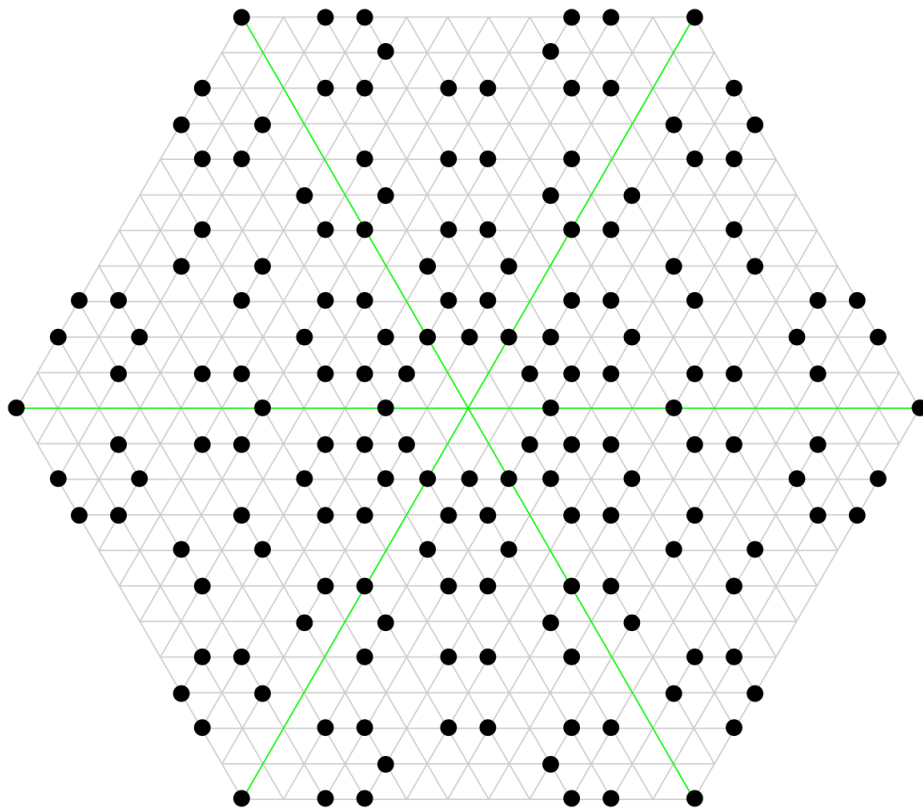


Algebra 1/2

Tobias Fritz (tobias.fritz@uibk.ac.at)

7. Oktober 2026

(Studienjahr 2025/26)



Die Eisenstein-Primzahlen:

Primelemente im Ring der komplexen Zahlen der Form $a + be^{2\pi i/3}$ (mit $a, b \in \mathbb{Z}$)

Dieses Werk ist lizenziert unter einer [Creative Commons „Namensnennung – Nicht-kommerziell – Weitergabe unter gleichen Bedingungen 4.0 International“](#) Lizenz.



Inhaltsverzeichnis

1	Einführung	4
1.1	Algebra und das Lösen von Gleichungen	4
1.2	Algebraische Strukturen	6
2	Gruppentheorie	8
2.1	Definitionen und Beispiele	8
2.2	Homomorphismen und Isomorphismen	16
2.3	Der erste Isomorphiesatz	26
2.4	Gruppenwirkungen	29
2.5	Auflösbare Gruppen	36
2.6	Endlich erzeugte abelsche Gruppen	37
3	Ordnungstheorie	47
3.1	Prägeordnete Mengen	47
3.2	Galois-Zusammenhänge	50
3.3	Binäre Suprema und Infima	55
4	Ringe	57
4.1	Definitionen und erste Beispiele	57
4.2	Unterringe	65
4.3	Ringhomomorphismen, Ideale und der Isomorphiesatz	66
4.4	Idealarithmetik und Chinesischer Restsatz	74
4.5	Integritätsringe und Teilbarkeitstheorie	78
4.6	Euklidische Ringe	82
4.7	Hauptidealringe	84
4.8	Faktorielle Ringe und Faktorisierungstheorie	85
4.9	Irreduzibilitätskriterien für Polynome	89
5	Körper	91
5.1	Grundlagen	91
5.2	Körpererweiterungen	95
5.3	Das Minimalpolynom	100
5.4	Zerfällungskörper	104
5.5	Galoisgruppen und Fixkörper	109
5.6	Normale und separable Erweiterungen	118
5.7	Der Hauptsatz der Galoistheorie	121
5.8	Unlösbarkeit von Gleichungen fünften Grades	122
	Index	125
	References	127

Vorwort

Feedback zu diesem Skript über das Forum in OLAT ist immer willkommen, insbesondere wenn etwas unklar formuliert ist oder wenn Fehler entdeckt werden.

Literatur

Andere wertvolle einführende Literatur zu Algebra ist folgende:

- ▷ Paolo Aluffi's "Algebra: Notes from the Underground" [1] ist ein sehr gutes Buch, welches neben den formalen Details auch die Motivation und Intuition hinter den Konzepten erklärt.
- ▷ Das Skript von Tim Netzer [5] bietet ebenfalls eine sehr gute Einführung mit etwas anderen Schwerpunkten.

Prüfungsrelevanz

Die Einführung (Abschnitt 1) ist nicht prüfungsrelevant.

$$x_j = -\frac{1}{3a} \left(b + \omega^j C + \frac{R}{\omega^j C} \right), \quad j = 0, 1, 2.$$

$$C = \sqrt[3]{\frac{S + \sqrt{S^2 - 4R^3}}{2}}, \quad R = b^2 - 3ac, \quad S = 2b^3 - 9abc + 27a^2d,$$

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

Abbildung 1: Lösungsformel für allgemeine Gleichungen dritten Grades (1.1).¹

1 Einführung

1.1 Algebra und das Lösen von Gleichungen

Das Wort *Algebra* stammt vom arabischen Wort *الجبر* (*al-jabr*), welches so viel wie “Vervollständigung” oder “Zusammenfügung” bedeutet und aus dem Titel eines im Jahr 820 entstandenen Buches des persischen Mathematikers Muhammad ibn Mūsā al-Chwārizmī stammt, welches als erstes Lehrbuch der Algebra im Sinne der heutigen Schulmathematik gilt. Er beschreibt dort unter anderem das Lösen von quadratischen Gleichungen.

In seiner modernen Verwendung bezieht sich das Wort **Algebra** auf ein abstrakteres Teilgebiet der Mathematik. Gemeint ist damit die Untersuchung von Strukturen, die durch eine Menge und eine oder mehrere Verknüpfungen (Operationen) auf dieser Menge definiert sind. Dazu gehört insbesondere die bereits bekannte **lineare Algebra**, die sich mit Vektorräumen und linearen Abbildungen beschäftigt. In diesem Fall sind die betrachteten Verknüpfungen also die Addition von Vektoren und die skalare Multiplikation.

Die Relevanz der linearen Algebra ergibt sich vor allem daraus, dass man eine elegante und sehr nützliche Theorie zur Lösung von linearen Gleichungssystemen erhält. Obwohl in vielen Anwendungsgebieten das Lösen von linearen Gleichungssystemen von zentraler Bedeutung ist, so sind doch viele Gleichungen, die in der mathematischen Praxis auftreten, *nicht* linear. Dazu gehören natürlich insbesondere die bereits erwähnten quadratischen Gleichungen in einer Variablen, deren Lösungsformel aus der Schulmathematik bekannt ist.

In vielen Anwendungen treten aber auch kompliziertere Gleichungen auf, die weder linear noch quadratisch sind. Zum Beispiel die *Van-der-Waals-Gleichung* aus der Thermodynamik, die den Zusammenhang zwischen Druck p , Volumen V und Temperatur T eines Gases beschreibt:

$$\left(p + a \frac{n^2}{V^2} \right) (V - nb) = nRT.$$

Wollen wir diese Gleichung nach V auflösen, zum Beispiel weil wir die anderen Größen gegeben haben, dann helfen uns weder die Schulmathematik noch die lineare Algebra weiter, denn nach Multiplikation mit V^2 und Ausmultiplizieren erhalten wir eine Gleichung dritten Grades in V ! Somit stellt sich die Frage:

1.1.1 Problem. *Gibt es eine allgemeine Lösungsformel für Gleichungen dritten Grades*

$$ax^3 + bx^2 + cx + d = 0 \quad ? \quad (1.1)$$

Die Antwort ist ja, und eine solche Lösungsformel wurde bereits im 16. Jahrhundert gefunden. Sie ist allerdings deutlich komplizierter als die bekannte Lösungsformel für quadratische Gleichungen und in Abbildung 1 dargestellt.

In der Formel für C in Abbildung 1 taucht eine Quadratwurzel und eine dritte Wurzel auf. Diese sind im Allgemeinen nicht eindeutig: gemeint ist jeweils *irgendeine* Zahl, deren dritte bzw. zweite Potenz die jeweilige Zahl unter der Wurzel ergibt. Denn insbesondere mit komplexen Koeffizienten a, b, c, d gibt es ja keine natürliche Wahl von den Wurzeln. Aber bekommt man nicht andere Lösungen des Gleichungssystems, falls man andere Wurzeln wählt?

Zur Beantwortung dieser Frage lohnt es sich, noch einmal die Lösungsformel für quadratische Gleichungen zu betrachten:

$$x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Hier ist es so, dass die Wahl der Wurzel nur bestimmt, welche Lösung man als x_1 und welche man als x_2 bezeichnet. Mit anderen Worten: eine andere Wahl der Wurzel *permutiert* die Lösungen, lässt die Lösungsmenge aber unverändert. Genauso ist es bei der Lösungsformel für kubische Gleichungen aus Abbildung 1: eine andere Wahl der Quadratwurzel vertauscht zwei der drei Lösungen (und hält die dritte fest), und eine andere Wahl der dritten Wurzel implementiert die zyklische Permutation

$$x_0 \mapsto x_1, \quad x_1 \mapsto x_2, \quad x_2 \mapsto x_0 \quad (1.2)$$

oder ihr inverses

$$x_0 \mapsto x_2, \quad x_2 \mapsto x_1, \quad x_1 \mapsto x_0. \quad (1.3)$$

1.1.2 Übung. *Rechne dies nach.*

Wir sehen also, dass das Lösen von Gleichungen eng mit **Permutationen** zusammenhängt, welche die Lösungen miteinander vertauschen. Wie wir noch sehen handelt es sich bei diesen Permutationen um **Symmetrien** der Gleichungen. Dies besser zu verstehen ist eines der Hauptziele dieser Vorlesung.

Da wir nun einen Einblick in das Lösen von Gleichungen dritten Grades gewonnen haben, stellt sich die Frage, ob es auch eine Lösungsformel für Gleichungen vierten Grades gibt. Dies ist tatsächlich der Fall, und die Lösungsformel ist noch wesentlich komplizierter als die für Gleichungen dritten Grades. Deswegen werden wir sie hier nicht hinschreiben. Wieder ist es so, dass in der Lösungsformel Wurzeln auftauchen, und dass die Wahl der Wurzeln die Lösungen permutiert.

Jetzt würde man vielleicht erwarten, dass es so weitergeht: auch für Gleichungen fünften Grades wird es dann ja wohl eine Lösungsformel geben, oder? Interessanterweise ist dies *nicht* der Fall: man kann streng beweisen, dass es für Gleichungen fünften Grades *keine* Lösungsformel gibt, die nur aus den Grundrechenarten und dem Ziehen von Wurzeln besteht. Dies ist eines der berühmtesten Resultate der Algebra und beruht auf der **Galoisttheorie**, die wir in Abschnitt 5 behandeln werden. Hier sei zunächst nur darauf hingewiesen, dass bereits das Angeben einer mathematisch präzisen Definition von “Lösungsformel” nicht offensichtlich ist.

Zusammenfassend können wir also sagen, dass die Theorie der polynomialen Gleichungen in einer Variablen ein zentrales Thema der Algebra ist, weil die in Abschnitt 5 behandelte Körpertheorie die dafür notwendigen Werkzeuge bereitstellt. Und wie bereits gesagt werden lineare Gleichungssysteme in mehreren Variablen durch die lineare Algebra abgedeckt. Der nächste logische Schritt wäre dann also, beides zu kombinieren und sich mit *nichtlinearen* Gleichungssystemen in *mehreren* Variablen zu beschäftigen. Dies ist das zentrale Thema der *algebraischen Geometrie*, die oft im Masterstudium behandelt wird und auf der Ring- und Körpertheorie aus den Abschnitten 4 und 5 aufbaut.

Zusammenfassend erhalten wir also folgendes Schema von mathematischen Disziplinen, die sich mit dem Lösen von Gleichungen beschäftigen:

	linear	polynomial
Eine Variable und eine Gleichung	Schulmathematik	Körpertheorie
Mehrere Variablen oder mehrere Gleichungen	lineare Algebra	Algebraische Geometrie

Natürlich gibt es auch noch viele nichtlineare Gleichungen, die in der Praxis auftreten und welche nicht polynomial sind. Auf Gleichungen dieser Art können die Werkzeuge der Algebra oft auch angewendet werden. Wir werden dies aber hier nicht betrachten, und für die praktische Anwendung sind andere Methoden meist besser geeignet.²

²Selbst zum numerischen Lösen von polynomialen Gleichungen dritter Ordnung und in einer Variablen ist die in Abbildung 1 angegebene Lösungsformel oft nicht die beste Wahl.

1.2 Algebraische Strukturen

Wie schon erwähnt beschäftigt sich die Algebra mit Strukturen, die durch eine Menge und eine oder mehrere Verknüpfungen (Operationen) auf dieser Menge definiert sind. Dazu gehören zum Beispiel die Ringe und Körper, wo die betrachteten Verknüpfungen die Addition und Multiplikation sind. Der Einfachheit halber beginnen wir aber mit Strukturen, bei denen es nur eine Verknüpfung gibt.

1.2.1 Definition. Ein **Magma** ist eine Menge M zusammen mit einer Abbildung

$$\begin{aligned} * : M \times M &\longrightarrow M \\ (x, y) &\longmapsto x * y. \end{aligned}$$

Ein Magma ist also einfach eine Menge, auf der eine Verknüpfung definiert ist, die zwei Elemente der Menge wieder zu einem Element der Menge kombiniert.

Ein Magma kann zusätzliche **Rechengesetze** erfüllen. Damit gemeint sind bestimmte Umformungsregeln, die für alle Elemente der Menge erfüllt sein müssen falls das Rechengesetz gilt. Wichtige Beispiele für Rechengesetze sind insbesondere die folgenden:

▷ **Assoziativität:** Für alle $x, y, z \in M$ gilt

$$(x * y) * z = x * (y * z). \quad (1.4)$$

▷ **Kommutativität:** Für alle $x, y \in M$ gilt

$$x * y = y * x. \quad (1.5)$$

▷ **Idempotenz:** Für alle $x \in M$ gilt

$$x * x = x. \quad (1.6)$$

▷ **Selbstdistributivität:** Für alle $x, y, z \in M$ gilt

$$x * (y * z) = (x * y) * (x * z). \quad (1.7)$$

1.2.2 Beispiel. (a) Die Menge der ganzen Zahlen $\mathbb{Z}$ mit der Addition $+$ ist ein Magma. Dieses erfüllt die Assoziativität, die Kommutativität, aber weder die Idempotenz noch die Selbstdistributivität.

(b) Eine beliebige Menge M wird zu einem Magma durch die Verknüpfung

$$x * y := x.$$

Dieses Magma erfüllt die Assoziativität, Idempotenz und die Selbstdistributivität, aber nicht die Kommutativität (falls M mehr als ein Element hat).

(c) Die natürlichen Zahlen $\mathbb{N}$ werden durch

$$x * y := x^y$$

zu einem Magma. Dieses erfüllt keines der oben genannten Rechengesetze. Stattdessen gilt folgendes etwas exotischeres Rechengesetz:

$$(x * y) * z = (x * z) * y.$$

Denn bekanntermaßen ist $(x^y)^z = x^{yz} = x^{zy} = (x^z)^y$.

(d) Die reellen Zahlen $\mathbb{R}$ werden durch

$$x * y := \max(x, y)$$

zu einem Magma. Dieses erfüllt alle der oben genannten Rechengesetze.

1.2.3 Bemerkung. Manchmal gibt es überraschende Implikationen zwischen verschiedenen Rechengesetzen. So gilt zum Beispiel die Implikation

$$(x * y) * x = y \quad \forall x, y \in M \quad \implies \quad x * (y * x) = y \quad \forall x, y \in M.$$

Der Beweis ist wie folgt:

$$\underline{x} * (y * x) = (\overline{(y * x) * y}) * \overline{(y * x)} = y.$$

Wie durch die Unterstreichung angedeutet, wurde im ersten Schritt das angenommene Rechengesetz mit x und y vertauscht angewendet, also $x = (y * x) * y$. Im zweiten Schritt wurde es dann mit $x * y$ anstelle von x angewendet (oberstrichen). Dies ist erlaubt, da das x im Rechengesetz ja beliebig gewählt werden darf.

1.2.4 Bemerkung. Die Verknüpfung in einem Magma ist **binär**, d.h. sie verknüpft jeweils zwei Elemente miteinander. Es gibt aber auch Verknüpfungen, die mehr als zwei Elemente miteinander verknüpfen. Betrachten wir zum Beispiel die Abbildung, welche jedem Dreieck seinen Inkreismittelpunkt zuordnet. Wenn wir ein Dreieck als durch seine Ecken gegeben betrachten, dann ist diese Abbildung von der Form³

$$\mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2.$$

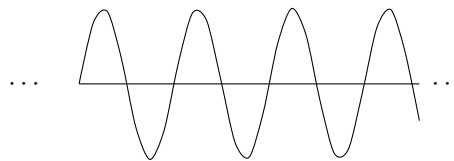
Dies ist also eine Verknüpfung, die *drei* Elemente des $\mathbb{R}^2$ miteinander kombiniert und ein neues Element des $\mathbb{R}^2$ ergibt.

Wir werden uns im Folgenden aber auf binäre Verknüpfungen beschränken. Denn diese sind in der mathematischen Praxis am wichtigsten, und viele Verknüpfungen mit mehr als zwei Argumenten können auf binäre Verknüpfungen zurückgeführt werden. Es ist etwas unklar, ob dies nur deshalb gilt, weil binäre Verknüpfungen mit dem menschlichen Verstand leichter zu erfassen sind und komplexere Verknüpfungen deshalb seltener untersucht werden, oder ob es einen tieferen Grund dafür gibt.

³Damit dies der Fall ist, muss der Inkreismittelpunkt auch für ausgeartete Dreiecke definiert sein, also wenn alle drei Ecken auf einer Geraden liegen oder sogar zusammenfallen. Die Frage, wie in diesen Fällen der Inkreismittelpunkt definiert ist, spielt für uns hier jedoch keine Rolle.



(a) Ein Muster mit Translationssymmetrie und Gleitspiegelungssymmetrie: sowohl durch eine Translation als auch durch eine geeignete Gleitspiegelung wird das Muster auf sich selber abgebildet.



(b) Hier gibt es zusätzlich noch eine Rotationssymmetrie: das Muster wird durch eine 180° Rotation um eine Nullstelle auf sich selber abgebildet.



(c) Ein Ornament (Fries) aus der Architektur. Welcher der beiden anderen Symmetrien entspricht dies?

Abbildung 2: Muster mit verschiedenen Symmetriegruppen.

2 Gruppentheorie

Die Gruppentheorie kann als die mathematische Untersuchung von Symmetrien verstanden werden. Symmetrien begegnen uns überall in der Natur, in der Kunst und in der Architektur. So sind z.B. Ornamente in der Architektur oft durch verschiedene Symmetrien gekennzeichnet. In Abbildung 2 sind drei Muster mit zwei verschiedenen Typen von Symmetrien dargestellt. Allen gemeinsam ist, dass eine geeignete Translation nach links oder rechts das jeweilige Muster auf sich selber abbildet. Ebenso kann man durch eine *Gleitspiegelung*, also eine Spiegelung an einer Achse kombiniert mit einer Translation um die halbe Länge, alle drei Muster auf sich selber abbilden.

In (b) gibt es aber noch eine weitere Symmetrie, die (a) nicht hat, nämlich eine 180° -Drehung um eine geeignete Stelle (Nullstelle der Kurve). Denn die Füße in (a) zeigen alle nach rechts, so dass eine Drehung das Muster nicht auf sich selber abbilden kann, während es in (b) keine Unterscheidung zwischen links und rechts gibt. In gruppentheoretischer Sprache können wir sagen, dass (a) und (b) verschiedene *Symmetriegruppen* haben.

2.1 Definitionen und Beispiele

Die Definition von Gruppe entsteht durch Abstraktion der Eigenschaften von Symmetrien. Zum Beispiel ist es eine grundlegende Eigenschaft von Symmetrien, dass die *Hintereinanderausführung* zweier Symmetrien wieder eine Symmetrie ist. Dies führt dazu, dass die Menge der Symmetrie mit der Hintereinanderausführung als Verknüpfung ein Magma bildet. Auf diese Weise bekommt man aber nicht beliebige Magmas, sondern nur Magmas mit bestimmten besonders schönen Eigenschaften wie folgt.

2.1.1 Definition. Ein **Monoid** ist ein Tripel $(M, \cdot, e)$ bestehend aus einem Magma $(M, \cdot)$ und einem Element $e \in M$, so dass gilt:

(a) Die Verknüpfung $\cdot$ ist assoziativ, erfüllt also (1.4).

(b) Für alle $x \in M$ gilt

$$x \cdot e = x = e \cdot x.$$

Das Element e heißt dabei auch **neutrales Element**.

2.1.2 Bemerkung. In jedem Monoid ist das neutrale Element eindeutig.⁴ Denn falls e' ebenfalls ein neutrales Element ist, dann erhalten wir

$$e' = e \cdot e' = e,$$

⁴Dies gilt (mit dem gleichen Beweis) sogar noch allgemeiner in jedem Magma mit einem neutralen Element.

wobei wir im ersten Schritt die Neutralität von e und im zweiten die von e' verwendet haben.

In der Praxis wird aufgrund der Eindeutigkeit das neutrale Element meist nicht explizit angegeben, denn es ist ja bereits durch die Angabe der Verknüpfung $\cdot$ eindeutig festgelegt. Um zu beweisen, dass eine gegebene Verknüpfung auf einer Menge eine Monoidstruktur definiert, muss man also nur die Assoziativität und die Existenz eines neutralen Elements nachweisen.

Unser erstes Beispiel zeigt, dass der Begriff des Monoids nicht nur für die Beschreibung von Symmetrien relevant ist, sondern auch arithmetische Operationen erfasst.

2.1.3 Beispiel. (a) Die natürlichen Zahlen $\mathbb{N}$ bilden ein Monoid bezüglich der Multiplikation $\cdot$ mit 1 als neutralem Element.

(b) Andererseits ist $\mathbb{N}$ auch ein Monoid bezüglich $+$ mit 0 als neutralem Element.

Obwohl wir in der allgemeinen Theorie die Verknüpfung in einem Monoid als Multiplikation schreiben und entsprechende Terminologie verwenden, kann es sich dabei auch um eine Addition handeln!

(c) Analog können wir auch alle anderen Zahlensysteme wie $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ als Monoide betrachten, sowohl bezüglich Addition als auch bezüglich Multiplikation.

2.1.4 Beispiel. Für eine beliebige Menge A sei A^* die Menge der endlichen Folgen von Elementen aus A . Dann ist A^* ein Monoid bezüglich der Konkatenation von Folgen,

$$(a_1, \dots, a_m) \cdot (b_1, \dots, b_n) := (a_1, \dots, a_m, b_1, \dots, b_n),$$

wobei die leere Folge $()$ als neutrales Element dient. Dieses Monoid wird z.B. in vielen Programmiersprachen verwendet, wo die Folgen als “Strings” und A als “Alphabet” bezeichnet werden. Die Konkatenation von Strings ist eine wichtige Operation, die z.B. in `Python` als “+” geschrieben wird.

Wir kehren zurück zur Betrachtung von Symmetrien. Wie wir noch genauer sehen werden sind Symmetrien Abbildungen, die eine bestimmte Zusatzstruktur erhalten, welche je nach Kontext variiert. Wie schon angedeutet ist die relevante Verknüpfung die Hintereinanderausführung von Abbildungen. Deshalb ist folgendes Beispiel zentral.

2.1.5 Beispiel. Sei X eine beliebige Menge und M_X die Menge aller Abbildungen $X \rightarrow X$ mit der Hintereinanderausführung $\circ$ als Verknüpfung. Für $f, g : X \rightarrow X$ ist dabei $g \circ f$ definiert als die Abbildung mit

$$(g \circ f)(x) = g(f(x)).$$

Dann ist M_X bezüglich $\circ$ ein Monoid, wie wir im folgenden nachweisen.

Falls $f, g, h : X \rightarrow X$ Abbildungen sind, dann müssen wir die Assoziativität

$$h \circ (g \circ f) = (h \circ g) \circ f$$

zeigen. Zwei Funktionen sind genau dann gleich, wenn sie auf allen Elementen des Definitionsbereichs die gleichen Werte annehmen. Somit reicht es aus zu zeigen, dass beide Seiten auf jedem $x \in X$ den gleichen Wert liefern. Das Einsetzen von x liefert jeweils

$$\begin{aligned} (h \circ (g \circ f))(x) &= h((g \circ f)(x)) = h(g(f(x))), \\ ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) = h(g(f(x))). \end{aligned}$$

Da die rechten Seiten übereinstimmen, ist somit die Assoziativität gezeigt.

Das neutrale Element ist die **Identitätsabbildung** $\text{id}_X : X \rightarrow X$, definiert als $\text{id}_X(x) = x$ für alle $x \in X$. Zum Nachweis desselben müssen wir zeigen, dass

$$f \circ \text{id}_X = f = \text{id}_X \circ f$$

für alle $f : X \rightarrow X$. Dafür setzen wir wieder ein beliebiges $x \in X$ ein, und bekommen

$$(f \circ \text{id}_X)(x) = f(\text{id}_X(x)) = f(x),$$

und analog

$$(\text{id}_X \circ f)(x) = \text{id}_X(f(x)) = f(x).$$

Somit ist gezeigt, dass id_X das neutrale Element ist.

2.1.6 Bemerkung. Wie es für die Multiplikation von Zahlen oder Matrizen allgemein üblich ist, lassen wir auch in einem Monoid $(M, \cdot)$ das Symbol für die Verknüpfung oft weg und schreiben zwei Elemente einfach direkt nebeneinander,

$$xy := x \cdot y.$$

Das Assoziativgesetz nimmt somit die visuell einfachere Form

$$\boxed{x(yz) = (xy)z \quad \forall x, y, z \in M}$$

an. Dementsprechend schreiben wir auch vereinfacht xyz . Dieser Ausdruck kann entweder als $x(yz)$ oder als $(xy)z$ gelesen werden. Aufgrund der Assoziativität stimmen diese beiden Lesarten überein.

Die analoge Aussage gilt sogar für Produkte beliebiger Länge:

2.1.7 Übung. Zeige, dass für jedes Monoid M und $x_1, \dots, x_n \in M$ das Produkt

$$x_1 x_2 \cdots x_n$$

unabhängig von der Klammerung ist.

Symmetrien wie in Abbildung 2 haben die zusätzliche Eigenschaft, dass jede der betrachteten Abbildungen invertierbar ist. Der allgemeine Begriff von Invertierbarkeit ist wie folgt.

2.1.8 Definition. Sei $(M, \cdot, e)$ ein Monoid.

(a) Ein Element $x \in M$ heißt **invertierbar**, falls es ein Element $y \in M$ gibt mit

$$xy = e = yx. \tag{2.1}$$

(b) M heißt **Gruppe**, falls jedes Element von M invertierbar ist.

Eine generische Gruppe werden wir im Folgenden meist mit $(G, \cdot, e)$ bezeichnen.

2.1.9 Bemerkung. (a) Falls y mit (2.1) existiert, dann ist es eindeutig bestimmt, und heißt das **Inverse** von x . Denn falls y' ebenfalls ein Inverses von x ist, dann gilt

$$y' = y'e = y'xy = ey = y.$$

Somit folgt die Eindeutigkeit, und wir können von *dem* Inversen von x sprechen. Wir bezeichnen das Inverse von x mit x^{-1} , sofern es existiert.

(b) In einer Gruppe gelten folgende Rechenregeln für das Bilden von Inversen:

$$\boxed{e^{-1} = e, \quad (xy)^{-1} = y^{-1}x^{-1}, \quad (x^{-1})^{-1} = x.} \tag{2.2}$$

Ersteres ist klar wegen $ee = e$, so dass e sein eigenes Inverses ist. Für die zweite Regel rechnen wir

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e,$$

und analog $(y^{-1}x^{-1})(xy) = e$. Somit ist $y^{-1}x^{-1}$ in der Tat das Inverse von xy .

Allgemeiner gelten (2.2) bereits in jedem Monoid für alle invertierbaren Elemente, mit dem gleichen Beweis. Dies wird in Beispiel 2.1.11 unten verwendet.

(c) In einer Gruppe gilt: falls $xy = e$, dann ist $y = x^{-1}$. Es muss also bloß eine der beiden Gleichungen in (2.1) gelten, und die andere folgt dann automatisch. Denn aus $xy = e$ folgt

$$y = ey = x^{-1}xy = x^{-1}e = x^{-1}. \tag{2.3}$$

Diese Eigenschaft ist aber spezifisch für Gruppen, denn:

2.1.10 Übung. Finde eine geeignete Menge X und zwei Funktionen $f, g : X \rightarrow X$, so dass

$$f \circ g = \text{id}_X, \quad g \circ f \neq \text{id}_X.$$

Wir kommen nun zu einigen Beispielen von Gruppen.

2.1.11 Beispiel. Die folgende Konstruktion erzeugt aus jedem Monoid eine Gruppe. Wie wir noch sehen werden liefert dies wichtige Beispiele von Gruppen, denn die folgenden Beispiele 2.1.12, 2.1.14 und 2.1.19 entstehen auf diese Weise.

Sei M ein Monoid und

$$M^\times := \{x \in M \mid x \text{ ist invertierbar}\}.$$

Dann ist $M^\times$ eine Gruppe bezüglich der Verknüpfung von M . Denn zunächst ist nach (2.2) das Produkt zweier invertierbarer Elemente wieder invertierbar, und somit ist $M^\times$ bezüglich der Verknüpfung abgeschlossen, also ein Magma. Die Verknüpfung ist assoziativ, weil sie es in M ist. Weiters ist das neutrale Element von M nach (2.1) invertierbar, und somit ist $M^\times$ ein Monoid. Nach Definition von $M^\times$ sind alle Elemente von $M^\times$ invertierbar, und ihre Inversen liegen dank (2.2) ebenfalls in $M^\times$. Somit ist $M^\times$ eine Gruppe.

2.1.12 Beispiel. Im Monoid der Abbildungen $X \rightarrow X$ von Beispiel 2.1.5 ist eine Abbildung $f : X \rightarrow X$ genau dann invertierbar, wenn sie bijektiv ist. Denn ist f bijektiv, so gibt es eine Umkehrabbildung f^{-1} , welche charakterisiert ist durch

$$f(x) = y \quad \Longleftrightarrow \quad f^{-1}(y) = x. \quad (2.4)$$

In diesem Fall überlegt man sich leicht, dass $f^{-1} \circ f = \text{id}_X = f \circ f^{-1}$ gilt. Andererseits, falls f invertierbar mit Inversem f^{-1} ist, dann folgt auch (2.4) leicht, und somit ist f bijektiv.

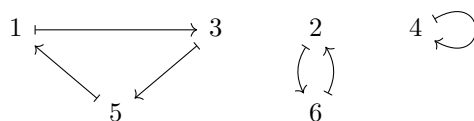
Die Menge der bijektiven Abbildungen $X \rightarrow X$ bildet somit eine Gruppe bezüglich der Hintereinanderausführung. Wir bezeichnen diese Gruppe mit S_X und nennen sie die **symmetrische Gruppe** über X . Oft betrachtet man

$$X = \{1, \dots, n\}$$

für ein $n \in \mathbb{N}$, und bezeichnet die symmetrische Gruppe über dieser Menge einfach mit S_n . Deren Elemente sind die bereits bekannten **Permutationen**, die wie aus der linearen Algebra bekannt als Hintereinanderausführung von Zykeln dargestellt werden können, also zum Beispiel

$$(1 \ 3 \ 5)(2 \ 6) \in S_6 \quad (2.5)$$

für die bijektive Abbildung



2.1.13 Definition. Eine Teilmenge $H \subseteq G$ einer Gruppe G heißt **Untergruppe** von G , falls gelten:

- (a) $e \in H$.
- (b) Für alle $x, y \in H$ gilt $xy \in H$.
- (c) Für alle $x \in H$ gilt $x^{-1} \in H$.

Man überzeugt sich leicht davon, dass jede Untergruppe H einer Gruppe G selbst wieder eine Gruppe ist bezüglich der Verknüpfung von G , weil die Rechengesetze wie das Assoziativgesetz von G auf H vererbt werden.

Jetzt können wir zu den Symmetrien zurückkehren. Eine **Symmetrie** eines mathematischen Objekts ist eine bijektive Abbildung von diesem Objekt auf sich selber, welches die Struktur des

Objekts erhält. Auch wenn wir keine formal präzise Definition von “Struktur” geben werden, legt dieses Prinzip nahe, dass die Symmetrien eines Objekts eine Untergruppe der symmetrischen Gruppe über der Grundmenge des Objekts bilden: die Identitätsabbildung ist strukturerhaltend, die Hintereinanderausführung zweier strukturerhaltender Abbildungen ist wieder strukturerhaltend, und das Inverse einer strukturerhaltenden Abbildung ist oft ebenfalls strukturerhaltend.

2.1.14 Beispiel. Für einen Körper K und $n \in \mathbb{N}$ betrachten wir den Vektorraum K^n und die “strukturerhaltenden” Abbildungen $K^n \rightarrow K^n$. Das Erhalten der Struktur des Vektorraums bedeutet, dass die Abbildung sowohl die Vektoraddition als auch die Skalarmultiplikation erhält, also linear ist. Die linearen Abbildungen $f : K^n \rightarrow K^n$ sind bekanntermaßen gerade die Abbildungen, die die Form

$$f(x) = Ax \quad (2.6)$$

für eine Matrix $A \in M_{n \times n}(K)$ haben.

Die Hintereinanderausführung zweier linearer Abbildungen ist wieder linear, und die Hintereinanderausführung entspricht genau der Matrixmultiplikation: für $f(x) = Ax$ und $g(x) = Bx$ ist

$$(g \circ f)(x) = g(f(x)) = g(Ax) = B(Ax) = (BA)x.$$

Außerdem ist die Identitätsabbildung (dargestellt durch die Einheitsmatrix $1_{n \times n}$) linear. Somit bilden die linearen Abbildungen $K^n \rightarrow K^n$ ein Monoid bezüglich der Hintereinanderausführung, welches auch als Monoid der $n \times n$ -Matrizen mit der Matrixmultiplikation beschrieben werden kann.

Eine lineare Abbildung (2.6) ist genau dann invertierbar, wenn die Matrix A invertierbar ist, und die inverse Abbildung wird durch die inverse Matrix A^{-1} dargestellt. Die invertierbaren linearen Abbildungen bzw. Matrizen bilden somit eine Gruppe, die sogenannte **allgemeine lineare Gruppe**. Sie wird mit

$$\mathrm{GL}_n(K)$$

bezeichnet.

2.1.15 Beispiel. Eine Matrix $A \in M_{n \times n}(\mathbb{R})$ heißt **orthogonal**, falls

$$A^t A = 1_{n \times n},$$

also falls $A^{-1} = A^t$ gilt. Eine orthogonale Matrix erhält die euklidische Norm, denn für alle $x \in \mathbb{R}^n$ gilt

$$\|Ax\|^2 = (Ax)^t(Ax) = x^t(A^t A)x = x^t 1_{n \times n} x = \|x\|^2,$$

also $\|Ax\| = \|x\|$. Man kann sogar zeigen, dass umgekehrt jede lineare Abbildung, welche die euklidische Norm erhält, durch eine orthogonale Matrix dargestellt wird.⁵ Somit sind die orthogonalen Matrizen genau die linearen Abbildungen, welche Abstände im $\mathbb{R}^n$ erhalten. Mit anderen Worten: die orthogonalen Matrizen sind die Symmetrien des $\mathbb{R}^n$, wenn man ihn als *normierten Raum* betrachtet. Die orthogonalen Matrizen bilden eine Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}_n(\mathbb{R})$, die sogenannte **orthogonale Gruppe**,

$$O(n) := \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^t A = 1_{n \times n}\}.$$

Es lohnt sich, die Elemente von $O(3)$ zu visualisieren: diese sind entweder Drehungen um eine Achse (durch den Ursprung) oder Drehspiegelungen an einer Ebene, wobei der Drehwinkel jeweils auch 0 sein kann (so dass man die Identität bzw. reine Spiegelungen erhält).⁶ Bei $O(2)$ haben wir es mit Drehungen um den Ursprung sowie mit Spiegelungen an einer Geraden durch den Ursprung zu tun.

2.1.16 Beispiel. Eine Abbildung $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ heißt **affin**, falls sie von der Form

$$f(x) = Ax + b \quad (2.7)$$

⁵Siehe z.B. math.stackexchange.com/q/1293901/745634.

⁶Siehe z.B. [3, Satz 1.8(b)].

für eine Matrix $A \in M_{n \times n}(\mathbb{R})$ und einen Vektor $b \in \mathbb{R}^n$ ist. Falls A orthogonal ist, dann erhält eine solche Abbildung (2.7) Abstände im $\mathbb{R}^n$, denn

$$\|f(x) - f(y)\| = \|(Ax + b) - (Ay + b)\| = \|A(x - y)\| = \|x - y\|.$$

Man kann sogar zeigen, dass umgekehrt jede Abbildung, die Abstände erhält, von der Form (2.7) mit orthogonaler A ist. Diese Aussage ist Teil des *Satzes von Mazur-Ulam*. Es ist überraschend, dass eine Abbildung, die Abstände erhält, bereits automatisch affin ist!

Man sieht relativ leicht aus der Definition von abstandserhaltenden Abbildungen, dass die Hintereinanderausführung zweier abstandserhaltender Abbildungen wieder abstandserhaltend ist, dass die Identitätsabbildung abstandserhaltend ist, und dass jede abstandserhaltende Abbildung invertierbar ist mit abstandserhaltender Inverser. All dies ist auch anhand der Form (2.7) mit orthogonaler A leicht nachzurechnen. Somit bilden die abstandserhaltenden Abbildungen $\mathbb{R}^n \rightarrow \mathbb{R}^n$ eine Untergruppe der symmetrischen Gruppe $S_{\mathbb{R}^n}$. Sie heißt **euklidische Gruppe** und wird mit

$$E(n) := \{f : \mathbb{R}^n \rightarrow \mathbb{R}^n \mid f(x) = Ax + b, A \in O(n), b \in \mathbb{R}^n\}$$

bezeichnet. Zum Beispiel zu $E(2)$ gehören die Drehungen und Spiegelungen, aber auch die Translationen und die *Gleitspiegelungen*, wie in Abbildung 2.

2.1.17 Beispiel. Jetzt kommen wir zurück zu den Mustern in Abbildung 2 und können den dort informell besprochenen Symmetriegruppen eine präzise Definition geben. Zunächst können wir ein Muster betrachten als eine Teilmenge der Ebene $\mathcal{M} \subseteq \mathbb{R}^2$. Die Symmetrien des Musters sind dann die abstandserhaltenden Abbildungen $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ welche das Muster auf sich selber abbilden, also

$$f(\mathcal{M}) = \mathcal{M}.$$

Es ist leicht zu sehen, dass diese Symmetrien eine Untergruppe der euklidischen Gruppe $E(2)$ bilden, denn:

- ▷ Die Identitätsabbildung bildet $\mathcal{M}$ auf sich selber ab.
- ▷ Falls $f(\mathcal{M}) = \mathcal{M}$ und $g(\mathcal{M}) = \mathcal{M}$, dann gilt auch

$$(g \circ f)(\mathcal{M}) = g(f(\mathcal{M})) = g(\mathcal{M}) = \mathcal{M}.$$

- ▷ Falls $f(\mathcal{M}) = \mathcal{M}$, dann gilt auch

$$f^{-1}(\mathcal{M}) = f^{-1}(f(\mathcal{M})) = \mathcal{M}.$$

2.1.18 Beispiel (Diedergruppen). Für $n \geq 3$ betrachten wir ein regelmäßiges n -Eck im $\mathbb{R}^2$ mit Mittelpunkt im Ursprung, wie in Abbildung 3. Die Symmetrien eines solchen n -Ecks bilden eine Untergruppe der euklidischen Gruppe $E(2)$, die sogenannte **Diedergruppe** D_{2n} .⁷

Zu D_{2n} gehört zunächst die Rotation um den Ursprung um $2\pi/n$, also

$$r := \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}.$$

Da D_{2n} ein Monoid ist, gehören auch alle Potenzen $r, r^2, \dots$ zu D_{2n} . Dabei gilt $r^n = \text{id}_{\mathbb{R}^2}$, also sind nur die Potenzen

$$\text{id}_{\mathbb{R}^2} = r^0, r^1, r^2, \dots, r^{n-1}$$

verschieden. Außerdem gehört die Spiegelung an der x -Achse

$$s := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

⁷Der Index $2n$ kommt daher, dass die Diedergruppe $2n$ Elemente hat, wie wir im folgenden sehen werden. Manchmal wird die Diedergruppe auch mit D_n bezeichnet, was zu Verwirrung führen kann.

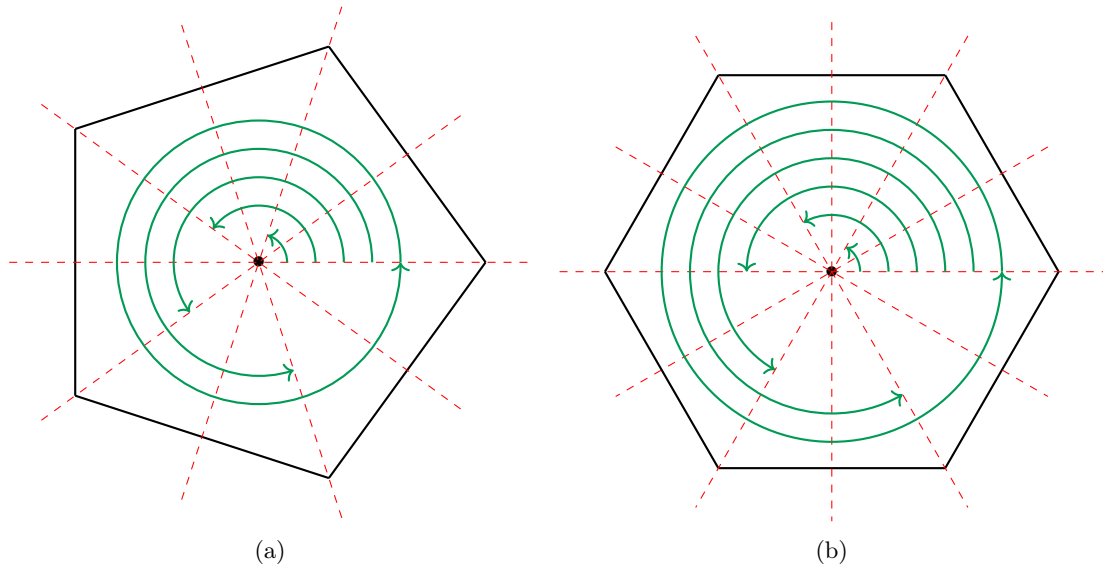


Abbildung 3: Zwei regelmäßige n -Ecke und ihre Symmetrien: Drehungen (grün), wobei die letzte volle Drehung die Identitätsabbildung ist, und Spiegelungsachsen (rot).

zu D_n . Da $s^2 = \text{id}_{\mathbb{R}^2}$ gilt, bekommen wir durch das Bilden von Potenzen von s keine neuen Symmetrien. Wir können aber weitere Symmetrien durch Hintereinanderausführung von s mit Potenzen von r erzeugen, also die Elemente

$$s, rs, r^2s, \dots, r^{n-1}s$$

betrachten. Hierzu kann man sich leicht überlegen (oder anhand der Matrixdarstellungen nachrechnen), dass $r^k s$ die Spiegelung an der Geraden durch den Ursprung mit Winkel $\frac{k\pi}{n}$ zur x -Achse ist.

Somit haben wir bisher n Rotationen (inklusive der Identität) und n Spiegelungen gefunden, also insgesamt $2n$ Symmetrien. Gibt es noch weitere? Dazu können wir zunächst feststellen, dass jede Symmetrie den Ursprung auf sich selber abbilden muss, denn der Ursprung ist der Schwerpunkt des n -Ecks, und Symmetrien müssen ausgezeichnete Punkte wie den Schwerpunkt erhalten. Somit muss jede Symmetrie nicht nur zu $E(2)$ gehören, sondern sogar zu $O(2)$, also entweder eine Drehung um den Ursprung oder eine Spiegelung an einer Geraden durch den Ursprung sein. Da eine Symmetrie Ecken auf Ecken abbilden muss, sind die einzigen erlaubten Drehungen die Potenzen von r . Die einzigen möglichen Spiegelungsachsen sind die Geraden durch den Ursprung mit Winkel $\frac{k\pi}{n}$ zur x -Achse, also die von uns bereits gefundenen Spiegelungen $r^k s$.⁸ Somit haben wir also alle Symmetrien gefunden. (Diese Argumente sollen keinen formalen Beweis darstellen, sondern eher eine Beweisskizze, die uns hilfreiche Intuition liefert. Im Rahmen dieser Vorlesung wollen wir es dabei belassen und stattdessen die Gruppe aus algebraischer Sicht untersuchen.)

Insgesamt haben wir also

$$D_{2n} = \{\text{id}_{\mathbb{R}^2}, r, \dots, r^{n-1}\} \cup \{s, rs, \dots, r^{n-1}s\}.$$

Wie sieht die Gruppenstruktur von D_{2n} aus? Zunächst ist wegen $r^n = e$ klar, dass mit den Potenzen von r modulo n zu rechnen ist, also

$$r^k \cdot r^\ell = r^{(k+\ell) \bmod n}. \quad (2.8)$$

Dies entspricht der Tatsache, dass der Drehwinkel nur bis auf Vielfache von 2π eindeutig bestimmt ist. Insbesondere gilt $r^{-1} = r^{n-1}$. Als wichtigste Relation halten wir außerdem fest, dass

$$rs = sr^{-1} \quad (2.9)$$

⁸Für ungerades n verbinden diese Geraden jeweils eine Ecke mit dem Mittelpunkt der gegenüberliegenden Seite. Für gerades n verbindet die Hälfte dieser Geraden gegenüberliegende Ecken, und die andere Hälfte die Mittelpunkte gegenüberliegender Seiten.

gilt: wenn wir zuerst spiegeln und dann um $\frac{2\pi}{n}$ drehen, dann ist dies dasselbe wie zuerst um $-\frac{2\pi}{n}$ zu drehen und dann zu spiegeln. Dies ist mit den Matrixdarstellungen leicht nachzurechnen, ist aber auch intuitiv einleuchtend anhand der geometrischen Bedeutung von r und s nach Abbildung 3.

Durch die Relation (2.9) und die Tatsache, dass D_{2n} eine Gruppe ist, sind alle anderen Multiplikationen in D_{2n} bereits bestimmt. Denn wie in (2.8) ist klar, wie man zwei Potenzen von r multipliziert. Die Multiplikation einer Rotation mit einer Spiegelung liefert

$$r^k \cdot r^\ell s = r^{(k+\ell) \bmod n} s, \quad r^k s \cdot r^\ell = r^{(k-\ell) \bmod n} s,$$

wobei die zweite Gleichung aus (2.9) durch mehrfaches Anwenden folgt: jeden Faktor r können wir an dem s vorbeiziehen, indem wir ihn durch r^{-1} ersetzen, und so ergibt sich $r^\ell s = sr^{-\ell}$. Zu guter Letzt ist die Multiplikation zweier Spiegelungen nach dem gleichen Argument durch

$$r^k s \cdot r^\ell s = r^{(k-\ell) \bmod n}$$

bestimmt.

Zusammenfassend können wir sagen: in der Diedergruppe D_{2n} können wir jedes Element bekommen, indem wir die Rotation r und die Spiegelung s wiederholt multiplizieren. Die Gruppenstruktur ist eindeutig durch die Relationen

$$\boxed{r^n = e, \quad s^2 = e, \quad rs = sr^{-1}} \quad (2.10)$$

bestimmt. Insbesondere können wir eine Potenz von r an der Spiegelung s vorbeiziehen, indem wir die Potenz von r invertieren. Durch diese Rechenregeln lässt sich in D_{2n} sehr einfach rechnen, ohne dass man Matrixdarstellungen verwenden oder an die geometrische Bedeutung denken muss.

Wir kommen nun zu einigen Beispielen, die weniger direkt mit Symmetrien zu tun haben, aber trotzdem wichtige Gruppen sind.

2.1.19 Beispiel. (a) Die Menge der ganzen Zahlen $\mathbb{Z}$ bildet eine Gruppe bezüglich der Addition $+$ mit 0 als neutralem Element. Das Inverse eines Elements $n \in \mathbb{Z}$ ist $-n$. Gleiches gilt für alle anderen Zahlensysteme, bzw. noch allgemeiner für Ringe (weil dies Teil der Definition von Ring ist).

(b) Betrachten wir entsprechend die Multiplikation als Verknüpfung, dann ist natürlich die 0 nicht invertierbar. Ein Zahlensystem wie $\mathbb{Z}$ oder $\mathbb{R}$ ist also keine Gruppe bezüglich der Multiplikation ist.

Wenn wir aber die 0 weglassen, dann bekommen wir in vielen Fällen eine Gruppe, nämlich zum Beispiel für $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ und $\mathbb{C} \setminus \{0\}$. In der Tat ist die Forderung, dass man eine Gruppe bezüglich der Multiplikation erhält wenn man die 0 weglässt, gerade Teil der Definition von Körper. Im Gegensatz dazu ist $\mathbb{Z} \setminus \{0\}$ aber keine Gruppe bezüglich der Multiplikation, denn z.B. ist 2 nicht multiplikativ invertierbar.

In diesen Beispielen arithmetischer Natur gilt bekanntermaßen auch das Kommutativgesetz:

2.1.20 Definition. Eine Gruppe G heißt **abelsch**, falls für alle $x, y \in G$ gilt

$$xy = yx.$$

Denn wie wir noch sehen werden, ist die Untersuchung von abelschen Gruppen einfacher als die von allgemeinen Gruppen. Zum Beispiel gelten:

▷ Die symmetrische Gruppe S_X von Beispiel 2.1.12 ist abelsch genau dann wenn $|X| \leq 2$. Denn in S_3 ist z.B. $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$, und analog wenn X mindestens drei Elemente hat.

Falls X leer ist oder bloß ein Element hat, dann enthält S_X nur die Identität und ist somit trivialerweise abelsch. Für eine Menge mit zwei Elementen $X = \{1, 2\}$ ist schließlich $S_X = \{\text{id}_X, (1\ 2)\}$, und diese Gruppe ist abelsch.

- ▷ Ähnliches gilt für die allgemeine lineare Gruppe $GL_n(K)$ aus Beispiel 2.1.14: diese ist abelsch für $n = 1$, aber nicht für $n \geq 2$. Zum Beispiel für $n = 2$ gilt

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Für $n > 2$ kann man dasselbe Beispiel verwenden, wenn man mit Einsen entlang der Diagonale und Nullen sonst auffüllt.

- ▷ Ähnlich dazu ist die orthogonale Gruppe $O(n)$ abelsch für $n = 1$, aber nicht für $n \geq 2$. Zum Beispiel gilt für $n = 2$,

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Das heißt: die Spiegelung an der x -Achse und die Spiegelung an der Winkelhalbierenden des ersten Quadranten kommutieren nicht.

- ▷ Die euklidische Gruppe $E(n)$ aus Beispiel 2.1.19 ist für alle $n \geq 1$ nicht abelsch. Zum Beispiel schon mit $n = 1$ und $f(x) = x + 1$ und $g(x) = -x$ ist

$$\begin{aligned} (f \circ g)(x) &= f(-x) = -x + 1, \\ (g \circ f)(x) &= g(x + 1) = -x - 1. \end{aligned}$$

- ▷ Die Diedergruppe D_{2n} ist für alle $n \geq 3$ wegen (2.9) und $r \neq r^{-1}$ nicht abelsch.
▷ Die Gruppen aus Beispiel 2.1.19 sind alle abelsch.

2.2 Homomorphismen und Isomorphismen

Für die Untersuchung von Symmetrien und anderen Anwendungen ist ein Verständnis der algebraischen Struktur von Gruppen essentiell. Dies ist das Hauptziel der Gruppentheorie.

Wir beginnen zunächst mit einigen weiteren grundlegenden Begriffen.

2.2.1 Definition. Eine Gruppe G heißt **erzeugt** durch gegebene Elemente $a_1, \dots, a_n \in G$, falls G die kleinste Untergruppe von G ist, die $a_1, \dots, a_n$ enthält.

Dies klingt etwas abstrakt, lässt sich aber leicht konkreter formulieren: G wird durch $a_1, \dots, a_n$ erzeugt, falls sich jedes Element von G als endliches Produkt der Elemente $a_1, \dots, a_n$ und ihrer Inversen $a_1^{-1}, \dots, a_n^{-1}$ schreiben lässt. Denn anhand von Definition 2.1.13 sieht man direkt, dass die Menge aller solchen Produkte eine Untergruppe von G ist. Es ist außerdem klar, dass es die kleinste Untergruppe ist, welche G enthält. Somit stimmt G genau dann mit dieser Untergruppe überein, wenn jedes Element von G als solches Produkt dargestellt werden kann.

2.2.2 Beispiel. Die Diedergruppe D_{2n} aus Beispiel 2.1.18 wird durch die Rotation r und die Spiegelung s erzeugt. Denn jedes Element von D_{2n} ist entweder eine Potenz von r oder eine Potenz von r gefolgt von s .

2.2.3 Definition. Eine Gruppe G heißt **zyklisch**, falls es ein Element $x \in G$ gibt, so dass G durch x erzeugt wird.

In einer zyklischen Gruppe ist also jedes Element eine Potenz von x . Dabei sind auch negative Potenzen erlaubt, denn wir schreiben

$$x^{-n} := (x^{-1})^n \quad \forall n \in \mathbb{N}$$

und $x^0 := e$, so dass die Potenzgesetze

$$\boxed{x^{m+n} = x^m x^n, \quad (x^m)^n = x^{mn}} \quad (2.11)$$

für alle $m, n \in \mathbb{Z}$ gelten. Ein formaler Beweis dieser Potenzgesetze ist eine gute Übung in der Anwendung der Gruppenaxiome und muss per Induktion über n und m geführt werden. Wir führen ihn hier nicht aus, weil er effektiv mit dem Beweis der Potenzgesetze für Zahlen übereinstimmt.

2.2.4 Beispiel. (a) $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, die durch 1 erzeugt wird. Denn jedes Element ist eine “Potenz” von 1, was in diesem Fall bedeutet, dass jedes Element eine wiederholte *Summe* von 1 oder -1 ist, da die Verknüpfung die Addition ist.

(b) Betrachte die Untergruppe von $\text{GL}_2(\mathbb{R})$ der Matrizen der Form

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

mit $n \in \mathbb{Z}$. Da

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$$

ist diese Gruppe ebenfalls zyklisch mit Erzeuger

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

2.2.5 Beispiel. (a) Die multiplikativ invertierbaren Elemente $(\mathbb{Z}, \cdot)^\times$ sind nur $\{1, -1\}$, und diese Gruppe wird offensichtlich durch -1 erzeugt und ist somit zyklisch.

(b) Noch allgemeiner: Sei G eine beliebige Gruppe mit zwei Elementen. Wir können $G = \{e, a\}$ mit $a \neq e$ schreiben. Dann ist $a^2 = e$, also $a^{-1} = a$. Außerdem ist klar, dass G durch a erzeugt wird, also ist G zyklisch.

(c) Auf ähnliche Weise ist die Menge der vierten Einheitswurzeln $\{\pm 1, \pm i\} \subseteq \mathbb{C}^\times$ eine zyklische Gruppe bezüglich der Multiplikation, da

$$-1 = i^2, \quad -i = i^3,$$

so dass jedes Element eine Potenz von i ist.

In einer zyklischen Gruppe ist die gesamte Gruppenstruktur durch die Potenzgesetze bestimmt:

2.2.6 Lemma. Sei G eine zyklische Gruppe mit Erzeuger x . Dann trifft genau eine der beiden Aussagen zu:

(a) G ist endlich, und mit $n = |G|$ gilt

$$G = \{e, x, x^2, \dots, x^{n-1}\}, \quad (2.12)$$

und die Multiplikation ist gegeben durch $x^k \cdot x^\ell = x^{(k+\ell) \bmod n}$ für alle $k, \ell \in \mathbb{Z}$ (Abbildung 4).

(b) G ist unendlich mit

$$G = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\}$$

und Multiplikation $x^k \cdot x^\ell = x^{k+\ell}$ für alle $k, \ell \in \mathbb{Z}$.

Insbesondere ist eine zyklische Gruppe abelsch, da die Addition der Potenzen abelsch ist.

Beweis. Wir zeigen zunächst:

▷ Falls $x^k = x^\ell$ für $k, \ell \in \mathbb{Z}$ mit $k \neq \ell$ gilt, dann ist G endlich mit $|G| \leq |k - \ell|$.

Dazu sein ohne Beschränkung der Allgemeinheit $k > \ell$, was die Notation leicht vereinfacht. Dann gilt nach den Potenzgesetzen also $x^{k-\ell} = e$. Daraus folgt, dass

$$x^{r+t(k-\ell)} = x^r (x^{k-\ell})^t = x^r e^t = x^r$$

für alle $r \in \{0, \dots, k - \ell - 1\}$ und $t \in \mathbb{Z}$. Wenn wir ein beliebiges $m \in \mathbb{Z}$ also per Division mit Rest als $m = r + t(k - \ell)$ mit $r \in \{0, \dots, k - \ell - 1\}$ und $t \in \mathbb{Z}$ schreiben, dann folgt daraus

$$x^m = x^{r+t(k-\ell)} = x^r.$$

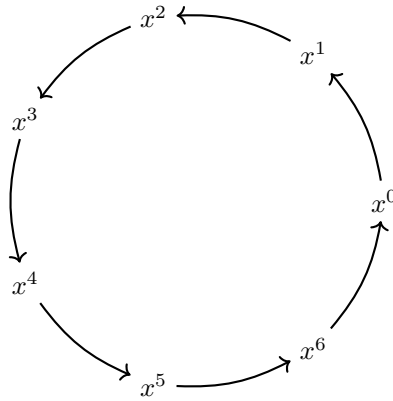


Abbildung 4: Gruppenstruktur einer zyklischen Gruppe mit 7 Elementen und Erzeuger x . Die Multiplikation mit x (von links oder rechts) ist durch die Pfeile dargestellt.

Somit ist jedes Element von G identisch mit einer der Potenzen $e = x^0, x^1, \dots, x^{k-\ell-1}$, und es folgt die Behauptung $|G| \leq k - \ell$.

Wir kommen zum Beweis der eigentlichen Aussage. Sei dazu zunächst G unendlich. Dann ist zu zeigen, dass die Potenzen x^m alle verschieden sind; die Multiplikationsregel ist dann ja bereits bekannt (2.11). Sei also $x^k = x^\ell$ für $k, \ell \in \mathbb{Z}$ doch der Fall mit $k \neq \ell$. Dann müsste nach obiger Hilfsaussage G endlich sein, was einen Widerspruch ergibt. Somit sind alle Potenzen verschieden, und der Fall $|G| = \infty$ ist erledigt.

Sei nun G endlich mit $|G| = n$. Dann zeigen wir zunächst, dass die Elemente $e, x, x^2, \dots, x^{n-1}$ verschieden sind. Denn wenn $x^k = x^\ell$ für $k, \ell \in \{0, \dots, n-1\}$ mit $k \neq \ell$ gilt, dann folgt aus der obigen Hilfsaussage, dass $|G| \leq |k - \ell| < n$ ist, was ein Widerspruch ist. Somit sind $e, x, x^2, \dots, x^{n-1}$ verschiedene Elemente von G . Und weil G genau n Elemente hat, folgt also gerade die behauptete Form (2.12). Als nächstes zeigen wir

$$x^n = e.$$

Dies gilt weil x^n ja mit einem der Elemente $e, x, x^2, \dots, x^{n-1}$ übereinstimmen muss. Und falls $x^n = x^k$ für $k \in \{1, \dots, n-1\}$ gilt, dann folgt aus der obigen Hilfsaussage, dass $|G| \leq n - k < n$ ist, was ein Widerspruch ist. Schlußendlich folgt dann die Multiplikationsregel

$$x^k \cdot x^\ell = x^{(k+\ell) \bmod n}$$

für alle $k, \ell \in \mathbb{Z}$ aus $x^n = e$ und den Potenzgesetzen (2.11), weil also Vielfache von n in den Exponenten weggelassen werden können. $\square$

Man wird vielleicht feststellen, dass sich alle zyklischen Gruppen mit gleich vielen Elementen komplett analog verhalten, da sich ja nur die Potenzen addieren. Dies wird durch den Begriff von *Isomorphismus* präzisiert, den wir im folgenden definieren.

2.2.7 Definition. Eine Abbildung zwischen zwei Gruppen G und H ,

$$f : G \rightarrow H,$$

heißt **Gruppenhomomorphismus** oder kurz **Homomorphismus**, falls für alle $x, y \in G$ gilt

$$f(xy) = f(x)f(y).$$

Ein Homomorphismus erhält per Definition also die Multiplikation. Dass er auch das neutrale Element sowie inverse Elemente erhält, folgt daraus bereits:

2.2.8 Lemma. Sei $f : G \rightarrow H$ ein Gruppenhomomorphismus. Dann gilt:

$$(a) \ f(e_G) = e_H.$$

(b) Für alle $x \in G$ gilt $f(x^{-1}) = f(x)^{-1}$.

Beweis. (a) Folgt aus

$$f(e_G) = f(e_G e_G) = f(e_G) f(e_G)$$

durch Multiplikation beider Seiten mit $f(e_G)^{-1}$ von links (oder rechts).

(b) Für jedes $x \in G$ gilt

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H.$$

Somit ist $f(x^{-1})$ das Inverse von $f(x)$ in H , also $f(x^{-1}) = f(x)^{-1}$. $\square$

2.2.9 Beispiel. (a) Das Bilden der Signatur ist eine Abbildung

$$\text{sgn} : S_n \rightarrow \{1, -1\},$$

welche die Multiplikativität

$$\text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma) \cdot \text{sgn}(\tau)$$

erfüllt. Wenn wir $\{1, -1\}$ als Gruppe bezüglich der Multiplikation betrachten, dann ist sgn also ein Gruppenhomomorphismus.

(b) Ähnlich ist auch die Determinante eine Abbildung

$$\det : \text{GL}_n(K) \rightarrow K^\times,$$

welche die Multiplikativität

$$\det(AB) = \det(A) \cdot \det(B)$$

erfüllt. Wenn wir $K^\times$ als Gruppe bezüglich der Multiplikation betrachten, dann ist $\det$ also ein Gruppenhomomorphismus.

(c) Wir können auch jede Permutation $\sigma \in S_n$ durch die Vorschrift

$$(A_\sigma)_{ij} := \begin{cases} 1 & \text{falls } j = \sigma(i), \\ 0 & \text{sonst} \end{cases}$$

als Matrix $A_\sigma \in \text{GL}_n(K)$ darstellen (eine sogenannte Permutationsmatrix). Man rechnet leicht nach, dass diese Konstruktion als Abbildung $S_n \rightarrow \text{GL}_n(K)$ ebenfalls die Verknüpfung von Permutationen auf das Matrixprodukt abbildet, also ein Gruppenhomomorphismus ist.

Dieser Gruppenhomomorphismus hat die interessante Eigenschaft, dass die Determinante der Permutationsmatrix gerade die Signatur der Permutation ist. Dies können wir zusammenfassen in dem Diagramm

$$\begin{array}{ccc} S_n & \longrightarrow & \text{GL}_n(K) \\ \text{sgn} \downarrow & & \downarrow \det \\ \{1, -1\} & \longrightarrow & K^\times \end{array}$$

wobei der untere horizontale Pfeil die Inklusionsabbildung $\{1, -1\} \rightarrow K^\times$ ist. Dieses Diagramm "kommutiert", womit man meint, dass die beiden möglichen Wege von S_n nach $K^\times$ dieselbe Abbildung ergeben. Dies drückt auf abstrakte Weise aus, dass die Determinante einer Permutationsmatrix gerade die Signatur der entsprechenden Permutation ist.

2.2.10 Beispiel. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann ist die Inklusionsabbildung $i : H \rightarrow G$, definiert durch $i(h) = h$ für alle $h \in H$, ein Gruppenhomomorphismus. Denn diese Aussage bedeutet gerade, dass wir in H die gleiche Multiplikation wie in G verwenden.

$\cdot$	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

$\circ$	e	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$
e	e	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	e	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\ 3\ 2)$	$(1\ 3\ 2)$	e	$(1\ 2\ 3)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2)$	e	$(1\ 3\ 2)$	$(1\ 2\ 3)$
$(1\ 2)$	$(1\ 2)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	e	$(1\ 3\ 2)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2)$	$(2\ 3)$	$(1\ 3\ 2)$	$(1\ 2\ 3)$	e

Abbildung 5: Multiplikationstabellen der Diedergruppe D_6 (oben) und der symmetrischen Gruppe S_3 (unten).

2.2.11 Lemma. Seien $f : G \rightarrow H$ und $g : H \rightarrow K$ zwei Gruppenhomomorphismen. Dann ist auch die Hintereinanderausführung

$$g \circ f : G \longrightarrow K$$

ein Gruppenhomomorphismus.

Beweis. Wir schreiben wieder gf als Abkürzung für $g \circ f$. Für alle $x, y \in G$ gilt dann

$$(gf)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (gf)(x)(gf)(y).$$

Somit ist auch gf ein Homomorphismus. □

2.2.12 Satz. Für einen Gruppenhomomorphismus $f : G \rightarrow H$ sind die folgenden Aussagen äquivalent:

- (a) f ist bijektiv.
- (b) Es gibt einen Gruppenhomomorphismus $g : H \rightarrow G$ mit $g \circ f = \text{id}_G$ und $f \circ g = \text{id}_H$.

Beweis. Sei f zunächst bijektiv. Dann zeigen wir, dass auch $g := f^{-1} : H \rightarrow G$ ein Homomorphismus ist. Für alle $x, y \in H$ gilt

$$f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(x))f(f^{-1}(y)) = xy,$$

weil f ein Homomorphismus ist. Durch Anwenden von f^{-1} auf beiden Seiten ergibt sich die gewünschte Gleichung $f^{-1}(x)f^{-1}(y) = f^{-1}(xy)$.

Sei umgekehrt f ein Homomorphismus mit inversem Homomorphismus f . Dann ist insbesondere g die Umkehrabbildung von f , und somit bijektiv. (Siehe Beispiel 2.1.12.) □

2.2.13 Definition. (a) Falls die äquivalenten Bedingungen aus Satz 2.2.12 erfüllt sind, heißt $f : G \rightarrow H$ ein **Gruppenisomorphismus**, oder kurz **Isomorphismus**.

- (b) Zwei Gruppen G und H heißen **isomorph**, falls es einen Isomorphismus $f : G \rightarrow H$ gibt.

Wie das folgende Beispiel zeigt, unterscheiden sich zwei isomorphe Gruppen im Wesentlichen nur um die Benennung ihrer Elemente. Was die Gruppenstruktur angeht, sind sie identisch, und insbesondere haben beide Gruppen genau die gleichen algebraischen Eigenschaften. (Also zB ob sie abelsch oder zyklisch sind, wie viele Elemente sie haben, usw.)

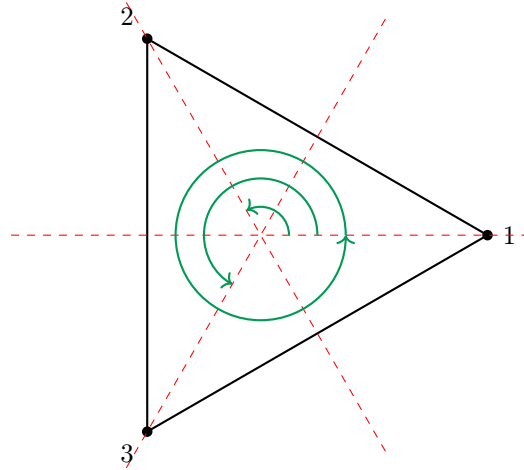


Abbildung 6

2.2.14 Beispiel. In Abbildung 5 sind die Multiplikationstabellen der Diedergruppe D_6 und der symmetrischen Gruppe S_3 dargestellt. Wie man durch Ablesen der Tabellen überprüfen kann, entsprechen sich diese Multiplikationstabellen genau. Dies bedeutet, dass die Abbildung

$$\begin{array}{lll} e \mapsto e, & r \mapsto (1\ 2\ 3), & r^2 \mapsto (1\ 3\ 2), \\ s \mapsto (2\ 3), & rs \mapsto (1\ 2), & r^2s \mapsto (1\ 3) \end{array}$$

ein Isomorphismus ist.

Diesen Isomorphismus kann man durch Abbildung 6 geometrisch verstehen: die Diedergruppe D_6 ist die Symmetriegruppe eines gleichseitigen Dreiecks, und die 6 Symmetrien entsprechen genau den 6 Permutationen der drei Ecken.

Aus Lemma 2.2.6 folgt:

2.2.15 Lemma. *Alle zyklischen Gruppen mit derselben Anzahl von Elementen sind isomorph.*

Informell sagt man auch, dass es für jede natürliche Zahl n genau eine zyklische Gruppe mit n Elementen gibt.

Beweis. Falls G und H zyklisch sind mit $|G| = |H|$ und Erzeugern $x \in G$ und $y \in H$, dann definiert die Abbildung

$$\begin{array}{l} G \longrightarrow H \\ x^k \longmapsto y^k \end{array}$$

einen Isomorphismus. □

Wir verwenden Homomorphismen unter anderem, um die Struktur von Gruppen genauer zu untersuchen. Dazu gehört insbesondere der Begriff des Kerns.

2.2.16 Definition. Der **Kern** eines Gruppenhomomorphismus $f : G \rightarrow H$ ist die Menge

$$\ker(f) := \{x \in G \mid f(x) = e_H\}.$$

Es ist leicht zu sehen, dass diese Menge $\ker(f)$ eine Untergruppe von G ist. Denn wegen $f(e_G) = e_H$ ist $e_G \in \ker(f)$. Für alle $x, y \in \ker(f)$ gilt außerdem

$$f(xy) = f(x)f(y) = e_H e_H = e_H,$$

also auch $xy \in \ker(f)$, sowie

$$f(x^{-1}) = f(x)^{-1} = e_H^{-1} = e_H,$$

so dass auch $x^{-1} \in \ker(f)$.

Wie für lineare Abbildungen bereits bekannt, ist der Kern eines Gruppenhomomorphismus ein Maß dafür, ob der Homomorphismus injektiv ist.

2.2.17 Lemma. Ein Gruppenhomomorphismus $f : G \rightarrow H$ ist injektiv genau dann, wenn sein Kern trivial ist, also $\ker(f) = \{e_G\}$.

Beweis. Falls f injektiv ist, dann gilt insbesondere, dass e_H höchstens ein Urbild haben kann. Da $f(e_G) = e_H$ gilt, ist also e_G das einzige Urbild von e_H , also $\ker(f) = \{e_G\}$.

Sei umgekehrt $\ker(f) = \{e_G\}$. Für $x, y \in G$ mit $f(x) = f(y)$ ist dann zu zeigen, dass bereits $x = y$ gelten muss. Aus der Annahme $f(x) = f(y)$ folgt

$$f(xy^{-1}) = f(x)f(y)^{-1} = f(y)f(y)^{-1} = e_H,$$

also $xy^{-1} \in \ker(f)$. Da der Kern als trivial vorausgesetzt wurde, erhalten wir daraus $xy^{-1} = e_G$, also $x = y$. $\square$

Der Kern ist aber nicht irgendeine Untergruppe, sondern von einer besonderen Art.

2.2.18 Definition. Eine Untergruppe $N \leq G$ heißt **normal**, falls für alle $x \in N$ und alle $a \in G$ gilt

$$axa^{-1} \in N.$$

Oft schreibt man diese Bedingung auch als $aNa^{-1} \subseteq N$. Die Multiplikation mit a von links und mit a^{-1} von rechts heißt auch **Konjugation** mit a .

2.2.19 Beispiel. (a) Für jeden Gruppenhomomorphismus $f : G \rightarrow H$ ist $\ker(f)$ eine normale Untergruppe von G . Denn für alle $x \in \ker(f)$ und alle $a \in G$ gilt

$$f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)e_Hf(a)^{-1} = f(a)f(a)^{-1} = e_H,$$

also auch $axa^{-1} \in \ker(f)$.

(b) Zum Beispiel gilt für die Signatur $\text{sgn} : S_n \rightarrow \{1, -1\}$, dass

$$A_n := \ker(\text{sgn}) = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\}$$

eine normale Untergruppe von S_n ist. Man nennt sie die **alternierende Gruppe**. Per Definition besteht A_n aus den geraden Permutationen in S_n .

Die kleinste nichttriviale alternierende Gruppe ist

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}, \quad (2.13)$$

eine zyklische Gruppe mit 3 Elementen. A_4 besteht aus der Identität, den ‘Doppeltranspositionen’ (welche die vier Elemente paarweise vertauschen), sowie den 3-Zyklen,

$$\begin{aligned} A_4 = \{e, \\ (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), \\ (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}. \end{aligned} \quad (2.14)$$

Diese Gruppe ist eines der zentralen Beispiele, weil sie klein genug ist, dass man gut rechnen kann, aber trotzdem schon interessante gruppentheoretische Eigenschaften besitzt.

(c) Ähnlich ist auch der Kern von $\det : \text{GL}_n(K) \rightarrow K^\times$ eine normale Untergruppe von $\text{GL}_n(K)$, nämlich die sogenannte **spezielle lineare Gruppe**

$$\text{SL}_n(K) := \ker(\det) = \{A \in \text{GL}_n(K) \mid \det(A) = 1\}.$$

(d) Falls G abelsch ist, dann ist jede Untergruppe $N \subseteq G$ normal, denn dann gilt für $x \in N$ und $a \in G$

$$axa^{-1} = aa^{-1}x = x \in N.$$

2.2.20 Bemerkung. (a) Falls $N \subseteq G$ normal ist, dann gilt nicht nur $aNa^{-1} \subseteq N$ für alle $a \in G$, sondern sogar automatisch die Gleichheit

$$aNa^{-1} = N \quad \forall a \in G.$$

Denn die Anwendung der Voraussetzung auf a^{-1} liefert $a^{-1}Na \subseteq N$, und somit durch Multiplikation mit a von links und mit a^{-1} von rechts die noch fehlende Inklusion $N \subseteq aNa^{-1}$.

(b) Falls G von $a_1, \dots, a_n$ erzeugt wird, dann reicht es zur Überprüfung der Normalität von $N \subseteq G$ aus, zu überprüfen, dass

$$a_i Na_i^{-1} \subseteq N \quad \wedge \quad a_i^{-1} Na_i \subseteq N \quad \forall i = 1, \dots, n \quad (2.15)$$

gelten. Denn aus dieser Bedingung folgt $xNx^{-1} \subseteq N$ allgemein, weil sich jedes $x \in G$ als Produkt der Erzeuger a_i und ihrer Inversen a_i^{-1} schreiben lässt.

2.2.21 Beispiel. (a) Zum Beispiel folgt aus dem Kriterium (2.15), dass

$$N := \{e, r, \dots, r^{n-1}\} \subseteq D_{2n}$$

eine normale Untergruppe von D_{2n} ist, denn für die Erzeuger r und s von D_{2n} gilt

$$r r^k r^{-1} = r^k \in N, \quad s r^k s^{-1} = r^{-k} \in N.$$

(b) Andererseits ist für $n \geq 3$ die Menge

$$\{e, s\} \subseteq D_{2n}$$

zwar eine Untergruppe, aber *nicht normal*, denn

$$r s r^{-1} = r^2 s$$

gehört nicht wieder zur Untergruppe.

2.2.22 Bemerkung. In $\text{GL}_n(K)$ kann man die Konjugation mit einem Element a auch als *Basiswechsel* interpretieren. Denn mit a als Basiswechselmatrix ist eine durch $b \in \text{GL}_n(K)$ dargestellte lineare Abbildung in der neuen Basis durch die Matrix

$$aba^{-1}$$

dargestellt. Die Normalität einer Untergruppe $N \subseteq \text{GL}_n(K)$ bedeutet also, dass die Untergruppe basisunabhängig definiert ist: eine lineare Abbildung gehört zu N genau dann, wenn sie in *irgendeiner* Basis durch eine Matrix aus N dargestellt wird.

2.2.23 Definition. Für eine Untergruppe $H \subseteq G$ und ein Element $x \in G$ ist:

(a) die **Linksnebenklasse** die Menge

$$xH := \{xy \mid y \in H\},$$

(b) die **Rechtsnebenklasse** die Menge

$$Hx := \{yx \mid y \in H\}.$$

Das bekannteste und wichtigste Beispiel ist dabei wie folgt.

2.2.24 Beispiel. Sei $n \in \mathbb{Z}$. Dann bilden die Vielfachen von n , also die Menge

$$n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$$

eine Untergruppe von $(\mathbb{Z}, +)$. Die Nebenklasse eines beliebigen Elements $x \in \mathbb{Z}$ ist dann gerade die Menge der ganzen Zahlen, die Rest x bei Division durch n haben:

$$x + n\mathbb{Z} = \{x + nk \mid k \in \mathbb{Z}\} = \{y \in \mathbb{Z} \mid y \equiv x \pmod{n}\}.$$

Da $\mathbb{Z}$ abelsch ist, stimmt diese Menge auch mit der Rechtsnebenklasse $n\mathbb{Z} + x$ überein.

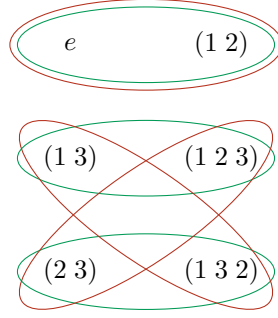


Abbildung 7: Linksnebenklassen (grün) und Rechtsnebenklassen (rot) der Untergruppe $H = \{e, (1\ 2)\} \subseteq S_3$.

2.2.25 Beispiel. Die Links- und Rechtsnebenklassen von $H = \{e, (1\ 2)\} \subseteq S_3$ sind in Abbildung 7 dargestellt. Wie wir in Lemma 2.2.26 sehen werden, bilden beide Arten von Nebenklassen eine Zerlegung der Gruppe.

Die Menge der Linksnebenklassen einer Untergruppe $H \subseteq G$ wird oft mit

$$G/H := \{xH \mid x \in G\}$$

bezeichnet. Zu beachten ist bei dieser Notation, dass falls $xH = yH$ gilt, dann sind diese beiden Nebenklassen identisch, repräsentieren also das gleiche Element von G/H . Nach dieser Definition ist G/H also eine Menge von Mengen. Dafür kann man auch folgende alternative Beschreibung verwenden: zwei Gruppenelemente $x, y \in G$ heißen **äquivalent modulo H** falls

$$x^{-1}y \in H. \quad (2.16)$$

In Anlehnung an den Fall von ganzen Zahlen (Beispiel 2.2.24) schreiben wir dies auch als

$$x \equiv y \pmod{H}.$$

Jetzt bedeutet (2.16) aber gerade, dass $x^{-1}yH = H$, oder anders geschrieben $yH = xH$. Somit sind die Nebenklassen also gerade die Äquivalenzklassen bezüglich der Äquivalenzrelation “ $\equiv \pmod{H}$ ”. Da eine Äquivalenzrelation auf einer Menge dieser immer in Äquivalenzklassen zerlegt, folgt daraus unmittelbar das folgende Lemma.

2.2.26 Lemma. Die Linksnebenklassen einer Untergruppe $H \subseteq G$ bilden eine Zerlegung von G , das heißt sie sind paarweise disjunkt und ihre Vereinigung ist ganz G .

Beweis. Für jedes $x \in G$ gilt offensichtlich $x \in xH$ da $e \in H$, also ist die Vereinigung aller Linksnebenklassen ganz G .

Nun zur paarweisen Disjunktheit. Es seien also xH und yH zwei beliebige Linksnebenklassen. Dann ist zu zeigen, dass entweder $xH = yH$ oder $xH \cap yH = \emptyset$ gilt. Falls $xH \cap yH \neq \emptyset$ ist, dann gibt es also ein Element $z \in G$ mit $z \in xH$ und $z \in yH$. Nach (2.16) bedeutet dies, dass

$$x^{-1}z \in H \quad \text{und} \quad y^{-1}z \in H.$$

Damit liegt auch das Element

$$(x^{-1}z)(y^{-1}z)^{-1} = x^{-1}zz^{-1}y = x^{-1}y$$

in H , so dass $x \equiv y \pmod{H}$ gilt, oder (wie oben bemerkt) $xH = yH$. $\square$

Alle Aussagen für Linksnebenklassen gelten analog auch für Rechtsnebenklassen, da man ja nur die Reihenfolge der Multiplikation ändert, sonst aber durchweg die gleichen Überlegungen anstellen kann. Für die Menge der Rechtsnebenklassen schreibt man manchmal auch

$$H \backslash G := \{Hx \mid x \in G\}.$$

Diese bilden also ebenfalls eine Zerlegung von G . Siehe Abbildung 7 für ein Beispiel dafür, wie diese beiden Zerlegungen ausschauen können.

2.2.27 Satz (Lagrange). Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Dann ist $|H|$ ein Teiler von $|G|$.

Beweis. Alle Linksnebenklassen haben dieselbe Anzahl von Elementen wie H , denn für jedes $x \in G$ ist die Multiplikation mit x von links

$$\begin{aligned} H &\longrightarrow xH \\ y &\longmapsto xy \end{aligned}$$

eine Bijektion, wobei die inverse Abbildung durch Multiplikation mit x^{-1} von links gegeben ist. Die Anzahl der Elemente von G ist somit gleich der Anzahl der Linksnebenklassen multipliziert mit der Anzahl der Elemente von H , also

$$|G| = |G/H| \cdot |H|, \quad (2.17)$$

so dass $|H|$ ein Teiler von $|G|$ ist. $\square$

2.2.28 Satz. Falls G eine endliche Gruppe und die Anzahl der Elemente $|G|$ eine Primzahl ist, dann ist G zyklisch.

Beweis. Sei x ein beliebiges Element von G , das nicht das neutrale Element ist. Dann bilden die Potenzen x^k für $k \in \mathbb{Z}$ eine Untergruppe von G . Nach Satz 2.2.27 ist die Anzahl der Elemente dieser Untergruppe ein Teiler von $|G|$, was als Primzahl vorausgesetzt ist. Also muss die Untergruppe entweder 1 oder $|G|$ Elemente haben.

Da $x \neq e$, hat die Untergruppe mindestens zwei Elemente, nämlich e und x . Also muss die Untergruppe $|G|$ Elemente haben, und somit ganz G sein. Deshalb ist G von x erzeugt, also zyklisch.⁹ $\square$

Wir kehren zur Betrachtung von normalen Untergruppen zurück und stellen fest, dass Normalität äquivalent als “Linksnebenklasse = Rechtsnebenklasse” formuliert werden kann.

2.2.29 Lemma. Für eine Untergruppe $N \subseteq G$ sind äquivalent:

- (a) N ist normal in G .
- (b) Für alle $a \in G$ gilt $aN = Na$.

Beweis. Sei N normal. Dann gilt $aNa^{-1} = N$ für alle $a \in G$ nach Bemerkung 2.2.20(a), also durch Multiplikation mit a von rechts die Gleichheit $aN = Na$. Die andere Richtung folgt analog durch Multiplikation mit a^{-1} von rechts. $\square$

2.2.30 Definition. Sei $N \subseteq G$ eine normale Untergruppe. Die **Quotientengruppe** G/N ist definiert als die Menge der Nebenklassen

$$G/N := \{xN \mid x \in G\}$$

mit der Verknüpfung

$$(xN) \cdot (yN) := xyN.$$

2.2.31 Satz. Das so definierte G/N ist eine Gruppe.

Beweis. Wir müssen zunächst zeigen, dass die Verknüpfung überhaupt wohldefiniert ist, also dass sie nicht von der Wahl der Repräsentanten x und y abhängt. Falls $xN = x'N$ und $yN = y'N$ gelten, dann müssen wir also zeigen, dass $xyN = x'y'N$ folgt. Dies sieht man am einfachsten anhand von Lemma 2.2.29, was ergibt

$$xyN = xNy = x'Ny = x'y'N = x'y'N,$$

so dass die Wohldefiniertheit bewiesen ist.

⁹Wir haben sogar bewiesen, dass G von jedem Element außer dem neutralen Element erzeugt wird.

Die Gruppenaxiome gelten, weil sie in G gelten. Insbesondere gilt die Assoziativität, weil die Multiplikation der Nebenklassen der Multiplikation der Repräsentanten entspricht, für welche die Assoziativität nach Voraussetzung gilt. Dass die Nebenklasse eN ein neutrales Element für die Verknüpfung ist folgt aus

$$(xN) \cdot (eN) = xeN = xN.$$

Das Inverse von xN ist $x^{-1}N$, denn

$$(xN) \cdot (x^{-1}N) = xx^{-1}N = eN.$$

Damit sind alle Gruppenaxiome erfüllt. $\square$

2.2.32 Bemerkung. Falls G eine additiv geschriebene abelsche¹⁰ Gruppe ist und $H \subseteq G$ eine Untergruppe, dann sind die Nebenklassen von der Form

$$x + H = \{x + y \mid y \in H\}.$$

Zum Beispiel ist für $n \in \mathbb{N}$ die Quotientengruppe $\mathbb{Z}/n\mathbb{Z}$ die Menge der Restklassen ganzer Zahlen modulo n mit der Addition als Verknüpfung, also

$$(x + n\mathbb{Z}) + (y + n\mathbb{Z}) = (x + y) + n\mathbb{Z}.$$

Der folgende Satz erklärt jetzt, warum die Gruppen $\mathbb{Z}/n\mathbb{Z}$ wichtig sind: es handelt sich genau um die endlichen zyklischen Gruppen.

2.2.33 Satz. (a) Jede endliche zyklische Gruppe ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$ mit $n = |G|$.

(b) Jede unendliche zyklische Gruppe ist isomorph zu $\mathbb{Z}$.

Beweis. (a) $\mathbb{Z}/n\mathbb{Z}$ ist zyklisch, erzeugt durch die Nebenklasse $1 + n\mathbb{Z}$, da die Elemente alle von der Form

$$k + n\mathbb{Z} = \underbrace{(1 + n\mathbb{Z}) + \cdots + (1 + n\mathbb{Z})}_{k \text{ mal}}$$

für $k \in \mathbb{N}$ sind. Die Behauptung folgt somit aus Lemma 2.2.6.

(b) Analog zum vorherigen Fall ist $\mathbb{Z}$ von 1 erzeugt, und die Behauptung folgt wieder aus Lemma 2.2.6. $\square$

Weitere Beispiele für Quotientengruppen werden wir im folgenden Abschnitt kennenlernen.

2.3 Der erste Isomorphiesatz

Bevor wir zur Gruppentheorie kommen zunächst eine rein mengentheoretische Beobachtung. Sei $f : X \rightarrow Y$ eine Abbildung zwischen Mengen. Dann definiert die Abbildung f eine Äquivalenzrelation $\sim$ auf X durch

$$x \sim x' \quad :\Longleftrightarrow \quad f(x) = f(x').$$

Dabei folgen die Eigenschaften einer Äquivalenzrelation (Reflexivität, Symmetrie, Transitivität) unmittelbar aus der Tatsache, dass diese Eigenschaften für $=$ gelten.

Wenn $X/\sim$ die Menge der Äquivalenzklassen bezüglich dieser Relation bezeichnet, dann gibt es eine kanonische Abbildung

$$\begin{aligned} X &\twoheadrightarrow X/\sim \\ x &\longmapsto [x] \end{aligned}$$

welche jedes Element auf seine Äquivalenzklasse abbildet. Die Notation “ $\twoheadrightarrow$ ” soll dabei andeuten, dass diese Abbildung surjektiv ist. Andererseits haben wir auch die kanonische Inklusionsabbildung

$$\text{im}(f) \hookrightarrow Y,$$

wobei die Notation “ $\hookrightarrow$ ” auf die Injektivität dieser Abbildung hinweist.¹¹ Diese beiden Abbildungen zusammen liefern eine kanonische Zerlegung von f im folgenden Sinne.

¹⁰Wir verwenden additive Schreibweise nur für abelsche Gruppen.

¹¹Vgl. das Ende des Pfeils mit dem Teilmengensymbol $\subset$.

2.3.1 Satz. Für jede Abbildung $f : X \rightarrow Y$ gibt es eine eindeutige Abbildung $\tilde{f} : X/\sim \rightarrow \text{im}(f)$, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow & \nearrow \\ & X/\sim & \xrightarrow{\tilde{f}} \text{im}(f) \end{array} \quad (2.18)$$

Dieses $\tilde{f}$ ist eine Bijektion.

2.3.2 Beispiel. Vor dem formalen Beweis kann ein Alltagsbeispiel der Veranschaulichung dienen. Sei dazu X die Menge aller Menschen und Y die Menge der endlichen Folgen von Buchstaben. Dann gibt es eine Abbildung $f : X \rightarrow Y$, welche jeder Person ihren Namen zuordnet. Die Äquivalenzrelation $\sim$ betrachtet zwei Menschen genau dann als äquivalent, wenn sie denselben Namen haben. Der Aussage des Satzes ist jetzt also: die Äquivalenzklassen—also die Mengen von Menschen mit demselben Namen—entsprechen genau den Symbolfolgen, welche als Namen verwendet werden. Diese Entsprechung ist implementiert durch die Abbildung $\tilde{f}$, welche jeder Äquivalenzklasse den Namen zuordnet, den alle Personen in dieser Klasse gemeinsam haben.

Beweis. Zunächst zur Existenz. Wir definieren $\tilde{f}$ durch $\tilde{f}([x]) := f(x)$, was offensichtlich zu $\text{im}(f)$ gehört. Dies ist wohldefiniert: falls $x \sim x'$, dann ist nach Definition ja $f(x) = f(x')$, also $\tilde{f}([x]) = \tilde{f}([x'])$.

Zur Eindeutigkeit sei $g : X/\sim \rightarrow \text{im}(f)$ eine Abbildung, so dass das Diagramm

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow & \nearrow \\ & X/\sim & \xrightarrow{g} \text{im}(f) \end{array}$$

kommutiert. Dies bedeutet aber gerade, dass $g([x]) = f(x)$ für alle $x \in X$ gilt. Somit muss bereits $g = \tilde{f}$ sein. $\square$

Jetzt ist es relativ einfach, eine entsprechende Aussage für Gruppen zu formulieren und zu beweisen.

2.3.3 Satz. Sei $f : G \rightarrow H$ ein Gruppenhomomorphismus. Dann gibt es einen eindeutigen Gruppenisomorphismus $\tilde{f} : G/\ker(f) \rightarrow \text{im}(f)$, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ & \searrow & \nearrow \\ & G/\ker(f) & \xrightarrow{\tilde{f}} \text{im}(f) \end{array} \quad (2.19)$$

Insbesondere gilt also

$$\boxed{G/\ker(f) \cong \text{im}(f).}$$

Die wesentliche Zusatzaussage von Satz 2.3.3 ist, dass der Isomorphismus explizit angegeben wird. Man spricht auch vom **ersten Isomorphiesatz** für Gruppen.

Beweis. Wir stellen zunächst fest, dass für alle $x, y \in G$ gilt

$$f(x) = f(y) \iff x \equiv y \pmod{\ker(f)}.$$

Denn $f(x) = f(y)$ ist äquivalent zu $f(x^{-1}y) = e_H$, also $x^{-1}y \in \ker(f)$, was per Definition von Kongruenz modulo $\ker(f)$ entsprechend (2.16) sich gerade als $x \equiv y \pmod{\ker(f)}$ schreiben lässt.

Somit sind die Nebenklassen $x\ker(f)$ also genau die Äquivalenzklassen bezüglich der Relation aus Satz 2.3.1, und die Diagramme (2.18) und (2.19) enthalten genau die gleichen Abbildungen.

Die Aussage ist also schon aus Satz 2.3.1 bekannt, abgesehen von der Behauptung, dass $\tilde{f}$ ein Homomorphismus ist. Dies müssen wir noch nachrechnen.

Dazu seien xN und yN zwei beliebige Elemente von $G/\ker(f)$. Dann gilt

$$\tilde{f}((xN) \cdot (yN)) = \tilde{f}(xyN) = f(xy) = f(x)f(y) = \tilde{f}(xN) \cdot \tilde{f}(yN),$$

so dass $\tilde{f}$ tatsächlich ein Homomorphismus ist. $\square$

Nicht nur ist der Beweis für Gruppenfall fast identisch zu dem für Mengen; auch die folgenden Beispiele versteht man am besten mit Beispiel 2.3.2 im Hinterkopf.

2.3.4 Beispiel. (a) Für den Homomorphismus $\text{sgn} : S_n \rightarrow \{1, -1\}$ ist der Kern die alternierende Gruppe A_n (Beispiel 2.2.19(b)). Die Nebenklassen σA_n sind dann genau die Mengen der geraden bzw. ungeraden Permutationen, wobei der Repräsentant σ eine beliebige gerade bzw. ungerade Permutation sein kann. Zwei Permutationen werden also als äquivalent modulo A_n betrachtet, wenn sie dieselbe Parität haben. Der Isomorphismus $\widetilde{\text{sgn}} : S_n/A_n \rightarrow \{1, -1\}$ besagt dann einfach, dass man die Äquivalenzklassen auch einfach direkt mit 1 bzw. -1 identifizieren kann, und sich die Multiplikation der Äquivalenzklassen genau wie die Multiplikation von 1 und -1 verhält.

(b) Ähnliches gilt für den Determinanten-Homomorphismus $\det : \text{GL}_n(K) \rightarrow K^\times$. Der Kern ist die spezielle lineare Gruppe $\text{SL}_n(K)$, und zwei Matrizen $A, B \in \text{GL}_n(K)$ sind genau dann äquivalent modulo $\text{SL}_n(K)$, wenn sie denselben Determinantenwert haben. Die Multiplikation der Äquivalenzklassen entspricht dann der Multiplikation der Determinantenwerte.

(c) Die euklidische Gruppe $E(n)$ aus Beispiel 2.1.16 enthält die Abbildungen der Form $f(x) = Ax + b$ mit $A \in O(n)$ und $b \in \mathbb{R}^n$. Wir können die Gruppenelemente also als Paare (A, b) mit $A \in O(n)$ und $b \in \mathbb{R}^n$ schreiben. Aufgrund von

$$A'(Ax + b) + b' = (A'A)x + (A'b + b')$$

ist in der Schreibweise mit Paaren die Gruppenverknüpfung durch

$$(A', b') \cdot (A, b) = (A'A, A'b + b')$$

gegeben. Aus dieser Gleichung wird klar, dass die Projektion auf die erste Komponente ein Homomorphismus

$$\begin{aligned} \pi : E(n) &\longrightarrow O(n) \\ (A, b) &\longmapsto A \end{aligned}$$

ist.¹² Der Kern $\ker(\pi)$ besteht aus den Abbildungen der Form $(1_{n \times n}, b)$ mit $b \in \mathbb{R}^n$, also den reinen Translationen $f(x) = x + b$.

Aus Satz 2.3.3 gewinnen wir also die Aussage: die Quotientengruppe $E(n)/\ker(\pi)$ ist isomorph zur orthogonalen Gruppe $O(n)$. Eine orthogonale Matrix $A \in O(n)$ wird also durch die Nebenklasse aller euklidischen Bewegungen dargestellt, die dieselbe lineare Komponente A haben.

Satz 2.3.3 ist der erste von insgesamt drei Isomorphiesätzen, die in der Gruppentheorie eine zentrale Rolle spielen. Die beiden anderen können aus dem ersten abgeleitet werden. Dies wird in den Übungen betrachtet werden.

¹²Man kann diesen Homomorphismus auch geometrisch interpretieren: betrachtet man den Sternenhimmel und führt eine euklidische Bewegung durch, so wird der Sternenhimmel *rotiert* (und/oder gespiegelt). Die Rotation ist gerade durch die Matrix A beschrieben, weil die Translation b den Sternenhimmel nicht verändert. Etwas formaler ausgedrückt: A beschreibt, wie die Bewegung auf sehr weit entfernten Punkten wirkt, wo die Translation einen vergleichsweise viel kleineren Effekt hat.

2.4 Gruppenwirkungen

Achtung: ab hier werden generische Gruppenelemente mit $g, h, \dots$ bezeichnet. Dies wäre vermutlich von Beginn an besser gewesen

Wir haben die Gruppentheorie durch die Betrachtung von Symmetrien motiviert. Dabei ist die Symmetriegruppe eines mathematischen Objekts mit Grundmenge X per Definition eine Untergruppe der symmetrischen Gruppe S_X , nämlich die Untergruppe der strukturerhaltenden Bijektionen. Wenn wir diese Symmetriegruppe aber allein als Gruppe betrachten, dann verlieren wir alle Information darüber, wie diese Symmetrien auf der Menge X wirken. Um diese Information zu behalten, betrachten hier Gruppen zusammen mit einer Wirkung auf einer Menge. Diese Theorie der Gruppenwirkungen ist mächtiges Werkzeug auch für die abstrakte Gruppentheorie selbst.

2.4.1 Definition. Eine **Gruppenwirkung** oder kurz **Wirkung** einer Gruppe G auf einer Menge X ist eine Abbildung

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto gx \end{aligned}$$

so dass für alle $g, h \in G$ und alle $x \in X$ gilt:

(a) Assoziativgesetz:

$$g(hx) = (gh)x. \quad (2.20)$$

(b) Neutrales Element:

$$ex = x. \quad (2.21)$$

Wie im ersten Absatz angedeutet, ist diese Definition durch folgende Klasse von Beispielen motiviert.

2.4.2 Beispiel. (a) Für jede Menge X wirkt die symmetrische Gruppe S_X auf X durch

$$\begin{aligned} S_X \times X &\longrightarrow X \\ (\sigma, x) &\longmapsto \sigma(x). \end{aligned}$$

Das Assoziativgesetz nimmt hier die Form

$$\sigma(\tau(x)) = (\sigma \circ \tau)(x)$$

an, was nach Definition der Verknüpfung $\circ$ in S_X gilt. Das neutrale Element ist die Identität id_X , welche in der Tat jedes Element auf sich selbst abbildet.

(b) Für jede Untergruppe $G \subseteq S_X$ ist die Einschränkung der obigen Wirkung eine Gruppenwirkung von G auf X . Jede Symmetriegruppe eines mathematischen Objekts wirkt also auf der Grundmenge dieses Objekts.

Zum Beispiel hatten wir die euklidische Gruppe $E(n)$ als Symmetriegruppe des euklidischen Raums $\mathbb{R}^n$ betrachtet (Beispiel 2.1.16). Eine Symmetrie $f \in E(n)$ hatte dabei die Form $f(x) = Ax + b$ für eine orthogonale Matrix $A \in O(n)$ und einen Vektor $b \in \mathbb{R}^n$. Diese Symmetriegruppe wirkt also per Definition auf dem $\mathbb{R}^n$, weil ein Element $f \in E(n)$ einen Punkt $x \in \mathbb{R}^n$ auf den Punkt $f(x) = Ax + b$ abbildet. Die Axiome einer Gruppenwirkung gelten aus dem gleichen Grund wie in (a).

(c) Sei weiters

$$S^{n-1} := \{x \in \mathbb{R}^n \mid \|x\| = 1\}$$

die Einheitssphäre im $\mathbb{R}^n$. Da die orthogonale Gruppe $O(n)$ aus linearen Abbildungen besteht, die Längen erhalten, wirkt $O(n)$ auf S^{n-1} durch Einschränkung der linearen Abbildungen auf S^{n-1} ,

$$\begin{aligned} O(n) \times S^{n-1} &\longrightarrow S^{n-1} \\ (A, x) &\longmapsto Ax. \end{aligned}$$

2.4.3 Lemma. Für jede Gruppenwirkung $G \times X \rightarrow X$ und jedes $g \in G$ ist die Wirkung von g , welche durch

$$\begin{aligned} X &\longrightarrow X \\ x &\longmapsto gx \end{aligned}$$

gegeben ist, eine Bijektion.

Beweis. Die inverse Abbildung ist

$$\begin{aligned} X &\longrightarrow X \\ x &\longmapsto g^{-1}x, \end{aligned}$$

denn für alle $x \in X$ gilt

$$g^{-1}(gx) = (g^{-1}g)x = ex = x,$$

und

$$g(g^{-1}x) = (gg^{-1})x = ex = x. \quad \square$$

Das folgende Lemma liefert eine alternative Beschreibung von Gruppenwirkungen.

2.4.4 Lemma. Äquivalent zu einer Gruppenwirkung im Sinne von Definition 2.4.1 ist die Angabe eines Gruppenhomomorphismus $\varphi : G \rightarrow S_X$.

Zum Beispiel wird so klar, dass die Symmetriegruppe eines Objekts $G \subseteq S_X$ bereits durch die Inklusionsabbildung $G \subseteq S_X$ auf X wirkt.

Beweis. Gegeben einen solchen Homomorphismus, so kann eine Wirkung durch

$$gx := \varphi(g)(x) \tag{2.22}$$

konstruiert werden. Denn es gelten (2.20) und (2.21) wegen der Homomorphieeigenschaft von φ ,

$$g(hx) = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x) = \varphi(gh)(x) = (gh)x, \tag{2.23}$$

und

$$ex = \varphi(e)(x) = \text{id}_X(x) = x.$$

Umgekehrt definiert eine Wirkung $G \times X \rightarrow X$ einen Homomorphismus $\varphi : G \rightarrow S_X$ durch

$$\varphi(g)(x) := gx. \tag{2.24}$$

Dank Lemma 2.4.3 gilt tatsächlich $\varphi(g) \in S_X$ für alle $g \in G$. Die Homomorphieeigenschaft ist im Prinzip die gleiche Rechnung wie (2.23),

$$\varphi(gh)(x) = (gh)x = g(hx) = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x).$$

Da dies für alle $x \in X$ gilt, folgt $\varphi(gh) = \varphi(g) \circ \varphi(h)$. Schließlich ist auch $\varphi(e) = \text{id}_X$ wegen (2.21).

Außerdem lässt sich leicht nachprüfen, dass die beiden Konstruktionen einer Wirkung aus einem Homomorphismus (2.22) und umgekehrt (2.24) zueinander invers sind. Daher haben wir tatsächlich eine Bijektion zwischen Gruppenwirkungen $G \times X \rightarrow X$ und Gruppenhomomorphismen $G \rightarrow S_X$ hergestellt. $\square$

2.4.5 Beispiel. Ein **dynamisches System** in diskreter Zeit ist eine Menge X zusammen mit einer Gruppenwirkung von $\mathbb{Z}$ auf X , wie in Abbildung 8 beispielhaft illustriert. Dabei stellen wir uns die Elemente von X als *Zustände* des Systems vor, also zum Beispiel die Positionen der Himmelskörper im Sonnensystem zu einem bestimmten Zeitpunkt. Die Gruppenwirkung

$$\begin{aligned} \mathbb{Z} \times X &\longrightarrow X \\ (n, x) &\longmapsto nx \end{aligned}$$

beschreibt dann die Entwicklung des Systems über die Zeit: der Zustand nx ist der Zustand, in dem sich das System nach n Zeiteinheiten befindet, wenn es zum Zeitpunkt 0 im Zustand x war. Die Bedingungen (2.20) und (2.21) entsprechen dabei den intuitiv erwarteten Eigenschaften der Zeitentwicklung: die Entwicklung um m Zeiteinheiten nach einer Entwicklung um n Zeiteinheiten entspricht der Entwicklung um $m + n$ Zeiteinheiten, und die Entwicklung um 0 Zeiteinheiten ändert den Zustand nicht.

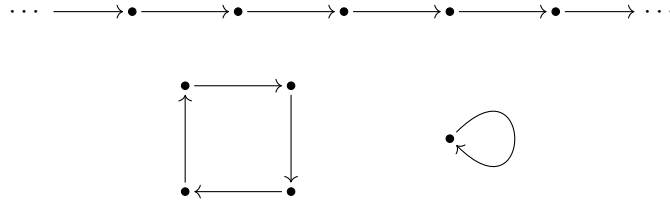


Abbildung 8: Ein Beispiel eines dynamischen Systems (Gruppenwirkung von $\mathbb{Z}$ auf einer Menge X). Die Pfeile geben an, wie das Element $1 \in \mathbb{Z}$ auf X wirkt. Mit anderen Worten: jeder Pfeil zeigt an, wie sich der Zustand des Systems in einem Zeitschritt verändert. Dadurch ist die Wirkung von beliebigen $n \in \mathbb{Z}$ auf X eindeutig bestimmt: folge den Pfeilen für n Schritte (insbesondere $|n|$ mal entgegen der Pfeilrichtung für $n < 0$).

2.4.6 Definition. Sei G eine Gruppe, die auf einer Menge X wirkt. Die **Bahn** eines Elements $x \in X$ ist dann die Menge aller Elemente, die von x durch die Wirkung von G erreicht werden können,

$$Gx := \{gx \mid g \in G\}.$$

Im dynamischen System aus Abbildung 8 gibt es genau drei Bahnen, und diese bilden eine Zerlegung der Grundmenge X in disjunkte Teilmengen. Dies ist tatsächlich immer der Fall, wie das folgende Lemma besagt.

2.4.7 Lemma. Die Bahnen einer Gruppenwirkung $G \times X \rightarrow X$ bilden eine Zerlegung von X in disjunkte Teilmengen.

Beweis. Zu zeigen sind hierbei zwei Dinge:

▷ Jedes $x \in X$ liegt in mindestens einer Bahn.

Dies ist klar, da $ex = x$ nach (2.21) gilt, also $x \in Gx$.

▷ Für alle $x_1, x_2 \in X$ sind die Bahnen entweder identisch oder disjunkt,

$$Gx_1 = Gx_2 \quad \text{oder} \quad Gx_1 \cap Gx_2 = \emptyset.$$

Betrachten wir also den Fall, dass $Gx_1 \cap Gx_2 \neq \emptyset$. Dann gibt es $y \in Gx_1 \cap Gx_2$, also existieren $g_1, g_2 \in G$ mit

$$y = g_1x_1 = g_2x_2.$$

Damit folgt aber bereits $Gx_1 = Gy$, denn alle Punkte die von x_1 erreicht werden können, können aufgrund von $x_1 = g_1^{-1}y$ auch von y erreicht werden, und umgekehrt. Formal geschrieben haben wir $Gg_1 = G$ dank der Invertierbarkeit von g_1 , also

$$Gy = Gg_1x_1 = Gx_1.$$

Nach dem gleichen Argument gilt auch $Gy = Gx_2$, also insgesamt $Gx_1 = Gx_2$. $\square$

Man wird vielleicht feststellen, dass dieser Beweis ganz analog zum Beweis von Lemma 2.2.26 verläuft, wo wir eine Gruppe in Linksnebenklassen bezüglich einer Untergruppe zerlegt haben. Dies ist kein Zufall, denn Lemma 2.2.26 ist tatsächlich ein Spezialfall von Lemma 2.4.7, wie das folgende Beispiel zeigt.

2.4.8 Beispiel. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann wirkt H auf G durch Multiplikation von links,

$$\begin{aligned} H \times G &\longrightarrow G \\ (h, g) &\longmapsto hg. \end{aligned}$$

Die Bahnen dieser Wirkung sind dann per Definition gerade die Rechtsnebenklassen Hg für $g \in G$. Somit folgt als Anwendung von Lemma 2.4.7, dass die Rechtsnebenklassen eine Zerlegung von G bilden.

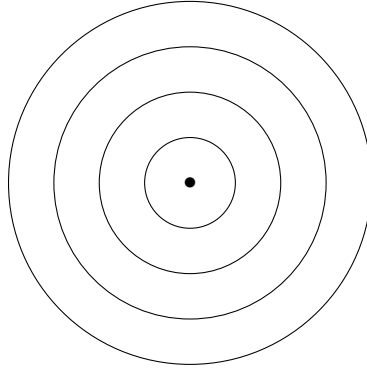


Abbildung 9: Bahnen der Wirkung von $O(2)$ auf $\mathbb{R}^2$.

Die Formulierung von Lemma 2.2.26 war aber für Linksnebenklassen. Bekommen wir diese auch als Bahnen einer Gruppenwirkung? In der Tat können auch die Multiplikation von rechts verwenden, um eine Wirkung von H auf G zu definieren, müssen dann aber das inverse Element verwenden:

$$\begin{aligned} H \times G &\longrightarrow G \\ (h, g) &\longmapsto gh^{-1}. \end{aligned}$$

Denn nur so bekommen wir das Assoziativgesetz in der Form (2.20) aus der Assoziativität der Gruppenverknüpfung,

$$(gh_1^{-1})h_2^{-1} = g(h_2h_1)^{-1}.$$

Mit dieser Definition sind die Bahnen tatsächlich die Linksnebenklassen gH für $g \in G$, und Lemma 2.2.26 erhalten wir als Spezialfall von Lemma 2.4.7.

Weitere Beispiele

2.4.9 Beispiel. (a) $GL_n(K)$ wirkt auf K^n durch Matrix-Vektor-Multiplikation. In diesem Fall gibt es genau zwei Bahnen: den Nullvektor $\{0\}$ und sein Komplement $K^n \setminus \{0\}$. Denn der Nullvektor wird nur auf sich selbst abgebildet, während durch geeignete Wahl von $A \in GL_n(K)$ jeder Vektor $x \in K^n \setminus \{0\}$ auf jeden anderen Vektor $y \in K^n \setminus \{0\}$ abgebildet werden kann.

(b) Wir können die Wirkung von $GL_n(\mathbb{R})$ auf $\mathbb{R}^n$ auch auf $O(n)$ einschränken, also

$$\begin{aligned} O(n) \times \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ (A, x) &\longmapsto Ax. \end{aligned}$$

Die Bahnen in diesem Fall sind die Sphären

$$S_r^{n-1} := \{x \in \mathbb{R}^n \mid \|x\| = r\}$$

für $r \geq 0$. Denn einerseits bleiben Längen durch orthogonale Matrizen erhalten, und andererseits kann durch geeignete Wahl von $A \in O(n)$ jeder Vektor x mit $\|x\| = r$ auf jeden anderen Vektor y mit $\|y\| = r$ abgebildet werden.¹³ Wieder ist der Ursprung seine eigene Bahn, nämlich $S_0^{n-1} = \{0\}$.

Was können wir darüber aussagen, wie die Bahnen einer Gruppenwirkung ausschauen können? Insbesondere, wie viele Elemente hat eine Bahn? Wie wir sehen wird ist dafür der folgende Begriff nützlich.

2.4.10 Definition. Sei G eine Gruppe, die auf einer Menge X wirkt. Dann ist der **Stabilisator** eines Elements $x \in X$ die Untergruppe von Elementen, die x fixieren,

$$\text{Stab}(x) := \{g \in G \mid gx = x\}.$$

¹³Dies ist nicht ganz offensichtlich, kann aber mit geeigneten Methoden der linearen Algebra gezeigt werden (zum Beispiel Gram-Schmidt-Orthogonalisierung).

Dass der Stabilisator tatsächlich eine Untergruppe ist, ist leicht zu sehen: für $g, h \in \text{Stab}(x)$ gilt $gx = x$ und $hx = x$, also auch

$$(gh)x = g(hx) = gx = x \quad \text{und} \quad g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = ex = x,$$

also auch $gh \in \text{Stab}(x)$ und $g^{-1} \in \text{Stab}(x)$. Außerdem enthält $\text{Stab}(x)$ das neutrale Element e , da $ex = x$.

2.4.11 Beispiel. Für ein dynamisches System im Sinne von Beispiel 2.4.5 und einen Zustand x ist $\text{Stab}(x)$ die Menge aller Zeitschritte, die den Zustand x unverändert lassen.

2.4.12 Beispiel. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann wirkt G auf der Menge der Linksnebenklassen G/H durch

$$\begin{aligned} G \times (G/H) &\longrightarrow G/H \\ (g, \tilde{g}H) &\longmapsto g\tilde{g}H. \end{aligned}$$

Dies ist wohldefiniert, weil $\hat{g}H = \tilde{g}H$ ergibt $g\hat{g}H = g\tilde{g}H$. Die Axiome einer Gruppenwirkung folgen direkt aus den Gruppenaxiomen in G .

Dieses Beispiel ist hier relevant, weil sich der Stabilisator einer Nebenklasse gH leicht bestimmen lässt:

$$\begin{aligned} \text{Stab}(gH) &= \{k \in G \mid kgH = gH\} \\ &= \{k \in G \mid g^{-1}kgH = H\} \\ &= \{k \in G \mid g^{-1}kg \in H\} \\ &= gHg^{-1}. \end{aligned}$$

Es handelt sich also um eine Untergruppe, die konjugiert zu H ist. Insbesondere gilt

$$\text{Stab}(eH) = H.$$

Stabilisatoren sind deswegen relevant, weil sie die Elemente einer Bahn gut beschreiben. Wir werden sehen, dass folgende Aussage nicht nur oberflächlich Ähnlichkeit mit dem ersten Isomorphiesatz (Satz 2.3.3) hat.

2.4.13 Satz (Bahnstabilisatorsatz). Für jedes $x \in X$ ist die Abbildung

$$\begin{aligned} G/\text{Stab}(x) &\longrightarrow Gx \\ g\text{Stab}(x) &\longmapsto gx \end{aligned} \tag{2.25}$$

eine wohldefinierte Bijektion.

Auch der Beweis entspricht dem des ersten Isomorphiesatzes.

Beweis. Für die Wohldefiniertheit sei $g'\text{Stab}(x) = g\text{Stab}(x)$. Dann gibt es also $h \in \text{Stab}(x)$ mit $g' = gh$, und somit

$$g'x = (gh)x = g(hx) = gx,$$

was zu zeigen war.

Die Abbildung ist surjektiv per Definition der Bahn Gx . Es bleibt also noch zu zeigen, dass die Abbildung injektiv ist. Dazu sei $g_1, g_2 \in G$ mit $g_1x = g_2x$. Dann folgt

$$g_2^{-1}g_1x = x,$$

also $g_2^{-1}g_1 \in \text{Stab}(x)$ und somit $g_1\text{Stab}(x) = g_2\text{Stab}(x)$. Deshalb ist die Abbildung auch injektiv, also bijektiv. $\square$

2.4.14 Bemerkung. Alternativ könnten wir Satz 2.4.13 auch folgendermaßen formulieren. Es gibt eine eindeutige Abbildung $G/\text{Stab}(x) \rightarrow Gx$, die das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{g \mapsto gx} & X \\ & \searrow & \nearrow \\ & G/\text{Stab}(x) \longrightarrow Gx & \end{array}$$

kommutativ macht, und diese Abbildung ist bijektiv. Denn um das Diagramm kommutativ zu machen, muss die Abbildung $G/\text{Stab}(x) \rightarrow Gx$ genau so definiert werden wie in Satz 2.4.13, also $g\text{Stab}(x) \mapsto gx$.

Die Ähnlichkeit von Satz 2.4.13 mit dem ersten Isomorphiesatz ist kein Zufall, wie das folgende Beispiel zeigt.

2.4.15 Beispiel. Sei $f : G \rightarrow H$ ein Gruppenhomomorphismus. Dann wirkt G auf H durch

$$\begin{aligned} G \times H &\longrightarrow H \\ (g, h) &\longmapsto f(g)h. \end{aligned}$$

Der Stabilisator von $e_H \in H$ ist dann gerade $\text{Stab}(e_H) = \ker(f)$, und die Bahn von e_H ist

$$Ge_H = \{f(g) \mid g \in G\} = \text{im}(f).$$

Auf diese Weise wird der erste Isomorphiesatz (Satz 2.3.3) *fast* zu einem Spezialfall von Satz 2.4.13. Ein wesentlicher Unterschied ist, dass der Isomorphiesatz auch besagt, dass $G/\ker(f) \rightarrow \text{im}(f)$ ein *Gruppenisomorphismus* ist. Im Bahnstabilisatorsatz haben wir aber nur eine Bijektion von Mengen.¹⁴

2.4.16 Beispiel. Betrachten wir die Wirkung von S_n auf $X = \{1, \dots, n\}$ (Beispiel 2.4.2(a)). Die Bahn von $n \in X$ ist dann offensichtlich die gesamte Menge $\{1, \dots, n\}$, da wir durch Permutation n auf jedes andere Element abbilden können. Der Stabilisator von n ist die Untergruppe von Permutationen, die n fixieren. Dies ist aber gerade die Gruppe der Permutationen von $\{1, \dots, n-1\}$, also S_{n-1} .

Der Bahnstabilisatorsatz liefert somit eine Bijektion

$$S_n/S_{n-1} \xrightarrow{\cong} \{1, \dots, n\}.$$

Diese entsteht dadurch, dass wir jeder Linksnebenklasse σS_{n-1} das Bild $\sigma(n)$ zuordnen.

Eine oft gebrauchte Folgerung aus dem Bahnstabilisatorsatz ist die folgende Aussage über die Kardinalität von Bahnen.

2.4.17 Satz. Sei G eine endliche Gruppe, welche auf einer endlichen Menge X wirkt, und $R \subseteq X$ eine Teilmenge, die aus jeder Bahn genau einen Repräsentanten enthält. Dann gilt

$$|X| = \sum_{x \in R} \frac{|G|}{|\text{Stab}(x)|}, \quad (2.26)$$

wobei jeder Term auf der rechten Seite ganzzahlig ist.

Beweis. Für jedes $x \in R$ gilt nach dem Satz von Lagrange (2.17), dass

$$|G/\text{Stab}(x)| = \frac{|G|}{|\text{Stab}(x)|},$$

und insbesondere ist die rechte Seite ganzzahlig. Die Bijektion (2.25) liefert also

$$|Gx| = |G/\text{Stab}(x)| = \frac{|G|}{|\text{Stab}(x)|}.$$

¹⁴Es gibt aber noch eine stärkere Version des Bahnstabilisatorsatzes, die wir nicht behandeln werden, und die tatsächlich den Isomorphiesatz voll umfasst.

Weiterhin zerlegt Lemma 2.4.7 die Menge X in Bahnen. Da wir mit R genau einen Repräsentanten pro Bahn gewählt haben, gilt somit

$$|X| = \sum_{x \in R} |Gx| = \sum_{x \in R} \frac{|G|}{|\text{Stab}(x)|},$$

was zu zeigen war. $\square$

Das folgende Ergebnis dient als beispielhafte Anwendung.

2.4.18 Satz. *Sei X eine endliche Menge mit ungerade vielen Elementen und $t : X \rightarrow X$ eine Abbildung mit $t \circ t = \text{id}_X$. Dann gibt es mindestens ein $x_0 \in X$ mit $t(x_0) = x_0$.*

Ein solches x_0 heißt auch **Fixpunkt**.

Beweis. Die Abbildung t definiert einen Gruppenhomomorphismus

$$\begin{aligned} \varphi : \mathbb{Z}/2\mathbb{Z} &\longrightarrow S_X \\ 0 + 2\mathbb{Z} &\longmapsto \text{id}_X \\ 1 + 2\mathbb{Z} &\longmapsto t, \end{aligned}$$

da dieser nach der Voraussetzung $t \circ t = \text{id}_X$ wohldefiniert ist.¹⁵ Nach der Korrespondenz von Lemma 2.4.4 entspricht dies einer Gruppenwirkung von $\mathbb{Z}/2\mathbb{Z}$ auf X .

Wenn wir jetzt (2.26) auf diese Gruppenwirkung anwenden, dann ist die linke Seite nach Voraussetzung ungerade. Da G in diesem Fall nur zwei Elemente hat, muss jeder Term auf der rechten Seite entweder 1 oder 2 sein. Damit die Summe ungerade sein kann, muss also mindestens ein Term den Wert 1 annehmen. Es muss also $x_0 \in X$ mit $\text{Stab}(x_0) = G$ geben. Ein solches x_0 ist ein Fixpunkt (nach Definition des Stabilisators), also $t(x_0) = x_0$. $\square$

2.4.19 Bemerkung. Satz 2.4.18 lässt sich auch leicht direkt beweisen: nehmen wir an, dass die Menge X nur Elemente enthält, die unter t *nicht* fix bleiben. Da diese immer als Paare $(x, t(x))$ auftreten, müsste $|X|$ also gerade sein. Dies ist bereits die gewünschte Aussage in kontrapositiver Form.

Dies ist aber eigentlich das gleiche Argument wie unser Beweis mit der Gruppenwirkung, da die Zerlegung von X in Paare und Fixpunkte genau die Bahnenzerlegung ist! Somit ist der Beweis mit Gruppenwirkungen eigentlich unnötig kompliziert. Mit den Gruppenwirkungen haben wir aber ein mächtiges Werkzeug, das uns Argumente dieser Form leicht auf andere Situationen verallgemeinern lässt.

Sogar in der Gruppentheorie selbst finden sich viele Anwendungen von Satz 2.4.18 und seinen Varianten, wie zum Beispiel folgende Aussage.

2.4.20 Korollar. *Sei G eine endliche Gruppe mit gerade vielen Elementen. Dann gibt es $g \in G$ mit*

$$g^2 = e, \quad g \neq e.$$

Beweis. Wir betrachten $X := G \setminus \{e\}$ mit $t : X \rightarrow X$ definiert durch $t(g) := g^{-1}$. Dann gilt $t \circ t = \text{id}_X$ wegen $(g^{-1})^{-1} = g$ für alle $g \in G$. $\square$

Auf die gleiche Weise wie Satz 2.4.18 lässt sich auch folgende allgemeinere Aussage zeigen.

2.4.21 Satz. *Sei X eine endliche Menge und $t : X \rightarrow X$ eine Bijektion mit $t^p = \text{id}_X$ für eine Primzahl p . Falls $p \nmid |X|$ gilt, dann hat t mindestens einen Fixpunkt.*

¹⁵Der einzige nichttriviale Fall der Homomorphieeigenschaft ist hier

$$\varphi(1 + 2\mathbb{Z}) \circ \varphi(1 + 2\mathbb{Z}) = t \circ t = \text{id}_X = \varphi(0 + 2\mathbb{Z}) = \varphi((1 + 2\mathbb{Z}) + (1 + 2\mathbb{Z})).$$

Beweis. Die Abbildung t definiert auch hier eine Wirkung der zyklischen Gruppe $\mathbb{Z}/p\mathbb{Z}$ auf X , gegeben durch

$$\begin{aligned}\mathbb{Z}/p\mathbb{Z} \times X &\longrightarrow X \\ (k + p\mathbb{Z}, x) &\longmapsto t^k(x).\end{aligned}$$

Die Bahnen haben entweder 1 oder p Elemente (da es nach dem Satz von Lagrange keine anderen Untergruppen gibt, die als Stabilisatoren in Frage kommen). Falls alle Bahnen p Elemente hätten, wäre $|X|$ durch p teilbar. Da dies nach Voraussetzung nicht der Fall ist, muss es mindestens eine Bahn mit 1 Element geben, also einen Fixpunkt. $\square$

2.4.22 Satz (Satz von Cauchy). *Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$. Dann gibt es ein Element $g \in G$ der Ordnung p .*

Beweis. Wir betrachten die Menge

$$X := \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = e\}.$$

Die ersten $p-1$ Einträge können beliebig gewählt werden, und danach ist g_p eindeutig bestimmt. Also gilt $|X| = |G|^{p-1}$, insbesondere $p \mid |X|$. Auf X wirkt die zyklische Verschiebung

$$t(g_1, \dots, g_p) := (g_2, \dots, g_p, g_1),$$

denn aus $g_1 \cdots g_p = e$ folgt $g_2 \cdots g_p g_1 = e$. Außerdem gilt $t^p = \text{id}_X$. Die Bahnen dieser Wirkung haben entweder 1 oder p Elemente. Da $p \mid |X|$ gilt, ist also auch die Anzahl der Fixpunkte durch p teilbar. Ein Fixpunkt ist genau ein Tupel $(g, \dots, g)$ mit $g^p = e$. Da $(e, \dots, e)$ ein solcher Fixpunkt ist, gibt es noch einen weiteren Fixpunkt $(g, \dots, g)$ mit $g \neq e$. Also gilt $g^p = e$ und somit hat g Ordnung p . $\square$

2.5 Auflösbare Gruppen

Auflösbare Gruppen sind eine Klasse von Gruppen, deren Struktur besonders gut durch sukzessive Zerlegungen in einfachere Gruppen beschrieben werden kann. Die Definition selbst ist im Moment relativ schwer zu motivieren. Wir werden aber in der Körpertheorie (Abschnitt 5) sehen, dass die Theorie auflösbare Gruppen bei der Untersuchung von Lösungsformeln für polynomiale Gleichungen sehr nützlich ist.

2.5.1 Definition. Eine Gruppe G heißt **auflösbar**, falls es eine endliche Kette von Untergruppen

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G \quad (2.27)$$

gibt, so dass $G_i \subseteq G_{i+1}$ normal ist für alle $i = 0, \dots, n-1$ und die Faktorgruppen G_{i+1}/G_i abelsch sind.

Als triviale Beispiele kann man jede abelsche Gruppe G betrachten, denn dann ist die Definition mit $n = 1$ erfüllt durch die Kette $\{e\} \subseteq G$, weil $G/\{e\} = G$ abelsch ist.

2.5.2 Beispiel. (a) Die alternierende Gruppe A_4 aus (2.14) ist auflösbar. Dazu sei

$$V_4 := \{e, (12)(34), (13)(24), (14)(23)\} \quad (2.28)$$

die Untergruppe, die aus den Doppeltranspositionen besteht. Dann ist

$$\{e\} \subseteq V_4 \subseteq A_4 \quad (2.29)$$

eine Kette wie in (2.27), denn:

▷ $\{e\} \subseteq V_4$ ist trivialerweise normal, und $V_4/\{e\} = V_4$ ist abelsch;

- ▷ $V_4 \subseteq A_4$ ist normal, da Doppeltranspositionen unter Konjugation mit einer beliebigen Permutation wieder auf Doppeltranspositionen abgebildet werden, z.B.

$$\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)).$$

Weiterhin ist A_4/V_4 eine Gruppe mit

$$|A_4/V_4| = \frac{|A_4|}{|V_4|} = \frac{12}{4} = 3$$

Elementen, also isomorph zu $\mathbb{Z}/3\mathbb{Z}$ (Satz 2.2.28) und somit ebenfalls abelsch.

- (b) Auch die symmetrische Gruppe S_4 ist auflösbar. Denn $A_4 \subseteq S_4$ ist normal, und somit können wir die Kette (2.29) erweitern zu

$$\{e\} \subseteq V_4 \subseteq A_4 \subseteq S_4.$$

Der Quotient $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$ ist ebenfalls abelsch, also ist S_4 auflösbar.

2.5.3 Satz. Die symmetrische Gruppe S_k ist nicht auflösbar für alle $k \geq 5$.

Beweis. Wir zeigen, dass es nur zwei mögliche normale Untergruppen $N \subseteq S_k$ mit S_k/N abelsch gibt, nämlich $N = S_k$ und $N = A_k$. Falls N von dieser Form ist und $\sigma, \tau \in S_k$ beliebig, dann gilt

$$\sigma\tau\sigma^{-1}\tau^{-1} \in N,$$

denn S_k/N ist abelsch, und somit ist der Kommutator $\sigma\tau\sigma^{-1}\tau^{-1}$ trivial im Quotienten S_k/N , liegt also in N . Insbesondere bedeutet dies, dass

$$(1\ 2\ 3)(1\ 4\ 5)(1\ 2\ 3)^{-1}(1\ 4\ 5)^{-1} = (2\ 4\ 1) \in N.$$

Durch andere Wahl der Zahlen können wir sogar schließen, dass alle 3-Zykel in N liegen. Dann liegen aber auch alle Doppeltranspositionen in N , denn z.B.

$$(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4).$$

Da sich aber jedes Element von A_4 als Produkt von gerade vielen Transpositionen schreiben lässt,¹⁶ folgt schließlich $N \supseteq A_k$. Dank des Satzes von Lagrange muss $|N|$ ein Teiler von $|S_k|$ sein. Weil A_k aber sogar schon die Hälfte der Elemente von S_k enthält, gibt es nur die Möglichkeiten $N = A_k$ oder $N = S_k$.

In einer Kette wie (2.27) können wir oBdA annehmen, dass $G_i \neq G_{i+1}$ für alle i gilt. Unter dieser Annahme muss für $G_n = S_k$ im vorletzten Schritt also $G_{n-1} = A_k$ gelten. Welche Möglichkeiten gibt es dann für G_{n-2} ? Es muss sich um eine normale Untergruppe $N \subseteq A_k$ mit A_k/N abelsch handeln. Jetzt können wir aber wieder genau das gleiche Argument wie oben anwenden (ersetze nur S_k durch A_k), um zu folgern, dass $N = A_k$ die einzige Möglichkeit ist. Da A_k selber aber nicht abelsch ist, sind wir bei einem Widerspruch angekommen. $\square$

2.5.4 Bemerkung. Es gilt eine noch stärkere Aussage: für $n \geq 5$ hat A_n sogar überhaupt keine nichttrivialen normalen Untergruppen. Der Beweis dieser Aussage ist aber noch komplizierter und wird hier nicht behandelt.

2.6 Endlich erzeugte abelsche Gruppen

Hier betrachten wir den Spezialfall von endlichen abelschen Gruppen. Dieser ist deswegen interessant, weil endliche abelsche Gruppen eine besonders einfache Struktur besitzen, die wir vollständig klassifizieren können. Mit *Klassifikation* ist hierbei gemeint, dass wir alle endlichen abelschen Gruppen bis auf Isomorphie angeben werden. Wir werden zeigen, dass jede endlich erzeugte abelsche Gruppe als Produkt zyklischer Gruppen dargestellt werden kann. Betrachte wir also zunächst Produkte von Gruppen.

¹⁶Jede Permutation in S_k ist Produkt von Transpositionen, also ist insbesondere jede gerade Permutation Produkt von gerade vielen Transpositionen. Falls in einer solchen Faktorisierung zwei benachbarte Transpositionen disjunkt sind, handelt es sich um eine Doppeltransposition; falls sie nicht disjunkt sind, dann ist ihr Produkt gerade ein 2-Zykel, wie in $(1\ 2)(2\ 3) = (1\ 2\ 3)$.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$+$	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

Abbildung 10: Multiplikationstabellen von $(\mathbb{Z}/8\mathbb{Z})^\times$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$. Alle Elemente haben Ordnung 2, und die Verknüpfung zweier nicht-neutraler Elemente liefert jeweils das dritte nicht-neutrale Element. Deshalb sind die beiden Gruppen isomorph. (Und jede Bijektion, welche die neutralen Elemente aufeinander abbildet, ist ein Isomorphismus.)

2.6.1 Definition. Für Gruppen $G_1, \dots, G_n$ ist das **Produkt** die Gruppe $G_1 \times \dots \times G_n$, deren Elemente Tupel $(g_1, \dots, g_n)$ mit $g_i \in G_i$ für alle $i = 1, \dots, n$ sind, und die Verknüpfung komponentenweise definiert ist durch

$$(g_1, \dots, g_n) \cdot (h_1, \dots, h_n) := (g_1 \cdot h_1, \dots, g_n \cdot h_n).$$

Man überzeugt sich leicht davon, dass $G_1 \times \dots \times G_n$ tatsächlich ebenfalls eine Gruppe ist, da die entsprechenden Eigenschaften komponentenweise erfüllt sind.

2.6.2 Beispiel. $S_k \times S_\ell$ ist isomorph zu einer Untergruppe von $S_{k+\ell}$. Denn wir können S_k als Permutationen von $\{1, \dots, k\}$ auffassen und S_ℓ als Permutationen von $\{k+1, \dots, k+\ell\}$. Damit lässt sich jedes Paar $(\sigma, \tau) \in S_k \times S_\ell$ als Element von $S_{k+\ell}$ darstellen, welches die ersten k Elemente mit σ permutiert und die letzten ℓ Elemente mit τ .

2.6.3 Notation. Ab sofort schreiben wir der Kürze halber

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$$

für die additive Gruppe der Restklassen modulo n , und für die Restklasse von $k \in \mathbb{Z}$ auch abkürzend $[k]$ anstatt $k + n\mathbb{Z}$.

Als degenerierte Spezialfälle haben wir dann insbesondere $\mathbb{Z}_0 = \mathbb{Z}$ und die triviale Gruppe $\mathbb{Z}_1 = \{[0]\}$.

2.6.4 Beispiel. Für $n \in \mathbb{N}$ können wir $\mathbb{Z}/n\mathbb{Z}$ auch als Monoid bezüglich der *Multiplikation* betrachten. Die Gruppe der invertierbaren Elemente $(\mathbb{Z}/n\mathbb{Z})^\times$ ist dann die Gruppe der Restklassen modulo n , welche teilerfremd zu n sind. Da die Multiplikation kommutativ ist, ist $(\mathbb{Z}/n\mathbb{Z})^\times$ eine abelsche Gruppe.

(a) Zum Beispiel gilt

$$(\mathbb{Z}/9\mathbb{Z})^\times = \{[1], [2], [4], [5], [7], [8]\}.$$

Diese Gruppe ist zyklisch von der Ordnung 6, denn $[2]$ ist ein Erzeuger: modulo 9 gilt

$$2^0 \equiv 1, \quad 2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 7, \quad 2^5 \equiv 5,$$

so dass alle Elemente von $(\mathbb{Z}/9\mathbb{Z})^\times$ als Potenzen von $[2]$ dargestellt werden können.

(b) Betrachten wir stattdessen

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}.$$

Ist diese Gruppe zyklisch? Nein, denn alle Elemente haben Ordnung zwei, denn modulo 8 gilt

$$3^2 \equiv 5^2 \equiv 7^2 \equiv 1,$$

so dass die Gruppe keinen einzelnen Erzeuger hat. Stattdessen gibt es einen Isomorphismus

$$(\mathbb{Z}/8\mathbb{Z})^\times \xrightarrow{\cong} \mathbb{Z}_2 \times \mathbb{Z}_2,$$

wie an den Multiplikationstabellen zu erkennen ist (Abbildung 10).

- (c) Für größeres n braucht man teilweise auch mehr als zwei Faktoren im Produkt. Zum Beispiel gibt es einen Isomorphismus

$$(\mathbb{Z}/80\mathbb{Z})^\times \xrightarrow{\cong} \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4.$$

Der Beweis dieser Aussage erfordert aber mehr Rechenarbeit und/oder etwas weitergehende Theorie.

Allgemein ist die Struktur der Gruppen $(\mathbb{Z}/n\mathbb{Z})^\times$ überraschend kompliziert. Ihre Untersuchung stellt ein wichtiges Thema der Zahlentheorie dar, mit Anwendungen in der Kryptographie.¹⁷

Die Tatsache, dass $(\mathbb{Z}/n\mathbb{Z})^\times$ immer isomorph zu einem Produkt zyklischer Gruppen ist, ist ein Spezialfall der Klassifikation endlich erzeugter abelscher Gruppen, die wir im Folgenden beweisen werden. Diese Klasse von Beispielen ist sehr instruktiv, weil die Konstruktion eines Isomorphismus zwischen $(\mathbb{Z}/n\mathbb{Z})^\times$ und einem Produkt zyklischer Gruppen alles andere als offensichtlich ist.

2.6.5 Beispiel. Seien $n, m \in \mathbb{Z}$ teilerfremd. Dann gibt es einen Isomorphismus

$$\begin{aligned} \varphi : \mathbb{Z}_{nm} &\xrightarrow{\cong} \mathbb{Z}_n \times \mathbb{Z}_m \\ [g] &\mapsto ([g], [g]). \end{aligned}$$

Dabei wird also eine Restklasse modulo nm auf ihre beiden “Reduktionen” modulo n und modulo m abgebildet. Diese ist wohldefiniert, denn falls $g \equiv g' \pmod{nm}$ gilt, dann gilt auch $g \equiv g' \pmod{n}$ und $g \equiv g' \pmod{m}$. Dass es sich um einen Homomorphismus handelt, ist ebenfalls klar,

$$\varphi([g+h]) = ([g+h], [g+h]) = ([g]+[h], [g]+[h]) = \varphi([g]) + \varphi([h]).$$

Weiterhin ist φ injektiv, denn der Kern ist trivial: falls eine Zahl g sowohl modulo n als auch modulo m Rest 0 hat, dann ist sie durch m und n teilbar, also auch durch nm aufgrund der Teilerfremdheit. Schließlich ist φ auch surjektiv, denn da die beiden Gruppen gleich viele Elemente haben, ist eine injektive Abbildung zwischen ihnen automatisch auch surjektiv (Schubfachprinzip).

In einer abelschen Gruppe G kann man ganzzahlige Linearkombinationen betrachten. Das heißt für $g_1, \dots, g_n \in G$ und $c_1, \dots, c_n \in \mathbb{Z}$ ist der Ausdruck

$$\sum_{i=1}^n c_i g_i = c_1 g_1 + \dots + c_n g_n$$

die additive Schreibweise für $g_1^{c_1} \cdots g_n^{c_n}$. Man kann sich nun überlegen, dass für diese Linearkombinationen die gleichen Rechenregeln gelten, wie für Linearkombinationen in der linearen Algebra (mit Koeffizienten in $\mathbb{Z}$ statt in einem Körper). Der einzige Unterschied ist, dass ein Koeffizient $c_i \neq 0$ meist nicht invertierbar ist. Diese Einschränkung führt zwar dazu, dass die Theorie komplizierter wird als die Theorie der Vektorräume, aber trotzdem können wir viele Konzepte aus der linearen Algebra “mutatis mutandis” übertragen. Informell können wir diese Überlegungen also folgendermaßen zusammenfassen.

2.6.6 Slogan. *Theorie abelscher Gruppen = lineare Algebra über $\mathbb{Z}$.*

Eine Schlüsselrolle im Beweis der Klassifikation wird die folgende Aussage spielen. Man kann sie sich im Rahmen dieser Analogie als eine Form der Gauß-Elimination für ganzzahlige Matrizen vorstellen.

¹⁷Siehe hierzu den *RSA-Algorithmus*, welcher immer noch einer der am weitesten verbreiteten Public-Key-Algorithmen ist, und zum Beispiel für Zertifikate im Internet und Verschlüsselung von E-Mails verwendet wird.

2.6.7 Satz (Smith-Normalform). Sei $A \in M_{m \times n}(\mathbb{Z})$ eine ganzzahlige Matrix. Dann gibt es invertierbare Matrizen $S \in \text{GL}_m(\mathbb{Z})$ und $T \in \text{GL}_n(\mathbb{Z})$ und $r \in \mathbb{N}$, so dass $r \leq \min(m, n)$ und

$$SAT = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad (2.30)$$

wobei die Zahlen $d_1, \dots, d_r \in \mathbb{N}$ die Eigenschaft haben, dass $d_i \mid d_{i+1}$ für alle $i = 1, \dots, r-1$.

Zu beachten ist hierbei, dass die Diagonalmatrix (2.30) nicht quadratisch sein muss: mit m Zeilen und n Spalten hat sie eben $m-r$ Nullzeilen unten und $n-r$ Nullspalten rechts.

Beweis. Auch der Beweis erinnert an die Gauß-Elimination, da wir die Matrizen S und T durch elementare Zeilen- und Spaltenoperationen konstruieren werden. Dabei sind als Operationen aber nur folgende erlaubt:

- ▷ Vertauschen zweier Zeilen bzw. Spalten,
- ▷ Addieren eines ganzzahligen Vielfachen einer Zeile bzw. Spalte zu einer anderen Zeile bzw. Spalte,
- ▷ Multiplizieren einer Zeile bzw. Spalte mit -1 .

Das Ausführen einer entsprechenden Zeilenoperation entspricht der Multiplikation mit einer geeigneten Matrix aus $\text{GL}_m(\mathbb{Z})$ von links, und das Ausführen einer Spaltenoperation entspricht der Multiplikation mit einer geeigneten Matrix aus $\text{GL}_n(\mathbb{Z})$ von rechts. Wenn wir die gegebene Matrix A also durch solche Operationen in die gewünschte Diagonalgestalt bringen, dann erhalten wir die gesuchten Matrizen S und T als Produkte der Matrizen, die den einzelnen Operationen entsprechen. Der folgende Algorithmus ist in Abbildung 11 an einem Beispiel illustriert.

Wir nehmen für den Beweis $A \neq 0$ an, denn falls A die Nullmatrix ist, dann ist die Aussage trivialerweise erfüllt. Welche Zahl sollte nun in die linke obere Ecke der Matrix? Dazu stellen wir fest, dass d_1 gerade der ggT aller Einträge der gewünschten Diagonalgestalt ist. Anhand der elementaren Operationen können wir aber den ggT aller Einträge der Matrix nicht verändern. Somit muss also d_1 gerade der ggT aller Matrixeinträge sein,

$$d_1 = \text{ggT} \{A_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq n\}.$$

Wir müssen also jetzt folgende Hilfsaussage beweisen:

Durch elementare Zeilen- und Spaltenoperationen können wir A in eine Matrix B umformen, so dass $B_{11} = d_1$ und $B_{i1} = B_{1j} = 0$ für alle $i, j > 1$.

Der Beweis dieser Aussage ist das Kernstück des gesamten Beweises. Dafür führen wir folgenden Algorithmus durch, der iterativ ausgehend von $B = A$ die Matrix B manipuliert, bis $B_{11} = d_1$ gilt.

- 1) Durch Vertauschen von Zeilen und Spalten können wir erreichen, dass B_{11} der kleinste Eintrag $\neq 0$ ist.¹⁸
- 2) Angenommen, es gibt einen Eintrag in der ersten Spalte $B_{i1} \neq 0$ mit $B_{11} \nmid B_{i1}$. Dann kann durch Addieren eines Vielfachen der ersten Zeile zur i -ten Zeile erreicht werden, dass $|B_{i1}| < |B_{11}|$. In diesem Fall gehen wir zum ersten Schritt zurück; wir wollen ja erreichen, dass B_{11} möglichst klein wird.

Da $|B_{11}|$ nicht unendlich oft verringert werden kann, muss diese Schleife irgendwann terminieren, also muss irgendwann $B_{11} \mid B_{ij}$ gelten.

¹⁸Hier und im Folgenden bedeutet "klein" immer "betragsmäßig klein", also für alle i und j gilt $|B_{ij}| \geq B_{11}$ oder $B_{ij} = 0$.

$$\begin{aligned}
& \begin{pmatrix} 3 & 2 & 0 \\ 2 & 8 & 6 \\ 0 & 6 & 6 \end{pmatrix} \xrightarrow{1)} \begin{pmatrix} 2 & 8 & 6 \\ 3 & 2 & 0 \\ 0 & 6 & 6 \end{pmatrix} \xrightarrow{2)} \begin{pmatrix} 2 & 8 & 6 \\ 1 & -6 & -6 \\ 0 & 6 & 6 \end{pmatrix} \xrightarrow{1)} \begin{pmatrix} 1 & -6 & -6 \\ 2 & 8 & 6 \\ 0 & 6 & 6 \end{pmatrix} \\
& \xrightarrow{4) \text{ auf Zeilen}} \begin{pmatrix} 1 & 8 & -6 \\ 0 & 20 & 18 \\ 0 & 6 & 6 \end{pmatrix} \xrightarrow{4) \text{ auf Spalten}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 20 & 18 \\ 0 & 6 & 6 \end{pmatrix} \xrightarrow{1)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 6 \\ 0 & 20 & 18 \end{pmatrix} \\
& \xrightarrow{2)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow{1)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 6 & 6 \end{pmatrix} \xrightarrow{4) \text{ auf Zeilen}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}
\end{aligned}$$

Abbildung 11: Beispiel für die Berechnung der Smith-Normalform.

- 3) Analog gehen wir jetzt mit der ersten Zeile vor: falls $B_{1j} \nmid B_{11}$, dann kann durch geeignete Spaltenoperationen ein kleinerer Eintrag erzeugt werden. Also wird irgendwann $B_{11} \mid B_{1j}$ für alle j gelten.
- 4) Jetzt können wir durch Addieren von geeigneten Vielfachen der ersten Zeile bzw. Spalte die Form

$$\begin{pmatrix} B_{11} & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

erreichen.

- 5) Angenommen, es gibt jetzt irgendeinen Eintrag B_{ij} mit $B_{11} \nmid B_{ij}$. Dann können wir die i -te Zeile zur ersten Zeile dazuaddieren, so dass das B_{ij} also auch in der ersten Zeile auftritt, und zu Schritt 2 zurückgehen.

Sobald der letzte Schritt nicht mehr aktiviert wird, sind wir also fertig. Die Tatsache, dass $|B_{11}|$ bei jedem Zurückspringen zu einem vorherigen Schritt echt kleiner wird, garantiert, dass dieser Algorithmus terminiert. Am Ende sind wir also bei dem gewünschten Ergebnis angelangt: es gilt $B_{11} \mid B_{ij}$ für alle i, j , und außerdem ist der Rest der ersten Spalte bzw. Zeile modulo B_{11} gleich 0.

Somit ist die Hilfsaussage bewiesen. Der Rest ist jetzt eigentlich klar: wir können jetzt die erste Zeile und Spalte vergessen und mit der verbleibenden Untermatrix der Größe $(m-1) \times (n-1)$ neu beginnen. Da alle Einträge jetzt Vielfache von d_1 sind, wird auch der ggT aller dieser Einträge ein Vielfaches von d_1 sein, und so erhalten wir $d_1 \mid d_2$. $\square$

2.6.8 Bemerkung. Die Smith-Normalform kann auch zum Lösen von linearen Gleichungssystemen mit Koeffizienten und Variablen aus $\mathbb{Z}$ verwendet werden, genauso wie der Gauß-Algorithmus für Gleichungssysteme über Körpern. Wir werden dies hier aber nicht weiter betrachten.

Wofür sind Matrizen in unserem Zusammenhang aber überhaupt relevant? Der Punkt ist, dass Matrizen mit ganzzahligen Einträgen bestimmte Gruppenhomomorphismen darstellen, ähnlich wie in der linearen Algebra Matrizen lineare Abbildungen zwischen Vektorräumen darstellen. Genauer gesagt definiert jede Matrix $A \in M_{m \times n}(\mathbb{Z})$ einen Gruppenhomomorphismus¹⁹

$$\begin{aligned}
\mathbb{Z}^n &\longrightarrow \mathbb{Z}^m \\
x &\longmapsto Ax,
\end{aligned}$$

¹⁹Wie üblich schreiben wir dabei

$$\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ Faktoren}}$$

für das Produkt der Gruppe $\mathbb{Z}$ mit sich selbst.

wobei wir jetzt die Elemente von $\mathbb{Z}^m$ und $\mathbb{Z}^n$ jeweils als Spaltenvektoren auffassen, so dass Ax die übliche Matrix-Vektor-Multiplikation ist. Wie die folgende Aussage zeigt, bekommt man so alle Homomorphismen $\mathbb{Z}^m \rightarrow \mathbb{Z}^n$ auf eindeutige Weise.

2.6.9 Lemma. *Für jeden Homomorphismus $\psi : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ gibt es eine eindeutige Matrix $A \in M_{m \times n}(\mathbb{Z})$, so dass $\psi(x) = Ax$ für alle $x \in \mathbb{Z}^n$.*

Beweis. Für gegebenes ψ suchen wir eine Matrix A , so dass $\psi(x) = Ax$ für alle $x \in \mathbb{Z}^n$ gilt. Damit dies der Fall ist, muss es jedenfalls für die Standardbasisvektoren $e_1, \dots, e_n \in \mathbb{Z}^n$ gelten, also

$$\psi(e_j) = Ae_j = \begin{pmatrix} A_{1j} \\ \vdots \\ A_{nj} \end{pmatrix} = \sum_{i=1}^n A_{ij}e_i.$$

Damit ist die Matrix A eindeutig bestimmt durch die Bilder der Standardbasisvektoren. Da ψ als Gruppenhomomorphismus auch alle ganzzahligen Linearkombinationen erhält, folgt für alle $x \in \mathbb{Z}^m$,

$$\psi(x) = \psi\left(\sum_{j=1}^m x_j e_j\right) = \sum_{j=1}^m x_j \psi(e_j) = \sum_{j=1}^m x_j Ae_j = A \sum_{j=1}^m x_j e_j = Ax,$$

so dass A tatsächlich die gewünschte Matrix ist. $\square$

Die Homomorphismen $\mathbb{Z}^n \rightarrow \mathbb{Z}^m$, welche den Diagonalmatrizen auf der rechten Seite von (2.30) entsprechen, sind besonders einfach zu beschreiben: man multipliziert einfach die ersten r Koordinaten mit den Zahlen $d_1, \dots, d_r$ und setzt die restlichen Koordinaten auf 0. Wir bezeichnen diesen Homomorphismus im Folgenden auch mit

$$\text{diag}(d_1, \dots, d_r) : \mathbb{Z}^m \rightarrow \mathbb{Z}^n. \quad (2.31)$$

Außerdem entspricht die Matrixmultiplikation, wie auf der linken Seite von (2.30), der Hintereinanderausführung von Homomorphismen. Damit können wir Satz 2.6.7 direkt in die folgende Aussage übersetzen.

2.6.10 Korollar. *Sei $\psi : \mathbb{Z}^m \rightarrow \mathbb{Z}^n$ ein Gruppenhomomorphismus. Dann gibt es $r \leq \min(m, n)$ und*

$$d_1 \mid d_2 \mid \dots \mid d_r \in \mathbb{N}_{>0}$$

und Automorphismen $\alpha : \mathbb{Z}^m \rightarrow \mathbb{Z}^m$ und $\beta : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$, so dass das Diagramm

$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{\psi} & \mathbb{Z}^n \\ \alpha \downarrow \cong & & \cong \downarrow \beta \\ \mathbb{Z}^m & \xrightarrow{\text{diag}(d_1, \dots, d_r)} & \mathbb{Z}^n \end{array}$$

kommutiert.

Denn die Gleichung (2.30) übersetzt sich dabei in

$$\beta \circ \psi \circ \alpha^{-1} = \text{diag}(d_1, \dots, d_r).$$

Dabei ist β der zu S gehörige Homomorphismus ist, welcher nach der Invertierbarkeit von S ein Automorphismus ist. Analog dazu ist α der zur Matrix T^{-1} gehörige Homomorphismus.

Neben der Smith-Normalform brauchen wir noch eine weitere vorbereitende Aussage. Wir erinnern dazu an Definition 2.2.1: eine Menge von Gruppenelementen $g_1, \dots, g_n \in G$ erzeugt G , falls sich jedes Element von G durch Anwendung der Gruppenoperationen aus den g_i erhalten lässt. In unserem momentanen Kontext sind diese Operationen $+$ und $-$, oder äquivalent dazu ganzzahlige Linearkombinationen. Eine (additiv geschriebene) abelsche Gruppe nennen wir also **endlich erzeugt**, falls es endlich viele Elemente $g_1, \dots, g_n \in G$ gibt, so dass jedes Element von G als ganzzahlige Linearkombination dieser Elemente geschrieben werden kann.

2.6.11 Beispiel. Die abelsche Gruppe $(\mathbb{Q}, +)$ ist *nicht* endlich erzeugt.

Denn angenommen, es gäbe $g_1, \dots, g_n \in \mathbb{Q}$, die $\mathbb{Q}$ erzeugen. Dann sei $d \in \mathbb{N}$ ein gemeinsamer Nenner aller g_i , also zum Beispiel das kgV der Nenner der g_i . Dann ist $dg_i \in \mathbb{Z}$ für alle $i = 1, \dots, n$. Deshalb ist auch $dq \in \mathbb{Z}$ für alle $q \in \mathbb{Q}$, die durch ganzzahlige Linearkombinationen der g_i dargestellt werden können. Da dies nicht für alle $q \in \mathbb{Q}$ gilt, können die g_i also nicht ganz $\mathbb{Q}$ erzeugen.

2.6.12 Lemma. Jede Untergruppe von $\mathbb{Z}^n$ ist endlich erzeugt.

Beweis. Wir zeigen per Induktion über n , dass jede Untergruppe von $\mathbb{Z}^n$ durch maximal n Elemente erzeugt werden kann.

Der Induktionsanfang $n = 1$ ist die Aussage, dass jede Untergruppe von $\mathbb{Z}$ zyklisch ist. Für eine gegebene Untergruppe $H \subseteq \mathbb{Z}$ zeigen wir dies folgendermaßen. Sei $h \in H$ die kleinste positive Zahl, welche zu H gehört.²⁰ Dann behaupten wir, dass $H = h\mathbb{Z}$ gilt. Denn einerseits ist $h\mathbb{Z} \subseteq H$ klar. Falls es andererseits ein $k \in H$ gibt, welches kein Vielfaches von h ist, dann würden wir per Division mit Rest

$$k = qh + r$$

ein $r \in H$ bekommen, für welches im Widerspruch zur Minimalität von h die Ungleichungen $0 < r < h$ gelten. Also ist jedes Element von H ein Vielfaches von h , oder

$$H = h\mathbb{Z}. \quad (2.32)$$

Somit ist H von h erzeugt und der Induktionsanfang bewiesen.

Für den Induktionsschritt sei jetzt $n > 1$ und $H \subseteq \mathbb{Z}^n$ eine Untergruppe. Dann betrachten wir, was die möglichen Werte für die letzte Koordinate sind,

$$R := \{r \in \mathbb{Z} \mid \exists g \in H : g_n = r\}.$$

Dann ist $R \subseteq \mathbb{Z}$ eine Untergruppe, welche man auch als das Bild von H unter dem Homomorphismus verstehen kann, welcher auf die letzte Koordinate projiziert. Nach dem Induktionsanfang gilt $R = d\mathbb{Z}$ für ein $d \in \mathbb{N}$. Nach Definition von R gibt es also ein Element $b \in H$ mit $b_n = d$.

Weiterhin betrachten wir

$$K := \{(g_1, \dots, g_{n-1}) \in \mathbb{Z}^{n-1} \mid (g_1, \dots, g_{n-1}, 0) \in H\}.$$

Dann ist K eine Untergruppe von $\mathbb{Z}^{n-1}$, und nach Induktionsvoraussetzung ist diese von höchstens $n - 1$ vielen Elementen erzeugt.

Zum Beweis der Aussage reicht es jetzt also aus zu zeigen, dass sich jedes $h \in H$ in der Form

$$h = qb + (k, 0)$$

schreiben lässt für geeignete $q \in \mathbb{Z}$ und $k \in K$. Dies ist aber in der Tat der Fall: die letzte Koordinate h_n ist ein Element von $R = d\mathbb{Z}$, also gibt es ein $q \in \mathbb{Z}$ mit $h_n = qd$. Dann hat

$$h - qb$$

die letzte Koordinate 0 und deshalb die Form $(k, 0)$ für ein $k \in K$. Insgesamt ist H also erzeugt von b zusammen mit einem beliebigen $(n - 1)$ -elementigen Erzeugendensystem von K . $\square$

2.6.13 Beispiel. Als Beispiel dazu betrachten wir die Menge

$$H = \{(x, y) \in \mathbb{Z}^2 \mid x - 2y \equiv 0 \pmod{5}\},$$

welche in Abbildung 12 dargestellt ist. Man sieht leicht, dass es sich um eine Untergruppe von $\mathbb{Z}^2$ handelt, zum Beispiel weil sie der Kern des Homomorphismus

$$\begin{aligned} \varphi : \mathbb{Z}^2 &\longrightarrow \mathbb{Z}_5 \\ (x, y) &\longmapsto [x - 2y] \end{aligned}$$

²⁰Falls H gar keine positive Zahl enthält, dann gilt natürlich $H = \{0\}$, wofür die Behauptung trivialerweise stimmt. Daher können wir annehmen, dass H eine positive Zahl enthält.

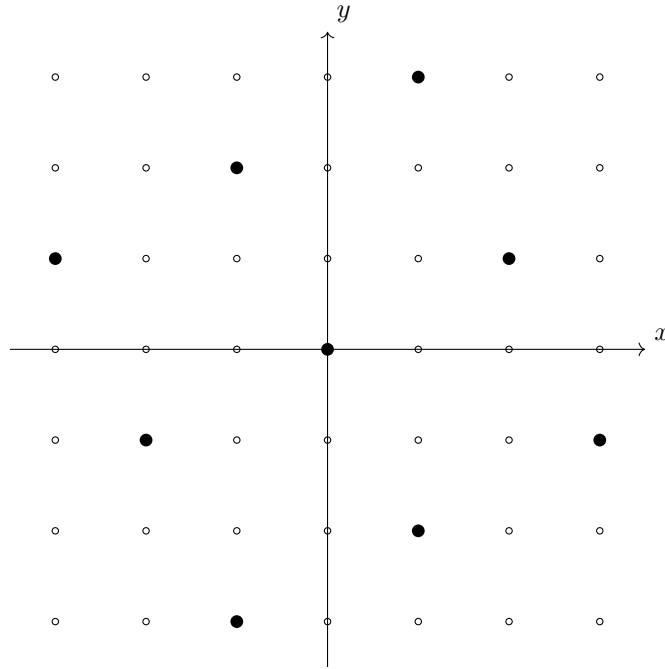


Abbildung 12: Die Untergruppe H aus Beispiel 2.6.13 als Gitterpunkte in der Ebene.

ist.

Die Projektion von H auf die letzte Koordinate ist dann die Gruppe

$$R = \{y \in \mathbb{Z} \mid \exists x \in \mathbb{Z} : (x, y) \in H\} = \mathbb{Z}.$$

Also können wir als ersten Erzeuger von H ein beliebiges Element mit zweiter Koordinate ± 1 wählen. Fixieren wir zum Beispiel $h = (2, 1)$. Weiterhin ist

$$\begin{aligned} K &= \{x \in \mathbb{Z} \mid (x, 0) \in H\} \\ &= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{5}\} \\ &= 5\mathbb{Z}. \end{aligned}$$

Der Beweis von Lemma 2.6.12 liefert somit, dass H von den beiden Elementen

$$(2, 1) \quad \text{und} \quad (5, 0)$$

erzeugt ist.

Für eine Untergruppe von $\mathbb{Z}^3$ würden wir entsprechend den Prozess noch einmal wiederholen, indem wir die gleiche Betrachtung für die Untergruppe $K \subseteq \mathbb{Z}^2$ durchführen, und so weiter. Insgesamt kann der Beweis von Lemma 2.6.12 also auch als rekursiver Algorithmus zur *Konstruktion* eines endlichen Erzeugendensystems für eine Untergruppe von $\mathbb{Z}^n$ verstanden werden.

Jetzt sind wir in der Lage, die Klassifikation endlich erzeugter abelscher Gruppen zu beweisen.

2.6.14 Satz. *Jede endlich erzeugte abelsche Gruppe G ist isomorph zu einem Produkt der Form*

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^s, \tag{2.33}$$

wobei $r, s \in \mathbb{N}$ und $d_1, \dots, d_r \in \mathbb{N}$ mit $d_i \mid d_{i+1}$ und $d_i \geq 2$ für alle $i = 1, \dots, r-1$. Die natürlichen Zahlen r, s und $d_1, \dots, d_r$ sind dabei eindeutig.

Beweis. Da die Eindeutigkeitsaussage in den Übungen behandelt wird, beschränken wir uns hier auf den Existenzbeweis.

Sei G durch $g_1, \dots, g_m$ erzeugt. Ein solches Erzeugendensystem definiert einen Homomorphismus

$$\begin{aligned} \varphi : \mathbb{Z}^m &\longrightarrow G \\ (c_1, \dots, c_m) &\longmapsto \sum_{i=1}^m c_i g_i, \end{aligned} \quad (2.34)$$

wobei die Erzeuger in G gerade den Bildern der Standardbasisvektoren von $\mathbb{Z}^m$ entsprechen. Nach Voraussetzung ist dieser Homomorphismus surjektiv. Der erste Isomorphiesatz (Satz 2.3.3) liefert uns dann

$$G \cong \mathbb{Z}^m / \ker(\varphi).$$

Nach Lemma 2.6.12 ist die Untergruppe $\ker(\varphi) \subseteq \mathbb{Z}^n$ endlich erzeugt, mit einem Erzeugendensystem $h_1, \dots, h_n \in \ker(\varphi)$. Ganz ähnlich wie in (2.34) definiert dieses Erzeugendensystem einen Homomorphismus

$$\begin{aligned} \psi : \mathbb{Z}^n &\longrightarrow \mathbb{Z}^m \\ (c_1, \dots, c_n) &\longmapsto \sum_{i=1}^n c_i h_i, \end{aligned}$$

dessen Bild durch $\text{im}(\psi) = \ker(\varphi)$ gegeben ist. Es gilt also

$$G \cong \mathbb{Z}^m / \text{im}(\psi).$$

Betrachten wir zunächst der Einfachheit halber den Fall $\psi = \text{diag}(d_1, \dots, d_r)$ für gewisse $d_1, \dots, d_r \in \mathbb{N}$ mit $d_i \mid d_{i+1}$. Dann besteht das Bild $\text{im}(\psi)$ aus genau den Vektoren $(c_1, \dots, c_m) \in \mathbb{Z}^m$ für die

$$d_i \mid c_i \quad \forall i = 1, \dots, r \quad \text{und} \quad c_i = 0 \quad \forall i = r+1, \dots, m$$

gilt. Dadurch besteht das Bilden des Quotienten $\mathbb{Z}^m / \text{im}(\psi)$ darin, die ersten r Koordinaten jeweils modulo $d_1, \dots, d_r$ zu betrachten. Dies ist dann aber genau die gewünschte Gruppe (2.33) mit $s = m - r$. Formal ausgedrückt: die Abbildung

$$\begin{aligned} \mathbb{Z}^m / \text{im}(\psi) &\longrightarrow \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{m-r} \\ (c_1, \dots, c_m) + \text{im}(\psi) &\longmapsto ([c_1], \dots, [c_r], c_{r+1}, \dots, c_m) \end{aligned}$$

ist ein Isomorphismus, dessen Inverse einfach durch

$$([c_1], \dots, [c_r], c_{r+1}, \dots, c_m) \longmapsto (c_1, \dots, c_r, c_{r+1}, \dots, c_m) + \text{im}(\psi)$$

gegeben ist. Man überprüft leicht, dass diese Abbildungen wohldefiniert sind und zueinander invers. Sie sind Homomorphismen, weil die Verknüpfung in beiden Gruppen die komponentenweise Addition ist.

Für den allgemeinen Fall wenden wir jetzt Korollar 2.6.10 an, wodurch wir das Problem auf den vorherigen bereits behandelten Fall zurückführen können. Im wesentlichen besagt Korollar 2.6.10 nämlich, dass jedes ψ durch einen *Basiswechsel* in $\mathbb{Z}^m$ und $\mathbb{Z}^n$ in eine Diagonalform überführt werden kann.²¹ Die Anwendung von Korollar 2.6.10 liefert ein kommutatives Diagramm

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{\psi} & \mathbb{Z}^n & \twoheadrightarrow & \mathbb{Z}^m / \text{im}(\psi) \\ \alpha \downarrow \cong & & \cong \downarrow \beta & & \downarrow \cong \gamma \\ \mathbb{Z}^m & \xrightarrow{\text{diag}(d_1, \dots, d_r)} & \mathbb{Z}^n & \twoheadrightarrow & \mathbb{Z}^m / \text{im}(\text{diag}(d_1, \dots, d_r)) \end{array} \quad (2.35)$$

wobei die $\twoheadrightarrow$ Pfeile die Homomorphismen sind, die jedem Element seine Nebenklasse zuordnen.

Den gestrichelten Isomorphismus γ konstruieren wir jetzt. Dessen Existenz ist ein Spezialfall einer allgemeineren Aussage: sei K eine Gruppe mit einem Automorphismus $\beta : G \rightarrow G$ und

²¹Dies soll hier keine präzise Aussage sein, weil wir gar keinen Begriff von Basis für abelsche Gruppen eingeführt haben, sondern nur eine informelle Erklärung der Idee hinter dem Beweis.

einer normalen Untergruppe $N \subseteq G$. Dann ist auch $\beta(N) \subseteq G$ normal, und es gibt einen Isomorphismus von Quotientengruppen

$$G/N \cong G/\beta(N).$$

Denn in der Tat ist

$$\begin{aligned} \gamma : G/N &\longrightarrow G/\beta(N) \\ gN &\longmapsto \beta(g)\beta(N) \end{aligned}$$

solch ein Isomorphismus, wie man leicht überprüft. Mit $G = \mathbb{Z}^m$ und $N = \text{im}(\psi)$ erhalten wir so den gesuchten Isomorphismus γ in (2.35), weil

$$\beta(\text{im}(\psi)) = \text{im}(\text{diag}(d_1, \dots, d_r)),$$

da beide Inklusionen $\subseteq$ und $\supseteq$ wegen der Kommutativität des linken Quadrats in (2.35) und der Bijektivität von β gelten. Somit ist durch die Smith-Normalform die allgemeine Aussage auf den bereits behandelten Spezialfall zurückgeführt, und der Beweis ist abgeschlossen. $\square$

2.6.15 Beispiel. Als beispielhafte Anwendung betrachten wir, wie viele abelsche Gruppen mit 360 Elementen es bis auf Isomorphie gibt. In einer Darstellung der Form (2.33) muss dann $s = 0$ gelten, da sonst die Gruppe unendlich viele Elemente hätte, und

$$\prod_{i=1}^r d_i = 360 = 2^3 \cdot 3^2 \cdot 5.$$

Somit entsprechen die Isomorphieklassen genau den Zerlegungen von $2^3 \cdot 3^2 \cdot 5$ in Faktoren $d_i \geq 2$ mit $d_i \mid d_{i+1}$. Davon gibt es genau folgende:

$$\begin{aligned} &360 \\ &2 \mid 180 \\ &3 \mid 120 \\ &6 \mid 60 \\ &2 \mid 2 \mid 90 \\ &2 \mid 6 \mid 30. \end{aligned}$$

Dass es keine weiteren Möglichkeiten gibt, sieht man daran, dass wegen $d_i \mid d_{i+1}$ für jeden Primfaktor in d_i der gleiche Primfaktor in d_{i+1} mit mindestens dem gleichen Exponenten auftreten muss. Somit gibt es genau sechs Isomorphieklassen von abelschen Gruppen mit 360 Elementen, nämlich die Isomorphieklassen von

$$\mathbb{Z}_{360}, \quad \mathbb{Z}_2 \times \mathbb{Z}_{180}, \quad \mathbb{Z}_3 \times \mathbb{Z}_{120}, \quad \mathbb{Z}_6 \times \mathbb{Z}_{60}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{90}, \quad \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}. \quad (2.36)$$

Eine analoge Betrachtung kann man für jede andere Zahl $k \in \mathbb{N}$ durchführen, um die Isomorphieklassen abelscher Gruppen mit k Elementen alle anzugeben.

3 Ordnungstheorie

Die Ordnungstheorie beschäftigt sich mit der Untersuchung von Mengen, auf denen eine Ordnungsrelation $\leq$ definiert ist. Sie tritt sowohl in der reinen als auch in der angewandten Mathematik auf vielfache Weise auf. Ein Grundverständnis der Ordnungstheorie ist daher für fast jede Art von mathematischer Arbeit nützlich. Dies gilt insbesondere für alle drei Bereiche der Algebra, die wir in diesem Skript behandeln.

3.1 Prägeordnete Mengen

Wir beginnen mit der grundlegenden Definition.

3.1.1 Definition. Eine **Präordnung** auf einer Menge M ist eine binäre Relation $\leq \subseteq M \times M$, die folgende Eigenschaften erfüllt:

(a) Reflexivität: für alle $x \in M$ gilt

$$x \leq x.$$

(b) Transitivität: für alle $x, y, z \in M$ gilt

$$x \leq y \wedge y \leq z \implies x \leq z.$$

Dabei schreiben wir $x \leq y$ als Abkürzung für $(x, y) \in \leq$. Eine Menge M , auf der eine Präordnung definiert ist, heißt **prägeordnete Menge**.

3.1.2 Beispiel. Die folgenden Relationen definieren prägeordnete Mengen:

- (a) Die normale kleiner-gleich-Relation $\leq$ auf den bekannten Zahlensystemen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$.
- (b) Die Inklusionsrelation $\subseteq$ auf der Potenzmenge 2^A einer Menge A .
- (c) Ähnlich: die Inklusionsrelation $\subseteq$ auf der Menge aller Untergruppen einer Gruppe G , oder auf der Menge der offenen Mengen eines topologischen Raums.
- (d) Die Teilbarkeitsrelation $x \mid y$ in der Zahlentheorie, z.B. auf $\mathbb{Z}$.

In allen Fällen entsprechen die Reflexivität und Transitivität der Relation bekannten Eigenschaften. Außerdem gibt es auf jeder Menge M auch noch zwei triviale Präordnungen:

- (e) $x \leq y$ für alle $x, y \in M$.
- (f) $x \leq y$ genau dann, wenn $x = y$.

Die folgenden Beispiele stammen aus angewandten Bereichen, und wir belassen es hier bei einer eher informellen Beschreibung.

- (g) Präferenzordnung in der Entscheidungs- und Spieltheorie: auf Mengen der Art

$$M = \{\text{Auto, Fahrrad, Einfamilienhaus, 1 Mio €}\}$$

schreiben wir $x \leq_P y$, falls Person P das Objekt y gegenüber x bevorzugt oder beide gleich gut findet. Die Präferenzen jeder Person P sind somit als Präordnung $\leq_P$ auf M modelliert.

- (h) Kausalitätsrelation in der Physik: auf der Menge aller Ereignisse im Universum schreiben wir $x \leq y$, falls x kausal y beeinflussen kann.
- (i) Reduktion in der Informatik: M ist eine Menge von algorithmischen Problemen, und wir schreiben $x \leq y$, falls Problem x effizient auf Problem y reduziert werden kann (so dass y also mindestens so schwer ist wie x).

Allen diesen Beispielen ist gemeinsam, dass die Reflexivität und Transitivität der Relation intuitiv klar sind.

3.1.3 Bemerkung. (a) Wie für die bekannten Präordnungen auf Zahlensystemen schreiben wir allgemein auch

$$x \geq y \quad :\Longleftrightarrow \quad y \leq x.$$

(b) Falls $\leq$ eine Präordnung auf M ist, so ist auch die

$$x \leq' y \quad :\Longleftrightarrow \quad x \geq y$$

eine Präordnung auf M , die sogenannte **umgekehrte Präordnung**.

Oft lassen wir die Präordnung implizit und sprechen von M selbst als prägeordneter Menge. In diesem Fall schreiben wir

$$M^{\text{op}}$$

für die prägeordnete Menge mit der umgekehrten Präordnung.

Falls für Elemente x und y einer prägeordneten Menge sowohl $x \leq y$ als auch $x \geq y$ gilt, so sind diese Elemente gewissermaßen “auf gleicher Stufe” und aus Sicht der Präordnung nicht unterscheidbar. Es lohnt sich, dies an den Fällen aus Beispiel 3.1.2 durchzudenken. Allgemein wird dies durch folgende Aussage erfasst.

3.1.4 Lemma. Sei $(M, \leq)$ eine prägeordnete Menge.

(a) Die Relation $\simeq$ auf M , definiert durch

$$x \simeq y : \Longleftrightarrow (x \leq y \wedge y \leq x),$$

ist eine Äquivalenzrelation.

(b) Es gilt

$$x \leq y, x' \simeq x, y' \simeq y \implies x' \leq y'. \quad (3.1)$$

Beweis. (a) Die Reflexivität $x \simeq x$ gilt aufgrund der Reflexivität $x \leq x$. Für die Symmetrie sei $x \simeq y$, also $x \leq y$ und $y \leq x$. Aufgrund genau dieser Ungleichungen gilt dann auch $y \simeq x$.

Für die Transitivität sei $x \simeq y$ und $y \simeq z$, also

$$x \leq y, \quad y \leq x, \quad y \leq z, \quad z \leq y.$$

Die erste und dritte Ungleichung zusammen mit der Transitivität der Präordnung ergeben $x \leq z$, und analog mit der zweiten und vierten $z \leq x$, also auch $x \simeq z$.

(b) Nach Voraussetzung haben wir insbesondere

$$x' \leq x \leq y \leq y'.$$

Also folgt $x' \leq y'$ aus zwei Anwendungen der Transitivität. $\square$

3.1.5 Beispiel. (a) In $\mathbb{Z}$ als prägeordneter Menge mit der Teilbarkeitsrelation $|$ gilt

$$n \simeq m \quad \Longleftrightarrow \quad n = \pm m,$$

denn zwei ganze Zahlen teilen einander genau dann, wenn sie bis auf Vorzeichen übereinstimmen.

(b) Für Mengen A und B schreiben wir $A \leq B$, falls es eine injektive Abbildung $A \hookrightarrow B$ gibt. Damit ist $\leq$ eine Präordnung auf der Klasse aller Mengen. Für zwei Mengen A und B gilt dann $A \simeq B$ also genau dann, wenn man jede der beiden Mengen in die jeweils andere einbetten kann. Der *Satz von Cantor–Schröder–Bernstein* aus der Mengenlehre besagt, dass dies genau dann der Fall ist, wenn es eine Bijektion zwischen A und B gibt.

3.1.6 Definition. Eine **teilgeordnete Menge** ist eine prägeordnete Menge $(M, \leq)$, für die zusätzlich die Antisymmetrie gilt:

$$x \leq y \wedge y \leq x \implies x = y.$$

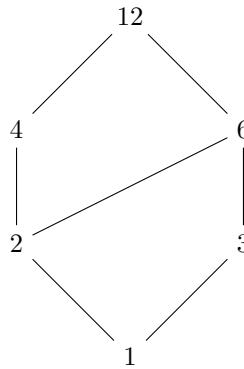


Abbildung 13: Das Hasse-Diagramm der positiven Teiler von 12 bezüglich der Teilbarkeitsrelation.

Mit anderen Worten: eine teilgeordnete Menge ist eine prägeordnete Menge, bei der die Äquivalenzrelation $\simeq$ mit $=$ übereinstimmt. Falls $(M, \leq)$ eine beliebige prägeordnete Menge ist, dann ist die Menge der Äquivalenzklassen $M/\simeq$ mit der Relation

$$[x] \leq [y] \quad :\Longleftrightarrow \quad x \leq y$$

eine teilgeordnete Menge. Dabei ist die Wohldefiniertheit der Relation durch (3.1) gewährleistet.

3.1.7 Beispiel. Alle prägeordneten Mengen aus Beispiel 3.1.2(a)–(c) sind bereits teilgeordnet.

3.1.8 Bemerkung. In der mathematischen Praxis ist die Unterscheidung zwischen prägeordneten und teilgeordneten Mengen meist irrelevant. Der Grund ist, dass man zwei Elemente $x \simeq y$ in einer prägeordneten Menge in der Regel als austauschbar betrachtet, und somit kann man gleich $=$ anstatt $\simeq$ schreiben, was auf die Bildung des Quotienten $M/\simeq$ hinausläuft. Beispiel 3.1.5 illustriert dies gut: wenn wir die ganzen Zahlen mit der Teilbarkeitsrelation betrachten, dann ist es egal, ob wir mit 2 oder -2 arbeiten, da dies bezüglich der Teilbarkeit keinen Unterschied macht.

Eine endliche teilgeordnete Menge lässt sich gut durch ein sogenanntes **Hasse-Diagramm** darstellen. Dabei werden die Elemente der Menge als Knoten eines Graphen gezeichnet, und es wird eine Kante von x nach y gezogen, falls $x < y$ gilt und es kein z mit $x < z < y$ gibt. In Abbildung 13 ist beispielhaft das Hasse-Diagramm der positiven Teiler von 12 bezüglich der Teilbarkeitsrelation dargestellt.

So wie man für Gruppen die Gruppenhomomorphismen als strukturerhaltende Abbildungen betrachtet, so gibt es auch für prägeordnete Mengen eine passende Definition von strukturerhaltender Abbildung.

3.1.9 Definition. Seien M und N prägeordnete Mengen. Eine Abbildung $f: M \rightarrow N$ heißt dann **monoton**, wenn für alle $x, y \in M$ gilt:

$$x \leq y \quad \Longrightarrow \quad f(x) \leq f(y).$$

3.1.10 Beispiel. (a) Wie aus der Analysis bekannt ist eine differenzierbare Abbildung $f: \mathbb{R} \rightarrow \mathbb{R}$ genau dann monoton, falls $f'(x) \geq 0$ für alle $x \in \mathbb{R}$ gilt.

(b) Für eine Abbildung $f: X \rightarrow Y$ zwischen Mengen und jede Teilmenge $A \subseteq X$ ist ihr Bild eine Teilmenge $f(A) \subseteq Y$ eine Teilmenge, und es gilt offensichtlich

$$A \subseteq A' \quad \Longrightarrow \quad f(A) \subseteq f(A').$$

Damit ist die Abbildung

$$\begin{aligned} 2^X &\longrightarrow 2^Y \\ A &\longmapsto f(A) \end{aligned}$$

monoton bezüglich der Inklusionsrelationen auf den Potenzmengen 2^X und 2^Y .

Andererseits kann man auch das Urbild $f^{-1}(B) \subseteq X$ einer Teilmenge $B \subseteq Y$ betrachten. Dies definiert eine monotone Abbildung in die umgekehrte Richtung,

$$\begin{aligned} 2^Y &\longrightarrow 2^X \\ B &\longmapsto f^{-1}(B). \end{aligned}$$

Im nächsten Unterabschnitt werden wir sehen, was diese beiden Abbildungen miteinander zu tun haben.

3.2 Galois-Zusammenhänge

Der folgende Begriff kommt in vielen Anwendungen der Ordnungstheorie vor. Der Einfachheit halber betrachten wir ihn nur für teilgeordnete Mengen.²²

3.2.1 Definition. Seien M und N teilgeordnete Mengen. Ein **Galois-Zusammenhang** zwischen M und N ist dann ein Paar von Abbildungen

$$\begin{array}{ccc} & f & \\ M & \xrightarrow{\quad} & N \\ & g & \end{array} \quad (3.2)$$

so dass für alle $x \in M$ und $y \in N$ gilt:

$$f(x) \leq y \iff x \leq g(y). \quad (3.3)$$

In diesem Fall heißt f **linksadjungiert** zu g , und g heißt **rechtsadjungiert** zu f .

3.2.2 Beispiel. (a) Betrachten wir $\mathbb{Z}$ und $\mathbb{R}$ als teilgeordnete Mengen mit der üblichen Ordnung. Dann bilden die Inklusion $\mathbb{Z} \hookrightarrow \mathbb{R}$ und die Abrundungsfunktion

$$\begin{aligned} \lfloor \cdot \rfloor : \mathbb{R} &\longrightarrow \mathbb{Z} \\ x &\longmapsto \max\{n \in \mathbb{Z} \mid n \leq x\} \end{aligned} \quad (3.4)$$

einen Galois-Zusammenhang

$$\begin{array}{ccc} & \hookrightarrow & \\ \mathbb{Z} & & \mathbb{R} \\ & \xleftarrow{\lfloor \cdot \rfloor} & \end{array}$$

In der Tat gilt für alle $n \in \mathbb{Z}$ und $x \in \mathbb{R}$, dass

$$n \leq x \iff n \leq \lfloor x \rfloor,$$

denn eine ganze Zahl n ist eine untere Schranke für eine reelle Zahl x genau dann, wenn sie eine untere Schranke für die abgerundete Zahl $\lfloor x \rfloor$ ist.

In diesem Beispiel ist also die Inklusionsabbildung linksadjungiert zur Abrundungsfunktion. Die Inklusionsabbildung ist aber auch rechtsadjungiert zur *Aufrundungsfunktion* $\lceil \cdot \rceil : \mathbb{R} \rightarrow \mathbb{Z}$, denn analog gilt für alle $n \in \mathbb{Z}$ und $x \in \mathbb{R}$, dass

$$x \leq n \iff \lceil x \rceil \leq n.$$

Wir bekommen so also den Galois-Zusammenhang

$$\begin{array}{ccc} & \lceil \cdot \rceil & \\ \mathbb{R} & \xrightarrow{\quad} & \mathbb{Z} \\ & \xleftarrow{\quad} & \end{array}$$

²²Für prägeordnete Mengen könnte man alles analog entwickeln, indem man überall $=$ durch $\simeq$ ersetzt. Bei der Eindeutigkeitsaussage von Korollar 3.2.5 muss man dann aber aufpassen, weil die Abbildungen dann nur bis auf $\simeq$ eindeutig sind.

- (b) Sei $2^{\mathbb{R}^n}$ die Menge aller Teilmengen des $\mathbb{R}^n$ und $\mathcal{C}(\mathbb{R}^n)$ die Menge der topologisch abgeschlossenen Teilmengen. Für $A \in 2^{\mathbb{R}^n}$ und $B \in \mathcal{C}(\mathbb{R}^n)$ gilt dann

$$A \subseteq B \iff \overline{A} \subseteq B, \quad (3.5)$$

wobei $\overline{A}$ den Abschluss von A bezeichnet. Daher ist die Inklusionsabbildung $\mathcal{C}(\mathbb{R}^n) \hookrightarrow 2^{\mathbb{R}^n}$ rechtsadjungiert zum Abschlussoperator $\overline{(\cdot)}: 2^{\mathbb{R}^n} \rightarrow \mathcal{C}(\mathbb{R}^n)$, und wir haben einen Galois-Zusammenhang

$$\begin{array}{ccc} & \overline{(\cdot)} & \\ & \curvearrowright & \\ 2^{\mathbb{R}^n} & & \mathcal{C}(\mathbb{R}^n) \\ & \curvearrowleft & \end{array}$$

Diese Tatsache wird, in der Form (3.5), sehr häufig in der Analysis verwendet.

- (c) Sei G eine Gruppe, 2^G die Menge aller Teilmengen von G und $\text{Sub}(G)$ die Menge aller Untergruppen von G . Für $A \in 2^G$ und $H \in \text{Sub}(G)$ gilt dann

$$A \subseteq H \iff \langle A \rangle \subseteq H,$$

wobei $\langle A \rangle$ die von A erzeugte Untergruppe bezeichnet, also wie nach Definition 2.2.1 die Untergruppe, welche aus allen endlichen Produkten von Elementen aus A und deren Inversen besteht. Dies sieht man leicht daran, dass wenn H eine Untergruppe ist und $A \subseteq H$ gilt, dann muss H auch alle solche Produkte enthalten. Also ist ähnlich wie bei (3.5) die Inklusionsabbildung $\text{Sub}(G) \hookrightarrow 2^G$ rechtsadjungiert zum Erzeugeroperator $\langle \cdot \rangle: 2^G \rightarrow \text{Sub}(G)$, und wir haben einen Galois-Zusammenhang

$$\begin{array}{ccc} & \langle \cdot \rangle & \\ & \curvearrowright & \\ 2^G & & \text{Sub}(G) \\ & \curvearrowleft & \end{array}$$

- (d) Sei $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$ die Menge der “erweiterten” reellen Zahlen. Dann schreiben wir $\overline{\mathbb{R}}^{\mathbb{N}}$ für die Menge der Folgen erweiterter reeller Zahlen mit der komponentenweisen Ordnung, also

$$(x_n)_{n \in \mathbb{N}} \leq (y_n)_{n \in \mathbb{N}} \iff x_n \leq y_n \quad \forall n \in \mathbb{N}.$$

Wir betrachten $\overline{\mathbb{R}}$ als die Untermenge der konstanten Folgen. Dann ist die Inklusionsabbildung $\overline{\mathbb{R}} \hookrightarrow \overline{\mathbb{R}}^{\mathbb{N}}$ rechtsadjungiert zur Abbildung, welche das Supremum bildet,²³

$$\begin{aligned} \sup : \overline{\mathbb{R}}^{\mathbb{N}} &\longrightarrow \overline{\mathbb{R}} \\ (x_n)_{n \in \mathbb{N}} &\longmapsto \sup_n x_n. \end{aligned}$$

Denn für alle $r \in \overline{\mathbb{R}}$ und $(x_n)_{n \in \mathbb{N}} \in \overline{\mathbb{R}}^{\mathbb{N}}$ gilt

$$\sup_n x_n \leq r \iff x_n \leq r \quad \forall n \in \mathbb{N}, \quad (3.6)$$

was äquivalent zur Definition des Supremums als kleinste obere Schranke ist. Dies wird unten anhand von Satz 3.2.4 noch klarer werden. Wir haben also den Galois-Zusammenhang

$$\begin{array}{ccc} & \sup & \\ & \curvearrowright & \\ \overline{\mathbb{R}}^{\mathbb{N}} & & \overline{\mathbb{R}} \\ & \curvearrowleft & \\ & r \mapsto (r, r, \dots) & \end{array}$$

In diesen Beispielen war jeweils eine der Abbildungen eine Inklusion. Dies ist zwar häufig der Fall, illustriert aber noch nicht die volle Allgemeinheit des Begriffs. Daher kommen wir jetzt zu Beispielen, bei denen beide Abbildungen nichttrivial sind.

²³Hier erklärt sich, warum wir ∞ zu den reellen Zahlen hinzugefügt haben: das Supremum einer Folge reeller Zahlen kann ∞ sein.

3.2.3 Beispiel. (a) Sei X eine beliebige Menge und $S \subseteq X$ eine Teilmenge. Dann gilt für alle $A, B \subseteq X$, dass

$$A \cap S \subseteq B \iff A \subseteq B \cup (X \setminus S),$$

weil beide Seiten äquivalent zu der Aussage sind, dass jedes Element von A auch in B oder nicht in S liegt. Wir haben also einen Galois-Zusammenhang

$$\begin{array}{ccc} 2^X & \xrightarrow{A \mapsto A \cap S} & 2^X \\ & \xleftarrow{B \mapsto B \cup (X \setminus S)} & \end{array}$$

(b) Für eine Abbildung $f : X \rightarrow Y$ zwischen Mengen bilden die zugehörigen Abbildungen aus Beispiel 3.1.10(b) einen Galois-Zusammenhang

$$\begin{array}{ccc} 2^X & \xrightarrow{f_*} & 2^Y \\ & \xleftarrow{f^*} & \end{array}$$

Dabei schreiben wir f_* für die Abbildung, welche das Bild einer Teilmenge nimmt, und entsprechend f^* für die Abbildung, welche Urbilder nimmt. Dann gilt für alle $A \subseteq X$ und $B \subseteq Y$, dass

$$f_*(A) \subseteq B \iff A \subseteq f^*(B).$$

Denn beide Seiten sind äquivalent zu $f(x) \in B \ \forall x \in A$.

3.2.4 Satz. Für jeden Galois-Zusammenhang gelten:

(a) Die Abbildungen f und g sind monoton.

(b) Für alle $x \in M$ gilt

$$f(x) = \min \{y \in N \mid x \leq g(y)\}. \quad (3.7)$$

und für alle $y \in N$ gilt

$$g(y) = \max \{x \in M \mid f(x) \leq y\}. \quad (3.8)$$

(c) Es gelten

$$g(f(x)) \geq x \quad \forall x \in M, \quad (3.9)$$

$$f(g(y)) \leq y \quad \forall y \in N. \quad (3.10)$$

(d) Es gelten

$$f \circ g \circ f = f, \quad g \circ f \circ g = g. \quad (3.11)$$

Hierbei bedeutet (3.7), dass das Element $f(x) \in N$ das kleinste Element in der auf der rechten Seite angegebenen Menge ist. Diese Aussage lässt sich in zwei Teilaussagen zerlegen:

▷ $f(x)$ gehört zur Menge, also $x \leq g(f(x))$.

▷ $f(x)$ ist eine untere Schranke der Menge, also für jedes $y \in N$ mit $x \leq g(y)$ gilt $f(x) \leq y$.

Analog besagt (3.8), dass $g(y)$ das größte Element in der auf der rechten Seite angegebenen Menge ist. Besonders intuitiv ist dies in Beispiel 3.2.2(a): $\lfloor x \rfloor$ ist die größte ganze Zahl $\leq x$, und $\lceil x \rceil$ ist die kleinste ganze Zahl $\geq x$. Weiterhin lohnt es sich aber auch, diese Eigenschaften in den anderen Beispielen durchzudenken. So wird zum Beispiel aus (3.6) direkt die Definition des Supremums einer Folge als kleinste obere Schranke der Folge.

Beweis. Wir zeigen die Aussagen in einer anderen Reihenfolge als angegeben, was sich als etwas einfacher erweist.

- (c) Für alle $x \in M$ gilt $f(x) \leq f(x)$, also

$$x \leq g(f(x))$$

da nach Voraussetzung g rechtsadjungiert zu f ist. Analog folgt $f(g(y)) \leq y$ für alle $y \in N$ aus $g(y) \leq g(y)$.

- (b) Wir beweisen die oben angegebenen Teilaussagen für (3.7).

Dass $f(x)$ zur Menge gehört, bedeutet gerade $x \leq g(f(x))$, was wir eben gezeigt haben.

Es bleibt zu zeigen, dass $f(x)$ eine untere Schranke der Menge ist. Sei also y ein Element der Menge, das heißt $y \in N$ mit $x \leq g(y)$. Dann folgt wiederum direkt aus der Definition des Galois-Zusammenhangs, dass tatsächlich $f(x) \leq y$ gilt. Somit ist $f(x)$ auch eine untere Schranke der Menge.

Die Ungleichung (3.8) folgt analog, indem man die Rollen von f und g sowie von M und N vertauscht und die Richtung der Ungleichungen umkehrt.

- (a) Für $x \leq x'$ in M gilt

$$x' \leq g(y) \implies x \leq g(y),$$

für alle $y \in N$ aufgrund der Transitivität, und daher

$$\{y \in N \mid x' \leq g(y)\} \subseteq \{y \in N \mid x \leq g(y)\}.$$

Weil das Minimum der größeren Menge auch eine untere Schranke der kleineren Menge ist, muss das Minimum der linken Menge $\leq$ dem Minimum der rechten Menge sein. Somit folgt $f(x) \leq f(x')$ aus (3.7). Die Monotonie von g folgt analog aus (3.8).

- (d) Für die erste Gleichung betrachten wir für alle $x \in M$ die Ungleichungen

$$f(x) \stackrel{(3.9)}{\leq} f(g(f(x))) \stackrel{(3.10)}{\leq} f(x),$$

wobei die erste Ungleichung eine Anwendung von (3.9) zusammen mit der Monotonie von f ist, und die zweite Ungleichung eine Anwendung von (3.10) mit $y = f(x)$. Somit folgt das gewünschte $f(g(f(x))) = f(x)$ aus der Antisymmetrie, da die Ungleichung in beide Richtungen gezeigt ist. Analog ergibt sich $g(f(g(y))) = g(y)$ für alle $y \in N$. $\square$

3.2.5 Korollar. In einem Galois-Zusammenhang gelten:

- (a) Jede der beiden Abbildungen f und g ist eindeutig durch die jeweils andere bestimmt.
(b) Mit

$$\overline{M} := \{x \in M \mid x = g(f(x))\}$$

$$\underline{N} := \{y \in N \mid y = f(g(y))\}$$

schränkt sich der ursprüngliche Galois-Zusammenhang (3.2) ein zu einem Isomorphismus zwischen den Teilmengen

$$\begin{array}{ccc} \overline{M} & \xrightarrow{f|_{\overline{M}}} & \underline{N} \\ & \xleftarrow{g|_{\underline{N}}} & \end{array} \quad (3.12)$$

- (c) Falls f (bzw. g) injektiv ist, dann ist g (bzw. f) surjektiv. In diesem Fall gilt $\overline{M} = M$ (bzw. $\underline{N} = N$).

Beweis. (a) f ist wegen (3.7) eindeutig durch g bestimmt, und umgekehrt ist g wegen (3.8) eindeutig durch f bestimmt.

- (b) Dank (3.11) gilt $f(x) = f(g(f(x)))$ für alle $x \in M$, was bereits $f(x) \in \underline{N}$ zeigt. Insbesondere kann f zu $f|_{\overline{M}}: \overline{M} \rightarrow \underline{N}$ eingeschränkt werden. Analog ergibt sich, dass man g auf eine Abbildung $\underline{N} \rightarrow \underline{M}$ einschränken kann.

Die Tatsache, dass diese beiden Abbildungen invers zueinander sind, gilt dann ebenfalls direkt per Definition: für $x \in \underline{M}$ ist $g(f(x)) = x$, und für $y \in \underline{N}$ ist $f(g(y)) = y$.²⁴

- (c) Falls f injektiv ist, dann kann in der Gleichung $f \circ g \circ f = f$ aus (3.11) die Funktion f auf beiden Seiten gekürzt werden, was $g \circ f = \text{id}_M$ ergibt und deshalb $\overline{M} = M$. Ebenfalls dank $g \circ f = \text{id}_M$ muss g surjektiv sein. Das gleiche Argument funktioniert auch mit vertauschten Rollen von f und g . $\square$

3.2.6 Bemerkung. Mit *Isomorphismus* ist in (b) eine bijektive monotone Abbildung gemeint, deren Umkehrabbildung ebenfalls monoton ist.

Im Gegensatz zur Situation in der Gruppentheorie, wo die Umkehrabbildung eines bijektiven Homomorphismus ebenfalls wieder ein Homomorphismus ist (Satz 2.2.12), muss die Umkehrabbildung einer bijektiven monotonen Abbildung nicht automatisch wieder monoton sein. So ist zum Beispiel die Identitätsabbildung $(\mathbb{N}, =) \rightarrow (\mathbb{N}, \leq)$ bijektiv und monoton, aber ihre Umkehrabbildung ist nicht monoton, da $x \leq y$ offensichtlich nicht $x = y$ impliziert.

3.2.7 Beispiel. In allen Fällen aus Beispiel 3.2.2 ist f bzw. g injektiv, so dass nach Korollar 3.2.5 der Isomorphismus (3.12) jeweils zwischen M bzw. N und dem Bild der anderen Abbildung besteht. Zum Beispiel im Fall der Abrundungsfunktion (3.4) erhalten wir so die (triviale) Aussage, dass die ganzen Zahlen genau denjenigen reellen Zahlen x entsprechen, welche $\lfloor x \rfloor = x$ erfüllen.

Es ist auch eine gute Übung, den Isomorphismus (3.12) für die Galois-Zusammenhänge aus Beispiel 3.2.3 auszuarbeiten.

Als letztes Beispiel behandeln wir noch einen etwas komplexeren Galois-Zusammenhang. Nachdem die bisherigen Beispiele eher als “Übungsbeispiele” dienten, bei denen die abstrakte Theorie eher wenig neue Erkenntnis liefert, wird jetzt ein Verständnis der allgemeinen Theorie auch für das Verständnis des Beispiels nützlich sein.

3.2.8 Beispiel. Sei G eine Gruppe, welche auf einer Menge X wirkt. Dann gibt es einen Galois-Zusammenhang

$$\begin{array}{ccc} & \xrightarrow{\text{Stab}} & \\ 2^X & & \text{Sub}(G)^{\text{op}} \\ & \xleftarrow{\text{Fix}} & \end{array}$$

Bevor wir die Abbildungen definieren, sei daran erinnert, dass $\text{Sub}(G)^{\text{op}}$ die teilgeordnete Menge der Untergruppen von G mit der *umgekehrten* Inklusionsordnung ist. Die Abbildungen Stab und Fix werden entsprechend Satz 3.2.4(a) also inklusionsumkehrend sein.

Für eine Teilmenge $A \subseteq X$ ist $\text{Stab}(A)$ die Untergruppe von G , welche alle Elemente von A fix lässt, also

$$\text{Stab}(A) := \{g \in G \mid gx = x \ \forall x \in A\},$$

und umgekehrt, gegeben eine Untergruppe $H \subseteq G$, enthält $\text{Fix}(H)$ genau die Elemente von X , welche von allen Elementen von H fixiert werden, also

$$\text{Fix}(H) := \{x \in X \mid hx = x \ \forall h \in H\}.$$

Dann haben wir einen Galois-Zusammenhang, denn für alle $A \subseteq X$ und $H \subseteq G$ gilt

$$H \subseteq \text{Stab}(A) \iff A \subseteq \text{Fix}(H). \quad (3.13)$$

Dies ist die relevante Äquivalenz, weil die linke Seite genau der Ungleichung $\text{Stab}(A) \leq H$ in $\text{Sub}(G)^{\text{op}}$ entspricht. Die Äquivalenz gilt, weil beide Seiten äquivalent dazu sind, dass $hx = x$ für alle $x \in A$ und $h \in H$ ist.

²⁴Es ist überraschend, dass für diesen Beweis die Eigenschaften eines Galois-Zusammenhangs überhaupt nicht gebraucht worden sind. Selbst für beliebige Abbildungen $f: M \rightarrow N$ und $g: N \rightarrow M$ bekommt man also nach dem gleichen Argument eine Bijektion zwischen $\overline{M}$ und $\underline{N}$.

Falls zum Beispiel $G = \mathbb{Z}$, dann interpretieren wir X wie in Beispiel 2.4.5 als Menge der “Zustände” eines dynamischen Systems mit diskreter Zeitentwicklung. In diesem Fall können wir die Äquivalenz (3.13) basierend auf den folgenden Beobachtungen etwas besser verstehen:

- ▷ Die Untergruppen von $\mathbb{Z}$ sind nach (2.32) alle von der Form $H = n\mathbb{Z}$ für ein $n \in \mathbb{N}$.
- ▷ Per Definition ist $\text{Fix}(n\mathbb{Z})$ die Menge aller Elemente von X , welche nach n Zeitschritten wieder zu sich selbst zurückkehren.
- ▷ Für eine Menge von Zuständen $A \subseteq X$ die Untergruppe $\text{Stab}(A)$ die Menge aller Zeitschritte, nach denen *alle* Zustände in A wieder zu sich selbst zurückkehren.

Beide Seiten der Äquivalenz (3.13) sagen für $H = n\mathbb{Z}$ dann also aus, dass alle Elemente in A nach n Zeitschritten wieder zu sich selbst zurückkehren.

Dieses Beispiel eines Galois-Zusammenhangs ist eine rein mengentheoretische Variante des Hauptsatzes der *Galoistheorie*, die wir in Abschnitt 5 im Kontext von Körpererweiterungen und deren Automorphismengruppen behandeln werden. Da dieser konkrete Galois-Zusammenhang auf Galois zurückgeht und historisch das erste tiefergehende Beispiel ist, ist der Begriff des Galois-Zusammenhangs auch allgemein nach ihm benannt.

3.3 Binäre Suprema und Infima

Diesen Abschnitt haben wir nicht mehr in der Vorlesung behandelt. Er ist daher auch nicht prüfungsrelevant.

3.3.1 Definition. Sei M eine prägeordnete Menge und $x, y \in M$. Ein **Supremum** von x und y ist ein Element $x \vee y \in M$, so dass gelten:

- ▷ $x \leq x \vee y$ und $y \leq x \vee y$, und
- ▷ für jedes $z \in M$ mit $x \leq z$ und $y \leq z$ gilt $x \vee y \leq z$.

In Worten: ein Supremum $x \vee y$ ist erstens eine obere Schranke für x und y ist, und zweitens ein kleinstes Element unter allen oberen Schranken. Ein solches Supremum ist bis auf Äquivalenz eindeutig, denn falls $x \sqcup y$ ein weiteres Supremum von x und y ist, dann ist es auch eine obere Schranke, also

$$x \vee y \leq x \sqcup y.$$

Da die andere Richtung analog gilt, folgt $x \sqcup y \simeq x \vee y$. Aus diesem Grund sprechen wir auch von *dem* Supremum von x und y , obwohl es eigentlich nur im teilgeordneten Fall strikt eindeutig ist.

Analog ist ein **Infimum** von x und y ein Element $x \wedge y \in M$, welches eine größte untere Schranke von x und y ist, also so dass gelten:

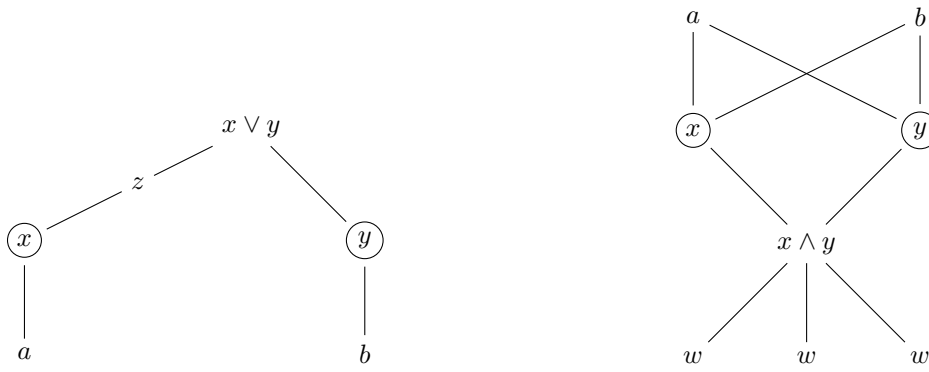
- ▷ $x \wedge y \leq x$ und $x \wedge y \leq y$, und
- ▷ für jedes $z \in M$ mit $z \leq x$ und $z \leq y$ gilt $z \leq x \wedge y$.

Per Definition ist ein Infimum also ein Supremum in der umgekehrten Ordnung M^{op} , und ebenso eindeutig bis auf Äquivalenz, so dass wir informell von *dem* Infimum sprechen.

3.3.2 Beispiel. (a) In der teilgeordneten Menge aus Abbildung 14(a) existiert das Supremum $x \vee y$. Es gibt aber gar keine gemeinsame untere Schranke von x und y , und daher auch kein Infimum.

In Abbildung 14(b) dagegen existiert das Infimum $x \wedge y$. Es gibt aber kein Supremum von x und y , weil die oberen Schranken genau die Elemente a und b sind, es wegen $a \not\leq b$ und $b \not\leq a$ aber keine kleinste obere Schranke gibt.

(b) In $(\mathbb{Z}, |)$ ist das Supremum zweier Zahlen per Definition ihr kgV und das Infimum ihr ggT. Beide existieren immer und sind eindeutig bis auf das Vorzeichen.



(a) Das Supremum $x \vee y$ existiert, aber kein Infimum von x und y .

(b) Das Infimum $x \wedge y$ existiert, aber kein Supremum von x und y .

Abbildung 14: Hasse-Diagramme zweier teilgeordneten Mengen mit Elementen x und y .

- (c) In einer Potenzmenge $(2^X, \subseteq)$ ist das Supremum zweier Teilmengen $A, B \subseteq X$ ihre Vereinigung $A \cup B$, und das Infimum ihre Schnittmenge $A \cap B$.

Folgende Beobachtung ist eng verwandt mit Beispiel 3.2.2(d).

3.3.3 Lemma. Sei M eine teilgeordnete Menge, in der alle binären Suprema existieren. Dann gibt es einen Galois-Zusammenhang

$$\begin{array}{ccc}
 & (x, y) \mapsto x \vee y & \\
 M \times M & \xrightarrow{\quad} & M \\
 & \xleftarrow{\quad} & \\
 & a \mapsto (a, a) &
 \end{array}$$

wobei $M \times M$ mit der komponentenweisen Ordnung versehen ist.

Beweis. Die Eigenschaft des Galois-Zusammenhangs besagt, dass für alle $x, y \in M$ und $a \in M$ gilt:

$$x \vee y \leq a \iff x \leq a \text{ und } y \leq a.$$

Die Implikationsrichtung $\Rightarrow$ besagt mit $a = x \vee y$ gerade, dass $x \vee y$ eine obere Schranke von x und y ist, und der Fall von allgemeinem a folgt daraus per Transitivität. Die Implikationsrichtung $\Leftarrow$ sagt dann genau aus, dass $x \vee y$ die *kleinste* obere Schranke ist. $\square$

Nach Korollar 3.2.5(a) ist die Bildung des Supremums als linksadjungierte Abbildung also eindeutig durch die Diagonaleinbettung $a \mapsto (a, a)$ bestimmt.

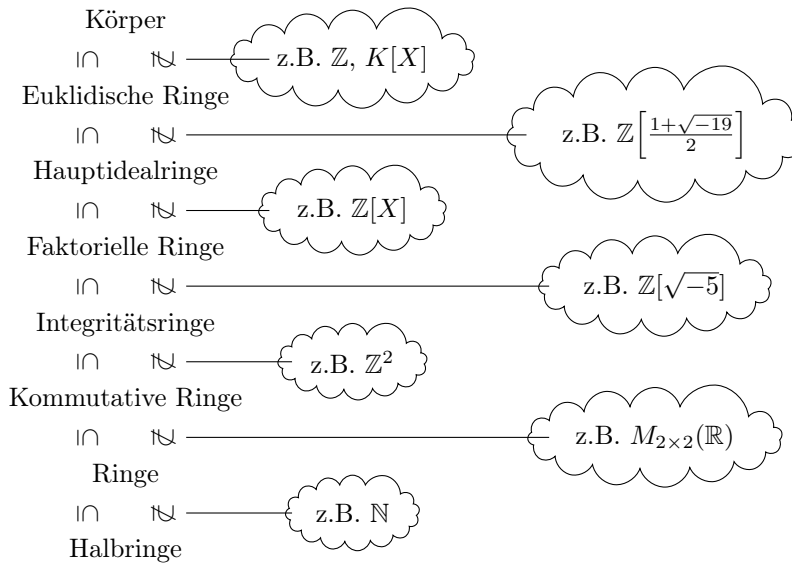


Abbildung 15: Die Klassen von Strukturen, um die es in diesem Kapitel hauptsächlich geht. Wie durch die Inklusionen von oben nach unten angegeben, sind weiter oben stehende Strukturen spezieller als weiter unten stehende. Dass es sich in allen Fällen um echte Inklusionen handelt, wird durch die rechts dargestellten Gegenbeispiele illustriert. Zum Beispiel sind $\mathbb{Z}$ und $K[X]$ euklidische Ringe, aber keine Körper.

4 Ringe

Im Laufe der Geschichte hat sich der Begriff der Zahl immer weiter verallgemeinert. Basierend auf dem Abzählen von Gegenständen bilden die natürlichen Zahlen $\mathbb{N}$ das vermutlich einfachste Zahlensystem überhaupt. Durch das “Entdecken” (oder Erfinden?) von negativen Zahlen, was zum Beispiel in der finanziellen Buchhaltung notwendig war, gelangt man von $\mathbb{N}$ zu den ganzen Zahlen $\mathbb{Z}$. Die Notwendigkeit, auch Brüche zu verwenden, führt dann zu den rationalen Zahlen $\mathbb{Q}$. Durch die Erkenntnis der Pythagoräer, dass $\sqrt{2}$ keine rationale Zahl sein kann, erreicht man als nächstes die reellen Zahlen $\mathbb{R}$. Schließlich führt das Hinzufügen der imaginären Einheit $i = \sqrt{-1}$ zu den komplexen Zahlen $\mathbb{C}$.

Ist das jetzt das Ende der Fahnenstange? Oder sind vielleicht noch zusätzliche Erweiterungen von Zahlensystemen sinnvoll, zum Beispiel durch das Hinzufügen von unendlichen großen oder infinitesimal kleinen Zahlen? In welchem mathematischen Rahmen können wir solche Fragen überhaupt präzisieren und sie schließlich beantworten?

Diese Fragen sollen uns als Motivation für die Entwicklung der Ringtheorie (dieses Kapitel) und der Körpertheorie (Abschnitt 5) dienen. Dies sind zwei sehr klassische Teilgebiete der Algebra, welche sich mit der abstrakten Theorie von Strukturen beschäftigen, die die Rechenregeln von Addition und Multiplikation erfüllen. Neben der Motivation durch die Erweiterung von Zahlensystemen gibt es aber auch viele weitere Anwendungen, sowohl innermathematisch als Grundlage für zum Beispiel die algebraische Geometrie und Zahlentheorie, aber auch außerhalb der Mathematik, zum Beispiel in der Kryptographie [4] und der Quantenmechanik [6].

4.1 Definitionen und erste Beispiele

Wir besprechen hier die Definitionen von Halbringen, (kommutativen) Ringen und Körpern. Die spezielleren Klassen von Ringen aus Abbildung 15 werden dann in den folgenden Unterabschnitten behandelt. Folgende Definition ist unter anderem motiviert durch die angegebenen Beispiele von Zahlensystemen, weil dort jeweils eine Addition und eine Multiplikation definiert ist, welche die folgenden Rechenregeln erfüllen.

4.1.1 Definition. Ein **Halbring** ist eine Menge R zusammen mit zwei Verknüpfungen

$$+ : R \times R \longrightarrow R, \quad \cdot : R \times R \longrightarrow R,$$

und Elementen $0, 1 \in R$, so dass die folgenden Rechenregeln erfüllt sind:

(a) $(R, +, 0)$ ist ein kommutatives Monoid: für alle $x, y, z \in R$ gilt

$$\begin{aligned} x + (y + z) &= (x + y) + z, \\ x + 0 &= 0 + x = x \\ x + y &= y + x. \end{aligned}$$

(b) $(R, \cdot, 1)$ ist ein Monoid: für alle $x, y, z \in R$ gilt

$$\begin{aligned} x(yz) &= (xy)z, \\ x \cdot 1 &= 1 \cdot x = x. \end{aligned}$$

(c) Distributivgesetze: für alle $x, y, z \in R$ gilt

$$\begin{aligned} (x + y)z &= xz + yz, \\ z(x + y) &= zx + zy. \end{aligned}$$

(d) Annihilationsgesetz: für alle $x \in R$ gilt

$$0 \cdot x = x \cdot 0 = 0.$$

Dabei schreiben wir wie üblich meist xy statt $x \cdot y$.

4.1.2 Bemerkung. Per Induktion über $n \in \mathbb{N}$ kann man zeigen, dass die Distributivgesetze auch in der allgemeineren Form

$$(x_1 + \dots + x_n)y = x_1y + \dots + x_ny, \quad x(y_1 + \dots + y_n) = xy_1 + \dots + xy_n$$

gelten. Dies macht sogar auch für $n = 0$ noch Sinn, und in diesem Fall entspricht es genau dem Annihilationsgesetz, denn eine leere Summe ist per Definition 0.

4.1.3 Beispiel. (a) $\mathbb{N}$ mit den üblichen Verknüpfungen ist ein Halbring. Auch alle anderen der üblichen Zahlensysteme, also $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind entsprechend Halbringe.

(b) Sei R ein Halbring und $n \in \mathbb{N}$. Dann ist auch $M_{n \times n}(R)$, die Menge der $n \times n$ -Matrizen mit Einträgen in R , ein Halbring bezüglich der eintragsweisen Addition und der Matrixmultiplikation, definiert durch

$$(AB)_{ij} := \sum_{k=1}^n A_{ik}B_{kj},$$

wobei man die Rechenregeln explizit nachrechnet. Die Nullmatrix sowie die Einheitsmatrix sind die neutralen Elemente.

(c) Für Halbringe $R_1, \dots, R_n$ ist ihr **Produkt** $R_1 \times \dots \times R_n$ definiert als das kartesische Produkt zusammen mit den komponentenweisen Operationen,

$$\begin{aligned} (a_1, \dots, a_n) + (b_1, \dots, b_n) &:= (a_1 + b_1, \dots, a_n + b_n), \\ (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) &:= (a_1 \cdot b_1, \dots, a_n \cdot b_n). \end{aligned}$$

Wie bei Definition 2.6.1 rechnet man leicht nach, dass dies tatsächlich wieder ein Halbring ist.

(d) Der **Nullhalbring** ist $N := \{0\}$. Da die 0 das einzige Element ist, ist natürlich

$$0 + 0 = 0, \quad 0 \cdot 0 = 0$$

die einzige Möglichkeit, Addition und Multiplikation zu definieren. Die Rechenregeln gelten trivialerweise, weil für jede Regel beide Seiten notwendigerweise $= 0$ sind. Das Einselement ist $1 = 0$.

Umgekehrt ist der Nullhalbring auch der *einzige* Halbring mit $1 = 0$. Denn falls $1 = 0$ in einem Halbring R , dann folgt für alle $x \in R$,

$$x = 1 \cdot x = 0 \cdot x = 0,$$

also ist 0 das einzige Element. (Genausogut könnten wir natürlich $N = \{1\}$ mit $1 + 1 = 1$ schreiben und sagen, dass 1 das einzige Element ist.)

(e) Auf wie viele Arten kann man $R = \{0, 1\}$ zu einem Halbring machen? Damit 0 das Nullelement ist, muss natürlich

$$0 + 0 = 0, \quad 1 + 0 = 0 + 1 = 1 \tag{4.1}$$

gelten. Die Multiplikation ist sogar bereits komplett durch die Axiome festgelegt, nämlich als

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1. \tag{4.2}$$

Jetzt gibt es noch zwei Möglichkeiten für die fehlende Addition, die sich beide als sehr interessant herausstellen:

▷ Es könnte

$$1 + 1 = 0$$

gelten. In diesem Fall bekommen wir tatsächlich einen Halbring, und sogar einen Körper. Es ist der einzige Körper mit 2 Elementen (bis auf Isomorphie), und wir werden ihn später mit $\mathbb{F}_2$ bezeichnen.

▷ Es könnte

$$1 + 1 = 1 \tag{4.3}$$

gelten. Auch in diesem Fall kann man sich durch Nachrechnen aller Rechengesetze davon überzeugen, dass es sich um einen Halbring handelt. Interpretiert man

$$0 = \text{falsch}, \quad 1 = \text{wahr}, \quad + = \text{oder}, \quad \cdot = \text{und},$$

dann entsprechen (4.1)–(4.3) genau den Regeln der Aussagenlogik. So bedeuten die Regeln für die Addition gerade, dass eine Aussage “ P oder Q ” genau dann wahr ist, wenn P oder Q wahr ist; und die Multiplikation entspricht der Tatsache, dass “ P und Q ” genau dann wahr ist, wenn P und Q wahr sind.

Für die allgemeine Theorie der Halbringe sei hier auf Literatur wie [2] verwiesen. Wir beschränken uns ab sofort auf die klassische Theorie der Ringe, welche dank der Existenz von additiven Inversen etwas einfacher zu handhaben ist.

4.1.4 Definition. Ein **Ring** ist ein Halbring $(R, +, \cdot)$, in dem jedes Element ein additives Inverses besitzt: für jedes $x \in R$ gibt es $-x \in R$ mit

$$x + (-x) = 0.$$

In einem Ring R ist $(R, +, 0)$ also eine abelsche Gruppe. Aufgrund der Eindeutigkeit von inversen Elementen in Gruppen allgemein (Bemerkung 2.1.9) ist $-x$ immer eindeutig durch x bestimmt.

4.1.5 Lemma. In jedem Ring gilt auch das Rechengesetz

$$(-a)b = a(-b) = -ab.$$

Beweis. Es genügt zu zeigen, dass $(-a)b$ ein additives Inverses von ab ist; der Beweis für $a(-b)$ ist analog. Dies folgt aus dem Distributivgesetz mittels

$$(-a)b + ab = (-a + a)b = 0 \cdot b = 0. \quad \square$$

Viele der Halbringe aus Beispiel 4.1.3 sind sogar Ringe.

4.1.6 Beispiel. (a) Die Zahlensysteme $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Ringe, weil man subtrahieren kann. $\mathbb{N}$ dagegen ist offensichtlich kein Ring, weil z.B. 1 kein additives Inverses hat.

(b) Der Nullhalbring $N = \{0\}$ ist ein Ring, in dem $1 = 0$ gilt. Wir bezeichnen ihn als **Nullring**.

(c) Falls R ein Ring ist, dann ist auch $M_{n \times n}(R)$ ein Ring, weil man das additive Inverse $-A$ einer Matrix A einfach durch Bilden der additiven Inversen der Einträge bekommt.

(d) Falls $R_1, \dots, R_n$ Ringe sind, dann ist auch $R_1 \times \dots \times R_n$ ein Ring, mit

$$-(a_1, \dots, a_n) = (-a_1, \dots, -a_n).$$

Die in der klassischen Algebra am häufigsten betrachteten Ringe sind kommutativ:

4.1.7 Definition. Ein **kommutativer Ring** ist ein Ring R , in dem für alle $x, y \in R$ gilt

$$xy = yx.$$

4.1.8 Bemerkung. Die Matrixringe $M_{n \times n}(R)$ sind im Allgemeinen nicht kommutativ, da die Matrixmultiplikation bekanntermaßen nicht kommutativ ist.²⁵ Diese nicht-kommutativen Ringe sind zum Beispiel in der Quantenmechanik von Bedeutung, was sich auch im Namen ihres historischen Vorläufers (der “Matrizenmechanik”) widerspiegelt. Die Theorie der kommutativen Ringe ist etwas einfacher als die der nicht-kommutativen, und wir beschränken uns für den Rest dieser Vorlesung auf den kommutativen Fall.

4.1.9 Beispiel. Sei M ein Monoid (Definition 2.1.1) und R ein kommutativer Ring. Der **Monoidring** $R[M]$ ist dann die Menge aller Funktionen $f: M \rightarrow R$ mit endlichem Träger, d. h.

$$R[M] = \{f: M \rightarrow R \mid \{x \in M : f(x) \neq 0\} \text{ ist endlich}\},$$

ausgestattet mit der punktweisen Addition

$$(f + g)(x) := f(x) + g(x)$$

und der Multiplikation

$$(f \cdot g)(x) := \sum_{(y,z) \in M : x=yz} f(y)g(z). \quad (4.4)$$

Hierdurch wird $R[M]$ tatsächlich zu einem Ring (Übung), und dieser Ring ist genau dann kommutativ, falls M kommutativ ist. Zunächst ist dabei zu zeigen, dass $f + g$ und $f \cdot g$ auch endlichen Träger haben, sobald dies für f und g selbst gilt. Falls $M = G$ eine Gruppe ist, dann bezeichnen wir $R[G]$ auch als **Gruppenring** $R[G]$.

Oft schreibt man eine Funktion $f: M \rightarrow R$ mit endlichem Träger auch als “formale Linearkombination”

$$f = \sum_{x \in M} f(x)x,$$

wobei aufgrund der Endlichkeit des Trägers nur endlich viele Terme $\neq 0$ sind. Falls zum Beispiel D_{10} die Diedergruppe zu $n = 5$ ist (Beispiel 2.1.18), dann schreibt man

$$3r^2 + 5r^3s - 7r^4s \in \mathbb{Z}[D_{10}]$$

²⁵Übung: zeige, dass $M_{n \times n}(R)$ genau dann kommutativ ist, wenn $n < 2$ oder R der Nullring ist.

für die Funktion, die r^2 auf 3, r^3s auf 5, r^4s auf -7 und alle anderen Elemente von D_{10} auf 0 abbildet. Zwei solche Ausdrücke werden multipliziert, indem man das Produkt der Summen formal ausmultipliziert und die Produkte der Elemente von M durch die Multiplikation in M berechnet und dann die Koeffizienten der gleichen Elemente von M addiert. So erhält man zum Beispiel

$$\begin{aligned}(3r^2 + 5r^3s) \cdot (r + 4s) &= 3r^2 \cdot r + 12r^2 \cdot s + 5r^3s \cdot r + 20r^3s \cdot s \\ &= 3r^3 + 12r^2s + 5r^2s + 20r^3 \\ &= 23r^3 + 17r^2s,\end{aligned}$$

Dies entspricht der Multiplikation von Funktionen durch (4.4) folgendermaßen: Im Produkt ist der Koeffizient von $x \in M$ einerseits durch $(f \cdot g)(x)$ gegeben, andererseits durch die Summe $\sum_{(y,z) \in M : x=yz} f(y)g(z)$, weil der zu jedem Paar (y, z) gehörige Term einen Beitrag zum Koeffizienten von $yz = x$ liefert, nämlich das Produkt $f(y)g(z)$, welches dem Produkt der Koeffizienten von y und z in den einzelnen Faktoren f und g entspricht.

Betrachten wir jetzt als zweites Beispiel $M = \mathbb{N}$ als Monoid bezüglich Addition. Dann wird $R[\mathbb{N}]$ aus folgendem Grund auch als **Polynomring** bezeichnet. Ein Element $a \in R[\mathbb{N}]$ ist eine Funktion $a : \mathbb{N} \rightarrow R$ mit endlichem Träger. Eine solche Funktion können wir auch als eine Folge $(a_0, a_1, a_2, \dots)$ von Elementen aus R auffassen, von denen nur endlich viele $\neq 0$ sind. Andererseits können wir eine solche Folge auch als Polynom

$$a_0 + a_1X + \dots + a_nX^n = \sum_{i=0}^n a_iX^i \quad (4.5)$$

schreiben, wobei die Notation implizit aussagt, dass $a_i = 0$ für $i > n$. In dieser Schreibweise heißen die Folgenglieder a_i die **Koeffizienten** des Polynoms, und falls $a_n \neq 0$ ist, dann heißt n der **Grad** des Polynoms und wird mit $\deg(a)$ bezeichnet. Die Nullfolge $(0, 0, 0, \dots)$ ist dabei ein ausgearteter Spezialfall, weil in diesem Fall der Ausdruck überhaupt keinen Term enthält, und der Grad deshalb als $-\infty$ definiert wird. Man spricht dann auch vom **Nullpolynom**. Das Symbol X in einem Polynom wird als “Variable” bezeichnet. Formal ist die einzige Bedeutung der Variable, dass ihr Exponent anzeigt, zu welchem Element der Folge der jeweilige Koeffizient a_i gehört. Dadurch können die einzelnen Terme in einem Polynom (4.5) in beliebiger Reihenfolge geschrieben werden.

Die Schreibweise als Polynom ist deswegen sinnvoll, weil die Addition und die Multiplikation genau der bekannten Addition und Multiplikation von Polynomen entsprechen,

$$\left(\sum_{i=0}^n a_iX^i \right) + \left(\sum_{i=0}^m b_iX^i \right) = \sum_{i=0}^{\max(n,m)} (a_i + b_i)X^i,$$

wobei wir $a_i := 0$ für $i > n$ und $b_i := 0$ für $i > m$ setzen, und

$$\left(\sum_{i=0}^n a_iX^i \right) \cdot \left(\sum_{j=0}^m b_jX^j \right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^k a_ib_{k-i} \right) X^k.$$

Diese Additions- und Multiplikationsregeln entsprechen genau den Regeln für das Rechnen in $R[\mathbb{N}]$, denn dort addiert und multipliziert man die Funktionen durch

$$(a + b)(k) = a(k) + b(k), \quad (a \cdot b)(k) = \sum_{i=0}^k a(i)b(k-i).$$

Eine Folge der Form $(r, 0, 0, \dots)$ mit $r \in R$ enthält nur den ersten Term und wird als das **konstante Polynom** r geschrieben, in dem die Variable X gar nicht vorkommt.

Für $d \in \mathbb{N}$ kann man allgemeiner auch $M = \mathbb{N}^d$ als Monoid bezüglich der komponentenweisen Addition betrachten. In diesem Fall kann man $R[\mathbb{N}^d]$ auch als Polynomring in d Variablen

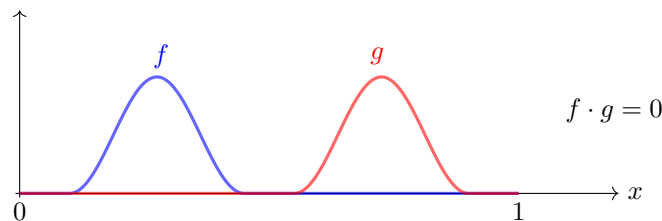


Abbildung 16: Skizze zweier stetiger Funktionen $f, g \in C([0, 1], \mathbb{R})$ mit $f, g \neq 0$, so dass $f \cdot g = 0$.

$X_1, \dots, X_d$ schreiben. Denn ähnlich wie oben entspricht eine Funktion $a : \mathbb{N}^d \rightarrow R$ mit endlichem Träger einem Polynom

$$\sum_{i_1, \dots, i_d \in \mathbb{N}} a_{i_1, \dots, i_d} X_1^{i_1} \cdots X_d^{i_d},$$

und die Rechenregeln für die Addition und Multiplikation von Funktionen entsprechen genau den Rechenregeln, wie man Polynome in mehreren Variablen addiert und multipliziert.

Zwei weitere Anmerkungen zu Polynomringen:

- ▷ Da Polynome eng verwandt mit der Analysis sind, bezeichnen wir Elemente eines Polynomrings meist mit Symbolen für Funktionen wie f und g , also zum Beispiel

$$f = \sum_{i_1, \dots, i_d \in \mathbb{N}} f_{i_1, \dots, i_d} X_1^{i_1} \cdots X_d^{i_d}.$$

- ▷ In einer Notation der Form $R[A]$ kann A sowohl ein Monoid sein, so dass $R[A]$ der Monoidring von A über R ist, oder eine Variable, in welchem Fall $R[A]$ ein Polynomring ist. Aus dem Kontext wird klar, welcher Fall gemeint ist.

Wir beschränken uns für den Rest der Vorlesung auf kommutative Ringe. Das folgende Beispiel führt eine Klasse von sehr “großen” kommutativen Ringen ein, die sich in mancher Hinsicht sehr anders als Polynomringe verhalten.

4.1.10 Beispiel. Sei T eine Teilmenge von $\mathbb{R}^n$ oder ein beliebiger topologischer Raum. Wir schreiben dann $C(T, \mathbb{R})$ für die Menge aller stetigen Funktionen $T \rightarrow \mathbb{R}$.²⁶ Da die punktweise Addition und Multiplikation stetiger Funktionen

$$(f + g)(t) := f(t) + g(t), \quad (fg)(t) := f(t)g(t)$$

wieder stetig sind, ist $C(T, \mathbb{R})$ abgeschlossen unter diesen Verknüpfungen. Man prüft dann weiterhin leicht nach, dass es sich bei $C(T, \mathbb{R})$ um einen kommutativen Ring handelt, dessen neutrale Elemente die konstanten Funktionen $t \mapsto 0$ und $t \mapsto 1$ sind. Wenn man komplexwertige Funktionen verwendet, bekommt man analog einen kommutativen Ring $C(T, \mathbb{C})$. Diese Ringe spielen in der Analysis eine wichtige Rolle. Für unsere Zwecke dienen sie eher als Beispiele für Ringe mit teilweise merkwürdigem Verhalten. Zum Beispiel gibt es $f, g \in C([0, 1], \mathbb{R})$ mit $f, g \neq 0$, so dass $f \cdot g = 0$ (Abbildung 16). Dies kann offensichtlich in den Zahlensystemen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ nicht passieren, weil dort die Multiplikation von Zahlen genau dann 0 ergibt, wenn mindestens einer der Faktoren 0 ist.

Ähnlich kann man anstatt mit stetigen Funktionen auch mit glatten Funktionen, messbaren Funktionen oder ähnlichem arbeiten, und erhält so jeweils wieder kommutative Ringe. Auch diese Ringe sind im jeweiligen Fachgebiet von wesentlicher Bedeutung.

Ein Ring R ist ein Monoid bezüglich der Multiplikation. Entsprechend ist die Menge der invertierbaren Elemente $R^\times$ eine Gruppe (Beispiel 2.1.11). Für diese Gruppe gibt es eine spezielle Terminologie.

4.1.11 Definition. Sei R ein Ring.

²⁶Das “C” steht für “continuous” (stetig).

- (a) Die **Einheitengruppe** von R ist die Gruppe der invertierbaren Elemente von R bezüglich der Multiplikation, also

$$R^\times = \{a \in R \mid \exists b \in R \text{ mit } ab = 1 = ba\}.$$

Die Elemente von $R^\times$, also die invertierbaren Elemente von R , heißen auch **Einheiten**.

- (b) R ist ein **Körper**, falls R kommutativ ist und

$$R^\times = R \setminus \{0\}.$$

Die Bezeichnung “Einheit” ist nicht besonders sinnvoll, weil man den Begriff von Einheit leicht mit der Einheit $1 \in R$ im Sinne von neutralem Element der Multiplikation verwechseln kann. Der Begriff ist historisch gewachsen und wird deshalb trotzdem verwendet.

4.1.12 Beispiel. (a) Für die ganzen Zahlen ist

$$\mathbb{Z}^\times = \{-1, 1\},$$

eine zyklische Gruppe der Ordnung 2.

- (b) Die Zahlensysteme $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind Körper.

- (c) Der Nullring $N = \{0\}$ dagegen ist kein Körper: das einzige Element 0 ist wegen

$$0 \cdot 0 = 0 \neq 1$$

invertierbar! Also gilt $N^\times = N \neq N \setminus \{0\}$, und daher ist N kein Körper, obwohl jedes Element invertierbar ist.

- (d) Für einen Körper K betrachten wir den Polynomring $K[X]$. Für die Multiplikation von Polynomen in $K[X]$ gilt

$$\deg(fg) = \deg(f) + \deg(g), \quad (4.6)$$

denn die Leitkoeffizienten von f und g sind $\neq 0$ und daher invertierbar in K , und daher ist auch ihr Produkt $\neq 0$. Mit anderen Worten, der Koeffizient von $X^{\deg(f)+\deg(g)}$ in fg ist $\neq 0$, und damit ist $\deg(fg) \geq \deg(f) + \deg(g)$. Andererseits ist klar, dass $\deg(fg) \leq \deg(f) + \deg(g)$, denn die Koeffizienten von X^n für $n > \deg(f) + \deg(g)$ in fg sind alle 0.

Somit folgt, dass ein nicht-konstantes Polynom f nicht invertierbar sein kann, denn falls $fg = 1$ für ein Polynom g gilt, dann muss $\deg(fg) = \deg(1) = 0$ sein, und damit $\deg(f) + \deg(g) = 0$, was nur möglich ist, wenn $\deg(f) = \deg(g) = 0$ ist, also f und g konstant sind. Andererseits ist jedes konstante Polynom $\neq 0$ auch invertierbar. Wir erhalten daher

$$K[X]^\times = K^\times.$$

Als weitere Folgerung aus (4.6) stellen wir fest, dass in $K[X]$ die Implikation

$$f, g \neq 0 \implies fg \neq 0$$

gilt. Dies ist als Gegensatz zu den stetigen Funktionen in Abbildung 16 zu sehen.

- (e) In $C(T, \mathbb{R})$ sind die Einheiten genau die stetigen Funktionen $T \rightarrow \mathbb{R}$, die keine Nullstelle haben.

Denn falls $f \in C(T, \mathbb{R})$ eine Nullstelle $t_0 \in T$ hat, dann ist $f(t_0) = 0$, und damit kann f nicht invertierbar sein. Falls umgekehrt f keine Nullstelle hat, dann können wir f^{-1} durch $f^{-1}(t) := f(t)^{-1}$ für alle $t \in T$ definieren, und man kann sich mit etwas Analysis davon überzeugen, dass f^{-1} ebenfalls stetig ist. Da die Multiplikation von Funktionen punktweise definiert ist, gilt dann auch $ff^{-1} = 1$, also ist f tatsächlich invertierbar.

Oft betrachtet man Elemente, die sich um eine Einheit unterscheiden, als gleichwertig. Zum Beispiel sind die ganzen Zahlen 3 und -3 beide Primzahlen, und Teiler von genau den gleichen Zahlen. Zwei Polynome, die sich nur um einen konstanten Faktor unterscheiden, verhalten sich aus Sicht der Algebra ebenfalls sehr ähnlich, zum Beispiel haben sie die gleichen Nullstellen. Deshalb führt man folgenden Begriff ein.

4.1.13 Definition. Sei R ein kommutativer Ring. Zwei Elemente $a_1, a_2 \in R$ heißen **assoziert**, wenn es eine Einheit $u \in R^\times$ mit $a_1 = ua_2$ gibt. In diesem Fall schreiben wir

$$a_1 \sim a_2.$$

Die folgenden Beobachtungen erfassen die wichtigsten Eigenschaften von Assoziiertheit.

4.1.14 Lemma. In jedem kommutativen Ring R gilt:

- (a) Assoziiertheit ist eine Äquivalenzrelation
- (b) Assoziiertheit ist kompatibel mit der Multiplikation:

$$a_1 \sim a_2, \quad b_1 \sim b_2 \quad \implies \quad a_1 b_1 \sim a_2 b_2. \quad (4.7)$$

Beweis. Wir zeigen die Eigenschaften einer Äquivalenzrelation:

- ▷ Reflexivität: Es gilt $a = 1 \cdot a$ für alle $a \in R$, also $a \sim a$.
- ▷ Symmetrie: Wenn $a_1 = ua_2$ mit $u \in R^\times$, dann ist auch $a_2 = u^{-1}a_1$, also $a_2 \sim a_1$.
- ▷ Transitivität: Wenn $a_1 = ua_2$ mit $u \in R^\times$ und $a_2 = va_3$ mit $v \in R^\times$, dann gilt auch

$$a_1 = uva_3$$

und $uv \in R^\times$, somit $a_1 \sim a_3$. □

Für die Kompatibilität mit der Multiplikation nehmen wir an, dass $a_1 = ua_2$ und $b_1 = vb_2$ für geeignete $u, v \in R^\times$. Dann folgt dank der Kommutativität

$$a_1 b_1 = ua_2 vb_2 = uva_2 b_2,$$

und aufgrund von $uv \in R^\times$ ist also $a_1 b_1 \sim a_2 b_2$.

Die Kompatibilität mit der Multiplikation impliziert, dass die Menge der Äquivalenzklassen ebenfalls ein kommutatives Monoid bezüglich der Multiplikation der Repräsentanten ist,

$$[a] \cdot [b] := [ab],$$

denn dies ist durch (4.7) wohldefiniert, d. h. die Wahl der Repräsentanten a und b spielt keine Rolle.

4.1.15 Beispiel. (a) Da $\mathbb{Z}^\times = \{-1, 1\}$, sind $a, b \in \mathbb{Z}$ genau dann assoziiert, wenn $a = \pm b$ gilt.

(b) In einem Körper K sind alle Elemente außer 0 Einheiten, also sind alle Elemente außer 0 miteinander assoziiert, und 0 ist nur mit sich selbst assoziiert.

(c) Zwei Polynome $f_1, f_2 \in K[X]$ sind genau dann assoziiert, wenn sie sich durch einen konstanten Faktor unterscheiden, also $f_1 = uf_2$ mit $u \in K^\times$.

(d) In $C(T, \mathbb{R})$ für $T \subseteq \mathbb{R}^n$ ist Assoziiertheit meist schwieriger zu charakterisieren. Einerseits impliziert $f \sim g$ natürlich, dass f und g die gleichen Nullstellen haben. Die Umkehrung gilt aber leider nicht. Zum Beispiel in $C([-1, 1], \mathbb{R})$ haben die Funktionen $f(t) = t$ und $g(t) = t^2$ die gleichen Nullstellen, nämlich 0, aber es gibt überhaupt kein $h \in C([-1, 1], \mathbb{R})$ mit $f = hg$, denn dann müsste für $t \neq 0$ gelten

$$h(t) = \frac{f(t)}{g(t)} = \frac{t}{t^2} = \frac{1}{t}.$$

Dies kann aber nicht stetig auf $t = 0$ fortgesetzt werden. Also sind f und g nicht assoziiert, obwohl sie die gleichen Nullstellen haben.

4.2 Unterringe

Hier und im Folgenden bezeichnet R stets einen kommutativen Ring.

4.2.1 Definition. Eine Teilmenge $S \subseteq R$ heißt **Unterring** von R , falls

(a) $0, 1 \in S$,

(b) für alle $x, y \in S$ gelten

$$x + y \in S, \quad xy \in S, \quad -x \in S.$$

Diese Bedingungen sind genau die, die nötig sind, damit $(S, +, \cdot)$ selbst ein kommutativer Ring mit den gleichen Verknüpfungen (eingeschränkt auf S) und den gleichen neutralen Elementen wie R ist. Denn die Rechengesetze wie das Distributivgesetz und Neutralität von 0 und 1 gelten in S , weil sie in R gelten.

In diesem Kapitel spielen Unterringe keine große Rolle. In Abschnitt 5 dagegen werden Unterkörper von Körpern das zentrale Thema sein, und deshalb ist es sinnvoll, hier Unterringe kurz zu behandeln.

4.2.2 Beispiel. (a) $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$, von $\mathbb{R}$ und von $\mathbb{C}$.

Umgekehrt hat $\mathbb{Z}$ keine echten Unterringe, da für jeden Unterring $S \subseteq \mathbb{Z}$ auch $1 \in S$ gelten muss, und S unter Addition und Subtraktion abgeschlossen sein muss. Also ist $S = \mathbb{Z}$ die einzige Möglichkeit.

(b) Jeden Ring R kann man als denjenigen Unterring von $R[X]$ auffassen, der aus den konstanten Polynomen besteht.

(c) Für jeden Ring R bilden die Diagonalmatrizen in $M_{n \times n}(R)$ einen Unterring, der isomorph zu $R^n = R \times \dots \times R$ ist, weil auf Diagonalmatrizen sowohl die Addition als auch die Multiplikation komponentenweise definiert ist.

(d) Für jeden Ring R und $n \in \mathbb{N}$ ist R^n ein Ring bezüglich der komponentenweisen Verknüpfungen. In R^n gibt es einen Unterring, der aus den Tupeln besteht, deren Einträge alle gleich sind. Dieser Unterring ist offensichtlich isomorph zu R .

(e) Die **gaußschen Zahlen**

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

sind eine Teilmenge von $\mathbb{C}$, die bezüglich der üblichen Addition und Multiplikation von komplexen Zahlen abgeschlossen ist. Da weiters auch $0, 1 \in \mathbb{Z}[i]$ gilt, ist $\mathbb{Z}[i]$ ein Unterring von $\mathbb{C}$.

(f) Noch allgemeiner: Für $a_1, \dots, a_n \in \mathbb{C}$ bezeichnen wir mit

$$\mathbb{Z}[a_1, \dots, a_n]$$

den kleinsten Unterring von $\mathbb{C}$, der $a_1, \dots, a_n$ enthält. Konkret besteht $\mathbb{Z}[a_1, \dots, a_n]$ aus allen komplexen Zahlen, die man als ganzzahlige Linearkombinationen von Produkten der a_i schreiben kann, oder anders ausgedrückt, die man als Polynome in den a_i schreiben kann. Es ist klar, dass dies tatsächlich der kleinste Unterring ist, der die a_i enthält: einerseits ist $a_i \in \mathbb{Z}[a_1, \dots, a_n]$ für alle i offensichtlich, und falls andererseits $R \subseteq \mathbb{C}$ ein Unterring mit $a_i \in R$ für alle i ist, dann muss R auch alle Polynome in den a_i enthalten, also $\mathbb{Z}[a_1, \dots, a_n] \subseteq R$.

Zum Beispiel gilt

$$\mathbb{Z}\left[\frac{1}{2}, \sqrt{2} + \sqrt{3}\right] = \mathbb{Z}\left[\frac{1}{2}, \sqrt{2}, \sqrt{3}\right]. \quad (4.8)$$

Denn einerseits haben wir $\subseteq$, weil sich die beiden Erzeuger $\frac{1}{2}$ und $\sqrt{2} + \sqrt{3}$ offensichtlich als Polynome in $\frac{1}{2}, \sqrt{2}$ und $\sqrt{3}$ mit Koeffizienten aus $\mathbb{Z}$ schreiben lassen, denn sie sind ja bereits von dieser Form. Andererseits gilt auch $\supseteq$, weil sich analog die Erzeuger $\frac{1}{2}, \sqrt{2}$ und

$\sqrt{3}$ als Polynome in $\frac{1}{2}$ und $\sqrt{2} + \sqrt{3}$ mit Koeffizienten aus $\mathbb{Z}$ schreiben lassen. Dies ist eher überraschend, gilt aber tatsächlich aufgrund von

$$\begin{aligned}\sqrt{2} &= \frac{1}{2}(\sqrt{2} + \sqrt{3})^3 - \frac{9}{2}(\sqrt{2} + \sqrt{3}) \\ \sqrt{3} &= -\frac{1}{2}(\sqrt{2} + \sqrt{3})^3 + \frac{11}{2}(\sqrt{2} + \sqrt{3})\end{aligned}$$

Wir werden uns mit Phänomenen dieser Form in Abschnitt 5 noch ausführlicher beschäftigen.

4.3 Ringhomomorphismen, Ideale und der Isomorphiesatz

Wie in der Gruppentheorie ist es auch in der Ringtheorie sinnvoll, die Beziehungen zwischen zwei Ringen mittels strukturerhaltender Abbildungen zu untersuchen. Mit “strukturerhaltend” ist hier gemeint, dass die Abbildung die Rechenregeln der Ringe respektiert, also die Addition und Multiplikation in den Ringen im folgenden Sinne miteinander verträglich sind:

4.3.1 Definition. Eine Abbildung zwischen kommutativen Ringen

$$\varphi : R \longrightarrow S$$

heißt **Ringhomomorphismus** oder kurz **Homomorphismus**, falls

$$\begin{aligned}\varphi(1_R) &= 1_S \\ \varphi(x + y) &= \varphi(x) + \varphi(y) \\ \varphi(xy) &= \varphi(x)\varphi(y)\end{aligned} \quad \forall x, y \in R.$$

Wir kürzen “Ringhomomorphismus” zu “Homomorphismus” ab, falls aus dem Kontext klar ist, dass wir uns auf Ringe beziehen. Durch Anwendung von Lemma 2.2.8 auf die additive Gruppe $(R, +, 0)$ folgt, dass ein Homomorphismus auch automatisch das Nullelement erhält, also

$$\varphi(0_R) = 0_S.$$

Da die Multiplikation aber meist keine Gruppe bildet, ist dieses Argument auf die Multiplikation nicht anwendbar, und in der Tat folgt die Anforderung $\varphi(1_R) = 1_S$ in der Definition von Homomorphismus nicht aus der Multiplikativität $\varphi(xy) = \varphi(x)\varphi(y)$, sondern muss explizit gefordert werden. Zum Beispiel ist für $m > n$ die Inklusionsabbildung $M_{n \times n}(\mathbb{R}) \hookrightarrow M_{m \times m}(\mathbb{R})$, welche eine $n \times n$ -Matrix mit Nullen auffüllt, additiv und multiplikativ, bildet aber nicht die Einheitsmatrix auf die Einheitsmatrix ab, ist also kein Homomorphismus in obigem Sinne.

4.3.2 Beispiel. (a) Für jeden Ring R und Unterring $S \subseteq R$ ist die Inklusionsabbildung

$$\begin{aligned}\iota : S &\longrightarrow R, \\ x &\longmapsto x\end{aligned}$$

ein Homomorphismus.

(b) Zu den wichtigsten Beispielen von Homomorphismen gehören die **Auswertungsabbildungen**. Sei dafür R ein kommutativer Ring und $a \in R$. Dann ist die Abbildung

$$\begin{aligned}\text{ev}_a : R[X] &\longrightarrow R, \\ \sum_{i=0}^n c_i X^i &\longmapsto \sum_{i=0}^n c_i a^i\end{aligned} \tag{4.9}$$

ein Homomorphismus. Polynome können also an Ringelementen ausgewertet werden, und dies wird algebraisch durch die Auswertungsabbildung beschrieben.

4.3.3 Definition. Ein **Ringisomorphismus** oder kurz **Isomorphismus** ist ein bijektiver Ringhomomorphismus.

Analog zu Satz 2.2.12 kann man zeigen, dass falls $\varphi : R \rightarrow S$ ein Isomorphismus ist, dann ist auch die Umkehrabbildung $\varphi^{-1} : S \rightarrow R$ ein Isomorphismus. Somit entsprechen die Ringisomorphismen genau den invertierbaren Ringhomomorphismen. Da wir in den folgenden Abschnitten viele weitere Beispiele von Ringisomorphismen sehen werden, soll ein einzelnes Beispiel hier genügen.

4.3.4 Beispiel. Seien R und S Ringe und $n \in \mathbb{N}$. Dann ist die Abbildung

$$\begin{aligned} M_{n \times n}(R) \times M_{n \times n}(S) &\longrightarrow M_{n \times n}(R \times S) \\ (A, B) &\longmapsto ((A_{ij}, B_{ij}))_{i,j=1}^n \end{aligned} \quad (4.10)$$

ein Isomorphismus. Diese Abbildung nimmt also eine Matrix A mit Einträgen aus R und eine Matrix B mit Einträgen aus S als Input und bildet daraus eine einzelne Matrix mit Einträgen aus $R \times S$, indem sie die Einträge von A und B paarweise kombiniert. Es ist klar, dass diese Abbildung bijektiv ist, denn umgekehrt kann eine Matrix mit Einträgen aus $R \times S$ in zwei einzelne Matrizen aufgespalten werden.

Es bleibt noch zu zeigen, dass die Abbildung (4.10) ein Homomorphismus ist. Die Addition wird offensichtlich erhalten, denn auf beiden Seiten wird eintragsweise und komponentenweise addiert. Für die Multiplikation gilt ähnliches, aber wir führen dies der Vollständigkeit halber explizit aus. Zwei Matrixpaare (A, B) und (A', B') werden auf der linken Seite zum Paar von Matrixprodukten

$$(AA', BB')$$

multipliziert. Die Bilder dieser Paare auf der rechten Seite multiplizieren sich zu

$$\begin{aligned} ((A_{ij}, B_{ij}))_{i,j=1}^n \cdot ((A'_{ij}, B'_{ij}))_{i,j=1}^n &= \left(\sum_{k=1}^n (A_{ik}, B_{ik})(A'_{kj}, B'_{kj}) \right)_{i,j=1}^n \\ &= \left(\sum_{k=1}^n (A_{ik}A'_{kj}, B_{ik}B'_{kj}) \right)_{i,j=1}^n \\ &= \left(\left(\sum_{k=1}^n A_{ik}A'_{kj}, \sum_{k=1}^n B_{ik}B'_{kj} \right) \right)_{i,j=1}^n \\ &= ((AA')_{ij}, (BB')_{ij})_{i,j=1}^n. \end{aligned}$$

wobei im ersten Schritt die Definition der Multiplikation in $M_{n \times n}(R \times S)$ verwendet wurde, im zweiten Schritt die Multiplikation in $R \times S$ und im dritten die Definition der Addition in $R \times S$.

Ein zentraler Begriff in der Ringtheorie ist der des Ideals. Ideale sind die ringtheoretische Entsprechung von normalen Untergruppen in der Gruppentheorie, mit dem wichtigen Unterschied, dass ein Ideal in den meisten Fällen kein Unterring ist. Der Einfachheit halber beschränken wir uns auf den kommutativen Fall.

4.3.5 Definition. Sei R ein kommutativer Ring. Eine Teilmenge $I \subseteq R$ heißt **Ideal**, falls:

- (a) $(I, +)$ ist eine additive Untergruppe von $(R, +)$,
- (b) für alle $r \in R$ und $x \in I$ gilt $rx \in I$.

Diese Definition hat eine leichte Redundanz: die zweite Eigenschaft impliziert $(-1)x = -x \in I$ für alle $x \in I$. Im ersten Teil könnten wir also stattdessen einfach fordern, dass I abgeschlossen unter Addition ist und 0 enthält, und die Abgeschlossenheit unter additiven Inversen folgt dann aus der zweiten Eigenschaft.

Die Relevanz von Idealen wird durch folgende Eigenschaft von Homomorphismen deutlich.

4.3.6 Lemma. Für jeden Ringhomomorphismus $\varphi : R \rightarrow S$ ist das Bild $\text{im}(\varphi) \subseteq S$ ein Unterring und der Kern $\ker(\varphi) \subseteq R$ ein Ideal.

Beweis. Die Behauptung über das Bild eines Homomorphismus ist leicht zu sehen.

Da ein Kern insbesondere eine additive Untergruppe sein muss, ist klar, dass $\ker(\varphi)$ die erste Bedingung von Definition 4.3.5 erfüllt. Für die zweite Bedingung sei also $r \in R$ und $x \in \ker(\varphi)$ gegeben. Dann folgt

$$\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0,$$

wobei im zweiten Schritt die Voraussetzung $x \in \ker(\varphi)$ verwendet wurde. Also gilt auch $rx \in \ker(\varphi)$, und damit ist $\ker(\varphi)$ tatsächlich ein Ideal. $\square$

4.3.7 Lemma. Sei R ein kommutativer Ring und $a_1, \dots, a_n \in R$. Dann ist die Menge

$$(a_1, \dots, a_n) := \{r_1 a_1 + \dots + r_n a_n \mid r_1, \dots, r_n \in R\}$$

ein Ideal von R , und zwar das kleinste Ideal, das die Elemente $a_1, \dots, a_n$ enthält.

Wir nennen $(a_1, \dots, a_n)$ das von $a_1, \dots, a_n$ **erzeugte Ideal**.

Beweis. Zunächst ist aufgrund der Kommutativität der Addition recht leicht zu sehen, dass die Menge eine additive Untergruppe ist, denn einerseits gilt

$$(r_1 a_1 + \dots + r_n a_n) + (s_1 a_1 + \dots + s_n a_n) = (r_1 + s_1) a_1 + \dots + (r_n + s_n) a_n,$$

und andererseits

$$-(r_1 a_1 + \dots + r_n a_n) = (-r_1) a_1 + \dots + (-r_n) a_n.$$

Außerdem ist die Menge abgeschlossen bezüglich Multiplikation mit einem beliebigen Ringelement $t \in R$, denn

$$t(r_1 a_1 + \dots + r_n a_n) = (tr_1) a_1 + \dots + (tr_n) a_n.$$

Somit ist $(a_1, \dots, a_n)$ tatsächlich ein Ideal.

Es bleibt zu zeigen, dass $(a_1, \dots, a_n)$ das kleinste Ideal ist, das die Elemente $a_1, \dots, a_n$ enthält. Zunächst ist klar, dass $(a_1, \dots, a_n)$ die Elemente $a_1, \dots, a_n$ enthält, denn für jedes i gilt

$$a_i = 0 \cdot a_1 + \dots + 1 \cdot a_i + \dots + 0 \cdot a_n,$$

wobei alle Terme außer dem i -ten Term verschwinden. Sei jetzt $I \subseteq R$ ein Ideal mit $a_1, \dots, a_n \in I$. Dann ist zu zeigen, dass auch $(a_1, \dots, a_n) \subseteq I$ gilt, also dass

$$r_1 a_1 + \dots + r_n a_n \in I$$

für alle $r_1, \dots, r_n \in R$. Weil I ein Ideal ist, gilt zunächst $r_i a_i \in I$ für alle i , und da I eine additive Untergruppe ist, liegt auch die angegebene Summe in I . $\square$

4.3.8 Bemerkung. (a) Für ein einzelnes Element $a \in R$ ist also insbesondere die Menge der Vielfachen von a , also

$$(a) := \{ar \mid r \in R\}$$

ein Ideal von R . Ein Ideal von dieser Form heißt **Hauptideal**, und wir schreiben manchmal auch aR statt (a) .

(b) Ein Ideal $I \subseteq R$ heißt **echtes Ideal**, wenn $I \neq R$ gilt. Dies gilt genau dann, wenn $1 \notin I$ gilt. Denn falls $1 \in I$, dann folgt für alle $r \in R$, dass auch

$$r = r \cdot 1 \in I,$$

also $I = R$.

(c) Der ganze Ring R selbst ist das einzige Ideal von R , welches gleichzeitig ein Unterring ist. Denn falls ein Ideal $I \subseteq R$ auch ein Unterring ist, dann muss $1 \in I$ gelten, und damit $I = R$.

4.3.9 Beispiel. (a) Für jedes $n \in \mathbb{N}$ ist

$$(n) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$$

ein Hauptideal von $\mathbb{Z}$. Weitere Ideale in $\mathbb{Z}$ gibt es keine: jedes Ideal von $\mathbb{Z}$ ist insbesondere eine additive Untergruppe von $\mathbb{Z}$, und die einzigen additiven Untergruppen von $\mathbb{Z}$ sind gerade die $n\mathbb{Z}$ für $n \in \mathbb{N}$. Dies haben wir im Beweis von Lemma 2.6.12 bereits gesehen. In der Terminologie von Abschnitt 4.7 bedeutet das, dass $\mathbb{Z}$ ein **Hauptidealring** ist.

(b) Auch in $K[X]$ für einen Körper K sind alle Ideale Hauptideale: jedes Ideal hat die Form (f) für ein Polynom f . Dies werden wir in Abschnitt 4.7 zeigen.

Als konkretes Beispiel betrachten wir das Ideal

$$(X^2 - 1, X^2 + X) \subseteq \mathbb{Q}[X].$$

Dieses Ideal stimmt mit dem Hauptideal $(X + 1)$ überein: einerseits gilt

$$X + 1 = (X^2 + X) - (X^2 - 1),$$

und somit $(X + 1) \subseteq (X^2 - 1, X^2 + X)$; andererseits sind sowohl $X^2 - 1$ als auch $X^2 + X$ Vielfache von $X + 1$, also folgt auch $(X^2 - 1, X^2 + X) \subseteq (X + 1)$.

Weiteres Beispiel: für jeden Körper K und $a \in K$ ist der Kern der Auswertungsabbildung (4.9) ein Ideal in $K[X]$. Dieses Ideal ist genau das Hauptideal

$$(X - a)$$

aus folgendem Grund: zunächst ist das Hauptideal im Kern enthalten, denn die Auswertung von $X - a$ an der Stelle a ergibt tatsächlich $a - a = 0$. Andererseits sei $f \in K[X]$ ein Polynom mit $f(a) = 0$. Dann können wir mittels Polynomdivision einen Faktor $X - a$ aus f abspalten, das Polynom also in der Form

$$f = (X - a)g \tag{4.11}$$

für ein Polynom $g \in K[X]$ schreiben. Daher gilt $f \in (X - a)$.

(c) Sei R ein kommutativer Ring und $a \in R$. Dann ist der **Annihilator**

$$\text{Ann}(a) := \{r \in R \mid ra = 0\}$$

ein Ideal von R , wie man leicht nachrechnet.

Zum Beispiel ist im Ring $C(X, \mathbb{R})$ aus Beispiel 4.1.10 der Annihilator eines Elements $f \in C(X, \mathbb{R})$ gegeben durch

$$\begin{aligned} \text{Ann}(f) &= \{g \in C(X, \mathbb{R}) \mid g(x)f(x) = 0 \ \forall x \in X\} \\ &= \{g \in C(X, \mathbb{R}) \mid g(x) = 0 \ \forall x \in X \text{ mit } f(x) \neq 0\}. \end{aligned}$$

Sei zum Beispiel $f \in C(\mathbb{R}, \mathbb{R})$ eine Funktion, die auf $[0, \infty)$ verschwindet aber auf $(-\infty, 0)$ nicht. Dann besteht $\text{Ann}(f)$ genau aus den Funktionen, die auf $(-\infty, 0)$ verschwinden, und wegen der Stetigkeit sogar auf $(-\infty, 0]$.

4.3.10 Warnung. Insbesondere in einem Polynomring $K[X]$ muss man mit der Notation aufpassen: wenn wir ähnlich zu (4.11)

$$g(X - a)$$

schreiben, dann kann dies zwei ganz unterschiedliche Dinge bedeuten: zum einen könnte damit die Multiplikation von dem Polynom g mit dem Polynom $X - a$ gemeint sein, also die Multiplikation in $K[X]$, zum anderen könnte damit das Einsetzen von $X - a$ in das Polynom g gemeint sein.

Bei der Bildung einer Quotientengruppe bildet man Restklassen einer Gruppe bezüglich einer normalen Untergruppe. Analog gibt es einen Begriff von **Restklassenring**, bei dem die Restklassen bezüglich eines Ideals gebildet werden.²⁷

4.3.11 Definition (Kongruenz modulo Ideal). *Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Zwei Elemente $x, y \in R$ sind **kongruent modulo I** , geschrieben*

$$x \equiv y \pmod{I},$$

falls $x - y \in I$.

4.3.12 Lemma. *Kongruenz modulo I ist eine Äquivalenzrelation auf R .*

Beweis. Dies ist bereits aus der Gruppentheorie bekannt, denn unsere Definition von Kongruenz modulo I ist genau die Definition von Kongruenz modulo einer additiven Untergruppe von R (die deswegen automatisch normal ist, weil die additive Gruppe von R abelsch ist). Siehe insbesondere Lemma 2.2.26, wo die Zerlegung in Äquivalenzklassen behandelt wurde. $\square$

Wir bezeichnen die Äquivalenzklasse von $x \in R$ bezüglich der Kongruenz modulo I mit $x + I$, denn die Elemente der Äquivalenzklasse von x sind genau die Elemente der Form $x + i$ mit $i \in I$. Die Menge der Äquivalenzklassen bezüglich der Kongruenz modulo I bezeichnen wir mit R/I .

4.3.13 Definition. *Sei $I \subseteq R$ ein Ideal in einem kommutativen Ring. Auf der Menge der Restklassen R/I definieren wir*

$$(x + I) + (y + I) := (x + y) + I, \quad (x + I) \cdot (y + I) := xy + I. \quad (4.12)$$

4.3.14 Lemma. *Die Verknüpfungen (4.12) sind wohldefiniert, und mit diesen Verknüpfungen ist R/I ein kommutativer Ring.*

Wir nennen R/I den **Restklassenring** von R bezüglich I .

Beweis. Wir beschränken uns auf die Wohldefiniertheit der Multiplikation und auf das Nachrechnen des Distributivgesetzes; der Rest ist ähnlich und ohnehin analog zur Konstruktion von Quotientengruppen (Satz 2.2.31).

Seien also $x, x' \in R$ und $y, y' \in R$ Elemente, die die gleichen Restklassen modulo I repräsentieren, also

$$x + I = x' + I \quad \text{und} \quad y + I = y' + I.$$

Dann gilt auch

$$xy + I = xy' + I = x'y' + I,$$

wobei die erste Gleichung aus der Tatsache folgt, dass $y - y' \in I$ und damit $x(y - y') \in I$ gilt, und analog für die zweite Gleichung. Alternative Schreibweise für das gleiche Argument: $x \equiv x' \pmod{I}$ und $y \equiv y' \pmod{I}$ implizieren $xy \equiv x'y' \pmod{I}$, weil aus $x - x' \in I$ und $y - y' \in I$ folgt, dass auch

$$xy - x'y' = (x - x')y + x'(y - y') \in I$$

gilt. Somit ist die Multiplikation wohldefiniert.

Das Distributivgesetz in R/I folgt aus der Tatsache, dass es in R gilt, denn wir addieren und multiplizieren die Repräsentanten der Restklassen, und für diese gilt das Distributivgesetz. Formal ausgeschrieben: für alle $x, y, z \in R$ gilt

$$\begin{aligned} (x + I) \cdot ((y + I) + (z + I)) &= (x + I) \cdot ((y + z) + I) \\ &= x(y + z) + I \\ &= (xy + xz) + I \\ &= xy + I + xz + I \\ &= (x + I) \cdot (y + I) + (x + I) \cdot (z + I). \end{aligned} \quad \square$$

²⁷Wir vermeiden hier die Bezeichnung "Quotientenring", weil dies zu Verwechslungen mit dem Begriff von Quotientenkörper führen könnte, den wir in Definition 5.1.5 einführen. Der Begriff "Restklassenring" ist direkt an die Bildung von Restklassen ganzer Zahlen angelehnt.

4.3.15 Beispiel. Für $n \in \mathbb{N}$ ist

$$\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$$

der Ring der Restklassen modulo n . Als additive Gruppe entspricht dies genau der Gruppe $\mathbb{Z}/n\mathbb{Z}$ aus Satz 2.2.31, aber jetzt haben wir zusätzlich die Multiplikation von Restklassen. Da wir sowohl die additive Gruppe als auch den Ring mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnen, muss man dem Kontext entnehmen, ob die Gruppe oder der Ring gemeint ist.

Wir könnten jetzt noch viele weitere Beispiele von Restklassenringen anführen. Interessant wird dies aber erst dann, wenn wir diese Ringe mit anderen bekannten Ringen in Beziehung setzen können. Damit dies möglich ist, müssen wir verstehen, wie man Homomorphismen von einem Restklassenring R/I in einen anderen Ring S konstruieren kann.

4.3.16 Lemma. Sei $I \subseteq R$ ein Ideal und S ein weiterer kommutativer Ring. Jeder Ringhomomorphismus $\varphi : R \rightarrow S$ mit $I \subseteq \ker(\varphi)$ faktorisiert eindeutig über den Restklassenring R/I , das heißt, es existiert genau ein Ringhomomorphismus $\bar{\varphi} : R/I \rightarrow S$, so dass das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{x \mapsto x+I} & R/I \\ & \searrow \varphi & \swarrow \bar{\varphi} \\ & S & \end{array}$$

kommutiert.

Der folgende Beweis erinnert an die Konstruktion von $\tilde{f}$ im mengentheoretischen Isomorphiesatz (Satz 2.3.1).

Beweis. Die Kommutativität des Diagramms bedeutet, dass für alle $x \in R$ die Gleichung

$$\bar{\varphi}(x + I) = \varphi(x) \quad (4.13)$$

gelten soll. Damit ist bereits die Eindeutigkeit von $\bar{\varphi}$ gezeigt, denn jedes Element von R/I ist von der Form $x + I$ für ein $x \in R$. Für die Existenz von $\bar{\varphi}$ müssen wir zeigen, dass (4.13) als Definition von $\bar{\varphi}$ tatsächlich einen wohldefinierten Ringhomomorphismus ergibt. Die Wohldefiniertheit von (4.13) bedeutet, dass falls $x + I = y + I$ für $x, y \in R$ gilt, dann auch $\varphi(x) = \varphi(y)$ gelten muss. Dies ist aber tatsächlich der Fall, denn $x + I = y + I$ bedeutet $x - y \in I$, und da $I \subseteq \ker(\varphi)$ gilt, folgt $\varphi(x - y) = 0$, also $\varphi(x) = \varphi(y)$.

Für die Homomorphismeigenschaft von $\bar{\varphi}$ sei $x, y \in R$ gegeben. Dann gilt

$$\begin{aligned} \bar{\varphi}((x + I)(y + I)) &= \bar{\varphi}(xy + I) \\ &= \varphi(xy) \\ &= \varphi(x)\varphi(y) \\ &= \bar{\varphi}(x + I) \cdot \bar{\varphi}(y + I). \end{aligned}$$

Analog zeigt man auch die Additivität von $\bar{\varphi}$. Schließlich ist $\bar{\varphi}(1_{R/I}) = 1_S$ klar, denn $1_{R/I} = 1_R + I$ und $\varphi(1_R) = 1_S$. $\square$

Ausgestattet mit der Konstruktion von Restklassenringen können wir nun den ersten Isomorphiesatz für Ringe formulieren, welcher analog zum ersten Isomorphiesatz für Gruppen (Satz 2.3.3) die Beziehung zwischen einem Ringhomomorphismus, seinem Kern und seinem Bild beschreibt.

4.3.17 Satz (Erster Isomorphiesatz für Ringe). Sei $\varphi : R \rightarrow S$ ein Ringhomomorphismus. Dann gibt es einen eindeutigen Ringisomorphismus $\tilde{\varphi} : R/\ker(\varphi) \rightarrow \text{im}(\varphi)$ so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & \searrow & \swarrow \\ R/\ker(\varphi) & \xrightarrow{\tilde{\varphi}} & \text{im}(\varphi) \end{array} \quad (4.14)$$

Insbesondere gilt also

$$\boxed{R/\ker(\varphi) \cong \text{im}(\varphi)}.$$

Der Beweis ist praktisch der gleiche wie in Satz 2.3.3 für Gruppen, indem man die Aussage auf den mengentheoretischen Fall von Satz 2.3.1 zurückführt, oder indem man direkt Lemma 4.3.16 anwendet. Wir lassen die Details daher hier weg; wichtiger als der Beweis ist sowieso die routinemäßige Anwendung des Isomorphiesatzes. Wir werden ihn im Folgenden immer wieder verwenden, wenn wir das Bild eines Homomorphismus mit den Restklassen bezüglich des Kerns identifizieren.

Wir können jetzt weitere Beispiele von Restklassenringen betrachten.

4.3.18 Beispiel. (a) Der Ring $\mathbb{R}[X]/(X^2 + 1)$ ist isomorph zum Körper der komplexen Zahlen $\mathbb{C}$ via

$$\begin{aligned} \mathbb{R}[X]/(X^2 + 1) &\longrightarrow \mathbb{C}, \\ f + (X^2 + 1) &\longmapsto f(i). \end{aligned} \quad (4.15)$$

Formal erhält man diesen Ringhomomorphismus, indem man zunächst den Auswertungshomomorphismus

$$\begin{aligned} \mathbb{R}[X] &\longrightarrow \mathbb{C}, \\ f &\longmapsto f(i) \end{aligned}$$

betrachtet und dann die Faktorisierung über den Restklassenring $\mathbb{R}[X]/(X^2 + 1)$ mittels Lemma 4.3.16. Da $X^2 + 1$ im Kern der Auswertungsabbildung liegt, ist die Voraussetzung dafür erfüllt.²⁸ Da sich jedes Element von $\mathbb{C}$ als Polynom in i mit Koeffizienten in $\mathbb{R}$ schreiben lässt, sind die beiden Homomorphismen surjektiv. Es bleibt also nur noch zu zeigen, dass der Kern der Auswertungsabbildung das Ideal $(X^2 + 1)$ nicht nur enthält, sondern damit übereinstimmt; dann folgt die Behauptung durch den ersten Isomorphiesatz. Mit anderen Worten: falls $f(i) = 0$ für ein Polynom $f \in \mathbb{R}[X]$ gilt, dann muss bereits f ein Vielfaches von $X^2 + 1$ sein. Dies sieht man am leichtesten durch Polynomdivision,

$$f = (X^2 + 1)g + r,$$

wobei $g, r \in \mathbb{R}[X]$ und $\deg(r) < 2$. Wegen $f(i) = 0$ gilt dann $r(i) = 0$, und da r höchstens Grad 1 hat, muss $r = 0$ sein, also f ein Vielfaches von $X^2 + 1$.

Informell ist der Isomorphismus (4.15) leicht zu verstehen: wenn wir anstatt X einfach i schreiben, dann sind die Elemente von $\mathbb{C}$ ja genau Äquivalenzklassen von Polynomen in i mit Koeffizienten in $\mathbb{R}$, wobei die Äquivalenzrelation durch Umformen mittels der Ringaxiome und $i^2 + 1 = 0$ definiert ist. Dieses Bilden der Äquivalenzklassen entspricht genau dem Bilden von Restklassen bezüglich des Ideals $(X^2 + 1)$ in $\mathbb{R}[X]$.

(b) Sei $\mathbb{Q}[\sqrt{2}]$ der kleinste Teilring von $\mathbb{C}$, der $\mathbb{Q}$ und $\sqrt{2}$ enthält. Wir zeigen, dass dieser Ring isomorph zu

$$\mathbb{Q}[X]/(X^2 - 2)$$

ist, wobei der Isomorphismus durch

$$\begin{aligned} \mathbb{Q}[X]/(X^2 - 2) &\longrightarrow \mathbb{Q}[\sqrt{2}], \\ f + (X^2 - 2) &\longmapsto f(\sqrt{2}). \end{aligned} \quad (4.16)$$

gegeben ist. Diesen Homomorphismus erhält man durch Anwendung von Lemma 4.3.16 auf den Auswertungshomomorphismus

$$\begin{aligned} \mathbb{Q}[X] &\longrightarrow \mathbb{Q}[\sqrt{2}] \\ f &\longmapsto f(\sqrt{2}). \end{aligned} \quad (4.17)$$

²⁸Weil der Kern ein Ideal ist, und $(X^2 + 1)$ das kleinste Ideal ist, welches $X^2 + 1$ enthält, liegt automatisch auch das ganze Ideal $(X^2 + 1)$ im Kern.

Beide Homomorphismen sind surjektiv, weil jedes Element von $\mathbb{Q}[\sqrt{2}]$ als Polynom in $\sqrt{2}$ mit Koeffizienten in $\mathbb{Q}$ geschrieben werden kann. Wenn wir jetzt zeigen, dass der Kern von (4.17) nicht nur das Ideal $(X^2 - 2)$ enthält, sondern mit ihm übereinstimmt, dann folgt die Behauptung durch den ersten Isomorphiesatz. Dazu verwenden wir erneut Polynomdivision: sei $f \in \mathbb{Q}[X]$ mit $f(\sqrt{2}) = 0$ gegeben. Dann können wir f in der Form

$$f = (X^2 - 2)g + r$$

schreiben, wobei $g, r \in \mathbb{Q}[X]$ und $\deg(r) < 2$ gilt. Also ist r von der Form $aX + b$ für $a, b \in \mathbb{Q}$, und $r(\sqrt{2}) = 0$ impliziert $a\sqrt{2} + b = 0$. Da $\sqrt{2}$ irrational ist, muss $a = b = 0$ gelten, also $r = 0$, und damit ist f ein Vielfaches von $X^2 - 2$.

- (c) Sei $d \in \mathbb{N}_{>0}$. Dann kann der Ring $\mathbb{R}[X]/(X^d)$ als Ring der Taylorpolynome bis zum Grad $d - 1$ aufgefasst werden. Denn jedes Polynom $f \in \mathbb{R}[X]$ ist modulo (X^d) kongruent zu einem Polynom vom Grad höchstens $d - 1$, nämlich dem Polynom, welches man durch Vernachlässigen aller Terme vom Grad d oder höher erhält. Dies ist genau das Taylorpolynom von f bis zum Grad $d - 1$ um die Stelle 0. Somit hat jedes Element von $\mathbb{R}[X]/(X^d)$ einen eindeutigen Repräsentanten der Form

$$a_0 + a_1X + \cdots + a_{d-1}X^{d-1} \quad \text{mit } a_0, \dots, a_{d-1} \in \mathbb{R}.$$

Zwei solche Polynome werden komponentenweise addiert. Zur Multiplikation verwendet man erst die normale Multiplikation von Polynomen und wirft dann alle Terme vom Grad d oder höher weg.

Informell kann man sich die Variable X als eine so kleine Zahl vorstellen, dass ihre d -te Potenz X^d vernachlässigbar ist, niedrigere Potenzen von X aber nicht. Mit dieser Interpretation schreibt man auch oft ε anstatt X . Den Ring $\mathbb{R}[\varepsilon]/(\varepsilon^2)$ nennt man auch den **Ring der dualen Zahlen**. Man rechnet hier also mit einer neuen "Zahl" ε , die als "so klein" angenommen ist, dass bereits $\varepsilon^2 = 0$ gilt (obwohl $\varepsilon \neq 0$).

Um die Nützlichkeit von Restklassenringen an sich zu illustrieren, betrachten wir zwei Anwendungen in der Zahlentheorie.

4.3.19 Lemma. *Die folgenden Gleichungen haben keine ganzzahligen Lösungen:*

$$(a) \quad x^2 = y^2 + 2.$$

$$(b) \quad x^3 + y^3 + z^3 = 4.$$

Die erste Gleichung gilt dann, wenn sich zwei Quadratzahlen um genau 2 unterscheiden. Dass es keine solchen Quadratzahlen gibt, sieht man auch leicht direkt. Deshalb dient uns die zweite Gleichung als schwierigeres Beispiel, bei dem die Nichtexistenz von ganzzahligen Lösungen alles andere als offensichtlich ist. Durch die Betrachtung eines geeigneten Restklassenrings und etwas Gruppentheorie können wir aber auch die zweite Gleichung als unlösbar nachweisen:

Beweis. (a) Sei $x, y \in \mathbb{Z}$ eine ganzzahlige Lösung der Gleichung $x^2 = y^2 + 2$. Dann gilt für deren Bilder unter dem kanonischen Homomorphismus $[\cdot] : \mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$, dass

$$[x]^2 = [y^2 + 2] = [y]^2 + [2],$$

wobei wir in der zweiten Gleichung die Homomorphismeigenschaft verwenden. In $\mathbb{Z}/4\mathbb{Z}$ gibt es nur die vier Elemente $[0], [1], [2], [3]$, und deren Quadrate sind

$$[0]^2 = [0], \quad [1]^2 = [1], \quad [2]^2 = [0], \quad [3]^2 = [1].$$

Die einzigen Quadrate in $\mathbb{Z}/4\mathbb{Z}$ sind also $[0]$ und $[1]$, und $[2]$ lässt sich nicht als Differenz von zwei Quadraten darstellen.

- (b) Sei $x, y, z \in \mathbb{Z}$ eine ganzzahlige Lösung der Gleichung $x^3 + y^3 + z^3 = 4$. Dann gilt für die Bilder modulo 9 ebenfalls aufgrund der Homomorphismeigenschaft von $[\cdot] : \mathbb{Z} \rightarrow \mathbb{Z}/9\mathbb{Z}$, dass

$$[x]^3 + [y]^3 + [z]^3 = [4]. \quad (4.18)$$

Falls wir zeigen, dass diese Gleichung keine Lösungen in $\mathbb{Z}/9\mathbb{Z}$ hat, dann kann es also auch keine ganzzahligen Lösungen geben. Um dies zu zeigen, bestimmen wir zunächst die dritten Potenzen in $\mathbb{Z}/9\mathbb{Z}$,

$$\begin{array}{lllll} [0]^3 = [0], & [1]^3 = [1], & [2]^3 = [8], & [3]^3 = [0], & [4]^3 = [1], \\ [8]^3 = [8], & [7]^3 = [1], & [6]^3 = [0], & [5]^3 = [8]. \end{array}$$

Dabei ist jeder Eintrag in der zweiten Zeile genau das additive Inverse in $\mathbb{Z}/9\mathbb{Z}$ des Eintrags in der ersten Zeile, der Wert folgt also direkt aus $(-a)^3 = -a^3$, was in jedem Ring gilt. Wir stellen somit fest, dass die einzigen dritten Potenzen in $\mathbb{Z}/9\mathbb{Z}$ die Elemente $[0], [1], [-1]$ sind, und $[4]$ lässt sich offensichtlich nicht als Summe von drei solchen Elementen darstellen. $\square$

4.4 Idealarithmetik und Chinesischer Restsatz

Es gibt verschiedene Arten, wie man aus gegebenen Idealen neue machen kann.

4.4.1 Lemma. Sei R ein kommutativer Ring und $I, J \subseteq R$ Ideale.

- (a) Der **Durchschnitt**

$$I \cap J$$

ist das größte Ideal, welches in I und J enthalten ist.

- (b) Die **Summe**

$$I + J := \{a + b \mid a \in I, b \in J\}$$

ist das kleinste Ideal, welches I und J enthält.

- (c) Das **Idealprodukt**

$$IJ := \left\{ \sum_{\ell=1}^n a_\ell b_\ell \mid n \in \mathbb{N}, a_\ell \in I, b_\ell \in J \right\}$$

ist ein Ideal.

Außerdem gelten

$$IJ \subseteq I \cap J \subseteq I + J. \quad (4.19)$$

Das Idealprodukt besteht in Worten ausgedrückt also aus allen endlichen Summen von Produkten aus einem Element von I und einem Element von J .

Beweis. (a) Falls $x, y \in I \cap J$, dann folgt auch $x + y \in I \cap J$, weil sowohl I als auch J abgeschlossen unter Addition sind. Für $r \in R$ folgt analog $rx \in I \cap J$. Also ist $I \cap J$ tatsächlich ein Ideal. Es ist klar, dass $I \cap J$ die größte Teilmenge von R ist, die sowohl in I als auch in J enthalten ist. Damit ist es auch automatisch das größte Ideal mit dieser Eigenschaft.

- (b) Falls

$$x_1 + y_1 \in I + J, \quad x_2 + y_2 \in I + J$$

mit $x_\ell \in I$ und $y_\ell \in J$, dann gilt auch $x_1 + x_2 \in I$ und $y_1 + y_2 \in J$, also

$$(x_1 + y_1) + (x_2 + y_2) \in I + J,$$

und somit ist $I + J$ abgeschlossen unter Addition. Falls außerdem $r \in R$, dann folgt auch

$$r(x_1 + y_1) = rx_1 + ry_1 \in I + J$$

wegen $rx_1 \in I$ und $ry_1 \in J$.

Es gilt $I \subseteq I + J$ weil $x + 0 \in I + J$ für alle $x \in I$, und analog $J \subseteq I + J$. Falls andererseits $K \subseteq R$ ein Ideal ist mit $I \subseteq K$ und $J \subseteq K$, dann gilt auch $I + J \subseteq K$, weil K abgeschlossen unter Addition ist.

- (c) Die Menge IJ ist per Definition abgeschlossen unter Summen. Sie ist abgeschlossen unter Multiplikation mit einem beliebigen $r \in R$, weil dies bereits für I gilt, und insbesondere $ra_\ell \in I$ in

$$r \cdot \sum_{\ell=1}^n a_\ell b_\ell = \sum_{\ell=1}^n (ra_\ell) b_\ell.$$

Bezüglich (4.19) ist die Inklusion $I \cap J \subseteq I + J$ klar, weil ja $I \cap J \subseteq I \subseteq I + J$. Für die Inklusion $IJ \subseteq I \cap J$ zeigen wir, dass jedes Element $\sum_{\ell=1}^n a_\ell b_\ell$ von IJ auch zu $I \cap J$ gehört. Zunächst gehört jedes Produkt $a_\ell b_\ell$ zu I , weil $a_\ell \in I$ und I abgeschlossen unter Multiplikation mit beliebigen Ringelementen ist, also insbesondere mit b_ℓ . Analog folgt, dass es zu J gehört, also sogar $a_\ell b_\ell \in I \cap J$. Weil $I \cap J$ als Ideal abgeschlossen unter Summen ist, folgt $\sum_{\ell=1}^n a_\ell b_\ell \in I \cap J$. $\square$

4.4.2 Bemerkung. (a) Die Menge der Ideale eines kommutativen Rings bildet eine teilgeordnete Menge bezüglich der Inklusion von Idealen, und wir bezeichnen sie mit

$$\text{Id}(R) := \{I \subseteq R \mid I \text{ ist ein Ideal}\}.$$

Durch die in Lemma 4.4.1 angegebenen Eigenschaften von Durchschnitt und Summe werden diese beiden zu binären Infima bzw. Suprema in $\text{Id}(R)$ (im Sinne von Abschnitt 3.3).

- (b) Die Inklusion $IJ \subseteq I \cap J$ mag kontraintuitiv erscheinen, weil man sich zunächst vielleicht ein Produkt IJ als “größer” als einen Durchschnitt vorstellt. Diese Intuition ist für das Idealprodukt aber komplett falsch. Dies ist eng verwandt damit, dass Teilbarkeit die Inklusion von Hauptidealen umkehrt: für $a = bc$ in R , also falls b ein Teiler von a ist, dann gilt offensichtlich

$$(a) \subseteq (b).$$

Zum Beispiel in $\mathbb{Z}$ ist $2 \mid 6$, aber $(6) \subseteq (2)$.

4.4.3 Beispiel. Für $n, m \in \mathbb{N}$ gelten in $\mathbb{Z}$ die Formeln

$$(n) \cap (m) = (\text{kgV}(n, m)), \quad (n) + (m) = (\text{ggT}(n, m)), \quad (n)(m) = (nm). \quad (4.20)$$

Insbesondere gilt für teilerfremde n, m ,

$$(n) \cap (m) = (nm) = (n)(m).$$

Jetzt zum Beweis der Formeln. Tatsächlich besteht $(n) \cap (m)$ genau aus den ganzen Zahlen, die sowohl durch n als auch durch m teilbar sind, also genau aus den Vielfachen von $\text{kgV}(n, m)$. Dagegen ist

$$(n) + (m) = \{an + bm \mid a, b \in \mathbb{Z}\},$$

und dies sind bekanntermaßen genau die Vielfachen von $\text{ggT}(n, m)$. Insbesondere ergibt sich daraus die **Bézout-Identität**: falls n und m teilerfremd sind, dann gibt es ganze Zahlen $a, b \in \mathbb{Z}$, so dass

$$an + bm = 1.$$

Schließlich besteht das Idealprodukt $(n)(m)$ per Definition aus endlichen Summen von Produkten von Vielfachen von n mit Vielfachen von m . Jedes solche Produkt ist ein Vielfaches von nm , und umgekehrt ist jedes Vielfache $k \cdot nm = kn \cdot m$ bereits ein solches Produkt. Also ist $(n)(m)$ genau das Hauptideal (nm) .

In Beispiel 2.6.5 hatten wir für teilerfremde $n, m \in \mathbb{Z}$ einen Isomorphismus von abelschen Gruppen

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

konstruiert. Der bald folgende chinesische Restsatz verallgemeinert diesen auf drei verschiedene Arten:

- ▷ von einem Isomorphismus von abelschen Gruppen auf einen Isomorphismus von Ringen,
- ▷ von zwei teilerfremden Zahlen auf beliebig viele teilerfremde Ideale, und

▷ von $\mathbb{Z}$ auf beliebige kommutative Ringe.

Für letztere Verallgemeinerung brauchen wir einen geeigneten Begriff von teilerfremden Idealen:

4.4.4 Definition. Zwei Ideale $I, J \subseteq R$ heißen **teilerfremd**, wenn $I + J = R$ gilt.

Mit anderen Worten: teilerfremd bedeutet, dass es $x \in I$ und $y \in J$ gibt, so dass $x + y = 1$.

4.4.5 Beispiel. In $\mathbb{Z}$ sind die Ideale (n) und (m) nach (4.20) genau dann teilerfremd, wenn n und m teilerfremd sind, also $\text{ggT}(n, m) = 1$ gilt.

Die folgende Aussage charakterisiert dann, was passiert, wenn wir Restklassen bezüglich eines Schnitts von teilerfremden Idealen bilden.

4.4.6 Satz (Chinesischer Restsatz). Sei R ein kommutativer Ring und $I_1, \dots, I_k \subseteq R$ paarweise teilerfremde Ideale. Dann ist die kanonische Abbildung

$$\begin{aligned} \varphi : R &\longrightarrow \prod_{j=1}^k R/I_j, \\ x &\longmapsto (x + I_1, \dots, x + I_k) \end{aligned} \tag{4.21}$$

(a) ein surjektiver Homomorphismus,

(b) hat Kern $\ker(\varphi) = \bigcap_{j=1}^k I_j$, und

(c) induziert einen Ringisomorphismus

$$R / \bigcap_{j=1}^k I_j \cong \prod_{j=1}^k R/I_j.$$

Beweis. Teil (c) folgt aus den anderen beiden Aussagen zusammen mit dem ersten Isomorphiesatz (Satz 4.3.17). Weiters ist Teil (b) klar, da $x \in \ker(\varphi)$ genau dann gilt, wenn $x \bmod I_j = 0$ für alle j , also $x \in I_j$ für alle j gilt. Es bleibt also nur die Surjektivität von φ zu zeigen.

Wir zeigen dann zunächst

$$I_1 + \prod_{j=2}^k I_j = R.$$

Nach Voraussetzung gibt es $x_j \in I_1$ und $y_j \in I_j$ mit $x_j + y_j = 1$ für alle $j \geq 2$. Also auch

$$\prod_{j=2}^k (x_j + y_j) = 1.$$

Ausmultiplizieren der linken Seite ergibt einerseits Terme, in denen mindestens ein Faktor x_j vorkommt, und andererseits den Term $y_2 \cdots y_k \in \prod_{j=2}^k I_j$. Die Terme vom ersten Typ liegen alle in I_1 , da I_1 ein Ideal ist, und somit liegt auch ihre Summe in I_1 . Also gilt in der Tat $1 \in I_1 + \prod_{j=2}^k I_j$, und damit $I_1 + \prod_{j=2}^k I_j = R$.

Allgemeiner gilt für alle ℓ also

$$I_\ell + \prod_{j \neq \ell} I_j = R.$$

Es gibt daher $a_\ell \in I_\ell$ und $b_\ell \in \prod_{j \neq \ell} I_j$ mit $a_\ell + b_\ell = 1$ für alle ℓ . Konkret können solche Elemente a_ℓ und b_ℓ durch die im vorherigen Absatz beschriebene Vorgehensweise gefunden werden. Auf der rechten Seite von (4.21) ist das Element b_ℓ genau 1 in der ℓ -ten Komponente und 0 in allen anderen Komponenten, denn

$$\varphi(b_\ell) = (b_\ell + I_1, \dots, b_\ell + I_k),$$

und es gilt $b_\ell + I_j = I_j$ wegen $b_\ell \in I_j$ für alle $j \neq \ell$, und $b_\ell + I_\ell = 1 - a_\ell + I_\ell = 1 + I_\ell$ wegen $a_\ell \in I_\ell$. Mit anderen Worten, $\varphi(b_\ell)$ ist genau der “Standardbasisvektor” mit 1 in der ℓ -ten Komponente und 0 in allen anderen Komponenten. Durch das Bilden von Linearkombinationen mit Koeffizienten aus R können wir dann jedes Element von $\prod_{j=1}^k R/I_j$ erreichen: für ein beliebiges Element

$$(z_1 + I_1, \dots, z_k + I_k) \in \prod_{j=1}^k R/I_j \quad (4.22)$$

gilt dann

$$\begin{aligned} \varphi\left(\sum_{\ell=1}^k z_\ell b_\ell\right) &= \sum_{\ell=1}^k \varphi(z_\ell) \varphi(b_\ell) = \sum_{\ell=1}^k \varphi(z_\ell) \cdot (0, \dots, 1 + I_\ell, \dots, 0) \\ &= \sum_{\ell=1}^k (0, \dots, z_\ell + I_\ell, \dots, 0) \\ &= (z_1 + I_1, \dots, z_k + I_k). \end{aligned}$$

Daher liegt das Element (4.22) im Bild von φ , und da es beliebig war, ist φ tatsächlich surjektiv. $\square$

4.4.7 Beispiel. Der klassische Fall ist $R = \mathbb{Z}$. In diesem Fall ist der chinesische Restsatz sehr nützlich für das konkrete Rechnen modulo n , insbesondere wenn n viele Primfaktoren hat. Denn mit der Primfaktorzerlegung $n = \prod p_i^{e_i}$ gilt

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_i \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

(a) Für $n = 10$ gilt

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

(b) Zum Beispiel für $n = 60 = 2^2 \cdot 3 \cdot 5$ erhalten wir

$$\mathbb{Z}/60\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Angenommen, wir wollen zum Beispiel $p(-2, 8)$ für ein kompliziertes Polynom $p \in \mathbb{Z}[X, Y]$ berechnen, wir brauchen aber nur den Wert von $p(-2, 8)$ modulo 60.²⁹ Dann können wir stattdessen wie im Beweis von Lemma 4.3.19 direkt mit Restklassen rechnen und $p([-2], [8]) \in \mathbb{Z}/60\mathbb{Z}$ bestimmen. Jetzt folgt die Anwendung des chinesischen Restsatzes:

- ▷ Anstatt der ursprünglichen Zahlen $[-2]$ und $[8]$ in $\mathbb{Z}/60\mathbb{Z}$ betrachten wir die Restklassen modulo 4, 3 und 5, also die Tripel

$$\begin{aligned} ([-2], [-2], [-2]) &= ([2], [1], [3]) \\ ([8], [8], [8]) &= ([0], [2], [3]) \end{aligned} \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

- ▷ Wir berechnen p für jede Komponente dieser Tripel, also $p([2], [0])$ in $\mathbb{Z}/4\mathbb{Z}$ und $p([1], [2])$ in $\mathbb{Z}/3\mathbb{Z}$ und $p([3], [3])$ in $\mathbb{Z}/5\mathbb{Z}$. Dies ist sinnvoll, weil eine Rechnung modulo 60 deutlich aufwändiger ist als drei Rechnungen modulo 4, 3 und 5!
- ▷ Als Ergebnis bekommen wir ein neues Tripel in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Jetzt müssen wir dieses Tripel nur noch zurückübersetzen in eine Restklasse modulo 60. Dies ist dank des chinesischen Restsatzes eindeutig möglich.

Auch für Polynomringe ist der chinesische Restsatz sehr nützlich. Dies wird in den Übungen genauer betrachtet.

²⁹Man denke zum Beispiel an Minuten oder Sekunden, die ja modulo 60 gezählt werden.

4.4.8 Beispiel. Ein Element $e \in R$ mit $e^2 = e$ heißt **idempotent**. Solche Elemente beschreiben Zerlegungen eines Ringes als Produkt, wie man nach dem chinesischen Restsatz folgendermaßen zeigt. Betrachte dazu die Ideale

$$I := (e), \quad J := (1 - e).$$

Dann sind I und J teilerfremd, denn

$$e + (1 - e) = 1.$$

Außerdem gilt sogar $I \cap J = \{0\}$. Ist nämlich $x \in I \cap J$, dann gibt es $a, b \in R$ mit

$$x = ae = b(1 - e),$$

und mit $e^2 = e$ folgt daraus

$$x = ae = ae^2 = b(1 - e)e = 0,$$

so dass in der Tat $I \cap J = \{0\}$. Nach dem chinesischen Restsatz folgt also, dass die Abbildung

$$\begin{aligned} R &\longrightarrow R/(e) \times R/(1 - e) \\ x &\longmapsto (x + (e), x + (1 - e)) \end{aligned}$$

ein Isomorphismus ist. Jedes idempotente Element e liefert also eine Zerlegung von R als Produkt von zwei Ringen, nämlich $R/(e)$ und $R/(1 - e)$.

Ein konkretes Beispiel, bei dem die Produktstruktur nicht schon in der Definition von R sichtbar ist, erhält man für

$$R := K[X]/(X^2 - X)$$

mit einem Körper K . Für die Restklasse

$$e := X + (X^2 - X) \in R$$

gilt

$$e^2 - e = X^2 - X + (X^2 - X) = 0,$$

also ist e idempotent.

Wir betrachten nun die durch Auswertung an 0 bzw. 1 gegebenen Abbildungen

$$\begin{aligned} \text{ev}_0 : R &\longrightarrow K & \text{ev}_1 : R &\longrightarrow K \\ f + (X^2 - X) &\longmapsto f(0), & f + (X^2 - X) &\longmapsto f(1). \end{aligned}$$

Weil beide Abbildungen offensichtlich surjektiv sind und Kern (e) bzw. $(1 - e)$ haben, folgt mit dem ersten Isomorphiesatz

$$R/(e) \cong K, \quad R/(1 - e) \cong K.$$

Zusammen mit der obigen Produktzerlegung ergibt sich also

$$K[X]/(X^2 - X) \cong K \times K.$$

4.4.9 Bemerkung. Der Chinesische Restsatz ist benannt nach dem chinesischen Mathematiker 孫子 (Sūnzǐ / Meister Sun, ca. 5. bis 3. Jahrhundert v.u.Z.), der in seinem mathematischen Handbuch ein Beispiel von Satz 4.4.6 formulierte. Korrekterweise sollten wir also eigentlich von dem *Satz von Sun* sprechen.

4.5 Integritätsringe und Teilbarkeitstheorie

Teilbarkeit von ganzen Zahlen ist ein zentrales Konzept in der Zahlentheorie und kommt auch in vielen Anwendungen der Mathematik vor, zum Beispiel in der Kryptographie.³⁰ In diesem Abschnitt untersuchen wir, ob und inwieweit sich die Teilbarkeitstheorie der ganzen Zahlen auf allgemeine kommutative Ringe übertragen lässt. Wie oft in der Mathematik funktioniert dies unter gewissen zusätzlichen Voraussetzungen besonders gut, und diese Voraussetzungen führen dann zu interessanten Klassen von Ringen.

³⁰Oder in überraschenden Kontexten wie zum Beispiel in der Biologie, wo der 17-jährige Lebenszyklus mancher Zikadenarten möglicherweise dadurch erklärt werden kann, dass 17 als Primzahl besonders gut geeignet ist, um sich vor Fressfeinden zu schützen, die kürzere Lebenszyklen haben.

4.5.1 Definition. Sei R ein kommutativer Ring und $a, b \in R$. Dann heißt a **Teiler** von b , geschrieben $a \mid b$, falls es ein $c \in R$ mit

$$b = ac$$

gibt.

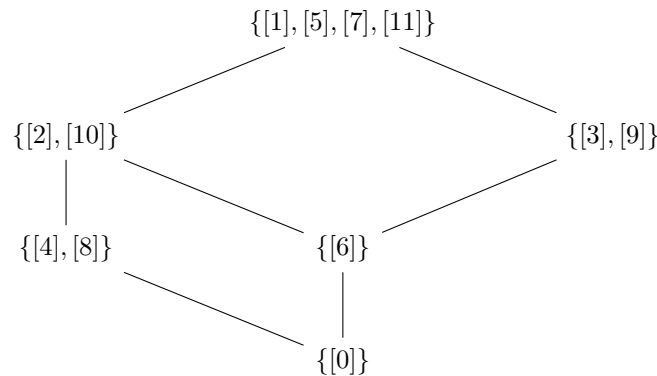
Man sieht leicht, dass Teilbarkeit eine reflexive und transitive Relation auf R ist. Somit handelt es sich um eine Präordnung auf R im Sinne von Definition 3.1.1.

4.5.2 Beispiel. (a) In $\mathbb{Z}$ ist dies genau die bekannte Teilbarkeitsrelation.

(b) In einem Körper ist $a \mid b$ für alle $a \neq 0$ und alle b .

(c) In jedem kommutativen Ring gilt $a \mid 0$ für alle a , weil $0 = a \cdot 0$.

(d) In $\mathbb{Z}/12\mathbb{Z}$ können wir Elemente, die sich gegenseitig teilen, zusammenfassen und die entstehenden Klassen durch *umgekehrte* Teilbarkeit anordnen. Dies ist deshalb sinnvoll, weil gewöhnliche Teilbarkeit der Inklusion von Hauptidealen entgegengesetzt ist (Bemerkung 4.4.2). Dies ergibt das folgende Hassediagramm:



Zum Beispiel liegen $[2]$ und $[10]$ in derselben Klasse, weil sie sich gegenseitig teilen. Die Klasse der Einheiten steht ganz oben, und $[0]$ steht ganz unten, weil jedes Element die Nullklasse teilt.

In der folgenden Klasse von Ringen funktioniert die Teilbarkeitstheorie besonders gut.

4.5.3 Definition. Ein kommutativer Ring R heißt **Integritätsring**, falls $0 \neq 1$ und

$$xy = 0 \implies x = 0 \text{ oder } y = 0 \quad (4.23)$$

in R .

Die Bedingung (4.23) nennt man auch die **Nullteilerfreiheit** von R , denn ein Element $x \neq 0$ mit $xy = 0$ für ein $y \neq 0$ heißt **Nullteiler**.

4.5.4 Beispiel. (a) Falls R ein Integritätsring ist, dann ist auch der Polynomring $R[X]$ ein Integritätsring. Sind nämlich $f, g \in R[X]$ zwei von 0 verschiedene Polynome, dann sind auch ihre Leitkoeffizienten $\neq 0$. Da R keine Nullteiler besitzt, ist auch das Produkt dieser Leitkoeffizienten $\neq 0$. Folglich ist der Koeffizient von $X^{\deg(f)+\deg(g)}$ in fg von 0 verschieden, also $fg \neq 0$. Insbesondere ist $K[X]$ für jeden Körper K ein Integritätsring.

(b) Für $n \in \mathbb{N}_{>0}$ ist $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Integritätsring, wenn n eine Primzahl ist.

Falls n nicht prim ist, so gibt es eine Zerlegung $n = ab$ mit $1 < a, b < n$. Dann sind $[a], [b] \neq [0]$ in $\mathbb{Z}/n\mathbb{Z}$, aber

$$[a][b] = [ab] = [n] = [0],$$

also ist $\mathbb{Z}/n\mathbb{Z}$ kein Integritätsring.

Falls umgekehrt $n = p$ prim ist und

$$[a][b] = [0]$$

in $\mathbb{Z}/p\mathbb{Z}$ gilt, dann bedeutet dies $p \mid ab$. Da p prim ist, folgt daraus $p \mid a$ oder $p \mid b$, also $[a] = [0]$ oder $[b] = [0]$. Somit ist $\mathbb{Z}/p\mathbb{Z}$ ein Integritätsring.

- (c) Falls R und S kommutative Ringe mit $0 \neq 1$ sind, dann ist der Produktring $R \times S$ kein Integritätsring. Denn in $R \times S$ gilt

$$(1, 0) \cdot (0, 1) = (0, 0),$$

obwohl sowohl $(1, 0)$ als auch $(0, 1)$ von $(0, 0)$ verschieden sind.

In jedem Integritätsring kann man in Gleichungen wie gewohnt kürzen, was in allgemeinen Ringen nicht möglich ist:

4.5.5 Lemma. *In jedem Integritätsring gilt für alle $a \in R \setminus \{0\}$,*

$$ax = ay \implies x = y.$$

Beweis. Falls $ax = ay$, dann gilt $a(x - y) = 0$. Da R ein Integritätsring ist, folgt daraus $x - y = 0$, also $x = y$. $\square$

Für Primzahlen $p \in \mathbb{Z}$ sind zwei Eigenschaften charakteristisch. Einerseits lässt sich eine Primzahl p nicht weiter faktorisieren: aus einer Zerlegung $p = ab$ folgt bereits, dass a oder b eine Einheit, also ± 1 , ist. Andererseits gilt das Lemma von Euklid:

$$p \mid xy \implies p \mid x \text{ oder } p \mid y.$$

Diese beiden Eigenschaften lassen sich auf allgemeine Integritätsringe übertragen, führen dort aber zu zwei verschiedenen Begriffen:

4.5.6 Definition. *Sei R ein Integritätsring und $p \in R$ mit $p \neq 0$ und $p \notin R^\times$.*

- (a) *Das Element p heißt **irreduzibel**, falls aus jeder Zerlegung $p = ab$ folgt, dass a oder b eine Einheit ist.*
- (b) *Das Element p heißt **prim**, falls für alle $x, y \in R$ gilt, dass*

$$p \mid xy \implies p \mid x \text{ oder } p \mid y.$$

In $\mathbb{Z}$ stimmen die Begriffe von irreduzibel und prim überein, weil beide Klassen von Elementen genau die Primzahlen sind. Im allgemeinen ist das aber nicht der Fall:

4.5.7 Beispiel. Betrachte den Ring

$$R := \mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}.$$

Dann ist $2 \in R$ irreduzibel, aber nicht prim.

▷ 2 ist nicht prim: Es gilt

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

Also teilt 2 das Produkt $(1 + \sqrt{-5})(1 - \sqrt{-5})$. Andererseits teilt 2 keinen der beiden Faktoren einzeln: aus

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

würde durch Koeffizientenvergleich $1 = 2a$ und $1 = 2b$ folgen, was in $\mathbb{Z}$ unmöglich ist. Analog teilt 2 auch $1 - \sqrt{-5}$ nicht.

- ▷ Um die Irreduzibilität von 2 zu zeigen, betrachten wir die “Norm” $N : R \rightarrow \mathbb{N}$ definiert durch

$$N(a + b\sqrt{-5}) := a^2 + 5b^2 = |a + b\sqrt{-5}|^2.$$

Diese ist multiplikativ, also $N(xy) = N(x)N(y)$, und es gilt $N(2) = 4$. Falls nun $2 = xy$ eine Zerlegung in R ist, dann folgt $4 = N(2) = N(x)N(y)$. Falls weder x noch y eine Einheit ist, dann gilt $N(x), N(y) > 1$, also notwendigerweise $N(x) = N(y) = 2$. Die Gleichung

$$a^2 + 5b^2 = 2$$

hat aber keine ganzzahlige Lösung.³¹ Also muss doch einer der beiden Faktoren eine Einheit sein, und somit ist 2 irreduzibel.

Allgemein gilt aber immerhin eine Implikationsrichtung:

4.5.8 Lemma. *In jedem Integritätsring ist jedes Primelement irreduzibel.*

Beweis. Sei $p \in R$ prim und eine Faktorisierung $p = ab$ gegeben. Dann gilt insbesondere $p \mid ab$. Da p prim ist, folgt also $p \mid a$ oder $p \mid b$. Im ersten Fall gibt es also ein $c \in R$ mit $a = pc$, und dann folgt

$$p = ab = pcb,$$

also nach $p \neq 0$ und Lemma 4.5.5 $cb = 1$, so dass b eine Einheit ist. Im Fall $p \mid b$ folgt analog, dass a eine Einheit ist. Also ist immer a oder b eine Einheit, und somit ist p irreduzibel. $\square$

Es stellt sich daher die Frage, unter welchen zusätzlichen Voraussetzungen an R die Begriffe von irreduzibel und prim zusammenfallen. Dazu kommen wir in den folgenden Abschnitten.

4.5.9 Beispiel. Im nächsten Abschnitt werden wir sehen, dass in $\mathbb{Z}[i]$ die Begriffe von irreduzibel und prim tatsächlich zusammenfallen. Diese Elemente von $\mathbb{Z}[i]$ werden auch **gaußsche Primzahlen** genannt.

- (a) Das Element $3 \in \mathbb{Z}[i]$ ist irreduzibel. Um dies zu sehen, betrachten wir die Norm

$$N(r + si) := |r + si|^2 = r^2 + s^2,$$

die multiplikativ ist. Aus einer Faktorisierung $3 = xy$ folgt dann

$$9 = N(3) = N(x)N(y).$$

Falls $N(x) = 1$, dann ist $x = \pm 1$ oder $x = \pm i$, also eine Einheit. Analog ist y eine Einheit, falls $N(y) = 1$ ist. In beiden Fällen ist also einer der Faktoren eine Einheit. Der übrige dritte Fall ist $N(x) = N(y) = 3$. Dies kann aber gar nicht auftreten, weil es gar kein Element $r + si \in \mathbb{Z}[i]$ mit Norm 3 gibt: die Gleichung

$$r^2 + s^2 = 3$$

hat keine ganzzahlige Lösung. Also muss in jeder Faktorisierung von 3 einer der beiden Faktoren eine Einheit sein, und damit ist 3 irreduzibel.

- (b) Andererseits ist 5 in $\mathbb{Z}[i]$ nicht irreduzibel, denn

$$5 = (2 + i)(2 - i),$$

und weder $2 + i$ noch $2 - i$ ist eine Einheit.³²

4.5.10 Satz. *Für jedes Ideal $I \subseteq R$ in einem kommutativen Ring R sind die folgenden Aussagen äquivalent:*

³¹Falls $b \neq 0$ wäre, dann wäre die linke Seite mindestens 5, also muss $b = 0$ sein. Dann wäre $a^2 = 2$, was bekanntermaßen keine ganzzahlige Lösung hat.

³²Die Einheitengruppe ist $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Es gibt keine anderen invertierbaren Elemente, weil $ab = 1$ impliziert $N(a)N(b) = N(ab) = N(1) = 1$, also $N(a) = N(b) = 1$, und die einzigen Elemente mit Norm 1 sind ± 1 und $\pm i$.

- (a) R/I ist ein Integritätsring.
 (b) Es gilt $I \neq R$, und für alle $x, y \in R$ ist

$$xy \in I \implies x \in I \text{ oder } y \in I. \quad (4.24)$$

Ein Ideal mit der Eigenschaft (b) heißt auch **Primideal**.

Beweis. Nach Definition des Restklassenrings gilt $0_{R/I} = I$ und $1_{R/I} = 1 + I$, also ist $0_{R/I} \neq 1_{R/I}$ äquivalent zu $I \neq R$.

Für $x, y \in R$ gilt nach Definitionen der Multiplikation in R/I , dass

$$(x + I)(y + I) = 0_{R/I} \iff xy \in I,$$

und $x + I = 0_{R/I}$ bzw. $y + I = 0_{R/I}$ ist äquivalent zu $x \in I$ bzw. $y \in I$. Dadurch übersetzt sich die Nullteilerfreiheit in R/I , also die Eigenschaft

$$(x + I)(y + I) = 0_{R/I} \implies x + I = 0_{R/I} \text{ oder } y + I = 0_{R/I},$$

gerade in die Primidealeigenschaft (4.24). $\square$

4.5.11 Lemma. In jedem Integritätsring gilt für Hauptideale:

$$(x) = (y) \iff x \sim y.$$

Beweis. Falls $x \sim y$, gibt es eine Einheit $u \in R^\times$ mit $x = uy$. Daraus folgt $x \in (y)$, also $(x) \subseteq (y)$. Da u invertierbar ist, gilt umgekehrt auch $y = u^{-1}x$, also genauso $(y) \subseteq (x)$, und somit $(x) = (y)$. Diese Richtung gilt insbesondere in jedem kommutativen Ring.

Sei umgekehrt $(x) = (y)$. Aus $x \in (y)$ und $y \in (x)$ folgt, dass es $a, b \in R$ gibt mit

$$x = ay, \quad y = bx.$$

Einsetzen liefert $x = abx$. Falls $x \neq 0$ ist, dann folgt $1 = ab$ nach Lemma 4.5.5, so dass $a, b \in R^\times$ und in der Tat $x \sim y$. Falls andererseits $x = 0$ ist, dann ist auch $y = 0$, und somit trivialerweise $x \sim y$. $\square$

4.6 Euklidische Ringe

Ein Euklidischer Ring ist ein Ring, in dem es Division mit Rest gibt, die auf ähnliche Art und Weise wie in $\mathbb{Z}$ funktioniert. In den folgenden Unterabschnitten werden wir sehen, dass dies viele weitere nützliche Konsequenzen hat, zum Beispiel eine verallgemeinerte Primfaktorzerlegung. Euklidische Ringe sind den ganzen Zahlen $\mathbb{Z}$ in vielen Eigenschaften ähnlich und bilden die kleinste Klasse von Ringen in Abbildung 15.

4.6.1 Definition. Ein Integritätsring R heißt **euklidisch**, falls es eine Abbildung

$$\nu : R \setminus \{0\} \longrightarrow \mathbb{N}$$

gibt mit folgender Eigenschaft: für jedes $x \in R$ und $a \in R \setminus \{0\}$ existieren $q, r \in R$ mit

$$x = qa + r, \quad (4.25)$$

und so dass entweder $r = 0$ oder $\nu(r) < \nu(a)$.

Eine solche Abbildung ν nennen wir **Gradfunktion**. Die Bezeichnung “euklidisch” geht dabei auf den euklidischen Algorithmus zur Berechnung des größten gemeinsamen Teilers von zwei ganzen Zahlen, der auf der Division mit Rest basiert, zurück. Der Begriff von euklidischem Ring axiomatisiert also Division mit Rest, so wie von den ganzen Zahlen bekannt und von Polynomen bekannt ist. Dies führt direkt zu den ersten beiden Beispielen.

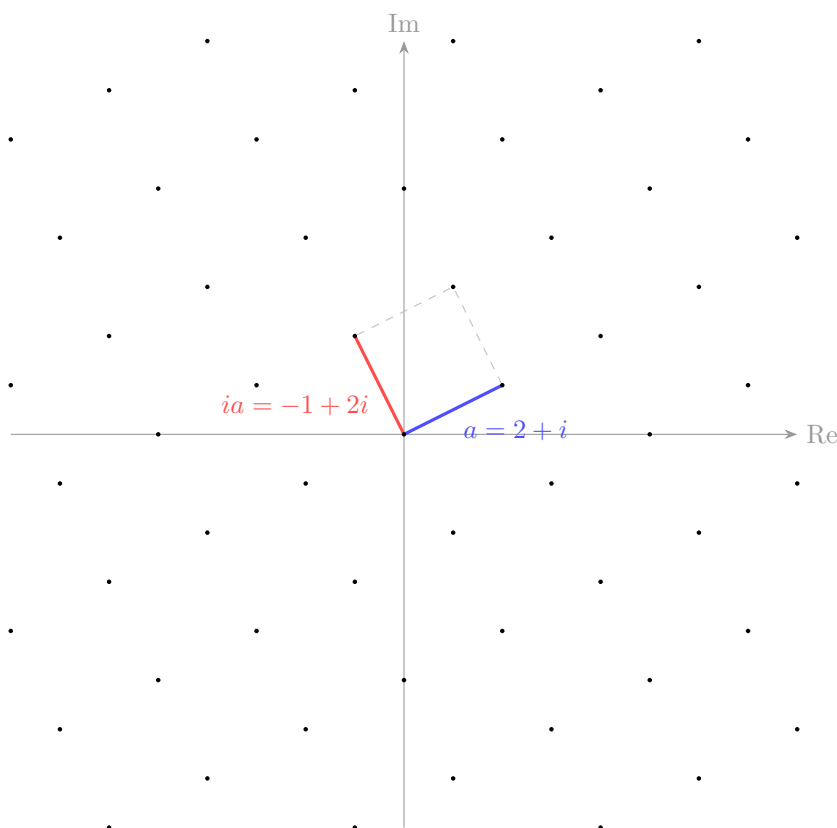


Abbildung 17: Beweis von Satz 4.6.3 mit $a = 2 + i$: die Vielfachen von a bilden ein Gitter.

4.6.2 Beispiel. (a) In $\mathbb{Z}$ ist für jedes $x \in \mathbb{Z}$ Division durch jedes $a \in \mathbb{Z} \setminus \{0\}$ mit Rest möglich, wobei für den Rest

$$0 \leq r < |a|$$

gilt. Mit $\nu(n) := |n|$ ist also die Definition erfüllt.

(b) Für jeden Körper K kann jedes Polynom $f \in K[X]$ durch jedes $a \in K[X] \setminus \{0\}$ mit Rest dividiert werden, wobei für den Rest r gilt, dass entweder $r = 0$ oder $\deg(r) < \deg(a)$ ist. Mit $\nu(f) := \deg(f)$ ist also auch $K[X]$ ein euklidischer Ring.

Das folgende Beispiel ist weniger einfach, und deshalb formulieren wir die Aussage als Satz.

4.6.3 Satz. Die gaußschen Zahlen $\mathbb{Z}[i]$ sind ein euklidischer Ring bezüglich

$$\nu(x) = |x|^2 = x\bar{x}.$$

Beweis. Zu zeigen ist, dass es für jedes $x, a \in \mathbb{Z}[i]$ mit $a \neq 0$ Elemente $q, r \in \mathbb{Z}[i]$ gibt mit

$$x = qa + r$$

und $|r| < |a|$. Dazu stellen wir uns die Menge der Vielfachen qa geometrisch vor. Diese Menge besteht aus a und ia und allen ganzzahligen Linearkombinationen davon, also aus allen Punkten eines Gitters, das durch die Punkte a und ia aufgespannt wird (Abbildung 17). Aufgrund elementarer euklidischer Geometrie ist klar, dass jeder Punkt in der komplexen Ebene höchstens um die halbe Diagonale eines fundamentalen Quadrats (gestrichelt), also $|a|/\sqrt{2}$, von einem Gitterpunkt entfernt ist. Somit kann $|r| \leq |a|/\sqrt{2} < |a|$ erreicht werden. $\square$

4.7 Hauptidealringe

Hier betrachten wir eine weitere etwas breitere Klasse von Ringen. In diesen Ringen gibt es nicht mehr unbedingt einen Begriff von Division mit Rest, aber wir werden sehen, dass diese Ringe immer noch sehr gute Eigenschaften haben, zum Beispiel eine Primfaktorzerlegung.

4.7.1 Definition. Ein Integritätsring R heißt **Hauptidealring**, falls jedes Ideal von einem Element erzeugt ist.

Mit anderen Worten: Hauptidealring bedeutet, dass die Ideale genau die Hauptideale sind, also die Ideale der Form $(a) = aR$ für $a \in R$.

4.7.2 Beispiel. In Beispiel 4.3.9(a) hatten wir bereits gesehen, dass diese Bedingung für $\mathbb{Z}$ erfüllt ist. Da $\mathbb{Z}$ sowieso ein Integritätsring ist, ist $\mathbb{Z}$ also ein Hauptidealring.

Wir beweisen jetzt eine der Inklusionen aus Abbildung 15, die weitere Beispiele von Hauptidealringen liefert.

4.7.3 Satz. Jeder euklidische Ring ist ein Hauptidealring.

Den folgenden Beweis kann man als Verallgemeinerung des Beweises für $\mathbb{Z}$ auffassen, den wir bei (2.32) geführt haben. (Dieser funktioniert deshalb auch ringtheoretisch, weil $\mathbb{Z}$ die besondere Eigenschaft hat, dass jede additive Untergruppe von $\mathbb{Z}$ bereits ein Ideal ist.)

Beweis. Sei R euklidisch und $I \subseteq R$ ein Ideal. Wenn $I = \{0\}$, dann ist I von 0 erzeugt, also Hauptideal. Ansonsten sei $a \in I$ ein Element mit minimalem $\nu(a)$, also $\nu(x) \geq \nu(a)$ für alle $x \in I \setminus \{0\}$. Wir behaupten dann $I = (a)$.

In der Tat ist $(a) \subseteq I$ trivial, denn $a \in I$ und (a) ist das kleinste Ideal, das a enthält. Sei umgekehrt $x \in I$. Dann betrachten wir Division mit Rest wie in Definition 4.6.1: es gibt eine Darstellung

$$x = qa + r$$

mit $q, r \in R$ und entweder $r = 0$ oder $\nu(r) < \nu(a)$. Der zweite Fall kann aber nicht eintreten, denn $r = x - qa \in I$ mit $\nu(r) < \nu(a)$ widerspricht der Minimalität von $\nu(a)$. Also muss $r = 0$ gelten, und damit $x = qa \in (a)$. $\square$

Der Beweis sagt uns sogar, wie wir für ein gegebenes Ideal ein erzeugendes Element finden, nämlich ein beliebiges $a \in I \setminus \{0\}$ mit minimalem $\nu(a)$.

Nach Beispiel 4.6.2 bekommen wir also folgende wichtige Konsequenz:

4.7.4 Korollar. Für jeden Körper K ist der Polynomring $K[X]$ ein Hauptidealring.

4.7.5 Beispiel. Nach Satz 4.6.3 sind auch die gaußschen Zahlen $\mathbb{Z}[i]$ ein Hauptidealring.

Es gibt aber auch Hauptidealringe, die nicht euklidisch sind:

4.7.6 Beispiel. Der Ring

$$\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right]$$

ist ein Hauptidealring, aber kein euklidischer Ring. Der Beweis wird in den Übungen über mehrere Aufgaben verteilt behandelt.

Im Gegensatz zu allgemeinen Integritätsringen haben Hauptidealringe eine besser kontrollierbare Teilbarkeitstheorie. Insbesondere:

4.7.7 Satz. In jedem Hauptidealring ist jedes irreduzible Element prim.

Beweis. Sei R ein Hauptidealring und $p \in R$ irreduzibel. Zu zeigen ist, dass p prim ist, also dass

$$p \mid xy \implies p \mid x \text{ oder } p \mid y \quad \forall x, y \in R.$$

Seien also $x, y \in R$ mit $p \mid xy$ gegeben. Angenommen, es gilt $p \nmid x$. Wir zeigen, dass dann $p \mid y$ der Fall sein muss. Da R ein Hauptidealring ist, gibt es $d \in R$ mit

$$(p, x) = (d). \quad (4.26)$$

Da $p \in (d)$ gilt, folgt $d \mid p$. Weil p irreduzibel ist, muss daher entweder d eine Einheit sein oder $d \sim p$ gelten.

Der zweite Fall ist unmöglich: Aus $d \sim p$ würde wegen $(d) = (p, x)$ auch $x \in (d) = (p)$ folgen, also $p \mid x$, im Widerspruch zur Annahme. Also ist d eine Einheit und damit $(p, x) = (d) = R$. Nach der Beschreibung von erzeugten Idealen (Lemma 4.3.7) gibt es daher $a, b \in R$ mit

$$ap + bx = 1.$$

Multiplikation mit y liefert

$$y = apy + bxy.$$

Da jetzt beide Summanden Vielfache von p sind, folgt wie gewünscht $p \mid y$, und damit ist p prim. $\square$

4.7.8 Beispiel. In $\mathbb{Z}$ gilt nach (4.20),

$$(m, n) = (m) + (n) = (\text{ggT}(m, n)), \quad (m) \cap (n) = (\text{kgV}(m, n)).$$

Die Tatsache, dass $\mathbb{Z}$ ein Hauptidealring ist, spiegelt sich hier darin wider, dass die Summe und der Durchschnitt von Hauptidealen wieder Hauptideale sind.

Man kann zeigen, dass diese Gleichungen sogar in jedem Hauptidealring gelten: Ein erzeugendes Element von $(a) + (b)$ ist ein größter gemeinsamer Teiler von a und b , und ein erzeugendes Element von $(a) \cap (b)$ ist ein kleinstes gemeinsames Vielfaches von a und b . Insbesondere gilt im vorherigen Beweis also $d = \text{ggT}(p, x)$, wodurch das Argument noch anschaulicher wird.

4.8 Faktorielle Ringe und Faktorisierungstheorie

In den ganzen Zahlen ist die Primfaktorzerlegung eines der wichtigsten Werkzeuge überhaupt: Jede ganze Zahl außer 0 und ± 1 lässt sich als Produkt von Primzahlen schreiben, und diese Darstellung ist eindeutig bis auf Reihenfolge und Vorzeichen. Da Vorzeichen genau Einheiten in $\mathbb{Z}$ sind, ist diese Eindeutigkeit also eigentlich eine Eindeutigkeit bis auf Reihenfolge und Assoziiertheit.

Für allgemeine Integritätsringe kann man nicht erwarten, dass sich die Teilbarkeitstheorie immer so gut verhält. So haben wir in Beispiel 4.5.7 bereits gesehen, dass die Begriffe irreduzibel und prim auseinanderfallen können. Trotzdem gibt es viele wichtige Ringe, in denen eine sinnvolle Version der eindeutigen Primfaktorzerlegung gilt. Dies führt zu folgender Definition.

4.8.1 Definition. Ein Integritätsring R heißt **faktoriell**, falls jedes Element von $R \setminus (\{0\} \cup R^\times)$ als Produkt von irreduziblen Elementen dargestellt werden kann und diese Darstellung bis auf Reihenfolge und Assoziiertheit eindeutig ist.

Formal ausbuchstabiert bedeutet dies folgendes für jedes $x \in R$ mit $x \neq 0$ und $x \notin R^\times$:

- (a) Es gibt eine Faktorisierung der Form

$$x = p_1 \cdots p_n, \quad (4.27)$$

wobei die $p_1, \dots, p_n \in R$ irreduzibel sind.

- (b) Falls es eine weitere Faktorisierung in irreduzible Elemente

$$x = q_1 \cdots q_m$$

gibt, dann gilt $m = n$ und es gibt eine Permutation $\sigma \in S_n$ mit

$$p_i \sim q_{\sigma(i)}.$$

4.8.2 Beispiel. $\mathbb{Z}$ ist faktoriell, denn die obigen Bedingungen sind genau die Eigenschaften der Primfaktorzerlegung in $\mathbb{Z}$, mit den Primzahlen als irreduziblen Elementen und $p_i = \pm q_{\sigma(i)}$ als Assoziiertheit. Dass die Eindeutigkeit nur bis auf Permutationen und Assoziiertheit gelten kann, ist unvermeidlich: in $\mathbb{Z}$ unterscheiden sich zum Beispiel die beiden Faktorisierungen

$$6 = 2 \cdot 3 = (-3) \cdot (-2)$$

durch die Reihenfolge der Faktoren und die Vorzeichen, also durch Permutationen und Assoziiertheit.

4.8.3 Bemerkung. Manchmal wird in der Faktorisierung (4.27) auch eine Einheit $u \in R^\times$ vorangestellt, also

$$x = up_1 \cdots p_n. \quad (4.28)$$

Dies macht aber keinen Unterschied, denn u kann man einfach zu einem der Faktoren p_i dazu-rechnen, also $p'_i = up_i$ verwenden, und p'_i ist dann immer noch irreduzibel.³³

Wir werden im Folgenden zeigen, dass alle Hauptidealringe faktoriell sind. Der Beweis besteht aus zwei Teilen. Zuerst braucht man eine Bedingung, die garantiert, dass iteriertes Faktorisieren jedes Elements irgendwann zum Ende kommt. Danach muss man zeigen, dass in Hauptidealringen irreduzible Elemente bereits prim sind, denn genau diese Eigenschaft wird die Eindeutigkeit der Faktorisierung nachweisen lassen. Beginnen wir mit der ersten Bedingung.

4.8.4 Definition. Ein kommutativer Ring R heißt **noethersch**,³⁴ falls jede aufsteigende Folge von Idealen

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

stabilisiert, das heißt, es gibt ein $n \in \mathbb{N}$ mit $I_n = I_{n+1} = I_{n+2} = \dots$.

4.8.5 Beispiel. $\mathbb{Z}$ ist noethersch, denn jede aufsteigende Folge von Idealen in $\mathbb{Z}$ hat die Form

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

für eine Folge von ganzen Zahlen mit

$$\dots \mid a_3 \mid a_2 \mid a_1.$$

Falls $a_n = 0$ für alle n , dann stabilisiert sich die Folge der Ideale trivialerweise. Sonst können wir bereits $a_1 \neq 0$ annehmen, indem wir gegebenenfalls das Nullideal zu Anfang weglassen. Dann gilt $|a_1| \geq |a_2| \geq |a_3| \geq \dots$, so dass sich die Folge der Beträge stabilisieren muss, also ab einem geeigneten n gilt

$$\pm a_n = \pm a_{n+1} = \pm a_{n+2} = \dots$$

Dies impliziert aber $(a_n) = (a_{n+1}) = (a_{n+2}) = \dots$, also stabilisiert sich die Folge der Ideale ab n .

Der Beweis folgender Aussage verallgemeinert dieses Beispiel und ist eine schöne Illustration des Begriffs von noetherschen Ringen.

4.8.6 Lemma. Jeder Hauptidealring ist noethersch.

Beweis. Sei R ein Hauptidealring und $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ eine aufsteigende Folge von Idealen in R . Wir betrachten dann die Menge

$$I_\infty := \bigcup_{n=1}^{\infty} I_n,$$

³³Falls a irreduzibel ist und u eine Einheit, dann ist ua auch irreduzibel, denn aus einer Zerlegung $ua = bc$ folgt $a = u^{-1}bc$, und da a irreduzibel ist, muss $u^{-1}b$ oder c eine Einheit sein, also auch b oder c .

³⁴Benannt nach *Emmy Noether*, die viele grundlegende Erkenntnisse zur Ringtheorie, linearen Algebra und mathematischen Physik beigetragen hat, trotz widriger Bedingungen für Frauen in der Mathematik zu Beginn des 20. Jahrhunderts.

und man sieht leicht, dass I_∞ wieder ein Ideal ist: für $x, y \in I_\infty$ gibt es $n, m \in \mathbb{N}$ mit $x \in I_n$ und $y \in I_m$, also $x + y \in I_{\max(n, m)} \subseteq I_\infty$; für $r \in R$ und $x \in I_\infty$ gibt es ein $n \in \mathbb{N}$ mit $x \in I_n$, also $rx \in I_n \subseteq I_\infty$.

Nach Voraussetzung gibt es ein $a \in R$ mit $I_\infty = (a)$. Da $a \in I_\infty$ liegt, gibt es ein $n \in \mathbb{N}$ mit $a \in I_n$, also $(a) \subseteq I_n$. Dann ist aber $I_\infty = (a) \subseteq I_n \subseteq I_\infty$, also $I_n = I_\infty$, und die Folge stabilisiert sich ab n . $\square$

4.8.7 Satz. Jeder Hauptidealring ist faktoriell.

Nach Satz 4.7.3 ist also auch jeder euklidische Ring faktoriell.

Beweis. Wir zeigen zunächst für jedes Element $a \in R \setminus (\{0\} \cup R^\times)$ die Existenz einer Zerlegung in irreduzible Elemente. Als Hilfsaussage beweisen wir erst, dass jedes solche a von einem irreduziblen Element geteilt wird. Falls $a_1 := a$ selber bereits irreduzibel ist, dann sind wir fertig. Ansonsten können wir das Element zerlegen als

$$a_1 = a_2 c$$

mit $a_2, c \not\sim a_1$. Letzteres impliziert $(a_1) \subsetneq (a_2)$, denn offensichtlich $a_1 \in (a_2)$, aber $(a_1) = (a_2)$ ist nach Lemma 4.5.11 ausgeschlossen. Falls a_2 irreduzibel ist, dann haben wir wie gewünscht einen irreduziblen Teiler gefunden. Sonst finden wir mit dem gleichen Argument einen echten Teiler $a_3 \mid a_2$ mit $(a_2) \subsetneq (a_3)$. Indem wir so fortfahren, erhalten wir eine aufsteigende Folge von Idealen

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

die entweder mit einem irreduziblen Element a_n endet oder unendlich fortgesetzt werden kann. Nach Lemma 4.8.6 ist letzteres aber ausgeschlossen. Also muss es ein n geben, so dass a_n irreduzibel ist. Dank

$$a_n \mid a_{n-1} \mid \dots \mid a_1$$

ist a_n auch ein Teiler des ursprünglichen Elements $a = a_1$, und die Hilfsaussage ist bewiesen.

Sei jetzt $b \in R \setminus (\{0\} \cup R^\times)$ ein beliebiges Element, von dem wir eine Zerlegung in irreduzible Elemente finden wollen. Dann können wir nach der Hilfsaussage ein irreduzibles Element p_1 abspalten, also

$$b = p_1 b_1$$

für ein Element $b_1 \in R \setminus \{0\}$. Falls b_1 eine Einheit ist, dann sind wir fertig. Sonst können wir ein weiteres irreduzibles Element p_2 von b_1 abspalten, also

$$b = p_1 p_2 b_2.$$

Indem wir so fortfahren, erhalten wir eine aufsteigende Folge von Idealen $(b) \subseteq (b_1) \subseteq (b_2) \subseteq \dots$. Jeder Abspaltungsschritt vor dem Erreichen einer Einheit vergrößert das Hauptideal echt: aus $b_j = p_{j+1} b_{j+1}$ folgt $(b_j) \subseteq (b_{j+1})$, und bei Gleichheit wären b_j und b_{j+1} nach Lemma 4.5.11 assoziiert, so dass p_{j+1} eine Einheit wäre. Nach Lemma 4.8.6 muss sich die Folge der Ideale aber stabilisieren. Deshalb muss irgendein b_n bereits eine Einheit sein. Somit erhalten wir eine Faktorisierung der Form (4.28).

Nun zur Eindeutigkeit. Seien also zwei Zerlegungen in Irreduzible gegeben,

$$a = p_1 \cdots p_n = q_1 \cdots q_m.$$

Wir zeigen dann per Induktion, dass die Faktorisierungen bis auf Reihenfolge und Assoziiertheit übereinstimmen müssen:

- ▷ Falls $n = 1$ oder $m = 1$ gilt, sind wir fertig, denn die jeweils andere Seite faktorisiert dann ein irreduzibles Element, was aber nur möglich ist, wenn $n = m = 1$ und die beiden irreduziblen Elemente assoziiert sind.
- ▷ Sonst ist $n, m > 1$. Da p_1 prim ist und $p_1 \mid q_1 \cdots q_m$, teilt p_1 eines der q_j und ist wegen Irreduzibilität dazu assoziiert. Nach Permutieren der q_j sei $p_1 \sim q_1$, und durch Abspalten einer geeigneten Einheit (und deren Absorption in p_2 oder q_2) können wir sogar $p_1 = q_1$ annehmen. Kürzen von p_1 nach Lemma 4.5.5 ergibt eine kürzere Gleichheit der gleichen Art, auf die die Induktionsannahme angewendet werden kann und die Behauptung liefert.

Damit ist die Zerlegung eindeutig bis auf Reihenfolge und Assoziiertheit. $\square$

4.8.8 Beispiel. Insbesondere ist der Polynomring $K[X]$ für jeden Körper K faktoriell, und jedes Polynom hat eine “Primfaktorzerlegung” in irreduzible Polynome, die eindeutig bis auf Reihenfolge und skalare Vielfache ist. Hierzu betrachten wir das Polynom

$$f = X^4 - 4$$

als konkretes Beispiel.

(a) In $\mathbb{C}[X]$ gilt

$$f = (X - \sqrt{2})(X + \sqrt{2})(X - i\sqrt{2})(X + i\sqrt{2}).$$

Dies muss die Primfaktorzerlegung von f in $\mathbb{C}[X]$ sein, denn Polynome vom Grad 1 sind offensichtlich irreduzibel.

(b) In $\mathbb{R}[X]$ gilt

$$f = (X - \sqrt{2})(X + \sqrt{2})(X^2 + 2).$$

Dies ist die Primfaktorzerlegung von f in $\mathbb{R}[X]$, denn auch der dritte Faktor ist irreduzibel: eine nichttriviale Faktorisierung müsste aus zwei Linearfaktoren bestehen, aber $X^2 + 2$ hat keine Nullstelle in $\mathbb{R}$.

(c) In $\mathbb{Q}[X]$ gilt

$$f = (X^2 - 2)(X^2 + 2). \quad (4.29)$$

Dies ist die Primfaktorzerlegung von f in $\mathbb{Q}[X]$, denn nach dem gleichen Argument wie in $\mathbb{R}[X]$ sind jetzt beide Faktoren irreduzibel, da sie keine Nullstellen in $\mathbb{Q}$ haben.

Eine wichtige Einsicht hier ist also, dass die Primfaktorzerlegung eines Polynoms von der Wahl des Grundkörpers abhängt. Durch das Bilden von *Körpererweiterungen* kann man die Primfaktorzerlegung eines Polynoms weiter verfeinern. Dies wird ein wichtiges Thema in Abschnitt 5 sein.

4.8.9 Beispiel. In $\mathbb{Z}[i]$ hat jedes Element eine Faktorisierung in gaußsche Primzahlen, die eindeutig bis auf Reihenfolge und Faktoren $\pm 1, \pm i$ ist. Zum Beispiel

$$5 = (2 + i)(2 - i),$$

wobei $2 + i$ und $2 - i$ beide irreduzibel sind, denn ihre Norm ist 5, also prim in $\mathbb{Z}$.

4.8.10 Beispiel. $\mathbb{Z}[\sqrt{-5}]$ ist kein faktorieller Ring, denn zum Beispiel hat die Zahl 6 zwei verschiedene Faktorisierungen in irreduzible Elemente:

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

Denn die vier Faktoren haben Normen

$$N(2) = 4, \quad N(3) = 9, \quad N(1 + \sqrt{-5}) = 6, \quad N(1 - \sqrt{-5}) = 6,$$

wodurch sich nach dem gleichen Argument wie in Beispiel 4.5.7 deren Irreduzibilität ergibt. Durch die Verschiedenheit der Normen ist auch klar, dass die Faktoren nicht assoziiert sein können, denn assoziierte Elemente haben die gleiche Norm.

4.8.11 Beispiel. Wie in Abbildung 15 dargestellt, gibt es faktorielle Ringe, die *nicht* Hauptidealringe sind, zum Beispiel $\mathbb{Z}[X]$. In diesen Fällen muss man die Faktorialität auf andere Weise als in Satz 4.8.7 beweisen. Wir lassen hier den Beweis, dass $\mathbb{Z}[X]$ faktoriell ist, der Kürze halber aus.³⁵

Wir können aber zumindest zeigen, dass $\mathbb{Z}[X]$ *kein* Hauptidealring ist, indem wir das Ideal

$$I := (X, 2) = \{Xf + 2g : f, g \in \mathbb{Z}[X]\}$$

³⁵Für Interessierte sei erwähnt, dass dies ein Spezialfall von folgendem Satz ist: falls R ein faktorieller Ring ist, dann ist auch der Polynomring $R[X]$ faktoriell [1, Remark 7.28].

betrachten. Dies besteht aus allen Polynomen, bei denen der konstante Koeffizient gerade ist: einerseits hat jedes Polynom der Form $2f + Xg$ offensichtlich diese Eigenschaft, und andererseits können wir jedes Polynom

$$a_n X^n + \cdots + a_1 X + a_0$$

mit geradem konstanten Koeffizienten $a_0 = 2a'_0$ in der Form

$$X \cdot (a_n X^{n-1} + \cdots + a_2 X + a_1) + 2 \cdot a'_0$$

schreiben.

Angenommen, dass I ein Hauptideal wäre, also $I = (h)$ für ein Polynom $h \in \mathbb{Z}[X]$. Da dann sowohl $2 \in I$ als auch $X \in I$ gilt, müsste h sowohl 2 als auch X teilen. Aus $h \mid 2$ folgt, dass h konstant ist, und wegen $h \mid X$ bleiben nur die Möglichkeiten $h = \pm 1$. Dann wäre aber $I = (h) = \mathbb{Z}[X]$, was nicht sein kann, da $1 \notin I$ ist. Also ist I kein Hauptideal und $\mathbb{Z}[X]$ somit kein Hauptidealring.

Aus Satz 4.7.3 folgt daher auch, dass es in $\mathbb{Z}[X]$ keine Division mit Rest im Sinne von Definition 4.6.1 geben kann.

4.9 Irreduzibilitätskriterien für Polynome

In Beispiel 4.8.8 war es relevant, zu bestimmen, ob ein gegebenes Polynom irreduzibel ist oder nicht. Dies wird auch in Abschnitt 5 eine wichtige Rolle spielen. Wie kann man dies also bestimmen?

Hier ist ein recht einfaches Kriterium.

4.9.1 Lemma. *Sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad 2 oder 3. Dann ist f genau dann irreduzibel, wenn f keine Nullstelle in K besitzt.*

Beweis. Wenn f eine Nullstelle $a \in K$ hat, dann ist $X - a$ ein Teiler von f , also ist f reduzibel.

Umgekehrt sei f reduzibel, also $f = gh$ mit $g, h \in K[X]$ von positiven Graden. Da $\deg(f) = 2$ oder $\deg(f) = 3$ gilt und sich die Grade von g und h zu $\deg(f)$ addieren, muss entweder $\deg(g) = 1$ oder $\deg(h) = 1$ gelten. Ohne Einschränkung sei $\deg(g) = 1$, also $g = aX - b$ für $a, b \in K$ mit $a \neq 0$. Dann ist $a^{-1}b$ eine Nullstelle von g , und somit wegen $f = gh$ auch von f . $\square$

Für höhere Grade reicht dies aber nicht mehr aus, denn zum Beispiel ein Polynom vom Grad 4 kann wie in (4.29) als Produkt zweier quadratischer Polynome zerfallen, ohne eine Nullstelle zu haben.

Für Polynome mit rationalen Koeffizienten ist das folgende Kriterium besonders nützlich. Um die Ringtheorie abschließen zu können, betrachten wir es hier ohne Beweis.

4.9.2 Satz (Eisenstein-Kriterium). *Sei*

$$f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

mit $n \geq 1$. Angenommen, es gibt eine Primzahl p mit

$$(a) \quad p \nmid a_n,$$

$$(b) \quad p \mid a_i \text{ für alle } 0 \leq i < n,$$

$$(c) \quad p^2 \nmid a_0.$$

Dann ist f irreduzibel in $\mathbb{Q}[X]$.

In der Anwendung kann man also zunächst schauen, ob die $a_0, \dots, a_{n-1}$ einen gemeinsamen Teiler haben. Gibt es einen gemeinsamen Primteiler p mit $p \nmid a_n$ und $p^2 \nmid a_0$, dann ist das Polynom irreduzibel in $\mathbb{Q}[X]$.

4.9.3 Beispiel. (a) Für jede Primzahl p und jedes $n \geq 1$ ist

$$X^n - p$$

irreduzibel in $\mathbb{Q}[X]$. Dies folgt direkt aus dem Eisenstein-Kriterium, angewandt auf die Primzahl p . Zum Beispiel sind also

$$X^2 - 2, \quad X^3 - 5, \quad X^{10} - 7$$

irreduzibel in $\mathbb{Q}[X]$. Insbesondere zeigt dies, dass diese Polynome keine Nullstelle in $\mathbb{Q}$ haben, dass also $\sqrt[n]{p}$ für $n \geq 2$ und Primzahlen p irrational ist!

(b) Manchmal muss man ein Polynom erst durch eine einfache Transformation in eine Form bringen, auf die das Eisenstein-Kriterium anwendbar ist. Sei p eine Primzahl und

$$\Phi_p := X^{p-1} + \dots + X + 1 = \frac{X^p - 1}{X - 1}$$

das sogenannte p -te *Kreisteilungspolynom*. Das Eisenstein-Kriterium ist direkt auf Φ_p nicht anwendbar, weil die Koeffizienten a_i für $i < n$ keinen gemeinsamen Teiler haben. Die Substitution $X \mapsto X + 1$ definiert einen Isomorphismus $\mathbb{Q}[X] \rightarrow \mathbb{Q}[X]$, erhält also Irreduzibilität. Es genügt daher, die Irreduzibilität von $\Phi_p(X + 1)$ zu zeigen. Da

$$\Phi_p(X + 1) = \frac{(X + 1)^p - 1}{(X + 1) - 1} = \sum_{k=1}^p \binom{p}{k} X^{k-1}$$

gilt, ist der Leitkoeffizient gleich 1, alle anderen Koeffizienten sind durch p teilbar,³⁶ und der konstante Koeffizient ist p . Nach dem Eisenstein-Kriterium ist also $\Phi_p(X + 1)$ irreduzibel in $\mathbb{Q}[X]$, und damit auch $\Phi_p(X) = \Phi_p$.

4.9.4 Bemerkung. Das Eisenstein-Kriterium ist nur ein hinreichendes Kriterium. Ein Polynom kann also irreduzibel sein, ohne dass das Kriterium direkt anwendbar ist. Wie das Beispiel der Kreisteilungspolynome zeigt, kann es aber helfen, vorher eine geeignete Variablensubstitution vorzunehmen.

Außerdem ist die Version des Kriteriums für $\mathbb{Q}[X]$ nur ein Spezialfall, und man kann das Eisenstein-Kriterium auch allgemein für Polynomringe über Quotientenkörper von faktoriellen Ringen formulieren. Quotientenkörper haben wir aber noch nicht behandelt (Definition 5.1.5).

³⁶Für $1 \leq k \leq p - 1$ gilt

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdot \dots \cdot (p-k+1)}{k!}.$$

Im Zähler kommt der Faktor p genau einmal vor, im Nenner dagegen gar nicht, weil $k < p$ ist. Also ist $\binom{p}{k}$ durch p teilbar.

5 Körper

Betrachten wir ein Polynom wie zum Beispiel

$$f = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]. \quad (5.1)$$

Dieses Polynom hat 4 komplexe Nullstellen, denn in $\mathbb{C}[X]$ gilt:

5.0.1 Satz. *Jedes Polynom $f \in \mathbb{C}[X]$ mit $\deg(f) > 0$ hat mindestens eine Nullstelle in $\mathbb{C}$, und faktorisiert somit durch wiederholte Polynomdivision in komplexe Linearfaktoren.*

Obwohl man diese Aussage größtenteils auch mit Methoden der Galoistheorie beweisen kann, setzen wir sie hier der Kürze halber als aus der Analysis bekannt voraus.

Falls wir die Nullstellen mit a_1, a_2, a_3, a_4 bezeichnen, dann folgt daraus die Faktorisierung

$$f = (X - a_1)(X - a_2)(X - a_3)(X - a_4) \quad (5.2)$$

in $\mathbb{C}[X]$. Die Reihenfolge dieser Nullstellen ist beliebig, und wir wissen auch nicht, ob sie überhaupt alle verschieden sind. Damit verwandt sind die Formeln von Vieta: durch Ausmultiplizieren von (5.2) und Koeffizientenvergleich mit (5.1) ergibt sich

$$\begin{aligned} a_1 a_2 a_3 a_4 &= 1, \\ a_1 a_2 a_3 + a_1 a_2 a_4 + a_1 a_3 a_4 + a_2 a_3 a_4 &= 0, \\ a_1 a_2 + a_1 a_3 + a_1 a_4 + a_2 a_3 + a_2 a_4 + a_3 a_4 &= -10, \\ a_1 + a_2 + a_3 + a_4 &= 0. \end{aligned}$$

Hierbei ist die linke Seite jeweils eine *symmetrische* Funktion der Nullstellen, also invariant unter Permutationen der Nullstellen. Dies legt nahe, *Permutationen* dieser Nullstellen zu betrachten.

Durch Nachrechnen kann man feststellen, dass eine der Nullstellen (die wir oBdA als a_1 bezeichnen) gegeben ist durch

$$a_1 = \sqrt{2} + \sqrt{3}.$$

Die Körpertheorie impliziert nun—allein aufgrund der Tatsache, dass die Koeffizienten von f rational sind—dass sogar alle vier Vorzeichenkombinationen

$$\pm\sqrt{2} \pm \sqrt{3}$$

Nullstellen von f sind. Somit haben wir bereits alle vier Nullstellen von f gefunden! Die Faktorisierung (5.2) ist also durch

$$f = (X - \sqrt{2} - \sqrt{3})(X - \sqrt{2} + \sqrt{3})(X + \sqrt{2} - \sqrt{3})(X + \sqrt{2} + \sqrt{3}) \quad (5.3)$$

gegeben.

Das Wechseln eines oder beider Vorzeichen implementiert eine Permutation der Nullstellen. Dies definiert eine Untergruppe der Permutationsgruppe S_4 , nämlich die **Vierergruppe** bestehend aus der Identität und den drei Doppeltranspositionen (2.28).

5.1 Grundlagen

5.1.1 Definition. *Ein **Körper** ist ein kommutativer Ring K , in dem*

$$K^\times = K \setminus \{0\} \quad (5.4)$$

gilt.

Zu den bekannten Beispielen zählen natürlich die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$, und man mag zunächst Schwierigkeiten haben, sich weitere Beispiele vorzustellen.

+	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

$\cdot$	0	1	a	$1+a$
0	0	0	0	0
1	0	1	a	$1+a$
a	0	a	$1+a$	1
$1+a$	0	$1+a$	1	a

Abbildung 18: Ein Körper mit vier Elementen.

5.1.2 Bemerkung. Die Gleichung (5.4) ist äquivalent zu den beiden Inklusionen $K^\times \supseteq K \setminus \{0\}$ und $K^\times \subseteq K \setminus \{0\}$.

- (a) Die erste Inklusion $K^\times \supseteq K \setminus \{0\}$ bedeutet, dass jedes Element $\neq 0$ invertierbar ist.
- (b) Die zweite Inklusion $K^\times \subseteq K \setminus \{0\}$ bedeutet, dass jedes invertierbare Element $\neq 0$ ist. Dies gilt in jedem Ring mit $1 \neq 0$, denn die Invertierbarkeit von 0 würde ja

$$1 = 0 \cdot 0^{-1} = 0$$

implizieren. Falls andererseits $1 = 0$ ist, also $K = \{0\}$ der Nullring ist, dann ist auch $K^\times = \{0\}$, also ist die Bedingung verletzt. Mit anderen Worten: die Inklusion $K^\times \subseteq K \setminus \{0\}$ besagt nur, dass der Nullring kein Körper ist.

Wenn man einen Körper stattdessen definiert als “kommutativer Ring, in dem alle Elemente $\neq 0$ invertierbar sind”, dann fehlt diese Bedingung und der Nullring ist erlaubt. Es besteht aber Einigkeit darüber, dass man den Nullring nicht als Körper betrachten sollte, und deshalb ist diese Definition eigentlich falsch.

5.1.3 Bemerkung. Eine andere Formulierung der Definition von Körper ist: Ein Körper ist ein kommutativer Ring K , der genau die zwei trivialen Ideale (0) und K selbst besitzt, also

$$\text{Id}(K) = \{(0), K\}. \quad (5.5)$$

Denn:

- ▷ Die Bedingung $(0) \neq K$ ist äquivalent zu $1 \neq 0$, also dass K nicht der Nullring ist.
- ▷ Falls es nach (5.5) keine anderen Ideale gibt, ist also für jedes $a \in K \setminus \{0\}$ notwendigerweise $(a) = K$, also $1 \in (a)$, also a invertierbar. Sei umgekehrt $I \subseteq K$ ein Ideal in einem Körper K . Falls $I \neq (0)$ ist, dann enthält I mindestens ein Element $a \neq 0$. Dann gilt aber auch $1 = a^{-1}a \in I$, also $I = K$ nach Bemerkung 4.3.8(b).

Im Beweis von Satz 5.1.9 unten wird (5.5) nützlich sein.

5.1.4 Beispiel. (a) Abbildung 18 definiert einen Körper mit vier Elementen.

Wir werden im Folgenden auch allgemeine Konstruktionsmethoden für endliche Körper kennenlernen, und sogar alle endlichen Körper bis auf Isomorphie klassifizieren können.

(b) Der Ring

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

ist ein Körper, denn jedes Element $a + b\sqrt{2} \neq 0$ mit $a, b \in \mathbb{Q}$ hat das Inverse

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in \mathbb{Q}[\sqrt{2}], \quad (5.6)$$

wobei der Nenner aufgrund der Irrationalität von $\sqrt{2}$ nicht null ist.

5.1.5 Definition. Sei R ein Integritätsring. Dann ist der **Quotientenkörper** von R der Körper $\text{Quot}(R)$ mit:

▷ Die Elemente sind Äquivalenzklassen von Brüchen $\frac{a}{b}$ mit $a, b \in R$ und $b \neq 0$, wobei

$$\frac{a}{b} \sim \frac{c}{d} \quad :\Longleftrightarrow \quad ad = bc.$$

▷ Die Addition und Multiplikation sind durch die üblichen Bruchregeln definiert,

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}. \quad (5.7)$$

Vollständig formal ausgedrückt sind die Elemente von $\text{Quot}(R)$ also Äquivalenzklassen von Paaren (a, b) mit $a, b \in R$ und $b \neq 0$, wobei $(a, b) \sim (c, d)$ genau dann gilt, wenn $ad = bc$, und man für die Äquivalenzklassen auch

$$\frac{a}{b} := [(a, b)]$$

schreibt.

5.1.6 Satz. Diese Definition macht $\text{Quot}(R)$ tatsächlich zu einem Körper, und durch die Abbildung

$$\begin{aligned} R &\longrightarrow \text{Quot}(R), \\ a &\longmapsto \frac{a}{1} \end{aligned}$$

wird R zu einem Unterring von $\text{Quot}(R)$.

Beweisskizze. Bekannt aus dem Fall von $\mathbb{Q} = \text{Quot}(\mathbb{Z})$, der allgemein genauso funktioniert. Die Voraussetzung, dass R ein Integritätsring ist, ist relevant einerseits dafür, dass der Nenner bd in (5.7) nicht null ist. Andererseits braucht man sie auch für den Beweis der Transitivität der Äquivalenzrelation: die Voraussetzung

$$\frac{a}{b} \sim \frac{c}{d} \sim \frac{e}{f}$$

bedeutet

$$ad = bc \quad \text{und} \quad cf = de.$$

Durch Multiplikation der ersten Gleichung mit f und der zweiten mit b ergibt sich

$$adf = bcf = bde.$$

Da $d \neq 0$ gilt, folgt die gewünschte Gleichung $af = be$ durch Kürzen von d (Lemma 4.5.5). $\square$

5.1.7 Beispiel. (a) Es gibt einen Isomorphismus

$$\text{Quot}(\mathbb{Z}[i]) \cong \mathbb{Q}[i],$$

denn der Inklusionshomomorphismus

$$\begin{aligned} \mathbb{Q}[i] &\hookrightarrow \text{Quot}(\mathbb{Z}[i]) \\ \frac{a}{c} + \frac{b}{c}i &\longmapsto \frac{a + bi}{c} \end{aligned}$$

ist surjektiv, weil sich jedes Element von $\text{Quot}(\mathbb{Z}[i])$ schreiben lässt als

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.$$

(b) Sei K ein Körper und X eine Variable. Dann heißt

$$K(X) := \text{Quot}(K[X])$$

der **Körper der rationalen Funktionen** über K , weil seine Elemente Brüche von Polynomen sind, also rationale Funktionen wie

$$\frac{X^2 + 1}{X^3 - 2X + 1} \in \mathbb{Q}(X).$$

Zu beachten ist hier, dass der Auswertungshomomorphismus (4.9) $K[X] \rightarrow K$, welcher an einer fixen Stelle $a \in K$ ausgewertet, sich *nicht* zu einem Homomorphismus $K(X) \rightarrow K$ fortsetzen lässt, weil der Nenner an der Stelle a null sein kann.

Eine weitere wichtige Konstruktion von Körpern ist über die Bildung von Restklassenringen. Natürlich ist nicht jeder Restklassenring R/I ein Körper, sondern nur für eine bestimmte Klasse von Idealen I .

5.1.8 Definition. Ein Ideal $I \subseteq R$ in einem kommutativen Ring R heißt **maximal**, falls:

- (a) $I \neq R$.
- (b) Es gibt kein Ideal echt zwischen I und R , also: für jedes Ideal J mit $I \subseteq J \subseteq R$ gilt $J = I$ oder $J = R$.

5.1.9 Satz. Sei R ein kommutativer Ring.

- (a) Für ein Ideal $I \subseteq R$ ist der Restklassenring R/I genau dann ein Körper, wenn I maximal ist.
- (b) Falls R ein Hauptidealring ist, dann ist für jedes irreduzible $a \in R$ das Ideal (a) maximal, so dass $R/(a)$ ein Körper ist.

Beweis. (a) Unter dem Projektionshomomorphismus

$$\begin{aligned} R &\longrightarrow R/I \\ a &\longmapsto a + I \end{aligned}$$

entsprechen die Ideale von R/I genau den Idealen von R , die I enthalten. Damit R/I also genau die zwei trivialen Ideale besitzt (Bemerkung 5.1.3), muss es also genau zwei Ideale in R geben, die I enthalten. Falls $I = R$ gibt es nur eines (und dann ist R/I der Nullring). Falls $I \neq R$ müssen diese beiden Ideale I und R selbst sein, so dass es keine weiteren dazwischen gibt.

- (b) Da a keine Einheit ist, gilt $(a) \neq R$. Sei andererseits J ein Ideal mit $(a) \subseteq J \subseteq R$. Weil R ein Hauptidealring ist, gibt es $b \in R$ mit $J = (b)$. Nach $(a) \subseteq (b)$ haben wir $b \mid a$. Durch die Irreduzibilität von a folgt, dass b entweder eine Einheit ist, also $(b) = R$, oder $b \sim a$, also $(b) = (a)$. $\square$

5.1.10 Beispiel. Für jede Primzahl p ist

$$\boxed{\mathbb{F}_p := \mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}}$$

ein Körper. Die neue Bezeichnung $\mathbb{F}_p$ hierbei ist eine gebräuchliche Kurzschreibweise für diesen Körper, die sinnvoll ist, weil die $\mathbb{F}_p$ selbst in der Zahlentheorie eine wichtige Rolle spielen.

Wir kommen nun zur Betrachtung einiger grundlegender Eigenschaften von Körpern.

5.1.11 Satz. Sei $f \in K[X] \setminus \{0\}$ ein Polynom. Dann hat f höchstens $\deg(f)$ viele Nullstellen in K .

Beweis. Induktion über den Grad $\deg(f)$. Der Induktionsanfang ist klar: Ein Polynom vom Grad 0 ist konstant ungleich null und hat somit keine Nullstellen. Für den Induktionsschritt sei also $\deg(f) > 0$ und $a \in K$ eine Nullstelle von f , also $f(a) = 0$. Durch Polynomdivision lässt sich f schreiben als

$$f = (X - a) \cdot g,$$

für ein Polynom $g \in K[X]$ mit $\deg(g) = \deg(f) - 1$. Dann hat g höchstens $\deg(g) = \deg(f) - 1$ viele Nullstellen nach der Induktionsvoraussetzung. Weil die Nullstellen von f aber genau die Nullstellen von g zusammen mit a sind, hat f höchstens $\deg(f)$ viele Nullstellen. $\square$

Dass sowohl die Betrachtung von Polynomen als auch die Gruppentheorie für die Körpertheorie extrem nützlich sind, zeigt sich am folgenden Beweis.

5.1.12 Satz. *Sei K ein endlicher Körper. Dann ist die multiplikative Gruppe $K^\times$ zyklisch.*

Beweis. Die Klassifikation endlicher abelscher Gruppen nach Satz 2.6.14 liefert uns einen Isomorphismus

$$K^\times \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$$

für geeignete natürliche Zahlen $d_1 \mid \cdots \mid d_r$, die ≥ 2 sind.³⁷ Insbesondere gilt, dass $x^{d_r} = 1$ für alle $x \in K^\times$, sowie

$$|K^\times| = d_1 \cdots d_r.$$

Weil das Polynom $X^{d_r} - 1$ aber höchstens d_r viele Nullstellen in K haben kann, muss nach Satz 5.1.11 also $|K^\times| \leq d_r$ gelten. Somit folgt $d_1 \cdots d_r = d_r$, was aber nur mit $r = 1$ möglich ist, also $K^\times \cong \mathbb{Z}_{d_1}$. $\square$

5.1.13 Definition. *Sei K ein Körper. Die **Charakteristik** $\text{char}(K)$ von K ist die kleinste Zahl $n \in \mathbb{N}_{>0}$ mit*

$$\underbrace{1 + \cdots + 1}_n = 0 \quad \text{in } K,$$

oder 0 falls es keine solche Zahl gibt.

5.1.14 Bemerkung. Es mag merkwürdig erscheinen, die Charakteristik als 0 anstatt ∞ zu definieren, falls das wiederholte Addieren von 1 nie null ergibt. Dies erklärt sich wie folgt. Der Ringhomomorphismus

$$\begin{aligned} \mathbb{Z} &\longrightarrow K \\ n &\longmapsto \underbrace{1 + \cdots + 1}_n \end{aligned} \tag{5.8}$$

hat einen Kern, der ein Ideal von $\mathbb{Z}$ ist, also von der Form $n\mathbb{Z}$ für eine eindeutige Zahl $n \in \mathbb{N}$. Dieses n ist genau die Charakteristik von K . Denn insbesondere falls der Kern trivial ist, dann ist der Kern das Nullideal, also $n = 0$.

5.1.15 Beispiel. (a) $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$.

(b) $\text{char}(\mathbb{F}_p) = p$ für jede Primzahl p .

5.1.16 Lemma. *Die Charakteristik jedes Körpers ist entweder 0 oder eine Primzahl.*

Beweis. Falls $\text{char}(K) \neq 0$ und keine Primzahl ist, dann müsste entweder $\text{char}(K) = 1$ sein oder $\text{char}(K) = nm$ für zwei natürliche Zahlen $n, m > 1$. Im ersten Fall wäre $1 = 0$, also K der Nullring, was kein Körper ist. Im zweiten Fall hätten wir

$$\underbrace{(1 + \cdots + 1)}_n \cdot \underbrace{(1 + \cdots + 1)}_m = \underbrace{1 + \cdots + 1}_{nm} = 0.$$

Da K insbesondere nullteilerfrei ist, müsste also einer der beiden Faktoren links verschwinden, was aber der Minimalität von $\text{char}(K)$ widerspricht. $\square$

5.2 Körpererweiterungen

Wir können jetzt unseren primären Gegenstand der Untersuchung definieren, nämlich die *Körpererweiterungen*, wie sie (jedenfalls implizit) in den Beispielen immer wieder auftaucht sind.

5.2.1 Definition (Körpererweiterung). *Eine **Körpererweiterung** ist ein Ringhomomorphismus $K \hookrightarrow L$ von Körpern.*

³⁷Für $K = \mathbb{F}_2$ ist $K^\times = \{1\}$ die triviale Gruppe, die tatsächlich zyklisch ist. Dies entspricht dem Fall $r = 0$. Für alle Körper mit ≥ 3 Elementen ist aber $K^\times$ nicht trivial, also $r \geq 1$, was wir im Folgenden annehmen können.

Wie durch die Notation $\hookrightarrow$ bereits angedeutet, ist ein solcher Homomorphismus stets injektiv: sein Kern ist ein Ideal von K , also (nach Bemerkung 5.1.3) entweder (0) oder K selbst. Letzteres ist aber dadurch ausgeschlossen, dass ein Ringhomomorphismus $1 \mapsto 1$ abbilden muss und $1 \neq 0$ in L gilt.

Normalerweise ist aus dem Zusammenhang klar, welcher Homomorphismus gemeint ist, wenn wir zwei Körper K und L angeben. Außerdem identifiziert man meist auch K mit seinem Bild in L , so dass der Homomorphismus $K \hookrightarrow L$ einfach als Inklusion $K \subseteq L$ geschrieben wird. Deshalb haben wir dem Homomorphismus auch keinen Namen gegeben. Wir bezeichnen K als **Unterkörper** von L und L als **Oberkörper** von K . Um auszudrücken, dass L eine Erweiterung von K ist, schreibt man oft auch

$$\boxed{L/K}$$

gesprochen als “ L über K ”.

5.2.2 Beispiel. (a) $\mathbb{C}/\mathbb{R}$ ist eine Körpererweiterung mit $\mathbb{R}$ als Unterkörper und $\mathbb{C}$ als Oberkörper.

(b) Ähnlich gilt $\mathbb{R}/\mathbb{Q}$ und $\mathbb{C}/\mathbb{Q}$.

(c) $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$.

(d) Für jeden Körper K ist K/K eine triviale Körpererweiterung.

(e) Wenn $K(X)$ den Körper der rationalen Funktionen aus Definition 5.1.5(b) bezeichnet, dann ist $K(X)/K$ eine Körpererweiterung, wobei K den konstanten Funktionen entspricht.

Die beiden folgenden Beispiele zeigen, dass jeder Körper einen kleinsten Unterkörper enthält, der entweder isomorph zu einem $\mathbb{F}_p$ oder zu $\mathbb{Q}$ ist.

(f) Falls K ein Körper von Charakteristik $p > 0$ ist, dann enthält K einen Unterkörper, der isomorph ist zu $\mathbb{F}_p$, nämlich die Elemente

$$0, \quad 1, \quad 1+1, \quad \dots, \quad \underbrace{1+\dots+1}_{p-1}.$$

Zum Beispiel ist der Körper mit vier Elementen aus Abbildung 18 ein Oberkörper von $\mathbb{F}_2$.

(g) Falls stattdessen K ein Körper von Charakteristik 0 ist, dann enthält K einen Unterkörper, der isomorph zu $\mathbb{Q}$ ist, weil die Injektivität des Homomorphismus $\mathbb{Z} \rightarrow K$ aus (5.8) impliziert, dass jede ganze Zahl $\neq 0$ in K ein inverses hat, so dass auch die rationalen Zahlen mit Elementen von K identifiziert werden können. Eine rationale Zahl $\frac{p}{q}$ mit $p, q \in \mathbb{Z}$ und $q \neq 0$ wird dabei abgebildet auf

$$\frac{p}{q} \mapsto \underbrace{(1+\dots+1)}_p \cdot \underbrace{(1+\dots+1)}_q^{-1}.$$

Man überzeugt sich zum Beispiel anhand der Rechenregeln in $\mathbb{Q}$ und in K davon, dass dies tatsächlich ein Homomorphismus $\mathbb{Q} \rightarrow K$ ist.

Bekanntermaßen ist $\mathbb{C}$ ein zweidimensionaler Vektorraum über $\mathbb{R}$. Außerdem sind lineare Algebra und analytische Geometrie bis zu einem gewissen Grad bei der Untersuchung von $\mathbb{C}$ hilfreich. Dies ist kein Zufall, sondern wieder eine allgemeine Eigenschaft von Körpererweiterungen.

5.2.3 Bemerkung. In jeder Körpererweiterung L/K gilt:

$$\boxed{L \text{ ist ein Vektorraum über } K.}$$

Denn L ist bereits eine abelsche Gruppe bezüglich der Addition, und durch $K \subseteq L$ lässt sich die Multiplikation in L zu einer skalaren Multiplikation

$$\begin{aligned} K \times L &\longrightarrow L \\ (a, x) &\longmapsto ax \end{aligned}$$

einschränken. Die Rechenregeln (Vektorraumaxiome) sind dann alle Spezialfälle der Rechenregeln für die Ringstruktur von L . Dadurch wird lineare Algebra zu einem wichtigen Werkzeug für die Untersuchung von Körpererweiterungen.

5.2.4 Definition. Der **Grad** einer Körpererweiterung L/K ist die Vektorraumdimension,

$$[L : K] := \dim_K(L).$$

5.2.5 Beispiel. (a) Eine ganze Zahl $D \in \mathbb{Z} \setminus \{0, \pm 1\}$ heißt **quadratifrei**, falls sie durch keine Quadratzahl > 1 teilbar ist, oder äquivalent, falls in ihrer Primfaktorzerlegung jede Primzahl höchstens einmal vorkommt. Dann ist $\sqrt{D} \in \mathbb{C}$ irrational, und

$$\mathbb{Q}[\sqrt{D}] = \{r + s\sqrt{D} : r, s \in \mathbb{Q}\} \quad (5.9)$$

ist nach einer Rechnung analog zu (5.6) ein Körper. Es gilt $\mathbb{Q}[\sqrt{D}]/\mathbb{Q}$. Für $D > 0$ ist $\mathbb{Q}[\sqrt{D}]$ ein Unterkörper von $\mathbb{R}$, und für $D < 0$ ein Unterkörper von $\mathbb{C}$.

Wie bereits an (5.9) erkennbar ist, gilt

$$[\mathbb{Q}[\sqrt{D}] : \mathbb{Q}] = 2,$$

und es bietet sich die Basis $\{1, \sqrt{D}\}$ an. Jedes Element $r + s\sqrt{D}$ definiert jetzt eine lineare Abbildung auf diesem Vektorraum, nämlich die Multiplikation mit $r + s\sqrt{D}$! Unter dieser Abbildung werden die Basisvektoren wie folgt abgebildet:

$$1 \mapsto r + s\sqrt{D}, \quad \sqrt{D} \mapsto Ds + r\sqrt{D}.$$

Also wird die Abbildung in dieser Basis durch die Matrix

$$\begin{pmatrix} r & Ds \\ s & r \end{pmatrix}$$

dargestellt. Interessant ist nun, sich deren Determinante anzuschauen, diese ist nämlich

$$N(r + s\sqrt{D}) = r^2 - Ds^2.$$

Es handelt sich um die bereits mehrfach verwendete *Norm* in $\mathbb{Q}[\sqrt{D}]$! Deren Multiplikativität ist jetzt einfach eine Konsequenz der Multiplikativität der Determinante zusammen mit der Tatsache, dass die Multiplikation mit einem Produkt von Elementen mit der Hintereinanderausführung der Multiplikationen mit den einzelnen Elementen übereinstimmt.

(b) Für den Körper der rationalen Funktionen $K(X)$ über einem Körper K gilt

$$[K(X) : K] = \infty,$$

denn bereits die Monome $1, X, X^2, \dots$ bilden eine unendliche Familie linear unabhängiger Elemente von $K(X)$ über K .³⁸

Eine weitere starke Konsequenz der Vektorraumstruktur von Körpererweiterungen ist folgende Aussage, die in die Richtung der Klassifikation von endlichen Körpern geht.

5.2.6 Lemma. Sei K ein endlicher Körper. Dann ist die Anzahl der Elemente von K eine Primzahlpotenz, und zwar

$$|K| = \text{char}(K)^{[K : \mathbb{F}_{\text{char}(K)}]}.$$

Beweis. Als abkürzende Notation schreiben wir $p := \text{char}(K)$ und $n := [K : \mathbb{F}_p]$. Dann ist K ein Vektorraum der Dimension n über $\mathbb{F}_p$, d.h. mit n Basisvektoren. Jedes Element von K lässt sich also eindeutig als Linearkombination dieser Basisvektoren darstellen. Für jeden Koeffizienten gibt es dabei genau p viele Möglichkeiten. Also gibt es insgesamt p^n viele Möglichkeiten, so dass $|K| = p^n$ gilt. $\square$

³⁸Eine tiefergehende Frage wäre, ob die Dimension von $K(X)$ über K abzählbar oder überabzählbar unendlich ist. Es stellt sich heraus, dass für überabzählbares K diese Dimension überabzählbar unendlich ist, obwohl der Polynomring $K[X]$ über K nur abzählbar unendliche Dimension hat.

Die Frage, ob es zum Beispiel einen Körper mit 60 Elementen gibt, lässt sich damit sofort beantworten: Nein, denn 60 ist keine Primzahlpotenz.

Wie wir bald sehen werden, ist folgende allgemeinere Konstruktion von Körpererweiterungen für die Körpertheorie zentral.

5.2.7 Satz. *Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom. Dann ist der Quotient $K[X]/(f)$ ein Körper, und der kanonische Homomorphismus*

$$\begin{aligned} K &\longrightarrow K[X]/(f), \\ a &\longmapsto a + (f) \end{aligned}$$

macht $K[X]/(f)$ zu einer Erweiterung von K , und es gilt

$$[K[X]/(f) : K] = \deg(f).$$

Beweis. Da f irreduzibel ist, ist das Ideal (f) maximal in $K[X]$. Weil außerdem $K[X]$ ein Hauptidealring ist, folgt, dass der Restklassenring $K[X]/(f)$ auch ein Körper ist (Satz 5.1.9). Der angegebene Homomorphismus ist injektiv, denn $(f) \cap K = \{0\}$, so dass der Kern trivial ist. Also können wir $K[X]/(f)$ als Erweiterung von K auffassen.

Sei nun $n := \deg(f)$. Durch Division mit Rest kann jedes Polynom $g \in K[X]$ eindeutig in der Form

$$g = qf + r$$

mit $q, r \in K[X]$ und $r = 0$ oder $\deg(r) < n$ geschrieben werden. Also hat jede Restklasse modulo (f) einen eindeutigen Repräsentanten der Form

$$a_0 + a_1X + \cdots + a_{n-1}X^{n-1}.$$

Damit bilden die Restklassen von $1, X, \dots, X^{n-1}$ eine Basis von $K[X]/(f)$ als K -Vektorraum. Insbesondere gilt

$$[K[X]/(f) : K] = n = \deg(f),$$

was die Behauptung zeigt. □

Dies liefert uns einige bereits bekannte Beispiele, aber auch neue.

5.2.8 Beispiel. (a) $X^2 + 1 \in \mathbb{R}[X]$ ist irreduzibel, also ist $\mathbb{R}[X]/(X^2 + 1)$ ein Körper. In Beispiel 4.3.18(a) hatten wir gesehen, dass dieser Körper isomorph ist zu $\mathbb{C}$, wobei die Restklasse von X dem Element $i \in \mathbb{C}$ entspricht.

(b) Das Polynom $X^3 - 3X + 1 \in \mathbb{Q}[X]$ ist irreduzibel: nach Lemma 4.9.1 müsste es sonst eine Nullstelle in $\mathbb{Q}$ haben. Dies kann aber nicht der Fall sein, weil wir dann teilerfremde $p, q \in \mathbb{Z}$ mit $q \neq 0$ hätten, so dass

$$\left(\frac{p}{q}\right)^3 - 3 \cdot \frac{p}{q} + 1 = 0,$$

oder äquivalent

$$p^3 - 3pq^2 + q^3 = 0.$$

Da die ersten beiden Terme Vielfache von p sind, muss also auch jeder Primteiler von p ein Primteiler von q sein. Weil p und q aber teilerfremd sind, kann es gar keinen solchen Primteiler geben, also muss $p = \pm 1$ sein. Analog erhält man $q = \pm 1$, indem man zunächst auch $p \neq 0$ feststellt. Die einzigen Kandidaten für Nullstellen von $X^3 - 3X + 1$ in $\mathbb{Q}$ sind also $\frac{p}{q} = \pm 1$. Durch Einsetzen sieht man aber, dass weder 1 noch -1 eine Nullstelle von $X^3 - 3X + 1$ ist. Dadurch ist das Polynom $X^3 - 3X + 1$ irreduzibel über $\mathbb{Q}$.

Also ist $\mathbb{Q}[X]/(X^3 - 3X + 1)$ ein Körper, und zwar eine Erweiterung von $\mathbb{Q}$.

(c) Nach Beispiel 4.9.3(a) ist $X^n - p$ irreduzibel in $\mathbb{Q}[X]$ für jede Primzahl p und jedes $n \geq 1$. Daher ist $\mathbb{Q}[X]/(X^n - p)$ ein Körper. Analog wie in Beispiel 4.3.18(b) können wir ihn mit $\mathbb{Q}[\sqrt[n]{p}]$ identifizieren, wobei die Restklasse von X der Zahl $\sqrt[n]{p}$ entspricht.

Wie die obigen Beispiele nahelegen, fügen wir durch Betrachten von $K[X]/(f)$ für ein irreduzibles Polynom f eine Nullstelle von f hinzu. Wir *erweitern* also den Körper K um eine Nullstelle von f , und erhalten so einen neuen Körper, in dem f eine Nullstelle hat:

5.2.9 Lemma. *Sei K ein Körper, $f \in K[X]$ irreduzibel, und $a := X + (f) \in K[X]/(f)$ die Restklasse von X . Dann ist a eine Nullstelle von f in $K[X]/(f)$, also $f(a) = 0$.*

Beweis. Es gilt

$$f(a) = f(X + (f)) = f(X) + (f) = 0 + (f),$$

wobei die zweite Gleichung aufgrund der Definition der Ringstruktur von $K[X]/(f)$ gilt. $\square$

5.2.10 Beispiel. Wir können jetzt auch verstehen, was die Körpertheorie mit Lösungsformeln für polynomielle Gleichungen zu tun hat. Betrachten wir hierzu zum Beispiel die allgemeine quadratische Gleichung

$$aX^2 + bX + c = 0. \quad (5.10)$$

Die Hauptidee ist jetzt, dass wir die linke Seite als Element des Polynomrings

$$\mathbb{Q}(a, b, c)[X]$$

auffassen. Weil $\mathbb{Q}(a, b, c)$ ein Körper ist, ist auch $\mathbb{Q}(a, b, c)[X]$ ein Hauptidealring, so dass unsere bisherige Theorie anwendbar ist. Falls die Gleichung (5.10) jetzt eine Lösungsformel hätte, die sich als rationale Funktion in a, b, c schreiben lässt, dann müsste das Polynom $aX^2 + bX + c$ in $\mathbb{Q}(a, b, c)[X]$ eine Nullstelle haben, nämlich diejenige, die durch die hypothetische Lösungsformel gegeben ist. Das ist aber nicht der Fall.³⁹ Insbesondere ist also auch $f := aX^2 + bX + c$ irreduzibel in $\mathbb{Q}(a, b, c)[X]$.

Wir können aber jetzt die gleiche Idee wie bisher anwenden und *formal* eine Nullstelle von $aX^2 + bX + c$ adjungieren, indem wir den Restklassenring

$$\mathbb{Q}(a, b, c)[X]/(aX^2 + bX + c)$$

betrachten. Hier ist die Restklasse von X eine Nullstelle von $aX^2 + bX + c$, und damit eine Lösung der quadratischen Gleichung (5.10) in diesem neuen Körper. Diese Erweiterung ist vom Grad 2 über $\mathbb{Q}(a, b, c)$, was damit zu tun hat, dass man die Nullstellen von $aX^2 + bX + c$ durch Ziehen einer Quadratwurzel bekommt.

5.2.11 Satz. *Seien L/K und M/L endliche Körpererweiterungen. Dann ist auch M/K eine endliche Körpererweiterung, und es gilt*

$$[M : K] = [M : L] \cdot [L : K].$$

Beweis. Die Erweiterung M/K ist durch Hintereinanderausführung der Homomorphismen $K \hookrightarrow L \hookrightarrow M$ gegeben.

Sei $(u_i)_{i \in I}$ eine Basis von L als K -Vektorraum und $(v_j)_{j \in J}$ eine Basis von M als L -Vektorraum. Wir zeigen, dass dann

$$(u_i v_j)_{(i,j) \in I \times J}$$

eine Basis von M als K -Vektorraum ist. Sei dazu $x \in M$. Da die v_j eine Basis von M über L bilden, können wir

$$x = \sum_j \lambda_j v_j$$

mit $\lambda_j \in L$ schreiben. Jedes λ_j können wir wiederum als endliche Linearkombination der u_i mit Koeffizienten in K schreiben. Damit ist x eine K -Linearkombination der Produkte $u_i v_j$.

Es bleibt die lineare Unabhängigkeit zu zeigen. Sei also

$$\sum_{i,j} c_{ij} u_i v_j = 0$$

³⁹Denn aus einer Nullstelle $g \in \mathbb{Q}(a, b, c)$ würde nach quadratischer Ergänzung folgen, dass $b^2 - 4ac = (2ag + b)^2$ ein Quadrat in $\mathbb{Q}(a, b, c)$ ist. Dies ist aber nicht der Fall: als Element von $\mathbb{Q}(a, b)(c)$ hat $b^2 - 4ac$ nur die einfache Nullstelle $\frac{b^2}{4a}$, während Quadrate rationaler Funktionen nur Nullstellen gerader Vielfachheit haben.

mit $c_{ij} \in K$. Dann können wir dies als

$$\sum_j \left(\sum_i c_{ij} u_i \right) v_j = 0$$

auffassen. Da die v_j linear unabhängig über L sind, gilt $\sum_i c_{ij} u_i = 0$ für jedes j . Da wiederum die u_i linear unabhängig über K sind, folgt $c_{ij} = 0$ für alle i, j . Also bilden die $u_i v_j$ tatsächlich eine Basis von M über K , und daher gilt

$$[M : K] = |I \times J| = |I| \cdot |J| = [L : K] \cdot [M : L]. \quad \square$$

5.2.12 Beispiel. Nach Gleichung (4.8) gilt

$$\mathbb{Q}[\sqrt{2} + \sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}].$$

Die offensichtlichen Inklusionen $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ definieren Körpererweiterungen

$$\mathbb{Q}[\sqrt{2}]/\mathbb{Q}, \quad \mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}[\sqrt{2}].$$

Beide diese Erweiterungen haben Grad 2, denn $\{1, \sqrt{2}\}$ ist eine Basis von $\mathbb{Q}[\sqrt{2}]$ über $\mathbb{Q}$, und $\{1, \sqrt{3}\}$ ist eine Basis von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ über $\mathbb{Q}[\sqrt{2}]$.⁴⁰ Nach Satz 5.2.11 hat daher $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$ Grad 4. In der Tat ist

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{2 \cdot 3}\}$$

eine Basis von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ über $\mathbb{Q}$, nämlich genau das im Beweis konstruierte “Produkt” der beiden Basen.

5.3 Das Minimalpolynom

Elemente eines Oberkörpers L in einer Erweiterung L/K gibt es in zwei Arten: solche, die eine nichttriviale Gleichung über K erfüllen, und solche, die das nicht tun.

5.3.1 Definition. Sei L/K eine Körpererweiterung.

- (a) Ein Element $a \in L$ heißt **algebraisch** über K , falls es ein Polynom $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$ gibt, und sonst **transzendent**.
- (b) Die Erweiterung L/K heißt **algebraisch**, falls jedes Element von L algebraisch über K ist.

5.3.2 Beispiel. (a) $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, denn $(\sqrt{2})^2 - 2 = 0$.

- (b) Jede komplexe Zahl $r + si$ ist algebraisch über $\mathbb{R}$, denn zum Beispiel

$$(r + si)^2 - 2r(r + si) + r^2 + s^2 = 0,$$

also $f(r + si) = 0$ für das Polynom $f = X^2 - 2rX + r^2 + s^2$. Damit ist $\mathbb{C}/\mathbb{R}$ eine algebraische Erweiterung.

- (c) Die Zahlen $\pi, e \in \mathbb{R}$ sind transzendent über $\mathbb{Q}$. Dies ist aber sehr schwer zu zeigen und braucht analytische Methoden.

Leichter zu sehen ist, dass es transzendente Zahlen über $\mathbb{Q}$ gibt: denn weil $\mathbb{Q}[X]$ nur abzählbar viele Polynome enthält, und jedes Polynom nur endlich viele Nullstellen hat, gibt es nur abzählbar viele algebraische Zahlen über $\mathbb{Q}$. Weil $\mathbb{R}$ aber überabzählbar viele Elemente enthält, muss es auch transzendente Zahlen geben.

5.3.3 Definition. Eine Körpererweiterung L/K heißt **endlich**, falls $[L : K] < \infty$.

5.3.4 Satz. Jede endliche Erweiterung ist algebraisch.

⁴⁰Dies verwendet, dass $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$: aus $\sqrt{3} = r + s\sqrt{2}$ mit $r, s \in \mathbb{Q}$ würde durch Quadrieren $3 = r^2 + 2s^2 + 2rs\sqrt{2}$ folgen. Koeffizientenvergleich liefert $rs = 0$, also entweder $r^2 = 3$ oder $2s^2 = 3$, beides unmöglich in $\mathbb{Q}$.

Beweis. Sei L/K endlich und $a \in L$ und $n := [L : K]$. Die Menge der Potenzen $\{1, a, \dots, a^n\}$ enthält $n + 1$ Elemente und ist daher notwendigerweise linear abhängig über K . Es gibt also ein Polynom $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$ und sogar mit $\deg(f) \leq n$. $\square$

Es lohnt sich, die Algebraizität von Elementen genauer zu quantifizieren:

5.3.5 Definition. Sei $a \in L$ algebraisch über K . Dann ist das **Minimalpolynom** $\min(a)$ das eindeutige Element von $K[X]$ mit Leitkoeffizient 1, für das

$$\{f \in K[X] : f(a) = 0\} = (\min(a))$$

gilt.

Weil ein nichttriviales Ideal in $K[X]$ immer von einem Element $\neq 0$ vom kleinsten Grad erzeugt wird (siehe den Beweis von Satz 4.7.3), kann das Minimalpolynom äquivalent als das eindeutige Polynom $f \in K[X]$ mit $f(a) = 0$ und Leitkoeffizient 1 charakterisiert werden, welches unter allen Polynomen mit diesen Eigenschaften minimalen Grad hat. Folgende Charakterisierung ist *noch* nützlicher für konkrete Berechnungen.

5.3.6 Lemma. Sei $a \in L$ algebraisch über K und $f \in K[X]$ ein Polynom mit $f(a) = 0$ und Leitkoeffizient 1. Dann sind äquivalent:

(a) $f = \min(a)$.

(b) f ist irreduzibel in $K[X]$.

Beweis. (a) $\Rightarrow$ (b): Sei $\min(a) = gh$ mit $g, h \in K[X]$. Dann gilt

$$g(a) \cdot h(a) = \min(a)(a) = 0.$$

Da L ein Körper ist, folgt $g(a) = 0$ oder $h(a) = 0$. Im ersten Fall gehört also auch g zum Annihilatorideal, und daher auch $\min(a) \mid g$. Aus $g \mid \min(a)$ und $\min(a) \mid g$ folgt dann, dass h eine Einheit sein muss. Im zweiten Fall muss analog g eine Einheit sein.

(b) $\Rightarrow$ (a): Wegen $f(a) = 0$ gilt $\min(a) \mid f$, also $(f) \subseteq (\min(a))$. Das Ideal (f) ist nach der Irreduzibilität von f aber bereits maximal, und wegen $(\min(a)) \neq K[X]$ muss also $(f) = (\min(a))$ gelten, so dass f und $\min(a)$ assoziiert sind. Weil beide Polynome den Leitkoeffizienten 1 haben, folgt $f = \min(a)$. $\square$

5.3.7 Bemerkung. Der Beweis von Satz 5.3.4 sowie Lemma 5.3.6 deuten an, wie man ein Minimalpolynom bestimmen kann. Dazu gibt es folgende allgemeine Strategien:

(a) Man schaut sich die Potenzen

$$a^n, \quad a^{n-1}, \quad \dots, \quad a, \quad 1$$

an und untersucht, ob diese linear abhängig über K sind. Sei n der kleinste Wert, für den das der Fall ist. In diesem Fall liefert uns eine lineare Relation

$$r_n a^n + r_{n-1} a^{n-1} + \dots + r_1 a + r_0 = 0$$

das Minimalpolynom: aufgrund der Minimalität von n muss nämlich $r_n \neq 0$ sein, so dass wir durch Skalieren $r_n = 1$ erreichen können. Damit ist

$$\min(a) = X^n + r_{n-1} X^{n-1} + \dots + r_1 X + r_0$$

das Minimalpolynom von a .

(b) Falls man bereits ein Polynom $f \in K[X]$ mit $f(a) = 0$ kennt, dann kann man schauen, ob f irreduzibel ist. Wenn ja, dann ist f bereits das Minimalpolynom von a . Wenn nein, dann faktorisiert man f in Faktoren, die nach Möglichkeit alle irreduzibel sind, und schaut, welcher Faktor a zu Null macht. Einer dieser irreduziblen Faktoren ist dann das Minimalpolynom.

5.3.8 Beispiel. (a) Was ist das Minimalpolynom einer komplexen Zahl $r + si$ über $\mathbb{R}$? Falls $s = 0$, dann sind bereits 1 und r linear abhängig über $\mathbb{R}$, und entsprechend ist $\min(r) = X - r$. Falls $s \neq 0$, dann sind 1 und $r + si$ linear unabhängig über $\mathbb{R}$. Sobald man aber $(r + si)^2$ dazunimmt, muss es aus Dimensionsgründen eine lineare Abhängigkeit geben, wie im Beweis von Satz 5.3.4. Diese kennen wir aber bereits aus Beispiel 5.3.2(b), so dass

$$\min(r + si) = X^2 - 2rX + (r^2 + s^2).$$

(b) Für eine Primzahl p und $n \in \mathbb{N}_{>0}$ ist das Minimalpolynom von $\sqrt[n]{p} \in \mathbb{R}$ über $\mathbb{Q}$ das Polynom

$$\min(\sqrt[n]{p}) = X^n - p, \quad (5.11)$$

denn $X^n - p$ ist an der Stelle $\sqrt[n]{p}$ gleich 0, und das Polynom $X^n - p$ ist nach Beispiel 4.9.3 bereits irreduzibel über $\mathbb{Q}$.

Für ein Element $a \in L$ bezeichnen wir mit $K[a]$ den kleinsten Unterring von L , der K und a enthält, also die Menge aller Elemente von L , die sich als Polynom in a mit Koeffizienten aus K schreiben lassen. Folgende Aussage erklärt dann, warum die Konstruktion aus Satz 5.2.7 so häufig vorkommt.

5.3.9 Satz. Sei L/K eine Erweiterung und $a \in L$ algebraisch über K . Dann ist $K[a]$ bereits ein Körper. Außerdem ist die Abbildung

$$\begin{aligned} K[X]/(\min(a)) &\longrightarrow K[a] \\ [g] &\longmapsto g(a) \end{aligned}$$

ein Isomorphismus.

Beweis. Die erste Behauptung folgt aus der zweiten, denn $K[X]/(\min(a))$ ist nach Satz 5.2.7 und Lemma 5.3.6 ein Körper. Daher reicht es aus, die zweite Behauptung zu zeigen.

Wir betrachten hierzu wieder den Auswertungshomomorphismus

$$\begin{aligned} \text{ev}_a : K[X] &\longrightarrow K[a] \\ g &\longmapsto g(a). \end{aligned}$$

Dieser ist surjektiv, weil $K[a]$ nach Definition aus allen Elementen besteht, die sich als Polynom in a mit Koeffizienten aus K schreiben lassen. Außerdem ist

$$\ker(\text{ev}_a) = \{g \in K[X] : g(a) = 0\} = (\min(a))$$

nach der Definition des Minimalpolynoms. Nach dem ersten Isomorphiesatz für Ringe (Satz 4.3.17) induziert ev_a also einen Isomorphismus

$$K[X]/(\min(a)) \cong K[a],$$

und dieser ist gerade durch $[g] \mapsto g(a)$ gegeben. □

5.3.10 Beispiel. (a) Der Homomorphismus

$$\begin{aligned} \mathbb{Q}[X]/(X^3 - 2) &\longrightarrow \mathbb{Q}[\sqrt[3]{2}] \\ [g] &\longmapsto g(\sqrt[3]{2}) \end{aligned}$$

ist ein Isomorphismus, so dass wir $\mathbb{Q}[X]/(X^3 - 2)$ mit $\mathbb{Q}[\sqrt[3]{2}]$ identifizieren können.

(b) Betrachten wir den Körper mit vier Elementen aus Abbildung 18 als Oberkörper von $\mathbb{F}_2$. Dann gilt

$$\min(a) = X^2 + X + 1,$$

weil a eine Nullstelle von $X^2 + X + 1$ ist, und dieses Polynom mangels Nullstellen in $\mathbb{F}_2$ irreduzibel über $\mathbb{F}_2$ ist. Also ist der Homomorphismus

$$\begin{aligned} \mathbb{F}_2[X]/(X^2 + X + 1) &\longrightarrow \mathbb{F}_2[a] \\ [g] &\longmapsto g(a) \end{aligned}$$

ein Isomorphismus.

5.3.11 Beispiel. Manchmal kann man auch Überlegungen zum Grad von Erweiterungen anstellen, um das Minimalpolynom zu bestimmen. Zum Beispiel gilt über $K = \mathbb{Q}$, dass

$$\min(\sqrt{2} + \sqrt{3}) = X^4 - 10X^2 + 1;$$

siehe auch die Diskussion zu Beginn des Kapitels. Dies sieht man folgendermaßen. Nach Beispiel 5.2.12 ist

$$[\mathbb{Q}[\sqrt{2} + \sqrt{3}] : \mathbb{Q}] = 4.$$

Nach Satz 5.3.9 hat also auch $\mathbb{Q}[X]/(\min(\sqrt{2} + \sqrt{3}))$ Grad 4 über $\mathbb{Q}$. Weil dieser Grad nach Satz 5.2.7 aber mit dem Grad von $\min(\sqrt{2} + \sqrt{3})$ übereinstimmen muss, gilt auch

$$\deg(\min(\sqrt{2} + \sqrt{3})) = 4.$$

Andererseits ist

$$(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 0.$$

Also muss $X^4 - 10X^2 + 1$ bereits das Minimalpolynom sein. Insbesondere folgt daraus jetzt auch, dass das Polynom irreduzibel ist, was ohne diese Überlegung nicht offensichtlich ist.

5.3.12 Beispiel (Einheitswurzeln). Für $n \in \mathbb{N}_{>0}$ sind die n -ten **Einheitswurzeln** die komplexen Zahlen z mit $z^n = 1$, also die Zahlen

$$1, \quad e^{2\pi i \cdot \frac{1}{n}}, \quad e^{2\pi i \cdot \frac{2}{n}}, \quad \dots, \quad e^{2\pi i \cdot \frac{n-1}{n}}.$$

Diese bilden eine abelsche Gruppe unter der Multiplikation, die zyklisch ist. Ein Erzeuger dieser Gruppe heißt **primitive n -te Einheitswurzel**. Zum Beispiel ist $\zeta := e^{2\pi i \cdot \frac{1}{n}}$ eine primitive n -te Einheitswurzel. Diese sind offensichtlich algebraisch über $\mathbb{Q}$, denn sie erfüllen die Gleichung $X^n - 1 = 0$. Damit ist ihr Minimalpolynom jedenfalls ein Teiler von $X^n - 1$. Aber wie schaut es genau aus?

Schauen wir uns einige konkrete Fälle an:

- (a) Die allereinfachsten Fälle sind $n = 1$ und $n = 2$, denn hier gilt

$$\begin{aligned} \zeta_1 &= 1, & \min(1) &= X - 1, \\ \zeta_2 &= -1, & \min(-1) &= X + 1. \end{aligned}$$

- (b) Der erste interessante Fall ist $n = 3$, denn hier gilt

$$\zeta_3 = e^{2\pi i \cdot \frac{1}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2},$$

und damit

$$\min(\zeta_3) = X^2 + X + 1.$$

In der Tat gilt $\zeta_3^2 + \zeta_3 + 1 = 0$, denn das reguläre Dreieck mit den Ecken $1, \zeta_3, \zeta_3^2$ hat den Ursprung als Schwerpunkt.

- (c) Für $n = 18$ gilt

$$\min(\zeta_{18}) = X^6 - X^3 + 1.$$

Tatsächlich ist einerseits ζ_{18} eine Nullstelle von $X^6 - X^3 + 1$, denn

$$(\zeta_{18}^3)^2 - \zeta_{18}^3 + 1 = 0$$

folgt aus

$$(\zeta_{18}^3)^3 = \zeta_{18}^9 = -1, \quad \zeta_{18}^3 \neq -1$$

und aus der Faktorisierung $Y^3 + 1 = (Y + 1)(Y^2 - Y + 1)$ durch Einsetzen von $Y = \zeta_{18}^3$.

Wir müssen also noch die Irreduzibilität von $X^6 - X^3 + 1$ über $\mathbb{Q}$ zeigen. Um das Eisenstein-Kriterium anwenden zu können, verschieben wir wieder die Variable wie in Beispiel 4.9.3(b),

$$(X - 1)^6 - (X - 1)^3 + 1 = X^6 - 6X^5 + 15X^4 - 21X^3 + 18X^2 - 9X + 3.$$

Dieses Polynom ist nach dem Eisenstein-Kriterium für $p = 3$ irreduzibel über $\mathbb{Q}$. Da die Substitution $X \mapsto X - 1$ die Irreduzibilität erhält, ist also auch $X^6 - X^3 + 1$ irreduzibel über $\mathbb{Q}$.

$$\begin{array}{r}
X^3 \qquad \qquad \qquad -3X \qquad \qquad \qquad +1 \quad : (X - a) = X^2 + aX + (a^2 - 3) \\
\hline
-(X^3 - aX^2) \\
\hline
aX^2 \qquad \qquad \qquad -3X \qquad \qquad \qquad +1 \\
\hline
-(aX^2 - a^2X) \\
\hline
(a^2 - 3)X \qquad \qquad \qquad +1 \\
\hline
-((a^2 - 3)X - a(a^2 - 3)) \\
\hline
a^3 - 3a + 1 = 0
\end{array}$$

Abbildung 19: Zu Beispiel 5.4.1(a): Polynomdivision von $X^3 - 3X + 1$ durch $X - a$ in $L[X]$. Der Rest verschwindet wegen $a^3 - 3a + 1 = 0$.

- (d) Für alle $n \leq 104$ hat $\min(\zeta_n)$ nur Koeffizienten aus $\{-1, 0, 1\}$. Aber bei $n = 105$ tritt zum ersten Mal ein Koeffizient -2 auf!

5.4 Zerfällungskörper

Wenn man den formalen Quotienten $K[X]/(f)$ bildet, um eine Nullstelle von f zu “adjungieren”, dann kann f in der Erweiterung bereits in Linearfaktoren zerfallen, muss aber nicht. Die folgenden Beispiele zeigen beide Verhaltensweisen über $\mathbb{Q}$.

5.4.1 Beispiel. (a) Wir betrachten zunächst den Körper

$$L := \mathbb{Q}[T]/(T^3 - 3T + 1),$$

aus Beispiel 5.2.8(b) und schreiben

$$a := T + (T^3 - 3T + 1) \in L.$$

Dann gilt $a^3 - 3a + 1 = 0$ nach Lemma 5.2.9, also hat das Polynom

$$X^3 - 3X + 1 \in \mathbb{Q}[X]$$

in L die Nullstelle a . Hier verwenden wir bewusst zwei verschiedene Variablennamen: T für die Konstruktion des Restklassenrings und X für das Polynom, das wir anschließend über L faktorisieren.

Tatsächlich zerfällt $X^3 - 3X + 1$ als Element von $L[X]$ bereits vollständig in Linearfaktoren. Denn zunächst erhält man durch Polynomdivision (Abbildung 19), dass

$$X^3 - 3X + 1 = (X - a)(X^2 + aX + (a^2 - 3)).$$

Jetzt ist erstmal unklar, ob der zweite Faktor noch weiter zerfällt. Durch quadratische Ergänzung kann man aber sehen, dass dieser Term weiter zerfällt, weil

$$\begin{aligned}
X^2 + aX + (a^2 - 3) &= \left(X + \frac{a}{2}\right)^2 - \left(3 - \frac{3}{4}a^2\right) \\
&= \left(X + \frac{a}{2}\right)^2 - \left(a^2 + \frac{a}{2} - 2\right)^2,
\end{aligned}$$

wobei der wesentliche Schritt der zweite ist, also die Feststellung, dass $3 - \frac{3}{4}a^2$ ein Quadrat in L ist. Daher sind die beiden Nullstellen gegeben durch

$$-\frac{a}{2} \pm \sqrt{3 - \frac{3}{4}a^2} = -\frac{a}{2} \pm \left(a^2 + \frac{a}{2} - 2\right) = \begin{cases} a^2 - 2, \\ -a^2 - a + 2. \end{cases}$$

Somit hat unser ursprüngliches Polynom in L noch die weiteren Nullstellen

$$a^2 - 2, \quad -a^2 - a + 2,$$

und es zerfällt daher vollständig in $L[X]$ in Linearfaktoren:

$$\begin{aligned} X^3 - 3X + 1 &= (X - a) \\ &\quad \cdot (X - (a^2 - 2)) \\ &\quad \cdot (X - (-a^2 - a + 2)). \end{aligned}$$

(b) Für das Polynom $X^3 - 2$ passiert dies dagegen nicht. Setze

$$M := \mathbb{Q}[T]/(T^3 - 2), \quad b := T + (T^3 - 2) \in M.$$

Dann bekommt man durch Polynomdivision

$$X^3 - 2 = (X - b)(X^2 + bX + b^2)$$

in $M[X]$, aber der quadratische Faktor zerfällt *nicht* weiter über M . Um dies zu sehen, identifizieren wir M nach Satz 5.3.9 mit $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, was wegen der Irreduzibilität von $T^3 - 2$ in $\mathbb{Q}[T]$ (Beispiel 4.9.3) möglich ist. Die beiden weiteren komplexen Nullstellen von $X^3 - 2$ sind

$$\omega \sqrt[3]{2}, \quad \omega^2 \sqrt[3]{2},$$

wobei $\omega := e^{2\pi i/3}$ eine primitive dritte Einheitswurzel ist. Diese beiden Nullstellen sind nicht reell und können daher nicht in $M \subseteq \mathbb{R}$ liegen. Somit zerfällt $X^3 - 2$ in $M[X]$ nicht vollständig in Linearfaktoren.

Das unterschiedliche Verhalten der beiden Polynome in den obigen Beispielen wird auch durch die folgende Definition abstrakt erfasst.

5.4.2 Definition. Eine Erweiterung L/K heißt **Zerfällungskörper** eines Polynoms $f \in K[X] \setminus \{0\}$, falls f in $L[X]$ vollständig in Linearfaktoren zerfällt,

$$f = c \prod_{i=1}^n (X - a_i) \quad \text{mit } c \in K, a_i \in L,$$

und $L = K[a_1, \dots, a_n]$ gilt.

Dabei ist $K[a_1, \dots, a_n]$ automatisch bereits ein Körper: jedes a_j ist algebraisch über K , und daher auch über dem Körper $K[a_1, \dots, a_{j-1}]$, so dass

$$K[a_1, \dots, a_j] = K[a_1, \dots, a_{j-1}][a_j]$$

nach Satz 5.3.9 wieder ein Körper ist.

5.4.3 Beispiel. (a) Für $L = \mathbb{Q}[T]/(T^3 - 3T + 1)$ aus Beispiel 5.4.1(a) ist L ein Zerfällungskörper von $X^3 - 3X + 1$, weil dieses Polynom in $L[X]$ vollständig in Linearfaktoren zerfällt, und weil L bereits von der einzelnen Nullstelle a erzeugt wird, zum Beispiel weil ja $\{1, a, a^2\}$ eine Basis von L über $\mathbb{Q}$ bildet.

(b) Für $M = \mathbb{Q}[T]/(T^3 - 2) \cong \mathbb{Q}[\sqrt[3]{2}]$ aus Beispiel 5.4.1(b) ist M *kein* Zerfällungskörper von $X^3 - 2$, weil dieses Polynom in $M[X]$ nicht vollständig in Linearfaktoren zerfällt, wie wir gesehen haben.

Ein Zerfällungskörper von $X^3 - 2$ als Unterkörper von $\mathbb{C}$ ist

$$\mathbb{Q}[\sqrt[3]{2}, \omega],$$

wobei $\omega := e^{2\pi i/3}$ eine primitive dritte Einheitswurzel ist. Denn in diesem Körper gilt

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \omega \sqrt[3]{2})(X - \omega^2 \sqrt[3]{2}),$$

und der Körper wird von diesen Nullstellen über $\mathbb{Q}$ erzeugt.

Unser Ziel wird jetzt sein, zu zeigen, dass jedes Polynom $f \in K[X]$ einen Zerfällungskörper besitzt, und dass dieser bis auf Isomorphismus eindeutig ist. Für letzteres präzisieren wir erst, was damit gemeint ist.

5.4.4 Definition. Für Körpererweiterungen L/K und M/K ist ein K -**Homomorphismus** ein Ringhomomorphismus $\sigma : L \rightarrow M$, der die Elemente von K festhält, also $\sigma(a) = a$ für alle $a \in K$.

Äquivalent kann man $\sigma(a) = a$ für alle $a \in K$ auch als Kommutativität des Diagramms

$$\begin{array}{ccc} & K & \\ \swarrow & & \searrow \\ L & \xrightarrow{\sigma} & M \end{array}$$

ausdrücken. Ein K -Isomorphismus ist dementsprechend ein K -Homomorphismus, der bijektiv ist. Wie schon bei Gruppenhomomorphismen und Ringhomomorphismen allgemein überlegt man sich leicht, dass damit auch der inverse Homomorphismus ein K -Homomorphismus ist.

5.4.5 Beispiel. (a) Der Isomorphismus zwischen $\mathbb{R}[X]/(X^2 + 1)$ und $\mathbb{C}$ aus (4.15) ist ein $\mathbb{R}$ -Isomorphismus, weil er die Elemente von $\mathbb{R}$ festhält.

(b) Der Isomorphismus $K[X]/(\min(a)) \cong K[a]$ aus Satz 5.3.9 ist ein K -Isomorphismus, weil er die Elemente von K festhält.

(c) Sei $\varphi : K \rightarrow L$ ein beliebiger Ringhomomorphismus zwischen zwei Körpern. Einen solchen kann es nur geben falls

$$\text{char}(K) = \text{char}(L).$$

Denn aufgrund der Injektivität von φ und $\varphi(1) = 1$ gilt $1 + \dots + 1 = 0$ in K genau dann, wenn $1 + \dots + 1 = 0$ in L gilt.

Jetzt können wir feststellen:

- ▷ Falls beide Körper Charakteristik 0 haben, dann ist $\mathbb{Q}$ sowohl in K als auch in L enthalten, und φ muss die Elemente von $\mathbb{Q}$ festhalten, weil es die Elemente von $\mathbb{Z}$ festhält. Also ist φ automatisch ein $\mathbb{Q}$ -Homomorphismus,
- ▷ Falls beide Körper Charakteristik $p > 0$ haben, dann ist $\mathbb{F}_p$ sowohl in K als auch in L enthalten, und φ ist analog automatisch ein $\mathbb{F}_p$ -Homomorphismus.

5.4.6 Bemerkung. Die Oberkörper L und M sind nach Bemerkung 5.2.3 ja automatisch K -Vektorräume. Bezüglich dieser Vektorraumstruktur ist jeder K -Homomorphismus $\varphi : L \rightarrow M$ automatisch K -linear, weil für $a \in K$ und $x \in L$ gilt

$$\varphi(ax) = \varphi(a)\varphi(x) = a\varphi(x),$$

und weil φ als Ringhomomorphismus ohnehin additiv ist. Diese K -Linearität von K -Homomorphismen wird bei zukünftigen Beweisen eine wichtige Rolle spielen, wo wir dann entsprechend Methoden aus der linearen Algebra verwenden können.

5.4.7 Lemma. Sei $\varphi : L \rightarrow M$ ein K -Homomorphismus und $f \in K[X]$ ein Polynom. Dann bildet φ die Nullstellen von f in L auf Nullstellen von f in M ab.

Beweis. Sei

$$f = c_n X^n + \dots + c_1 X + c_0$$

und $a \in L$ eine Nullstelle von f , also $f(a) = 0$. Dann gilt

$$\begin{aligned} f(\varphi(a)) &= c_n \varphi(a)^n + \dots + c_1 \varphi(a) + c_0 \\ &= c_n \varphi(a^n) + \dots + c_1 \varphi(a) + c_0 \\ &= \varphi(c_n a^n + \dots + c_1 a + c_0) \\ &= \varphi(f(a)) \\ &= \varphi(0) \\ &= 0, \end{aligned} \tag{5.12}$$

wobei wir im ersten Schritt die Exponenten durch die Multiplikativität von φ hineinziehen und im zweiten Schritt die K -Linearität von φ verwenden. Also ist $\varphi(a)$ eine Nullstelle von f in M . $\square$

5.4.8 Lemma. Sei L/K beliebig und $g \in K[X]$ irreduzibel. Dann gibt es eine Bijektion zwischen den K -Homomorphismen $\varphi : K[X]/(g) \rightarrow L$ und den Nullstellen von g in L , gegeben durch

$$\varphi \mapsto \varphi(X + (g)).$$

Dass wir Homomorphismen über K betrachten, bedeutet also dass das Diagramm

$$\begin{array}{ccc} & K & \\ \swarrow & & \searrow \\ K[X]/(g) & \xrightarrow{\varphi} & L \end{array}$$

kommutiert, so dass φ die Elemente von K festhält.

Beweis. Weil $X + (g)$ eine Nullstelle von g in $K[X]/(g)$ ist, folgt aus Lemma 5.4.7, dass $\varphi(X + (g))$ tatsächlich eine Nullstelle von g in L ist.

Für die Injektivität seien $\varphi, \sigma : K[X]/(g) \rightarrow L$ zwei Homomorphismen über K mit $\varphi(X + (g)) = \sigma(X + (g))$. Wie in (5.12) gilt dann für jedes $f \in K[X]$

$$\varphi(f + (g)) = f(\varphi(X + (g))) = f(\sigma(X + (g))) = \sigma(f + (g)).$$

Also muss $\varphi = \sigma$ der Fall sein, so dass die Konstruktion tatsächlich injektiv ist.

Für die Surjektivität sei $a \in L$ eine Nullstelle von g . Definiere $\varphi : K[X]/(g) \rightarrow L$ durch

$$\varphi(f + (g)) := f(a).$$

Dies ist nach der Abbildungseigenschaft von Restklassenringen (Lemma 4.3.16) und der Annahme $g(a) = 0$ wohldefiniert und ein Homomorphismus. Falls f ein konstantes Polynom ist, dann bildet φ es auch auf das entsprechende Element von $K \subseteq L$ ab, so dass φ ein Homomorphismus über K ist. Es ist klar, dass in der Tat $\varphi(X + (g)) = a$ gilt. $\square$

5.4.9 Satz. Für jedes Polynom $f \in K[X] \setminus \{0\}$ über einem Körper K existiert ein Zerfällungskörper. Dieser ist eindeutig bis auf Isomorphismus von Erweiterungen von K .

Ab hier werden die Beweise nur noch teilweise besprochen

Beweis. Falls $\deg(f) \leq 1$, dann ist f bereits ein Produkt von Linearfaktoren, also K selbst ein Zerfällungskörper von f .

Allgemein verwenden wir Induktion über $\deg(f)$. Für den Induktionsschritt sei also $\deg(f) > 1$. Falls f bereits über K vollständig in Linearfaktoren zerfällt, dann sind wir wieder fertig. Andernfalls hat f einen irreduziblen Faktor $g \in K[X]$ vom Grad ≥ 2 . Nach Satz 5.2.7 ist

$$L := K[T]/(g(T))$$

eine Körpererweiterung von K , und für $a_1 := T + (g(T)) \in L$ gilt $g(a_1) = 0$ nach Lemma 5.2.9. Wegen $g \mid f$ gilt also auch $f(a_1) = 0$. Somit können wir f in $L[X]$ in der Form

$$f = (X - a_1)h$$

mit einem Polynom $h \in L[X]$ schreiben. Nach Induktionsannahme besitzt h einen Zerfällungskörper M/L . Dann zerfällt auch f über M vollständig in Linearfaktoren.

Sind $a_2, \dots, a_n \in M$ die Nullstellen von h , dann ist

$$M = L[a_2, \dots, a_n] = K[a_1, a_2, \dots, a_n].$$

Also ist M/K ein Zerfällungskörper von f .

Nun zur Eindeutigkeit. Wir verwenden Induktion über $\deg(f)$, um die folgende allgemeinere Aussage zu zeigen:

- ▷ Ist $\tau : K \rightarrow K'$ ein Isomorphismus von Körpern, L/K ein Zerfällungskörper eines Polynoms $f \in K[X] \setminus \{0\}$ und L'/K' ein Zerfällungskörper von $\tau(f)$, dann gibt es einen Isomorphismus $\sigma : L \rightarrow L'$, so dass das Diagramm

$$\begin{array}{ccc} K & \xrightarrow{\tau} & K' \\ \downarrow & & \downarrow \\ L & \xrightarrow{\sigma} & L' \end{array} \quad (5.13)$$

kommutiert, also so dass σ die Elemente von K gemäß τ abbildet.

Hierbei ist mit $\tau(f) \in K'[X]$ das Polynom gemeint, das man durch Anwenden von τ auf die Koeffizienten von f erhält. Die im Satz behauptete Eindeutigkeit ist der Spezialfall $K' = K$ und $\tau = \text{id}_K$. Der Grund dafür, dass wir die Aussage in dieser allgemeineren Form zeigen, ist, dass so der Induktionsbeweis über $\deg(f)$ durchführbar wird: wir haben zwar eine stärkere Aussage zu zeigen, können dafür aber auch eine stärkere Induktionsannahme verwenden.

Induktionsanfang: falls $\deg(f) \leq 1$, dann sind die Zerfällungskörper gleich den Grundkörpern, und wir können $\sigma = \tau$ verwenden.

Induktionsschritt: Sei jetzt also $\deg(f) > 1$. Betrachten wir zunächst den Fall, dass f irreduzibel ist. Dann sei $a \in L$ eine beliebige Nullstelle von f und $b \in L'$ eine Nullstelle von $\tau(f)$. Wenn wir oBdA annehmen, dass der Leitkoeffizient von f gleich 1 ist, dann gilt aufgrund der Irreduzibilität von f über K also $f = \min(a)$. Analog erhalten wir $\tau(f) = \min(b)$. Wir betrachten dann das Diagramm

$$\begin{array}{ccccccc} K & \xlongequal{\quad} & K & \xrightarrow{\tau} & K' & \xlongequal{\quad} & K' \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ K[a] & \xleftarrow{\cong} & K[X]/(f) & \xrightarrow{\cong} & K'[X]/(\tau(f)) & \xrightarrow{\cong} & K'[b] \end{array}$$

Hierbei ergeben sich die Isomorphismen unten links und unten rechts aus Satz 5.3.9. Sei $\lambda : K[a] \rightarrow K'[b]$ der Isomorphismus, der sich aus der Verknüpfung der drei unteren Isomorphismen ergibt.

Durch Polynomdivision erhalten wir

$$f = (X - a) \cdot g$$

mit $g \in K[a][X]$. Da L/K ein Zerfällungskörper von f ist, folgt, dass $L/K[a]$ ein Zerfällungskörper von g ist. Weil λ eine Fortsetzung von τ ist, gilt

$$\tau(f) = (X - b) \cdot \lambda(g),$$

und $L'/K'[b]$ ist ein Zerfällungskörper von $\lambda(g)$. Weil $\deg(g) < \deg(f)$ gilt, können wir die Induktionsannahme auf diese beiden Zerfällungskörper anwenden, und erhalten so einen Isomorphismus $\sigma : L \rightarrow L'$, so dass das Diagramm

$$\begin{array}{ccc} K[a] & \xrightarrow{\lambda} & K'[b] \\ \downarrow & & \downarrow \\ L & \xrightarrow{\sigma} & L' \end{array}$$

kommutiert. Durch Kombination der beiden Diagramme ergibt sich dann das gewünschte kommutative Diagramm

$$\begin{array}{ccc} K & \xrightarrow{\tau} & K' \\ \downarrow & & \downarrow \\ K[a] & \xrightarrow{\lambda} & K'[b] \\ \downarrow & & \downarrow \\ L & \xrightarrow{\sigma} & L' \end{array}$$

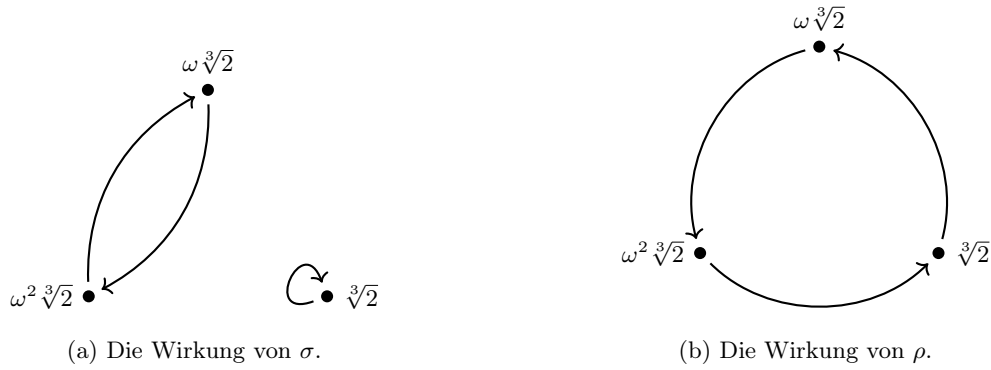


Abbildung 20: Wirkung der Elemente $\sigma, \rho \in \text{Gal}(\mathbb{Q}[\sqrt[3]{2}, \omega]/\mathbb{Q})$ aus (5.15) auf die Nullstellen von $X^3 - 2$.

Insbesondere setzt σ auch τ fort, womit der irreduzible Fall erledigt ist.

Es bleibt der Fall, dass f nicht irreduzibel ist. Dann können wir

$$f = f_1 f_2$$

mit Polynomen $f_1, f_2 \in K[X]$ schreiben, für die

$$0 < \deg(f_1), \deg(f_2) < \deg(f)$$

gilt. Sei $E \subseteq L$ der von den Nullstellen von f_1 erzeugte Körper über K . Dann ist E/K ein Zerfällungskörper von f_1 . Analog sei $E' \subseteq L'$ der von den Nullstellen von $\tau(f_1)$ erzeugte Körper über K' . Dann ist E'/K' ein Zerfällungskörper von $\tau(f_1)$. Nach Induktionsannahme gibt es also einen Isomorphismus $\lambda : E \rightarrow E'$, der τ fortsetzt.

Nun ist L/E ein Zerfällungskörper von f_2 , denn L wird über K von den Nullstellen von $f = f_1 f_2$ erzeugt, und die Nullstellen von f_1 liegen bereits in E . Ebenso ist L'/E' ein Zerfällungskörper von $\tau(f_2)$. Da λ die Abbildung τ fortsetzt, gilt $\lambda(f_2) = \tau(f_2)$. Wir können daher die Induktionsannahme ein zweites Mal anwenden, diesmal auf den Isomorphismus $\lambda : E \rightarrow E'$ und das Polynom $f_2 \in E[X]$. Dadurch erhalten wir einen Isomorphismus $\sigma : L \rightarrow L'$, der λ fortsetzt. Insbesondere setzt σ auch τ fort, womit auch dieser Fall erledigt ist. $\square$

5.4.10 Bemerkung. Zerfällungskörper sind insbesondere dann von Interesse, falls das Polynom f irreduzibel ist. Aber sowohl die Definition als auch der Beweis von Satz 5.4.9 brauchen die Irreduzibilität von f nicht.

5.5 Galoisgruppen und Fixkörper

Wir kommen jetzt zur Untersuchung der Symmetrien von Körpererweiterungen. Dies wird uns stärkere Ergebnisse über die Struktur von Körpererweiterungen liefern und tiefgreifende Anwendungen ermöglichen.

5.5.1 Definition. Die **Galoisgruppe** einer Erweiterung L/K ist

$$\text{Gal}(L/K) := \{K\text{-Isomorphismen } \sigma : L \rightarrow L\},$$

betrachtet als Gruppe bezüglich der Hintereinanderausführung von Funktionen.

Weil $\sigma : L \rightarrow L$ den Körper L auf sich selber abbildet, sprechen wir auch von **K -Automorphismen** von L .

5.5.2 Beispiel. (a) Für jede Erweiterung L/K ist $\text{id}_L \in \text{Gal}(L/K)$. Falls $L = K$ gilt, dann ist dies der einzige K -Automorphismus, also

$$\text{Gal}(K/K) = \{\text{id}_K\}.$$

- (b) Für die Erweiterung $\mathbb{C}/\mathbb{R}$ gibt es genau zwei $\mathbb{R}$ -Automorphismen, nämlich $\text{id}_{\mathbb{C}}$ und die komplexe Konjugation $\sigma : z \mapsto \bar{z}$. Also gilt

$$\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}_{\mathbb{C}}, \sigma\} \cong \mathbb{Z}_2.$$

Der Grund ist, dass ein $\mathbb{R}$ -Automorphismus insbesondere $\mathbb{R}$ -linear ist und i auf eine Nullstelle von $X^2 + 1$ schicken muss. Also kann i nur auf i oder auf $-i$ abgebildet werden. Zusammen mit $1 \mapsto 1$ und der $\mathbb{R}$ -Linearität ergibt sich dann die Behauptung.

- (c) Sei $D \in \mathbb{Z} \setminus \{0, \pm 1\}$ quadratfrei. Für die quadratische Erweiterung $\mathbb{Q}[\sqrt{D}]/\mathbb{Q}$ gilt analog

$$\text{Gal}(\mathbb{Q}[\sqrt{D}]/\mathbb{Q}) = \{\text{id}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z},$$

wobei

$$\sigma(r + s\sqrt{D}) = r - s\sqrt{D}$$

für $r, s \in \mathbb{Q}$ gilt. Ein $\mathbb{Q}$ -Automorphismus muss nämlich $\sqrt{D}$ auf eine Nullstelle von $X^2 - D$ abbilden, also auf $\sqrt{D}$ oder $-\sqrt{D}$, und ist dann wegen $\mathbb{Q}$ -Linearität eindeutig festgelegt.

- (d) Die Erweiterung $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ aus Beispiel 5.4.1(b) dagegen hat triviale Galoisgruppe, also

$$\text{Gal}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = \{\text{id}\}.$$

Denn ein $\mathbb{Q}$ -Automorphismus von L muss $\sqrt[3]{2}$ auf eine Nullstelle von $X^3 - 2$ in $\mathbb{Q}[\sqrt[3]{2}]$ abbilden. Wie wir in Beispiel 5.4.1(b) gesehen haben, ist $\sqrt[3]{2}$ aber die einzige solche Nullstelle in $\mathbb{Q}[\sqrt[3]{2}]$. Also wird $\sqrt[3]{2}$ festgehalten, und damit auch ganz $\mathbb{Q}[\sqrt[3]{2}]$.

- (e) Der Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$ ist nach Beispiel 5.4.3

$$L = \mathbb{Q}[\sqrt[3]{2}, \omega],$$

wobei ω eine primitive dritte Einheitswurzel ist. Ein $\mathbb{Q}$ -Automorphismus von L muss $\sqrt[3]{2}$ auf eine der drei Nullstellen

$$\sqrt[3]{2}, \quad \omega\sqrt[3]{2}, \quad \omega^2\sqrt[3]{2} \tag{5.14}$$

von $X^3 - 2$ abbilden, und ω auf eine der beiden primitiven dritten Einheitswurzeln ω oder ω^2 . Um zu sehen, dass diese Möglichkeiten tatsächlich vorkommen, betrachten wir die beiden Abbildungen $\rho, \sigma : L \rightarrow L$, die durch

$$\begin{aligned} \sigma(\sqrt[3]{2}) &= \sqrt[3]{2}, & \sigma(\omega) &= \omega^2, \\ \rho(\sqrt[3]{2}) &= \omega\sqrt[3]{2}, & \rho(\omega) &= \omega \end{aligned} \tag{5.15}$$

bereits festgelegt sind, weil sie sich durch Multiplikativität und $\mathbb{Q}$ -Linearität auf ganz L eindeutig fortsetzen.

Die Abbildung σ ist gerade die Einschränkung der komplexen Konjugation auf L , denn $\sqrt[3]{2}$ ist reell und $\bar{\omega} = \omega^2$. Damit ist klar, dass σ tatsächlich ein $\mathbb{Q}$ -Automorphismus von L ist. Dass ρ ein $\mathbb{Q}$ -Automorphismus von L ist, sieht man zum Beispiel dadurch, dass man seine Werte auf der $\mathbb{Q}$ -Basis⁴¹

$$\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{2}^2\}$$

ausrechnet und dann auf allen Paaren von Basisvektoren überprüft, dass die Multiplikation erhalten bleibt. Dann folgt die Erhaltung der Multiplikation allgemein aus der $\mathbb{Q}$ -Linearität von ρ und der $\mathbb{Q}$ -Bilinearität der Multiplikation in L .

In Abbildung 20 ist die Wirkung von σ und ρ auf den drei Nullstellen von $X^3 - 2$ dargestellt. Weil diese beiden Permutationen die symmetrische Gruppe S_3 der Permutationen der drei Nullstellen (5.14) erzeugen (siehe Beispiel 2.2.14), erhalten wir, dass die Galoisgruppe mit der symmetrischen Gruppe S_3 übereinstimmt, also

$$\text{Gal}(L/\mathbb{Q}) \cong S_3.$$

⁴¹Denn $X^3 - 2$ ist irreduzibel über $\mathbb{Q}$, also ist $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ eine $\mathbb{Q}$ -Basis von $\mathbb{Q}[\sqrt[3]{2}]$. Außerdem ist $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$, aber $\omega \notin \mathbb{R}$, also ist $X^2 + X + 1$ über $\mathbb{Q}[\sqrt[3]{2}]$ irreduzibel und $\{1, \omega\}$ eine Basis von L über $\mathbb{Q}[\sqrt[3]{2}]$. Zusammensetzen dieser beiden Basen wie im Beweis von Satz 5.2.11 liefert die angegebene Basis.

Am Schluss haben wir dabei bereits die folgende Beobachtung verwendet.

5.5.3 Lemma. *Sei L/K Zerfällungskörper eines Polynoms $f \in K[X] \setminus \{0\}$ mit Nullstellen $a_1, \dots, a_n \in L$. Dann permutiert jedes $\sigma \in \text{Gal}(L/K)$ diese Nullstellen, und dies induziert einen Homomorphismus*

$$\text{Gal}(L/K) \hookrightarrow S_n,$$

wodurch $\text{Gal}(L/K)$ zu einer Untergruppe der symmetrischen Gruppe S_n der Permutationen von n Elementen wird.

Hierbei werden die Nullstellen $a_1, \dots, a_n$ *ohne* Wiederholung betrachtet, d.h. dass jede mehrfache Nullstelle nur einmal vorkommt. In der Terminologie von Abschnitt 2.4 können wir auch sagen, dass $\text{Gal}(L/K)$ auf der Menge der Nullstellen *wirkt*. In dieser Situation nennt man $\text{Gal}(L/K)$ auch die **Galoisgruppe von f** .

Beweis. Nach Lemma 5.4.7 bildet jedes $\sigma \in \text{Gal}(L/K)$ Nullstellen von f wieder auf Nullstellen von f ab. Also induziert σ eine Abbildung

$$\{a_1, \dots, a_n\} \longrightarrow \{a_1, \dots, a_n\}.$$

Dieselbe Aussage gilt aber auch für σ^{-1} . Daher ist diese Abbildung bijektiv, also eine Permutation der Nullstellen.

Da L/K ein Zerfällungskörper von f ist, wird L von diesen Nullstellen erzeugt:

$$L = K[a_1, \dots, a_n].$$

Jedes Element von L lässt sich also als Polynom in $a_1, \dots, a_n$ mit Koeffizienten in K schreiben. Wenn zwei K -Automorphismen von L auf allen Nullstellen a_i übereinstimmen, dann stimmen sie deshalb auf jedem solchen Polynom überein. Also stimmen sie auf ganz L überein. Die Zuordnung

$$\text{Gal}(L/K) \longrightarrow S_n, \quad \sigma \longmapsto \sigma|_{\{a_1, \dots, a_n\}},$$

ist daher injektiv. Sie ist außerdem ein Gruppenhomomorphismus, denn die Wirkung von $\sigma \circ \tau$ auf die Nullstellen ist die Hintereinanderausführung der Wirkungen von τ und σ . $\square$

Wir betrachten ein weiteres instruktives Beispiel, welches die Diskussion zu Beginn des Kapitels und Beispiele 5.2.12 und 5.3.11 weiterführt.

5.5.4 Beispiel. Wie wir bereits wissen, ist

$$f = X^4 - 10X^2 + 1$$

das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$, wobei (5.3) die Faktorisierung in Linearfaktoren über $\mathbb{C}$ ist, und es gilt

$$\mathbb{Q}[\sqrt{2} + \sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}].$$

Insbesondere ist also $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ ein Zerfällungskörper von f über $\mathbb{Q}$.

Was ist jetzt die Galoisgruppe von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ über $\mathbb{Q}$? Nach Lemma 5.5.3 können wir sie als Untergruppe der Permutationen der vier Nullstellen $\pm\sqrt{2} \pm \sqrt{3}$ auffassen. Andererseits muss ein $\mathbb{Q}$ -Automorphismus von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ die beiden Nullstellen von $X^2 - 2$ aufeinander abbilden, und analog mit den Nullstellen von $X^2 - 3$. Deshalb muss es Vorzeichen $v, w \in \{\pm 1\}$ geben, so dass ein $\mathbb{Q}$ -Automorphismus $\sigma : \mathbb{Q}[\sqrt{2}, \sqrt{3}] \rightarrow \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ die Gleichungen

$$\sigma(\sqrt{2}) = v\sqrt{2}, \quad \sigma(\sqrt{3}) = w\sqrt{3}$$

erfüllt. Außerdem ist klar, dass σ dadurch eindeutig durch diese Gleichungen sowie Additivität und Multiplikativität bestimmt ist. Umgekehrt definiert jede Wahl von v und w tatsächlich einen $\mathbb{Q}$ -Automorphismus von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, der auf den Basisvektoren $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2 \cdot 3}\}$ durch

$$1 \mapsto 1, \quad \sqrt{2} \mapsto v\sqrt{2}, \quad \sqrt{3} \mapsto w\sqrt{3}, \quad \sqrt{2 \cdot 3} \mapsto vw\sqrt{2 \cdot 3}$$

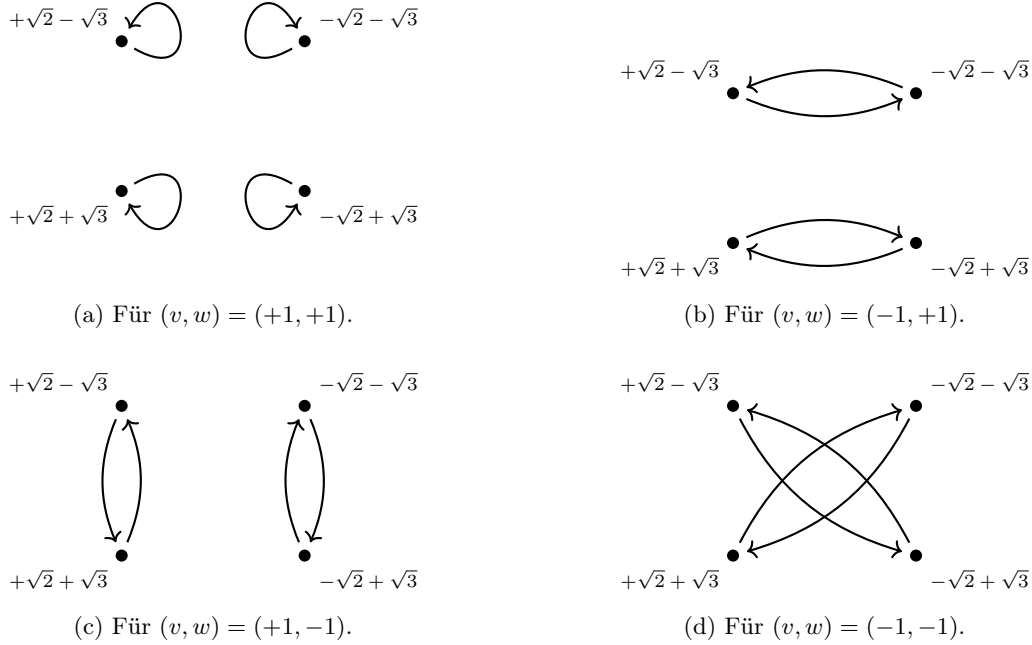


Abbildung 21: Wirkung der vier Elemente von $\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ auf die Nullstellen von $X^4 - 10X^2 + 1$.

definiert ist. Diese Abbildung erhält in der Tat die Multiplikation, wie man direkt nachrechnen kann.⁴² Somit besteht die Galoisgruppe genau aus den vier Automorphismen, deren Wirkung auf die Nullstellen von f in Abbildung 21 dargestellt ist.

Wenn man zwei solche Automorphismen mit den Vorzeichen (v, w) und (v', w') hintereinander ausführt, dann multiplizieren sich die Vorzeichen komponentenweise. Daher können wir die Galoisgruppe identifizieren mit

$$\text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Siehe hierzu auch die Gruppe V_4 aus Beispiel 2.5.2.

Wir haben Beispiele gesehen, wo die Anzahl der Elemente der Galoisgruppe $\text{Gal}(L/K)$ mit dem Grad $[L : K]$ übereinstimmt, und Beispiele wo sie kleiner ist. Die folgende Aussage zeigt, dass die Galoisgruppe nicht größer sein kann als der Grad.

5.5.5 Satz. (a) Die Teilmenge

$$\text{Gal}(L/K) \subseteq \text{Lin}_K(L, L)$$

ist linear unabhängig über L .

(b) Falls L/K endlich ist, gilt

$$|\text{Gal}(L/K)| \leq [L : K]. \quad (5.16)$$

Mit $\text{Lin}_K(L, L)$ bezeichnen wir hier die Menge aller K -linearen Abbildungen von L nach L . Diese ist bezüglich der punktweisen Addition und skalaren Multiplikation ein L -Vektorraum, und auf diese Vektorraumstruktur bezieht sich die lineare Unabhängigkeit.⁴³

Beweis. (a) Seien $\sigma_1, \dots, \sigma_m \in \text{Gal}(L/K)$ paarweise verschieden, und angenommen, es gibt eine lineare Gleichung

$$c_1\sigma_1 + \dots + c_m\sigma_m = 0$$

⁴²Aufgrund der $\mathbb{Q}$ -Linearität von σ und der Bilinearität der Multiplikation reicht es, dies auf allen Paaren von Basisvektoren nachzurechnen.

⁴³Siehe auch den folgenden Beweis zum besseren Verständnis.

mit Koeffizienten $c_i \in L$, die nicht alle null sind. Unter allen solchen Gleichungen wählen wir eine mit minimalem m . Dann ist $c_i \neq 0$ für alle i , denn sonst könnten wir einen Summanden weglassen und hätten eine lineare Gleichung mit weniger als m Summanden.

Der Raum aller solcher Koeffizienten $c = (c_1, \dots, c_m)$ ist ein L -Untervektorraum von L^m . Wir zeigen zunächst, dass dieser Untervektorraum eindimensional ist. Falls wir zwei linear unabhängige Koeffizientenvektoren c und d mit der obigen Eigenschaft hätten, dann könnten wir eine Linearkombination von c und d bilden, in der der Koeffizient von σ_m verschwindet. Damit hätten wir eine lineare Gleichung mit weniger als m Summanden, was der Minimalität von m widerspricht. Also ist der Untervektorraum eindimensional, d.h. die Koeffizienten c_i sind bis auf Skalierung durch ein Element von L eindeutig bestimmt.

Nach Voraussetzung gilt

$$c_1\sigma_1(x) + \dots + c_m\sigma_m(x) = 0 \quad \forall x \in L.$$

Wenn wir jetzt ein Produkt $ax \in L$ einsetzen und die Multiplikativität der σ_i verwenden, erhalten wir

$$c_1\sigma_1(a) \cdot \sigma_1(x) + \dots + c_m\sigma_m(a) \cdot \sigma_m(x) = 0 \quad \forall x \in L.$$

Nach der Eindeutigkeitsbetrachtung gibt es also ein $r_a \in L$ mit

$$c_i\sigma_i(a) = r_a c_i \quad \forall i.$$

Wegen $c_i \neq 0$ folgt

$$\sigma_i(a) = r_a \quad \forall i,$$

also insbesondere $\sigma_i(a) = \sigma_j(a)$ für alle i, j . Weil a beliebig war, folgt, dass $\sigma_1 = \dots = \sigma_m$ gilt. Da die σ_i paarweise verschieden waren, kann dies nur für $m = 1$ möglich sein. Dies ist aber auch unmöglich, denn dann würde direkt $c_1\sigma_1(1) = c_1 = 0$ folgen. Also kann es keine nichttriviale lineare Gleichung geben und die lineare Unabhängigkeit ist gezeigt.

(b) Es gilt

$$\dim_K(\text{Lin}_K(L, L)) = \dim_K(L)^2,$$

wie man zum Beispiel nach Wahl einer Basis in L sieht, welche die K -linearen Abbildungen mit den Matrizen der Größe $\dim_K(L) \times \dim_K(L)$ identifiziert. Wie im Beweis der Gradformel aus Satz 5.2.11 zeigt man jetzt, dass andererseits

$$\dim_K(\text{Lin}_K(L, L)) = \dim_L(\text{Lin}_K(L, L)) \cdot [L : K]$$

gilt.⁴⁴ Da per Definition ja aber $[L : K] = \dim_K(L)$ gilt, bekommen wir

$$\dim_L(\text{Lin}_K(L, L)) = [L : K].$$

Nach (a) folgt also $|\text{Gal}(L/K)| \leq [L : K]$. □

5.5.6 Definition. Sei L/K eine Körpererweiterung.

- (a) Ein **Zwischenkörper** von L/K ist eine Teilmenge $Z \subseteq L$ mit $K \subseteq Z$, die ebenfalls ein Körper ist.
- (b) Die Menge aller Zwischenkörper von L/K bezeichnen wir mit $\text{ZwiKö}(L/K)$, und wir betrachten sie als teilgeordnete Menge bezüglich der Inklusion.

5.5.7 Beispiel. (a) Die Erweiterung $\mathbb{C}/\mathbb{Q}$ hat sehr viele Zwischenkörper, und viele unserer Beispiele in diesem Kapitel gehören dazu, insbesondere $\mathbb{R}$, $\mathbb{Q}[\sqrt{D}]$, $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[\sqrt[3]{2}, \omega]$, etc.

- (b) $\mathbb{Q}[\sqrt[3]{2}]$ ist ein Zwischenkörper von $\mathbb{Q}[\sqrt[3]{2}, \omega]/\mathbb{Q}$.

⁴⁴Die allgemeine Aussage, welche sowohl den Beweis von Satz 5.2.11 als auch die jetzige Aussage verallgemeinert, ist die folgende: wenn man einen L -Vektorraum V als K -Vektorraum betrachtet indem man die skalare Multiplikation von L auf K einschränkt, dann gilt $\dim_K(V) = \dim_L(V) \cdot [L : K]$. Der Beweis ist genau wie in Satz 5.2.11.

(c) $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{Q}[\sqrt{3}]$ sind Zwischenkörper von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$.

Die wesentliche Beobachtung der **Galoistheorie**⁴⁵ ist folgende Beziehung zwischen Zwischenkörpern und Untergruppen der Galoisgruppe, die wir im Folgenden noch verfeinern werden. Wie in Beispiel 3.2.2(c) bezeichnen wir mit $\text{Sub}(G)$ für eine Gruppe G die Menge aller Untergruppen von G , teilgeordnet durch Inklusion.

5.5.8 Satz. *Es gibt einen Galois-Zusammenhang*

$$\begin{array}{ccc} & \text{Stab} & \\ \text{ZwiKö}(L/K) & \xrightarrow{\quad} & \text{Sub}(\text{Gal}(L/K))^{\text{op}} \\ & \xleftarrow{\quad \text{Fix} \quad} & \end{array} \quad (5.17)$$

wobei:

▷ Für einen Zwischenkörper F von L/K ist

$$\text{Stab}(F) := \{\sigma \in \text{Gal}(L/K) : \sigma(x) = x \text{ für alle } x \in F\}$$

die Untergruppe der Galoisgruppe, die alle Elemente von F festhält.

▷ Für eine Untergruppe $G \subseteq \text{Gal}(L/K)$ ist

$$\text{Fix}(G) := \{x \in L : \sigma(x) = x \text{ für alle } \sigma \in G\}$$

die Menge der Elemente von L , die von allen Elementen von G festgehalten werden.

Zum Verständnis der Aussage sei insbesondere an Beispiel 3.2.8 erinnert, welches eine ähnliche Aussage in einem einfacheren Kontext ist.

Beweis. Man rechnet leicht nach, dass $\text{Fix}(G)$ tatsächlich ein Zwischenkörper von L/K ist, d.h. abgeschlossen bezüglich Addition, Multiplikation und additiven sowie multiplikativen Inversen. Außerdem ist klar, dass $\text{Stab}(F)$ eine Untergruppe von $\text{Gal}(L/K)$ ist, denn die Identität hält alle Elemente von F fest, und wenn σ und τ alle Elemente von F festhalten, dann ist dies auch für $\sigma \circ \tau$ und σ^{-1} der Fall.

Für den Galois-Zusammenhang müssen wir jetzt zeigen, dass für alle $F \in \text{ZwiKö}(L/K)$ und $G \in \text{Sub}(\text{Gal}(L/K))$ gilt, dass

$$G \subseteq \text{Stab}(F) \iff F \subseteq \text{Fix}(G).$$

Das ist aber wie im Beweis von Beispiel 3.2.8 ganz klar, denn beide Seiten sind äquivalent zu der Aussage, dass jedes $\sigma \in G$ alle Elemente von F festhält. $\square$

5.5.9 Bemerkung. (a) Die Abbildung Stab kann man auch mit $F \mapsto \text{Gal}(L/F)$ identifizieren.

(b) Den Galois-Zusammenhang aus Satz 5.5.8 kann man auf ganz ähnliche Weise für praktisch alle mathematischen Strukturen betrachten: jedes mathematische Objekt hat eine gewisse Symmetriegruppe, jede Untergruppe dieser Symmetriegruppe definiert ein gewisses Unterobjekt bestehend aus der Menge der Fixpunkte, und umgekehrt hat jedes Unterobjekt einen Stabilisator. Mit dem gleichen Argument wie oben folgt dann, dass man es mit einem Galois-Zusammenhang zu tun hat.

In der Körpertheorie ist diese Methode jedoch besonders fruchtbar, unter anderem durch die Verbindung zwischen den Symmetriegruppen und den Permutationen der Nullstellen von Polynomen (Lemma 5.5.3).

Bevor wir zu den Beispielen kommen, lohnt es sich, allgemeine Eigenschaften des Galois-Zusammenhangs genauer zu untersuchen.

⁴⁵Benannt nach ihrem Begründer Évariste Galois (1811–1832), der die Theorie in seiner Jugend entwickelte (teilweise als politischer Gefangener) und bei einem Duell ums Leben kam.

5.5.10 Lemma. Sei L/K eine endliche Erweiterung und $G \subseteq \text{Gal}(L/K)$ eine Untergruppe. Dann ist $L/\text{Fix}(G)$ endlich, und es gilt

$$[L : \text{Fix}(G)] \leq |G|.$$

Beweis. Schreibe $n = |G|$. Seien $x_1, \dots, x_m \in L$ mit $m > n$. Dann ist zu zeigen, dass die x_i linear abhängig sind über $\text{Fix}(G)$ als Grundkörper.

Das homogene lineare Gleichungssystem

$$\sum_{j=1}^m c_j \sigma(x_j) = 0 \quad \forall \sigma \in G \quad (5.18)$$

hat aus Dimensionsgründen eine nichttriviale Lösung $c_1, \dots, c_m \in L$. Wähle eine solche Lösung mit minimalem m , indem gegebenenfalls einige der x_i weggelassen werden. Wie im Beweis von Satz 5.5.5(a) folgt dann, dass diese Koeffizienten bis auf Skalierung durch ein Element von L eindeutig bestimmt sind. Wir zeigen, dass $c_j \in \text{Fix}(G)$ für alle j gilt, was die gewünschte lineare Abhängigkeit über $\text{Fix}(G)$ ergibt.

Für jedes $\rho \in G$ ist auch $(\rho(c_1), \dots, \rho(c_m))$ wieder eine Lösung der Gleichung, weil

$$\sum_{j=1}^m \rho(c_j) \sigma(x_j) = \sum_{j=1}^m \rho(c_j) \rho(\rho^{-1} \sigma(x_j)) = \rho \left(\sum_{j=1}^m c_j (\rho^{-1} \sigma)(x_j) \right) = 0,$$

wobei wir im zweiten Schritt verwenden, dass ρ ein Automorphismus von L ist. Im dritten Schritt benutzen wir (5.18) mit dem Element $\rho^{-1} \sigma \in G$ anstelle von $\sigma \in G$, was zulässig ist, weil (5.18) ja für alle σ gilt.

Dank der Eindeutigkeitsbetrachtung gibt es also ein $r \in L$ mit

$$\rho(c_j) = r c_j \quad \forall j = 1, \dots, m.$$

Da wir durch Skalierung aber oBdA $c_1 = 1$ annehmen können, folgt $r = \rho(c_1) = 1$, also $\rho(c_j) = c_j$ für alle j . Weil $\rho \in G$ beliebig war, bedeutet dies $c_j \in \text{Fix}(G)$ für alle j , was zu zeigen war. $\square$

Besonders nützlich ist Satz 5.5.8 dann, wenn die beiden Abbildungen bijektiv sind. Die Frage ist jetzt also, unter welchen Voraussetzungen dies der Fall ist. Zunächst stellen wir fest, dass dies zumindest in eine Richtung für jede endliche Erweiterung gilt.

5.5.11 Satz. Sei L/K endlich. Für jede Untergruppe $G \subseteq \text{Gal}(L/K)$ gilt dann

$$\text{Stab}(\text{Fix}(G)) = G.$$

Beweis. Die Inklusion

$$G \subseteq \text{Stab}(\text{Fix}(G))$$

ist klar: jedes Element von G hält per Definition jedes Element von $\text{Fix}(G)$ fest. Dies kann man auch als Spezialfall von (3.10) sehen, wenn man das “op” in (5.17) berücksichtigt, wodurch $\geq$ zu $\subseteq$ wird.

Nach Lemma 5.5.10 und (5.16) gilt

$$|\text{Stab}(\text{Fix}(G))| = |\text{Gal}(L/\text{Fix}(G))| \leq [L : \text{Fix}(G)] \leq |G|.$$

Wegen $G \subseteq \text{Stab}(\text{Fix}(G))$ folgt also

$$\text{Stab}(\text{Fix}(G)) = G,$$

wie behauptet. $\square$

Mit dem allgemeinen Korollar 3.2.5(c) zu Galois-Zusammenhängen können wir also schließen:

5.5.12 Korollar. (a) Fix ist injektiv.

(b) Stab ist surjektiv.

(c) Es gelten

$$\begin{aligned} F &\subseteq \text{Fix}(\text{Stab}(F)) & \forall F \in \text{ZwiKö}(L/K), \\ G &\subseteq \text{Stab}(\text{Fix}(G)) & \forall G \in \text{Sub}(\text{Gal}(L/K)). \end{aligned}$$

(d) Der Galois-Zusammenhang (5.17) identifiziert $\text{Sub}(\text{Gal}(L/K))^{\text{op}}$ mit einer Teilmenge von $\text{ZwiKö}(L/K)$.

Die Bestimmung der Zwischenkörper von L/K ist also dadurch zumindest teilweise auf die Bestimmung der Untergruppen von $\text{Gal}(L/K)$ zurückgeführt. Dies ist oft deutlich einfacher, wie die folgenden Beispiele zeigen werden. Im nächsten Abschnitt werden wir außerdem sehen, dass Fix und Stab in vielen Fällen sogar bijektiv sind, so dass die Zwischenkörper von L/K genau durch die Untergruppen von $\text{Gal}(L/K)$ beschrieben werden können.

5.5.13 Beispiel. (a) Für die Erweiterung $\mathbb{C}/\mathbb{R}$ ist $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}_{\mathbb{C}}, \sigma\}$ mit $\sigma : z \mapsto \bar{z}$. Die Zwischenkörper sind nur $\mathbb{R}$ und $\mathbb{C}$ selbst, weil $\mathbb{C}$ ja nur Grad 2 über $\mathbb{R}$ hat, und also jeder Zwischenkörper einen Grad zwischen 1 und 2 haben muss. Die Untergruppen von $\text{Gal}(\mathbb{C}/\mathbb{R})$ sind nur die triviale Gruppe und $\text{Gal}(\mathbb{C}/\mathbb{R})$ selbst. Als Hasse-Diagramme:

$$\begin{array}{ccc} \mathbb{C} & & \{\text{id}_{\mathbb{C}}\} \\ | & & | \\ \mathbb{R} & & \{\text{id}_{\mathbb{C}}, \sigma\} \end{array}$$

Hier haben wir die Untergruppen von $\text{Gal}(\mathbb{C}/\mathbb{R})$ bezüglich der umgekehrten Inklusion geordnet, damit die beiden Hasse-Diagramme sich gemäß (5.17) entsprechen: $\mathbb{C}$ ist genau der Fixkörper der Identität, und $\mathbb{R}$ ist der Fixkörper der Identität und komplexer Konjugation. Umgekehrt ist $\text{Gal}(\mathbb{C}/\mathbb{R})$ per Definition die Gruppe aller Automorphismen von $\mathbb{C}$, die $\mathbb{R}$ festhalten. Somit stellen Fix und Stab eine genaue Entsprechung zwischen den Zwischenkörpern und den Untergruppen der Galoisgruppe her.

(b) Sei allgemeiner L/K eine beliebige quadratische Erweiterung, d.h. $[L : K] = 2$, und sei $\text{char}(K) \neq 2$. Wähle $a \in L \setminus K$. Dann gilt $L = K[a]$, und das Minimalpolynom von a über K hat die Form

$$\min(a, K) = X^2 + uX + v$$

mit $u, v \in K$. Neben a hat dieses Polynom nach Vieta die zweite Nullstelle

$$b = -u - a,$$

und diese liegt ebenfalls in L . Außerdem ist $b \neq a$, denn mit $b = a$ wäre mit $\text{char}(K) \neq 2$ auch $a = -u/2 \in K$, im Widerspruch zu $a \notin K$. Also erhalten wir einen nichttrivialen K -Automorphismus

$$\sigma : L \longrightarrow L, \quad r + sa \longmapsto r + sb$$

für $r, s \in K$. Dass σ die Multiplikation erhält, folgt daraus, dass a und b dieselbe Relation $a^2 + ua + v = 0$ bzw. $b^2 + ub + v = 0$ erfüllen: denn dadurch gilt

$$\sigma(a \cdot a) = \sigma(a) \cdot \sigma(a),$$

so dass σ jedenfalls multiplikativ auf den Basisvektoren $\{1, a\}$ ist, wobei $a \cdot a$ der einzige nichttriviale Fall ist. Außerdem ist σ ein Automorphismus, weil $\sigma \circ \sigma = \text{id}_L$ gilt aufgrund $\sigma(a) = b$ und $\sigma(b) = a$, also σ die beiden Nullstellen von $\min(a, K)$ vertauscht.

Insgesamt erhalten wir also die Hasse-Diagramme

$$\begin{array}{ccc} L & & \{\text{id}\} \\ | & & | \\ K & & \{\text{id}, \sigma\} \end{array}$$

Die Zwischenkörper und Untergruppen der Galoisgruppe stehen also in perfekter Entsprechung zueinander.

- (c) Für ein Beispiel mit echten Zwischenkörpern führen wir Beispiel 5.5.4 fort. Wir schreiben $L := \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ und bezeichnen die drei nichttrivialen Automorphismen von $L/\mathbb{Q}$ mit $\sigma_2, \sigma_3, \sigma_6$, wobei

$$\begin{aligned}\sigma_2(\sqrt{2}) &= -\sqrt{2}, & \sigma_2(\sqrt{3}) &= +\sqrt{3}, \\ \sigma_3(\sqrt{2}) &= +\sqrt{2}, & \sigma_3(\sqrt{3}) &= -\sqrt{3}, \\ \sigma_6(\sqrt{2}) &= -\sqrt{2}, & \sigma_6(\sqrt{3}) &= -\sqrt{3}.\end{aligned}$$

Die nichttrivialen Untergruppen von $\text{Gal}(L/\mathbb{Q})$ sind

$$\langle \sigma_2 \rangle = \{\text{id}, \sigma_2\}, \quad \langle \sigma_3 \rangle = \{\text{id}, \sigma_3\}, \quad \langle \sigma_6 \rangle = \{\text{id}, \sigma_6\},$$

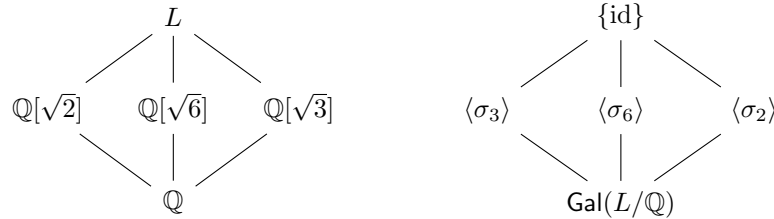
denn jede nichttriviale Untergruppe muss zwei der vier Elemente enthalten, also genau die Identität und eine der drei Nichtidentitäten. Die zugehörigen Fixkörper sind

$$\mathbb{Q}[\sqrt{3}], \quad \mathbb{Q}[\sqrt{2}], \quad \mathbb{Q}[\sqrt{6}].$$

Denn zum Beispiel ist $\text{Fix}(\langle \sigma_2 \rangle) = \mathbb{Q}[\sqrt{3}]$, weil ein Element

$$r + s\sqrt{2} + t\sqrt{3} + u\sqrt{6}$$

genau dann von σ_2 festgehalten wird, wenn $s = u = 0$ gilt. Als Hasse-Diagramme erhalten wir also:

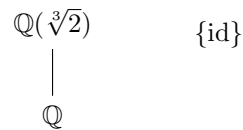


Dass es keine weiteren Zwischenkörper gibt, sieht man so: nach Beispiel 5.2.12 ist $[L : \mathbb{Q}] = 4$, so dass ein echter Zwischenkörper F den Grad 2 über $\mathbb{Q}$ haben muss. Dann gilt $[L : F] = 2$ nach der Gradformel aus Satz 5.2.11. Nach dem vorherigen Beispiel folgt dann, dass L einen nichttrivialen F -Automorphismus hat, also dass $\text{Stab}(F)$ nichttrivial ist. Folglich ist $\text{Stab}(F)$ eine der drei obigen Untergruppen. Außerdem gilt

$$F \subseteq \text{Fix}(\text{Stab}(F)) \neq \text{Fix}(\{\text{id}\}) = L,$$

wobei die Ungleichheit in der Mitte aus der Injektivität von Fix folgt. Also muss bereits $F = \text{Fix}(\text{Stab}(F))$ gelten, so dass F einer der drei obigen Zwischenkörper sein muss. Wir haben somit alle Zwischenkörper von $L/\mathbb{Q}$ bestimmt!

- (d) Die Erweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ hat nach Beispiel 5.5.2(d) triviale Galoisgruppe, aber dennoch *zwei* Zwischenkörper, nämlich $\mathbb{Q}$ und $\mathbb{Q}(\sqrt[3]{2})$ selbst. Die Galoisgruppe ist also nicht in der Lage, alle Zwischenkörper zu unterscheiden. Als Hasse-Diagramme:



Durch Fix wird die triviale rechte Seite in die nichttriviale linke Seite eingebettet. Aber der Unterkörper $\mathbb{Q}$ tritt jetzt nicht als Fixkörper einer Untergruppe auf und der Galois-Zusammenhang (5.17) ist nicht bijektiv.

5.6 Normale und separable Erweiterungen

Wir kommen jetzt zu den Zusatzbedingungen, die garantieren, dass der Galois-Zusammenhang (5.17) eine Bijektion zwischen den Zwischenkörpern von L/K und den Untergruppen von $\text{Gal}(L/K)$ herstellt. Die erste wichtige Bedingung ist folgende.

5.6.1 Definition. Eine Erweiterung L/K heißt **normal**, falls jedes irreduzible Polynom $f \in K[X]$, das eine Nullstelle in L hat, bereits in $L[X]$ vollständig in Linearfaktoren zerfällt.

5.6.2 Satz. Die folgenden Aussagen sind äquivalent für jede endliche Erweiterung L/K :

- (a) Die Erweiterung L/K ist normal.
- (b) L/K ist Zerfällungskörper eines Polynoms $f \in K[X]$.

Beweis. Sei zunächst L/K Zerfällungskörper eines Polynoms $f \in K[X]$. Wir bezeichnen die Nullstellen von f in L mit $a_1, \dots, a_n$, so dass oBdA

$$f = d \prod_{i=1}^n (X - a_i)$$

mit $d \in K^\times$ gilt. Dann ist zu zeigen, dass jedes irreduzible Polynom $g \in K[X]$, das eine Nullstelle in L hat, bereits in $L[X]$ vollständig in Linearfaktoren zerfällt. Wir können annehmen, dass g normiert ist. Sei also $b \in L$ mit $g(b) = 0$, und sei M/L ein Zerfällungskörper von g . Wir müssen zeigen, dass jede Nullstelle von g in M bereits in L liegt.

Sei dazu $c \in M$ eine weitere Nullstelle von g . Da g irreduzibel ist und $g(b) = g(c) = 0$ gilt, folgt

$$\min(b) = \min(c) = g.$$

Nach Satz 5.3.9 gibt es daher einen K -Isomorphismus

$$\lambda : K[b] \longrightarrow K[c]$$

mit $\lambda(b) = c$. Wenn wir f als Polynom über $K[b]$ betrachten, dann ist $L/K[b]$ ein Zerfällungskörper von f , weil

$$L = K[a_1, \dots, a_n] = K[b][a_1, \dots, a_n].$$

Ebenso ist $L[c]/K[c]$ ein Zerfällungskörper von f als Element von $K[c][X]$ betrachtet; der einzige Unterschied ist, dass $b \in L$, und wir $c \in L$ noch nicht wissen, weil es gerade die zu beweisende Aussage ist.

Nach der Eindeutigkeit von Zerfällungskörpern in der bei (5.13) angegebenen Form setzt sich λ also zu einem K -Isomorphismus

$$\sigma : L \longrightarrow L[c]$$

fort. Insbesondere gilt $[L : K] = [L(c) : K]$. Da $L \subseteq L(c)$ und L/K endlich ist, folgt daraus $L = L[c]$. Also gilt $c \in L$. Damit sind alle Nullstellen von g bereits in L enthalten, und g zerfällt schon über L vollständig in Linearfaktoren. Daher ist L/K normal.

Sei umgekehrt L/K endlich und normal. Wähle eine Basis $u_1, \dots, u_m$ von L als K -Vektorraum und setze

$$F := \prod_{i=1}^m \min(u_i) \in K[X].$$

Nach Normalität zerfällt jedes der Polynome $\min(u_i)$ in $L[X]$ vollständig in Linearfaktoren, also auch F . Sei $E \subseteq L$ der von allen Nullstellen von F erzeugte Körper über K . Dann gilt einerseits $E \subseteq L$, weil alle Nullstellen von F in L liegen. Andererseits sind $u_1, \dots, u_m$ selbst Nullstellen von F , also liegen sie in E . Da die u_i eine Basis von L über K bilden, folgt $L \subseteq E$. Also ist $E = L$, und damit ist L/K der Zerfällungskörper von F . $\square$

5.6.3 Beispiel. Die ersten drei Beispiele aus Beispiel 5.5.13 sind alle normal, während das vierte Beispiel nicht normal ist. Dies wird der Grund dafür sein, dass im ersten Beispiel die Zwischenkörper genau durch die Untergruppen der Galoisgruppe beschrieben werden können, während dies im vierten Beispiel nicht der Fall ist.

5.6.4 Lemma. Sei L/K algebraisch und normal, und sei F ein Zwischenkörper von L/K . Dann ist auch L/F normal.

Beweis. Sei $g \in F[X]$ irreduzibel und habe eine Nullstelle $a \in L$. Wir müssen zeigen, dass g über L vollständig in Linearfaktoren zerfällt. Wir können annehmen, dass g normiert ist. Sei $m := \min(a, K)$. Da L/K normal ist, zerfällt m in $L[X]$ vollständig in Linearfaktoren. Andererseits gilt $m(a) = 0$, also teilt $g = \min(a, F)$ das Polynom m in $F[X]$. Daher sind alle Nullstellen von g auch Nullstellen von m und liegen somit in L . Also zerfällt g in $L[X]$ vollständig in Linearfaktoren, und L/F ist normal. $\square$

Die andere relevante Zusatzbedingung beruht auf folgendem Begriff.

5.6.5 Definition. Ein Polynom $f \in K[X]$ heißt **separabel**, falls es in seinem Zerfällungskörper nur einfache Nullstellen besitzt.

Die Separabilität eines Polynoms kann man anhand des folgenden Kriteriums recht einfach überprüfen:

5.6.6 Lemma. Sei K ein Körper und sei

$$f = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$$

ein nichtkonstantes Polynom. Die **formale Ableitung** von f ist

$$f' := na_n X^{n-1} + \cdots + 2a_2 X + a_1.$$

Dann ist f genau dann separabel, wenn

$$\text{ggT}(f, f') = 1.$$

Insbesondere ist ein irreduzibles Polynom $f \in K[X]$ genau dann separabel, wenn $f' \neq 0$ gilt.

Beweis. Sei L/K ein Zerfällungskörper von f . Dann können wir in $L[X]$ schreiben

$$f = c \prod_{i=1}^r (X - a_i)^{m_i},$$

wobei die a_i paarweise verschieden sind und $m_i \geq 1$ gilt. Eine Nullstelle a_i ist genau dann mehrfach, wenn $(X - a_i)$ sowohl f als auch f' teilt. Dies sieht man direkt aus

$$f = (X - a_i)^{m_i} h \quad \text{mit } h(a_i) \neq 0 :$$

Die formale Ableitung erfüllt die Produktregel, wie man direkt nachrechnet. Daher ist

$$f' = m_i (X - a_i)^{m_i-1} h + (X - a_i)^{m_i} h'.$$

Für $m_i \geq 2$ ist dies durch $X - a_i$ teilbar, während für $m_i = 1$ der Wert

$$f'(a_i) = h(a_i)$$

nicht verschwindet. Also hat f genau dann eine mehrfache Nullstelle, wenn f und f' in $L[X]$ einen gemeinsamen Linearfaktor haben.

Wenn $\text{ggT}(f, f') = 1$ in $K[X]$ gilt, dann gibt es Polynome $u, v \in K[X]$ mit

$$uf + vf' = 1.$$

Diese Gleichung gilt auch in $L[X]$, also können f und f' in $L[X]$ keinen gemeinsamen Linearfaktor haben. Umgekehrt liefert ein nichtkonstanter gemeinsamer Teiler von f und f' in $K[X]$ nach Übergang nach $L[X]$ einen gemeinsamen Linearfaktor. Damit ist die Äquivalenz bewiesen.

Falls f irreduzibel ist, sind die einzigen Teiler von f die konstanten Polynome und skalare Vielfache von f . Daher ist $\text{ggT}(f, f') \neq 1$ genau dann möglich, wenn $f \mid f'$ gilt. Da aber $\deg(f') < \deg(f)$ gilt, passiert dies genau dann, wenn $f' = 0$ ist. $\square$

Die allermeisten irreduziblen Polynome sind separabel, wie die folgende Aussage zeigt:

5.6.7 Lemma. *Sei K ein Körper mit $\text{char}(K) = 0$ und $f \in K[X]$ irreduzibel. Dann ist f separabel.*

Beweis. Nach Lemma 5.6.6 ist das irreduzible Polynom f genau dann separabel, wenn $f' \neq 0$ gilt. Falls $\text{char}(K) = 0$ ist, kann die Ableitung eines nichtkonstanten Polynoms nicht verschwinden: Ist

$$f = a_n X^n + \cdots + a_0$$

mit $a_n \neq 0$, dann ist der Leitkoeffizient von f' gleich $na_n \neq 0$. Also ist f separabel. $\square$

5.6.8 Beispiel. In Charakteristik $p > 0$ gibt es viele nicht-separable Polynome.

(a) Das einfachste Beispiel ist

$$X^p - 1 \in \mathbb{F}_p[X].$$

Die Ableitung ist gleich 0, und tatsächlich gilt

$$X^p - 1 = (X - 1)^p$$

in $\mathbb{F}_p[X]$, so dass die einzige Nullstelle mehrfach ist.

(b) Es gibt sogar irreduzible nicht-separable Polynome. Sei dazu $K := \mathbb{F}_p(T)$ der Körper der rationalen Funktionen in einer Variablen T über $\mathbb{F}_p$. Dann ist

$$X^p - T \in K[X]$$

nicht separabel, denn seine Ableitung verschwindet. Das Polynom ist irreduzibel: Sei a eine Nullstelle in einem Zerfällungskörper. Dann gilt

$$X^p - T = (X - a)^p.$$

Somit hat das Polynom eine mehrfache Nullstelle.

Zur Irreduzibilität: hätte $X^p - T$ einen echten nichtkonstanten Faktor in $K[X]$, dann müsste dieser über dem Zerfällungskörper von der Form $(X - a)^m$ mit $1 \leq m < p$ sein, jedenfalls bis auf Skalierung durch ein Element von $K^\times$. Der Koeffizient von X^{m-1} in einem solchen Faktor wäre dann $-ma$, was in K liegen muss. Da $m \neq 0$ in K gilt, würde also $a \in K$ folgen. Dann wäre $T = a^p$ eine p -te Potenz in $\mathbb{F}_p(T)$. Die Variable T selbst hat aber in $\mathbb{F}_p(T)$ keine p -te Wurzel.⁴⁶

5.6.9 Definition. Eine algebraische Erweiterung L/K heißt **separabel**, falls das Minimalpolynom jedes Elements $a \in L$ über K separabel ist.

5.6.10 Lemma. Eine Erweiterung der Form $L/\text{Fix}(G)$ für eine endliche Untergruppe $G \subseteq \text{Gal}(L/K)$ ist separabel.

Beweis. Sei $a \in L$ und $G \cdot a$ die Bahn von a unter der Wirkung von G . Dann betrachten wir das Polynom

$$q_a := \prod_{b \in G \cdot a} (X - b) \in L[X].$$

Es gilt $q_a \in \text{Fix}(G)[X]$, weil jedes $\tau \in G$ die Bahn $G \cdot a$ permutiert. Es gilt $q_a(a) = 0$, und die Linearfaktoren von q_a sind paarweise verschieden. Das Minimalpolynom $\min(a, \text{Fix}(G))$ teilt daher das separable Polynom q_a . Also ist auch $\min(a, \text{Fix}(G))$ separabel. Da $a \in L$ beliebig war, ist $L/\text{Fix}(G)$ separabel. $\square$

5.6.11 Lemma. Sei L/K separabel und F ein Zwischenkörper von L/K . Dann ist auch L/F separabel.

Beweis. Sei $a \in L$ beliebig. Wir müssen zeigen, dass $\min(a, F)$ separabel ist. Da L/K separabel ist, ist $\min(a, K)$ separabel. Außerdem gilt $\min(a, K)(a) = 0$, also teilt $\min(a, F)$ das Polynom $\min(a, K)$ in $F[X]$. Jeder Teiler eines separablen Polynoms ist wieder separabel. Also ist $\min(a, F)$ separabel. Damit ist L/F separabel. $\square$

⁴⁶Sei $T = (f/g)^p$ mit $f, g \in \mathbb{F}_p[T]$ teilerfremd und $\neq 0$. Dies bedeutet $f^p = Tg^p$. Der Grad auf der linken Seite ist jetzt ein Vielfaches von p , der Grad auf der rechten Seite aber nicht.

5.7 Der Hauptsatz der Galoistheorie

Jedenfalls für endliche Erweiterungen sind die Normalität und Separabilität von L/K , wie wir jetzt zeigen werden, ausreichend dafür, dass der Galois-Zusammenhang (5.17) bijektiv wird.

5.7.1 Lemma. *Sei L/K endlich, normal und separabel, und seien $a, b \in L$ mit $\min(a, K) = \min(b, K)$. Dann gibt es ein $\sigma \in \text{Gal}(L/K)$ mit $\sigma(a) = b$.*

Beweis. Setze $g := \min(a, K) = \min(b, K)$. Da g irreduzibel ist und sowohl a als auch b als Nullstellen hat, erhalten wir nach Lemma 5.4.8 einen K -Isomorphismus

$$\lambda : K[a] \longrightarrow K[b]$$

mit $\lambda(a) = b$.

Da L/K normal und endlich ist, ist L/K nach Satz 5.6.2 ein Zerfällungskörper eines Polynoms über K . Sei also $f \in K[X]$ ein Polynom, dessen Zerfällungskörper über K gerade L ist. Dann ist $L/K[a]$ ein Zerfällungskörper von f , und ebenso ist $L/K[b]$ ein Zerfällungskörper von f . Nach der Eindeutigkeit von Zerfällungskörpern aus Satz 5.4.9 setzt sich λ daher zu einem Isomorphismus

$$\sigma : L \longrightarrow L$$

fort. Dieser Isomorphismus hält K fest, also ist $\sigma \in \text{Gal}(L/K)$, und nach Konstruktion gilt $\sigma(a) = b$. $\square$

Die folgende Aussage ist jetzt der Hauptsatz der Galoistheorie.

5.7.2 Satz. *Sei L/K eine endliche Erweiterung, die normal und separabel ist. Dann ist der Galois-Zusammenhang (5.17) bijektiv, und es gilt*

$$[L : K] = |\text{Gal}(L/K)|.$$

Beweis. Für die Bijektivität des Galois-Zusammenhangs bleibt noch zu zeigen: für jeden Zwischenkörper F gilt

$$\text{Fix}(\text{Gal}(L/F)) = F.$$

Die Inklusion $\supseteq$ ist dabei klar.

Sei also $a \in L \setminus F$. Dann müssen wir beweisen, dass es ein $\sigma \in \text{Gal}(L/F)$ mit $\sigma(a) \neq a$ gibt. Nach Lemmata 5.6.4 und 5.6.11 ist auch L/F normal und separabel. Das Minimalpolynom $\min(a, F) \in F[X]$ hat $\text{Grad} > 1$, denn $a \notin F$. Da L/F normal ist, zerfällt $\min(a, F)$ in $L[X]$ vollständig in Linearfaktoren. Da L/F separabel ist, sind diese Linearfaktoren paarweise verschieden. Also besitzt $\min(a, F)$ eine weitere Nullstelle $b \in L$ mit $b \neq a$. Da $\min(a, F)$ irreduzibel ist, gilt auch $\min(b, F) = \min(a, F)$. Nach Lemma 5.7.1, angewandt auf die Erweiterung L/F , gibt es dann ein $\sigma \in \text{Gal}(L/F)$ mit

$$\sigma(a) = b.$$

Insbesondere ist $\sigma(a) \neq a$, also liegt a nicht in $\text{Fix}(\text{Gal}(L/F))$. Damit ist $\text{Fix}(\text{Gal}(L/F)) \subseteq F$ gezeigt, und somit gilt

$$\text{Fix}(\text{Gal}(L/F)) = F.$$

Es bleibt die Formel für die Kardinalität der Galoisgruppe. Setze $G := \text{Gal}(L/K)$. Nach dem bereits bewiesenen Teil gilt $\text{Fix}(G) = K$. Daher liefert Lemma 5.5.10

$$[L : K] = [L : \text{Fix}(G)] \leq |G|.$$

Die umgekehrte Ungleichung ist genau (5.16). Also folgt

$$[L : K] = |\text{Gal}(L/K)|,$$

was zu zeigen war. $\square$

5.8 Unlösbarkeit von Gleichungen fünften Grades

Zum Abschluss kommen wir zurück zur Frage aus der Einführung, ob es allgemeine Lösungsformeln für Polynomgleichungen gibt. Hierbei sind im Prinzip verschiedene Arten von “Lösungsformeln” denkbar; zum Beispiel haben wir in Beispiel 5.2.10 argumentiert, dass es keine allgemeine Lösungsformel für quadratische Gleichungen $aX^2 + bX + c = 0$ gibt, die als rationale Funktion der Koeffizienten a, b, c ausgedrückt werden könnte.

Für die allgemeine quadratische Gleichung gibt es aber eine Lösungsformel, falls man das Ziehen von Wurzeln zulässt, nämlich

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Diese Formel (zusammen mit der normalen Herleitung) gilt dabei in jedem Körper K . Die Wurzel steht hierbei für ein beliebiges Element in K , dessen Quadrat gleich $b^2 - 4ac$ ist. Falls ein solches Element existiert, ist es bis auf Vorzeichen eindeutig, und die Formel liefert damit tatsächlich die beiden Nullstellen von $aX^2 + bX + c$. Falls es keine solche Wurzel gibt, dann hat die Gleichung keine Lösung in K .

Letzteres kann schon anders aussehen, wenn wir zu einem Oberkörper L in einer Körpererweiterung L/K übergehen, denn jetzt kann die benötigte Wurzel in L existieren, auch wenn sie in K nicht existiert. Wir brauchen also bloß ein Element $t \in L$ mit

$$t^2 = b^2 - 4ac.$$

Außerdem brauchen wir sonst keine weiteren Elemente aus L , es reicht also aus, $L = K[t]$ zu setzen. Wenn wir in der Lösungsformel eine dritte Wurzel brauchen würden, dann hätten wir links entsprechend t^3 stehen.

Falls in der Lösungsformel mehrere Wurzeln auftreten, und insbesondere falls diese Wurzeln ineinander geschachtelt sind, dann müssen wir diese Wurzeln nacheinander ziehen, also entsprechend iterierte Körpererweiterungen anschauen. Denn zum Beispiel für eine Wurzel der Form

$$\sqrt{2 + \sqrt{3}} \tag{5.19}$$

bilden wir die Körperkette

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}] \subseteq \mathbb{Q}\left[\sqrt{2 + \sqrt{3}}\right].$$

Im ersten Schritt können wir statt $\sqrt{3}$ auch einen beliebigen Oberkörper wählen, der ein t mit $t^2 = 3$ enthält. Im zweiten Schritt brauchen wir dann entsprechend ein Element s mit $s^2 = 2 + t$. Dies suggeriert die folgende Definition.

5.8.1 Definition. Sei $K \subseteq \mathbb{C}$ ein Körper. Eine Erweiterung L/K heißt **Radikalerweiterung**, falls es eine Kette von Körpern

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L$$

gibt, so dass Elemente $t_j \in K_j$ und $n_j \in \mathbb{N}_{>0}$ existieren mit

$$K_j = K_{j-1}[t_j], \quad t_j^{n_j} \in K_{j-1} \quad \forall j = 1, \dots, m.$$

Ein Polynom $f \in K[X]$ heißt **durch Radikale lösbar**, falls es in einer Radikalerweiterung von K in Linearfaktoren zerfällt.

Der Begriff *Radikal* steht hier für das Ziehen von Wurzeln (nach dem lateinischen *radix* für Wurzel). Die entscheidende Verbindung zur Gruppentheorie ist dann die folgende Aussage.

5.8.2 Satz. Sei $K \subseteq \mathbb{C}$ ein Körper und $f \in K[X]$. Falls f durch Radikale über K lösbar ist, dann ist die Galoisgruppe von f über K auflösbar.

Beweisskizze. Die Grundidee ist, dass das Adjungieren einer n -ten Wurzel nur abelsche Symmetrien erzeugt, sobald die n -ten Einheitswurzeln ebenfalls vorhanden sind: ein Automorphismus muss eine Nullstelle t von $X^n - c$ auf eine andere Nullstelle abbilden, also auf ζt für eine n -te Einheitswurzel ζ . Dadurch wird die Galoisgruppe zu einer Untergruppe der Gruppe der n -ten Einheitswurzeln, und diese ist abelsch.

Betrachtet man die ganze Kette von Radikalerweiterungen, so zerlegt sich dadurch die Galoisgruppe $\text{Gal}(L/K)$ in mehrere aufeinanderfolgende Schritte, die jeweils abelsche Quotienten haben. Nach Definition 2.5.1 bedeutet dies, dass $\text{Gal}(L/K)$ auflösbar ist. $\square$

Um Nichtauflösbarkeit durch Radikale zu zeigen, genügt daher die Kontraposition: wenn ein Polynom eine nicht auflösbare Galoisgruppe hat, dann gibt es keine Lösungsformel durch Radikale. Wir betrachten nun ein Kriterium, das sich besonders gut auf konkrete Polynome fünften Grades anwenden lässt.

5.8.3 Lemma. Sei $f \in \mathbb{Q}[X]$ irreduzibel vom Grad 5 und habe genau zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$. Dann ist die Galoisgruppe von f über $\mathbb{Q}$ isomorph zu S_5 .

Beweis. Sei $L/\mathbb{Q}$ der Zerfällungskörper von f . Da f irreduzibel ist, wirkt $\text{Gal}(L/\mathbb{Q})$ nach Lemma 5.5.3 auf den fünf Nullstellen von f so, dass der zugehörige Gruppenhomomorphismus

$$\text{Gal}(L/\mathbb{Q}) \hookrightarrow S_5$$

injektiv ist. Außerdem ist $L/\mathbb{Q}$ normal und separabel, da L ein Zerfällungskörper über $\mathbb{Q}$ ist und $\text{char}(\mathbb{Q}) = 0$ gilt. Je zwei Nullstellen von f haben wegen der Irreduzibilität von f dasselbe Minimalpolynom über $\mathbb{Q}$. Nach Lemma 5.7.1 kann daher jede Nullstelle von f durch ein Element von $\text{Gal}(L/\mathbb{Q})$ auf jede andere Nullstelle abgebildet werden. Eine solche Untergruppe von S_5 nennen wir *transitiv*.

Außerdem liegen die beiden nicht-reellen Nullstellen als komplex konjugiertes Paar vor. Die komplexe Konjugation ist daher ein Element von $\text{Gal}(L/\mathbb{Q})$, das diese beiden Nullstellen vertauscht und die drei reellen Nullstellen festhält. Die Transposition dieser beiden Nullstellen gehört also zur entsprechenden Untergruppe von S_5 .

Es genügt nun die folgende gruppentheoretische Beobachtung: Die einzige transitive Untergruppe von S_5 , die eine Transposition enthält, ist bereits ganz S_5 . Denn aus dem Bahnstabilisatorsatz 2.4.13, angewandt auf die Wirkung auf $\{1, \dots, 5\}$, folgt, dass eine transitive Untergruppe von S_5 eine durch 5 teilbare Ordnung hat. Nach dem Satz von Cauchy 2.4.22 enthält sie damit ein Element der Ordnung 5, also einen 5-Zykel. Nach Umnummerierung der fünf Nullstellen sei dieser 5-Zykel

$$\gamma = (1\ 2\ 3\ 4\ 5).$$

Die vorhandene Transposition können wir mit Potenzen von γ konjugieren, so dass sie nach eventuellem Ersetzen von γ durch γ^{-1} entweder die Form $(1\ 2)$ oder $(1\ 3)$ hat. Im ersten Fall liefern die Konjugierten $\gamma^k(1\ 2)\gamma^{-k}$ alle benachbarten Transpositionen

$$(1\ 2),\ (2\ 3),\ (3\ 4),\ (4\ 5),$$

und diese erzeugen S_5 . Im zweiten Fall liefern die Konjugierten von $(1\ 3)$ die benachbarten Transpositionen bezüglich der Reihenfolge

$$1, 3, 5, 2, 4,$$

und erzeugen daher ebenfalls S_5 . Also gilt $\text{Gal}(L/\mathbb{Q}) \cong S_5$. $\square$

5.8.4 Satz. Die Gleichung

$$X^5 - 4X + 2 = 0$$

ist über $\mathbb{Q}$ nicht durch Radikale lösbar.

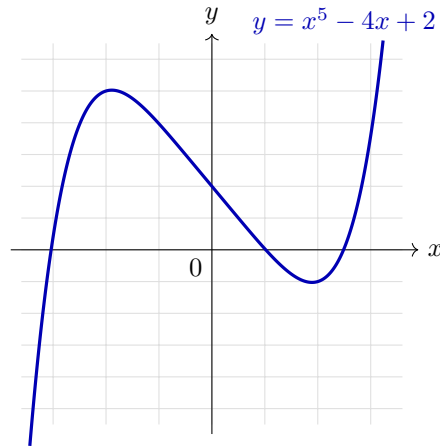


Abbildung 22: Der Graph von $f = X^5 - 4X + 2$. Man erkennt, dass es anscheinend genau drei reelle Nullstellen gibt. Der formale Beweis dieser Aussage ist eine Übung in Analysis.

Beweisskizze. Setze

$$f := X^5 - 4X + 2 \in \mathbb{Q}[X].$$

Dieses Polynom ist nach dem Eisenstein-Kriterium für $p = 2$ irreduzibel über $\mathbb{Q}$. Für die Anwendung von Lemma 5.8.3 müssen wir nur noch zeigen, dass f genau drei reelle Nullstellen hat. Dies ist jetzt ein Problem aus der Analysis, so dass wir die Details hier nicht weiter ausführen. Abbildung 22 zeigt aber informell, dass es tatsächlich genau drei reelle Nullstellen gibt.

Nach Lemma 5.8.3 ist die Galoisgruppe von f über $\mathbb{Q}$ isomorph zu S_5 . Nach Satz 2.5.3 ist S_5 nicht auflösbar. Mit Satz 5.8.2 folgt daher, dass f nicht durch Radikale lösbar ist. $\square$

Damit ist präzisiert, in welchem Sinne es keine allgemeine Lösungsformel für Gleichungen fünften Grades geben kann: es gibt bereits eine einzige konkrete Gleichung fünften Grades mit rationalen Koeffizienten, nämlich zum Beispiel

$$X^5 - 4X + 2 = 0,$$

deren Lösungen sich nicht durch die Grundrechenarten und wiederholtes Ziehen von Wurzeln aus rationalen Zahlen ausdrücken lassen!

Index

- K -Automorphism, 109
- K -Homomorphismus, 106
- abelsche Gruppe, 15
- affine Abbildung, 12
- algebraisch, 100
 - Erweiterung, 100
- allgemeine lineare Gruppe, 12
- alternierende Gruppe, 22
- Assoziativität, 6
- Assoziiiertheit, 64
- auflösbare Gruppe, 36
- Bahn, 31
- Charakteristik, 95
- Diedergruppe, 13
- Einheit, 63
- Einheitengruppe, 63
- Einheitswurzel, 103
- Eisenstein-Kriterium, 89
- endlich erzeugte abelsche Gruppe, 42
- Erzeuger (einer Gruppe), 16
- euklidische Gruppe, 13
- euklidischer Ring, 82
- faktorieller Ring, 85
- formale Ableitung, 119
- Galois-Zusammenhang, 50
- Galoisgruppe
 - einer Körpererweiterung, 109
 - eines Polynoms, 111
- Galoistheorie, 114
- gaußsche Primzahl, 81
- gaußsche Zahlen, 65
- Grad
 - eines Polynoms, 61
 - Körpererweiterung, 97
- Gradfunktion, 82
- Gruppe, 10
- Gruppenhomomorphismus, 18
- Gruppenisomorphismus, 20
- Gruppenring, 60
- Gruppenwirkung, 29
- Halbring, 58
- Hasse-Diagramm, 49
- Hauptideal, 68
- Hauptidealring, 84
- Ideal, 67
 - echtes Ideal, 68
 - erzeugtes Ideal, 68
 - Hauptideal, 68
 - maximal, 94
- idempotent, 78
- Idempotenz, 6
- Infimum, 55
- Integritätsring, 79
- Inverses, 10
- Invertierbarkeit, 10
- irreduzibel, 80
- isomorphe Gruppen, 20
- Isomorphiesatz
 - erster, 27
- Kern (eines Gruppenhomomorphismus), 21
- Koeffizient
 - Polynom, 61
- kommutativer Ring, 60
- Kommutativität, 6
- Kongruenz
 - modulo Ideal, 70
- Konjugation, 22
- Körper, 63, 91
- Körper der rationalen Funktionen, 94
- Körpererweiterung, 95
 - normal, 118
 - separabel, 120
- linksadjungiert, 50
- Linksnebenklasse, 23
- Magma, 6
- Minimalpolynom, 101
- Monoid, 8
- Monoidring, 60
- monotone Abbildung, 49
- Nebenklasse, 23
- neutrales Element, 8
- noetherscher Ring, 86
- normale Untergruppe, 22
- Nullhalbring, 59
- Nullring, 60
- Nullteiler, 79
- Nullteilerfreiheit, 79
- Oberkörper, 96
- op, 48
- orthogonale Gruppe, 12
- orthogonale Matrix, 12
- Permutation, 11
- Polynom
 - konstantes Polynom, 61
 - Nullpolynom, 61
 - separabel, 119
- Polynomring, 61

prim, 80
Primelement, 80
Primideal, 82
primitive Einheitswurzel, 103
Produkt von Gruppen, 38
prägeordnete Menge, 47
Präordnung, 47

quadratfrei, 97
Quotientengruppe, 25
Quotientenkörper, 92

Radikalerweiterung, 122
Rechengesetz, 6
rechtsadjungiert, 50
Rechtsnebenklasse, 23
Restklassenring, 70
Ring, 59
Ringhomomorphismus, 66
Ringisomorphismus, 66

separabel, 119
Spezielle lineare Gruppe, 22
Stabilisator, 32
Supremum, 55
symmetrische Gruppe, 11

Teiler, 79
teilgeordnete Menge, 48
transzendent, 100

umgekehrte Präordnung, 48
Untergruppe, 11
Unterkörper, 96
Unterring, 65

Vierergruppe, 91

Wirkung, 29

Zerfällungskörper, 105
Zwischenkörper, 113
zyklische Gruppe, 16

Literatur

- [1] Paolo Aluffi. *Algebra: Notes from the Underground*. Cambridge Mathematical Textbooks, 2021.
- [2] Jonathan S. Golan. *Semirings and their applications*. Kluwer, 1999.
- [3] Urs Hartl. *Ergänzungen zur Analysis und Linearen Algebra*. ivv5hpp.uni-muenster.de/u/uhartl/15wi_ErgAnaLA/
- [4] Neal Koblitz. *A Course in Number Theory and Cryptography*. Bd. 114. Graduate Texts in Mathematics. Springer, 1994.
- [5] Tim Netzer. *Algebra*. uibk.ac.at/mathematik/algebra/media/teaching/algebra.pdf.
- [6] Franco Strocchi. *An introduction to the mathematical structure of quantum mechanics*. Bd. 28. Advanced Series in Mathematical Physics. World Scientific, 2008.