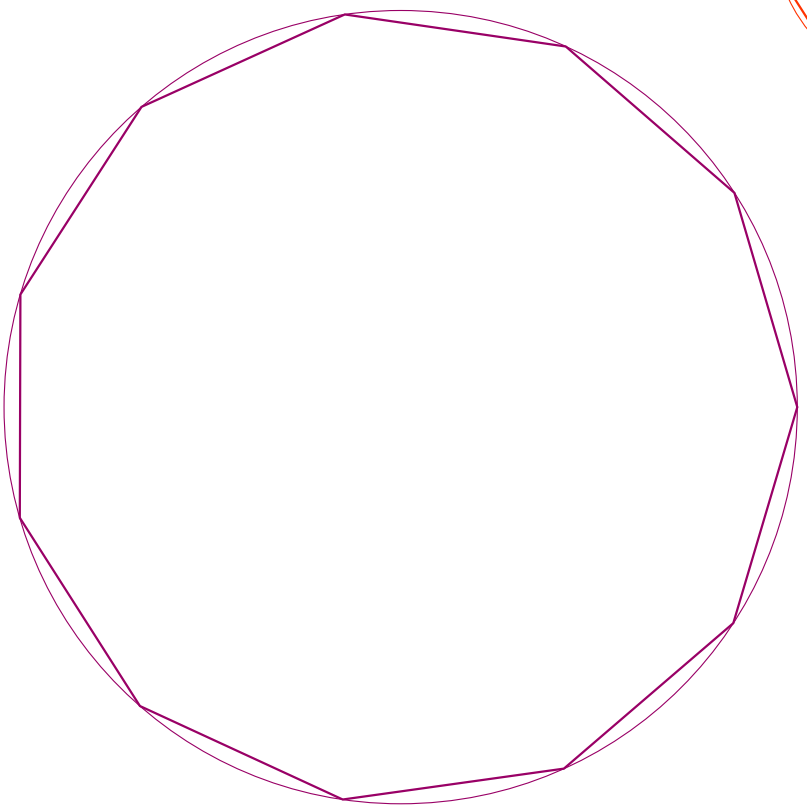
Algebra

Wintersemester 2025/26

Clara Löh



Version vom 6. Februar 2026
clara.loeh@mathematik.uni-regensburg.de
Fakultät für Mathematik, Universität Regensburg, 93040 Regensburg

Inhaltsverzeichnis

Literaturhinweise vii

0 Einführung 1

1 Gruppen 7

1.1 Die Kategorie der Gruppen 8

1.1.1 Vorbereitung: Monoide und Monoidhomomorphismen 8

1.1.2 Gruppen und Gruppenhomomorphismen 12

1.1.3 Automorphismengruppen 16

1.1.4 Untergruppen 18

1.1.5 Erzeugendensysteme 24

1.1.6 Quotientengruppen 26

1.1.7 Produkte und Erweiterungen 35

1.2 Gruppenoperationen 42

1.2.1 Gruppenoperationen 42

1.2.2 Zählen durch Gruppenoperationen 47

1.3 Struktur endlicher Gruppen 53

1.3.1 Endliche abelsche Gruppen 54

1.3.2 Symmetrische Gruppen 57

1.3.3 Die allgemeine Klasifikationsstrategie 62

1.3.4 Auflösbare Gruppen 65

1.3.5 Die Sylowsätze 70

2 Ringe 81

2.1 Die Kategorie der Ringe 82

2.1.1 Ringe und Ringhomomorphismen 82

2.1.2 Polynomringe 85

2.1.3 Quotientenkörper 88

2.1.4 Ideale und Restklassenringe 91
2.2 Die Primeigenschaft 95
2.2.1 Teilbarkeit 96
2.2.2 Primzahlen 98
2.2.3 Primideale und Restklassenringe 101
2.2.4 Der kleine Satz von Fermat 106
2.2.5 Faktorielle Ringe 112
2.2.6 Irreduzibilitätskriterien 121

3 Körper 129
3.1 Die Kategorie der Körper 130
3.1.1 Körper und Körperhomomorphismen 130
3.1.2 Die Einheitengruppe eines Körpers 132
3.2 Die Kategorie der Körpererweiterungen 133
3.2.1 Körpererweiterungen 133
3.2.2 Algebraische Zahlen 140
3.2.3 Algebraische Körpererweiterungen 147
3.2.4 Zerfällungskörper 149
3.2.5 Der algebraische Abschluss 156
3.3 Endliche Körper 160
3.3.1 Klassifikation endlicher Körper 160
3.3.2 Anwendungen endlicher Körper 163
3.4 Galoiserweiterungen 163
3.4.1 Normale Körpererweiterungen 165
3.4.2 Separable Körpererweiterungen 166
3.4.3 Galoiserweiterungen 170
3.4.4 Der Hauptsatz der Galoistheorie 173
3.5 Anwendungen der Galoistheorie 178
3.5.1 Vorbereitung: Kreisteilungskörper 178
3.5.2 Auflösbarkeit durch Radikale 182
3.5.3 Konstruierbarkeit mit Zirkel und Lineal 189
3.5.4 Der Fundamentalsatz der Algebra 192
3.5.5 Die letzte Seite zur Körpertheorie 195

A Anhang A.1
A.1 Die komplexen Zahlen A.2
A.2 Kategorien A.6
A.3 Freie Gruppen A.9
A.4 Formalisierte Algebra A.13
A.5 Sylow-Zoo A.17
A.6 Euklidische Ringe A.21
A.7 Konstruierbarkeit mit Zirkel und Lineal A.27
A.8 Anwendungen endlicher Körper A.32
A.9 Funktoren A.37

B Übungsblätter B.1

C Organisatorisches C.1

Literaturverzeichnis C.1

Wörterbuch C.4

Index C.13

Literaturhinweise

Die Vorlesung wird sich nicht an einer einzelnen Quelle orientieren – Sie sollten also individuell je nach Thema und eigenen Vorlieben die Literatur auswählen, die am besten zu Ihnen passt.

Sie sollten mehrere solche Bücher anschauen und dann entscheiden, (ob) welche davon für Sie als Ergänzung zur Vorlesung geeignet sind. Das Material wird nicht immer in derselben Reihenfolge präsentiert und es gibt bei Konventionen und Schwerpunkten Unterschiede.

Die nachfolgende Liste enthält Anregungen für ergänzende und vertiefende Literatur. Manche Dinge werden dort anders behandelt als in dieser Vorlesung!

Algebra

- M. A. Armstrong. *Groups and Symmetry*, Undergraduate Texts in Mathematics, Springer, 1988.

- S. Bosch. *Algebra*, achte Auflage, Springer Spektrum, 2013.

- S. Lang. *Algebra*, Graduate Texts in Mathematics, 211, dritte überarbeitete Auflage, Springer, 2002.

- B. L. van der Waerden. *Algebra I*, neunte Auflage, Springer, 1993.

Beweisen und Problemlösen

- A. Beutelspacher. *Das ist o.B.d.A. trivial!*, neunte Auflage, Vieweg+-Teubner, 2009.
- J. Cummings. *Proofs: A Long-Form Mathematics Textbook*, Indepdently published, 2021.
- A. G. Konforowitsch. *Logischen Katastrophen auf der Spur*, zweite Auflage, Fachbuchverlag Leipzig, 1994.
- L. Lamport. How to write a 21st century proof, *J. Fixed Point Theory Appl.*, 11(1), 43–63, 2012.
- C. Löh. *Exploring Formalisation. A Primer in Human-Readable Mathematics in Lean 3 with Examples from Simplicial Topology*, Surveys and Tutorials in the Applied Mathematical Sciences, 11, Springer, 2022.
- C. Löh, S. Krauss, N. Kilbertus (Hrsg.). *Quod erat knobelandum*, zweite Auflage, Springer, 2019.
- G. Polya, J.H. Conway (Hrsg.). *How to Solve it: A New Aspect of Mathematical Method*, Princeton Science Library, 2014.
- T. Tao. *Solving mathematical problems. A personal perspective*, Oxford University Press, 2006.

Weiterführende Literatur

- J. Avigad, L. de Moura, S. Kong. *Theorem Proving in Lean*, https://lean-lang.org/theorem_proving_in_lean/, 2023.
- I. M. Banks. *The Algebraist*, Orbit, 2004.
- M. Brandenburg. *Einführung in die Kategorientheorie: Mit ausführlichen Erklärungen und zahlreichen Beispielen*, Springer Spektrum, 2015.
- J. J. Rotman. *An Introduction to the Theory of Groups*, Graduate Texts in Mathematics, 148, vierte Auflage, 1995.
- Geogebra, https://www.geogebra.org/

0
Einführung

Die Algebra befasst sich mit der abstrakten Struktur allgemeiner „Zahlenbereiche“. Lineare Strukturen, d.h. Vektorräume, Moduln und lineare Abbildungen, haben wir bereits in der Linearen Algebra kennengelernt. Wir werden nun

- Gruppen,
- Ringe und
- Körper

genauer untersuchen.

Warum Algebra?

Um einzusehen, warum Grundkenntnisse in Algebra so fundamental sind, betrachten wir die folgende Sammlung von Aufgaben:

Aufgabe 1. Konstruiere mit Zirkel und Lineal aus einer Strecke der Länge 1 die Seitenlänge eines Quadrats, dessen Flächeninhalt mit dem Flächeninhalt des Einheitskreises übereinstimmt.

Aufgabe 2. Konstruiere mit Zirkel und Lineal aus einer Strecke der Länge 1 die Seitenlänge eines Würfels, der das Volumen 2 besitzt.

Aufgabe 3.

1. Konstruiere mit Zirkel und Lineal aus einer Strecke der Länge 1 die Seitenlänge eines regulären 9-Ecks mit Radius 1.

2. Konstruiere mit Zirkel und Lineal aus einer Strecke der Länge 1 die Seitenlänge eines regulären 17-Ecks mit Radius 1.

Aufgabe 4. Bestimme alle Nullstellen der Funktion

$$\begin{aligned} \mathbb{C} &\longrightarrow \mathbb{C} \\ x &\longmapsto x^5 - 4 \cdot x^2 + 2. \end{aligned}$$

Aufgabe 5.

1. Bestimme die erste Ziffer (im Zehnersystem) der Zahl $(2026^{2026})^{2026}$.
2. Bestimme die letzte Ziffer (im Zehnersystem) der Zahl $(2026^{2026})^{2026}$.
3. Bestimme den Rest von 4242^{2026} bei Division durch 2026.

Aufgabe 6. Beim 14/15-*Puzzle* sind fünfzehn numerierte Plättchen und eine „Lücke“ auf einem quadratischen Brett verteilt (siehe Abbildung (a)). Wie kann man die Position in Abbildung (b) durch Verschieben der Plättchen aus Position (a) erreichen?

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(a)

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

(b)

Die obigen Aufgabenstellungen sind mit dem Schulwissen der Mittelstufe zu verstehen (mit Ausnahme der komplexen Zahlen in Aufgabe 4, da die komplexen Zahlen derzeit nicht Teil des Lehrplans sind).

- Wäre es eine gute Idee, diese Aufgaben in der Schule zu stellen? Im Unterricht? Als Hausaufgabe? In einer Klausur?
- Sind diese Aufgaben überhaupt alle lösbar? Welche sind nicht lösbar? Warum?

Wir werden in dieser Vorlesung Techniken entwickeln, die zeigen, dass *nicht* alle der obigen Aufgaben lösbar sind; umgekehrt werden wir auch sehen, wie man die lösbaren Aufgaben lösen kann.

Überblick über die Vorlesung

Das Hauptziel der Vorlesung ist die Entwicklung der (elementaren) Galoistheorie. Mithilfe dieser Theorie können

- Konstruierbarkeitsprobleme und
- die (Nicht-)Auflösbarkeit von Gleichungen durch iteriertes Wurzelziehen

behandelt werden (obwohl es zunächst so scheint als ob diese Probleme nichts miteinander zu tun hätten!).

Die Galoistheorie befasst sich mit Körpererweiterungen und übersetzt die Klassifikation gewisser Körpererweiterungen mithilfe der sogenannten Galoisgruppen in die Klassifikation endlicher Gruppen. Daher werden wir im ersten Teil der Vorlesung Gruppentheorie behandeln. Um die Grundlagen von Körpererweiterungen zu verstehen und Galoisgruppen berechnen zu können, wird etwas Ringtheorie benötigt. Daher werden wir im zweiten Teil der Vorlesung Ringtheorie behandeln. Im dritten Teil werden wir dann die Theorie der Körpererweiterungen inklusive elementarer Galoistheorie behandeln. Zum Abschluss werden wir uns mit Anwendungen der Galoistheorie beschäftigen.

Weitere Anwendungen der Algebra, auf die wir eingehen werden, sind:

- Lösung von Zählproblemen mithilfe von Gruppentheorie
- Verschlüsselung mithilfe von Ringtheorie
- Datensicherung mithilfe der Theorie endlicher Körper

Diese Anwendungen zeigen, dass die Algebra auch außerhalb der theoretischen Mathematik vielseitig einsetzbar ist. Diese Vielseitigkeit basiert auf der zugrundeliegenden Abstraktion – nur Theorien, die geeignet abstrahiert sind, können so vielseitig angewendet werden!

Zusätzlich ist die Algebra ein zentraler Baustein innerhalb der theoretischen Mathematik und dient als Grundlage für

- die algebraische Zahlentheorie,
- die algebraische Geometrie,
- die „brave new algebra“ von Ringspektren in der Homotopietheorie,
- ...

sowie als algebraisches Pendant zur Überlagerungstheorie in der Topologie.

Anmerkung für Lehramtsstudenten. Auf ganz natürliche Weise werden wir dabei Begriffen und Themen aus der Schulmathematik begegnen und diese vertiefen. Zudem begnegnen wir Aspekten der Mathematik, die in Zukunft Bestandteil der Schulmathematik werden könnten. Wichtiger als die Beherrschung des aktuellen Lehrplans ist es, ein solides Fundament zu erlernen, das es erlaubt, Mathematik inhaltlich korrekt, nachvollziehbar und souverän zu lehren und auf das der Unterricht im Rahmen des aktuellen und der zukünftigen Lehrpläne aufbauen kann.

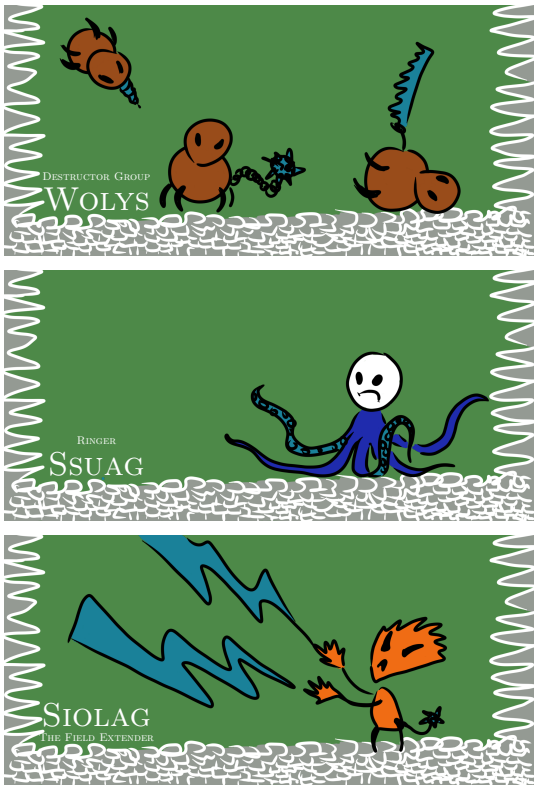
Insbesondere haben die folgenden Themen der Vorlesung Algebra einen direkten Bezug zu derzeitigem Schulstoff:

- Konstruierbarkeit mit Zirkel und Lineal
- Lösbarkeit polynomialer Gleichungen
- Grundlagen der Teilbarkeitstheorie bzw. von Primelementen
- Anwendungen im Alltag

Anmerkung zum Lernen (Angst vor Algebra?!)**.** Algebra mag zunächst schwierig erscheinen, weil sie sehr abstrakt wirkt. Man sollte sich davon auf keinen Fall abschrecken oder entmutigen lassen:

- Viele der Konzepte aus dieser Vorlesung lassen sich an konkreten einfachen Beispielen ausprobieren.
- Wenn man sich an den Abstraktionsgrad gewöhnt hat, wird man feststellen, dass er viele Vorzüge besitzt.

Mit Übung und etwas Mut lassen sich die Themen der Algebra bezwingen und genießen!



Anmerkung zum Lernen (Skript)**.** Dieses Vorlesungsskript dokumentiert den Fortschritt dieser Vorlesung, die besprochenen Themen und zusätzliches optionales Material. Der Besuch der Vorlesung erleichtert es, die Entwicklung der Begriffe, Beweise, etc. nachzuvollziehen. Zusätzliches Material wird in GRIPS und auf der Vorlesungshomepage bereitgestellt:

https://loeh.app.ur.de/teaching/algebra_ws2526

Anhänge und Ausblicke sind *nicht* prüfungsrelevant, sondern dienen der Allgemeinbildung.

Dieses Skript dokumentiert die in der Vorlesung behandelten Inhalte. Es dient keineswegs dazu, den Besuch der Vorlesung oder gar der Übungen zu ersetzen. Außerdem spiegelt sich in diesem Skript nur ein kleiner Ausschnitt der Algebra wider. Sie sollten sich unbedingt auch mithilfe anderer Quellen (Bücher!) selbst ein Bild des gesamten Gebietes machen!

Referenzen der Form „Satz I.6.5.12“ oder „Satz II.2.4.34“ verweisen auf die entsprechende Stelle im Skript zur Linearen Algebra I bzw. II:

https://loeh.app.ur.de/teaching/linalg1_ws2425/lecture_notes.pdf
https://loeh.app.ur.de/teaching/linalg2_ss25/lecture_notes.pdf

Die Algebra baut auf den Grundkenntnissen der Linearen Algebra auf. Lücken in der Linearen Algebra sollten Sie also zügig füllen.

Anmerkung zum Lernen (Fingerübungen)**.** Dieses Vorlesungsskript enthält einige Selbsttests und Fingerübungen, deren Feedback teilweise in die PDF-Datei integriert ist. Diese Funktionalität beruht auf PDF Layers (nicht auf JavaScript) und wird von vielen PDF-Viewern unterstützt, z.B. Acrobat Reader, Evince, Foxit Reader, Okular, ... Einfacher Test, ob das funktioniert: Haben Sie auf “Nein” gedrückt?

Ja Nein Nein, Sie haben nicht getan, was Sie behauptet haben

Sie sollten natürlich erst dann die Hinweise und Antworten ansehen, wenn Sie bereits über das Problem nachgedacht haben; man kann schließlich nie wissen, was passiert, wenn man voreilig auf irgendeinen Knopf drückt.

GROAAARR!

Literaturaufgabe (Bibliothek)**.** Wie finden Sie im Regensburger Katalog und in der Teilbibliothek Mathematik Literatur über die Themen der Vorlesung? Welche weiteren Informationsquellen könnten nützlich sein?

Zusätzliche Anregungen finden Sie auf S. vii.

Konvention. Die Menge $\mathbb{N}$ der natürlichen Zahlen enthält 0.

1

Gruppen

Gruppen sind algebraische Strukturen, die (das Verhalten von) Symmetrien von Objekten aller Art modellieren. Wir wiederholen die Grundbegriffe für Gruppen und präsentieren grundlegende Konstruktionen von Gruppen. Außerdem werden wir die Verallgemeinerung von Symmetriegruppen zu Gruppenoperationen betrachten. Dies nutzen wir unter anderem dazu, ein besseres Verständnis der Struktur endlicher Gruppen zu erhalten. Dies wird insbesondere auch für die erfolgreiche Anwendung der Galoistheorie nötig sein.

Überblick über dieses Kapitel.

1.1	Die Kategorie der Gruppen	8
1.2	Gruppenoperationen	42
1.3	Struktur endlicher Gruppen	53

Schlüsselbeispiel. endliche abelsche Gruppen, symmetrische Gruppen, Diedergruppen, Sylowgruppen

1.1 Die Kategorie der Gruppen

Die Kategorie der Gruppen besteht aus Gruppen und Gruppenhomomorphismen. Wir wiederholen zunächst kurz, aufbauend auf Monoiden, die Grundbegriffe und erklären den Zusammenhang mit Symmetrie- und Automorphismengruppen. Danach untersuchen wir Untergruppen, Erzeugendensysteme und Quotientengruppen genauer. Als wichtige weitere Konstruktion betrachten wir semi-direkte Produkte.

1.1.1 Vorbereitung: Monoide und Monoidhomomorphismen

Monoide sind eine grundlegende algebraische Struktur, die Verknüpfungen aller Art modelliert. Der Vorzug der Abstraktion zu Monoiden liegt darin, dass wir jede allgemein für Monoide gezeigte Aussage auf jeden Monoid anwenden können und nicht in jedem einzelnen Fall neu beweisen müssen. Dies sorgt für eine robustere, übersichlichere und effizientere Theorie. Zum Beispiel können wir in allen kommutativen Monoiden, die additiv bzw. multiplikativ geschrieben werden, Summen- und Produktnotationen wie in Notation I.2.1.13 einführen. Viele weitere algebraische Strukturen bauen auf dem Begriff des Monoids auf, z.B. Gruppen, Ringe und Körper.

Definition 1.1.1 (Monoid)**.** Ein *Monoid* ist ein Tripel $(M, \cdot, e)$, bestehend aus

- einer Menge M,
- einer Abbildung $\cdot\colon M \times M \longrightarrow M$,
- einem Element e,

mit folgenden Eigesnchaften:

- *Assoziativität.* Für alle $x, y, z \in M$ gilt
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$
- *Neutrales Element.* Für alle $x \in M$ gilt
$$x \cdot e = x \quad \text{und} \quad x = e \cdot x.$$

Der Monoid $(M, \cdot, e)$ heißt *kommutativ*, wenn für alle $x, y \in M$ gilt, dass
$$x \cdot y = y \cdot x.$$

Ist $x \in M$, so heißt x *(in* $(M, \cdot, e)$ *invertierbar*, wenn x ein *Inverses* besitzt, d.h., wenn es ein Element $y \in M$ mit folgender Eigenschaft gibt:

$$x \cdot y = e \quad \text{und} \quad e = y \cdot x$$

Notation 1.1.2. Falls die Daten der Verknüpfung $\cdot$ und des neutralen Elements e aus dem Kontext klar sind, sagt man auch kurz „Sei M ein Monoid ...“ etc.

Beispiel 1.1.3 (Monoidstrukturen auf den natürlichen Zahlen)**.**

- Es ist $(\mathbb{N}, +, 0)$ ein kommutativer Monoid. Dabei ist ? 0 das einzige invertierbare Element von $(\mathbb{N}, +, 0)$.
- Es ist $(\mathbb{N}, \cdot, 1)$ ein kommutativer Monoid. Dabei ist ? 1 das einzige invertierbare Element von $(\mathbb{N}, \cdot, 1)$.
- Die Tripel

$$\big(\mathbb{N}, (m,n) \mapsto m^n, 1\big)$$
$$\big(\mathbb{N}, (m,n) \mapsto m^2 + n^2, 0\big)$$

  sind *keine* Monoide (nachrechnen!).

Beispiel 1.1.4 (Selbstabbildungen als Monoid)**.** Sei X eine Menge und sei $\mathrm{Abb}(X, X)$ die Menge aller Abbildungen $X \longrightarrow X$. Dann ist das Tripel $(\mathrm{Abb}(X, X), \circ, \mathrm{id}_X)$ ein Monoid (Bemerkung I.1.5.21).

Ein Element $f\colon X \longrightarrow X$ dieses Monoids ist genau dann invertierbar, wenn ? die Abbildung $f\colon X \longrightarrow X$ bijektiv ist (Proposition I.1.5.29).

Im allgemeinen ist der Monoid $(\mathrm{Abb}(X, X), \circ, \mathrm{id}_X)$ *nicht* kommutativ, denn: Für $X := \{1, 2, 3\}$ betrachten wir die Abbildungen

$$f := (1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3)$$
$$g := (1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2).$$

Dann ist $g \circ f \neq f \circ g$, denn

$$g \circ f(1) = g\big(f(1)\big) = g(2) = 3 \neq 2 = f(1) = f\big(g(1)\big) = f \circ g(1).$$

Beispiel 1.1.5 (Wörter als Monoid)**.** Sei Σ eine Menge und sei Σ^* die Menge aller Wörter über Σ. Ein *Wort über* Σ ist dabei eine endliche Folge aus Elementen von Σ, d.h. eine Abbildung vom Typ $\{1, \ldots, n\} \longrightarrow \Sigma$, wobei $n \in \mathbb{N}$. Sei $\varepsilon \in \Sigma^*$ das *leere Wort* und sei $*\colon \Sigma^* \times \Sigma^* \longrightarrow \Sigma^*$ die Abbildung, die die gegebenen Wörter „hintereinanderschreibt“. Dann ist $(\Sigma^*, *, \varepsilon)$ ein Monoid.

Das einzige invertierbare Element dieses Monoids ist ε. Im allgemeinen ist dieser Monoid *nicht* kommutativ, denn: Sei $X := \{\mathrm{a}, \ldots, \mathrm{z}\}$. Dann ist

$$\mathrm{hunde} * \mathrm{kuchen} = \mathrm{hundekuchen} \neq \mathrm{kuchenhunde} = \mathrm{kuchen} * \mathrm{hunde}.$$

Proposition 1.1.6 (Eindeutigkeit des neutralen Elements und von Inversen)**.** *Sei $(M, \cdot, e)$ ein Monoid.*

1. *Sei $e' \in M$ mit*
$$\forall_{x \in M} \quad x \cdot e' = x.$$
Dann folgt $e' = e$.

2. *Sei $e' \in M$ mit*
$$\forall_{x \in M} \quad e' \cdot x = x.$$
Dann folgt $e' = e$.

3. *Sei $x \in M$ invertierbar. Dann besitzt x genau ein Inverses; dieses wird mit x^{-1} bezeichnet.*

4. *Insbesondere ist $(x^{-1})^{-1} = x$.*

5. *Sind $x, y \in M$ invertierbar, so ist auch $x \cdot y$ invertierbar und*
$$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}. \qquad \textit{(Reihenfolge!)}$$

Beweis. Es handelt sich hierbei um Standardargumente, wie wir sie bereits in der Linearen Algebra kennengelernt haben (Proposition I.2.1.30, Proposition I.2.1.31). □

Notation 1.1.7. In additiv notierten Monoiden bezeichnen wir das Inverse von invertierbaren Elementen x mit $-x$.

Anmerkung zum Lernen. Falls Sie sich nicht daran erinnern können, wie man die obigen Aussagen beweist, ist es eine gute Übung, sich selbst am Beweis zu versuchen (und bei Bedarf im Material zur Linearen Algebra nachzuschlagen).

Wie jede algebraische Theorie besitzt die Theorie der Monoide neben Objekten (den Monoiden) auch strukturerhaltende Morphismen zwischen solchen Objekten. Diese sind die sogenannten Monoidhomomorphismen.

Definition 1.1.8 (Monoidhomomorphismus)**.** Seien M, N Monoide.

- Ein *Monoidhomomorphismus* $M \longrightarrow N$ ist eine Abbildung $f \colon M \longrightarrow N$ mit folgenden Eigenschaften:
  - *Verträglichkeit mit der Verknüpfung.* Für alle $x, y \in M$ gilt
  $$f(x \cdot y) = f(x) \cdot f(y).$$
  - *Verträglichkeit mit dem neutralen Element.* Es gilt
  $$f(e) = e.$$

- Ein *Monoidisomorphismus* $M \longrightarrow N$ ist ein Monoidhomomorphismus $f\colon M \longrightarrow N$, für den es einen Monoidhomomorphismus $g\colon N \longrightarrow M$ mit $f \circ g = \mathrm{id}_N$ und $g \circ f = \mathrm{id}_M$ gibt.

Beispiel 1.1.9 (Monoidhomomorphismen)**.** Sind die folgenden Abbildungen Monoidhomomorphismen?

- Die Abbildung $(\mathbb{N}, +, 0) \longrightarrow (\mathbb{N}, +, 0)$, $n \longmapsto 2026 \cdot n$.

  Ja Nein Die korrekte Antwort ist „Ja“. ×
- Die Abbildung $(\mathbb{N}, +, 0) \longrightarrow (\mathbb{N}, +, 0)$, $n \longmapsto 2026 + n$.

  Ja Nein Die korrekte Antwort ist „Nein“. (neutrales Element?). ×
- Die Abbildung $(\{\mathrm{a}, \mathrm{b}\}^*, *, \varepsilon) \longrightarrow (\{\mathrm{a}, \mathrm{b}\}^*, *, \varepsilon)$, $x \longmapsto x * x$.

  Ja Nein Die korrekte Antwort ist „Nein“. (da abab $\neq$ aabb) ×

Beispiel 1.1.10 (ein Monoidhomomorphismus)**.** Die Abbildung

$$\begin{aligned} \mathbb{N} &\longrightarrow \{\mathrm{a}\}^* \\ n &\longmapsto \underbrace{\mathrm{a} \ldots \mathrm{a}}_{n\text{-mal}} \end{aligned}$$

ist ein Monoidhomomorphismus $(\mathbb{N}, +, 0) \longrightarrow (\{\mathrm{a}\}^*, *, \varepsilon)$ (nachrechnen!).

Proposition 1.1.11 (Monoidhomomorphismen, grundlegende Eigenschaften)**.**

1. *Ist M ein Monoid, so ist $\mathrm{id}_M\colon M \longrightarrow M$ ein Monoidhomomorphismus.*
2. *Die Komposition von Monoidhomomorphismen ist ein Monoidhomomorphismus.*
3. *Sind M und N Monoide, ist $f\colon M \longrightarrow N$ ein Monoidhomomorphismus und ist $x \in M$ invertierbar in M, so ist auch $f(x)$ in N invertierbar und*
$$\big(f(x)\big)^{-1} = f(x^{-1}).$$

Beweis. Die ersten beiden Aussagen ergeben sich durch direktes Nachrechnen.

Zu 3. Sei $y := f(x^{-1})$. Wir zeigen, dass y das Inverse von $f(x)$ ist, indem wir die entsprechenden Gleichungen etablieren. Es gilt

$$\begin{aligned} f(x) \cdot y &= f(x) \cdot f(x^{-1}) && \text{(Definition von } y\text{)} \\ &= f(x \cdot x^{-1}) && (f \text{ ist ein Monoidhomomorphismus}) \\ &= f(e) && (x^{-1} \text{ ist invers zu } x) \\ &= e. && (f \text{ ist ein Monoidhomomorphismus}) \end{aligned}$$

Mit einer analogen Rechnung ergibt sich $y \cdot f(x) = e$ (nachrechnen!). Also ist $f(x)$ invertierbar, mit Inversem y. □

1.1.2 Gruppen und Gruppenhomomorphismen

Wir bauen den Gruppenbegriff auf dem Begriff des Monoids auf. Gruppen sind Monoide, in denen jedes Element invertierbar ist. Gruppenhomomorphismen sind Monoidhomomorphismen zwischen Gruppen.

Definition 1.1.12 (Gruppe, abelsche Gruppe)**.** Eine *Gruppe* ist ein Monoid $(G, \cdot, e)$ mit der folgenden Eigenschaft: Jedes Element aus G besitzt ein Inverses in $(G, \cdot, e)$.

Eine Gruppe heißt *abelsch*, wenn sie (als Monoid) kommutativ ist.

Beispiel 1.1.13 (Gruppen)**.** Aus der Linearen Algebra kennen wir bereits einige Beispiele von Gruppen:

- Es ist $(\mathbb{Z}, +, 0)$ eine abelsche Gruppe, aber $(\mathbb{N}, +, 0)$ und $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$ sind *keine* Gruppen.
- Ist $(K, +, \cdot, 0, 1)$ ein Körper, so sind $(K, +, 0)$ und $(K \setminus \{0\}, \cdot, 1)$ abelsche Gruppen.
- Ist $n \in \mathbb{Z}$, so bildet $\mathbb{Z}/n$ bezüglich repräsentantenweiser Addition modulo n und dem neutralen Element $[0]$ eine (abelsche) Gruppe.

  Zur Erinnerung: Es ist $\mathbb{Z}/n = \{k + n \cdot \mathbb{Z} \mid k \in \mathbb{Z}\} = \{[0], \ldots, [n-1]\}$ und die Addition ist durch

  $$\begin{aligned} \mathbb{Z}/n \times \mathbb{Z}/n &\longrightarrow \mathbb{Z}/n \\ (k + n \cdot \mathbb{Z}, m + n \cdot \mathbb{Z}) &\longmapsto \big((k+m) + n \cdot \mathbb{Z}\big) \end{aligned}$$

  gegeben. Die abelsche Gruppe $\mathbb{Z}/12$ kann verwendet werden, um die Arithmetik von Stunden oder Halbtönen zu modellieren; die abelsche Gruppe $\mathbb{Z}/7$ kann verwendet werden, um die Arithmetik von Wochentagen zu modellieren (Beispiel II.2.3.18).
- Allgemeiner kann jeder $\mathbb{Z}$-Modul als abelsche Gruppe bezüglich Addition aufgefasst werden (und umgekehrt).
- Ist X eine Menge, so bildet die Menge S_X aller Bijektionen $X \longrightarrow X$ eine Gruppe bezüglich Komposition und id_X, die *symmetrische Gruppe von* X (Beispiel I.2.2.21). Enthält X mindestens drei verschiedene Elemente x, y, z, so ist S_X *nicht* abelsch, denn die Transpositionsbijektionen, die x und y bzw. y und z miteinander vertauschen, kommutieren *nicht*.

  Ist $n \in \mathbb{N}$, so schreiben wir

  $$S_n := S_{\{1,\ldots,n\}}.$$

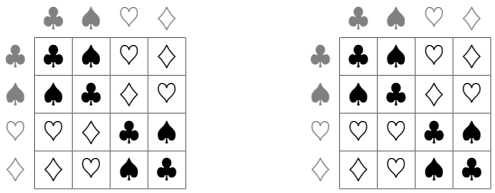


Abbildung 1.1.: Verknüpfungstabellen

Die symmetrische Gruppe S_n tritt zum Beispiel in der Formulierung der Leibniz-Formel (Satz I.5.4.17) auf und spielt für das Verständnis der Struktur endlicher Gruppen eine wesentliche Rolle.

Beispiel 1.1.14 (Verknüpfungstabellen)**.** Gruppen mit wenigen Elementen können beschrieben werden, indem man die Verknüpfungsabbildung als Tabelle darstellt. Zum Beispiel liefern die Tabellen in Abbildung 1.1 für die Menge $G := \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$ Abbildungen

$$G \times G \longrightarrow G.$$

Die linke Tabelle definiert eine Gruppenstruktur auf G mit neutralem Element $\clubsuit$ (nachrechnen; kennen Sie eine angenehmere Beschreibung dieser Gruppe?!); die rechte Tabelle erfüllt jedoch für kein potentielles neutrales Element alle Gruppenaxiome (Übungsaufgabe).

Definition 1.1.15 (Gruppenhomomorphismus, Gruppenisomorphismus, Kern, Bild)**.** Seien G, H Gruppen.

- Ein *Gruppenhomomorphismus* $G \longrightarrow H$ ist eine Monoidhomomorphismus $G \longrightarrow H$ der unterliegenden Monoide (Definition 1.1.8).
- Ein *Gruppenisomorphimus* $G \longrightarrow H$ ist ein Isomorphismus $G \longrightarrow H$ der unterliegenden Monoide (Definition 1.1.8).
- Gibt es einen Gruppenisomorphismus $G \longrightarrow H$, so nennen wir die Gruppen G und H *isomorph* und schreiben $G \cong_{\mathsf{Group}} H$.
- Wir definieren *Kern* und *Bild* eines Gruppenhomomorphismus $f\colon G \longrightarrow H$ durch

$$\ker f := \big\{g \in G \;\big|\; f(g) = e\big\} \subset G,$$
$$\operatorname{im} f := \big\{f(g) \;\big|\; g \in G\big\} \subset H.$$

Beispiel 1.1.16 (Gruppenhomomorphismen)**.**

- Ist $n \in \mathbb{Z}$, so ist die Multiplikationsabbildung

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto n \cdot x \end{aligned}$$

ein Gruppenhomomorphismus; das Bild ist $n \cdot \mathbb{Z}$ und ist $n \neq 0$, so ist der Kern $\{0\}$. Die Abbildung

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto x^2 \end{aligned}$$

ist *kein* Gruppenhomomorphismus, denn

$$f(1+1) = f(2) = 4 \neq 2 = 1 + 1 = f(1) + f(1).$$

- Allgemeiner gilt: Ist A eine abelsche Gruppe und $n \in \mathbb{Z}$, so ist

$$\begin{aligned} A &\longrightarrow A \\ x &\longmapsto n \cdot x := \begin{cases} \sum_{j=1}^{n} x & \text{falls } n \geq 0 \\ -\sum_{j=1}^{-n} x & \text{falls } n < 0 \end{cases} \end{aligned}$$

ein Gruppenhomomorphismus.

- Insbesondere: Ist K ein Körper und $n \in \mathbb{Z}$, so ist

$$\begin{aligned} K^\times &\longrightarrow K^\times \\ x &\longmapsto x^n \end{aligned}$$

ein Gruppenhomomorphismus der Einheitengruppe $K^\times$ (bezüglich Multiplikation, mit dem neutralen Element 1) von K. Im allgemeinen ist dieser Gruppenhomomorphismus weder injektiv noch surjektiv.

- Die Abbildungen

$$\begin{aligned} \exp\colon \mathbb{R} &\longrightarrow \mathbb{R}_{>0} \\ \ln\colon \mathbb{R}_{>0} &\longrightarrow \mathbb{R} \end{aligned}$$

sind zueinander inverse Gruppenisomorphismen, wobei wir auf $\mathbb{R}$ die Addition als Verknüpfung betrachten (mit neutralem Element 0) und auf $\mathbb{R}_{>0}$ die Multiplikation (mit neutralem Element 1). Dass es sich dabei um Gruppenisomorphismen handelt, wird im Rahmen der Analysis gezeigt. Diese Isomorphismen sind die Grundlage für Rechenschieber (Übungsaufgabe).

- Bis auf Isomorphie gibt es genau eine Gruppe mit nur einem Element, „die“ *triviale Gruppe*; je nach Kontext bezeichnen wir diese mit $\{e\}$ oder $\{1\}$ oder $\{0\}$.
- Die Gruppe aus Beispiel 1.1.14 ist isomorph zur abelschen Gruppe $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ (nachrechnen).

Proposition 1.1.17 (Gruppenhomomorphismen, grundlegende Eigenschaften)**.** *Seien G und H Gruppen und sei $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann gilt:*

1. *Für alle $x \in G$ ist $f(x^{-1}) = \big(f(x)\big)^{-1}$.*
2. *Ist $f'\colon G \longrightarrow H$ eine Abbildung mit*

$$\forall_{x,y\in G} \quad f'(x \cdot y) = f'(x) \cdot f'(y),$$

   so ist f' bereits ein Gruppenhomomorphismus.
3. *Die Abbildung f ist genau dann injektiv, wenn $\ker f = \{e\}$ ist.*
4. *Die Abbildung f ist genau dann surjektiv, wenn $\operatorname{im} f = H$ ist.*
5. *Der Gruppenhomomorphismus f ist genau dann ein Gruppenisomorphismus $G \longrightarrow H$, wenn f bijektiv ist.*
6. *Kompositionen von Gruppenhomomorphismen sind Gruppenhomomorphismen.*
7. *Kompositionen von Gruppenisomorphismen sind Gruppenisomorphismen.*

Beweis. Zu 1. Dies folgt aus der entsprechenden Aussage für Monoidhomomorphismen (Proposition 1.1.11), da jedes Element in G invertierbar ist.

Zu 2. Es gilt $f'(e) = e$, denn: Sei $h := f'(e)$. Wir zeigen zunächst, dass $h \cdot h = h$ gilt: Da f' mit den Verknüpfungen verträglich ist, folgt

$$h \cdot h \overset{?}{=} f'(e) \cdot f'(e) = f'(e \cdot e) = f'(e) = h.$$

Durch Multiplikation mit dem Inversen h^{-1} von links erhalten wir daraus

$$h \overset{?}{=} e \cdot h = h^{-1} \cdot h \cdot h = h^{-1} \cdot h = e.$$

Also ist $f'(e) = h = e$, wie behauptet.

Die anderen Aussagen folgen mit Argumenten, die wir bereits so ähnlich in der linearen Algebra für lineare Abbildungen gesehen haben (nachrechnen). □

Caveat 1.1.18. Die analogen Aussagen für den zweiten bzw. dritten Teil aus der obigen Proposition 1.1.17 gelten im allgemeinen *nicht* für Monoidhomomorphismen.

1.1.3 Automorphismengruppen

Das Konzept und die Axiomatisierung der Gruppen ist ursprünglich aus der Beobachtung entstanden, dass gewisse Mengen von rückgängig-machbaren Transformationen von geometrischen oder algebraischen Objekten in denselben abstraken Rahmen passen. Viele interessante Beispiele von Gruppen treten kanonisch in dieser Form als Gruppen von invertierbaren Transformationen auf. Umgekehrt ist es in vielen Situationen so, dass die algebraischen Eigenschaften solcher Gruppen interessante geometrische/algebraische Eigenschaften des unterliegenden Objekts widerspiegeln.

Beispiel 1.1.19 (symmetrische Gruppen)**.** In der Mengenlehre sind invertierbare (d.h. bijektive) Abbildungen die relevanten invertierbaren Transformationen. Ist X eine Menge, so kann man die symmetrische Gruppe S_X daher auch als „Symmetriegruppe“ der Menge X auffassen.

Beispiel 1.1.20 (spezielle/allgemeine lineare Gruppe)**.** In der linearen Algebra sind ? Vektorraumisomorphismen die relevanten invertierbaren Transformationen. Ist K ein Körper und ist V ein K-Vektorraum, so bildet

$$\mathrm{Aut}_K(V) := \{f \mid f\colon V \longrightarrow V \text{ ist ein } K\text{-Vektorraumisomorphismus}\}$$

eine Gruppe bezüglich Abbildungskomposition, mit neutralem Element id_V (nachrechnen). Ist $n \in \mathbb{N}$, so sind die damit verwandten Konstrukte

$$\mathrm{GL}_n(K) := \big\{A \in \mathrm{M}_{n\times n}(K) \;\big|\; A \text{ invertierbar}\big\} \quad (\textit{allgemeine lineare Gruppe})$$
$$\mathrm{SL}_n(K) := \big\{A \in \mathrm{GL}_n(K) \;\big|\; \det A = 1\big\} \quad (\textit{spezielle lineare Gruppe})$$

Gruppen bezüglich Matrixmultiplikation, mit neutralem Element I_n. Der Matrizenkalkül für lineare Abbildungen liefert einen kanonischen Isomorphismus $\mathrm{Aut}_K(K^n) \cong_{\mathsf{Group}} \mathrm{GL}_n(K)$ (die Spalten ...).

Ist $n \in \mathbb{N}_{>0}$, so zeigen die grundlegenden Eigenschaften der Determinante (Kapitel I.5.4), dass $\det\colon \mathrm{M}_{n\times n}(K) \longrightarrow K$ ein Monoidhomomorphismus (bezüglich Matrixmultiplikation und der Multiplikation auf K) und $\det|_{\mathrm{GL}_n(K)}\colon \mathrm{GL}_n(K) \longrightarrow K^\times$ ein Gruppenhomomorphismus ist. Dabei ist

$$\mathrm{SL}_n(K) = \ker(\det|_{\mathrm{GL}_n(K)}).$$

Beispiel 1.1.21 (Isometriegruppen)**.** Im Kontext von metrischer Geometrie bzw. metrischen Räumen, sind ? Isometrien (abstandserhaltende invertierbare Abbildungen) die relevanten invertierbaren Transformationen. Ist (X, d) ein metrischer Raum, so bildet

$$\mathrm{Isom}(X, d) := \{f \mid f\colon (X, d) \longrightarrow (X, d) \text{ ist eine Isometrie}\}$$

eine Gruppe bezüglich Abbildungskomposition mit neutralem Element id_X (nachrechnen), die *Isometriegruppe von* (X,d).

Ist $x \in X$, so ist auch $\mathrm{Isom}(X,d)_x := \{f \in \mathrm{Isom}(X,d) \mid f(x) = x\}$ eine Gruppe (nachrechnen). Zum Beispiel kann man zeigen, dass

$$\mathrm{Isom}(\mathbb{R}^n, d_2)_0 \cong_{\mathsf{Group}} \mathrm{O}(n)$$

für alle $n \in \mathbb{N}$ gilt [19, Satz 3.4.5]; dabei ist

$$\begin{aligned}\mathrm{O}(n) &:= \left\{A \in \mathrm{GL}_n(\mathbb{R}) \;\middle|\; L(A) \in \mathrm{Isom}(\mathbb{R}^n, \|\cdot\|_2)\right\}\\ &= \left\{A \in \mathrm{M}_{n\times n}(\mathbb{R}) \;\middle|\; A^{\mathsf{T}} \cdot A = I_n\right\}\end{aligned}$$

die *orthogonale Gruppe* (Korollar II.1.2.17). Die Gruppen $\mathrm{O}(2)$ und $\mathrm{O}(3)$ sind also ein essentieller Baustein der euklidischen ebenen bzw. räumlichen Geometrie und ihre Elemente lassen sich konkret durch geeignete Spiegelungen und Rotationen beschreiben (Satz II.1.2.18).

Die Isometriegruppen regulärer Polygone werden wir noch genauer untersuchen (Proposition 1.1.70).

Beispiel 1.1.22 (Galoisgruppe)**.** Sei L ein Körper und sei $K \subset L$ ein Teilkörper (z.B. $\mathbb{R} \subset \mathbb{C}$). Dann ist

$$\begin{aligned}\mathrm{Gal}(L,K) := \big\{f\colon L \longrightarrow L \;\big|\;& \\ & f \text{ ist ein invertierbarer Körperhomomorphismus} \\ & \text{mit } f|_K = \mathrm{id}_K\big\}\end{aligned}$$

eine Gruppe bezüglich Abbildungskomposition mit neutralem Element id_L (nachrechnen). Diese Gruppe bezeichnet man als *Galoisgruppe der Körpererweiterung* $K \subset L$.

Das Hauptziel dieser Vorlesung ist, gewisse Körpererweiterungen mithilfe von Galoisgruppen zu verstehen. Es wird daher also nötig sein, so viel Gruppentheorie zu entwickeln, dass unser Wissen über Gruppen ausreicht, um in der Galoistheorie interessante Aussagen abzuleiten. Insbesondere wird es uns damit gelingen, viele klassische Fragen zu beantworten (Kapitel 3.5).

Beispiel 1.1.23 (Automorphismengruppe)**.** Auch innerhalb der Gruppentheorie können wir Gruppen invertierbarer Transformationen betrachten; in der Gruppentheorie sind diese Transformationen Gruppenisomorphismen. Genauer: Sei G eine Gruppe. Einen Gruppenisomorphismus $G \longrightarrow G$ bezeichnet man auch als *Automorphismus von* G. Dann bildet

$$\mathrm{Aut}(G) := \{f \mid f\colon G \longrightarrow G \text{ ist ein Automorphismus}\}$$

eine Gruppe bezüglich Komposition mit neutralem Element id_G (nachrechnen), die *Automorphismengruppe von* G.

Ist $g \in G$, so ist

$$\begin{aligned} c_g \colon G &\longrightarrow G \\ h &\longmapsto g \cdot h \cdot g^{-1} \end{aligned}$$

die *Konjugationsabbildung bezüglich g*; diese ist ein Automorphismus von G (Übungsaufgabe). Man bezeichnet die Konjugationsabbildungen auch als *innere Automorphismen von G*.

Anmerkung zum Lernen (griechische Bausteine für den Morphismen-Zoo)**.** Man kann sich die Begriffsbildung zu Morphismen leicht merken, wenn man die griechischen Bausteine kennt:

griechisch	deutsch	Eselsbrücke
ἴσος	gleich	Isotop
μόνος	allein	Monolog
ἐπί	auf, darauf	Epidermis
ἔνδον	innerhalb	Endoskopie
αὐτός	selbst	Automobil

Bemerkung 1.1.24 (allgemeine Automorphismengruppen)**.** Die obigen Beispiele folgen alle demselben allgemeinen Muster: es handelt sich dabei um Automorphismengruppen in Kategorien (Anhang A.2).

- Ist C eine Kategorie und ist $X \in \mathrm{Ob}(C)$, so ist

  $$\mathrm{Aut}_C(X) := \big\{ f \in \mathrm{Mor}_C(X,X) \;\big|\; f \text{ ist ein Isomorphismus in } C \big\}$$

  eine Gruppe bezüglich der Komposition von Morphismen in C; dies ist die *Automorphismengruppe von X in C*.

- Umgekehrt gilt: Ist G eine Gruppe, so gibt es eine Kategorie C und ein Objekt $X \in \mathrm{Ob}(C)$ mit $G = \mathrm{Aut}_C(X)$. Zum Beispiel kann man die Kategorie C so konstruieren, dass sie nur ein Objekt X enthält, dass $\mathrm{Mor}_C(X,X) = G$ ist und dass die Komposition von Morphismen in C gerade als Verknüpfung in G definiert ist (Beispiel A.2.6).

Anmerkung zum Lernen. Fallen Ihnen noch weitere Instanzen dieses Prinzips ein? Jedesmal, wenn Sie im Studium eine neue Theorie kennenlernen, sollten Sie sich überlegen, was die zugehörigen Automorphismengruppen sind!

1.1.4 Untergruppen

Wie in vielen anderen Theorien (Vektorräume, Moduln, metrische Räume, topologische Räume, ...) ist es auch in der Gruppentheorie sinnvoll, geeignete Unterobjekte zu betrachten. Analog zur Definition von Untervektorräumen formulieren wir die folgende Definition:

Definition 1.1.25 (Untergruppe)**.** Sei $(G, \cdot, e)$ eine Gruppe. Eine *Untergruppe von* G ist eine Teilmenge $H \subset G$ mit folgenden Eigenschaften:

- Die Verknüpfungsabbildung $\cdot\colon G \times G \longrightarrow G$ schränkt sich zu einer Abbildung $\cdot H \times H \longrightarrow H$ ein.
- Es ist $e \in H$.
- Die Menge H bildet bezüglich der eingeschränkten Verknüpfung eine Gruppe.

Ist H eine Untergruppe von G, so schreibt man dafür oft auch $H < G$.

Anmerkung zum Lernen (Unter...)**.** Die Definition von Untervektorräumen folgt einem allgemeinen Prinzip: Im Normalfall erhält man aus der Definition von *Irgendwas* die Definition von *Unter-Irgendwas*, indem man eine geeignete Teilmenge betrachtet und verlangt, dass sich die Struktur des großen Irgendwas auf diese Teilmenge einschränkt und die Teilmenge mit dieser eingeschränkten Struktur die Bedingungen der Definition von Irgendwas erfüllt. Auf diese Weise erhält man auch den Begriff Untergruppe, Untermodul, Untermannigfaltigkeit, Teilkörper, Teilraum (im Sinne der Topologie), ...

Proposition 1.1.26 (Charakterisierung von Untergruppen)**.** *Sei* $(G, \cdot)$ *eine Gruppe und sei* $H \subset G$ *eine nicht-leere Teilmenge. Dann ist* H *genau dann eine Untergruppe von* G*, wenn folgende Bedingungen beide erfüllt sind:*

① *Für alle* $x, y \in H$ *gilt* $x \cdot y \in H$*.*

② *Für alle* $x \in H$ *ist* $x^{-1} \in H$*.*

Beweis. Wir verfahren analog zum Beweis der entsprechenden Charakterisierung für Untervektorräume (Proposition I.3.2.3):

Ist H eine Untergruppe von G, so sind die beiden Bedingungen nach Definition erfüllt.

Es erfülle umgekehrt $H \subset G$ die beiden obigen Bedingungen. Dann ist H eine Untergruppe von G, denn: Da die Bedingung ① erfüllt ist, schränkt sich die Verknüpfungsabbildung auf G zu einer Abbildung auf H ein.

1. Die Assoziativität der Verknüpfung vererbt sich von G auf H.
2. Es ist $e \in H$, denn: Wegen $H \neq \emptyset$ gibt es ein $x \in H$. Nach ② ist dann auch $x^{-1} \in H$. Also ist
$$e = x \cdot x^{-1} \in H$$
nach ①. Außerdem ist dieses Element auch für die auf H eingeschränkte Verknüpfung neutral.
3. Nach ② besitzt jedes Element aus H ein Inverses in H.

Also ist H eine Untergruppe von G. □

Beispiel 1.1.27 (Untergruppen, generische Beispiele)**.**

- Ist G eine Gruppe (mit neutralem Element e), so gibt es immer die folgenden Untergruppen von G:
  - klein? die *triviale Untergruppe* $\{e\}$;
  - groß? die Gruppe G selbst.
- Sei G eine Gruppe. Sind H und K Untergruppen von G, so ist auch $H \cap K$ eine Untergruppe von G (nachrechnen); allgemeiner sind Durchschnitte über nicht-leere Familien von Untergruppen von G wieder Untergruppen (nachrechnen).

  Im allgemeinen ist die Vereinigung von Untergruppen von G jedoch *keine* Untergruppe von G !
- Ist G eine Gruppe und sind $H, K \subset G$ mit $K < H$ und $H < G$, so ist K auch eine Untergruppe von G (nachrechnen).
- Ist $f\colon G \longrightarrow H$ eine Gruppenhomomorphismus, so ist das Bild im f eine Untergruppe von H und der Kern $\ker f$ ist eine Untergruppe von G (nachrechnen).

Beispiel 1.1.28 (Untergruppen, konkrete Beispiele)**.**

- Wir haben die folgende Kette von Untergruppen (jeweils bezüglich Addition):
$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}.$$
- Ist $n \in \mathbb{Z}$, so ist $n \cdot \mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ (bezüglich Addition). Allgemeiner gilt: Untermoduln von $\mathbb{Z}$-Moduln entsprechen Untergruppen der zugehörigen additiven abelschen Gruppen.
- Ist $n \in \mathbb{N}$, so ist $\mathrm{O}(n)$ eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$.
- Ist K ein Körper und $n \in \mathbb{N}_{>0}$, so ist $\mathrm{SL}_n(K)$ eine Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}_n(K)$, nämlich der Kern der Determinantenabbildung $\det|_{\mathrm{GL}_n(K)}\colon \mathrm{GL}_n(K) \longrightarrow K^\times$ (Beispiel 1.1.20).
- Ist (X, d) ein metrischer Raum und $x \in X$, so ist $\mathrm{Isom}(X, d)_x$ eine Untergruppe von $\mathrm{Isom}(X, d)$.

Die Klassifikation der Vektorräume erfolgt über die Dimension. Die Gruppentheorie ist deutlich komplizierter. Ein erster Schritt zum Verständnis der „Größe“ von Untergruppen im Vergleich zur umgebenden Gruppe ist der Index; der Index misst, „wie oft“ die gegebene Untergruppe in die umgebende Gruppe passt (Abbildung 1.2):

Definition 1.1.29 (Linksnebenklasse, Index)**.** Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe.

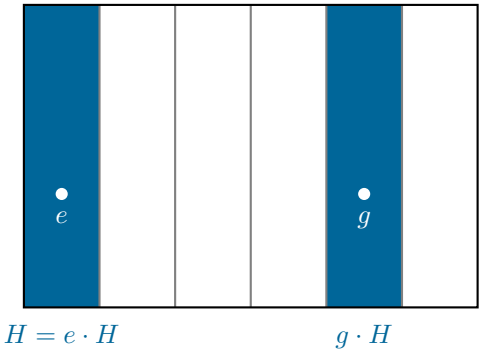


Abbildung 1.2.: Linksnebenklassen, schematisch

- Ist $g \in G$, so schreiben wir $g \cdot H := \{g \cdot h \mid h \in H\}$ für die *Linksnebenklasse von g bezüglich H*.
- Die Anzahl (bzw. Kardinalität)

$$[G : H] := \#\{g \cdot H \mid g \in G\}$$

bezeichnet man als *Index von H in G*.

Anmerkung zum Lernen. Untervektorräume bilden (additive) Untergruppen von Untervektorräumen. Warum haben wir uns in der linearen Algebra nicht mit dem zugehörigen Index von Untervektorräumen beschäftigt?!

Bemerkung 1.1.30 (Linksnebenklassen als Äquivalenzklassen)**.** Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe. Dann betrachten wir die Relation $\sim_H$ auf G definiert durch

$$\sim_H := \left\{(g, g') \in G \times G \;\middle|\; g^{-1} \cdot g' \in H\right\}$$

Diese Relation $\sim_H$ auf G ist eine Äquivalenzrelation und die Äquivalenzklassen bezüglich $\sim_H$ sind genau die Linksnebenklassen von H in G (Übungsaufgabe). Insbesondere gilt also:

- Für alle $g_1, g_2 \in G$ ist $g_1 \cdot H = g_2 \cdot H$ oder $g_1 \cdot H \cap g_2 \cdot H = \emptyset$.
- Es ist

$$G = \bigcup (G/\sim_H)$$

eine disjunkte Vereinigung. Man schreibt auch G/H für die Menge $G/\sim_H$ der Äquivalenzklassen von $\sim_H$. Also ist $[G : H] = \#(G/H)$.

Analog kann man natürlich mit Rechtsnebenklassen $H \cdot g$ mit $g \in G$ verfahren.

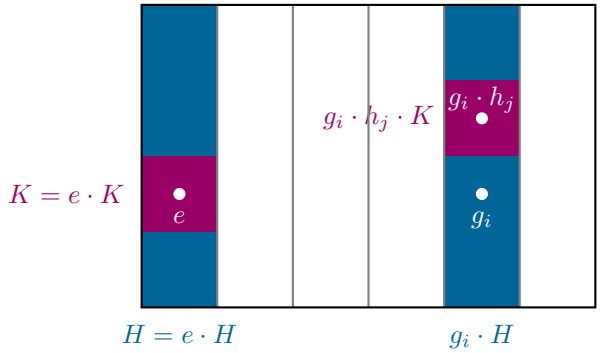


Abbildung 1.3.: Der Satz von Lagrange, schematisch

Beispiel 1.1.31 (Index von Untergruppen)**.**

- Ist G eine Gruppe, so ist $[G : \{e\}] =$? $\#G$ und $[G : G] =$? 1.
- Sei $n \in \mathbb{N}_{>0}$. Dann hat $n\cdot\mathbb{Z}$ als Untergruppe von $\mathbb{Z}$ den Index ? n. Die Linksnebenklassen entsprechen genau den n verschiedenen Restklassen bei Division von ganzen Zahlen durch n.

  Die triviale Untergruppe $\{0\}$ von $\mathbb{Z}$ hat in $\mathbb{Z}$ den Index ? ∞, denn jede Linksnebenklasse besteht nur aus einem Element in $\mathbb{Z}$.
- Sei $n \in \mathbb{N}$. Die spezielle orthogonale Gruppe $\mathrm{SO}(n)$ hat in $\mathrm{O}(n)$ den Index ? 2 (Satz II.1.2.18)).

Satz 1.1.32 (Satz von Lagrange)**.** *Sei G eine Gruppe und seien $H \subset G$, $K \subset H$ Untergruppen. Dann gilt*

$$[G : K] = [G : H] \cdot [H : K].$$

Insbesondere: Falls H endlichen Index in G hat und K endlichen Index in H hat, so hat auch K endlichen Index in G.

Beweis. Wir argumentieren mit Repräsentantensystemen. Sei $(g_i)_{i\in I}$ ein Repräsentantensystem für $\sim_H$ auf G, d.h. die Familie enthält für jede Linksnebenklasse von H in G genau ein Element; sei $(h_j)_{j\in J}$ ein Repräsentantensystem für $\sim_K$ auf H. Insbesondere gilt also

$$\#I = [G : H] \quad \text{und} \quad \#J = [H : K]$$

und es genügt zu zeigen, dass $(g_i \cdot h_j)_{(i,j)\in I\times J}$ ein Repräsentantensystem für $\sim_K$ auf G ist (Abbildung 1.3).

- Jede Linksnebenklasse von K in G besitzt einen solchen Repräsentanten: Sei $g \in G$. Da $(g_i)_{i\in I}$ ein Repräsentantensystem für H in G ist, gibt es ein $i \in I$ mit ${g_i}^{-1} \cdot g \in H$. Da $(h_j)_{j\in J}$ ein Repräsentantensystem für K in H ist, gibt es ein $j \in J$ mit ${h_j}^{-1} \cdot g_i^{-1} \cdot g \in K$. Also ist
$$(g_i \cdot h_j)^{-1} \cdot g = h_j^{-1} \cdot g_i^{-1} \cdot g \in K.$$
- Jede Linksnebenklasse von K in G besitzt nicht mehr als einen solchen Repräsentanten: Seien also $(i,j),(i',j') \in I \times J$ mit $(g_{i'} \cdot h_{j'})^{-1} \cdot (g_i \cdot h_j) \in K$ bzw.
$$g_i \cdot h_j \cdot K = g_{i'} \cdot h_{j'} \cdot K.$$
Dann folgt (durch Multiplikation mit H von rechts), dass $g_i \cdot H = g_{i'} \cdot H$, und damit $i = i'$ bzw. $g_i = g_{i'}$. Aus der obigen Gleichung erhalten wir somit $h_j \cdot K = h_{j'} \cdot K$, und damit $j = j'$. Also ist $(i,j) = (i',j')$.

Somit ist $(g_i \cdot h_j)_{(i,j)\in I\times J}$ ein Repräsentantensystem für $\sim_K$ auf G, und wir erhalten
$$[G : K] = \#(I \times J) = \#I \cdot \#J = [G : H] \cdot [H : K],$$
wie behauptet. □

Beispiel 1.1.33. Ist $p \in \mathbb{N}$ prim und ist K eine Untergruppe einer Gruppe G mit $[G : K] = p$, so gibt es *keine* Untergruppe $H \subset G$ mit
$$K < H < G \quad \text{und} \quad K \neq H \neq G,$$
denn sonst wäre $[G : H]$ ein nicht-trivialer Teiler der Primzahl $[G : K] = p$.

Korollar 1.1.34 (Satz von Lagrange für endliche Gruppen)**.** *Sei G eine endliche Gruppe und $H \subset G$ eine Untergruppe. Dann gilt*
$$\#G = [G : H] \cdot \#H$$
und insbesondere ist $\#H$ ein Teiler von $\#G$.

Beweis. Wir wollen den Satz von Lagrange (Satz 1.1.32) auf eine geeignete Kette von Untergruppen anwenden. Wie können wir die Anzahlen $\#G$ und $\#H$ mit dem Index von Untergruppen in Verbindung bringen? Für die triviale Untergruppe $\{e\}$ gilt (Beispiel 1.1.31)
$$\big[G : \{e\}\big] = \#G \quad \text{und} \quad \big[H : \{e\}\big] = \#H.$$
Wir wenden den Satz von Lagrange auf die Kette $K := \{e\} < H < G$ von Untergruppen an. Nach dem Satz von Lagrange gilt also
$$\#G = [G : K] = [G : H] \cdot [H : K] = [G : H] \cdot \#H.$$ □

Caveat 1.1.35. Der Satz von Lagrange (Korollar 1.1.34) liefert nur notwendige Bedingungen für die Existenz von Untergruppen, aber keine hinreichenden!

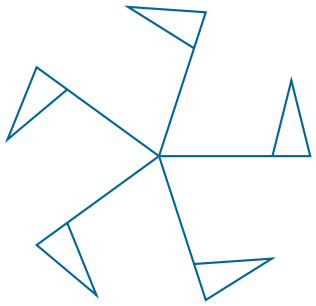


Abbildung 1.4.: Eine Teilmenge von $\mathbb{R}^2$, deren Isometriegruppe isomorph zu $\mathbb{Z}/5$ ist (nachrechnen).

Beispiel 1.1.36. Sei $X \subset \mathbb{R}^2$ eine Teilmenge, die nicht in einer (affinen) Gerade enthalten ist, mit der Eigenschaft, dass die Isometriegruppe $\mathrm{Isom}(X, d_2)$ endlich ist und aus einer ungeraden Anzahl von Elementen besteht (ein Beispiel ist in Abbildung 1.4 gegeben). Zur Erinnerung: Ein *affiner Unterraum* eines Vektorraums V ist eine Menge der Form $v+U$, wobei $v \in V$ und $U \subset V$ ein Untervektorraum ist.

Dann gibt es *keine* Spiegelung $s\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ (an einer affinen Geraden) mit $s(X) = X$, denn: *Angenommen,* es gäbe eine solche Spiegelung s. Wegen $s^2 = \mathrm{id}_{\mathbb{R}^2}$ wäre dann $H := \{\mathrm{id}_X, s|_X\}$ eine Untergruppe von $\mathrm{Isom}(X, d_2)$. Dabei ist $\#H = 2$, denn $s|_X \neq \mathrm{id}_X$ (da X nicht in einer affinen Geraden enthalten ist). Nach dem Satz von Lagrange (Korollar 1.1.34) müsste $\#H = 2$ somit ein Teiler der ungeraden Zahl $\#\,\mathrm{Isom}(X, d_2)$ sein, was nicht sein kann. Also gibt es *keine* solche Spiegelung s.

1.1.5 Erzeugendensysteme

In der linearen Algebra beschreiben wir (Unter)Vektorräume oft durch geeignete Erzeugendensysteme, anstatt *alle* Elemente einzeln anzugeben. Analog können wir auch (Unter)Gruppen durch Erzeugendensysteme beschreiben:

Definition 1.1.37 (erzeugte Untergruppe, Erzeugendensystem, zyklische Gruppe)**.** Sei G eine Gruppe und sei $S \subset G$.

- Dann ist
$$\langle S\rangle_G := \bigcap_{H \in U_S(G)} H$$
die *von S erzeugte Untergruppe von G*. Dabei bezeichnet $U_S(G) \subset P(G)$ die Menge aller Untergruppen H von G mit $S \subset H$ (insbesondere ist $G \in U_S(G)$).

- Ist $\langle S\rangle_G = G$, so ist S ein *Erzeugendensystem von* G.
- Falls G ein endliches Erzeugendensystem besitzt, ist G *endlich erzeugt*.
- Falls G ein ein-elementiges Erzeugendensystem besitzt, ist G eine *zyklische Gruppe*.

Nach Beispiel 1.1.27 handelt es sich bei $\langle S\rangle_G$ tatsächlich um eine Untergruppe von G.

Bemerkung 1.1.38 (explizite Beschreibung erzeugter Untergruppen)**.** Sei G eine Gruppe und $S \subset G$ eine Teilmenge. Nach Definition ist $\langle S\rangle_G$ die (bezüglich Inklusion) kleinste Untergruppe von G, die S enthält. Dabei gilt

$$\langle S\rangle_G = \left\{ s_1^{\varepsilon_1} \cdot \dots \cdot s_n^{\varepsilon_n} \;\middle|\; n \in \mathbb{N},\ s_1, \dots, s_n \in S,\ \varepsilon_1, \dots, \varepsilon_n \in \{-1, +1\} \right\}.$$

Dies zeigt man analog zum Fall von Vektorräumen (Proposition I.3.2.12).

Bemerkung 1.1.39 („Geraden“ in der Gruppentheorie)**.** In der Linearen Algebra sind Untervektorräume, die von einem (nicht-trivialen) Element erzeugt werden, mit dem geometrischen Konzept der Geraden verwandt. In der Gruppentheorie übernehmen (nicht-triviale) zyklische Untergruppen eine ähnliche Rolle. Da Gruppen jedoch deutlich wilder sein können als Vektorräume, ist auch die Interaktion zwischen zyklischen Untergruppen komplizierter als die Interaktion zwischen Geraden in Vektorräumen.

Beispiel 1.1.40 (Erzeugendensysteme)**.**

- Es ist $\langle\{1\}\rangle_{\mathbb{Z}} = ?\ \mathbb{Z}$, $\langle\{2,3\}\rangle_{\mathbb{Z}} = ?\ \mathbb{Z}$, aber $\langle\{2\}\rangle_{\mathbb{Z}} = ?\ 2\cdot\mathbb{Z} \neq \mathbb{Z}$.
- Sei $n \in \mathbb{N}_{>0}$. Dann ist (nachrechnen, Abbildung 1.5)
$$\langle\{e^{2\cdot\pi\cdot i/n}\}\rangle_{\mathbb{C}^\times} \cong_{\mathsf{Group}} \mathbb{Z}/n.$$
- Ist X eine Menge, so ist die symmetrische Gruppe S_X genau dann endlich erzeugt, wenn X endlich ist: Ist X endlich, so ist S_X endlich, und damit insbesondere endlich erzeugt. Ist X unendlich, so ist S_X im Gegensatz zu endlich erzeugten Gruppen überabzählbar (nachrechnen).

Caveat 1.1.41 (Freiheit und das Wortproblem)**.** Die Theorie der linearen Algebra ist deshalb so gutartig und algorithmisch zugänglich, weil jeder Vektorraum besonders einfache Erzeugendensysteme besitzt, nämlich Basen (bzw. freie Erzeugendensysteme). Viele der grundlegenden Begriffe, Tatsachen und Techniken beruhen auf dieser Tatsache.

Die analogen Aussagen in der Gruppentheorie sind *nicht* zutreffend: Im allgemeinen besitzen Gruppen *keine* sogenannten freien Erzeugendensysteme (Anhang A.3). Dies hat weitreichende Konsequenzen:

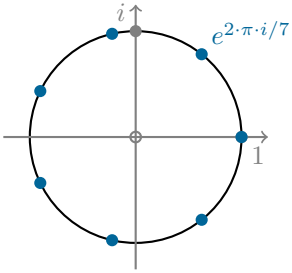


Abbildung 1.5.: Eine endliche zyklische Gruppe in $\mathbb{C}^\times$

- Gruppen und Gruppenelemente sind im allgemeinen *nicht* algorithmisch behandelbar. Genauer gilt die *Unlösbarkeit des Wortproblems*: Man kann beweisen, dass es keine solchen Algorithmen für allgemeine (endlich erzeugte bzw. sogar endliche präsentierte) Gruppen gibt [27, Chapter 12].
- Die Konstruktion, Beschreibung und Klassifikation von Gruppenhomomorphismen ist komplizierter als die Theorie der linearen Abbildungen.

Ausblick 1.1.42 (Cayleygraphen und Geometrische Gruppentheorie)**.** Die Kombinatorik bzw. Geometrie von Erzeugendensystemen kann sehr kompliziert sein; eine Möglichkeit, diese Kombinatorik einzufangen, sind sogenannte Cayley-Graphen [20]: Ist G eine Gruppe und $S \subset G$ ein Erzeugendensystem, so ist der zugehörige *Cayleygraph* wie folgt definiert:

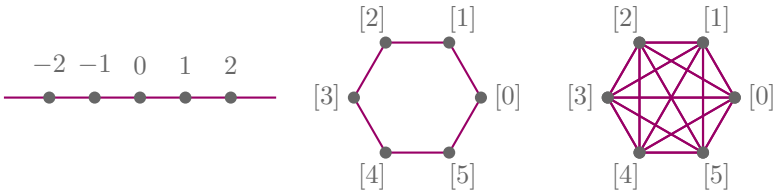
$$\mathrm{Cay}(G,S) := \big(G, \{\{g, g\cdot s\} \mid g \in G, s \in (S \cup S^{-1}) \setminus \{e\}\}\big);$$

die Knoten von $\mathrm{Cay}(G,S)$ sind also die Gruppenelemente von G und je zwei Knoten werden genau dann durch eine Kante verbunden, wenn sich die zugehörigen Gruppenelemente um ein (Inverses von einem) Element aus S durch Multiplikation von rechts unterscheiden. Einfache Beispiele für Cayleygraphen finden sich in Abbildung 1.6.

Die *Geometrische Gruppentheorie* untersucht systematisch die Geometrie von Cayleygraphen und den Zusammenhang zwischen geometrischen und algebraischen Eigenschaften von Gruppen [20].

1.1.6 Quotientengruppen

Als nächsten Schritt betrachten wir Quotientengruppen. Wie im Fall von Quotientenvektorräumen (Proposition I.3.5.16) ist es manchmal günstig, den



$\mathrm{Cay}(\mathbb{Z}, \{1\})$ $\mathrm{Cay}(\mathbb{Z}/6, \{[1]\})$ $\mathrm{Cay}(\mathbb{Z}/6, \mathbb{Z}/6)$

Abbildung 1.6.: Beispiele für Cayleygraphen

Quotienten einer Gruppe nach einer Untergruppe zu betrachten, indem man alles „vergisst“, was in dieser Untergruppe passiert. Quotientengruppen liefern insbesondere einen ersten Schritt, um die Struktur endlicher Gruppen durch einfache Bausteine zu beschreiben.

Ist G eine Gruppe und H eine Untergruppe, so haben wir bereits die Menge G/H der Linksnebenklassen von H in G kennengelernt. Es ist naheliegend, auf diesem Quotienten G/H eine Gruppenstruktur mithilfe der Gruppenstruktur auf G zu definieren. An dieser Stelle ergibt sich – im Vergleich zur Vektorraumtheorie – ein kleines Problem:

Caveat 1.1.43. Ist G eine Gruppe und $H \subset G$, so bildet G/H im allgemeinen *keine* Gruppe bezüglich repräsentantenweiser Verknüpfung! Genauer gesagt, funktioniert diese Konstruktion genau dann, wenn H ein sogenannter Normalteiler in G ist (Proposition 1.1.47).

Definition 1.1.44 (Normalteiler)**.** Sei G eine Gruppe. Eine Untergruppe $N \subset G$ ist ein *Normalteiler in* G (oder *normal in* G), wenn

$$\forall_{n \in N} \quad \forall_{g \in G} \quad g \cdot n \cdot g^{-1} \in N$$

ist. Ist N ein Normalteiler in G, so schreibt man auch $N \lhd G$.

Beispiel 1.1.45 (Normalteiler, generische Beispiele)**.**

- Ist G eine Gruppe, so gibt es immer die folgenden Normalteiler von G:
  - klein? die triviale Untergruppe $\{e\}$;
  - groß? die Gruppe G selbst.
- Ist G abelsch, so ist jede Untergruppe ein Normalteiler in G (nachrechnen).
- Sei G eine Gruppe. Sind H und K Normalteiler von G, so ist auch $H \cap K$ ein Normalteiler von G (nachrechnen); allgemeiner sind Durchschnitte über nicht-leere Familien von Normalteilern von G wieder Normalteiler (nachrechnen).

- Ist G eine Gruppe und sind $H, K \subset G$ Untergruppen mit $K \lhd H$ und $H \lhd G$, so ist K im allgemeinen *kein* Normalteiler in G.

- Ist $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus, so ist $\ker f$ ein Normalteiler, denn: Wir wissen bereits, dass $\ker f$ eine Untergruppe von G ist (Beispiel 1.1.27). Außerdem gilt für alle $n \in \ker f$ und alle $g \in G$ wegen

$$f(g \cdot n \cdot g^{-1}) \overset{?}{=} f(g) \cdot f(n) \cdot f(g)^{-1} = f(g) \cdot e \cdot f(g)^{-1} = f(g) \cdot f(g)^{-1} = e$$

  auch $g \cdot n \cdot g^{-1} \in \ker f$.

  Es gilt sogar auch die Umkehrung: Jeder Normalteiler ist Kern eines geeigneten Gruppenhomomorphismus (Bemerkung 1.1.49).

Beispiel 1.1.46 (Normalteiler, konkrete Beispiele)**.**

- Ist $n \in \mathbb{Z}$, so ist $n \cdot \mathbb{Z}$ ein Normalteiler in $\mathbb{Z}$, da $\mathbb{Z}$ abelsch ist.

- Ist $n \in \mathbb{N}$, so ist die alternierende Gruppe

$$A_n = \{\sigma \in S_n \mid \operatorname{sgn} \sigma = 1\}$$

  ein Normalteiler in S_n, denn: Nach Definition ist A_n der Kern der Signumsabbildung $\operatorname{sgn}\colon S_n \longrightarrow \{-1, 1\}$ (wobei wir $\{-1, 1\}$ als Gruppe bezüglich Multiplikation auffassen, Proposition I.5.4.20).

- Die Untergruppe $H := \{\mathrm{id}, \tau\}$ von S_3 mit $\tau := (1\ 2)$, d.h.

$$\begin{aligned} \tau\colon \{1,2,3\} &\longrightarrow \{1,2,3\} \\ 1 &\longmapsto 2 \\ 2 &\longmapsto 1 \\ 3 &\longmapsto 3 \end{aligned}$$

  ist *kein* Normalteiler in S_3, denn: Sei $\sigma \in S_3$ die Permutation, die 1, 2, 3 zyklisch durchtauscht. Dann ist

$$\sigma \circ \tau \circ \sigma^{-1} = (2\ 3) \notin H.$$

- Ist K ein Körper und $n \in \mathbb{N}_{>0}$, so ist $\mathrm{SL}_n(K)$ ein Normalteiler in $\mathrm{GL}_n(K)$, nämlich der Kern von $\det|_{\mathrm{GL}_n(K)}\colon \mathrm{GL}_n(K) \longrightarrow K^\times$.

Normalteiler erlauben es, Quotientengruppen zu konstruieren, und diese besitzen die erwartetet universelle Eigenschaft:

Proposition 1.1.47 (Quotientengruppe)**.** *Sei G eine Gruppe und sei $N \subset G$ eine Untergruppe.*

1. *Es ist*

$$\begin{aligned} G/N \times G/N &\longrightarrow G/N \\ (g \cdot N, h \cdot N) &\longmapsto (g \cdot h) \cdot N \end{aligned}$$

genau dann eine wohldefinierte Abbildung, wenn N ein Normalteiler in G ist.

2. *Falls N ein Normalteiler ist, so ist G/N eine Gruppe bezüglich dieser Verknüpfung mit neutralem Element $e \cdot N$, die* Quotientengruppe von G modulo N.

Beweis. Sei N ein Normalteiler in G. Dann ist die obige Verknüpfung wohldefiniert, denn: Es ist zu zeigen, dass ? die obige Definition *nicht* von den gewählten Repräsentanten abhängt. Seien $g, h, g', h' \in G$ mit

$$g \cdot N = g' \cdot N \quad \text{und} \quad h \cdot N = h' \cdot N;$$

also gibt es $n, m \in N$ mit

$$g' = g \cdot n \quad \text{und} \quad h' = h \cdot m.$$

Somit erhalten wir

$$\begin{aligned} (g' \cdot h') \cdot N &= (g \cdot n \cdot h \cdot m) \cdot N \\ &= (g \cdot n \cdot h) \cdot N && (\text{da } m \in N) \\ &= \big(g \cdot h \cdot (h^{-1} \cdot n \cdot h)\big) \cdot N. \end{aligned}$$

Da N ein Normalteiler ist, ist $n' := h^{-1} \cdot n \cdot h = h^{-1} \cdot n \cdot (h^{-1})^{-1} \in N$, und es folgt

$$\begin{aligned} (g' \cdot h') \cdot N &= (g \cdot h \cdot n') \cdot N \\ &= (g \cdot h) \cdot N && (\text{da } n' \in N) \end{aligned}$$

bzw. $(g \cdot h) \cdot N = (g' \cdot h') \cdot N$. Also ist die obige Verknüpfung auf G/N wohldefiniert.

Dass es sich dabei um eine Gruppenstruktur auf G/N handelt, erhält man aus den entsprechenden Eigenschaften der Verknüpfung auf G (nachrechnen).

Sei umgekehrt die obige Verknüpfung auf G/N wohldefiniert. Dann ist N ein Normalteiler in G, denn: Sei $n \in N$ und $g \in G$. Dann ist $g \cdot N = (g \cdot n) \cdot N$ und mit der Wohldefiniertheit folgt

$$\begin{aligned} N &= (g \cdot g^{-1}) \cdot N \\ &= (g \cdot n \cdot g^{-1}) \cdot N; \end{aligned}$$

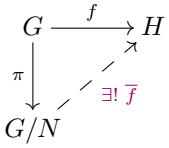
insbesondere ist $g \cdot n \cdot g^{-1} \in N$. Also ist N ein Normalteiler in G. □

Proposition 1.1.48 (Quotientengruppe, universelle Eigenschaft)**.** *Sei N ein Normalteiler in G. Dann ist die kanonische Projektion*

$$\begin{aligned} \pi\colon G &\longrightarrow G/N \\ g &\longmapsto g \cdot N \end{aligned}$$

ein Gruppenhomomorphismus mit $\ker \pi = N$ und G/N erfüllt zusammen mit π die folgende universelle Eigenschaft: Für jede Gruppe H und jeden Gruppenhomomorphismus $f\colon G \longrightarrow H$ mit $N \subset \ker f$ gibt es genau einen Gruppenhomomorphismus $\overline{f}\colon G/N \longrightarrow H$ mit

$$\overline{f} \circ \pi = f.$$



Beweis. Nach Konstruktion der Gruppenstruktur auf G/N ist π ein Gruppenhomomorphismus und offenbar ist $\ker \pi = N$.

Sei H eine Gruppe und sei $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus mit $N \subset \ker f$. Dann ist

$$\begin{aligned} \overline{f}\colon G/N &\longrightarrow H \\ g \cdot N &\longmapsto f(g) \end{aligned}$$

ein wohldefinierter (wegen $N \subset \ker f$, nachrechnen) Gruppenhomomorphismus (nachrechnen) mit $\overline{f} \circ \pi = f$ (nach Konstruktion). Die Eindeutigkeit von $\overline{f}$ ergibt sich direkt aus der Surjektivität von π. □

Anmerkung zum Lernen (universelle Eigenschaft von Quotienten)**.** Vergleichen Sie diese universelle Eigenschaft mit der universellen Eigenschaft von Quotientenvektorräumen, Quotientenmoduln, Quotientenräumen in der Topologie, ... In all diesen Fällen ist es einfach, Abbildungen *aus Quotienten heraus* zu konstruieren/beschreiben.

Bemerkung 1.1.49 (Normalteiler = Kerne)**.** Sei G eine Gruppe und sei $N \subset G$ eine Untergruppe. Dann ist N genau dann ein Normalteiler in G, wenn es eine Gruppe H und einen Gruppenhomomorphismus $f\colon G \longrightarrow H$ mit $\ker f = N$ gibt, denn:

- Ist N der Kern eines Gruppenhomomorphismus, so ist N ein Normalteiler (Beispiel 1.1.45).
- Ist N eine Normalteiler, so ist N der Kern des kanonischen Projektionshomomorphismus $G \longrightarrow G/N$ (Proposition 1.1.48).

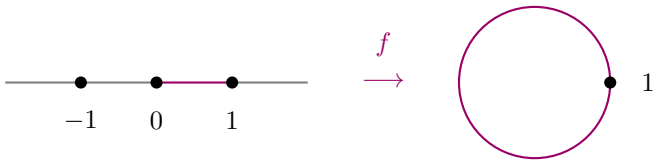


Abbildung 1.7.: Die Gruppe $S^1 \cong \mathbb{R}/\mathbb{Z}$

Beispiel 1.1.50 (zyklische Gruppen)**.** Sei $n \in \mathbb{N}$. Dann ist $n\cdot\mathbb{Z}$ ein Normalteiler in $\mathbb{Z}$ und $\mathbb{Z}/n \cong_{\mathsf{Group}} \mathbb{Z}/n\cdot\mathbb{Z}$; diese Gruppe ist zyklisch, erzeugt von ? [1].

Korollar 1.1.51 (Homomorphiesatz)**.** *Ist $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus, so ist*

$$\begin{aligned} \overline{f}\colon G/\ker f &\longrightarrow \operatorname{im} f \\ g\cdot(\ker f) &\longmapsto f(g) \end{aligned}$$

ein wohldefinierter Gruppenisomorphismus.

Beweis. Wir erhalten die Wohldefiniertheit von $\overline{f}$ aus der universellen Eigenschaft des Quotienten $G/\ker f$. Nach Konstruktion ist der Homomorphismus $\overline{f}$ surjektiv und injektiv (da der Kern trivial ist; nachrechnen), und damit ein Gruppenisomorphismus (Proposition 1.1.17). □

Beispiel 1.1.52 (die Gruppe S^1)**.** Die Teilmenge

$$S^1 := \left\{ z \in \mathbb{C} \;\middle|\; |z| = 1 \right\}$$

ist eine Gruppe bezüglich Multiplikation (nachrechnen). Der Gruppenhomomorphismus (Abbildung 1.7)

$$\begin{aligned} f\colon \mathbb{R} &\longrightarrow S^1 \\ t &\longmapsto e^{2\cdot\pi\cdot i\cdot t} \end{aligned}$$

ist surjektiv und $\ker f = \mathbb{Z}$ (s. Analysis). Also ist $S^1 \cong_{\mathsf{Group}} \mathbb{R}/\mathbb{Z}$.

Beispiel 1.1.53 (Signum)**.** Sei $n \in \mathbb{N}_{>1}$. Dann induziert die Signumsabbildung $\operatorname{sgn}\colon S_n \longrightarrow \{-1,1\}$ nach dem Homomorphiesatz einen Isomorphismus

$$S_n/A_n = S_n/\ker\operatorname{sgn} \cong_{\mathsf{Group}} \operatorname{im}\operatorname{sgn} \cong_{\mathsf{Group}} \mathbb{Z}/2.$$

Beispiel 1.1.54 (Determinante)**.** Sei K ein Körper und $n \in \mathbb{N}_{>0}$. Dann induziert die Determinantenabbildung $\det|_{\mathrm{GL}_n(K)}\colon \mathrm{GL}_n(K) \longrightarrow K^\times$ nach dem Homomorphiesatz einen Isomorphismus

$$\mathrm{GL}_n(K)/\mathrm{SL}_n(K) = \mathrm{GL}_n(K)/\ker(\det|_{\mathrm{GL}_n(K)}) \cong_{\mathsf{Group}} \operatorname{im}(\det|_{\mathrm{GL}_n(K)}) = K^\times.$$

Als erste Anwendung von Quotientengruppen betrachten wir zyklische (Unter-)Gruppen genauer:

Definition 1.1.55 (Ordnung)**.** Sei G eine Gruppe und sei $g \in G$. Dann ist

$$\operatorname{ord}(g) := \min\{n \in \mathbb{N}_{>0} \mid g^n = e\} \in \mathbb{N}_{>0} \cup \{\infty\}$$

die *Ordnung von* g (wobei wir die Konvention $\min \emptyset := \infty$ verwenden).

Beispiel 1.1.56 (Ordnung)**.**

- Das Element $1 \in \mathbb{Z}$ hat Ordnung ? ∞ in $(\mathbb{Z}, +, 0)$.
- Die Transposition $(1\ 2) \in S_3$ hat Ordnung ? 2.
- Der Zyklus $(1\ 2\ 3) \in S_3$ hat Ordnung ? 3.

Proposition 1.1.57 (Ordnung und zyklische Gruppen)**.** *Sei G eine Gruppe und sei $g \in G$.*

1. *Ist $d := \operatorname{ord} g$ endlich, so ist*

$$\begin{aligned} \mathbb{Z}/d &\longrightarrow \langle g \rangle_G \\ [k] &\longmapsto g^k \end{aligned}$$

   ein wohldefinierter Gruppenisomorphismus.

2. *Ist $\operatorname{ord} g = \infty$, so ist*

$$\begin{aligned} \mathbb{Z} &\longrightarrow \langle g \rangle_G \\ k &\longmapsto g^k \end{aligned}$$

   ein Gruppenisomorphismus.

Beweis. Die Idee ist, den Homomorphiesatz (Korollar 1.1.51) auf einen geeigneten Gruppenhomomorphismus anzuwenden. Wir betrachten den Gruppenhomomorphismus

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow G \\ k &\longmapsto g^k. \end{aligned}$$

Dann ist $\operatorname{im} f = \langle g \rangle_G$ (nachrechnen). Was ist mit $\ker f$?

① Wir betrachten zunächst den Fall, dass $d := \operatorname{ord} g$ endlich ist. Dann ist $\ker f = d \cdot \mathbb{Z}$, denn: Ist $k \in d \cdot \mathbb{Z}$, so gibt es ein $n \in \mathbb{Z}$ mit $k = d \cdot n$, und damit ist

$$f(k) = ? \quad f(d \cdot n) = g^{d \cdot n} = (g^d)^n = e^n = e.$$

Sei umgekehrt $k \in \ker f$. Dann ist $g^k = f(k) = e$. Um k und d zu verbinden, betrachten wir Division von k mit Rest durch d; dies liefert $n \in \mathbb{Z}$ und $r \in \{0, \dots, d-1\}$ mit $k = d \cdot n + r$. Also ist

$$e = g^k = g^{d \cdot n + r} = (g^d)^n \cdot g^r = e^n \cdot g^r = g^r.$$

Die Definition von $d = \operatorname{ord} g$ liefert somit $r = 0$. Also ist $k = d \cdot n$, und damit $k \in d \cdot \mathbb{Z}$.

Mit dem Homomorphiesatz (Korollar 1.1.51) erhalten wir somit, dass f den gewünschten Isomorphismus $\mathbb{Z}/d = \mathbb{Z}/\ker f \cong_{\mathsf{Group}} \langle g \rangle_G$ induziert.

② Ist $\operatorname{ord} g = \infty$, so ist $\ker f = \{0\}$ (nachrechnen). Mit dem Homomorphiesatz (Korollar 1.1.51) folgt daher, dass f den gewünschten Isomorphismus $\mathbb{Z} \cong \mathbb{Z}/\{0\} = \mathbb{Z}/\ker f \cong_{\mathsf{Group}} \langle g \rangle_G$ induziert. □

Korollar 1.1.58 (Klassifikation der zyklischen Gruppen)**.** *Ist G eine zyklische Gruppe, so gibt es genau ein $n \in \mathbb{N}$ mit $G \cong_{\mathsf{Group}} \mathbb{Z}/n$.*

Beweis. Sei G eine zyklische Gruppe und sei $g \in G$ mit $\langle g \rangle_G = G$.

- *Existenz.* Dann gibt es ein $n \in \mathbb{N}$ mit $G = \langle g \rangle_G \cong_{\mathsf{Group}} \mathbb{Z}/n$ (Proposition 1.1.57).
- *Eindeutigkeit.* Da die Mächtigkeit einer Gruppe eine Isomorphieinvariante ist (Gruppenisomorphismen sind bijektiv! Proposition 1.1.17), folgt, dass n eindeutig bestimmt ist. □

Korollar 1.1.59 (Satz von Lagrange für Ordnungen)**.** *Sei G eine endliche Gruppe und $g \in G$. Dann ist die Ordnung* $\operatorname{ord} g$ *ein Teiler von $\#G$; insbesondere ist $g^{\#G} = e$.*

Beweis. Wir führen dies auf den Satz von Lagrange für endliche Gruppen zurück: Dazu betrachten wir die Untergruppe $H := \langle \{g\} \rangle_G$. Nach Proposition 1.1.57 gilt $\#H = \operatorname{ord} g$. Mit dem Satz von Lagrange für endliche Gruppen (Korollar 1.1.34) folgt daher, dass $\operatorname{ord} g = \#H$ ein Teiler von $\#G$ ist. □

Caveat 1.1.60. Die Umkehrung gilt im allgemeinen *nicht*. Zum Beispiel ist 6 ein Teiler von $\#S_3$, aber S_3 enthält *kein* Element der Ordnung 6.

Beispiel 1.1.61 (Standard-Lagrange-Argumente)**.**

- Sei $g \in \mathbb{Z}/2027 \setminus \{[0]\}$. Da 2027 prim ist, folgt mit dem Satz von Lagrange für Ordnungen (Korollar 1.1.59), dass $\operatorname{ord} g = 2027$ ist. Dies liefert außerdem auch $\langle g \rangle_{\mathbb{Z}/2027} = \mathbb{Z}/2027$.
- Die Gruppe S_3 enthält *kein* Element der Ordnung 4, denn $\#S_3 = 6$ und 4 ist *kein* Teiler von 6.

Für Quotientengruppen sind die folgenden „Kürzungsregeln“ hilfreich:

Satz 1.1.62 (Isomorphiesätze). *Sei G eine Gruppe.*

1. Erster Isomorphiesatz. *Sei H eine Untergruppe von G und sei $N \lhd G$ ein Normalteiler in G. Dann ist $H \cap N$ ein Normalteiler in H, die Menge $H \cdot N := \{h \cdot n \mid h \in H,\ n \in N\}$ ist eine Untergruppe von G und die Abbildung*

$$\begin{aligned} H/(H \cap N) &\longrightarrow (H \cdot N)/N \\ h \cdot (H \cap N) &\longmapsto (h \cdot e) \cdot N \end{aligned}$$

ist ein wohldefinierter Gruppenisomorphismus.

2. Zweiter Isomorphiesatz. *Seien $N, K \lhd G$ Normalteiler in G mit $N \subset K \subset G$. Dann ist K/N ein Normalteiler in G/N und die Abbildung*

$$\begin{aligned} G/K &\longrightarrow (G/N) \,/\, (K/N) \\ g \cdot K &\longmapsto (g \cdot N) \cdot (K/N) \end{aligned}$$

ist ein wohldefinierter Gruppenisomorphismus.

Beweis. Zu 1. Es ist $H \cap N$ ein Normalteiler in H (da N ein Normalteiler in G und H ein Normalteiler in H ist).

Es ist $H \cdot N$ eine Untergruppe von G, denn: Wir verwenden das Kriterium aus Proposition 1.1.26.

- Wegen $e = e \cdot e$ ist $H \cdot N \neq \emptyset$.
- Sind $h_1, h_2 \in H$, $n_1, n_2 \in N$, so ist $h_2^{-1} \cdot n_1 \cdot h_2 \in N$ (da N ein Normalteiler in G ist!) und daher

$$\begin{aligned} (h_1 \cdot n_1) \cdot (h_2 \cdot n_2) &= h_1 \cdot h_2 \cdot h_2^{-1} \cdot n_1 \cdot h_2 \cdot n_2 \\ &\in h_1 \cdot h_2 \cdot N \subset H \cdot N. \end{aligned}$$

- Ist $h \in H$, $n \in N$, so ist

$$(h \cdot n)^{-1} = n^{-1} \cdot h^{-1} = h^{-1} \cdot h \cdot n^{-1} \cdot h^{-1} \in h^{-1} \cdot N \subset H \cdot N.$$

Also ist $H \cdot N$ eine Untergruppe von G. Außerdem ist N ein Normalteiler in $H \cdot N$, denn N ist ein Normalteiler in (der größeren Gruppe) G.

Wir betrachten den Gruppenhomomorphismus

$$\begin{aligned} f \colon H &\longrightarrow (H \cdot N)/N \\ h &\longmapsto (h \cdot e) \cdot N, \end{aligned}$$

also die Komposition der Inklusion $H \longrightarrow H \cdot N$ mit der kanonischen Projektion $H \cdot N \longrightarrow (H \cdot N)/N$.

Eine einfache Rechnung zeigt, dass f surjektiv ist und dass $\ker f = H \cap N$ ist (nachrechnen). Mit ? dem Homomorphiesatz (Korollar 1.1.51) folgt daher die Behauptung.

Zu 2. Es ist K/N ein Normalteiler in G/N, denn: Da K eine Untergruppe von G ist, folgt, dass K/N eine Untergruppe in G/N ist (nachrechnen). Seien $k \in K$ und $g \in G$. Dann ist $g \cdot k \cdot g^{-1} \in K$ (da K ein Normalteiler in G ist), und somit

$$(g \cdot N) \cdot (k \cdot N) \cdot (g \cdot N)^{-1} = (g \cdot k \cdot g^{-1}) \cdot N \in K/N.$$

Also ist K/N ein Normalteiler in G/N.

Der Homomorphismus

$$\begin{aligned} f \colon G &\longrightarrow (G/N) \,/\, (K/N) \\ g &\longmapsto (g \cdot N) \cdot (K/N), \end{aligned}$$

gegeben als Komposition der kanonischen Projektionen $G \longrightarrow G/N$ und $G/N \longrightarrow (G/N)/(K/N)$, ist surjektiv und erfüllt $\ker f = K$ (nachrechnen). Mit ? dem Homomorphiesatz (Korollar 1.1.51) folgt daher die Behauptung. □

1.1.7 Produkte und Erweiterungen

Normalteiler erlauben es, Gruppen durch Übergang zur Quotientengruppe in kleinere Bausteine zu „zerlegen“. Umgekehrt überlegen wir uns, wie man aus Gruppen neue Gruppen zusammensetzen kann. Eine wichtige solche Konstruktion für Vektorräume ist das direkte Produkt. Direkte Produkte gibt es auch in der Kategorie der Gruppen:

Definition 1.1.63 (Produkt)**.** Sei $(G_i)_{i \in I}$ eine (nicht-leere) Familie von Gruppen; der Einfachheit halber notieren wir die neutralen Elemente in jeder der Gruppen G_i mit e. Die Menge

$$\prod_{i \in I} G_i := \left\{ f \in \mathrm{Abb}\Big(I, \bigcup_{i \in I} G_i\Big) \;\middle|\; \forall_{i \in} \quad f(i) \in G_i \right\}$$

ist bezüglich komponentenweiser Verknüpfung eine Gruppe mit neutralem Element $(e)_{i \in I}$, das *Produkt der* $(G_i)_{i \in I}$. Die Elemente von $\prod_{i \in I} G_i$ notieren wir oft statt als Abbildungen als Familien $(x_i)_{i \in I}$ (wobei dann $x_i \in G_i$ für jedes $i \in I$ gilt).

- Ist $j \in I$, so schreiben wir

$$\begin{aligned}\pi_j \colon \prod_{i\in I} G_i &\longrightarrow G_j \\ (x_i)_{i\in I} &\longmapsto x_j\end{aligned}$$

für die *Projektion auf den j-ten Faktor*

- und

$$\begin{aligned}i_j \colon G_j &\longmapsto \prod_{i\in I} G_i \\ x &\longmapsto \left(i \mapsto \begin{cases} x & \text{falls } i = j \\ e & \text{falls } i \neq j \end{cases}\right)\end{aligned}$$

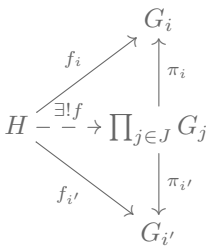
für die *Inklusion des j-ten Faktors.*

Ist die Indexmenge $I = \{i, j\}$ eine zweielementige Menge, so schreiben wir auch $G_i \times G_j$ für das Produkt.

Beispiel 1.1.64. Sind A und B abelsche Gruppen, so ist $A \times B$ die Gruppe, die man als additive Gruppe des $\mathbb{Z}$-Moduls $\widetilde{A} \oplus \widetilde{B}$ erhält (wobei $\widetilde{A}$ und $\widetilde{B}$ die von der Gruppenstruktur induzierten $\mathbb{Z}$-Moduln bezeichenn).

Bemerkung 1.1.65 (universelle Eigenschaft des Produkts)**.** Sei $(G_i)_{i\in I}$ eine Familie von Gruppen. Dann besitzt $G := \prod_{i\in I} G_i$ zusammen mit den kanonischen Projektionen $(\pi_i)_{i\in I}$ die folgende universelle Eigenschaft: Für jede Gruppe H und jede Familie $(f_i \colon H \to G_i)_{i\in I}$ von Gruppenhomomorphismen gibt es genau einen Gruppenhomomorphismus $f \colon H \longrightarrow G$ mit

$$\forall_{i\in I} \quad \pi_i \circ f = f_i$$



Mithilfe der universellen Eigenschaft von Produkten ist es also leicht, Homomorphismen *in Produkte hinein* zu charakterisieren.

Ausblick 1.1.66 (Koprodukt von Gruppen)**.** Eine weitere, vielleicht sogar vertrautere, Konstruktion für Vektorräume ist die direkte Summe; dabei handelt es sich (im kategorientheoretischen Sinne) um ein sogenanntes Koprodukt, das durch eine passende universelle Eigenschaft charakterisiert wird. Analog

kann man auch für Gruppen die universelle Eigenschaft des Koprodukts formulieren; die Konstruktion solcher Gruppen ist jedoch nicht ganz so einfach wie im Vektorraumfall [20, Kapitel 2]; zum Beispiel ist das Koprodukt von $\mathbb{Z}$ mit $\mathbb{Z}$ eine freie Gruppe vom Rang 2 (freie Gruppen werden in Anhang A.3 erklärt). Da wir diese Konstruktion im folgenden nicht benötigen werden, gehen wir nicht näher darauf ein.

Wir modifizieren die Konstruktion des Produkts, indem wir die Verknüpfung in kontrollierter Weise „deformieren“:

Definition 1.1.67 (semi-direktes Produkt)**.** Seien N und Q Gruppen und sei $\varphi\colon Q \longrightarrow \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Das *semi-direkte Produkt $N \rtimes_\varphi Q$ von N und Q bezüglich φ* besteht aus der Menge $N \times Q$, der Verknüpfung

$$\begin{aligned}(N \times Q) \times (N \times Q) &\longrightarrow N \times Q\\ \big((n,q),(n',q')\big) &\longmapsto \big(n \cdot \varphi(q)(n'), q \cdot q'\big)\end{aligned}$$

und dem neutralen Element (e,e).

Anmerkung zum Lernen. Wie kann man sich diese Verknüpfung merken? Möchte man das Produkt $(n,q)\cdot(n',q')$ berechnen, so muss man q an n' „vorbeiziehen“, und der Preis dafür ist, φ (auf q) anzuwenden.

Beispiel 1.1.68 (Produkte sind semi-direkte Produkte)**.** Seien N und Q Gruppen und sei

$$\begin{aligned}\varphi\colon Q &\longrightarrow \mathrm{Aut}(N)\\ q &\longmapsto \mathrm{id}_N\,.\end{aligned}$$

Dann ist $N \rtimes_\varphi Q$ nichts anderes als ? die Produktgruppe $N \times Q$ (nachrechnen).

Proposition 1.1.69 (grundlegende Eigenschaften von semi-direkten Produkten)**.** *Seien N und Q Gruppen und sei $\varphi\colon Q \longrightarrow \mathrm{Aut}(N)$ ein Gruppenhomomorphismus.*

1. *Dann erfüllt $N \rtimes_\varphi Q$ tatsächlich die Gruppenaxiome.*
2. *Die Abbildung*

$$\begin{aligned}\pi\colon N \rtimes_\varphi Q &\longrightarrow Q\\ (n,q) &\longmapsto q\end{aligned}$$

ist ein surjektiver Gruppenhomomorphismus und $\ker\pi = N \times \{e\}$. Insbesondere ist $N \times \{e\}$ ein Normalteiler in $N \rtimes_\varphi Q$ und π induziert nach dem Homomorphiesatz einen Isomorphismus $N \rtimes_\varphi Q / N \times \{e\} \cong_{\mathsf{Group}} Q$.

3. Die Abbildung

$$\begin{aligned} s\colon Q &\longrightarrow N \rtimes_\varphi Q \\ q &\longmapsto (e, q) \end{aligned}$$

ist ein Gruppenhomomorphismus mit $\pi \circ s = \mathrm{id}_Q$ *(d.h.* s *ist ein Spalt von* π*).*

4. Für alle $n \in N$ *und* $q \in Q$ *gilt*

$$(e, q) \cdot (n, e) \cdot (e, q)^{-1} = \big(\varphi(q)(n), e\big).$$

Beweis. Alle Aussagen folgen durch hinreichend ausdauerndes Nachrechnen:

Zu 1. Das Paar (e, e) ist das neutrale Element in $N \rtimes_\varphi Q$ und jedes Element aus $N \rtimes_\varphi Q$ besitzt ein Inverses: das Inverse zu (n, q) ist $\big(\varphi(q^{-1})(n^{-1}), q^{-1}\big)$ (Übungsaufgabe).

Die Verknüpfung auf $N \rtimes_\varphi Q$ ist assoziativ, denn: Für alle (n, q), (n', q'), $(n'', q'') \in N \rtimes_\varphi Q$ gilt

$$\begin{aligned} &(n, q) \cdot \big((n', q') \cdot (n'', q'')\big) \\ &\quad = (n, q) \cdot \big(n' \cdot \varphi(q')(n''), q' \cdot q''\big) \\ &\quad = \big(n \cdot \varphi(q)(n' \cdot \varphi(q')(n'')), q \cdot q' \cdot q''\big) \\ &\quad = \big(n \cdot \varphi(q)(n') \cdot \varphi(q)(\varphi(q')(n'')), q \cdot q' \cdot q''\big) \quad (\text{da } ? \ \varphi(q) \text{ ein Homomorphismus ist}) \\ &\quad = \big(n \cdot \varphi(q)(n') \cdot \varphi(q \cdot q')(n''), q \cdot q' \cdot q''\big) \quad (\text{da } ? \ \varphi \text{ ein Homomorphismus ist}) \\ &\quad = \big(n \cdot \varphi(q)(n'), q \cdot q'\big) \cdot (n'', q'') \\ &\quad = \big((n, q) \cdot (n', q')\big) \cdot (n'', q''). \end{aligned}$$

Zu 2. Für alle $(n, q), (n', q') \in N \rtimes_\varphi Q$ gilt

$$\begin{aligned} \pi\big((n, q) \cdot (n', q')\big) &= \pi(\ldots, q \cdot q') \\ &= q \cdot q' \\ &= \pi(n, q) \cdot \pi(n', q'). \end{aligned}$$

Also ist π ein Gruppenhomomorphismus. Der Definition von π ist direkt anzusehen, dass π surjektiv und $\ker \pi = N \times \{e\}$ ist.

Zu 3. Für alle $q, q' \in Q$ ist

$$\begin{aligned} s(q) \cdot s(q') &= (e, q) \cdot (e, q') \\ &= \big(e \cdot \varphi(q)(e), q \cdot q'\big) \\ &= \big(e \cdot \mathrm{id}_N(e), q \cdot q'\big) \\ &= (e, q \cdot q') \\ &= s(q \cdot q') \end{aligned}$$

und für alle $q \in Q$ ist $\pi \circ s(q) = \pi(e, q) = q = \mathrm{id}_Q(q)$.

Zu 4. Mit der Formel für Inverse aus dem ersten Teil folgt: Für alle $n \in N$ und alle $q \in Q$ gilt

$$\begin{aligned}(e,q) \cdot (n,e) \cdot (e,q)^{-1} &= \big(e \cdot \varphi(q)(n), q \cdot e\big) \cdot (e, q^{-1}) \\ &= \big(\varphi(q)(n), q\big) \cdot (e, q^{-1}) \\ &= \big(\varphi(q)(n) \cdot \varphi(q)(e), q \cdot q^{-1}\big) \\ &= \big(\varphi(q)(n) \cdot e, e\big) \\ &= \big(\varphi(q)(n), e\big). \end{aligned}$$

□

Proposition 1.1.70 (Diedergruppen). *Sei $n \in \mathbb{N}_{\geq 3}$ und sei $X_n \subset \mathbb{R}^2$ ein reguläres n-Eck in $(\mathbb{R}^2, d_2)$. Dann ist*

$$\mathrm{Isom}(X_n, d_2) \cong_{\mathsf{Group}} \mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2,$$

wobei

$$\begin{aligned}\varphi\colon \mathbb{Z}/2 &\longrightarrow \mathrm{Aut}(\mathbb{Z}/n) \\ [1] &\longmapsto -\mathrm{id}_{\mathbb{Z}/n}\,.\end{aligned}$$

Man bezeichnet die Gruppe $\mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2$ als Diedergruppe *D_n.*

Beweis. Als ersten Schritt versuchen wir, möglichst viele Isometrien von X_n zu finden: Wir können ohne Einschränkung annehmen, dass der Mittelpunkt von X_n der Nullpunkt 0 ist. Sei $s\colon X_n \longrightarrow X_n$ gegeben durch Rotation um $2 \cdot \pi/n$ um den Nullpunkt und sei $t\colon X_n \longrightarrow X_n$ die Spiegelung an einer Geraden durch den Nullpunkt und eine Ecke von X_n (Abbildung 1.8). Dann gilt $s, t \in \mathrm{Isom}(X_n, d_2)$ und die Elemente

$$\mathrm{id},\ s,\ \ldots,\ s^{n-1},\ t,\ s \circ t,\ s^2 \circ t,\ \ldots, s^{n-1} \circ t$$

sind alle verschieden (nachrechnen, z.B. auf den Eckpunkten). Dabei ist $\mathrm{ord}\, s =$? n und $\mathrm{ord}\, t =$? 2.

Als zweiten Schritt zeigen wir, dass die Gruppe $G := \mathrm{Isom}(X_n, d_2)$ keine weiteren Elemente enthält:

- Jedes Element aus G bildet die Ecken von X_n (bijektiv) auf die Ecken von X_n ab (charakterisiert via maximale Abstände); dabei werden „benachbarte“ Ecken auf „benachbarte“ Ecken abgebildet.
- Jeder Punkt in X_n ist eindeutig durch die Abstände zu zwei gegebenen benachbarten Ecken bestimmt. Also ist jedes Element in G durch den Wert auf zwei benachbarten Ecken eindeutig bestimmt.

Da die Elemente $\mathrm{id}, s, \ldots, s^{n-1}, t, s \circ t, s^2 \circ t, \ldots, s^{n-1} \circ t$ alle solchen Eckenbijektionen realisieren (nachrechnen), gibt es keine weiteren Elemente in G. Wir haben somit eine vollständige konkrete Beschreibung von G.

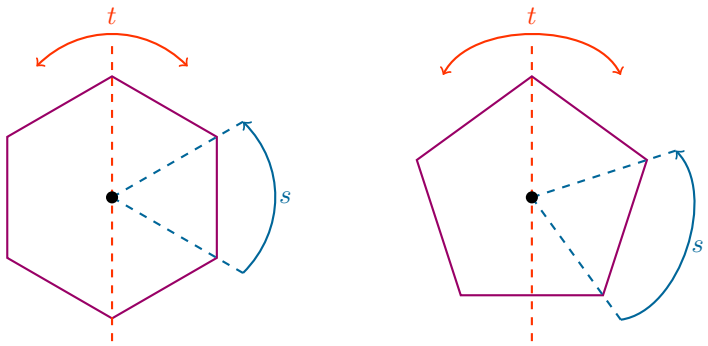


Abbildung 1.8.: Elemente der Isometriegruppe des regulären Sechs- bzw. Fünfecks

Wir betrachten nun die Untergruppen

$$N := \langle s \rangle_G \cong_{\mathsf{Group}} \mathbb{Z}/n \quad \text{und} \quad Q := \langle t \rangle_G \cong_{\mathsf{Group}} \mathbb{Z}/2,$$

sowie die Abbildung

$$\begin{aligned} \psi \colon Q &\longrightarrow \mathrm{Aut}(N) \\ \mathrm{id} &\longmapsto \mathrm{id}_N \\ t &\longmapsto (f \mapsto t \circ f \circ t^{-1}) = \boxed{?} \quad - \mathrm{id}_N \,. \end{aligned}$$

Eine einfache Rechnung zeigt, dass ψ ein wohldefinierter Gruppenhomomorphismus ist (nachrechnen) und dass

$$\begin{aligned} \mathbb{Z}/n \rtimes_\varphi \mathbb{Z}/2 \longrightarrow & N \rtimes_\psi Q \longrightarrow \mathrm{Isom}(X_n, d_2) \\ \big([k], [\ell]\big) \longmapsto & \ (s^k, t^\ell) \\ & (f, g) \longmapsto f \circ g \end{aligned}$$

Gruppenisomorphismen sind (nachrechnen). □

Beispiel 1.1.71 (euklidische Isometriegruppe)**.** Sei $n \in \mathbb{N}$. Dann ist

$$\begin{aligned} \mathbb{R}^n \rtimes_\varphi \mathrm{O}(n) &\longrightarrow \mathrm{Isom}(\mathbb{R}^n, d_2) \\ (x, A) &\longmapsto (v \mapsto A \cdot v + x) \end{aligned}$$

ein Gruppenisomorphismus, wobei

$$\begin{aligned} \varphi \colon \mathrm{O}(n) &\longrightarrow \mathrm{Aut}(\mathbb{R}^n) \\ A &\longmapsto (x \mapsto A \cdot x). \end{aligned}$$

Dies kann wie folgt gezeigt werden: Die obige Abbildung $\mathbb{R}^n \rtimes_\varphi \mathrm{O}(n) \longrightarrow \mathrm{Isom}(\mathbb{R}^n, d_2)$ ist ein Gruppenhomomorphismus (nachrechnen) und dieser ist injektiv (nachrechnen). Warum ist er auch surjektiv? Es ist

$$\begin{aligned} \mathrm{O}(n) &\longrightarrow \mathrm{Isom}(\mathbb{R}^n, d_2)_0 \\ A &\longmapsto (v \mapsto A \cdot v) \end{aligned}$$

ein Gruppenisomorphismus (Beispiel 1.1.21). Ist $f \in \mathrm{Isom}(\mathbb{R}^n, d_2)$, so ist

$$\begin{aligned} \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ v &\longmapsto f(v) - f(0) \end{aligned}$$

ein Element von $\mathrm{Isom}(\mathbb{R}^n, d_2)_0$. Dies liefert die Surjektivität.

Beispiel 1.1.72 („innere" semi-direkte Produkte)**.** Sei G eine Gruppe, sei $N \subset G$ ein Normalteiler in G und sei $H \subset G$ eine Untergruppe mit $H \cap N = \{e\}$. Dann ist

$$\begin{aligned} N \rtimes_\varphi H &\longrightarrow H \cdot N \\ (n, h) &\longmapsto n \cdot h = h \cdot (h^{-1} \cdot n \cdot h) \end{aligned}$$

ein Gruppenisomorphismus (nachrechnen); hierbei bildet $H \cdot N$ wie im ersten Isomorphiesatz (Satz 1.1.62) eine Gruppe und

$$\begin{aligned} \varphi\colon H &\longrightarrow \mathrm{Aut}(N) \\ h &\longmapsto (n \mapsto h \cdot n \cdot h^{-1}). \end{aligned}$$

Caveat 1.1.73 (Gruppenerweiterungen)**.** Eine *Gruppenerweiterung* ist eine kurze exakte Sequenz

$$\{e\} \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow \{e\}$$

in der Kategorie der Gruppen (d.h. $i\colon N \longrightarrow G$ ist ein injektiver Gruppenhomomorphismus, $\pi\colon G \longrightarrow Q$ ist ein surjektiver Gruppenhomomorphismus und $\operatorname{im} i = \ker \pi$).

Produkte und semi-direkte Produkte liefern in kanonischer Weise (spaltende) Gruppenerweiterungen. Im allgemeinen ist jedoch die mittlere Gruppe in einer Gruppenerweiterung *kein* (semi-direktes) Produkt der äußeren Gruppen; ein drastisches Beispiel ist etwa

$$\{0\} \longrightarrow \mathbb{Z} \xrightarrow{n \mapsto 2 \cdot n} \mathbb{Z} \xrightarrow{n \mapsto [n]} \mathbb{Z}/2 \longrightarrow \{0\}$$

(denn $\mathbb{Z}$ enthält keine zu $\mathbb{Z}/2$ isomorphe Untergruppe).

Ist

$$\{e\} \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow \{e\}$$

eine Gruppenerweiterung und gibt es einen Homomorphismus (!) $s\colon Q \longrightarrow G$ mit $\pi \circ s = \mathrm{id}_Q$, so gibt es einen Gruppenhomomorphismus $\varphi\colon Q \longrightarrow \mathrm{Aut}(N)$ mit $G \cong_{\mathsf{Group}} N \rtimes_\varphi Q$ (Übungsaufgabe).

Ist $n \in \mathbb{N}_{\geq 2}$, so folgt auf diese Weise, dass es einen Gruppenhomomorphismus $\varphi\colon \mathbb{Z}/2 \longrightarrow \mathrm{Aut}(A_n)$ mit $S_n \cong_{\mathsf{Group}} A_n \rtimes_\varphi \mathbb{Z}/2$ gibt (nachrechnen). Analog erhält man auch Isomorphismen der Form

$$\mathrm{O}(n) \cong_{\mathsf{Group}} \mathrm{SO}(n) \rtimes_{\dots} \mathbb{Z}/2$$
$$\mathrm{GL}_n(K) \cong_{\mathsf{Group}} \mathrm{SL}_n(K) \rtimes_{\dots} K^\times$$

für alle $n \in \mathbb{N}_{\geq 2}$ und alle Körper K (Übungsaufgabe).

Allgemeiner lassen sich Gruppenerweiterungen über sogenannte *Gruppenkohomologie* klassifizieren [7].

1.2 Gruppenoperationen

Gruppenoperationen verallgemeinern Gruppen bzw. den Zusammenhang zwischen Gruppen und Symmetriegruppen. Zwei typische Situationen dieser Art sind:

- Ist G eine Gruppe und $H \subset G$ eine Untegruppe, so induziert die Gruppenstruktur auf G im allgemeinen *keine* Gruppenstruktur auf G/H. Aber die Verknüpfung von G liefert immer noch eine Gruppenoperation auf G/H.
- Ist G die Automorphismengruppe eines Objekts X und ist $H \subset G$ eine Untergruppe von G, so ist H zwar im allgemeinen nicht mehr die ganze Automorphismengruppe, aber die Elemente aus H operieren immer noch auf X.

Gruppenoperationen werden sich zum Beispiel bei Zählproblemen und bei der Untersuchung der Struktur endlicher Gruppen als nützlich erweisen. Außerdem spielen Gruppenoperationen in der Galoistheorie und der Geometrie bzw. der geometrischen Gruppentheorie eine wichtige Rolle [20].

1.2.1 Gruppenoperationen

Definition 1.2.1 (Gruppenoperation)**.** Sei X eine Menge und sei G eine Gruppe. Eine *Gruppenoperation von G auf X* ist ein Gruppenhomomorphismus $G \longrightarrow S_X$.

Ausblick 1.2.2. Dieser Begriff der Gruppenoperation lässt sich gut verallgemeinern: Sei C eine Kategorie und sei X ein Objekt von C; sei G eine Gruppe.

Eine *Gruppenoperation von G auf X (in C)* ist ein Gruppenhomomorphismus $G \longrightarrow \mathrm{Aut}_C(X)$. Auf diese Weise erhält man

- isometrische Operationen (Operationen in der Kategorie der metrischen Räumen)
- stetige Operationen (Operationen in der Kategorie der topologischen Räume)
- lineare Darstellungen (Operationen in der Kategorie der Vektorräume)
- (invertierbare) dynamische Systeme (Operationen in der Kategorie der Wahrscheinlichkeitsräume/maßerhaltenden Transformationen)
- ...

Bemerkung 1.2.3 (Gruppenoperationen auf Mengen, explizit)**.** Sei G eine Gruppe und sei X eine Menge. Dann ist

$$\begin{aligned} \mathrm{Abb}\big(G, \mathrm{Abb}(X,X)\big) &\longrightarrow \mathrm{Abb}(G \times X, X) \\ f &\longmapsto \big((g,x) \mapsto f(g)(x)\big) \end{aligned}$$

eine Bijektion (Exponentialgesetz für Abbildungen).

- Ist $\varrho\colon G \longrightarrow S_X$ eine Gruppenoperation von G auf X, so hat die zugehörige Abbildung $\cdot : G \times X \longrightarrow X$ die folgenden Eigenschaften:

$$\begin{aligned} \forall_{x\in X} \quad e \cdot x \overset{?}{=} \varrho(e)(x) = \mathrm{id}_X(x) = x \\ \forall_{g,h\in G} \quad \forall_{x\in X} \quad (g\cdot h)\cdot x \overset{?}{=} \varrho(g\cdot h)(x) = \varrho(g)\big(\varrho(h)(x)\big) = g\cdot(h\cdot x) \end{aligned}$$

  (welcher Punkt „$\cdot$“ hat dabei welche Bedeutung?!).

- Ist umgekehrt $\cdot : G \times X \longrightarrow X$ eine Abbildung mit

$$\begin{aligned} \forall_{x\in X} \quad e\cdot x = x \\ \forall_{g,h\in G} \quad \forall_{x\in X} \quad (g\cdot h)\cdot x = g\cdot(h\cdot x), \end{aligned}$$

  so ist

$$\begin{aligned} G &\longrightarrow S_X \\ g &\longmapsto (x \mapsto g\cdot x) \end{aligned}$$

  eine Gruppenoperation im Sinne von Definition 1.2.1 (nachrechnen).

Wir werden im folgenden im Normalfall die Beschreibung über Abbildungen der Form $G \times X \longrightarrow X$ verwenden, da sie meistens etwas intuitiver ist. Als Definition ist die Beschreibung als Homomorphismus $G \longrightarrow S_X$ jedoch geschickter, da sie sich leichter verallgemeinern lässt.

Beispiel 1.2.4 (Gruppenoperationen)**.**

- Sei G eine Gruppe und X eine Menge. Dann ist

$$\begin{aligned} G &\longrightarrow S_X \\ g &\longmapsto \mathrm{id}_X \end{aligned}$$

eine Gruppenoperation, die *triviale Operation von G auf X*. In der expliziten Beschreibung bedeutet dies $g \cdot x = x$ für alle $g \in G$ und $x \in X$.

Insbesondere gibt es für jede Gruppe auf jeder Menge eine Gruppenoperation. Die Kunst besteht darin, Gruppenoperationen zu finden, die einen interessanten Zusammenhang zwischen der Gruppe und der Menge herstellen.

- Sei X eine Menge und sei $H \subset S_X$ eine Untergruppe. Dann ist

$$\begin{aligned} H \times X &\longrightarrow X \\ (f, x) &\longmapsto f(x) \end{aligned}$$

eine Gruppenoperation.

Allgemeiner: Automorphismengruppen operieren auf den unterliegenden Objekten. Zum Beispiel operieren Isometriegruppen auf den unterliegenden metrischen Räumen und ist K ein Körper und $n \in \mathbb{N}$, so operiert $\mathrm{GL}_n(K)$ via

$$\begin{aligned} \mathrm{GL}_n(K) \times K^n &\longrightarrow K^n \\ (A, x) &\longmapsto A \cdot x \end{aligned}$$

auf K^n.

- Sei G eine Gruppe und $H \subset G$ eine Untergruppe. Dann ist

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

eine wohldefinierte Gruppenoperation auf G/H (nachrechnen), die *Linkstranslationsoperation* auf der Menge G/H der Linksnebenklassen.

Beispiel 1.2.5 (eine wohlklingende Diedergruppenoperation)**.** Wir betrachten den zyklischen Graphen der zwölf (gleichstufig gestimmten) Halbtöne einer Oktave (Abbildung 1.9). Darauf operiert die Diedergruppe $D_{12} = \mathbb{Z}/12 \rtimes_\varphi \mathbb{Z}/2$ auf folgende Weise:

- Das Element $s := ([1], [0])$ operiert durch Transposition um einen Halbton nach oben.
- Das Element $t := ([0], [1])$ operiert durch Inversion an D.

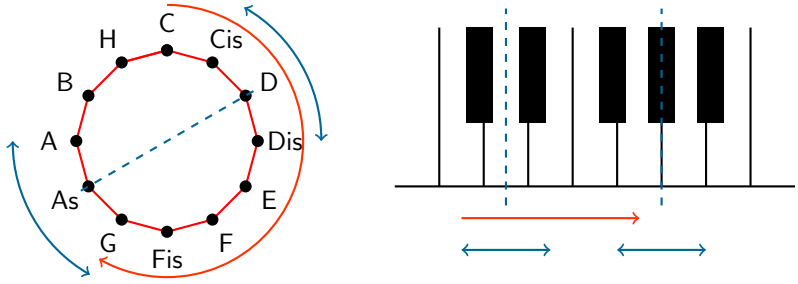


Abbildung 1.9.: Die zwölf Halbtöne und die Gruppe D_{12}; rot: Transposition um sieben Halbtöne nach oben; blau: Inversion an D bzw. As (auf dem Klavier leicht zu spielen).

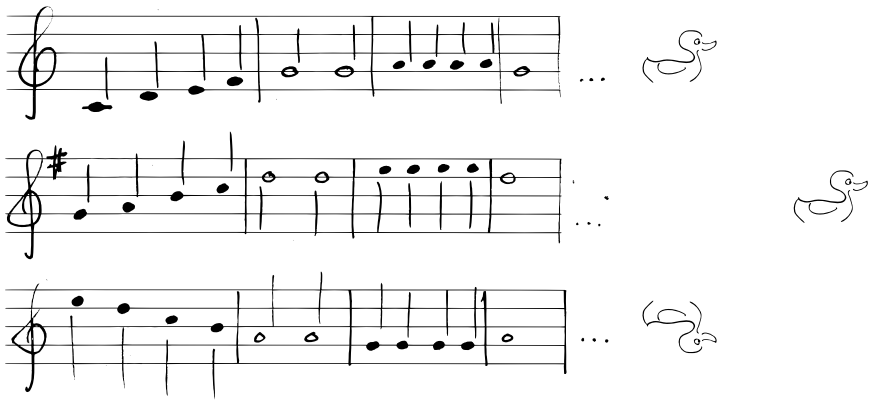


Abbildung 1.10.: Original, Transposition, Inversion

Eine elementare Rechnung zeigt, dass es sich dabei tatsächlich um eine Gruppenoperation handelt. Einfache Beispiele für die Operation von s^7 und $s^2 \cdot t \cdot s^{-2}$ finden sich in Abbildung 1.10.

Diese Operation ist ein wichtiges Hilfsmittel in der klassischen Komposition und findet sich daher in fast allen klassischen Werken.

Außerdem induziert diese Operation von D_{12} auch eine interessante Operation von D_{12} auf der Menge der Dur- und Molldreiklänge [10].

Der Zusammenhang zwischen der operierenden Gruppe und dem unterliegenden Objekt ist besonders stark, wenn die Operation im folgenden Sinne frei oder transitiv ist:

Definition 1.2.6 (freie Operation, transitive Operation)**.** Eine Gruppenoperation einer Gruppe G auf einer Menge X ist

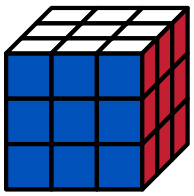


Abbildung 1.11.: Rubik's Cube

- *frei*, wenn für jedes $g \in G \setminus \{e\}$ und jedes $x \in X$ bereits $g \cdot x \neq x$ gilt.
- *transitiv*, wenn
$$\forall_{x,y \in X} \quad \exists_{g \in G} \quad g \cdot x = y.$$

Beispiel 1.2.7 (freie/transitive Operationen)**.**

- Ist (X, d) ein metrischer Raum, so ist die kanonische Operation der Isometriegruppe $\mathrm{Isom}(X, d)$ auf X im allgemeinen *nicht* frei: Ist t die Spiegelung eines Quadrats entlang einer Diagonalen, so ist t *nicht* das neutrale Element und fixiert alle Elemente auf dieser Diagonalen.

  Solche Operationen sind im allgemeinen auch *nicht* transitiv: Alle Isometrien eine Quadrats bilden den Mittelpunkt des Quadrats auf den Mittelpunkt des Quadrats ab (und Ecken auf Ecken).

- Ist $\alpha \in S^1$, so ist die Rotationsoperation
$$\begin{aligned} \mathbb{Z} \times S^1 &\longrightarrow S^1 \\ (n, z) &\longmapsto \alpha^n \cdot z \end{aligned}$$
genau dann frei, wenn wir $\alpha = e^{2 \cdot \pi \cdot i \cdot t}$ mit irrationalem $t \in \mathbb{R}$ schreiben können (nachrechnen). Aus Mächtigkeitsgründen ist *keine* dieser Operationen transitiv.

Beispiel 1.2.8 (Rubik's Cube)**.** Sei R die Menge aller (relativen) Positionen des Zauberwürfels (Abbildung 1.11). Dann können wir die Rotation der Vorderseite durch eine Operation von $\mathbb{Z}$ (erzeugt von der Drehung der Vorderseite um $\pi/2$ gegen der Uhrzeigersinn, wobei die beiden hinteren Schichten des Würfels an ihrem ursprünglichen Ort bleiben) auf R modellieren. Diese Operation ist *nicht* frei, da 4 trivial operiert (viermaliges Drehen derselben Seite um $\pi/2$ ist dasselbe wie nichts zu tun). Offenbar ist diese Operation auch *nicht* transitiv.

Um den Zauberwürfel vollständig zu modellieren, benötigt man natürlich auch noch die Operation der Drehungen der anderen fünf Seiten. Insgesamt erhält man auf diese Weise eine Operation der freien Gruppe vom Rang 6 auf R. Eine alternative Möglichkeit der Modellierung ist, einfach nur die

Untergruppe von S_R zu betrachten, die von den sechs Rotationspermutationen in S_R erzeugt werden. Diese zweite Möglichkeit ist zwar mathematisch einfacher zu verwenden, aber die Modellierung mithilfe von Operationen ist eigentlich näher an der realen Situation.

Ein wichtiges weiteres Beispiel für eine freie Operation ist die Linkstranslationsoperation einer Gruppe auf sich selbst:

Satz 1.2.9 (Satz von Cayley)**.** *Sei G eine Gruppe. Dann ist G zu einer Untergruppe der symmetrischen Gruppe S_G isomorph.*

Beweis. Die *Linkstranslationsoperation*

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

von G auf sich selbst ist frei (und transitiv). Insbesondere ist die zugehörige Abbildung

$$\begin{aligned} \varrho \colon G &\longrightarrow S_G \\ g &\longmapsto (x \mapsto g \cdot x) \end{aligned}$$

ein injektiver Gruppenhomomorphismus. Nach dem Homomorphiesatz (Korollar 1.1.51) ist somit

$$G \cong_{\mathsf{Group}} G/\{e\} = G/\ker \varrho \cong_{\mathsf{Group}} \operatorname{im} \varrho;$$

dabei ist $\operatorname{im} \varrho$ eine Untergruppe von S_G. □

Korollar 1.2.10. *Sei G eine endliche Gruppe und sei K ein Körper. Dann gibt es ein $n \in \mathbb{N}$, so dass G zu einer Untergruppe von $\mathrm{GL}_n(K)$ isomorph ist.*

Beweis. Nach dem Satz von Cayley (Satz 1.2.9) genügt es, die symmetrische Gruppe S_G für hinreichend großes $n \in \mathbb{N}$ in $\mathrm{GL}_n(K)$ einzubetten. Dies ist auf einfache Weise möglich (Übungsaufgabe). □

1.2.2 Zählen durch Gruppenoperationen

Allgemeine Gruppenoperationen sind weder frei noch transitiv. Es ist daher naheliegend, Gruppenoperationen in einfachere Bausteine zu zerlegen. Diese Bausteine werden auch nützlich sein, um Gruppenoperationen zur Lösung gewisser Zählprobleme einzusetzen.

Definition 1.2.11 (Orbit/Bahn, Stabilisator)**.** Sei G eine Gruppe, sei X eine Menge und es sei eine Gruppenoperation von G auf X gegeben.

- Der *Orbit* (oder die *Bahn*) eines Elements $x \in X$ unter dieser Operation ist die Menge
$$G \cdot x := \{g \cdot x \mid g \in G\} \subset X.$$
- Der *Orbitraum* (*Bahnenraum*) dieser Gruppenoperation ist die Menge
$$G \setminus X := \{G \cdot x \mid x \in X\}$$
aller Bahnen. Wir schreiben „$G \setminus X$“, da G „von links“ operiert.
- Der *Stabilisator* (oder die *Standgruppe*, *Isotropiegruppe*) eines Elements $x \in X$ ist
$$G_x := \{g \in G \mid g \cdot x = x\} \subset G.$$
- Die *Fixpunktmenge* eines Elements $g \in G$ ist
$$X^g := \{x \in X \mid g \cdot x = x\} \subset X.$$

Bemerkung 1.2.12. Ist eine Gruppenoperation einer Gruppe G auf einer Menge X gegeben und $x \in X$, so ist der Stabilisator G_x eine Untergruppe von G (nachrechnen mithilfe von Proposition 1.1.26), aber im allgemeinen *kein* Normalteiler in G.

Bemerkung 1.2.13 (Bahnen als Äquivalenzklassen)**.** Ist eine Gruppenoperation einer Gruppe G auf einer Menge X gegeben, so definiert
$$\sim := \left\{(x, y) \in X \times X \;\middle|\; \exists_{g \in G} \quad g \cdot x = y\right\}$$
eine Äquivalenzrelation auf X (nachrechnen). Die Äquivalenzklassen dieser Äquivalenzrelation sind genau ? die Orbits der gegebenen Gruppenoperation. Insbesondere erhalten wir:

- Sind $x, y \in X$, so ist $G \cdot x = G \cdot y$ oder $G \cdot x \cap G \cdot y = \emptyset$.
- Es ist $X = \bigcup(X/\sim) = \bigcup G \setminus X$ eine disjunkte Vereinigung.

Anmerkung zum Lernen. Was haben Bahnen und Standgruppen mit Freiheit bzw. Transitivität von Gruppenoperationen zu tun? Was hat die Äquivalenzrelation aus Bemerkung 1.2.13 mit Linksnebenklassen zu tun?

Beispiel 1.2.14 (Bahnen und Fixpunkte)**.**

- Wir betrachten die Operation von $S^1 \subset \mathbb{C}^\times$ auf $X := \mathbb{C}$ durch komplexe Multiplikation.
  - Die Bahn von 0 ist ? $\{0\}$;
  - die Bahn eines Elements $z \in \mathbb{C} \setminus \{0\}$ ist ? der Kreis um 0 vom Radius $|z|$ (Abbildung 1.12).

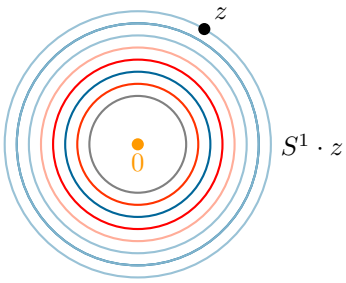


Abbildung 1.12.: Orbits der S^1-Operation durch Multiplikation auf $\mathbb{C}$

  - Ist $g \in S^1 \setminus \{1\}$, so ist die Fixpunktmenge ? $X^g = \{0\}$.
- Wir betrachten die Operation von $\mathrm{GL}_2(\mathbb{R})$ auf $\mathbb{R}^2$ durch Matrixmultiplikation.
  - Ist $x \in \mathbb{R}^2 \setminus \{0\}$, so ist die Bahn von x die Menge ? $\mathbb{R}^2 \setminus \{0\}$.
  - Der Stabilisator von e_1 ist die Menge

$$? \quad \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \;\middle|\; b \in \mathbb{R},\ d \in \mathbb{R} \setminus \{0\} \right\} \subset \mathrm{GL}_2(\mathbb{R}).$$

  - Ist $A \in \mathrm{GL}_2(\mathbb{R})$, so ist die Fixpunktmenge von A unter dieser Operation genau die Menge ? $V(A - 1 \cdot I_2, 0)$ (das hat womöglich etwas mit Eigenvektoren zu tun ...).
- Ist (X, d) ein metrischer Raum und ist $x \in X$, so ist die Untergruppe $\mathrm{Isom}(X, d)_x$ aus Beispiel 1.1.21 der Stabilisator von x unter der kanonischen $\mathrm{Isom}(X, d)$-Operation auf X (und dies rechtfertigt auch die Notation).

Satz 1.2.15 (Bahnengleichung). *Sei G eine Gruppe, sei X eine Menge und es sei eine Gruppenoperation von G auf X gegeben.*

1. *Ist $x \in X$, so ist*

$$\begin{aligned} A_x \colon G/G_x &\longrightarrow G \cdot x \\ g \cdot G_x &\longmapsto g \cdot x \end{aligned}$$

   eine wohldefinierte und bijektive Abbildung.

2. Bahnengleichung. *Ist $G \setminus X$ endlich, so gilt*

$$\#X = \sum_{G \cdot x \in G \setminus X} [G : G_x].$$

Expliziter: Ist $(x_i)_{i\in I}$ ein Vertretersystem für die G-Bahnen in X, so gilt $\#X = \sum_{i\in I}[G : G_{x_i}]$.

3. *Die Anzahl der Bahnen stimmt mit der durchschnittlichen Anzahl der Fixpunkte einzelner Gruppenelemente überein: Ist G endlich, so gilt*

$$\#(G \setminus X) = \frac{1}{\#G} \cdot \sum_{g\in G} \#(X^g).$$

Beweis. Zu 1. Wir zeigen als erstes, dass A_x wohldefiniert ist: Seien $g, h \in G$ mit $g \cdot G_x = h \cdot G_x$; also gibt es ein $k \in G_x$ mit $g = h \cdot k$. Dann ist

$$g \cdot x = (h \cdot k) \cdot x = h \cdot (k \cdot x) = h \cdot x$$

(denn $k \in G_x$; wissen Sie noch, welcher Punkt „$\cdot$“ welche Bedeutung besitzt?!). Dies zeigt die Wohldefiniertheit von A_x.

Nach Konstruktion ist A_x surjektiv. Warum ist A_x injektiv? Seien $g, h \in G$ mit $g \cdot x = h \cdot x$. Dann folgt

$$(g^{-1} \cdot h) \cdot x = g^{-1} \cdot (h \cdot x) = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = e \cdot x = x,$$

und damit $g^{-1} \cdot h \in G_x$. Also ist $g \cdot G_x = h \cdot G_x$, was die Injektivität von A_x beweist.

Zu 2. Nach Bemerkung 1.2.13 ist $X = \bigcup_{G\cdot x\in G\setminus X} G \cdot x$ eine disjunkte Vereinigung, und damit

$$\#X = \sum_{G\cdot x\in G\setminus X} \#(G \cdot x).$$

Nach dem ersten Teil gilt $\#(G \cdot x) = \#(G/G_x) = [G : G_x]$ für alle $x \in X$. Dies liefert die behauptete Gleichung.

Zu 3. Wir beweisen diese Gleichung durch doppeltes Abzählen: Dazu betrachten wir die Menge $F := \{(g, x) \mid g \in G,\ x \in X, g \cdot x = x\} \subset G \times X$. Nach Definition der Stabilisatoren und Fixpunktmengen ist

$$\sum_{x\in X} \#G_x = \#F = \sum_{g\in G} \#(X^g).$$

Es genügt daher, die linke Seite besser zu verstehen. Nach dem Satz von Lagrange für endliche Gruppen (Korollar 1.1.34) gilt $\#G = [G : G_x] \cdot \#G_x$ für alle $x \in X$. Mit dem ersten Teil erhalten wir somit

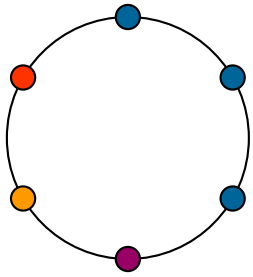


Abbildung 1.13.: Eine Perlenkette

$$\begin{aligned}\sum_{x\in X} \#G_x &= \sum_{x\in X} \frac{\#G}{[G:G_x]} = \sum_{x\in X} \frac{\#G}{\#(G\cdot x)} \\ &= \sum_{G\cdot x\in G\backslash X} \sum_{y\in G\cdot x} \frac{\#G}{\#(G\cdot x)} = \sum_{G\cdot x\in G\backslash X} \#(G\cdot x)\cdot \frac{\#G}{\#(G\cdot x)} \\ &= \#(G\setminus X)\cdot \#G. \end{aligned}$$

□

Beispiel 1.2.16 (Perlenketten)**.** Sei $k \in \mathbb{N}$. Wir betrachten (geschlossene) Ketten, die mit sechs äquidistanten Perlen dekoriert sind. Die Perlen haben dabei jeweils eine von k Farben (Abbildung 1.13). Wieviele essentiell verschiedene solcher Perlenketten gibt es?

Zunächst überlegen wir uns, was es bedeutet, dass zwei Perlenketten essentiell verschieden sind: Falls sich zwei solche Perlenketten durch geeignete Bewegungen (aber ohne zerlegen/wieder zusammensetzen) so ineinander überführen lassen, dass die Perlenfarben übereinstimmen, werden wir sie *nicht* als essentiell verschieden ansehen (und umgekehrt). Welche „Bewegungen“ sind dabei möglich? Wir können die Perlenkette „in Bandrichtung drehen“ und wir können die Kette „spiegeln“. Dies liefert eine D_6-Operation auf der Menge X aller Perlenfarbenkombinationen einer (unbeweglichen) Kette. Insgesamt stellt man auf diese Weise fest, dass zwei Perlenfarbenkombinationen genau dann essentiell verschiedene Ketten liefern, wenn sie *nicht* im selben D_6-Orbit dieser Operation liegen.

Um das Zählproblem zu lösen, müssen wir also, in der Sprache von Gruppenoperationen ausgedrückt, die Anzahl ? der D_6-Orbits dieser Operation auf X bestimmen. Nach der Bahnengleichung (Satz 1.2.15) stimmt die Anzahl dieser Orbits mit der durchschnittlichen Anzahl der Fixpunkte einzelner Gruppenelemente überein. Wir bestimmen daher für jedes Element aus $D_6 = \mathbb{Z}/6 \rtimes \mathbb{Z}/2$ die Anzahl der entsprechenden Fixpunkte in X: Dazu schreiben wir $s := ([1],[0])$ und $t := ([0],[1]) \in D_6$.

- Element $([0],[0])$: ? alle $\#X = k^6$ Elemente.

- Elemente s, s^5: ? je k Elemente (da jede Perle dieselbe Farbe wie ihre Nachbarn haben muss).
- Elemente s^2, s^4: ? je k^2 Elemente (da jede zweite Perle dieselbe Farbe haben muss).
- Element s^3: ? genau k^3 Elemente.
- Elemente t, $s^2 \cdot t$, $s^4 \cdot t$: ? je $k^2 \cdot k^2$ Elemente.
- Elemente $s \cdot t$, $s^3 \cdot t$, $s^5 \cdot t$: ? je k^3 Elemente.

Somit erhalten wir (Satz 1.2.15)

$$\begin{aligned}\#(D_6 \setminus X) &= \frac{1}{\#D_6} \cdot \sum_{g \in D_6} \#(X^g) \\ &= \frac{1}{12} \cdot (1 \cdot k^6 + 2 \cdot k + 2 \cdot k^2 + 1 \cdot k^3 + 3 \cdot k^4 + 3 \cdot k^3) \\ &= \frac{1}{12} \cdot (k^6 + 3 \cdot k^4 + 4 \cdot k^3 + 2 \cdot k^2 + 2 \cdot k).\end{aligned}$$

Zum Beispiel: Bei fünf Farben gibt es also genau 1505 essentiell verschiedene dieser Ketten. Bei 2026 Farben gibt es genau 5763094191651094201 essentiell verschiedene dieser Ketten.

Eine für die Gruppentheorie wichtige Anwendung der Bahnengleichung ist die Klassengleichung. Wir erhalten die Klassengleichung als Bahnengleichung der Konjugationsoperation einer Gruppe auf sich selbst. Um die Klassengleichung formulieren zu können, benötigen wir den Begriff des Zentralisators bzw. des Zentrums:

Definition 1.2.17 (Zentralisator, Zentrum)**.** Sei G eine Gruppe.

- Das *Zentrum von* G ist
$$Z(G) := \left\{ g \in G \;\middle|\; \forall_{h \in G} \quad g \cdot h = h \cdot g \right\} \subset G.$$
- Ist $h \in G$, so ist der *Zentralisator von* h *in* G definiert als
$$Z_G(h) := \{ g \in G \mid g \cdot h = h \cdot g \} \subset G.$$

Bemerkung 1.2.18. Das Zentrum $Z(G)$ einer Gruppe G ist offenbar ein Normalteiler in G (nachrechnen) und es gilt

$$Z(G) = \bigcap_{h \in G} Z_G(h).$$

Beispiel 1.2.19 (Konjugationsoperation)**.** Sei G eine Gruppe. Die Abbildung

$$\begin{aligned} G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto c_g = (h \mapsto g \cdot h \cdot g^{-1}) \end{aligned}$$

beschreibt eine Operation von G auf sich selbst, die *Konjugationsoperation* (Übungsaufgabe).

Ist $g \in Z(G)$, so ist die Bahn von g unter der Konjugationsoperation die einelementige Menge $\{g\}$ und der SStabilisator ist G. Allgemeiner gilt: Ist $g \in G$, so ist

- der Stabilisator von g unter der Konjugationsoperation der Zentralisator $Z_G(g)$ von g in G (Übungsaufgabe) und
- die Bahn von g unter der Konjugationsoperation ist die Menge aller zu g konjugierten Elemente von G (die sogenannte *Konjugationsklasse von g in G*).

Korollar 1.2.20 (Klassengleichung)**.** *Sei G eine endliche Gruppe und sei $(g_i)_{i\in I}$ ein Repräsentantensystem für die nicht-trivialen Konjugationsklassen in G (d.h. für die Bahnen der Konjugationsoperation von G auf G, die nicht von Elementen aus dem Zentrum stammen). Dann ist*

$$\#G = \#\big(Z(G)\big) + \sum_{i\in I} \big[G : Z_G(g_i)\big].$$

Beweis. Wir wenden die Bahnengleichung (Satz 1.2.15) auf die Konjugationsoperation von G auf G an; mit den Überlegungen aus Beispiel 1.2.19 folgt die Behauptung. □

In günstigen Fällen erlaubt es die Klassengleichung, durch reine Zählargumente festzustellen, dass das Zentrum nicht-trivial ist. Ähnliche Operationen und Argumente werden wir auch im Kontext der Sylowsätze verwenden (Kapitel 1.3.5).

1.3 Struktur endlicher Gruppen

Eine grundlegende Fragestellung in jeder mathematischen Theorie ist die Frage nach der Klassifikation aller Objekte (bis auf Isomorphie). Wie wir bereits erwähnt haben (Caveat 1.1.41), ist es nicht möglich alle endlich erzeugten (bzw. endlich präsentierten) Gruppen zu klassifizieren. Für die Anwendungen der Galoistheorie genügt uns aber die Kenntnis der endlichen Gruppen und für endliche Gruppen ist das Klassifikationsproblem lösbar. Die Lösung ist jedoch recht umfangreich und wir werden uns im folgenden auf die ersten Schritte beschränken.

Wir beginnen mit den Extremfällen der abelschen bzw. symmetrischen Gruppen. Danach formulieren wir die allgemeine Klassifkationsstrategie und gehen näher auf die Klasse der auflösbaren Gruppen ein. Zum Abschluss beweisen wir die Sylowsätze, die in vielen konkreten Beispielen helfen können, Gruppen zu zerlegen.

1.3.1 Endliche abelsche Gruppen

Wir beginnen mit der uns vertrautesten Klasse von endlichen Gruppen, den endlichen abelschen Gruppen. Für diese Klasse kennen wir bereits aus der Linearen Algebra das Klassifikationsresultat (Korollar II.2.5.17):

Satz 1.3.1 (Klassifikation endlicher abelscher Gruppen)**.** *Sei A eine endliche abelsche Gruppe. Dann gibt es $k \in \mathbb{N}$, Primzahlen $p_1, \dots, p_k \in \mathbb{N}$ und Zahlen $n_1, \dots, n_k \in \mathbb{N}_{>0}$ mit*

$$A \cong_{\mathsf{Group}} \prod_{j \in \{1,\dots,k\}} \mathbb{Z}/p_j^{n_j}.$$

Dabei sind k und die Paare $(p_1, n_1), \dots, (p_k, n_k)$ (bis auf die Reihenfolge) eindeutig durch A bestimmt und $\#A = \prod_{j \in \{1,\dots,k\}} p_j^{n_j}$.

Beweis. Die Existenz einer solchen Zerlegung haben wir bereits in der Linearen Algebra gezeigt (Korollar II.2.5.17); genauer gesagt haben wir dazu den Elementarteilersatz für Matrizen verwendet, um eine Zerlegung in zyklische Gruppen zu erhalten und diese dann mit dem Chinesischen Restsatz nach Primpotenzen sortiert.

Auch die Eindeutigkeit kann mit diesen Techniken nachgewiesen werden; da wir dies in der Linearen Algebra nicht im Detail ausgeführt haben, geben wir für den Fall der endlichen abelschen Gruppen noch ein elementares, direktes Argument:

Wir überlegen uns zunächst, dass es genügt, den Fall zu betrachten, in dem nur Potenzen einer einzigen Primzahl auftreten: Ist $A = \prod_{j=1}^{k} \mathbb{Z}/p_j^{n_j}$ eine endliche abelsche Gruppe und ist $p \in \mathbb{N}$ prim, so zeigt eine einfache Rechnung (mit dem Satz von Lagrange für Ordnungen (Korollar 1.1.59) und der Voraussetzung, dass p prim ist), dass

$$A(p) \cong_{\mathsf{Group}} \prod_{j \in \{\ell \in \{1,\dots,k\} \mid p_\ell = p\}} \mathbb{Z}/p_j^{n_j} = \prod_{j \in \{\ell \in \{1,\dots,k\} \mid p_\ell = p\}} \mathbb{Z}/p^{n_j}$$

(wobei der p-Anteil $A(p)$ von A wie in Lemma 1.3.2 definiert ist). Nach dem zweiten Teil von Lemma 1.3.2 genügt es also folgende Eindeutigkeitsaussage zu zeigen: Ist $p \in \mathbb{N}$ prim und sind $k, \ell, r, s \in \mathbb{N}$, $n_1, \dots, n_k, m_1, \dots, m_\ell \in \mathbb{N}_{>1}$ mit

$$A := \prod_{j=1}^{k} \mathbb{Z}/p^{m_j} \times (\mathbb{Z}/p)^r \cong_{\mathsf{Group}} \prod_{j=1}^{\ell} \mathbb{Z}/p^{n_j} \times (\mathbb{Z}/p)^s =: B,$$

so folgt $k = \ell$, $r = s$ und $(m_1, \dots m_k)$ ist eine Permutation von $(n_1, \dots, n_\ell)$. Wir beweisen diese Eindeutigkeitsaussage durch Induktion über die Anzahl $\#A = \#B$ der Gruppenelemente:

- *Induktionsanfang.* Haben die obigen Gruppen jeweils nur ein Element, so ist $k = 0 = \ell$ und $r = 0 = s$.
- *Induktionsvoraussetzung.* Es sei daher nun $k + r > 0$ und $\ell + s > 0$ und die obige Eindeutigkeitsaussage sei für Gruppen der obigen Form mit weniger Elementen bereits gezeigt.
- *Induktionsschritt.* Wir zeigen, dass die Eindeutigkeitsaussage auch für A und B gilt. Wegen $A \cong_{\mathsf{Group}} B$ folgt auch $p \cdot A \cong_{\mathsf{Group}} p \cdot B$ (nachrechnen); dabei ist $p \cdot A := \{p \cdot g \mid g \in A\}$ eine Untergruppe von A (wobei wir in diesem Beweis abelsche Gruppen additiv schreiben). Andererseits ist

  $$p \cdot A \cong_{\mathsf{Group}} \text{?} \quad \prod_{j=1}^{k} \mathbb{Z}/p^{m_j - 1} \quad \text{und} \quad p \cdot B \cong_{\mathsf{Group}} \text{?} \quad \prod_{j=1}^{\ell} \mathbb{Z}/p^{n_j - 1}$$

  (nachrechnen); insbesondere folgt $\#(p \cdot A) < \#A$. Aus der Induktionsvoraussetzung erhalten wir daher $k = \ell$ und dass $(m_1 - 1, \dots, m_k - 1)$ eine Permutation des Tupels $(n_1 - 1, \dots, n_\ell - 1)$ ist; somit ist $(m_1, \dots, m_k)$ eine Permutation von $(n_1, \dots, n_\ell)$ und insbesondere gilt $m_1 + \dots + m_k = n_1 + \dots + n_\ell$.

  Wegen $A \cong_{\mathsf{Group}} B$ ist andererseits auch

  $$p^{m_1 + \dots + m_k} \cdot p^r = \#A = \#B = p^{n_1 + \dots + n_\ell} \cdot p^s.$$

  Mit den obigen Überlegungen folgt daraus $p^r = p^s$ bzw. $r = s$. Dies vervollständigt den Induktionsschritt.

Damit ist die Eindeutigkeitsaussage gezeigt. □

Lemma 1.3.2. *Sei $(A, \cdot, e)$ eine abelsche Gruppe und sei $p \in \mathbb{N}$ prim.*

1. *Dann ist*
   $$A(p) := \left\{ g \in A \;\middle|\; \exists_{k \in \mathbb{N}} \quad g^{p^k} = e \right\}$$
   eine Untergruppe von A.
2. *Ist B eine abelsche Gruppe mit $B \cong_{\mathsf{Group}} A$, so folgt $B(p) \cong_{\mathsf{Group}} A(p)$.*

Beweis. Zu 1. Wir beweisen dies mithilfe der Charakterisierung von Untergruppen aus Proposition 1.1.26 und schreiben die Gruppe A multiplikativ.

- Offenbar ist das neutrale Element $e \in A$ in $A(p)$, denn $e^{p^0} = e$.

- Ist $g \in A(p)$, so ist wegen $(g^{-1})^n = (g^n)^{-1}$ für alle $n \in \mathbb{N}$ auch $g^{-1} \in A(p)$.

- Sind $g, h \in A(p)$, so ist auch $g \cdot h \in A(p)$, denn: Wegen $g, h \in A(p)$ gibt es $m, n \in \mathbb{N}$ mit $g^{p^m} = e = h^{p^n}$. Da A abelsch ist, folgt

$$(a \cdot b)^{p^{m+n}} = a^{p^{m+n}} \cdot b^{p^{m+n}} = (a^{p^m})^{p^n} \cdot (b^{p^n})^{p^m} = e \cdot e = e,$$

  und damit $g \cdot h \in A(p)$.

Also ist $A(p)$ eine Untergruppe von A.

Zu 2. Ist $f\colon B \longrightarrow A$ ein Gruppenhomomorphismus, so gilt $f(B(p)) \subset A(p)$ (nachrechnen). Wendet man diese Beobachtung auf einen Isomorphismus $B \longrightarrow A$ und sein Inverses an, so erhält man einen Isomorphismus $B(p) \longrightarrow A(p)$. □

Anmerkung zum Lernen. Um sich den Klassifikationssatz zu merken, genügt es eigentlich, sich die folgenden beiden Beispiele zu merken:

- Es gilt $\mathbb{Z}/2^2 = \mathbb{Z}/4 \ncong_{\mathsf{Group}} \mathbb{Z}/2 \times \mathbb{Z}/2$ (denn die linke Gruppe enthält ein Element der Ordnung 4 im Gegensatz zur rechten Gruppe).

- Es gilt $\mathbb{Z}/2 \times \mathbb{Z}/3 \cong_{\mathsf{Group}} \mathbb{Z}/6$ (wie man leicht nachrechnen kann oder aus dem Chinesischen Restsatz folgern kann).

Außerdem empfiehlt es sich, auch nochmal den Klassifikationssatz für endlich erzeugte abelsche Gruppen genauer anzusehen (Korollar II.2.5.17).

Beispiel 1.3.3 (Standard-Argument zur Klassifikation endlicher abelscher Gruppen)**.** Wieviele Isomorphieklassen von abelschen Gruppen A mit $\#A = 1988$ gibt es? Wir beantworten diese Frage mit dem Klassifikationssatz für endliche abelsche Gruppen (Satz 1.3.1):

Dazu bestimmen wir zunächst die Primfaktorzerlegung von 1988, nämlich

$$1988 = 2^2 \cdot 7 \cdot 71.$$

Nach dem Klassifkationssatz für endliche abelsche Gruppen ist daher

? $\mathbb{Z}/4 \times \mathbb{Z}/7 \times \mathbb{Z}/71 \cong_{\mathsf{Group}} \mathbb{Z}/1988, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/7 \times \mathbb{Z}/71$

ein Repräsentantensystem für die Menge der Isomorphieklassen aller abelschen Gruppen mit 1988 Elementen. Also gibt es genau zwei solcher Isomorphieklassen.

Mit dem Klassifikationssatz können zum Beispiel auch Fragen zur Anzahl von Elementen gegebener Ordnung und zur Klassifikation von Homomorphismen zwischen abelschen Gruppen beantwortet werden.

1.3.2 Symmetrische Gruppen

Nach dem Satz von Cayley (Satz 1.2.9) kann jede Gruppe als Untergruppe einer symmetrischen Gruppe aufgefasst werden. Es lohnt sich daher, symmetrische Gruppen und ihre Elemente etwas genauer zu betrachten.

Definition 1.3.4 (Zykel)**.** Sei $n \in \mathbb{N}$. Eine Permutation $\sigma \in S_n$ ist ein *Zykel*, wenn es $k \in \mathbb{N}$ und paarweise verschiedene $x_1, \ldots, x_k \in \{1, \ldots, n\}$ mit

$$\forall_{j \in \{1,\ldots,k-1\}} \quad \sigma(x_j) = x_{j+1}, \quad \sigma(x_k) = x_1, \quad \sigma_{\{1,\ldots,n\} \setminus \{x_1,\ldots,x_k\}} = \mathrm{id}$$

gibt. Dabei ist k die *Länge des Zykels* σ, wir notieren σ auch kurz in der Form

$$\sigma = (x_1 \ x_2 \ \ldots \ x_k)$$

und wir nennen $\{x_1, \ldots, x_k\}$ den *Träger des Zykels* σ.

Beispiel 1.3.5 (Zykel)**.**

- Transpositionen sind nichts anderes als Zykel der Länge 2.
- Die durch

  $$\begin{aligned} 1 &\longmapsto 2 \\ 2 &\longmapsto 1 \\ 3 &\longmapsto 4 \\ 4 &\longmapsto 3 \end{aligned}$$

  gegebene Permutation in S_4 ist *kein* Zykel (hat aber Ordnung 2!).
- Ist $n \in \mathbb{N}$ und sind $\sigma, \tau \in S_n$ Zykel mit disjunkten Trägern, so gilt

  $$\sigma \cdot \tau = \tau \cdot \sigma.$$

- Ist $n \in \mathbb{N}$, ist $\sigma = (x_1 \ \ldots \ x_k) \in S_n$ ein Zykel und ist $\tau \in S_n$, so gilt (nachrechnen)

  $$\tau \cdot \sigma \cdot \tau^{-1} = \big(\tau(x_1) \ \ldots \ \tau(x_k)\big).$$

Nicht jede Permutation ist ein Zykel, aber jede Permutation kann (im wesentlichen eindeutig) als Produkt von Zykeln geschrieben werden:

Proposition 1.3.6 (Zykelzerlegung)**.** *Sei $n \in \mathbb{N}$ und $\sigma \in S_n$. Dann gibt es $k \in \mathbb{N}$ und Zykel $\sigma_1, \ldots, \sigma_k \in S_n$ der Länge mindestens 2 mit paarweise disjunkten Trägern mit*

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_k.$$

Dabei sind k und $\{\sigma_1, \ldots, \sigma_k\}$ eindeutig durch σ bestimmt.

Beweis. Man kann diese Behauptung mit etwas Geduld direkt von Hand beweisen. Etwas einfacher lässt sich der Beweis mit dem folgenden Trick organisieren:

Wir betrachten die kanonische Operation von $\langle\sigma\rangle_{S_n} < S_n$ auf $\{1,\dots,n\}$. Dann liefern die Bahnen dieser Operation mit mehr als einem Element eine Zykelzerlegung von σ der obigen Form.

Umgekehrt lässt sich aus jeder Zykelzerlegung von σ die Bahnenzerlegung dieser Gruppenoperation rekonstruieren; dies zeigt die Eindeutigkeit. □

Satz 1.3.7 (Erzeugendensysteme symmetrischer Gruppen)**.** *Sei $n \in \mathbb{N}$. Dann ist jede der folgenden Mengen ein Erzeugendensystem von S_n:*

1. *Die Menge aller Zykel in S_n.*
2. *Die Menge $\big\{(j\ k) \mid j,k \in \{1,\dots,n\},\ j \neq k\big\}$ aller Transpositionen in S_n.*
3. *Die Menge $\big\{(1\ 2),(2\ 3),\dots,(n-1\ n)\big\}$.*
4. *Die (zwei-elementige!) Menge $\big\{(1\ 2),(1\ 2\ \dots\ n)\big\}$.*

Beweis. Zu 1. Dass die Menge aller Zykel ein Erzeugendensystem von S_n bildet, ist eine direkte Konsequenz aus der Zykelzerlegung (Proposition 1.3.6).

Zu 2. Nach dem ersten Teil genügt es zu zeigen, dass jeder Zykel als Produkt von Transpositionen geschrieben werden kann: Ist $k \in \mathbb{N}$ und sind $x_1,\dots,x_k \in \{1,\dots,n\}$ paarweise verschieden, so gilt (nachrechnen)

$$(x_1\ x_2\ \dots\ x_k) = \text{?}\quad (x_1\ x_2)\cdot(x_2\ x_3)\cdot\dots\cdot(x_{k-1}\ x_k)$$

Dies zeigt die zweite Aussage.

Zu 3. Jänich beschreibt dies wie folgt: „Offensichtlich kann man jede Permutation durch Hintereinanderanwendung endlich vieler Nachbarnvertauschungen herbeiführen, manche Bibliotheken weisen ihre Benutzer flehentlich auf diese Gefahr hin.“ [18, S. 153] Die Tatsache, dass Nachbarnvertauschungen ein Erzeugendensystem von S_n bilden, wird implizit auch im Sortierverfahren *bubble sort* verwendet.

Nach dem zweiten Teil genügt es zu zeigen, dass jede Transposition durch „Nachbarnvertauschungen“ erzeugt werden kann: Seien $j,k \in \{1,\dots,n\}$ mit $j \neq k$, ohne Einschränkung $j < k$. Dann ist (nachrechnen)

$$\begin{aligned}(j\ k) &= (j\ j+1\ \dots\ k)\cdot(k-1\ k-2\ \dots\ j)\\ &= \text{?}\quad (j\ j+1)\cdot\dots\cdot(k-1\ k)\cdot(k-1\ k-2)\cdot\dots\cdot(j+1\ j).\end{aligned}$$

Zu 4. Nach dem dritten Teil genügt es zu zeigen, dass jede Nachbarnvertauschung in der von $(1\ 2)$ und $(1\ 2\ \dots\ n)$ erzeugten Untergruppe von S_n liegt: Mit Beispiel 1.3.5 erhalten wir für alle $j \in \{1,\dots,n-1\}$, dass

$$(j\ j+1) = \text{?}\quad (1\ 2\ \dots\ n)^{j-1}\cdot(1\ 2)\cdot(1\ 2\ \dots\ n)^{-j+1}.$$ □

Insbesondere die vierte Aussage wird sich zum Beispiel in der Galoistheorie noch als nützlich erweisen: Möchte man zeigen, dass eine Untergruppe von S_n bereits ganz S_n ist, genügt es eine Transposition und einen kompatiblen n-Zykel in dieser Untergruppe zu finden! (Beispiel 3.5.12)

Ein wichtiges Hilfsmittel bei der Untersuchung symmetrischer Gruppen ist das Signum (s. Beweis der Leibniz-Formel für die Determinante (Satz I.5.4.17, Beispiel 1.1.46, Beispiel 1.1.53)). Wir erinnern an die Definition und die wichtigsten Eigenschaften:

Definition 1.3.8 (Signum, gerade/ungerade Permutation)**.** Sei $n \in \mathbb{N}$. Dann definieren wir das *Signum* durch

$$\begin{aligned} \operatorname{sgn}\colon S_n &\longrightarrow \{-1, 1\} \\ \sigma &\longmapsto \prod_{(j,k)\in J_n} \frac{\sigma(k) - \sigma(j)}{k - j}, \end{aligned}$$

wobei $J_n := \{(j,k) \mid j,k \in \{1,\dots,n\} \text{ und } j < k\}$. Permutationen $\sigma \in S_n$ mit $\operatorname{sgn}\sigma = 1$ bezeichnet man als *gerade Permutationen*, die anderen als *ungerade Permutationen*.

Man beachte, dass sgn tatsächlich nur die Werte -1 und 1 annimmt: Ist $\sigma \in S_n$, so haben die beiden Produkte $\prod_{(j,k)\in J_n}(\sigma(k) - \sigma(j))$ und $\prod_{(j,k)\in J_n}(k - j)$ bis auf das Vorzeichen dieselben Faktoren. Nach Definition misst das Signum wie sehr Permutation die Ordnung umkehren. Um das Signum besser zu verstehen, betrachten wir zwei wichtige Eigenschaften:

Beispiel 1.3.9 (Signum von Transpositionen)**.** Sei $n \in \mathbb{N}$. Für alle $J, K \in \{1,\dots,n\}$ mit $J \neq K$ gilt

$$\operatorname{sgn}(J\ K) = -1,$$

denn: Sei ohne Einschränkung $J < K$; wir schreiben $\sigma := (J\ K)$. Nach Definition ist $\operatorname{sgn}(\sigma) = (-1)^m$, wobei m die Anzahl der Paare $(j,k) \in J_n$ ist, für die $\sigma(k) < \sigma(j)$ ist. Im Fall der Transposition $\sigma = (J\ K)$ sind dies genau die folgenden Paare:

- Das Paar (J,K), sowie
- die Paare (J,k) mit $k \in \{J+1,\dots,K-1\}$ und
- die Paare (j,K) mit $j \in \{J+1,\dots,K-1\}$.

Also ist

$$\operatorname{sgn}(\sigma) = (-1)^{1+K-1-J+K-1-J} = -1.$$

Proposition 1.3.10 (Multiplikativität des Signums)**.** *Sei $n \in \mathbb{N}$. Dann gilt für alle $\sigma, \tau \in S_n$, dass*

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

Also ist sgn *ein Gruppenhomomorphismus von S_n in die multiplikative Gruppe $\{-1, 1\}$.*

Beweis. Seien $\sigma, \tau \in S_n$. Dann gilt

$$\begin{aligned}
\operatorname{sgn}(\sigma \circ \tau) &= \prod_{(j,k)\in J_n} \frac{\sigma\circ\tau(k) - \sigma\circ\tau(j)}{k-j} \\
&= \prod_{(j,k)\in J_n} \frac{\sigma\circ\tau(k) - \sigma\circ\tau(j)}{\tau(k)-\tau(j)} \cdot \frac{\tau(k)-\tau(j)}{k-j} \\
&= \Big(\prod_{(j,k)\in J_n} \frac{\sigma\circ\tau(k) - \sigma\circ\tau(j)}{\tau(k)-\tau(j)}\Big) \cdot \operatorname{sgn}(\tau) \\
&= \Big(\prod_{(j,k)\in J_n} \frac{\sigma(k) - \sigma(j)}{k-j}\Big) \cdot \operatorname{sgn}(\tau) \qquad \text{(siehe unten)} \\
&= \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau).
\end{aligned}$$

Im vorletzten Schritt haben wir verwendet, dass $\tau\colon \{1,\dots,n\} \longrightarrow \{1,\dots,n\}$ bijektiv ist, und die folgende Fallunterscheidung gemacht: Sei $(j,k) \in J_n$.

- Ist $\tau(j) < \tau(k)$, so ist $(\tau(j), \tau(k)) \in J_n$.
- Ist $\tau(j) > \tau(k)$, so ist $(\tau(k), \tau(j)) \in J_n$ und

$$\frac{\sigma\circ\tau(k) - \sigma\circ\tau(j)}{\tau(k)-\tau(j)} = \frac{\sigma\circ\tau(j) - \sigma\circ\tau(k)}{\tau(j)-\tau(k)}.$$

Also ist $\operatorname{sgn}(\sigma\circ\tau) = \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau)$. □

Beispiel 1.3.11. Für die zyklische Permutation $(1\ 2\ 3) \in S_3$ gilt

$\operatorname{sgn}(1\ 2\ 3) =$? $\operatorname{sgn}\big((2\ 3)\circ(1\ 2)\big) = \operatorname{sgn}(2\ 3)\cdot\operatorname{sgn}(1\ 2) = (-1)\cdot(-1) = 1.$

Korollar 1.3.12 (gerade Permutationen sind gerade)**.** *Sei $n \in \mathbb{N}$ und $\sigma \in S_n$. Es gebe $d \in \mathbb{N}$ und Transpositionen $\tau_1, \dots, \tau_d \in S_n$ mit $\sigma = \tau_d \circ \cdots \circ \tau_1$. Dann sind die folgenden Aussagen äquivalent:*

1. *Die Permutation σ ist gerade.*
2. *Die Zahl d ist gerade.*

Beweis. Per Induktion folgt aus Beispiel 1.3.9 und Propositon 1.3.10, dass $\operatorname{sgn}(\sigma) = (-1)^d$ ist. □

Da sich jede Permutation als Produkt endlich vieler Transpositionen schreiben lässt (Satz 1.3.7), sind die geraden Permutationen somit genau die

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(a)

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

(b)

Abbildung 1.14.: Das 14/15-Puzzle

Permutationen, die sich als Produkt einer *geraden* Anzahl von Transpositionen schreiben lassen. Die Menge der geraden Permutationen S_n ist als Kern von sgn ein Normalteiler in S_n, die *alternierende Gruppe* A_n (Beispiel 1.1.46).

Zum Beispiel erlaubt es das Signum, das folgende Problem zu analysieren (Aufgabe 6 aus der Einführung):

Beispiel 1.3.13 (das 14/15-Puzzle)**.** Beim 14/15-*Puzzle* sind fünfzehn numerierte Plättchen und eine „Lücke“ auf einem quadratischen Brett verteilt (siehe Abbildung 1.14(a)). Dann ist es *nicht* möglich, durch Verschieben der Plättchen die Position in Abbildung 1.14(b) zu erreichen (Übungsaufgabe).

Satz 1.3.14 (Erzeugendensysteme alternierender Gruppen)**.** *Sei $n \in \mathbb{N}$.*

1. *Dann ist die alternierende Gruppe A_n die Menge aller Elemente von S_n, die sich als Produkt von 3-Zykeln schreiben lassen.*

2. *Sei $n \in \mathbb{N}_{\geq 5}$. Dann gilt: Je zwei 3-Zykel in A_n sind (in A_n) konjugiert zueinander.*

Beweis. Zu 1. Jeder 3-Zykel in S_n liegt in A_n (Beispiel 1.3.11).

Ist umgekehrt $\sigma \in A_n$, so ist σ ein Produkt einer geraden Anzahl von Transpositionen. Induktiv erhalten wir aus den folgenden Beobachtungen, dass σ als Produkt von 3-Zykeln geschrieben werden kann:

Seien $x_1, \ldots, x_4 \in \{1, \ldots, n\}$ mit $x_1 \neq x_2$ und $x_3 \neq x_4$. Wir unterscheiden die folgenden Fälle:

① Ist $\{x_1, x_2\} = \{x_3, x_4\}$, so ist $(x_1\ x_2) \cdot (x_3\ x_4) = \mathrm{id}_{\{1,\ldots,n\}}$ das leere Produkt von 3-Zykeln.

② Ist $\#\{x_1, \ldots, x_4\} = 3$, ohne Einschränkung etwa $x_2 = x_3$, so gilt

$$(x_1\ x_2) \cdot (x_3\ x_4) = (x_1\ x_2) \cdot (x_2\ x_4) = (x_1\ x_2\ x_4).$$

③ Sind $x_1, \ldots, x_4$ alle verschieden, so gilt (nachrechnen)

$$(x_1\ x_2) \cdot (x_3\ x_4) = (x_1\ x_3\ x_2) \cdot (x_1\ x_3\ x_4).$$

Zu 2. Seien $(x_1\ x_2\ x_3), (y_1\ y_2\ y_3) \in A_n$ zwei 3-Zykel. Sei $\sigma \in S_n$ eine Permutation mit

$$\sigma(x_1) = y_1, \quad \sigma(x_2) = y_2, \quad \sigma(x_3) = y_3.$$

Dann gilt (in S_n), dass

$$(y_1\ y_2\ y_3) = \big(\sigma(x_1)\ \sigma(x_2)\ \sigma(x_3)\big) = \sigma \cdot (x_1\ x_2\ x_3) \cdot \sigma^{-1}$$

(Beispiel 1.3.5).

① Ist $\sigma \in A_n$, so ist nichts mehr zu zeigen.

② Ist σ ungerade, so können wir wegen $n \geq 5$ zwei Elemente $r, s \in \{1, \ldots, n\} \setminus \{x_1, x_2, x_3\}$ mit $r \neq s$ finden; dann ist $\tau := \sigma \circ (r\ s) \in A_n$ und

$$(y_1\ y_2\ y_3) = \tau \cdot (x_1\ x_2\ x_3) \cdot \tau^{-1},$$

wie gewünscht. □

Insbesondere werden wir diese Tatsachen verwenden, um zu zeigen, dass alternierende Gruppen im Sinne der Strukturtheorie einfach sind (Satz 1.3.17).

1.3.3 Die allgemeine Klasifikationsstrategie

Die Klassifikation endlicher Gruppen folgt dem allgemeinen Prinzip *divide et impera* (divide and conquer, teile und herrsche): Sei G eine endliche Gruppe.

- Wir versuchen einen Normalteiler $N \subset G$ mit $N \neq \{e\}$ und $N \neq G$ zu finden und betrachten die Quotientengruppe $Q := G/N$.
- Dann gilt $\#N < \#G$ und $\#Q < \#G$ und wir können induktiv annehmen, dass wir N und Q bereits verstehen.
- Um G zu verstehen, muss man also die zugehörige Gruppenerweiterung (Caveat 1.1.73)

  $$\{e\} \longrightarrow N \longrightarrow G \longrightarrow Q = G/N \longrightarrow \{e\}$$

  genauer untersuchen. Im einfachsten Fall besitzt diese Erweiterung einen Spalt und G ist ein semi-direktes Produkt von N und Q; es können aber auch kompliziertere Erweiterungen auftreten.

Die atomaren Bausteine dieser Strategie sind Gruppen, die *keine* nichttrivialen Normalteiler bzw. Quotientengruppen besitzen; dies sind die sogenannten einfachen Gruppen:

Definition 1.3.15 (einfache Gruppe)**.** Eine Gruppe G ist *einfach*, wenn $\{e\}$ und G die einzigen Normalteiler in G sind.

Beispiel 1.3.16 (einfache Gruppen)**.**

- Die triviale Gruppe ist einfach.
- Ist $p \in \mathbb{N}$ prim, so ist $\mathbb{Z}/p$ eine einfache Gruppe; dies folgt bereits aus dem Satz von Lagrange (Beispiel 1.1.33).
- Ist die Gruppe $\mathbb{Z}/2 \times \mathbb{Z}/2$ einfach?

  Ja Nein Die korrekte Antwort ist „Nein“. Die Untergruppe $\mathbb{Z}/2 \times \{[0]\}$ ist ein geeigneter Normalteiler. ×
- Ist die Gruppe $\mathbb{Z}/4$ einfach?

  Ja Nein Die korrekte Antwort ist „Nein“. Die von $[2]$ erzeugte Untergruppe ist ein geeigneter Normalteiler. ×
- Ist die Gruppe $\mathbb{Z}$ einfach?

  Ja Nein Die korrekte Antwort ist „Nein“. Die von 2 erzeugte Untergruppe ist ein geeigneter Normalteiler. ×
- Ist die Gruppe $\mathrm{GL}_2(\mathbb{R})$ einfach?

  Ja Nein Die korrekte Antwort ist „Nein“. Die Untergruppen $\mathrm{SL}_2(\mathbb{R})$ und $\{\lambda \cdot I_2 \mid \lambda \in \mathbb{R}^\times\}$ sind Beispiele für geeignete Normalteiler. ×
- Seien N, Q nicht-triviale Gruppen und $\varphi\colon Q \longrightarrow \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Ist $N \rtimes_\varphi Q$ einfach?

  Ja Nein Die korrekte Antwort ist „Nein“. Die Untergruppe $N \times \{e\}$ ist ein geeigneter Normalteiler. ×

Satz 1.3.17 (Einfachheit alternierender Gruppen)**.** *Sei $n \in \mathbb{N}$. Dann ist die alternierende Gruppe A_n genau dann einfach, wenn $n \neq 4$ ist.*

Beweis. Wir beginnen mit den kleinen alternierenden Gruppen:

- Die Gruppen $A_0 = S_0$, $A_1 = S_1$, und $A_2 = \{\mathrm{id}_{\{1,2\}}\}$ sind trivial und damit insbesondere einfach.
- Die Gruppe $A_3 = \langle\{(1\ 2\ 3)\}\rangle_{S_3} \cong_{\mathsf{Group}} \mathbb{Z}/3$ ist zyklisch von Primzahlordnung und daher einfach.
- Die Gruppe A_4 ist *nicht* einfach, denn

  $$\big\{\mathrm{id}, (1\ 2) \cdot (3\ 4), (1\ 3) \cdot (2\ 4), (1\ 4) \cdot (2\ 3)\big\}$$

  ist ein geeigneter Normalteiler von A_4 (nachrechnen; mithilfe von Beispiel 1.3.5).

Sei nun $n \geq 5$. Dann ist A_n einfach, denn: Sei $N \subset A_n$ ein Normalteiler mit $N \neq \{e\}$. Wir zeigen, dass dann bereits $N = A_n$ gilt. Wegen Satz 1.3.14 und der Abgeschlossenheit von N unter Konjugation (Normalteiler ...) genügt es dafür nachzuweisen, dass N mindestens einen 3-Zykel enthält:

Wir betrachten der Einfachheit (sic!) halber nur den Fall $n = 5$; der allgemeine Fall kann mit einer ähnlichen Zykelanalyse oder per Induktion aus diesem Fall erhalten werden [27, Theorem 3.11].

Wegen $N \neq \{e\}$ gibt es ein $\sigma \in N \setminus \{e\}$. Wir betrachten die Zykelzerlegung von σ (Proposition 1.3.6). Da σ eine gerade Permutation ist und $n = 5$ ist, können nur die folgenden Fälle eintreten:

① Es ist σ bereits ein 3-Zykel.

② Die Zykelzerlegung von σ ist

$$\sigma = (x\ y) \cdot (z\ w).$$

③ Die Zykelzerlegung von σ ist

$$\sigma = (x\ y\ z\ v\ w).$$

Zykelzerlegungen der Form $(x\ y) \cdot (z\ v\ w)$ oder $(x\ y\ z\ w)$ sind ungerade Permutationen und liegen daher nicht in A_5.

Im Fall ① ist nichts mehr zu tun.

Im Fall ② betrachten wir $\tau := (x\ y\ v)$ mit $v \in \{1, \ldots, 5 = n\} \setminus \{x, y, z, w\}$. Dann ist

$$\begin{aligned} (x\ y\ v) &= \sigma \cdot \tau \cdot \sigma \cdot \tau^{-1} && \text{(nachrechnen)} \\ &\in \sigma \cdot N && \text{(wegen ? } N \lhd G) \\ &\in N && \text{(wegen } \sigma \in N). \end{aligned}$$

Im Fall ③ betrachten wir $\tau := (x\ y) \cdot (z\ v)$. Dann ist

$$\begin{aligned} (x\ w\ z) &= \sigma \cdot \tau \cdot \sigma \cdot \tau^{-1} && \text{(nachrechnen)} \\ &\in \sigma \cdot N && \text{(wegen ? } N \lhd G) \\ &\in N && \text{(wegen } \sigma \in N). \end{aligned}$$

Also enthält N in jedem der Fälle einen 3-Zykel, wie gewünscht. □

Ausblick 1.3.18 (einfache Automorphismengruppen)**.** (Varianten von) Automorphismengruppen sind „oft“ gute Kandidaten für einfache Gruppen [13].

Ausblick 1.3.19 (Klassifikation der endlichen einfachen Gruppen)**.** Die Klassifikation der endlichen einfachen Gruppen besagt, dass jede endliche einfache Gruppe zu einer der folgenden Gruppen isomorph ist [4, 5]:

- einer zyklischen Gruppe $\mathbb{Z}/p$ mit einer Primzahl p,
- einer alternierenden Gruppe A_n mit $n \in \mathbb{N}_{\geq 5}$,
- einer endlichen Gruppe von „Lie-Typ“,
- einer der 26 „sporadischen Gruppen“,
- der Tits-Gruppe (die manchmal auch in eine der vorigen beiden Klassen einsortiert wird).

Der Beweis dieses Satzes ist *sehr* umfangreich und ist einer der Meilensteine der Mathematik des 20. Jahrhunderts.

1.3.4 Auflösbare Gruppen

Wir konzentrieren uns nun auf Gruppen, die auf einfache Weise in kleine, angenehme (nämlich abelsche), Stücke zerlegt werden können, die sogenannten auflösbaren Gruppen. Diese bilden einerseits eine naheliegende, gut analysierbare Klasse von interessanten Gruppen; andererseits werden diese Gruppen bei der Auflösung (daher der Name!) von polynomialen Gleichungen durch Radikale eine zentrale Rolle spielen (Kapitel 3.5.2). Als ersten Schritt betrachten wir Kommutatoren und abelsche Quotienten:

Definition 1.3.20 (Kommutator(untergruppe))**.** Sei G eine Gruppe.

- Seien $g, h \in G$. Der *Kommutator von g und h* ist definiert als
$$[g, h] := g \cdot h \cdot g^{-1} \cdot h^{-1}.$$
- Die *Kommutatoruntergruppe von G* ist die Untergruppe
$$[G, G] := \langle \{[g, h] \mid g, h \in G\} \rangle_G \subset G$$
die von den Kommutatoren in G erzeugt wird.

Bemerkung 1.3.21. Der Name *Kommutator* leitet sich aus der folgenden Beobachtung ab: Ist G eine Gruppe und sind $g, h \in G$, so gilt genau dann $[g, h] = e$, wenn
$$g \cdot h = h \cdot g$$
ist. Kommutatoren messen also, inwieweit Gruppenelemente miteinander kommutieren.

Die Kommutatoruntergruppe einer Gruppe G ist ein Normalteiler in G, da die Menge aller Kommutatoren in G ein konjugationsinvariantes Erzeugendensystem von $[G, G]$ ist: Für alle $g, h, k \in G$ gilt

$$\begin{aligned} k \cdot [g,h] \cdot k^{-1} &= k \cdot g \cdot h \cdot g^{-1} \cdot h^{-1} \cdot k^{-1} \\ &= k \cdot g \cdot k^{-1} \cdot k \cdot h \cdot k^{-1} \cdot k \cdot g^{-1} \cdot k^{-1} \cdot k \cdot h^{-1} \cdot k^{-1} \\ &= (k \cdot g \cdot k^{-1}) \cdot (k \cdot h \cdot k^{-1}) \cdot (k \cdot g^{-1} \cdot k^{-1})^{-1} \cdot (k \cdot h^{-1} \cdot k^{-1})^{-1} \\ &= [k \cdot g \cdot k^{-1}, k \cdot h \cdot k^{-1}]. \end{aligned}$$

Beispiel 1.3.22 (Kommutatoren)**.**

- Ist A abelsch, so ist $[A,A] = \{e\}$.
- Ist $n \in \mathbb{N}_{\geq 3}$, so gilt in S_n:

$$\big[(1\ 3),(2\ 3)\big] = \ ? \quad (1\ 3) \cdot (2\ 3) \cdot (1\ 3)^{-1} \cdot (2\ 3)^{-1} = (1\ 2\ 3)$$

- Ist $n \in \mathbb{N}_{\geq 3}$, so ist $[D_n, D_n]$ zyklisch (Übungsaufgabe).

Caveat 1.3.23. Ist G eine Gruppe, so bildet die Menge

$$\big\{[g,h] \;\big|\; g,h \in G\big\}$$

im allgemeinen *keine* Untergruppe von G; es ist aber etwas mühsam, explizite Beispiele dieser Form zu konstruieren bzw. zu überführen [27, Exercise 2.43]. Es ist daher bei der Definition der Kommutatorgruppe wichtig, die *von den Kommutatoren erzeugte Untergruppe* zu betrachten.

Proposition 1.3.24 (Abelianisierung)**.** *Sei G eine Gruppe und sei*

$$G_{\mathrm{ab}} := G/[G,G]$$

die Abelianisierung von G*.*

1. *Dann ist G_{ab} abelsch.*
2. *Die Gruppe G_{ab} ist der „größte“ abelsche Quotient von G: Ist $N \subset G$ ein Normalteiler, für den die Quotientengruppe G/N abelsch ist, so ist $[G,G] \subset N$.*
3. *Die Abelianisierung G_{ab} besitzt zusammen mit der kanonischen Projektion $\pi\colon G \longrightarrow G_{\mathrm{ab}}$ die folgende* universelle Eigenschaft*: Ist A eine abelsche Gruppe und $f\colon G \longrightarrow A$ ein Gruppenhomomorphismus, so gibt es genau einen Gruppenhomomorphismus $\overline{f}\colon G_{\mathrm{ab}} \longrightarrow A$ mit $\overline{f} \circ \pi = f$.*

Beweis. Wir machen zuerst eine vorbereitende Rechnung: Für alle $g,h \in G$ gilt

$$g \cdot h = h \cdot g \cdot [g^{-1}, h^{-1}].$$

Ist $N \subset G$ ein Normalteiler, so erhalten wir also in G/N die Gleichung

$$\begin{aligned}(g \cdot N) \cdot (h \cdot N) &= (g \cdot h) \cdot N \\ &= \big(h \cdot g \cdot [g^{-1}, h^{-1}]\big) \cdot N \\ &= (h \cdot N) \cdot (g \cdot N) \cdot \big([g^{-1}, h^{-1}] \cdot N\big)\end{aligned}$$

für alle $g, h \in G$.

Zu 1. Aus der obigen Gleichung folgt, dass $G_{\mathrm{ab}} = G/[G,G]$ abelsch ist (da der letzte Faktor in $G/[G,G]$ trivial ist).

Zu 2. Sei umgekehrt $N \subset G$ ein Normalteiler, für den G/N abelsch ist. Aus der obigen Gleichung folgt daher

$$\forall_{g,h \in G} \quad [g^{+1}, h^{+1}] \cdot N = N,$$

und damit

$$K := \big\{ [g,h] \;\big|\; g, h \in G \big\} \subset N.$$

Also ist auch $[G,G] = \langle K \rangle_G \subset \langle N \rangle_G = N$.

Zu 3. Dies ist eine Konsequenz aus den ersten beiden Teilen und der universellen Eigenschaft von Quotientengruppen (Proposition 1.1.48; nachrechnen). □

In gutartigen Gruppen erwarten wir, dass die Kommutatorgruppe kleiner ist als die ursprüngliche Gruppe bzw., dass wir nach endlich vielen Schritten durch Bildung iterierter Kommutatorgruppen bei der trivialen Gruppe ankommen. Dies definiert die Klasse der auflösbaren Gruppen:

Definition 1.3.25 (auflösbare Gruppe)**.** Sei G eine Gruppe.

- Dann definieren wir die *abgeleiteten Gruppen von* G induktiv durch $G^{(0)} := G$ und für alle $n \in \mathbb{N}$:

$$G^{(n+1)} := \big[G^{(n)}, G^{(n)}\big] \subset G^{(n)}$$

- Die Gruppe G ist *auflösbar*, wenn es ein $n \in \mathbb{N}$ mit $G^{(n)} = \{e\}$ gibt.

Beispiel 1.3.26 (auflösbare Gruppen)**.**

- Alle abelschen Gruppen sind auflösbar, denn ? die erste abgeleitete Gruppe ist bereits trivial.
- Ist $n \in \mathbb{N}_{>0}$, so ist die Diedergruppe D_n auflösbar, denn ? die erste abgeleitete Gruppe ist abelsch (Beispiel 1.3.22).
- Ist G eine nicht-triviale Gruppe mit $[G,G] = G$, so ist G *nicht* auflösbar.

Proposition 1.3.27 (Vererbungseigenschaften auflösbarer Gruppen)**.**

1. *Untergruppen auflösbarer Gruppen sind auflösbar.*

2. *Quotientengruppen von auflösbaren Gruppen sind auflösbar.*

3. *Erweiterungen von auflösbaren Gruppen sind auflösbar: Ist G eine Gruppe und ist $N \subset G$ ein Normalteiler in G, für den N und G/N auflösbar sind, so ist auch G auflösbar.*

Beweis. Zu 1. Ist $H \subset G$ eine Untergruppe von G, so folgt induktiv $H^{(n)} \subset G^{(n)}$ für alle $n \in \mathbb{N}$. Ist G auflösbar, so ist also auch H auflösbar.

Zu 2. Sei G eine auflösbare Gruppe und sei N ein Normalteiler in G. Dann ist auch $Q := G/N$ auflösbar, denn: Sei $\pi\colon G \longrightarrow Q$ die kanonische Projektion. Induktiv folgt für alle $n \in \mathbb{N}$, dass

$$Q^{(n)} = \pi(G^{(n)})$$

(nachrechnen). Da G auflösbar ist, gibt es ein $n \in \mathbb{N}$ mit $G^{(n)} = \{e\}$. Dann ist insbesondere auch $Q^{(n)} = \pi(G^{(n)}) = \pi(\{e\})$ die triviale Gruppe. Also ist auch Q auflösbar.

Zu 3. Da N und $Q := G/N$ auflösbar sind, gibt es $n, m \in \mathbb{N}$ mit $N^{(n)} = \{e\}$ und $Q^{(m)} = \{e\}$. Sei $\pi\colon G \longrightarrow Q$ die kanonische Projektion. Dann folgt wie im zweiten Teil, dass

$$\pi(G^{(m)}) = Q^{(m)} = \{e\},$$

und damit $G^{(m)} \subset \ker \pi = N$. Wie im ersten Teil erhalten wir dann aber

$$G^{(m+n)} \subset N^{(n)} = \{e\}.$$

Also ist G auflösbar. □

Satz 1.3.28 ((Nicht-)Auflösbarkeit symmetrischer Gruppen)**.** *Sei $n \in \mathbb{N}_{>0}$. Dann sind äquivalent:*

1. *Es ist $n \leq 4$.*

2. *Die Gruppe S_n ist auflösbar.*

3. *Die Gruppe A_n ist auflösbar.*

Beweis. Zu 1. $\Longrightarrow$ 2. Die Gruppen S_1 und S_2 sind abelsch, und damit auflösbar (Beispiel 1.3.26).

Außerdem ist $S_3 \cong_{\mathsf{Group}} D_3$ auflösbar (Beispiel 1.3.26).

Dass S_4 auflösbar ist, kann man zum Beispiel durch Berechnung der abgeleiteten Gruppen von S_4 oder durch Angabe einer geeigneten Normalreihe mit abelschen Faktoren nachweisen (Satz 1.3.31, Caveat 1.3.30; nachrechnen).

Zu 2. $\Longrightarrow$ 3. Ist S_n auflösbar, so ist auch die Untergruppe $A_n \subset S_n$ auflösbar (Proposition 1.3.27).

Zu 3. $\Longrightarrow$ 1. Sei $n \in \mathbb{N}_{\geq 5}$. Wir zeigen, dass A_n *nicht* auflösbar ist. Da A_5 zu einer Untergruppe von A_n isomorph ist, genügt es nach den Vererbungseigenschaften auflösbarer Gruppen (Proposition 1.3.27) zu zeigen, dass A_5 *nicht* auflösbar ist:

Es ist $[A_5, A_5] = A_5$, denn: Da A_5 einfach ist (Satz 1.3.17) und $[A_5, A_5]$ ein Normalteiler in A_5 ist, ist $[A_5, A_5] = \{e\}$ oder $[A_5, A_5] = A_5$. Wegen

$$(1\ 2\ 4) \cdot (1\ 3\ 5) \cdot (1\ 2\ 4)^{-1} \cdot (1\ 3\ 5)^{-1} = \text{?} \quad (1\ 2\ 3) \in A_5$$

(nachrechnen) ist $[A_5, A_5] \neq \{e\}$; also ist $[A_5, A_5] = A_5$.

Insbesondere ist A_5 (nach Definition von Auflösbarkeit über iterierte Kommutatorgruppen) *nicht* auflösbar. □

Alternativ können wir auflösbare Gruppen durch Normalreihen charakterisieren. Diese Charakterisierung werden wir im Zusammenhang mit der Auflösbarkeit von Gleichungen durch Radikale verwenden.

Definition 1.3.29 (Normalreihen)**.** Sei G eine Gruppe.

- Eine *Normalreihe* von G ist eine Folge $G_0, G_1, \ldots$ von Untergruppen von G mit $G_{n+1} \lhd G_n$ für alle $n \in \mathbb{N}$. Die *Faktoren* einer solchen Normalreihe sind die Quotientengruppen $G_0/G_1, G_1/G_2, \ldots$.
- Eine *endliche Normalreihe* von G ist eine Normalreihe

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}.$$

  endlicher Länge, die in der trivialen Gruppe endet.

Caveat 1.3.30 (Ketten von Normalteilern)**.** Ist $G = G_0 \rhd G_1 \rhd \ldots$ eine Normalreihe in G, so sind $G_2, G_3, \ldots$ im allgemeinen *keine* Normalteiler in G (sondern nur in der jeweils vorangegangenen Untergruppe). Dies kann zum Beispiel in A_4 beobachtet werden: Sei

$$K := \big\{\mathrm{id}, (1\ 2) \cdot (3\ 4), (1\ 3) \cdot (2\ 4), (1\ 4) \cdot (2\ 3)\big\} \subset A_4.$$

Dann ist $K \cong_{\mathsf{Group}} \mathbb{Z}/2 \times \mathbb{Z}/2$ ein Normalteiler in A_4 und $N := \{\mathrm{id}, (1\ 2) \cdot (3\ 4)\}$ ist ein Normalteiler in K. Aber N ist *kein* Normalteiler in A_4 (nachrechnen).

Satz 1.3.31 (Auflösbarkeit und Normalreihen)**.** *Sei G eine Gruppe. Dann sind äquivalent:*

1. *Die Gruppe G ist auflösbar.*
2. *Die Gruppe G besitzt eine endliche Normalreihe mit abelschen Faktoren.*

Ist G endlich, so ist G genau dann auflösbar, wenn G eine endliche Normalreihe mit zyklischen Faktoren besitzt.

Beweis. Zu 1. $\Longrightarrow$ 2. Dies folgt aus der Definition von Auflösbarkeit durch abgeleitete Gruppen und den Eigenschaften der Abelianisierung (Proposition 1.3.24).

Zu 2. $\Longrightarrow$ 1. Sei umgekehrt $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$ eine Normalreihe von G mit abelschen Faktoren. Wir zeigen induktiv, dass G_n, $G_{n-1}, \ldots, G_0 = G$ auflösbar sind:

Die triviale Gruppe G_n ist auflösbar. Ist G_{k+1} auflösbar, so ist auch G_k auflösbar, denn: Da sowohl der Normalteiler $G_{k+1} \lhd G_k$ als auch der (abelsche!) Quotient G_k/G_{k+1} auflösbar sind, ist auch die Erweiterungsgruppe G_k auflösbar (Proposition 1.3.27). Induktiv ergibt sich somit, dass $G = G_0$ auflösbar ist.

(Alternativ könnte man induktiv mithilfe von Proposition 1.3.24 zeigen, dass $G^{(k)} \subset G_k$ gilt und somit auf $G^{(n)} = \{e\}$ schließen.)

Jede Normalreihe mit (endlichen) abelschen Faktoren kann mithilfe der Zerlegung endlicher abelscher Gruppen in zyklische Gruppen zu einer Normalreihe mit zyklischen Faktoren verfeinert werden (Übungsaufgabe). □

Ausblick 1.3.32 (der Satz von Feit–Thompson)**.** Nach dem Satz von Feit und Thompson ist jede endliche Gruppe, die aus einer ungeraden Anzahl von Elementen besteht, auflösbar (!) [14, 17]. Der Beweis ist nicht in Reichweite dieser Vorlesung und wir werden diesen Satz daher nicht anwenden. Auch nicht in den Übungsaufgaben ... Es ist jedoch zur Plausibilitätsüberprüfung bei der Untersuchung endlicher Gruppen nützlich, diesen Satz zu kennen.

Wir werden im folgenden Techniken kennenlernen, die uns bei einigen Gruppen helfen werden, die Auflösbarkeit nachzuweisen.

1.3.5 Die Sylowsätze

Nach dem Satz von Lagrange für Ordnungen (Korollar 1.1.59) wissen wir, dass die Ordnungen von Gruppenelementen in endlichen Gruppen die Gesamtanzahl der Gruppenelemente teilen muss. Wie sieht es mit der Umkehrung aus?

Caveat 1.3.33 (Umkehrung des Satzes von Lagrange für Ordnungen?)**.** Im allgemeinen werden wir *nicht* zu jedem Teiler auch Elemente dieser Ordnung finden: zum Beispiel enthält $\mathbb{Z}/2 \times \mathbb{Z}/2$ *kein* Element der Ordnung 4.

Wir werden aber sehen, dass jeder Primteiler als Ordnung eines Elements auftritt (Korollar 1.3.40).

Allgemeiner können wir die analoge Frage nicht nur für Elemente, sondern auch für Untergruppen stellen.

Caveat 1.3.34 (Umkehrung des Satzes von Lagrange für Untergruppen von endlichen Gruppen?)**.** Im allgemeinen werden wir *nicht* zu jedem Teiler auch eine Untergruppe mit dieser Anzahl an Elementen finden: zum Beispiel enthält A_5 *keine* Untergruppe mit genau 30 Elementen (denn diese hätte Index 2 und wäre somit normal (Übungsaufgabe), im Widerspruch zur Einfachheit von A_5 (Satz 1.3.17)).

Wir werden aber sehen, dass Teiler, die (maximale) Primpotenzen sind, durch Untergruppen realisierbar sind. In diesem Zusammenhang spielen sogenannte p-Gruppen und Sylowgruppen eine wichtige Rolle. Sylowgruppen sind auflösbar und in günstigen Fällen gibt es sogar normale Sylowgruppen. Sylowgruppen sind daher ein bewährtes Mittel, um interessante Normalteiler aufzuspüren oder Auflösbarkeit nachzuweisen.

Definition 1.3.35 (p-Gruppe, Sylowgruppe)**.** Sei $p \in \mathbb{N}$ prim.

- Eine endliche Gruppe G ist eine *(endliche) p-Gruppe*, wenn es ein $k \in \mathbb{N}$ mit $\#G = p^k$ gibt.
- Sei G eine endliche Gruppe. Eine *p-Sylowgruppe in G* ist eine Untergruppe $S \subset G$ von G, die eine p-Gruppe ist und für die der Index $[G : S]$ *nicht* durch p teilbar ist (d.h. $\#S$ ist die maximale p-Potenz, die $\#G$ teilt).

Beispiel 1.3.36 (Sylowgruppen)**.**

- Die Diedergruppe D_4 ist wegen $\#D_4 = 8 = 2^3$ eine 2-Gruppe. Insbesondere sind *nicht* alle 2-Gruppen abelsch.
- Die Gruppe D_5 ist *keine* 2-Gruppe, denn $\#D_5 = 10 = 2 \cdot 5$. Eine 5-Sylowgruppe von $D_5 = \mathbb{Z}/5 \rtimes \mathbb{Z}/2$ ist ? $\mathbb{Z}/5 \times \{[0]\}$.

  Beispiele für 2-Sylowgruppen von D_5 sind ? $\{[0]\} \times \mathbb{Z}/2$ und $\{([0],[0]),([1],[1])\}$. Insbesondere sind 2-Sylowgruppen im allgemeinen weder eindeutig noch Normalteiler.
- Ist A eine endliche abelsche Gruppe, so ist die Gruppe $A(p)$ aus Lemma 1.3.2 bzw. Satz 1.3.1 eine p-Sylowgruppe in A (nachrechnen).

Zwar sind p-Gruppen im allgemeinen nicht abelsch, sie eignen sich aufgrund ihrer Auflösbarkeit aber dennoch gut als elementare Bausteine:

Satz 1.3.37 (Auflösbarkeit von p-Gruppen)**.** *Sei $p \in \mathbb{N}$ prim und sei G eine endliche p-Gruppe. Dann gilt:*

1. *Das Zentrum $Z(G)$ von G ist nicht-trivial (falls G nicht-trivial ist).*
2. *Die Gruppe G ist auflösbar.*
3. *Ist $\#G = p^2$, so ist G bereits abelsch (und damit entweder isomorph zu $\mathbb{Z}/p^2$ oder zu $\mathbb{Z}/p \times \mathbb{Z}/p$).*

Beweis. Zu 1. Der Schlüssel ist die Klassengleichung (Korollar 1.2.20): Sei $\#G \neq 1$ und sei $(g_i)_{i \in I}$ ein Repräsentantensystem für die nicht-trivialen Konjugationsklassen in G. Dann liefert die Klassengleichung:

$$\#Z(G) = \#G - \sum_{i \in I} [G : Z_G(g_i)]$$

Ist $i \in I$, so ist $Z_G(g_i) \neq G$, da ja g_i *nicht* im Zentrum von g liegt. Daher sind nach dem Satz von Lagrange (Korollar 1.1.34) alle Terme auf der rechten Seite (als Teiler der p-Potenz $\#G$) nicht-triviale Potenzen von p, und damit durch p teilbar. Also ist auch $\#Z(G)$ durch p teilbar; insbesondere ist die Gruppe $Z(G)$ nicht-trivial.

Zu 2. Wir beweisen dies durch Induktion über $\#G$:

- *Induktionsanfang.* Ist $\#G = p^0 = 1$, so ist die Gruppe G trivial, und damit insbesondere auflösbar.
- *Induktionsvoraussetzung.* Es sei $\#G > 1$ und es sei bereits gezeigt, dass alle p-Gruppen mit weniger als $\#G$ Elementen auflösbar sind.
- *Induktionsschritt.* Wir zeigen, dass dann auch G auflösbar ist: Nach dem ersten Teil ist das Zentrum $Z(G)$ ein Normalteiler in G mit $\#Z(G) \neq 1$. Wir betrachten die Quotientengruppe

$$Q := G/Z(G).$$

  Dann ist $\#Q < \#G$ und nach dem Satz von Lagrange ist auch Q eine p-Gruppe (denn $\#Q$ ist ein Teiler der p-Potenz $\#G$). Nach Induktionsvoraussetzung ist Q also auflösbar. Als abelsche Gruppe ist außerdem auch $Z(G)$ auflösbar. Daher ist auch die Erweiterungsgruppe G auflösbar (Proposition 1.3.27).

Zu 3. Ist G eine Gruppe und ist $G/Z(G)$ zyklisch, so ist G bereits abelsch (Übungsaufgabe). Zusammen mit dem ersten Teil kann man dann aus $\#G = p^2$ schließen, dass G abelsch ist (Übungsaufgabe). □

Bemerkung 1.3.38 (Klassifikation der acht-elementigen Gruppen)**.** Bis auf Isomorphie gibt es genau fünf acht-elementige Gruppen, nämlich:

- Die abelschen Gruppen ? $\mathbb{Z}/8$, $\mathbb{Z}/4 \times \mathbb{Z}/2$, $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.
- Die Diedergruppe D_4.
- Die *Quaternionengruppe* Q_8, d.h. die multiplikative Untergruppe der Quaternionen, die von $1, i, j, k$ erzeugt wird (Abbildung 1.15).

Wie kann man dies zeigen? Sei G eine Gruppe mit $\#G = 8 = 2^3$. Also ist das Zentrum $Z(G)$ nicht-trivial (Satz 1.3.37); nach dem Satz von Lagrange (Korollar 1.1.34) ist somit $\#Z(G) \in \{2, 4, 8\}$.

- Ist $\#Z(G) = 8$, so ist $G = Z(G)$ abelsch und wir können den Klassifikationssatz für endliche abelsche Gruppen anwenden (Satz 1.3.1).
- Ist $\#Z(G) = 4$, so ist $G/Z(G) \cong_{\mathsf{Group}} \mathbb{Z}/2$ (es gibt keine weitere Isomorphieklasse zwei-elementiger Gruppen); insbesondere ist $G/Z(G)$ zyklisch, und daher ist G abelsch (Übungsaufgabe). Dann ist aber $\#Z(G) \neq 4$. Dieser Fall kann also nicht eintreten.

·	e	i	j	k	E	I	J	K
e	e	i	j	k	E	I	J	K
i	i	E	k	J	I	e	K	j
j	j	K	E	i	J	k	e	I
k	k	j	I	E	K	J	i	e
E	E	I	J	K	e	i	j	k
I	I	e	K	j	i	E	K	j
J	J	k	e	I	j	K	E	i
K	K	J	i	e	k	j	I	E

Abbildung 1.15.: Die Verknüpfungstabelle der Quaternionengruppe Q_8; dabei sind e, i, j, k die Elemente 1, i, j, k aus der Quaternionenalgebra (diese bilden eine $\mathbb{R}$-Basis) und es stimmen E, I, J, K mit den additiven Inversen von 1, i, j, k in der Quaternionenalgebra überein.

- Ist $\#Z(G) = 2$, so ist $G/Z(G)$ eine vier-elementige Gruppe und daher nach Satz 1.3.37 (oder zu Fuß) isomorph zu $\mathbb{Z}/4$ (was aber wieder zyklisch ist und damit G abelsch wäre ...) oder zu $\mathbb{Z}/2 \times \mathbb{Z}/2$. Im letzteren Fall kann man von Hand Schritt für Schritt nachrechnen, dass G zu D_8 oder zu Q_8 isomorph ist.

Außerdem sind D_4 und Q_8 nicht abelsch und es gilt $D_4 \ncong_{\mathsf{Group}} Q_8$ (wie zum Beispiel an der Anzahl der Elemente der Ordnung 4 abgelesen werden kann).

Satz 1.3.39 (Sylowsätze). *Sei G eine endliche Gruppe und sei $p \in \mathbb{N}$ prim. Dann gilt:*

1. *Es gibt eine p-Sylowgruppe in G.*
2. *Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.*
3. *Je zwei p-Sylowgruppen von G sind konjugiert (insbesondere isomorph) zueinander.*
4. *Sei s_p die Anzahl der p-Sylowgruppen von G. Dann gilt*

$$s_p \mid \#G \quad \textit{und} \quad s_p \equiv 1 \mod p.$$

Bevor wir diesen Satz beweisen, zeigen wir wie man den Satz bei der Untersuchung endlicher Gruppen einsetzen kann:

Korollar 1.3.40 (Satz von Cauchy). *Sei G eine endliche Gruppe und sei $p \in \mathbb{N}$ ein Primteiler von $\#G$. Dann gibt es ein Element der Ordnung p in G.*

Beweis. Nach den Sylowsätzen (Satz 1.3.39) enthält G eine p-Sylowgruppe S; sei $k \in \mathbb{N}$ mit $\#S = p^k$. Da p ein Teiler von $\#G$ ist, ist $k \geq 1$. Sei $g \in S \setminus \{e\}$. Nach dem Satz von Lagrange (Korollar 1.1.59) gibt es also ein $\ell \in \{1, \dots, k\}$ mit

$$\operatorname{ord} g = p^\ell.$$

Dann ist $g^{p^{\ell-1}}$ ein Element der Ordnung p in G (nachrechnen). □

Bemerkung 1.3.41 (nochmal p-Gruppen)**.** Sei $p \in \mathbb{N}$ prim. Aus dem Satz von Cauchy (Korollar 1.3.40) und dem Satz von Lagrange (Korollar 1.1.59) folgt insbesondere: Eine endliche Gruppe G ist genau dann eine endliche p-Gruppe, wenn

$$\forall_{g \in G} \quad \exists_{k \in \mathbb{N}} \quad \operatorname{ord} g = p^k$$

gilt. Für unendliche Gruppen verwendet man daher diese Eigenschaft als Definition von p-Gruppen.

Korollar 1.3.42 (Sylownormalteiler)**.** *Sei G eine endliche Gruppe, sei $p \in \mathbb{N}$ ein Primteiler von $\#G$ und sei s_p die Anzahl der p-Sylowgruppen von G. Dann sind äquivalent:*

1. *Jede p-Sylowgruppe von G ist ein Normalteiler.*
2. *Eine p-Sylowgruppe von G ist ein Normalteiler.*
3. *Es gilt $s_p = 1$.*

Beweis. Die Äquivalenz folgt daraus, dass nach den Sylowsätzen (Satz 1.3.39) alle p-Sylowgruppen zueinander konjugiert sind und eine Untergruppe $H \subset G$ genau dann ein Normalteiler ist, wenn

$$\forall_{g \in G} \quad g \cdot H \cdot g^{-1} = H$$

gilt. □

Korollar 1.3.43 (Auflösbarkeit via Sylowsätze)**.** *Seien $p, q \in \mathbb{N}$ prim und sei G eine Gruppe mit $\#G = p \cdot q$ (zum Beispiel 4034 oder 55 oder ...). Dann ist G auflösbar.*

Beweis. Ist $p = q$, so wissen wir bereits, dass G auflösbar (sogar abelsch) ist (Satz 1.3.37).

Ohne Einschränkung sei nun $q < p$. Nach den Sylowsätzen (Satz 1.3.39) gibt es eine p-Sylowgruppe $S \subset G$; diese ist als p-Gruppe auflösbar (in diesem Fall gilt sogar $\#S = p$, und damit $S \cong_{\mathsf{Group}} \mathbb{Z}/p$).

Wir verwenden die Sylowsätze, um zu zeigen, dass S auch ein Normalteiler von G ist: Sei s_p die Anzahl der p-Sylowgruppen von G. Dann gilt nach den Sylowsätzen (Satz 1.3.39):

$$s_p \mid \#G \quad \text{und} \quad s_p \equiv 1 \mod p.$$

Wegen $s_p \mid \#G$ und der Voraussetzung, dass p und q prim sind, folgt

$$s_p \in \boxed{?} \quad \{1, q, p, p \cdot q\}.$$

Aus der zweiten Gleichung und $1 < q < p$ schließen wir, dass nur $s_p = 1$ infrage kommt. Also ist S ein Normalteiler in G (Korollar 1.3.42).

Mit dem Satz von Lagrange (Korollar 1.1.34) folgt, dass die Quotientengruppe G/S genau q Elemente enthält. Da q prim ist, ist G/S auflösbar (sogar $G/S \cong_{\mathsf{Group}} \mathbb{Z}/q$).

Da S und G/S auflösbar sind, ist auch die Erweiterungsgruppe G auflösbar (Proposition 1.3.27). □

In Anhang A.5 sind Beispiele zusammengestellt, wie man Gruppen mit gegebenen Anzahlen mithilfe der Sylowsätze analysieren kann.

Anmerkung zum Lernen. Bei der Untersuchung endlicher Gruppen sollte man sich die folgenden Fragen stellen:

- Greift ein allgemeiner Struktursatz? Oder ist eine Analyse „von Hand“ erforderlich?
- Zu welchen Primzahlen existieren nicht-triviale Sylowgruppen?
- Welche Anzahlen von Sylowgruppen sind jeweils möglich?
- Wie können/müssen/sollen die Sylowgruppen (zu gleichen oder unterschiedlichen Primzahlen) interagieren?
- Im Falle normaler Sylowgruppen: Was kann man über die Quotientengruppe sagen?
- Im Falle nicht-normaler Sylowgruppen: Was kann man über die Konjugationsoperation auf der Menge der Sylowgruppen sagen?
- Wie vergleichen sich die Ergebnisse mit vertrauten Beispielgruppen?

Anmerkung für Lehramtsstudenten. Staatsexamensaufgaben zu endlichen Gruppen involvieren oft Sylowargumente vom obigen Typ bzw. geeignete Varianten davon. Um Aufgaben dazu erfolgreich lösen zu können, ist es wichtig, diese Art von Argumenten und Rechnungen so intensiv zu üben, dass man die einzelnen Handgriffe gut und flüssig beherrscht.

Wir können die behandelten Klassifikationstechniken grob wie in Abbildung 1.16 zusammenfassen. Die Sylowsätze helfen dabei zum Beispiel bei der Überprüfung nach Auflösbarkeit bzw. beim Auffinden interessanter Normalteiler. In den roten „Blättern“ dieses Baums geht man induktiv vor und muss jeweils die entsprechenden Erweiterungsprobleme betrachten. Für viele endliche Gruppen liefern diese Bausteine bereits genug Informationen, um mit

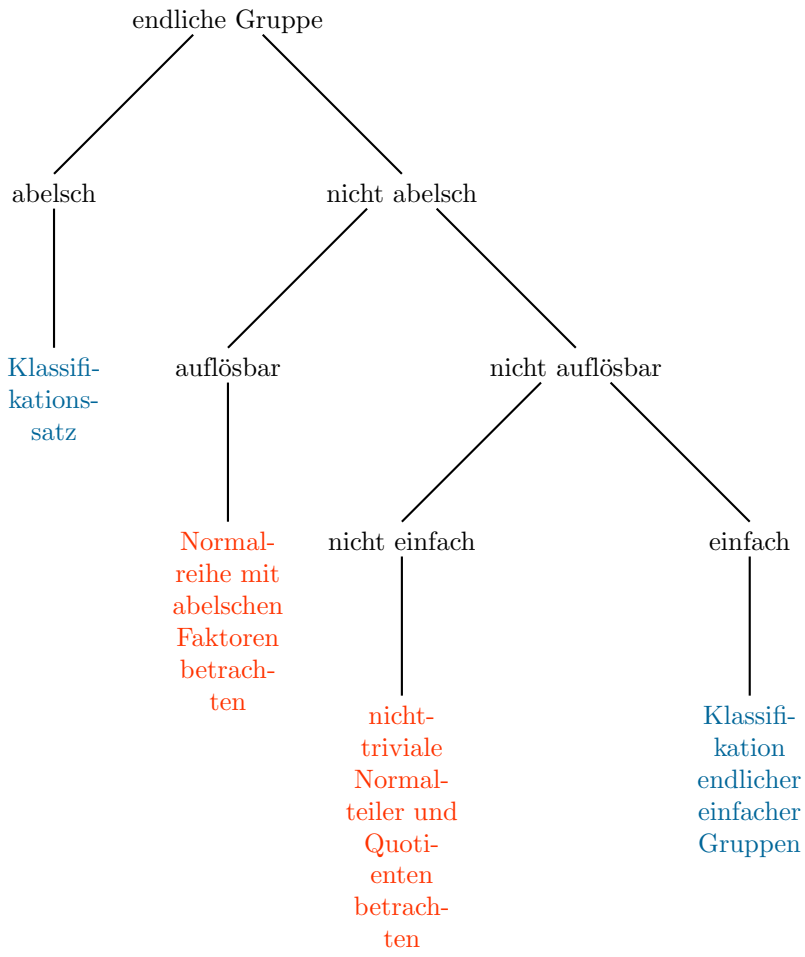


Abbildung 1.16.: Zerlegung von endlichen Gruppen

wenigen zusätzlichen Überlegungen ein gutes Verständnis der betrachteten Gruppe zu erlangen.

Wir geben nun einen Beweis der Sylowsätze:

Beweis von Satz 1.3.39. Der Beweis der Sylowsätze beruht auf einer geschickten Anwendung von geeigneten Gruppenoperationen und Teilbarkeitsargumenten: Ohne Einschränkung sei p ein Teiler von $\#G$.

Zu 1. Wir schreiben $\#G = p^k \cdot m$ mit $k, m \in \mathbb{N}$ und $p \nmid m$ und betrachten die Menge

$$X := \left\{ A \subset G \;\middle|\; \#A = p^k \right\}.$$

Dann operiert G auf X durch Linkstranslation. Die Idee ist, zu zeigen, dass die Standgruppe eines geeigneten Elements aus X eine p-Sylowgruppe von G ist. Wir erhalten für die obige G-Operation auf X mit der Bahnengleichung (Satz 1.2.15)

$$\binom{m \cdot p^k}{p^k} = \#X = \sum_{G \cdot A \in G \backslash X} [G : G_A].$$

Der Binomialkoeffizient auf der linken Seite ist *nicht* durch p teilbar, denn:

$$\binom{m \cdot p^k}{p^k} = \prod_{j=0}^{p^k-1} \frac{m \cdot p^k - j}{p^k - j}$$

und keiner dieser Faktoren ist durch p teilbar, denn: Sei $j \in \{0, \ldots, p^k - 1\}$. *Angenommen,* es gäbe $r \in \mathbb{N}$ mit $m \cdot p^k - j = p \cdot r \cdot (p^k - j)$. Dann folgt

$$j \cdot (1 - p \cdot r) = m \cdot p^k - p^{k+1} \cdot r = p^k \cdot (m - p \cdot r).$$

Da $1 - p \cdot r$ *nicht* durch p teilbar ist und p prim ist, muss p^k ein Teiler von j sein. Wegen $j \in \{0, \ldots, p^k - 1\}$ ist also $j = 0$. Dies ergibt aber

$$m \cdot p^k = p \cdot r \cdot p^k,$$

im Widerspruch dazu, dass p kein Teiler von m ist.

Also ist auch $\sum_{G \cdot A \in G \backslash X} [G : G_A]$ *nicht* durch p teilbar. Insbesondere gibt es ein $A \in X$, für das $[G : G_A]$ nicht durch p teilbar ist.

Wir zeigen, dass die soeben aus dem Hut gezauberte Gruppe G_A eine p-Sylowgruppe von G ist, indem wir $\#G_A = p^k$ nachweisen: Einerseits ist nach dem Satz von Lagrange (Korollar 1.1.34)

$$m \cdot p^k = \#G = [G : G_A] \cdot \#G_A,$$

und damit p^k ein Teiler von $\#G_A$. Andererseits gilt (nach Definition des Stabilisators G_A)

$$\forall_{a \in A} \quad \forall_{g \in G_A} \quad g \cdot a \in g \cdot A = A,$$

und damit (da $A \neq \emptyset$) $\#G_A \leq \#A = p^k$. Also ist $\#G_A = p^k$, wie gewünscht.

Zu 2. Sei $H \subset G$ eine p-Untergruppe von G (d.h. eine Untergruppe von G, die eine p-Gruppe ist); nach dem ersten Teil besitzt G eine p-Sylowgruppe S. Wir zeigen, dass es $g \in G$ mit $H \subset g \cdot S \cdot g^{-1}$ gibt: Dazu betrachten wir die Linkstranslationsoperation

$$\begin{aligned} H \times X &\longrightarrow X \\ (h, g \cdot S) &\longmapsto (h \cdot g) \cdot S \end{aligned}$$

auf der Menge $X := G/S$ der Linksnebenklassen von S in G.

Die Bahnengleichung (Satz 1.2.15) liefert für diese H-Operation:

$$[G : S] = \#(G/S) = \#X = \sum_{H \cdot x \in H \backslash X} [H : H_x]$$

Da H eine p-Gruppe ist, folgt mit dem Satz von Lagrange (Korollar 1.1.34), dass $[H : H_x]$ durch p teilbar ist, falls $H_x \neq H$ ist. Andererseits gilt: Da S eine p-Sylowgruppe von G ist, ist die linke Seite der Bahnengleichung *nicht* durch p teilbar. Also gibt es ein $x \in X$ mit $H_x = H$.

Wir übersetzen dies zurück in Linksnebenklassen: Es gibt somit ein $g \in G$ mit $H \cdot g \cdot S \subset g \cdot S$, und damit $H \cdot g \subset g \cdot S$ bzw.

$$H \subset g \cdot S \cdot g^{-1}.$$

Mit S ist auch die konjugierte Untergruppe $g \cdot S \cdot g^{-1}$ eine p-Sylowgruppe in G. Insbesondere ist H in einer p-Sylowgruppe von G enthalten.

Zu 3. Seien S und T zwei p-Sylowgruppen in G; insbesondere handelt es sich dabei um p-Gruppen. Nach dem Beweis des zweiten Teiles existiert ein $g \in G$ mit

$$T \subset g \cdot S \cdot g^{-1}.$$

Da S und T als p-Sylowgruppen in G dieselbe (endliche) Anzahl an Elementen besitzen und Konjugation mit g auf G bijektiv ist, folgt daraus bereits

$$T = g \cdot S \cdot g^{-1}.$$

Zu 4. Sei X die Menge aller p-Sylowgruppen von G; also ist $s_p = \#X$. Die Gruppe G operiert durch Konjugation auf X.

Nach dem ersten Teil ist $X \neq \emptyset$; sei etwa $x \in X$. Da die Konjugationsoperation von G auf X nach dem dritten Teil transitiv ist, gilt (Satz 1.2.15)

$$s_p = \#X = \#(G \cdot x) = [G : G_x].$$

Mit dem Satz von Lagrange (Korollar 1.1.34) erhalten wir also insbesondere, dass s_p ein Teiler von $\#G$ ist.

Warum ist $s_p \equiv 1 \mod p$? Sei S eine p-Sylowgruppe in G (eine solche existiert nach dem ersten Teil). Wir schränken die Konjugationsoperation von G auf X zur Konjugationsoperation von S auf X ein. Dann liefert die Bahnengleichung (Satz 1.2.15), dass

$$s_p = \#X = \sum_{S \cdot x \in S \backslash X} [S : S_x].$$

Ist $x \in X$ *kein* S-Fixpunkt dieser Operation, so ist $[S : S_x]$ nach dem Satz von Lagrange (Korollar 1.1.34) durch p teilbar. Aufgrund der obigen Gleichung ist somit

$$s_p \equiv \#\{x \in X \mid \forall_{s \in S} \quad s \cdot x = x\} \mod p.$$

Es genügt daher zu zeigen, dass diese Operation genau einen S-Fixpunkt besitzt (nämlich $S \in X$): Sei $T = h \cdot S \cdot h^{-1}$ mit $h \in G$ ein S-Fixpunkt. Dann ist S eine Untergruppe der Gruppe (der sogenannte *Normalisator* von T in G)

$$N_G(T) := \{g \in G \mid g \cdot T \cdot g^{-1} = T\} < G$$

und T ist nach Konstruktion ein Normalteiler in $N_G(T)$. Mit dem ersten Isomorphiesatz (angewendet auf die umgebende Gruppe $N_G(T)$; Satz 1.1.62) und dem Satz von Lagrange (Korollar 1.1.34) erhalten wir daher

$$\begin{aligned} \#(S \cdot T) &= \#T \cdot [S \cdot T : T] && \text{(Satz von Lagrange)} \\ &= \#T \cdot [S : (S \cap T)]. && \text{(erster Isomorphiesatz)} \\ &= \#S \cdot [S : (S \cap T)]. \end{aligned}$$

Also ist $S \cdot T$ eine p-Untergruppe von G; insbesondere ist $\#S \geq \#(S \cdot T)$ und mit der obigen Gleichung folgt $[S : (S \cap T)] = 1$ bzw. $S \cap T = S$. Wegen $\#S = \#T$ folgt $T = S$. Somit besitzt die S-Konjugationsoperation auf X genau einen Fixpunkt und es folgt

$$s_p \equiv 1 \mod p$$

wie behauptet. □

Bemerkung 1.3.44 (alternativer Beweis der Existenz von Sylowgruppen)**.** Der erste Teil der Sylowsätze (Satz 1.3.39) kann alternativ zum Beispiel auch wie folgt durch Induktion über $\#G$ bewiesen werden, analog zum Beweis der Auflösbarkeit von p-Gruppen (Satz 1.3.37):

- *Induktionsanfang.* Ist $\#G = 1$, so ist die Behauptung trivialerweise erfüllt. Allgemeiner: Ist p *kein* Teiler von G, so ist die triviale Untergruppe eine p-Sylowgruppe von G.
- *Induktionsvoraussetzung.* Es sei p ein Teiler von $\#G$ und die Behauptung sei bereits für alle kleineren Gruppen gezeigt.
- *Induktionsschritt.* Wir zeigen, dass die Behauptung auch für G gilt: Wir betrachten die Klassengleichung: Sei $(g_i)_{i \in I}$ ein Repräsentantensystem der nicht-trivialen Konjugationsklassen von G. Dann ist (Korollar 1.2.20)

  $$\#G = \#Z(G) + \sum_{i \in I} \big[G : Z_G(g_i)\big].$$

  Wir unterscheiden die folgenden Fälle:

  ① Ist $i \in I$ und ist p *kein* Teiler von $[G : Z_G(g_i)]$, so ist jede p-Sylowgruppe von $Z_G(g_i)$ eine p-Sylowgruppe von G.

  Wegen $\#Z_G(g_i) < \#G$ besitzt $Z_G(g_i)$ nach Induktionsvoraussetzung eine p-Sylowgruppe.

② Sei p für jedes $i \in I$ ein Teiler von $[G : Z_G(g_i)]$. Da p auch ein Teiler von $\#G3$ ist, ist somit p ein Teiler von $\#Z(G)$. Da $Z(G)$ abelsch ist, besitzt $Z(G)$ eine (nicht-triviale) p-Sylowgruppe T (Beispiel 1.3.36). Da T im Zentrum von G liegt, ist T ein Normalteiler in G und $\#(G/T) < \#G$.

Nach Induktionsvoraussetzung besitzt somit G/T eine p-Sylowgruppe U. Sei $\pi\colon G \longrightarrow G/T$ die kanonische Projektion und

$$S := \pi^{-1}(U).$$

Dann ist $S/T \cong_{\mathsf{Group}} U$ (nach dem Homomorphiesatz, Korollar 1.1.51) und daher (Satz von Lagrange, Korollar 1.1.34)

$$\#S = \#T \cdot \#U.$$

Ein Vergleich mit den p-Potenzen in $\#G = \#T \cdot \#(G/T)$ liefert, dass $\#S$ eine p-Sylowgruppe von G ist.

Eine weitere Beweismöglichkeit besteht darin, Matrixgruppen geschickt einzsuetzen [22, Kapitel 10].

Ausblick 1.3.45 (Tori in Lie-Gruppen)**.** Die Sylowsätze sind strukturell ähnlich zu den klassischen Sätzen über maximale Tori in Lie-Gruppen: Jede kompakte zusammenhängende Lie-Gruppe enthält einen maximalen Torus (jedes Element ist sogar in einem solchen enthalten) und alle maximalen Tori sind konjugiert zueinander [8, Kapitel 16]. Tori sind dabei abelsche Lie-Gruppen und daher gut zu verstehen.

2

Ringe

Ringe sind algebraische Strukturen, die es erlauben die Interaktion zwischen Addition und Multiplikation und insbesondere Teilbarkeitseigenschaften zu modellieren und zu studieren. Ein zentraler Bestandteil der Ringtheorie ist die Primeigenschaft. Wir wiederholen die Grundbegriffe für Ringe und präsentieren grundlegende Konstruktionen von Ringen. Das Ziel dabei ist, die Ringtheorie soweit zu entwickeln, dass wir sie auf Probleme aus der elementaren Zahlentheorie und zur Untersuchung von Körpern bzw. Körpererweiterungen anwenden können.

Überblick über dieses Kapitel.

2.1 Die Kategorie der Ringe 82
2.2 Die Primeigenschaft 95

Schlüsselbeispiel. die ganzen Zahlen, Polynomringe, Körper, Restklassenringe

2.1 Die Kategorie der Ringe

Die Kategorie der Ringe besteht aus Ringen und Ringhomomorphismen. Wir wiederholen kurz die Grundbegriffe und untersuchen dann Konstruktionen von Ringen genauer.

2.1.1 Ringe und Ringhomomorphismen

Wir schränken uns im folgenden der Einfachheit halber immer auf kommutative Ringe mit Eins ein.

Definition 2.1.1 (Ring)**.** Ein *Ring* ist ein Quintupel $(R, +, \cdot, 0, 1)$ bestehend aus einer Menge R, Abbildungen $+, \cdot : R \times R \longrightarrow R$ (*Addition* bzw. *Multiplikation*) und Elementen $0, 1 \in R$ mit folgenden Eigenschaften:

- Das Tripel $(R, +, 0)$ bildet eine abelsche Gruppe.
- das Tripel $(R, \cdot, 1)$ ist ein kommutativer (!) Monoid.
- Es gilt das *Distributivgesetz*, d.h. für alle $x, y, z \in R$ gilt

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Wie im Falle anderer algebraischer Strukturen werden wir auch einfach „Sei R ein Ring." etc. schreiben, wenn die restliche Struktur/Notation aus dem Kontext klar ist.

Beispiel 2.1.2 (Ringe)**.**

- Etwas exotisch ist der *Nullring*; die unterliegende Menge ist $\{0\}$ und die Addition bzw. Multiplikation sind jeweils die einzig mögliche Abbildung $\{0\} \times \{0\} \longrightarrow \{0\}$. In diesem Ring ist 0 sowohl das neutrale Element bezüglich Addition als auch das neutrale Element bezüglich Multiplikation (also „$0 = 1$").
- Die ganzen Zahlen $\mathbb{Z}$ bilden bezüglich der gewöhnlichen Addition und Multiplikation sowie den gewöhnlichen Elementen $0, 1 \in \mathbb{Z}$ einen Ring.
- Die natürlichen Zahlen $\mathbb{N}$ bilden bezüglich der gewöhnlichen Addition und Multiplikation *keinen* Ring, da $\mathbb{N}$ bezüglich Addition *keine* Gruppe ist.
- Jeder Körper bildet einen Ring (z.B. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_2$).

- Ist K ein Körper, so ist der Polynomring $K[T]$ ein Ring; wir werden Polynomringe in Kapitel 2.1.2 genauer betrachten.
- Die Menge
$$\mathbb{Z}[i] := \{a + i \cdot b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$
bildet bezüglich der von $\mathbb{C}$ induzierten Addition und Multiplikation und den gewöhnlichen Elementen $0, 1 \in \mathbb{C}$ einen Ring (nachrechnen), die *Gaußschen ganzen Zahlen*.

  Dieser Ring kann zum Beispiel verwendet werden, um zu untersuchen, welche ganzen Zahlen als Summe zweier Quadratzahlen geschrieben werden können: Denn in $\mathbb{Z}[i]$ gilt für alle $a, b \in \mathbb{Z}$, dass
$$a^2 + b^2 = (a + i \cdot b) \cdot (a - i \cdot b).$$
- Die äußere Algebra $\bigwedge \mathbb{F}_2$ über $\mathbb{F}_2$ ist ein Ring (sogar kommutativ!). Ist K ein Körper und $n \geq \mathbb{N}_{\geq 2}$, so bildet $\mathrm{M}_{n\times n}(K)$ einen *nicht-kommutativen* Ring mit Eins.

Ringhomomorphismen sind strukturerhaltende Abbildungen von Ringen:

Definition 2.1.3 (Ringhomomorphismus)**.** Seien R, S Ringe. Ein *Ringhomomorphismus* $R \longrightarrow S$ ist eine Abbildung $f\colon R \longrightarrow S$ mit folgenden Eigenschaften:

- Die Abbildung f ist ein Gruppenhomomorphismus der unterliegenden additiven abelschen Gruppen, d.h. es gilt ? $f(0) = 0$ und
$$\forall_{x,y\in R} \quad f(x + y) = f(x) + f(y).$$
- Die Abbildung f ist ein Monoiodhomomorphismus der unterliegenden multiplikativen Monoide, d.h. es gilt ? $f(1) = 1$ und
$$\forall_{x,y\in R} \quad f(x \cdot y) = f(x) \cdot f(y).$$

Ein *Ringisomorphismus* $R \longrightarrow S$ ist ein Ringhomomorphismus $f\colon R \longrightarrow S$, für den es einen Ringhomomorphismus $g\colon S \longrightarrow R$ mit
$$f \circ g = \mathrm{id}_S \quad \text{und} \quad g \circ f = \mathrm{id}_R$$
gibt. In diesem Fall nennt man R und S *isomorph* und schreibt $R \cong_{\mathsf{Ring}} S$.

Beispiel 2.1.4 (Ringhomomorphismen)**.**

- Ist die Abbildung
$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z} \\ n &\longmapsto 2 \cdot n \end{aligned}$$

ein Ringhomomorphismus?

Ja Nein Die korrekte Antwort ist „Nein“. Denn die Eins wird nicht auf die Eins abgebildet. ×

- Ist K ein Körper und $x \in K$, so ist der *Einsetzungshomomorphismus*

$$\begin{aligned} K[T] &\longrightarrow K \\ f &\longmapsto f(x) \end{aligned}$$

ein Ringhomomorphismus. Allgemeiner ergibt sich dies aus der universellen Eigenschaft von Polynomringen (Bemerkung 2.1.16).

- Verknüpfungen von Ringhomomorphismen sind Ringhomomorphismen und die Identitätsabbildung auf einem Ring ist ein Ringhomomorphismus. Somit bilden Ringe und Ringhomomorphismen eine Kategorie Ring.

Allgemeine Ringe sind viel zu wild, um vernünftig damit arbeiten zu können. Wir werden uns daher im folgenden zumeist auf algebraisch gutartige Ringe einschränken.

Definition 2.1.5 (Integritätsring)**.** Sei R ein (kommutativer) Ring mit $1 \neq 0$. Man bezeichnet den Ring R als *Integritätsring*, wenn er *nullteilerfrei* ist, d.h., wenn

$$\forall_{x,y \in R} \quad x \cdot y = 0 \Longrightarrow (x = 0 \vee y = 0).$$

Beispiel 2.1.6 (Integritätsringe)**.**

- Der Ring $\mathbb{Z}$ ist ein Integritätsring. Alle Körper sind Integritätsringe (und damit auch alle Unterringe, wie zum Beispiel $\mathbb{Z}[i] \subset \mathbb{C}$).

- Ist K ein Körper, so ist der Polynomring $K[T]$ ein Integritätsring (wie man anhand der Gradfunktion ablesen kann; Proposition II.2.2.5, Proposition 2.1.14).

- Sind S und R Ringe, so ist $S \times R$ bezüglich komponentenweiser Addition und Multiplikation ein Ring mit neutralen Elementen $(0,0)$ bzw. $(1,1)$ (der *Produktring von S und R*). Sind S und R nicht-triviale Ringe (d.h. $0 \neq 1$), so ist $S \times R$ *kein* Integritätsring, denn es gilt z.B.

? $(1,0) \cdot (0,1) = (0,0)$

obwohl $(1,0) \neq (0,0)$ und $(0,1) \neq (0,0)$ (und $(0,0)$ ist das neutrale Element bezüglich Addition in $S \times R$).

Bemerkung 2.1.7 (endliche Integritätsringe)**.** Jeder endliche Integritätsring ist bereits ein Körper (Übungsaufgabe).

Caveat 2.1.8 (Kaplansky-Vermutung)**.** Im allgemeinen ist es nicht besonders leicht, festzustellen, ob ein Ring ein Integritätsring ist oder nicht. Im Fall von nicht-kommutativen Ringen besagt zum Beispiel die *Kaplansky-Vermutung*, dass Gruppenringe von torsionsfreien Gruppen (d.h. Gruppen ohne nicht-triviale Elemente endlicher Ordnung) nullteilerfrei sind. Für viele Gruppen ist diese Vermutung bestätigt (oft mit analytischen Tricks), aber im allgemeinen ist die Vermutung noch immer offen.

2.1.2 Polynomringe

Wir wiederholen die Konstruktion des Polynomrings und erweitern sie auf Polynomringe über allgemeinen (kommutativen) Ringen (statt nur von Körpern). Wir erinnern uns dabei insbesondere daran, dass Polynome durch ihre Koeffizienten beschrieben werden, und dass es einen Unterschied zwischen Polynomen und Polynomfunktionen gibt.

Definition 2.1.9 (Polynomring)**.** Sei R ein Ring. Der *Polynomring $R[T]$ über R in einer Variablen T* ist wie folgt definiert:

- Als additive Gruppe ist $R[T]$ die direkte Summe $\bigoplus_{\mathbb{N}} R$. In anderen Worten: als additive Gruppe ist $R[T]$ die Untergruppe

$$\left\{(a_n)_{n\in\mathbb{N}} \in \mathrm{Abb}(\mathbb{N}, R) \;\middle|\; \exists_{d\in\mathbb{N}} \quad \forall_{n\in\mathbb{N}_{>d}} \quad a_n = 0\right\}$$

  von $\mathrm{Abb}(\mathbb{N}, R)$.

- Wir schreiben $T := e_1 \in \bigoplus_{\mathbb{N}} R$.

- Wir definieren auf $R[T]$ die Multiplikation durch

$$\begin{aligned} \cdot : R[T] \times R[T] &\longrightarrow R[T] \\ \big((a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}\big) &\longmapsto \left(\sum_{j=0}^{n} a_j \cdot b_{n-j}\right)_{n\in\mathbb{N}} \end{aligned}$$

  Man beachte dabei, dass das Bild dieser Abbildung tatsächlich wieder in $R[T]$ liegt, und, dass $T^n = e_n$ für alle $n \in \mathbb{N}$ gilt.

- Ist $f = (a_n)_{n\in\mathbb{N}} \in R[T]$, so ist

$$\deg f := \sup\{n \in \mathbb{N} \mid a_n \neq 0\} \in \{-\infty\} \cup \mathbb{N}$$

  der *Grad von f*. Dabei verwenden wir die Konvention $\sup \emptyset := -\infty$; insbesondere ist das Nullpolynom das einzige Polynom in $R[T]$ mit Grad $-\infty$.

Die Elemente von $R[T]$ bezeichnet man als *Polynome in der Variablen T mit Koeffizienten in R.*

Notation 2.1.10 (Polynome)**.** Sei R ein Ring. Für alle $n \in \mathbb{N}$ gilt in $R[T]$, dass $T^n = e_n$ ist. Die Familie $(T^n)_{n\in\mathbb{N}}$ ist eine R-Basis von $R[T]$ (aufgefasst als R-Modul $\bigoplus_{\mathbb{N}} R$). Ist $f = (a_n)_{n\in\mathbb{N}} \in R[T]$ und $d := \deg p$, so schreibt man daher dafür normalerweise

$$f = \sum_{n=0}^{d} a_n \cdot T^n.$$

Die Definition der Multiplikation liefert $T^n \cdot T^m = T^{n+m}$ für alle $n, m \in \mathbb{N}$. Die allgemeine Multiplikation von Polynomen erfolgt durch R-bilineares Ausmultiplizieren dieser Gleichung auf den Potenzen der Variablen T. Nachrechnen zeigt, dass $R[T]$ tatsächlich bezüglich den obigen Verknüpfungen (und den neutralen Elementen $0 = 0 \cdot T^0$ und $1 = 1 \cdot T^0$) einen Ring bildet und dass

$$\begin{aligned} R &\longrightarrow R[T] \\ x &\longmapsto x \cdot T^0 \end{aligned}$$

ein injektiver Ringhomomorphismus ist.

Definition 2.1.11 (Polynomfunktion, Nullstelle)**.** Sei R ein Ring und $p = \sum_{j=0}^{d} a_j \cdot T^j \in R[T]$. Die *zugehörige Polynomfunktion* ist als

$$\begin{aligned} f_p \colon R &\longrightarrow R \\ x &\longmapsto \sum_{j=0}^{d} a_j \cdot x^j \end{aligned}$$

definiert. Ist $x \in R$, so schreiben wir $p(x) := f_p(x)$. Ist $x \in R$ mit $p(x) = 0$, so ist x eine *Nullstelle von p (in R).*

Caveat 2.1.12 (Polynom vs. Polynomfunktion)**.** Im allgemeinen gibt es einen Unterschied zwischen Polynomen und Polynomfunktionen. Zum Beispiel sind die Polynome $f := T$ und $g := T^2 \in \mathbb{F}_2[T]$ verschieden (da sie verschiedene Koeffizienten haben), aber die zugehörigen Polynomfunktionen sind gleich:

$$\forall_{x\in\mathbb{F}_2} \quad f(x) = x = x^2 = g(x).$$

Notation 2.1.13 (iterierte Polynomringe)**.** Sei R ein Ring. Dann schreiben wir auch kurz

$$R[X, Y] := \big(R[X]\big)[Y].$$

Die Elemente von $R[X, Y]$ können wir dabei auch in der Form

$$\sum_{n=0}^{d}\sum_{j=0}^{n} a_{n,j}\cdot X^j\cdot Y^{n-j}$$

mit $d\in\mathbb{N}$ und $a_{0,0},a_{1,0},\dots,a_{d,d}\in R$ notieren; zwei solche Polynome in X und Y stimmen genau dann überein, wenn sie dieselben Koeffizienten haben. Analog kann man auch Polynomringe in noch mehr Variablen betrachten.

Proposition 2.1.14 (Wann sind Polynomringe nullteilerfrei?)**.** *Sei R ein Ring. Dann ist der Polynomring $R[T]$ genau dann ein Integritätsring, wenn R ein Integritätsring ist.*

Beweis. Nach Konstruktion ist $R[T]$ genau dann der Nullring, wenn R der Nullring ist (nachrechnen). Sei daher ohne Einschränkung R nicht der Nullring. Es genügt zu zeigen, dass $R[T]$ genau dann nullteilerfrei ist, wenn R nullteilerfrei ist.

Ist $R[T]$ ein Integritätsring, so vererbt sich die Nullteilerfreiheit von $R[T]$ auch auf den Unterring R (der konstanten Polynome).

Sei umgekehrt R ein Integritätsring. Dann ist auch $R[T]$ ein Integritätsring, denn: Wie im Beweis von Proposition II.2.2.5 verwenden wir dazu die Gradfunktion. Für alle $f,g\in R[T]$ gilt

$$\deg(f\cdot g)=\deg f+\deg g,$$

denn: Sei $n:=\deg f$ und $m:=\deg g$; ohne Einschränkung sei $f\neq 0$ und $g\neq 0$. Also können wir $f=\sum_{j=0}^{n}a_j\cdot T^j$ bzw. $g=\sum_{j=0}^{m}b_j\cdot T^j$ mit $a_n\neq 0$ und $b_m\neq 0$ schreiben. Nach Definition der Multiplikation von Polynomen ist

$$\begin{aligned} f\cdot g &= \left(\sum_{j=0}^{n}a_j\cdot T^j\right)\cdot\left(\sum_{j=0}^{m}b_j\cdot T^j\right)=\sum_{j=0}^{m+n}\left(\sum_{k=\max(0,j-m)}^{\min(n,j)}a_k\cdot b_{j-k}\right)\cdot T^j\\ &= (a_n\cdot b_m)\cdot T^{n+m}+\sum_{j=0}^{m+n-1}\left(\sum_{k=\max(0,j-m)}^{\min(n,j)}a_k\cdot b_{j-k}\right)\cdot T^j. \end{aligned}$$

Da R nullteilerfrei ist, ist $a_n\cdot b_m\neq 0$. Also ist $\deg(f\cdot g)=n+m=\deg f+\deg g$.

Seien $f,g\in R[T]\setminus\{0\}$. Dann ist $\deg f\geq 0$ und $\deg g\geq 0$. Mit der obigen Überlegung folgt somit $\deg(f\cdot g)=\deg f+\deg g\geq 0$, und daher insbesondere auch $f\cdot g\neq 0$. □

Beispiel 2.1.15 (Polynomringe)**.**

- Ist $\mathbb{Z}[X,Y]$ ein Integritätsring?

  Ja Nein Die korrekte Antwort ist „Ja“. Wir können Proposition 2.1.14 zweimal anwenden, um $\mathbb{Z}[X,Y]=\big(\mathbb{Z}[X]\big)[Y]$ als Integritätsring zu erkennen. ×

- Ist $(\mathbb{Z} \times \mathbb{Z})[X]$ ein Integritätsring?

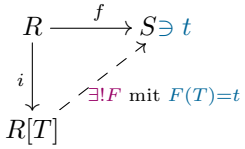
  Ja Nein Die korrekte Antwort ist „Nein“. Denn $\mathbb{Z} \times \mathbb{Z}$ ist *kein* Integritätsring. ×

Bemerkung 2.1.16 (universelle Eigenschaft des Polynomrings)**.** Sei R ein Ring. Dann besitzt der Polynomring $R[T]$ zusammen mit der kanonischen Inklusion $i\colon R \longrightarrow R[T]$ die folgende universelle Eigenschaft (nachrechnen): Zu jedem Ring S, zu jedem Ringhomomorphismus $f\colon R \longrightarrow S$ und zu jedem $t \in S$ gibt es genau einen Ringhomomorphismus $F\colon R[T] \longrightarrow S$ mit

$$F \circ i = f \quad \text{und} \quad F(T) = t,$$

nämlich

$$\begin{aligned} F\colon R[T] &\longrightarrow S \\ \sum_{j=0}^{d} a_j \cdot T^j &\longmapsto \sum_{j=0}^{d} f(a_j) \cdot t^j. \end{aligned}$$



2.1.3 Quotientenkörper

Zwei wichtige Methoden, um aus Ringen weitere Ringe (und in guten Fällen sogar Körper) zu konstruieren, sind

- Lokalisierung und
- das Ausdividieren von Idealen.

Wir beginnen mit einem Spezialfall der Lokalisierungskonstruktion, nämlich der Konstruktion von Quotientenkörpern (allgemeine Lokalisierungen untersuchen wir in der *Kommutativen Algebra*). Ideale und die zugehörigen Restklassenringe betrachten wir in Kapitel 2.1.4.

Die Quotientenkörperkonstruktion ist eine Verallgemeinerung der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ mithilfe von Brüchen: Brüche der Form $\frac{x}{y}$ modellieren wir durch Paare (x, y) mit $y \neq 0$. Sind $x, x' \in \mathbb{Z}$ und $y, y' \in \mathbb{Z} \setminus \{0\}$, so gilt in den rationalen Zahlen, dass

$$\frac{x}{y} = \frac{x'}{y'} \Longleftrightarrow x \cdot y' = x' \cdot y.$$

Die Gleichung auf der rechten Seite lässt sich bereits in $\mathbb{Z}$ formulieren und ist daher ein geeigneter Ausgangspunkt für die Konstruktion von Brüchen über allgemeineren Ringen:

Proposition 2.1.17 (Quotientenkörper). *Sei R ein Integritätsring.*

1. *Dann ist*

$$\sim := \big\{ \big((x,y),(x',y')\big) \mid x,x' \in R,\ y,y' \in R \setminus \{0\},\ x \cdot y' = x' \cdot y \big\}$$

eine Äquivalenzrelation auf $R \times (R \setminus \{0\})$.

2. *Sei*

$$Q(R) := \big(R \times (R \setminus \{0\})\big/ \sim$$

Dann sind

$$\begin{aligned} +\colon Q(R) \times Q(R) &\longrightarrow Q(R) \\ \big([(x,y)],[(x',y')]\big) &\longmapsto \big[(x \cdot y' + x' \cdot y, y \cdot y')\big] \quad \textit{(Addition von Brüchen!)} \\ \cdot\colon Q(R) \times Q(R) &\longrightarrow Q(R) \\ \big([(x,y)],[(x',y')]\big) &\longmapsto \big[(x \cdot x', y \cdot y')\big] \end{aligned}$$

wohldefinierte Abbildungen und $Q(R)$ bildet bezüglich dieser Addition und Multiplikation und $[(0,1)]$ bzw. $[(1,1)]$ einen Körper.

3. *Die Abbildung*

$$\begin{aligned} R &\longrightarrow Q(R) \\ x &\longmapsto \big[(x,1)\big] \end{aligned}$$

ist ein injektiver Ringhomomorphismus.

Beweis. Alle Aussagen folgen durch direktes Nachrechnen (nachrechnen; an welchen Stellen geht essentiell ein, dass R nullteilerfrei ist?!). □

Notation 2.1.18 (Brüche). Sei R ein Integritätsring und seien $x, y \in R$ mit $y \neq 0$. In $Q(R)$ gilt (nachrechnen)

$$\big[(x,y)\big] = \big[(x,1)\big] \cdot \big[(1,y)\big] = \big[(x,1)\big] \cdot \big[(y,1)\big]^{-1}.$$

Man schreibt daher auch

$$\frac{x}{y} := \big[(x,y)\big]$$

und stellt fest, dass sich Addition und Multiplikation in $Q(R)$ wie die gewohnte Bruchrechnung verhalten (nachrechnen).

Beispiel 2.1.19 (Quotientenkörper).

- Nach Konstruktion der rationalen Zahlen ist $\mathbb{Q} = Q(\mathbb{Z})$.

- Ist K ein Körper, so liefert $x \mapsto [(x,1)]$ einen Ring- bzw. Körperisomorphismus $K \longrightarrow Q(K)$. Die Surjektivität folgt aus folgender Überlegung: Ist $x \in K$ und $y \in K \setminus \{0\}$, so gilt

$$(x,y) \sim (\text{?} \quad x \cdot y^{-1}, 1)$$

  (für die Relation $\sim$ aus Proposition 2.1.17).

- Ist K ein Körper, so ist $K[T]$ ein Integritätsring. Den zugehörigen Quotientenkörper

$$K(T) := Q\big(K[T]\big)$$

  bezeichnet man als *(rationalen) Funktionenkörper über K*. Elemente in $K(T)$ schreibt man als Brüche der Form f/g mit $f, g \in K[T]$ und $g \neq 0$. Durch Einsetzen liefern Elemente von $K[T]$ rationale Funktionen auf K (wobei bei den Nennernullstellen bzw. dem genauen Definitionsbereich etwas Vorsicht nötig ist!).

  Zum Beispiel erhält man aus Elementen aus $\mathbb{C}(T)$ meromorphe Funktionen $\widehat{\mathbb{C}} \longrightarrow \widehat{\mathbb{C}}$ auf der riemannschen Zahlenkugel.

- Insbesondere erhalten wir so einen unendlichen Körper K, der $x+x=0$ für alle $x \in K$ erfüllt, nämlich zum Beispiel $K = \mathbb{F}_2(T)$.

Bemerkung 2.1.20 (universelle Eigenschaft des Quotientenkörpers)**.** Sei R ein Integritätsring. Dann hat der Quotientenkörper $Q(R)$ zusammen mit der kanonischen Abbildung

$$\begin{aligned} i\colon R &\longrightarrow Q(R) \\ x &\longmapsto \big[(x,1)\big] \end{aligned}$$

die folgende universelle Eigenschaft (nachrechnen): Ist K ein Körper und ist $f\colon R \longrightarrow K$ ein injektiver Ringhomomorphismus, so gibt es genau einen Ringhomomorphismus $Q(f)\colon Q(R) \longrightarrow K$ mit

$$f = Q(f) \circ i$$

$$\begin{array}{ccc} R & \xrightarrow{f \text{ (inj.)}} & K \\ {\scriptstyle i}\downarrow & \nearrow_{\exists! Q(f)} & \\ Q(R) & & \end{array}$$

Der Quotientenkörper $Q(R)$ ist also der „kleinste“ Körper, der R enthält.

2.1.4 Ideale und Restklassenringe

Wie im Fall von Vektorräumen, Moduln und Gruppen gibt es auch in der Kategorie der Ringe die Möglichkeit, Ringe durch Quotientenbildung nach geeigneten Unterstrukturen zu konstruieren.

Definition 2.1.21 (Ideal)**.** Sei R ein Ring. Ein *(linksseitiges) Ideal* in R ist ein R-Untermodul des R-Moduls R. Expliziter: Eine Teilmenge $a \subset R$ ist ein Ideal in R, wenn folgende Bedingungen erfüllt sind:

- Die Teilmenge a von R bildet eine Untergruppe bezüglich Addition.
- Für alle $x \in a$ und alle $r \in R$ gilt $r \cdot x \in a$.

Bemerkung 2.1.22. In der Literatur werden Ideale oft durch Frakturbuchstaben oder sonstigen unnötig komplizierten Symbolen bezeichnet. Wir werden im folgenden Ideale meist durch gewöhnliche Kleinbuchstaben notieren.

Bemerkung 2.1.23 (erzeugte Ideale)**.** Sei R ein Ring und sei $A \subset R$. Dann schreiben wir (A) für das von A *erzeugte Ideal*, d.h. für das bezüglich Inklusion kleinste Ideal von R, das A enthält. Eine einfache Rechnung zeigt, dass

$$(A) = \left\{ \sum_{j=1}^{n} a_j \cdot r_j \;\middle|\; n \in \mathbb{N},\ r_1, \dots, r_n \in R,\ a_1, \dots, a_n \in A \right\}.$$

Sind $a_1, \dots, a_n \in R$, so schreibt man auch $(a_1, \dots, a_n)$ statt $(\{a_1, \dots, a_n\})$.

Beispiel 2.1.24 (Ideale)**.**

- Ist R ein Ring, so gilt $(0) =$? $\{0\}$ und $(1) =$? R.
- Ist $n \in \mathbb{Z}$, so ist $(n) = n \cdot \mathbb{Z}$ ein Ideal in $\mathbb{Z}$. In $\mathbb{Z}$ gilt
$$(2) \neq \mathbb{Z} = (2, 3).$$
- Ist $f \colon R \longrightarrow S$ ein Ringhomomorphismus, so ist der *Kern*
$$\ker f := \big\{ x \in R \;\big|\; f(x) = 0 \big\} = f^{-1}(\{0\}) \subset R$$
von f ein Ideal in R (nachrechnen!). Das Bild $\operatorname{im} f := f(R)$ ist im allgemeinen *kein* Ideal in S.

Proposition 2.1.25 (Charakterisierung von Körpern über Ideale)**.** *Sei R ein Ring mit $R \ncong_{\mathsf{Ring}} \{0\}$. Dann ist R genau dann ein Körper, wenn R nur die beiden Ideale $\{0\}$ und R besitzt.*

Beweis. Dies folgt, indem man sich überlegt, was mit Idealen zu nicht-invertierbaren Elementen passiert (Übungsaufgabe). □

Proposition 2.1.26 (Restklassenring). *Sei R ein Ring und sei $a \subset R$ ein Ideal. Dann ist $R/a = \{x + a \mid x \in R\}$ eine abelsche Gruppe (bezüglich der von der Addition auf R induzierten Addition auf R/a). Außerdem gilt:*

1. *Es ist*

$$\begin{aligned} \cdot : R/a \times R/a &\longrightarrow R/a \\ (x + a, y + a) &\longmapsto (x \cdot y) + a \end{aligned}$$

   eine wohldefinierte Abbildung.

2. *Die Menge R/a bildet bezüglich der obigen Addition bzw. Multiplikation und den neutralen Elementen $0 + a$ bzw. $1 + a$ einen Ring, den* Restklassenring von R modulo a.

Beweis. Als Ideal ist a insbesondere eine additive Untergruppe von R (und damit auch ein additiver Normalteiler) und wir können daher tatsächlich von der Quotientengruppe R/a bezüglich Addition sprechen.

Zu 1. Seien $x, y, x', y' \in R$ mit $x + a = x' + a$ und $y + a = y' + a$. Dann gilt auch $(x \cdot y) + a = (x' \cdot y') + a$, denn: Dafür genügt es nachzuweisen, dass $x \cdot y - x' \cdot y'$ in a liegt. Es gilt

$$\begin{aligned} x \cdot y - x' \cdot y' &= x \cdot y - x \cdot y' + x \cdot y' - x' \cdot y' \\ &= x \cdot (y - y') - (x' - x) \cdot y'. \end{aligned}$$

Wegen $y + a = y' + a$ ist $y - y' \in a$; die Idealeigenschaft liefert daher auch $x \cdot (y - y') \in a$. Analog folgt (da R kommutativ ist!) auch $(x' - x) \cdot y' \in a$. Also ist nach der obigen Rechnung $x \cdot y - x' \cdot y' \in a$, wie behauptet.

Zu 2. Die Ringeigenschaften vererben sich von R auf R/a, da Addiition und Multiplikation auf R/a repräsentantenweise definiert sind (nachrechnen). □

Notation 2.1.27 (Restklassen). Sei R ein Ring und $a \subset R$ ein Ideal. Ist $x \in R$, so schreiben wir für das Element $x + a \in R/a$ oft auch kurz $[x]_a$ bzw. $[x]$, wenn aus dem Kontext klar ist, um welches Ideal es sich handelt.

Bemerkung 2.1.28 (Quotientenring). Wir verwenden den Begriff Restklassenring statt Quotientenring (was vielleicht naheliegender wäre), um Verwechslungen mit der Quotientenkörperkonstruktion zu vermeiden.

Beispiel 2.1.29 (Restklassenringe).

- Ist $n \in \mathbb{Z}$, so bildet $\mathbb{Z}/(n)$ bezüglich repräsentantenweiser Addition und Multiplikation einen Ring. Die unterliegende additive Gruppe ist die zyklische Gruppe $\mathbb{Z}/n$; insbesondere enthält $\mathbb{Z}/(n)$ für $n \in \mathbb{N}_{>0}$ genau n Elemente: $[0], [1], \ldots [n-1]$.

  Zum Beispiel gilt in $\mathbb{Z}/(12)$, dass

$$[3] \cdot [4] = \text{?} \quad [12] = [0],$$

obwohl $[3], [4] \in \mathbb{Z}/(12) \setminus \{[0]\}$. Also ist $\mathbb{Z}/(12)$ *kein* Integritätsring.

Außerdem gilt in $\mathbb{Z}/(12)$, dass

$$[5]^2 = \text{?} \quad [5] \cdot [5] = [25] = [1 + 2 \cdot 12] = [1];$$

also besitzt $[5]$ ein multiplikatives Inverses in $\mathbb{Z}/(12)$.

Der Ring $\mathbb{Z}/(2)$ ist isomorph zum Körper $\mathbb{F}_2$. Bzw. umgekehrt könnte man auch $\mathbb{F}_2$ als diesen Ring definieren.

An dieser Stelle kommt vielleicht bereits der Verdacht auf, dass $\mathbb{Z}/(n)$ genau dann ein Körper ist, wenn n ? eine Primzahl in $\mathbb{Z}$ ist. Dies werden wir in Kapitel 2.2.3 genauer untersuchen.

- Ist R ein Ring, so sind die Ringe $R[T]/(T)$ und R (kanonisch) isomorph (nachrechnen). Insbesondere gilt auch $R[X, Y]/(Y) \cong_{\mathsf{Ring}} R[X]$.

Beispiel 2.1.30 (int)**.** Die Arithmetik auf Datentypen für natürliche/ganze Zahlen mit fester Länge in Programmiersprachen ist oft als Arithmetik in dem entsprechenden Restklassenring spezifiziert; zum Beispiel erhält man somit in *unsigned 64 bit integers* in C, dass $2^{63} + 2^{63}$ das Ergebnis 0 liefert. Dieses Verhalten kann natürlich äußerst unangenehme Nebeneffekte haben!

Moderne Hardware unterstützt daher effiziente Mechanismen, um solche arithmetischen Overflows abzufangen und (je nach Sprachspezifikation) bei der Ausführung des Programms eine Gelegenheit zur Fehlerbehandlung zu liefern (z.B. durch runtime exceptions).

Beispiel 2.1.31 (elementare Zahlentheorie)**.** Die Arithmetik in den Restklassenringen der Form $\mathbb{Z}/(n)$ kann manchmal verwendet werden, um zu zeigen, dass gewisse Gleichungen *keine* ganzzahligen Lösungen besitzen. Wir betrachten ein sehr einfaches Beispiel dieser Form: Es gibt *keine* Zahlen $x, y \in \mathbb{Z}$ mit

$$x^2 + x + y^2 + y = 2025,$$

denn: *Angenommen,* es gäbe $x, y \in \mathbb{Z}$ mit $x^2 + x + y^2 + y = 2025$. Wir betrachten die kanonische Projektion $\pi \colon \mathbb{Z} \longrightarrow \mathbb{Z}/(2)$. Da π ein Ringhomomorphismus ist, folgt

$$\pi(x)^2 + \pi(x) + \pi(y)^2 + \pi(y) = \pi(x^2 + x + y^2 + y) = \pi(2025) = [1].$$

Wegen (nachrechnen)

$$\forall_{z \in \mathbb{Z}/(2)} \quad z^2 + z = [0]$$

ergibt die linke Seite aber $[0] \in \mathbb{Z}/(2)$. Dies liefert den Widerspruch $[0] \neq [1]$ in $\mathbb{Z}/(2)$. Also ist die obige Gleichung in $\mathbb{Z}$ *nicht* lösbar.

Die Kunst bei diesem Verfahren besteht darin, einen geeigneten Restklassenring zu finden (falls ein solcher überhaupt existiert …) und geeignete Gleichungen bzw. Invarianten in solchen Restklassenringen zu kennen.

Anmerkung für Lehramtsstudenten (Wettbewerbsaufgaben)**.** Die (Un)Lösbarkeit von bestimmten Gleichungen in $\mathbb{Z}$ ist ein beliebter Gegenstand für Wettbewerbsaufgaben (z.B. Landes-/Bundeswettbewerb, Mathematik-Olympiaden, etc.). In vielen Fällen hilft dabei die Betrachtung der entsprechenden Gleichungen in geeigneten Restklassenringen. Bei Quadraten und vierten Potenzen bieten sich $\mathbb{Z}/(4)$ und $\mathbb{Z}/(8)$ an; bei dritten Potenzen $\mathbb{Z}/(7)$ oder $\mathbb{Z}/(9)$. Auch die Koeffizienten der Gleichung spielen natürlich bei der Auswahl der Restklassenringe eine Rolle.

Bemerkung 2.1.32 (universelle Eigenschaft von Restklassenringen)**.** Sei R ein Ring und sei $a \subset R$ ein Ideal. Dann ist die kanonische Projektion

$$\begin{aligned} \pi\colon R &\longrightarrow R/a \\ x &\longmapsto x + a \end{aligned}$$

ein surjektiver Ringhomomorphismus (da die Verknüpfungen auf R/a repräsentantenweise definiert sind) mit $\ker \pi = a$.

Der Restklassenring R/a erfüllt zusammen mit π die folgende *universelle Eigenschaft* (nachrechnen!): Für jeden Ring S und für jeden Ringhomomorphismus $f\colon R \longrightarrow S$ mit $a \subset \ker f$ gibt es genau einen Ringhomomorphismus $\overline{f}\colon R/a \longrightarrow S$ mit

$$\overline{f} \circ \pi = f$$

(nämlich $[x] \longmapsto f(x)$).

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\overline{f}} & \\ R/a & & \end{array}$$

Insbesondere zeigt dies wie im Fall von Gruppen (Bemerkung 1.1.49), dass eine Teilmenge von R genau dann ein Ideal in R ist, wenn sie Kern eines auf R definierten Ringhomomorphismus ist.

Bemerkung 2.1.33 (Homomorphie-/Isomorphiesätze für Ringe)**.** Aus der universellen Eigenschaft von Restklassenringen (Bemerkung 2.1.32) lassen sich analog zum Gruppenfall (Korollar 1.1.51, Satz 1.1.62) auch

- der Homomorphiesatz für Ringhomomorphismen und
- Isomorphiesätze für Restklassenringe

ableiten.

Beispiel 2.1.34 (algebraische Geometrie)**.** In der *Algebraischen Geometrie* untersucht man polynomiale Gleichungen und ihre Lösungsmengen mit geometrischen und algebraischen Methoden. Ist K ein Körper, so studiert man zum Beispiel die Lösungsmenge (Abbildung 2.1)

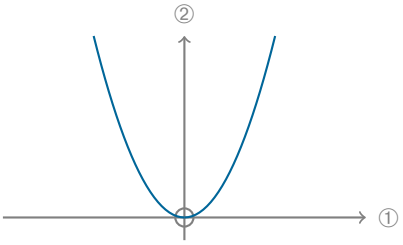


Abbildung 2.1.: Die Menge $\{(x, y) \in K^2 \mid y = x^2\}$, schematisch

$$P := \left\{(x, y) \in K^2 \;\middle|\; y = x^2\right\} \subset K^2,$$

indem man den zugehörigen Restklassenring $K[X, Y]/(Y - X^2)$ untersucht.

Mit der universellen Eigenschaft von Polynom- und Restklassenringen folgt, dass

$$\begin{aligned} K[X, Y]/(Y - X^2) &\longrightarrow K[X] \\ [x \in K] &\longmapsto x \\ [X] &\longmapsto X \\ [Y] &\longmapsto X^2 \end{aligned}$$

und

$$\begin{aligned} K[X] &\longrightarrow K[X, Y]/(Y - X^2) \\ K \ni x &\longmapsto [x] \\ X &\longmapsto [X] \end{aligned}$$

wohldefinierte zueinander inverse Ringisomorphismen sind (nachrechnen; am besten mit universellen Eigenschaften!). Diese Tatsache stimmt mit der Anschauung überein, dass die „Parabel P“ aus einer „glatten, unverzweigten, sich nicht schließenden Linie“ besteht und dass der Ring $K[X]$ zur Geraden $K = \{x \in K \mid\}$ korrespondiert.

2.2 Die Primeigenschaft

Eine wichtige Anwendung der Ringtheorie ist die Untersuchung von Teilbarkeitsbeziehungen. In den ganzen Zahlen spielen bei Teilbarkeitsfragen die Primzahlen eine ausgezeichnete Rolle. Man betrachtet daher auch in allgemeineren Ringen Primeigenschaften von Elementen und von Idealen.

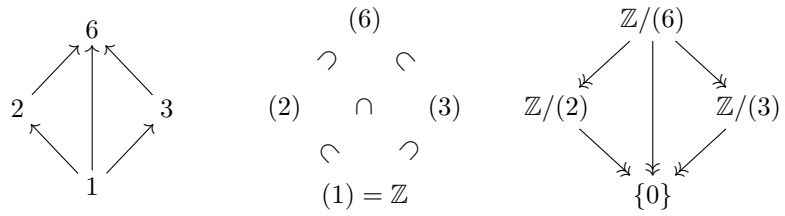


Abbildung 2.2.: Teilbarkeit, Idealinklusionen, kanonische Projektionen zwischen den zugehörigen Restklassenringen; links bedeuten dabei die Pfeile „ist ein Teiler von“.

2.2.1 Teilbarkeit

Wir erinnern zunächst an die grundlegenden Teilbarkeitsbegriffe.

Definition 2.2.1 (Einheit, assoziiert, teilt)**.** Einheit Sei R ein Integritätsring.

- Ein Element $x \in R$ ist eine *Einheit*, wenn es ein $y \in R$ mit $x \cdot y = 1$ gibt. Wir schreiben $R^\times$ für die Gruppe (bezüglich Multiplikation!) der Einheiten von R.
- Elemente $x, y \in R$ heißen *assoziiert*, wenn es eine Einheit $s \in R^\times$ mit $x = s \cdot y$ gibt.
- Ein Element $y \in R$ *teilt* ein Element x, wenn es ein $s \in R$ mit $x = s \cdot y$ gibt. In diesem Fall schreibt man auch kurz $y \mid x$ („y teilt x“).

Bemerkung 2.2.2 (Teilbarkeit und Ideale)**.** Sei R ein Integritätsring und seien $x, y \in R$. Teilbarkeit und Assoziiertheit lassen sich dann wie folgt durch die zugehörigen Ideale (x) und (y) ausdrücken (nachrechnen):

1. Es gilt genau dann $y \mid x$, wenn $(x) \subset (y)$ ist.
2. Es gilt genau dann $(x) = (y)$, wenn x und y assoziiert sind.

Beispiel 2.2.3. Wir betrachten die Elemente $1, 2, 3, 6$ in $\mathbb{Z}$. Dann gilt

$$1 \mid 2, \quad 1 \mid 3, \quad 1 \mid 6, \quad 2 \mid 6, \quad 3 \mid 6$$

und es bestehen keine weiteren Teilbarkeiten. Dies liefert entsprechende Inklusionsbeziehungen zwischen den zugehörigen Hauptidealen und kanonischen Projektionen zwischen den zugehörigen Restklassenringen (Abbildung 2.2) .

Bemerkung 2.2.4 (Hauptidealringe)**.** Ein Ideal, das von einem Element erzeugt wird, wird als *Hauptideal* bezeichnet. Ein *Hauptidealring* ist ein Integritätsring, in dem alle Ideale Hauptideale sind.

- Körper sind Hauptidealringe (die einzigen Ideale sind ? (0) und (1)).
- Der Ring $\mathbb{Z}$ und Polynomringe über Körpern sind Hauptidealringe (Kapitel II.2.4.2, da es sich dabei um sogenannte euklidische Ringe handelt). Euklidische Ringe werden in Anhang A.6 wiederholt.
- Der Ring $\mathbb{Q}[X, Y]$ ist *kein* Hauptidealring, denn das Ideal (X, Y) ist *kein* Hauptideal (nachrechnen).

  Der Ring $\mathbb{Z}[T]$ ist *kein* Hauptidealring, denn das Ideal $(2, T)$ ist *kein* Hauptideal (nachrechnen).
- Hauptidealringe sind im allgemeinen *nicht* euklidisch (Caveat A.6.7).

Will man mehrere Hauptideale zu neuen Idealen kombinieren, so kommen der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache ins Spiel:

Definition 2.2.5 (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)**.** Sei R ein Integritätsring und sei $S \subset R$.

- Ein *größter gemeinsamer Teiler von* S ist ein Element $d \in R$ mit folgender Eigenschaft: Es gilt $d \mid s$ für alle $s \in S$ und für alle $x \in R$ gilt
$$\big(\forall_{s\in S} \quad x \mid s\big) \Longrightarrow x \mid d.$$
- Ein *kleinstes gemeinsames Vielfaches von* S ist ein Element $m \in R$ mit folgender Eigenschaft: Es gilt $s \mid m$ für alle $s \in S$ und für alle $x \in R$ gilt
$$\big(\forall_{s\in S} \quad s \mid x\big) \Longrightarrow m \mid x.$$

Proposition 2.2.6 (grundlegende Eigenschaften des ggT)**.** *Sei R ein Integritätsring und seien $x, y \in R$.*

1. *Falls es in R einen größten gemeinsamen Teiler von x und y gibt, so ist dieser bis auf Assoziiertheit eindeutig bestimmt; wir schreiben dann $\operatorname{ggT}(x, y)$ für einen/den größten gemeinsamen Teiler von x und y.*
2. *Gibt es ein $d \in R$ mit $(d) = (x, y)$, so ist d ein größter gemeinsamer Teiler von x und y.*
3. *Ist R ein Hauptidealring, so gibt es einen größten gemeinsamen Teiler von x und y und für jeden größten gemeinsamen Teiler d von x und y gilt $(d) = (x, y)$. Insbesondere gibt es $r, s \in R$ mit*
$$d = r \cdot x + s \cdot y.$$

Beweis. Zu 1. Dies folgt aus der Definition größter gemeinsamer Teiler, da sich je zwei gößte gemeinsame Teiler von x und y gegenseitig teilen.

Zu 2. Sei $d \in R$ mit $(d) = (x, y)$. Dann ist insbesondere $(x) \subset (d)$ und $(y) \subset (d)$ bzw. $d \mid x$ und $d \mid y$ (Bemerkung 2.2.2). Wegen $d \in (x, y)$ gibt es $r, s \in R$ mit $d = r \cdot x + s \cdot y$; daraus folgt, dass jedes Element, das x und y teilt, auch ein Teiler von d ist. Also ist d ein größter gemeinsamer Teiler von x und y.

Zu 3. Da R ein Hauptidealring ist, gibt es ein $c \in R$ mit $(c) = (x, y)$. Nach dem zweiten Teil handelt es sich dabei um einen/den größten gemeinsamen Teiler von x und y.

Ist $d \in R$ ein größter gemeinsamer Teiler von x und y, so ist d nach dem ersten Teil zu c assoziiert. Somit folgt $(d) = (c) = (x, y) = \mathrm{Span}_R\{x, y\}$. Insbesondere gibt es $r, s \in R$ mit $d = r \cdot x + s \cdot y$. □

Proposition 2.2.7 (grundlegende Eigenschaften des kgV)**.** *Sei R ein Integritätsring und seien $x, y \in R$.*

1. *Falls es in R ein kleinstes gemeinsames Vielfaches von x und y gibt, so ist dieses bis auf Assoziiertheit eindeutig bestimmt; wir schreiben dann* $\mathrm{kgV}(x, y)$ *für ein/das kleinste gemeinsame Vielfache von x und y.*
2. *Gibt es ein $m \in R$ mit $(m) = (x) \cap (y)$, so ist m ein kleinstes gemeinsames Vielfaches von x und y.*
3. *Ist R ein Hauptidealring, so gibt es ein kleinstes gemeinsames Vielfaches m von x und y und es gilt $(m) = (x) \cap (y)$.*

Beweis. Die ersten beiden Aussagen folgen ähnlich wie im Beweis von Proposition 2.2.6. Die dritte Aussage folgt aus der zweiten Aussage. □

In euklidischen Ringen kann der größte gemeinsame Teiler mit dem euklidischen Algorithmus (durch iterierte Division mit Rest) bestimmt werden (Algorithmus A.6.8).

2.2.2 Primzahlen

Mithilfe von Teilbarkeit können wir die Primeigenschaft für Elemente in Ringen formulieren.

Definition 2.2.8 (irreduzibel, prim)**.** Sei R ein Integritätsring.

- Ein Element $p \in R \setminus \{0\}$ ist *irreduzibel*, wenn p keine Einheit ist und folgendes gilt: Für alle $x, y \in R$ mit $p = x \cdot y$ ist $x \in R^\times$ oder $y \in R^\times$.
- Ein Element $p \in R \setminus \{0\}$ ist *prim*, wenn p keine Einheit ist und folgendes gilt:
$$\forall_{x,y \in R} \quad p \mid x \cdot y \Longrightarrow (p \mid x \vee p \mid y).$$

Beispiel 2.2.9 ((ir)reduzible/prime Elemente)**.**

- Die Zahl 2025 ist in $\mathbb{Z}$ *nicht* prim, denn es gilt

$$2025 \mid 5 \cdot 405,$$

  aber $2025 \nmid 5$ und $2025 \nmid 405$.

- Die Zahlen 2027 und 2029 sind in $\mathbb{Z}$ irreduzibel (nachrechnen ...).

- Das Element $2 \in \mathbb{Z}[i] = \{x + i \cdot y \mid x, y \in \mathbb{Z}\} \subset \mathbb{C}$ ist *nicht* irreduzibel (obwohl 2 in $\mathbb{Z}$ irreduzibel ist), denn

$$2 = (1 + i) \cdot (1 - i)$$

  und $1 + i$, $1 - i$ sind *keine* Einheiten in $\mathbb{Z}[i]$ (Übungsaufgabe).

- Das Element $2 \in \mathbb{Z}[i\sqrt{5}] = \{x + i\sqrt{5} \cdot y \mid x, y \in \mathbb{Z}\} \subset \mathbb{C}$ ist irreduzibel (nachrechnen mithilfe von $|\cdot|^2$), aber *nicht* prim, denn in $\mathbb{Z}[i\sqrt{5}]$ gilt

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

  aber $2 \nmid 1 + i \cdot \sqrt{5}$ und $2 \nmid 1 - i\sqrt{5}$ (nachrechnen mithilfe von Division in $\mathbb{C}$). Im allgemeinen sind irreduzible Elemente also *nicht* prim!

Bemerkung 2.2.10 (Primelemente sind irreduzibel)**.** Sei R ein Integritätsring und sei $p \in R \setminus \{0\}$ keine Einheit. Ist p prim, so ist p auch irreduzibel, denn: Seien $x, y \in R$ mit $p = x \cdot y$. Dann ist p insbesondere ein Teiler von $x \cdot y$. Da p prim ist, ist somit p ein Teiler von x oder von y. Ohne Einschränkung gelte $p \mid x$. Also gibt es ein $s \in R$ mit $x = s \cdot p$. Insgesamt erhalten wir daraus

$$p = x \cdot y = s \cdot p \cdot y = s \cdot y \cdot p,$$

und damit (da R nullteilerfrei ist) $1 = s \cdot y$. Insbesondere ist y eine Einheit.

In Hauptidealringen sind irreduzible Elemente bereits prim:

Proposition 2.2.11 (Primelemente in Hauptidealringen)**.** *Sei R ein Hauptidealring und sei $p \in R \setminus \{0\}$ keine Einheit. Dann ist p genau dann prim, wenn p irreduzibel ist.*

Beweis. Der Vollständigkeit halber wiederholen wir das Argument aus der Linearen Algebra (Proposition II.2.4.18):

Wir wissen bereits, dass Primelemente irreduzibel sind (Bemerkung 2.2.10). Sei umgekehrt p irreduzibel. Dann ist p prim, denn: Seien $x, y \in R$ mit $p \mid x \cdot y$. Um die Voraussetzung, dass R ein Hauptidealring ist, nutzen zu können, liegt es nahe, ein geeignetes Ideal zu untersuchen. Wir betrachten das Ideal

$$a := (p, x) = \mathrm{Span}_R\{a, x\} \subset R.$$

Da R ein Hauptidealring ist, ist a ein Hauptideal; also gibt es ein $z \in R$ mit $a = (z)$. Wegen $p \in a$ und $x \in a$ folgt somit

$$z \mid p \quad \text{und} \quad z \mid x.$$

Insbesondere gibt es ein $s \in R$ mit $p = s \cdot z$. Da p irreduzibel ist, ist s oder z eine Einheit. Wir betrachten nun diese beiden Fälle:

① Es sei s eine Einheit. Dann ist $z = s^{-1} \cdot p$. Wegen $z \mid x$ erhalten wir somit auch $p \mid x$.

② Es sei z eine Einheit. Dann ist

$$R = R \cdot z = (z) = a = \mathrm{Span}_R\{p, x\}.$$

Insbesondere gibt es also $r, t \in R$ mit

$$1 = r \cdot p + t \cdot x.$$

Multiplikation mit y liefert

$$y = r \cdot p \cdot y + t \cdot x \cdot y.$$

Da p beide Summanden auf der rechten Seite teilt, ist somit p ein Teiler von y.

Insgesamt erhalten wir $p \mid x$ oder $p \mid y$. Es handelt sich bei p also um ein Primelement. □

Beispiel 2.2.12 (Primelemente)**.**

- Insbesondere sind ganze Zahlen genau dann prim, wenn man es (nach dem Schulwissen) erwarten würde. Zum Beispiel: Die Zahl 2027 ist in $\mathbb{Z}$ irreduzibel (nachrechnen). Da $\mathbb{Z}$ ein Hauptidealring ist, ist 2027 somit prim in $\mathbb{Z}$. Analog ist 2029 prim in $\mathbb{Z}$.

- Das Polynom $T^2 + T + 1 \in \mathbb{F}_2[T]$ ist irreduzibel (nachrechnen; wegen des niedrigen Grades genügt es, Nullstellen zu untersuchen!), und damit prim in $\mathbb{F}_2[T]$.

Anmerkung für Lehramtsstudenten (unendlich viele Primzahlen)**.** Dass es in den ganzen Zahlen unendlich viele Primzahlen gibt, ist mindestens seit Euklid bekannt [2, Kapitel 1]. Jeder Schüler (und Lehrer ...) sollte diesen wunderbaren (und einfachen) Beweis kennen!

Literaturaufgabe (der Primzahlsatz)**.** Die Verteilung der Primzahlen in $\mathbb{Z}$ ist einerseits sehr chaotisch; andererseits gehorcht sie asymptotisch durchaus einer gewissen Regelmäßigkeit: Wir definieren die Primzahl-Zähl-Funktion

$$\begin{aligned}\pi\colon \mathbb{R} &\longrightarrow \mathbb{R}\\ x &\longmapsto \#\{p \in \mathbb{N} \mid p \text{ prim und } p \leq x\}.\end{aligned}$$

Nach dem *Primzahlsatz* gilt

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Asymptotisch wächst die Anzahl der Primzahlen kleiner gleich x also wie $x/\ln x$. Man kann diesen erstaunlichen Satz zum Beispiel mithilfe der Funktionentheorie beweisen. Überfliegen Sie Kapitel VII aus dem Buch *Funktionentheorie 1* von E. Freitag und R. Busam [15].

2.2.3 Primideale und Restklassenringe

Ein allgemeines Prinzip der Zahlentheorie ist es, Begriffe und Sachverhalte von Elementen in Ringen auf Ideale zu erweitern. Diese Verallgemeinerung ermöglicht es, Zusammenhänge besser zu beschreiben, die auf dem Niveau der Ringelemente nicht oder nur schwer erkennbar sind.

Inklusionsbeziehungen zwischen Hauptidealen lassen sich auch durch Teilbarkeitsbeziehungen ihrer Erzeuger charakterisieren (Bemerkung 2.2.2). Dies führt zum Begriff des Primideals, als Verallgemeinerung von Primelementen:

Definition 2.2.13 (Primideal, maximales Ideal)**.** Sei R ein Ring.

- Ein Ideal $p \subset R$ in R ist *prim*, wenn $p \neq R$ ist und
$$\forall_{x,y\in R} \quad x \cdot y \in p \Longrightarrow (x \in p \vee y \in p).$$
- Ein Ideal $m \subset R$ in R ist *maximal*, wenn $m \neq R$ und für alle Ideale $a \subset R$ in R gilt: Ist $m \subset a$, so folgt bereits $a = m$ oder $a = R$.

Beispiel 2.2.14 (Primideale, maximale Ideale)**.**

- Das Ideal (2025) in $\mathbb{Z}$ ist weder ein Primideal noch maximal: Es gilt $5 \cdot 405 \in (2025)$, aber weder $5 \in (2025)$ noch $405 \in (2025)$. Also ist (2025) *kein* Primideal in $\mathbb{Z}$.

  Wegen $(2025) \subset (5) \subset \mathbb{Z}$ und da diese beiden Inklusionen strikt sind, ist (2025) *kein* maximales Ideal in $\mathbb{Z}$.

- Allgemeiner gilt: Sei R ein Integritätsring und $p \in R\setminus(\{0\}\cup R^\times)$. Dann ist das Hauptideal (p) genau dann prim, wenn p prim ist, denn:

  Sei p prim und seien $x, y \in R$ mit $x \cdot y \in (p)$. Dann ist p ein Teiler von $x \cdot y$. Da p prim ist, ist p somit ein Teiler von x oder von y. Im ersten Fall folgt $x \in (p)$, im zweiten Fall folgt $y \in (p)$. Also ist (p) ein Primideal. Außerdem ist $(p) \neq R$, da $p \notin R^\times$.

Sei umgekehrt (p) ein Primideal in R. Dann ist p prim, denn: Seien $x, y \in R$ mit $p \mid x \cdot y$. Also ist $x \cdot y \in (p)$. Da (p) ein Primideal ist, folgt $x \in (p)$ oder $y \in (p)$. Im ersten Fall ist p ein Teiler von x, im zweiten Fall ist p ein Teiler von y.

- Ist R ein Hauptidealring und ist $p \in R$ prim, so ist (p) ein maximales Ideal in R (dies folgt aus dem Zusammenhang zwischen Teilbarkeit und Hauptidealen, Bemerkung 2.2.2).
- Sei R ein Ring mit $0 \neq 1$. Dann ist das Nullideal (0) genau dann ein Primideal in R, wenn R ein ? Integritätsring ist.

Satz 2.2.15 (Restklassenringe zu Primidealen/maximalen Idealen)**.** *Sei R ein Ring und sei $a \subset R$ ein Ideal mit $a \neq R$. Dann gilt:*

1. *Der Restklassenring R/a ist genau dann nullteilerfrei, wenn a ein Primideal ist.*
2. *Der Restklassenring R/a ist genau dann ein Körper, wenn a ein maximales Ideal ist.*

Beweis. Zu 1. Für alle $x, y \in R$ gilt

$$[x] \cdot [y] = 0 \in R/a \iff x \cdot y \in a$$

und

$$\big([x] = 0 \in R/a \vee [y] = 0 \in R/a\big) \iff (x \in a \vee y \in a).$$

Also ist R/a genau dann nullteilerfrei, wenn a ein Primideal ist.

Zu 2. Wir verwenden die Charakterisierung von Körpern über Ideale (Proposition 2.1.25). Sei $\pi\colon R \longrightarrow R/a$ die kanonische Projektion. Dann sind

$$\begin{aligned} \{b \subset R \mid b \text{ Ideal in } R \text{ mit } a \subset b\} &\longrightarrow \{b \subset R/a \mid b \text{ Ideal in } R/a\} \\ b &\longmapsto \pi(b) \\ \pi^{-1}(b) &\longmapsfrom b \end{aligned}$$

zueinander inverse Bijektionen (nachrechnen).

Ist R/a ein Körper, so hat R/a nur die beiden Ideale $\{0\}$ und R/a (Proposition 2.1.25). Mit den obigen Bijektionen folgt daraus, dass a ein maximales Ideal in R ist.

Ist umgekehrt a ein maximales Ideal in R, so ist R/a *nicht* der Nullring. Mit der obigen Bijektion folgt, dass R/a nur die Ideale $\{0\}$ und R/a besitzt. Daher ist R/a ein Körper (Proposition 2.1.25). □

Korollar 2.2.16. *Maximale Ideale sind prim.*

Beweis. Sei R ein Ring und sei $a \subset R$ ein maximales Ideal. Dann ist R/a ein Körper (Satz 2.2.15), und damit insbesondere ein Integritätsring. Also ist a prim (Satz 2.2.15).

Alternativ kann man dies auch direkt zeigen (ähnlich zum Beweis von Proposition 2.2.11): Sei $a \subset R$ ein maximales Ideal, seien $x, y \in R$ mit $x \cdot y \in a$. Dann ist $x \in a$ oder $y \in a$, denn: Ist $x \notin a$, so betrachten wir das Ideal

$$b := \big(a \cup \{x\}\big) \subset R$$

in R. Nach Konstruktion ist $a \subset b$. Da a ein maximales Ideal ist, liefert dies $b = R$. Insbesondere ist $1 \in b$; also gibt es ein $z \in a$ und $r \in R$ mit

$$1 = z + r \cdot x.$$

Damit erhalten wir

$$y = 1 \cdot y = (z + r \cdot x) \cdot y = z \cdot y + r \cdot x \cdot y.$$

Wegen $z \in a$ ist $z \cdot y \in a$ (da a ein Ideal ist); außerdem ist $r \cdot x \cdot y \in a$, da $x \cdot y$ nach Voraussetzung in a liegt. Insgesamt folgt daher $y \in a$, wie gewünscht. □

Beispiel 2.2.17 (der Körper $\mathbb{F}_p$)**.** Sei $p \in \mathbb{N}$ prim. Dann ist $(p) \subset \mathbb{Z}$ ein maximales Ideal in $\mathbb{Z}$ (Beispiel 2.2.14). Nach Satz 2.2.15 ist somit der Restklassenring

$$\mathbb{F}_p := \mathbb{Z}/(p)$$

ein Körper. Wir werden später noch weitere Beispiele für endliche Körper kennenlernen (Kapitel 3.3).

Jeder Ring enthält maximale Ideale; genauer gilt sogar:

Satz 2.2.18 (Existenz maximaler Ideale)**.** *Sei R ein Ring und sei $a \subset R$ ein Ideal mit $a \neq R$. Dann gibt es ein maximales Ideal $m \subset R$ mit $a \subset m$.*

Beweis. Wir beweisen diese Aussage mit dem Lemma von Zorn (Satz I.3.4.23): Dazu betrachten wir die Menge

$$M := \{b \subset R \mid b \text{ Ideal in } R,\ a \subset b,\ b \neq R\},$$

partiell geordnet durch Inklusion. Warum sind die Voraussetzungen des Lemmas von Zorn erfüllt? Es ist $M \neq \emptyset$ (denn $a \in M$). Ist $(b_i)_{i \in I}$ eine total geordnete Kette in M, so ist $b := \bigcup_{i \in I} b_i$ ein Element von M und eine obere Schranke von $(b_i)_{i \in I}$, denn:

- Nach Konstruktion ist $a \subset b$ und $b_i \subset b$ für alle $i \in I$.
- Die Vereinigung $b = \bigcup_{i \in I} b_i$ ist tatsächlich ein Ideal, denn $(b_i)_{i \in I}$ ist eine total geordnete Kette (nachrechnen).
- Außerdem ist $b \neq R$, denn: *Angenommen,* es wäre $b = R$. Dann wäre $1 \in b = \bigcup_{i \in I} b_i$; also gäbe es ein $i \in I$ mit $1 \in b_i$. Dann wäre aber bereits $b_i = R$, im Widerspruch zu $b_i \in M$.

Nach dem Lemma von Zorn besitzt M somit ein maximales Element m. Nach Konstruktion von M ist $a \subset m$ und m ist ein maximales Ideal in R. □

Korollar 2.2.19 (Restklassenkörper)**.** *Sei R ein Ring und sei $a \subset R$ ein Ideal mit $a \neq R$. Dann gibt einen Körper K und einen surjektiven Ringhomomorphismus $f\colon R \longrightarrow K$ mit*

$$\forall_{x \in a} \quad f(x) = 0.$$

Beweis. Wegen $a \neq R$ gibt es ein maximales Ideal $m \subset R$ mit $a \subset m$ (Satz 2.2.18). Insbesondere ist R/m ein Körper (Satz 2.2.15) und die kanonische Projektion

$$R \longrightarrow R/m$$

hat die gewünschte Eigenschaft. □

Beispiel 2.2.20. Wir betrachten das Ideal $a := (2025)$ in $\mathbb{Z}$. Maximale Ideale von $\mathbb{Z}$, die a enthalten sind ? (3) und (5). Somit sind die kanonischen Projektionen ? $\mathbb{Z} \longrightarrow \mathbb{F}_3$ und $\mathbb{Z} \longrightarrow \mathbb{F}_5$ surjektive Ringhomomorphismen in Körper, die auf a verschwinden.

Ein wichtiges Hilfsmittel in der elementaren Zahlentheorie und in der Strukturtheorie von Moduln über Hauptidealringen ist der Chinesische Restsatz. Wir werden nun die Version des Chinesischen Restsatzes für Ideale und Restklassenringe (statt „nur“ für Moduln) untersuchen.

Definition 2.2.21 (koprim)**.** Sei R ein Ring. Ideale $a, b \subset R$ heißen *koprim*, wenn das von a und b erzeugte Ideal $a + b = (a \cup b)$ ganz R ist.

Beispiel 2.2.22 (koprime Ideale)**.**

1. Die Ideale (2) und (3) in $\mathbb{Z}$ sind koprim, denn $1 = 3 - 2 \in (2, 3)$.
2. Die Ideale (4) und (6) in $\mathbb{Z}$ sind *nicht* koprim, denn

$$(4, 6) = \big(\mathrm{ggT}(4, 6)\big) = (2) \neq \mathbb{Z}.$$

Satz 2.2.23 (Chinesischer Restsatz)**.** *Sei R ein Ring und seien $a, b \subset R$ koprime Ideale. Dann ist*

$$\begin{aligned} R/a \cap b &\longrightarrow R/a \times R/b \\ [x]_{a \cap b} &\longmapsto \big([x]_a, [x]_b\big) \end{aligned}$$

ein wohldefinierter Ringisomorphismus. Dabei trägt die rechte Seite die Produktringstruktur.

Beweis. Wir betrachten den Ringhomomorphismus

$$\begin{aligned} f\colon R &\longrightarrow R/a \times R/b \\ x &\longmapsto \big([x]_a, [x]_b\big). \end{aligned}$$

Mit der universellen Eigenschaft des Restklassenrings $R/\ker f$ erhalten wir somit einen wohldefinierten Ringhomomorphismus

$$\begin{aligned}\overline{f}\colon R/\ker f &\longrightarrow R/a \times R/b\\ [x]_{\ker f} &\longmapsto \big([x]_a, [x]_b\big).\end{aligned}$$

Wir bestimmen den Kern und das Bild von f:

- Nach Konstruktion ist $\ker f = a \cap b$.
- Der Ringhomomorphismus f ist surjektiv, denn: Seien $x, y \in R$. Da a und b koprim sind, gibt es $x' \in a$ und $y' \in b$ mit

  $$x' + y' = 1$$

  (in euklidischen Ringen kann hierbei der euklidische Algorithmus bei der Bestimmung von x' und y' helfen). Dann ist

  $$f(y' \cdot x + x' \cdot y) = \big([x]_a, [y]_b\big),$$

  denn es gilt (wegen $x' \in a$)

  $$\begin{aligned}[y' \cdot x + x' \cdot y]_a &= [y' \cdot x]_a && \text{(wegen } x' \in a\text{)}\\ &= [y' \cdot x + x' \cdot x]_a && \text{(wegen } x' \in a\text{)}\\ &= \big[(y' + x') \cdot x\big]\\ &= [1 \cdot x]_a\end{aligned}$$

  (und analog für die Reduktion modulo b).

Also ist $\overline{f}$ ein Ringisomorphismus; wegen $\ker f = a \cap b$ zeigt dies die Behauptung. □

Beispiel 2.2.24 (letzte Ziffer)**.** Ist $n \in \mathbb{N}$, so erhält man die letzte Ziffer der Dezimaldarstellung von n als Standardrepräsentant von $[n] \in \mathbb{Z}/(10)$. Nach dem Chinesischen Restsatz (Satz 2.2.23) ist wegen $10 = \mathrm{kgV}(2,5)$, $\mathrm{ggT}(2,5) = 1$ und Proposition 2.2.7 die Abbildung

$$\begin{aligned}\mathbb{Z}/(10) = \mathbb{Z}/((2) \cap (5)) &\longrightarrow \mathbb{Z}/(2) \times \mathbb{Z}/(5)\\ [n]_{10} &\longmapsto \big([n]_2, [n]_5\big)\end{aligned}$$

ein Ringisomorphismus. Möchte man die letzte Ziffer der Dezimaldarstellung von n bestimmen, so genügt es also den Rest von n bei Division durch 2 und durch 5 zu kennen. Genauer: Nach dem Beweis des Chinesischen Restsatzes (Satz 2.2.23) ist

$$\begin{aligned}\mathbb{Z}/(2) \times \mathbb{Z}/(5) &\longrightarrow \mathbb{Z}/(10) = \mathbb{Z}/((2) \cap (5))\\ \big([x]_2, [y]_5\big) &\longmapsto \boxed{?} \quad [5 \cdot x - 4 \cdot y]_{10}\end{aligned}$$

das Inverse des obigen Ringisomorphismus, denn

$$-4+5=1 \quad \text{und} \quad -4 \in (2), \quad 5 \in (5).$$

Bemerkung 2.2.25 (Chinesischer Restsatz, mehr Faktoren)**.** Analog zur obigen Version des Chinesischen Restsatzes erhält man auch: Sei R ein Ring, sei $n \in \mathbb{N}$ und seien $a_1, \ldots, a_n$ paarweise koprime Ideale in R. Dann ist

$$\begin{aligned} R/\bigcap_{j=1}^{n} a_j &\longrightarrow \prod_{j=1}^{n} R/a_j \\ [x] &\longmapsto \left([x]_{a_j}\right)_{j\in\{1,\ldots,n\}} \end{aligned}$$

ein wohldefinierter Ringisomorphismus [6, Satz 2.3.12].

2.2.4 Der kleine Satz von Fermat

Als Anwendung der bisher entwickelten Ringtheorie beschäftigen wir uns mit dem kleinen Satz von Fermat aus der elementaren Zahlentheorie:

Satz 2.2.26 (kleiner Satz von Fermat)**.** *Sei $p \in \mathbb{N}$ prim. Dann gilt*

$$x^{p-1} \equiv 1 \mod p$$

für alle $x \in \mathbb{Z}$ mit $p \nmid x$.

Beweis. Wir beweisen dies, indem wir die dazu äquivalente Behauptung

$$\forall_{z\in(\mathbb{Z}/(p))\setminus\{0\}} \quad z^{p-1} = [1]$$

in $\mathbb{Z}/(p)$ beweisen. Wir wissen bereits, dass $\mathbb{Z}/(p)$ ein Körper ist (Beispiel 2.2.17); insbesondere ist $(\mathbb{Z}/(p))\setminus\{0\}$ eine Gruppe bezüglich Multiplikation mit genau $p-1$ Elementen. Mit dem Satz von Lagrange (Korollar 1.1.59) folgt, dass $z^{p-1} = [1]$ für alle $z \in \mathbb{Z}/(p) \setminus \{0\}$ gilt. □

Mit dem kleinen Satz von Fermat (Satz 2.2.26) können wir Fragen vom Typ der Aufgabe 5 aus der Einleitung lösen. Wir beginnen mit einem besonders einfachen Fall:

Beispiel 2.2.27. Wir bestimmen den Rest der Potenz 4242^{2027} bei Division durch 2027: Da 2027 prim ist und kein Teiler von 4242 ist, gilt nach dem kleinen Satz von Fermat (SatZ 2.2.26)

$$4242^{2027} \equiv 1 \cdot 4242 \mod 2027.$$

Wegen $4242 = 2 \cdot 2027 + 188$ liefert also 4242^{2027} den Rest ? 188 bei Division durch 2027.

Um kompliziertere Aufgaben dieser Art zu lösen, bietet es sich an, die folgende Vorüberlegung zu machen:

Bemerkung 2.2.28. Sei $p \in \mathbb{N}$ prim, sei $x \in \mathbb{Z}$ nicht durch p teilbar und sei $k \in \mathbb{N}$. Sei $r \in \mathbb{N}$ der Rest von k bei Division durch $p-1$. Dann gilt

$$x^k \equiv x^r \mod p,$$

denn: Nach Definition von r gibt es $s \in \mathbb{Z}$ mit

$$k = s \cdot (p-1) + r.$$

Daher liefert der kleine Satz von Fermat (Satz 2.2.26) in $\mathbb{Z}/(p)$ die Gleichung

$$[x^k] = [x^{s\cdot(p-1)+r}] = [x^{p-1}]^s \cdot [x^r] = [1]^s \cdot [x^r] = [x^r].$$

Beispiel 2.2.29. Wir bestimmen den Rest der Potenz 4242^{2026} bei Division durch 2026: Die Primfaktorzerlegung von 2026 ist $2026 = 2 \cdot 1013$. Nach dem Chinesischen Restsatz genügt es, zunächst

① den Rest von 4242^{2026} bei Division durch 2 und

② den Rest von 4242^{2026} bei Division durch 1013

zu bestimmen.

Zu ①. Da 4242 gerade und $2026 > 0$ ist, ist auch 4242^{2026} gerade, und damit ist der gesuchte Rest 0.

Zu ②. Wir verwenden Bemerkung 2.2.28: Ganzzahlige Division mit Rest liefert

$$4242 = 4 \cdot 1013 + 190$$

insbesondere ist 4242 nicht durch 1013 teilbar. Außerdem ist

$$2026 = 2 \cdot 1012 + 2.$$

Mit Bemerkung 2.2.28 erhalten wir somit in $\mathbb{Z}/(1013)$, dass

$$[4242^{2026}] = [4242^2] = [4242]^2 = [190]^2. = [190 \cdot 190] = [645].$$

Die letzte Gleichheit kann von Hand erhalten werden, indem man zunächst $190 \cdot 190$ mit schriftlicher Multiplikation berechnet und dann den Rest bei Division durch 1013 mit schriftlicher Division ausrechnet.

Wir setzen die Ergebnisse aus ① und ② nun zusammen: Wegen

$$1 \cdot 1013 - 506 \cdot 2 = 1013 - 1012 = 1$$

erhalten wir aus dem Beweis des Chinesischen Restsatzes (Satz 2.2.23) in $\mathbb{Z}/(2026)$, dass

$$[4242^{2026}] = [1013 \cdot 0 - 1012 \cdot 645] = [1658].$$

Somit ist 1658 der gesuchte Rest.

Beispiel 2.2.30 (Ziffern bestimmen)**.** Wir bestimmen die letzte Ziffer der Zahl $(2026^{2026})^{2026}$ im Zehnersystem:

Es gilt in $\mathbb{Z}/10$:

$$\left[((2026)^{2026})^{2026}\right] = \left([2026]^{2026}\right)^{2026} = \left([6]^{2026}\right)^{2026} = [6],$$

denn aus $6 \cdot 6 = 36$ folgt induktiv $[6]^n = [6]$ in $\mathbb{Z}/(10)$ für alle $n \in \mathbb{N}$.

Beispiel 2.2.31 (Ziffern bestimmen)**.** Wir bestimmen die letzte Ziffer der Zahl $(2027^{2027})^{2027}$ im Zehnersystem:

Nach dem Chinesischen Restsatz (Satz 2.2.23, Beispiel 2.2.24) genügt es, die Reste bei Division durch 2 und 5 zu bestimmen.

- Da 2027 ungerade ist, ist der Rest von $(2027^{2027})^{2027}$ bei Division durch 2 gleich 1.
- Für den Rest bei Division durch 5 verwenden wir den kleinen Satz von Fermat in der Form von Bemerkung 2.2.28: Es ist 2027 nicht durch 5 teilbar und $2027 \cdot 2027$ ergibt bei Division durch $4 = 5 - 1$ den Rest 1. Also erhalten wir in $\mathbb{Z}/(5)$:

$$[(2027^{2027})^{2027}] = [2027^1] = [2].$$

Insgesamt ergibt sich so der Rest ? 7 bei Division durch 10. Die letzte Ziffer ist somit 7.

Der erste Teil von Aufgabe 5 scheint jedoch schwierig zu sein: Zur Berechnung der ersten Ziffer der Dezimaldarstellung wird man mehr oder weniger das gesamte Ergebnis berechnen müssen ... (die Antwort ist 3, aber das ist von Hand nicht machbar).

Ausblick 2.2.32 (probabilistischer Primzahltest)**.** Man kann den kleinen Satz von Fermat wie folgt als probabilistischen Primzahltest verwenden: Sei $p \in \mathbb{N}$ gegeben. Wir wollen feststellen, ob p prim ist oder nicht. Das naheliegende (aber sehr ineffiziente) Verfahren ist, zu überprüfen, ob $2, 3, \ldots, \lfloor\sqrt{p}\rfloor$ ein Teiler von p ist. Alternativ kann man z.B. wie folgt vorgehen:

- Wir wählen $a \in \{2, \ldots, p-2\}$ „zufällig“ aus und berechnen den Rest r von a^{p-1} bei Division durch p.
- Ist $r \neq 1$, so ist p nach dem kleinen Satz von Fermat (Satz 2.2.26) *nicht* prim.
- Ist $r = 1$, so iterieren wir das Verfahren einige Male (mit „unabhängigen“, „zufälligen“ a).

Wenn wir für „viele“ $a \in \{2, \dots, p-2\}$ als Rest von a^{p-1} bei Division durch p den Rest 1 erhalten, so verhält sich p „mit hoher Wahrscheinlichkeit“ wie eine Primzahl (im Bezug auf den kleinen Satz von Fermat). Tatsächlich ist dies in der Praxis ein brauchbarer Schnelltest. Neben der probablistischen Natur dieses Tests besteht aber auch das Problem, dass es Zahlen p gibt, die diesen Test für alle a erfüllen, aber *nicht* prim sind: die *Carmichael-Zahlen* (Ausblick 2.2.33).

Ausblick 2.2.33 (Carmichael-Zahlen)**.** Eine natürliche Zahl $p \in \mathbb{N}$ ist eine *Carmichael-Zahl*, wenn sie *keine* Primzahl ist, aber den kleinen Satz von Fermat (Satz 2.2.26) erfüllt, d.h. für alle $a \in \{1, \dots, p-1\}$ mit $\mathrm{ggT}(a, p) = 1$ gilt

$$a^{p-1} \equiv 1 \mod p.$$

Zum Beispiel ist 561 eine Carmichael-Zahl. Es ist bekannt, dass es unendlich viele Carmichael-Zahlen gibt [3].

Literaturaufgabe (PRIMES is in P)**.** Es gibt Algorithmen, die in polynomieller Zeit (gemessen in der Länge der Dezimaldarstellung der Eingabezahl) testen, ob eine natürliche Zahl prim ist oder nicht. Der erste Algorithmus dieser Art wurde von Agrawal, Kayal und Saxena entdeckt und beruht auf einer Variante des kleinen Satzes von Fermat [1]. Lesen Sie diesen Artikel!

Der kleine Satz von Fermat besitzt auch eine Formulierung für „Teiler“, die nicht prim sind. Dazu benötigen wir die folgende Beobachtung:

Proposition 2.2.34 (eulersche φ-Funktion)**.** *Sei $m \in \mathbb{N}_{>0}$.*

1. *Sei $x \in \mathbb{Z}$. Dann ist $[x]$ genau dann eine Einheit in $\mathbb{Z}/(m)$, wenn $\mathrm{ggT}(x, m) = 1$ ist.*
2. *Sei $\varphi(m) := \#\big\{x \in \{1, \dots, m-1\} \;\big|\; \mathrm{ggT}(x, m) = 1\big\} \in \mathbb{N}$. Dann folgt insbesondere*
$$\#\big(\mathbb{Z}/(m)^\times\big) = \varphi(m).$$

Beweis. Der erste Teil folgt aus den grundlegenden Eigenschaften des größten gemeinsamen Teilers von x und m im Hauptidealring $\mathbb{Z}$ (Proposition 2.2.6): Sei $x \in \mathbb{Z}$. Dann ist $[x]$ genau dann eine Einheit in $\mathbb{Z}/(m)$, wenn es ein $y \in \mathbb{Z}$ gibt mit

$$x \cdot y \in 1 + m \cdot \mathbb{Z}.$$

Ist $\mathrm{ggT}(x, m) = 1$, so gibt es wegen der Darstellbarkeit des größten gemeinsamen Teilers (Proposition 2.2.6) ganze Zahlen $y, s \in \mathbb{Z}$ mit

$$x \cdot y + m \cdot s = 1;$$

insbesondere ist $x \cdot y = 1 - m \cdot s \in 1 + m \cdot \mathbb{Z}$.

Ist umgekehrt $x \cdot y \in 1 + m \cdot \mathbb{Z}$, so ist jeder gemeinsame Teiler von x und m auch ein Teiler von 1; also ist $\mathrm{ggT}(x, m) = 1$.

Der zweite Teil ist eine direkte Folgerung aus dem ersten Teil. □

Beispiel 2.2.35 (eulersche φ-Funktion)**.** Ist $p \in \mathbb{N}$ prim, so ist $\varphi(p) = p - 1$. Sind $p, q \in \mathbb{N}$ prim mit $p \neq q$, so gilt (nachzählen)

$$\varphi(p \cdot q) = \text{?} \quad p \cdot q - p - q + 1 = (p-1) \cdot (q-1).$$

Insbesondere ist $\varphi(10) = \text{?}$ $1 \cdot 4 = 4$.

Satz 2.2.36 (kleiner Satz von Fermat; allgemeine Version)**.** *Sei $m \in \mathbb{N}_{>0}$. Dann gilt*

$$x^{\varphi(m)} \equiv 1 \mod m$$

für alle $x \in \mathbb{Z}$ mit $\mathrm{ggT}(x, m) = 1$. Dabei ist φ die eulersche φ-Funktion (Proposition 2.2.34).

Beweis. Wie im Beweis des kleinen Satzes von Fermat beweisen wir die zur Behauptung äquivalente Aussage

$$\forall_{x \in \mathbb{Z}} \quad \mathrm{ggT}(x, m) = 1 \Longrightarrow [x]^{\varphi(m)} = [1]$$

in $\mathbb{Z}/(m)$. Sei $x \in \mathbb{Z}$ mit $\mathrm{ggT}(x, m) = 1$. Nach Proposition 2.2.34 ist $[x]$ dann eine Einheit in $\mathbb{Z}/(m)$; außerdem enthält die Einheitengruppe $\mathbb{Z}/(m)^\times$ von $\mathbb{Z}/(m)$ genau $\varphi(m)$ Elemente. Mit dem Satz von Lagrange (Korollar 1.1.59) erhalten wir daher in $\mathbb{Z}/(m)$:

$$[x]^{\varphi(m)} = [1] \qquad \square$$

Ausblick 2.2.37 (RSA)**.** Eine wichtige Anwendung des kleinen Satzes von Fermat ist das RSA-Verschlüsselungsverfahren [25], ein Beispiel eines asymmetrischen Verschlüsselungsverfahrens (d.h., dass die Schlüssel zur Ver- bzw. Entschlüsselung *nicht* übereinstimmen). Wir benötigen dazu die folgenden Zutaten:

- Seien $p, q \in \mathbb{N}$ zwei (große) verschiedene Primzahlen und sei $m := p \cdot q$. Dann ist $\varphi(m) = (p-1) \cdot (q-1)$ (Beispiel 2.2.35).
- Seien außerdem $d, e \in \mathbb{N}$ (große, verschiedene) Zahlen mit

$$\mathrm{ggT}\big(d, \varphi(m)\big) = 1 \quad \text{und} \quad d \cdot e \equiv 1 \mod \varphi(m).$$

Das Paar (e, m) ist der *öffentliche Schlüssel*, das Paar (d, m) der *private Schlüssel*. Wir betrachten die Abbildungen

$$\begin{aligned} E \colon \mathbb{Z}/(m) &\longmapsto \mathbb{Z}/(m) && \text{„Encryption“} \\ x &\longmapsto x^e, \\ D \colon \mathbb{Z}/(m) &\longmapsto \mathbb{Z}/(m) && \text{„Decryption“} \\ x &\longmapsto x^d. \end{aligned}$$

Dann gilt $D \circ E = \mathrm{id}_{\mathbb{Z}/(m)}$, denn: Mit dem kleinen Satz von Fermat (Satz 2.2.36) erhalten wir (wegen $d \cdot e \equiv 1 \mod \varphi(m)$, analog zu Bemerkung 2.2.28)

$$D \circ E(x) = x^{d \cdot e} = x^1$$

für alle $x \in \mathbb{Z}/(m)^\times$; ist $x \in \mathbb{Z}/(m)$ keine Einheit, so ist x (bzw. seine Repräsentanten) durch p oder q teilbar, und wir erhalten die obige Identität mithilfe des kleinen Satzes von Ferma (Satz 2.2.26) und dem Chinesischen Restsatz (Satz 2.2.23; nachrechnen).

Wie kann man dies für Verschlüsselung verwenden?

- Der Empfänger wählt Zahlen p, q, d, e mit den obigen Eigenschaften und stellt den öffentlichen Schlüssel (e, m) öffentlich (!) zur Verfügung (jeder potentielle Sender an diesen Empfänger kann also den öffentlichen Schlüssel verwenden); der Empfänger behält jedoch den privaten Schlüssel (d, m) für sich.
- Der Sender transformiert Nachrichten in injektiver, standardisierter Weise in Elemente von $\mathbb{Z}/(m)$ (z.B. durch Aufteilen in geeignete, kleine, Blöcke).
- Zur Verschlüsselung einer Nachricht $x \in \mathbb{Z}/(m)$ wendet der Sender die Verschlüsselungsabbildung E (encryption) auf x an (dafür muss er nur den öffentlichen Schlüssel des Empfängers kennen!). Er sendet die verschlüsselte Nachricht $E(x)$ an den Empfänger.
- Der Empfänger wendet die Entschlüsselungsabbildung D (decryption) auf die verschlüsselte Nachricht $E(x)$ an. Wegen $D \circ E = \mathrm{id}_{\mathbb{Z}/(m)}$ erhält er auf diese Weise das Original x zurück.

Wie sicher ist dieses Verfahren? Die erste Beobachtung ist, dass E und D im allgemeinen verschieden sind (das Verfahren ist asymmetrisch). Die Sicherheit des Verfahrens hängt im wesentlichen davon ab, wie „gut“ und „groß“ die erstellten (Prim)Zahlen sind und dass Entschlüsselung mindestens so schwierig zu sein scheint wie die Faktorisierung der Zahl m in die Primfaktoren p und q. Da bislang kein effizienter Faktorisierungsalgorithmus bekannt ist (und viele vermuten, dass es einen solchen nicht geben kann), wird angenommen, dass das RSA-Verfahren bei vernünftiger Schlüsselwahl ziemlich sicher ist.

Wie kann der Empfänger geeignete Zahlen p, q, d, e finden? Man wählt zufällig „große“ Zahlen; mit dem Primzahlsatz (Literaturaufgabe 2.2.2) kann man abschätzen, wieviele Kandidaten man testen muss, um Primzahlen zu finden. Als Schnelltest bietet sich dabei ein probabilistischer Primzahltest wie in Ausblick 2.2.32 an. Mit diesem Verfahren erhält man p und q. Man wählt dann auf ähnliche Weise eine „große“ Zahl d mit $\mathrm{ggT}(d, \varphi(m)) = 1$ (zum Beispiel eine Primzahl in einem geeigneten Bereich). Die Zahl e kann man dann mit dem euklidischen Algorithmus aus d bestimmen, sofern man $\varphi(m)$ kennt. In der Praxis gibt es natürlich noch weitere Details zu beachten, um einfache brute-force-Attacken unmöglich zu machen.

Außerdem ist relevant, das E und D effizient berechnet werden können (zum Beispiel durch Ersetzen der Exponentiation mit Exponent e bzw. d durch geeignetes iteriertes Quadrieren).

Das RSA-Verfahren wird in vielen elektronischen Komponenten für die Verschlüsselung privater Daten und für elektronische Signatur-Verfahren genutzt. Es ist ein eindrucksvolles Beispiel dafür, dass mathematische Forschung, von der vormals geglaubt wurde, dass sie nie eine Anwendung haben würde (in diesem Fall die Zahlentheorie), plötzlich große praktische Relevanz im Alltag erlangen kann.

Literaturaufgabe (RSA)**.** Lesen Sie den Original-Artikel von Rivest, Shamir und Adleman [25].

Literaturaufgabe (großer Fermat)**.** Was besagt der *große Satz von Fermat*? Was hat er mit Fermat zu tun? Wann wurde er bewiesen? Lesen Sie das Buch *Fermat's Last Theorem* [28] von S. Singh.

2.2.5 Faktorielle Ringe

In der elementaren Zahlentheorie (d.h. der Theorie der Arithmetik von $\mathbb{Z}$) sind die Primelemente die grundlegenden Bausteine: jede ganze Zahl außer 0, 1, -1 lässt sich (eindeutig) als Produkt von Primzahlen schreiben. Wir werden im folgenden allgemeiner untersuchen, welche Ringe Primfaktorzerlegungen erlauben.

Definition 2.2.38 (faktorieller Ring)**.** Ein *faktorieller Ring* ist ein Integritätsring R, in dem sich jedes Element aus $R \setminus (\{0\} \cup R^\times)$ als endliches Produkt von Primelementen schreiben lässt.

Bemerkung 2.2.39 (Eindeutigkeit von Primfaktorzerlegungen)**.** Primfaktorzerlegungen sind (wenn sie existieren) im wesentlichen eindeutig: Sei R ein Integritätsring und seien $p_1, \ldots, p_n, q_1, \ldots, q_m \in R$ Primelemente mit

$$\prod_{j=1}^{n} p_j = \prod_{j=1}^{m} q_j.$$

Dann folgt $n = m$ und es gibt eine Permutation $\sigma \in S_n$ sowie Einheiten $\varepsilon_1, \ldots, \varepsilon_n \in R^\times$ mit

$$\forall_{j \in \{1,\ldots,n\}} \quad p_j = \varepsilon_j \cdot q_{\sigma(j)}.$$

Man kann diese Aussage per Induktion über n aus der definierenden Eigenschaft von Primelementen ableiten (nachrechnen). Diese Eindeutigkeitsaussage ist der wesentliche Grund für die Formulierung der Definition der Primeigenschaft.

Bemerkung 2.2.40 (Primelemente in faktoriellen Ringen)**.** Ist R ein faktorieller Ring und ist $p \in R$ irreduzibel, so ist p bereits prim, denn: Da R faktoriell und $p \notin \{0\} \cup R^\times$ ist, besitzt p eine Primfaktorzerlegung in R. Da p irreduzibel ist, besteht diese aber nur aus einem einzigen Primelement. Also ist p dieses Primelement und damit prim.

Satz 2.2.41 (Hauptidealringe sind faktoriell)**.** *Ist R ein Hauptidealring, so gilt:*

1. *Der Ring R ist* noethersch*, d.h. jede aufsteigende Folge von Idealen in R wird stationär; genauer: für jede Folge $(a_n)_{n\in\mathbb{N}}$ von Idealen in R mit $a_0 \subset a_1 \subset a_2 \subset \dots$ gibt es ein $N \in \mathbb{N}$ mit*

$$\forall_{n\in\mathbb{N}_{\geq N}} \quad a_n = a_N.$$

2. *Der Ring R ist faktoriell.*

Beweis. Wir haben diesen Satz bereits in der Linearen Algebra II bewiesen (Lemma II.2.4.23, Satz II.2.4.22) und wir erinnern daher nur kurz an die wesentlichen Ideen:

Zu 1. Die Vereinigung $\bigcup_{n\in\mathbb{N}} a_n$ ist (da die Idealfolge aufsteigend ist) ein Ideal in R und daher ein Hauptideal, etwa erzeugt von $x \in R$. Insbesondere gibt es ein $N \in \mathbb{N}$ mit $x \in a_N$, woraus folgt, dass $a_n = a_N$ für alle $n \in \mathbb{N}_{\geq N}$ gilt.

Zu 2. Die Grundidee ist, Elemente schrittweise in Primfaktoren zu zerlegen: Ist das betrachtete Element irreduzibel, so ist es (da R ein Hauptidealring ist; Proposition 2.2.11) bereits prim. Ist es nicht irreduzibel, so kann es als Produkt zweier Nicht-Einheiten geschrieben werden, die man nach demselben Verfahren weiter zerlegen kann. Mit dem ersten Teil kann man zeigen, dass dieses Verfahren nach endlich vielen Schritten terminiert:

Sei $Q \subset R$ die Menge aller Elemente $x \in R \setminus (\{0\} \cup R^\times)$, die *nicht* als endliches Produkt von Primelementen geschrieben werden können. Wir betrachten dann die Menge $S := \{(x) \mid x \in Q\}$ der zugehörigen Hauptideale und zeigen, dass $S = \emptyset$ ist:

Angenommen, S wäre nicht-leer. Aus dem ersten Teil folgt dann, dass S Elemente enthält, die bezüglich Inklusion maximal sind, d.h. es gibt ein $a \in S$ mit:

$$\forall_{b\in S} \quad a \subset b \Longrightarrow a = b.$$

Etwas genauer: *Angenommen,* es gäbe *kein* maximales Element in $S \neq \emptyset$. Sei $a_0 \in S$. Da a_0 nicht maximal ist, existiert ein $a_1 \in S$ mit $a_0 \subset a_1$ und $a_1 \neq a_0$. Da auch a_1 nicht maximal ist, gibt es dann ein $a_2 \in S$ mit $\dots$. Dies liefert eine echt aufsteigende Kette $(a_n)_{n\in\mathbb{N}}$ von Idealen in R, im Widerspruch zum ersten Teil. Strenggenommen haben wir bei der Konstruktion der Folge $(a_n)_{n\in\mathbb{N}}$ eine etwas schwächere Variante des Auswahlaxioms, das *Axiom of Dependent Choice*, verwendet. Also enthält S ein maximales Element a.

Sei nun $z \in Q$ mit $a = (z)$. Wegen $z \in Q$ ist z insbesondere *kein* Primelement und daher (da R ein Hauptidealring ist) auch nicht irreduzibel. Es gibt also $x, y \in R \setminus R^\times$ mit

$$z = x \cdot y.$$

Wegen $z \in Q$ ist auch $x \in Q$ oder $y \in Q$. Ohne Einschränkung sei $x \in Q$. Aus $x \mid z$ erhalten wir aber $a = (z) \subset (x)$. Da a in S maximal ist, folgt $(z) = (x)$, und damit, dass z und x assoziiert sind. Dies steht jedoch im Widerspruch dazu, dass y keine Einheit ist. Also ist $S = \emptyset$, und damit auch $Q = \emptyset$. □

Beispiel 2.2.42 (faktorielle Ringe)**.**

- Der Ring $\mathbb{Z}$ der ganzen Zahlen ist faktoriell (da er ein Hauptidealring ist).
- Ist K ein Körper, so ist der Polynomring $K[T]$ faktoriell (da er ein Hauptidealring ist). Ähnlich wie für $\mathbb{Z}$ kann man zeigen, dass $K[T]$ unendlich viele Primelemente enthält (modulo Assoziiertheit; Übungsaufgabe).
- Der Ring $\mathbb{Z}[i\sqrt{5}]$ ist *nicht* faktoriell, denn: In $\mathbb{Z}[i\sqrt{5}]$ gilt

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

  Bis auf Assoziiertheit besitzt 6 keine weiteren Teiler. Aber wir wissen bereits, dass keiner der obigen Teiler eine Einheit oder prim ist (Beispiel 2.2.9). Also besitzt 6 *keine* Primfaktorzerlegung in $\mathbb{Z}[i\sqrt{5}]$.

Kennt man die Primfaktorzerlegungen, so kann man zum Beispiel größte gemeinsame Teiler und kleinste gemeinsame Vielfache bestimmen. Um effizient darüber sprechen zu können, führen wir die folgende Notation ein:

Definition 2.2.43 (Primbewertungen)**.** Ist R ein Integritätsring und $p \in R$ prim, so definieren wir

$$\begin{aligned} \nu_p \colon R &\longrightarrow \mathbb{N} \cup \{\infty\} \\ x &\longmapsto \sup\{n \in \mathbb{N} \mid p^n \text{ teilt } x\}. \end{aligned}$$

Bemerkung 2.2.44 (Darstellung der Primfaktorzerlegung über Primbewertungen)**.** Sei R ein faktorieller Ring und sei $P \subset R$ ein Repräsentantensystem aller Primelemente von R modulo Assoziiertheit. Für jedes $x \in \mathbb{R} \setminus (\{0\} \cup R^\times)$ gibt es eine Einheit $\varepsilon \in R^\times$ mit

$$x = \varepsilon \cdot \prod_{p \in P} p^{\nu_p(x)}.$$

Dies ergibt sich aus der Existenz und Eindeutigkeit der Primfaktorzerlegung von x (nachrechnen).

Bemerkung 2.2.45 (Darstellung des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen in faktoriellen Ringen)**.** Ist R faktoriell, ist $P \subset R$

ein Repräsentantensystem aller Primelemente modulo Assoziiertheit, sind $x, y \notin \{0\} \cup R^\times$ und sind

$$x = x' \cdot \prod_{p \in P} p^{\nu_p(x)} \quad \text{und} \quad y = y' \cdot \prod_{p \in P} p^{\nu_p(y)}$$

mit $x', y' \in R^\times$ die zugehörigen Primfaktorzerlegungen von x bzw. y, so gilt (nachrechnen)

- $\prod_{p \in P} p^{\min(\nu_p(x), \nu_p(y))}$ ist ein größter gemeinsamer Teiler von x und y;
- $\prod_{p \in P} p^{\max(\nu_p(x), \nu_p(y))}$ ist ein kleinstes gemeinsames Vielfaches von x und y.

Wir wissen bereits, dass $\mathbb{Z}[T]$ und $\mathbb{Q}[X, Y]$ *keine* Hauptidealringe sind (Bemerkung 2.2.4). Aber als Polynomringe über faktoriellen Ringen sind sie immerhin faktoriell:

Satz 2.2.46 (Satz von Gauß)**.** *Ist R ein faktorieller Ring, so ist auch der Polynomring $R[T]$ faktoriell.*

Beispiel 2.2.47 (faktorielle Polynomringe)**.**

- Da $\mathbb{Z}$ als Hauptidealring ein faktorieller Ring ist, ist $\mathbb{Z}[T]$ nach dem Satz von Gauß (Satz 2.2.46) faktoriell. Eine weitere Anwendung des Satzes von Gauß liefert, dass auch $\mathbb{Z}[X, Y]$ faktoriell ist ...
- Ist K ein Körper und $n \in \mathbb{N}$, so folgt induktiv mit dem Satz von Gauß (Satz 2.2.46), dass der iterierte Polynomring

  $$K[X_1, \ldots, X_n] = \big((K[X_1])[X_2]\big) \ldots [X_n]$$

  faktoriell ist.
- Der Ring $\mathbb{Z}[i]$ ist euklidisch (Übungsaufgabe) und daher ein Hauptidealring (Proposition A.6.5); insbesondere ist $\mathbb{Z}[i]$ faktoriell. Also ist nach dem Satz von Gauß (Satz 2.2.46) auch $(\mathbb{Z}[i])[T]$ faktoriell.

Wie beweist man den Satz von Gauß? Sei R ein faktorieller Ring. Wir betrachten den Quotientenkörper $Q(R)$ (Proposition 2.1.17) von R. Da $Q(R)$ ein Körper ist, wissen wir bereits, dass der Polynomring $Q(R)[T]$ faktoriell ist (als Hauptidealring). Die kanonische Einbettung von R in $Q(R)$ liefert auch eine Einbettung von $R[T]$ in $Q(R)[T]$. Daher genügt es, zu überlegen, wie man aus Primfaktorzerlegungen in $Q(R)[T]$ Primfaktorzerlegungen in $R[T]$ erhält.

Als Hilfsmittel erweitern wir die Bewertungen ν_p von R auf $Q(R)$ und $Q(R)[T]$:

Definition 2.2.48 (Primbewertungen auf Quotientenkörpern)**.** Sei R ein faktorieller Ring und sei $p \in R$ prim.

- Ist $[x/y] \in Q(R)$ mit $x \in R, y \in R \setminus \{0\}$, so schreiben wir

$$\nu_p\left[\frac{x}{y}\right] := \nu_p(x) - \nu_p(y) \in \mathbb{Z} \cup \{\infty\}.$$

  Man beachte dabei, dass dies tatsächlich wohldefiniert ist (nachrechnen).

- Ist $f = \sum_{j=0}^{n} a_j \cdot T^j \in Q(R)[T]$ mit $a_0, \ldots, a_n \in Q(R)$, so schreiben wir

$$\nu_p(f) := \min\big\{\nu_p(a_j) \;\big|\; j \in \{0, \ldots, n\}\big\} \in \mathbb{Z} \cup \{\infty\}.$$

Beispiel 2.2.49. In $\mathbb{Q} = Q(\mathbb{Z})$ gilt

$$\nu_5(2025) = \boxed{?}\ 2 \quad \text{und} \quad \nu_5\Big(\frac{1}{2025}\Big) = \boxed{?}\ -2.$$

Mit der Familie der Funktionen ν_p zu allen Primelementen p kann man also die „arithmetische Größe“ von Polynomen in $Q(R)[T]$ messen und insbesondere testen, ob ein Polynom in $Q(R)[T]$ bereits in $R[T]$ liegt:

Bemerkung 2.2.50 (Bewertungstest)**.** Sei R ein faktorieller Ring und sei $f \in Q(R)[T]$. Dann ist f genau dann bereits ein Element des Unterrings $R[T]$ von $Q(R)[T]$, wenn für alle Primelemente $p \in R$

$$\nu_p(f) \geq 0$$

gilt (nachrechnen).

Als erste Vorüberlegung zeigen wir, dass die Primbewertungen auf dem Polynomring des Quotientenkörpers sich im folgenden Sinne wie Gradfunktionen verhalten (die ja im Beweis, dass Polynomringe über Körpern Hauptidealringe sind eine wichtige Rolle gespielt haben):

Lemma 2.2.51 (Lemma von Gauß)**.** *Sei R ein faktorieller Ring und sei $p \in R$ prim.*

1. *Dann gilt für alle $f, g \in Q(R)[T]$:*

$$\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$$

2. *Insbesondere: Sind $f, g \in Q(R)[T]$ normierte Polynome mit $f \cdot g \in R[T]$, so sind bereits $f, g \in R[T]$. Ein Polynom $\sum_{j=0}^{n} a_j \cdot T^j$ vom Grad $n \in \mathbb{N}$ mit $a_0, \ldots, a_n$ ist dabei* normiert*, wenn $a_n = 1$ gilt.*

Beweis. Zu 2. Der zweite Teil folgt aus dem ersten Teil: Sei $p \in R$ prim. Da f und g normiert sind, gilt $\nu_p(f) \leq \nu_p(1) = 0$ und $\nu_p(g) \leq \nu_p(1) = 0$. Wegen $f \cdot g$ ist $\nu_p(f \cdot g) \geq 0$, und daher erhalten wir mit dem ersten Teil

$$\nu_p(f) + \nu_p(f) = \nu_p(f \cdot g) \geq 0.$$

Wege $\nu_p(f) \leq 0$ und $\nu_p(g) \leq 0$ ergibt sich

$$\nu_p(f) = 0 = \nu_p(g).$$

Da dies für alle Primelemente gilt, folgt mit dem Bewertungstest (Bemerkung 2.2.50), dass in f und g keine echten Nenner auftreten können. Also gilt $f, g \in R[T]$.

Zu 1. Man kann dies mit genug Geduld direkt mit der Definition des Produkts von Polynomen nachrechnen. Wir gehen stattdessen etwas modularer in den folgenden Schritten vor:

① Sind $f, g \in Q(R)$, so gilt $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$, wie man leicht an der Primfaktorzerlegung der Zähler/Nenner erkennt (nachrechnen).

② Ist $f \in Q(R)$ und $g \in Q(R)[T]$, so gilt $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$, denn: Wir schreiben $g = \sum_{j=0}^{n} b_j \cdot T^j$. Dann folgt mit dem ersten Schritt

$$\begin{aligned}
\nu_p(f \cdot g) &= \nu_p\left(\sum_{j=0}^{n} f \cdot b_j \cdot T^j\right) \\
&= \min\left\{\nu_p(f \cdot b_j) \;\middle|\; j \in \{0, \ldots, n\}\right\} \\
&= \min\left\{\nu_p(f) + \nu_p(b_j) \;\middle|\; j \in \{0, \ldots, n\}\right\} \qquad \text{(nach ①)} \\
&= \nu_p(f) + \min\left\{\nu_p(b_j) \;\middle|\; j \in \{0, \ldots, n\}\right\} \\
&= \nu_p(f) + \nu_p(g).
\end{aligned}$$

③ Sind $f, g \in R[T]$ mit $\nu_p(f) = 0 = \nu_p(g)$, so ist $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$, denn: Wir betrachten den von der kanonischen Projektion $R \longrightarrow R/(p)$ induzierten Ringhomomorphismus

$$\pi \colon R[T] \longrightarrow R/(p)[T].$$

Da p prim ist, ist (p) ein Primideal in R (Beispiel 2.2.14); also ist $R/(p)$ ein Integritätsring (Satz 2.2.15); daher ist auch $R/(p)[T]$ ein Integritätsring (Proposition 2.1.14). Nach Konstruktion ist dabei

$$\ker \pi = \left\{h \in R[T] \;\middle|\; \nu_p(h) \overset{?}{>} 0\right\}.$$

Wegen $\nu_p(f) = 0 = \nu_p(g)$ ist $\pi(f) \neq 0$ und $\pi(g) \neq 0$. Da $R/(p)[T]$ ein Integritätsring ist, ist somit auch $\pi(f \cdot g) \neq 0$. Also ist $f \cdot g \notin \ker \pi$, und damit $\nu_p(f \cdot g) = 0$.

④ Der allgemeine Fall: Seien $f, g \in Q(R)[T]$. Nach Konstruktion von $Q(R)$ gibt es dann $c, d \in Q(R)^\times$ mit $c \cdot f, d \cdot g \in R[T]$ und $\nu_p(c \cdot f) = 0$ und $\nu_p(d \cdot g) = 0$ (man kann zum Beispiel mit dem Produkt aller Nenner multiplizieren und durch geeignete p-Potenzen dividieren). Dann erhalten wir

$$\begin{aligned}\nu_p(c\cdot d)+\nu_p(f\cdot g) &= \nu_p(c\cdot f\cdot d\cdot g) && \text{(nach ②)}\\ &= \nu_p(c\cdot f)+\nu_p(d\cdot g) && \text{(nach ③)}\\ &= \nu_p(c\cdot d)+\nu_p(f)+\nu_p(g) && \text{(nach ②/①),}\end{aligned}$$

und damit $\nu_p(f\cdot g)=\nu_p(f)+\nu_p(g)$.

Insgesamt folgt damit der erste Teil. □

Definition 2.2.52 (primitives Polynom)**.** Sei R ein faktorieller Ring. Ein Polynom $f\in R[T]$ ist *primitiv*, wenn für alle Primelemente $p\in R$ gilt, dass

$$\nu_p(f)=0.$$

Beispiel 2.2.53. Wir betrachten den Polynomring $\mathbb{Z}[T]$ über $\mathbb{Z}$.

- Ist $4\cdot T^2+2\cdot T-42\in\mathbb{Z}[T]$ primitiv?

  Ja Nein Die korrekte Antwort ist „Nein“. ×

- Ist $4\cdot T^2+2\cdot T-21\in\mathbb{Z}[T]$ primitiv?

  Ja Nein Die korrekte Antwort ist „Ja“. ×

Wir beweisen nun den Satz von Gauß (Satz 2.2.46):

Beweis von Satz 2.2.46. Wir zeigen die folgenden Aussagen:

1. Ist $q\in R$ prim, so ist q (aufgefasst als konstantes Polynom) auch in $R[T]$ prim.

2. Ist $q\in R[T]$ primitiv (im Sinne von Definition 2.2.52) und prim als Element von $Q(R)[T]$, so ist q bereits prim in $R[T]$.

3. Jedes Element in $R[T]\setminus\{0\}$ ist ein Produkt von Einheiten in R, von Primelementen von R und von primitiven Polynomen in $R[T]$, die prim in $Q(R)[T]$ sind.

Kombinieren diese Behauptungen, so erhalten wir insbesondere, dass jedes nicht-triviale Element in $R[T]$ eine Primfaktorzerlegung in $R[T]$ besitzt; also ist $R[T]$ faktoriell. Es genügt daher, die obigen Behauptungen zu zeigen:

Zu 1. Sei $q\in R$ prim. Dann ist (wie wir bereits im Beweis von Lemma 2.2.51 gesehen haben), $R/(q)[T]$ ein Integritätsring. Der kanonische Ringisomorphismus (nachrechnen; mithilfe der universellen Eigenschaften)

$$\begin{aligned}\big(R[T]\big)/(q) &\longrightarrow \big(R/(q)\big)[T]\\ [R\ni r] &\longmapsto [r]\\ [T] &\longmapsto T\end{aligned}$$

zeigt, dass dann auch $(R[T])/(q)$ ein Integritätsring ist. Also ist das von q erzeugte Ideal in $R[T]$ prim (Satz 2.2.15); daher ist q prim in $R[T]$ (Beispiel 2.2.14).

Alternativ könnte man dies auch von Hand über die Primeigenschaft nachrechnen.

Zu 2. Sei $q \in R[T]$ primitiv und prim in $Q(R)[T]$. Seien $f, g \in R[T]$ mit $q \mid f \cdot g$. Dann ist q auch in $Q(R)[T]$ ein Teiler von $f \cdot g$. Da q prim in $Q(R)[T]$ ist, ist q ein Teiler von f oder g in $Q(R)[T]$; ohne Einschränkung trete der erste Fall ein, d.h. es gibt ein $h \in Q(R)[T]$ mit

$$f = q \cdot h.$$

Mit dem Lemma von Gauß (Lemma 2.2.51) und der Tatsache, dass q primitiv ist, erhalten wir für alle Primelemente $p \in R$, dass

$$\begin{aligned} \nu_p(h) &= \nu_p(q \cdot h) - \nu_p(q) && \text{(Lemma von Gauß)} \\ &= \nu_p(f) - \nu_p(q) && \text{(wegen } f = q \cdot h\text{)} \\ &= \nu_p(f) && \text{(da } q \text{ primitiv ist)} \\ &\geq 0. && \text{(wegen } f \in R[T]\text{)} \end{aligned}$$

Also ist $h \in R[T]$ (Bemerkung 2.2.50); insbesondere ist q ein Teiler von f in $R[T]$. Somit ist q prim in $R[T]$.

Zu 3. Sei $f \in R[T] \setminus \{0\}$. Wir reduzieren uns zunächst auf den primitiven Fall: Indem wir den größten gemeinsamen Teiler der Koeffizienten von f ausmultiplizieren, erhalten wir eine Zerlegung

$$f = c \cdot g$$

mit $c \in R \setminus \{0\}$ und einem primitiven Polynom $g \in R[T]$. Da R faktoriell ist, ist c eine Einheit in R (und damit auch in $R[T]$) oder c besitzt eine Primfaktorzerlegung in R. Nach dem ersten Schritt ist eine solche Primfaktorzerlegung auch eine Primfaktorzerlegung in $R[T]$.

Es genügt also eine Primfaktorzerlegung für primitive Polynome $f \in R[T]$ mit $\deg f > 0$ zu finden: Der Ring $Q(R)[T]$ ist als Hauptidealring über einem Körper faktoriell (Satz 2.2.41). Aufgefasst als Element von $Q(R)[T]$ besitzt f somit eine Primfaktorzerlegung der Form

$$f = \prod_{j=1}^{n} p_j$$

mit $n \in \mathbb{N}_{>0}$ und Primelementen $p_1, \ldots, p_n \in Q(R)[T]$. Indem wir mit den Nennern der Koeffizienten dieser Polynome multiplizieren und jeweils durch den größten gemeinsamen Teiler der entstehenden Koeffizienten dividieren, erhalten wir $c_1, \ldots, c_n \in R \setminus \{0\}$ und primitive Polynome $q_1, \ldots, q_n \in R[T]$ mit

$$f = \prod_{j=1}^{n} \frac{1}{c_j} \cdot q_j = \prod_{j=1}^{n} \frac{1}{c_j} \cdot \prod_{j=1}^{n} q_j;$$

außerdem ist q_j in $Q(R)[T]$ zu dem Primelement p_j assoziiert, und damit prim in $Q(R)[T]$. Dabei liegt $c := \prod_{j=1}^{n} 1/c_j$ bereits in $R^\times$, denn: Da f und $q_1, \ldots, q_n$ primitiv sind, folgt mit dem Lemma von Gauß (Lemma 2.2.51) für alle Primelemente $p \in R$, dass

$$\nu_p(c) = \nu_p(f) - \sum_{j=1}^{n} \nu_p(q_j) = 0 - 0 = 0.$$

Also ist $c \in R$ (Bemerkung 2.2.50) bzw. wegen $1/c = c_1 \cdot \cdots \cdot c_n$ sogar $c \in R^\times$. Somit ist

$$f = (c \cdot q_1) \cdot q_2 \cdot \cdots \cdot q_n$$

eine Faktorisierung der gewünschten Form. □

Der Satz von Gauß und die darin verwendeten Techniken werden auch bei den Irreduzibilitätskriterien im folgenden Abschnitt eine Rolle spielen. Als Vorbereitung dafür merken wir uns eine Konsequenz aus dem obigen Beweis des Satzes von Gauß:

Korollar 2.2.54. *Sei R ein faktorieller Ring und sei $f \in R[T]$ ein primitives Polynom. Dann sind die folgenden Aussagen äquivalent:*

1. *Das Polynom f ist in $R[T]$ prim.*
2. *Das Polynom f ist in $R[T]$ irreduzibel.*
3. *Das Polynom f ist in $Q(R)[T]$ prim.*
4. *Das Polynom f ist in $Q(R)[T]$ irreduzibel.*

Beweis. Da R faktoriell ist, ist $R[T]$ nach dem Satz von Gauß (Satz 2.2.46) faktoriell; außerdem ist auch $Q(R)[T]$ faktoriell (da $Q(R)[T]$ sogar ein Hauptidealring ist). Daher sind Elemente genau dann in $R[T]$ (bzw. $Q(R)[T]$) irreduzibel, wenn sie prim sind (Bemerkung 2.2.40, Proposition 2.2.11).

Es genügt daher, die Äquivalenz der ersten und dritten Aussage zu zeigen:

Zu $3 \Longrightarrow 1$*:* Ist das primitive Polynom f prim in $Q(R)[T]$, so ist f auch in $R[T]$ prim (wie wir bereits im Beweis des Satzes von Gauß gesehen haben; Aussage 2.).

Zu $1 \Longrightarrow 3$*:* Sei umgekehrt f prim in $R[T]$. Nach den im Beweis des Satzes von Gauß gezeigten Aussagen besteht die Primfaktorzerlegung von f in $R[T]$ aus Primelementen von R und primitiven Polynomen in $R[T]$, die prim in $Q(R)[T]$ sind. Da f in $R[T]$ prim ist, besteht diese Produktzerlegung aus nur einem Faktor. Da f primitiv ist, ist f *kein* Primelement von R; also ist f prim in $Q(R)[T]$. □

Die bisher betrachteten Ringeigenschaften und ihre Beziehungen sind in Abbildung 2.3 zusammengestellt.

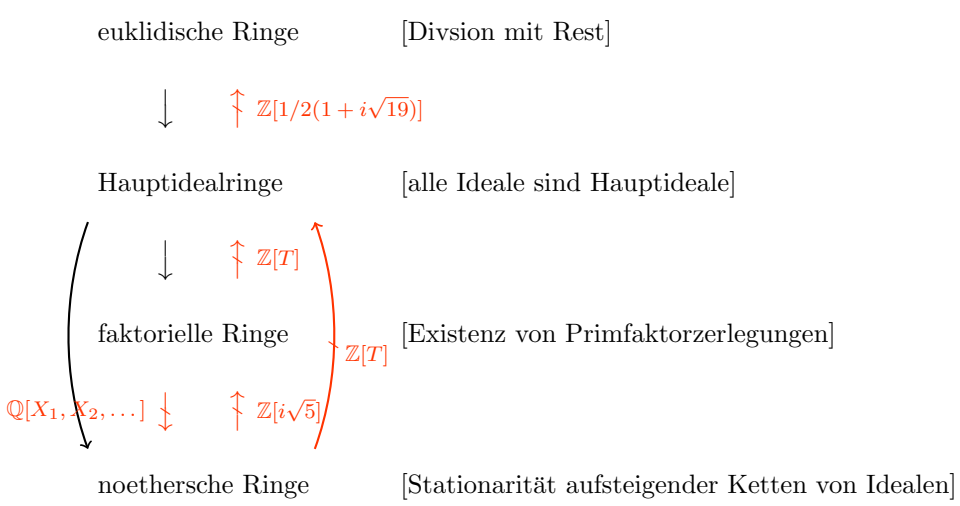


Abbildung 2.3.: Eigenschaften von Ringen

2.2.6 Irreduzibilitätskriterien

Ist K ein Körper, so wissen wir bereits folgendes: Ist $f \in K[T]$ irreduzibel, so ist f prim in $K[T]$ (Proposition 2.2.11), und damit ist (f) sogar ein maximales Ideal des Hauptidealrings $K[T]$ (Beispiel 2.2.14). Insbesondere ist der Restklassenring

$$K[T]/(f)$$

ein Körper (Satz 2.2.15). Irreduzible Polynome in Polynomringen über Körpern liefern also eine Möglichkeit, Körper zu konstruieren. Bei geschickter Wahl der Polynome erhält man auf diese Weise interessante Körper.

Beispiel 2.2.55 (komplexe Zahlen)**.** Das Polynom $T^2+1 \in \mathbb{R}[T]$ ist irreduzibel in $\mathbb{R}[T]$ (nachrechnen); also ist $\mathbb{R}[T]/(T^2+1)$ ein Körper (siehe oben). Genauer gilt: Mit der universellen Eigenschaft von Polynom- bzw. Restklassenringen folgt, dass

$$\begin{aligned} \mathbb{R}[T]/(T^2+1) &\longrightarrow \mathbb{C} \\ [\mathbb{R} \ni x] &\longmapsto x \\ [T] &\longmapsto i \end{aligned}$$

ein Ringisomorphismus ist (Übungsaufgabe). Man kann die imaginäre Einheit i auf diese Weise also durch eine einfache algebraische Konstruktion ge-

winnen. Analog erhält man so den Körper $\mathbb{F}_7[T]/(T^2+1)$ mit 49 Elementen (Übungsaufgabe).

Beispiel 2.2.56 (eine Wurzel aus 2)**.** Das Polynom $T^2-2 \in \mathbb{Q}[T]$ ist irreduzibel in $\mathbb{Q}[T]$ (nachrechnen); also ist $\mathbb{Q}[T]/(T^2-2)$ ein Körper (siehe oben). In diesem Körper gilt

$$[T]^2 = [T^2] = [T^2 - 2 + 2] = [2] = 2 \cdot [1].$$

Also enthält dieser Körper $\mathbb{Q}[T]/(T^2-2)$ ein „Wurzel" aus 2. Man beachte dabei, dass wir diese Wurzel mit algebraischen Mitteln (nicht mit analytischen) konstruiert haben.

Daher ist es nützlich, Kriterien zu kennen, die zeigen, dass gewisse Polynome irreduzibel sind. Wir behandeln die folgenden Kriterien und geben Standardbeispiele dazu:

- das Nullstellenkriterium
- das Reduktionskriterium
- das Eisensteinsche Irreduzibilitätskriterium

Proposition 2.2.57 (Nullstellenkriterium)**.** *Sei K ein Körper und $f \in K[T]$.*

1. *Ist $x \in K$ mit $f(x) = 0$, so ist $T - x$ in $K[T]$ ein Teiler von f.*

   Insbesondere: Ist $\deg f > 1$ und hat f eine Nullstelle in K, so ist f nicht irreduzibel in $K[T]$; genauer: Es gibt $g, h \in K[T]$ mit

   $$f = g \cdot h \quad \textit{und} \quad \deg g \geq 1, \quad \deg h \geq 1.$$

2. *Gilt*

   $$\deg f \in \{2, 3\} \quad \textit{und} \quad \forall_{x \in K} \quad f(x) \neq 0,$$

   so ist f in $K[T]$ irreduzibel (und prim).

Beweis. Zu 1. Dies folgt mithilfe von Division mit Rest in $K[T]$ von f durch $T - x$ (Polynomdivision; Proposition II.2.4.14).

Zu 2. Sei $\deg f \in \{2, 3\}$. Wir beweisen die Behauptung durch Kontraposition:

Sei f nicht irreduzibel in $K[T]$. Wegen $\deg f > 0$ ist $f \notin \{0\} \cup K[T]^\times$; also existieren $g, h \in K[T]$ mit

$$f = g \cdot h \quad \text{und} \quad g, h \notin \{0\} \cup K[T]^\times.$$

Insbesondere ist $\deg g > 0$ und $\deg h > 0$. Wegen

$$\deg g + \deg h = \deg(g \cdot h) = \deg f \in \{2, 3\}$$

folgt $\deg g = 1$ oder $\deg h = 1$; ohne Einschränkung sei $\deg g = 1$. Somit gibt es $a \in K \setminus \{0\}$ und $b \in K$ mit $g = a \cdot T + b$. Dann folgt

$$f\Big(-\frac{b}{a}\Big) = g\Big(-\frac{b}{a}\Big) \cdot h\Big(-\frac{b}{a}\Big) = 0 \cdot h\Big(-\frac{b}{a}\Big) = 0. \qquad \square$$

Korollar 2.2.58. *Sei K ein Körper und $f \in K[T] \setminus \{0\}$. Dann hat f höchstens $\deg f$ Nullstellen in K.*

Beweis. Ist $N \subset K$ eine endliche Menge von Nullstellen von f, so folgt induktiv aus Proposition 2.2.57, dass $\prod_{x \in N}(T - x)$ ein Teiler von f ist. Insbesondere ist $\#N \leq \deg f$. $\square$

Das Nullstellenkriterium eignet sich gut für Polynome niedrigen Grades und kann oft mit dem Reduktionskriterium kombiniert werden.

Satz 2.2.59 (Reduktionskriterium)**.** *Sei R ein faktorieller Ring, sei $p \in R$ prim und sei $\pi\colon R[T] \longrightarrow (R/(p))[T]$ der von der kanonischen Projektion $R \longrightarrow R/(p)$ induzierte Ringhomomorphismus. Sei $f \in R[T]$ mit $\deg f > 0$ und p sei* kein *Teiler des höchsten Koeffizienten von f. Dann gilt:*

1. *Ist f primitiv und ist $\pi(f)$ in $R/(p)[T]$ irreduzibel, so ist f in $R[T]$ irreduzibel (und prim).*
2. *Ist $\pi(f)$ in $R/(p)[T]$ irreduzibel, so ist f in $Q(R)[T]$ irreduzibel (und prim).*

Beweis. Zu 1. Wir beweisen die Aussage per Kontraposition: Sei f primitiv und nicht irreduzibel in $R[T]$. Dann ist $\pi(f)$ nicht irreduzibel in $R/(p)[T]$, denn: Da f in $R[T]$ nicht irreduzibel ist und $\deg f > 0$ ist, gibt es $g, h \in R[T]$ mit $f = g \cdot h$ und $g, h \notin R[T]^\times$. Also ist

$$\pi(f) = \pi(g \cdot h) = \pi(g) \cdot \pi(h).$$

Wir zeigen, dass $\pi(g)$ und $\pi(h)$ keine Einheiten in $R/(p)[T]$ sind: Da f primitiv ist, folgt $\deg g > 0$ und $\deg h > 0$; da p nicht den höchsten Koeffizienten von f teilt, ist außerdem $\deg \pi(f) = \deg f$. Also erhalten wir (da R und $R/(p)$ Integritätsringe sind, sind die Grade auf den zugehörigen Polynomringen additiv; Beweis von Proposition 2.1.14)

$$\begin{aligned} \deg g + \deg h &= \deg f \\ &= \deg \pi(f) \\ &= \deg\big(\pi(g) \cdot \pi(h)\big) \\ &= \deg \pi(g) + \deg \pi(h) \\ &\leq \deg g + \deg h, \end{aligned}$$

und damit $\deg \pi(g) = \deg g > 0$ und $\deg \pi(h) = \deg h > 0$. Somit ist $\pi(f)$ nicht irreduzibel in $R/(p)[T]$.

Zu 2. Wir schreiben

$$f = c \cdot g$$

mit $c \in R$ und einem primitiven Polynom $g \in R[T]$ (indem wir den größten gemeinsamen Teiler der Koeffizienten von f herausziehen). Ist $\pi(f)$ irreduzibel in $R/(p)[T]$, so ist $\pi(g)$ erst recht irreduzibel. Nach dem ersten Teil ist dann das primitive Polynom g in $R[T]$ irreduzibel. Mit Korollar 2.2.54 ist somit g auch in $Q(R)[T]$ irreduzibel. Da c in $Q(R)$ eine Einheit ist, ist daher f in $Q(R)[T]$ irreduzibel. □

Beispiel 2.2.60 (Reduktionskriterium, in Kombination mit dem Nullstellkriterium)**.**

- Das Polynom
$$f := T^2 + 5555 \cdot T - 2027 \in \mathbb{Z}[T]$$
ist irreduzibel in $\mathbb{Z}[T]$ (und $\mathbb{Q}[T]$), denn: Reduktion modulo $5 \in \mathbb{Z}$ liefert das Polynom
$$? \quad T^2 - [2] \in \mathbb{F}_5[T],$$
welches nach dem Nullstellenkriterium (Proposition 2.2.57) in $\mathbb{F}_5[T]$ irreduzibel ist (nachrechnen). Das Reduktionskriterium (Satz 2.2.59; anwendbar!) liefert, dass f in $\mathbb{Z}[T]$ und $\mathbb{Q}[T]$ irreduzibel ist.

  Wie kommt man darauf, Reduktion modulo 5 zu betrachten? Das Polynom hat einen niedrigen Grad, daher ist es verlockend, das Nullstellenkriterium auf eine geeignete Reduktion auf einen endlichen Körper der Form $\mathbb{F}_p = \mathbb{Z}/(p)$ anzuwenden. Wie wählt man p ? Die Primzahl darf kein Teiler des konstanten Anteils sein (denn sonst ist das reduzierte Polynom durch T teilbar ...); andererseits sollte die Primzahl so gewählt sein, dass sich die Koeffizienten geeignet vereinfachen. Daher ist es in dem obigen Fall naheliegend, einen Teiler von 5555 auszuprobieren, zum Beispiel 5.

- Das Polynom
$$f := X^6 \cdot Y^2 + Y^2 - X^2 + 1 \in \mathbb{R}[X, Y]$$
ist irreduzibel in $\mathbb{R}[X, Y]$, denn: Wir fassen f als Polynom in $(\mathbb{R}[X])[Y]$ auf und wenden Reduktion modulo $X \in \mathbb{R}[X]$ (dies ist ein Primelement) an. Dadurch erhalten wir das Polynom
$$? \quad Y^2 + 1 \in \big(\mathbb{R}[X]/(X)\big)[Y] \cong_{\mathsf{Ring}} \mathbb{R}[Y],$$
welches nach dem Nullstellenkriterium (Proposition 2.2.57) in $\mathbb{R}[Y]$ irreduzibel ist (nachrechnen). Das Reduktionskriterium (Satz 2.2.59; anwendbar!) liefert, dass f in $\mathbb{R}[X, Y]$ irreduzibel ist.

Satz 2.2.61 (Eisensteinsches Irreduzibilitätskriterium)**.** *Sei R ein faktorieller Ring, sei $p \in R$ prim und sei $f = \sum_{j=0}^{n} a_j \cdot T^j \in R[T]$ mit $n \in \mathbb{N}$ und $a_0, \ldots, a_n \in R$. Dabei gelte:*

- *Das Polynom f ist primitiv und $n = \deg f > 0$.*
- *Es gelte*

$$p \nmid a_n \quad \textit{und} \quad \forall_{j \in \{0,\ldots,n-1\}} \quad p \mid a_j \quad \textit{und} \quad p^2 \nmid a_0.$$

Dann ist f in $R[T]$ und $Q(R)[T]$ irreduzibel.

Beweis. Man kann dies auf das Reduktionskriterium (Satz 2.2.59) zurückführen [6, S. 62] oder die Behauptung von Hand nachrechnen. Wir werden letzteres durchführen: Es genügt zu zeigen, dass f in $R[T]$ irreduzibel ist (Korollar 2.2.54).

Seien $g = \sum_{j=0}^{r} b_j \cdot T^j$, $h = \sum_{j=0}^{s} c_j \cdot T^j \in R[T]$ mit $f = g \cdot h$ sowie $b_r \neq 0$ und $c_s \neq 0$. Der Einfachheit halber schreiben wir $b_j = 0$ für $j \in \mathbb{N}_{>r}$ und $c_j = 0$ für $j \in \mathbb{N}_{>s}$. Wegen

$$\sum_{j=0}^{n} a_j \cdot T^j = f = g \cdot h = \sum_{j=0}^{n} \left(\sum_{k=0}^{j} b_k \cdot c_{j-k} \right) \cdot T^j$$

und den Voraussetzungen an die Koeffizienten von f erhalten wir

$$p \mid b_0 \cdot c_0, \quad p^2 \nmid b_0 \cdot c_0, \quad p \nmid b_r \cdot c_s.$$

Da p prim ist, folgt $p \mid b_0$ oder $p \mid c_0$; ohne Einschränkung gelte $p \mid b_0$. Wegen $p^2 \nmid b_0 \cdot c_0$ folgt $p \nmid c_0$. Sei nun $j \in \mathbb{N}$ so gewählt, dass $p \mid b_k$ für alle $k \in \{0, \ldots, j\}$ und $p \nmid b_{j+1}$ gilt (ein solcher Index existiert wegen $p \mid b_0$ und $p \nmid b_r$). Dann folgt

$$a_{j+1} = \sum_{k=0}^{j} b_k \cdot c_{j+1-k} + b_{j+1} \cdot c_0.$$

Nach Wahl von j ist somit p *kein* Teiler von a_{j+1}. Die Voraussetzungen an die Koeffizienten von f liefern daher $j + 1 = n$. Wegen $b_{j+1} \neq 0$ (da p kein Teiler von b_{j+1} ist) erhalten wir die Ungleichungskette

$$n = j + 1 \leq r \leq r + s = n,$$

und damit $s = 0$. Wegen $p \nmid c_0$ ist $h = c_0 \in R \setminus \{0\}$. Da f primitiv ist, ist h eine Einheit in R bzw. $R[T]$. Also ist f in $R[T]$ irreduzibel. □

Beispiel 2.2.62 (Eisenstein)**.**

- Die Polynome $T^3 - 2$ und $T^{2025} - 2$ sind irreduzibel in $\mathbb{Q}[T]$; dies folgt, indem wir das Eisensteinsche Irreduzibilitätskriterium auf das Primelement $2 \in \mathbb{Z}$ anwenden.

  Alternativ kann man für $T^3 - 2$ zum Beispiel auch das Reduktionskriterium auf die Reduktion modulo 7 anwenden, denn $2 \in \mathbb{F}_7$ ist *keine* dritte Potenz (nachrechnen).

- Sei $p \in \mathbb{N}$ prim. Dann ist

  $$f := T^{p-1} + \cdots + T + 1 \in \mathbb{Q}[T]$$

  irreduzibel in $\mathbb{Q}[T]$, denn: Wir betrachten stattdessen

  $$g := f(T+1) \in \mathbb{Q}[T]$$

  und zeigen, dass g in $\mathbb{Q}[T]$ irreduzibel ist: Im rationalen Funktionenring $\mathbb{Q}(T)$ gilt $f = (T^p - 1)/(T - 1)$, und damit (da sich die Substitution auf $\mathbb{Q}(T)$ fortsetzt)

  $$\begin{aligned} g &= \frac{(T+1)^p - 1}{T + 1 - 1} \\ &= \frac{1}{T} \cdot \left(\sum_{j=0}^{p} \binom{p}{j} \cdot T^j - 1 \right) \\ &= T^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} \cdot T^{j-1} + \binom{p}{1} \\ &= T^{p-1} + \sum_{j=1}^{p-1} p \cdot \frac{(p-1)!}{j! \cdot (p-j)!} \cdot T^{j-1} + p. \end{aligned}$$

  Dieses Polynom erfüllt die Voraussetzungen des Eisensteinschen Irreduzibilitätskriteriums (Satz 2.2.61) für das Primelement $p \in \mathbb{Z}$ (nachrechnen). Also ist g in $\mathbb{Q}[T]$ irreduzibel.

  Der Isomorphismus

  $$\begin{aligned} \mathbb{Q}[T] &\longrightarrow \mathbb{Q}[T] \\ 1 &\longmapsto 1 \\ T &\longmapsto T + 1 \end{aligned}$$

  zeigt, dass auch f in $\mathbb{Q}[T]$ irreduzibel ist.

Anmerkung für Lehramtsstudenten. Irreduzibilitätsprobleme gehören zu den kanonischen Staatsexamensaufgaben. Im Normalfall sind die obigen drei Kriterien und ein paar Standardtricks ausreichend, um diese Aufgaben ohne

Schwierigkeiten zu lösen. Wie bei den Sylowsätzen ist aber auch hier eine gewisse Routine nötig. Daher hilft nur üben, üben, üben ...

Man beachte, dass das Nullstellenkriterium, das Reduktionskriterium und das Eisensteinsche Irreduzibilitätskriterium jeweils nur *hinreichende* Kriterien sind. Es gibt also im allgemeinen irreduzible Polynome, auf die keines dieser Kriterien anwendbar ist!

3

Körper

Körper sind Ringe mit vielen multiplikativen Einheiten und sind zum Beispiel dafür geeignet, Konstruierbarkeitsprobleme mit Zirkel und Lineal oder die Auflösung von polynomialen Gleichungen durch Radikale zu modellieren. In diesem Kontext ist es nützlich, nicht nur einzelne Körper, sondern Körpererweiterungen zu betrachten. Wir werden zunächst die Grundlagen über Körper und Körpererweiterungen kennenlernen und einige Konstruktionsprinzipien für Körper studieren. Insbesondere werden wir dabei die endlichen Körper klassifizieren.

Wir werden uns dann auf eine besonders gutartige Klasse von Körpererweiterungen konzentrieren, die sogenannten Galoiserweiterungen. Ein zentrales Hilfsmittel bei der Untersuchung und Klassifikation von Galoiserweiterungen ist die Galoisgruppe. Insbesondere wird uns die Theorie der endlichen Gruppen dabei helfen, Konstruierbarkeitsprobleme mit Zirkel und Lineal und die Auflösung von polynomialen Gleichungen durch Radikale besser zu verstehen.

Überblick über dieses Kapitel.

3.1	Die Kategorie der Körper	130
3.2	Die Kategorie der Körpererweiterungen	133
3.3	Endliche Körper	160
3.4	Galoiserweiterungen	163
3.5	Anwendungen der Galoistheorie	178

Schlüsselbeispiel. Teilkörper von $\mathbb{C}$, endliche Körper

3.1 Die Kategorie der Körper

3.1.1 Körper und Körperhomomorphismen

Wir wiederholen den Begriff des Körpers, führen die Charakteristik von Körpern ein und beschäftigen uns kurz mit Körperhomomorphismen.

Definition 3.1.1 (Körper)**.** Ein *Körper* ist ein Ring K (im Sinne von Definition 2.1.1) mit $1 \neq 0$, für den $K \setminus \{0\}$ die Einheitengruppe ist.

Beispiel 3.1.2 (der Körper der konstruierbaren Punkte)**.** Eine klassische Frage in der Geometrie ist es, welche geometrischen Objekte bzw. welche Punkte in der Ebene sich mit Zirkel und Lineal konstruieren lassen. Für die Beantwortung dieser Frage ist die folgende Beobachtung zentral:

Sei ZL die Menge aller Punkte in $\mathbb{C}$, die mit Zirkel und Lineal aus $\{0, 1\}$ konstruiert werden können. Dann ist ZL ein Körper (Anhang A.7).

Definition 3.1.3 (Körperhomomorphismus)**.** Ein *Körperhomomorphismus* ist ein Ringhomomorphismus zwischen Körpern.

Proposition 3.1.4 (Charakteristik eines Körpers)**.** *Sei K ein Körper. Dann gibt es einen eindeutigen Ringhomomorphismus $f\colon \mathbb{Z} \longrightarrow K$ und es gilt:*

1. *Entweder ist f injektiv (in diesem Fall sagen wir, dass K* Charakteristik 0 *hat,* $\operatorname{char} K := 0$*),*
2. *oder es gibt eine (eindeutige) Primzahl $p \in \mathbb{N}$ mit $\ker f = (p) \subset \mathbb{Z}$ (in diesem Fall sagen wir, dass K* Charakteristik p *hat,* $\operatorname{char} K := p$*).*

Beweis. Da K als Körper nullteilerfrei ist und $0 \neq 1$ gilt, ist $\operatorname{im} f \subset K$ ein Integritätsring. Wegen $\mathbb{Z}/\ker f \cong \operatorname{im} f$ ist $\ker f$ somit ein Primideal in $\mathbb{Z}$ (Satz 2.2.15). Also ist entweder $\ker f = \{0\}$ oder es gibt ein (eindeutig bestimmtes) Primelement $p \in \mathbb{N}$ mit $\ker f = (p) \subset \mathbb{Z}$. □

Anschaulich gesprochen gibt die Charakteristik eines Körpers also an, ob/wie man durch Aufaddieren der Eins die Null erhalten kann.

Korollar 3.1.5 (Primkörper)**.** *Sei K ein Körper.*

1. *Dann enthält K genau einen bezüglich Inklusion kleinsten Körper, den* Primkörper von K*.*
2. *Es gilt:*
   - *Ist* $\operatorname{char} K = 0$*, so ist der Primkörper von K isomorph zu $\mathbb{Q}$.*

- *Ist $p \in \mathbb{N}$ prim und $\operatorname{char} K = p$, so ist der Primkörper von K isomorph zu $\mathbb{F}_p$.*

Beweis. Für den ersten Teil ist es günstig, den Durchschnitt über alle Körper in K anzusehen (Übungsaufgabe). Für den zweiten Teil kann man den kanonischen Ringhomomorphismus $\mathbb{Z} \longrightarrow K$ betrachten (Übungsaufgabe). □

Die Standardbeispiele für Körper, die wir bereits in der Linearen Algebra, in der Analysis und in der Algebra kennengelernt haben, sind:

Beispiel 3.1.6 (Körper)**.**

- Die rationalen Zahlen bilden den Körper $\mathbb{Q}$.

  Dieser Körper hat Charakteristik ? 0.

- Die reellen Zahlen bilden den Körper $\mathbb{R}$.

  Dieser Körper hat Charakteristik ? 0.

- Die komplexen Zahlen bilden den Körper $\mathbb{C}$.

  Dieser Körper hat Charakteristik ? 0.

- Ist $p \in \mathbb{N}$ prim, so ist $\mathbb{F}_p = \mathbb{Z}/(p)$ ein Körper.

  Dieser Körper hat Charakteristik ? p.

- Der Restklassenring $\mathbb{F}_7[T]/(T^2+1)$ ist ein Körper (Beispiel 2.2.55).

  Dieser Körper hat Charakteristik ? 7.

- Ist K ein Körper, so ist $K(T)$ ein Körper.

  Dieser Körper hat Charakteristik ? $\operatorname{char} K$.

Caveat 3.1.7 (Charakteristik vs. Endlichkeit)**.** Körper positiver Charakteristik sind im allgemeinen *nicht* endlich: Zum Beispiel ist der Funktionenkörper $\mathbb{F}_2(T)$ ein Körper der Charakteristik 2, der den unendlichen Ring $\mathbb{F}_2[T]$ enthält (Beispiel 2.1.19).

Die Ringtheorie ermöglicht es, mithilfe von Polynomen aus Körpern weitere Körper zu konstruieren (Beispiele 2.2.55, 2.2.56). Bei geeigneter Wahl der Polynome erhält man auf diese Weise interessante Beispiele von Körpern. Die systematische Konstruktion von Körpern werden wir in Kapitel 3.2 genauer behandeln.

Proposition 3.1.8 (Injektivität von Körperhomomorphismen)**.** *Jeder Körperhomomorphismus ist injektiv.*

Beweis. Seien K und L Körper und sei $f\colon K \longrightarrow L$ ein Ringhomomorphismus. Dann ist $\ker f$ ein Ideal in K. Da K ein Körper ist, folgt $\ker f = \{0\}$ oder $\ker f = K$ (Proposition 2.1.25). Wegen $f(1) = 1 \neq 0$ ist $\ker f \neq K$. Also bleibt nur die Möglichkeit, dass $\ker f = \{0\}$ ist. Somit ist f injektiv. □

Das Studium von Körperhomomorphismen entspricht also dem Studium von Einbettungen bzw. von Automorphismen. Die Sprache der Körpererweiterungen ist dafür der richtige Rahmen.

3.1.2 Die Einheitengruppe eines Körpers

Zum Abschluss der allgemeinen Einführung in die Körpertheorie betrachten wir die Einheitengruppen von Körpern etwas genauer:

Satz 3.1.9. *Sei K ein Körper und $G \subset K^\times$ eine endliche Untergruppe der Einheitengruppe von K. Dann ist G zyklisch.*

Beweis. Sei $n := \#G$ und sei

$$G \cong_{\mathsf{Group}} \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_k^{n_k}$$

mit $k \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_k \in \mathbb{N}$ und $n_1, \ldots, n_k \in \mathbb{N}_{>0}$ die Zerlegung in zyklische Gruppen aus dem Klassifikationssatz für endliche abelsche Gruppen (Satz 1.3.1). Sei $m \in \mathbb{N}$ das kleinste gemeinsame Vielfache von $p_1^{n_1}, \ldots, p_k^{n_k}$; insbesondere ist $m \leq n$ und es genügt (nach einer iterativen Anwendung des Chinesischen Restsatzes 2.2.23) zu zeigen, dass $m = n$ ist.

Wir betrachten dazu das Polynom

$$f := T^m - 1 \in K[T].$$

Nach Wahl von m gilt dann in K (nachrechnen)

$$\forall_{g \in G} \quad f(g) = g^m - 1 = 1 - 1 = 0.$$

Da das Polynom f vom Grad m höchstens m Nullstellen in K besitzt (Korollar 2.2.58), folgt $n \leq m$. Insgesamt erhalten wir daher $m = n$, wie gewünscht.

Man kann diesen Satz auch beweisen, ohne den Klassifikationssatz für endliche abelsche Gruppen zu verwenden [6, Kapitel 3.6]. □

Im Kontext von Einheitswurzeln und Kreisteilungskörpern wird dieser Satz hilfreich sein (Beispiel 3.2.27).

Korollar 3.1.10 (Einheitengruppen endlicher Körper)**.** *Ist K ein endlicher Körper, so ist die Gruppe $K^\times$ zyklisch (und damit isomorph zu $\mathbb{Z}/(\#K - 1)$).*

Beweis. Dies folgt direkt aus dem Satz über endliche Untergruppen der Einheitengruppe von Körpern (Satz 3.1.9) und der Klassifikation zyklischer Gruppen (Korollar 1.1.58). □

Diese Tatsache wird bei der Konstruktion von linear feedback shift registers und bei der Umsetzung von RAID(6) genutzt (Beispiel A.8.2, A.8.3)

3.2 Die Kategorie der Körpererweiterungen

Körpererweiterungen beschreiben das Verhältnis zweier Körper zueinander. Wir geben eine kurze Einführung in die Grundbegriffe für Körpererweiterungen und beschäftigen uns dann mit algebraischen Körpererweiterungen.

3.2.1 Körpererweiterungen

Definition 3.2.1 (Körpererweiterung, Zwischenkörper)**.** Sei K ein Körper.

- Eine *Körpererweiterung von* K ist ein Körper L mit $K \subset L$. Wir schreiben in diesem Fall auch „$L \mid K$“ für die Körpererweiterung L über K.
- Ist $L \mid K$ eine Körpererweiterung von K, so bezeichnet man einen Körper M als *Zwischenkörper der Körperweiterung* $L \mid K$, wenn $K \subset M$ und $M \subset L$ gilt.

Bemerkung 3.2.2 (Notationen für Körpererweiterungen)**.** Ist $L \mid K$ eine Körpererweiterung, so findet man in der Literatur auch die Notation L/K (was aber leicht zu Verwechslungen mit Quotientenkonstruktionen führen kann) bzw. $L \supset K$. Anschaulich und hilfreich (aber platzverschwendend) ist die Notation

$$\begin{array}{c} L \\ | \\ K \end{array}$$

Ist M ein Zwischenkörper von $L \mid K$, so entspricht dies einem Diagramm der Form

$$\begin{array}{c} L \\ | \\ M \\ | \\ K \end{array}$$

Da Körperhomomorphismen grundsätzlich injektiv sind (Proposition 3.1.8), sind Körpererweiterungen im wesentlichen nichts anderes als Körperhomomorphismen. Man schreibt daher für Körpererweiterungen $L \mid K$ manchmal auch $K \longrightarrow L$ oder $K \hookrightarrow L$. Diese Perspektive ist insbesondere dann nützlich, wenn man die Theorie der Erweiterungen auf andere Kategorien übertragen möchte.

Beispiel 3.2.3 (Körpererweiterungen)**.**

- Es sind $\mathbb{C} \mid \mathbb{C}$, $\mathbb{C} \mid \mathbb{R}$, $\mathbb{C} \mid \mathbb{Q}$ und $\mathbb{R} \mid \mathbb{Q}$ Körpererweiterungen; außerdem ist $\mathbb{R}$ ein Zwischenkörper von $\mathbb{C} \mid \mathbb{R}$ und $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{R}$ sind Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$.
- Es ist $\mathrm{ZL} \mid \mathbb{Q}$ eine Körpererweiterung von $\mathbb{Q}$.
- Ist K ein Körper, so liefert die kanonische Inklusion $K \longrightarrow K(T)$ eine Körpererweiterung $K(T) \mid K$.
- Jeder Körper liefert eine Körpererweiterung über seinem Primkörper.

Um weitere Beispiele effizient beschreiben zu können, ist es nützlich, über erzeugte Zwischenkörper zu sprechen.

Definition 3.2.4 (erzeugter Zwischenkörper, Kompositum)**.** Sei $L \mid K$ eine Körpererweiterung.

- Ist $S \subset L$, so ist
$$K(S) := \bigcap_{M \in Z_S(L|K)} M$$
der *von S erzeugte Zwischenkörper von $L \mid K$*. Dabei ist $Z_S(L \mid K)$ die Menge aller Zwischenkörper M von $L \mid K$ mit $S \subset M$. Man sagt in diesem Fall auch, dass $K(S)$ *durch Adjunktion von S in $L \mid K$ zu K* entsteht.
- Sind M und N Zwischenkörper von $L \mid K$, so bezeichnet man
$$M \cdot N := K(M \cup N)$$
als *Kompositum von M und N in $L \mid K$*.

Man beachte, dass Durchschnitte von Körpern Körper sind und dass die Menge $Z_S(L \mid K)$ in der obigen Definition nicht-leer ist (da sie L enthält). Daher ist $K(S)$ ein Zwischenkörper von $L \mid K$, und zwar der bezüglich Inklusion kleinste, der S enthält.

Caveat 3.2.5 (umgebende Körper)**.** Sowohl für erzeugte Zwischenkörper als auch für Komposita ist es zwingend notwendig, die umgebende Körpererweiterung zu spezifizieren. Die allgemein gebräuchliche Notation (wie auch in der obigen Definition verwendet) verschweigt dies leider. Es ist daher im Umgang mit diesen Konstruktionen immer besondere Vorsicht geboten.

Bemerkung 3.2.6 (explizite Beschreibung erzeugter Zwischenkörper)**.** Es sei $L \mid K$ eine Körpererweiterung und sei $\alpha \in L$. Dann kann der von α erzeugte Zwischenkörper $K(\alpha)$ von $L \mid K$ expliziter auch wie folgt beschrieben werden: Wir betrachten den Einsetzungshomomorphismus

$$\begin{aligned} E_\alpha \colon K[T] &\longrightarrow L \\ f &\longmapsto f(\alpha); \end{aligned}$$

insbesondere ist $\operatorname{im} E_\alpha \subset K(\alpha)$. Es können die folgenden Fälle eintreten:

- Der Homomorphismus E_α ist injektiv. Dann induziert E_α einen wohldefinierten Körperhomomorphismus

  $$\overline{E}_\alpha \colon K(T) \longrightarrow L$$

  (Bemerkung 2.1.20) und es gilt $\operatorname{im} \overline{E}_\alpha = K(\alpha)$ (nachrechnen). In diesem Fall besteht also $K(\alpha)$ aus allen Brüchen von polynomialen Ausdrücken in α über K (wobei der Nenner nicht Null ist).

- Der Homomorphismus E_α ist *nicht* injektiv. Dann ist das Ideal $a := \ker E_\alpha \subset K[T]$ ein Primideal (da $\operatorname{im} E_\alpha \cong_{\mathsf{Ring}} K[T]/\ker E_\alpha$ als Unterring des Körpers L ein Integritätsring ist; Satz 2.2.15) und a ist nicht das Nullideal.

  Da $K[T]$ ein Hauptidealring ist, ist a bereits maximal (Beispiel 2.2.14); also ist $\operatorname{im} E_\alpha \cong_{\mathsf{Ring}} K[T]/a$ ein Körper (Satz 2.2.15). Wegen $\alpha \in \operatorname{im} E_\alpha \subset K(\alpha)$ folgt somit

  $$K(\alpha) = \operatorname{im} E_\alpha \cong_{\mathsf{Ring}} K[T]/\ker E_\alpha.$$

  In diesem Fall besteht also $K(\alpha)$ aus allen polynomialen Ausdrücken in α über K. Daher stimmt $K(\alpha)$ in diesem Fall mit dem von α und K erzeugten Unterring $K[\alpha]$ von L überein.

Analog kann man diese Beschreibung auch auf größere Mengen von adjungierten Elementen verallgemeinern (mithilfe von Polynomringen bzw. rationalen Funktionenkörpern in entsprechend vielen Variablen).

Beispiel 3.2.7 (erzeugte Zwischenkörper)**.** Wir betrachten die Körpererweiterung $\mathbb{C} \mid \mathbb{Q}$. Dann ist (jeweils in $\mathbb{C} \mid \mathbb{Q}$)

$$\mathbb{Q}(\sqrt{2}) = \{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\}$$

(nachrechnen) und

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

(nachrechnen) aber (wie wir in Beispiel 3.2.26 sehen werden)

$$\mathbb{Q}(\sqrt[3]{2}) \neq \{a + b \cdot \sqrt[3]{2} \mid a, b \in \mathbb{Q}\}.$$

Einer der Grundgedanken der algebraischen Zahlentheorie ist es, dass sich die algebraischen Eigenschaften von Zahlen α in $\mathbb{C}$ (relativ zu $\mathbb{Q}$) in der zugehörigen Körpererweiterung $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ widerspiegeln.

Eine erste Möglichkeit, die Komplexität einer Körpererweiterung zu messen, ist der Grad. Dabei verwendet man die folgende Tatsache: Ist $L \mid K$ eine Körpererweiterung, so ist L bezüglich der Multiplikation mit Elementen aus K insbesondere ein K-Vektorraum und besitzt somit eine Dimension über K.

Definition 3.2.8 (Grad, endliche Körpererweiterung)**.** Sei $L \mid K$ eine Körpererweiterung.

- Der *Grad von* $L \mid K$ ist definiert als
$$[L : K] := \dim_K L \in \mathbb{N}_{\geq 1} \cup \{\infty\}.$$
- Ist $[L : K]$ endlich, so ist $L \mid K$ eine *endliche* Körpererweiterung; ist $[L : K]$ unendlich, so ist $L \mid K$ eine *unendliche* Körpererweiterung.

Beispiel 3.2.9 (Grad von Körpererweiterungen)**.**

- Es ist
$$[\mathbb{C} : \mathbb{R}] = ? \quad 2,$$
$$[\mathbb{C} : \mathbb{Q}] = ? \quad \infty,$$
$$[\mathbb{Q}(i) : \mathbb{Q}] = ? \quad 2.$$
- Ist K ein Körper, so ist $[K(T) : K] = ?$ ∞ und $[K : K] = ?$ 1.

Analog zum Index von Untergruppen in der Gruppentheorie erhalten wir:

Proposition 3.2.10 (Multiplikativität des Grads)**.** *Sei $L \mid K$ eine Körpererweiterung und sei M ein Zwischenkörper von $L \mid K$. Dann gilt*
$$[L : K] = [L : M] \cdot [M : K].$$

Beweis. Sei $(b_i)_{i \in I}$ eine K-Basis von M und sei $(c_j)_{j \in J}$ eine M-Basis von L. Dann ist die Familie $(b_i \cdot c_j)_{(i,j) \in I \times J}$ in L linear unabhängig (über K) und erzeugend (über K) (jeweils nachrechnen), und damit eine K-Basis von L. Also ist
$$\begin{aligned}[L : K] &= \dim_K L = \#(I \times J) = \#I \cdot \#J = \dim_K M \cdot \dim_M L \\ &= [L : M] \cdot [M : K].\end{aligned}$$
□

Bemerkung 3.2.11 (endliche Körpererweiterungen sind endlich erzeugt)**.** Sei $L \mid K$ eine endliche Körpererweiterung (d.h. $\dim_K L < \infty$). Dann ist $L \mid K$ auch *endlich erzeugt*, d.h. es gibt eine endliche Menge $S \subset L$ mit $L = K(S)$, denn: Da $L \mid K$ endlich ist, gibt es eine endliches Erzeugendensystem $S \subset L$ von L als K-Vektorraum. Wegen

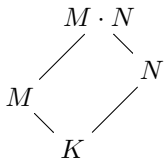


Abbildung 3.1.: Der Diamant des Kompositums $M \cdot N$ in $L \mid K$

$$L = \operatorname{Span}_K S \subset K(S) \subset L$$

folgt bereits $L = K(S)$.

Proposition 3.2.12 (Grade von Komposita)**.** *Sei $L \mid K$ eine Körpererweiterung und seien M, N Zwischenkörper von $L \mid K$.*

1. *Dann ist $[M \cdot N : M] \leq [N : K]$ und somit*

$$[M \cdot N : K] \leq [M : K] \cdot [N : K].$$

2. *Ist $\operatorname{ggT}\big([M : K], [N : K]\big) = 1$, so ist*

$$[M \cdot N : K] = [M : K] \cdot [N : K].$$

Beweis. Zu 1. Ist $[N : K] = \infty$, so ist nichts zu zeigen. Ist $N \mid K$ endlich, so ist $N \mid K$ endlich erzeugt (Bemerkung 3.2.11). Induktiv erhält man dann mithilfe von Bemerkung 3.2.6 die Ungleichung $[M \cdot N : M] \leq [N : K]$ (Übungsaufgabe). Die zweite Ungleichung ergibt sich daraus mit der Multiplikativität des Grades (Proposition 3.2.10).

Zu 2. Der zweite Teil folgt aus dem ersten Teil, indem man den Diamanten aus Abbildung 3.1 betrachtet (Übungsaufgabe). □

Caveat 3.2.13 (Grade von Komposita)**.** Sei $L \mid K$ eine Körpererweiterung und seien M, N Zwischenkörper von $L \mid K$. Im allgemeinen gilt

$$[M \cdot N : K] \neq [M : K] \cdot [N : K],$$

wie man leicht an dem Beispiel

$$[\mathbb{C} \cdot \mathbb{C} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2 \neq 4 = [\mathbb{C} : \mathbb{R}] \cdot [\mathbb{C} : \mathbb{R}]$$

in $\mathbb{C} \mid \mathbb{R}$ erkennen kann.

Bevor wir kompliziertere Kenngrößen von Körpererweiterungen betrachten, zeigen wir die Nützlichkeit des Gradbegriffs an einem kleinen Beispiel:

Beispiel 3.2.14 (Gibt es einen Körper mit genau 2026 Elementen?)**.** Ist F ein endlicher Körper und $P \subset F$ der Primkörper von F, so ist (da F als P-Vektorraum zu $P^{\dim_P F}$ isomorph ist)

$$\#F = \#\left(P^{\dim_P F}\right) = (\#P)^{\dim_P F} = (\#P)^{[F:P]} = (\operatorname{char} F)^{[F:P]}.$$

Insbesondere ist $\#F$ eine Primpotenz.

Da 2026 *keine* Primpotenz ist (nachrechnen), gibt es also *keinen* Körper mit genau 2026 Elementen.

Ein etwas feineres Maß als der Grad einer Körpererweiterung ist die Automorphismengruppe (oder geometrischer: die Symmetriegruppe):

Definition 3.2.15 (Morphismen von Körpererweiterungen)**.** Sei K ein Körper.

- Sind $L \mid K$ und $M \mid K$ Körpererweiterungen von K, so ist ein *Morphismus von $L \mid K$ nach $M \mid K$* ein Körperhomomorphismus $f\colon L \longrightarrow M$ mit
$$f|_K = \mathrm{id}_K\,.$$
$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ | & & | \\ K & \xrightarrow[\mathrm{id}_K]{} & K \end{array}$$
- Ein Morphismus von Körperweiterungen über K, der einen (bezüglich Komposition) inversen Morphismus von Körpererweiterungen besitzt, ist ein *Isomorphismus von Körpererweiterungen über K*.

Bemerkung 3.2.16 (Kategorie der Körpererweiterungen)**.** Ist K ein Körper, so bildet die Klasse aller Körpererweiterungen von K zusammen mit den obigen Morphismen von Körperweiterungen über K und der gewöhnlichen Abbildungskomposition eine Kategorie.

Definition 3.2.17 (Galoisgruppe)**.** Sei $L \mid K$ eine Körpererweiterung. Die Automorphismengruppe von $L \mid K$ in der Kategorie der Körpererweiterungen über K, also

$$\begin{aligned}\mathrm{Gal}(L,K) = \big\{ f\colon L \longrightarrow L \;\big|\; & \\ & f \text{ ist ein invertierbarer Körperhomomorphismus} \\ & \text{mit } f|_K = \mathrm{id}_K \big\},\end{aligned}$$

bezeichnet man als *Galoisgruppe von $L \mid K$*.

Eine einfache Rechnung zeigt, dass Galoisgruppen tatsächlich Gruppen (bezüglich Komposition und der Identität) sind.

Bemerkung 3.2.18. Manchmal wird der Begriff „Galoisgruppe“ in der Literatur nur für gutartige Körpererweiterungen (sogenannte Galoiserweiterungen) verwendet, da diese Gruppe nur dann besonders schöne Eigenschaften aufweist.

Beispiel 3.2.19 (die Galoisgruppe von $\mathbb{C} \mid \mathbb{R}$)**.** Als erstes Beispiel bestimmen wir die Galoisgruppe $\mathrm{Gal}(\mathbb{C}, \mathbb{R})$: Offenbar ist $\mathrm{id}_{\mathbb{C}} \in \mathrm{Gal}(\mathbb{C}, \mathbb{R})$. Welche weiteren Elemente gibt es noch? Sei $\sigma \in \mathrm{Gal}(\mathbb{C}, \mathbb{R})$. Wegen $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$ (Bemerkung 3.2.6) ist σ durch $\sigma(i)$ bereits eindeutig bestimmt. Also genügt es, die möglichen Werte $\sigma(i)$ zu bestimmen und zu zeigen, dass diese Werte alle durch Elemente der Galoisgruppe realisiert werden können:

Da σ ein Körperhomomorphismus (mit $\sigma|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$) ist, ist

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -\sigma(1) = -1,$$

und damit $\sigma(i) \in \{i, -i\}$. Der Fall $\sigma(i) = i$ liefert $\sigma = \mathrm{id}_{\mathbb{C}}$. Der Fall $\sigma(i) = -i$ liefert, dass σ die komplexe Konjugation ist.

Da die komplexe Konjugation c ein Körperisomorphismus $\mathbb{C} \longrightarrow \mathbb{C}$ ist, der auf $\mathbb{R}$ als Identität wirkt, erhalten wir somit

$$\mathrm{Gal}(\mathbb{C}, \mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, c\}$$

bzw. $\mathrm{Gal}(\mathbb{C}, \mathbb{R}) \cong_{\mathsf{Group}}$? $\mathbb{Z}/2$.

Mit demselben Argument folgt auch (in $\mathbb{C} \mid \mathbb{Q}$)

$$\mathrm{Gal}\big(\mathbb{Q}(i), \mathbb{Q}\big) \cong_{\mathsf{Group}} ? \quad \mathbb{Z}/2$$
$$\mathrm{Gal}\big(\mathbb{Q}(\sqrt{2}), \mathbb{Q}\big) \cong_{\mathsf{Group}} ? \quad \mathbb{Z}/2.$$

Andererseits ist $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$ trivial, denn $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ (da $\mathbb{R}$ ein Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$ ist, der $\sqrt[3]{2}$ enthält) und $T^3 - 2 \in \mathbb{Q}[T]$ besitzt in $\mathbb{R}$ nur die Nullstelle $\sqrt[3]{2}$.

Dieses Grundprinzip werden wir in Proposition 3.2.28 und Korollar 3.2.29 allgemeiner formulieren und beweisen.

Wir beschäftigen uns in den nächsten Abschnitten mit den folgenden Fragen:

- Welche Situationen kann man mithilfe von Körpererweiterungen modellieren bzw. formulieren?
- Wie kann man Galoisgruppen von Körpererweiterungen bestimmen?
- Was sagen Galoisgruppen über die unterliegenden Körpererweiterungen bzw. die dadurch modellierten Situationen aus?

3.2.2 Algebraische Zahlen

Die Untersuchung der Lösungen bzw. der Geometrie der Lösungsmengen von polynomialen Gleichungen ist eines der Hauptziele der Algebra bzw. der Algebraischen Geometrie. Man führt daher für die Lösung polynomialer Gleichungen geeignete Begriffe ein:

Definition 3.2.20 (algebraisch, transzendent)**.** Sei $L \mid K$ eine Körpererweiterung und sei $\alpha \in L$.

- Das Element α ist *algebraisch über* K, wenn es ein $f \in K[T] \setminus \{0\}$ mit $f(\alpha) = 0$ gibt (d.h., wenn α Lösung einer über K definierten polynomialen Gleichung ist).
- Das Element α ist *transzendent über* K, wenn es *nicht* algebraisch über K ist.

Caveat 3.2.21 (Wurzeln)**.** Sei $L \mid K$ eine Körpererweiterung, sei $c \in K$ und sei $n \in \mathbb{N}_{\geq 2}$. Ist $\alpha \in L$ mit $\alpha^n = c$ (also eine Nullstelle des Polynoms $T^n - c$), so bezeichnet man α auch als eine *n-te Wurzel von c in L*. Im allgemeinen sind solche Wurzeln *nicht* eindeutig und im allgemeinen gibt es *keine* kanonische Wahl einer solchen Wurzel.

Ein Spezialfall ist der folgende: Ist $L = K = \mathbb{R}$ und $c \in \mathbb{R}_{\geq 0}$, so gibt es genau eine n-te Wurzel von c in $\mathbb{R}_{\geq 0}$ (Analysis I) und diese wird mit $\sqrt[n]{c}$ bezeichnet. Wir werden die Notation $\sqrt[n]{c}$ daher ausschließlich in diesem Fall verwenden.

Beispiel 3.2.22 (algebraische/transzendente Zahlen)**.**

- Die Zahl $\sqrt{2} \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$, da sie eine Nullstelle von $T^2 - 2$ ist. Analog sind auch i und $\sqrt[3]{2}$ algebraisch über $\mathbb{Q}$.
- Die Zahlen π und e in $\mathbb{C}$ sind transzendent über $\mathbb{Q}$ [30, Kapitel 21].

  Es ist wichtig, den Grundkörper anzugeben: Über $\mathbb{R}$ sind π und e algebraisch (als Nullstellen von $T - \pi$ bzw. $T - e \in \mathbb{R}[T]$).
- Die Zahl
$$\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$$
ist transzendent über $\mathbb{Q}$ (Übungsaufgabe). Allgemeiner sind alle Zahlen, die sich „gut“ durch rationale Zahlen approximieren lassen transzendent.
- Sei K ein Körper. Dann ist $T \in K(T)$ transzendent über K, da $K[T]$ injektiv in $K(T)$ enthalten ist.

Bemerkung 3.2.23 (viele transzendente Zahlen)**.** Da $\mathbb{Q}[T]$ abzählbar ist und jedes Polynom in $\mathbb{Q}[T] \setminus \{0\}$ nur endlich viele Nullstellen in $\mathbb{C}$ besitzt (Korollar 2.2.58), gibt es in $\mathbb{C}$ nur abzählbar viele über $\mathbb{Q}$ algebraische Zahlen. Also gibt es in $\mathbb{C}$ überabzählbar viele über $\mathbb{Q}$ transzendente Zahlen. Von einer gegebenen komplexen Zahl zu entscheiden, ob sie algebraisch oder transzendent über $\mathbb{Q}$ ist, ist im allgemeinen nicht ganz einfach. Zum Beispiel ist *nicht* bekannt, ob e/π algebraisch über $\mathbb{Q}$ ist oder nicht (!).

Wir kommen noch einmal auf die explizite Beschreibung erzeugter Zwischenkörper aus Bemerkung 3.2.6 zurück:

Proposition 3.2.24 (Minimalpolynom)**.** *Sei $L \mid K$ eine Körpererweiterung, sei $\alpha \in L$ und sei*

$$\begin{aligned} E_\alpha \colon K[T] &\longrightarrow L \\ f &\longmapsto f(\alpha) \end{aligned}$$

der Einsetzungshomomorphismus zu α.

1. *Dann ist α genau dann algebraisch über K, wenn E_α* nicht *injektiv ist.*
2. *Ist α transzendent über K, so ist die Körpererweiterung $K(\alpha) \mid K$ isomorph zu $K(T) \mid K$. Insbesondere ist*

$$K(\alpha) \cong_{\mathsf{Ring}} K(T) \quad \textit{und} \quad [K(\alpha) : K] = \infty.$$

3. *Ist α algebraisch über K, so ist die Körpererweiterung $K(\alpha) \mid K$ isomorph zu $K[T]/\ker E_\alpha \mid K$. Insbesondere gilt*

$$K(\alpha) \cong_{\mathsf{Ring}} K[T]/\ker E_\alpha.$$

und es gibt ein eindeutig bestimmtes normiertes Polynom $\mu_\alpha \in K[T]$ minimalen Grades mit $\mu_\alpha(\alpha) = 0$, das Minimalpolynom von α über K. *Dieses Polynom ist prim und es gilt $\ker E_\alpha = (\mu_\alpha)$ sowie*

$$\big[K(\alpha) : K\big] = \deg \mu_\alpha.$$

Beweis. Zu 1. Dies ist nur eine Reformulierung der Definition von algebraischen Elementen.

Zu 2. Dies folgt aus Bemerkung 3.2.6 und $\dim_K K(T) \geq \dim_K K[T] = \infty$.

Zu 3. Sei α algebraisch über K. Nach Bemerkung 3.2.6 ist dann $K(\alpha) \cong_{\mathsf{Ring}} K[T]/\ker E_\alpha$ und $\ker E_\alpha$ ist ein (nicht-triviales) Primideal in $K[T]$.

Da $K[T]$ ein Hauptidealring und K ein Körper ist, gibt es somit ein eindeutig bestimmtes normiertes Primpolynom $p \in K[T]$ mit $(p) = \ker E_\alpha$ (als Ideale in $K[T]$). Division mit Rest zeigt, dass es sich dabei auch um das eindeutig bestimmte normierte Polynom in $K[T]$ minimalen Grades mit Nullstelle α handelt (nachrechnen; wie im Beweis von Proposition II.3.2.1).

Wir bestimmen den Grad $[K(\alpha) : K]$: Sei $d := \deg \mu_\alpha$. Wir zeigen, dass die Familie $(1, \alpha, \ldots, \alpha^{d-1})$ eine K-Basis von $K(\alpha)$ ist:

- Diese Familie ist erzeugend, denn: Sei $x \in K(\alpha)$. Wegen $K(\alpha) = \operatorname{im} E_\alpha \cong_{\mathsf{Ring}} K[T]/(\mu_\alpha)$ gibt es ein $g \in K[T]$ mit

  $$x = g(\alpha).$$

  Division mit Rest von g durch μ_α zeigt, dass wir außerdem g so wählen können, dass $\deg g < \deg \mu_\alpha = d$ ist. Also ist

  $$x = g(\alpha) \in \operatorname{Span}_K\{1, \alpha, \ldots, \alpha^{d-1}\}.$$

- Diese Familie ist linear unabhängig über K, denn: Seien $\lambda_0, \ldots, \lambda_{d-1} \in K$ mit

  $$0 = \sum_{j=0}^{d-1} \lambda_j \cdot \alpha^j.$$

  Dann ist α eine Nullstelle des Polynoms $f := \sum_{j=0}^{d-1} \lambda_j \cdot T^j \in K[T]$. Aufgrund der Minimalität von μ_α und $\deg f \leq d - 1 < \deg \mu_\alpha$ folgt (nach Normierung), dass f das Nullpolynom ist. Also ist $\lambda_j = 0$ für alle $j \in \{0, \ldots, d-1\}$.

Also ist $(1, \alpha, \ldots, \alpha^{d-1})$ eine K-Basis von $K(\alpha)$; insbesondere ist

$$\big[K(\alpha) : K\big] = d = \deg \mu_\alpha. \qquad \square$$

Anmerkung zum Lernen (Minimalpolynome)**.** Sei $L \mid K$ eine Körpererweiterung und $\alpha \in L$. Wie kann man das Minimalpolynom von α auch als Minimalpolynom (im Sinne der Linearen Algebra) eines geeigneten K-linearen Endomorphismus von L beschreiben?

Bemerkung 3.2.25 (Bestimmung von Minimalpolynomen)**.** Sei $L \mid K$ eine Körpererweiterung und sei $\alpha \in L$ algebraisch über K. In vielen Fällen kann man mit einer der beiden folgenden Strategien das Minimalpolynom von α über K bestimmen:

- Wir betrachten die Familie $(\alpha^j)_{j \in \mathbb{N}}$ in L. Da α über K algebraisch ist, ist diese Familie über K linear abhängig. Mithilfe von Linearer Algebra können wir dann das kleinste $d \in \mathbb{N}$ bestimmen, für das die Familie $(1, \alpha, \ldots, \alpha^d)$ über K linear abhängig ist; außerdem können wir durch Lösen eines linearen Gleichungssystems die Werte $\lambda_0, \ldots, \lambda_{d-1} \in K$ bestimmen, für die

  $$\alpha^d + \sum_{j=0}^{d-1} \lambda_j \cdot \alpha^j = 0$$

ist. Dann ist $\sum_{j=0}^{d-1} \lambda_j \cdot T^j + T^d \in K[T]$ das Minimalpolynom von α über K (nach Definition des Minimalpolynoms).

- Ist $f \in K[T]$ ein normiertes irreduzibles Polynom mit $f(\alpha) = 0$, so ist f das Minimalpolynom von α über K, denn: Mit der Notation aus dem Beweis von Proposition 3.2.24 folgt $f \in \ker E_\alpha = (\mu_\alpha)$. Also ist μ_α in $K[T]$ ein Teiler von f. Da f irreduzibel und normiert ist, folgt daraus bereits $f = \mu_\alpha$.

  Bei dieser Variante sind die Irreduzibilitätskriterien aus Kapitel 2.2.6 hilfreich!

  Liegt zunächst nur ein normiertes Polynom $f \in K[T]$ mit $f(\alpha) = 0$ vor, so kann man durch Faktorisierung von f in (normierte) Primpolynome in $K[T]$ das Minimalpolynom von α finden.

Beispiel 3.2.26 (reelle Wurzeln)**.** Wir betrachten den Zwischenkörper $\mathbb{Q}(\sqrt[3]{2})$ von $\mathbb{C} \mid \mathbb{Q}$. Es gilt

$$\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3,$$

denn: Wir bestimmen dazu zunächst das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$. Das Polynom $T^3 - 2 \in \mathbb{Q}[T]$ ist irreduzibel (Beispiel 2.2.62) und normiert und daher das Minimalpolynom der Nullstelle $\sqrt[3]{2}$ (Bemerkung 3.2.25). Also erhalten wir mit Proposition 3.2.24, dass

$$\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = \boxed{?} \quad \deg(T^3 - 2) = 3.$$

Insbesondere ist $\mathbb{Q}(\sqrt[3]{2}) \neq \{a + b \cdot \sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$, da der rechte $\mathbb{Q}$-Vektorraum höchstens Dimension 2 besitzt.

Analog folgt: ist $p \in \mathbb{N}$ prim und $n \in \mathbb{N}_{\geq 2}$, so ist

$$\left[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}\right] = \boxed{?} \quad n;$$

je größer n ist, desto „weiter“ ist also $\sqrt[n]{p}$ von $\mathbb{Q}$ „entfernt“. Daraus erhalten wir mit Proposition 3.2.12 zum Beispiel

$$\left[\mathbb{Q}(\sqrt[1013]{2}, \sqrt{2027}) : \mathbb{Q}\right] = \boxed{?} \quad 1013 \cdot 2 = 2026.$$

Beispiel 3.2.27 (Einheitswurzeln und Kreisteilungspolynome)**.** Sei $L \mid K$ eine Körpererweiterung und sei $n \in \mathbb{N}_{>0}$. Man bezeichnet α als *n-te Einheitswurzel in L*, wenn

$$\alpha^n = 1$$

ist. Insbesondere sind Einheitswurzeln also algebraisch über K, ihre Minimalpolynome über K sind Teiler von $T^n - 1$ in $K[T]$ und es gibt höchstens n verschiedene Einheitswurzeln in L, da jede solche Einheitswurzel eine Nullstelle von $T^n - 1$ in L ist (Korollar 2.2.58).

Mit $U_n(L)$ bezeichnen wir die Menge der n-ten Einheitswurzeln in L. Dann ist $U_n(L)$ eine Gruppe bezüglich Multiplikation (nachrechnen) und als

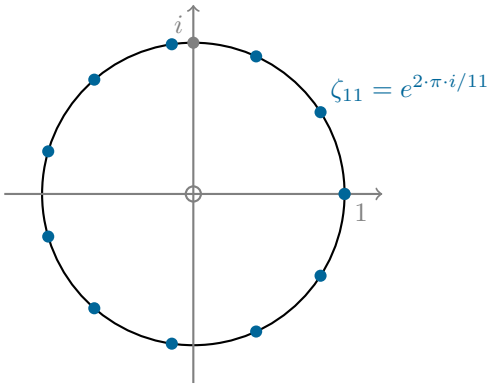


Abbildung 3.2.: Die elften Einheitswurzeln in $\mathbb{C}$

endliche Untergruppe von $L^\times$ zyklisch (nach Satz 3.1.9). Eine Einheitswurzel $\alpha \in U_n(L)$ ist *primitiv*, wenn sie die Gruppe $U_n(L)$ erzeugt.

Ist $L = \mathbb{C}$ (und zum Beispiel $K = \mathbb{Q}$) und $\zeta_n := e^{2\pi\cdot i/n}$, so sind

$$1,\ \zeta_n,\ \ldots,\ \zeta_n^{n-1}$$

die n-ten Einheitswurzeln in $\mathbb{C}$ (Abbildung 3.2). Es gilt $U_n(\mathbb{C}) \cong_{\mathsf{Group}} \mathbb{Z}/n$ (nachrechnen) und eine n-te Einheitswurzel ζ_n^k mit $k \in \mathbb{Z}$ ist genau dann primitiv, wenn $\mathrm{ggT}(k, n) = 1$ ist (nachrechnen mit Proposition 2.2.34). Insbesondere gibt es in $\mathbb{C}$ genau ? $\varphi(n)$ primitive n-te Einheitswurzeln.

Das Minimalpolynom von ζ_n über $\mathbb{Q}$ bezeichnet man als *n-tes Kreisteilungspolynom* Φ_n; der Name soll natürlich an die geometrische Lage der n-ten Einheitswurzeln auf dem Einheitskreis erinnern. Wir werden diese Polynome in Proposition 3.5.1 genauer untersuchen.

Wie wir bereits in Caveat 3.2.21 kurz angesprochen haben, gibt es im allgemeinen in Körpererweiterungen mehrere Elemente, die dasselbe Minimalpolynom besitzen (man bezeichnet diese Elemente dann auch als *konjugiert*). Kunjugierte Elemente sind der Schlüssel zum Verständnis von Morphismen von Körpererweiterungen der zugehörigen Zwischenkörper:

Proposition 3.2.28 (Konjugationsprinzip für algebraische Zahlen)**.** *Seien $L \mid K$ und $L' \mid K'$ Körpererweiterungen, sei $\sigma\colon K \longrightarrow K'$ ein Körperisomorphismus und sei $\alpha \in L$ algebraisch über K. Sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K. Mit $\mu_\alpha^\sigma \in K'[T]$ bezeichnen wir das Polynom, das man aus μ_α durch Anwendung von σ auf die Koeffizienten erhält. Dann gilt:*

1. *Ist $\widetilde{\sigma}\colon L \longrightarrow L'$ ein Körpermorphismus mit $\widetilde{\sigma}|_K = \sigma$, so ist $\widetilde{\sigma}(\alpha)$ eine Nullstelle von μ_α^σ in L' und $\widetilde{\sigma}|_{K(\alpha)}$ ist durch $\widetilde{\sigma}(\alpha)$ eindeutig bestimmt.*

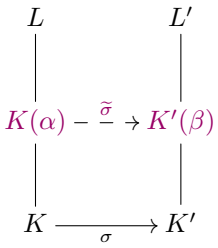


Abbildung 3.3.: Das Konjugationsprinzip, schematisch

2. *Ist $\beta \in L'$ eine Nullstelle von μ_α^σ, so gibt es genau einen Körperisomorphismus $\widetilde{\sigma}\colon K(\alpha) \longrightarrow K'(\beta)$ mit $\widetilde{\sigma}|_K = \sigma$ und $\widetilde{\sigma}(\alpha) = \beta$.*

Der zweite Teil von Proposition 3.2.28 ist in Abbildung 3.3 illustriert. Oft wird das Konjugationsprinzip im Spezialfall „$\sigma = \mathrm{id}_K\colon K \longrightarrow K$“ angewendet; manchmal ist es aber auch hilfreich, auf den Grundkörpern mehr Flexibilität zu haben (vor allem in induktiven Konstruktionen von Körpermorphismen).

Beweis. Zu 1. Wegen $\mu_\alpha \in K[T]$ und $\widetilde{\sigma}|_K = \sigma$ gilt

$$\mu_\alpha^\sigma\big(\widetilde{\sigma}(\alpha)\big) = \widetilde{\sigma}\big(\mu_\alpha(\alpha)\big) = \widetilde{\sigma}(0) = 0.$$

Wegen $K(\alpha) = \operatorname{im} E_\alpha$ (Proposition 3.2.24) ist $\widetilde{\sigma}|_{K(\alpha)}\colon K(\alpha) \longrightarrow L'$ eindeutig durch den Wert $\widetilde{\sigma}(\alpha)$ bestimmt.

Zu 2. Die Eindeutigkeit folgt aus dem ersten Teil. Warum existiert ein solcher Morphismus? Seien

$$E_\alpha\colon K[T] \longrightarrow L$$
$$E_\beta\colon K'[T] \longrightarrow L'$$

die Einsetzungshomomorphismen zu $\alpha \in L$ bzw. $\beta \in L'$.

Wir bestimmen das Minimalpolynom von β über K': Da μ_α normiert und in $K[T]$ irreduzibel ist und $\sigma\colon K \longrightarrow K'$ ein Körperisomorphismus ist, ist auch μ_α^σ normiert und in $K'[T]$ irreduzibel. Somit ist μ_α^σ das Minimalpolynom von β (Bemerkung 3.2.25).

Daher induzieren die Einsetzungshomomorphismen Körperisomorphismen

$$F_\alpha\colon K[T]/(\mu_\alpha) \longrightarrow K(\alpha) \quad \text{und} \quad F_\beta\colon K'[T]/(\mu_\alpha^\sigma) \longrightarrow K'(\beta)$$

(Proposition 3.2.24). Somit ist $\widetilde{\sigma} := F_\beta \circ ([f] \mapsto [f^\sigma]) \circ F_\alpha^{-1}\colon K(\alpha) \longrightarrow K(\beta)$ ein Körperisomorphismus mit $\widetilde{\sigma}|_K = \sigma$ und $\sigma(\alpha) = F_\beta([T]) = \beta$. □

Insbesondere können wir Galoisgruppen auch als (Untergruppen von) Symmetriegruppen von Nullstellenmengen auffassen:

Korollar 3.2.29 (die Galoisoperation auf den Nullstellen)**.** *Sei $L \mid K$ eine Körpererweiterung, sei $\alpha \in L$ algebraisch über K und sei $X \subset K(\alpha)$ die Menge der Nullstellen in $K(\alpha)$ (!) des Minimalpolynoms μ_α von α über K. Dann gilt:*

1. *Für alle $\beta \in X$ ist $K(\beta) = K(\alpha)$.*
2. *Es ist*

$$\begin{aligned} \operatorname{Gal}\big(K(\alpha), K\big) &\longrightarrow S_X \\ \sigma &\longmapsto \big(x \mapsto \sigma(x)\big) \end{aligned}$$

   ein wohldefinierter und injektiver Gruppenhomomorphismus. Die zugehörige Gruppenoperation von $\operatorname{Gal}(K(\alpha), K)$ auf X ist transitiv.

3. *Dabei gilt*

$$\#\operatorname{Gal}\big(K(\alpha), K\big) = \#X \leq \deg \mu_\alpha = \big[K(\alpha) : K\big].$$

Beweis. Zu 1. Sei $\beta \in X$. Wegen $\beta \in K(\alpha)$ ist $K(\beta) \subset K(\alpha)$. Da α und β dasselbe Minimalpolynom μ_α über K besitzen, folgt mit Proposition 3.2.24, dass

$$\dim_K K(\beta) = \text{?} \quad \big[K(\beta) : K\big] = \deg \mu_\alpha = \big[K(\alpha) : K\big] = \dim_K K(\alpha).$$

Da diese Dimensionen endlich sind, erhalten wir somit $K(\beta) = K(\alpha)$.

Zu 2. Nach dem ersten Teil ist dies eine Reformulierung des Konjugationsprinzips (Proposition 3.2.28) mithilfe von Gruppentheorie bzw. Gruppenoperationen. Wir wenden das Konjugationsprinzip dabei auf den Spezialfall an, dass der bereits gegebene Körperisomorphismus $K \longrightarrow K$ die Identität ist.

Zu 3. Aus dem Konjugationsprinzip erhalten wir $\#\operatorname{Gal}(K(\alpha), K) = \#X$. Da μ_α in $K(\alpha)$ höchstens $\deg \mu_\alpha$ Nullstellen besitzt (Korollar 2.2.58), folgt zusammen mit Proposition 3.2.24 die gesamte (Un)Gleichungskette. □

Zum Beispiel haben wir das obige Prinzip implizit bei der Berechnung der Galoisgruppe von $\mathbb{C} \mid \mathbb{R}$ verwendet (Beispiel 3.2.19). Wir werden das Konjugationsprinzip in einigen weitere Beispiele und allgemeinen Konstruktionen anwenden.

Wollen wir algebraische Zahlen besser verstehen, so bietet es sich an, die zugehörigen Körpererweiterungen genauer zu betrachten. Zum Beispiel ist aus der Definition algebraischer Zahlen nicht unmittelbar klar, ob die Summe zweier algebraischer Zahlen algebraisch ist oder nicht – mithilfe der Theorie algebraischer Körpererweiterungen ist dies aber leicht zu beantworten (Korollar 3.2.36).

3.2.3 Algebraische Körpererweiterungen

Eine Körpererweiterung ist algebraisch, wenn sie ausschließlich aus algebraischen Elementen besteht:

Definition 3.2.30 (algebraische/tranzendente Körpererweiterung)**.** Sei $L \mid K$ eine Körpererweiterung.

- Die Erweiterung $L \mid K$ ist *algebraisch*, wenn jedes Element aus L algebraisch über K ist.
- Die Erweiterung $L \mid K$ ist *transzendent*, wenn sie nicht algebraisch ist (d.h. mindestens ein Element enthält, das nicht algebraisch über K ist).

Beispiel 3.2.31 (algebraische/transzendente Erweiterungen)**.**

- Ist K ein Körper, so ist die triviale Körpererweiterung $K \mid K$ algebraisch.
- Ist K ein Körper, so ist die Körpererweiterung $K(T) \mid K$ transzendent, denn $T \in K(T)$ ist transzendent über K (Beispiel 3.2.22).
- Die Körpererweiterungen $\mathbb{C} \mid \mathbb{Q}$ und $\mathbb{R} \mid \mathbb{Q}$ sind transzendent (Beispiel 3.2.22).

Proposition 3.2.32. *Endliche Körpererweiterungen sind algebraisch.*

Beweis. Sei $L \mid K$ eine endliche Körpererweiterung und sei $\alpha \in L$. Dann ist α algebraisch über K, denn: Wegen

$$\big[K(\alpha) : K\big] \cdot \big[L : K(\alpha)\big] = [L : K] < \infty$$

(Proposition 3.2.10) ist auch die Körpererweiterung $K(\alpha) \mid K$ endlich. Somit ist α *nicht* transzendent über K (Proposition 3.2.24), also algebraisch über K.

Alternativ kann man auch etwas direkter vorgehen: Wegen $\dim_K L = [L : K] < \infty$ ist die Familie $(\alpha^n)_{n\in\mathbb{N}}$ linear abhängig über K. Also gibt es ein $d \in \mathbb{N}$ und $\lambda_0, \ldots, \lambda_{d-1} \in K$ mit

$$\alpha^d + \sum_{j=0}^{d-1} \lambda_j \cdot \alpha^j = 0.$$

Dann ist α eine Nullstelle des Polynoms $T^d + \sum_{j=0}^{d-1} \lambda_j \cdot T^j \in K[T] \setminus \{0\}$. Insbesondere ist α algebraisch über K. □

Beispiel 3.2.33. Also sind zum Beispiel (in $\mathbb{C} \mid \mathbb{Q}$) die Körpererweiterungen

$$\mathbb{C} \mid \mathbb{R}, \quad \mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}, \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}, \quad \mathbb{Q}(\zeta_{11}) \mid \mathbb{Q}, \quad \ldots$$

sowie $\mathbb{F}_7[T]/(T^2+1) \mid \mathbb{F}_7$ algebraisch (da wir bereits wissen, dass sie endlich sind; erinnern Sie sich in jedem dieser Fälle, warum die Erweiterung endlich ist?!).

Korollar 3.2.34 (Vererbung von Algebraizität)**.** *Seien $M \mid L$ und $L \mid K$ algebraische Körpererweiterungen. Dann ist auch die Komposition $M \mid K$ algebraisch.*

Beweis. Sei $\alpha \in M$. Indem man die Koeffizienten des Minimalpolynoms von α über L betrachtet, kann man sich auf den Fall zurückziehen, dass die Erweiterung $L \mid K$ endlich ist. Dies liefert, dass $K(\alpha) \mid K$ (mit $K(\alpha) \subset M$) eine endliche Erweiterung ist ... (Übungsaufgabe). □

Korollar 3.2.35. *Sei $L \mid K$ eine Körpererweiterung. Ist $S \subset L$ eine Menge von über K algebraischen Elementen, so ist die Erweiterung $K(S) \mid K$ algebraisch.*

Beweis. Sei $\alpha \in K(S)$. Dann gibt es bereits eine endliche Teilmenge $S' \subset S$ mit $\alpha \in K(S')$, denn: Sei F die Menge aller endlichen Teilmengen von S. Dann ist $K' := \bigcup_{S' \in F} K(S')$ ein Körper (nachrechnen!) und $S \subset K'$. Also ist $K(S) \subset K'$ Insbesondere gibt es eine endliche Teilmenge $S' \subset S$ mit $\alpha \in K(S')$.

Induktiv (über $\#S'$) folgt mithilfe von Proposition 3.2.24, dass die Erweiterung $K(S') \mid K$ endlich ist (nachrechnen!). Daher ist die Erweiterung $K(S') \mid K$ algebraisch (Proposition 3.2.32). Insbesondere ist somit auch das Element $\alpha \in K(S')$ algebraisch über K. □

Korollar 3.2.36 (Zwischenkörper der algebraischen Zahlen)**.** *Sei $L \mid K$ eine Körpererweiterung und sei $A \subset L$ die Menge der algebraischen Elemente über K. Dann ist A ein Zwischenkörper von $L \mid K$. Insbesondere ist die Summe, das Produkt, ... von über K algebraischen Elementen auch algebraisch über K.*

Beweis. Sei $M := K(A)$. Wir zeigen, dass $A = M$ ist: Nach Konstruktion ist $A \subset K(A) = M$.

Warum ist $M \subset A$? Nach Definition ist M ein Zwischenkörper von $L \mid K$. Da alle Elemente aus A über K algebraisch sind, ist die Erweiterung $M \mid K$ algebraisch (Korollar 3.2.35). Nach Definition von A ist somit $M \subset A$.

Insbesondere ist $A = M = K(A)$ ein Zwischenkörper von $L \mid K$. □

Beispiel 3.2.37. Also ist zum Beispiel auch die komplexe Zahl

$$\frac{\sqrt[2025]{2026 + \sqrt[42]{2027}}}{42 + \sqrt[1944]{702}}$$

algebraisch über $\mathbb{Q}$ (nachrechnen), obwohl wir vielleicht nicht unbedingt ein explizites Polynom in $\mathbb{Q}[T]$ suchen wollen, das diese Zahl als Nullstelle besitzt.

Caveat 3.2.38. Algebraische Körpererweiterungen sind im allgemeinen *nicht* endlich: Sei $K \subset \mathbb{C}$ der Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$ aller über $\mathbb{Q}$ algebraischen Elemente in $\mathbb{C}$. Dann ist $K \mid \mathbb{Q}$ eine algebraische Körpererweiterung (Korollar 3.2.36). Es gilt $[K : \mathbb{Q}] = \infty$, denn: Wegen

$$\forall_{n \in \mathbb{N}_{>0}} \quad \left[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}\right] = n$$

(Beispiel 3.2.26) und $\mathbb{Q}(\sqrt[n]{2}) \subset K$ erhalten wir aus der Multiplikativität des Grades (Proposition 3.2.10), dass

$$[K : \mathbb{Q}] = \infty.$$

3.2.4 Zerfällungskörper

Bei der Untersuchung polynomialer Gleichungen betrachten wir Körper, die „alle möglichen“ Lösungen der gegebenen Gleichung enthalten; außerdem soll der betrachtete Körper dabei „möglichst klein“ sein. Dies führt zum Begriff des Zerfällungskörpers:

Definition 3.2.39 (Zerfällungskörper)**.** Sei K ein Körper und $f \in K[T]$ normiert. Ein *Zerfällungskörper von f über K* ist ein Körper L mit:

- Es gilt $K \subset L$ und das Polynom f zerfällt über L in Linearfaktoren, d.h. es gibt $n \in \mathbb{N}$ und $\alpha_1, \ldots, \alpha_n \in L$ mit

$$f = \prod_{j=1}^{n} (T - \alpha_j) \in L[T].$$

- Es gilt $L = K\big(\{\alpha_1, \ldots, \alpha_n\}\big)$.

Beispiel 3.2.40 (Zerfällungskörper)**.**

- Es ist ? $\mathbb{C}$ ein Zerfällungskörper von $T^2 + 1$ über $\mathbb{R}$.
- Wegen $\sqrt{2}, -\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \subset \mathbb{C}$ ist $\mathbb{Q}(\sqrt{2})$ ein Zerfällungskörper von $T^2 - 2$ über $\mathbb{Q}$.
- Aber $\mathbb{R}$ ist *kein* Zerfällungskörper von $T^2 - 2$ über $\mathbb{Q}$ (da $\mathbb{R}$ „zu groß“ ist).

Beispiel 3.2.41. Wir bestimmen einen Zerfällungskörper für $T^3 - 2 \in \mathbb{Q}[T]$ über $\mathbb{Q}$: Dazu betrachten wir die Körpererweiterung $\mathbb{C} \mid \mathbb{Q}$. Über $\mathbb{C}$ zerfällt $T^3 - 2$ in Linearfaktoren und in $\mathbb{C}$ hat $T^3 - 2$ genau drei Nullstellen, nämlich

? $\sqrt[3]{2}, \quad \zeta_3 \cdot \sqrt[3]{2}, \quad \zeta_3^2 \cdot \sqrt[3]{2}.$

Also ist

$$K := \mathbb{Q}(\sqrt[3]{2}, \zeta_3 \cdot \sqrt[3]{2}, \zeta_3^2 \cdot \sqrt[3]{2})$$

ein Zerfällungskörper von $\mathbb{Q}$. Aber wegen $\zeta_3 \cdot \sqrt[3]{2} \notin \mathbb{R}$ ist $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ *kein* Zerfällungskörper von $T^3 - 2$ über $\mathbb{Q}$!

Zusätzlich versuchen wir nun, die Erweiterung $K \mid \mathbb{Q}$ etwas besser zu verstehen: Im folgenden schreiben wir $\alpha := \sqrt[3]{2}$.

- Es gilt $K = \mathbb{Q}(\alpha, \zeta_3)$, denn: Wegen $\zeta_3 = \zeta_3 \cdot \alpha \cdot 1/\alpha$ ist $\mathbb{Q}(\alpha, \zeta_3) \subset K$.

  Umgekehrt gilt wegen $\zeta_3 \cdot \alpha, \zeta_3^2 \cdot \alpha \in \mathbb{Q}(\alpha, \zeta_3)$ auch die umgekehrte Inklusion $K = \mathbb{Q}(\alpha, \zeta_2 \cdot \alpha, \zeta_3^2 \cdot \alpha) \subset \mathbb{Q}(\alpha, \zeta_3)$. Also ist $K = \mathbb{Q}(\alpha, \zeta_3)$.

- Bestimmung von $[K : \mathbb{Q}]$: Nach der obigen Überlegung ist K das Kompositum von $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\zeta_3)$ in $\mathbb{C} \mid \mathbb{Q}$.

  Wir wissen bereits $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ (Beispiel 3.2.26); außerdem ist $T^2 + T + 1 \in \mathbb{Q}[T]$ das Minimalpolynom von ζ_3 über $\mathbb{Q}$ (nachrechnen), und damit $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$. Wegen $\operatorname{ggT}(3, 2) = 1$ erhalten wir (Proposition 3.2.12)

  $$[K : \mathbb{Q}] = \text{?} \quad \big[\mathbb{Q}(\alpha) \cdot \mathbb{Q}(\zeta_3) : \mathbb{Q}\big] = \big[\mathbb{Q}(\alpha) : \mathbb{Q}\big] \cdot \big[\mathbb{Q}(\zeta_3) : \mathbb{Q}\big] = 3 \cdot 2 = 6.$$

  Außerdem: Wegen (Proposition 3.2.10)

  $$6 = [K : \mathbb{Q}] = \big[\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}(\zeta_3)\big] \cdot \big[\mathbb{Q}(\zeta_3) : \mathbb{Q}\big]$$

  und wegen des Zusammenhangs zwischen Minimalpolynomen und Erweiterungsgraden (Proposition 3.2.24) ist somit $T^3 - 2$ auch das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}(\zeta_3)$.

- Wir bestimmen die Galoisgruppe $\operatorname{Gal}(K, \mathbb{Q})$: Dazu verwenden wir die Zerlegung von $K \mid \mathbb{Q}$ in die beiden Schritte $\mathbb{Q}(\zeta_3) \mid \mathbb{Q}$ und $K \mid \mathbb{Q}(\zeta_3)$ und gehen wie folgt vor:

  1. Wir zeigen, dass die Einschränkung auf $\mathbb{Q}(\zeta_3)$ einen wohldefinierten Gruppenhomomorphismus $\operatorname{Gal}(K, \mathbb{Q}) \longrightarrow \operatorname{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q})$ liefert.
  2. Wir bestimmen die Gruppe $\operatorname{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q})$ mit dem Konjugationsprinzip.
  3. Wir bestimmen für jedes Element von $\operatorname{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q})$ alle möglichen Fortsetzungen zu Elementen von $\operatorname{Gal}(K, \mathbb{Q})$ mit dem Konjugationsprinzip. Damit erhalten wir $\operatorname{Gal}(K, \mathbb{Q})$ als Menge.
  4. Wir bestimmen die Gruppenstruktur auf $\operatorname{Gal}(K, \mathbb{Q})$ durch Berechnung der Werte von Verknüpfungen auf ζ_3 und α.

  Zu 1. Sei $\sigma \in \operatorname{Gal}(K, \mathbb{Q})$. Dann bildet σ Nullstellen von $T^2 + T + 1$ auf Nullstellen von $T^2 + T + 1$ ab (Proposition 3.2.28). Die komplexen Nullstellen von $T^2 + T + 1$ sind ζ_3 und $\zeta_3^2 \in \mathbb{Q}(\zeta_3)$. Also ist

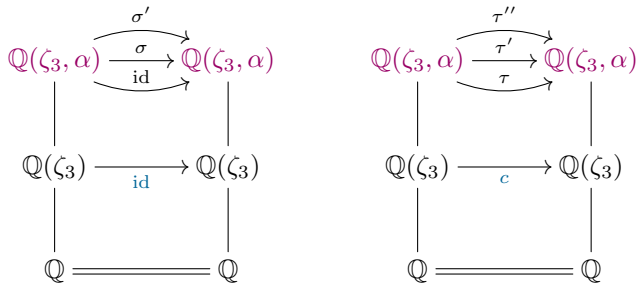


Abbildung 3.4.: Die Elemente von $\mathrm{Gal}(K, \mathbb{Q})$, schematisch

$\sigma(\mathbb{Q}(\zeta_3)) \subset \mathbb{Q}(\zeta_3)$. Indem wir dieses Argument auch auf σ^{-1} anwenden, erkennen wir, dass $\sigma|_{\mathbb{Q}(\zeta_3)}$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q})$ liegt. Außerdem ist die Einschränkungsabbildung mit Abbildungskomposition verträglich.

Zu 2. Wegen $\zeta_3^2 = \overline{\zeta}_3$ erhalten wir mit dem Konjugationsprinzip (Korollar 3.2.29, Beispiel 3.2.19) daher, dass

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_3), \mathbb{Q}\big) = \boxed{?} \quad \{\mathrm{id}, c\} \cong_{\mathsf{Group}} \mathbb{Z}/2,$$

wobei c die Einschränkung der komplexen Konjugation auf $\mathbb{Q}(\zeta_3)$ bezeichnet.

Zu 3. Da $T^3 - 2$ das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}(\zeta_3)$ ist und K ein Zerfällungskörper von $T^3 - 2$ über $\mathbb{Q}(\zeta_3)$ ist (siehe oben), können wir die Fortsetzungen wie folgt mit dem Konjugationsprinzip (Proposition 3.2.28) bestimmen (Abbildung 3.4):

– Fortsetzungen von $\mathrm{id}_{\mathbb{Q}(\zeta_3)}$: Es gibt genau drei solche Fortsetzungen und diese sind jeweils eindeutig durch die folgenden Zuordnungen bestimmt (zusätzlich zu $\zeta_3 \longmapsto \zeta_3$):

$$\begin{aligned}
\sqrt[3]{2} &\longmapsto \sqrt[3]{2} && \text{(dies liefert die Identität auf } K\text{)} \\
\sqrt[3]{2} &\longmapsto \zeta_3 \cdot \sqrt[3]{2} && \text{(diesen Automorphismus nennen wir } \sigma\text{)} \\
\sqrt[3]{2} &\longmapsto \zeta_3^2 \cdot \sqrt[3]{2} && \text{(diesen Automorphismus nennen wir } \sigma'\text{)}
\end{aligned}$$

– Fortsetzungen von c: Es gibt genau drei solche Fortsetzungen und diese sind jeweils eindeutig durch die folgenden Zuordnungen bestimmt (zusätzlich zu $\zeta_3 \longmapsto \zeta_3^2$):

Automorphismus	Wert auf ζ_3	Wert auf $\alpha = \sqrt[3]{2}$
id	ζ_3	α
σ	ζ_3	$\zeta_3 \cdot \alpha$
σ'	ζ_3	$\zeta_3^2 \cdot \alpha$
σ^2	ζ_3	$\sigma(\zeta_3 \cdot \alpha) = \sigma(\zeta_3) \cdot \sigma(\alpha) = \zeta_3^2 \cdot \alpha$
σ^3	ζ_3	$\sigma^2(\zeta_3 \cdot \alpha) = \zeta_3^3 \cdot \alpha = \alpha$
τ	ζ_3^2	α
τ^2	$\tau(\zeta_3^2) = \tau(\zeta_3) \cdot \tau(\zeta_3) = \zeta_3^4 = \zeta_3$	α
$\tau \circ \sigma \circ \tau$	$\cdots = \zeta_3$	$\cdots = \zeta_3^2 \cdot \alpha$
komplexe Konjugation	$\overline{\zeta}_3 = \zeta_3^2$	$\overline{\alpha} = \alpha$

Abbildung 3.5.: Bestimmung der Gruppenstruktur auf $\mathrm{Gal}(K, \mathbb{Q})$

$$\sqrt[3]{2} \longmapsto \sqrt[3]{2} \qquad \text{(diesen Automorphismus nennen wir } \tau\text{)}$$
$$\sqrt[3]{2} \longmapsto \zeta_3 \cdot \sqrt[3]{2} \qquad \text{(diesen Automorphismus nennen wir } \tau'\text{)}$$
$$\sqrt[3]{2} \longmapsto \zeta_3^2 \cdot \sqrt[3]{2} \qquad \text{(diesen Automorphismus nennen wir } \tau''\text{)}$$

Dabei folgt aus der Eindeutigkeit, dass τ mit der komplexen Konjugation auf K übereinstimmt.

Also ist

$$\mathrm{Gal}(K, \mathbb{Q}) = \{\mathrm{id}_K, \sigma, \sigma', \tau, \tau', \tau''\}.$$

Zu 4. Nach dem vorherigen Schritt handelt es sich bei $\mathrm{Gal}(K, \mathbb{Q})$ um eine Gruppe mit genau sechs Elementen. Um die Gruppenstruktur zu bestimmen, berechnen wir die Werte gewisser Verknüpfungen (Abbildung 3.5).

Da Elemente aus $\mathrm{Gal}(K, \mathbb{Q})$ eindeutig durch ihre Werte auf ζ_3 und α bestimmt sind, können wir die folgenden Beziehungen ablesen:

$$\sigma^2 = \sigma', \quad \mathrm{ord}(\sigma) = 3, \quad \mathrm{ord}(\tau) = 2, \quad \tau \circ \sigma \circ \tau = \sigma^2 = \sigma^{-1}, \quad \ldots$$

Eine einfache Rechnung zeigt, dass $\mathrm{Gal}(K, \mathbb{Q})$? das semi-direkte Produkt von $\langle\sigma\rangle_{\mathrm{Gal}(K,\mathbb{Q})} \cong_{\mathsf{Group}} \mathbb{Z}/3$ mit $\langle\tau\rangle_{\mathrm{Gal}(K,\mathbb{Q})} \cong_{\mathsf{Group}} \mathbb{Z}/2$ ist, wobei letztere Gruppe auf der ersten durch Inversion operiert. Also ist (Abbildung 3.6)

$$\mathrm{Gal}(K, \mathbb{Q}) \cong_{\mathsf{Group}} ? \quad D_3 \cong_{\mathsf{Group}} S_3.$$

Caveat 3.2.42. Man beachte, dass das Verfahren zur Bestimmung der Galoisgruppe im vorigen Beispiel mit der Zerlegung in $K \mid \mathbb{Q}(\alpha)$ und $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ *nicht* auf dieselbe Weise funktioniert hätte, da $\mathbb{Q}(\alpha)$ *kein* Zerfällungskörper

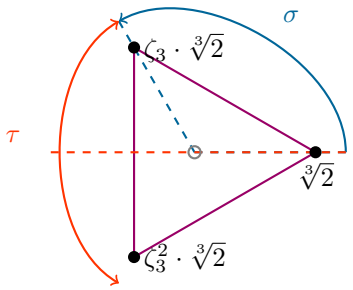


Abbildung 3.6.: Geometrie der Operation der Galoisgruppe $\mathrm{Gal}(K, \mathbb{Q})$ auf den Nullstellen $\{\sqrt[3]{2}, \zeta_3 \cdot \sqrt[3]{2}, \zeta_3^3 \cdot \sqrt[3]{2}\}$ von $T^3 - 2$ in K

von $T^3 - 2$ über $\mathbb{Q}$ ist und sich somit nicht jedes Element von $\mathrm{Gal}(K, \mathbb{Q})$ zu einem Element von $\mathrm{Gal}(\mathbb{Q}(\alpha), \mathbb{Q})$ einschränkt!

Anmerkung zum Lernen. Beispiel 3.2.41 erlaubt es, fast alle Aspekte der Galoistheorie zu illustrieren. Es ist daher äußerst nützlich, dieses Beispiel wirklich gut zu verstehen.

Zerfällungskörper können induktiv durch geeignete Restklassenringe von Polynomen konstruiert werden:

Satz 3.2.43 (Existenz von Zerfällungskörpern)**.** *Sei K ein Körper, $f \in K[T]$ ein normiertes Polynom. Dann gibt es einen Zerfällungskörper von f über K.*

Beweis. Es genügt, die folgende Aussage zu zeigen:

(Z) Ist K ein Körper und $f \in K[T]$ ein normiertes Polynom, so gibt es eine Körpererweiterung $L \mid K$, so dass f über L in Linearfaktoren zerfällt.

Ist nämlich $L \mid K$ eine Körpererweiterung wie in (Z), und ist

$$f = \prod_{j=1}^{n} (T - \alpha_j)$$

mit $\alpha_1, \ldots, \alpha_n \in L$, so ist $K(\alpha_1, \ldots, \alpha_n)$ ein Zerfällungskörper von f über K.

Es bleibt also die Aussage (Z) zu beweisen. Wir gehen dazu induktiv vor:

- *Induktionsanfang.* Ist $\deg f \leq 1$, so hat die Erweiterung $K \mid K$ die gewünschte Eigenschaft.
- *Induktionsvoraussetzung.* Wir nehmen nun an, dass $\deg f > 1$ ist und dass (Z) für Polynome von kleinerem Grad bereits bewiesen ist.

- *Induktionsschritt.* Wir zeigen, dass (Z) dann auch für f gilt. Wir unterscheiden dabei zwei Fälle:

  ① Ist f reduzibel, so gibt es normierte Polynome $g, h \in K[T]$ mit $f = g \cdot h$ und $\deg g < \deg f$, $\deg h < \deg f$. Nach Induktionsvoraussetzung gibt es dann Körpererweiterungen $M \mid K$ und $N \mid M$ (über M, nicht über K), so dass g über M und h über N in Linearfaktoren zerfällt. Dann zerfällt f über N in Linearfaktoren.

  ② Ist f irreduzibel, so ist $M := K[T]/(f)$ ein Körper mit kanonischer Inklusion $K \hookrightarrow M$. Außerdem besitzt f in M eine Nullstelle (nach Konstruktion nämlich die Restklasse von T im Restklassenring M; analog zu Beispiel 2.2.56).

  Damit ist f reduzibel über M und wir können den reduziblen Fall ① auf f als Polynom in $M[T]$ anwenden. □

Satz 3.2.44 (Eindeutigkeit von Zerfällungskörpern)**.** *Sei K ein Körper und $f \in K[T]$ ein normiertes Polynom. Sind L und M Zerfällungskörper von f über K, so sind die Körpererweiterungen $L \mid K$ und $M \mid K$ isomorph.*

Beweis. Man beweist mithilfe des Konjugationsprinzips durch Induktion über den Grad von f die folgende, etwas allgemeinere, Aussage:

(E) Sei $\sigma\colon K \longrightarrow K'$ ein Körperisomorphismus, sei $f \in K[T]$ ein normiertes Polynom und seien L und L' Zerfällungskörper von f über K bzw. von f^σ über $K'[T]$. Dann gibt es einen Körperisomorphismus $\widetilde{\sigma}\colon L \longrightarrow L'$ mit $\widetilde{\sigma}|_K = \sigma$.

- *Induktionsanfang.* Ist $\deg f \leq 1$, so ist $L = K$ und $L' = K'$ und $\widetilde{\sigma} = \sigma$ ist die gesuchte Fortsetzung.

- *Induktionsvoraussetzung.* Es sei $n \in \mathbb{N}_{\geq 2}$ und die Behauptung (E) gelte in allen Situationen mit Polynomen vom Grad kleiner als n.

- *Induktionsschritt.* Sei $\sigma\colon K \longrightarrow K'$ ein Körperisomorphismus, sei $f \in K[T]$ ein normiertes Polynom vom Grad n und seien L und L' Zerfällungskörper von f über K bzw. von f^σ über $K'[T]$. Wir unterscheiden zwei Fälle:

  ① Das Polynom f in $K[T]$ ist reduzibel: Dann existieren normierte Polynome $g, h \in K[T]$ mit $f = g \cdot h$ und $\deg g < n$, $\deg h < n$. Da L ein Zerfällungskörper von f über K ist, gibt es insbesondere $m \in \mathbb{N}_{\geq 1}$ und $\alpha_1, \ldots, \alpha_m \in L$ mit

  $$g = \prod_{j=1}^{m} (T - \alpha_j).$$

  Dann ist der Zwischenkörper $M := K(\alpha_1, \ldots, \alpha_m)$ ein Zerfällungskörper von g über K. Analog finden wir einen Zwischenkörper M'

von $L' \mid K'$, der ein Zerfällungskörper von g^σ über K ist. Nach Induktionsvoraussetzung gibt es daher einen Körperisomorphismus $\tau\colon M \longrightarrow M'$ mit $\tau|_K = \sigma$.

Wegen $f = g \cdot h$ und $f^\sigma = g^\sigma \cdot h^\sigma$ sind L bzw. L' Zerfällungskörper von h über M bzw. von h^σ über M'. Nach Induktionsvoraussetzung gibt es somit einen Körperisomorphismus $\widetilde{\sigma}\colon L \longrightarrow L'$ mit $\sigma|_M = \tau$. (Dies erklärt auch, warum man für den Induktionsbeweis auf den Grundkörpern allgemeinere Körperisomorphismen als nur die Identität benötigt.) Insbesondere ist

$$\widetilde{\sigma}|_K = \tau|_K = \sigma.$$

② Das Polynom f in $K[T]$ ist irreduzibel: Sei $\alpha \in L$ eine Nullstelle von f. Dann gibt es ein $g \in K(\alpha)[T]$ mit

$$f = (T - \alpha) \cdot g.$$

Analog sei $\beta \in L'$ eine Nullstelle von f^σ. Da f irreduzibel ist, erhalten wir mit dem Konjugationsprinzip (Proposition 3.2.28) einen Körperisomorphismus $\tau\colon K(\alpha) \longrightarrow K'(\beta)$ mit

$$\tau(\alpha) = \beta \quad \text{und} \quad \sigma'|_K = \sigma.$$

Außerdem ist L ein Zerfällungskörper von g über $K(\alpha)$ und L' ein Zerfällungskörper von g^τ über $K'(\beta)$ (denn $f^\sigma = f^\tau = (T - \beta) \cdot g^\tau$). Nach Induktionsvoraussetzung gibt es daher einen Körperisomorphismus $\widetilde{\sigma}\colon L \longrightarrow L'$ mit $\widetilde{\sigma}|_{K(\alpha)} = \tau$. Insbesondere ist

$$\widetilde{\sigma}|_K = \tau|_K = \sigma. \qquad \square$$

Invarianten von Zerfällungskörpern liefern also Invarianten der gegebenen Polynome. Zum Beispiel erhält man auf diese Weise die Galoisgruppe von polynomialen Gleichungen:

Definition 3.2.45 (Galoisgruppe einer Gleichung)**.** Sei K ein Körper und sei $f \in K[T]$ ein normiertes Polynom. Ist L ein Zerfällungskörper von f über K, so bezeichnet man $\mathrm{Gal}(L, K)$ auch als *Galoisgruppe von f über K* bzw. als *Galoisgruppe der Gleichung $f(x) = 0$ in der Variablen x über K*.

Galoisgruppen von Gleichungen sind dabei strenggenommen nur bis auf Isomorphie wohldefiniert. Es ist daher besser, nur vom Isomorphietyp der Galoisgruppe eines Polynoms/einer Gleichung zu sprechen.

Beispiel 3.2.46 ($x^3 - 2 = 0$)**.** Zum Beispiel ist die Galoisgruppe von $T^3 - 2$ über $\mathbb{Q}$ isomorph zu S_3 (Beispiel 3.2.41).

Bei der Auflösbarkeit von polynomialen Gleichungen durch iteriertes Wurzelziehen spielen die Auflösbarkeitseigenschaften der zugehörigen Galoisgruppen eine entscheidende Rolle (Kapitel 3.5.2).

3.2.5 Der algebraische Abschluss

Möchte man nicht nur Nullstellen für ausgewählte Polynome, sondern für *alle* Polynome über einem gegebenen Körper zur Verfügung haben, geht man zum algebraischen Abschluss über:

Definition 3.2.47 (algebraischer Abschluss)**.**

- Ein Körper K ist *algebraisch abgeschlossen*, wenn jedes Polynom in $K[T]$ vom Grad mindestens 1 mindestens eine Nullstelle in K besitzt.
- Sei K ein Körper. Ein *algebraischer Abschluss von* K ist eine algebraische Körpererweiterung $L \mid K$, wobei L algebraisch abgeschlossen ist.

Beispiel 3.2.48 (algebraisch abgeschlossene Körper)**.**

- Der Körper $\mathbb{C}$ ist nach dem Fundamentalsatz der Algebra (Satz 3.5.27) algebraisch abgeschlossen. Da die Erweiterung $\mathbb{C} \mid \mathbb{R}$ algebraisch ist, ist $\mathbb{C} \mid \mathbb{R}$ somit ein algebraischer Abschluss von $\mathbb{R}$.

  Da die Erweiterung $\mathbb{C} \mid \mathbb{Q}$ *nicht* algebraisch ist, ist $\mathbb{C} \mid \mathbb{Q}$ *kein* algebraischer Abschluss von $\mathbb{Q}$.
- Sei $\overline{\mathbb{Q}} \subset \mathbb{C}$ der Körper der über $\mathbb{Q}$ algebraischen Zahlen in $\mathbb{C} \mid \mathbb{Q}$. Dann ist $\overline{\mathbb{Q}} \mid \mathbb{Q}$ ein algebraischer Abschluss von $\mathbb{Q}$ (nachrechnen; Korollar 3.2.36).
- Ist K ein endlicher Körper, so ist K *nicht* algebraisch abgeschlossen, denn das Polynom
$$\prod_{\alpha \in K} (T - \alpha) + 1 \in K[T]$$
hat Grad mindestens 1 aber *keine* Nullstelle in K.
- Ist K ein Körper, so ist der rationale Funktionenkörper $K(T)$ *nicht* algebraisch abgeschlossen: zum Beispiel besitzt das Polynom $X^2 - T \in K(T)[X]$ *keine* Nullstelle in $K(T)$ (nachrechnen oder mit dem Eisensteinschen Irreduzibilitätskriterium (Satz 2.2.61) argumentieren).

Bemerkung 3.2.49. Ein Körper K ist genau dann algebraisch abgeschlossen, wenn jedes Polynom in $K[T]$ vom Grad mindestens 1 über K in Linearfaktoren zerfällt (dies folgt induktiv mithilfe von Proposition 2.2.57).

Satz 3.2.50 (Existenz algebraischer Abschlüsse)**.** *Jeder Körper besitzt einen algebraischen Abschluss.*

Beweis. Der Beweis ist ähnlich zum Beweis der Existenz von Zerfällungskörpern. Wir zeigen dazu:

(C) Für jeden Körper K existiert eine algebraische Körpererweiterung

$$C(K) \mid K$$

von K, so dass jedes Polynom in $K[T]$ vom Grad mindestens 1 mindestens eine Nullstelle in $C(K)$ besitzt.

Warum folgt aus (C) die Existenz algebraischer Abschlüsse? Sei K ein Körper. Indem wir die Aussage (C) iterativ anwenden, erhalten wir den Körperturm

$$K \subset C(K) \subset C^2(K) \subset \dots.$$

Wir betrachten dann (dies ist ein Körper! (nachrechnen))

$$L := \bigcup_{n \in \mathbb{N}} C^n(K)$$

bzw. die zugehörige Körpererweiterung $L \mid K$. Diese Erweiterung $L \mid K$ ist ein algebraischer Abschluss von K, denn:

- Die Erweiterung $L \mid K$ ist algebraisch: Sei $\alpha \in L$. Dann gibt es ein $n \in \mathbb{N}$ mit $\alpha \in C^n(K)$. Da die Erweiterungen $C(K) \mid K$, $C^2(K) \mid C(K)$, ... algebraisch sind, ist auch die Erweiterung $C^n(K) \mid K$ algebraisch (Korollar 3.2.34). Also ist α algebraisch über K.
- Existenz von Nullstellen: Sei $f \in L[T]$ ein Polynom mit $\deg f \geq 1$. Jeder der endlich vielen nicht-trivialen Koeffizienten von f liegt in einem der Zwischenkörper $C^{\cdots}(K)$. Indem wir das Maximum der auftretenden Stufen betrachten, erhalten wir ein $n \in \mathbb{N}$ mit $f \in C^n(K)$. Dann besitzt f eine Nullstelle in $C^{n+1}(K)$. Wegen $C^{n+1}(K) \subset L$ hat f also insbesondere eine Nullstelle in L.

Um die Behauptung (C) zu zeigen, gehen wir analog zur Konstruktion von Zerfällungskörpern vor (Beweis von Satz 3.2.43); um Nullstellen von mehreren Polynomen auf einmal zu konstruieren, verwenden wir dabei einen Polynomring in entsprechend vielen Variablen. Ist $(T_i)_{i \in I}$ eine Familie von Variablen, so kann man den zugehörigen Polynomring $K[(X_i)_{i \in I}]$ über K zum Beispiel als

$$K[(X_i)_{i \in I}] := \bigcup_{J \in P^{\mathrm{fin}}(I)} K[(X_i)_{i \in J}]$$

aus Polynomringen in endlich vielen Variablen konstruieren; dabei ist $P^{\mathrm{fin}}(I)$ die Menge aller endlichen Teilmengen von I und die Vereinigung erfolgt bezüglich den kanonischen Inklusionen der einzelnen Polynomringe.

Sei $R := K\big[(T_f)_{f \in K[T] \setminus K}\big]$ der Polynomring über K mit durch $K[T] \setminus K$ indizierten Variablen. In R betrachten wir das Ideal

$$a := \big(\{f(T_f) \mid f \in K[T] \setminus K\}\big) = \mathrm{Span}_R\{f(T_f) \mid f \in K[T] \setminus K\} \subset R.$$

Dann ist $a \neq R$, denn: *Angenommen,* es wäre $a = R$, und damit $1 \in a$. Dann gäbe es eine endliche Teilmenge $F \subset K[T] \setminus K$ und Koeffizienten $(g_f)_{f\in F}$ in R mit

$$1 = \sum_{f\in F} g_f \cdot f(T_f).$$

Mit Satz 3.2.43 erhalten wir einen Erweiterungskörper K' von K, in dem jedes $f \in F$ eine Nullstelle $\alpha_f \in K'$ besitzt. Indem wir diese Nullstellen simultan für die (verschiedenen!) Variablen $(T_f)_{f\in F}$ (und für die anderen Variablen Null) einsetzen, bekommen wir in K' die Gleichung

$$1 = \sum_{f\in F} g_f\big((T_h \rightsquigarrow \alpha_h)_{h\in F}\big) \cdot f(\alpha_f) = 0,$$

was nicht sein kann. Also ist $a \neq R$. Daher gibt es ein maximales Ideal $m \subset R$ mit $a \subset m$ (Satz 2.2.18); wegen $1 \notin m$ ist dabei $m \cap K = \{0\}$. Somit erhalten wir den Körper

$$C(K) := R/m$$

(Satz 2.2.15) und einen kanonischen Körpermorphismus $K \longrightarrow C(K)$. Nach Konstruktion ist für jedes $f \in K[T] \setminus K$ die Restklasse von X_f in $C(K)$ eine Nullstelle von f; insbesondere ist die Erweiterung $C(K) \mid K$ algebraisch (Korollar 3.2.35). Damit ist (C) gezeigt.

In der obigen Konstruktion ist sogar bereits $C(K)$ ein algebraischer Abschluss von K [6, Aufgabe 11 in Kapitel 3.7]. □

Beispiel 3.2.51. Insbesondere gibt es algebraisch abgeschlossene Körper positiver Charakteristik, z.B. ein algebraischer Abschluss von $\mathbb{F}_2$.

Beispiel 3.2.52 (Jordansche Normalform)**.** Sei K ein Körper und $n \in \mathbb{N}$ und sei $L \mid K$ ein algebraischer Abschluss von K. Ist $A \in \mathrm{M}_{n\times n}(K)$, so gibt es nach dem Satz über die Jordansche Normalform (Satz II.3.3.1) eine Matrix $S \in \mathrm{GL}_n(L)$ mit der Eigenschaft, dass $S \cdot A \cdot S^{-1}$ über L in Jordan-Normalform ist.

Satz 3.2.53 (Eindeutigkeit algebraischer Abschlüsse)**.** *Sei K ein Körper und sei $M \mid K$ ein algebraischer Abschluss von K. Dann gilt:*

1. *Ist $L \mid K$ eine algebraische Erweiterung, so gibt es einen Morphismus von $L \mid K$ nach $M \mid K$.*
2. *Jeder Körperhomomorphismus $\sigma\colon M \longrightarrow M$ mit $\sigma|_K = \mathrm{id}_K$ ist ein Isomorphismus.*
3. *Ist $N \mid K$ ein algebraischer Abschluss von K, so sind die Erweiterungen $M \mid K$ und $N \mid K$ über K (i.a.* nicht *kanonisch) isomorph.*

Beweis. Analog zum Beweis der Eindeutigkeit von Zerfällungskörpern beruht der Beweis auf eine geeigneten Anwendung des Konjugationsprinzips.

Zu 1. Dies folgt mit dem Lemma von Zorn (Satz I.3.4.23) aus dem Konjugationsprinzip (Proposition 3.2.28): Wir betrachten dazu die Menge

$$F := \big\{(Z,f) \;\big|\; Z \text{ ist ein Zwischenkörper von } L \mid K \text{ und } f\colon Z \longrightarrow M \text{ ist ein Körpermorphismus mit } f|_K = \mathrm{id}_K\big\}.$$

Diese Menge ist durch Inklusion/Fortsetzung partiell geordnet und nichtleer (denn $(K, K \hookrightarrow M) \in F$). Außerdem besitzt jede total geordnete Kette $(Z_i, f_i)_{i\in I}$ in F eine obere Schranke in F, nämlich

$$\begin{aligned} \bigcup_{i\in I} Z_i &\longrightarrow M \\ Z_i \ni x &\longmapsto f_i(x) \end{aligned}$$

(nachrechnen). Nach dem Lemma von Zorn gibt es somit ein maximales Element (Z,f) in F. Dabei ist $Z = L$, denn:

Angenommen, $Z \neq L$. Dann gäbe es ein $\alpha \in L\backslash Z$. Da $L \mid K$ algebraisch ist, ist α algebraisch über K bzw. Z; sei $\mu_\alpha \in Z[T]$ das Minimalpolynom von α über Z. Da M algebraisch abgeschlossen ist, besitzt μ_α^f eine Nullstelle $\beta \in M$. Nach dem Konjugationsprinzip gibt es somit einen Körpermorphismus

$$\sigma\colon Z(\alpha) \longrightarrow M$$

mit $\sigma(\alpha) = \beta$ und $\sigma|_Z = f$. Dann ist $(Z(\alpha), \sigma)$ in F und echt größer als (Z,f), im Widerspruch zur Maximalität von (Z,f). Also ist $Z = L$, und damit ist $f\colon L = Z \longrightarrow M$ der gesuchte Morphismus.

Zu 2. Als Körpermorphismus ist σ injektiv (Proposition 3.1.8). Warum ist σ surjektiv? Sei $\beta \in M$. Da $M \mid K$ algebraisch ist, ist β algebraisch über K; sei $\mu_\beta \in K[T]$ das Minimalpolynom von β. Da σ ein (injektiver) Körpermorphismus ist, induziert σ eine (injektive) Abbildung

$$\big\{x \in M \;\big|\; \mu_\beta(x) = 0\big\} \longrightarrow \big\{x \in M \;\big|\; \mu_\beta(x) = 0\big\}$$

(Konjugationsprinzip; Proposition 3.2.28). Da die Menge dieser Nullstellen endlich ist, ist diese Abbildung bijektiv. Insbesondere liegt β im Bild dieser Abbildung, und damit auch im Bild von σ.

Zu 3. Dies folgt aus den ersten beiden Aussagen: Mit dem ersten Teil erhalten wir Körperhomomorphismen $f\colon M \longrightarrow N$ und $g\colon N \longrightarrow M$ mit $f|_K = \mathrm{id}_K$ und $g|_K = \mathrm{id}_K$.

Nach dem zweiten Teil sind $g \circ f\colon M \longrightarrow M$ und $f \circ g\colon M \longrightarrow M$ Isomorphismen. Also sind auch f und g bereits Isomorphismen. □

3.3 Endliche Körper

Wir verwenden die bisher entwickelten Techniken für Körpererweiterungen, um endliche Körper zu klassifizieren und Anwendungen der Theorie endlicher Körper zu geben.

3.3.1 Klassifikation endlicher Körper

Ist F ein endlicher Körper, so wissen wir bereits, dass es eine Primzahl p und ein $k \in \mathbb{N}_{>0}$ mit $\#F = p^k$ gibt (Beispiel 3.2.14). Wir müssen uns also nur noch überlegen, ob es zu jeder Primpotenz einen entsprechenden endlichen Körper gibt und ob dieser eindeutig (bis auf Isomorphie) ist.

Satz 3.3.1 (Klassifikation endlicher Körper)**.** *Sei $p \in \mathbb{N}$ prim und sei $k \in \mathbb{N}_{>0}$.*

1. *Dann gibt es bis auf Isomorphie genau einen Körper mit genau p^k Elementen. Dieser ist ein Zerfällungskörper (über dem Primkörper $\cong_{\mathsf{Ring}} \mathbb{F}_p$) des Polynoms*
$$T^{p^k} - T.$$

2. *Sei F ein Körper mit $\#F = p^k$ und Primkörper $K \cong_{\mathsf{Ring}} \mathbb{F}_p$. Dann ist*
$$\begin{aligned} \sigma \colon F &\longrightarrow F \\ x &\longmapsto x^p \end{aligned}$$
ein Automorphismus von $F \mid K$ (der Frobeniusendomorphismus*) und σ liefert einen Gruppenisomorphismus*
$$\begin{aligned} \mathbb{Z}/k &\longrightarrow \mathrm{Gal}(F, K) \\ [n] &\longmapsto \sigma^n. \end{aligned}$$

Beweis. Wir betrachten in diesem Beweis das Polynom

$$f := T^{p^k} - T \in \mathbb{F}_p[T].$$

Eindeutigkeit. Sei F ein endlicher Körper mit $\#F = p^k$. Dann ist $p = \operatorname{char} F$; ohne Einschränkung sei der Primkörper von F der Körper $\mathbb{F}_p$ (und nicht nur isomorph dazu).

Als ersten Schritt zeigen wir, dass alle Elemente von F Nullstellen von f sind: Mit dem Satz von Lagrange (Korollar 1.1.59) erhalten wir

$$\forall_{x \in F^\times} \quad x^{p^k - 1} = 1$$

bzw.

$$\forall_{x\in F} \quad f(x) = x^{p^k} - x = x \cdot (x^{p^k-1} - 1) = 0.$$

Warum ist F ein Zerfällungskörper von f ? Das Polynom f hat in F bereits $\#F = p^k = \deg f$ Nullstellen; also zerfällt f in F in Linearfaktoren (Korollar 2.2.58). Da jedes Element von F eine Nullstelle von f ist, ist F über $\mathbb{F}_p$ von den Nullstellen von f erzeugt. Somit ist F ein Zerfällungskörper von f über $\mathbb{F}_p$. Mit der Eindeutigkeit (bis auf Isomorphie) von Zerfällungskörpern (Satz 3.2.44) folgt somit die behauptete Eindeutigkeit im ersten Teil.

Bestimmung der Galoisgruppe. Wegen $\operatorname{char} F = p$ ist der Frobeniusendomorphismus $\sigma\colon F \longrightarrow F$ tatsächlich ein Körperisomorphismus mit $\sigma|_K = \mathrm{id}_K$ (Übungsaufgabe).

Warum erzeugt σ die Gruppe $\mathrm{Gal}(F, K)$? Dafür genügt es zu zeigen, dass $\#\operatorname{Gal}(F, K) \leq k$ und $\operatorname{ord}\sigma \geq k$ ist:

- Es ist $\#\operatorname{Gal}(F, K) \leq k$, denn: Die Einheitengruppe $F^\times$ ist zyklisch (Korollar 3.1.10). Sei $\alpha \in F^\times$ ein Erzeuger dieser Einheitengruppe; insbesondere ist $K(\alpha) = F$ (in $F \mid K$) und α ist algebraisch über K (da $F \mid K$ endlich ist). Mit der Galoisoperation (Korollar 3.2.29) folgt somit

  $$\#\operatorname{Gal}(F, K) \leq \big[K(\alpha) : K\big] = [F : K] = \log_p p^k = k.$$

- Außerdem ist $\operatorname{ord}\sigma \geq k$, denn: Sei $m := \operatorname{ord}\sigma \in \mathbb{N}_{>0}$. Dann ist $\sigma^m = \mathrm{id}_F$, d.h.

  $$\forall_{x\in F} \quad x^{p^m} = \sigma^m(x) = x.$$

  Also sind alle Elemente von F Nullstellen des Polynoms $T^{p^m} - T \in K[T]$. Somit ist (Korollar 2.2.58)

  $$p^k = \#F \leq \deg(T^{p^m} - T) = p^m,$$

  und damit $k \leq m$.

Also erzeugt σ die Gruppe $\mathrm{Gal}(F, K)$ und induziert somit einen Gruppenisomorphismus $\mathbb{Z}/k \cong_{\mathsf{Group}} \mathrm{Gal}(F, K)$.

Existenz. Sei F ein Zerfällungskörper von f über $\mathbb{F}_p$. Wir zeigen, dass $\#F = p^k$ ist: Sei $N \subset F$ die Menge der Nullstellen von f (in F).

Aus der Tatsache, dass der Frobeniusendomorphismus σ ein Körperhomomorphismus ist, folgt, dass N ein Körper ist (nachrechnen). Da N ein Zwischenkörper von $F \mid \mathbb{F}_p$ ist, der alle Nullstellen von f enthält, folgt somit $N = F$ (nach Konstruktion ist F ein Zerfällungskörper von f). Somit folgt

$$\#F = \boxed{?} \quad \#N \leq \deg f = p^k.$$

Es bleibt noch zu zeigen, dass $\#F = \#N \geq p^k$ ist, d.h., dass f in F *keine* mehrfachen Nullstellen enthält. Dazu verwenden wir das Ableitungskriterium (Proposition 3.3.3): Wegen

$$Df = \overset{?}{} \quad p^k \cdot T^{p^k-1} - 1 \cdot T^0 = -1$$

hat f in F keine mehrfachen Nullstellen. Also ist $\#N \geq \deg f = p^k$. □

Es bleibt, das Argument für mehrfache Nullstellen zu vervollständigen. In Anlehnung an die Analysis und als Verallgemeinerung von Proposition 2.2.57 definiert man mehrfache Nullstellen wie folgt:

Definition 3.3.2 (mehrfache Nullstelle)**.** Sei K ein Körper und sei $f \in K[T]$. Eine Nullstelle $\alpha \in K$ von f ist eine *mehrfache Nullstelle von* f, wenn $(T-\alpha)^2$ ein Teiler von f in $K[T]$ ist.

Proposition 3.3.3 (Ableitungskriterium für mehrfache Nullstellen)**.** *Sei K ein Körper, sei $f \in K[T]$ normiert und sei $L \mid K$ eine Körpererweiterung mit der Eigenschaft, dass f in $L[T]$ in Linearfaktoren zerfällt.*

1. *Das Polynom f besitzt genau dann eine mehrfache Nullstelle in L, wenn* $\operatorname{ggT}(f, Df) \neq 1$ *(in $K[T]$) ist.*
2. *Ist f in $K[T]$ irreduzibel, so besitzt f genau dann eine mehrfache Nullstelle in L, wenn $Df = 0$ ist.*

Dabei bezeichnet D die formale Ableitung *von Polynomen:*

$$\begin{aligned} D\colon K[T] &\longrightarrow K[T] \\ \sum_{j=0}^{n} a_j \cdot T &\longmapsto \sum_{j=1}^{n} a_j \cdot j \cdot T^{j-1} \end{aligned}$$

Beweis. Die erste Aussage folgt, indem man zunächst eine Leibnizregel für die formale Ableitung beweist, und sich dann überlegt, wie Nullstellen von f in L und von Df in L zusammenhängen. Die zweite Aussage kann man aus der ersten folgern (Übungsaufgabe). □

Anmerkung zum Lernen. Inwiefern kann man den ersten Teil von Satz 3.3.1 als eine Verallgemeinerung des kleinen Satzes von Fermat (Satz 2.2.26) auffassen?

Notation 3.3.4 (endliche Körper)**.** Sei $p \in \mathbb{N}$ prim und sei $k \in \mathbb{N}_{>0}$. Dann bezeichnet man „den“ (bis auf Isomorphie eindeutig bestimmen) Körper mit genau p^k Elementen mit $\mathbb{F}_{p^k}$. (Da Primpotenzen sowohl die Primzahl als auch den Exponenten eindeutig bestimmen, ist diese Notation wohldefiniert.)

Beispiel 3.3.5 (ein Körper mit vier Elementen)**.** Es gibt einen (bis auf Isomorphie eindeutigen) Körper mit $4 = 2^2$ Elementen (Satz 3.3.1). Zum Beispiel kann man diesen Körper auch als $\mathbb{F}_2[T]/(T^2+T+1)$ beschreiben (nachrechnen). Man beachte, dass dieser Körper als Ring *nicht* isomorph zu $\mathbb{Z}/(4)$ oder $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ (was ja *keine* Körper sind!) ist. Die *additive* Gruppe von F ist auch nicht isomorph zu $\mathbb{Z}/4$, sondern zu $\mathbb{Z}/2 \times \mathbb{Z}/2$ (nachrechnen).

Korollar 3.3.6 (Klassifikation der endlichen Körpererweiterungen von endlichen Körpern)**.** *Sei F ein endlicher Körper und sei $k \in \mathbb{N}_{\geq 1}$.*

1. *Bis auf Isomorphie gibt es genau eine Körpererweiterung $L \mid F$ über F vom Grad k.*

2. *Die Galoisgruppe dieser Körpererweiterung $L \mid F$ ist isomorph zu $\mathbb{Z}/k$, erzeugt vom relativen Frobeniusendomorphismus.*

Beweis. Dies folgt aus (dem Beweis von) Satz 3.3.1 (Übungsaufgabe) und der Tatsache, dass für jeden Körper K und alle $m, n \in \mathbb{N}$ das Polynom $T^m - T$ in $K[T]$ ein Teiler von $T^{m^n} - T$ ist. □

Bemerkung 3.3.7 (algebraische Abschlüsse endlicher Körper)**.** Sei $p \in \mathbb{N}$ prim und sei $L \mid \mathbb{F}_p$ ein algebraischer Abschluss von $\mathbb{F}_p = \mathbb{Z}/(p)$. Nach der Klassifikation endlicher Körper mit Charakteristik p (Satz 3.3.1, Korollar 3.3.6) ist L also eine (aufsteigende) Vereinigung von Zerfällungskörpern der Polynome $T^p - T$, $T^{p^2} - T$, $T^{p^{2\cdot 3}} - T \ldots$. Etwas salopp schreibt man dafür manchmal auch

$$L = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}.$$

3.3.2 Anwendungen endlicher Körper

In Kombination mit der Tatsache, dass endliche Körper zyklische Einheitengruppen haben, erhalten wir interessante Anwendungen endlicher Körper, insbesondere in der Informatik: Sogenannte *linear feedback shift registers (LFSR)* basieren auf der Theorie der endlichen Körper. solche LFSR kommen zum Beispiel bei der Erzeugung von Pseudozufallszahlen oder bei der praktischen Umsetzung von RAID(6) (zur Absicherung gegen Datenverlust) zum Einsatz. Diese Anwendungen sind in Anhang A.8 näher beschrieben.

3.4 Galoiserweiterungen

Für gutartige endliche Körpererweiterungen $L \mid K$ erwarten wir folgendes:

- Es gilt $\#\operatorname{Gal}(L, K) = [L : K]$
- und $K = L^{\operatorname{Gal}(L,K)} := \{x \in L \mid \forall_{f \in \operatorname{Gal}(L,K)} \quad f(x) = x\}$.
- Die Struktur (der Untergruppen) von $\operatorname{Gal}(L, K)$ korrespondiert zur Struktur (der Zwischenkörper) von $L \mid K$.

Es gibt zwei offensichtliche Weisen, in denen dies schiefgehen kann; beide haben damit zu tun, dass L „nicht genug“ Nullstellen enthält. Wir erklären dies in dem Fall, dass es ein $\alpha \in L$ mit $L = K(\alpha)$ gibt: Sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K. Mit dem Konjugationsprinzip (Korollar 3.2.29) erhalten wir:

① Wenn das Minimalpolynom μ_α über L *nicht* in Linearfaktoren zerfällt, ist $\#\operatorname{Gal}(L,K) < \deg \mu_\alpha = [L:K]$.

② Wenn μ_α über L zwar in Linearfaktoren zerfällt, aber mehrfache Nullstellen besitzt, ist $\#\operatorname{Gal}(L,K) < \deg \mu_\alpha = [L:K]$.

Das Problem in ① wird in sogenannten normalen Körpererweiterungen ausgeschlossen (Kapitel 3.4.1), das Problem in ② in sogenannten separablen Körpererweiterungen (Kapitel 3.4.2). Algebraische Erweiterungen, die normal und separabel sind, werden als Galoiserweiterungen bezeichnet (Kapitel 3.4.3) und haben das gewünschte Verhalten in Bezug auf die Galoisgruppe (Kapitel 3.4.4):

Satz 3.4.1 (Hauptsatz der Galoistheorie)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung.*

1. *Dann sind*

$$\begin{aligned} \mathsf{Subext}(L,K) &\longrightarrow \mathsf{Subgroup}\operatorname{Gal}(L,K) \\ M &\longmapsto \operatorname{Gal}(L,M) \\ \mathsf{Subgroup}\operatorname{Gal}(L,K) &\longrightarrow \mathsf{Subext}(L,K) \\ H &\longmapsto L^H \end{aligned}$$

   zueinander inverse Bijektionen. Dabei bezeichnet $\mathsf{Subgroup}\operatorname{Gal}(L,K)$ *die Menge aller Untergruppen von* $\operatorname{Gal}(L,K)$ *und* $\mathsf{Subext}(L,K)$ *die Menge aller Zwischenkörper von $L \mid K$.*

2. *Sei M ein Zwischenkörper von $L \mid K$. Dann ist die Körpererweiterung $M \mid K$ genau dann normal, wenn* $\operatorname{Gal}(L,M)$ *ein Normalteiler in* $\operatorname{Gal}(L,K)$ *ist. In diesem Fall ist*

$$\begin{aligned} \operatorname{Gal}(L,K)/\operatorname{Gal}(L,M) &\longrightarrow \operatorname{Gal}(M,K) \\ [\sigma] &\longmapsto \sigma|_M \end{aligned}$$

   ein wohldefinierter Gruppenisomorphismus.

Im folgenden entwickeln wir die nötige Theorie zu normalen und separablen Körpererweiterungen, um diesen Satz zu beweisen. Anwendungen geben wir in Kapitel 3.5.

3.4.1 Normale Körpererweiterungen

Definition 3.4.2 (normale Körpererweiterung)**.** Eine algebraische Körpererweiterung $L \mid K$ ist *normal*, wenn für jedes $\alpha \in L$ das Minimalpolynom von α über K bereits in $L[T]$ in Linearfaktoren zerfällt.

Die Bezeichnung solcher Körpererweiterungen als „normal“ hängt mit dem Normalteilerbegriff für Gruppen zusammen, wie wir im Hauptsatz der Galoistheorie sehen.

Beispiel 3.4.3 (normale Erweiterungen)**.**

- Jede Körpererweiterung vom Grad 2 ist normal (nachrechnen).
- Ist $L \mid K$ ein algebraischer Abschluss eines Körpers K, so ist die Körpererweiterung $L \mid K$ normal.
- Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ ist *nicht* normal (Beispiel 3.2.41).

Caveat 3.4.4. Normalität von Körpererweiterungen ist im allgemeinen *nicht* transitiv, denn: Die Körpererweiterungen (in $\mathbb{C} \mid \mathbb{Q}$)

$$\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}(\sqrt{2}) \quad \text{und} \quad \mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$$

sind normal (da beide vom Grad 2 sind), aber die zusammengesetzte Körpererweiterung

$$\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}$$

ist *nicht* normal (da die nicht-reellen Nullstellen des Minimalpolynoms $T^4 - 2$ von $\sqrt[4]{2}$ nicht in $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ enthalten sind).

Man erinnere sich bei dieser Gelegenheit daran, dass auch die Normalteilereigenschaft in der Gruppentheorie im allgemeinen *nicht* transitiv ist (Caveat 1.3.30).

Die folgenden beiden Kriterien helfen in vielen Fällen, Normalität nachzuweisen:

Proposition 3.4.5 (alternative Charakterisierung von Normalität)**.** *Sei $L \mid K$ eine algebraische Körpererweiterung und sei $M \mid L$ ein algebraischer Abschluss von L. Dann sind äquivalent:*

1. *Die Körpererweiterung $L \mid K$ ist normal.*
2. *Es gibt eine Teilmenge $S \subset L$ mit $L = K(S)$ und der Eigenschaft, dass für jedes $\alpha \in S$ das Minimalpolynom von α über K in $L[T]$ in Linearfaktoren zerfällt.*
3. *Für jeden Körperhomomorphismus $\sigma\colon L \longrightarrow M$ mit $\sigma|_K = \mathrm{id}_K$ gilt bereits $\sigma(L) \subset L$.*

Beweis. *Zu* 1. $\Longrightarrow$ 2. Wir können $S = L$ wählen; dann folgt dies direkt aus der Definition.

Zu 2. $\Longrightarrow$ 3. Diese Implikation folgt aus dem Konjugationsprinzip (Proposition 3.2.28): Sei S wie in Aussage 2. und sei $\sigma\colon L \longrightarrow M$ ein Körperhomomorphismus mit $\sigma|_K = \mathrm{id}_K$. Da $L = K(S)$ und da $\sigma(L)$ ein Körper ist, genügt es zu zeigen, dass $\sigma(S) \subset L$ ist.

Sei $\alpha \in S$. Aus der Voraussetzung, dass das Minimalpolynom von α über K bereits über L in Linearfaktoren zerfällt, folgt mit dem Konjugationsprinzip (Proposition 3.2.28), dass $\sigma(\alpha) \in L$.

Zu 3. $\Longrightarrow$ 1. Es gelte Aussage 3. Dann ist $L \mid K$ normal, denn: Sei $\alpha \in L$, sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K. Da μ_α über dem algebraischen Abschluss M in Linearfaktoren zerfällt, genügt es zu zeigen, dass alle M-Nullstellen von μ_α bereits in L liegen.

Sei also $\beta \in M$ eine Nullstelle von μ_α. Nach dem Konjugationsprinzip (Proposition 3.2.28) existiert ein Körperhomomorphismus $\sigma\colon K(\alpha) \longrightarrow M$ mit $\sigma|_K = \mathrm{id}_K$ und $\sigma(\alpha) = \beta$. Analog zum Beweis der Eindeutigkeit von algebraischen Abschlüssen (Satz 3.2.53) können wir mithilfe des Konjugationsprinzips und Induktion bzw. des Zornschen Lemmas den Körperhomomorphismus σ zu einem Körperhomomorphismus $\widetilde{\sigma}\colon L \longrightarrow M$ mit $\widetilde{\sigma}|_{K(\alpha)} = \sigma$ fortsetzen. Nach Voraussetzung ist also

$$\beta = \sigma(\alpha) = \widetilde{\sigma}(\alpha) \in \widetilde{\sigma}(L) \subset L. \qquad \square$$

Beispiel 3.4.6. Zerfällungskörper liefern also normale Körpererweiterungen.

Beispiel 3.4.7. Ist $L \mid K$ eine algebraische Erweiterung eines *endlichen* Körpers K, so ist die Erweiterung $L \mid K$ bereits normal, denn: Sei $\alpha \in L$ und $M := K(\alpha) \subset L$; dann ist $M \mid K$ eine endliche Erweiterung. Also ist M ein Zerfällungskörper eines Polynoms über dem Primkörper P von K (Satz 3.3.1); somit ist $M \mid P$ normal (Proposition 3.4.5). Dann ist auch $M \mid K$ normal (nachrechnen).

3.4.2 Separable Körpererweiterungen

Definition 3.4.8 (separables Polynom, separable Körpererweiterung)**.** Sei K ein Körper und sei $M \mid K$ ein algebraischer Abschluss von K.

- Ein normiertes Polynom $f \in K[T]$ ist *separabel (über K)*, wenn es über M in paarweise verschiedene normierte Linearfaktoren zerfällt (äquivalent: wenn es in M keine mehrfachen Nullstellen besitzt).

- Sei $L \mid K$ eine Körpererweiterung. Ein über K algebraisches Element $\alpha \in L$ ist *separabel über K*, wenn das Minimalpolynom von α über K separabel ist.

- Eine algebraische Körpererweiterung $L \mid K$ ist *separabel*, wenn jedes Element aus L separabel über K ist.

- Ist $L \mid K$ eine Körpererweiterung, so bezeichnet man die Anzahl

$$[L : K]_s := \#\{\sigma \colon L \longrightarrow M \mid \sigma \text{ ist ein Körpermorphismus und } \sigma|_K = \mathrm{id}_K\}$$

der Einbettungen von $L \mid K$ nach $M \mid K$ als *Separabilitätsgrad* der Erweiterung $L \mid K$.

Bemerkung 3.4.9. Die obigen Begriffe sind unabhängig vom gewählten algebraischen Abschluss, da ? algebraische Abschlüsse bis auf Isomorphie eindeutig bestimmt sind (Satz 3.2.53) und die obigen Eigenschaften unter Isomorphie von Körpererweiterungen erhalten bleiben (nachrechnen).

Beispiel 3.4.10 (Separabilität)**.** Mit dem Ableitungskriterium für mehrfache Nullstellen (Proposition 3.3.3) folgt:

- Ist K ein Körper mit $\operatorname{char} K = 0$ und ist $f \in K[T]$ normiert und irreduzibel, so ist f separabel (denn $Df \neq 0$; nachrechnen). Insbesondere sind algebraische Körpererweiterungen in Charakteristik 0 separabel.

- Ist F ein endlicher Körper der Charakteristik p, ist $L \mid F$ eine algebraische Körpererweiterung und ist $\alpha \in L \setminus \{0\}$, so ist das Minimalpolynom μ_α von α über F ein Teiler eines Polynoms $T^{p^k} - T$ mit $k \in \mathbb{N}_{>0}$ (Beweis von Satz 3.3.1). Da $T^{p^k} - T$ nach dem Ableitungskriterium über F separabel ist, ist somit auch μ_α über F separabel. Also ist die Körperweiterung $L \mid F$ separabel.

- Ist $p \in \mathbb{N}$ prim, so ist das normierte Polynom

$$X^p - T \in \mathbb{F}_p(T)[X]$$

über $\mathbb{F}_p(T)$ irreduzibel (nach dem Eisensteinschen Irreduzibilitätskriterium; Satz 2.2.61) und nach dem Ableitungskriterium (in der Variablen X) *nicht* separabel. Insbesondere ist die Körpererweiterung

$$\begin{array}{c} \mathbb{F}_p(T)[X]/(X^p - T) \\ \Big| \\ \mathbb{F}_p(T) \end{array}$$

algebraisch, aber *nicht* separabel.

Bemerkung 3.4.11 (vollkommene/perfekte Körper)**.** Ist K ein Körper mit der Eigenschaft, dass jede algebraische Erweiterung über K separabel ist, so bezeichnet man K auch als *perfekten* oder *vollkommenen* Körper. Mit Beispiel folgt somit:

- Jeder Körper mit Charakteristik 0 ist perfekt.
- Jeder endliche Körper ist perfekt.
- Ist $p \in \mathbb{N}$ prim, so ist $\mathbb{F}_p(T)$ *kein* perfekter Körper.

Proposition 3.4.12 (Separabilität von einfachen Erweiterungen)**.** *Sei $L \mid K$ eine Körpererweiterung und sei $\alpha \in L$ algebraisch über K. Dann sind die folgenden Aussagen äquivalent:*

1. *Das Element α ist separabel über K.*
2. *Es gilt $[K(\alpha) : K]_s = [K(\alpha) : K]$.*

Beweis. Dies ist eine Umformulierung des Konjugationsprinzips (Proposition 3.2.28, Korollar 3.2.29), denn: Ist $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K und ist $M \mid K$ ein algebraischer Abschluss von K, so gilt

$$\begin{aligned} \big[K(\alpha) : K\big] &= \deg \mu_\alpha \\ \big[K(\alpha) : K\big]_s &= \#\big\{x \in M \;\big|\; \mu_\alpha(x) = 0\big\}. \end{aligned}$$

□

Satz 3.4.13 (Satz vom primitiven Element)**.** *Sei $L \mid K$ eine endliche separable Körpererweiterung.*

1. *Dann gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.*
2. *Insbesondere gilt*
$$[L : K]_s = [L : K].$$

Beweis. Zu 2. Der zweite Teil folgt mithilfe von Propoosition 3.4.12 aus dem ersten Teil.

Zu 1. Wir unterscheiden zwei Fälle: Ist K endlich, so ist auch L endlich, und damit ist $L^\times$ zyklisch (Korollar 3.1.10). Insbesondere hat dann jeder Erzeuger α von $L^\times$ die Eigenschaft, dass $L = K(\alpha)$ ist.

Sei im folgenden K unendlich. Indem wir induktiv vorgehen, genügt es, die Behauptung für den Fall $L = K(\beta, \gamma)$ mit $\beta, \gamma \in L$ zu beweisen (nachrechnen). Sei $n := [L : K]_s$. Wir zeigen:

① Es gibt ein $\alpha \in L$ mit $[K(\alpha) : K] \geq n$.

② Es gilt dann bereits $K(\alpha) = L$.

Zu ①. Sei $M \mid K$ ein algebraischer Abschluss von K und seien $\sigma_1, \dots, \sigma_n$ die n Körpermorphismen $L \longrightarrow M$. Die Idee ist, das Polynom

$$f := \prod_{j,k \in \{1,\dots,n\}, j<k} \Big(\big(\sigma_j(\beta) - \sigma_k(\beta)\big) + \big(\sigma_j(\gamma) - \sigma_k(\gamma)\big) \cdot T \Big) \in M[T]$$

zu betrachten. Da die $\sigma_1, \dots, \sigma_n$ alle verschieden sind und wegen $L = K(\beta, \gamma)$ durch ihre Werte auf $\{\beta, \gamma\}$ eindeutig bestimmt sind, ist f *nicht* das Nullpolynom (nachrechnen). Also besitzt f in K nur endlich viele Nullstellen (Korollar 2.2.58). Da K unendlich ist, gibt es somit ein $x \in K$ mit $f(x) \neq 0$. Wir betrachten

$$\alpha := \beta + x \cdot \gamma \in L$$

und die „konjugierten“ Elemente

$$\alpha_j := \sigma_j(\alpha) \in M$$

mit $j \in \{1, \dots, n\}$.

Die Elemente $\alpha_1, \dots, \alpha_n$ sind alle verschieden, denn: Für alle $j \in \{1, \dots, n\}$ ist

$$\alpha_j = \sigma_j(\alpha) = \sigma_j(\beta + x \cdot \gamma) = \sigma_j(\beta) + x \cdot \sigma_j(\gamma).$$

Wegen $f(x) \neq 0$ zeigt die Konstruktion von f, dass $\alpha_j \neq \alpha_k$ für alle $j, k \in \{1, \dots, n\}$ mit $j \neq k$ gilt.

Sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K. Mit dem Konjugationsprinzip (Proposition 3.2.28) folgt, dass μ_α in M mindestens die n Nullstellen $\alpha_1, \dots, \alpha_n$ besitzt. Also ist

$$\big[K(\alpha) : K\big] = \deg \mu_\alpha \geq n.$$

Zu ②. Es ist $K(\alpha) \subset L$. Sei umgekehrt $z \in L$. Es genügt zu zeigen, dass $z \in K(\alpha)$ ist bzw. dass $[K(\alpha)(z) : K(\alpha)] = 1$ ist.

Mit dem Konjugationsprinzip und ① erhalten wir

$$\begin{aligned}
n &= [L : K]_s && \text{(Definition von } n\text{)} \\
&\geq \big[K(\alpha)(z) : K\big]_s && \text{(Wegen } K(\alpha, z) \subset L\text{; Konjugationsprinzip)} \\
&\geq \big[K(\alpha)(z) : K(\alpha)\big]_s \cdot \big[K(\alpha) : K\big]_s && \text{(Konjugationsprinzip)} \\
&= \big[K(\alpha)(z) : K(\alpha)\big]_s \cdot \big[K(\alpha) : K\big] && \text{(Proposition 3.4.12, } \alpha \text{ ist separabel über } K\text{)} \\
&\geq \big[K(\alpha)(z) : K(\alpha)\big]_s \cdot n. && \text{(Teil ①)}
\end{aligned}$$

Da das Minimalpolynom von z über K (bzw. dann auch über $K(\alpha)$) nach Voraussetzung separabel ist, folgt mit Proposition 3.4.12

$$\big[K(\alpha)(z) : K(\alpha)\big]_s = \big[K(\alpha)(z) : K(\alpha)\big].$$

Also ist

$$n = [L : K]_s \geq \big[K(\alpha)(z) : K(\alpha)\big] \cdot n = \big[K(\alpha)(z) : K(\alpha)\big] \cdot n \geq n,$$

und damit $[K(\alpha)(z) : K(\alpha)] = 1$, wie gewünscht. □

Bemerkung 3.4.14. Der Beweisschritt ① im Satz vom primitiven Element (Satz 3.4.13) gibt eine Anleitung, mit der man (induktiv) primitive Elemente finden kann.

Beispiel 3.4.15 (Konstruktion eines primitiven Elements)**.** Wir betrachten die Eweiterung $\mathbb{Q}(i, \sqrt{2}) \mid \mathbb{Q}$ (in $\mathbb{C} \mid \mathbb{Q}$). Diese Erweiterung ist endlich und separabel. Wir bestimmen mit dem Verfahren aus dem Beweis des Satzes vom primitiven Element ein primitives Element für diese Erweiterung:

Wir betrachten dazu den algebraischen Abschluss $\overline{\mathbb{Q}} \mid \mathbb{Q}$ von $\mathbb{Q}$ aus Beispiel 3.2.48. Es gibt genau vier Körpermorphismen $\mathbb{Q}(i, \sqrt{2}) \longrightarrow \overline{\mathbb{Q}}$ über $\mathbb{Q}$ und diese sind durch die folgende Wertetabelle eindeutig bestimmt (nachrechnen):

	i	$\sqrt{2}$
σ_1	i	$\sqrt{2}$
σ_2	$-i$	$\sqrt{2}$
σ_3	i	$-\sqrt{2}$
σ_4	$-i$	$-\sqrt{2}$

Mit der Notation aus dem Beweis von Satz 3.4.13 erhalten wir das Polynom

$$f = 2 \cdot i \cdot 2 \cdot \sqrt{2} \cdot T \cdot (2 \cdot i + 2\sqrt{2} \cdot T) \cdot (-2 \cdot i + 2 \cdot \sqrt{2} \cdot T) \cdot 2 \cdot \sqrt{2} \cdot T \cdot 2 \cdot i.$$

Wegen $f(1) \neq 0$ ist also $\mathbb{Q}(i + 1 \cdot \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$ (s. Beweis von Satz 3.4.13).

3.4.3 Galoiserweiterungen

Wie bereits angekündigt, werden wir uns nun mit algebraischen Körpererweiterungen beschäftigen, die „genug Nullstellen“ enthalten:

Definition 3.4.16 (Galoiserweiterung)**.** Eine *Galoiserweiterung* ist eine algebraische Körpererweiterung, die normal und separabel ist.

Bemerkung 3.4.17 (Évariste Galois)**.** Die Galoistheorie geht auf den französischen Mathematiker Évariste Galois (25. Oktober 1811–31. Mai 1832) zurück. Galois hat die Auflösbarkeit von polynomialen Gleichungen durch Radikale untersucht; er hat dabei die Galoisgruppe als Symmetriegruppe der Lösungen (und damit auch die algebraische Sicht auf den Gruppenbegriff!) eingeführt und den Zusammenhang zwischen algebraischen Eigenschaften der Galoisgruppe von Zerfällungskörpern und der Auflösbarkeit von polynomialen Gleichungen entdeckt. Seine letzte Fassung dieser Erkenntnisse (sowie weitere Ergebnisse) hat er in wenigen Tagen vor seinem letztlich fatalen Duell (!) am 30. Mai 1832 in Briefen an Chevalier skizziert ...

Beispiel 3.4.18 (Galoiserweiterungen)**.**

- Ist K ein Körper der Charakteristik 0 oder ein endlicher Körper, so ist jeder algebraische Abschluss $L \mid K$ von K eine Galoiserweiterung.
- Ist K ein Körper der Charakteristik 0 und ist $f \in K[T]$ ein normiertes Polynom, so liefert jeder Zerfällungskörper L von f über K eine Galoiserweiterung $L \mid K$ (Proposition 3.4.5).
- Endliche Erweiterungen von endlichen Körpern sind Galoiserweiterungen (Beispiel 3.4.7, Beispiel 3.4.11).
- Es ist $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ *keine* Galoiserweiterung, da diese Erweiterung *nicht* normal ist (Beispiel 3.4.3).
- Ist $p \in \mathbb{N}$ prim, so ist $\mathbb{F}_p(T)[X]/(X^p - T) \mid \mathbb{F}_p(T)$ *keine* Galoiserweiterung, da diese Erweiterung *nicht* separabel ist (Beispiel 3.4.11).

Wir zeigen, dass für Galoiserweiterungen tatsächlich der angestrebte Zusammenhang zwischen Grad, Galoisgruppe und Fixkörpern besteht.

Proposition 3.4.19 (Grad endlicher Galoiserweiterungen)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung. Dann ist*

$$[L : K] = [L : K]_s = \#\operatorname{Gal}(L, K).$$

Beweis. Nach dem Satz vom primitiven Element (Satz 3.4.13) gibt es $\alpha \in L$ mit $L = K(\alpha)$ und

$$[L : K] = \big[K(\alpha) : K\big] = \big[K(\alpha) : K\big]_s = [L : K]_s.$$

Da die Körpererweiterung $K(\alpha) \mid K$ normal ist, erhalten wir aus dem Konjugationsprinzip (Proposition 3.2.28 und Proposition 3.4.5) auch

$$\big[K(\alpha) : K\big]_s = \#\operatorname{Gal}\big(K(\alpha), K\big) = \#\operatorname{Gal}(L, K).$$

Zusammen liefern diese Beobachtungen die behauptete Gleichungskette. □

Satz 3.4.20 (Fixkörper)**.** *Sei $L \mid K$ eine Körpererweiterung, sei G eine endliche Untergruppe von* $\operatorname{Gal}(L, K)$ *und sei*

$$L^G := \big\{x \in L \;\big|\; \forall_{\sigma \in G} \quad \sigma(x) = x\big\}$$

der zugehörige Fixkörper*. Dann gilt:*

1. *Es ist L^G ein Zwischenkörper von $L \mid K$.*
2. *Es ist $L \mid L^G$ eine Galoiserweiterung.*
3. *Es gilt*
$$[L : L^G] = \#G \quad \textit{und} \quad \operatorname{Gal}(L, L^G) = G.$$

Beweis. Zu 1. Dies ist eine einfache Rechnung (Übungsaufgabe).

Zu 2. Dass die Erweiterung $L \mid L^G$ normal und separabel ist, kann man mit dem folgenden Trick von Artin zeigen (Übungsaufgabe): Sei $\alpha \in L$ und sei $(\sigma_1, \dots, \sigma_m)$ eine maximale Familie in G, für die $\sigma_1(\alpha), \dots, \sigma_m(\alpha)$ alle verschieden sind. Dann liegt das Polynom

$$f := \prod_{j=1}^{m} \big(T - \sigma_j(\alpha)\big) \in L[T].$$

bereits in $L^G[T]$ (Übungsaufgabe). Insbesondere folgt daraus:

- Das Element α ist algebraisch über L^G.
- Das Minimalpolynom von α über L^G hat höchstens Grad $\#G$ (und damit $[L^G(\alpha) : L^G] \leq \#G$) und
- es zerfällt in L in paarweise verschiedene Linearfaktoren.

Also ist die Erweiterung $L \mid L^G$ normal und separabel, d.h. eine Galoiserweiterung.

Zu 3. Da die Grade von Elementen über L^G nach dem Beweis des zweiten Teils durch $\#G$ nach oben beschränkt sind, gibt es ein $\alpha \in L$, für das $[L^G(\alpha) : L^G]$ maximal ist.

Wir zeigen, dass dann bereits $L^G(\alpha) = L$ ist: Sei $\beta \in L$. Dann ist $L^G(\alpha)(\beta) \mid L^G$ endlich (nach der Schranke aus dem zweiten Teil) und separabel (da nach dem zweiten Teil $L \mid L^G$ separabel ist). Nach dem Satz vom primitiven Element (Satz 3.4.13) gibt es ein $\alpha' \in L$ mit $L^G(\alpha)(\beta) = L^G(\alpha')$. Mit der Maximalität von α folgt

$$\big[L^G(\alpha) : L^G\big] \geq \big[L^G(\alpha') : L^G\big] = \big[L^G(\alpha)(\beta) : L^G(\alpha)\big] \cdot \big[L^G(\alpha) : L^G\big]$$

und damit $[L^G(\alpha)(\beta) : L^G(\alpha)] = 1$ bzw. $\beta \in L^G(\alpha)$. Also ist $L^G(\alpha) = L$.

Nach Definition des Fixkörpers L^G ist $G \subset \mathrm{Gal}(L, L^G)$. Also erhalten wir mit Proposition 3.4.19 das Ungleichungs-Sandwich

$$\#G \leq \#\,\mathrm{Gal}(L, L^G) = [L : L^G] = \big[L^G(\alpha) : L^G\big] \leq \#G,$$

und daher bereits Gleichheit in dieser Kette. Da G endlich ist und $G \subset \mathrm{Gal}(L, L^G)$ ist, liefert dies auch $G = \mathrm{Gal}(L, L^G)$. □

Korollar 3.4.21 (Fixkörper der Galoisgruppe)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung. Dann ist*

$$L^{\mathrm{Gal}(L,K)} = K.$$

Beweis. Sei $G := \mathrm{Gal}(L, K)$. Einerseits ist $[L : K] = \#G$. (Proposition 3.4.19); andererseits gilt $[L : L^G] = \#G$ (Satz 3.4.20). Mit der Multiplikativität des Grades (Proposition 3.2.10) erhalten wir also

$$[L^G : K] = \text{?} \quad \frac{[L:K]}{[L:L^G]} = \frac{\#G}{\#G} = 1,$$

und damit $L^G = K$. □

Korollar 3.4.22 (Realisierung von endlichen Gruppen als Galoisgruppen)**.** *Sei G eine endliche Gruppe. Dann gibt es eine Galoiserweiterung $L \mid K$ mit*

$$\mathrm{Gal}(L,K) \cong_{\mathsf{Group}} G.$$

Beweis. Sei $n := \#G$ und sei K ein Körper. Nach dem Satz von Cayley (Satz 1.2.9) ist G zu einer Untergruppe von S_n isomorph. Die Gruppe S_n operiert via Permutation der Variablen durch Körperisomorphismen auf dem Körper

$$L := K(T_1, \ldots, T_n) := Q\big(K[T_1, \ldots, T_n]\big);$$

dies liefert eine zu S_n isomorphe Untergruppe S in $\mathrm{Gal}(L,K)$ (nachrechnen). Außerdem ist G nach Konstruktion zu einer Untergruppe H von S isomorph.

Nach Satz 3.4.20 ist $L \mid L^H$ eine endliche Galoiserweiterung mit

$$\mathrm{Gal}(L, L^H) = H \cong_{\mathsf{Group}} G$$ □

Caveat 3.4.23. Es ist ein offenes Problem, zu entscheiden, welche (Isomorphietypen von) endlichen Gruppen als Galoisgruppen von Galoiserweiterungen über $\mathbb{Q}$ auftreten können. (Bei der Konstruktion im Beweis von Korollar 3.4.22 haben wir kaum Kontrolle über den entstehenden Grundkörper.)

3.4.4 Der Hauptsatz der Galoistheorie

Wir fassen die Ergebnisse zu Galoiserweiterungen zusammen:

Satz 3.4.24 (Hauptsatz der Galoistheorie)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung.*

1. *Dann sind*

$$\begin{aligned} \mathsf{Subext}(L,K) &\longrightarrow \mathsf{Subgroup}\,\mathrm{Gal}(L,K) \\ M &\longmapsto \mathrm{Gal}(L,M) \\ \mathsf{Subgroup}\,\mathrm{Gal}(L,K) &\longrightarrow \mathsf{Subext}(L,K) \\ H &\longmapsto L^H \end{aligned}$$

   zueinander inverse Bijektionen. Dabei bezeichnet $\mathsf{Subgroup}\,\mathrm{Gal}(L,K)$ *die Menge aller Untergruppen von* $\mathrm{Gal}(L,K)$ *und* $\mathsf{Subext}(L,K)$ *die Menge aller Zwischenkörper von $L \mid K$.*

2. *Sei M ein Zwischenkörper von $L \mid K$. Dann ist die Körpererweiterung $M \mid K$ genau dann normal, wenn $\mathrm{Gal}(L,M)$ ein Normalteiler*

in $\mathrm{Gal}(L,K)$ *ist. In diesem Fall ist*

$$\begin{aligned}\mathrm{Gal}(L,K)/\mathrm{Gal}(L,M) &\longrightarrow \mathrm{Gal}(M,K)\\ [\sigma] &\longmapsto \sigma|_M\end{aligned}$$

ein wohldefinierter Gruppenisomorphismus.

Zwischenkörper von Galoiserweiterungen $L \mid K$ werden also durch die zugehörigen Untergruppen der Galoisgruppe $\mathrm{Gal}(L,K)$ klassifiziert. Dies kann in beide Richtungen verwendet werden:

- Versteht man die Untergruppen von $\mathrm{Gal}(L,K)$ gut genug, so kann man damit Zwischenkörper von $L \mid K$ untersuchen.
- Versteht man Zwischenkörper von $L \mid K$ gut genug, so kann man damit die Gruppe $\mathrm{Gal}(L,K)$ besser verstehen.

Zusätzlich hilft bei der Analyse der Zwischenkörper/Galoisgruppe der Zusammenhang zwischen Graden und Größenbegriffen aus der Gruppentheorie:

Bemerkung 3.4.25. Sei $L \mid K$ eine endliche Galoiserweiterung und sei M ein Zwischenkörper von $L \mid K$. Mit dem Hauptsatz der Galoistheorie (Satz 3.4.24) und Satz 3.4.20 erhalten wir für die beiden zugehörigen Körpergrade:

$$\begin{aligned}[L:M] &= [L:L^{\mathrm{Gal}(L,M)}] = \#\,\mathrm{Gal}(L,M)\\ [M:K] &= \frac{[L:K]}{[L:M]} = \frac{\#\,\mathrm{Gal}(L,K)}{\#\,\mathrm{Gal}(L,M)} = \big[\mathrm{Gal}(L,K) : \mathrm{Gal}(L,M)\big].\end{aligned}$$

Beweis von Satz 3.4.24. Zu 1. Sei $H \subset \mathrm{Gal}(L,K)$ eine Untergruppe; da $\mathrm{Gal}(L,K)$ endlich ist (Proposition 3.4.19), ist H eine endliche Gruppe. Dann ist L^H ein Zwischenkörper von $L \mid K$ und Satz 3.4.20 liefert

$$\mathrm{Gal}(L,L^H) = H.$$

Sei umgekehrt M ein Zwischenkörper von $L \mid K$. Dann ist $L \mid M$ eine endliche Galoiserweiterung (nachrechnen) und wir wissen bereits (Korollar 3.4.21), dass

$$M = L^{\mathrm{Gal}(L,M)},$$

Zu 2. Sei M ein Zwischenkörper von $L \mid K$ und sei $H := \mathrm{Gal}(L,M)$.

- Sei $M \mid K$ normal. Dann ist H ein Normalteiler in $\mathrm{Gal}(L,K)$, denn: Da $M \mid K$ normal ist, ist

$$\begin{aligned}R\colon\ \mathrm{Gal}(L,K) &\longrightarrow \mathrm{Gal}(M,K)\\ \sigma &\longmapsto \sigma|_M\end{aligned}$$

ein wohldefinierter (nachrechnen mithilfe des Konjugationsprinzips; Proposition 3.2.28) Gruppenhomomorphismus (nachrechnen).

Wir wenden den Homomorphiesatz (Korollar 1.1.51) auf R an: Der Gruppenhomomorphismus R ist surjektiv (nachrechnen; dies folgt wie in Beispiel 3.2.41 mit dem Konjugationsprinzip). Nach Konstruktion ist

$$\ker R = \left\{\sigma \in \mathrm{Gal}(L,K) \;\middle|\; \sigma|_M = \mathrm{id}_M\right\} = \mathrm{Gal}(L,M).$$

Also ist $\mathrm{Gal}(L,M)$ ein Normalteiler in $\mathrm{Gal}(L,K)$ und R induziert den behaupteten Isomorphismus $\mathrm{Gal}(L,K)/\mathrm{Gal}(L,M) \cong_{\mathsf{Group}} \mathrm{Gal}(M,K)$.

- Sei umgekehrt H ein Normalteiler in $\mathrm{Gal}(L,K)$. Dann ist die Erweiterung $M \mid K$ normal, denn: Sei $\alpha \in M$, sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K. Da $L \mid K$ eine normale Körpererweiterung ist, zerfällt μ_α über L in Linearfaktoren und es genügt zu zeigen, dass jede Nullstelle in L von μ_α bereits in M liegt.

  Sei also $\beta \in L$ eine Nullstelle von μ_α. Wegen $M = L^H$ (nach dem ersten Teil) genügt es zu zeigen, dass β im Fixkörper L^H liegt. Durch (mehrfache) Anwendung des Konjugationsprinzips (Proposition 3.2.28) erhalten wir einen Körperisomorphismus $\sigma \in \mathrm{Gal}(L,K)$ mit

  $$\sigma(\alpha) = \beta.$$

  Da H ein Normalteiler in $\mathrm{Gal}(L,K)$ ist, gilt $H = \sigma \cdot H \cdot \sigma^{-1}$. Wegen

  $$\forall_{\tau \in H \subset \mathrm{Gal}(L,L^H)} \quad \sigma \circ \tau \circ \sigma^{-1}(\beta) = \boxed{?} \quad \sigma \circ \tau(\alpha) = \sigma(\alpha) = \beta$$

  ist $\beta \in L^{\sigma \cdot H \cdot \sigma^{-1}} = L^H = M$. □

Anmerkung zum Lernen. Untersuchen Sie, an welchen Stellen wir im Beweis verwendet haben, dass die gegebene Körpererweiterung endlich ist. Welche der Argumente lassen sich so verbessern, dass sie auch für unendliche Galoiserweiterungen gelten?

Ausblick 3.4.26 (Überlagerungstheorie)**.** In der algebraischen Topologie gibt es das folgende Analogon des Hauptsatzes der Galoistheorie [21, Kapitel 2.3.5]: Dort wird die Struktur von (Zwischen-)Überlagerungen durch die Struktur von (Unter-)Gruppen der Fundamentalgruppe klassifiziert. Zusätzlich gibt es im Falle normaler Untergruppen eine topologische Entsprechung für die zugehörigen Überlagerungen. Mithilfe der Überlagerungstheorie lassen sich dann gruppentheoretische Probleme in topologische Probleme übersetzen; in einigen Fällen sind diese Probleme einfacher zu lösen als die ursprünglichen algebraischen Probleme.

Jede algebraische Körpererweiterung eines Körpers K kann als Zwischenkörper eines algebraischen Abschlusses von K aufgefasst werden (und jede

Galoiserweiterung als Zwischenkörper eines separablen Abschlusses). Analog gibt es im topologischen Fall eine sogenannte universelle Überlagerung.

Ausblick 3.4.27 (Kategorientheorie)**.** Der Hauptsatz der Galoistheorie verführt zur folgenden, abstrakten, Formulierung: Sei $L \mid K$ eine endliche Galoiserweiterung. Dann sind

$$\begin{aligned} \mathsf{Subext}(L,K) &\longrightarrow \mathsf{Subgroup}\,\mathrm{Gal}(L,K) \\ M &\longmapsto \mathrm{Gal}(L,M) \\ M \supset M' &\longmapsto \big(\mathrm{Gal}(L,M) \hookrightarrow \mathrm{Gal}(L,M')\big) \\ \mathsf{Subgroup}\,\mathrm{Gal}(L,K) &\longrightarrow \mathsf{Subext}(L,K) \\ H &\longmapsto L^H \\ H \subset H' &\longmapsto (L^{H'} \hookrightarrow L^H) \end{aligned}$$

zueinander inverse Funktoren (Anhang A.9).

Dabei bezeichnen $\mathsf{Subgroup}\,\mathrm{Gal}(L,K)$ und $\mathsf{Subext}(L,K)$ die folgenden Kategorien: Jede partiell geordnete Menge $(X,\leq)$ liefert eine Kategorie:

- die Objekte sind die Elemente von X,
- es gibt genau dann (genau) einen Morphismus von $x \in X$ nach $y \in X$, wenn $x \leq y$ gilt,
- und die Verknüpfung von Morphismen ist dadurch bereits eindeutig bestimmt.

Die Menge $\mathsf{Subgroup}\,\mathrm{Gal}(L,K)$ der Untergruppen von $\mathrm{Gal}(L,K)$ ist partiell geordnet via „ist Untergruppe von“ die Menge $\mathsf{Subext}(L,K)$ der Zwischenkörper von $L \mid K$ ist partiell geordnet via „ist ein Erweiterungskörper von“. Wir betrachten die durch diese partiellen Ordnungen definierten Kategorien. Indem man die Begriffe von Zwischenkörpern bzw. Untergruppen aufweicht (und jeweils durch injektive Morphismen ersetzt), gelangt man so zu einer Formulierung des Hauptsatzes der Galoistheorie als Äquivalenz von Kategorien (bzw. als Satz über adjungierte Funktoren). Dieser Blickwinkel ist vor allem dann interessant, wenn man Varianten des Hauptsatzes der Galoistheorie in allgemeineren Kontexten formulieren und beweisen möchte.

Wir illustrieren die Aussagen des Hauptsatzes der Galoistheorie an einem Beispiel. Man sollte dabei auch nachverfolgen, wie der Hauptsatz mit den Argumenten/Berechnungen in Beispiel 3.2.41 zusammenpasst.

Beispiel 3.4.28. Wir betrachten die Erweiterung $\mathbb{Q}(\sqrt[3]{2},\zeta_3) \mid \mathbb{Q}$ aus Beispiel 3.2.41. Diese Körpererweiterung ist eine endliche Galoiserweiterung, denn:

- Die Erweiterung ist endlich (nachrechnen).

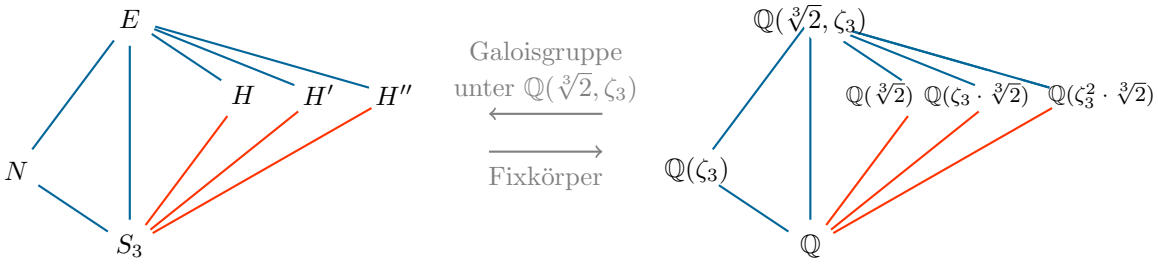


Abbildung 3.7.: Der Hauptsatz der Galoistheorie für $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \mid \mathbb{Q}$; normale Erweiterungen/Untergruppen sind blau, die nicht-normalen rot, dargestellt

- Die Erweiterung ist normal, da $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ ein Zerfällungskörper des Polynoms $T^3 - 2$ über $\mathbb{Q}$ ist (Beispiel 3.2.41, Beispiel 3.4.6).
- Die Erweiterung ist separabel, da es sich um eine Erweiterung in Charakteristik 0 handelt (Beispiel 3.4.11).

Außerdem haben wir in Beispiel 3.2.41 bereits die Galoisgruppe von dieser Erweiterung explizit bestimmt; wir verwenden im folgenden die Notation aus Beispiel 3.2.41. Die Galoisgruppe ist zu S_3 isomorph und besitzt somit genau die folgenden Untergruppen (nachrechnen): ?

$$
\begin{aligned}
G &:= \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{Q}) \cong_{\mathsf{Group}} S_3, \\
H &:= \langle \tau \rangle_G \cong_{\mathsf{Group}} \mathbb{Z}/2, \\
H' &:= \langle \tau \circ \sigma \rangle_G \cong_{\mathsf{Group}} \mathbb{Z}/2, \\
H'' &:= \langle \tau \circ \sigma^2 \rangle_G \cong_{\mathsf{Group}} \mathbb{Z}/2, \\
N &:= \langle \sigma \rangle_G \cong_{\mathsf{Group}} \mathbb{Z}/3, \\
E &:= \{\mathrm{id}\}.
\end{aligned}
$$

Die zugehörigen Fixkörper sind ? $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta_3 \cdot \sqrt[3]{2})$, $\mathbb{Q}(\zeta_3^2 \cdot \sqrt[3]{2})$, $\mathbb{Q}(\zeta_3)$, bzw. $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ (nachrechnen). Damit ergibt sich die in Abbildung 3.7 abgebildete Korrespondenz zwischen Zwischenkörpern und Untergruppen.

Außerdem lässt sich daran schön die Beziehung zwischen Normalität der Untergruppen und Normalität der zugehörigen Erweiterungen über dem Grundkörper $\mathbb{Q}$ ablesen.

Bemerkung 3.4.29 (induktive Berechnung von Galoisgruppen)**.** Sei $L \mid K$ eine endliche Galoiserweiterung. Dann können wir versuchen, die Galoisgruppe $\mathrm{Gal}(L, K)$ mit der folgenden Zerlegungsstrategie zu bestimmen:

Wir versuchen, einen Zwischenkörper M von $L \mid K$ zu finden, für den

- die Erweiterung $M \mid K$ normal ist und
- die Galoisgruppe $\mathrm{Gal}(M, K)$ bekannt ist und
- die Galoisgruppe $\mathrm{Gal}(L, M)$ bekannt ist.

Nach dem Hauptsatz der Galoistheorie (Satz 3.4.24) gibt es dann eine Gruppenerweiterung (Caveat 1.1.73) der folgenden Form:

$$\{e\} \longrightarrow \mathrm{Gal}(L, M) \longrightarrow \mathrm{Gal}(L, K) \longrightarrow \mathrm{Gal}(M, K) \longrightarrow \{e\}$$

In günstigen Fällen kann man dieses „Erweiterungsproblem“ lösen und damit $\mathrm{Gal}(L, K)$ bestimmen (wie in Beispiel 3.2.41). Im allgemeinen ist dabei der Isomorphietyp von $\mathrm{Gal}(L, K)$ aber *nicht* durch die Isomorphietypen von $\mathrm{Gal}(L, M)$ und $\mathrm{Gal}(M, K)$ eindeutig festgelegt!

3.5 Anwendungen der Galoistheorie

Wir haben die Galoistheorie hinreichend weit entwickelt, um eindrucksvolle Anwendungen davon zu genießen:

- Wir zeigen, dass polynomiale Gleichungen über $\mathbb{Q}$ im allgemeinen *nicht* durch iterierte Wurzelformeln lösbar sind (Kapitel 3.5.2).
- Wir zeigen die Nicht-Konstruierbarkeit mit Zirkel und Lineal einiger klassischer geometrischer Größen (Kapitel 3.5.3).
- Außerdem geben wir einen Beweis des Fundamentalsatzes der Algebra mithilfe der Galoistheorie (Kapitel 3.5.4).

3.5.1 Vorbereitung: Kreisteilungskörper

Als Vorbereitung für die oben genannten Anwendungen, untersuchen wir Kreisteilungspolynome und Kreisteilungskörper über $\mathbb{Q}$; der Name erinnert an die geometrische Lage der n-ten Einheitswurzeln auf dem Einheitskreis in $\mathbb{C}$.

Proposition 3.5.1 (Kreisteilungskörper). *Sei $n \in \mathbb{N}_{\geq 2}$, sei $\zeta_n := e^{2 \cdot \pi \cdot i/n} \in \mathbb{C}$ und sei $K := \mathbb{Q}(\zeta_n) \subset \mathbb{C}$ der n-te* Kreisteilungskörper in $\mathbb{C}$. *Dann gilt:*

1. *Das Minimalpolynom von ζ_n über $\mathbb{Q}$ ist*

$$\Phi_n := \prod_{\zeta \in U_n(\mathbb{C})^\times} (T - \zeta),$$

wobei $U_n(\mathbb{C})^\times$ die Menge der primitiven n-ten Einheitswurzeln in $\mathbb{C}$ bezeichnet. Das Polynom Φ_n heißt auch n-tes Kreisteilungspolynom über $\mathbb{Q}$.

2. *Es gilt $[K : \mathbb{Q}] = \varphi(n)$.*

3. *Die Abbildung*

$$\begin{aligned} \mathrm{Gal}(K, \mathbb{Q}) &\longrightarrow \big(\mathbb{Z}/(n)\big)^\times \\ \sigma &\longmapsto [k], \text{ wobei } k \in \mathbb{Z} \text{ mit } \sigma(\zeta_n) = {\zeta_n}^k \end{aligned}$$

ist ein wohldefinierter Gruppenisomorphismus.

Beweis. Zu 1. Sei $f \in \mathbb{Q}[T]$ das Minimalpolynom von ζ_n über $\mathbb{Q}$. Da f irreduzibel ist und $\operatorname{char} \mathbb{Q} = 0$ ist, ist f separabel (Beispiel 3.4.11); es genügt daher zu zeigen, dass f und Φ_n dieselben Nullstellen in $\mathbb{C}$ besitzen.

Ist $\alpha \in \mathbb{C}$ eine Nullstelle von f, so gibt es nach dem Konjugationsprinzip (Proposition 3.2.28) einen Körperhomomorphismus $\sigma\colon \mathbb{Q}(\zeta_n) \longrightarrow \mathbb{C}$ (sogar in $\mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})$) mit $\sigma(\zeta_n) = \alpha$, und damit (in $\mathbb{C}^\times$; da σ injektiv ist)

$$\operatorname{ord} \alpha = \operatorname{ord} \sigma(\zeta_n) = \operatorname{ord} \zeta_n = n.$$

Jede Nullstelle von f ist also eine primitive n-te Einheitswurzel in $\mathbb{C}$.

Warum ist umgekehrt jede primitive n-te Einheitswurzel eine Nullstelle von f ? Im Gegensatz zum vorigen Argument werden wir nun verwenden müssen, dass wir uns über dem Grundkörper $\mathbb{Q}$ befinden. Diese Voraussetzung kann man wie folgt nutzen: Nach Konstruktion ist $\mathbb{Q}$ der Quotientenkörper von $\mathbb{Z}$. Ganzzahlige Information wiederum kann man oft dadurch verstehen, dass man für geeignete Primzahlen $p \in \mathbb{N}$ die Reduktion von $\mathbb{Z}$ nach $\mathbb{F}_p = \mathbb{Z}/(p)$ betrachtet. Dieser Trick ist eines der wichtigsten Prinzipien der Zahlentheorie.

Sei also $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Dann gibt es ein $k \in \{1, \dots, n-1\}$ mit $\mathrm{ggT}(k, n) = 1$ (Beispiel 3.2.27) und $\zeta = {\zeta_n}^k$. Indem wir induktiv vorgehen, genügt es den Fall zu betrachten, dass k prim ist und *kein* Teiler von n ist (nachrechnen; man muss dabei die primitiven Einheitswurzeln induktiv anpassen).

Sei $p \in \mathbb{N}$ prim und $p \nmid n$. Da ζ_n eine Nullstelle von $T^n - 1$ ist, ist f ein Teiler von $T^n - 1$, d.h. es gibt ein $g \in \mathbb{Q}[T]$ mit

$$T^n - 1 = f \cdot g.$$

Da $T^n - 1 \in \mathbb{Z}[T]$ ist und mit f und $T^n - 1$ auch das Polynom g normiert ist, liefert das Lemma von Gauß (Lemma 2.2.51), dass f und g in $\mathbb{Z}[T]$ liegen.

Angenommen, $f({\zeta_n}^p) \neq 0$. Wegen

$$0 = ({\zeta_n}^p)^n - 1 = (f \cdot g)({\zeta_n}^p) = f({\zeta_n}^p) \cdot g({\zeta_n}^p),$$

folgt dann $g(\zeta_n{}^p) = 0$. Also ist ζ_n eine Nullstelle von $g(T^p) \in \mathbb{Z}[T]$. Da f das Minimalpolynom von ζ_n über $\mathbb{Q}$ ist, ist somit f in $\mathbb{Q}[T]$ ein Teiler von $g(T^p)$, d.h. es gibt ein $h \in \mathbb{Q}[T]$ mit

$$g(T^p) = f \cdot h.$$

Mit dem Lemma von Gauß (Lemma 2.2.51) erhalten wir wieder $h \in \mathbb{Z}[T]$.

Sei $\pi\colon \mathbb{Z}[T] \longrightarrow \mathbb{F}_p[T]$ der Reduktionshomomorphismus modulo p. Dann ist

$$\begin{aligned}
\big(\pi(g)\big)^p &= \pi(g^p) \\
&= \pi\big(g(T^p)\big) && \text{(da in Charakteristik } p\text{; Frobenius auf } \mathbb{F}_p(T)) \\
&= \pi(f \cdot h) && \text{(Konstruktion von } h) \\
&= \pi(f) \cdot \pi(h).
\end{aligned}$$

Insbesondere haben $\pi(f)$ und $\pi(g)$ in $\mathbb{F}_p[T]$ einen gemeinsamen Primteiler. Also ist das Polynom

$$T^n - [1] = \pi(T^n - 1) = \pi(f) \cdot \pi(g) \in \mathbb{F}_p[T]$$

nicht separabel. Da p *kein* Teiler von n ist, steht dies jedoch im Widerspruch zum Ableitungskriterium (Proposition 3.3.3). Also ist $f(\zeta_n{}^p) = 0$.

Zu 2. Wir wissen bereits, dass $\#(U_n(\mathbb{C})^\times) = \varphi(n)$ ist (Beispiel 3.2.27). Also ist

$$[K : \mathbb{Q}] = \boxed{?} \quad \deg \Phi_n = \#\big(U_n(\mathbb{C})^\times\big) = \varphi(n).$$

Zu 3. Dies folgt mit den Überlegungen aus Beispiel 3.2.27 und dem Konjugationsprinzip (Korollar 3.2.29) aus dem ersten Teil (nachrechnen). □

Anmerkung zum Lernen. Die Galoisgruppen der Kreisteilungskörper lassen sich mit dem Chinesischen Restsatz (Satz 2.2.23) explizit in kleine Teile zerlegen. Bestimmen Sie $(\mathbb{Z}/(n))^\times$ für $n \in \{1, \dots, 25\}$, um ein besseres Gefühl für diese Gruppen zu bekommen!

Beispiel 3.5.2 (elfte Einheitswurzeln)**.** Nach Proposition 3.5.1 ist

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{11}), \mathbb{Q}\big) \cong_{\mathsf{Group}} \big(\mathbb{Z}/(11)\big)^\times.$$

Da 11 prim ist, enthält diese (abelsche) Gruppe genau zehn Elemente. Da $\mathbb{Z}/(11)$ ein (endlicher) Körper ist, ist $(\mathbb{Z}/(11))^\times$ eine zyklische Gruppe mit genau 10 Elementen (Satz 3.1.9). Somit erhalten wir

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{11}), \mathbb{Q}\big) \cong_{\mathsf{Group}} \big(\mathbb{Z}/(11)\big)^\times \cong_{\mathsf{Group}} \mathbb{Z}/10.$$

Alternativ kann man auch mit dem Chinesischen Restsatz (Satz 2.2.23) oder mit dem Klassifikationssatz für endliche abelsche Gruppen (Satz 1.3.1) ar-

gumentieren; oder direkt nachrechnen, dass $[2] \in \mathbb{Z}/(11)$ die multiplikative Ordnung 10 besitzt und auf diese Weise auf $(\mathbb{Z}/(11))^\times \cong_{\mathsf{Group}} \mathbb{Z}/10$ schließen.

Beispiel 3.5.3 (Prim-Einheitswurzeln)**.** Allgemeiner gilt: Ist $p \in \mathbb{N}$ prim, so ist

$$T^p - 1 = (T-1) \cdot \boxed{?} \quad (T^{p-1} + \cdots + T + 1),$$

und wir wissen bereits (Beispiel 2.2.62), dass der zweite Faktor in $\mathbb{Q}[T]$ irreduzibel ist. Also ist

$$\Phi_p = \sum_{j=0}^{p-1} T^j.$$

Dabei ist $\mathrm{Gal}(\mathbb{Q}(\zeta_p), \mathbb{Q})) \cong_{\mathsf{Group}} \boxed{?} \quad (\mathbb{Z}/(p))^\times \cong_{\mathsf{Group}} \mathbb{Z}/(p-1)$.

Kreisteilungskörper liefern eine bequeme Möglichkeit, endliche Galoiserweiterungen von $\mathbb{Q}$ mit vorgegebener abelscher Galoisgruppe zu konstruieren (indem wir die Proposition „rückwärts“ lesen):

Beispiel 3.5.4 (eine nicht-zyklische abelsche Galoisgruppe über $\mathbb{Q}$)**.** Die Galoisgruppe von $\mathbb{Q}(\zeta_{15}) \mid \mathbb{Q}$ ist abelsch, aber *nicht* zyklisch (Übungsaufgabe).

Beispiel 3.5.5 (gleicher Grad, verschiedene Galoisgruppen)**.** Mit Proposition 3.5.1 folgt

$$\big[\mathbb{Q}(\zeta_7) : \mathbb{Q}\big] = \boxed{?} \quad \varphi(7) = 6 \quad \text{und} \quad \mathrm{Gal}\big(\mathbb{Q}(\zeta_7), \mathbb{Q}\big) \cong_{\mathsf{Group}} \boxed{?} \quad \big(\mathbb{Z}/(7)\big)^\times \cong_{\mathsf{Group}} \mathbb{Z}/6.$$

Andererseits ist (Beispiel 3.2.41)

$$\big[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}\big] = \boxed{?} \quad 6 \quad \text{und} \quad \mathrm{Gal}\big(\mathbb{Q}(\zeta_3, \sqrt[3]{2}), \mathbb{Q})\big) \cong_{\mathsf{Group}} \boxed{?} \quad S_3.$$

Endliche Galoiserweiterungen mit demselben Grad haben also im allgemeinen *nicht* isomorphe Galoisgruppen. Insbesondere sind die Körper $\mathbb{Q}(\zeta_7)$ und $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ *nicht* isomorph (ohne Galoistheorie ist das nicht ohne weiteres klar).

Beispiel 3.5.6 (gleiche Galoisgruppe, verschiedene Galoiserweiterungen)**.** Mit Proposition 3.5.1 folgt

$$\big[\mathbb{Q}(\zeta_3) : \mathbb{Q}\big] = \boxed{?} \quad \varphi(3) = 2 \quad \text{und} \quad \mathrm{Gal}\big(\mathbb{Q}(\zeta_3), \mathbb{Q}\big) \cong_{\mathsf{Group}} \boxed{?} \quad \big(\mathbb{Z}/(3)\big)^\times \cong_{\mathsf{Group}} \mathbb{Z}/2.$$

Außerdem ist auch

$$\big[\mathbb{Q}(\sqrt{2}), \mathbb{Q}\big] = \boxed{?} \quad 2 \quad \text{und} \quad \mathrm{Gal}\big(\mathbb{Q}(\sqrt{2}), \mathbb{Q}\big) \cong_{\mathsf{Group}} \boxed{?} \quad \mathbb{Z}/2.$$

Aber es gilt $\mathbb{Q}(\zeta_3) \ncong_{\mathsf{Group}} \mathbb{Q}(\sqrt{2})$ (nachrechnen mit der konkreten Darstellung dieser Körper durch Linearkombinationen über $\mathbb{Q}$).

Beispiel 3.5.7 ($\mathbb{Z}/3$ als Galoisgruppe über $\mathbb{Q}$)**.** Wir verwenden Kreisteilungskörper, um eine Galoiserweiterung $L \mid \mathbb{Q}$ mit $\mathrm{Gal}(L,\mathbb{Q}) \cong_{\mathsf{Group}} \mathbb{Z}/3$ zu konstruieren: Nach dem Hauptsatz der Galoistheorie (Satz 3.4.24) genügt es dafür, eine endliche Galoiserweiterung von $\mathbb{Q}$ zu finden, deren Galoisgruppe G einen Normalteiler N mit $G/N \cong_{\mathsf{Group}} \mathbb{Z}/3$ enthält. Günstig wäre es also zum Beispiel, eine endliche Galoiserweiterung von $\mathbb{Q}$ mit Galoisgruppe $\mathbb{Z}/6$ zu haben – und eine solche kennen wir bereits (Beispiel 3.5.5).

Sei $H \subset \mathrm{Gal}(\mathbb{Q}(\zeta_7),\mathbb{Q}) \cong_{\mathsf{Group}} \mathbb{Z}/6$ die (normale) Untergruppe, die unter diesem Isomorphismus der Untergruppe $\{[0],[3]\} \subset \mathbb{Z}/6$ entspricht. Dann ist

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_7),\mathbb{Q}\big)/H \cong_{\mathsf{Group}} (\mathbb{Z}/6)/\{[0],[3]\} \cong_{\mathsf{Group}} \mathbb{Z}/3.$$

Nach dem Hauptsatz der Galoistheorie ist somit $L := \mathbb{Q}(\zeta_7)^H$ ein Zwischenkörper mit

$$\mathrm{Gal}(L,\mathbb{Q}) \cong_{\mathsf{Group}} \mathrm{Gal}\big(\mathbb{Q}(\zeta_7),\mathbb{Q}\big)/H \cong_{\mathsf{Group}} \mathbb{Z}/3.$$

Ausblick 3.5.8 (abelsche Erweiterungen von $\mathbb{Q}$)**.** Allgemeiner gilt nach dem Satz von Kronecker–Weber [31, Kapitel 14]: Ist $L \mid \mathbb{Q}$ eine endliche Galoiserweiterung mit abelscher Galoisgruppe, so gibt es ein $n \in \mathbb{N}_{\geq 2}$ mit $L \subset \mathbb{Q}(\zeta_n)$.

3.5.2 Auflösbarkeit durch Radikale

Wir beantworten die Frage, welche polynomialen Gleichungen durch „iteriertes Wurzelziehen“ gelöst werden können. Der Einfachheit halber beschränken wir uns dabei auf den Fall von Charakteristik 0 (im Fall von positiver Charakteristik ergeben sich zusätzliche Komplikationen). Mithilfe der Körpertheorie können wir das „iterierte Wurzelziehen“ wie folgt modellieren:

Definition 3.5.9 (auflösbar durch Radikale)**.** Sei K ein Körper mit $\mathrm{char}\, K = 0$.

- Eine *Wurzelerweiterung* ist eine Körpererweiterung $L \mid K$, so dass es ein $\alpha \in L$, ein $n \in \mathbb{N}_{>0}$ und $c \in K$ mit

  $$L = K(\alpha) \quad \text{und} \quad \alpha^n = c$$

  gibt.

- Eine Körpererweiterung $L \mid K$ ist *durch Radikale auflösbar*, wenn es eine Körpererweiterung $M \mid K$ mit folgenden Eigenschaften gibt: Es ist L ein Zwischenkörper von $M \mid K$ und es gibt ein $n \in \mathbb{N}$ und eine Kette

  $$M_0 := K \subset M_1 \subset \cdots \subset M_n := M$$

  von Zwischenkörpern von $M \mid K$, so dass $M_j \mid M_{j-1}$ für jedes $j \in \{1,\dots,n\}$ eine Wurzelerweiterung ist.

- Ein normiertes Polynom $f \in K[T]$ ist *über K durch Radikale auflösbar*, wenn für einen (dann jeden) Zerfällungskörper L von f über K die zugehörige Erweiterung $L \mid K$ durch Radikale auflösbar ist.

Beispiel 3.5.10 (Mitternachtsformel)**.** Sei K ein Körper mit $\operatorname{char} K = 0$ und seien $b, c \in K$. Dann ist das Polynom

$$f := T^2 + b \cdot T + c \in K[T]$$

über K durch Radikale auflösbar, denn: Sei $M \mid K$ ein algebraischer Abschluss von K und sei $\alpha \in M$ mit

$$\alpha^2 = b^2 - 4 \cdot c$$

(d.h. α ist eine „Wurzel“ aus $b^2 - 4 \cdot c$). Dann ist $K(\alpha) \mid K$ (in $M \mid K$) eine Wurzelerweiterung von K und $K(\alpha)$ ist ein Zerfällungskörper von f, denn in $K(\alpha)[T]$ gilt (Mitternachtsformel)

$$f = \left(T - \frac{-b + \alpha}{2}\right) \cdot \left(T - \frac{-b - \alpha}{2}\right)$$

und $K(\alpha) = K((-b + \alpha)/2, (-b - \alpha)/2)$.

Satz 3.5.11 (Charakterisierung von Auflösbarkeit)**.** *Sei $f \in \mathbb{Q}[T]$ ein normiertes Polynom. Dann sind äquivalent:*

1. *Das Polynom f ist über $\mathbb{Q}$ durch Radikale auflösbar.*
2. *Die Galoisgruppe von f über $\mathbb{Q}$ ist auflösbar.*

Ist die Symmetriegruppe einer polynomialen Gleichung zu kompliziert, so ist diese Gleichung also *nicht* durch Radikale auflösbar.

Bevor wir den Beweis dieses Satzes skizzieren, verwenden wir ihn, um zu zeigen, dass Aufgabe 4 aus der Einführung *nicht* durch iteriertes Wurzelziehen lösbar ist:

Beispiel 3.5.12 (eine komplizierte polynomiale Gleichung)**.** Sei

$$f := T^5 - 4 \cdot T^2 + 2 \in \mathbb{Q}[T].$$

Dann ist f über $\mathbb{Q}$ *nicht* durch Radikale auflösbar, denn: Sei $X := \{x \in \mathbb{C} \mid f(x) = 0\}$ die Menge der komplexen Nullstellen von f und sei $L := \mathbb{Q}(X) \subset \mathbb{C}$. Dann ist L ein Zerfällungskörper von f über $\mathbb{Q}$. Nach Satz 3.5.11 genügt es zu zeigen, dass die Galoisgruppe $G := \operatorname{Gal}(L, \mathbb{Q})$ von f über $\mathbb{Q}$ *nicht* auflösbar ist.

Wir zeigen im folgenden, dass G isomorph zu S_5 ist. Insbesondere liefert dies, dass G *nicht* auflösbar ist (Satz 1.3.28).

Die Galoisgruppe G operiert *effektiv* auf der (fünf-elementigen) Menge X der komplexen Nullstellen von f (Korollar 3.2.29), d.h. der zugehörige Gruppenhomomorphismus $G \longrightarrow S_X$ ist injektiv. Da 5 prim ist, genügt es zu

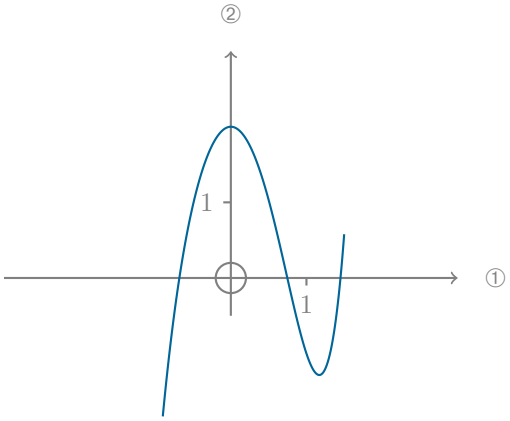


Abbildung 3.8.: Die reelle Polynomfunktion zu $T^5 - 4 \cdot T^2 + 2$

zeigen, dass G eine Transposition von zwei Nullstellen von f und einen 5-Zykel enthält (dies folgt aus Satz 1.3.7; Übungsaufgabe).

- Existenz einer Transposition in G: Das Polynom f besitzt genau drei reelle Nullstellen (nachrechnen per Kurvendiskussion; Abbildung 3.8). Da f unter komplexer Konjugation invariant ist, ist auch die Menge X der Nullstellen von f in $\mathbb{C}$ unter komplexer Konjugation invariant. Die Einschränkung τ der komplexen Konjugation auf L erfüllt somit $\tau(L) \subset L$ und $\tau \in \mathrm{Gal}(L, \mathbb{Q})$ induziert auf X eine Transposition (der beiden nicht-reellen Nullstellen).

- Existenz eines 5-Zykels in G: Mit der Zykelzerlegung (Proposition 1.3.6) folgt, dass jedes Element von S_5 der Ordnung 5 ein 5-Zykel ist. Es genügt also, ein Element der Ordnung 5 in G zu finden. Es gilt (Proposition 3.4.19)
$$\#G = \#\,\mathrm{Gal}(L, \mathbb{Q}) = [L : \mathbb{Q}].$$
Das Polynom f ist über $\mathbb{Q}$ irreduzibel (nach dem Eisensteinschen Irreduzibilitätskriterium; Satz 2.2.61). Wegen $\deg f = 5$ erhalten wir daher aus der Multiplikativität des Grades (Proposition 3.2.10) und da L eine (sogar jede) Nullstelle von f enthält, dass 5 ein Teiler von $[L : \mathbb{Q}]$ ist.

  Mit den Sylowsätzen (Satz 1.3.39) bzw. dem Satz von Cauchy (Korollar 1.3.40) folgt, dass G ein Element der Ordnung 5 enthält.

Mithilfe von symmetrischen Funktionen lässt sich zeigen, dass es sich bei der Nicht-Auflösbarkeit von polynomialen Gleichungen höheren Grades um „generisches“ Verhalten handelt [6, S. 266f].

Umgekehrt liefert Satz 3.5.11 auch, dass polynomiale Gleichungen niedrigen Grades durch Radikale auflösbar sind:

Beispiel 3.5.13 (niedrige Grade)**.** Sei $f \in \mathbb{Q}[T]$ normiertes Polynom mit $n := \deg f \leq 4$ und sei $L \mid \mathbb{Q}$ ein Zerfällungskörper von f über $\mathbb{Q}$. Dann ist

$$[L : \mathbb{Q}] \leq n! \leq 24$$

(nachrechnen; mithilfe der induktiven Konstruktion von Zerfällungskörpern im Beweis von Satz 3.2.43). Also ist auch

$$\#\operatorname{Gal}(L, \mathbb{Q}) = [L : \mathbb{Q}] \leq 24$$

(Proposition 3.4.19). Daher handelt es sich bei $\operatorname{Gal}(L, \mathbb{Q})$ um eine auflösbare Gruppe (Bemerkung A.5.6). Also ist f durch Radikale auflösbar (Satz 3.5.11). Dies kann auch explizit gemacht werden [6, Kapitel 6.2] (die Formeln für Grad 3 und 4 sind jedoch komplizierter als die Mitternachtsformel ...).

Anmerkung für Lehramtsstudenten. Warum sind diese Resultate relevant für den Schulunterricht?

Wir skizzieren einen Beweis von Satz 3.5.11: Der Beweis beruht im wesentlichen auf der Charakterisierung von Wurzelerweiterungen als zyklische Erweiterungen (Proposition 3.5.15), dem geschickten Einsatz von Einheitswurzeln und dem Hauptsatz der Galoistheorie. Dazu müssen wir einerseits genug Einheitswurzeln hinzufügen (Proposition 3.5.16) und andererseits zur normalen Hülle übergehen (Proposition 3.5.17).

Caveat 3.5.14 (primitive Einheitswurzel)**.** In der Literatur bedeuten Formulierungen der Art „Sei $n \in \mathbb{N}_{>0}$ und sei K ein Körper, der eine primitive n-te Einheitswurzel enthält." im Normalfall, dass angenommen wird, dass K eine primitve n-te Einheitswurzel eines algebraischen Abschlusses von K enthält (ansonsten ist es keine wirkliche Bedingung ...). Ist $\operatorname{char} K = 0$, so ist dies äquivalent zur Existenz eines Elements mit multiplikativer Ordnung n.

Proposition 3.5.15 (Wurzelerweiterung vs. zyklische Erweiterung)**.** *Sei $n \in \mathbb{N}_{>0}$, sei K ein Körper, der ein Element $\zeta \in K^\times$ mit $\operatorname{ord} \zeta = n$ enthält und sei $L \mid K$ eine endliche Erweiterung. Dann gilt:*

1. *Gibt es ein $\alpha \in L$ mit $L = K(\alpha)$ und $\alpha^n \in K$, so ist $L \mid K$ eine Galoiserweiterung mit zyklischer Galoisgruppe.*
2. *Ist $L \mid K$ eine Galoiserweiterung mit $\operatorname{Gal}(L, K) \cong_{\mathsf{Group}} \mathbb{Z}/n$, so ist $L \mid K$ eine Wurzelerweiterung.*

Beweis. Zu 1. Ist $\alpha \in L$ und gilt $L = K(\alpha)$ sowie $c := \alpha^n \in K$, so ist $L = K(\alpha)$ ein Zerfällungskörper von $T^n - c$ über K, denn

$$T^n - c = \prod_{k=0}^{n-1} (T - \zeta^k \cdot \alpha).$$

Da diese Nullstellen wegen $\operatorname{ord}\zeta = n$ alle verschieden sind, ist $T^n - c$ über K (und damit auch α über K) separabel. Also ist $L \mid K$ eine Galoiserweiterung (Proposition 3.4.5, Proposition 3.4.12). Dass die Galoisgruppe $\mathrm{Gal}(L,K)$ zyklisch ist, folgt aus der obigen Zerlegung von $T^n - c$ und dem Konjugationsprinzip (Korollar 3.2.29) (Übungsaufgabe).

Zu 2. Sei umgekehrt $L \mid K$ eine Galoiserweiterung mit $\mathrm{Gal}(L,K) \cong_{\mathsf{Group}} \mathbb{Z}/n$. Sei $\sigma \in \mathrm{Gal}(L,K) \cong_{\mathsf{Group}} \mathbb{Z}/n$ ein Erzeuger dieser zyklischen Gruppe.

Wir fassen σ als K-linearen Endomorphismus von L auf; dann gibt es eine primitive n-te Einheitswurzel in K, die ein Eigenwert von σ ist (Übungsaufgabe; mithilfe von den Argumenten aus Beispiel II.A.4.5). Sei $\alpha \in L$ ein zugehöriger Eigenvektor. Dann liegt

$$c := \alpha^n$$

in K (Übungsaufgabe; Fixkörper!).

Wie im ersten Teil sieht man, dass $K(\alpha)$ ein Zerfällungskörper von $T^n - c$ über K ist. Mit einer Gradabschätzung erhalten wir nun, dass $L = K(\alpha)$ ist (Übungsaufgabe). □

Proposition 3.5.16 (Hinzufügen von Einheitswurzeln)**.** *Sei $L \mid \mathbb{Q}$ eine endliche Körpererweiterung mit $L \subset \mathbb{C}$ und sei $\zeta \in \mathbb{C}$ eine Einheitswurzel.*

1. *Dann ist die Erweiterung $L \mid \mathbb{Q}$ genau dann durch Radikale auflösbar, wenn $L(\zeta) \mid \mathbb{Q}(\zeta)$ durch Radikale auflösbar ist.*
2. *Ist $L \mid \mathbb{Q}$ eine Galoiserweiterung, so gilt: Die Gruppe $\mathrm{Gal}(L,\mathbb{Q})$ ist genau dann auflösbar, wenn $\mathrm{Gal}(L(\zeta),\mathbb{Q}(\zeta))$ auflösbar ist.*

Beweis. Zu 1. Dies folgt aus der Tatsache, dass $L(\zeta) \mid L$ und $\mathbb{Q}(\zeta) \mid \mathbb{Q}$ Wurzelerweiterungen sind und dass Verschiebungen von Wurzelerweiterungen durch Bildung des Kompositums mit einem gegebenen Körper wieder Wurzelerweiterungen sind (nachrechnen).

Zu 2. Es gilt $L(\zeta) = L \cdot \mathbb{Q}(\zeta)$ und $\mathbb{Q}(\zeta) \mid \mathbb{Q}$ ist eine Galoiserweiterung mit abelscher Galoisgruppe (Proposition 3.5.1). Mit denselben Methoden sieht man, dass auch $L(\zeta) \mid L$ eine Galoiserweiterung mit abelscher Galoisgruppe ist (nachrechnen) und dass $L(\zeta) \mid \mathbb{Q}$ galoissch ist. Mit Bemerkung 3.4.29 erhalten wir also eine Gruppenerweiterung der Form

$$\{e\} \longrightarrow \mathrm{Gal}\big(L(\zeta), L\big) \longrightarrow \mathrm{Gal}\big(L(\zeta), \mathbb{Q}\big) \longrightarrow \mathrm{Gal}\big(L, \mathbb{Q}\big) \longrightarrow \{e\}.$$

Aus den Vererbungseigenschaften auflösbarer Gruppen (Proposition 1.3.27) folgt somit, dass $\mathrm{Gal}(L(\zeta),\mathbb{Q})$ genau dann auflösbar ist, wenn $\mathrm{Gal}(L,\mathbb{Q})$ auflösbar ist. Analog erhalten wir eine Gruppenerweiterung der Form

$$\{e\} \longrightarrow \mathrm{Gal}\big(L(\zeta), \mathbb{Q}(\zeta)\big) \longrightarrow \mathrm{Gal}\big(L(\zeta), \mathbb{Q}\big) \longrightarrow \mathrm{Gal}\big(\mathbb{Q}(\zeta), \mathbb{Q}\big) \longrightarrow \{e\}$$

und somit, dass $\mathrm{Gal}(L(\zeta),\mathbb{Q})$ genau dann auflösbar ist, wenn $\mathrm{Gal}(L(\zeta),\mathbb{Q}(\zeta))$ auflösbar ist. □

Proposition 3.5.17 (normale Hülle von Wurzelerweiterungen). *Sei $K \mid \mathbb{Q}$ eine endliche normale Körpererweiterung mit $K \subset \mathbb{C}$, sei $n \in \mathbb{N}_{>0}$ und sei $\alpha \in \mathbb{C}$ mit $c := \alpha^n \in K$. Dann gibt es einen Zwischenkörper L von $\mathbb{C} \mid K(\alpha)$, sodass $L \mid K(\alpha)$ durch Radikale auflösbar ist und $L \mid \mathbb{Q}$ normal ist.*

Beweis. Sei $N := \{x \in \mathbb{C} \mid x^n = \sigma(c) \text{ und } \sigma \in \mathrm{Gal}(K, \mathbb{Q})\} \subset \mathbb{C}$ und

$$L := K(N) \subset \mathbb{C}.$$

Nach Konstruktion ist L ein Zwischenkörper von $\mathbb{C} \mid K(\alpha)$ und die Erweiterung $L \mid K(\alpha)$ ist durch Radikale auflösbar (da $K \mid \mathbb{Q}$ normal ist, gilt $\sigma(c) \in K$ für alle $\sigma \in \mathrm{Gal}(K, \mathbb{Q})$).

Außerdem ist die Erweiterung $L \mid \mathbb{Q}$ normal, denn: Das Polynom

$$f := \prod_{\sigma \in \mathrm{Gal}(K,\mathbb{Q})} \big(T^n - \sigma(c)\big) \in K[T]$$

zerfällt (nach Konstruktion von L und der algebraischen Abgeschlossenheit von $\mathbb{C}$) über L in Linearfaktoren. Außerdem gilt (nach Konstruktion von f)

$$\forall_{\sigma \in \mathrm{Gal}(K,\mathbb{Q})} \quad f^\sigma = f,$$

und damit $f \in K^{\mathrm{Gal}(K,\mathbb{Q})}[T]$. Wegen $K^{\mathrm{Gal}(K,\mathbb{Q})} = \mathbb{Q}$ (Korollar 3.4.21) ist $f \in \mathbb{Q}[T]$. Insbesondere sind die Minimalpolynome über $\mathbb{Q}$ der Elemente von N Teiler von f und zerfallen über L in Linearfaktoren. Damit ist $L \mid \mathbb{Q}$ normal (Proposition 3.4.5). □

Beweis von Satz 3.5.11. Zu 1. $\Longrightarrow$ 2. Sei f über $\mathbb{Q}$ durch Radikale auflösbar und sei $L \subset \mathbb{C}$ ein Zerfällungskörper von f über $\mathbb{Q}$ (ein solcher kann aus den komplexen Nullstellen von f konstruiert werden). Dann ist $\mathrm{Gal}(L, \mathbb{Q})$ auflösbar, denn:

Mithilfe der normalen Hüllen aus Proposition 3.5.17 erhalten wir induktiv einen Zwischenkörper M von $\mathbb{C} \mid L$ mit folgenden Eigenschaften:

- Die Erweiterung $M \mid \mathbb{Q}$ ist normal
- und $M \mid \mathbb{Q}$ ist durch Radikale auflösbar (wobei die Wurzeltürme bei M enden).

Sei $n \in \mathbb{N}$ das Produkt der Exponenten in einer Kette von Wurzelerweiterungen von $\mathbb{Q}$ nach M und sei $\zeta := e^{2 \cdot \pi \cdot i/n} \in \mathbb{C}$. Dann ist $L(\zeta) \mid \mathbb{Q}(\zeta)$ eine Galoiserweiterung (nachrechnen), die durch Radikale auflösbar ist (Proposition 3.5.16).

Mit dem Fall einer einzelnen Wurzelerweiterung über einem Grundkörper mit passenden Einheitswurzeln (Proposition 3.5.15), den Gruppenerweiterungen aus dem Hauptsatz der Galoistheorie (Bemerkung 3.4.29) und den Vererbungseigenschaften auflösbarer Gruppen (Proposition 1.3.27) folgt induktiv

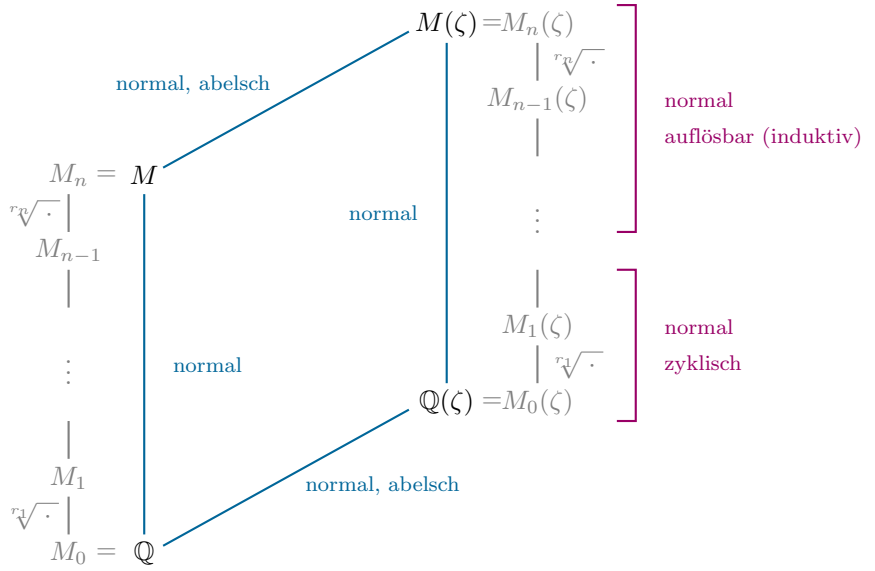


Abbildung 3.9.: Durch Radikale auflösbare Polynome haben auflösbare Galoisgruppe, schematisch

(von unten nach oben, mit einer leicht allgemeineren Induktionsbehauptung) wie in Abbildung 3.9 angedeutet: Die Gruppe $\mathrm{Gal}(M(\zeta), \mathbb{Q}(\zeta))$ ist auflösbar.

Proposition 3.5.16 zeigt dann, dass auch $\mathrm{Gal}(M, \mathbb{Q})$ auflösbar ist. Da $L \mid \mathbb{Q}$ normal ist, folgt mit einer weiteren Anwendung des Hauptsatzes der Galoistheorie und der Vererbungseigenschaften auflösbarer Gruppen, dass $\mathrm{Gal}(L, \mathbb{Q})$ (als Quotient von $\mathrm{Gal}(M, \mathbb{Q})$) auflösbar ist.

Zu 2. $\Longrightarrow$ 1. Wir skizzieren die Argumente für die Umkehrung: Sei $L \mid \mathbb{Q}$ ein Zerfällungskörper von f über $\mathbb{Q}$ mit $L \subset \mathbb{C}$, sei $G := \mathrm{Gal}(L, \mathbb{Q})$ auflösbar, sei $n := \#G$ und sei $\zeta := e^{2 \cdot \pi \cdot i/n} \in \mathbb{C}$.

Nach Proposition 3.5.16 ist auch $\overline{G} := \mathrm{Gal}(L(\zeta), \mathbb{Q}(\zeta))$ auflösbar. Daher besitzt $\overline{G}$ eine Normalreihe mit zyklischen Faktoren (Satz 1.3.31) und $\#\overline{G}$ ist ein Teiler von $\#G$ (nachrechnen). Mit dem Hauptsatz der Galoistheorie (Satz 3.4.24) folgt induktiv über die Anzahl der zyklischen Faktoren aus dem zyklischen Fall (Proposition 3.5.15), dass die Erweiterung $L(\zeta) \mid \mathbb{Q}(\zeta)$ durch Radikale auflösbar ist.

Nach Proposition 3.5.16 ist dann auch $L \mid \mathbb{Q}$ durch Radikale auflösbar. □

Ausblick 3.5.18 (elementare Integration)**.** Eine weitere naheliegende Unmöglichkeitsfrage aus der Analysis ist: (Wie) Kann man zeigen, dass gewisse Funktionen *keine* „elementaren“ Stammfunktionen besitzen? Konkrete Beispiele dafür sind die in der Wahrscheinlichkeitstheorie zentrale Funktion

$$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto e^{-x^2} \end{aligned}$$

und die für die Zahlentheorie zentrale Funktion (Literaturaufgabe 2.2.2)

$$\begin{aligned} \mathbb{R}_{>1} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{x}{\ln x}. \end{aligned}$$

Mit einer entsprechend angepassten Variante von Körpererweiterungen kann man diese Fragen behandeln und zeigen, dass die obigen Funktionen tatsächlich keine „elementaren“ Stammfunktionen besitzen [26, 11].

3.5.3 Konstruierbarkeit mit Zirkel und Lineal

Eine klassische Frage in der Geometrie ist es, welche geometrischen Objekte bzw. welche Punkte in der Ebene sich mit Zirkel und Lineal konstruieren lassen. Sei ZL die Menge aller Punkte in $\mathbb{C}$, die aus $\{0, 1\}$ mit Zirkel und Lineal konstruiert werden können (Anhang A.7).

Satz 3.5.19 (der Körper der konstruierbaren Punkte; Satz A.7.4)**.**

1. *Die Menge* $\mathrm{ZL} \subset \mathbb{C}$ *ist ein Körper bezüglich der arthmetischen Operationen auf* $\mathbb{C}$*. Dabei gilt* $\mathbb{Q} \subset \mathrm{ZL}$*.*

2. *Der Körper* ZL *ist im folgenden Sinne unter Quadratwurzeln abgeschlossen: Ist* $z \in \mathrm{ZL}$*, so liegen alle Elemente* $\alpha \in \mathbb{C}$ *mit* $\alpha^2 = z$ *auch in* ZL*.*

Satz 3.5.20 (Charakterisierung von Konstruierbarkeit)**.** *Sei* $z \in \mathbb{C}$*. Die folgenden Aussagen sind äquivalent:*

1. *Es gilt* $z \in \mathrm{ZL}$*.*

2. *Es gibt ein* $n \in \mathbb{N}$ *und eine Folge* $L_0 := \mathbb{Q} \subset L_1 \subset \cdots \subset L_n \subset \mathbb{C}$ *von Teilkörpern von* $\mathbb{C}$ *mit* $z \in L_n$ *und*

$$[L_j : L_{j-1}] = 2$$

   für alle $j \in \{1, \ldots, n\}$*.*

3. *Es gibt eine endliche Galoiserweiterung* $L \mid \mathbb{Q}$ *mit* $z \in L$*, deren Galoisgruppe* $\mathrm{Gal}(L, \mathbb{Q})$ *eine 2-Gruppe ist.*

4. *Es gibt eine endliche Galoiserweiterung* $L \mid \mathbb{Q}$ *und* $n \in \mathbb{N}$ *mit* $z \in L$ *und* $[L : \mathbb{Q}] = 2^n$*.*

Beweis. Zu 1. $\Longrightarrow$ 2. Sei $z \in \mathrm{ZL}$, d.h. es gibt ein $n \in \mathbb{N}$ mit $z \in \mathrm{ZL}^n(\{0,1\})$. Wir beweisen Aussage 2. durch Induktion über n: Ist $n = 0$, so ist nach Definition $z \in \{0,1\}$.

Für den Induktionsschritt sei $n \in \mathbb{N}_{>0}$ und die Behauptung sei für niedrigere Anzahlen bereits gezeigt.

Nach Definition von $\mathrm{ZL}^n(\{0,1\}) = \mathrm{ZL}(\mathrm{ZL}^{n-1}(\{0,1\}))$ gibt es eine endliche Menge $M \subset \mathrm{ZL}^{n-1}(\{0,1\})$ mit $z \in \mathrm{ZL}(M) \subset \mathrm{ZL}(\mathbb{Q}(M))$.

Nach Induktionsvoraussetzung gibt es zu jedem der Elemente aus M einen Erweiterungsturm aus Erweiterungen vom Grad 2. Durch Kombination dieser Türme folgt (mit Proposition 3.2.12), dass auch $\mathbb{Q}(M)$ in einem Erweiterungsturm aus Erweiterungen vom Grad 2 enthalten ist.

Wir verwenden die folgende essentielle Beobachtung: Sei $L \subset \mathrm{ZL}$ ein Teilkörper. Dann gilt (nachrechnen [6, Kapitel 6.4]):

- *Schnittpunkte von konstruierbaren Geraden.* Ist $x \in \mathrm{ZL}_1(L)$, so ist $L(x) = L$.
- *Schnittpunkte konstruierbarer Geraden mit konstruierbaren Kreisen.* Ist $x \in \mathrm{ZL}_2(L)$, so ist $[L(x) : L] \leq 2$.
- *Schnittpunkte zweier konstruierbarer Kreise.* Ist $x \in \mathrm{ZL}_3(L)$, so ist $[L(x) : L] \leq 2$.

Insgesamt folgt somit

$$\big[\mathbb{Q}(M)(z) : \mathbb{Q}(M)\big] \leq 2$$

und durch Kombination mit dem Erweiterungsturm für $\mathbb{Q}(M)$ erhalten wir einen Erweiterungsturm für $\mathbb{Q}(z)$ bzw. z von der gewünschten Form.

Zu 2. $\Longrightarrow$ 3. Dies kann man mit ähnlichen Argumenten wie im Beweis der Implikation 1. $\Longrightarrow$ 2. von Satz 3.5.11 zeigen (nachrechnen).

Zu 2. $\Longrightarrow$ 1. Da ZL unter Quadratwurzeln abgeschlossen ist (Satz A.7.4), folgt (nachrechnen): Ist $L \mid \mathbb{Q}$ eine endliche Erweiterung mit $L \subset \mathrm{ZL}$ und ist $M \subset \mathbb{C}$ mit $[M : L] = 2$, so ist $M \subset \mathrm{ZL}$. Induktiv folgt damit die gewünschte Implikation.

Zu 3. $\Longrightarrow$ 2. Ist $L \mid \mathbb{Q}$ eine endliche Galoiserweiterung, deren Galoisgruppe $\mathrm{Gal}(L, \mathbb{Q})$ eine 2-Gruppe ist, so folgt analog zu Satz 1.3.31, dass $\mathrm{Gal}(L, \mathbb{Q})$ eine Normalreihe mit Faktoren isomorph zu $\mathbb{Z}/2$ besitzt. Der Hauptsatz der Galoistheorie (Satz 3.4.24) übersetzt eine solche Normalreihe in eine Erweiterungskette wie in Aussage 2.

Zu 3. $\Longleftrightarrow$ 4. Die Aussagen 3. und 4. sind via Proposition 3.4.19 äquivalent. □

Mit dieser Theorie können wir Aufgabe 1, Aufgabe 2 und Aufgabe 3 aus der Einführung behandeln:

Beispiel 3.5.21 (Quadratur des Kreises)**.** Es ist *nicht* möglich, mit Zirkel und Lineal aus $\{0,1\}$ die Seitenlänge eines Quadrats zu konstruieren, dessen Flächeninhalt mit dem Flächeninhalt des Einheitskreises übereinstimmt, denn:

Angnommen, dies wäre möglich. Dann wäre auch $\sqrt{\pi} \in \mathrm{ZL}$ (nachrechnen). Da π über $\mathbb{Q}$ transzendent ist (Beispiel 3.2.22), ist auch $\sqrt{\pi}$ über $\mathbb{Q}$ transzendent (nachrechnen). Insbesondere ist $\sqrt{\pi}$ *nicht* in einer endlichen Erweiterung von $\mathbb{Q}$ enthalten. Dies steht jedoch nach Satz 3.5.20 im Widerspruch zu $\sqrt{\pi} \in \mathrm{ZL}$.

Beispiel 3.5.22 (Würfelverdopplung)**.** Es ist *nicht* möglich, mit Zirkel und Lineal aus $\{0,1\}$ die Seitenlänge eines Würfels zu konstruieren, dessen Volumen 2 ist, denn:

Angenommen, dies wäre möglich. Dann wäre auch $\sqrt[3]{2} \in \mathrm{ZL}$ (nachrechnen). Wegen

$$\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = ? \quad 3$$

und der Multiplikativität des Grades (Proposition 3.2.10) folgt, dass $\sqrt[3]{2}$ *nicht* in einer Körpererweiterung von $\mathbb{Q}$ enthalten ist, deren Grad eine Zweierpotenz ist. Dies steht jedoch nach Satz 3.5.20 im Widerspruch zu $\sqrt[3]{2} \in \mathrm{ZL}$.

Beispiel 3.5.23 (reguläre Polygone)**.** Es ist *nicht* möglich, mit Zirkel und Lineal aus $\{0,1\}$ die Seitenlänge eines regulären Neunecks mit Radius 1 zu konstruieren, denn:

Angenommen, dies wäre möglich. Dann wäre auch $\zeta_9 \in \mathrm{ZL}$ (nachrechnen). Wegen

$$\left[\mathbb{Q}(\zeta_9) : \mathbb{Q}\right] = ? \quad \varphi(9) = 6$$

(Proposition 3.5.1; nachrechnen) und der Multiplikativität des Grades (Proposition 3.2.10) folgt, dass ζ_9 *nicht* in einer Körpererweiterung von $\mathbb{Q}$ enthalten ist, deren Grad eine Zweierpotenz ist. Dies steht jedoch nach Satz 3.5.20 im Widerspruch zu $\zeta_9 \in \mathrm{ZL}$.

Analog folgt, dass auch das reguläre Elfeck nicht konstruierbar ist (mithilfe von Beispiel 3.5.2).

Im Gegensatz dazu ist das reguläre Siebzehneck tatsächlich mit Zirkel und Lineal konstruierbar (Gauß), denn $\mathbb{Q}(\zeta_{17}) \mid \mathbb{Q}$ ist eine Galoiserweiterung und

$$\left[\mathbb{Q}(\zeta_n) : \mathbb{Q}\right] = ? \quad \varphi(17) = |17 - 1| = 2^4$$

(da 17 prim ist). Allgemeiner gilt: Ist $n \in \mathbb{N}_{\geq 3}$, so ist das reguläre n-Eck mit Radius 1 genau dann mit Zirkel und Lineal aus $\{0,1\}$ konstruierbar, wenn $\varphi(n)$ eine Zweierpotenz ist.

Beispiel 3.5.24 (Winkeldreiteilung)**.** Im allgemeinen ist die Drittelung eines gegebenen Winkels *nicht* mit Zirkel und Lineal konstruierbar (Übungsaufgabe).

Anmerkung für Lehramtsstudenten. Warum sind diese Resultate relevant für den Schulunterricht?

Caveat 3.5.25. Sei $z \in \mathbb{C}$. Ist $[\mathbb{Q}(z) : \mathbb{Q}]$ eine Zweierpotenz, so ist z im allgemeinen *nicht* mit Zirkel und Lineal aus $\{0,1\}$ konstruierbar: Es gibt

Beispiele für $z \in \mathbb{C}$ mit $[\mathbb{Q}(z) : \mathbb{Q}] = 4$, aber der Eigenschaft, dass jede Galoiserweiterung $L \mid \mathbb{Q}$ mit $z \in L \subset \mathbb{C}$ die Eigenschaft

$$3 \mid [L : \mathbb{Q}]$$

besitzt (zum Beispiel kann man zeigen, dass die Galoisgruppe von $T^4 - T - 1$ über $\mathbb{Q}$ isomorph zu S_4 ist).

Ausblick 3.5.26 (Origami-Konstruierbarkeit)**.** Ähnlich zur Konstruierbarkeit mit Zirkel und Lineal kann man auch die Konstruierbarkeit durch elementare Origami-Operationen formalisieren (Übungsaufgabe) und mithilfe der Galoistheorie charakterisieren [12, Kapitel 10]. Zum Beispiel ergibt sich, dass die Winkeldreiteilung mit Origami möglich ist, dass aber das reguläre 11-Eck auch mit dieser Art von Origami nicht aus dem gegebenen Radius konstruierbar ist.

3.5.4 Der Fundamentalsatz der Algebra

Satz 3.5.27 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Beweis. Da $\mathbb{R}$ durch eine analytische Konstruktion (Vervollständigung) aus $\mathbb{Q}$ entsteht, ist davon auszugehen, dass analytische Eigenschaften in den Beweis eingehen. Wir verwenden die folgenden analytischen Eigenschaften von $\mathbb{R}$ und $\mathbb{C} = \mathbb{R}(i)$:

① Ist $f \in \mathbb{R}[T]$ und ist $\deg f$ ungerade, so besitzt f mindestens eine Nullstelle in $\mathbb{R}$ (Zwischenwertsatz); insbesondere ist f in $\mathbb{R}[T]$ *nicht* irreduzibel, wenn $\deg f$ ungerade und größer als 1 ist.

② Ist $c \in \mathbb{R}_{\geq 0}$, so gibt es ein $x \in \mathbb{R}$ mit $x^2 = c$ (explizite Konstruktion einer rationalen Approximation oder ein Stetigkeits-/Zwischenwertargument für die Quadratfunktion).

③ Ist $c \in \mathbb{C}$, so gibt es ein $z \in \mathbb{C}$ mit $z^2 = c$ (nachrechnen, mithilfe von ② und der Konstruktion von $\mathbb{C}$ aus $\mathbb{R}$).

④ Ist $f \in \mathbb{C}[T]$ mit $\deg f = 2$, so besitzt f eine Nullstelle in $\mathbb{C}$ (nachrechnen, mithilfe von ③); insbesondere ist f in $\mathbb{C}[T]$ *nicht* irreduzibel.

Warum ist $\mathbb{C}$ algebraisch abgeschlossen? Es genügt, die folgende Aussage zu zeigen (indem wir Zerfällungskörper von komplexen Polynomen betrachten):

Ist $L \mid \mathbb{C}$ eine endliche Körpererweiterung, so ist $L = \mathbb{C}$.

Sei also $L \mid \mathbb{C}$ eine endliche Galoiserweiterung; dann ist auch die induzierte Erweiterung $L \mid \mathbb{R}$ endlich. Sei $M \mid L$ ein algebraischer Abschluss von L und sei $S \subset L$ eine endliche Teilmenge von M mit

$$L = \mathbb{R}(S).$$

Indem wir die Menge $\overline{S}$ aller M-Nullstellen der Minmalpolynome über $\mathbb{R}$ der Elemente aus S betrachten, erhalten wir einen Körper $\overline{L} := \mathbb{R}(\overline{S})$ mit $L \subset \overline{L}$, für den die Erweiterung $L \mid \mathbb{R}$ eine endliche Galoiserweiterung ist (Proposition 3.4.5; Separabilität ist in Charakteristik 0 automatisch erfüllt: Beispiel 3.4.11). Wir können daher im folgenden ohne Einschränkung annehmen, dass $L \mid \mathbb{R}$ eine endliche Galoiserweiterung ist. Sei $G := \mathrm{Gal}(L, \mathbb{R})$.

Wir verwenden die folgende Strategie:

- Wir zeigen mithilfe von ①, dass G eine 2-Gruppe ist.
- Mit ④ folgern wir daraus, dass $\#G = 2$ und $L = \mathbb{C}$ ist.

Die Gruppe G ist eine 2-Gruppe, denn: Wir schreiben

$$[L : \mathbb{R}] = \#G = 2^k \cdot m$$

mit $k \in \mathbb{N}$ und einer ungeraden Zahl $m \in \mathbb{N}_{>0}$. Wegen $[\mathbb{C} : \mathbb{R}] = 2$ ist dabei $k \geq 1$. Nach den Sylowsätzen (Satz 1.3.39) enthält G eine 2-Sylowgruppe H. Also gilt

$$[L : L^H] = \#H = 2^k$$

(Satz 3.4.20), und damit ist

$$[L^H : \mathbb{R}] = \frac{[L : \mathbb{R}]}{[L : L^H]} = \frac{2^k \cdot m}{2^k} = m$$

ungerade. Nach dem Satz vom primitiven Element (Satz 3.4.13) gibt es ein $\alpha \in L$ mit $L^H = \mathbb{R}(\alpha)$. Ist $f \in \mathbb{R}[T]$ das Minimalpolynom von α, so ist

$$\deg f = [\mathbb{R}(\alpha) : \mathbb{R}] = [L^H : \mathbb{R}] = m$$

ungerade. Mit ① erhalten wir daraus $\deg f = 1$ bzw. $\alpha \in \mathbb{R}$. Daher ist (Satz 3.4.24)

$$L^H = \mathbb{R}(\alpha) = \mathbb{R} \quad \text{und} \quad H = G.$$

Insbesondere ist G eine 2-Gruppe.

Es gilt $\#G = 2$ und $L = \mathbb{C}$, denn: Sei $N := \mathrm{Gal}(L, \mathbb{C})$. Da $\mathbb{C} \mid \mathbb{R}$ normal ist, ergibt sich mit dem Hauptsatz der Galoistheorie (Satz 3.4.24)

$$\frac{\#G}{\#N} = \#(G/N) = \#\,\mathrm{Gal}(\mathbb{C}, \mathbb{R}) = 2.$$

Also ist auch N eine 2-Gruppe. *Angenommen,* die Gruppe N wäre *nicht* trivial. Dann besitzt N eine Untergruppe $N' \subset N$ vom Index 2 (dies folgt analog zum Beweis von Satz 1.3.37 per Induktion über $\#N$). Insbesondere ist N' ein Normalteiler von N (Übungsaufgabe). Nach dem Hauptsatz der Galoistheorie ist dann

$$[L^{N'} : \mathbb{C}] = \#\operatorname{Gal}(L^{N'}, \mathbb{C}) = \#(N/N') = [N : N'] = 2.$$

Dies ist aber ein Widerspruch zu ④ (nachrechnen).

Also ist $\operatorname{Gal}(L, \mathbb{C}) = N = \{e\}$ und, da $L \mid \mathbb{C}$ eine Galoiserweiterung ist, erhalten wir $L = \mathbb{C}$, wie gewünscht. □

Bemerkung 3.5.28 (weitere Beweise des Fundamentalsatzes der Algebra)**.** Weitere schöne Beweise des Fundamentalsatzes erhält man zum Beispiel mit der Funktionentheorie oder Homotopie- bzw. (Ko)Homologiegruppen.

Der obige, algebraische, Beweis hat den Vorzug, dass er nicht nur für $\mathbb{C} \mid \mathbb{R}$, sondern allgemeiner im Kontext der reell abgeschlossenen Körper funktioniert.

3.5.5 Die letzte Seite zur Körpertheorie

Anmerkung zum Lernen. Bei der Untersuchung endlicher Körpererweiterungen sollte man sich die folgenden Fragen stellen:

- Wie lässt sich die gegebene Fragestellung im Rahmen der Körpererweiterungen formalisieren?
- Greift ein allgemeiner Struktur-/Klassifikationssatz? (zum Beispiel bei endlichen Körpern oder bei Kreisteilungskörpern.) Oder ist eine Analyse von Hand erforderlich?
- Sind die relevanten Körpererweiterungen separabel? (fast immer: ja) Sind die die relevanten Körpererweiterungen normal? (oft genug: leider nicht; wie kann man das beheben?)
- Was liefert der Hauptsatz der Galoistheorie in dieser Situation?
- (Wie) Lässt sich das Problem in kleinere Probleme zerlegen?
  - Gibt es offensichtliche „einfache“ Zwischenkörper?
  - Gibt es offensichtliche Automorphismen/Einbettungen?
  - Gibt es offensichtliche Untergruppen der Galoisgruppe? Helfen die Sylowsätze dabei? Was kann man über die entsprechenden Fixkörper sagen?
  - Gibt es ein offensichtliches primitives Element? Welches Minimalpolynom hat es? Helfen die Irreduzibilitätskriterien dabei? Was liefert das Konjugationsprinzip?
  - Gibt es einen Zusammenhang mit Einheitswurzeln?
- Wie vergleicht sich die Situation mit bereits bekannten Beispielen?

Anmerkung für Lehramtsstudenten. Aufgaben zu Körpererweiterungen bzw. zur Galoistheorie sind ein fester Bestandteil der Staatsexamensklausuren. Wie immer gilt: Übung macht den Meister! Umgekehrt helfen Beispiele natürlich auch dabei, die allgemeine Theorie besser zu verstehen. Sie sollten das Erlernen der Galoistheorie aber nicht als Last oder unnötige Komplikation auf dem Weg in den Schuldienst empfinden, sondern stolz darauf sein, dass Sie damit eine Methode beherrschen, mit der sich viele klassische Probleme (die auch für die Schulmathematik relevant sind) lösen lassen.

A
Anhang

Überblick über dieses Kapitel.

A.1	Die komplexen Zahlen	A.2
A.2	Kategorien	A.6
A.3	Freie Gruppen	A.9
A.4	Formalisierte Algebra	A.13
A.5	Sylow-Zoo	A.17
A.6	Euklidische Ringe	A.21
A.7	Konstruierbarkeit mit Zirkel und Lineal	A.27
A.8	Anwendungen endlicher Körper	A.32
A.9	Funktoren	A.37

A.1 Die komplexen Zahlen

Die reellen Zahlen sind bezüglich der Ordnungsrelation vollständig. Aus algebraischer Sicht sind sie jedoch nicht vollständig genug: Nicht alle polynomialen Gleichungen mit reellen Koeffizienten besitzen eine reelle Nullstelle. Ein Körper ist algebraisch abgeschlossen, wenn jede (nicht-konstante) polynomiale Gleichung mindestens eine Lösung besitzt. Die komplexen Zahlen sind die „kleinste“ Erweiterung der reellen Zahlen zu einem algebraisch abgeschlossenen Körper. Faszinierenderweise genügt es dabei, geeignet eine Zahl i hinzuzufügen, die $i^2 = -1$ erfüllt.

Definition A.1.1 (algebraisch abgeschlossen)**.** Ein Körper K ist *algebraisch abgeschlossen*, wenn folgendes gilt: Für alle $n \in \mathbb{N}\backslash\{0\}$ und alle $a_0, \dots, a_n \in K$ mit $a_n \neq 0$ gibt es (mindestens) ein $x \in K$ mit

$$\sum_{j=0}^{n} a_j \cdot x^k = 0.$$

Beispiel A.1.2.

- Die rationalen Zahlen sind *nicht* algebraisch abgeschlossen, da es zum Beispiel kein $x \in \mathbb{Q}$ mit $x^2 = 2$ gibt (Beispiel I.1.4.9).
- Die reellen Zahlen sind *nicht* algebraisch abgeschlossen, da es kein $x \in \mathbb{R}$ mit $x^2 = -1$ gibt (Bemerkung I.A.5.10).

Satz A.1.3 (die komplexen Zahlen [?])**.** *Sei* $\mathbb{C} := \mathbb{R} \times \mathbb{R}$*. Wir bezeichnen* $\mathbb{C}$ *als Menge der* komplexen Zahlen*. Bezüglich den Operationen*

$$\begin{aligned} +\colon \mathbb{C} \times \mathbb{C} &\longrightarrow \mathbb{C} \\ \big((x,y),(x',y')\big) &\longmapsto (x+x', y+y') \\ \cdot\colon \mathbb{C} \times \mathbb{C} &\longrightarrow \mathbb{C} \\ \big((x,y),(x',y')\big) &\longmapsto (x \cdot x' - y \cdot y', x \cdot y' + x' \cdot y) \end{aligned}$$

bildet $\mathbb{C}$ *einen algebraisch abgeschlossenen Körper mit additiv neutralem Element* $(0,0)$ *und multiplikativ neutralem Element* $(1,0)$*. Die Abbildung*

$$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{C} \\ x &\longmapsto (x,0) \end{aligned}$$

ist injektiv und mit Addition bzw. Multiplikation verträglich. Elemente im Bild dieser Abbildung heißen reell*. Bis auf „kanonischen Isomorphismus“ ist* $\mathbb{C}$ *der „kleinste“ algebraisch abgeschlossene Körper, der* $\mathbb{R}$ *umfasst.*

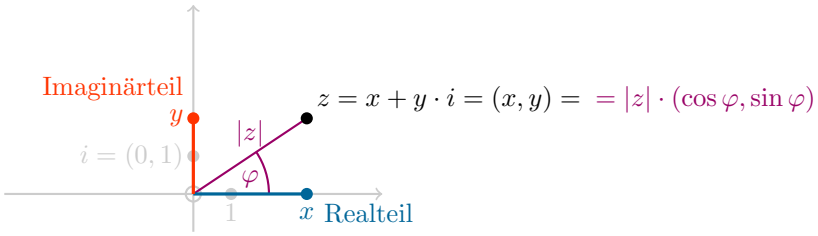


Abbildung A.1.: komplexe Zahlen, schematisch

Beispiel A.1.4 (die imaginäre Einheit, Realteil/Imaginärteil)**.** Man bezeichnet

$$i := (0,1) \in \mathbb{C}$$

als *imaginäre Einheit*. Ist $z = (x, y) \in \mathbb{C}$ mit $x, y \in \mathbb{R}$, so bezeichnet man (Abbildung A.1)

- x als *Realteil von* z und
- y als *Imaginärteil von* z.

Wir schreiben dann für $(x, y) \in \mathbb{C}$ mit $x, y \in \mathbb{R}$ auch

$$x + y \cdot i := (x, y) \in \mathbb{C};$$

diese Notation ist mit der kanonischen Inklusion $\mathbb{R} \longrightarrow \mathbb{C}$ und den Rechenoperationen verträglich (nachrechnen!).

Nach Konstruktion gilt

$$\begin{aligned} i^2 &= i \cdot i \\ &= (0,1) \cdot (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -(1, 0) \\ &= -1. \end{aligned}$$

Insbesondere gibt es *keine* totale Ordnung auf $\mathbb{C}$, die $\mathbb{C}$ zu einem angeordneten Körper macht (Bemerkung I.A.5.10).

Beispiel A.1.5 (Summe von Quadraten)**.** Für alle $x, y \in \mathbb{R}$ gilt

$$\begin{aligned} (x + y \cdot i) \cdot (x - y \cdot i) &= x^2 + y \cdot i \cdot x - x \cdot y \cdot i - y \cdot i \cdot y \cdot i \\ &= x^2 + x \cdot y \cdot i - x \cdot y \cdot i - y^2 \cdot i^2 \\ &= x^2 + 0 - y^2 \cdot (-1) \\ &= x^2 + y^2. \end{aligned}$$

Beispiel A.1.6 (komplexe Division)**.** Die Berechnung aus Beispiel A.1.5 ist insbesondere hilfreich, um komplexe Divisionen durch geeignetes Erweitern von Hand zu berechnen: Zum Beispiel gilt

$$\begin{aligned}\frac{1}{2+i} &= \frac{1\cdot(2-i)}{(2+i)\cdot(2-i)} && (? \text{ Erweitern mit } 2-i)\\ &= \frac{2-i}{4+1} && (? \text{ nach Beispiel A.1.5})\\ &= \frac{2}{5} - \frac{1}{5}\cdot i.\end{aligned}$$

Also hat $1/(2+i)$ den Realteil ? $2/5$ und den Imaginärteil ? $-1/5$.

Ausblick A.1.7 (Absolutbetrag)**.** Die „Größe“ von reellen bzw. komplexen Zahlen wird durch den (Absolut-)Betrag gemessen: Man definiert

$$\begin{aligned}&|\cdot|\colon \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}\\ &\qquad x \longmapsto \sqrt{x^2} = \begin{cases} x & \text{falls } x \geq 0\\ -x & \text{falls } x < 0\end{cases}\\ &|\cdot|\colon \mathbb{C} \longrightarrow \mathbb{R}_{\geq 0}\\ &\quad (x,y) \longmapsto \sqrt{x^2+y^2}. && (\text{„Pythagoras“})\end{aligned}$$

Diese Funktionen erfüllen die *Dreiecksungleichung*

$$|x| - |y| \leq |x+y| \leq |x| + |y|$$

für alle reellen/komplexen Zahlen x und y. Die Körper $\mathbb{R}$ und $\mathbb{C}$ sind bezüglich diesen Betragsfunktionen im analytischen Sinne vollständig.

Ausblick A.1.8 (Anschauung und Polardarstellung)**.** Wenn man $\mathbb{C}$ als reelle Ebene $\mathbb{R}^2$ veranschaulicht, entspricht die Addition auf $\mathbb{C}$ der Vektoraddition auf $\mathbb{R}^2$ und damit der „Verschiebung“ (Abbildung A.2).

Die Multiplikation auf $\mathbb{C}$ entspricht in diesem Bild der „Streckung und Rotation“. Genauer lässt sich dies in Polarkoordinaten erklären: Mit analytischen Mitteln kann man zeigen, dass jede komplexe Zahl $z = x + y\cdot i$ mit $x, y \in \mathbb{R}$ in der *Polardarstellung*

$$z = |z| \cdot (\cos\varphi, \sin\varphi) = |z| \cdot e^{i\cdot\varphi}$$

geschrieben werden kann, wobei $\varphi = \arctan(x/y)$; ist $y = 0$, so setzt man $\varphi = 0$. Dann gilt: Sind $r, r', \varphi, \varphi' \in \mathbb{R}$, so ist

$$(r\cdot e^{i\cdot\varphi})\cdot(r'\cdot e^{i\cdot\varphi'}) = (r\cdot r')\cdot e^{i\cdot(\varphi+\varphi')};$$

der vordere Term ist dabei eine „Streckung“, der hintere eine „Rotation“.

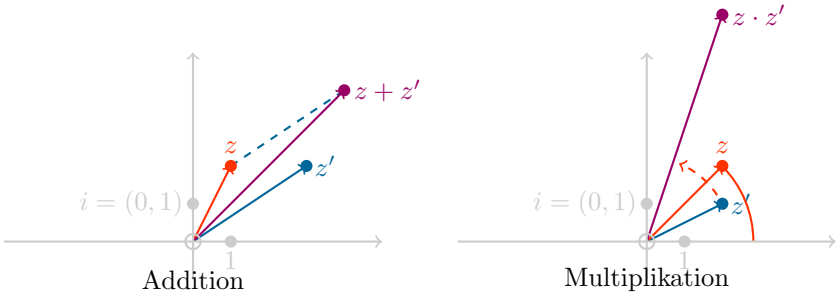


Abbildung A.2.: Addition/Multiplikation komplexer Zahlen, schematisch

Der Absolutbetrag einer komplexen Zahl stimmt dabei mit dem euklidischen Abstand zuR 0 überein (nach dem Satz des Pythagoras).

Bemerkung A.1.9 (komplexe Konjugation)**.** Die Abbildung

$$\begin{aligned} \overline{\cdot}\colon \mathbb{C} &\longrightarrow \mathbb{C} \\ (x, y) &\longmapsto (x, -y) \end{aligned}$$

wird als *komplexe Konjugation* bezeichnet. Geometrisch handelt es sich dabei um die Spiegelung an der reellen Achse. Algebraisch betrachtet ist die komplexe Konjugation ein Automorphismus des Körpers $\mathbb{C}$ (d.h. mit Addition und Multiplikation verträglich). Dieser erlaubt es, viele Aspekte des Zusammenspiels zwischen reellen und komplexen Zahlen zu beschreiben. Zum Beispiel gilt (nachrechnen):

- Ist $z \in \mathbb{C}$, so ist z genau dann reell, wenn $\overline{z} = z$ ist.
- Für alle $z \in \mathbb{C}$ ist $z + \overline{z}$ reell.
- Für alle $z \in \mathbb{C}$ ist $z \cdot \overline{z}$ reell und nicht-negativ. Es ist $|z| = \sqrt{z \cdot \overline{z}}$.

A.2 Kategorien

Mathematische Theorien bestehen aus Objekten (z.B. Gruppen, reelle Vektorräume, topologische Räume, messbare Räume, ...) und strukturerhaltenden Abbildungen (z.B. Gruppenhomomorphismen, $\mathbb{R}$-lineare Abbildungen, stetige Abbildungen, messbare Abbildungen, ...) dazwischen. Dies abstrahiert man zum Begriff der Kategorie [9, 24, 23]:

Definition A.2.1 (Kategorie)**.** Eine *Kategorie* C besteht aus den folgenden Komponenten:

- Einer Klasse[1] $\mathrm{Ob}(C)$; die Elemente von $\mathrm{Ob}(C)$ heißen *Objekte von* C.
- Zu je zwei Objekten $X, Y \in \mathrm{Ob}(C)$ einer Menge $\mathrm{Mor}_C(X, Y)$; die Elemente von $\mathrm{Mor}_C(X, Y)$ heißen *Morphismen von* X *nach* Y *in* C. (Dabei wird implizit angenommen, dass die Morphismenmengen zwischen verschiedenen Objektpaaren disjunkt sind.)
- Zu je drei Objekten $X, Y, Z \in \mathrm{Ob}(C)$ einer Verknüpfung

$$\begin{aligned} \circ\colon \mathrm{Mor}_C(Y, Z) \times \mathrm{Mor}_C(X, Y) &\longrightarrow \mathrm{Mor}_C(X, Z) \\ (g, f) &\longmapsto g \circ f \end{aligned}$$

  von Morphismen.

Dabei müssen folgende Bedingungen erfüllt sein:

- Für jedes Objekt X in C gibt es einen Morphismus $\mathrm{id}_X \in \mathrm{Mor}_C(X, X)$ mit folgender Eigenschaft: Für alle $Y \in \mathrm{Ob}(C)$ und alle Morphismen $f \in \mathrm{Mor}_C(X, Y)$ bzw. $g \in \mathrm{Mor}_C(Y, X)$ gilt

$$f \circ \mathrm{id}_X = f \qquad \text{und} \qquad \mathrm{id}_X \circ g = g.$$

  (Dadurch ist id_X eindeutig bestimmt und heißt *Identitätsmorphismus von* X *in* C.)

- Die Verknüpfung von Morphismen ist assoziativ: Für alle Objekte W, X, Y, Z in C und alle Morphismen $f \in \mathrm{Mor}_C(W, X)$, $g \in \mathrm{Mor}_C(X, Y)$ und $h \in \mathrm{Mor}_C(Y, Z)$ gilt

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

[1] Klassen sind eine Verallgemeinerung von Mengen; so gibt es etwa die Klasse aller Mengen [16, 29].

Caveat A.2.2. Das Konzept der Morphismen und Verknüpfungen ist nach dem Beispiel der Abbildungen zwischen Mengen und der gewöhnlichen Abbildungskomposition modelliert. Im allgemeinen muss es sich bei Morphismen aber nicht um Abbildungen zwischen Mengen und bei der Verknüpfung nicht um Abbildungskomposition handeln!

Beispiel A.2.3 (leere Kategorie)**.** Die *leere Kategorie* ist die (eindeutig bestimmte) Kategorie, deren Objektklasse die leere Menge ist.

Beispiel A.2.4 (Mengenlehre)**.** Die Kategorie Set der Mengen besteht aus:

- Objekte: Es sei $\mathrm{Ob}(\mathsf{Set})$ die Klasse(!) aller Mengen.
- Morphismen: Sind X und Y Mengen, so sei $\mathrm{Mor}_{\mathsf{Set}}(X, Y)$ die Menge aller mengentheoretischen Abbildungen $X \longrightarrow Y$.
- Verknüpfungen: Sind X, Y und Z Mengen, so sei die Verknüpfung $\mathrm{Mor}_{\mathsf{Set}}(Y, Z) \times \mathrm{Mor}_{\mathsf{Set}}(X, Y) \longrightarrow \mathrm{Mor}_{\mathsf{Set}}(X, Z)$ die gewöhnliche Abbildungskomposition.

Es ist klar, dass die Verknüpfung assoziativ ist. Ist X eine Menge, so ist die gewöhnliche Identitätsabbildung

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

der Identitätsmorphismus id_X von X in Set.

Beispiel A.2.5 (Algebra)**.** Die Kategorie $\mathsf{Vect}_{\mathbb{R}}$ der $\mathbb{R}$-Vektorräume besteht aus:

- Objekte: Es sei $\mathrm{Ob}(\mathsf{Vect}_{\mathbb{R}})$ die Klasse aller $\mathbb{R}$-Vektorräume.
- Morphismen: Sind V und W reelle Vektorräume, so sei $\mathrm{Mor}_{\mathsf{Vect}_{\mathbb{R}}}(V, W)$ die Menge aller linearen Abbildungen $V \longrightarrow W$.
- Verknüpfungen: Die Verknüpfung sei durch die gewöhnliche Abbildungskomposition gegeben.

Analog erhält man auch die Kategorie Group der Gruppen, die Kategorie Ab der abelschen Gruppen, die Kategorie Mod_R der R-Rechtsmoduln bzw. die Kategorie ${}_R\mathsf{Mod}$ der R-Linksmoduln über einem Ring R, ...

Beispiel A.2.6 (Gruppen als Kategorien)**.** Sei G eine Gruppe. Dann erhalten wir wie folgt eine Kategorie C_G:

- Objekte: Die Kategorie C_G besitze genau ein Objekt, etwa 0.
- Morphismen: Es sei $\mathrm{Mor}_C(0, 0) := G$.

- Verknüpfungen: Die Verknüpfung sei wie folgt gegeben:

$$\begin{aligned} \mathrm{Mor}_C(0,0) \times \mathrm{Mor}_C(0,0) &\longrightarrow \mathrm{Mor}_C(0,0) \\ (g,h) &\longmapsto g \cdot h. \end{aligned}$$

Beispiel A.2.7 (Topologie)**.** Die Kategorie Top der topologischen Räume besteht aus:

- Objekte: Es sei Ob(Top) die Klasse aller topologischen Räume.
- Morphismen: Sind X und Y topologische Räume, so sei

$$\mathrm{map}(X,Y) := \mathrm{Mor}_{\mathsf{Top}}(X,Y)$$

  die Menge aller stetigen Abbildungen $X \longrightarrow Y$.

- Verknüpfungen: Die Verknüpfung sei durch die gewöhnliche Abbildungskomposition gegeben.

Alle Begriffe, die sich durch Objekte und (Komposition von) Morphismen ausdrücken lassen, lassen sich zu entsprechenden Begriffen in allgemeinen Kategorien verallgemeinern. Ein erstes Beispiel ist der Isomorphiebegriff:

Definition A.2.8 (Isomorphismus)**.** Sei C eine Kategorie. Objekte $X, Y \in \mathrm{Ob}(C)$ sind *isomorph in* C, wenn es Morphismen $f \in \mathrm{Mor}_C(X,Y)$ und $g \in \mathrm{Mor}_C(Y,X)$ mit

$$g \circ f = \mathrm{id}_X \qquad \text{und} \qquad f \circ g = \mathrm{id}_Y$$

gibt. In diesem Fall sind f und g *Isomorphismen in* C und wir schreiben $X \cong_C Y$ (oder wenn die Kategorie aus dem Kontext klar ist: $X \cong Y$).

Beispiel A.2.9 (Isomorphismenbegriffe)**.**

- Objekte in Set sind genau dann isomorph, wenn sie gleichmächtig sind.
- Objekte in Group, Ab, $\mathsf{Vect}_{\mathbb{R}}$, ... sind genau dann im obigen Sinne isomorph, wenn sie im gewöhnlichen algebraischen Sinne isomorph sind.
- Objekte in Top sind genau dann isomorph, wenn sie homöomorph sind.

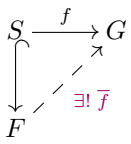
Definition A.2.10 (Automorphismengruppe)**.** Sei C eine Kategorie und sei $X \in \mathrm{Ob}(C)$. Dann bildet die Menge $\mathrm{Aut}(X)$ aller Isomorphismen $X \longrightarrow X$ in C bezüglich der Komposition von Morphismen in C eine Gruppe, die *Automorphismengruppe von* X *in* C.

A.3 Freie Gruppen

Vektorräume besitzen ausgezeichnete Erzeugendensysteme, nämlich die Erzeugendensysteme, die so „frei“ wie möglich sind. Genauso kann man in der Gruppentheorie formulieren, was es bedeutet, ein freies Erzeugendensystem zu sein. Ein wesentlicher Unterschied ist jedoch, dass Gruppen im allgemeinen *keine* freie Erzeugendensysteme besitzen.

Für die Definition von Freiheit in der Gruppentheorie übersetzen wir die universelle Eigenschaft von Basen (Satz I.4.3.1) in die Gruppentheorie:

Definition A.3.1 (freies Erzeugendensystem, freie Gruppe)**.** Sei S eine Menge. Eine Gruppe F, die S enthält, ist *frei von S erzeugt*, wenn F die folgende Eigenschaft besitzt: Für jede Gruppe G und jede Abbildung $f\colon S \longrightarrow G$ gibt es genau einen Gruppenhomomorphismus $\overline{f}\colon F \longrightarrow G$, der f fortsetzt:



Eine Gruppe ist *frei*, wenn sie ein freies Erzeugendensystem enthält.

Beispiel A.3.2 ((un)freie Gruppen)**.**

- Die triviale Gruppe ist frei, frei erzeugt von der leeren Menge.
- Die Menge $\{1\}$ ist ein freies Erzeugendensystem von $\mathbb{Z}$. Insbesondere ist $\mathbb{Z}$ eine freie Gruppe.

  Die Menge $\{1,-1\}$ ist *kein* freies Erzeugendensystem von $\mathbb{Z}$, denn: Wir betrachten die Abbildung

  $$\begin{aligned} f\colon \{1,-1\} &\longrightarrow \mathbb{Z} \\ 1 &\longmapsto 1 \\ -1 &\longmapsto 0. \end{aligned}$$

  Angenommen, es gäbe einen Gruppenhomomorphismus $\overline{f}\colon \mathbb{Z} \longrightarrow \mathbb{Z}$, der f fortsetzt. Dann wäre (in $\mathbb{Z}$)

  $$0 = f(-1) = \overline{f}(-1) = -\overline{f}(1) = -f(1) = -1,$$

  was nicht sein kann.

  Analog ist auch $\{2,3\}$ *kein* freies Erzeugendensystem von $\mathbb{Z}$.
- Die Gruppen $\mathbb{Z}/2$ und $\mathbb{Z}^2$ sind *nicht* frei (Übungsaufgabe).

- Sei
$$a := \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \quad \text{und} \quad b := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$
Dann ist die Gruppe
$$\langle \{a, b\} \rangle_{\mathrm{SL}_2(\mathbb{R})}$$
frei mit freiem Erzeugendensystem $\{a, b\}$. Dies ist *nicht* offensichtlich. Es gibt einen geometrischen Trick, mit dem das nachgewiesen werden kann [20].

Satz A.3.3 (Eindeutigkeit freier Gruppen). *Sei S eine Menge. Dann gibt es (bis auf kanonische Isomorphie) höchstens eine Gruppe, die frei von S erzeugt ist.*

Beweis. Dies folgt aus dem Standardargument für die Eindeutigkeit von durch universelle Eigenschaften charakterisierten Objekten (*Brüderchen, komm tanz mit mir. Einmal hin, einmal her; rundherum, das ist nicht schwer* ..., Abbildung II.2.2). □

Satz A.3.4 (Existenz freier Gruppen). *Sei S eine Menge. Dann gibt es eine Gruppe, die frei von S erzeugt ist.*

Beweisskizze. Die Idee ist, aus „Wörtern“ mit Symbolen aus S (und deren Inversen) eine Gruppe zu konstruieren, indem man nur die offensichtlichen Verknüpfungs- und Kürzungsregeln verwendet. Dazu betrachten wir das Alphabet
$$A := S \cup \widehat{S},$$
wobei $\widehat{S} := \{\widehat{s} \mid s \in S\}$ eine disjunkte Kopie von S ist; d.h. $\widehat{\cdot} : S \longrightarrow \widehat{S}$ ist eine Bijektion und $S \cap \widehat{S} = \emptyset$. Für $s \in S$ wird $\widehat{s}$ die Rolle des Inversen von s übernehmen.

- Als ersten Schritt definieren wir A^* als die Menge aller endlichen Folgen über A. Insbesondere ist die leere Folge ε in A^* und A^* bildet einen Monoid bezüglich Hintereinanderschreiben von Wörtern (mit neutralem Element ε).
- Als zweiten Schritt definieren wir
$$F(S) := A^*/\!\sim,$$
wobei $\sim$ die Äquivalenzrelation auf A^* ist, die von
$$\forall_{x,y \in A^*} \quad \forall_{s \in S} \quad x s \widehat{s} y \sim xy,$$
$$\forall_{x,y \in A^*} \quad \forall_{s \in S} \quad x \widehat{s} s y \sim xy$$
erzeugt wird. Das heißt, $\sim$ ist die kleinste (bezüglich Inklusion) Äquivalenzrelation auf A^*, die die obigen Bedingungen erfüllt.

  Dann induziert die Verknüpfung auf A^* eine wohldefinierte Abbildung $\cdot : F(S) \times F(S) \longrightarrow F(S)$ (nachrechnen).

Die Menge $F(S)$ bildet bezüglich der obigen Verknüpfung eine Gruppe (nachrechnen). Außerdem ist $F(S)$ frei von S erzeugt; an dieser Stelle muss man vorsichtig vorgehen, da zunächst gar nicht klar ist, dass die kanonische Abbildung $S \longrightarrow F(S)$ überhaupt injektiv ist (nachrechnen). □

Insbesondere folgt aus der obigen Konstruktion und der Eindeutigkeit freier Gruppen, dass freie Erzeugendensysteme tatsächlich *erzeugend* sind.

A.4 Formalisierte Algebra

Die Mathematik basiert auf einem formalen Fundament, bestehend aus Logik und Mengenlehre (im klassischen Fall). Alle zulässigen Beweisschritte, Axiome, Definitionen können vollständig formalisiert werden. Aufbauend darauf können dann auch Sätze, Beweise, Konstruktionen und Beispiele formalisiert werden.

Auf den ersten Blick mag eine solche vollständige Formalisierung übertrieben und für Menschen unlesbar zu sein. Sie hat jedoch den Vorzug, dass sie maschinentauglich und maschinell überprüfbar ist und einen dazu erzieht, sauber und modular zu argumentieren. Sogenannte *proof assistants* ermöglichen es, formalisierte Mathematik zu implementieren und zu überprüfen. Leistungsstarke *proof assistants* sind zum Beispiel Lean [**?**], Coq [**?**] und Isabelle [**?**].

Auf den folgenden Seiten geben wir ein Beispiel für eine Formalisierung in Lean des Beginns dieser Algebra-Vorlesung, d.h. eine Formalisierung der gruppentheoretischen Grundbegriffe. Auch ohne mit den Details von Lean vertraut zu sein, ist die Nähe zur „gewöhnlichen“ Formulierung dieser Definitionen, Sätze und Beweise deutlich zu erkennen. Lean kann bequem im Webbrowser ausprobiert werden: https://live.lean-lang.org/

Die folgende Implementation zeigt nur, dass es prinzipiell möglich ist, mathematische Theorien, Definitionen, Sätze und Beweise zu formalisieren. In der Praxis würde man natürlich auf die bereits vorhandenen, umfangreichen, Bibliotheken (wie mathlib für Lean) zurückgreifen und den Quellcode ausführlicher kommentieren.

Ein Monoidtheorie-Fragment in Lean

```
universe u -- fixing a background universe

-- Definition: monoids (unital, associative)
class monoid
 (a : Type u) [BEq a]
where
 -- structure
 comp : a -> a -> a
 e : a
 -- properties
 is_associative : ∀ (x : a) (y : a) (z : a),
             comp x (comp y z) = comp (comp x y) z
 is_neutral : ∀ (x : a), comp x e = x ∧ comp e x = x
```

```
-- inverses of elements in monoids
def is_inverse_of
  (a : Type u) [BEq a] [m : monoid a]
  (x : a)
  (y : a)
:= m.comp x y = m.e ∧ m.comp y x = m.e

-- an element of a monoid is invertible if there exists an inverse element
def is_invertible
  (a : Type u) [BEq a] [m : monoid a]
  (x : a)
:= ∃ y : a, is_inverse_of a x y

-- elements in monoids that behave like the neutral element
-- are equal to the neutral element
theorem neutral_element_is_unique
  (a : Type u) [BEq a] [m : monoid a]
  (e' : a)
  (is_neutral_e' : ∀ x : a, m.comp x e' = x ∧ m.comp e' x = x)
: m.e = e'
:=
calc
  m.e = m.comp m.e e' := by exact (is_neutral_e' m.e).1.symm
  _   = e'            := by exact (m.is_neutral e').2

-- Definition: monoid homomorphism
class monoid_hom
  (a : Type u) [BEq a] [ma : monoid a]
  (b : Type u) [BEq b] [mb : monoid b]
where
  -- structure
  map : a -> b
  -- properties
  is_multiplicative : ∀ (x : a) (y : a),
                 mb.comp (map x) (map y) = map (ma.comp x y)
  preserves_neutral_elt : map (ma.e) = mb.e

-- applying a monoid homomorphism to an invertible element
-- results in an invertible element
theorem monoid_hom_of_invertible_element
  (a : Type u) [BEq a] [ma : monoid a]
  (b : Type u) [BEq b] [mb : monoid b]
  (f : monoid_hom a b)
  (x : a)
```

```
  (is_inv_x : is_invertible a x)
: is_invertible b (f.map x)
:=
by
  -- because x is invertible, there is an inverse, called y
  have ⟨y, y_is_inv_of_x⟩ := is_inv_x

  -- we show that f(y) is the inverse of f(x),
  -- by verifying the two relevant equations
  have fy_is_inverse_of_fx : is_inverse_of b (f.map x) (f.map y)
  := by
    have fxfy_is_e : mb.comp (f.map x) (f.map y) = mb.e
    := calc mb.comp (f.map x) (f.map y)
          = f.map (ma.comp x y) := by exact f.is_multiplicative x y
        _ = f.map ma.e          := by rw[y_is_inv_of_x.1]
        _ = mb.e                := by exact f.preserves_neutral_elt

    have fyfx_is_e : mb.comp (f.map y) (f.map x) = mb.e
    := calc mb.comp (f.map y) (f.map x)
          = f.map (ma.comp y x) := by exact f.is_multiplicative y x
        _ = f.map ma.e          := by rw[y_is_inv_of_x.2]
        _ = mb.e                := by exact f.preserves_neutral_elt

    exact And.intro fxfy_is_e fyfx_is_e

  -- the element f(y) witnesses that f(x) is invertible
  show is_invertible b (f.map x)
  exact Exists.intro (f.map y) fy_is_inverse_of_fx
```

A.5 Sylow-Zoo

Die folgenden Beispiele zu Gruppen mit gegebenen Anzahlen demonstrieren Handgriffe, die bei der Verwendung der Sylowsätze für Klassifikationsfragen nützlich sind.

Beispiel A.5.1 (333)**.** Es gibt *keine* einfache Gruppe G mit $\#G = 333$, denn: Wir bestimmen zunächst die Primfaktorzerlegung von 333. Es gilt

$$333 = 3^2 \cdot 37.$$

Sei s_{37} die Anzahl der 37-Sylowgruppen von G. Mit den Sylowsätzen folgt

$$s_{37} \mid 333 \quad \text{und} \quad s_{37} \equiv 1 \mod 37.$$

Aus diesen beiden Bedingungen erhalten wir bereits (wie im Beweis von Korollar 1.3.43), dass $s_{37} = 1$ ist und damit, dass die (eindeutig bestimmte) 37-Sylowgruppe S von G ein Normalteiler in G ist (Korollar 1.3.42). Da G keine 37-Gruppe ist, folgt $S \neq G$. Außerdem ist S nicht die triviale Gruppe, da 37 ein Teiler von $\#G$ ist. Insbesondere ist G *nicht* einfach.

Beispiel A.5.2 (33)**.** Ist G eine Gruppe mit $\#G = 33$, so ist G bereits zyklisch, denn: Wir bestimmen zunächst die Primfaktorzerlegung von 33. Es gilt

$$33 = 3 \cdot 11.$$

Sei s_3 die Anzahl der 3-Sylowgruppen von G. Mit den Sylowsätzen folgt

$$s_3 \mid 33 \quad \text{und} \quad s_3 \equiv 1 \mod 3.$$

Aus diesen beiden Bedingungen erhalten wir bereits (wie im Beweis von Korollar 1.3.43), dass $s_3 = 1$ ist und damit, dass die (eindeutig bestimmte) 3-Sylowgruppe S von G ein Normalteiler in G ist (Korollar 1.3.42). Dabei gilt $S \cong_{\mathsf{Group}} \mathbb{Z}/3$, da 3 prim ist; sei $g \in S \setminus \{e\}$ (insbesondere ist $\operatorname{ord} g = 3$ und g erzeugt S).

Da 11 ein Primteiler von $\#G$ ist, gibt es außerdem ein Element $h \in G$ mit $\operatorname{ord} h = 11$ (Korollar 1.3.40). Sei $T := \langle h \rangle_G$.

Da alle nicht-trivialen Elemente von S Ordnung 3 haben und alle nicht-trivialen Elemente von T Ordnung 11 haben, folgt $S \cap T = \{e\}$. Wir zeigen:

1. Die Gruppe $H := T \cdot S \subset G$ ist abelsch.
2. Es gilt $H = G$.
3. Die Gruppe G ist zyklisch.

Zu 1. Es genügt zu zeigen, dass $g \cdot h = h \cdot g$ ist, da S und T zyklisch sind und von g bzw. h erzeugt werden. Da S ein Normalteiler ist, liefert Konjugation mit h einen Isomorphismus $f\colon S \longrightarrow S$. Wegen $S = \{e, g, g^2\}$ gibt es nur die Möglichkeit, dass $f(g) = g$ oder $f(g) = g^2$ ist.

Angenommen, es wäre $f(g) = g^2$. Wegen $h^{11} = e$ wäre dann aber

$$g = \mathrm{id}(g) = f^{11}(g) = g^{2^{11}} = g^{2048} = (g^3)^{682} \cdot g^2 = g^2,$$

im Widerspruch zu $\operatorname{ord} g = 3$. Also ist $f(g) = g$, und damit $f = \mathrm{id}_S$. Insbesondere ist

$$h \cdot g = h \cdot g \cdot h^{-1} \cdot h = f(g) \cdot h = g \cdot h.$$

Zu 2. Mit dem Satz von Lagrange (Korollar 1.1.34) und den Isomorphiesätzen (Satz 1.1.62) erhalten wir wegen $S \cap T = \{e\}$, dass

$$\#H = \#(T \cdot S) = \#S \cdot [T \cdot S : S] = \#S \cdot [T : (T \cap S)] = \#S \cdot \#T = 33 = \#G.$$

Wegen $H \subset G$ folgt somit $H = G$.

Zu 3. Aus der Klassifikation endlicher abelscher Gruppen (oder auch aus den Argumenten in den ersten beiden Teilen) folgt, dass

$$G \cong_{\mathsf{Group}} \mathbb{Z}/3 \times \mathbb{Z}/11.$$

Mit dem Chinesischen Restsatz (oder durch Berechnung von $\operatorname{ord}(g \cdot h)$) erhalten wir daraus, dass $G \cong_{\mathsf{Group}} \mathbb{Z}/33$ ist. Insbesondere ist G zyklisch.

Beispiel A.5.3 (21)**.** Ist G eine Gruppe mit $\#G = 21$, so ist G im allgemeinen *nicht* abelsch, denn: Das semi-direkte Produkt

$$\mathbb{Z}/7 \rtimes_\varphi \mathbb{Z}/3$$

mit

$$\begin{aligned} \varphi\colon \mathbb{Z}/3 &\longrightarrow \mathrm{Aut}(\mathbb{Z}/7) \\ [n] &\longmapsto \big([x] \mapsto [x^{2^n}]\big) \end{aligned}$$

ist *nicht* abelsch (nachrechnen).

Wie könnte man mit den Sylowsätzen darauf kommen? Wie in Korollar 1.3.43 kann man zeigen, dass es genau eine 7-Sylowgruppe T in G gibt (die daher ein Normalteiler in G ist; Korollar 1.3.42) und dass $T \cong_{\mathsf{Group}} \mathbb{Z}/7$ ist. Außerdem gibt es eine 3-Sylowgruppe S und wegen $\#G = 21 = 3 \cdot 7$ folgt $\#S = 3$, und damit $S \cong_{\mathsf{Group}} \mathbb{Z}/3$.

Wie in Beispiel A.5.2 erhalten wir $S \cap T = \{e\}$ und $S \cdot T = G$. Also ist G ein semi-direktes Produkt $T \rtimes S$ von T und S (Beispiel 1.1.72). Somit ist

$$G \cong_{\mathsf{Group}} \mathbb{Z}/7 \rtimes_\varphi \mathbb{Z}/3$$

für ein geeignetes $\varphi\colon \mathbb{Z}/3 \longrightarrow \mathrm{Aut}(\mathbb{Z}/7)$. Daher müssen wir nur untersuchen, ob es ein solches nicht-triviales φ gibt ...

Beispiel A.5.4 (12)**.** Ist G eine Gruppe mit $\#G = 12$, so ist G auflösbar, denn: Wir betrachten zunächst die Primfaktorzerlegung von 12. Es gilt

$$12 = 2^2 \cdot 3.$$

Sei s_2 die Anzahl der 2-Sylowgruppen von G und s_3 die Anzahl der 3-Sylowgruppen von G. Mit den Sylowsätzen (Satz 1.3.39) folgt

$$\begin{aligned} s_2 \mid 12 \quad &\text{und} \quad s_2 \equiv 1 \mod 2, \\ s_3 \mid 12 \quad &\text{und} \quad s_3 \equiv 1 \mod 3. \end{aligned}$$

Also ist

$$s_2 \in \{1, 3\} \quad \text{und} \quad s_3 \in \{1, 4\}.$$

Wir zeigen, dass $s_2 = 1$ oder $s_3 = 1$ gilt: Sei $s_3 \neq 1$, d.h. $s_3 = 4$. dann ist $s_2 = 1$, denn: Ist S eine 3-Sylowgruppe von G, so ist $\#S = 3$ und damit $S \cong_{\mathsf{Group}} \mathbb{Z}/3$. Je zwei 3-Sylowgruppen S, T von G erfüllen also $S = T$ oder $S \cap T = \{e\}$. Wegen $s_3 = 4$ liegen

$$1 + 4 \cdot (3 - 1) = 9$$

Elemente in der Vereinigung V_3 aller 3-Sylowgruppen von G.

Ist S eine 2-Sylowgruppe von G, so ist $\#S = 4$ und aus dem Satz von Lagrange (Korollar 1.1.34) folgt

$$V_3 \cap S = \{e\}.$$

Wegen

$$\#(G \setminus V_3) = \#G - \#V_3 = 12 - 9 = 3$$

erhalten wir somit, dass es in G nur Platz für eine 2-Sylowgruppe gibt. Also ist $s_2 = 1$.

Daher ist $s_2 = 1$ oder $s_3 = 1$. Somit gibt es eine normale 2-Sylowgruppe oder eine normale 3-Sylowgruppe in G (Korollar 1.3.42). Wegen

$$\frac{12}{3} = 4 = 2^2 \quad \text{und} \quad \frac{12}{4} = 3$$

sind die zugehörigen Quotientengruppen auflösbar (Satz 1.3.37). Da die Sylowgruppen auch auflösbar sind (Satz 1.3.37), erhalten wir mit Proposition 1.3.27, dass auch die Erweiterungsgruppe G auflösbar ist.

Man beachte dabei, dass die Fälle $s_2 \neq 1$ bzw. $s_3 \neq 1$ beide vorkommen (nämlich in D_6 bzw. A_4).

Beispiel A.5.5 (24)**.** Ist G eine Gruppe mit $\#G = 24$, so ist G *nicht* einfach, denn: Wir betrachten zunächst die Primfaktorzerlegung von 24. Es gilt

$$24 = 2^3 \cdot 3.$$

Sei s_2 die Anzahl der 2-Sylowgruppen von G und s_3 die Anzahl der 3-Sylowgruppen von G. Mit den Sylowsätzen (Satz 1.3.39) folgt

$$s_2 \mid 24 \quad \text{und} \quad s_2 \equiv 1 \mod 2$$

Also ist

$$s_2 \in \{1, 3\}.$$

Ist $s_2 = 1$, so besitzt G einen nicht-trivialen Normalteiler (nämlich eine/die 2-Sylowgruppe; Korollar 1.3.42). Sei also im folgenden $s_2 = 3$. Wir betrachten die Konjugationsoperation

$$\begin{aligned} \varrho\colon G &\longrightarrow S_X \\ g &\longmapsto (S \mapsto g \cdot S \cdot g^{-1}) \end{aligned}$$

von G auf der Menge X der 2-Sylowgruppen von G. Sei

$$N := \ker \varrho.$$

Dann ist N ein Normalteiler in G.

- Es ist $N \neq \{e\}$, denn: Wäre $N = \{e\}$, so wäre ϱ injektiv. Aber es gilt $\#G = 24 > 6 = \#S_X$ (wegen $\#X = 3$). Also ist $N \neq \{e\}$.
- Es ist $N \neq G$, denn: Wäre $N = G$, so wäre $\varrho(g) = \mathrm{id}_X$ für alle $g \in G$, und damit
$$\forall_{g \in G} \quad \forall_{S \in X} \quad g \cdot S \cdot g^{-1} = S.$$
Also wäre jede 2-Sylowgruppe in G normal, im Widerspruch zu $s_2 \neq 1$ (und der Tatsache, dass alle 2-Sylowgruppen konjugiert zueinander sind; Korollar 1.3.42). Also ist $N \neq G$.

Daher ist N ein Normalteiler in G, der zeigt, dass G *nicht* einfach ist.

(Mit unseren bisherigen Beispielen und Methoden folgt bereits, dass alle Gruppen mit höchstens 12 Elementen auflösbar sind; in Kombination mit dem obigen Argument zeigt dies, dass auch alle Gruppen G mit $\#G = 24$ auflösbar sind.)

Bemerkung A.5.6 (für lange Winterabende ...)**.** Mit den bisher entwickelten Techniken kann man nachweisen, dass jede Gruppe G mit $\#G < 60$ auflösbar ist.

A.6 Euklidische Ringe

Der Vollständigkeit halber wiederholen wir Grundlagen über euklidische Ringe aus der Linearen Algebra II (Kapitel II.2.4.2ff): Wie können wir beweisen, dass $\mathbb{Z}$ und Polynomringe über Körpern Hauptidealringe sind? Die grundlegende Idee dazu ist, Division mit Rest zu nutzen. Wir können dies folgendermaßen formalisieren:

Definition A.6.1 (euklidischer Ring)**.** Sei R ein Integritätsring.

- Eine *euklidische Gradfunktion* auf R ist eine Abbildung $\delta\colon R \longrightarrow \mathbb{N}$ mit: Für alle $x \in R$ und alle $y \in R \setminus \{0\}$ gibt es $r, s \in R$ mit

$$x = s \cdot y + r \quad \text{und} \quad \big[\delta(r) < \delta(y) \text{ oder } r = 0\big].$$

- Der Ring R ist ein *euklidischer Ring*, wenn er eine euklidische Gradfunktion besitzt.

Da euklidische Ringe eine Verallgemeinerung großer Teile der elementaren Zahlentheorie (in $\mathbb{Z}$) erlauben, die auch von Euklid untersucht wurde, tragen auch diese Strukturen den Namen Euklids.

Beispiel A.6.2 (die ganzen Zahlen als euklidischer Ring)**.** Die Abbildung (wobei $|\cdot|$ den gewöhnlichen Absolutbetrag auf $\mathbb{R}$ bezeichnet)

$$\begin{aligned} \delta\colon \mathbb{Z} &\longrightarrow \mathbb{N} \\ x &\longmapsto |x| \end{aligned}$$

ist eine euklidische Gradfunktion auf $\mathbb{Z}$, denn: Seien $x, y \in \mathbb{Z}$ mit $y \neq 0$. Wir betrachten nur den Fall $x, y > 0$ (die anderen Fälle gehen analog). Sei

$$s := \max\{n \in \mathbb{N} \mid n \cdot y \leq x\}.$$

Wegen $y \neq 0$ ist die Menge $\{n \in \mathbb{N} \mid n \cdot y < x\}$ endlich; außerdem enthält diese Menge 0 und ist somit nicht-leer. Das Maximum existiert somit. Nach Konstruktion hat dabei $r := x - s \cdot y$ die Eigenschaft $r \in \{0, \ldots, y-1\}$ und daher ist die Darstellung $x = s \cdot y + r$ von der gewünschten Form.

Proposition A.6.3 (Polynomringe als euklidische Ringe)**.** *Sei K ein Körper. Dann ist der Polynomring $K[T]$ ein euklidischer Ring bezüglich der modifizierten Gradabbildung* $\max(\deg, 0)\colon K[T] \longrightarrow \mathbb{N}$.

Beweis. Wir schreiben $\delta := \max(\deg, 0)\colon K[T] \longrightarrow \mathbb{N}$. Der Beweis, dass δ eine euklidische Gradfunktion ist, verwendet die *Polynomdivision*, die wie folgt algorithmisch durchgeführt werden kann:

Gegeben seien $a, b \in K[T]$ mit $b \neq 0$. Wir zeigen per Induktion über $\delta(a)$, dass es $r, s \in K[T]$ mit $a = s \cdot b + r$ und $\delta(r) < \delta(b)$ (oder sogar $r = 0$) gibt.

- *Induktionsanfang.* Sei $\delta(a) = 0$.

  ① Ist $\delta(b) = 0$, so ist $b \in K \setminus \{0\}$. Daher ist $a = a/b \cdot b + 0$ eine Darstellung der gewünschten Form.

  ② Ist $\delta(b) > 0 = \delta(a)$, so ist $a = 0 \cdot b + a$ eine Darstellung der gewünschten Form.

- *Induktionsvoraussetzung.* Sei $\delta(a) > 0$ und für alle $a' \in K[T]$ mit $\delta(a') < \delta(a)$ gebe es $r', s' \in K[T]$ mit $a' = s' \cdot b + r'$ und $\delta(r') < \delta(b)$ (oder sogar $r' = 0$).

- *Induktionsschritt.* Ohne Einschränkung sei $\delta(b) \leq \delta(a)$ (sonst ist $a = 0 \cdot b + a$ eine Darstellung der gewünschten Form). Wir schreiben

$$b = \sum_{j=0}^{n} b_j \cdot T^j \quad \text{und} \quad a = \sum_{j=0}^{m} a_j \cdot T^j$$

  mit $a_0, \ldots, a_m, b_0, \ldots, b_n \in K$ und $a_m \neq 0 \neq b_n$. Wegen $b_n \neq 0$ und $m \leq n$ können wir das Polynom (Elimination der höchsten T-Potenz aus a)

$$a' := a - \frac{a_m}{b_n} \cdot T^{m-n} \cdot b \in K[T]$$

  definieren; nach Konstruktion ist $\delta(a') < m = \delta(a)$ und

$$a = a' + \frac{a_m}{b_n} \cdot T^{m-n} \cdot b.$$

  Nach Induktionsvoraussetzung gibt es $r', s' \in K[T]$ mit $a' = s' \cdot b + r'$ und $\delta(r') < \delta(b)$ (oder sogar $r' = 0$). Damit ist

$$a = \left(s' + \frac{a_m}{b_n} \cdot T^{m-n}\right) \cdot b + r'$$

  eine Darstellung der gewünschten Form. □

Anmerkung zum Lernen. Warum funktioniert der obige Beweis *nicht* für $\mathbb{Z}[T]$ oder $\mathbb{Q}[X, Y]$?!

Beispiel A.6.4 (Polynomdivision)**.** Dividieren wir $T^3 - 1$ in $\mathbb{Q}[T]$ mit Rest durch $T + 2$, so erhalten wir $T^2 - 2 \cdot T + 4$ mit Rest -9, denn

$$T^3 - 1 = (T + 2) \cdot (T^2 - 2 \cdot T + 4) - 9.$$

Von Hand kann man dies wie folgt bestimmen:

$$
\begin{array}{rl}
T^3 & +0\cdot T^2+0\cdot T\ -1\ = (T+2)\cdot(1\cdot T^2-2\cdot T+4)-9 \\
-(\ T^3 & +2\cdot T^2\ ) \\
\hline
 & -2\cdot T^2+0\cdot T\ -1 \\
 & -(\ -2\cdot T^2-4\cdot T\ ) \\
\hline
 & \qquad +4\cdot T\ -1 \\
 & \qquad -(\ +4\cdot T\ +8\ ) \\
\hline
 & \qquad\qquad -9
\end{array}
$$

Proposition A.6.5 (euklidische Ringe sind Hauptidealringe)**.** *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei R ein euklidischer Ring mit eukildischer Gradfunktion $\delta\colon R \longrightarrow \mathbb{N}$. Da R nach Definition ein Integritätsring ist, genügt es zu zeigen, dass jedes Ideal in R ein Hauptideal ist.

Sei $A \subset R$ ein Ideal. Ohne Einschränkung sei $A \neq \{0\}$. Wir betrachten ein Element $b \in A$ mit der Minimalitätseigenschaft

$$\delta(b) = \min\big\{\delta(a) \;\big|\; a \in A \setminus \{0\}\big\} \in \mathbb{N};$$

ein solches Element existiert, da $A \setminus \{0\}$ nicht-leer ist und $\mathbb{N}$ wohlgeordnet ist. Dann gilt

$$A = \mathrm{Span}_R\{b\},$$

denn:

- Da $b \in A$ und A ein Ideal ist, ist $\mathrm{Span}_R\{b\} \subset A$.
- Sei umgekehrt $a \in A$. Da δ eine euklidische Gradfunktion ist, gibt es $r, s \in R$ mit

  $$a = s\cdot b + r \quad \text{und} \quad \big[\delta(r) < \delta(b) \text{ oder } r = 0\big].$$

  Wegen $r = a - s\cdot b$ und $a, b \in A$ folgt auch $r \in A$. Aufgrund der Minimalität von b bezüglich δ erhalten wir daraus $r = 0$.

Also ist $a = s\cdot b \in \mathrm{Span}_R\{b\}$. □

Korollar A.6.6.

1. *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Hauptidealring.*
2. *Ist K ein Körper, so ist $K[T]$ ein Hauptidealring.*

Beweis. Sowohl $\mathbb{Z}$ als auch $K[T]$ sind euklidische Ringe (Beispiel A.6.2, Proposition A.6.3). Also sind diese Ringe insbesondere auch Hauptidealringe (Proposition A.6.5). □

Caveat A.6.7 (ein nicht-euklidischer Hauptidealring)**.** Hauptidealringe sind im allgemeinen *nicht* euklidisch. Ein Beispiel für einen solchen Ring ist der Ring

$$R := \mathbb{Z}[\alpha] \subset \mathbb{C},$$

der von $\mathbb{Z}$ und

$$\alpha := \frac{1 + i \cdot \sqrt{19}}{2}$$

erzeugt wird: Eine einfache Rechnung zeigt, dass

$$R = \{x + \alpha \cdot y \mid x, y \in \mathbb{Z}\}$$

gilt (nachrechnen). Mithilfe der multiplikativen Funktion

$$\begin{aligned} N \colon R &\longrightarrow \mathbb{R}_{\geq 0} \\ z &\longmapsto |z|^2 \end{aligned}$$

kann man zeigen, dass $R^\times = \{1, -1\}$ ist und dass die Elemente 2 und 3 in R irreduzibel sind (nachrechnen).

Der Ring R ist *nicht* euklidisch, denn: *Angenommen,* es gäbe eine euklidische Gradfunktion $d \colon R \longrightarrow \mathbb{N}$. Sei $m \in R \setminus (\{0\} \cup R^\times)$ ein d-minimales Element (ein solches existiert!). Division mit Rest liefert dann $r, s \in R$ mit

$$2 = s \cdot m + r \quad \text{und} \quad \big[d(r) < d(m) \text{ oder } r = 0\big].$$

Die Minimalität von m, die Irreduzibilität von 2 bzw. 3 und $R^\times = \{1, -1\}$ ergeben somit $r \in \{0, 1, -1\}$ und

$$m \in \{-3, -2, 2, 3\} =: M.$$

Desweiteren liefert Division mit Rest $r', s' \in R$ mit

$$\alpha = s' \cdot m + r' \quad \text{und} \quad \big[d(r') < d(m) \text{ oder } r' = 0\big].$$

Analog zum vorigen Schritt folgt $r' \in \{0, 1, -1\}$, und damit, dass m in R ein Teiler von α, $\alpha + 1$ oder $\alpha - 1$ ist. Aber eine einfache Berechnung in $\mathbb{C}$ zeigt, dass α/m , $(\alpha + 1)/m$, $(\alpha - 1)/m$ für kein $m \in M$ in R liegt. Dieser Widerspruch zeigt, dass R *nicht* euklidisch ist.

Außerdem kann man mithilfe der Funktion N und einer geeigneten Verallgemeinerung des Beweises von Proposition A.6.5 zeigen, dass R ein Hauptidealring ist (die Funktion N ist zwar keine euklidische Gradfunktion auf R, aber gerade noch gut genug, um einen ähnlichen, aber etwas aufwendigeren, Beweis zu führen).

In euklidischen Ringen können wir größte gemeinsame Teiler (Definition 2.2.5) auf einfache Weise algorithmisch bestimmen. Dieses Verfahren geht auf Euklid zurück.

Algorithmus A.6.8 (der euklidische Algorithmus)**.** Sei R ein euklidischer Ring mit der euklidischen Gradfunktion $\delta\colon R \longrightarrow \mathbb{N}$. Außerdem sei ein Algorithmus für die Division mit Rest bezüglich δ gegeben. Seien $x, y \in R$. Wir berechnen nun daraus wie folgt ein Element von R:

- Ist $y = 0$, so beenden wir den Algorithmus mit x als Ergebnis.
- Ist $y \neq 0$, so bestimmen wir durch Division mit Rest $r, s \in R$ mit

$$x = s \cdot y + r \quad \text{und} \quad \big[\delta(r) < \delta(y) \text{ oder } r = 0\big]$$

  und wenden den Algorithmus rekursiv auf y und r an.

Proposition A.6.9 (Analyse des euklidischen Algorithmus)**.** *Sei R ein euklidischer Ring und seien $x, y \in R$. Dann gilt: Wendet man den euklidischen Algorithmus auf x und y bzgl. einer euklidischen Gradfunktion $\delta\colon R \longrightarrow \mathbb{N}$ auf R an, so terminiert der Algorithmus und für das resultierende Element $z \in R$ gilt*

$$(x, y) = (z)$$

bzw. $z = \mathrm{ggT}(x, y)$.

Beweis. Der Algorithmus terminiert, da in jedem Rekursionsschritt der δ-Wert des zweiten Elements sinkt (oder der Algorithmus im darauffolgenden Schritt terminiert).

Außerdem hat das berechnete Element die gewünschte Eigenschaft, denn:

- Ist $y = 0$, so ist $(x, y) = (x, 0) = (x)$.
- Ist $y \neq 0$ und sind $r, s \in R$ mit

$$x = s \cdot y + r,$$

  so gilt $(x, y) = (y, r)$ (nachrechnen).

Induktiv folgt somit die Behauptung. □

Bemerkung A.6.10 (der euklidische Algorithmus in Haskell)**.** In der funktionalen Programmiersprache Haskell (https://www.haskell.org) lässt sich der euklidische Algorithmus zum Beispiel wie folgt definieren:

```
gcd       :: (Integral a) => a -> a -> a
gcd x y   =  gcd' (abs x) (abs y)
             where gcd' a 0  =  a
                   gcd' a b  =  gcd' b (a `rem` b)
```

Beispiel A.6.11. Wir bestimmen den größten gemeinsamen Teiler von 14 und 34 in $\mathbb{Z}$ mit dem euklidischen Algorithmus:

- Anwendung auf $(14, 34)$: Division mit Rest liefert $14 = 0 \cdot 34 + 14$.
- Anwendung auf $(34, 14)$: Division mit Rest liefert $34 = 2 \cdot 14 + 6$.
- Anwendung auf $(14, 6)$: Division mit Rest liefert $14 = 2 \cdot 6 + 2$.
- Anwendung auf $(6, 2)$: Division mit Rest liefert $6 = 3 \cdot 2 + 0$.
- Anwendung auf $(2, 0)$: Das Ergebnis ist 2.

Also ist 2 der größte gemeinsame Teiler von 14 und 34.

Indem wir rückwärts durch die Berechnungen durchgehen und jeweils geeignet auflösen, erhalten wir die folgende Darstellung des größten gemeinsamen Teilers durch die Ausgangszahlen:

$$\begin{aligned} 2 &= 14 - 2 \cdot 6 \\ &= 14 - 2 \cdot (34 - 2 \cdot 14) \\ &= 5 \cdot 14 - 2 \cdot 34. \end{aligned}$$

A.7 Konstruierbarkeit mit Zirkel und Lineal

Eine klassische Frage in der Geometrie ist es, welche geometrischen Objekte bzw. welche Punkte in der Ebene sich mit Zirkel und Lineal konstruieren lassen. Indem wir das Lineal durch reelle Geraden in $\mathbb{C}$ und den Zirkel durch Kreise in $\mathbb{C}$ modellieren, erhalten wir den folgenden Konstruierbarkeitsbegriff:

Definition A.7.1 (Konstruierbarkeit mit Zirkel und Lineal)**.** Sei $M \subset \mathbb{C}$, wobei wir die euklidische Metrik auf $\mathbb{C}$ (bzw. $\mathbb{R}^2$) betrachten. Dann schreiben wir

$$\mathrm{ZL}(M) := \mathrm{ZL}_1(M) \cup \mathrm{ZL}_2(M) \cup \mathrm{ZL}_3(M),$$

wobei die elementaren Konstruktionsschritte ZL_1, ZL_2, ZL_3 wie folgt definiert sind: Sei $G(M)$ die Menge aller reellen Geraden in $\mathbb{C}$, die zwei verschiedene Punkte aus M enthalten; sei $C(M)$ die Menge aller Kreise in $\mathbb{C}$, deren Mittelpunkt in M liegt und deren Radius gleich dem Abstand zweier Punkte aus M ist. Wir schreiben (Abbildung A.3)

- $\mathrm{ZL}_1(M)$ für die Menge aller Schnittpunkte zweier verschiedener Geraden aus $G(M)$,
- $\mathrm{ZL}_2(M)$ für die Menge aller Schnittpunkte von Geraden aus $G(M)$ mit Kreisen aus $C(M)$,
- $\mathrm{ZL}_3(M)$ für die Menge aller Schnittpunkte zweier verschiedener Kreise aus $C(M)$.

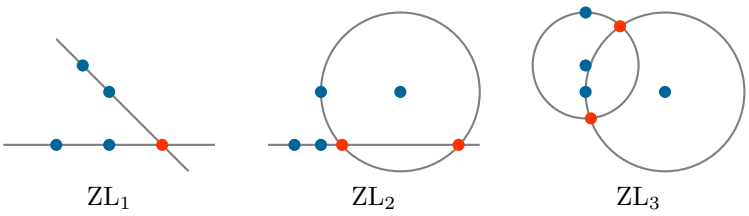


Abbildung A.3.: Die elementaren Konstruktionsschritte mit Zirkel und Lineal: bereits konstruierte Punkte (blau), Hilfsgeraden/-kreise (grau), neue Punkte (rot)

Zu $n \in \mathbb{N}$ definieren wir $\mathrm{ZL}^n(M)$ rekursiv durch

$$\begin{aligned} \mathrm{ZL}^0(M) &:= M \\ \mathrm{ZL}^{n+1}(M) &:= \mathrm{ZL}\big(\mathrm{ZL}^n(M)\big) \quad \text{für alle } n \in \mathbb{N}. \end{aligned}$$

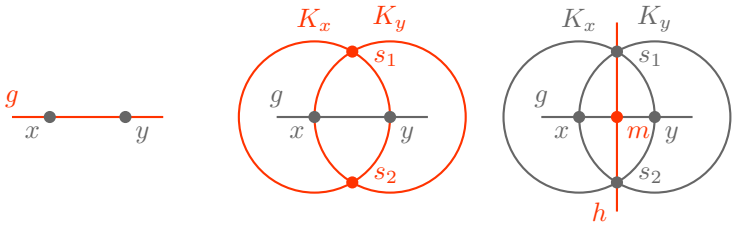


Abbildung A.4.: Konstruktion des Mittelpunktes von x und y

Ein Punkt $x \in \mathbb{C}$ ist *aus M mit Zirkel und Lineal konstruierbar*, wenn es ein $n \in \mathbb{N}$ mit $x \in \mathrm{ZL}^n(M)$ gibt.

Mit $\mathrm{ZL} := \bigcup_{n\in\mathbb{N}} \mathrm{ZL}^n(\{0,1\})$ bezeichnen wir die Menge aller aus $\{0,1\} \subset \mathbb{C}$ mit Zirkel und Lineal konstruierbaren Punkte in $\mathbb{C}$. Wir sagen, dass $\varphi \in \mathbb{R}$ ein *konstruierbarer Winkel* ist, wenn φ als Winkel zwischen zwei Geraden in $G(\mathrm{ZL})$ auftritt.

Der Vollständigkeit halber geben wir ein Beispiel für die Lösung eines Konstruktionsproblems mit Zirkel und Lineal in der ebenen Geometrie [19, Kapitel 2.4].

Beispiel A.7.2 (Konstruktion des Mittelpunkts einer Strecke)**.**

Konstruktionsproblem. Gegeben seien zwei Punkte $x, y \in \mathbb{C}$ mit $x \neq y$. Gesucht ist eine Konstruktion des Mittelpunkts $m := 1/2 \cdot (x + y) \in \mathbb{C}$ von x und y.

Konstruktion. (s. Abbildung A.4)

1. Wir zeichnen die Gerade g durch x und y.
2. Wir zeichnen den Kreis K_x um x mit Radius $r := |y - x|$ und den Kreis K_y um y mit Radius r.
3. Wir bezeichnen die beiden Schnittpunkte von K_x und K_y mit s_1 und s_2.
4. Wir zeichnen die Gerade h durch s_1 und s_2.
5. Der Schnittpunkt von g und h ist dann der gesuchte Punkt m.

Beweis der Korrektheit der Konstruktion. Wir zeigen Schritt für Schritt, dass die Konstruktionsschritte durchgeführt werden können und dass die Konstruktion das gewünschte leistet:

1. Da $x \neq y$ ist, gibt es genau eine reelle Gerade g in $\mathbb{C}$, die x und y enthält.

2. Wegen $x \neq y$ ist $r := |x - y| > 0$. Insbesondere gibt es somit (eindeutige) Kreise K_x und K_y um x bzw. y vom Radius r.

3. Es gilt $\#(K_x \cap K_y) = 2$, denn: Nachrechnen (durch Auflösen der entsprechenden quadratischen Gleichungen) zeigt: Wegen

$$r - r < |x - y| < r + r$$

haben K_x und K_y genau zwei Schnittpunkte. Andererseits zeigt Einsetzen, dass die Punkte

$$s_1 := m + \frac{\sqrt{3}}{2} \cdot A \cdot (y - x)$$
$$s_2 := m - \frac{\sqrt{3}}{2} \cdot A \cdot (y - x)$$

mit

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

in $K_x \cap K_y$ liegen.

4. Nach dem letzten Schritt ist $s_1 \neq s_2$. Es gibt also genau eine reelle Gerade h in $\mathbb{C}$, die s_1 und s_2 enthält.

5. Die Geraden g und h haben genau einen Schnittpunkt, nämlich m, denn: Da s_1 und s_2 nicht auf g liegen, ist $g \neq h$. Also haben g und h höchstens einen Schnittpunkt und es genügt somit zu zeigen, dass m auf g und h liegt. Offensichtlich gilt $m \in g$. Außerdem ist auch $m \in h$, denn

$$m = \frac{1}{2} \cdot (s_1 + s_2).$$

Beispiel A.7.3. Es gilt $i \in \mathrm{ZL}$, denn: Aus 0 und 1 können wir den Kreis um 0 vom Radius 1 und die reelle Achse konstruieren. Der Punk -1 ist der zweite (neben 1) Schnittpunkt der reellen Achse mit diesem Kreis und ist somit konstruierbar. Die imaginäre Achse können wir dann als Mittelsenkrechte von 1 und -1 konstruieren. Die imaginäre Achse schneidet den Einheitskreis in genau zwei Punkten, nämlich i und $-i$. Aus der Orientierung der komplexen Ebene ergibt sich, welcher der beiden Punkte i ist. Insbesondere ist daher i konstruierbar und auch der Winkel $\pi/2$.

Satz A.7.4 (der Körper der konstruierbaren Punkte)**.**

1. *Die Menge* $\mathrm{ZL} \subset \mathbb{C}$ *ist ein Körper bezüglich der arthmetischen Operationen auf* $\mathbb{C}$*. Dabei gilt* $\mathbb{Q} \subset \mathrm{ZL}$*.*

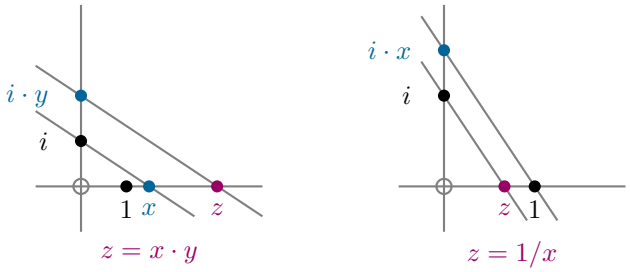


Abbildung A.5.: Produkte und Quotienten, geometrisch

2. *Der Körper* ZL *ist im folgenden Sinne unter Quadratwurzeln abgeschlossen: Ist* $z \in \mathrm{ZL}$*, so liegen alle Elemente* $\alpha \in \mathbb{C}$ *mit* $\alpha^2 = z$ *auch in* ZL*.*

Beweis. Ist $z \in \mathbb{C}$, so sind äquivalent (nachrechnen):

1. Es gilt $z \in \mathrm{ZL}$.
2. Es gilt $\operatorname{Re} z \in \mathrm{ZL}$ und $\operatorname{Im} z \in \mathrm{ZL}$.
3. Es gilt $r \in \mathrm{ZL}$ und φ ist ein konstruierbarer Winkel, wobei $z = e^{i \cdot \varphi} \cdot r$ mit $r \in \mathbb{R}_{\geq 0}$ und $\varphi \in [0, 2 \cdot \pi)$ die Polardarstellung von z ist.

Somit genügt es, die folgenden Aussagen zu zeigen (aus ① und ③ ergibt sich $\mathbb{Q} \subset \mathrm{ZL}$; aus ①, ②, ③ ergibt sich, dass ZL ein Körper ist; aus ④, ⑤ ergibt sich, dass ZL unter Quadratwurzeln abgeschlossen ist):

① Sind $x, y \in \mathbb{R} \cap \mathrm{ZL}$, so gilt auch $x + y \in \mathrm{ZL}$ und $x - y \in \mathrm{ZL}$.

② Sind φ, $\psi \in \mathbb{R}$ konstruierbare Winkel, so sind auch $\varphi + \psi$ und $\varphi - \psi$ konstruierbare Winkel.

③ Sind $x, y \in \mathbb{R} \cap \mathrm{ZL} \setminus \{0\}$, so gilt auch $x \cdot y \in \mathrm{ZL}$ und $1/x \in \mathrm{ZL}$.

④ Ist $\varphi \in \mathbb{R}$ ein konstruierbarer Winkel, so ist auch $\varphi/2$ ein konstruierbarer Winkel.

⑤ Ist $x \in \mathbb{R}_{>0} \cap \mathrm{ZL}$, so ist auch $\sqrt{x} \in \mathrm{ZL}$.

Bis auf die Aussagen ③ und ⑤ sind dies elementare Konstruktionen (nachrechnen; Mittelstufe!).

Zu ③. Wir verwenden $i \in \mathrm{ZL}$ (Beispiel A.7.3) und zeigen die Behauptung mithilfe des Strahlensatzes (Abbildung A.5):

Konstruktion von $x \cdot y$: Wir konstruieren die Gerade durch x und i sowie die dazu parallele Gerade durch $i \cdot y$ (konstruierbar!). Sei z der Schnittpunkt

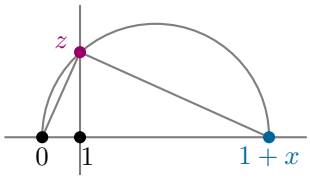


Abbildung A.6.: Reelle Quadratwurzeln, geometrisch

der reellen Achse (konstruierbar!) mit dieser Geraden. Nach dem Strahlensatz gilt dann

$$z = x \cdot \frac{z}{x} = x \cdot \frac{y}{1} = x \cdot y.$$

Konstruktion von $1/x$: Wir konstruieren die Gerade durch $i \cdot x$ und 1 sowie die dazu parallele Gerade durch i (konstruierbar!). Sei z der Schnittpunkt der reellen Achse (konstruierbar!) mit dieser Geraden. Nach dem Strahlensatz gilt dann

$$z = \frac{z}{1} = \frac{1}{x}.$$

Zu ⑤. Wir zeigen dies mithilfe des Höhensatzes (Abbildung A.6): Wir konstruieren auf der reellen Achse den Punkt $1+x$ sowie einen (Halb-)Kreis über der Strecke von 0 nach $1 + x$ (indem man zuerst den Mittelpunkt von 0 und $1 + x$ konstruiert). Man konstruiert dann die zur reellen Achse orthogonale Gerade durch 1 (konstruierbar!).

Sei z der Schnittpunkt dieser Geraden mit dem zuvor konstruierten Halbkreis. Nach dem Satz von Thales sind dann 0, z und $1 + x$ die Ecken eines rechtwinkligen Dreiecks und nach dem Höhensatz ist

$$1 \cdot x = |z - 1|^2.$$

Somit ist auch die Wurzel $|z - 1|$ aus x konstruierbar. □

Beispiel A.7.5 (Konstruierbarkeitsprobleme)**.** Klassische Konstruierbarkeitsprobleme übersetzen sich daher wie folgt in Fragen über den Körper ZL:

- Quadratur des Kreises (Aufgabe 1):
  Ist $\sqrt{\pi}$ in ZL ?
- Würfelverdopplung (Aufgabe 2):
  Ist $\sqrt[3]{2}$ in ZL ?
- Konstruierbarkeit regulärer Polygone (Aufgabe 3):
  Für welche $n \in \mathbb{N}_{\geq 3}$ ist $e^{2\pi i/n}$ in ZL ?
- Winkeldreiteilung:
  Ist für alle $\varphi \in [0, 1]$ mit $e^{i\cdot\varphi} \in$ ZL auch $e^{i\cdot\varphi/3}$ in ZL ?

A.8 Anwendungen endlicher Körper

Beispiel A.8.1 (ein Körper mit 256 Elementen)**.** Sei F ein endlicher Körper der Charakteristik p. Wir wissen bereits, dass die Einheitengruppe $F^\times$ zyklisch ist (Korollar 3.1.10). Sei $\alpha \in F^\times$ ein Erzeuger dieser Einheitengruppe und sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über dem Primkörper $K \cong_{\mathsf{Ring}} \mathbb{F}_p$ von F. Dann ist

$$\begin{aligned} K[T]/(\mu_\alpha) &\longrightarrow F \\ K \ni x &\longmapsto x \\ [T] &\longmapsto \alpha \end{aligned}$$

ein Körperisomorphismus. Da α ein Erzeuger von $F^\times$ ist, erhalten wir

$$\big(K[T]/(\mu_\alpha)\big)^\times = \big\{[T^j] \;\big|\; j \in \{0, \dots, |F| - 1\}\big\}.$$

Wir geben ein konkretes Beispiel für diese Situation in $\mathbb{F}_{256}$: Sei

$$f := T^8 + T^4 + T^3 + T^2 + 1 \in \mathbb{F}_2[T].$$

Man kann zeigen, dass f in $\mathbb{F}_2[T]$ irreduzibel ist (es gibt nur endliche viele Polynome in $\mathbb{F}_2[T]$ mit Grad kleiner 8 und man kann für jedes dieser Polynome per Polynomdivision nachrechnen, dass es kein Teiler von f ist). Also ist $F := \mathbb{F}_2[T]/(f)$ ein Körper mit $\#\mathbb{F}_2^{\deg f} = 2^8 = 256$ Elementen.

Das Element $[T] \in F$ ist ein Erzeuger von $F^\times$, denn: Da die Gruppe $F^\times$ genau 255 Elemente enthält, genügt es zu zeigen, dass $[T]$ die (multiplikative) Ordnung 255 hat. Nach dem Satz von Lagrange (Korollar 1.1.59) müssen wir wegen $255 = 3 \cdot 5 \cdot 17$ dafür nur nachweisen, dass $[T]$ *nicht* die Ordnung 1, 3, 5, 15, 17, 51 oder 85 besitzt. Dies kann man nachprüfen, indem man den Rest von T^j bei Division durch f für diese Werte von j bestimmt. Zum Beispiel ist

$$T^{15} = (T^7 + T^3 + T^2 + T) \cdot f + T^5 + T^2 + T,$$

und damit $[T^{15}] \neq [1]$ in F. Also ist in diesem Fall

$$F^\times = \big\{[1], [T], \dots, [T^{254}]\big\}.$$

Beispiel A.8.2 (LFSR)**.** Sei $f \in \mathbb{F}_2[T]$ das Polynom aus Beispiel A.8.1 und

$$F := \mathbb{F}_2[T]/(f).$$

Da $\big([1], \dots, [T^7]\big)$ eine $\mathbb{F}_2$-Basis von F ist (Beweis von Proposition 3.2.24), können wir Elemente aus F bezüglich dieser Basis darstellen; dies liefert einen

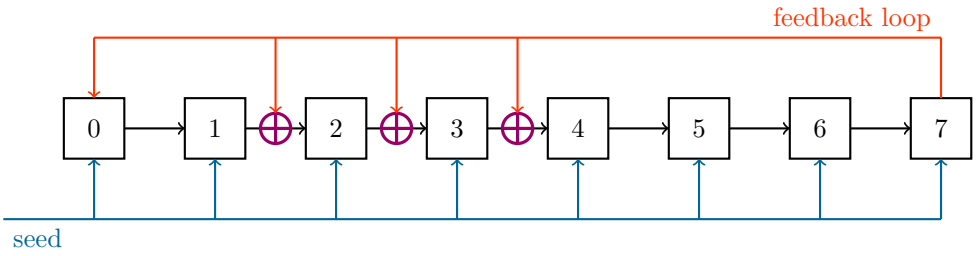


Abbildung A.7.: Das LFSR zum Polynom $T^8 + T^4 + T^3 + T^2 + 1 \in \mathbb{F}_2[T]$

$\mathbb{F}_2$-Vektorraumisomorphismus

$$F \longrightarrow {\mathbb{F}_2}^8.$$

Multiplikation mit $[T]$ in F liefert unter diesem Isomorphismus die Abbildung

$$\begin{aligned} R\colon {\mathbb{F}_2}^8 &\longrightarrow {\mathbb{F}_2}^8 \\ x &\longmapsto \begin{pmatrix} x_7 \\ x_0 \\ x_1 + x_7 \\ x_2 + x_7 \\ x_3 + x_7 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} \end{aligned}$$

(nachrechnen). Indem man Elemente von ${\mathbb{F}_2}^8$ als 8-bit-Wörter (d.h. bytes) interpretiert, kann man diese Abbildung effizient durch die Schaltung in Abbildung A.7, ein sogenanntes *linear feedback shift register (LFSR)*, berechnen:

Beginnt man nun mit einem 8-bit-Startwert $x \in {\mathbb{F}_2}^8 \setminus \{0\}$ (dem sogenannten *seed*), so kann man mit dem LFSR aus Abbildung A.7 sehr schnell 255 verschiedene Werte (nämlich $x, R(x), \ldots, R^{254}(x)$) berechnen, die „auf den ersten Blick recht durcheinander wirken“: Zum Beispiel erhalten wir, wenn wir das obige LFSR auf den seed $(1,1,1,0,1,1,0,1)^\mathsf{T}$ anwenden und die entstehenden Binärfolgen als Binärdarstellungen von Zahlen in $\{0,\ldots,255\}$ interpretieren, die Folge:

> 237, 206, 103, 139, 253, 198, 99, 137, 252, 126, 63, 167, 235, 205, 222, 111, 143, 255, 199, 219, 213, 210, 105, 140, 70, 35, 169, 236, 118, 59, 165, 234, 117, 130, 65, 152, 76, 38, 19, 177, 224, 112, 56, 28, 14, 7, 187, 229, 202, 101, 138, 69, 154, 77, 158, 79, 159, 247, 195, 217, 212, 106, 53, 162, 81, 144, 72, 36, 18, 9, 188, 94, 47, 175, 239, 207, 223, 215, 211, 209, 208, 104, 52, 26, 13, 190, 95, 151, 243, 193, 216, 108, 54, 27, 181,

226, 113, 128, 64, 32, 16, 8, 4, 2, 1, 184, 92, 46, 23, 179, 225, 200, 100, 50, 25, 180, 90, 45, 174, 87, 147, 241, 192, 96, 48, 24, 12, 6, 3, 185, 228, 114, 57, 164, 82, 41, 172, 86, 43, 173, 238, 119, 131, 249, 196, 98, 49, 160, 80, 40, 20, 10, 5, 186, 93, 150, 75, 157, 246, 123, 133, 250, 125, 134, 67, 153, 244, 122, 61, 166, 83, 145, 240, 120, 60, 30, 15, 191, 231, 203, 221, 214, 107, 141, 254, 127, 135, 251, 197, 218, 109, 142, 71, 155, 245, 194, 97, 136, 68, 34, 17, 176, 88, 44, 22, 11, 189, 230, 115, 129, 248, 124, 62, 31, 183, 227, 201, 220, 110, 55, 163, 233, 204, 102, 51, 161, 232, 116, 58, 29, 182, 91, 149, 242, 121, 132, 66, 33, 168, 84, 42, 21, 178, 89, 148, 74, 37, 170, 85, 146, 73, 156, 78, 39, 171

Mechanismen dieser Art werden zum Beispiel in Kombination mit anderen Bausteinen in Hardware-Komponenten bei der Erzeugung von (Pseudo-)-Zufallszahlen eingesetzt, da sie schnell, „durcheinander“, viele verschiedene Werte erzeugen können. Pseudozufallszahlen werden in vielen Anwendungen benötigt, zum Beispiel für probabilistische Primzahltests (Ausblick 2.2.32).

Beispiel A.8.3 (RAID(6))**.** Eine Anwendung von LFSRs (Beispiel A.8.2) ist bei der praktischen Umsetzung von RAID(6): Möchte man große Mengen von Daten speichern, so verteilt man diese Daten auf mehrere Speichermedien (z.B. Festplatten, SSDs, ...). Um sich gegen Datenverlust durch technische Probleme auf einer oder mehrerer Festplatten abzusichern (klassische Festplatten sind tatsächlich relativ anfällig für alle möglichen technischen Defekte), ist es dabei vernünftig, die Daten so zu speichern, dass selbst beim Ausfall einer oder mehrerer Festplatten, die Daten mithilfe der auf den anderen Festplatten noch vorhandenen Daten rekonstruiert werden können. Die RAID-Technologie (Redundant Array of Independent Disks) beschreibt Schemata dieser Art.

Für RAID(6) benötigt man $n \in \{4, \dots, 257\}$ Festplatten. Die Daten werden in Blöcke aufgeteilt. Zusätzlich zu je $n-2$ Blöcken $x_1, \dots, x_{n-2}$ von Daten werden zusätzlich zwei Kontrollblöcke $P(x)$ und $Q(x)$ abgespeichert. Dabei werden die Daten und Kontrollblöcke wie in Abbildung A.8 auf die n Festplatten verteilt.

Wir beschreiben nun die Paritätsfunktionen P und Q für RAID(6) für $n \in \{4, \dots, 257\}$ Festplatten: Der Einfachheit halber nehmen wir an, dass wir unsere Daten in byte-Blöcke aufgeteilt haben, d.h. in Elemente aus dem folgenden Körper F: Sei $f \in \mathbb{F}_2[T]$ das Polynom aus Beispiel A.8.1, sei

$$F := \mathbb{F}_2[T]/(f)$$

und sei $\alpha := [T] \in F$. Dann ist α ein Erzeuger von $F^\times$ (Beispiel A.8.1) und die Potenzen von α können effizient mithilfe eines LFSR berechnet werden (Beispiel A.8.2). Wir betrachten die Abbildungen

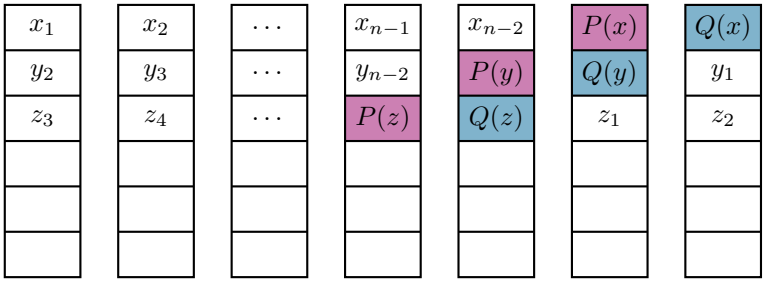


Abbildung A.8.: RAID(6), schematische Verteilung von Datenblöcken und Kontrollblöcken

$$\begin{aligned} P\colon F^{n-2} &\longrightarrow F \\ x &\longmapsto \sum_{j=1}^{n-2} x_j \end{aligned}$$

und

$$\begin{aligned} Q\colon F^{n-2} &\longrightarrow F \\ x &\longmapsto \sum_{j=0}^{n-2} x_{j+1} \cdot \alpha^j. \end{aligned}$$

Zusätzlich zu je $n-2$ Datenblöcken $x_1, \ldots, x_{n-2}$ werden dann jeweils die bytes $P((x_1, \ldots, x_{n-2})^\mathsf{T})$ und $Q((x_1, \ldots, x_{n-2})^\mathsf{T})$ abgespeichert.

Warum bietet dieses Verfahren Sicherheit gegen den Ausfall von zwei der n Festplatten? Sei $x \in F^{n-2}$. Wir müssen zeigen, dass wir x rekonstruieren können, wenn wir

$$\big(x_1, \ldots, x_{n-2}, P(x), Q(x)\big)$$

bis auf zwei Komponenten kennen.

Es können die folgenden Fälle eintreten:

- Wir kennen x, nicht aber $P(x)$ und $Q(x)$. In diesem Fall müssen wir x nicht rekonstruieren.

- Wir kennen $j \in \{1, \ldots, n-2\}$ und $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{n-2}$ und $P(x)$. Dann können wir x_j (und damit ganz x) durch

  $$x_j = P(x) - \sum_{k \in \{1,\ldots,n-2\} \setminus \{j\}} x_k$$

  rekonstruieren.

- Wir kennen $j \in \{1, \ldots, n-2\}$ und $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{n-2}$ und $Q(x)$. Dann können wir x_j (und damit auch x) durch

$$x_j = \frac{1}{\alpha^{j+1}} \cdot \left(Q(x) - \sum_{k \in \{1,\ldots,n-2\} \setminus \{j\}} x_{k-1} \cdot \alpha^k \right)$$

  rekonstruieren.

- Wir kennen $j, k \in \{1, \ldots, n-2\}$ mit $j < k$ und $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{k-1}, x_{k+1}, \ldots, x_{n-2}$ und $P(x)$ und $Q(x)$. Dann können wir x_j und x_k wie folgt rekonstruieren: Aus den bekannten Daten kennen wir die Summen

$$\begin{aligned} x_j + x_k & \qquad (\text{aus } P(x)) \\ \alpha^j \cdot x_j + \alpha^k \cdot x_k & \qquad (\text{aus } Q(x)) \end{aligned}$$

  Wegen

$$\det{}_F \begin{pmatrix} 1 & 1 \\ \alpha^j & \alpha^k \end{pmatrix} = \alpha^k - \alpha^j \neq 0$$

  (da die Potenzen $1, \alpha, \ldots, \alpha^{254}$ alle verschieden sind) besitzt dieses lineare Gleichungssystem (in den „Variablen“ x_j und x_k, über F) eindeutige Lösungen $x_j, x_k \in F$ (und diese können einfach berechnet werden). Also können wir x_j und x_k (und damit x) auf diese Weise rekonstruieren.

A.9 Funktoren

Die Übersetzung zwischen mathematischen Theorien (d.h. zwischen Kategorien) erfolgt durch sogenannte Funktoren. Grob gesagt handelt es sich dabei um „strukturerhaltende Abbildungen zwischen Kategorien“ (Abbildung A.9).

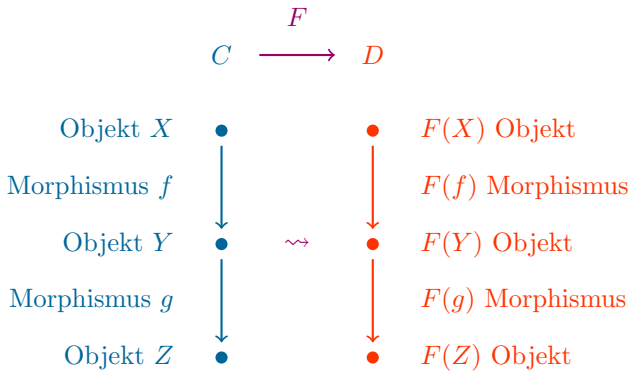


Abbildung A.9.: Funktor, schematisch

Definition A.9.1 (Funktor)**.** Seien C und D Kategorien. Ein *(kovarianter) Funktor* $F\colon C \longrightarrow D$ besteht aus folgenden Komponenten:

- Einer Abbildung $F\colon \mathrm{Ob}(C) \longrightarrow \mathrm{Ob}(D)$.
- Zu je zwei Objekten $X, Y \in \mathrm{Ob}(C)$ einer Abbildung

$$F\colon \mathrm{Mor}_C(X,Y) \longrightarrow \mathrm{Mor}_C\big(F(X), F(Y)\big).$$

Dabei müssen folgende Bedingungen erfüllt sein:

- Für alle $X \in \mathrm{Ob}(C)$ ist $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$.
- Für alle $X, Y, X \in \mathrm{Ob}(C)$ und alle $f \in \mathrm{Mor}_C(X,Y)$, $g \in \mathrm{Mor}_C(Y,Z)$ gilt
$$F(g \circ f) = F(g) \circ F(f).$$

Beispiel A.9.2 (Identitätsfunktor)**.** Sei C eine Kategorie. Dann ist der *Identitätsfunktor* $\mathrm{Id}_C\colon C \longrightarrow C$ wie folgt definiert:

- Auf Objekten betrachten wir die Abbildung

$$\begin{aligned} \mathrm{Ob}(C) &\longrightarrow \mathrm{Ob}(C) \\ X &\longmapsto X. \end{aligned}$$

- Auf Morphismen: Für alle $X, Y \in \mathrm{Ob}(C)$ betrachten wir

$$\begin{aligned} \mathrm{Mor}_C(X,Y) &\longrightarrow \mathrm{Mor}_C(X,Y) \\ f &\longmapsto f. \end{aligned}$$

Beispiel A.9.3 (Vergissfunktor)**.** Der Vergissfunktor $\mathsf{Top} \longrightarrow \mathsf{Set}$ ist wie folgt definiert:

- Auf Objekten betrachten wir die Abbildung $\mathrm{Ob}(\mathsf{Top}) \longrightarrow \mathrm{Ob}(\mathsf{Set})$, die einem topologischen Raum die unterliegende Menge zuordnet.
- Auf Morphismen: Für alle topologischen Räume X, Y betrachten wir

$$\begin{aligned} \mathrm{Mor}_{\mathsf{Top}}(X,Y) = \mathrm{map}(X,Y) &\longrightarrow \mathrm{Mor}_{\mathsf{Set}}(X,Y) \\ f &\longmapsto f. \end{aligned}$$

Analog erhält man Vergissfunktoren $\mathsf{Vect}_{\mathbb{R}} \longrightarrow \mathsf{Set}$, $\mathsf{Vect}_{\mathbb{R}} \longrightarrow \mathsf{Ab}$, ...

Beispiel A.9.4 (basierte Vektorräume)**.** Man kann die Mengenlehre über den folgenden Funktor $F\colon \mathsf{Set} \longrightarrow \mathsf{Vect}_{\mathbb{R}}$ in die lineare Algebra übersetzen:

- Auf Objekten definieren wir

$$\begin{aligned} F\colon \mathrm{Ob}(\mathsf{Set}) &\longrightarrow \mathrm{Ob}(\mathsf{Vect}_{\mathbb{R}}) \\ X &\longmapsto \bigoplus_X \mathbb{R}. \end{aligned}$$

  (Wir betrachten dabei eine Menge X in kanonischer Weise als Teilmenge, bzw. sogar Basis, von $\bigoplus_X \mathbb{R}$.)

- Auf Morphismen definieren wir F wie folgt: Sind X, Y Mengen und ist $f\colon X \longrightarrow Y$ eine Abbildung, so definieren wir $F(f)\colon \bigoplus_X \mathbb{R} \longrightarrow \bigoplus_Y \mathbb{R}$ als die eindeutig bestimmte $\mathbb{R}$-lineare Abbildung, die f von der Basis X auf ganz $\bigoplus_X \mathbb{R}$ fortsetzt.

Dies liefert tatsächlich einen Funktor. Analog erhält man auch einen freien Erzeugungsfunktor $\mathsf{Set} \longrightarrow \mathsf{Ab}$.

Beispiel A.9.5 (Tensorprodukte)**.** Sei K ein Körper und sei V ein K-Vektorraum. Dann ist $V \otimes_K \cdot : \mathsf{Vect}_K \longrightarrow \mathsf{Vect}_K$ ein Funktor (Satz II.4.2.9):

- Auf Objekten:

$$\begin{aligned} \mathrm{Ob}(\mathsf{Vect}_K) &\longrightarrow \mathrm{Ob}(\mathsf{Vect}_K) \\ W &\longmapsto V \otimes_K W. \end{aligned}$$

- Auf Morphismen: Für alle $\mathbb{R}$-Vektorräume V, W betrachten wir

$$\begin{aligned} \mathrm{Hom}_K(W, W') &\longrightarrow \mathrm{Hom}_K(V \otimes_K W, V \otimes_K W') \\ f &\longmapsto \mathrm{id}_V \otimes_K f. \end{aligned}$$

Beispiel A.9.6 (Tensorprodukte und Basiswechsel)**.** Sei K ein Körper und sei A eine kommutative K-Algebra. Dann ist $A \otimes_K \ \cdot : \mathsf{Vect}_K \longrightarrow \mathsf{Mod}_A$ ein Funktor (Beispiel II.4.2.13).

Eine wesentliche Eigenschaft von Funktoren ist, dass sie – da sie mit Verknüpfungen und Identitätsmorphismen verträglich sind – Isomorphie erhalten und somit ein geeignetes Konzept für Invarianten liefern:

Proposition A.9.7 (Funktoren erhalten Isomorphie)**.** *Seien C, D Kategorien, sei $F\colon C \longrightarrow D$ ein Funktor und seien $X, Y \in \mathrm{Ob}(C)$.*

1. *Ist $f \in \mathrm{Mor}_C(X, Y)$ ein Isomorphismus in C, so ist der übersetzte Morphismus $F(f) \in \mathrm{Mor}_D(F(X), F(Y))$ ein Isomorphismus in D.*
2. *Insbesondere: Ist $X \cong_C Y$, so folgt $F(X) \cong_D F(Y)$. Bzw.: Ist $F(X) \ncong_D F(Y)$, so ist $X \ncong_C Y$.*

Beweis. Der erste Teil folgt direkt aus den definierenden Eigenschaften von Funktoren: Sei $g \in \mathrm{Mor}_C(Y, X)$ invers zu f. Dann gilt

$$\begin{aligned} F(g) \circ F(f) &= F(g \circ f) = F(\mathrm{id}_X) \\ &= \mathrm{id}_{F(X)} \end{aligned}$$

und analog $F(f) \circ F(g) = \mathrm{id}_{F(Y)}$.

Der zweite Teil ist eine unmittelbare Folgerung aus dem ersten Teil. □

Geeignete Funktoren können also helfen zu zeigen, dass gewisse Objekte *nicht* isomorph sind.

Caveat A.9.8. Die Umkehrung gilt im allgemeinen *nicht*! D.h. Objekte, die unter einem Funktor auf isomorphe Objekte abgebildet werden, sind im allgemeinen *nicht* isomorph.

B
Übungsblätter

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 1 vom 17. Oktober 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Lineare Algebra)**.** Welche Beispiele von Gruppen kennen Sie aus der Linearen Algebra? Wozu wurden sie verwendet?

Fingerübung B (Wiederholung: Aufschreiben)**.** Wie schreibt man Voraussetzungen, Behauptungen, Beweise, Beispiele, Berechnungen, Lösungen von Gleichungen sauber auf? Wo verwendet man Konjunktiv, wo Indikativ?

Fingerübung C (Quadrate)**.** Sei $(G, \cdot, e)$ eine Gruppe. Welche der folgenden Aussagen sind in dieser Situation immer wahr?

1. Ist $g \in G$ mit $g \cdot g = g$, so folgt $g = e$.
2. Ist $g \in G$ mit $g \cdot g = e$, so folgt $g = e$.

Fingerübung D (Linksnebenklassen)**.** Sei $(G, \cdot, e)$ eine Gruppe und sei $H \subset G$ eine Untergruppe.

1. Wiederholen Sie den Begriff *Äquivalenzrelation*.
2. Zeigen Sie, dass folgendes eine Äquivalenzrelation auf G definiert:
$$\sim_H := \left\{(g, g') \in G \times G \;\middle|\; g^{-1} \cdot g' \in H\right\}$$
3. Zeigen Sie: Für alle $g \in G$ ist $g \cdot H = \{g' \in G \mid g \sim_H g'\}$.
4. Was ist die entsprechende Situation bei Vektorräumen?

Hinweis. Achten Sie beim Aufschreiben auf eine sprachlich präzise und übersichtliche Darstellung!

Aufgabe 1 (Verknüpfungstabellen; 4 (=2+2) Punkte)**.**

1. Sei $(G, \cdot, e)$ eine Gruppe. Zeigen Sie: Für jedes $g \in G$ ist die folgende Abbildung bijektiv:
$$\begin{aligned} G &\longrightarrow G \\ h &\longmapsto g \cdot h \end{aligned}$$
2. Folgern Sie: Die untenstehende Verknüpfungstabelle definiert *keine* Gruppenstruktur auf $\{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$:

	♣	♠	♡	♢
♣	♣	♠	♡	♢
♠	♠	♣	♢	♡
♡	♡	♡	♣	♠
♢	♢	♡	♠	♣

Bitte wenden

Aufgabe 2 (Monoide und Gruppen; 4 (=2+2) Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Die Menge $\{n^2 \mid n \in \mathbb{N}\}$ bildet bezüglich der gewöhnlichen Multiplikation und 1^2 einen Monoid.

2. Die Menge $\{1/n \mid n \in \mathbb{N}_{>0}\}$ bildet bezüglich der gewöhnlichen Multiplikation und $1/1$ eine Gruppe.

Aufgabe 3 (aabbeellsscchh; 4 Punkte)**.** Sei $(G, \cdot, e)$ eine Gruppe mit

$$\forall_{g \in G} \quad g \cdot g = e.$$

Zeigen Sie, dass die Gruppe $(G, \cdot, e)$ abelsch ist.
Hinweis. Wenn Sie es geschickt anstellen, lässt sich das sehr schön in einer einzelnen Zeile (normaler Länge ...) beweisen!

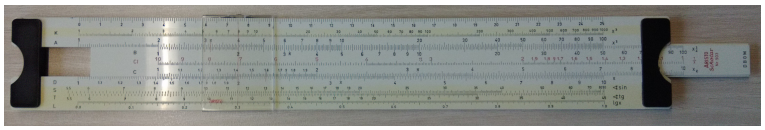
Aufgabe 4 (Konjugation; 4 (=2+2) Punkte)**.** Sei $(G, \cdot, e)$ eine Gruppe.

1. Zeigen Sie: Ist $g \in G$, so ist die folgende Abbildung ein Automorphimus von G:

$$\begin{aligned} c_g \colon G &\longrightarrow G \\ h &\longmapsto g \cdot h \cdot g^{-1}. \end{aligned}$$

2. Folgern Sie: Ist $\mathrm{Aut}(G) = \{\mathrm{id}_G\}$, so ist G abelsch.

Bonusaufgabe (Rechenschieber; 4 Punkte)**.** Wie funktionieren Rechenschieber? Was hat das mit dem Gruppenisomorphismus $\exp \colon (\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}_{>0}, \cdot, 1)$ zu tun?



Hinweis. Die Bonusaufgaben sind ein freiwilliges Zusatzangebot, sind oft manchmal komplexer oder aufwendiger bzw. basieren auf Material oder Fähigkeiten, die über die Vorlesung und die Übungen hinausgehen. Diese Aufgaben werden nicht in den Übungsgruppen besprochen. Sie dienen einfach nur als zusätzliche Anregung und Herausforderung. Man kann sich also gerne die Zähne daran ausbeißen oder sie fröhlich ignorieren.

Abgabe bis 24. Oktober 2025, 8:15, via Briefkasten/GRIPS

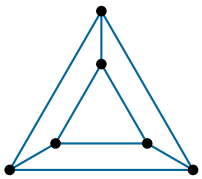
Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann Blatt 2 vom 24. Oktober 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: universelle Eigenschaften)**.** Wiederholen Sie die Konstruktion und die universelle Eigenschaft von *Quotientenvektorräumen* aus der Linearen Algebra.

Fingerübung B (die symmetrische Gruppe S_3, anschaulich)**.** Beschriften Sie die Knoten des abgebildeten Graphen so mit den Elementen von S_3, dass Elemente $x, y \in S_3$ genau dann durch eine Kante miteinander verbunden sind, wenn es ein $\sigma \in \{(1\ 2), (1\ 2\ 3), (1\ 3\ 2)\}$ mit $x = y \cdot \sigma$ gibt.



Fingerübung C (Matrixgruppen)**.**

1. Sei $n \in \mathbb{N}$. Bildet die Menge der invertierbaren Matrizen in $\mathrm{GL}_n(\mathbb{C})$ in Jordan-Normalform einen Normalteiler in $\mathrm{GL}_n(\mathbb{C})$?
2. Sei K ein Körper und $n \in \mathbb{N}$. Wie kann man aus dem Gauß-Algorithmus ein Erzeugendensystem für $\mathrm{GL}_n(K)$ extrahieren?

Fingerübung D (Gruppen für Neandertaler)**.** Erklären Sie

- den Begriff der *Gruppe*,
- den Begriff des *Normalteilers*,
- die *universelle Eigenschaft von Quotientengruppen*,

indem sie nur einsilbige Wörter verwenden!

Aufgabe 1 (Ordnung in der symmetrischen Gruppe S_3; 4 (=2+2) Punkte)**.** Wir betrachten die Permutationen $\sigma := (3\ 2\ 1)$ und $\tau := (2\ 3)$ in S_3.

1. Schreiben Sie $(1\ 3)$ als ein Produkt in S_3, das nur σ und τ als Faktoren enthält (jeweils möglicherweise mehrfach).
2. Zeigen Sie mit dem Satz von Lagrange, dass $\{\sigma, \tau\}$ ein Erzeugendensystem von S_3 ist.

Bitte wenden

Aufgabe 2 ((Ur)Bilder von Normalteilern; 4 (=2+2) Punkte)**.** Seien G, H Gruppen und sei $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort!

1. Ist $N \subset G$ ein Normalteiler in G, so ist $f(N)$ ein Normalteiler in H.
2. Ist $N \subset H$ ein Normalteiler in H, so ist $f^{-1}(N)$ ein Normalteiler in G.

Aufgabe 3 (Untergruppen vom Index 2; 4 (=2+2) Punkte)**.**

1. Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe vom Index 2. Zeigen Sie, dass H bereits ein Normalteiler in G ist.
2. Äußerst nützliche (?!) Folgerung: Sei G eine endliche Gruppe mit $\#G = 4058$. Zeigen Sie, dass jede Untergruppe H von G mit $\#H \geq 42$ bereits ein Normalteiler von G ist.

Aufgabe 4 (Untergruppen von $\mathbb{Q}$ von endlichem Index; 4 (=2+2) Punkte)**.** Sei H eine Untergruppe der additiven Gruppe $\mathbb{Q}$ von endlichem Index. Zeigen Sie, dass $H = \mathbb{Q}$ gilt, indem Sie wie folgt vorgehen:

1. Verwenden Sie den Satz von Lagrange, um zu zeigen, dass es ein $n \in \mathbb{N}_{>0}$ mit folgender Eigenschaft gibt:

$$\forall_{x \in \mathbb{Q}} \quad n \cdot x \in H.$$

   Hinweis. Auf welche Gruppe wendet man welche Version des Satzes von Lagrange an?!

2. Folgern Sie daraus, dass $H = \mathbb{Q}$ ist.

Bonusaufgabe (unfrei! 4 (=2+2) Punkte)**.** Lesen Sie den Anhang über freie Gruppen im Skript.

1. Zeigen Sie, dass die Gruppe $\mathbb{Z}/2025$ *nicht* frei ist.
2. Zeigen Sie, dass die Gruppe $\mathbb{Z}^{2025}$ *nicht* frei ist.

Abgabe bis 31. Oktober 2025, 8:15, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 3 vom 31. Oktober 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Produkte, direkte Summen)**.** Wiederholen Sie die Konstruktion von *direkten Produkten* und *direkten Summen* von Vektorräumen bzw. Moduln in der linearen Algebra. Welche universellen Eigenschaften haben diese Konstruktionen?

Fingerübung B (Quotientengruppen)**.** Geben Sie ein Beispiel für eine Gruppe, die sowohl eine Quotientengruppe isomorph zu $\mathbb{Z}/2025$ als auch eine Quotientengruppe isomorph zu S_{2025} besitzt.

Fingerübung C (Gruppoku)**.** Vervollständigen Sie die untenstehende Tabelle so, dass sich eine Verknüpfungstabelle für eine Gruppe mit den acht (verschiedenen) Elementen x, a, b, c, X, A, B, C ergibt.

·	x	a	b	c	X	A	B	C
x	x							
a		X	c			x		
b		C	X					
c				X				
X					x			
A								
B								
C								

Ist diese Gruppe isomorph zu $\mathbb{Z}/8$, $\mathbb{Z}/2 \times \mathbb{Z}/4$, $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, D_4 ?

Fingerübung D (D_5)**.** Enthält D_5 einen Normalteiler N mit $\#N = 2$?

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Gleichungen in Gruppen; 2 (= 1 + 1) Punkte)**.** Sei $(G, \cdot, e)$ eine Gruppe. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort!

1. Für alle $g, h \in G$ gibt es ein $x \in G$ mit $x \cdot g \cdot x^{-1} = h$.
2. Für alle $g, h \in G$ gibt es ein $x \in G$ mit $g \cdot x \cdot h = h \cdot g$.

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (Diedergruppen; 4 (=0+2+2) Punkte)**.** Sei $n \in \mathbb{N}_{\geq 3}$.

0. Wiederholen Sie den Begriff der *Diedergruppe* D_n. Welche geometrische Relevanz hat sie?
1. Zeigen Sie, dass D_n zu einer Untergruppe von S_n isomorph ist.

   Hinweis. Verwenden Sie die geometrische Beschreibung von D_n.
2. Sei $\varphi\colon D_n \longrightarrow S_n$ der in der ersten Teilaufgabe konstruierte injektive Gruppenhomomorphismus. Ist die durch φ definierte Gruppenoperation von D_n auf $\{1, \dots, n\}$ frei? Ist sie transitiv? Begründen Sie jeweils Ihre Antwort!

Bitte wenden

Aufgabe 2 (Quotientengruppen; 4 (=2+2) Punkte)**.** Seien G und G' Gruppen und seien $N \subset G$, $N' \subset G'$ Normalteiler in G bzw. G'. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort!

1. Ist $N \cong_{\mathsf{Group}} N'$ und $G/N \cong_{\mathsf{Group}} G'/N'$, so folgt $G \cong_{\mathsf{Group}} G'$.
2. Ist $G \cong_{\mathsf{Group}} G'$ und $N \cong_{\mathsf{Group}} N'$, so folgt $G/N \cong_{\mathsf{Group}} G'/N'$.

Aufgabe 3 (semi-direkte Produkte; 4 (=0+1+2+1) Punkte)**.** Seien N, Q Gruppen und sei $\varphi\colon Q \longrightarrow \mathrm{Aut}(N)$ ein Gruppenhomomorphismus.

0. Wiederholen Sie die Konstruktion des *semi-direkten Produkts* $N \rtimes_\varphi Q$.
1. Zeigen Sie, dass (e, e) das neutrale Element von $N \rtimes_\varphi Q$ ist.
2. Zeigen Sie: Ist $(n, q) \in N \rtimes_\varphi Q$, so ist $(\varphi(q^{-1})(n^{-1}), q^{-1})$ das Inverse von (n, q) in $N \rtimes_\varphi Q$.
3. Geben Sie ein Beispiel, das zeigt, dass im allgemeinen (n^{-1}, q^{-1}) *nicht* das Inverse von (n, q) in $N \rtimes_\varphi Q$ ist.

Aufgabe 4 (spaltende Erweiterungen; 4 (=2+2) Punkte)**.**

1. Sei G eine Gruppe, sei $N \subset G$ ein Normalteiler und sei $Q := G/N$, mit kanonischer Projaktion $\pi\colon G \longrightarrow G/N = Q$. Es gebe einen Gruppenhomomorphismus $s\colon Q \longrightarrow G$ mit $\pi \circ s = \mathrm{id}_Q$. Zeigen Sie: Dann gibt es einen Gruppenhomomorphismus $\varphi\colon Q \longrightarrow \mathrm{Aut}(N)$ mit

$$G \cong_{\mathsf{Group}} N \rtimes_\varphi Q.$$

2. Folgern Sie: Ist K ein Körper und $n \in \mathbb{N}_{\geq 1}$, so gibt es einen Gruppenhomomorphismus $\varphi\colon K^\times \longrightarrow \mathrm{Aut}(\mathrm{SL}_n(K))$ mit

$$\mathrm{GL}_n(K) \cong_{\mathsf{Group}} \mathrm{SL}_n(K) \rtimes_\varphi K^\times.$$

Bonusaufgabe (Formalisierung von Gruppen; 4 (=2+2) Punkte)**.** Erweitern Sie die Lean 4-Datei

https://loeh.app.ur.de/teaching/algebra_ws2526/monoid.lean

um folgendes:

1. Ein theorem das formuliert, dass Inverse von invertierbaren Elementen in Monoiden eindeutig sind;
2. einen Beweis dieser Aussage.

Hinweis. Falls Sie Lean 4 nicht installieren möchten, können Sie im Browser https://live.lean-lang.org/ verwenden.

Es werden nur Abgaben korrigiert, die via GRIPS als Quellcode-Textdatei abgegeben werden, die vom Lean 4-Interpreter fehlerfrei akzeptiert werden und aussagekräftig dokumentiert sind.

Abgabe bis 7. November 2025, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 4 vom 7. November 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Basen)**.** Wiederholen Sie die *universelle Eigenschaft von Basen* aus der Linearen Algebra.

Fingerübung B (Konjugationsoperation)**.** Sei G eine Gruppe. Zeigen Sie, dass

$$\begin{aligned} \varrho\colon G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto c_g := (x \mapsto g \cdot x \cdot g^{-1}) \end{aligned}$$

eine Gruppenoperation von G auf G definiert und dass der Stabilisator von $x \in G$ der Zentralisator $Z_G(x)$ von $x \in G$ ist.

Fingerübung C (Konjugation von Matrizen)**.** Sei $n \in \mathbb{N}$. Wir betrachten die Konjugationsoperation

$$\begin{aligned} \mathrm{GL}_n(\mathbb{C}) \times \mathrm{M}_{n\times n}(\mathbb{C}) &\longrightarrow \mathrm{M}_{n\times n}(\mathbb{C}) \\ (S, A) &\longmapsto S \cdot A \cdot S^{-1} \end{aligned}$$

von $\mathrm{GL}_n(\mathbb{C})$ auf $\mathrm{M}_{n\times n}(\mathbb{C})$. Was sind die Bahnen dieser Operation?
Hinweis. Jordansche Normalform!

Fingerübung D (endliche abelsche Gruppen)**.** Bestimmen sie für jede der folgenden Zahlen $n \in \mathbb{N}$ die Klassifikation der abelschen Gruppen mit genau n Elementen:

$$2025, \quad 2026, \quad 2027, \quad 2028, \quad 2029, \quad 2030$$

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (symmetrische Gruppen; 2 (= 1 + 1) Punkte)**.** Sei $H := \langle (1\ 2), (3\ 4) \rangle_{S_4}$. Begründen Sie jeweils Ihre Antwort!

1. Ist H ein Normalteiler von S_4 ?
2. Welchen Index hat die Untegruppe H von S_4 ?

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (endliche abelsche Gruppen; 4 (=0+3+1) Punkte)**.** Seien $p, q \in \mathbb{N}$ Primzahlen mit $p \neq q$.

0. Wiederholen Sie den *Klassifikationssatz* für endliche abelsche Gruppen.
1. Bestimmen Sie ein Repräsentantensytem für die Isomorphieklassen abelscher Gruppen A mit $\#A = p^2 \cdot q^2$.
2. Folgern Sie, dass jede abelsche Gruppe mit $\#A = p^2 \cdot q^2$ ein zwei-elementiges Erzeugendensystem besitzt.

Bitte wenden

Aufgabe 2 (Bahnen und Stabilisatoren; 4 (=2+2) Punkte)**.** Sei X eine Menge, sei G eine Gruppe, es sei eine Gruppenoperation von G auf X gegeben und es seien $x, y \in X$. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Ist $G \cdot x = G \cdot y$, so folgt $G_x \cong G_y$.
2. Ist $G_x \cong G_y$, so folgt $G \cdot x = G \cdot y$.

Aufgabe 3 (symmetrische Gruppen in Matrixgruppen; 4 Punkte)**.** Sei $n \in \mathbb{N}$ und K ein Körper. Zeigen Sie, dass es ein $N \in \mathbb{N}$ gibt, so dass S_n zu einer Untergruppe von $\mathrm{GL}_N(K)$ isomorph ist.
Hinweis. Was ist eine günstige Wahl für N ? Wie erhält man mühelos lineare Abbildungen aus Abbildungen?

Aufgabe 4 (Triforce-Münzen; 4 Punkte)**.** Die Zentralbank von Hyrule beschließt, Münzen in Umlauf zu bringen. Die Münzen haben die Form eines gleichseitigen Dreiecks, unterteilt in vier kongruente gleichseitige Dreiecke (Abbildung (a)).

(a) (b) (c) (d)

Um verschiedene Sorten Münzen zu ermöglichen, können aus den vier Dreiecken noch Kreise oder seitenparallele Dreiecke ausgestanzt werden. Wieviele essentiell verschiedene solcher Münzen gibt es? Begründen Sie Ihre Antwort!
Hinweis. Die Münzen in Abbildung (b) und (c) sind essentiell verschieden, aber die Münzen in Abbildung (c) und (d) *nicht*. Modellieren und lösen Sie das Problem mithilfe einer geeigneten Gruppenoperation. Achten Sie auf eine übersichtliche und nachvollziehbare Darstellung der Lösung.

Bonusaufgabe (GAP; 4 (=1+1+1+1) Punkte)**.** Das System GAP und Dokumentation dazu finden Sie unter: https://www.gap-system.org/. Geben Sie bei den folgenden Aufgaben den GAP-Code und gegebenenfalls die Ausgabe von GAP an.

1. Verwenden Sie das Computeralgebrasystem GAP, um die Menge aller Konjugationsklassen von Elementen in S_8 zu bestimmen.
2. Verwenden Sie das Computeralgebrasystem GAP, um herauszufinden, wieviele Untergruppen die Gruppe S_8 besitzt.
3. Wie kann man mit GAP die Zykelzerlegung eines Elements in einer endlichen symmetrischen Gruppe bestimmen?
4. Wie kann man mit GAP herausfinden, ob eine Teilmenge einer endlichen symmetrischen Gruppe ein Erzeugendensystem dieser Gruppe ist?

Abgabe bis 14. November 2025, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 5 vom 14. November 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Quotienten)**.** Wiederholen Sie die *universelle Eigenschaft von Quotientengruppen*.

Fingerübung B (Permutationen)**.** Berechnen Sie folgende Permutationen in S_5 und geben Sie jeweils eine möglichst einfache Beschreibung des Ergebnisses:

1. $(1\ 2\ 3) \cdot (4\ 5) \cdot (3\ 2\ 1)$
2. $(1\ 2\ 3) \cdot (1\ 4) \cdot (3\ 2\ 1)$
3. $(1\ 3\ 2) \cdot (1\ 3\ 4) \cdot (1\ 2) \cdot (3\ 4)$
4. $(1\ 2) \cdot (2\ 3) \cdot (1\ 2) \cdot (2\ 3)$

Fingerübung C (Zykelzerlegungen)**.** Bestimmen Sie und skizzieren Sie die Zykelzerlegungen der folgenden Permutationen in S_6. Bestimmen Sie dann die Ordnungen dieser Elemente.

1. $1 \mapsto 3,\ 2 \mapsto 5,\ 3 \mapsto 4,\ 4 \mapsto 2,\ 5 \mapsto 1,\ 6 \mapsto 6$
2. $1 \mapsto 3,\ 2 \mapsto 5,\ 3 \mapsto 1,\ 4 \mapsto 2,\ 5 \mapsto 4,\ 6 \mapsto 6$
3. $1 \mapsto 3,\ 2 \mapsto 5,\ 3 \mapsto 1,\ 4 \mapsto 6,\ 5 \mapsto 2,\ 6 \mapsto 4$
4. $1 \mapsto 6,\ 2 \mapsto 5,\ 3 \mapsto 2,\ 4 \mapsto 1,\ 5 \mapsto 3,\ 6 \mapsto 4$

Fingerübung D (Normalreihen)**.** Sei A eine endliche abelsche Gruppe. Zeigen Sie, dass A eine Normalreihe mit zyklischen Faktoren besitzt.

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (semi-direkte Produkte; 2 $(= 0 + 1 + 1)$ Punkte)**.** Wir betrachten die Gruppe $D_\infty := \mathbb{Z} \rtimes_\varphi \mathbb{Z}/2$, wobei $\varphi\colon \mathbb{Z}/2 \longrightarrow \mathrm{Aut}(\mathbb{Z})$ durch $\varphi([1]) = -\mathrm{id}_\mathbb{Z}$ gegeben ist. Begründen Sie jeweils Ihre Antwort!

0. Wiederholen Sie die Definition des *semi-direkten Produkts*.
1. Welche Ordnung besitzt $(1, [1])$?
2. Geben Sie ein Beispiel für Elemente $g, h \in D_\infty$ mit $\operatorname{ord} g = 2 = \operatorname{ord} h$ und $\operatorname{ord}(g \cdot h) = \infty$ (!) an.

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (Diedergruppen; 4 (=0+3+1) Punkte)**.** Sei $n \in \mathbb{N}_{\geq 3}$.

0. Wiederholen Sie die Definition der *Diedergruppe* D_n.
1. Zeigen Sie, dass die Kommutatoruntergruppe $[D_n, D_n]$ zyklisch ist.
2. Wieviele Elemente enthält $D_n/[D_n, D_n]$? Begründen Sie Ihre Antwort!

Bitte wenden

Aufgabe 2 (Zykelsalat; 4 (=2+2) Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Die Menge $\{(5\ 1), (7\ 1\ 3\ 4\ 2\ 5\ 6)\}$ ist ein Erzeugendensystem von S_7.
2. Die Menge $\{(5\ 1\ 2), (7\ 1\ 3\ 4\ 2\ 5\ 6)\}$ ist ein Erzeugendensystem von S_7.

Hinweis. Verwenden Sie Ergebnisse und Werkzeuge aus der Vorlesung, um dies knapp und präzise zu lösen. Evtl. kann es helfen, sich zu überlegen, was passiert, wenn man Elemente umbenennt und wie sich das auf den symmetrischen Gruppen widerspiegelt.

Aufgabe 3 (14/15-Puzzle; 4 Punkte)**.** Beim 14/15-*Puzzle* sind fünfzehn numerierte Plättchen und eine „Lücke“ auf einem quadratischen Brett verteilt (siehe linke Abbildung). Zeigen Sie mithilfe von symmetrischen Gruppen und des Signums, dass es *nicht* möglich ist, durch Verschieben der Plättchen die Position in der rechten Abbildung zu erreichen.
Hinweis. Modellieren Sie nur die Aspekte, die für die Lösung dieses Problems nötig sind.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Aufgabe 4 (Zykelzerlegung; 4 (=2+2) Punkte)**.** Begründen Sie jeweils Ihre Antwort!

1. Gibt es einen injektiven Gruppenhomomorphismus $\mathbb{Z}/8 \longrightarrow S_7$?
2. Gibt es einen injektiven Gruppenhomomorphismus $\mathbb{Z}/10 \longrightarrow S_7$?

Hinweis. Die Gruppe S_7 enthält nicht nur Zykel ...

Bonusaufgabe (Durcheinander; 4 (=1+1+1+1) Punkte)**.** Wir betrachten jeweils ein gewöhnliches Kartenspiel mit 52 Karten.

1. Modellieren Sie das „Abheben“ eines Kartenstapels mithilfe von symmetrischen Gruppen.
2. Zeigen Sie, dass man durch iteriertes Abheben, einen Kartenstapel *nicht* beliebig durchmischen kann. Stellen Sie den Beweis so dar, dass er von einem Mittelstufenschüler verstanden werden könnte.
3. Modellieren Sie „4-strip shuffles“ eines Kartenstapels mithilfe von symmetrischen Gruppen.
4. Kann man durch Iterieren von Abheben und 4-strip shuffles einen Kartenstapel beliebig durchmischen? Begründen Sie Ihre Antwort!

Abgabe bis 21. November 2025, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 6 vom 21. November 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Gruppentheorie)**.** Geben Sie eine Zusammenfassung von Kapitel 1 (Gruppen).

Fingerübung B (Sylowgruppen)**.** Bestimmen Sie jeweils zu jedem Primteiler der Anzahl der Gruppenelemente eine Sylowgruppe in der angegebenen Gruppe.

1. $\mathbb{Z}/4$
2. $\mathbb{Z}/100$
3. $\mathbb{Z}/21 \times \mathbb{Z}/42$
4. $D_5 \times \mathbb{Z}/2$

Fingerübung C (Sylowzahlen)**.** Sei n jeweils eine der folgenden Zahlen. Gibt es dann eine Gruppe G mit $\#G = n$ mit genau fünf 2-Sylowgruppen?

$$5, \quad 8, \quad 10, \quad 30$$

Fingerübung D (Sylow-Zoo)**.** Lesen Sie Anhang A.4 und machen Sie sich mit den dort gegebenen Beispielen vertraut.

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Fixpunkte; 2 (=0+1+1) Punkte)**.** Sei X eine Menge, sei G eine Gruppe und es sei eine Gruppenoperation von G auf X gegeben. Ein Element $x \in X$ ist ein *Fixpunkt* dieser Operation, wenn $g \cdot x = x$ für alle $g \in G$ gilt.

0. Wiederholen Sie die *Bahnengleichung*.
1. Zeigen Sie: Ist $\#G = 77$ und $\#X = 20$, so besitzt diese Operation mindestens zwei Fixpunkte.
2. Zeigen Sie: Ist $\#G = 77$ und $\#X = 37$, so besitzt diese Operation mindestens einen Fixpunkt.

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (Sylowgruppen; 4 (=0+2+2) Punkte)**.** Begründen Sie jeweils Ihre Antwort!

0. Wiederholen Sie den Begriff der *Sylowgruppen*. Was sagen die *Sylowsätze* über die Anzahl der Sylowgruppen?
1. Wieviele 3-Sylowgruppen enthält S_4 ?
2. Wieviele 2-Sylowgruppen enthält S_4 ?

Bitte wenden

Aufgabe 2 (Sylowlogie; 4 (=2+2) Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Jede Gruppe G mit $\#G = 2026$ ist auflösbar..
2. Jede Gruppe G mit $\#G = 2040$ ist auflösbar..

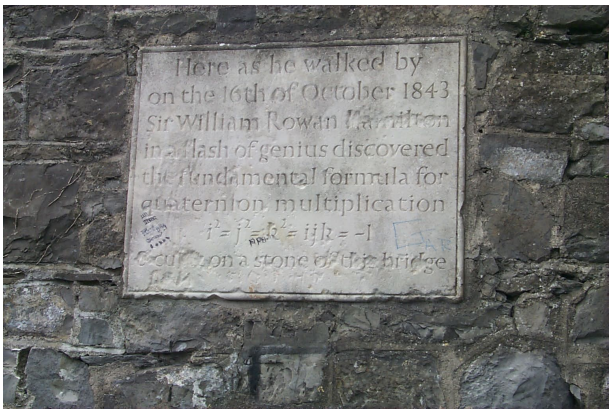
Aufgabe 3 (Primquadrate; 4 (=2+2) Punkte)**.**

1. Zeigen Sie: Ist G eine Gruppe, für die $G/Z(G)$ zyklisch ist, so ist G abelsch.
2. Folgern Sie: Ist G eine Gruppe und $p \in \mathbb{N}$ prim mit $\#G = p^2$, so ist G abelsch.

Aufgabe 4 (1001 Nacht und die Wilde 13; 4 Punkte)**.** Sei G eine Gruppe mit $\#G = 1001$. Zeigen Sie, dass es einen Gruppenhomomorphismus $G \longrightarrow \mathbb{Z}/13$ gibt, der surjektiv ist.
Hinweis. Sylow!

Bonusaufgabe (Quaternionen; 4 (=2+1+1) Punkte)**.**

1. Wie sind die Quaternionen definiert?
2. Welche algebraischen Eigenschaften besitzen die Quaternionen?
3. Was hat es mit dem Bild unten auf sich?



Hinweis. Belegen Sie alle Aussagen durch (seriöse, nachvollziehbare) Quellen.

Abgabe bis 28. November 2025, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 7 vom 28. November 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Polynomringe über Körpern)**.** Wiederholen Sie Eigenschaften von Polynomringen über Körpern, die in der Linearen Algebra behandelt wurden.

Fingerübung B (universelle Eigenschaft des Polynomrings)**.** Wiederholen und beweisen Sie die universelle Eigenschaft des Polynomrings.

Fingerübung C (Ideale)**.** Welche der folgenden Ideale in $\mathbb{Z}$ stimmen überein?

$$(1, 24), \quad (12, 4) \quad (12, 34), \quad (123, 4)$$

Fingerübung D (Restklassenringe)**.** Welche der folgenden Ringe sind isomorph?

$$\mathbb{Z}/(2) \times \mathbb{Z}/(2), \quad \mathbb{Z}/(4), \quad \mathbb{Z}/(5), \quad \mathbb{Z}/(2) \times \mathbb{Z}/(3), \quad \mathbb{Z}/(3) \times \mathbb{Z}/(2), \quad \mathbb{Z}/(6)$$

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Permutationen/Ordnung; 2 (=0+1+1) Punkte)**.** Begründen Sie jeweils Ihre Antwort!

0. Wiederholen Sie das *Signum* und die *Zykelzerlegung* von Permutationen.
1. Geben Sie ein Beispiel für eine Permutation in S_5 mit Ordnung 6.
2. Gegen Sie ein Beispiel für eine Permutation in A_7 mit Ordnung 6.

Hinweis. Beide Teilaufgaben besitzen sehr kurze Lösungen aus dem Wald!

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (vierte Potenzen; 4 (=0+1+3) Punkte)**.**

0. Wiederholen Sie die Konstruktion des Rings $\mathbb{Z}/(8)$.
1. Bestimmen Sie alle vierten und alle achten Potenzen in $\mathbb{Z}/(8)$.

   Hinweis. Man muss dafür fast nichts ausrechnen!
2. Folgern Sie, dass die Gleichung

   $$x^{2026} - 2 \cdot y^{84} - x^{124} \cdot y^{224} - 88 \cdot x \cdot y^{2025} \cdot z^{2026} = 123456789$$

   keine Lösung $x, y, z \in \mathbb{Z}$ besitzt.

   Hinweis. Seien Sie sparsam beim Rechnen!

Bitte wenden

Aufgabe 2 (Funktionenringe; 4 (=2+2) Punkte)**.** Sei $R := C([0,1], \mathbb{R})$ der Ring der stetigen Funktionen $[0,1] \longrightarrow \mathbb{R}$ bezüglich punktweiser Addition/Multiplikation, mit den konstanten Funktionen 0 bzw. 1 als neutralen Elementen. Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Die Menge $\{f \in R \mid f(0) = 0 = f(1)\}$ ist ein Ideal in R.
2. Die Abbildung $f \longmapsto \int_0^1 f(x)\, dx$ ist ein Ringhomomorphismus $R \longrightarrow \mathbb{R}$.

Aufgabe 3 (endliche Integritätsringe; 4 Punkte)**.** Zeigen Sie, dass jeder endliche Integritätsring ein Körper ist.
Hinweis. Ist X eine endliche Menge und ist $f\colon X \longrightarrow X$ injektiv, so ist f bereits bijektiv.

Aufgabe 4 (Charakterisierung von Körpern über Ideale; 4 Punkte)**.** Sei R ein Ring mit $R \ncong_{\mathsf{Ring}} \{0\}$. Zeigen Sie, dass folgende Aussagen äquivalent sind:

1. Der Ring R ist ein Körper.
2. Der Ring R enthält nur die Ideale $\{0\}$ und R.

Hinweis. Was ist mit Idealen, die nicht-invertierbare Elemente enthalten?

Bonusaufgabe (drittelbar; 4 (=2+2) Punkte)**.** Sei $f \in \mathbb{Z}[T]$.

1. Zeigen Sie: Für alle $m, n \in \mathbb{Z}$ ist $m - n$ ein Teiler von $f(m) - f(n)$.
2. Folgern Sie: Gibt es $k \in \mathbb{Z}$, so dass $f(k)$, $f(k+1)$ und $f(k+2)$ alle durch 3 teilbar sind, so folgt: Für jedes $n \in \mathbb{Z}$ ist $f(n)$ durch 3 teilbar.

Abgabe bis 5. Dezember 2025, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Lö-hö-hö/F. Ho-Ho-Hofmann Blatt 8 vom 5. Dezember 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: euklidischer Algorithmus)**.** Wiederholen Sie den *euklidischen Algorithmus* aus der Linearen Algebra.

Fingerübung B (ggT)**.** Bestimmen Sie in $\mathbb{F}_2[T]$ den größten gemeinsamen Teiler von $T^7+T^4+T^3+T+1$ und T^3+T+1.

Fingerübung C (Primideale, maximale Ideale)**.** Welche der folgenden Ideale sind prim? Welche maximal?

1. (4242) in $\mathbb{Z}$; (4242) in $\mathbb{Q}$
2. (T^2+2) in $\mathbb{Q}[T]$; (T^2+2) in $\mathbb{R}[T]$
3. $(2,T)$ in $\mathbb{Z}[T]$; $(2,T)$ in $\mathbb{Q}[T]$
4. (X,Y) in $\mathbb{Z}[X,Y]$; (X,Y) in $\mathbb{Q}[X,Y]$

Fingerübung D (Reste)**.** Bestimmen Sie mit dem chinesischen Restsatz alle ganzen Zahlen n mit

$$n \equiv 3 \mod 17 \quad \text{und} \quad n \equiv 13 \mod 71 \quad \text{und} \quad n \in \{1,\dots,1111\}.$$

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Sylow 85; 2 (=0+1+1) Punkte)**.** Begründen Sie jeweils Ihre Antwort!

0. Wiederholen Sie die *Sylowsätze*.
1. Wieviele 17-Sylowgruppe enthält eine Gruppe G mit $\#G = 85$?
2. Ist jede Gruppe G mit $\#G = 85$ auflösbar?

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (Adventskalender; 4 (=1+3) Punkte)**.** Über die Adventszeit auf dem Planeten Blorx ist folgendes bekannt:

- Fertigt man einen Adventskalender mit 93er-Reihen, so benötigt man zusätzlich eine Reihe mit 57 Türchen.
- Fertigt man einen Adventskalender mit 112er-Reihen, so benötigt man zusätzlich eine Reihe mit 98 Türchen.
- Die blorxische Adventszeit ist länger als ein Blorxmonat, aber kürzer als ein Blorxjahr.

Ein Blorxjahr hat bekannterweise 8888 Tage, ein Blorxmonat hat 888 Tage.

1. Modellieren Sie diese Situation durch geeignete Restklassenringe.
2. Wie lange dauert die blorxische Adventszeit? Begründen Sie Ihre Antwort!

Bitte wenden

Aufgabe 2 (komplexe Zahlen?!; 4 (=2+2) Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Es gilt $\mathbb{R}[T]/(T^2+1) \cong_{\text{Ring}} \mathbb{C}$.
2. Es gilt $\mathbb{R}[T]/(T^3+1) \cong_{\text{Ring}} \mathbb{C}$.

Aufgabe 3 (Ringe mit p bzw. $p \cdot q$ Elementen; 4 (=2+2) Punkte)**.**

1. Sei $p \in \mathbb{N}$ prim und sei R ein Ring mit $\#R = p$. Zeigen Sie, dass der Ring R zu $\mathbb{Z}/(p)$ isomorph ist.
2. Seien $p, q \in \mathbb{N}$ prim mit $p \neq q$ und sei R ein Ring mit $\#R = p \cdot q$. Zeigen Sie, dass der Ring R zu $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ isomorph ist.

Hinweis. Wie sieht die unterliegende additive Gruppe aus? Was liefert das Distributivgesetz? Welche Produkte von Elementen muss man also nur kennen? Was liefert das multiplikative neutrale Element?

Aufgabe 4 (gaußsche Primzahlen; 4 (=2+2) Punkte)**.** Wir betrachten die *Normabbildung*

$$\begin{aligned} N\colon \mathbb{Z}[i] &\longrightarrow \mathbb{N} \\ z &\longmapsto |z|^2 = z \cdot \overline{z} = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 \end{aligned}$$

auf den gaußschen ganzen Zahlen $\mathbb{Z}[i] \subset \mathbb{C}$. Bearbeiten Sie zwei der folgenden vier Aufgaben:

1. Bestimmen Sie mithilfe von N die Einheitengruppe von $\mathbb{Z}[i]$.
2. Zeigen Sie, dass $\mathbb{Z}[i]$ ein euklidischer Ring bezüglich der euklidischen Gradfunktion N ist.
3. Zeigen Sie: Ist $p \in \mathbb{Z}[i]$ ein Element, für das $N(p)$ prim in $\mathbb{Z}$ ist, so ist p bereits prim in $\mathbb{Z}[i]$.
4. Ist $10 - 29 \cdot i$ prim in $\mathbb{Z}[i]$? Begründen Sie Ihre Antwort!

Bo-Ho-Honusaufgabe (Nikolausaufgabe; 4 Punkte)**.**

Commander Blorx passiert den Nikolaus bei einem nur mittelmäßig riskanten Überholmanöver und grüßt ihn gut gelaunt mit „HO-HO-HO“.

Gar nicht amüsiert zetert der Nikolaus: „Nix HO-HO-HO! Erstens hast Du als Amateur ja gar keine Ahnung von der Materie und sicher nur zufällig HO-HO-HO gesagt, statt zum Beispiel HO-HO-HO-HO-HO-HO-HO-HO-HO-HO-HO-HO. Wie der Profi weiß, sind nämlich nur Primpotenzen zulässig.

Zweitens tun immer alle so, als ob es beliebig viele HO gäbe. Stimmt aber nicht. Im diesjährigen Budget sind nur noch 2025^{2025} HO verfügbar!

Drittens ist nur der der wahre Nikolaus, der das letzte HO verbraucht.“

Diese klare Ansage motiviert Commander Blorx selbstverständlich zu völlig sinnlosen Höchstleistungen. Wie kann Blorx dafür sorgen, dass er der wahre Nikolaus ist, wenn er und der (bald ehemalige) Nikolaus jeweils abwechselnd nach den obigen Regeln mit HO kommunizieren und Blorx beginnt? Begründen Sie Ihre Antwort!

Bild: Aura Lö-hö-hö

Abgabe bis 12. Dezember 2025, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 9 vom 12. Dezember 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Primfaktorzerlegungen)**.** Wiederholen Sie die *Eindeutigkeit von Primfaktorzerlegungen* und geben Sie einen Beweis.

Fingerübung B (letzte Ziffern)**.** Bestimmen Sie die letzte Ziffer von

1. 43^{42} im Zehnersystem;
2. 43^{42} im Zwölfersystem.

Fingerübung C (Baby-RSA)**.** Bestimmen Sie sinnvolle private und öffentliche Schlüssel für das RSA-Verfahren, wenn man mit den Primzahlen 11 und 17 beginnt.

Fingerübung D (Primbewertungen)**.** Berechnen Sie jeweils die folgenden Bewertungen zu den angegebenen Primelementen in den angegebenen Ringen:

1. $\nu_3(\frac{42}{99})$ in $Q(\mathbb{Z})$ für $3 \in \mathbb{Z}$
2. $\nu_3(\frac{99}{42})$ in $Q(\mathbb{Z})$ für $3 \in \mathbb{Z}$
3. $\nu_3(3 \cdot T^3 + \frac{1}{3} \cdot T^2 - 7 \cdot T + 99)$ in $Q(\mathbb{Z})[T]$ für $3 \in \mathbb{Z}$
4. $\nu_T(3 \cdot T^3 + \frac{1}{3} \cdot T^2 - 7 \cdot T + 99)$ in $\mathbb{Q}[T]$ für $T \in \mathbb{Q}[T]$

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Restklassenringe; 2 (=0+1+1) Punkte)**.** Begründen Sie jeweils Ihre Antwort!

0. Wiederholen Sie die Konstruktion von *Restklassenringen*.
1. Bestimmen Sie alle Ideale des Rings $\mathbb{Z}/(42)$.
2. Bestimmen Sie alle Ideale des Rings $\mathbb{Z}/(3) \times \mathbb{Z}/(14)$.

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 ((vor)letzte Ziffern; 4 (=1+3) Punkte)**.** Bestimmen Sie ...

1. die letzte Ziffer der Dezimaldarstellung von $(87^{88})^{99}$.
2. die letzten beiden Ziffern der Dezimaldarstellung von $(13^{1313})^{131313}$.

Hinweis. Die Lösungen müssen so dargestellt sein, dass sie ohne technische Hilfsmittel nachvollziehbar sind.

Bitte wenden

Aufgabe 2 (ganz kleiner Fermat; 4 (=2+2) Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Ist $m \in \mathbb{N}_{>0}$ und $x \in \mathbb{Z}$, so gilt $x^m \equiv x \mod m$.
2. Ist $p \in \mathbb{N}$ prim und $x \in \mathbb{Z}$, so gilt $x^{p+1} \equiv x^2 \mod p$.

Aufgabe 3 (RSA; 4 (=2+2) Punkte)**.** Wir betrachten das RSA-Verfahren.

1. Bestimmen Sie einen passenden privaten Schlüssel zu dem öffentlichen Schlüssel $(4891, 8633)$. Erklären Sie Ihr Vorgehen.
2. Entschlüsseln Sie mit diesem privaten Schlüssel den folgenden mit dem öffentlichen Schlüssel $(4891, 8633)$ verschlüsselten Klassiker (Goethe!). Erklären Sie, wie Sie bei der Entschlüsselung vorgegangen sind und welche Hilfsmittel Sie wie eingesetzt haben.

   1405, 8498, 5261, 6651, 7932, 6255, 6651, 815, 6745, 7124, 4394, 334, 3844, 8498, 5038, 3826, 3757, 2624, 8357, 6188, 7195, 5587, 8059, 5057, 858, 1220, 815, 6745, 1413, 1764, 4046, 334, 8498, 5038, 3826, 7031, 334, 7091, 2876, 5386, 656, 6651, 1076, 4201, 5718, 1912, 3826, 759, 538, 6741, 7251, 5447, 8222, 5454, 6255, 1, 5261, 770, 1836, 3848, 8357, 6188, 2876, 5129, 4874, 2876, 5386, 7836, 4228, 1076, 6741, 846, 5647, 8498, 5038, 3826, 926, 6315, 492, 8357, 6188, 1, 7091, 6680, 4257, 198, 6651, 4394, 307, 7243, 7512, 5038, 6080, 8357, 6188, 4682, 6632, 6745, 6770, 6680, 334, 3844, 8357, 6188, 7195, 815, 6745, 6770, 6680, 1169, 6071, 4394, 2775, 4394, 6770, 6680, 2775, 4394, 7573, 8494, 4689, 6071, 1814, 4034, 6071, 4394

   Hinweis. Das Leerzeichen wird durch 0 repräsentiert, die Buchstaben A, ..., Z des Alphabets durch $1, \ldots, 26$. Die Zahlen x, y zu zwei aufeinanderfolgenden Buchstaben werden zu $[100 \cdot x + y] \in \mathbb{Z}/(8633)$ zusammengefasst. Dies wurde dann mit RSA verschlüsselt.

Aufgabe 4 (Primpolynome; 4 Punkte)**.** Sei R ein faktorieller Ring. Zeigen Sie, dass der Polynomring $R[T]$ unendlich viele Primelemente enthält.
Hinweis. Was würde Euklid tun?

Bonusaufgabe (Kauderwelsch; 4 Punkte)**.** Entschlüsseln Sie folgenden deutschen Text. Erklären Sie Ihr Vorgehen. Skizzieren Sie insbesondere, in welcher Reihenfolge Sie welche Dinge entschlüsseln/erkennen konnten.

> YUJECWCOFCNGHNWAOLCO AOV DOIHBWC. VDC XKIACBCNDOOCO AOV XKIACBCN ... RHYWUNDXDCNCO OHWACNBDKIC FHIBCO AOV CNJDWWCBO VCNCO ENDJRHYWUNFCNBCLAOL, GUTCD XDC XDKI VCN CDOVCAWDLYCDW VDCXCN FCNBCLAOL TCGAXXW XDOV; TCDJ RHYWUNDXDCNCO GCOVCO XDC HAKI NCLCBO RACN VDC WCDBTHNYCDW VANKI FGCD, VNCD, RACOR AOV FCIO FDCBLCNDKIWCW HO. XDC OAWFCO VDCXC YCOOWODXXC HAKI RACN HNLAJCOWHWDUOCO, FAJ TCDXEDCB DJ NHIJCO VCN TCHOWGUNWAOL HBBWHLXOHICN RNHLCXWCBBAOLCO.

Hinweis. Jedes Zeichen steht dabei immer für denselben Buchstaben. Satzzeichen bleiben unverschlüsselt. Welche Buchstaben sind im Deutschen am häufigsten? Zusatzfrage: Woher stammt dieser Text?

Abgabe bis 19. Dezember 2025, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

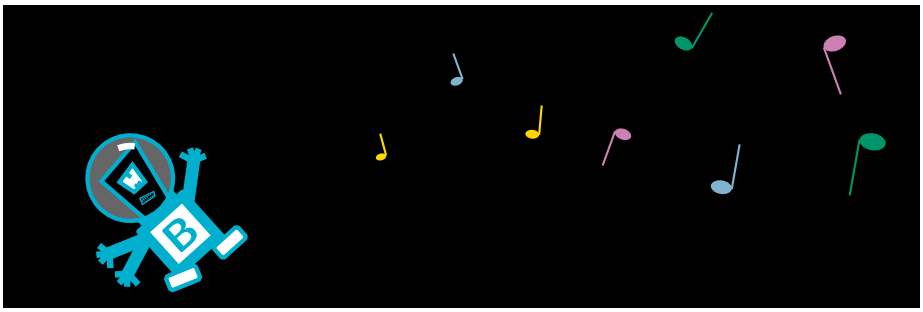
Prof. Dr. C. Löh/F. Hofmann — Blatt $9\frac{1}{2}$ vom 16. Dezember 2025

WANTED!

Bonusaufgabe (Hojotoho! 2 Punkte)**.** Inspiriert von den großen Künstlern Troubadix (Dorf der Verrückten), Bianca Castafiore (Mailand/Mühlenhof), Pavo (Bellhart) sowie Orpheus und Scylla (Unterwelt) sucht das Blorxchester dringend Texte, die auf eines der sonst unter den Codenamen

- Alle Jahre wieder
- Leise rieselt der Schnee
- Kling Glöckchen
- Oh du fröhliche

bekannten Lieder passen. Da sich das Blorxchester im Algebrarausch befindet, muss der Text die Definition faktorieller Ringe und die Formulierung des Satzes von Gauß enthalten.



Hinweis.

- Die besten Abgaben werden prämiert!
- Bitte beachten Sie, dass für diese Aufgabe nur die Abgabe per GRIPS möglich ist, damit die Direktion effizient auswählen kann.
- Hochdeutsch ist erlaubt. Dialekte auch.

Abgabe bis 19. Dezember 2025, 8:25, via GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann Blatt 10 vom 19. Dezember 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: irreduzibel, prim, maximal)**.** Wieder holen Sie die Begriffe *irreduzibles Element*, *Primelement*, *Primideal*, *maximales Ideal* in Ringen. Wie hängen diese Begriffe zusammen?

Fingerübung B (irreduzibel?)**.** Welche der folgenden Polynome sind irreduzibel?

1. $T^2 + 2 \in \mathbb{F}_3[T]$,
2. $T^{2026} + 2027 \cdot T^{2025} - 2027 \in \mathbb{Z}[T]$
3. $5 \cdot T^3 + 555 \cdot T^2 + 555555 \cdot T + 2055 \in \mathbb{Z}[T]$,
4. $\frac{1}{2} \cdot T^3 + 1 \in \mathbb{Q}[T]$.

Fingerübung C (irreduzibel??)**.** Welche der folgenden Aussagen sind wahr?

1. Jedes irreduzible Polynom in $\mathbb{Z}[T]$ ist auch in $\mathbb{Q}[T]$ irreduzibel.
2. Jedes Polynom in $\mathbb{Z}[T]$, das in $\mathbb{Q}[T]$ irreduzibel ist, ist in $\mathbb{Z}[T]$ irreduzibel.

Fingerübung D (Restklassenring)**.** Welche der folgenden Aussagen sind wahr?

1. Ist $p \in \mathbb{Z}[T]$ prim, so ist $\mathbb{Z}[T]/(p)$ ein Körper.
2. Ist $p \in \mathbb{Q}[T]$ prim, so ist $\mathbb{Q}[T]/(p)$ ein Körper.

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Restklassenkörper; 2 (=0+2) Punkte)**.** Begründen Sie jeweils Ihre Antwort!

0. Wiederholen Sie, wann ein Restklassenring ein Körper ist.
1. Zeigen Sie, dass $\mathbb{F}_7[T]/(T^2 + 1)$ ein Körper mit genau 49 Elementen ist.

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (Körper? 4 (=2+2) Punkte)**.** Zu $a \in \mathbb{Z}$ sei $f_a := T^4 + a \cdot T + 2 \in \mathbb{Z}[T]$ und $K_a := \mathbb{Q}[T]/(f_a)$.

1. Zeigen Sie: Es gibt unendlich viele $a \in \mathbb{Z}$, für die K_a ein Körper ist.
2. Geben Sie ein Beispiel für eine Zahl $a \in \mathbb{Z}$, für die K_a *kein* Körper ist. Begründen Sie Ihre Antwort!

Bitte wenden

Aufgabe 2 (irreduzibel? 4 (=2+2) Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Das Polynom $T^3 + 2025 \cdot T^2 + 42 \cdot T + 9 \in \mathbb{Z}[T]$ ist irreduzibel in $\mathbb{Z}[T]$.
2. Das Polynom $X^2 \cdot Y + Y^2 \cdot X^{2025} + X + Y + 1$ ist irreduzibel in $\mathbb{F}_2[X, Y]$.

Aufgabe 3 (noch ein Irreduzibilitätskriterium; 4 (=3+1) Punkte)**.**

1. Sei $f \in \mathbb{Z}[T]$ ein normiertes Polynom vom Grad höchstens 3 mit folgender Eigenschaft: Für alle $a \in \mathbb{Z}$ gilt
$$a \mid f(0) \Longrightarrow f(a) \neq 0.$$
Zeigen Sie, dass f in $\mathbb{Z}[T]$ und in $\mathbb{Q}[T]$ irreduzibel ist.
2. Geben Sie ein Beispiel für ein Polynom, auf das dieses Kriterium anwendbar ist, auf das aber das Eisensteinsche Reduzibilitätskriterium für keine Primzahl anwendbar ist. Begründen Sie Ihre Antwort!

Aufgabe 4 (iterirreduzibel; 4 = (1+1+1+1) Punkte)**.** Wir betrachten die Folge $(f_n)_{n\in\mathbb{N}}$ in $\mathbb{Z}[T]$, die durch $f_0 := T$, $f_1 := T^2 - 2$ und
$$f_{n+1} := f_1(f_n)$$
für $n \in \mathbb{N}_{>0}$ rekursiv durch Einsetzen definiert ist.

1. Bestimmen Sie die Koeffizienten von f_3.
2. Zeigen Sie: Für alle $n \in \mathbb{N}_{>0}$ gilt $f_n(0) = 2$.
3. Bestimmen Sie für alle $n \in \mathbb{N}$ die Reduktion von f_n modulo 2.
4. Zeigen Sie, dass f_n in $\mathbb{Q}[T]$ irreduzibel ist.

Rob Lavinsky, iRocks.com–CC-BY-SA-3.0

Bonusaufgabe (invariant und irreduzibel; 4 Punkte)**.** Sei $p \in \mathbb{N}$ prim. Zeigen Sie, dass
$$T^p - T - 1 \in \mathbb{F}_p[T]$$
in $\mathbb{F}_p[T]$ irreduzibel ist.
Hinweis. Dieses Polynom ist unter dem von „$T \longmapsto T + 1$“ induzierten Ringisomorphismus $\mathbb{F}_p[T] \longrightarrow \mathbb{F}_p[T]$ invariant. Betrachten Sie nun die Primfaktorzerlegung ...

Abgabe bis 9. Januar 2026, 8:25, via Briefkasten/GRIPS

Frohe Weihnachten und ein gutes Neues Jahr!

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 11 vom 9. Januar 2026

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Körper aus Polynomen)**.** Wiederholen Sie, warum folgende Konstruktion funktioniert: Ist K ein Körper und $f \in K[T]$ irreduzibel, so ist $K[T]/(f)$ ein Körper.

Fingerübung B (Körper?)**.** Welche der folgenden Teilmengen von $\mathbb{C}$ sind Körper bezüglich den gewöhnlichen arithmetischen Operationen auf $\mathbb{C}$?

1. $\{a + i \cdot \sqrt{3} \cdot b \mid a, b \in \mathbb{Z}\}$
2. $\{a + i \cdot \sqrt{3} \cdot b \mid a, b \in \mathbb{Q}\}$
3. $\{a + i \cdot \sqrt{3} \cdot b \mid a, b \in \mathbb{R}\}$
4. $\{a + i \cdot \sqrt{3} \cdot b \mid a, b \in \mathbb{C}\}$

Fingerübung C (Körperhomomorphismen)**.** Sei K einer der folgenden Körper. Entscheiden Sie jeweils, ob es mehr als einen Körperhomomorphismus $K \longrightarrow K$ gibt.

$$\mathbb{Q}, \quad \mathbb{C}, \quad \mathbb{F}_7, \quad \mathbb{F}_3[T]/(T^2 + 1)$$

Fingerübung D (Einheiten)**.** Sei $n \in \mathbb{N}_{>0}$. Zeigen Sie, dass die multiplikative Gruppe $\mathbb{C}^\times$ eine Untergruppe enthält, die zu $\mathbb{Z}/n$ isomorph ist.

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (letzte Ziffern; 2 (=0+2) Punkte)**.**

0. Wiederholen Sie den *kleinen Satz von Fermat*.
1. Bestimmen Sie die letzten beiden Ziffern von 2026^{2020} im Siebenersystem.

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (ungerade Grade; 4 Punkte)**.** Sei $L \mid K$ eine Körpererweiterung und sei $\alpha \in L$ mit $[K(\alpha) : K] = 2025$. Zeigen Sie, dass $K(\alpha) = K(\alpha^2)$.
Hinweis. Was wissen Sie über $[K(\alpha) : K(\alpha^2)]$?

Aufgabe 2 (Charakteristik; 4 (=2+2) Punkte)**.** Seien K und L Körper. Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Ist $L \mid K$ eine Körpererweiterung, so gilt $\operatorname{char} K = \operatorname{char} L$.
2. Ist $\operatorname{char} K = \operatorname{char} L$, so ist $L \mid K$ eine Körpererweiterung.

Bitte wenden

Aufgabe 3 (Primkörper; 4 (=2+2) Punkte)**.** Sei K ein Körper.

1. Zeigen Sie, dass K genau einen bezüglich Inklusion kleinsten Körper enthält, den *Primkörper von* K.
2. Zeigen Sie:
   - Ist $\operatorname{char} K = 0$, so ist der Primkörper von K isomorph zu $\mathbb{Q}$.
   - Ist $p \in \mathbb{N}$ prim und $\operatorname{char} K = p$, so ist der Primkörper von K isomorph zu $\mathbb{F}_p$.

Aufgabe 4 (Frobenius; 4 (=1+1+1+1) Punkte)**.** Sei $p \in \mathbb{N}$ prim, sei K ein Körper der Charakteristik p und sei

$$\begin{aligned} F \colon K &\longrightarrow K \\ x &\longmapsto x^p \end{aligned}$$

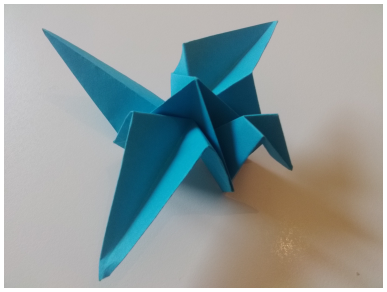
der *Frobeniusendomorphismus*.

1. Zeigen Sie, dass F tatsächlich ein Ringhomomorphismus ist.
2. Wie kann man den Frobeniusendomorphismus von $\mathbb{F}_p$ auch beschreiben?
3. Zeigen Sie: Ist K endlich, so ist F ein Isomorphismus.
4. Zeigen Sie: Ist K unendlich, so ist F im allgemeinen *kein* Isomorphismus.

Bonusaufgabe (Origami-Konstruierbarkeit; 4 (=2+2) Punkte)**.**

1. Schlagen Sie in der Literatur nach, wie *Origami-Konstruierbarkeit* (analog zur Konstruierbarkeit mit Zirkel und Lineal) definiert ist.
2. Skizzieren Sie einen Beweis dafür, dass die Menge der in $\mathbb{C}$ aus $\{0, 1\}$ Origami-konstruierbaren Punkte einen Körper bildet.

Hinweis. Im Sinne der guten wissenschaftlichen Praxis: Geben Sie vollständige, nachvollziehbare Quellen an.



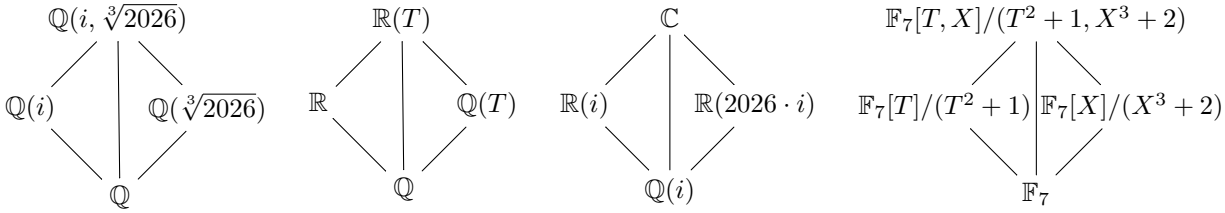
Abgabe bis 16. Januar 2026, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 12 vom 16. Januar 2026

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Grade)**.** Wiederholen Sie den Begriff des *Grads* einer Körpererweiterung und bestimmen Sie zu jeder der folgenden Körpererweiterungen den Grad:



Fingerübung B (algebraische Zahlen)**.** Sei $\alpha \in \mathbb{C}$ mit

$$\alpha^5 + 2 \cdot \alpha^3 - 42 \cdot \alpha + 402 = 0.$$

Schreiben Sie die folgenden Zahlen als $\mathbb{Q}$-Linearkombination von $1, \alpha, \dots, \alpha^4$:

$$\alpha^5, \quad \alpha^6, \quad \frac{1}{\alpha}.$$

Fingerübung C (Minimalpolynome)**.** Bestimmen Sie für die folgenden komplexen Zahlen das Minimalpolynom über den angegebenen Grundkörpern:

1. von $\sqrt{2026}$ über $\mathbb{Q}$
2. von $\sqrt{2026}$ über $\mathbb{Q}(\sqrt[3]{2026})$
3. von $\sqrt{2026}$ über $\mathbb{Q}(\sqrt[4]{2026})$
4. von $\sqrt{2026}$ über $\mathbb{R}$

Fingerübung D (Zwischenkörper)**.** Sei $L \mid K$ eine Körpererweiterung und seien $S, S' \subset L$. Zeigen Sie:

$$\big(K(S)\big)(S') = K(S \cup S') = K(S) \cdot K(S')$$

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (irreduzibel? 2 (=0+2) Punkte)**.**

0. Wiederholen Sie die behandelten *Irreduzibilitätskriterien*. Achten Sie auf vollständige Voraussetzungen und präzise Formulierungen!
1. Ist das Polynom $3 \cdot T^{2026} + 424242 \cdot T^{42} + 123456789$ in $\mathbb{Q}[T]$ irreduzibel? Begründen Sie Ihre Antwort!

Bitte wenden

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (ein Zerfällungskörper von $T^4 - 42$ über $\mathbb{Q}$; 4 (=2+2) Punkte)**.** Wir betrachten den Zwischenkörper $K := \mathbb{Q}(\sqrt[4]{42}, i)$ in $\mathbb{C} \mid \mathbb{Q}$. Bearbeiten Sie zwei der folgenden vier Aufgaben:

1. Liegen alle komplexen Nullstellen von $T^4 - 42$ in K ? Liegen alle komplexen Nullstellen von $T^4 - 42$ in $\mathbb{Q}(\sqrt[4]{42})$? Begründen Sie Ihre Antwort!
2. Bestimmen Sie $a, b, c, d \in \mathbb{Q}$ mit
$$\frac{1}{\sqrt[4]{42} - 1} = a + b \cdot \sqrt[4]{42} + c \cdot \sqrt{42} + d \cdot \sqrt{42} \cdot \sqrt[4]{42}.$$
3. Zeigen Sie, dass $[K : \mathbb{Q}] = 8$ ist.
   Hinweis. Zeigen Sie zunächst $\mathbb{Q}(\sqrt[4]{42}) \cap \mathbb{Q}(i) = \mathbb{Q}$. Warum hilft das?
4. Zeigen Sie, dass $\mathrm{Gal}(K, \mathbb{Q})$ *kein* Element der Ordnung 8 enthält.
   Hinweis. Wieviele Nullstellen haben $T^4 - 42$ bzw. $T^2 + 1$ in K ?

Aufgabe 2 (algebraische Zahlen; 4 (=2+2) Punkte)**.** Sei $L \mid K$ eine Körpererweiterung und seien $\alpha, \beta \in L$ algebraisch über K. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort!

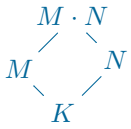
1. Ist $K(\alpha) = K(\beta)$, so haben α und β dasselbe Minimalpolynom über K.
2. Haben α und β dasselbe Minimalpolynom über K, so ist $K(\alpha) = K(\beta)$.

Aufgabe 3 (algebraische Erweiterungen; 4 Punkte)**.** Sei $L \mid K$ eine Körpererweiterung und sei M ein Zwischenkörper von $L \mid K$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

1. Die Körpererweiterung $L \mid K$ ist algebraisch.
2. Die Körpererweiterungen $L \mid M$ und $M \mid K$ sind algebraisch.

Aufgabe 4 (Grade von Komposita; 4 (=2+2) Punkte)**.** Sei $L \mid K$ eine Körpererweiterung und seien M, N Zwischenkörper von $L \mid K$.

1. Zeigen Sie, dass $[M \cdot N : M] \leq [N : K]$ ist.
   Hinweis. Ist $[N : K]$ endlich, so ist $N \mid K$ insbesondere auch endlich erzeugt und man kann induktiv argumentieren ...
2. Folgern Sie: Ist $\mathrm{ggT}\big([M : K], [N : K]\big) = 1$, so ist
$$[M \cdot N : K] = [M : K] \cdot [N : K].$$



Bonusaufgabe (Transzendenz; 4 Punkte)**.** Zeigen Sie, dass die reelle Zahl
$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.110001000000000000000001\ldots$$
über $\mathbb{Q}$ transzendent ist.
Hinweis. Warum ist diese Zahl nicht rational? Zeigen Sie, dass sich algebraische Zahlen „nicht zu gut durch rationale Zahlen“ approximieren lassen. Schließen Sie dann daraus, dass die obige Zahl nicht algebraisch über $\mathbb{Q}$ ist.

Abgabe bis 23. Januar 2026, 8:25, via Briefkasten/GRIPS

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 13 vom 23. Januar 2026

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Symmetrien)**.** Wiederholen Sie Grundlagen zu Symmetrien, d.h. zu *Gruppenoperationen* und zu *symmetrischen Gruppen*.

Fingerübung B (Konjugationsprinzip für algebraische Zahlen)**.** Wir betrachten den Zwischenkörper $K := \mathbb{Q}(\sqrt[5]{2026}, i, \zeta_5)$ von $\mathbb{C} \mid \mathbb{Q}$. Sei $\sigma \in \mathrm{Gal}(K, \mathbb{Q})$. Welche der folgenden Gleichungen sind möglich?

1. $\sigma(i) = -i$
2. $\sigma(\sqrt[5]{2026}) = -i$
3. $\sigma(\zeta_5) = -\zeta_5$
4. $\sigma(\zeta_5) = {\zeta_5}^4$

Fingerübung C (Galoisgruppe)**.** Bestimmen Sie $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i), \mathbb{Q})$ mit dem Konjugationsprinzip. Wieviele Elemente enthält diese Gruppe? Wie kann man diese Elemente explizit beschreiben? Welchen Isomorphietyp hat diese Gruppe? Ist diese Gruppe abelsch, zyklisch, ... ?

Fingerübung D (Zerfällungskörper)**.**

1. Ist $\mathbb{Q}(\zeta_2) \subset \mathbb{C}$ ein Zerfällungskörper von $T^4 - 1$ über $\mathbb{Q}$?
2. Ist $\mathbb{Q}(\zeta_4) \subset \mathbb{C}$ ein Zerfällungskörper von $T^2 - 1$ über $\mathbb{Q}$?
3. Ist $\mathbb{Q}(\zeta_5) \subset \mathbb{C}$ ein Zerfällungskörper von $T^5 - 1$ über $\mathbb{Q}$?
4. Ist $\mathbb{Q}(\zeta_5) \subset \mathbb{C}$ ein Zerfällungskörper von $(T - 1)^5$ über $\mathbb{Q}$?

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Körper; 2 (=0+2) Punkte)**.**

0. Wiederholen Sie *Grundlagen zu Körpern* (Charakteristik, Primkörper, endliche Untergruppen der Einheitengruppe).
1. Geben Sie je eine Verknüpfungstabelle für die Addition und die Multiplikation auf dem Körper $\mathbb{F}_2[T]/(T^2 + T + 1)$ an. Wie haben Sie diese Verknüpfungstabellen bestimmt?

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (Wurzeln; 4 (= 2+2) Punkte)**.** Sei $n \in \mathbb{N}_{\geq 2}$, sei K ein Körper, der ein Zerfällungskörper von $T^n - 1 \in K[T]$ über K ist (d.h. $T^n - 1$ zerfällt über K in Linearfaktoren), und sei $c \in K \setminus \{0\}$. Außerdem sei $L \mid K$ eine Körpererweiterung und $\alpha \in L$ mit $\alpha^n = c$.

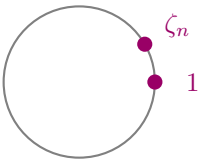
1. Zeigen Sie, dass $K(\alpha) \subset L$ ein Zerfällungskörper von $T^n - c$ über K ist.
2. Zeigen Sie, dass $\mathrm{Gal}(K(\alpha), K)$ zyklisch ist.

   Hinweis. Konstruieren Sie mithilfe des Konjugationsprinzips und einer primitiven n-ten Einheitswurzel einen injektiven Gruppenhomomorphismus von $\mathrm{Gal}(K(\alpha), K)$ in eine zyklische Gruppe.

Bitte wenden

Aufgabe 2 (Zerfällungskörper; 4 (=2+2) Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Es ist $\mathbb{Q}(\zeta_6) \subset \mathbb{C}$ ein Zerfällungskörper von $(T^3 - 1) \cdot (T^6 - 1)$ über $\mathbb{Q}$.
2. Es ist $\mathbb{R}(\zeta_3) \subset \mathbb{C}$ ein Zerfällungskörper von $T^3 - 2$ über $\mathbb{R}$.



Aufgabe 3 (Fixkörper; 4 (=1+1+1+1) Punkte)**.** Sei $L \mid K$ eine endliche Körpererweiterung, sei $G \subset \mathrm{Gal}(L, K)$ eine Untergruppe und sei

$$M := L^G := \{x \in L \mid \forall_{\sigma \in G} \quad \sigma(x) = x\}$$

der *Fixkörper von* $L \mid K$ *bezüglich* G. Sei $\alpha \in L$.

1. Zeigen Sie, dass M ein Zwischenkörper von $L \mid K$ ist.
2. Sei $(\sigma_1, \ldots, \sigma_m)$ eine maximale Familie in G, für die $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$ alle verschieden sind, und sei

   $$f := \prod_{j=1}^{m} \big(T - \sigma_j(\alpha)\big) \in L[T].$$

   Zeigen Sie, dass f bereits in $M[T]$ liegt.
3. Zeigen Sie, dass $[M(\alpha) : M] \leq \#G$.
4. Zeigen Sie: Das Minimalpolynom von α über M zerfällt in L in paarweise verschiedene Linearfaktoren.

Aufgabe 4 (Ableitungskriterium; 4 (=2+2) Punkte)**.** Sei K ein Körper, sei $f \in K[T] \setminus K$ normiert und sei $L \mid K$ eine Körpererweiterung mit der Eigenschaft, dass f in $L[T]$ in Linearfaktoren zerfällt.

1. Zeigen Sie, dass f genau dann eine mehrfache Nullstelle in L besitzt, wenn $\mathrm{ggT}(f, Df) \neq 1$ in $L[T]$ gilt (Bonusaufgabe: in $K[T]$).
2. Zeigen Sie: Ist $f \in K[T]$ irreduzibel, so besitzt f genau dann eine mehrfache Nullstelle in L, wenn $Df = 0$ ist.

Bonusaufgabe (endliche Körper für Schüler; 4 Punkte)**.** Entwickeln Sie eine Anleitung und vier Aufgaben, womit (Mittelstufen-)schüler lernen können, dass es einen Körper mit genau vier Elementen gibt. Entwerfen Sie zusätzlich einen Lösungsvorschlag, der den zu erwartenden Kenntnissen solcher Schüler angemessen ist.
Hinweis. Mittelstufenschüler kennen die Definition des Begriffs *Körper* nicht! Es schadet außerdem nicht, wenn die Anleitung auch einen Absatz dazu enthält, warum man sich für so etwas interessieren könnte.

Abgabe bis 30. Januar 2026, 8:25, via Briefkasten/GRIPS

Dies ist das letzte reguläre Übungsblatt. Alle Punkte von Blatt 14 zählen als Bonuspunkte.

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 14 vom 30. Januar 2026

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Auflösbarkeit)**.** Wiederholen Sie den Begriff der *Auflösbarkeit* aus der Gruppentheorie. Wie kann man in diesem Kontext die *Sylowsätze* einsetzen?

Fingerübung B ($\mathbb{F}_{16}$)**.** Beantworten Sie die folgenden Fragen mithilfe des Klassifikationssatzes für endliche Körper:

1. Wie kann man $\mathbb{F}_{16}$ aus $\mathbb{F}_2$ konstruieren? Wie sieht der Frobeniusendomorphismus $\sigma\colon \mathbb{F}_{16} \longrightarrow \mathbb{F}_{16}$ in dieser Beschreibung aus?
2. Warum besitzt $\mathbb{F}_{16} \mid \mathbb{F}_2$ genau einen Zwischenkörper K mit $\#K = 4$?
3. Welche Potenzen von σ liegen in $\mathrm{Gal}(\mathbb{F}_{16}, K)$?
4. Warum besitzt $\mathbb{F}_8 \mid \mathbb{F}_2$ *keinen* Zwischenkörper K mit $\#K = 4$?

Fingerübung C (normale Körpererweiterungen)**.** Welche der folgenden Körpererweiterungen sind normal?

1. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2026}) \mid \mathbb{Q}(\sqrt{2026})$
2. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2026}) \mid \mathbb{Q}(\sqrt[3]{2})$
3. $\mathbb{Q}(i \cdot \sqrt{2026}) \mid \mathbb{Q}$
4. $\mathbb{Q}(i, \sqrt{2026}) \mid \mathbb{Q}$

Fingerübung D (primitive Elemente)**.** Bestimmen Sie ein primitives Element für die Körpererweiterung $\mathbb{Q}(\zeta_3, \sqrt[3]{2}) \mid \mathbb{Q}$.

Hinweis. Die Wiederholungsaufgaben sind freiwillig, knnen aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Grade; 2 (=0+2) Punkte)**.**

0. Wiederholen Sie den Begriff des *Grades* einer Körpererweiterung.
1. Wir betrachten die Zwischenkörper $\mathbb{Q}(\sqrt[42]{5})$ und $\mathbb{Q}(\sqrt[5]{42})$ von $\mathbb{C} \mid \mathbb{Q}$. Bestimmen Sie $[\mathbb{Q}(\sqrt[42]{5}, \sqrt[5]{42}) : \mathbb{Q}(\sqrt[5]{42})]$. Begründen Sie Ihre Antwort!

Bonusaufgabe (Wiederholung) (fünfzehn I; 2 (=1+1) Punkte)**.** Begründen Sie jeweils Ihre Antwort!

1. Konstruieren Sie einen Isomorphismus $\big(\mathbb{Z}/(15)\big)^\times \cong_{\mathsf{Group}} \mathbb{Z}/4 \times \mathbb{Z}/2$.
2. Bestimmen Sie alle Untergruppen von $\mathbb{Z}/4 \times \mathbb{Z}/2$.

   Hinweis. Es sind acht.

Bitte wenden

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (fünfzehn II; 4 (= 2+2) Punkte)**.** Sei $\zeta_{15} := e^{2\cdot\pi\cdot i/15} \in \mathbb{C}$.

1. Bestimmen Sie für jedes Element von $\mathrm{Gal}\big(\mathbb{Q}(\zeta_{15}), \mathbb{Q}\big)$, worauf ζ_{15} abgebildet wird und geben Sie in dieser Beschreibung einen Gruppenisomorphismus $\mathrm{Gal}(\mathbb{Q}(\zeta_{15}), \mathbb{Q}) \cong_{\mathsf{Group}} \mathbb{Z}/4 \times \mathbb{Z}/2$ an.

2. Bestimmen Sie alle Zwischenkörper von $\mathbb{Q}(\zeta_{15}) \mid \mathbb{Q}$.

   Hinweis. Geben Sie primitive Elemente an. Was hat das mit $\sqrt{5}$ zu tun?!

Hinweis. Falls Ihnen „fünfzehn“ zu übermütig erscheint, können Sie alternativ die entsprechenden Fragen für „fünf“ bearbeiten.

Aufgabe 2 (Galoiskorrespondenz; 4 (=2+2) Punkte)**.** Sei $L \mid K$ eine endliche Galoiserweiterung mit $\mathrm{Gal}(L, K) \cong_{\mathsf{Group}} A_5$. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort!

1. Es gibt einen Zwischenkörper M von $L \mid K$ mit $[M : K] = 2$.

2. Es gibt einen Zwischenkörper M von $L \mid K$ mit $\#\,\mathrm{Gal}(L, M) = 5$.

Aufgabe 3 (schon wieder fünfzehn; 4 Punkte)**.** Sei $L \mid K$ eine Galoiserweiterung vom Grad 15. Zeigen Sie: Ist M ein Zwischenkörper von $L \mid K$, so ist auch $M \mid K$ eine Galoiserweiterung.
Hinweis. Es war einmal ein Sylowsatz ...

Aufgabe 4 (Klassifikation endlicher Körpererweiterungen von endlichen Körpern; 4 (=2+2) Punkte)**.** Sei F ein endlicher Körper und sei $k \in \mathbb{N}_{\geq 1}$.

1. Zeigen Sie: Bis auf Isomorphie gibt es genau eine Körpererweiterung $L \mid F$ über F vom Grad k.

   Hinweis. Sei K ein Körper und $m, n \in \mathbb{N}$. Zeigen Sie, dass dann $T^m - T$ ein Teiler von $T^{m^n} - T$ in $K[T]$ ist. Warum hilft das?

2. Zeigen Sie, dass die Galoisgruppe dieser Körpererweiterung $L \mid F$ isomorph zu $\mathbb{Z}/k$ ist (erzeugt von einer geeigneten Potenz des Frobeniusendomorphismus von L).

Bonusaufgabe (Geschichte; 4 Punkte)**.** Beantworten Sie für

Gauß, Galois, E. Artin, Kummer

die folgenden Fragen:

- Wann haben sie gelebt und (wo) hängt ihr Bild in der Fakultät für Mathematik?
- Was haben sie mit Galoistheorie zu tun?

Keine Abgabe!

Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann — Blatt 15 vom 6. Februar 2026

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: alles!)**.** Wiederholen Sie das Material der gesamten Vorlesung. Organisieren Sie das Material so, dass Sie es sich gut merken können. Was ist wichtig? Überlegen Sie sich einfache Fragen/Aufgaben dazu!
Hinweis. Machen Sie sich nicht verrückt! Manchmal ist es besser, ausgeschlafen zu sein statt bis zur letzten Sekunde Material einzufüllen.

Fingerübung B (Galoiskorrespondenz)**.** Sei $L \mid K$ eine endliche Galoiserweiterung mit $\mathrm{Gal}(L,K) \cong_{\mathsf{Group}} S_5$. Welche der folgenden Aussagen treffen zu?

1. Es gilt $[L:K] = 5$.
2. Es gibt Zwischenkörper M von $L \mid K$, für die $M \mid K$ nicht normal ist.
3. Es gibt Zwischenkörper M von $L \mid K$ mit $\mathrm{Gal}(L,M) \cong_{\mathsf{Group}} \mathbb{Z}/30$.
4. Es gibt Zwischenkörper M von $L \mid K$ mit $[M:K] = 2$.
5. Es gibt Zwischenkörper M von $L \mid K$ mit $\#\,\mathrm{Gal}(L,M) = 3$.
6. Es gibt Zwischenkörper M von $L \mid K$ mit $\#\,\mathrm{Gal}(L,M) = 2026$.

Fingerübung C (Realisierung als Galoisgruppen)**.** Geben Sie für die folgenden Gruppen G eine endliche Galoiserweiterung über $\mathbb{Q}$ an, deren Galoisgruppe zu G isomorph ist. Was wissen Sie dann über die Zwischenkörper dieser Erweiterung?

1. $\mathbb{Z}/2$
2. $\mathbb{Z}/2 \times \mathbb{Z}/2$
3. $\mathbb{Z}/4$
4. S_3

Fingerübung D (Durcheinander)**.**

1. Sind alle Untergruppen von S_5 mit genau acht Elementen isomorph zueinander?
2. Bestimmen Sie die letzte Ziffer der Dezimaldarstellung von 111213^{1415}.
3. Ist $\mathbb{Z}[T]/(T^2+T+1)$ ein Körper?
4. Ist $\mathbb{Q}[T]/(T^2+T+1)$ ein Körper?
5. Konstruieren Sie einen Körper mit genau acht Elementen.
6. Ist die Körpererweiterung $\mathbb{C} \mid \mathbb{Q}(\sqrt{2}, i)$ algebraisch?

Bitte wenden

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 (Triangulatur des Quadrats)**.**

1. Zeigen Sie algebraisch, dass man aus den vier Ecken des Einheitsquadrats in $\mathbb{C}$ mit Zirkel und Lineal ein gleichseitiges Dreieck mit demselben Flächeninhalt konstruieren kann.

2. Beschreiben Sie geometrisch wie man mit Zirkel und Lineal aus den vier Ecken des Einheitsquadrats in $\mathbb{C}$ ein gleichseitiges Dreieck mit demselben Flächeninhalt konstruieren kann.

Aufgabe 2 (Auflösbarkeit durch Radikale)**.** Sei $f \in \mathbb{Q}[T]$ ein normiertes Polynom und sei G die Galoisgruppe von f über $\mathbb{Q}$. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Ist $\#G = 2048$, so ist f über $\mathbb{Q}$ durch Radikale auflösbar.

2. Ist $\deg f = 2048$, so ist f über $\mathbb{Q}$ durch Radikale auflösbar.

Aufgabe 3 (Rarität von Einheitswurzeln)**.** Sei $L \mid \mathbb{Q}$ eine endliche Körpererweiterung. Zeigen Sie, dass L nur endlich viele Einheitswurzeln enthält.
Hinweis. Was passiert mit $\varphi(n)$ für $n \to \infty$?!

Aufgabe 4 (Winkeldreiteilung)**.**

1. Geben Sie eine präzise Definition von „konstruierbaren Winkeln“ (mit Zirkel und Lineal) und der „Konstruierbarkeit der Winkeldreiteilung mit Zirkel und Lineal“.

2. Zeigen Sie: Im allgemeinen ist *nicht* für jeden mit Zirkel und Lineal konstruierbaren Winkel auch die zugehörige Winkeldreiteilung mit Zirkel und Lineal konstruierbar.

Bonusaufgabe (zyklische Erweiterungen)**.** Sei K ein Körper, sei $n \in \mathbb{N}_{>0}$ und K enthalte n verschiedene n-te Einheitswurzeln. Sei $L \mid K$ eine Galoiserweiterung mit $\mathrm{Gal}(L, K) \cong_{\mathsf{Group}} \mathbb{Z}/n$. Zeigen Sie, dass es dann ein $c \in K$ gibt, so dass L ein Zerfällungskörper von $T^n - c$ über K ist.
Hinweis. Sei $\sigma \in \mathrm{Gal}(L, K) \cong_{\mathsf{Group}} \mathbb{Z}/n$ ein Erzeuger.

1. Fassen Sie σ als K-linearen Endomorphismus von L auf und zeigen Sie, dass es eine primitive n-te Einheitswurzel gibt, die ein Eigenwert von σ ist. Sei $\alpha \in L$ ein zugehöriger Eigenvektor.

2. Zeigen Sie, dass $c := \alpha^n$ in K liegt (Fixkörper!).

3. Erinnern Sie sich daran, dass $K(\alpha) \subset L$ ein Zerfällungskörper von $T^n - c$ über K ist (Aufgabe 13.1).

4. Zeigen Sie, dass $L = K(\alpha)$ ist (Grade?!).

Keine Abgabe!

C

Organisatorisches

Algebra: Organisatorisches

Prof. Dr. C. Löh/F. Hofmann Oktober 2025

Homepage. Alle aktuellen Informationen zur Vorlesung, zu den Übungen, zu Sprechstunden, Literaturangaben, sowie die Übungsblätter/Lesepläne finden Sie auf der Homepage zur Vorlesung bzw. in GRIPS:

https://loeh.app.ur.de/teaching/algebra_ws2526

https://elearning.uni-regensburg.de/course/view.php?id=72280

Vorlesung. Die Vorlesung findet jeweils dienstags und freitags (8:15–10:00; H 31) statt. Das Vorlesungsskript ist über die Vorlesungshomepage und GRIPS zugänglich; das Skript wird jeweils *nach* der Vorlesung im Verlauf des Tages aktualisiert.

Ich möchte alle Teilnehmer dazu ermutigen, sich aktiv an der Vorlesung zu beteiligen und Fragen zu stellen bzw. zu beantworten. Deshalb möchte ich die Atmosphäre so locker, informell und unverbindlich wie möglich halten.

Übungen. Die neuen Übungsaufgaben werden wöchentlich freitags spätestens um 10:00 Uhr auf den obigen Homepages online gestellt und sind bis zum Freitag eine Woche später um 8:15 Uhr abzugeben (in die Briefkästen oder via GRIPS).

Auf jedem Übungsblatt gibt es vier reguläre Aufgaben (je 4 Punkte), Bonusaufgaben (je 4 Bonuspunkte) und ab Blatt 3 eine Wiederholungsaufgabe (je 2 Bonuspunkte).

Sie dürfen und sollen die Aufgaben in kleinen Gruppen bearbeiten; aber die Lösungen müssen individuell ausformuliert und aufgeschrieben werden, andernfalls werden die Punkte aberkannt. Sie dürfen (müssen aber nicht!) Lösungen zu zweit abgeben; in diesem Fall müssen selbstverständlich jeweils beide Autoren in der Lage sein, *alle* der Zweiergruppe abgegebenen Lösungen zu präsentieren, andernfalls werden die Punkte aberkannt.

Die Übungsgruppen beginnen in der zweiten Vorlesungswoche; in diesen ersten Übungen werden die Fingerübungen von Blatt 1 besprochen.

Zentralübung. Zusätzlich zur Vorlesung und den Übungen bietet die Zentralübung die Gelegenheit, Fragen zu stellen, den Stoff der Vorlesung zu wiederholen und weitere Beispiele zu behandeln. Die Zentralübung findet donnerstags (14:15–15:45; H 31) statt. Die Zentralübung beginnt in der ersten Vorlesungswoche und ist ein freiwilliges Zusatzangebot.

Fingerübungen. Das Skript und die Übungsblätter enthalten Fingerübungen, die elementare Techniken und Begriffe trainieren. Diese Aufgaben sollten im Idealfall so einfach sein, dass sie innerhalb weniger Minuten gelöst werden können. Diese Aufgaben werden nicht abgegeben bzw. korrigiert. Die Fingerübungen auf den Übungsblättern werden in den Übungsgruppen gemeinsam behandelt und können zusätzlich auch gut zum „Aufwärmen“ beim täglichen Üben genutzt werden.

Einteilung in die Übungsgruppen. Die Einteilung in die Übungsgruppen erfolgt über GRIPS.

Sie können sich bis Mittwoch, den 15. Oktober 2025, um 9:00 Uhr für die Übungen anmelden; Sie können dort Ihre Präferenzen für die Übungstermine auswählen und wir werden versuchen, diese Wünsche zu erfüllen. Bitte beachten Sie jedoch, dass es sein kann, dass wir nicht alle Wünsche erfüllen können.

Anmeldungen über EXA/SPUR für die Übungsgruppen werden *nicht* berücksichtigt!

Die endgültige Einteilung der Übungsgruppen wird voraussichtlich am Donnerstag, den 16. Oktober 2025, in GRIPS bekanntgegeben. Ein Wechsel in volle Übungsgruppen ist dann nur durch Tausch mit einem Tauschpartner möglich.

Bei Fragen zum Übungsbetrieb wenden Sie sich bitte an Franziska Hofmann (franziska2.hofmann@mathematik.uni-r.de).

Prüfungs-/Studienleistungen. Die Vorlesung *Algebra* kann wie in den Modulkatalogen spezifiziert in die Studiengänge eingebracht werden.

- *Studienleistung*: Erfolgreiche Teilnahme an den Übungen: Mindestens 50% der (in den regulären Aufgaben) möglichen Punkte, mindestens einmal zufriedenstellend vorrechnen.
- *Prüfungsleistung*: schriftliche Klausur (120 Minuten).

Die Wiederholungsklausur kann auch als Erstversuch geschrieben werden; diese Option ist nur in Einzelfällen sinnvoll: der nächste Wiederholungstermin ist dann erst ein Jahr später im Rahmen der nächsten Vorlesung Algebra.

Um das Modul *MAT-BAlg1* bzw. *MAT-LA-GyAlg* erfolgreich abzuschließen, müssen folgende Leistungen erbracht werden

- Studienleistung Algebra
- Prüfungsleistung Algebra
- Fr MAT-LA-GyAlg außerdem: Studienleistung Examenskurs Algebra und Zahlentheorie

Sie müssen sich in FlexNow für die Studienleistung und die Prüfungsleistung anmelden. Bitte informieren Sie sich frühzeitig über die für Sie gültigen Modalitäten (Prüfungsordnung, Modulkatalog, ggf. Studiengangskoordination und Studienberatung). Berücksichtigen Sie bitte auch (implizite) Fristen der entsprechenden Prüfungsordnungen bis wann (Wiederholungs-)Prüfungen abgelegt werden müssen.

Klausurtermine. Die Klausuren finden zu folgenden Terminen statt:

- Klausur: 09.02.2026
- Wiederholungsklausur: am Ende der Semesterferien (Termin wird rechtzeitig bekanntgegeben).

Wichtige Informationen im Krankheitsfall finden Sie unter:

https://www.uni-regensburg.de/studium/startseite/verhalten-krankheitsfall/index.html

Hinweise für Wiederholer. Studenten, die bereits in einem vorangegangenen Semester an der Vorlesung teilgenommen haben, aber im entsprechenden Semester die Klausur nicht bestanden haben oder nicht an der Klausur teilgenommen haben, können auch an den oben genannten Klausurterminen teilnehmen, sofern noch ein Prüfungsanspruch besteht. Informieren Sie sich rechtzeitig über den Stoffumfang dieser Vorlesung (z.B. über das Skript und die Übungsblätter). Außerdem kann es je nach Kenntnisstand sinnvoll sein, nochmal an den Übungen oder der Vorlesung teilzunehmen.

Falls Sie an den Übungen teilnehmen möchten, ohne dass Ihre Lösungen korrigiert werden sollen, schreiben Sie bitte eine email an Franziska Hofmann (franziska2.hofmann@mathematik.uni-r.de) mit Ihren Wunschterminen (damit die Übungsgruppen einigermaßen gleichmäßig besucht sind).

Ansprechpartner.

- Bei Fragen zur Organisation des Übungsbetriebs wenden Sie sich bitte an Franziska Hofmann (franziska2.hofmann@mathematik.uni-r.de).
- Bei Fragen zu den Übungsaufgaben wenden Sie sich bitte an Ihren Übungsleiter oder fragen Sie in der Zentralübung.
- Bei mathematischen Fragen zur Vorlesung wenden Sie sich bitte an Ihren Übungsleiter, an Franziska Hofmann oder an Clara Löh.
- Bei Fragen zur Planung Ihres Studiums bzw. zur Prüfungsordnung wenden Sie sich bitte an die zuständige Studienberatung, die Studiengangskoordination oder das zuständige Prüfungsamt.
- Bei vielen Fragen kann Ihnen auch die Fachschaft weiterhelfen:

https://www.uni-regensburg.de/studium/fachschaft-mathe-physik/startseite/index.html

Algebra: Üben

Prof. Dr. C. Löh/F. Hofmann Oktober 2025

Wissen, Verstehen, Üben

Wissen, Verstehen, Üben bedingen und verstärken sich gegenseitig. Insbesondere hilft das Üben dabei, Wissen, Verständnis und spezifische Beweis-, Rechen- und Problemlösetechniken zu automatisieren. Diese Automatisierung ist für das Lösen komplexerer Probleme unerlässlich und gibt den Freiraum für die Entwicklung mathematischer Kreativität.

Üben Sie jeden Tag ein bisschen; es ist besser, jeden Tag eine Stunde Algebra zu üben als einmal in der Woche viele Stunden am Stück!

Ziel der Übungsaufgaben ist, sich aktiv mit den behandelten Definitionen, Sätzen, Beispielen und Beweistechniken auseinanderzusetzen und zu lernen, damit umzugehen. Insbesondere ist der Weg das Ziel: Es ist wertvoller, eigenständig eine Aufgabe suboptimal zu bearbeiten als eine korrektere Lösung von anderen zu übernehmen. Nutzen Sie den Luxus, dass Sie für Ihre Abgaben *individuelle* Rückmeldung erhalten!

Das Punkteminimum für die Studienleistung ist das *Minimum*. Sie sollten versuchen, möglichst viele Punkte zu erreichen und nicht nach Erreichen dieser Minimalzahl die Übungen schleifen lassen!

Tag 0: Das neue Übungsblatt

- Beginnen Sie mit der Bearbeitung des Übungsblattes an dem Tag, an dem das Übungsblatt erscheint – manche Dinge brauchen einfach ein paar Tage Zeit.
- Lesen Sie sich alle Aufgaben gründlich durch.
- Kennen Sie die auftretenden Begriffe? Wenn nicht: Nachschlagen/Merken!
- Verstehen Sie, was in der Aufgabe verlangt wird? Insbesondere: Was ist gegeben? Was ist zu tun/zeigen? Welche Ansätze kommen für die Lösung strukturell in Frage?
- Gibt es Sätze/Beispiele aus der Vorlesung, die auf diese Situation passen?
- Welche Lösungsstrategien bzw. Beweisstrategien passen auf die Aufgabe? Kann man einfach direkt mit den Definitionen arbeiten und so zum Ziel gelangen?
- Ist die Aufgabe plausibel? Versuchen Sie, die behaupteten Aussagen an einfachen Beispielen nachzuvollziehen!
- Falls Sie die Aufgabe unplausibel finden, können Sie versuchen, sie zu widerlegen und untersuchen, woran dieses Vorhaben scheitert.
- Kann man die Situation durch eine geeignete Skizze graphisch darstellen?

Tägliche Routine

- Schaffen Sie ein Umfeld, in dem Sie konzentriert, produktiv, ablenkungsfrei (Mobiltelefon?!) und ergonomisch arbeiten können.
- Überlegen Sie sich, woran Sie arbeiten möchten bzw. welche Ziele Sie in dieser Übeeinheit erreichen möchten.
- Beginnen Sie zum „Aufwärmen“ mit einfachen Dingen. Zum Beispiel mit dem Lernen von in der Vorlesung behandelten Begriffen/Sätzen, mit den Fingerübungen auf den Übungsblättern oder mit den Fragen/Beispielen im Skript.
- Bearbeiten Sie dann die Aufgaben auf dem Übungsblatt.

  Verwenden Sie viel Schmierpapier und geben Sie sich genug Zeit, an der Aufgabe herumzuexperimentieren! Selbst wenn Sie die Aufgabe nicht vollständig oder nicht korrekt lösen, werden Sie auf diese Weise viel lernen, da Sie sich aktiv mit dem Material auseinandersetzen.

  Wenn Sie nicht weiterwissen, diskutieren Sie die Aufgabe mit Kommilitonen oder verwenden Sie Literatur. Lassen Sie sich aber auf keinen Fall dazu verleiten, einfach Lösungen irgendwo abzuschreiben, K„I“-Systemen blind zu vertrauen oder ausschließlich in Gruppen zu arbeiten. Mathematik kann man nur lernen, wenn man aktiv damit arbeitet und seine Gedanken selbst formuliert!

  Notieren und sammeln Sie Ihre Fragen. Können Sie Ihre Fragen vom Vortag beantworten? Woran möchten Sie am nächsten Tag weiterarbeiten?
- Planen Sie Pausen ein (mental und physisch).
- Beenden Sie Ihre Übeeinheit mit einem Aspekt von Mathematik, der Ihnen uneingeschränkt Spaß macht. Zum Beispiel mit ergänzender Literatur/ergänzenden digitalen Angeboten, mit mathematischen Rätseln, Cartoons, Spielen ... Für Lehramtskandidaten: (wie) könnte das Gelernte in der Schule eingesetzt werden?

Aufschreiben von Lösungen

- Lesen Sie die Korrektur Ihrer vorigen Übungsblätter. Was können Sie für die aktuelle Abgabe daraus lernen?
- Auch wenn Sie in einer größeren Gruppe kooperiert haben: Schreiben Sie Ihre Lösungen selbständig auf.
- Gliedern Sie Ihre Lösung sauber in Voraussetzung, Behauptung und Beweis. Passt dies mit der Aufgabe zusammen?
- Teilen Sie Ihre Beweise in sinnvolle Zwischenschritte auf (auch optisch!).
- Achten Sie darauf, dass Sie verständlich formulieren und dass die Argumente logisch aufeinander aufbauen.
- Ist Ihre Argumentationskette wirklich lückenlos? Seien Sie misstrauisch gegenüber Ihrer eigenen Lösung und versuchen Sie, alle potentiellen Schwachpunkte ausfindig zu machen!

- Wenn Sie einzelne Beweisschritte nicht vollständig durchführen können, können Sie in Ihrer Lösung darauf hinweisen – die restliche Lösung kann trotzdem Punkte erhalten.
- Achten Sie darauf, dass Sie alle Bezeichner einführen und dass Sie mathematische Symbole und Fachbegriffe korrekt verwenden.
- Versuchen Sie, sich so präzise wie möglich auszudrücken.
- Versuchen Sie, indirekte Argumente so weit wie möglich zu vermeiden.
- Überprüfen Sie am Ende, ob Sie wirklich das bewiesen haben, was Sie ursprünglich behauptet haben.
- Oft ist es auch hilfreich zu überprüfen, ob/wie alle in der Aufgabe gegebenen Voraussetzungen verwendet wurden.
- Würden Sie Ihre Lösung verstehen, wenn Sie sie zum ersten Mal lesen würden?
- Alles, was Sie abgeben, müssen Sie eigenständig formuliert und auch verstanden haben.
- Geben Sie Literaturangaben an, wenn Sie zusätzliche Quellen verwendet haben.
- Teilen Sie Ihre Lösungen vor dem Abgabetermin *nicht* auf sozialen Netzwerken etc. mit den anderen Teilnehmern der Vorlesung. Nichts ist demotivierender, als eine Aufgabe zu bearbeiten, für die bereits Lösungen offen kursieren. Es spricht aber natürlich nichts dagegen, konkrete Fragen anderer Teilnehmer zu beantworten.

Tag $n-1$: Checkliste vor der Abgabe

- Verstehen Sie Ihre Lösung immer noch?
- Bei jeder Aufgabe: Lösung sauber strukturiert?

  Insbesondere (fast immer): Voraussetzung, Behauptung, Beweis!
- Name(n) auf der Abgabe?

  Nummer der Übungsgruppe auf der Abgabe?
- Können alle Autoren die abgegebenen Lösungen vorstellen?
- Achten Sie bitte auf gute Lesbarkeit und Verständlichkeit;
  lassen Sie genug Platz für Korrekturanmerkungen.
- Papierabgabe:
  - Blätter im A4-Format?
  - Blätter zusammengetackert?
    Bitte keine Umschläge, Hefter, ... verwenden!
  - In den richtigen Briefkasten einwerfen!

- Digitale Abgabe:
  - Abgabe nur im pdf-Format möglich
  - Bei gescannten Lösungen: Lesbarkeit?!

Bewertungskriterien

- Wurden Voraussetzung, Behauptung, Beweis deutlich gekennzeichnet und voneinander getrennt?
- Stimmen die Voraussetzungen? Sind sie sauber formuliert?
- Stimmen die Behauptungen/Zwischenbehauptungen? Sind sie sauber formuliert?
- Ist die Argumentationskette der Beweisschritte vollständig?
- Sind die Beweisschritte präzise formuliert und verständlich?
- Sind alle Bezeichner eingeführt?
- Werden mathematische Symbole und Fachbegriffe korrekt eingesetzt?
- Ist an jeder Stelle des Beweises klar, was passiert?
- Werden die neu erlernten Begriffe und Techniken passend eingesetzt?
- Wurde die gestellte Aufgabe vollständig gelöst?
- Falls Lösungen abgeschrieben wurden und dies von den Übungsleitern entdeckt wird, erhalten Sie auf diese Aufgaben keine Punkte. Mal abgesehen davon, dass es weder sinnvoll noch fair ist, abzuschreiben.

Fehlerkultur

Fehler sind ein natürlicher und wichtiger Bestandteil in jedem Lernprozess. Sie bieten gute Gelegenheiten, ein besseres Verständnis zu erlangen.

- Haben Sie keine Angst vor Fehlern!
- Langfristig sollen Fehler minimiert werden. Kurzfristig sind sie aber hilfreich beim Lernen, da sie die Grenze zwischen „korrekt“ und „inkorrekt“ deutlicher hervortreten lassen.
- Wichtig ist, dass Sie nach der Korrektur/Diskussion verstehen, warum ein Fehler vorliegt und wie man ihn beheben kann.

  Insbesondere: Schauen Sie sich die Korrekturen Ihrer Übungsabgaben genau an. Nutzen Sie diese individuelle Rückmeldung zu Ihrem aktuellen Stand!
- Fehler sollten nach Möglichkeit nicht wiederholt werden.
- Falls Sie Fehler in der Vorlesung oder auf den Übungsblättern entdecken, geben Sie bitte Franziska Hofmann oder Clara Löh Bescheid.

Übungsgruppe

Ziel der Übungsgruppen ist nicht nur die Rückgabe der Korrekturen und das Besprechen von Lösungen. Sie sollen lernen, mathematisch zu diskutieren, Strategien zur Problemlösung zu finden/anzuwenden, und Sie sollen lernen, mathematische Fehler zu erkennen bzw. zu beheben.

- Beantwortung von Fragen zur Vorlesung und zu den Übungsaufgaben.

  Bereiten Sie sich entsprechend vor, sammeln Sie Ihre Fragen und stellen Sie diese während des Übungstermins.

- Bearbeitung (einer Auswahl) von Fingerübungen auf den Übungsblättern.

  Bereiten Sie sich darauf vor, indem Sie die Aufgaben beim täglichen Üben anschauen bzw. bearbeiten. Fragen Sie, wenn Sie Schwierigkeiten bei diesen Aufgaben haben!

- Besprechung von Lösungen der korrigierten Aufgaben.

  Im Normalfall sollen die Teilnehmer vorrechnen! Haben Sie keine Angst, eine Aufgabe vorzurechnen. Auch dann nicht, wenn Ihre Lösung nicht ganz richtig oder vollständig ist. Die Übungsgruppe ist *keine* Prüfung und *keine* Verkündung von „Musterlösungen“, sondern eine Gelegenheit, Mathematik und Kommunikation von Mathematik gemeinsam zu üben.

Zentralübung

Die Zentralübung bietet die Gelegenheit, Fragen zu stellen, den Stoff der Vorlesung zu wiederholen und weitere Beispiele zu behandeln.

- Bereiten Sie sich darauf vor, indem Sie im Voraus Fragen sammeln.
- Sie können auch das anonyme Frageforum in GRIPS nutzen, um Fragen vorab zu stellen (bzw. gegebenenfalls direkt Antworten zu erhalten).
- Die Zentralübung lebt von Ihren Fragen. Haben Sie keine Angst, Fragen zu stellen. Je mehr verschiedene Teilnehmer Fragen stellen, desto mehr interessante und hilfreiche Blickwinkel ergeben sich.

Viel Erfolg und viel Spaß bei den Übungen!

Algebra:
Hinweise zur Prüfungsvorbereitung

Prof. Dr. C. Löh/F. Hofmann Oktober 2025

Ziel der Prüfungsvorbereitung

Hauptziel der Prüfungsvorbereitung ist die souveräne Beherrschung des behandelten Fachgebiets. Die Prüfung sichert ab, dass dies tatsächlich der Fall ist, ist aber nicht das eigentliche inhaltliche Ziel der Vorlesung/Übungen. Beherrscht werden sollten also:

- aktive Kenntnis der Fachbegriffe und Formalisierungsmethoden
- Verständnis der Ideen, die zu diesen Fachbegriffen und Formalisierungen führen
- wichtige Probleme und Fragestellungen, die das Gebiet maßgeblich beeinflusst haben bzw. die durch das Gebiet gelöst werden können
- wichtige Resultate und Zusammenhänge innerhalb des Gebiets
- wichtige Beweis- und Lösungsstrategien
- repräsentative Beispiele
- Anwendungen des Gebiets und Interaktion mit anderen Gebieten
- Fähigkeit, auf all diesen Kenntnissen weiter aufzubauen.

Insbesondere müssen Definitionen und Sätze inhaltlich präzise und vollständig reproduziert werden können, inklusive aller Voraussetzungen, Quantoren, ... Es genügt *nicht*, nur eine vage Vorstellung des Inhalts der Definitionen und Sätze zu haben.

Erreichen dieses Ziels

Während der Vorlesungszeit:

- aktive Auseinandersetzung mit den Übungsaufgaben
- Erlernen des Fachwissens (Definitionen, Sätze), notfalls mit Karteikarten
- Sortierung des Materials in zentrale/wichtige Dinge und eher unwichtige; diese Priorisierung beim Lernen berücksichtigen
- weiteres aktives Üben mit zusätzlichen Aufgaben und Vertiefung der Kenntnisse durch Selbststudium (Bibliothek und Computer-Werkzeuge)
- Bei Fragen: Betreuungsangebote nutzen!

Es ist viel einfacher, sich Definitionen, Sätze und Beweise inhaltlich präzise zu merken, wenn man sie und die unterliegenden Ideen genau verstanden hat. Lernen mit Verständnis ist daher viel effizienter, robuster und flexibler als Lernen ohne Verständnis.

Während der gezielten Prüfungsvorbereitung:

- Wiederholung und Festigung des gelernten Fachwissens
- weiteres aktives Üben
- Zusammenfassung der wichtigsten Inhalte der Vorlesung auf wenigen Seiten (es geht darum, selbst eine Zusammenfassung zu erstellen, *nicht* eine solche von jemand anderem auswendig zu lernen!)
- Bei Fragen: Kommilitonen oder Studenten aus höheren Semestern ansprechen
- Pausen einplanen
- *nicht* erst nach der vorigen Prüfung mit der Vorbereitung auf die nächste Prüfung beginnen

Kurz vor der Prüfung:

- Kann ich mein Wissen präzise, verständlich und flüssig schriftlich bzw. mündlich präsentieren? (Das kann man einfach an anderen Kommilitonen ausprobieren ...)
- Was könnten typische Prüfungsfragen sein? Was sind gute Lösungen zu diesen Fragen? (Dabei können insbesondere Probeklausuren, Altklausuren und Gedächtnisprotokolle von Prüfungen hilfreich sein.)
- Wie belastbar sind meine Fähigkeiten? Was muss ich noch verbessern?
- Bei Fragen: Kommilitonen oder Studenten aus höheren Semestern ansprechen

Im Falle einer Wiederholungsprüfung:

- kritisch hinterfragen, was bei der Vorbereitung für den vorigen Prüfungsversuch suboptimal gelaufen ist; Lernstrategie und Lernorganisation entsprechend anpassen

Bewertungskriterien

In der Prüfung werden folgende Fähigkeiten abgeprüft:

- Fachwissen (Definitionen, Sätze, Beweise, Beispiele, Anschauung, Zusammenhänge, Anwendungen, ...)
- präzises und korrektes, logisch schlüssiges, Formulieren und Argumentieren
- Lösen von Standardproblemen
- Kreativität bei der Lösung von Problemen

Es gelten sinngemäß dieselben Grundsätze wie beim Aufschreiben/Präsentieren von Lösungen in Übungsgruppen und wie bei der Bewertung von Abgaben zu Übungsblättern:

- https://loeh.app.ur.de/teaching/algebra_ws2526/ueben.pdf
- https://loeh.app.ur.de/teaching/linalg1_ws2425/richtungen.pdf

Konkrete Hinweise

Definitionen:

- Was sind die Voraussetzungen?
- Welcher Begriff wird definiert?
- Warum genau so und nicht anders? (Beispiele, Zusammenhang mit anderen Definitionen, weitere Verwendung in der Theorie und in Anwendungen)
- Was sind Beispiele, die die Definition erfüllen? (Sowohl einfache als auch komplexere)
- Was sind Beispiele, die die Definition nicht erfüllen? (Sowohl einfache als auch komplexere)

Sätze, Propositionen, etc.:

- Was sind die Voraussetzungen?
- Was wird behauptet?
- Warum genau so und nicht anders? (Beispiele, Zusammenhang mit anderen Resultate, weitere Verwendung in der Theorie und in Anwendungen)
- Was passiert, wenn nicht alle Voraussetzungen erfüllt sind?
- Was sind einfache konkrete Beispiele, auf die dieser Satz angewendet werden kann? Was liefert der Satz in diesem Fall?
- Was sind wichtige weitere Anwendungen dieses Satzes?
- In welchen zentralen Beweisen wird dieser Satz verwendet?
- Wie kann man den Satz beweisen?

Beweise:

- Was ist die unterliegende Idee? Was ist die unterliegende Struktur?
- Was ist speziell/interessant an diesem Beweis?
- Benötigt der Beweis einen Trick?
- Gibt es weitere Sätze, die mit einer ähnlichen Technik bewiesen werden?
- Ginge das nicht auch einfacher?! Falls ja: prima! Falls nein: Warum nicht?
- Welche Hilfsmittel/vorigen Resultate gehen in diesen Beweis ein?
- Können Sie den Beweis kurz zusammenfassen? Können Sie ihn dann wieder zu einem vollständigen Beweis auffüllen?

Staatsexamen?!

Falls Sie auf Lehramt Gymnasium studieren: Sie werden im ersten Staatsexamen unter anderem eine Klausur zur Algebra schreiben. Thema sind Gruppen, Ringe, Körper und insbesondere Galoistheorie (wie in der Vorlesung Algebra behandelt), sowie Grundkenntnisse der Linearen Algebra I/II.

Ziel der Staatsexamenskurse ist

- *nicht* die Vermittlung des Vorlesungsstoffes der Algebra (bzw. Linearen Algebra I/II). Diesen sollten Sie in dem Semester lernen, in dem Sie die Vorlesung Algebra (bzw. Lineare Algebra I/II) besuchen und vor dem Staatsexamenskurs kurz auffrischen,
- sondern das Üben der Klausursituation anhand von Originalaufgaben aus den vorigen Staatsexamensklausuren.

Viel Erfolg bei der Prüfung!

Literaturverzeichnis

Bitte beachten Sie, dass das Literaturverzeichnis im Laufe der Vorlesung wachsen wird und sich daher auch die Nummern der Quellen ändern werden!

[1] M. Agrawal, N. Kayal, N. Saxena. PRIMES is in P, *Ann. of Math. (2)*, 160(2), pp. 781–793, 2004. Cited on page: 109

[2] M. Aigner, G.M. Ziegler, *Proofs from The Book*, dritte Auflage, Springer, 2004. Cited on page: 100

[3] W.R. Alford, A. Granville, C. Pomerance. There are infinitely many Carmichael numbers, *Ann. of Math. (2)*, 139(3), pp. 703–722, 1994. Cited on page: 109

[4] M. Aschbacher. The Status of the Classification of the Finite Simple Groups, *Notices of the American Mathematical Society*, 51(7), pp. 736–740, 2004. Cited on page: 64

[5] ATLAS of finite group representations, version 3. http://brauer.maths.qmul.ac.uk/Atlas/v3/ Cited on page: 64

[6] S. Bosch. *Algebra*, sechste Auflage, Springer Spektrum, 2006. Cited on page: 106, 125, 132, 158, 184, 185, 190

[7] K.S. Brown. *Cohomology of Groups*, Graduate Texts in Mathematics, 87, Springer, 1982. Cited on page: 42

[8] D. Bump. *Lie Groups*, Graduate Texts in Mathematics, 225, zweite Auflage, Springer, 2013. Cited on page: 80

[9] P.J. Cameron. *Sets, Logic and Categories*, Universitext, Springer, 1998. Cited on page: A.6

[10] A. Crans, T. Fiore, R. Satyendra. Musical Actions of Dihedral Groups, *American Mathematical Monthly* 116(6), S. 479–495, 2009. Cited on page: 45

[11] B. Conrad. Impossibility theorems for elementary integration, http://www2.maths.ox.ac.uk/cmi/library/academy/LectureNotes05/Conrad.pdf Cited on page: 189

[12] D.A. Cox. *Galois Theory*, Wiley, 2004. Cited on page: 192

[13] D.M. Evans, Z. Ghadernezhad, K. Tent. Simplicity of the automorphism groups of some Hrushovski constructions, *Ann. Pure Appl. Logic* 167(1), S. 22–48, 2016. Cited on page: 64

[14] W. Feit, J.G. Thompson. A solvability criterion for finite groups and some consequences, *Proc. Nat. Acad. Sci. U.S.A.* 48, S. 968–970, 1962. Cited on page: 70

[15] E. Freitag, R. Busam. *Funktionentheorie 1*, vierte Auflage, Springer, 2006. Cited on page: 101

[16] U. Friedrichsdorf, A. Prestel. *Mengenlehre für den Mathematiker*, Vieweg, 1985. Cited on page: A.6

[17] G. Gonthier, A. Asperti, J. Avigad et al.. A machine-checked proof of the odd order theorem, *Interactive theorem proving*, S. 163–179, *Lecture Notes in Comput. Sci.* 7998, Springer, 2013. Cited on page: 70

[18] K. Jänich. *Lineare Algebra*, 11. Auflage, Springer, 2013. Cited on page: 58

[19] C. Löh. *Geometrie (Lehramt Gymnasium)*, Vorlesungsskript, SS 2023, Universität Regensburg, 2023. Cited on page: 17, A.28

[20] C. Löh. *Geometric Group Theory, an Introduction*, Universitext, Springer, 2018. Cited on page: 26, 37, 42, A.10

[21] C. Löh. *Algebraic Topology*, Vorlesungsskript, WS 2021/22, Universität Regensburg, 2022. Cited on page: 175

[22] Falko Lorenz. *Einführung in die Algebra I*, dritte Auflage, Spektrum Akademischer Verlag, 1996. Cited on page: 80

[23] S. MacLane. *Categories for the Working Mathematician*, zweite Auflage, Springer, 1998. Cited on page: A.6

[24] B.C. Pierce. *Basic Category Theory for Computer Scientists*, MIT Press, 1991. Cited on page: A.6

[25] R.L. Rivest, A. Shamir, L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2), pp. 120–126, 1978. Cited on page: 110, 112

[26] M. Rosenlicht. Integration in finite terms, *The American Mathematical Monthly*. 79(9), pp. 963–972, 1972. Cited on page: 189

[27] Joseph J. Rotman. *An Introduction to the Theory of Groups*, Graduate Texts in Mathematics, 148, vierte Auflage, Springer, 1995. Cited on page: 26, 64, 66

[28] S. Singh. *Fermat's Last Theorem*, Fourth Estate Ltd., 1997. Cited on page: 112

[29] R.M. Smullyan, M. Fitting. *Set theory and the continuum problem*, überarbeitete Auflage, Dover, 2010. Cited on page: A.6

[30] M. Spivak. *Calculus*, dritte Auflage, Cambridge University Press, 2006. Cited on page: 140

[31] L.C. Washington. *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, 83, Springer, 1982 Cited on page: 182

Deutsch → English

A

Abelianisierung	abelianisation	66
abelsch	abelian	12
abgeleitete Gruppe	derived (sub)group	67
Absolutbetrag	absolute value	A.4
algebraisch abgeschlossen	algebraically closed	A.2
algebraischer Abschluss	algebraic closure	156
allgemeine lineare Gruppe	general linear group	16
auflösbar durch Radikale	solvable by radicals	182
auflösbare Gruppe	solvable group	65
Automorphismus	automorphism	16

B

Bahnengleichung	orbit-stabiliser theorem	49
Bewertung	valuation	114
Bild	image	13

D

Diedergruppe	dihedral group	39

E

einfache Gruppe	simple group	62
endlich erzeugt	finitely generated	24
Erzeugendensystem	generating set	24
erzeugte Untergruppe	generated subgroup	24
euklidischer Ring	euclidean ring	A.21

F

faktorieller Ring	unique factorisation domain (UFD)	112
formale Ableitung	formal derivative	162
freie Gruppe	free group	A.9
Funktionenkörper	function field	90

G

Galoiserweiterung	Galois extension	163
Galoisgruppe	Galois group	17
gerade Permutation	even permutation	59
größter gemeinsamer Teiler	greatest common divisor (gcd)	97
Grad	degree	136
Gruppe	group	7
Gruppenerweiterung	group extension	35
Gruppenoperation	group action	42

H

Hauptideal	principal ideal	97
Hauptidealring	principal ideal domain (PID)	97

I

Ideal	ideal	91
imaginäre Einheit	imaginary unit	A.3
Imaginärteil	imaginary part	A.3
Index	index	21
innerer Automorphismus	inner automorphism	18
Integritätsring	integral domain	84
invertierbar	invertible	8
Isometriegruppe	isometry group	16

K

Kategorie	category	A.6
Kern	kernel	13
Kette	necklace	51
kleinstes gemeinsames Vielfaches	least common multiple (lcm)	97
Kommutator	commutator	65
Kommutatoruntergruppe	commutator subgroup	65
komplexe Konjugation	complex conjugation	A.5
Koprodukt	coproduct	36
Körpererweiterung	field extension	133
Kreisteilungskörper	cyclotomic field	178

L

Linksnebenklasse	left coset	20
Linkstranslationsoperation	left translation action	44

M

Monoid	monoid	8
Monoidhomomorphismus	monoid homomorphism	10

N

Nebenklasse	coset	20
Normalisator	normaliser	79
Normalreihe	normal series	69
Normalreihe mit abelschen Faktoren	normal series with Abelian factors	69
Normalteiler	normal subgroup	27
Nullstelle	zero	86

O

Orbit	orbit	47
orthogonale Gruppe	orthogonal group	17

P

Polynomdivision	polynomial long division	A.21
Polynomfunktion	polynomial function	86
Polynomring	polynomial ring	85
primitives Polynom	primitive polynomial	118
Primkörper	prime field	130

Q

Quotientenkörper	field of fractions	89

R

Realteil	real part	A.3
Rechtsnebenklasse	right coset	20
Ring	ring	81

S

semi-direktes Produkt	semi-direct product	37
separabel	separable	166
signum	sign	59
Spalt	section	38
spezielle lineare Gruppe	special linear group	16
Stabilisator	isotropy group	47
Stabilisator	stabiliser	47
Sylowsätze	Sylow theorems	70

T

triviale Gruppe	trivial group	15

U

ungerade Permutation	odd permutation	59
Untergruppe	subgroup	19

W

Wortproblem	word problem	25

Z

Zentralisator	centraliser	52
Zentrum	centre	52
Zerfällungskörper	splitting field	149
Zykel	cycle	57
zyklische Gruppe	cyclic group	24

English → Deutsch

A

abelian	abelsch	12
abelianisation	Abelianisierung	66
absolute value	Absolutbetrag	A.4
algebraic closure	algebraischer Abschluss	156
algebraically closed	algebraisch abgeschlossen	A.2
automorphism	Automorphismus	16

C

category	Kategorie	A.6
centraliser	Zentralisator	52
centre	Zentrum	52
commutator	Kommutator	65
commutator subgroup	Kommutatoruntergruppe	65
complex conjugation	komplexe Konjugation	A.5
coproduct	Koprodukt	36
coset	Nebenklasse	20
cycle	Zykel	57
cyclic group	zyklische Gruppe	24
cyclotomic field	Kreisteilungskörper	178

D

degree	Grad	136
derived (sub)group	abgeleitete Gruppe	67
dihedral group	Diedergruppe	39

E

euclidean ring	euklidischer Ring	A.21

even permutation	gerade Permutation	59

F

field of fractions	Quotientenkörper	89
finitely generated	endlich erzeugt	24
formal derivative	formale Ableitung	162
free group	freie Gruppe	A.9
function field	Funktionenkörper	90

G

Galois extension	Galoiserweiterung	163
Galois group	Galoisgruppe	17
general linear group	allgemeine lineare Gruppe	16
generated subgroup	erzeugte Untergruppe	24
generating set	Erzeugendensystem	24
greatest common divisor (gcd)	größter gemeinsamer Teiler	97
group	Gruppe	7
group action	Gruppenoperation	42
group extension	Gruppenerweiterung	35

I

ideal	Ideal	91
image	Bild	13
imaginary part	Imaginärteil	A.3
imaginary unit	imaginäre Einheit	A.3
index	Index	21
inner automorphism	innerer Automorphismus	18
integral domain	Integritätsring	84
invertible	invertierbar	8
isometry group	Isometriegruppe	16
isotropy group	Stabilisator	47

K

kernel	Kern	13

L

least common multiple (lcm)	kleinstes gemeinsames Vielfaches	97
left coset	Linksnebenklasse	20
left translation action	Linkstranslationsoperation	44

M

monoid	Monoid	8
monoid homomorphism	Monoidhomomorphismus	10

N

necklace	Kette	51
normal series	Normalreihe	69

normal series with Abelian factors	Normalreihe mit abelschen Faktoren	69
normal subgroup	Normalteiler	27
normaliser	Normalisator	79

O

odd permutation	ungerade Permutation	59
orbit	Orbit	47
orbit-stabiliser theorem	Bahnengleichung	49
orthogonal group	orthogonale Gruppe	17

P

polynomial function	Polynomfunktion	86
polynomial long division	Polynomdivision	A.21
polynomial ring	Polynomring	85
prime field	Primkörper	130
primitive polynomial	primitives Polynom	118
principal ideal	Hauptideal	97
principal ideal domain (PID)	Hauptidealring	97

R

real part	Realteil	A.3
right coset	Rechtsnebenklasse	20
ring	Ring	81

S

section	Spalt	38
semi-direct product	semi-direktes Produkt	37
separable	separabel	166
sign	signum	59
simple group	einfache Gruppe	62
solvable by radicals	auflösbar durch Radikale	182
solvable group	auflösbare Gruppe	65
special linear group	spezielle lineare Gruppe	16
splitting field	Zerfällungskörper	149
stabiliser	Stabilisator	47
subgroup	Untergruppe	19
Sylow theorems	Sylowsätze	70

T

trivial group	triviale Gruppe	15

U

unique factorisation domain (UFD)	faktorieller Ring	112

V

valuation	Bewertung	114

W

word problem	Wortproblem	25

Z

zero	Nullstelle	86

Index

Symbole

14/15-Puzzle, 2, 61, B.10

A

Abelianisierung, 66
    universelle Eigenschaft, 66
abelsch, 12
abelsche Erweiterung, 182
abelsche Gruppe
    Klassifikation endlicher, 54
Ableitung, 162
Ableitungskriterium, 162, B.27
Absolutbetrag, A.4
Adjunktion, 134
Adventskalender, B.16
affine Gerade, 24
affiner Unterraum, 24
Algebra
    Anwendungen, 2
    warum?, 1
algebraisch, 140, B.25
algebraisch abgeschlossen, 156, A.2
algebraische Erweiterung, B.25
algebraische Geometrie, 94
algebraische Körpererweiterung, 147
algebraische Zahl, 140, B.25
algebraischer Abschluss, 156
    von endlichen Körper, 163
Algorithmus
    euklidischer, A.25
    Polynomdivision, A.21
allgemeine lineare Gruppe, 16
alternierende Gruppe, 28
    Auflösbarkeit, 68
    Einfachheit, 63
    Erzeugendensystem, 61
Answendung
    Konstruierbarkeit mit Zirkel und Lineal, 189
Anwendung
    Auflösbarkeit durch Radikale, 182, B.31
    endliche Körper, A.32
    Galoistheorie, 178
    Konstruktion mit Zirkel und Lineal, B.31
arithmetic overflow, 93
assoziiert, 96
asymmetrische Verschlüsselung, 110
auflösbar
    durch Radikale, 182
auflösbare Gruppe, 65, 67, B.12
    alternierende Gruppe, 68
    Normalreihe, 69

p-Gruppe, 71
symmetrische Gruppe, 68
Vererbungseigenschaften, 67
Auflösbarkeit durch Radikale, 182, B.31
Auflösung durch Radikale, 2
auflösbare Gruppe, 69
Automorphismengruppe, 16, 17, 44
in Kategorien, 18
Automorphismus
innerer, 18
von Gruppen, 17, B.1
Automrphismengruppe, A.8

B

Bahn, 48, B.8
Bahnengleichung, 49, B.8
Bahnenraum, 48
Beweis
formalisiert/verifiziert, A.13
Bewertung, 114, 115, B.18
Bewertungstest, 116
Bibliothek, 5, 58
Bild
eines Gruppenhomomorphismus, 13, 15
Ringhomomorphismus, 91
Blorx, B.16
Blorxchester, B.20
Bruch, 89
bubble sort, 58
byte, A.33

C

Carmichael-Zahl, 109
Cauchy
Satz von, 73
Cayley
Satz von, 47
Cayleygraph, 26
Charakteristik, 130, B.23
Chinesischer Restsatz, 104, B.16
Computeralgebrasystem, B.8

D

Determinante, 16, 31
Dezimaldarstellung
Ziffer, B.18
Diedergruppe, 39, B.10
Musik, 44
Division mit Rest, A.21
doppeltes Abzählen, 50
Duelle, 170

E

effektiv, 183
einfache Gruppe, 62, 63
alternierende Gruppe, 63
Einheit, 96
Einheitengruppe, 96, 132
Einheitskreis, 31
Einheitswurzel, 143, 178, 180, 181, B.27
primitiv, 144
primitive, 185
Eisen-Stein, B.21
Eisensteinsches Irreduzibilitätskriterium, 124
elementare Zahlentheorie, 93
endlich erzeugt
Gruppe, 25
endlich erzeugte Körpererweiterung, 136
endliche abelsche Gruppe, 54, B.8
endliche Gruppe
abelsche, 54, B.8
Struktur, 53
endliche Körper, 103
Anwendung, A.32
endliche Körpererweiterung, 136
endlicher Körper, 160, B.29
Einheitengruppe, 132
Klassifikation, 160
Körpererweiterungen, 163
erster Isomorphiesatz, 34
Erweiterung, 35
Erzeugendensystem
alternierende Gruppe, 61
frei, A.10
symmetrische Gruppe, 58

von Gruppen, 25
erzeugte Untergruppe, 24
explizite Beschreibung, 25
erzeugter Zwischenkörper, 134
erzeugtes Ideal, 91
euklidische
Isometriegruppe, 40
euklidische Gradfunktion, A.21
euklidischer Algorithmus, A.25, B.16
euklidischer Ring, A.21
eulersche φ-Funktion, 109

F

Faktoren
einer Normalreihe, 69
faktorieller Ring, 112
Feit–Thompson Theorem, 70
Fermat
großer Satz, 112
kleiner Satz, 106, 110
kleiner Satz von Fermat, B.18
Fixkörper, 171, B.31
Fixpunktmenge, 48
formale Ableitung, 162
formalisierter Beweis, A.13
Formalisierung, B.6
freie Gruppe, A.9, B.4
freie Gruppenoperation, 45
freies Erzeugendensystem, A.9
Frobeniusendomorphismus, 160, B.23
Fundamentalsatz der Algebra, 192
Funktionenkörper, 90
Funktionenring, B.14
Funktor
Tensorprodukt, A.38

G

Galois, 170
Galoiserweiterung, 163, 164, 170
Fixkörper, 172
Grad, 171
Galoisgruppe, 17, 138, B.31
einer Gleichung, 155
Fixkörper, 172
Größe, 171
induktive Berechnung, 177
Realisierung als, 173, 181
Galoistheorie
Anwendungen, B.31
Hauptsatz, 164, 173
kategoriell, 176
GAP, B.8
Gauß
Lemma von, 116
Satz von, 115
Gaußsche ganze Zahlen, 83
Geometrische Gruppentheorie, 26
Gerade
affin, 24
gerade Permutation, 59, 60
ggT, 97, A.25, B.16
Gleichung
Galoisgruppe, 155
Goethe, B.18
Grad einer Körpererweiterung, 136
Gradfunktion
euklidische, A.21
großer Satz von Fermat, 112
größter gemeinsamer Teiler, 97, 114, A.25
Gruppe, 7, 12, B.4
Abelianisierung, 66
abelsch, 12
abelsche, 54
allgemeine lineare, 16
als Automorphismengruppe, 18
als Kategorie, A.7
alternierende, 28
auflösbar, 65, 67, 69, B.12
Automorphismengrupe, 16
Automorphismus, B.1
Cayleygraph, 26
Dieder-, 39
Diedergruppe, B.10
einfach, 62, 63
endlich erzeugt, 25
endliche abelsche, 54, B.8
Erweiterung, 35
Erzeugendensystem, 25

für Neandertaler, B.4
frei, A.10
freie, B.4
Galois-, 17
Gruppenoperation, 42
Homomorphismus, B.1
Isometrie-, 16
Isometriegruppe, 24
Kommutator, 65, 66
Konjugation, B.8
Koprodukt, 36
Matrixgruppe, 16, B.4
Normalisator, 79
Normalreihe, 69
Normalteiler, 27, B.4
Operation, 44
orthogonale, 17
p-Gruppe, 71
Produkt, 35, 37
Quaternionen, 72
Quotientengruppe, 29, B.6
semi-direktes Produkt, 37, B.6
spezielle lineare, 16
Struktur, 53
Sylowgruppe, 71, B.12
symmetrische, 12, 57, B.8
triviale, 15
Untergruppe, 18, 19, 20, B.1
Verknüpfungstabelle, 13
Wortproblem, 25
Zentralisator, 52
Zentrum, 52
zyklisch, 25, 33
zyklische, 31
Gruppenautomorphismus, 17
Gruppenelement
Konjugationsklasse, 53
Ordnung, 32
Gruppenerweiterung, 41, 62
semi-direktes Produkt, 41
spaltende, B.6
Gruppenhomomorphismus, 12, 13, 14, 15
Bild, 13, 15
Kern, 13, 15
Gruppenisomorphismus, 13, 15
Gruppenkohomologie, 42
Gruppenoperation, 42, 44
Automorphismengruppe, 44
Bahn, 48, B.8
Bahnengleichung, 49, B.8
Bahnenraum, 48
effektiv, 183
explizit, 43
Fixpunktmenge, 48
freie, 45
in der Musik, 44
Isotropiegruppe, 48
Klassengleichung, 53
Konjugationsoperation, 53
Linkstranslation, 44, 47
Orbit, 48
Orbitraum, 48
Rotationsoperation, 46
Rubik's Cube, 46
Stabilisator, 48, B.8
Standgruppe, 48
transitive, 45
trivial, 44
Zählproblem, 51
Gruppoku, B.6

H

Halbgruppe, *siehe* Monoid
Hauptideal, 97
Hauptidealring, 97
nicht euklidisch, A.24
Hauptsatz der Galoistheorie, 164, 173, B.31
Ho-Ho-Ho, B.16
homöomorph, A.8
Homomorphiesatz, 31
für Ringe, 94
Homomorphismus
von Gruppen, 12, 13, 14, 15, B.1
von Monoiden, 8, 10, 11
von Ringen, 83

I

Ideal, 91, B.18
als Kern, 94
erzeugt von, 91
Hauptideal, 97
koprim, 104
maximal, 101
prim, 101
Primideal, B.16
Restklasse, 92
Identitätsmorphismus, A.6
imaginäre Einheit, A.3
Imaginärteil, A.3
Index, B.4
Ideal in Körpern, 91
Untergruppe, 20, 22
innerer Automorphismus, 18
int, 93
Integritätsring, 84, B.14
Inverses, 8
Eindeutigkeit, 10
von Produkten, 10
invertierbar, 8
Irgendwas, 19
irreduzibel, 98, 120, 121, B.21
Irreduzibilitätskriterien, 121
Irreduzibilitätskriterium, B.25
Isometriegruppe, 16, 24
euklidische, 40
Isomorphiesätze
für Ringe, 94
Isomorphiesatz, 34
Isomorphismus, A.8
von Gruppen, 13, 15
Isoomorphismus
von Monoiden, 10, 11
Isotropiegruppe, 48

K

Körper
endlich, 103
kanonische Projektion, 30
Kaplansky-Vermutung, 85
Kartenmischen, B.10
Kategorie, A.6
Automorphismengruppe, 18, A.8
Beispiele, A.7
der Gruppen, 8
der Körper, 130
der Körpererweiterungen, 133, 138
der Mengen, A.7
der Ringe, 82
der topologischen Räume, A.8
der Vektorräume, A.7
Gruppe, A.7
Gruppenoperation, 42
Isomorphismus, A.8
leer, A.7
Morphismus, A.6
Objekt, A.6
Kern
als Ideal, 94
als Normalteiler, 30
eines Gruppenhomomorphismus, 13, 15
Ringhomomorphismus, 91
kgV, 98
Klasse, A.6
Klassengleichung, 53
Klassifikation
zyklischer Gruppen, 33
kleiner Satz von Fermat, 106, 110
kleinstes gemeinsames Vielfaches, 97, 98, 114
kommutativer Ring, 82
Kommutator, 65, 66
Kommutatoruntergruppe, 65, 66
kompelxe Zahlen
Imaginärteil, A.3
komplexe Konjugation, A.5
komplexe Zahlen, 121, A.2
Absolutbetrag, A.4
Anschauung, A.4
komplexe Konjugation, A.5
Polardarstellung, A.4
Realteil, A.3
Kompositum, 134
Konjugation, B.1
Matrizen, B.8
Konjugationsabbildung, 18

Konjugationsklasse, 53
Konjugationsoperation, 53, B.8
Konjugationsprinzip, 144
konjugierte Nullstellen, 144
konstruierbar
  Punkt, A.28
  Winkel, A.28
Konstruierbarkeit, 130, A.27
  Beispiele, A.31
  Körper, 189, A.29
  Mittelpunkt, A.28
  Origami, B.23
Konstruierbarkeit mit Zirkel und Lineal, 1, 189
Konstruktion mit Zirkel und Lineal, B.31
kopmlexe Zahlen
  imaginäre Einheit, A.3
koprim, 104
Koprodukt
  von Gruppen, 36
Körper, 129, 130, B.23
  algebraisch abgeschlossen, 156, A.2
  Charakteristik, 130, B.23
  Einheitengruppe, 132
  endliche, 160
  Fixkörper, 171
  Frobeniusendomorphismus, B.23
  Funktionenkörper, 90
  Ideale, 91
  Kompositum, 134
  Kreisteilungskörper, 178, B.31
  perfekt, 167
  Primkörper, 130, B.23
  Quotientenkörper, 89
  Zerfällungskörper, 149, B.27
Körpererweiterung, 133, B.29
  abelsche, 182
  algebraisch, 147, B.25
  endlich erzeugt, 136
  endliche, 136
  erzeugter Zwischenkörper, 134
  Galoiserweiterung, 163, 170
  Galoisgruppe, 138, B.29
  Grad, 136, B.31
  Kategorie, 138
  Kompositum, 134, B.25
  Morphismen von, 138
  normal, 165
  separabel, 166
  transzendent, 147
  unendliche, 136
  von endlichen Körpern, 163
  Wurzelerweiterung, 182
  Zwischenkörper, 133
  zyklische, 185
Körperhomomorphismus, 130, 131
Kreisteilungskörper, 178, B.31
Kreisteilungspolynom, 144, 178

L

Länge
  eines Zykels, 57
Lagrange
  Satz von, 22, 23, 33, B.4
  Standard-Argumente, 33
Lean, A.13, B.6
leere Kategorie, A.7
LFSR, A.32
Lineal, 130, A.27
linear feedback shift register, A.32
Linksnebenklasse, 21
Linkstranslationsoperation, 44, 47

M

Matrix
  Konjugation, B.8
Matrixgruppe, 16, 28, 31, 42
  Determinante, 16
maximales Ideal, 101, B.16
mehrfache Nullstelle, 162, B.27
Minimalpolynom, 141, 142, B.25
  Bestimmung, 142
Mischen, B.10
Mitternachtsformel, 183
Monod
  Inverses, 8
  invertierbar, 8

Monoid, 8
Homomorphismus, 10, 11
Inverses, 10
Isomorphismus, 10, 11
natürliche Zahlen, 9
neutrales Element, 8, 10
Selbstabbildungen, 9
Wörter, 9
Monoidhomomorphismus, 8, 10, 11
Monoidisomorphismus, 10, 11
Morphismen-Zoo, 18
Morphismus, A.6
Morphismus von Körpererweiterungen, 138

N

neutrales Element, 8
Eindeutigkeit, 10
noetherscher Ring, 113
normale Hülle, 187
normale Körpererweiterung, 165
Normalisator, 79
Normalreihe, 69
Auflösbarkeit, 69
Normalteiler, 27, B.4
als Kern, 30
Kette, 69
normiertes Polynom, 116
Nullring, 82
Nullstelle
konjugiert, 144
mehrfache, 162, B.27
nullteilerfrei, 84

O

Objekt, A.6
Operation, *siehe* Gruppenoperation
Orbit, 48
Orbitraum, 48
Ordnung, 32
Satz von Lagrange, 33
Origami-Konstruierbarkeit, B.23
orthogonale Gruppe, 17

P

perfekter Körper, 167
Perlenketten, 51
Permuation
ungerade, 59
Permutation, B.10
gerade, 59, 60
Signum, 59
p-Gruppe, 71
auflösbar, 71
Polardarstellung, A.4
Polynom, 86
Auflösbarkeit, 182
Galoisgruppe, 155
irreduzibel, 120, B.21
irreduzibles, 121
Kreisteilungspolynom, 144, 178
normiertes, 116
prim, 120, B.21
primitiv, 120
primitives, 118
separables, 166
Polynomdivision, A.22
Polynomfunktion, 86
polynomiale Gleichung
Auflösbarkeit, 155, 182
Polynomring, 85, 86, 157, B.14
als euklidischer Ring, A.21
iteriert, 86
Polynomdivision, A.21
Polynomfunktion, 86
Primelement, B.18
universelle Eigenschaft, 88
prim, 95, 98, 120, B.21
Primbewertung, 114, 115
Primfaktorzerlegung, 112, 114
Primideal, 101, B.16
primitiv, 120
primitive Einheitswurzel, 144, 185
primitives Element, 168
primitives Polynom, 118
Primkörper, 130, B.23
Primpolynom, B.18
Primzahl
2027, 100

2029, 100
unendlich viele, 100
Verteilung, 100
Primzahlsatz, 100
Primzahltest, 109
probabilistischer, 108
probabilistischer Primzahltest, 108
Produkt
universelle Eigenschaft, 36
von Gruppen, 35, 37
Produktring, 84
proof assistant, A.13
Pseudozufallszahlen, A.34
public key cryptography, 110

Q

Quadratur des Kreises, 190
Quaternionen, B.12
Quaternionengruppe, 72
Quotientengruppe, 29, B.6
universelle Eigenschaft, 30
Quotientenkörper, 89
universelle Eigenschaft, 90
Quotientenring, 92

R

Radikal
Auflösbarkeit, 182
RAID(6), A.34
rationaler Funktionenkörper, 90
Realteil, A.3
Rechenschieber, 14
Rechtsnebenklasse, 21
Reduktionskriterium, 123
reelle Zahlen
Absolutbetrag, A.4
Referenzen zur LA, 5
Restklasse, 92
Restklassenkörper, 104
Restklassenring, 92, B.16
universelle Eigenschaft, 94
Ring, 81, 82, B.16
Eigenschaften, 120
Einheit, 96
Einheitengruppe, 96
euklidisch, A.21
faktoriell, 112
Funktionenring, B.14
Gaußsche ganze Zahlen, 83
ggT, 97
Hauptidealring, 97
Homomorphismus, 83
Ideal, 91, B.14
Integritätsring, 84, B.14
Isomorphismus, 83
kgV, 97, 98
kommutativ, 82
maximal, B.16
mit Eins, 82
noethersch, 113
Nullring, 82
nullteilerfrei, 84
Polynomring, 85, 86, B.14
prim, B.16
Produktring, 84
Quotientenring, 92
Restklassenring, 92, B.16
Teilbarkeit, 96
Ringhomomorphismus, 83
Bild, 91
Ideal, 94
Kern, 91, 94
Ringisomorphismus, 83
Rotationsoperation, 46
RSA, 110, B.18
Rubik's Cube, 46

S

Satz
Ableitungskriterium, 162
Bahnengleichung, 49
Chinesischer Restsatz, 104, B.16
Eisensteinsches Irreduzibilitätskriterium, 124
Feit–Thompson, 70
Fundamentalsatz der Algebra, 192
großer Satz von Fermat, 112

Hauptsatz der Galoistheorie, 164, 173, B.31
Homomorphiesatz, 31
Isomorphiesatz, 34
Klassengleichung, 53
Klassifikation endlicher abelscher Gruppen, 54
Klassifikation endlicher Körper, 160
kleiner Satz von Fermat, 106, 110, B.18
Lemma von Gauß, 116
Primzahlsatz, 100
Reduktionskriterium, 123
Sylow, 70
Sylowsätze, 73, A.17, B.12
vom primitiven Element, 168
von Cauchy, 73
von Cayley, 47
von Gauß, 115
von Lagrange, 22, 70, B.4
Satz von Lagrange
für endliche Gruppen, 23
für Ordnungen, 33
Standard-Argumente, 33
seed, A.33
semi-direktes Produkt, 37, 41, B.6
separabel, 166
Signum, 28, 31, 59
gerade Permutation, 60
Multiplikativität, 59
Transposition, 59
Spalt, 38, B.6
spezielle lineare Gruppe, 16
Stabilisator, 48, B.8
Standard-Argument
Klassifikation endlicher abelscher Gruppen, 56
Satz von Lagrange, 33
Standgruppe, 48
Struktur
endlicher Gruppen, 53
Sylowgruppe, 71, B.12
Normalteiler?, 74
Sylowsätze, 70, 73, A.17, B.12
symmetrische Gruppe, 12, 16, 42, 57, B.10
Auflösbarkeit, 68
Erzeugendensystem, 58
Signum, 28, 31, 59
Zykel, 57
Zykelzerlegung, 57, B.14

T

Teilbarkeit, 96
teilt, 96
Träger
eines Zykels, 57
transitive Gruppenoperation, 45
Transposition
Signum, 59
transzendent, 140
transzendente Körpererweiterung, 147
transzendente Zahl, B.25
Triangulator des Kreises, B.31
triviale Gruppe, 15
triviale Gruppenoperation, 44
triviale Untergruppe, 20, 27

U

Überlagerungstheorie, 175
unendliche Körpererweiterung, 136
ungerade Permutation, 59
unit, 96
universelle Eigenschaft
Abelianisierung, 66
Polynomring, 88
Produkt, 36
Quotientengruppe, 30
Quotientenkörper, 90
Restklassenring, 94
Unter. . . , 19
Untergruppe, 18, 19, 20, B.1
erzeugte, 24
Index, 20, 22, B.4
Linksnebenklasse, 20, 21
normal, 27
Sylowgruppe, 71

triviale, 20, 27
Unterraum
affin, 24

V

verifizierter Beweis, A.13
Verknüpfungstabelle, 13
Verschlüsselung, 110
vollkommener Körper, 167
Vorlesung
Überblick, 2

W

Würfelverdopplung, 191
warum Algebra?, 1
Wiederholung, B.31
Winkel
konstruierbar, A.28
Winkeldreiteilung, B.31
Wörter, 9
Wortproblem, 25
Wurzel, 122, 140, B.27
Wurzelerweiterung, 182

Z

Zählproblem, 51
Zahl
algebraische, 140, B.25
komplexe, A.2
transzendente, B.25
Zahlentheorie, 93
Zauberwürfel, 46
Zentralisator, 52
Zentrum, 52
Zerfällungskörper, 149, B.27
Ziffer, B.18
erste, 108
letzte, 108
Zirkel, 130, A.27
zweiter Isomorphiesatz, 34
Zwischenkörper, 133, B.29
erzeugter Zwischenkörper, 134
Zykel, 57, B.10
Länge, 57
Träger, 57
Zykelzerlegung, 57, B.14
zyklische Erweiterung, 185
zyklische Gruppe, 25, 31, 33

Finger weg! Gaaaaa! . . . Das war der lila Knopf. Jetzt kann alles mögliche passieren! Aber fürs Drucken kann das durchaus nützlich sein . . .