

Ist $\langle T\rangle = G$, dann heißt T ein *Erzeugendensystem* von G. Ist dabei T endlich, dann heißt G *endlich erzeugt*. Gilt $T = \{g\}$, also $G = \langle g\rangle$, dann heißt G *zyklisch*. zyklische Gruppe

Für $g \in G$ heißt $\operatorname{ord}(g) = \#\langle g\rangle \in \mathbb{Z}_{>0} \cup \{\infty\}$ die *Ordnung* von g. ♢ Ordnung eines Elements

Beachten Sie, dass es in der Gruppentheorie *zwei* Begriffe von „Ordnung“ gibt: Die Ordnung einer (endlichen) Gruppe und die Ordnung eines Elements. Auch wenn es zwischen den beiden einen Zusammenhang gibt (darauf kommen wir bald noch zu sprechen), muss man die beiden Begriffe sorgfältig auseinanderhalten.

12.8. **Beispiel.** Was ist $\langle\ \rangle_G = \langle\emptyset\rangle_G$? In diesem Fall ist die Bedingung $\emptyset \subset H$ stets erfüllt; man bekommt also die kleinste Untergruppe von G, das ist $\{e\}$. ♣

BSP $\langle\ \rangle$

12.9. **Definition.** In einer multiplikativ geschriebenen Gruppe G definieren wir die *Potenz* g^n für $g \in G$ und $n \in \mathbb{Z}$ wie üblich durch

$$g^0 = 1_G\,, \qquad g^{n+1} = g \cdot g^n \quad \text{für } n \geq 0\,, \qquad g^{-n} = (g^{-1})^n \quad \text{für } n > 0.$$

Man beweist dann leicht die „Potenzrechengesetze“

$$g^{m+n} = g^m \cdot g^n \qquad \text{und} \qquad (g^m)^n = g^{mn}$$

durch Induktion und Fallunterscheidung nach den Vorzeichen von m und n. Beachte: In nicht-abelschen Gruppen gilt im Allgemeinen *nicht*, dass $(gh)^n = g^n h^n$ ist!

In additiv geschriebenen (abelschen) Gruppen entspricht der Potenz das (ganzzahlige) *Vielfache* $n \cdot g$ mit den Regeln

$$(m+n)\cdot g = m\cdot g + n\cdot g\,, \quad (mn)\cdot g = m\cdot(n\cdot g) \quad \text{und} \quad n\cdot(g+h) = n\cdot g + n\cdot h\,. \ \diamondsuit$$

DEF Potenzen/ Vielfache

12.10. **Lemma.** *Seien G eine multiplikativ geschriebene Gruppe und $g \in G$. Dann ist*

$$\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}\,.$$

Insbesondere sind zyklische Gruppen abelsch.

Ist $\mathbb{Z} \to G$, $n \mapsto g^n$, injektiv, dann ist $\operatorname{ord}(g) = \infty$. Anderenfalls ist

$$\operatorname{ord}(g) = \min\{n \in \mathbb{Z}_{>0} \mid g^n = 1_G\} < \infty\,.$$

LEMMA zyklische Gruppen

Charakterisierung von $\operatorname{ord}(g)$

Beweis. Die Menge $U = \{g^n \mid n \in \mathbb{Z}\}$ enthält offensichtlich $g = g^1$, und jede g enthaltende Untergruppe von G muss U enthalten. Aus den Potenzrechengesetzen folgt, dass U bereits eine Untergruppe von G ist. Damit muss U die kleinste Untergruppe sein, die g enthält, also ist $\langle g\rangle = U$. Wegen $g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m$ ist U abelsch.

Wir betrachten jetzt $f\colon \mathbb{Z} \to G$, $n \mapsto g^n$ mit $\langle g\rangle = \operatorname{im}(f)$. Ist f injektiv, dann ist $\operatorname{ord}(g) = \#\langle g\rangle = \infty$. Anderenfalls gibt es $m < n$ in $\mathbb{Z}$ mit $f(m) = g^m = g^n = f(n)$; es folgt $g^{n-m} = 1_G$, also ist die Menge $\{n \in \mathbb{Z}_{>0} \mid g^n = 1_G\}$ nicht leer. Sei N ihr Minimum. Dann gilt für $n = qN + r$ mit $0 \leq r < N$, dass

$$g^n = g^{qN+r} = (g^N)^q \cdot g^r = 1_G^q \cdot g^r = g^r$$

ist; es folgt $\#\operatorname{im}(f) \leq N$. Auf der anderen Seite müssen alle g^r mit $0 \leq r < N$ verschieden sein, sonst würde man wie oben aus $0 \leq r < r' < N$ mit $g^r = g^{r'}$ den Widerspruch $g^{r'-r} = 1_G$ bekommen. Also gilt auch $\#\operatorname{im}(f) \geq N$ und damit insgesamt $\operatorname{ord}(g) = N$. ❑

Allgemeiner kann man sich überlegen, dass $\langle T\rangle$ genau aus allen endlichen Produkten beliebiger Länge von Elementen von T und deren Inversen besteht. Im Allgemeinen kommt es dabei auf die Reihenfolge der Faktoren an, da etwa xyz, xzy, yxz usw. alle verschieden sein können. In abelschen Gruppen lässt sich das vereinfachen.

Man beachte die folgenden Rechenregeln, die in allen Gruppen gelten:

$$(xy)^{-1} = y^{-1}x^{-1} \qquad \text{und} \qquad (x^{-1})^{-1} = x\,.$$

Daraus folgt, dass die Menge der Produkte wie oben nicht nur unter der Verknüpfung (das sollte klar sein), sondern auch unter der Inversenbildung abgeschlossen ist. Das neutrale Element ist als leeres Produkt ebenfalls enthalten. Damit ist die Menge P der Produkte tatsächlich eine Untergruppe, und da jede T enthaltende Untergruppe offensichtlich P enthalten muss, folgt $\langle T\rangle = P$.

Wir bringen noch einige Beispiele für Ordnungen von Gruppen und ihren Elementen.

12.11. **Beispiele.** **BSP** Ordnung **DEF** Diedergruppe

(1) Die Ordnung der *Diedergruppe* D_n, also der Gruppe der Bewegungen der Ebene, die ein reguläres n-Eck invariant lassen, ist $2n$, denn ihre Elemente sind n Drehungen (um Vielfache von $2\pi/n$ um den Mittelpunkt des n-Ecks) und n Spiegelungen (an Geraden durch den Mittelpunkt des n-Ecks; falls n ungerade ist, gehen diese Geraden jeweils durch einen Eckpunkt und den gegenüberliegenden Kantenmittelpunkt, falls n gerade ist, gehen $n/2$ dieser Geraden durch zwei gegenüberliegende Ecken und die anderen $n/2$ Geraden durch zwei gegenüberliegende Kantenmittelpunkte). Diese Gruppe enthält (z.B.) Elemente der Ordnung n und der Ordnung 2.

(2) Ist G eine endliche Gruppe und ist $g \in G$ ein Element mit $\operatorname{ord}(g) = \#G$, dann ist $G = \langle g\rangle$ zyklisch.

(3) Ist F ein endlicher Körper mit $\#F = q$ und $n \geq 1$, dann gilt

$$\#\operatorname{GL}(n, F) = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})\,.$$

Dazu überlegt man sich, dass es für die erste Spalte einer invertierbaren Matrix $q^n - 1$ Möglichkeiten gibt (sie darf nicht null sein), für die zweite dann $q^n - q$ Möglichkeiten (sie darf nicht im von der ersten Spalte erzeugten Untervektorraum liegen), …, für die m-te Spalte $q^n - q^{m-1}$ Möglichkeiten (sie darf nicht im von den ersten $m-1$ Spalten (die nach Konstruktion linear unabhängig sind) erzeugten Untervektorraum liegen), …, für die n-te Spalte noch $q^n - q^{n-1}$ Möglichkeiten. ♣

12.12. **Definition.** Sei G eine Gruppe und seien $A, B \subset G$ zwei Teilmengen. Wir schreiben **DEF** Produkt von Teilmengen

$$AB = \{ab \mid a \in A, b \in B\}$$

für das elementweise Produkt der Mengen A und B. Im Fall $A = \{a\}$ schreiben wir auch aB, im Fall $B = \{b\}$ entsprechend Ab. ♢

12.13. **Beispiel.** Sind U_1 und U_2 Untergruppen von G, dann muss U_1U_2 nicht unbedingt ebenfalls eine Untergruppe sein. Zum Beispiel können wir in $G = S_3$ die Untergruppen $U_1 = \langle\tau_1\rangle$ und $U_2 = \langle\tau_2\rangle$ betrachten, wobei τ_1 die Elemente 1 und 2 und τ_2 die Elemente 2 und 3 der Menge $\{1, 2, 3\}$ vertauscht. Dann ist **BSP** U_1U_2 keine Untergruppe

$$U_1U_2 = \{\mathrm{id}, \tau_1, \tau_2, \tau_1 \circ \tau_2\}\,;$$

diese Menge ist weder unter der Verknüpfung noch unter der Inversenbildung abgeschlossen, da $\tau_2 \circ \tau_1 = (\tau_1 \circ \tau_2)^{-1}$ nicht in ihr enthalten ist. ($\tau_1 \circ \tau_2$ hat den Effekt $1 \mapsto 2 \mapsto 3 \mapsto 1$, während $\tau_2 \circ \tau_1$ den Effekt $1 \mapsto 3 \mapsto 2 \mapsto 1$ hat.)

Wir werden bald eine Bedingung kennenlernen, die garantiert, dass U_1U_2 tatsächlich eine Untergruppe ist. ♣

Eine Untergruppe einer Gruppe G führt zu einer Aufteilung von G in Teilmengen.

∗ 12.14. **Definition.** Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Für $g \in G$ heißt gU die *Linksnebenklasse von g bezüglich U* und Ug die *Rechtsnebenklasse von g bezüglich U*. Wir schreiben $G/U = \{gU \mid g \in G\}$ („G modulo U“) für die Menge der Linksnebenklassen bezüglich U in G und $U\backslash G = \{Ug \mid g \in G\}$ für die Menge der Rechtsnebenklassen bezüglich U in G. ♢

DEF Nebenklasse

12.15. **Lemma.** *Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Für Elemente $g, h \in G$ sind äquivalent:*

(1) $h^{-1}g \in U$,

(2) $g \in hU$,

(3) $gU \subset hU$,

(4) $gU = hU$,

(5) $gU \cap hU \neq \emptyset$.

Insbesondere definiert $g \sim h \iff gU = hU$ eine Äquivalenzrelation auf G; G/U ist die Menge der zugehörigen Äquivalenzklassen.

LEMMA Nebenklassen bilden Partition

Natürlich gelten die entsprechenden Aussagen auch für *Rechts*nebenklassen Ug.

Beweis. Wir zerlegen den Beweis in mehrere Schritte.

„(1) $\Rightarrow$ (2)“: $h^{-1}g \in U \Rightarrow \exists u \in U : h^{-1}g = u \Rightarrow \exists u \in U : g = hu \Rightarrow g \in hU$.

„(2) $\Rightarrow$ (3)“: $g \in hU$ bedeutet $g = hu$ für ein $u \in U$; es folgt für $u' \in U$ beliebig, dass $gu' = (hu)u' = h(uu') \in hU$ ist. Das bedeutet $gU \subset hU$.

„(3) $\Rightarrow$ (5)“ ist trivial, da $gU \neq \emptyset$.

„(5) $\Rightarrow$ (1)“: Aus (5) folgt $gu_1 = hu_2$ mit geeigneten $u_1, u_2 \in U$, also $h^{-1}g = u_2u_1^{-1} \in U$ und damit (1).

„(1) $\Rightarrow$ (4)“: Aus (1) folgt auch $g^{-1}h = (h^{-1}g)^{-1} \in U$ und damit nach dem schon Gezeigten $gU \subset hU$ und $hU \subset gU$, also $gU = hU$.

„(4) $\Rightarrow$ (3)“ ist trivial. ❑

12.16. **Lemma.** *Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Dann wird durch $x \mapsto x^{-1}$ eine Bijektion*

$$G/U \longrightarrow U\backslash G\,, \qquad gU \longmapsto Ug^{-1}$$

induziert. Insbesondere gilt $\#(G/U) = \#(U\backslash G)$.

LEMMA G/U und $U\backslash G$

Beweis. Die Abbildung $x \mapsto x^{-1}$ bildet $gU = \{gu \mid u \in U\}$ ab auf

$$\{(gu)^{-1} \mid u \in U\} = \{u^{-1}g^{-1} \mid u \in U\} = \{ug^{-1} \mid u \in U\} = Ug^{-1}\,.$$

Sie induziert also eine wohldefinierte Abbildung $G/U \longrightarrow U\backslash G$. Diese Abbildung ist bijektiv, weil sie die offensichtliche Inverse $Ug \mapsto g^{-1}U$ hat (die ebenfalls von $x \mapsto x^{-1}$ induziert wird). ❑

12.17. **Definition.** Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Dann heißt $\#(G/U) = \#(U\backslash G)$ der *Index* $(G : U)$ der Untergruppe U in G. ♢

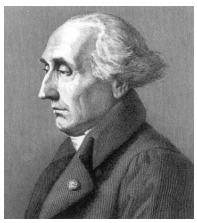
DEF Index

Der Index kann endlich sein, auch wenn G und U unendlich sind. Zum Beispiel hat $\mathbb{Z}$ die Untergruppe $n\mathbb{Z}$ (für jedes $n \in \mathbb{Z}_{>0}$) vom Index n.

12.18. **Lemma.** *Seien G eine Gruppe, $U \leq G$ und $g, h \in G$. Dann definiert $x \mapsto (hg^{-1})x$ eine Bijektion $gU \to hU$. Insbesondere gilt, dass alle (Links-)Nebenklassen bzgl. U dieselbe Anzahl von Elementen haben.*

LEMMA
$\#gU = \#hU$

Die analoge Aussage gilt natürlich auch für Rechtsnebenklassen. Da U selbst sowohl Links- als auch Rechtsnebenklasse bezüglich U ist (von 1_G), folgt $\#gU = \#U = \#Uh$ für alle $g, h \in G$.



J.-L. Lagrange
1736–1813

Beweis. Die Abbildung schickt $gu \in gU$ auf $hg^{-1} \cdot gu = hu \in hU$, ist also wohldefiniert als Abbildung $gU \to hU$. Es gibt eine analoge Abbildung $x \mapsto gh^{-1} \cdot x$ von hU nach gU; die Abbildungen sind offensichtlich invers zueinander. ❑

* 12.19. **Folgerung.** *Seien G eine endliche Gruppe und U eine Untergruppe von G. Dann gilt $\#G = (G : U) \cdot \#U$. Insbesondere ist $\#U$ ein Teiler von $\#G$.*

FOLG
Satz von Lagrange

Beweis. Es gilt $\#G = \sum_{gU \in G/U} \#gU$. Da nach Lemma 12.18 alle Nebenklassen gU dieselbe Kardinalität $\#gU = \#U$ haben, folgt die Behauptung. ❑

12.20. **Folgerung.** *Seien G eine endliche Gruppe und $g \in G$. Dann ist $\operatorname{ord}(g)$ ein Teiler der Gruppenordnung $\#G$. Insbesondere gilt $g^{\#G} = 1$.*

FOLG
$\operatorname{ord}(g) \mid \#G$

Beweis. Wir wenden Folgerung 12.19 auf $U = \langle g \rangle$ an. Es gilt dann $\#G = m \operatorname{ord}(g)$ mit $m = (G : \langle g \rangle) \in \mathbb{Z}$. Es folgt $g^{\#G} = (g^{\operatorname{ord}(g)})^m = 1^m = 1$. ❑

Wir können damit einen weiteren Beweis des Kleinen Satzes von Fermat (Satz 11.1) geben:

12.21. **Folgerung.** *Sei p eine Primzahl. Für alle ganzen Zahlen a mit $p \nmid a$ gilt*

$$a^{p-1} \equiv 1 \bmod p\,.$$

FOLG
Kleiner Satz von Fermat

Beweis. Wir wenden Folgerung 12.20 auf die multiplikative Gruppe $\mathbb{F}_p^\times$ an. ❑

Das lässt sich verallgemeinern: Anwendung auf die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ der Ordnung $\varphi(n)$ (Eulersche φ-Funktion) liefert:

12.22. **Folgerung.** *Seien $n \in \mathbb{Z}_{>0}$ und $a \in \mathbb{Z}$ mit $a \perp n$. Dann gilt*

$$a^{\varphi(n)} \equiv 1 \bmod n\,.$$

FOLG
Satz von Euler

Dieser Satz ist recht nützlich, wenn man Potenzen modulo n berechnen will. Wie findet man zum Beispiel die Restklasse von $7^{11^{13}}$ mod 15? Der Satz von Euler sagt uns, dass $7^{\varphi(15)} = 7^8 \equiv 1 \bmod 15$ ist; es kommt also nur auf den Exponenten 11^{13} mod 8 an. Der Satz sagt dann wieder, dass $11^4 \equiv 1 \bmod 8$ ist (tatsächlich gilt ja sogar $a^2 \equiv 1 \bmod 8$ für alle ungeraden ganzen Zahlen a; der Satz ist also nicht „scharf“ — im Gegensatz zum kleinen Satz von Fermat, wie wir im nächsten Semester sehen werden), also ist $11^{13} \equiv 11^1 \equiv 3 \bmod 8$ und damit

$$7^{11^{13}} \equiv 7^3 = 343 \equiv -2 \bmod 15\,.$$

Wir formulieren noch ein nützliches Kriterium dafür, wann eine Potenz eines Elements trivial ist.

12.23. **Lemma.** *Seien G eine Gruppe und $g \in G$ ein Element endlicher Ordnung. Für $n \in \mathbb{Z}$ gilt dann*

LEMMA
$g^n = 1$

$$g^n = 1_G \iff \operatorname{ord}(g) \mid n\,.$$

Beweis. Übung. ❑

Man kann sich jetzt die Frage stellen, welche Teiler der Gruppenordnung als Ordnung eines Elements auftreten. Das sind im Allgemeinen sicher nicht alle, denn zum Beispiel folgt aus $\operatorname{ord}(g) = \#G$, dass die Gruppe G zyklisch ist. (In diesem Fall treten tatsächlich alle Teiler von $\#G$ als Elementordnung auf — Übung!) Man kann aber folgende allgemeine Aussage machen.

12.24. **Satz.** *Sei G eine endliche Gruppe und sei p ein Primteiler von $\#G$. Dann gibt es in G (mindestens) ein Element der Ordnung p.*

SATZ
Satz von Cauchy

Beweis. Der Beweis verwendet einen Trick: Wir betrachten die Menge

$$M = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = 1_G\}\,.$$

A.-L. Cauchy
1789–1857

Da das letzte Element g_p in so einem Tupel eindeutig durch die ersten $p-1$ Elemente bestimmt ist ($g_p = (g_1 \cdots g_{p-1})^{-1}$), gilt $\#M = (\#G)^{p-1}$; wegen $p \mid \#G$ (und $p - 1 \geq 1$) ist das eine durch p teilbare Zahl.

Auf der anderen Seite können wir M aufteilen in eine Menge

$$M_1 = \{(g, g, \ldots, g) \mid (g, g, \ldots, g) \in M\}$$

und eine Menge $M_2 = M \setminus M_1$. Die Elemente von M_2 können wir zu je p zusammenfassen:

$$(g_1, g_2, \ldots, g_p), \quad (g_2, g_3, \ldots, g_p, g_1), \quad \ldots, \quad (g_p, g_1, g_2, \ldots, g_{p-1})$$

(Man beachte, dass $(g_2, g_3, \ldots, g_p, g_1)$ wieder in M ist, denn

$$g_1 g_2 \cdots g_p = 1_G \implies g_2 \cdots g_p = g_1^{-1} \implies g_2 \cdots g_p g_1 = 1_G\,.)$$

Diese Elemente sind alle verschieden, denn die Periode der Folge

$$g_1, g_2, \ldots, g_p, g_1, g_2, \ldots, g_p, g_1, \ldots$$

kann nur p oder 1 sein, und M_2 enthält genau die Elemente von M nicht, bei denen die Periode 1 ist. Es folgt, dass $\#M_2$ durch p teilbar ist. Dann muss aber auch $\#M_1 = \#M - \#M_2$ durch p teilbar sein. M_1 enthält mindestens das Element $(1_G, 1_G, \ldots, 1_G)$; es folgt, dass M_1 noch mindestens $p - 1 > 0$ weitere Elemente enthalten muss. Für so ein Element $(g, g, \ldots, g)$ gilt dann aber $g \neq 1_G$ und $g^p = 1_G$, also $\operatorname{ord}(g) = p$. ❑

Im nächsten Semester werden wir sehen, dass dieser Beweis eine Anwendung der sogenannten *Bahnengleichung* für die Operation (durch zyklische Vertauschung der Komponenten) der zyklischen Gruppe $\mathbb{Z}/p\mathbb{Z}$ auf M ist.

Damit die bisher eingeführten Begriffe etwas konkreter fassbar werden, betrachten wir als (relativ) einfaches Beispiel die Gruppe S_3.

12.25. **Beispiel.** Wir notieren für dieses Beispiel eine Permutation $\sigma \in S_n$ in der Form $[\sigma(1)\sigma(2)\dots\sigma(n)]$. Dann ist in S_3 $\mathrm{id} = [123]$ und **BSP** S_3

$$S_3 = \{[123], [213], [321], [132], [231], [312]\}\,.$$

Die Ordnungen dieser Elemente sind (in der angegebenen Reihenfolge) $1, 2, 2, 2, 3, 3$. Wir sehen also, dass es Elemente der Ordnungen 2 und 3 gibt, wie vom Satz von Cauchy 12.24 vorhergesagt. Da S_3 nicht abelsch, also insbesondere nicht zyklisch ist, kann es kein Element der Ordnung 6 geben.

Welche Untergruppen hat die S_3? Abgesehen von den *trivialen Untergruppen* $\{\mathrm{id}\}$ und S_3 muss eine Untergruppe nach dem Satz von Lagrange 12.19 die Ordnung 2 oder 3 haben. Eine Untergruppe der Ordnung 2 besteht aus der Identität und einem Element der Ordnung 2, und eine Untergruppe der Ordnung 3 besteht aus der Identität und zwei (zueinander inversen) Elementen der Ordnung 3. Es gibt also drei Untergruppen

$$\{[123], [213]\}, \quad \{[123], [321]\}, \quad \{[123], [132]\}$$

der Ordnung 2 und eine Untergruppe

$$\{[123], [231], [312]\}$$

der Ordnung 3. (Für einen Primteiler p der Ordnung einer endlichen Gruppe G gilt stets, dass die Anzahl u_p der Untergruppen der Ordnung p die Kongruenz $u_p \equiv 1 \bmod p$ erfüllt; das kann man aus dem Satz von Cauchy folgern. Wir werden diese Aussage später in stärkerer Form beweisen.)

Nach der Indexformel im Satz von Lagrange gilt dann, dass die Untergruppen der Ordnung 2 den Index 3 und die Untergruppen der Ordnung 3 den Index 2 haben. Ist $U_2 = \{[123], [213]\}$, dann sind die verschiedenen Linksnebenklassen von U_2

$$U_2 = \{[123], [213]\}, \quad [231]U_2 = \{[231], [321]\}, \quad [312]U_2 = \{[312], [132]\}$$

und die Rechtsnebenklassen sind

$$U_2 = \{[123], [213]\}, \quad U_2[231] = \{[231], [132]\}, \quad U_2[312] = \{[312], [321]\}\,;$$

man sieht, dass sie von den Linksnebenklassen (abgesehen natürlich von U_2 selbst) verschieden sind. Für die Untergruppe U_3 der Ordnung 3 gibt es jeweils nur eine nichttriviale (also $\neq U_3$) Links- und Rechtsnebenklasse, die gleich $S_3 \setminus U_3$ sein muss. Untergruppen mit der Eigenschaft, dass ihre Links- und Rechtsnebenklassen übereinstimmen, werden wir noch genauer betrachten. ♣

13. Gruppenhomomorphismen

Als Nächstes betrachten wir die strukturerhaltenden Abbildungen von Gruppen.

∗ 13.1. **Definition.** Seien G, G' zwei Gruppen. Eine Abbildung $\phi\colon G \to G'$ heißt ein *Gruppenhomomorphismus* (oder auch nur *Homomorphismus*), wenn für alle $g_1, g_2 \in G$ gilt, dass $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ ist.

DEF Gruppenhomomorphismus

Wie üblich nennt man ϕ einen *Monomorphismus*, *Epimorphismus*, *Isomorphismus*, *Endomorphismus* bzw. *Automorphismus*, falls ϕ injektiv, ϕ surjektiv, ϕ bijektiv, $G = G'$ bzw. ϕ bijektiv und $G = G'$ ist. Die Gruppen G und G' heißen *isomorph* und wir schreiben $G \cong G'$, wenn es einen Isomorphismus $G \to G'$ gibt. Der *Kern* von ϕ ist definiert als

isomorph

Kern

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1_{G'}\}\,.$$

Wir schreiben $\mathrm{Aut}(G)$ für die Menge der Automorphismen von G. ♢

$\mathrm{Aut}(G)$

Aus $\phi(1_G) = \phi(1_G^2) = \phi(1_G)^2$ folgt $\phi(1_G) = 1_{G'}$, und aus

$$1_{G'} = \phi(1_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

folgt $\phi(g^{-1}) = \phi(g)^{-1}$; ein Homomorphismus erhält also wirklich die komplette Gruppenstruktur. Man sieht auch leicht, dass für einen Isomorphismus ϕ die Umkehrabbildung ϕ^{-1} ebenfalls ein Isomorphismus ist und dass die Komposition zweier Gruppenhomomorphismen wieder ein Gruppenhomomorphismus ist. Es folgt unmittelbar:

13.2. **Lemma.** *Sei G eine Gruppe. Dann ist $\mathrm{Aut}(G)$ mit der Komposition von Abbildungen als Verknüpfung eine Gruppe.*

LEMMA $\mathrm{Aut}(G)$ ist Gruppe

Wir betrachten jetzt das Verhalten von Untergruppen unter Homomorphismen.

13.3. **Lemma.** *Sei $\phi\colon G \to G'$ ein Gruppenhomomorphismus. Dann gilt:*

LEMMA Homomorphismen und Untergruppen

(1) *Ist $U \leq G$, dann ist $\phi(U) \leq G'$. Insbesondere ist das Bild von ϕ eine Untergruppe von G'.*

(2) *Ist $U' \leq G'$, dann ist $\phi^{-1}(U') \leq G$. Insbesondere ist der Kern von ϕ eine Untergruppe von G.*

(3) *ϕ ist genau dann injektiv, wenn $\ker(\phi)$ trivial ist.*

Beweis.

(1) $1_{G'} = \phi(1_G) \in \phi(U)$; mit $u_1' = \phi(u_1)$ und $u_2' = \phi(u_2)$ sind auch $u_1'u_2' = \phi(u_1u_2)$ und $(u_1')^{-1} = \phi(u_1^{-1})$ in $\phi(U)$.

(2) $\phi(1_G) = 1_{G'}$, also ist $1_G \in \phi^{-1}(U')$. Sind $u_1, u_2 \in \phi^{-1}(U')$, das bedeutet $\phi(u_1), \phi(u_2) \in U'$, dann folgt $\phi(u_1u_2) = \phi(u_1)\phi(u_2) \in U'$ und $\phi(u_1^{-1}) = \phi(u_1)^{-1} \in U'$ und damit $u_1u_2, u_1^{-1} \in \phi^{-1}(U')$.

(3) „⇒“ ist trivial. Für die Gegenrichtung sei $\ker(\phi) = \{1_G\}$. Dann gilt für $g_1, g_2 \in G$:

$$\begin{aligned}\phi(g_1) = \phi(g_2) &\Rightarrow \phi(g_1g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = 1_{G'}\\ &\Rightarrow g_1g_2^{-1} \in \ker(\phi) = \{1_G\}\\ &\Rightarrow g_1g_2^{-1} = 1_G \Rightarrow g_1 = g_2\,.\end{aligned}$$

❑

Wir werden im nächsten Abschnitt sehen, dass Kerne von Homomorphismen sogar spezielle Untergruppen sind.

13.4. **Beispiele.** Wir bringen eine Reihe von Beispielen von Gruppenhomomorphismen und definieren dabei gleich noch einige Begriffe.

BSP Gruppenhomomorphismen

(1) Für beliebige Gruppen G und G' gibt es immer den *trivialen Homomorphismus* $G \to G'$, $g \mapsto 1_{G'}$.

(2) Die Determinante ist multiplikativ. Das bedeutet, dass für jeden Körper K und jede Zahl $n \in \mathbb{Z}_{\geq 0}$ die Abbildung $\det\colon \mathrm{GL}(n,K) \to K^\times$ ein Gruppenhomomorphismus ist. Der Kern wird $\mathrm{SL}(n,K)$ (oder $\mathrm{SL}_n(K)$) geschrieben und heißt *spezielle lineare Gruppe*. Für $n \geq 1$ ist det ein Epimorphismus.

DEF $\mathrm{SL}(n,K)$

(3) Für eine Permutation $\sigma \in S_n$ sei $P(\sigma) \in \mathrm{GL}(n,\mathbb{R})$ die zugehörige Permutationsmatrix (d.h., der Eintrag in Zeile $\sigma(i)$ und Spalte i ist 1, für $i = 1,\dots,n$; alle anderen Einträge sind 0), sodass gilt $P(\sigma)\mathbf{e}_i = \mathbf{e}_{\sigma(i)}$, wobei $(\mathbf{e}_1,\dots,\mathbf{e}_n)$ die Standardbasis von $\mathbb{R}^n$ ist. Dann ist $P\colon S_n \to \mathrm{GL}_n(\mathbb{R})$ ein Gruppenhomomorphismus. Das Bild von P liegt in der orthogonalen Gruppe $\mathrm{O}(n)$, denn $P(\sigma)^\top = P(\sigma^{-1})$, also gilt $P(\sigma)P(\sigma)^\top = I_n$.

(4) Die Komposition $\mathrm{sign} = \det \circ P\colon S_n \to \{\pm 1\}$ ergibt das *Signum* einer Permutation. Für $n \geq 2$ ist diese Abbildung surjektiv, denn eine *Transposition* (also eine Permutation, die zwei Elemente vertauscht und alle anderen fest lässt) hat Signum -1. Der Kern dieses Homomorphismus heißt die *alternierende Gruppe* A_n (häufig auch $\mathfrak{A}_n$ geschrieben). Die alternierende Gruppe besteht also aus allen *geraden* Permutationen (denen mit Signum $+1$).

DEF alternierende Gruppe

(5) Ist G eine Gruppe und $g \in G$, dann ist $\mathbb{Z} \to G$, $n \mapsto g^n$ ein Homomorphismus. Sein Kern ist trivial, falls g unendliche Ordnung hat, sonst ist der Kern $\mathrm{ord}(g)\mathbb{Z}$, siehe Lemma 12.10 und Lemma 12.23. ♣

Die folgenden Beispiele behandeln Automorphismen, die in jeder Gruppe existieren.

13.5. **Beispiele.**

BSP innere Automorphismen

(1) Seien G eine Gruppe und $g \in G$. Dann ist $c_g\colon G \to G$, $x \mapsto gxg^{-1}$ ein Automorphismus von G. Solche Automorphismen heißen *innere Automorphismen* von G; die Abbildung c_g heißt die *Konjugation* mit g. Wir zeigen, dass c_g ein Homomorphismus ist:

DEF innerer Automorphismus

Konjugation

$$c_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = gxg^{-1}\cdot gyg^{-1} = c_g(x)c_g(y)\,.$$

Offensichtlich ist $c_{g^{-1}}$ die zu c_g inverse Abbildung, also ist c_g sogar ein Isomorphismus. c_g ist genau dann die Identität id_G, wenn $gxg^{-1} = x$, also $gx = xg$ gilt für alle $x \in G$. Das bedeutet gerade, dass g ein Element des *Zentrums*

DEF Zentrum

$$Z(G) = \{g \in G \mid gx = xg \text{ für alle } x \in G\}$$

von G ist. Zum Beispiel hat eine abelsche Gruppe keine inneren Automorphismen außer der Identität, denn dann ist $Z(G) = G$.

(2) Die Abbildung

$$c\colon G \longrightarrow \mathrm{Aut}(G), \quad g \longmapsto c_g$$

ist ein Gruppenhomomorphismus. Es gilt nämlich für alle $g, h, x \in G$

$$(c_g \circ c_h)(x) = c_g\big(c_h(x)\big) = c_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = c_{gh}(x)\,,$$

also ist $c_g \circ c_h = c_{gh}$. Es gilt $\ker(c) = Z(G)$, siehe oben; damit ist auch klar, dass $Z(G)$ eine Untergruppe von G ist. ♣

13.6. **Definition.** Sei G eine Gruppe. Die Gruppe $\mathrm{Aut}(G)$ heißt die *Automorphismengruppe* von G. Die Untergruppe $\mathrm{Inn}(G) = \{c_g \mid g \in G\}$ (mit $c_g\colon x \mapsto gxg^{-1}$ wie oben) heißt die *innere Automorphismengruppe* von G. ♢

DEF Automorphismengruppe

Beachte, dass $\mathrm{Inn}(G)$ als Bild des Homomorphismus c aus Beispiel 13.5 tatsächlich eine Untergruppe von $\mathrm{Aut}(G)$ ist.

13.7. **Beispiele.**

BSP Automorphismengruppen

(1) Es gilt $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}) \cong S_3$. Denn jede Permutation von $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, die das neutrale Element fest lässt, aber die übrigen drei Elemente beliebig vertauscht, ist ein Automorphismus.

(2) Für $n \geq 3$ ist das Zentrum von S_n trivial: Sei $\tau \in S_n$ eine beliebige Transposition, τ vertausche etwa r und s. Wir setzen $T = \{r, s\}$. Für $\sigma \in S_n$ gilt dann

$$\sigma \circ \tau = \tau \circ \sigma \iff \sigma(T) = T\,.$$

Die Richtung „$\Leftarrow$“ ist leicht zu sehen und für unser Argument nicht relevant. Für die Gegenrichtung nehmen wir $\sigma(T) \neq T$ an, also ohne Einschränkung $\sigma(r) \notin T$. Dann ist

$$(\sigma \circ \tau)(r) = \sigma\big(\tau(r)\big) = \sigma(s) \quad \text{und} \quad (\tau \circ \sigma)(r) = \tau\big(\sigma(r)\big) = \sigma(r) \neq \sigma(s)\,,$$

also sind $\sigma \circ \tau$ und $\tau \circ \sigma$ verschieden.

Ist $\sigma \in Z(S_n)$ und $n \geq 3$, dann vertauscht σ mit allen Transpositionen τ. Ist $i \in \{1, 2, \ldots, n\}$, dann gibt es zwei weitere Elemente j und k (hier verwenden wir $n \geq 3$). Aus obiger Äquivalenz folgt, dass $\sigma(\{i, j\}) = \{i, j\}$ und $\sigma(\{i, k\}) = \{i, k\}$ ist, was nur geht, wenn $\sigma(i) = i$ ist. Da hier i beliebig war, folgt $\sigma = \mathrm{id}$. Damit ist $Z(S_n) = \{\mathrm{id}\}$ trivial wie behauptet.

Es folgt, dass für $n \geq 3$ die oben betrachtete Abbildung $c\colon S_n \to \mathrm{Aut}(S_n)$ injektiv ist; damit ist $\mathrm{Inn}(S_n) \cong S_n$. Für $n \leq 2$ sind $\mathrm{Aut}(S_n)$ und $\mathrm{Inn}(S_n)$ beide trivial. ♣

Man kann auch zeigen, dass $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$ ist für alle $n \geq 3$ mit $n \neq 6$. Die symmetrische Gruppe S_6 hat dagegen äußere (also nicht-innere) Automorphismen.

14. Normalteiler und Faktorgruppen

Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Wie in anderen Situationen auch, würden wir gerne auf der Menge G/U (oder $U\backslash G$) eine Gruppenstruktur definieren, sodass die kanonische Abbildung $G \to G/U$, $g \mapsto gU$, ein Homomorphismus wird. Dazu müssten wir definieren $gU \cdot g'U = (gg')U$. Hier ergibt sich aber ein Problem: Diese Verknüpfung ist nicht immer wohldefiniert. Wenn wir $g = 1_G$ nehmen, dann ist jedes $u \in U$ ein anderer Repräsentant von $gU = U$, also sollte $ug' \in g'U$ sein für alle $u \in U$. Das bedeutet $Ug' \subset g'U$. Das muss für alle $g' \in G$ gelten, also insbesondere auch für $(g')^{-1}$; zusammen folgt $Ug' = g'U$: Links- und Rechtsnebenklassen müssen übereinstimmen. Dies ist jedoch nicht immer der Fall (siehe Beispiel 12.25 für $G = S_3$). Daher führt man einen neuen Begriff ein.

* 14.1. **Definition.** Seien G eine Gruppe und $U \leq G$ eine Untergruppe. Dann heißt U ein *Normalteiler* von G oder *normal* in G, wenn für alle $g \in G$ gilt $gU = Ug$. Man schreibt dann $U \triangleleft G$. ♢

DEF Normalteiler

Äquivalent dazu ist $gUg^{-1} = U$ oder auch nur $gUg^{-1} \subset U$ für alle $g \in G$ (aus $gUg^{-1} \subset U$ und $g^{-1}Ug \subset U$ folgt $gUg^{-1} = U$). Normalteiler sind also Untergruppen, die von allen Konjugationsabbildungen c_g als Menge fest gelassen werden. Üblicherweise zeigt man, dass eine Untergruppe U ein Normalteiler von G ist, indem man für alle $u \in U$ und $g \in G$ nachprüft, dass $gug^{-1} \in U$ ist.

14.2. **Beispiele.**

BSP Normalteiler

(1) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.

(2) Ist G eine Gruppe und $U \leq G$ mit $(G : U) = 2$, dann ist U ein Normalteiler. Denn für gU bzw. Ug gibt es nur die beiden Möglichkeiten U und $G \setminus U$; aus $gU \cap Ug \neq \emptyset$ folgt also $gU = Ug$. Zum Beispiel ist für $n \geq 2$ die alternierende Gruppe A_n ein Normalteiler von S_n, denn $(S_n : A_n) = 2$ nach dem Homomorphiesatz 14.6 unten.

(3) Sei $g \in G$ mit $\operatorname{ord}(g) = 2$. Dann ist $\langle g \rangle = \{1_G, g\}$ genau dann ein Normalteiler von G, wenn $g \in Z(G)$ ist. Zum Beispiel sind die Untergruppen der Ordnung 2 von S_3 keine Normalteiler.

DEF trivialer Normalteiler

(4) In jeder Gruppe sind die Untergruppen $\{1_G\}$ und G Normalteiler, die *trivialen Normalteiler* von G.

(5) In jeder Gruppe G gilt $Z(G) \triangleleft G$, denn für $g \in G$ und $z \in Z(G)$ gilt $gzg^{-1} = z \in Z(G)$ (hier gilt die Bedingung für einen Normalteiler sogar elementweise). ♣

14.3. **Lemma.** *Sei $\phi\colon G \to G'$ ein Gruppenhomomorphismus.*

LEMMA Homomorphismen und Normalteiler

(1) *Ist $N' \triangleleft G'$, dann ist auch $\phi^{-1}(N') \triangleleft G$. Insbesondere ist $\ker(\phi)$ ein Normalteiler von G.*

(2) *Ist ϕ **surjektiv** und $N \triangleleft G$, dann gilt auch $\phi(N) \triangleleft G'$.*

Beweis.

(1) Wir wissen bereits (Lemma 13.3), dass $\phi^{-1}(N')$ eine Untergruppe von G ist. Außerdem gilt für $g \in G$ und $n \in \phi^{-1}(N')$:
$$\phi\big(gng^{-1}\big) = \phi(g)\phi(n)\phi(g)^{-1} \in \phi(g)N'\phi(g)^{-1} = N'$$
und damit
$$g\phi^{-1}(N')g^{-1} \subset \phi^{-1}(N')\,.$$

(2) Wir wissen bereits, dass $\phi(N)$ eine Untergruppe von G' ist (Lemma 13.3). Da ϕ surjektiv ist, lässt sich jedes $g' \in G'$ schreiben als $\phi(g)$ mit $g \in G$. Damit gilt dann
$$g'\phi(N)(g')^{-1} = \phi(g)\phi(N)\phi(g^{-1}) = \phi(gNg^{-1}) = \phi(N)\,. \qquad \text{❑}$$

Wie schon angedeutet, haben Normalteiler $N \triangleleft G$ die Eigenschaft, dass man auf der Menge G/N in natürlicher Weise eine Gruppenstruktur definieren kann.

* 14.4. **Satz.** *Seien G eine Gruppe und N ein Normalteiler von G. Dann definiert $gN \cdot hN = (gN)(hN) = (gh)N$ eine Gruppenstruktur auf G/N, sodass die kanonische Abbildung $\phi\colon G \to G/N$, $g \mapsto gN$, ein Homomorphismus ist. Es gilt $\ker(\phi) = N$.* **SATZ** Faktorgruppe

Beweis. Wegen der Assoziativität der Verknüpfung, und weil N Normalteiler ist, gilt $(gN)(hN) = g(Nh)N = g(hN)N = (gh)(NN) = (gh)N$; damit ist auch klar, dass diese Verknüpfung wohldefiniert ist und dass $\phi(gh) = \phi(g)\phi(h)$ gilt. Letzteres, zusammen mit der Surjektivität von ϕ, erzwingt die Gültigkeit der Gruppenaxiome für G/N. Dass $\ker(\phi) = N$ ist, folgt aus
$$\phi(g) = 1_{G/N} = N \iff gN = N \iff g \in N\,. \qquad \text{❑}$$

14.5. **Definition.** Die Gruppe G/N heißt die *Faktorgruppe* (oder *Quotientengruppe*) von G nach (oder modulo) N; ϕ heißt *kanonischer Epimorphismus*. ♢ **DEF** Faktorgruppe

Wir sehen also, dass die Normalteiler von G genau die Kerne von Gruppenhomomorphismen mit Definitionsbereich G sind. Das ist vergleichbar mit der Situation bei Ringen, wo die Kerne genau die Ideale sind (und nicht etwa die Unterringe).

Wir haben den üblichen Homomorphiesatz.

* 14.6. **Satz.** *Sei $\phi\colon G \to G'$ ein Gruppenhomomorphismus. Dann induziert ϕ einen Isomorphismus*
$$\tilde{\phi}\colon G/\ker(\phi) \longrightarrow \operatorname{im}(\phi)\,, \qquad g\ker(\phi) \longmapsto \phi(g)\,.$$
Insbesondere gilt $(G : \ker(\phi)) = \#\operatorname{im}(\phi)$. Für jeden Normalteiler $N \triangleleft G$ mit $N \subset \ker(\phi)$ erhalten wir einen induzierten Homomorphismus $G/N \to G'$ mit Bild $\operatorname{im}(\phi)$. **SATZ** Homomorphiesatz für Gruppen

Beweis. Wir zeigen zuerst die letzte Aussage: $\phi_N\colon G/N \to G'$, $gN \mapsto \phi(g)$ ist wohldefiniert, denn für $g' = gn$ mit $n \in N$ gilt $\phi(g') = \phi(gn) = \phi(g)\phi(n) = \phi(g)$, da $\phi|_N = 1_{G'}$. Außerdem ist ϕ_N ein Homomorphismus, denn
$$\phi_N\big((gN)(hN)\big) = \phi_N\big((gh)N\big) = \phi(gh) = \phi(g)\phi(h) = \phi_N(gN)\phi_N(hN)\,.$$
Es ist auch klar, dass $\operatorname{im}(\phi_N) = \operatorname{im}(\phi)$ ist. Für $N = K := \ker(\phi)$ erhalten wir $\tilde{\phi}$; es bleibt zu zeigen, dass $\tilde{\phi}$ injektiv ist. Es gilt
$$\tilde{\phi}(gK) = 1_{G'} \iff \phi(g) = 1_{G'} \iff g \in K \iff gK = K\,,$$

also besteht der Kern von $\tilde\phi$ nur aus dem Element K. Es folgt auch (da $\tilde\phi$ bijektiv ist)

$$\big(G : \ker(\phi)\big) = \#\big(G/\ker(\phi)\big) = \#\operatorname{im}(\phi)\,. \qquad \text{❑}$$

14.7. **Beispiel.** Eine typische Anwendung des Satzes ist die Berechnung der Ordnung von $\ker(\phi)$, denn es gilt (wenn G endlich ist) **BSP** $\#\ker(\phi)$

$$\#\ker(\phi) = \frac{\#G}{(G : \ker(\phi))} = \frac{\#G}{\#\operatorname{im}(\phi)}\,.$$

Zum Beispiel ist $\#A_n = \frac{n!}{2}$ für $n \geq 2$, denn A_n ist der Kern des surjektiven Homomorphismus $\operatorname{sign}\colon S_n \to \{\pm 1\}$. Analog findet man

$$\#\operatorname{SL}(2,\mathbb{F}_p) = \frac{\#\operatorname{GL}(2,\mathbb{F}_p)}{\#\mathbb{F}_p^\times} = \frac{(p^2-1)(p^2-p)}{p-1} = (p^2-1)p = (p-1)p(p+1)\,,$$

denn $\operatorname{SL}(2,\mathbb{F}_p) = \ker(\det\colon \operatorname{GL}(2,\mathbb{F}_p) \to \mathbb{F}_p^\times)$, und det ist in diesem Fall surjektiv. ♣

14.8. **Beispiel.** Satz 14.6 liefert einen Isomorphismus **BSP** innere Automorphismen

$$G/Z(G) \xrightarrow{\cong} \operatorname{Inn}(G)\,.$$

Die Gruppe $\operatorname{Inn}(G)$ der inneren Automorphismen einer Gruppe G ist ein Normalteiler der Automorphismengruppe $\operatorname{Aut}(G)$. Dafür ist zu zeigen, dass für jedes $g \in G$ und jeden Automorphismus $\phi \in \operatorname{Aut}(G)$ die Abbildung $\phi \circ c_g \circ \phi^{-1}$ wieder ein innerer Automorphismus ist, also die Form $c_{g'}$ hat für ein $g' \in G$. Es ist für $x \in G$

$$\begin{aligned}(\phi \circ c_g \circ \phi^{-1})(x) &= \phi\big(c_g(\phi^{-1}(x))\big) = \phi\big(g\phi^{-1}(x)g^{-1}\big)\\ &= \phi(g)\phi\big(\phi^{-1}(x)\big)\phi(g^{-1}) = \phi(g)x\phi(g)^{-1}\\ &= c_{\phi(g)}(x)\,,\end{aligned}$$

also gilt $\phi \circ c_g \circ \phi^{-1} = c_{\phi(g)}$.

Die Faktorgruppe $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ heißt die *äußere Automorphismengruppe* von G und wird $\operatorname{Out}(G)$ geschrieben („outer automorphisms“). ♣ **DEF** äußere Automorphismengruppe

Aus dem Homomorphiesatz 14.6 kann man weitere „Isomorphiesätze“ folgern. Zum Beispiel ist der folgende gelegentlich nützlich.

14.9. **Folgerung.** *Seien G eine Gruppe, $U \leq G$ eine Untergruppe und $N \lhd G$ ein Normalteiler. Dann ist $NU = UN$ eine Untergruppe von G, $N \cap U$ ist ein Normalteiler von U und* **FOLG** Isomorphie-Satz

$$\phi\colon U/(N\cap U) \longrightarrow NU/N, \quad u(N\cap U) \longmapsto uN$$

ist ein Isomorphismus. Insbesondere gilt $(NU : N) = (U : N \cap U)$.

Beweis. Wir zeigen zuerst, dass $NU = UN$ ist. Für $u \in U$, $n \in N$ gilt $Nu = uN$; die Vereinigung über alle $u \in U$ liefert $NU = UN$. Wir zeigen, dass das eine Untergruppe von G ist: $1_G \in UN$ ist klar. Sind $g_1, g_2 \in NU = UN$, dann gibt es $u_1, u_2 \in U$ und $n_1, n_2 \in N$ mit $g_1 = n_1u_1$ und $g_2 = u_2n_2$; es ist dann $g_1g_2 = n_1(u_1u_2)n_2 \in NUN = NNU = NU$ und $g_1^{-1} = u_1^{-1}n_1^{-1} \in UN = NU$.

Sei $\phi_0\colon U \to NU \to NU/N$, $u \mapsto uN$, die Komposition der Inklusionsabbildung mit dem kanonischen Epimorphismus. Wir zeigen, dass ϕ_0 surjektiv ist: Sei gN ein Element

von NU/N mit $g \in NU = UN$, dann ist $g = un$ mit $u \in U$ und $n \in N$; es folgt $gN = unN = uN = \phi_0(u)$. Der Kern von ϕ_0 ist

$$\ker(\phi_0) = \{u \in U \mid uN = N\} = \{u \in U \mid u \in N\} = N \cap U\,;$$

also ist $N \cap U$ ein Normalteiler von U und der von ϕ_0 induzierte Homomorphismus ϕ ist nach Satz 14.6 ein Isomorphismus. ❑

Ist U auch ein Normalteiler von G, dann gilt für $g \in G$, dass $gNU = NgU = NUg$ ist, also ist NU in diesem Fall ebenfalls ein Normalteiler von G.

DEF einfache Gruppe

14.10. **Definition.** Eine Gruppe G heißt *einfach*, wenn G nicht trivial ist und außer den trivialen Normalteilern $\{1_G\}$ und G keine Normalteiler hat. ♢

Anders gesagt: Jedes *epimorphe Bild* von G (also jede Faktorgruppe G/N) ist entweder trivial oder (mittels des Epimorphismus) isomorph zu G. Es gibt also kein „vereinfachtes Abbild“ der Gruppe, daher der Name.

In der Literatur wird nicht immer gefordert, dass G nicht trivial ist (z.B. [Fi]). Im Hinblick auf die unten beschriebene „Zerlegung“ einer Gruppe in einfache Gruppen ist diese Forderung aber sinnvoll, analog dazu, dass man von einer Primzahl verlangt, $\neq 1$ zu sein.

In gewisser Weise spielen einfache Gruppen für die Gruppentheorie eine ähnliche Rolle wie Primzahlen für die multiplikative Theorie der ganzen Zahlen. Wenn G etwa eine nichttriviale endliche Gruppe ist, dann ist G entweder einfach, oder G hat einen nichttrivialen Normalteiler N. In diesem Fall kann man G aus N und G/N „zusammensetzen“ (allerdings gibt es bei gegebenen Gruppen N und G/N im Allgemeinen mehrere Möglichkeiten, wie man daraus eine Gruppe zusammenbauen kann, insofern ist die Situation deutlich komplizierter als bei den ganzen Zahlen); N und G/N lassen sich weiter zerlegen, bis man bei einfachen Gruppen ankommt. Man kann zeigen, dass die einfachen Gruppen, die man bekommt, bis auf Isomorphie eindeutig bestimmt sind, unabhängig davon, wie man diesen Prozess durchführt — das ist das Analogon zum Satz über die eindeutige Primfaktorzerlegung.

Für endliche *abelsche* Gruppen ist die Klassifikation der einfachen Gruppen recht übersichtlich.

SATZ abelsche einfache Gruppen

14.11. **Satz.** *Eine endliche abelsche Gruppe ist genau dann einfach, wenn ihre Ordnung eine Primzahl ist.*

Beweis. Sei A eine einfache endliche abelsche Gruppe. Dann ist A nicht trivial, also hat $\#A$ einen Primteiler p. Nach dem Satz von Cauchy 12.24 hat A ein Element a der Ordnung p und damit eine Untergruppe $\langle a\rangle$ der Ordnung p. In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler; da A einfach ist, muss $\langle a\rangle = A$ sein, und es gilt $\#A = p$.

Ist umgekehrt p eine Primzahl und A eine Gruppe mit $\#A = p$, dann gilt für jeden Normalteiler N von A, dass $\#N$ ein Teiler von p ist (Satz von Lagrange 12.19), also ist $\#N = 1$ und damit $N = \{1_A\}$ oder $\#N = p$ und damit $N = A$. ❑

Damit haben wir bereits eine unendliche Familie von endlichen einfachen Gruppen kennen gelernt. Die Klassifikation der endlichen einfachen Gruppen wurde (im Wesentlichen — eine Lücke im Beweis wurde erst 2002 geschlossen) in den 1980er Jahren vollendet; der Beweis verteilt sich auf viele Tausend Seiten und eine große Zahl mathematischer Arbeiten. Das Resultat ist, dass es 18 unendliche

Familien endlicher einfacher Gruppen gibt und dazu noch 26 sogenannte „sporadische einfache Gruppen“. Die größte dieser Gruppen ist das manchmal so genannte „Monster“; diese Gruppe hat eine Ordnung von

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$
$$= 8080\,17424\,79451\,28758\,86459\,90496\,17107\,57005\,75436\,80000\,00000\,.$$

Eine weitere Familie von einfachen Gruppen sind die alternierenden Gruppen A_n mit $n \geq 5$:

SATZ A_n ist einfach

14.12. **Satz.** *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

Beweis. Wir geben hier nur eine grobe Skizze. Ein *3-Zykel* ist eine Permutation, die genau drei Elemente a, b, c in der Form $a \mapsto b \mapsto c \mapsto a$ bewegt und alle anderen Elemente fest lässt. Jeder 3-Zykel ist gerade, also ein Element von A_n. Man zeigt dann:

- Die A_n wird von den 3-Zykeln erzeugt.
- Ist $n \geq 5$, dann sind alle 3-Zykel in der A_n konjugiert: Zu je zwei 3-Zykeln σ, σ' gibt es $\tau \in A_n$ mit $\tau\sigma\tau^{-1} = \sigma'$.

Daraus folgt, dass ein Normalteiler $N \triangleleft A_n$ (mit $n \geq 5$), der einen 3-Zykel enthält, schon die ganze A_n sein muss (da dann *alle* 3-Zykel in N sind). Schließlich zeigt man noch:

- Ist $\{\mathrm{id}\} \neq N \triangleleft A_n$ und $n \geq 5$, dann enthält N einen 3-Zykel.

Es folgt, dass es nur die beiden Normalteiler $\{\mathrm{id}\}$ und A_n gibt.

Siehe zum Beispiel [KM, § 9.3.2]. ❑

Zum Beispiel ist die A_5 (mit $\#A_5 = 60$) die kleinste nicht-abelsche einfache Gruppe.

Die anderen unendlichen Familien sind „Gruppen vom Lie-Typ“. Eine davon erhält man wie folgt:

Zu jeder Primzahlpotenz $q = p^e$ gibt es einen (bis auf Isomorphie eindeutigen) Körper $\mathbb{F}_q$ mit q Elementen (das werden wir im nächsten Semester beweisen). Wir können dann die Gruppe $\mathrm{SL}(n, \mathbb{F}_q)$ betrachten. Ihr Zentrum besteht aus den skalaren Matrizen λI_n mit $\lambda^n = 1$ und ist ein Normalteiler. Der Quotient $\mathrm{PSL}(n, \mathbb{F}_q) := \mathrm{SL}(n, \mathbb{F}_q)/Z(\mathrm{SL}(n, \mathbb{F}_q))$ ist einfach, außer für sehr kleine Werte von n und q. Zum Beispiel ist die $\mathrm{PSL}(2, \mathbb{F}_7)$ der Ordnung 168 die zweitkleinste nicht-abelsche einfache Gruppe.

15. Endlich erzeugte abelsche Gruppen

Unser Ziel in diesem Abschnitt ist es, einen Struktur- und Klassifikationssatz über endlich erzeugte abelsche Gruppen zu beweisen. Im Wesentlichen sagt dieser Satz, dass jede endlich erzeugte abelsche Gruppe zu einem direkten Produkt von zyklischen Gruppen isomorph ist. Daher definieren wir zuerst einmal, was so ein direktes Produkt von Gruppen ist. Die Konstruktion ist analog zu der bei Ringen, vergleiche Beispiel 3.1 (1).

DEF direktes Produkt von Gruppen

15.1. **Definition.** Sei $(G_i)_{i\in I}$ eine Familie von (multiplikativ geschriebenen) Gruppen. Sei $G = \prod_{i\in I} G_i$ ihr kartesisches Produkt. Dann ist G eine Gruppe, wenn wir die Verknüpfung komponentenweise definieren:

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

Die Gruppe G heißt das *direkte Produkt* der Gruppen G_i. Ist $I = \{1, 2, 3, \dots, n\}$ endlich, dann schreiben wir auch

$$G = G_1 \times G_2 \times \cdots \times G_n\,.$$

Ist die Indexmenge I leer, dann ist G trivial. ♢

Dass G wirklich eine Gruppe ist, prüft man leicht nach.

Sind alle Gruppen G_i abelsch, dann ist auch G abelsch. Wir werden in diesem Abschnitt abelsche Gruppen meist additiv schreiben. Die Verknüpfung in G ist dann dementsprechend

$$(g_i)_{i\in I} + (h_i)_{i\in I} = (g_i + h_i)_{i\in I}\,.$$

Wir erinnern uns an die Schreibweise $n \cdot g$ für $n \in \mathbb{Z}$ und $g \in G$ für die Vielfachen von g, wenn G eine additive Gruppe ist (siehe Definition 12.9). Damit lässt sich das Erzeugnis einer endlichen Teilmenge wie folgt beschreiben.

LEMMA Erzeugnis in abelscher Gruppe

15.2. **Lemma.** *Sei G eine additiv geschriebene abelsche Gruppe. Seien außerdem $g_1, g_2, \dots, g_n \in G$. Dann ist*

$$\langle g_1, g_2, \dots, g_n\rangle = \{m_1 \cdot g_1 + m_2 \cdot g_2 + \ldots + m_n \cdot g_n \mid m_1, m_2, \dots, m_n \in \mathbb{Z}\}$$

die Menge der „ganzzahligen Linearkombinationen“ der Elemente $g_1, g_2, \dots, g_n$.

Beweis. Sei U die Menge auf der rechten Seite. Da G abelsch ist, gilt

$$(m_1 \cdot g_1 + \ldots + m_n \cdot g_n) + (m_1' \cdot g_1 + \ldots + m_n' \cdot g_n) = (m_1 + m_1') \cdot g_1 + \ldots + (m_n + m_n') \cdot g_n$$

und

$$-(m_1 \cdot g_1 + \ldots + m_n \cdot g_n) = (-m_1) \cdot g_1 + \ldots + (-m_n) \cdot g_n\,,$$

woraus man sieht, dass U eine Untergruppe ist, die $g_1, \dots, g_n$ enthält. Auf der anderen Seite muss jede Untergruppe von G, die $g_1, \dots, g_n$ enthält, auch die Elemente von U enthalten, und die Behauptung folgt. ❑

Wir haben nun folgendes erstes Resultat, das zeigt, dass „endlich erzeugt“ und „abelsch“ zwei gut verträgliche Eigenschaften sind.

15.3. **Satz.** *Sei $G = \langle g_1, g_2, \ldots, g_n\rangle$ eine endlich erzeugte abelsche Gruppe und sei $U \leq G$ eine Untergruppe. Dann ist U ebenfalls von (höchstens) n Elementen erzeugt.*

SATZ Endliche Erzeugtheit von Untergruppen

Beweis. Induktion über die Anzahl n der Erzeuger von G.

Im Fall $n = 0$ ist G trivial. Dann ist auch U trivial und daher von null Elementen erzeugt.

Im Fall $n = 1$ ist G zyklisch. Dann ist auch jede Untergruppe U von G zyklisch (Übungsaufgabe) und damit ebenfalls von einem Element erzeugt.

Sei jetzt $n \geq 2$. Wir betrachten $V = \langle g_n\rangle \leq G$ und $G' = G/V$. Sei $\pi\colon G \to G'$ der kanonische Epimorphismus; dann ist $\pi(g_n) = 0_{G'}$, also wird

$$G' = \pi(G) = \langle \pi(g_1), \ldots, \pi(g_{n-1}), \pi(g_n)\rangle = \langle \pi(g_1), \ldots, \pi(g_{n-1})\rangle$$

von $n-1$ Elementen erzeugt. Nach Induktionsannahme ist dann $U' = \pi(U)$ ebenfalls von $n-1$ Elementen erzeugt; etwa $U' = \langle \pi(u_1), \ldots, \pi(u_{n-1})\rangle$ mit geeigneten $u_1, \ldots, u_{n-1} \in U$. Sei $U'' = U \cap V = \ker(\pi|_U)$. Dann ist U'' als Untergruppe der zyklischen Gruppe V von einem Element erzeugt: $U'' = \langle u_n\rangle$.

Es gilt nun $U = \langle u_1, \ldots, u_{n-1}, u_n\rangle$: „$\supset$“ ist klar. Für „$\subset$“ sei $u \in U$ beliebig. Dann gibt es $m_1, \ldots, m_{n-1} \in \mathbb{Z}$ mit $\pi(u) = m_1 \cdot \pi(u_1) + \ldots + m_{n-1} \cdot \pi(u_{n-1})$. Es folgt, dass $u'' = u - (m_1 \cdot u_1 + \ldots + m_{n-1} \cdot u_{n-1}) \in U''$ ist (denn $\pi(u'') = 0$), also gibt es $m_n \in \mathbb{Z}$ mit $u'' = m_n \cdot u_n$. Insgesamt sehen wir, dass $u = m_1 \cdot u_1 + \ldots + m_{n-1} \cdot u_{n-1} + m_n \cdot u_n$ ist wie gewünscht. ❑

Der Satz und das vorangegangene Lemma erinnern an Aussagen aus der Linearen Algebra: Der von gewissen Elementen erzeugte Untervektorraum besteht aus allen Linearkombinationen dieser Elemente, und die Dimension eines Untervektorraums kann nicht größer sein als die des umgebenden Vektorraums. Das ist kein Zufall: Abelsche Gruppen kann man auch als „$\mathbb{Z}$-Moduln“ betrachten; dabei ist für einen Ring R ein R-Modul genauso definiert wie ein „R-Vektorraum“, nur dass die Skalare aus einem Ring kommen statt aus einem Körper. Viele (aber nicht alle — zum Beispiel hat ein endlich erzeugter Modul nicht immer eine Basis) Resultate aus der Linearen Algebra lassen sich auf diese allgemeinere Situation übertragen.

Für nicht-abelsche Gruppen ist die Aussage von Satz 15.3 im Allgemeinen *falsch*: Es gibt endlich erzeugte Gruppen mit Untergruppen, die nicht endlich erzeugt sind. (Frage: Wo geht der Beweis oben schief, wenn G nicht abelsch ist?)

Ist G eine (additive) abelsche Gruppe und sind $g_1, g_2, \ldots, g_n \in G$, dann ist die „Linearkombinationenabbildung“

$$\phi\colon \mathbb{Z}^n \longrightarrow G, \quad (m_1, \ldots, m_n) \longmapsto m_1 \cdot g_1 + \ldots + m_n \cdot g_n$$

ein Gruppenhomomorphismus. ϕ ist genau dann surjektiv, wenn $(g_1, \ldots, g_n)$ ein Erzeugendensystem von G ist.

∗ 15.4. **Definition.** Ist $G \cong \mathbb{Z}^n$ für ein $n \in \mathbb{Z}_{\geq 0}$, dann heißt G eine *freie abelsche Gruppe* vom Rang n. ♢

DEF freie abelsche Gruppe

15.5. **Lemma.** *Sei $G = \langle g_1, \dots, g_n \rangle$ eine endlich erzeugte abelsche Gruppe. Gilt für alle $m_1, \dots, m_n \in \mathbb{Z}$ die Implikation*

$$m_1 \cdot g_1 + \dots + m_n \cdot g_n = 0 \implies m_1 = \dots = m_n = 0\,,$$

dann ist ϕ wie oben ein Isomorphismus. Insbesondere ist G frei vom Rang n.

LEMMA freies EZS

Beweis. Wir wissen bereits, dass ϕ surjektiv ist; es genügt also zu zeigen, dass ϕ auch injektiv ist. Sei dazu $(m_1, \dots, m_n) \in \ker(\phi)$. Das bedeutet

$$0 = \phi(m_1, \dots, m_n) = m_1 \cdot g_1 + \dots + m_n \cdot g_n\,,$$

nach Voraussetzung also $(m_1, \dots, m_n) = (0, \dots, 0)$. Wir sehen, dass ϕ trivialen Kern hat; damit ist ϕ injektiv. ❑

15.6. **Lemma.** *Der Rang einer endlich erzeugten freien abelschen Gruppe ist eindeutig bestimmt.*

LEMMA Rang eind. bestimmt

Beweis. Angenommen, G ist frei abelsch vom Rang m und n mit $m < n$. Dann gibt es einen Isomorphismus $\phi\colon \mathbb{Z}^n \to \mathbb{Z}^m$. Analog wie bei Vektorräumen ist ϕ durch eine Matrix $A \in \mathrm{Mat}(m \times n, \mathbb{Z})$ gegeben (in der $j$ten Spalte von A steht das Bild von $(0, \dots, 0, 1, 0, \dots, 0)$, wo die Eins an der $j$ten Position steht). Wir können A auch als Matrix über $\mathbb{Q}$ betrachten; dann gilt $\mathrm{rk}(A) \leq m < n$, also hat A nichttrivialen Kern: Es gibt $(0, \dots, 0) \neq (x_1, \dots, x_n) \in \mathbb{Q}^n$ mit $A(x_1, \dots, x_n)^\top = \mathbf{0}$. Nach Multiplikation mit dem Hauptnenner der x_j können wir annehmen, dass $(x_1, \dots, x_n) \in \mathbb{Z}^n$ ist. Dann ist $\phi(x_1, \dots, x_n) = (0, \dots, 0)$, also kann ϕ nicht injektiv sein. Damit ist die Annahme zum Widerspruch geführt, und die Aussage des Lemmas muss richtig sein. ❑

15.7. **Definition.** Seien G eine Gruppe und $g \in G$. g heißt ein *Torsionselement*, wenn g endliche Ordnung hat. Die Gruppe G heißt *torsionsfrei*, wenn 1_G das einzige Torsionselement in G ist. ♢

DEF Torsionselement

torsionsfrei

Zum Beispiel sind $\mathbb{Z}$ und allgemeiner jede freie abelsche Gruppe torsionsfrei.

15.8. **Lemma.** *Ist G eine (additiv geschriebene) abelsche Gruppe, dann ist die Menge*

$$T = \{g \in G \mid \mathrm{ord}(g) < \infty\} = \{g \in G \mid \exists n \in \mathbb{Z}_{>0}\colon n \cdot g = 0\}$$

der Torsionselemente von G eine Untergruppe von G. Die Faktorgruppe G/T ist torsionsfrei.

Ist G endlich erzeugt, dann ist T endlich.

LEMMA Torsionsuntergruppe

Beweis. Es ist $0 \in T$. Da g und $-g$ dieselbe Ordnung haben (denn $\langle -g \rangle = \langle g \rangle$), ist T abgeschlossen unter Inversenbildung. Es bleibt zu zeigen, dass T auch unter der Addition abgeschlossen ist. Seien also $g, h \in T$. Dann gibt es $m > 0$, $n > 0$ mit $m \cdot g = n \cdot h = 0$. Es folgt

$$(mn) \cdot (g + h) = (mn) \cdot g + (mn) \cdot h = 0 + 0 = 0\,,$$

also ist $g + h \in T$. (Die erste Gleichheit benutzt, dass G abelsch ist.)

Sei nun $\pi\colon G \to G/T$ der kanonische Epimorphismus und sei $t \in G/T$ ein Torsionselement, etwa $n \cdot t = 0$ für ein $n > 0$. Dann gibt es $g \in G$ mit $\pi(g) = t$; es folgt $\pi(n \cdot g) = n \cdot t = 0$, also ist $n \cdot g \in \ker(\pi) = T$. Es gibt also $m > 0$ mit

$0 = m \cdot (n \cdot g) = (mn) \cdot g$; damit ist $g \in T$ und $t = \pi(g) = 0$. Außer 0 gibt es also keine Torsionselemente in G/T.

Sei jetzt G endlich erzeugt. Nach Satz 15.3 ist dann auch T endlich erzeugt; sei etwa $T = \langle t_1, \ldots, t_n \rangle$ und seien $k_1, \ldots, k_n$ die Ordnungen von $t_1, \ldots, t_n$. Jedes Element t von T kann geschrieben werden als

$$t = m_1 \cdot t_1 + m_2 \cdot t_2 + \ldots + m_n \cdot t_n$$

mit $m_1, \ldots, m_n \in \mathbb{Z}$; wegen $k_j \cdot t_j = 0$ kann man zusätzlich $0 \leq m_j < k_j$ erreichen. Es gibt dann aber nur endlich viele Möglichkeiten für $(m_1, \ldots, m_n)$, also muss T endlich sein. ❑

In nicht-abelschen Gruppen ist die Menge der Torsionselemente im Allgemeinen *keine* Untergruppe (Übung).

15.9. **Definition.** In der Situation von Lemma 15.8 heißt $G_{\text{tors}} = T$ die *Torsionsuntergruppe* von G. ♢

DEF Torsionsuntergruppe

15.10. **Lemma.** *Eine zyklische Gruppe $G = \langle g \rangle$ ist entweder isomorph zu $\mathbb{Z}$, wenn ihr Erzeuger g unendliche Ordnung hat, oder isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{Z}_{>0}$, wenn g Ordnung n hat.*

LEMMA zyklische Gruppen

Beweis. Wir schreiben G additiv und betrachten den Homomorphismus $\phi\colon \mathbb{Z} \to G$, $n \mapsto n \cdot g$. Aus Lemma 12.10 und Lemma 12.23 wissen wir, dass $\ker(\phi)$ trivial ist, wenn g unendliche Ordnung hat, sonst ist $\ker(\phi) = n\mathbb{Z}$ mit $\operatorname{ord}(g) = n$. Die Behauptung folgt jetzt aus dem Homomorphiesatz 14.6. ❑

Wir können jetzt einen Satz über die Struktur von endlich erzeugten abelschen Gruppen beweisen.

15.11. **Satz.** *Jede endlich erzeugte abelsche Gruppe $G = \langle g_1, \ldots, g_n \rangle$ ist isomorph zu einem direkten Produkt von n zyklischen Gruppen.*

SATZ Struktur von endl. erzeugten abelschen Gruppen

Beweis. Induktion über die Anzahl n der Erzeuger von G. Ist $n \leq 1$, dann ist die Behauptung klar (G ist trivial oder zyklisch). Sei also $n \geq 2$. Unser Ziel ist es, zu zeigen, dass man die Erzeuger so wählen kann, dass $G \cong \langle g_1, \ldots, g_{n-1} \rangle \times \langle g_n \rangle$ ist. Die Behauptung folgt dann aus der Induktionsannahme.

Sei dazu $\phi\colon \mathbb{Z}^n \to G$ die "Linearkombinationenabbildung". Wir betrachten die Menge aller nichttrivialen Relationen zwischen den Erzeugern, also

$$\begin{aligned} M &= \left\{(m_1, \ldots, m_n) \in \mathbb{Z}^n \mid m_1 \cdot g_1 + \ldots + m_n \cdot g_n = 0, (m_1, \ldots, m_n) \neq (0, \ldots, 0)\right\} \\ &= \ker(\phi) \setminus \{0_{\mathbb{Z}^n}\}\,. \end{aligned}$$

Ist $M = \emptyset$, dann ist nach Lemma 15.5 $G \cong \mathbb{Z}^n = \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n \text{ Faktoren}}$ ein Produkt von n zyklischen Gruppen. Wir können also $M \neq \emptyset$ annehmen. Sei $(m_1, \ldots, m_n) \in M$ mit $\min\{|m_j| \mid m_j \neq 0\}$ minimal. Nach eventueller Änderung der Reihenfolge der Erzeuger können wir annehmen, dass $|m_n|$ dieses Minimum ist, und nach eventuellem Ersetzen von g_n durch $-g_n$ können wir zusätzlich $m_n > 0$ annehmen. Für $1 \leq j < n$ schreiben wir $m_j = q_j m_n + r_j$ mit $0 \leq r_j < m_n$ und setzen

$$g_n' = q_1 \cdot g_1 + q_2 \cdot g_2 + \ldots + q_{n-1} \cdot g_{n-1} + g_n\,.$$

Dann ist $(g_1, \ldots, g_{n-1}, g'_n)$ ebenfalls ein Erzeugendensystem von G, und es gilt

$$r_1 \cdot g_1 + r_2 \cdot g_2 + \ldots + r_{n-1} \cdot g_{n-1} + m_n \cdot g'_n = 0\,.$$

Ist hier ein $r_j \neq 0$, dann haben wir (für das neue Erzeugendensystem) eine Relation mit kleinerem Minimum als m_n. Wir können dann wiederum ein neues Erzeugendensystem wählen usw. Da das Minimum jedes Mal echt kleiner wird, haben wir nach endlich vielen Schritten ein Erzeugendensystem erreicht (das wir der Einfachheit halber wieder mit $(g_1, \ldots, g_n)$ bezeichnen) mit der Eigenschaft, dass die Relation mit dem kleinsten Minimum die Form $m_n \cdot g_n = 0$ hat.

Dann ist $\langle g_n \rangle \cong \mathbb{Z}/m_n\mathbb{Z}$ (denn m_n muss die Ordnung von g_n sein), und die Abbildung

$$\psi\colon \langle g_1, \ldots, g_{n-1} \rangle \times \langle g_n \rangle \longrightarrow G, \quad (g, h) \longmapsto g + h$$

ist ein Isomorphismus: Es ist leicht zu sehen, dass ψ ein Homomorphismus ist (dazu verwendet man die Kommutativität von G). Weil G von $(g_1, \ldots, g_n)$ erzeugt wird, ist ψ auch surjektiv. Es bleibt zu zeigen, dass ψ injektiv ist. Sei dazu $(g, h) \in \ker(\psi)$. Dann ist $g = k_1 \cdot g_1 + \ldots + k_{n-1} \cdot g_{n-1}$ und $h = k_n \cdot g_n$ mit $k_1, \ldots, k_{n-1}, k_n \in \mathbb{Z}$ und $k_1 \cdot g_1 + \ldots + k_{n-1} \cdot g_{n-1} + k_n \cdot g_n = g + h = 0$. Dabei muss nun k_n ein Vielfaches von m_n sein: Schreibe $k_n = qm_n + r$ mit $0 \leq r < m_n$. Durch Subtraktion des q-Fachen der Relation $m_n \cdot g_n = 0$ können wir oben k_n durch r ersetzen. Da aber m_n das Minimum der Beträge der nichttrivialen Koeffizienten in allen Relationen ist, muss dann $r = 0$ sein. Es folgt $k_n = qm_n$ und damit $h = k_n \cdot g_n = 0$, also auch $g = -h = 0$. Somit ist $\ker(\psi)$ trivial und ψ injektiv.

Nach Induktionsannahme ist $\langle g_1, \ldots, g_{n-1} \rangle$ isomorph zu einem Produkt von $n-1$ zyklischen Gruppen; die Behauptung für G folgt. ❑

15.12. **Folgerung.** *Sei G eine endlich erzeugte abelsche Gruppe.*

FOLG torsionsfrei = frei

(1) *Ist G torsionsfrei, dann ist G frei.*

(2) *Es ist $G \cong G_{\text{tors}} \times \mathbb{Z}^n$, wobei G_{tors} endlich und $G/G_{\text{tors}} \cong \mathbb{Z}^n$ ist.*

(3) *Ist G frei vom Rang n und $U \leq G$ eine Untergruppe, dann ist U frei vom Rang $m \leq n$.*

Beweis.

(1) Nach Satz 15.11 ist G isomorph zu einem Produkt von nichttrivialen zyklischen Gruppen (triviale Faktoren können weggelassen werden). Ist G torsionsfrei, dann kann keiner der Faktoren die Form $\mathbb{Z}/n\mathbb{Z}$ mit $n > 0$ haben, also ist G isomorph zu einem Produkt von endlich vielen Faktoren $\mathbb{Z}$ und damit frei.

(2) Für beliebiges G können wir schreiben $G \cong T \times \mathbb{Z}^n$, wobei T das Produkt der endlichen zyklischen Faktoren ist. Dann ist

$$G_{\text{tors}} \cong (T \times \mathbb{Z}^n)_{\text{tors}} = T_{\text{tors}} \times \mathbb{Z}^n_{\text{tors}} = T \times \{(0, \ldots, 0)\} \cong T\,,$$

also ist $G \cong G_{\text{tors}} \times \mathbb{Z}^n$. Nach Lemma 15.8 ist G/G_{tors} torsionsfrei, also nach Teil (1) frei; damit ist $G/G_{\text{tors}} \cong \mathbb{Z}^m$ für ein $m \in \mathbb{Z}_{\geq 0}$. Wir müssen noch zeigen, dass $m = n$ ist. Die Komposition

$$G_{\text{tors}} \times \mathbb{Z}^n \xrightarrow{\cong} G \longrightarrow G/G_{\text{tors}} \cong \mathbb{Z}^m$$

ist surjektiv und hat Kern $G_{\text{tors}} \times \{(0,\dots,0)\}$. Nach dem Homomorphiesatz 14.6 ist also

$$\mathbb{Z}^n \cong (G_{\text{tors}} \times \mathbb{Z}^n)/(G_{\text{tors}} \times \{(0,\dots,0)\}) \cong \mathbb{Z}^m$$

und damit nach Lemma 15.6 $n = m$.

(3) Sei G frei vom Rang n, dann ist G insbesondere torsionsfrei. Damit ist auch jede Untergruppe U von G torsionsfrei, nach Teil (1) also frei. Nach Satz 15.3 kann U von höchstens n Elementen erzeugt werden, also ist der Rang m von U höchstens n. ❑

Um eine Klassifikation der endlich erzeugten abelschen Gruppen zu erhalten, genügt es also, die endlichen abelschen Gruppen zu klassifizieren. Dies wird von unserem Struktursatz noch nicht geleistet, denn es gilt zum Beispiel

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \qquad \text{oder} \qquad \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}\,;$$

die Darstellung als Produkt von zyklischen Gruppen ist also nicht eindeutig. Wir können sie jedoch eindeutig machen, wenn wir uns an den Chinesischen Restsatz erinnern.

LEMMA Zerlegung zyklischer Gruppen

15.13. **Lemma.** *Sei $n \in \mathbb{Z}_{>0}$ mit Primfaktorzerlegung $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Dann ist die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ isomorph zu $\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$.*

Beweis. Nach dem Chinesischen Restsatz 7.7 gilt die Isomorphie für die Faktorringe $\mathbb{Z}/n\mathbb{Z}$ bzw. $\mathbb{Z}/p_j^{e_j}\mathbb{Z}$ von $\mathbb{Z}$. Dieser Isomorphismus ist auch ein Isomorphismus der additiven Gruppen. ❑

* **SATZ** Klassifikation endlicher abelscher Gruppen

15.14. **Satz.** *Jede endliche abelsche Gruppe G ist isomorph zu einem Produkt von zyklischen Gruppen, deren Ordnung eine Primzahlpotenz ist. Dieses Produkt ist bis auf die Reihenfolge der Faktoren eindeutig bestimmt.*

Beweis. Nach Satz 15.11 ist G isomorph zu einem Produkt zyklischer Gruppen; da G endlich ist, müssen diese zyklischen Gruppen ebenfalls endlich sein, sind also von der Form $\mathbb{Z}/n\mathbb{Z}$. Nach Lemma 15.13 kann jeder solche Faktor wiederum als Produkt von zyklischen Gruppen von Primzahlpotenzordnung geschrieben werden.

Zur Eindeutigkeit: Für eine beliebige abelsche Gruppe G' und $m \in \mathbb{Z}_{>0}$ setzen wir $mG' = \{m \cdot g' \mid g' \in G'\}$; mG' ist eine Untergruppe von G'. Ist $G' = \mathbb{Z}/n\mathbb{Z}$, dann ist mG' als Untergruppe einer zyklischen Gruppe ebenfalls zyklisch. Außerdem gilt $(G' : mG') = \operatorname{ggT}(m,n)$, denn das Bild von $m\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ besteht aus allen Restklassen, die durch eine Zahl der Form $am + bn$ repräsentiert werden; diese Zahlen sind genau die Vielfachen von $\operatorname{ggT}(m,n)$. Ist G' das Produkt der zyklischen Gruppen $\mathbb{Z}/n_j\mathbb{Z}$, $j = 1,\dots,k$, dann ist entsprechend $(G' : mG') = \prod_{j=1}^k \operatorname{ggT}(m,n_j)$.

Für $G \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$ (mit Primzahlen $p_1,\dots,p_k$, die nicht verschieden sein müssen) und eine Primzahl q ergibt sich dann

$$(G : q^f G) = \prod_{j=1}^{k} \operatorname{ggT}(p_j^{e_j}, q^f) = q^{\sum_{j:p_j=q} \min\{e_j,f\}}$$

und daher für $f \geq 1$

$$\frac{(G : q^f G)}{(G : q^{f-1} G)} = q^{\sum_{j:p_j=q}(\min\{e_j,f\}-\min\{e_j,f-1\})} = q^{\#\{j \mid p_j=q, e_j \geq f\}}$$

(denn $\min\{e,f\} - \min\{e,f-1\} = 0$ für $e < f$ und $= 1$ für $e \geq f$). Aus diesen Quotienten (für $f = 1, 2, \ldots$) können wir also ablesen, wie viele Faktoren $\mathbb{Z}/q^e\mathbb{Z}$ im Produkt vorkommen. Da das für jede Primzahl q gilt und die Quotienten nur von G abhängen, sind die Häufigkeiten der Faktoren durch G eindeutig bestimmt. ❑

BSP abelsche Gruppen der Ordnung 72

15.15. **Beispiel.** Mithilfe dieses Satzes lassen sich Fragen beantworten wie „Wie viele abelsche Gruppen der Ordnung 72 gibt es bis auf Isomorphie?“

Dazu schreiben wir $72 = 2^3 \cdot 3^2$. Eine abelsche Gruppe G der Ordnung 72 ist isomorph zu einem Produkt $\mathbb{Z}/2^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/2^{e_k}\mathbb{Z} \times \mathbb{Z}/3^{f_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/3^{f_l}\mathbb{Z}$ mit $2^{e_1+\ldots+e_k} \cdot 3^{f_1+\ldots+f_l} = 72$, also $e_1 + \ldots + e_k = 3$ und $f_1 + \ldots + f_l = 2$. Da es auf die Reihenfolge der Faktoren nicht ankommt, können wir $e_1 \geq \ldots \geq e_k > 0$ und $f_1 \geq \ldots \geq f_l > 0$ annehmen. Dann gibt es für die e_i genau die drei Möglichkeiten $(1,1,1)$, $(2,1)$ und (3) und für die f_j die beiden Möglichkeiten $(1,1)$ und (2). Diese können wir beliebig miteinander kombinieren; das liefert $3 \cdot 2 = 6$ verschiedene Isomorphietypen:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z},$$
$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad \text{und} \quad \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}\,. \qquad \clubsuit$$

Nicht-abelsche Gruppen gegebener Ordnung n zu klassifizieren, ist dagegen sehr viel schwieriger. Zum Beispiel gibt es 44 Isomorphieklassen nicht-abelscher Gruppen der Ordnung 72 und 2313 Isomorphieklassen nicht-abelscher Gruppen der Ordnung 128 (dazu 15 abelsche Isomorphieklassen). Gerade die Zahl der Isomorphieklassen von Gruppen der Ordnung 2^n wächst rasant mit n: Für $n = 8$ hat man 56 092 und für $n = 9$ bereits 10 494 213 Isomorphieklassen!

Das obige Beispiel motiviert die folgende Definition.

DEF Partitionszahl

15.16. **Definition.** Sei $n \in \mathbb{Z}_{\geq 0}$. Die *Partitionszahl* von n, $p(n)$, ist die Anzahl der verschiedenen Möglichkeiten, n ohne Berücksichtigung der Reihenfolge als Summe positiver ganzer Zahlen zu schreiben. ♢

Formaler kann man definieren (λ_m zählt, wie oft m in der Summe vorkommt):

$$p(n) = \#\{(\lambda_1, \lambda_2, \ldots) \in \mathbb{Z}_{\geq 0}^{\mathbb{N}} \mid \sum_{j=1}^{\infty} j\lambda_j = n\}$$

Man erhält die folgende Tabelle von Werten für kleine n:

n	0	1	2	3	4	5	6	7	8	9
$p(n)$	1	1	2	3	5	7	11	15	22	30

Die Partitionszahlen bilden eine sehr interessante Zahlenfolge. Sie treten als Koeffizienten der folgenden Potenzreihe auf:

$$\sum_{n=0}^{\infty} p(n) z^n = \prod_{m=1}^{\infty} \frac{1}{1 - z^m}$$

(Als Gleichung zwischen formalen Potenzreihen bekommt man das durch Ausmultiplizieren der geometrischen Reihen auf der rechten Seite, denn der Koeffizient von z^n ist genau durch die Anzahl der Lösungen von $\sum_{j=1}^{\infty} j\lambda_j = n$ gegeben. Beide Seiten konvergieren absolut für $|z| < 1$, also gilt die Gleichheit in diesem Bereich auch als Funktionen von z.)

Der Pentagonalzahlensatz von Euler gibt die Relation

$$\prod_{m=1}^{\infty}(1-z^m)=\sum_{k\in\mathbb{Z}}(-1)^k z^{k(3k-1)/2}=1-z-z^2+z^5+z^7-\dots\,.$$

Daraus erhält man

$$\left(\sum_{k\in\mathbb{Z}}(-1)^k z^{k(3k-1)/2}\right)\left(\sum_{n=0}^{\infty}p(n)z^n\right)=1\,,$$

was sich in die Rekursion $p(0)=1$ und für $n>0$

$$p(n)=\sum_{0\neq k\in\mathbb{Z},k(3k-1)\leq 2n}(-1)^{k-1}p\big(n-\tfrac{k(3k-1)}{2}\big)=p(n-1)+p(n-2)-p(n-5)-p(n-7)+\dots$$

übersetzt. Damit lassen sich die Zahlen $p(n)$ recht schnell berechnen.

Eine andere interessante Eigenschaft der Partitionszahlen ist ihr Wachstumsverhalten. Mithilfe der Potenzreihe oben kann man Folgendes zeigen:

$$\lim_{n\to\infty}\frac{p(n)}{e^{\pi\sqrt{2n/3}}/(4n\sqrt{3})}=1$$

Die Anzahl der Dezimalziffern von $p(n)$ wächst also etwa wie $\sqrt{n}$ (und damit z.B. deutlich langsamer als die der Fibonacci-Zahlen).

Das Beispiel lässt sich dann verallgemeinern:

15.17. **Folgerung.** *Sei $n\in\mathbb{Z}_{>0}$ mit Primfaktorzerlegung $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$. Dann gibt es genau $p(e_1)p(e_2)\cdots p(e_k)$ Isomorphieklassen von abelschen Gruppen der Ordnung n.*

FOLG Anzahl abelscher Gruppen gegebener Ordnung

Beweis. Wie im Beispiel gibt es für die zyklischen Faktoren mit Ordnung eine p_j-Potenz genau $p(e_j)$ Möglichkeiten. Die Möglichkeiten für die verschiedenen Primteiler können beliebig miteinander kombiniert werden, also erhält man insgesamt gerade $p(e_1)p(e_2)\cdots p(e_k)$ verschiedene Produkte von zyklischen Gruppen von Primzahlpotenzordnung, sodass das Produkt Ordnung n hat. ❑

Zum Abschluss geben wir noch eine zweite Variante des Klassifikationssatzes. In Satz 15.14 haben wir die Darstellung als Produkt zyklischer Gruppen gegeben, die am meisten nichttriviale Faktoren hat. Man kann auch eine Version formulieren, die möglichst wenige Faktoren benutzt. Um die resultierende Darstellung eindeutig zu machen, muss man noch eine zusätzliche Bedingung an die Ordnungen der Faktoren stellen.

15.18. **Satz.** *Jede endliche abelsche Gruppe G ist isomorph zu einem Produkt*

$$\mathbb{Z}/d_1\mathbb{Z}\times\mathbb{Z}/d_2\mathbb{Z}\times\dots\mathbb{Z}/d_m\mathbb{Z}$$

von zyklischen Gruppen, deren Ordnungen $d_1,d_2,\dots,d_m$ zusätzlich die Bedingung $1<d_1\mid d_2\mid\dots\mid d_m$ erfüllen. Die Ordnungen $(d_1,d_2,\dots,d_m)$ sind eindeutig bestimmt; m ist die minimale Zahl von Erzeugern von G.

SATZ Klassifikation endlicher abelscher Gruppen

Beweis. Dazu überlegt man sich, dass die einzige Möglichkeit, die zyklischen Faktoren in Satz 15.14 mithilfe des Chinesischen Restsatzes zu zyklischen Gruppen zusammenzufassen, die die Zusatzbedingung erfüllen, darin besteht, jeweils die höchsten, die zweithöchsten, ... vorkommenden Potenzen aller Primteiler der Gruppenordnung miteinander zu kombinieren. Das liefert dann die zyklischen Faktoren der Ordnung d_m, d_{m-1} usw.

Dass G von m Elementen erzeugt werden kann, ist offensichtlich. Sei nun p ein Primteiler von d_1. Dann ist $G/pG \cong (\mathbb{Z}/p\mathbb{Z})^m$; die Gruppe rechts ist die additive Gruppe des m-dimensionalen $\mathbb{F}_p$-Vektorraums $\mathbb{F}_p^m$ und kann deswegen nicht von weniger als m Elementen erzeugt werden. Da jedes Erzeugendensystem von G auf ein Erzeugendensystem von G/pG abgebildet wird, kann auch G nicht von weniger als m Elementen erzeugt werden. ❑

15.19. **Beispiel.** Für die oben klassifizierten Isomorphietypen von abelschen Gruppen der Ordnung 72 sieht die alternative Klassifizierung so aus: **BSP** abelsche Gruppen der Ordnung 72

$$\begin{aligned}
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \\
\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \\
\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} &\cong \mathbb{Z}/72\mathbb{Z}
\end{aligned}$$

♣

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, sodass 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, sodass 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.