Algebra

Wintersemester 2017/18
Universität Regensburg

Clara Löh

Version vom 9. Februar 2018
clara.loeh@mathematik.uni-regensburg.de
Fakultät für Mathematik, Universität Regensburg, 93040 Regensburg
©Clara Löh, 2017

Inhaltsverzeichnis

Literaturhinweise vii

0 Einführung 1

1 Gruppen 5

1.1 Die Kategorie der Gruppen 6

1.1.1 Gruppen und Gruppenhomomorphismen 6

1.1.2 Automorphismengruppen 11

1.1.3 Untergruppen 13

1.1.4 Erzeugendensysteme 18

1.1.5 Quotientengruppen 21

1.1.6 Produkte und Erweiterungen 28

1.2 Gruppenoperationen 35

1.2.1 Gruppenoperationen 35

1.2.2 Zählen durch Gruppenoperationen 40

1.3 Struktur endlicher Gruppen 45

1.3.1 Endliche abelsche Gruppen 46

1.3.2 Symmetrische Gruppen 48

1.3.3 Die allgemeine Klasifikationsstrategie 52

1.3.4 Auflösbare Gruppen 55

1.3.5 Die Sylowsätze 60

2 Ringe 69

2.1 Die Kategorie der Ringe 70

2.1.1 Ringe und Ringhomomorphismen 70

2.1.2 Polynomringe 73

2.1.3 Quotientenkörper 75

2.1.4 Ideale und Restklassenringe 77

2.2 Die Primeigenschaft 82
2.2.1 Teilbarkeit 82
2.2.2 Primzahlen 85
2.2.3 Primideale und Restklassenringe 88
2.2.4 Der kleine Satz von Fermat 92
2.2.5 Faktorielle Ringe 97
2.2.6 Irreduzibilitätskriterien 106

3 Körper 111
3.1 Die Kategorie der Körper 112
3.1.1 Körper und Körperhomomorphismen 112
3.1.2 Die Einheitengruppe eines Körpers 113
3.2 Die Kategorie der Körpererweiterungen 114
3.2.1 Körpererweiterungen 114
3.2.2 Algebraische Zahlen 121
3.2.3 Algebraische Körpererweiterungen 127
3.2.4 Zerfällungskörper 130
3.2.5 Der algebraische Abschluss 136
3.3 Endliche Körper 140
3.3.1 Klassifikation endlicher Körper 140
3.3.2 Anwendungen endlicher Körper 143
3.4 Galoiserweiterungen 148
3.4.1 Normale Körpererweiterungen 148
3.4.2 Separable Körpererweiterungen 150
3.4.3 Galoiserweiterungen 154
3.4.4 Der Hauptsatz der Galoistheorie 157
3.5 Anwendungen der Galoistheorie 161
3.5.1 Vorbereitung: Kreisteilungskörper 162
3.5.2 Auflösbarkeit durch Radikale 165
3.5.3 Konstruierbarkeit mit Zirkel und Lineal 172
3.5.4 Der Fundamentalsatz der Algebra 179
3.5.5 Die letzte Seite zur Körpertheorie 182

A Anhang A.1
A.1 Formalisierte Algebra A.3
A.2 Kategorien A.7
A.3 Freie Gruppen A.11
A.4 Sylow-Zoo A.15
A.5 Euklidische Ringe A.19
A.6 Funktoren A.25

B Übungsblätter B.1

C Fingerübungen C.1

D Allgemeine Hinweise D.1

Literaturverzeichnis E.1

Symbolverzeichnis E.5

Index E.9

Literaturhinweise

Die Vorlesung wird sich nicht an einer einzelnen Quelle orientieren und es gibt sehr viele Bücher, die den Standardstoff behandeln – Sie sollten also individuell je nach Thema und eigenen Vorlieben die Literatur auswählen, die am besten zu Ihnen passt.

Algebra

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

Lösungsstrategien

- A. Beutelspacher. *Das ist o.B.d.A. trivial!*, neunte Auflage, Vieweg+-Teubner, 2009.
  http://link.springer.com/book/10.1007%2F978-3-8348-9599-8
- A.G. Konforowitsch. *Logischen Katastrophen auf der Spur*, zweite Auflage, Fachbuchverlag Leipzig, 1994.
- C. Löh, S. Krauss, N. Kilbertus. *Quod erat knobelandum*, Springer Spektrum, 2016.
- 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

- M. Brandenburg. *Einführung in die Kategorientheorie: Mit ausführlichen Erklärungen und zahlreichen Beispielen*, Springer Spektrum, 2015.
- Joseph J. Rotman. *An Introduction to the Theory of Groups*, Graduate Texts in Mathematics, 148, vierte Auflage, 1995.
- Geogebra, https://www.geogebra.org/
- Isabelle, https://www.cl.cam.ac.uk/research/hvg/Isabelle/

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 $(2017^{2017})^{2017}$.
2. Bestimme die letzte Ziffer (im Zehnersystem) der Zahl $(2017^{2017})^{2017}$.
3. Bestimme den Rest von 4242^{2017} bei Division durch 2017.

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 natürlich auch 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 sowie auch 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.

Anmerkung zum Lernen. 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 natürlich 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.6.4.11“ oder „Satz II.2.4.33“ verweisen auf die entsprechende Stelle im Skript zur Linearen Algebra I bzw. II:

http://www.mathematik.uni-r.de/loeh/teaching/linalg1_ws1617/lecture_notes.pdf
http://www.mathematik.uni-r.de/loeh/teaching/linalg2_ss17/lecture_notes.pdf

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

Literaturaufgabe. Waren Sie schon einmal in der Bibliothek im Mathematikgebäude? Nicht nur an den Tischen, sondern auch bei den Regalen? Wo stehen die Algebra-Bücher?

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	6
1.2	Gruppenoperationen	35
1.3	Struktur endlicher Gruppen	45

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 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 Gruppen und Gruppenhomomorphismen

Definition 1.1.1 (Gruppe, abelsche Gruppe)**.** Eine *Gruppe* ist ein Paar $(G, \cdot)$, bestehend aus einer Menge G und einer Abbildung $\cdot : G \times G \longrightarrow G$ (sogenannte *Verknüpfung* der Gruppe) mit folgenden Eigenschaften:

- Es gibt ein Element $e \in G$ mit

  $$\forall_{g \in G} \quad g \cdot e = g = e \cdot g.$$

  Wir bezeichnen dann e als *neutrales Element* der Gruppe.

- Zu jedem $g \in G$ gibt es ein $h \in G$ mit

  $$g \cdot h = e = h \cdot g.$$

  Wir bezeichnen dann h als *inverses Element von* g und schreiben dafür auch g^{-1}.

- Die Verknüpfung $\cdot$ ist *assoziativ*, d.h.

  $$\forall_{g,h,k \in G} \quad (g \cdot h) \cdot k = g \cdot (h \cdot k).$$

Oft unterdrückt man in der Notation auch die Verknüpfung und sagt kurz (aber etwas schlampig), dass „G eine Gruppe“ ist.

Eine Gruppe $(G, \cdot)$ heißt *abelsch*, wenn die Verknüpfung kommutativ ist, d.h., wenn folgendes gilt:

$$\forall_{g,h \in G} \quad g \cdot h = h \cdot g.$$

Wir werden abelsche Gruppen im folgenden oft additiv notieren.

Bemerkung 1.1.2 (Eindeutigkeit des neutralen Elements und von Inversen)**.** Sei $(G, \cdot)$ eine Gruppe. Dann gilt (Proposition I.2.2.11):

1. Sind $e, f \in G$ neutrale Elemente von $(G, \cdot)$, so folgt $e = f$.
2. Ist $g \in G$ und sind $h, k \in G$ inverse Elemente von g in $(G, \cdot)$, so folgt $h = k$.

Insbesondere können wir in Gruppen von *dem* neutralen Element sprechen und von *dem* inversen Element eines Gruppenelements!

Im Normalfall bezeichnen wir das neutrale Element einer Gruppe mit e; in multiplikativen Gruppen manchmal auch mit 1 und in additiven Gruppen mit 0. Das inverse Element eines Gruppenelements g bezeichnen wir gewöhnlich mit g^{-1} (bzw. $-g$ in additiven Gruppen).

Ausblick 1.1.3 (formalisierte/verifizierte Beweise)**.** Wie kann man überprüfen, ob ein Beweis korrekt ist? Die naheliegende Methode ist, von Hand, Schritt für Schritt nachzuprüfen, ob wirklich nur zulässige Beweisschritte und Axiome (oder bereits bewiesene Tatsachen) verwendet wurden.

Aber wie kann man überprüfen, ob diese Überprüfung korrekt ist? Ein zeitgemäßes Verfahren dafür ist die vollständige Formalisierung der zulässigen Beweisschritte, Axiome, etc. in einem *proof assistant*, der dann maschinell überprüfen kann, ob der gegebene Beweis korrekt ist; auch die Implementierung des *proof assistant* kann man dieser Überprüfung unterziehen.

Ein Beispiel für eine solche Formalisierung von Grundbegriffen der Gruppentheorie und einfachen Eigenschaften von Gruppen bzw. Gruppenhomomorphismen findet sich in Anhang A.1 mithilfe von Isabelle [18].

Beispiel 1.1.4 (Gruppen)**.** Aus der Linearen Algebra kennen wir bereits einige Beispiele für Gruppen:

- Es ist $(\mathbb{Z}, +)$ eine (abelsche) Gruppe, aber $(\mathbb{Z}, \cdot)$ und $(\mathbb{Z} \setminus \{0\}, \cdot)$ sind *keine* Gruppen.
- Ist $(K, +, \cdot)$ ein Körper, so sind $(K, +)$ und $(K^\times = K \setminus \{0\}, \cdot)$ (abelsche) Gruppen.
- Ist $n \in \mathbb{Z}$, so bildet $\mathbb{Z}/n$ bezüglich (repräsentantenweiser) Addition modulo n eine (abelsche) Gruppe.

  Zur Erinnerung: Es ist $\mathbb{Z}/n = \{k + n \cdot \mathbb{Z} \mid k \in \mathbb{Z}\} = \{[0], \dots, [n-1]\}$ 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).

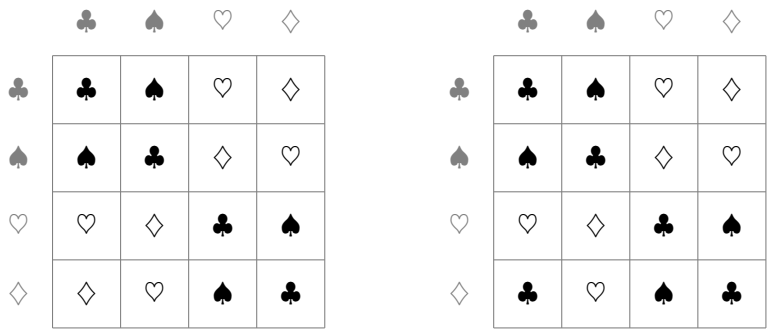


Abbildung 1.1.: Verknüpfungstabellen

- Ist X eine Menge, so bildet die Menge S_X aller Bijektionen $X \longrightarrow X$ eine Gruppe bezüglich Komposition, die *symmetrische Gruppe von* X (Proposition I.2.2.16). 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

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

  Die symmetrische Gruppe S_n tritt zum Beispiel in der Formulierung der Leibniz-Formel (Satz I.5.3.16) auf.

Beispiel 1.1.5 (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 (nachrechnen; kennen Sie eine angenehmere Beschreibung dieser Gruppe?!); die rechte Tabelle erfüllt jedoch *nicht* alle Gruppenaxiome (Übungsaufgabe).

Morphismen erlauben es, Objekte miteinander zu vergleichen. In der Kategorie der Gruppen betrachten wir Morphismen, die mit der Verknüpfungsstruktur verträglich sind:

Definition 1.1.6 (Gruppenhomomorphismus, Gruppenisomorphismus, Kern, Bild)**.** Seien G, H Gruppen.

- Ein *Gruppenhomomorphismus* $G \longrightarrow H$ ist eine Abbildung $f\colon G \longrightarrow H$ mit

  $$\forall_{g,g' \in G} \quad f(g \cdot g') = f(g) \cdot f(g').$$

- Ein *Gruppenisomorphismus* $G \longrightarrow H$ ist ein Gruppenhomomorphismus $f\colon G \longrightarrow H$, für den es einen Gruppenhomomorphismus $g\colon H \longrightarrow G$ mit
$$g \circ f = \mathrm{id}_G \quad \text{und} \quad f \circ g = \mathrm{id}_H$$
gibt. Falls es einen Gruppenisomorphismus $G \longrightarrow H$ gibt, nennen wir die Gruppen G und H *isomorph*; in diesem Fall schreiben wir $G \cong H$.

- Ist $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus, so bezeichnet man
$$\operatorname{im} f := f(G) = \big\{ f(g) \;\big|\; g \in G \big\} \subset H$$
als *Bild von* f und
$$\ker f := f^{-1}(\{e\}) = \big\{ g \in G \;\big|\; f(g) = e \big\} \subset G$$
als *Kern von* f.

Anmerkung zum Lernen. Vergleichen Sie Definition 1.1.6 mit den Definitionen der entsprechenden Begriffe für Vektorräume, Moduln, ...

Beispiel 1.1.7 (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
$$\begin{aligned} A &\longrightarrow A \\ x &\longmapsto n \cdot x := \begin{cases} \sum_{j=1}^{n} x & \text{falls } n \geq 0 \\ -\sum_{j=1}^{-n} x & \text{falsl } n < 0 \end{cases} \end{aligned}$$
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) 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 und auf $\mathbb{R}_{>0}$ die Multiplikation (s. Analysis I; dieser Isomorphismus ist die Grundlage für Rechenschieber).

- 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 $\{0\}$.

Proposition 1.1.8 (grundlegende Eigenschaften von Gruppenhomomorphismen)**.** *Seien G und H Gruppen und sei $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann gilt:*

1. *Es ist $f(e) = e$.*
2. *Für alle $g \in G$ ist $f(g^{-1}) = \big(f(g)\big)^{-1}$.*
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.*

Beweis. Im Rahmen der Linearen Algebra haben wir bereits viele Beweise dieser Art kennengelernt. Wir beweisen daher stellvertretend nur den ersten Teil:

Sei $h := f(e)$. Dann gilt $h = h \cdot h$, denn: Da f ein Gruppenhomomorphismus ist, ist

$$h = f(e) = f(e \cdot e) = f(e) \cdot f(e) = h \cdot h.$$

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

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

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

1.1.2 Automorphismengruppen

Das Konzept und die Axiomatisierung der Gruppen ist ursprünglich aus der Beobachtung entstanden, dass gewisse Familien 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 1.1.9 (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 1.1.10 (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 (nachrechnen). Ist K ein Körper und $n \in \mathbb{N}$, so sind die damit verwandten Konstrukte

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

Gruppen bezüglich Matrixmultiplikation.

Beispiel 1.1.11 (Isometriegruppen)**.** Im Kontext von metrischer Geometrie bzw. metrischen Räumen, sind Isometrien (abstandserhaltende invertierbare Abbildungen) die relevanten 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 (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

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

für alle $n \in \mathbb{N}$ gilt [22, Satz 3.5.1]; dabei ist

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

die *orthogonale Gruppe* (Korollar II.1.2.17). Die Gruppen O(2) und 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 1.1.57).

Beispiel 1.1.12 (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 (nachrechnen). Diese Gruppe bezeichnet man als *Galoisgruppe der Körpererweiterung* $K \subset L$ und 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 1.1.13 (Automorphismengruppe)**.** Auch innerhalb der Gruppentheorie können wir Gruppen invertierbarer Transformationen betrachten; in der Gruppentheorie sind diese Transformationen Gruppenisomorphismen. Genauer: Sei G eine Gruppe. Ein Gruppenisomorphismus $G \longrightarrow G$ bezeichnet man auch als *Automorphismus von* G (erinnern Sie sich noch an die griechischen Bausteine für den Morphismen-Zoo?!). Dann bildet

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

eine Gruppe bezüglich Komposition (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.

Bemerkung 1.1.14 (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* 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.2.4).

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!

1.1.3 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 1.1.15 (Untergruppe)**.** Sei $(G,\ \cdot\ )$ eine Gruppe. Eine *Untergruppe von* G ist eine Teilmenge $H \subset G$ mit folgenden Eigenschaften:

- Die Abbildung $\cdot\colon G \times G \longrightarrow G$ schränkt sich zu einer Abbildung $\cdot H \times H \longrightarrow H$ ein.
- Die Menge H bildet bezüglich dieser eingeschränkten Verknüpfung eine Gruppe.

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

Proposition 1.1.16 (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* $g, h \in H$ *gilt* $g \cdot h \in H$*.*

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

Beweis. Wir verfahren analog zum Beweis der entsprechenden Charakterisierung für Untervektorräume (Proposition I.3.1.13):

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 Verknüpfungsabbildung 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 $h \in H$. Nach ② ist dann auch $h^{-1} \in H$. Also ist
$$e = h \cdot h^{-1} \in H$$
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 1.1.17 (Untergruppen, generische Beispiele)**.**

- Ist G eine Gruppe (mit neutralem Element e), so ist $\{e\}$ eine Untergruppe von G, die *triviale Untergruppe*.
- 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 Untergruppe 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 1.1.18 (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.

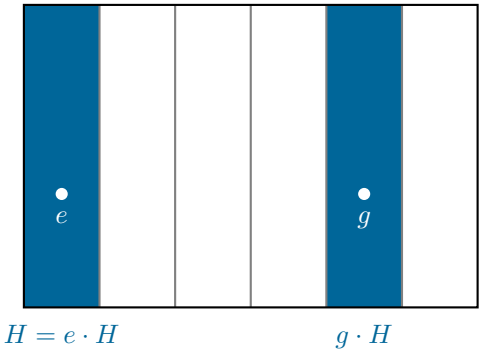


Abbildung 1.2.: Linksnebenklassen, schematisch

- 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 $\det\colon \mathrm{GL}_n(K) \longrightarrow K^\times$.
- 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 1.1.19 (Linksnebenklasse, Index)**.** Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe.

- 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
$$[G : H] := \big|\{g \cdot H \mid g \in G\}\big|$$
bezeichnet man als *Index von H in G*.

Bemerkung 1.1.20 (Linksnebenklassen als Äquivalenzklassen)**.** Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe. Dann betrachten wir die Relation $\sim_H$ auf G mit
$$\forall_{g_1, g_2 \in G} \quad g_1 \sim_H g_2 \iff g_1^{-1} \cdot g_2 \in H.$$
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.

Beispiel 1.1.21 (Index von Untergruppen)**.**

- Sei $n \in \mathbb{N}_{>0}$. Dann hat $n \cdot \mathbb{Z}$ Index n in $\mathbb{Z}$. Die Linksnebenklassen entsprechen genau den n verschiedenen Restklassen bei Division von ganzen Zahlen durch n.

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

Satz 1.1.22 (Satz von Lagrange)**.** *Sei G eine Gruppe und seien $K \subset H$, $H \subset G$ Untergruppen von endlichem Index. Dann ist auch $[G : K]$ endlich und es gilt*
$$[G : K] = [G : H] \cdot [H : K].$$

Beweis. 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 $g_i^{-1} \cdot g \cdot K = h_j \cdot K$. Also ist
$$g \cdot K = g_i \cdot h_j \cdot K.$$
- Jede Linksnebenklasse von K in G besitzt nicht mehr als einen solchen Repräsentanten: Seien also $(i, j), (i', j') \in I \times J$ mit
$$g_i \cdot h_j \cdot K = g_{i'} \cdot h_{j'} \cdot K.$$
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 $(i, j) = (i', j')$.

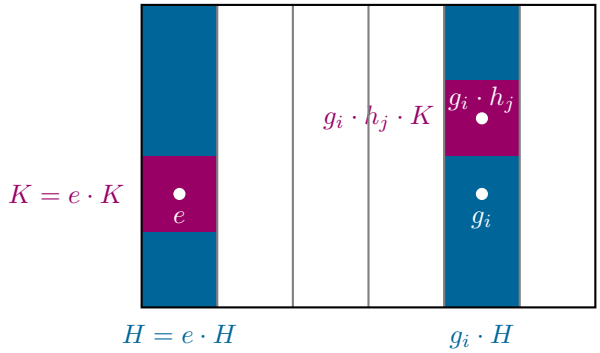


Abbildung 1.3.: Der Satz von Lagrange, schematisch

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 1.1.23. 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 1.1.24 (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 1.1.22) 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

$$\big[G : \{e\}\big] = |G| \quad \text{und} \quad \big[H : \{e\}\big] = |H|.$$

Wir wenden nun den Satz von Lagrange auf die Kette $K := \{e\} < H < G$ von Untergruppen an; da G endlich ist, sind $[G : H]$ und $[H : K]$ beide endlich (und daher ist der Satz anwendbar). Nach dem Satz von Lagrange gilt also

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

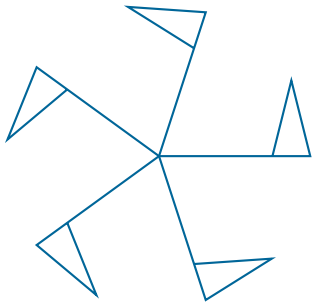


Abbildung 1.4.: Eine Teilmenge von $\mathbb{R}^2$, deren Isometriegruppe isomorph zu $\mathbb{Z}/5$ ist (nachrechnen).

Beispiel 1.1.25. Sei $X \subset \mathbb{R}^2$ eine Teilmenge, die nicht in einer (affinen[1]) 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).

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 $\mathrm{Isom}(X, d_2)$. Also müsste $|H| = 2$ ein Teiler der ungeraden Zahl $|\mathrm{Isom}(X, d_2)|$ sein, was nicht sein kann. Also gibt es *keine* solche Spiegelung s.

1.1.4 Erzeugendensysteme

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

Definition 1.1.26 (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*.

[1] Ein *affiner Unterraum* eines Vektorraums V ist eine Menge der Form $v+U$, wobei $v \in V$ und $U \subset V$ ein Untervektorraum ist.

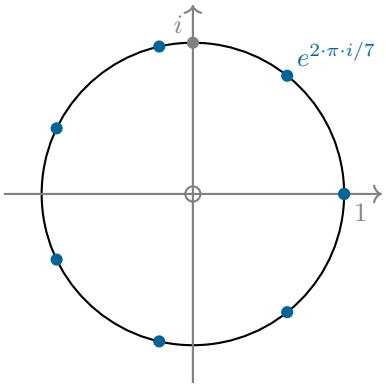


Abbildung 1.5.: Eine endliche zyklische Gruppe in $\mathbb{C}^\times$

- Falls G ein endliches Erzeugendensystem besitzt, ist G *endlich erzeugt*.
- Falls G ein ein-elementiges Erzeugendensystem besitzt, ist G eine *zyklische Gruppe*.

Bemerkung 1.1.27 („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.

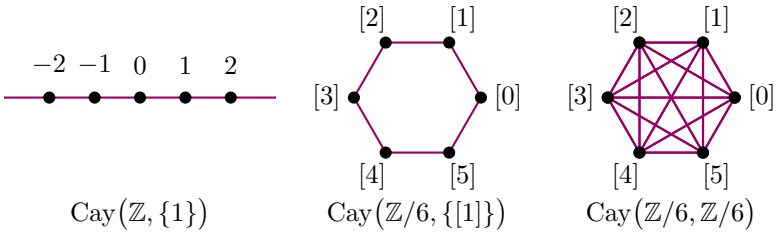
Beispiel 1.1.28 (Erzeugendensysteme)**.**

- Es ist $\langle\{1\}\rangle_\mathbb{Z} = \mathbb{Z}$ und $\langle\{2,3\}\rangle_\mathbb{Z} = \mathbb{Z}$, 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)
$$\langle\{e^{2\cdot\pi\cdot i/n}\}\rangle_{\mathbb{C}^\times} \cong \mathbb{Z}/n.$$
- Ist X eine Menge, so ist die symmetrische Gruppe S_X genau dann endlich erzeugt, wenn X endlich ist (Übungsaufgabe).

Bemerkung 1.1.29 (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.3.1.21).



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

Abbildung 1.6.: Beispiele für Cayleygraphen

Caveat 1.1.30 (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:

- 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 1.1.31 (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].

1.1.5 Quotientengruppen

Als nächsten Schritt werden wir Quotientengruppen betrachten – wie im Fall von Quotientenvektorräumen (Proposition I.3.4.14) ist es manchmal günstig, den Quotienten einer Gruppe nach einer Untergruppe zu betrachten, indem man alles „vergisst“, was in dieser Untergruppe passiert.

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 nun 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 1.1.32. 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 1.1.36).

Definition 1.1.33 (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 (d.h., wenn die Menge N konjugationsinvariant ist). Ist N ein Normalteiler in G, so schreibt man auch $N \lhd G$.

Beispiel 1.1.34 (Normalteiler, generische Beispiele)**.** Sei G eine Gruppe.

- Die Untergruppen $\{e\}$ und G sind Normalteiler in G.
- Ist G abelsch, so ist jede Untergruppe ein Normalteiler in G (nachrechnen).
- 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. Außerdem gilt für alle $n \in \ker f$ und alle $g \in G$ wegen

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

  auch $g \cdot n \cdot g^{-1} \in \ker f$. Es gilt sogar auch die Umkehrung (Bemerkung 1.1.38).

Beispiel 1.1.35 (Normalteiler, konkrete Beispiele)**.**

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

- 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.5.3.19).

- 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 $\det\colon \mathrm{GL}_n(K) \longrightarrow K^\times$.

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

Proposition 1.1.36 (Quotientengruppe). *Sei G eine Gruppe und sei $N \subset G$ eine Untergruppe.*

1. *Die Abbildung*

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

ist genau dann wohldefiniert, wenn N ein Normalteiler in G ist.

2. *Falls N ein Normalteiler ist, so ist G/N eine Gruppe bezüglich dieser Verknüpfung, 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 also $g, h, g', h' \in G$ 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 $n' := h^{-1} \cdot n \cdot h \in N$, 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

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

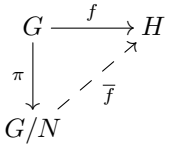
insbesondere ist $g \cdot n \cdot g^{-1} \in N$. Also ist N ein Normalteiler in G. □

Proposition 1.1.37 (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 1.1.38 (Kern vs. Normalteiler)**.** 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 1.1.34).
- Ist N eine Normalteiler, so ist N der Kern des kanonischen Projektionshomomorphismus $G \longrightarrow G/N$ (Proposition 1.1.37).

Beispiel 1.1.39 (zyklische Gruppen)**.** Sei $n \in \mathbb{N}$. Dann ist $n\cdot\mathbb{Z}$ ein Normalteiler in $\mathbb{Z}$ und $\mathbb{Z}/n \cong \mathbb{Z}/n \cdot \mathbb{Z}$ (im Sinne der Gruppentheorie); diese Gruppe ist zyklisch, erzeugt von [1].

Korollar 1.1.40 (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. □

Beispiel 1.1.41 (die Gruppe S^1)**.** Die Teilmenge

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

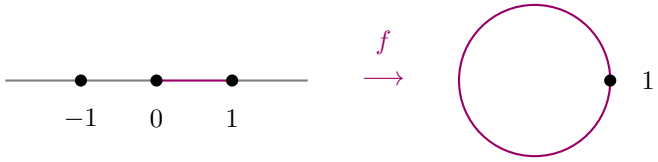


Abbildung 1.7.: Die Gruppe $S^1 \cong \mathbb{R}/\mathbb{Z}$

ist eine Gruppe bezüglich Multiplikation (nachrechnen). Der Gruppenhomomorphismus

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

ist surjektiv und $\ker f = \mathbb{Z}$ (s. Analysis). Also ist $S^1 \cong \mathbb{R}/\mathbb{Z}$ (Abbildung 1.7).

Beispiel 1.1.42 (Signum)**.** Sei $n \in \mathbb{N}_{>1}$. Dann induziert die Signumsabbildung $\operatorname{sgn}\colon S_n \longrightarrow \{-1, 1\}$ nach dem Homomorphiesatz einen Isomorphismus

$$S_n/A_n = S_n/\ker \operatorname{sgn} \cong \mathbb{Z}/2.$$

Beispiel 1.1.43 (Determinante)**.** Sei K ein Körper und $n \in \mathbb{N}_{>0}$. Dann induziert die Determinantenabbildung $\det\colon \mathrm{GL}_n(K) \longrightarrow K^\times$ nach dem Homomorphiesatz einen Isomorphismus

$$\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^\times.$$

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

Definition 1.1.44 (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 1.1.45 (Ordnung)**.**

- Das Element $1 \in \mathbb{Z}$ hat unendliche Ordnung in $(\mathbb{Z}, +)$.
- Die Transposition $(1\ 2) \in S_3$ hat Ordnung 2.

Proposition 1.1.46 (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* $\mathbb{Z} \cong \langle\{g\}\rangle_G$ *(via* $k \mapsto g^k$*).*

Beweis. 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

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

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 1.1.40) erhalten wir somit, dass f den gewünschten Isomorphismus $\mathbb{Z}/d = \mathbb{Z}/\ker f \cong \langle g\rangle_G$ induziert.

② Ist $\operatorname{ord} g = \infty$, so ist $\ker f = \{0\}$ (nachrechnen). Mit dem Homomorphiesatz (Korollar 1.1.40) folgt daher, dass f den gewünschten Isomorphismus $\mathbb{Z} \cong \mathbb{Z}/\{0\} = \mathbb{Z}/\ker f \cong \langle g\rangle_G$ induziert. □

Korollar 1.1.47 (Klassifikation der zyklischen Gruppen)**.** *Ist* G *eine zyklische Gruppe, so gibt es genau ein* $n \in \mathbb{N}$ *mit* $G \cong \mathbb{Z}/n$*.*

Beweis. Sei G eine zyklische Gruppe und sei $g \in G$ mit $\langle g\rangle_G = G$. Dann gibt es ein $n \in \mathbb{N}$ mit $G = \langle g\rangle_G \cong \mathbb{Z}/n$ (Proposition 1.1.46). Da die Mächtigkeit einer Gruppe eine Isomorphieinvariante ist (Gruppenisomorphismen sind bijektiv!), folgt, dass n eindeutig bestimmt ist. □

Korollar 1.1.48 (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 1.1.46 gilt $|H| = \operatorname{ord} g$. Mit dem Satz von Lagrange für endliche Gruppen (Korollar 1.1.24) folgt daher, dass $\operatorname{ord} g = |H|$ ein Teiler von $|G|$ ist. □

Beispiel 1.1.49 (Standard-Lagrange-Argumente)**.**

- Sei $g \in \mathbb{Z}/2017 \setminus \{[0]\}$. Dann ist $\operatorname{ord} g = 2017$ (da 2017 prim ist), und damit $\langle g \rangle_{\mathbb{Z}/2017} = \mathbb{Z}/2017$.
- Die Gruppe S_3 enthält *kein* Element der Ordnung 4, denn $|S_3| = 6$ und 4 ist *kein* Teiler von 6.

Für Quotienten sind außerdem folgende „Kürzungsregeln“ hilfreich:

Satz 1.1.50 (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 1.1.16.

- 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

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

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

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

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 nun den Gruppenhomomorphismus

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

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. Mit dem Homomorphiesatz (Korollar 1.1.40) 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 1.1.40) folgt daher die Behauptung. □

1.1.6 Produkte und Erweiterungen

Umgekehrt werden wir uns nun überlegen, 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 1.1.51 (Produkt)**.** Sei $(G_i)_{i\in I}$ eine (nicht-leere) Familie von Gruppen. Die Menge

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

ist bezüglich komponentenweiser Verknüpfung eine Gruppe, das *Produkt der* $(G_i)_{i\in I}$. Die Elemente von $\prod_{i\in I} G_i$ notieren wir oft statt als Abbildungen auch 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

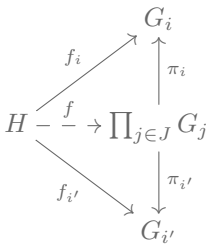
$$\begin{aligned} i_j \colon G_j &\longmapsto \prod_{i\in I} G_i \\ x &\longmapsto \left(i \mapsto \begin{cases} x & \text{falls } i = j \\ e & \text{falls } i \neq j \end{cases} \right) \end{aligned}$$

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.

Bemerkung 1.1.52 (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 1.1.53 (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 von zwei Elementen frei erzeugte Gruppe (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 nun, indem wir die Verknüpfung in kontrollierter Weise deformieren:

Definition 1.1.54 (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 $N \times Q$ mit der folgenden Verknüpfung:

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

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 anzuwenden.

Beispiel 1.1.55 (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 gewöhnliche Produktgruppe $N \times Q$ (nachrechnen).

Proposition 1.1.56 (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 $\ker \pi = N \times \{e\}$.

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

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

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

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

□

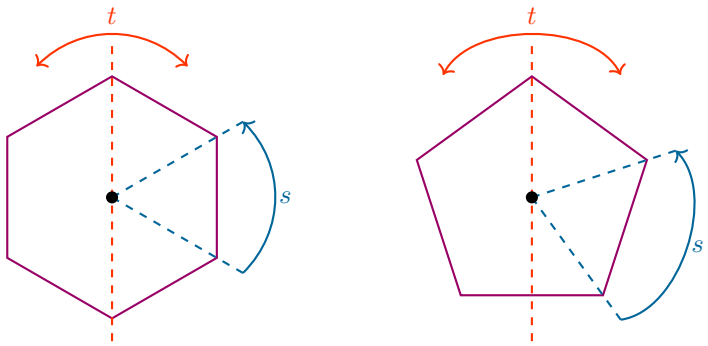


Abbildung 1.8.: Elemente der Isometriegruppe des regulären Sechs- bzw. Fünfecks

Proposition 1.1.57 (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*

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

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). Dabei ist $\mathrm{ord}\, s = n$ und $\mathrm{ord}\, t = 2$.

Die Gruppe $G := \mathrm{Isom}(X_n, d_2)$ enthält keine weiteren Elemente, denn:

- 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 $\mathrm{id}, s, \dots, s^{n-1}, t, s\circ t, s^2\circ t, \dots, s^{n-1}\circ t$ alle zulässigen Eckenbijektionen realisieren, gibt es keine weiteren Elemente in G.

Wir betrachten nun

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

sowie

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

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 1.1.58 (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 1.1.11). 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 1.1.59 („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

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

ein Gruppenisomorphismus (nachrechnen); hierbei bildet $H \cdot N$ wie im ersten Isomorphiesatz (Satz 1.1.50) 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 1.1.60 (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 $G \cong N \rtimes_\varphi Q$ (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 $S_n \cong A_n \rtimes_\varphi \mathbb{Z}/2$ gibt (Übungsaufgabe). Analog erhält man auch Isomorphismen der Form

$$\begin{aligned} \mathrm{O}(n) &\cong \mathrm{SO}(n) \rtimes \mathbb{Z}/2 \\ \mathrm{GL}_n(K) &\cong \mathrm{SL}_n(K) \rtimes K^\times \end{aligned}$$

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

Allgemeiner lassen sich Gruppenerweiterungen über sogenannte *Gruppenkohomologie* klassifizieren [8].

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 Geometrie und 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:

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

  (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 From $G \times X \longrightarrow X$ 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*.

- 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.

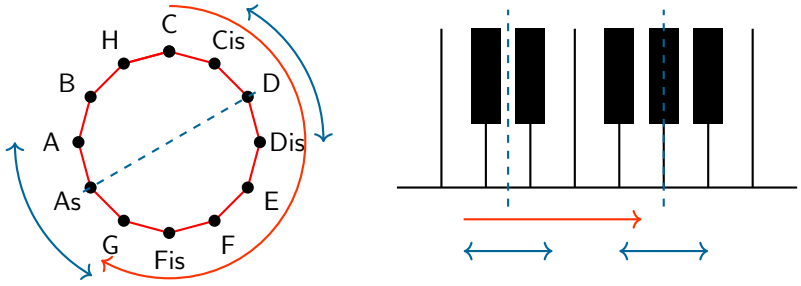


Abbildung 1.9.: Die zwölf Halbtöne und die Gruppe D_{12}; rot: Transposition um sieben Halbtöne nach oben; blau: Inversion an D bzw. As (auf dem Klavier leicht zu spielen).

- 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.

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 C.

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 [13].

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

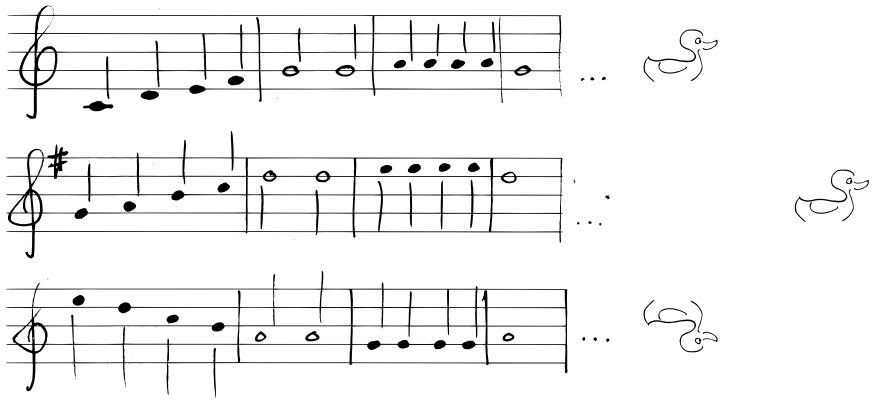


Abbildung 1.10.: Original, Transposition, Inversion

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

- *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.

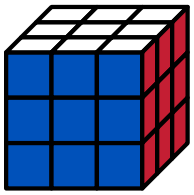


Abbildung 1.11.: Rubik's Cube

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). Daher 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 1.1.40) ist somit $G \cong \operatorname{im} \varrho$; dabei ist $\operatorname{im} \varrho$ eine Untergruppe von S_G. □

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 1.2.10 (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 1.2.11. 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 1.1.16), aber im allgemeinen *kein* Normalteiler in G.

Bemerkung 1.2.12 (Bahnen als Äquivalenzklassen)**.** Ist eine Gruppenoperation einer Gruppe G auf einer Menge X gegeben, so definiert
$$\forall_{x,y \in X} \quad x \sim y \Longleftrightarrow \exists_{g \in G} \quad g \cdot x = y$$
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.

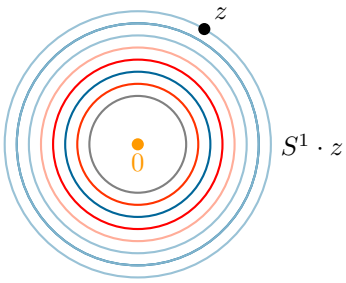


Abbildung 1.12.: Orbits der S^1-Operation durch Multiplikation auf $\mathbb{C}$

Anmerkung zum Lernen. Was haben Bahnen und Standgruppen mit Freiheit bzw. Transitivität von Gruppenoperationen zu tun?

Beispiel 1.2.13 (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). 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

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

  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 1.1.11 der Stabilisator von x unter der kanonischen $\mathrm{Isom}(X,d)$-Operation auf X (und dies rechtfertigt auch die Notation).

Satz 1.2.14 (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 die Abbildung*

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

   wohldefiniert und bijektiv.

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 1.2.12 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 $F := \big\{(g, x) \;\big|\; g \in G,\ x \in X, g \cdot x = x\big\} \subset G \times X$. 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 weiter zu bearbeiten. Nach dem Satz von Lagrange für endliche Gruppen (Korollar 1.1.24) gilt $|G| = [G : G_x] \cdot |G_x|$ für alle $x \in X$. Mit dem ersten Teil erhalten wir somit

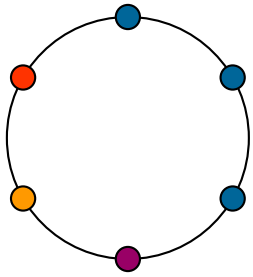


Abbildung 1.13.: Eine Perlenkette

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

□

Beispiel 1.2.15 (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 die Anzahl der D_6-Orbits bei der Operation auf X bestimmen. Nach Satz 1.2.14 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 1.2.14)

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

Zum Beispiel: Bei fünf Farben gibt es also genau 1505 essentiell verschiedene dieser Ketten. Bei 2017 Farben gibt es genau 5611183399506640033 essentiell verschiedene dieser Ketten.

Eine für die Gruppentheorie wichtige Anwendung der Bahnengleichung ist die Klassengleichung. Dafür benötigen wir den Begriff des Zentralisators bzw. des Zentrums:

Definition 1.2.16 (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 1.2.17. Das Zentrum $Z(G)$ einer Gruppe G ist offenbar ein Normalteiler in G (nachrechnen) und es gilt

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

Das Zentrum und Zentralisatoren treten auf natürliche Weise im Zusammenhang mit Konjugationsoperationen auf:

Beispiel 1.2.18 (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 $\{g\}$. 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 1.2.19 (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*

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

Beweis. Wir wenden die Bahnengleichung (Satz 1.2.14) auf die Konjugationsoperation von G auf G an; mit den Überlegungen aus Beispiel 1.2.18 folgt die Behauptung. □

In günstigen Fällen, erlaubt es die Klassengleichung durch reine Zählargumente festzustellen, dass das Zentrum nicht-trivial ist. Außerdem werden wir ähnliche Operationen und Argumente 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 1.1.30), 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.2.5.16):

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*

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

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.2.5.16); 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 1.1.48) und der Voraussetzung, dass p prim ist), dass

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

(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

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

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 nun durch Induktion über die Anzahl $|A| = |B|$ der Gruppenelemente:

- *Induktionsanfang.* Haben die obigen Gruppen jeweils nur ein Element, so ist $k = 0 = \ell$ und $r = 0 = s$.
- *Induktionsschritt.* 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.

  Wegen $A \cong B$ folgt auch $p \cdot A \cong p \cdot B$ (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

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

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

  Wegen $A \cong B$ ist andererseits auch

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

  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 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 $B \cong A$, so folgt $B(p) \cong A(p)$.*

Beweis. Zu 1. Wir beweisen dies mithilfe der Charakterisierung von Untergruppen aus Proposition 1.1.16 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 $\mathbb{Z}/2^2 = \mathbb{Z}/4 \ncong \mathbb{Z}/2 \times \mathbb{Z}/2$ (denn die linke Gruppe enthält ein Element der Ordnung 4 im Gegensatz zur rechten Gruppe).
- Es gilt $\mathbb{Z}/2 \times \mathbb{Z}/3 \cong \mathbb{Z}/6$ (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.2.5.16).

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

$$\mathbb{Z}/4 \times \mathbb{Z}/7 \times \mathbb{Z}/71 \cong \mathbb{Z}/1988, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/7 \times \mathbb{Z}/71$$

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 Zyklen 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 Zyklen $\sigma_1, \ldots, \sigma_k \in S_n$ 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 $\{1, \ldots, n\}$. 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 Zyklen 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 Zyklen 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)

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

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.“ [19, S. 153]

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)

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

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

$$(j\ j+1) = (1\ 2\ \dots\ n)^{j-1} \cdot (1\ 2) \cdot (1\ 2\ \dots\ n)^{-j+1}$$

gilt. □

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 geeignete 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.5.3.16, Beispiel 1.1.35, Beispiel 1.1.42)). Wir erinnern noch einmal an die wichtigsten Eigenschaften:

Bemerkung 1.3.8 (Signum). Sei $n \in \mathbb{N}$. Dann definieren wir das *Signum* durch

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

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

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*.

- Ist $\sigma \in S_n$ eine Transposition, so ist $\operatorname{sgn}\sigma = -1$.
- Das Signum ist ein Gruppenhomomorphismus (in die multiplikative Gruppe $\{-1,1\}$): Für alle $\sigma,\tau \in S_n$ gilt (Proposition I.5.3.19)

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

- Den Kern $A_n := \{\sigma \in S_n \mid \operatorname{sgn}\sigma = 1\}$ bezeichnet man als *alternierende Gruppe* A_n.
- Eine Permutation ist genau dann gerade, wenn sie sich als Produkt einer geraden Anzahl von Transpositionen schreiben lässt.

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

Beispiel 1.3.9 (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 1.3.10 (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-Zyklen schreiben lassen.*
2. *Sei $n \in \mathbb{N}_{\geq 5}$. Dann gilt: Je zwei 3-Zykel in A_n sind konjugiert zueinander.*

Beweis. Zu 1. Seien $x_1, \ldots, x_4 \in \{1, \ldots, n\}$.

- Sind x_1, x_2, x_3 verschieden, so gilt

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

  Insbesondere ist jeder 3-Zykel eine gerade Permutation und somit in A_n.

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

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

Ist $\sigma \in A_n$, so ist σ ein Produkt einer geraden Anzahl von Transpositionen. Induktiv folgt mit den obigen Beobachtungen also, dass σ als Produkt von 3-Zyklen geschrieben werden kann.

Zu 2. Seien $(x_1\ x_2\ x_3), (y_1\ y_2\ y_3) \in A_n$ zwei 3-Zyklen. 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). Ist $\sigma \in A_n$, so ist nichts mehr zu zeigen. 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 $\tau := \sigma \circ (j\ k) \in A_n$ und

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

wie gewünscht. □

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 1.1.60)

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

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

Die atomaren Bausteine dieser Klassifikation sind Gruppen, die keine nicht-trivialen Normalteiler bzw. Quotientengruppen besitzen; dies sind die sogenannten einfachen Gruppen:

Definition 1.3.11 (einfache Gruppe)**.** Eine Gruppe G ist *einfach*, wenn $\{e\}$ und G die einzigen Normalteiler in G sind.

Beispiel 1.3.12 (einfache Gruppen)**.**

- Ist $p \in \mathbb{N}$ prim, so ist $\mathbb{Z}/p$ eine einfache Gruppe (dies folgt bereits aus dem Satz von Lagrange für endliche Gruppen (Korollar 1.1.24)).
- Die Gruppe $\mathbb{Z}/4$ ist *nicht* einfach (die von [2] erzeugte Untergruppe ist ein geeigneter Normalteiler).
- Die Gruppe $\mathbb{Z}$ ist *nicht* einfach (die von 2 erzeugte Untergruppe ist ein geeigneter Normalteiler).
- Die Gruppe $\mathrm{GL}_2(\mathbb{R})$ ist *nicht* einfach (die Untergruppen $\mathrm{SL}_2(\mathbb{R})$ und $\{\lambda \cdot I_2 \mid \lambda \in \mathbb{R}^\times\}$ sind geeignete Normalteiler).

Satz 1.3.13 (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 $A_3 = \langle\{(1\ 2\ 3)\}\rangle_{S_3} \cong \mathbb{Z}/3$ 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 1.3.10 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 nun 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

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

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

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

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

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

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

Ausblick 1.3.14 (einfache Automorphismengruppen)**.** (Varianten von) Automorphismengruppen sind „oft“ gute Kandidaten für einfache Gruppen [14].

Ausblick 1.3.15 (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 1.3.16 (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 Gruppe
$$[G, G] := \langle \{[g, h] \mid g, h \in G\} \rangle_G \subset G$$
die von den Kommutatoren in G erzeugt wird.

Bemerkung 1.3.17. 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 (wenn g und h 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 1.3.18 (Kommutatoren)**.**

- Ist A abelsch, so ist $[A, A] = \{e\}$.
- Ist $n \in \mathbb{N}_{\geq 3}$, so gilt in S_n:
$$\big[(1\ 3), (2\ 3)\big] = (1\ 3) \cdot (2\ 3) \cdot (1\ 3)^{-1} \cdot (2\ 3)^{-1} = (1\ 2\ 3)$$
- Ist $n \in \mathbb{N}_{\geq 3}$, so ist $[D_n, D_n]$ zyklisch (Übungsaufgabe).

Caveat 1.3.19. 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 1.3.20 (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 1.1.37). □

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 1.3.21 (auflösbare Gruppe)**.** Sei G eine Gruppe.

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

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

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

Beispiel 1.3.22 (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 1.3.18).
- Ist G eine nicht-triviale Gruppe mit $[G, G] = G$, so ist G *nicht* auflösbar.

Proposition 1.3.23 (Vererbungseigenschaften auflösbarer Gruppen)**.**

1. *Untergruppen auflösbarer Gruppen sind auflösbar.*
2. *Quotientengruppen einer auflösbaren Gruppen sind auflösbar.*
3. *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 1.3.24 ((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 1.3.22). Außerdem ist $S_3 \cong D_3$ auflösbar (Beispiel 1.3.22). 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 (Caveat 1.3.26).

Zu 2. $\Longrightarrow$ 3. Ist S_n auflösbar, so ist auch die Untergruppe $A_n \subset S_n$ auflösbar (Proposition 1.3.23).

Zu 3. $\Longrightarrow$ 1. Es genügt zu zeigen, dass A_n für jedes $n \in \mathbb{N}_{\geq 5}$ *nicht* auflösbar ist bzw. (wegen Proposition 1.3.23), dass A_5 *nicht* auflösbar ist:

Es ist $[A_5, A_5] = A_5$, denn: Da A_5 einfach ist (Satz 1.3.13) 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

$$(1\ 2\ 3) = (1\ 2\ 4) \cdot (1\ 3\ 5) \cdot (1\ 2\ 4)^{-1} \cdot (1\ 3\ 5)^{-1}$$

(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 1.3.25 (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 1.3.26 (Ketten von Normalteilern)**.** Ist $G = G_0 \rhd G_1 \rhd \dots$ eine Normalreihe in G, so sind $G_2, G_3, \dots$ 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 $K \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ 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 1.3.27 (Auflösbarkeit und Normalreihen)**.** *Sei G eine endliche Gruppe. Dann sind äquivalent:*

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

Beweis. Zu 1. $\Longrightarrow$ 2. Dies folgt aus der Definition von Auflösbarkeit durch abgeleitete Gruppen und die Eigenschaften der Abelianisierung (Proposition 1.3.20).

Zu 2. $\Longrightarrow$ 3. Jede Normalreihe mit abelschen Faktoren kann mithilfe der Zerlegung endlicher abelscher Gruppen in zyklische Gruppen zu einer Normalreihe mit zyklischen Faktoren verfeinert werden.

Zu 2./3. $\Longrightarrow$ 1. Sei $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$ eine Normalreihe von G mit abelschen (oder sogar zyklischen) Faktoren. Induktiv folgt dann mithilfe von Proposition 1.3.20, dass $G^{(k)} \subset G_k$ für alle $k \in \{0, \dots, n\}$ gilt: Nach Konstruktion ist $G^{(0)} = G = G_0$. Ist $k \in \{0, \dots, n-1\}$ und $G^{(k)} \subset G_k$, so folgt mit Proposition 1.3.20, dass

$$G_{k+1} \subset [G_k, G_k] \subset \big[G^{(k)}, G^{(k)}\big] = G^{(k+1)},$$

da der Quotient G_k/G_{k+1} abelsch ist.

Insbesondere ist $G^{(n)} = G_n = \{e\}$; also ist G auflösbar. □

Ausblick 1.3.28 (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 (!) [15, 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 1.1.48) wissen wir, dass die Ordnungen von Gruppenelementen in endlichen Gruppen die Gesamtanzahl der Gruppenelemente teilen muss. Wie sieht es mit der Umkehrung aus?

Caveat 1.3.29 (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 1.3.36).

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

Caveat 1.3.30 (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 1.3.13)).

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 1.3.31 (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 1.3.32 (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 $\{([0],[0]),([1],[1])\}$.

- 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 1.3.33 (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 1.2.19): Sei $|G| \neq 1$ und sei $(g_i)_{i\in I}$ ein Repräsentantensystem für die nicht-trivialen Konjugationsklassen in G. Dann liefert die Klassengleichung:

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

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 1.1.24) 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.
- *Induktionsschritt.* Es sei nun $|G| > 1$ und es sei bereits gezeigt, dass alle kleineren p-Gruppen auflösbar sind. Dann ist auch G auflösbar, denn: Nach dem ersten Teil ist das Zentrum $Z(G)$ ein Normalteiler in G mit $|Z(G)| \neq 1$. Wir betrachten dann 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 1.3.23).

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 1.3.34 (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.

Wie kann man dies zeigen? Sei G eine Gruppe mit $|G| = 8 = 2^3$. Also ist das Zentrum $Z(G)$ nicht-trivial (Satz 1.3.33); nach dem Satz von Lagrange (Korollar 1.1.24) 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 $G/Z(G) \cong \mathbb{Z}/2$ (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.
- Ist $|Z(G) = 2$, so ist $G/Z(G)$ eine vier-elementige Gruppe und daher nach Satz 1.3.33 (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 nun 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 $D_4 \ncong Q_8$ (wie zum Beispiel an der Anzahl der Elemente der Ordnung 4 abgelesen werden kann).

Satz 1.3.35 (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 1.3.36 (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 1.3.35) 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 1.1.48) gibt es also ein $\ell \in \{1, \ldots, k\}$ mit

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

Dann ist $g^{p^{\ell-1}}$ ein Element der Ordnung p in G (nachrechnen). □

Bemerkung 1.3.37 (nochmal p-Gruppen)**.** Sei $p \in \mathbb{N}$ prim. Aus dem Satz von Cauchy (Korollar 1.3.36) und dem Satz von Lagrange (Korollar 1.1.48) 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 1.3.38 (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 1.3.33). Ohne Einschränkung sei nun $q < p$. Nach den Sylowsätzen (Satz 1.3.35) gibt es eine p-Sylowgruppe $S \subset G$; diese ist als p-Gruppe auflösbar (in diesem Fall gilt sogar $|S| = p$, und damit $S \cong \mathbb{Z}/p$).

Wir verwenden nun 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 1.3.35):

$$s_p \mid |G| \quad \text{und} \quad s_p \equiv 1 \mod p.$$

Wegen $s_p \mid |G|$ und der Voraussetzung, dass p und q prim sind, folgt

$$s_p \in \{1, q, p, p \cdot q\}.$$

Aus der zweiten Gleichung und $1 < q < p$ schließen wir, dass nur $s_p = 1$ infrage kommt. Also ist S die *einzige* p-Sylowgruppe von G. Da die zu S konjugierten Gruppen auch p-Sylowgruppen von G sind, folgt

$$\forall_{g \in G} \quad g \cdot S \cdot g^{-1} = S.$$

Also ist S ein Normalteiler von G.

Mit dem Satz von Lagrange (Korollar 1.1.24) folgt, dass die Quotientengruppe G/S genau q Elemente enthält. Da q prim ist, ist G/S auflösbar (sogar $G/S \cong \mathbb{Z}/q$).

Da S und G/S auflösbar sind, ist auch die Erweiterungsgruppe G auflösbar (Proposition 1.3.23). □

In Anhang A.4 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 1.15 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 wenigen zusätzlichen Überlegungen ein gutes Verständnis der betrachteten Gruppe zu erlangen.

Wir geben nun einen Beweis der Sylowsätze:

Beweis von Satz 1.3.35. 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

$$X := \big\{ A \subset G \;\big|\; |A| = p^k \big\}.$$

Dann operiert G auf X durch Linkstranslation und wir erhalten mit der Bahnengleichung (Satz 1.2.14)

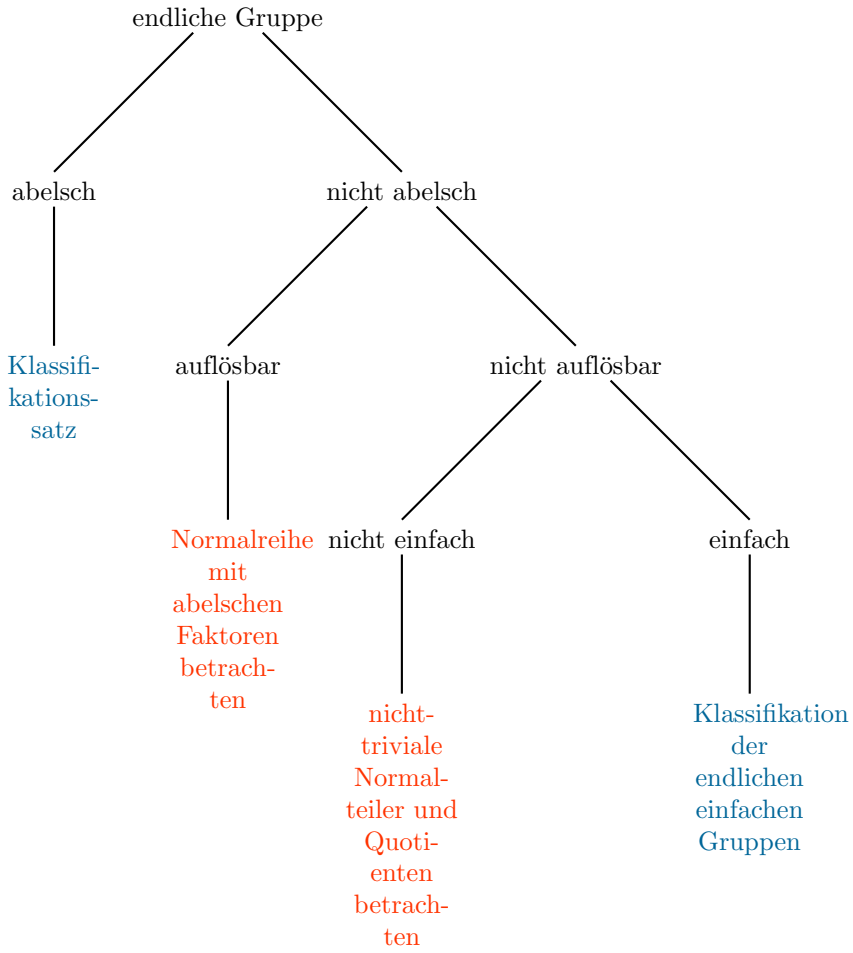


Abbildung 1.15.: Zerlegung von endlichen Gruppen

$$\binom{m \cdot p^k}{p^k} = |X| = \sum_{G \cdot A \in G \setminus X} [G : G_A].$$

Der Binomialkoeffizient auf der linken Seite ist *nicht* durch p teilbar, denn:

$$\binom{m \cdot p^k}{p^k} = \prod_{j=1}^{p^k-1} \frac{m \cdot p^k - x}{p^k - x}$$

und keiner dieser Faktoren ist durch p teilbar (nachrechnen).

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 nun, 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 1.1.24)

$$m\cdot p^k=|G|=[G:G_A]\cdot|G_A|,$$

und damit p^k ein Teiler von $|G_A|$. Andererseits gilt (nach Definition des Stabilisators G_A)

$$\forall_{a\in A}\quad\forall_{g\in G_A}\quad g\cdot a\subset A,$$

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 betrachten 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 1.2.14) liefert also

$$[G:S]=|G/S|=|X|=\sum_{H\cdot x\in H\backslash X}[H:H_x].$$

Da H eine p-Gruppe ist, folgt mit dem Satz von Lagrange (Korollar 1.1.24), 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 nun wieder 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 1.2.14)

$$s_p = |X| = |G \cdot x| = [G : G_x].$$

Mit dem Satz von Lagrange (Korollar 1.1.24) 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 nun die Konjugationsoperation von G auf X zur Konjugationsoperation von S auf X ein. Dann liefert die Bahnengleichung (Satz 1.2.14), 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 1.1.24) durch p teilbar. Aufgrund der obigen Gleichung ist somit

$$s_p \equiv \left|\{x \in X \mid \forall_{s \in S} \quad s \cdot x = x\}\right| \mod p.$$

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. Daher 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 (Satz 1.1.50) und dem Satz von Lagrange (Korollar 1.1.24) erhalten wir daher

$$\begin{aligned} |S \cdot T| &= |T| \cdot [S \cdot T : T] \\ &= |S| \cdot [S : (S \cap T)]. \end{aligned}$$

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. $T = S$. Somit besitzt die S-Konjugationsoperation auf X genau einen Fixpunkt und es folgt

$$s_p \equiv 1 \mod p$$

wie behauptet. □

Bemerkung 1.3.39 (alternativer Beweis der Existenz von Sylowgruppen)**.** Der erste Teil der Sylowsätze (Satz 1.3.35) kann alternativ zum Beispiel auch wie folgt durch Induktion über $|G|$ bewiesen werden, analog zum Beweis der Auflösbarkeit von p-Gruppen (Satz 1.3.33):

- *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.

- *Induktionsschritt.* Es sei nun p ein Teiler von $|G|$ und die Behauptung sei bereits für alle kleineren Gruppen gezeigt. Wir betrachten die Klassengleichung: Sei $(g_i)_{i\in I}$ ein Repräsentantensystem der nicht-trivialen Konjugationsklassen von G. Dann ist (Korollar 1.2.19)

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

  Wir unterscheiden nun 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 $|G|$ ist, ist somit p ein Teiler von $Z(G)$. Da $Z(G)$ abelsch ist, besitzt $Z(G)$ eine (nicht-triviale) p-Sylowgruppe T (Beispiel 1.3.32). 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 $S/T \cong U$ (nach dem Homomorphiesatz, Korollar 1.1.40) und daher (Satz von Lagrange, Korollar 1.1.24)

$$|S| = |T| \cdot |U|.$$

  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 [23, Kapitel 10].

Ausblick 1.3.40 (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 [9, 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 70
2.2 Die Primeigenschaft 82

Schlüsselbeispiel. die ganzen Zahlen, Polynomringe, Körper, Restklassenringe

2.1 Die Kategorie der Ringe

Die Kategorie der Ringe besteht aus Ringen und Ringhomomorphismen. Wir wiederholen zunächst 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 Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und Abbildungen $+, \cdot : R \times R \longrightarrow R$ (*Addition* bzw. *Multiplikation*) mit folgenden Eigenschaften:

- Das Paar $(R, +)$ bildet eine abelsche Gruppe. Wir schreiben 0 für das neutrale Element dieser Gruppe.
- Die Multiplikation ist assoziativ und es gibt ein neutrales Element bezüglich Multiplikation; dieses ist dann eindeutig bestimmt (nachrechnen) und wird mit 1 bezeichnet.
- Es gilt das *Distributivgesetz*, d.h. für alle $x, y, z \in R$ gilt

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

- Die Multiplikation ist *kommutativ*, d.h.

$$\forall_{x,y \in R} \quad x \cdot y = y \cdot x.$$

Beispiel 2.1.2 (Ringe)**.**

- Die ganzen Zahlen $\mathbb{Z}$ bilden bezüglich der gewöhnlichen Addition und Multiplikation 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 ist bezüglich seiner Addition und Multiplikation ein 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 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
$$a^2 + b^2 = (a + i \cdot b) \cdot (a - i \cdot b).$$

- 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 auch das neutrale Element der Multiplikation (also „$0 = 1$“).

- 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 $M_{n \times n}(K)$ einen *nichtkommutativen* Ring mit Eins.

Ringhomomorphismen sind strukturerhaltende Abbildungen zwischen 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
$$\forall_{x,y \in R} \quad f(x + y) = f(x) + f(y).$$

- 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.

Beispiel 2.1.4 (Ringhomomorphismen)**.**

- Die Abbildung
$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z} \\ n &\longmapsto 2 \cdot n \end{aligned}$$

ist *kein* Ringhomomorphismus, 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.

- Verknüpfungen von Ringhomomorphismen sind Ringhomomorphismen und die Identitätsabbildung auf einem Ring ist ein Ringhomomorphismus.

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 $\mathbb{Z}[i]$).
- 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 2.1.13).
- Sind S und R Ringe, so ist $S \times R$ bezüglich komponentenweiser Addition und Multiplikation ein Ring (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
$$(1, 0) \cdot (0, 1) = (0, 0)$$
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 Ringen (statt nur von Körpern). Wir erinnern uns dabei insbesondere daran, dass Polynome einfach 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

$$\left\{(a_n)_{n\in\mathbb{N}} \in \mathrm{Abb}(\mathbb{N}, R) \;\middle|\; \exists_{d\in\mathbb{N}} \quad \forall_{n\in\mathbb{N}_{\geq d}} \quad a_n = 0\right\}$$

  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. Die Familie $(T^n)_{n\in\mathbb{N}}$ ist eine R-Basis von $R[T]$. 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 einfach durch R-bilineares Ausmultiplizieren dieser Gleichung auf den Potenzen der Variablen T. Nachrechnen zeigt, dass $R[T]$ tatsächlich bezüglich den obigen Verknüpfungen einen Ring bildet.

Caveat 2.1.11 (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 2.1.12 (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 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 $a_{0,0}, a_{1,0}, \ldots, a_{d,d} \in R$ 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 2.1.13 (Wann sind Polynomringe nullteilerfrei?)**.** *Sei R ein Ring. Dann ist der Polynomring $R[T]$ genau dann ein Integritätsring, wenn R ein Integritätsring ist.*

Beweis. 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 2.1.14 (Polynomringe)**.**

- Der Polynomring $\mathbb{Z}[X, Y] = \big(\mathbb{Z}[X]\big)[Y]$ ist ein Integritätsring (wir können Proposition 2.1.13 zweimal anwenden).
- Der Polynomring $(\mathbb{Z} \times \mathbb{Z})[T]$ ist *kein* Integritätsring.

Bemerkung 2.1.15 (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: 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 2.1.16 (Quotientenkörper). *Sei R ein Integritätsring.*

1. *Dann ist*

$$\sim := \big\{\big((x,y),(x',y')\big) \;\big|\; x,x' \in R,\ y,y' \in R\setminus\{0\},\ x\cdot y' = x'\cdot y\big\}$$

   eine Äquivalenzrelation auf $R \times (R\setminus\{0\})$.

2. *Die Menge*

$$Q(R) := \big(R\times(R\setminus\{0\})\big/\sim$$

   bildet bezüglich der folgenden (wohldefinierten!) Addition und Multiplikation einen Körper, den Quotientenkörper *von R:*

$$\begin{aligned} +\colon Q(R)\times Q(R) &\longrightarrow Q(R)\\ \big([(x,y)],[(x',y')]\big) &\longmapsto \big[(x\cdot y' + x'\cdot y, y\cdot y')\big]\\ \cdot\colon Q(R)\times Q(R) &\longrightarrow Q(R)\\ \big([(x,y)],[(x',y')]\big) &\longmapsto \big[(x\cdot x', y\cdot y')\big] \end{aligned}$$

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?!). □

Beispiel 2.1.17 (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

$$(x,y) \sim (x\cdot y^{-1}, 1)$$

  (für die Relation $\sim$ aus Proposition 2.1.16).

- 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 2.1.18 (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: 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

$$f = Q(f) \circ i$$

$$\begin{array}{ccc} R & \xrightarrow{f \text{ (inj.)}} & K \\ {\scriptstyle i}\downarrow & \nearrow_{Q(f)} & \\ Q(R) & & \end{array}$$

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 2.1.19 (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 2.1.20. In der Literatur werden Ideale mit durch Frakturbuchstaben oder sonstigen unnötig komplizierten Symbolen bezeichnet. Wir werden im folgenden Ideale meist durch gewöhnliche Kleinbuchstaben notieren.

Bemerkung 2.1.21 (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

$$(A) = \left\{ \sum_{j=1}^{n} a_j \cdot r_j \;\middle|\; n \in \mathbb{N},\ r_1, \ldots, r_n \in R,\ a_1, \ldots, a_n \in A \right\}.$$

Sind $a_1, \ldots, a_n \in R$, so schreibt man auch $(a_1, \ldots, a_n)$ statt $(\{a_1, \ldots, a_n\})$.

Beispiel 2.1.22 (Ideale)**.**

- Ist R ein Ring, so sind $\{0\} = (0)$ und $R = (1)$ Ideale in 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. Das Bild $\operatorname{im} f := f(R)$ ist im allgemeinen *kein* Ideal in S.

Proposition 2.1.23 (Charakterisierung von Körpern über Ideale)**.** *Sei R ein Ring mit $R \ncong \{0\}$. 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 nichtinvertierbaren Elementen passiert (Übungsaufgabe). □

Proposition 2.1.24 (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. *Die Abbildung*
$$\begin{aligned} \cdot : R/a \times R/a &\longrightarrow R/a \\ (x + a, y + a) &\longmapsto (x \cdot y) + a \end{aligned}$$
ist wohldefiniert.
2. *Die Menge R/a bildet bezüglich der obigen Addition bzw. Multiplikation 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.

$$\begin{aligned} x \cdot y - x' \cdot y' &= x \cdot y - x \cdot y' + x \cdot y' - x' \cdot y' \\ &= x \cdot (y - y') - (x' - x) \cdot y'. \end{aligned}$$

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 2.1.25 (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 $[x]$, wenn aus dem Kontext klar ist, um welches Ideal es sich handelt.

Bemerkung 2.1.26 (Quotientenring)**.** Wir verwenden den Begriff Restklassenring statt Quotientenring (was vielleicht naheliegender wäre), um Verwechslungen mit der Quotientenkörperkonstruktion zu vermeiden.

Beispiel 2.1.27 (Restklassenringe)**.**

- Ist $n \in \mathbb{Z}$, so bildet $\mathbb{Z}/(n)$ bezüglich repräsentantenweiser Addition und Multiplikation ein Ring (die unterliegende additive Gruppe ist die zyklische Gruppe $\mathbb{Z}/n$; insbesondere enthält $\mathbb{Z}/(n)$ genau n Elemente: $[0], [1], \ldots [n-1]$).

  Zum Beispiel gilt in $\mathbb{Z}/(12)$, dass

  $$[3] \cdot [4] = [12] = [0],$$

  obwohl $[3], [4] \in \mathbb{Z}/(12) \setminus \{[0]\}$. Also ist $\mathbb{Z}/(12)$ *kein* Integritätsring.

  Außerdem gilt in $\mathbb{Z}/(12)$, dass

  $$[5]^2 = [5] \cdot [5] = [25] = [1 + 2 \cdot 12] = [1];$$

  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 $R[X,Y]/(Y) \cong R[X]$.

Beispiel 2.1.28 (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 2.1.29 (elementare Zahlentheorie)**.** Die Arithmetik in den Restklassenringen der Form $\mathbb{Z}/(n)$ kann zum Beispiel 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

$$x^2 + x + y^2 + y = 2017,$$

denn: *Angenommen,* es gäbe $x, y \in \mathbb{Z}$ mit $x^2 + x + y^2 + y = 2017$. Wir betrachten die kanonische Projektion $\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/(2)$. Da π ein Ringhomomorphismus ist, folgt

$$\pi(x)^2 + \pi(x) + \pi(y)^2 + \pi(y) = \pi(2017) = [1].$$

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 natürlich darin, einen geeigneten Restklassenring zu finden (falls ein solcher überhaupt existiert ...) und geeignete Gleichungen bzw. Invarianten in solchen Restklassenringen zu kennen.

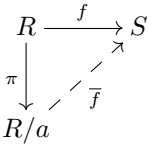
Anmerkung für Lehramtsstudenten (Wettbewerbsaufgaben)**.** Die (Un)Lösbarkeit von bestimmten Gleichungen in $\mathbb{Z}$ ist ein beliebter Gegenstand für Wettbewerbsaufgaben (z.B. Landes-/Bundeswettbewerb, Mathematik-Olympiaden, etc.). In vielen Fällen hilft dabei die Betrachtung der entsprechenden Gleichungen 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 2.1.30 (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 Ringhomomorphismus (da die Verknüpfungen auf R/a repräsentantenweise definiert sind). Der Restklassenring R/a erfüllt zusammen mit π die folgende universelle Eigenschaft: 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

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



Insbesondere zeigt dies wie im Fall von Gruppen (Bemerkung 1.1.38), dass eine Teilmenge von R genau dann ein Ideal in R ist, wenn sie Kern eines auf R definierten Ringhomomorphismus ist.

Bemerkung 2.1.31 (Homomorphie-/Isomorphiesätze für Ringe)**.** Aus der universellen Eigenschaft von Restklassenringen (Bemerkung 2.1.30) lassen sich analog zum Gruppenfall (Korollar 1.1.40, Satz 1.1.50) auch

- der Homomorphiesatz für Ringhomomorphismen und
- Isomorphiesätze für Restklassenringe

ableiten.

Beispiel 2.1.32 (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)

$$P := \left\{(x, y) \in K^2 \;\middle|\; y = x^2\right\} \subset K^2,$$

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

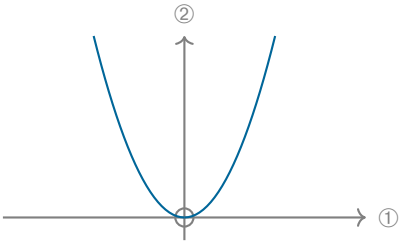


Abbildung 2.1.: Die Menge $\{(x, y) \in K^2 \mid y = x^2\}$, schematisch

$$\begin{aligned} K[X] &\longrightarrow K[X,Y]/(Y - X^2) \\ K \ni x &\longmapsto [x] \\ X &\longmapsto [X] \end{aligned}$$

wohldefinierte zueinander inverse Ringisomorphismen sind (nachrechnen). 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.

2.2.1 Teilbarkeit

Wir erinnern zunächst an die grundlegenden Teilbarkeitsbegriffe.

Definition 2.2.1 (Einheit, assoziiert, teilt)**.** 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“).

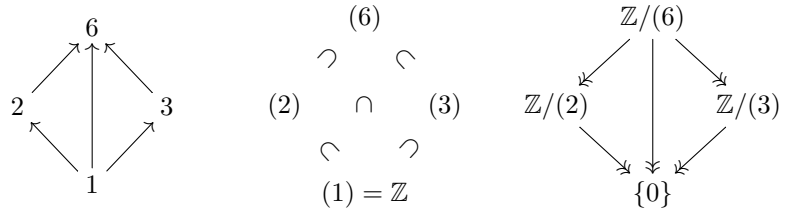


Abbildung 2.2.: Teilbarkeit, Idealinklusionen, kanonische Projektionen zwischen den zugehörigen Restklassenringen; links bedeuten dabei die Pfeile „ist ein Teiler von“.

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)**.** Sei R ein Integritätsring. Ein *Hauptideal* in R ist ein Ideal, das von einem einzelnen Element erzeugt werden kann. Man bezeichnet R als *Hauptidealring*, wenn alle Ideale in R 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.5 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.5.7).

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
$$\left(\forall_{s \in S} \quad x \mid s\right) \Longrightarrow x \mid d.$$
- 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
$$\left(\forall_{s \in S} \quad s \mid x\right) \Longrightarrow m \mid x.$$

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 $\mathrm{ggT}(x, y)$ 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.5.8).

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 2018 ist in $\mathbb{Z}$ *nicht* prim, denn es gilt
$$2018 \mid 2 \cdot 1009,$$
aber $2018 \nmid 2$ und $2018 \nmid 1009$.

- Die Zahl 2017 ist 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.2.4.17):

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 2017 ist in $\mathbb{Z}$ irreduzibel (nachrechnen). Da $\mathbb{Z}$ ein Hauptidealring ist, ist 2017 somit 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

$$\begin{aligned} \pi \colon \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \big|\{p \in \mathbb{N} \mid p \text{ prim und } p \leq x\big|. \end{aligned}$$

Nach dem *Primzahlsatz* gilt

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Asymptotisch wächst die Anzahl der Primzahlen kleiner als 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 [16].

2.2.3 Primideale und Restklassenringe

Inklusionsbeziehungen zwischen Hauptidealen lassen sich auch durch Teilbarkeitsbeziehungen ihrer Erzeuger charakterisieren (Bemerkung 2.2.2). Es liegt daher nahe, Teilbarkeitsbegriffe auch auf Ideale zu verallgemeinern. Zum Beispiel erhalten wir auf diese Weise den Begriff des Primideals:

Definition 2.2.13 (Primideal, maximales Ideal)**.** Sei R ein Ring.

- Ein Ideal $p \subset R$ in R ist *prim*, wenn $p \neq R$ 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 (2018) in $\mathbb{Z}$ ist weder ein Primideal noch maximal: Es gilt $2 \cdot 1009 \in (2018)$, aber weder $2 \in (2018)$ noch $1009 \in (2018)$. Also ist (2018) *kein* Primideal in $\mathbb{Z}$.

  Wegen $(2018) \subset (2) \subset \mathbb{Z}$ und da diese beiden Inklusionen strikt sind, ist (2018) *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 2.1.23). 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).

Sei nun R/a ein Körper. Dann hat R/a nur die beiden Ideale $\{0\}$ und R/a (Proposition 2.1.23). 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 2.1.23). □

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.3.3.19): 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 $b := \bigcup_{i \in I} b_i$ eine obere Schranke von $(b_i)_{i \in I}$ und $b \in M$, 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 $a \neq R$ ist insbesondere R nicht der Nullring. Nach Satz 2.2.18 gibt es ein maximales Ideal $m \subset R$ mit $a \subset m$. Dann hat die kanonische Projektion

$$R \longrightarrow R/m$$

in den Restklassenkörper R/m zu m (Satz 2.2.15) die gewünschte Eigenschaft. □

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 2.2.20 (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 2.2.21 (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 2.2.22 (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.

Beispiel 2.2.23 (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 2.2.22) ist wegen $10 = \mathrm{kgV}(2, 5)$ 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.

Beweis von Satz 2.2.22. 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 nun 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 $x' \in a$)

  $$[y' \cdot x + x' \cdot y]_a = [y' \cdot x]_a = [y' \cdot x + x' \cdot x]_a = [1 \cdot x]_a$$

  (und analog für die Reduktion modulo b).

Also ist $\overline{f}$ ein Ringisomorphismus; wegen $\ker f = a \cap b$ zeigt dies die Behauptung. □

Bemerkung 2.2.24 (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

$$\begin{aligned} R/\bigcap_{j=1}^{n} a_j &\longrightarrow \prod_{j=1}^{n} R/a_j \\ [x] &\longmapsto \big([x]_{a_j}\big)_{j \in \{1,\ldots,n\}} \end{aligned}$$

ein wohldefinierter Ringisomorphismus [7, 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 2.2.25 (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 1.1.48) folgt, dass $z^{p-1} = 1$ für alle $z \in \mathbb{Z}/(p)\setminus\{0\}$ gilt. □

Beispiel 2.2.26. Mit dem kleinen Satz von Fermat (Satz 2.2.25) können wir insbesondere den dritten Teil von Aufgabe 5 lösen: Da 2017 prim ist und kein Teiler von 4242 ist, gilt

$$4242^{2017} \equiv 1 \cdot 4242 \mod 2017.$$

Wegen $4242 = 2 \cdot 2017 + 208$ liefert also 4242^{2017} den Rest 208 bei Division durch 2017.

Im Zusammenspiel mit dem Chinesischen Restsatz (Satz 2.2.22 und Beispiel 2.2.23) können wir auch den zweiten Teil von Aufgabe 5 lösen:

Beispiel 2.2.27 (Ziffern bestimmen)**.** Wir bestimmen die letzte Ziffer der Zahl $(2017^{2017})^{2017}$ im Zehnersystem: Dazu machen wir noch die folgende Vorüberlegung: Sei $p \in \mathbb{N}$ prim, sei $x \in \mathbb{Z}$ und sei $k \in \mathbb{N}$. Wir bestimmen dann den Rest von x^k bei Division durch p wie folgt:

Division von k mit Rest durch $p-1$ ergibt $s, r \in \mathbb{N}$ mit

$$k = s \cdot (p-1) + r$$

und $r \in \{0, \ldots, p-2\}$. Dann liefert der kleine Satz von Fermat (Satz 2.2.25), dass

$$[x^k] = [x^{s\cdot(p-1)+r}] = [x^{p-1}]^s \cdot [x^r] = 1 \cdot [x^r]$$

in $\mathbb{Z}/(p)$ gilt (auch im Fall $p \mid x$, wenn $r \neq 0$ ist; nachrechnen).

Also erhalten wir in $\mathbb{Z}/(2)$, dass

$$\left[(2017^{2017})^{2017}\right] = [2017^{2017\cdot 2017}] = [1^0] = [1]$$

(kürzer: Potenzen ungerader Zahlen sind ungerade) bzw. in $\mathbb{Z}/(5)$, dass

$$\left[(2017^{2017})^{2017}\right] = [2017^{2017\cdot 2017}] = [2^{1\cdot 1}] = [2].$$

Mit dem Chinesischen Restsatz (Satz 2.2.22 und Beispiel 2.2.23) erhalten wir daraus, dass 7 die gesuchte Endziffer ist.

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 4, aber das ist von Hand nicht machbar).

Ausblick 2.2.28 (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 2.2.25) *nicht* prim.
- Ist $r = 1$, so iterieren wir das Verfahren einige Male (mit „unabhängigen“, „zufälligen“ a).

Wenn wir für „viele“ $a \in \{2, \ldots, p-2\}$ 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 2.2.29).

Ausblick 2.2.29 (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 2.2.25) erfüllt, d.h. für alle $a \in \{1, \ldots, p-1\}$ 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 2.2.30 (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 $\varphi(m) := \left|\{x \in \{1, \ldots, m-1\} \mid \mathrm{ggT}(x, m) = 1\}\right| \in \mathbb{N}$. Dann folgt insbesondere*
$$\left|\mathbb{Z}/(m)^\times\right| = \varphi(m).$$

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 2.2.31 (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)

$$\varphi(p \cdot q) = p \cdot q - p - q + 1 = (p - 1) \cdot (q - 1).$$

Insbesondere ist $\varphi(10) = 1 \cdot 4 = 4$.

Satz 2.2.32 (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 2.2.30).

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 2.2.30 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 1.1.48) erhalten wir daher in $\mathbb{Z}/(m)$:

$$[x]^{\varphi(m)} = [1]$$ □

Ausblick 2.2.33 (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 2.2.31).

- 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 nun die Abbildungen

$$\begin{aligned} E\colon \mathbb{Z}/(m) &\longmapsto \mathbb{Z}/(m) \\ x &\longmapsto x^e, \\ D\colon \mathbb{Z}/(m) &\longmapsto \mathbb{Z}/(m) \\ x &\longmapsto x^d. \end{aligned}$$

Mit dem kleinen Satz von Fermat (Satz 2.2.32) erhalten wir (wegen $d \cdot e \equiv 1 \mod \varphi(m)$, analog zu Beispiel 2.2.27)

$$D \circ E(x) = x^{d \cdot e} = x^1$$

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 von Satz 2.2.25 und dem Chinesischen Restsatz (Satz 2.2.22).

Wie kann man dies nun 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 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 2.2.28 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 nun mit dem euklidischen Algorithmus aus d bestimmen. 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* [29] 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 2.2.34 (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.

Wir verwenden außerdem die folgende Notation: Ist $p \in R$ 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 2.2.35 (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 $\sigma \in S_n$ und 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. Diese Eindeutigkeitsaussage ist der Grund für die Formulierung der Definition der Primeigenschaft.

Bemerkung 2.2.36 (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 2.2.37 (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 $a_0 \subset a_1 \subset a_2 \subset \ldots$ 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.2.4.22, Satz II.2.4.21) 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 be-

trachten 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 .... 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, *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 2.2.38 (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:

Bemerkung 2.2.39 (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)

$$\begin{aligned} \mathrm{ggT}(x, y) &= \prod_{p \in P} p^{\min(\nu_p(x), \nu_p(y))} \\ \mathrm{kgV}(x, y) &= \prod_{p \in P} p^{\max(\nu_p(x), \nu_p(y))}. \end{aligned}$$

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 2.2.40 (Satz von Gauß)**.** *Ist R ein faktorieller Ring, so ist auch der Polynomring $R[T]$ faktoriell.*

Beispiel 2.2.41 (faktorielle Polynomringe)**.**

- Da $\mathbb{Z}$ als Hauptidealring ein faktorieller Ring ist, ist $\mathbb{Z}[T]$ nach dem Satz von Gauß (Satz 2.2.40) 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 2.2.40), 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.5.5); insbesondere ist $\mathbb{Z}[i]$ faktoriell. Also ist nach dem Satz von Gauß (Satz 2.2.40) auch $(\mathbb{Z}[i])[T]$ faktoriell.

Wie beweist man den Satz von Gauß? Sei R ein faktorieller Ring. Dann betrachten wir den Quotientenkörper $Q(R)$ (Proposition 2.1.16) 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 auf $Q(R)$ und $Q(R)[T]$:

Definition 2.2.42 (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

$$\nu_p\Big[\frac{x}{y}\Big] := \nu_p(x) - \nu_p(y) \in \mathbb{Z} \cup \{\infty\}.$$

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
$$\nu_p(f) := \min\big\{\nu_p(a_j) \;\big|\; j \in \{0, \ldots, n\}\big\} \in \mathbb{Z} \cup \{\infty\}.$$

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 2.2.43 (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 2.2.44 (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 von Lemma 2.2.44. 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

$$\begin{aligned}\nu_p(f\cdot g) &= \nu_p\Big(\sum_{j=0}^{n} f\cdot b_j\cdot T^j\Big)\\ &= \min\big\{\nu_p(f\cdot b_j)\;\big|\; j\in\{0,\dots,n\}\big\}\\ &= \min\big\{\nu_p(f)+\nu_p(b_j)\;\big|\; j\in\{0,\dots,n\}\big\}\\ &= \nu_p(f)+\min\big\{\nu_p(b_j)\;\big|\; j\in\{0,\dots,n\}\big\}\\ &= \nu_p(f)+\nu_p(g).\end{aligned}$$

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 2.1.13). Nach Konstruktion ist dabei

$$\ker\pi=\big\{h\in R[T]\;\big|\;\nu_p(h)>0\big\}.$$

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

$$\begin{aligned}\nu_p(c\cdot d)+\nu_p(f\cdot g) &= \nu_p(c\cdot f\cdot d\cdot g) && \text{(nach dem zweiten Schritt)}\\ &= 0=\nu_p(c\cdot f)+\nu_p(d\cdot g) && \text{(nach dem dritten Schritt)}\\ &= \nu_p(c\cdot d)+\nu_p(f)+\nu_p(g) && \text{(nach dem zweiten/ersten Schritt),}\end{aligned}$$

und damit $\nu_p(f\cdot g)=\nu_p(f)+\nu_p(g)$.

Insgesamt folgt damit der erste Teil.

Zu 2. Mit f und g ist auch das Produkt $f\cdot g$ normiert (nachrechnen). Sei $p\in R$ prim. Da f und g normiert sind, folgt $\nu_p(f)\leq 0$ und $\nu_p(g)\leq 0$. Da $f\cdot g$ normiert ist und alle Koeffizienten in R liegen, gilt sogar $\nu_p(f\cdot g)=0$. Aus dem ersten Teil erhalten wir daher

$$0=\nu_p(f\cdot g)=\nu_p(f)+\nu_p(g),$$

und damit

$$\nu_p(f)=0=\nu_p(g).$$

Da dies für alle Primelemente gilt, folgt, dass in f und g keine echten Nenner auftreten können. Also gilt $f, g \in R[T]$. □

Definition 2.2.45 (primitives Polynom)**.** Sei R ein faktorieller Ring. Ein Polynom $f \in R[T]$ ist *primitiv*, wenn für alle Primelemente $p \in R$ gilt, dass

$$\nu_p(f) = 0.$$

Wir beweisen nun den Satz von Gauß (Satz 2.2.40):

Beweis von Satz 2.2.40. 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 2.2.45) 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 2.2.44 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).

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 2.2.44) und der Tatsache, dass q primitiv ist, erhalten wir für alle Primelemente $p \in R$, dass

$$\nu_p(h) = \nu_p(q \cdot h) - \nu_p(q) = \nu_p(f) - \nu_p(q) = \nu_p(f) \geq 0.$$

Also ist $h \in R[T]$ (Bemerkung 2.2.43); 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 2.2.37). 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 2.2.44) 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 $c \in R$ 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:

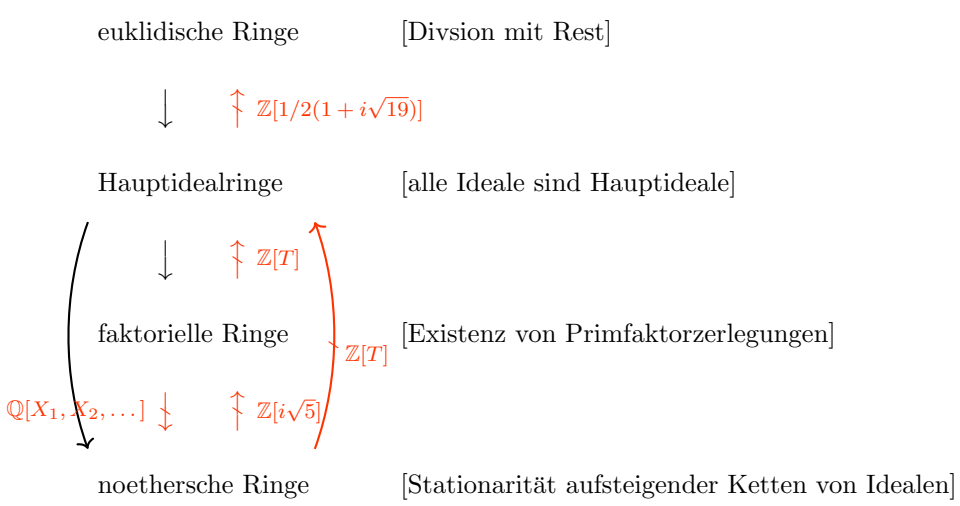


Abbildung 2.3.: Eigenschaften von Ringen

Korollar 2.2.46. *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 2.2.40) 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 2.2.36, Proposition 2.2.11).

Es genügt daher, die Äquivalenz der ersten und dritten Aussage zu zeigen:

Zu $3 \implies 1$*:* 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 $1 \implies 3$*:* 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.

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 so interessante Körper.

Beispiel 2.2.47 (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. Genauer gilt: Mit der universellen Eigenschaft von Polynom- bzw. Restklassenringen folgt, dass

$$\begin{aligned} \mathbb{R}[T]/(X^2+1) &\longrightarrow \mathbb{C} \\ [\mathbb{R} \ni x] &\longmapsto x \\ [X] &\longmapsto i \end{aligned}$$

ein Ringisomorphismus ist (Übungsaufgabe). Man kann die imaginäre Einheit i auf diese Weise also durch eine einfache algebraische Konstruktion gewinnen. Analog erhält man so den Körper $\mathbb{F}_7[T]/(T^2+1)$ mit 49 Elementen (Übungsaufgabe).

Daher ist es nützlich, Kriterien zu kennen, die zeigen, dass gewisse Polynome irreduzibel sind. Wir behandeln im folgenden das Nullstellenkriterium, das Reduktionskriterium und das Eisensteinsche Irreduzibilitätskriterium und geben ein paar Standardbeispiele dazu.

Proposition 2.2.48 (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 reduzibel in $K[T]$.*
2. *Gilt*
$$\deg f \in \{2, 3\} \quad \text{und} \quad \forall_{x \in K} \quad f(x) \neq 0,$$
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 $\deg f \in \{2, 3\}$. Wegen $\deg f > 0$ ist $f \notin \{0\} \cup K[T]^\times$. Wir beweisen die Behauptung durch Kontraposition:

Sei f reduzibel in $K[T]$. 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

$$f\Big(-\frac{b}{a}\Big) = g\Big(-\frac{b}{a}\Big) \cdot h\Big(-\frac{b}{a}\Big) = 0. \qquad \square$$

Korollar 2.2.49. *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 2.2.48, 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 2.2.50 (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. Sei f primitiv und reduzibel in $R[T]$. Dann ist $\pi(f)$ reduzibel in $R/(p)[T]$, denn: Da f in $R[T]$ reduzibel ist, gibt es $g, h \in R[T]$ mit $f = g \cdot h$. Also ist

$$\pi(f) = \pi(g \cdot h) = \pi(g) \cdot \pi(h).$$

Wir zeigen nun, 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 zusätzlich $\deg \pi(f) = \deg f$. Also erhalten wir (da R und $R/(p)$ Integritätsringe sind, sind die Grade auf den zugehörigen Polynomringen additiv; Beweis von Proposition 2.1.13)

$$\begin{aligned} \deg g + \deg h &= \deg f \\ &= \deg \pi(f) \\ &= \deg\big(\pi(g) \cdot \pi(h)\big) \\ &= \deg \pi(g) + \deg \pi(h) \\ &\leq \deg g + \deg h, \end{aligned}$$

und damit $\deg \pi(g) = \deg g > 0$ und $\deg \pi(h) = \deg h > 0$. Somit ist $\pi(f)$ reduzibel 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 2.2.46 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 2.2.51 (Reduktionskriterium, in Kombination mit dem Nullstellkriterium)**.**

- Das Polynom
$$f := T^2 + 5555 \cdot T - 2017 \in \mathbb{Z}[T]$$
ist irreduzibel in $\mathbb{Z}[T]$ (und $\mathbb{Q}[T]$), denn: Reduktion modulo $5 \in \mathbb{Z}$ liefert das Polynom
$$T^2 - 2 \in \mathbb{F}_5[T],$$
welches nach dem Nullstellenkriterium (Proposition 2.2.48) in $\mathbb{F}_5[T]$ irreduzibel ist (nachrechnen). Das Reduktionskriterium (Satz 2.2.50; 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
$$Y^2 + 1 \in \big(\mathbb{R}[X]/(X)\big)[Y] \cong \mathbb{R}[Y],$$
welches nach dem Nullstellenkriterium (Proposition 2.2.48) in $\mathbb{R}[Y]$ irreduzibel ist (nachrechnen). Das Reduktionskriterium (Satz 2.2.50; anwendbar!) liefert, dass f in $\mathbb{R}[X, Y]$ irreduzibel ist.

Satz 2.2.52 (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 $a_0, \ldots, a_n \in R$. 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 2.2.50) zurückführen [7, S. 62] oder die Behauptung von Hand nachrechnen. Wir werden letzteres durchführen: Es genügt zu zeigen, dass f in $R[T]$ irreduzibel ist (Korollar 2.2.46). 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 p 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 2.2.53 (Eisenstein)**.**

- Die Polynome $T^3 - 2$ und $T^{2017} - 2$ 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 $T^3 - 2$ 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 2.2.52) 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 dann, 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 aber 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	112
3.2	Die Kategorie der Körpererweiterungen	114
3.3	Endliche Körper	140
3.4	Galoiserweiterungen	148
3.5	Anwendungen der Galoistheorie	161

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, Körperhomomorphismus)**.** 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. Ein *Körperhomomorphismus* ist ein Ringhomomorphismus zwischen Körpern.

Proposition 3.1.2 (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 3.1.3 (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 3.1.4 (Körper)**.**

- Die rationalen Zahlen bilden den Körper $\mathbb{Q}$ (der Charakteristik 0).
- Die reellen Zahlen bilden den Körper $\mathbb{R}$ (der Charakteristik 0).
- Die komplexen Zahlen bilden den Körper $\mathbb{C}$ (der Charakteristik 0).
- Ist $p \in \mathbb{N}$ prim, so ist $\mathbb{F}_p = \mathbb{Z}/(p)$ ein Körper der Charakteristik p.
- Der Körper $\mathbb{F}_7[T]/(T^2+1)$ (Beispiel 2.2.47) hat Charakteristik 7.
- Ist K ein Körper, so ist $K(T)$ unendlich und $\operatorname{char} K(T) = \operatorname{char} K$.

Caveat 3.1.5 (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 2.1.17).

Die Ringtheorie ermöglicht es, mithilfe von Polynomen aus Körpern weitere Körper zu konstruieren (Beispiel 2.2.47). 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 3.1.6 (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 2.1.23). 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 3.1.7. *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

$$G \cong \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_k^{n_k}$$

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 2.2.22) zu zeigen, dass $m = n$ ist.

Wir betrachten dazu das Polynom

$$f := T^m - 1 \in K[T].$$

Nach Wahl von m gilt dann (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 2.2.49), 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 [7, Kapitel 3.6]). □

Im Kontext von Einheitswurzeln und Kreisteilungskörpern wird dieser Satz hilfreich sein (Beispiel 3.2.27).

Korollar 3.1.8 (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 3.1.7) und Korollar 1.1.47. □

Diese Tatsache wird bei der Konstruktion von linear feedback shift registers und bei der Umsetzung von RAID(6) genutzt (Beispiel 3.3.9, 3.3.10)

Wie bereits angedeutet, werden wir uns nun genauer mit Körpererweiterungen statt mit einzelnen Körpern auseinandersetzen; in diesem Kontext werden wir systematisch Konstruktionen von Körpern untersuchen.

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 platzverschendend) 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 3.1.6), 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 $\mathbb{C} \mid \mathbb{C}$, $\mathbb{C} \mid \mathbb{R}$ und $\mathbb{R} \mid \mathbb{Q}$ Körpererweiterungen; außerdem ist $\mathbb{R}$ ein Zwischenkörper von $\mathbb{C} \mid \mathbb{R}$.
- 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 nun 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 2.1.18) 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 $\operatorname{im} E_\alpha \cong K[T]/\ker E_\alpha$ als Unterring des Körpers L ein Integritätsring ist; Satz 2.2.15). Da $K[T]$ ein Hauptidealring ist, ist a bereits maximal (Beispiel 2.2.14); also ist $\operatorname{im} E_\alpha \cong K[T]/a$ ein Körper (Satz 2.2.15). Wegen $\alpha \in \operatorname{im} E_\alpha \subset K(\alpha)$ folgt somit

$$K(\alpha) = \operatorname{im} E_\alpha \cong K[T]/\ker E_\alpha.$$

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 $[\mathbb{C} : \mathbb{R}] = 2$ und $[\mathbb{C} : \mathbb{Q}] = \infty$ sowie $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.
- Ist K ein Körper, so ist $[K(T) : K] = \infty$ 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

$$L = \operatorname{Span}_K S \subset K(S) \subset L$$

folgt dann 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 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 zum Beispiel 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.

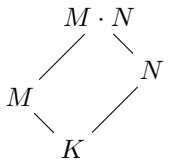


Abbildung 3.1.: Der Diamant des Kompositums $M \cdot N$ in $L \mid K$

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 2018 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 2018 *keine* Primpotenz ist (nachrechnen), gibt es also *keinen* Körper mit genau 2018 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* $L \mid K$.

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:

Da σ ein Körperhomomorphismus (mit $\sigma|_\mathbb{Q} = \mathrm{id}_\mathbb{Q}$) 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. $\mathrm{Gal}(\mathbb{C},\mathbb{R}) \cong \mathbb{Z}/2$.

Mit demselben Argument folgt auch (in $\mathbb{C} \mid \mathbb{Q}$)

$$\begin{aligned}\mathrm{Gal}\big(\mathbb{Q}(i),\mathbb{Q}\big) &\cong \mathbb{Z}/2 \\ \mathrm{Gal}\big(\mathbb{Q}(\sqrt{2}),\mathbb{Q}\big) &\cong \mathbb{Z}/2.\end{aligned}$$

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 $\sqrt[3]{2}$ und ist invariant unter Elementen von $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q})$.

Wir werden uns in den nächsten Abschnitten mit den folgenden Fragen beschäftigen:

- 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 $\mathbb{Q}$ [28, 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 2.2.49), 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 nun 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*

$$K(\alpha) \cong K(T) \quad \textit{und} \quad [K(\alpha) : K] = \infty.$$

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*

$$K(\alpha) \cong K[T]/\ker E_\alpha.$$

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 $K(\alpha) \cong K[T]/\ker E_\alpha$ 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 nun noch $[K(\alpha) : K]$: Sei $d := \deg \mu_\alpha$. Wir zeigen, dass die Familie $(1, \alpha, \dots, \alpha^{d-1})$ eine K-Basis von $K(\alpha)$ ist:

- Diese Familie ist erzeugend, denn: Sei $x \in K(\alpha)$. Wegen $K(\alpha) = \operatorname{im} E_\alpha \cong K[T]/(\mu_\alpha)$ 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

  $$x = g(\alpha) \in \operatorname{Span}_K\{1, \alpha, \dots, \alpha^{d-1}\}.$$

- Diese Familie ist linear unabhängig über K, denn: Seien $\lambda_0, \dots, \lambda_{d-1} \in K$ 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, dass f das Nullpolynom ist. Also ist $\lambda_j = 0$ für alle $j \in \{0, \dots, d-1\}$.

Also ist $(1, \alpha, \dots, \alpha^{d-1})$ 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 $(1, \alpha, \dots, \alpha^{d-1})$ über K linear abhängig ist; außerdem können wir durch Lösen eines linearen Gleichungssystems die Werte $\lambda_0, \dots, \lambda_{d-1} \in K$ 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!)

Beispiel 3.2.26 (reelle Wurzeln)**.** Wir betrachten den Zwischenkörper $\mathbb{Q}(\sqrt[3]{2})$ von $\mathbb{C} \mid \mathbb{Q}$. Es gilt

$$\big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big] = 3,$$

denn: Das Polynom $T^3 - 2 \in \mathbb{Q}[T]$ ist irreduzibel (Beispiel 2.2.53) und normiert und daher das Minimalpolynom der Nullstelle $\sqrt[3]{2}$ (Bemerkung 3.2.25). Also erhalten wir mit Proposition 3.2.24, dass

$$\big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big] = \deg(T^3 - 2) = 3.$$

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

$$\big[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}\big] = n;$$

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

$$\big[\mathbb{Q}(\sqrt[1009]{2}, \sqrt{2017}) : \mathbb{Q}\big] = 1009 \cdot 2 = 2018.$$

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 2.2.49).

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 endliche Untergruppe von $L^\times$ zyklisch (nach Satz 3.1.7). 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

$$1,\ \zeta_n,\ \ldots,\ \zeta_n^{n-1}$$

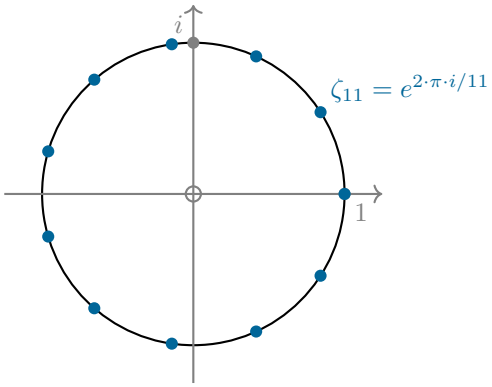


Abbildung 3.2.: Die elften Einheitswurzeln in $\mathbb{C}$

die n-ten Einheitswurzeln in $\mathbb{C}$ (Abbildung 3.2). Es gilt $U_n(\mathbb{C}) \cong \mathbb{Z}/n$ (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 2.2.30). 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.*

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.*

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 $\widetilde{\sigma}|_K = \sigma$ mit $\widetilde{\sigma}(\alpha) = \beta$.*

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

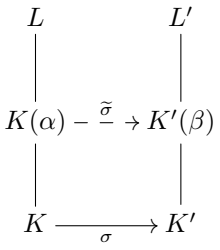


Abbildung 3.3.: Das Konjugationsprinzip, schematisch

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. $\beta \in L'$. 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. 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). Dann 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.*

1. *Für alle $\beta \in X$ gilt $K(\beta) = K(\alpha)$.*

2. Dann ist

$$\begin{aligned} \mathrm{Gal}\big(K(\alpha), K\big) &\longrightarrow S_X \\ \sigma &\longmapsto \big(x \mapsto \sigma(x)\big) \end{aligned}$$

ein wohldefinierter und injektiver Gruppenhomomorphismus. Die zugehörige Gruppenoperation von $\mathrm{Gal}(K(\alpha), K)$ *auf* X *ist transitiv.*

3. Dabei gilt

$$\big|\mathrm{Gal}\big(K(\alpha), K\big)\big| = |X| \leq \deg \mu_\alpha = \big[K(\alpha) : K\big].$$

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

$$\dim_K K(\beta) = \big[K(\beta) : K\big] = \deg \mu_\alpha = \big[K(\alpha) : K\big] = \dim_K K(\alpha).$$

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 $|\mathrm{Gal}(K(\alpha), K)| = |X|$. Da μ_α in $K(\alpha)$ höchstens $\deg \mu_\alpha$ Nullstellen besitzt (Korollar 2.2.49), folgt zusammen mit Proposition 3.2.24 die gesamte (Un)Gleichungskette. □

Zum Beispiel haben wir das obige Prinzip bei der Berechnung der Galoisgruppe von $\mathbb{C} \mid \mathbb{R}$ verwendet (Beispiel 3.2.19).

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.
- 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. Also ist α *nicht* transzendent über K (Proposition 3.2.24), und damit 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

$$\mathbb{C} \mid \mathbb{R},\ \mathbb{Q}(\sqrt{2}) \mid \mathbb{Q},\ \mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q},\ \mathbb{Q}(\zeta_{11}) \mid \mathbb{Q}, \ldots$$

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 $\alpha \in K(S')$ (dies kann man zum Beispiel aus der expliziten Darstellung aus Bemerkung 3.2.6 ableiten).

Induktiv (über $|S'|$) folgt mithilfe von Proposition 3.2.24, dass die Erweiterung $K(S') \mid K$ endlich ist. 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

$$\frac{\sqrt[2017]{2018 + \sqrt[42]{2019}}}{42 + \sqrt[1995]{386}}$$

algebraisch über $\mathbb{Q}$ (nachrechnen), obwohl wir vielleicht nicht unbedingt ein 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. 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 $\mathbb{R}$.
- Aber $\mathbb{R}$ ist *kein* Zerfällungskörper von $T^2 - 2$ über $\mathbb{Q}$ (da $\mathbb{R}$ „zu groß“ ist).
- 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 $\mathbb{Q}$.

Beispiel 3.2.41. Wir bestimmen einen Zerfällungskörper für $T^3 - 2 \in \mathbb{Q}[T]$ über $\mathbb{Q}$: Dazu betrachten wir die Körpererweiterung $\mathbb{C} \mid \mathbb{Q}$. 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 $\mathbb{Q}$!

Wir versuchen 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 $\mathrm{ggT}(3, 2) = 1$ erhalten wir (Proposition 3.2.12)

$$[K : \mathbb{Q}] = \big[\mathbb{Q}(\alpha) \cdot \mathbb{Q}(\zeta_3) : \mathbb{Q}\big] = \big[\mathbb{Q}(\alpha) : \mathbb{Q}\big] \cdot \big[\mathbb{Q}(\zeta_3) : \mathbb{Q}\big] = 3 \cdot 2 = 6.$$

  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 dem Zusammenhang 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 nun $\mathrm{Gal}(K, \mathbb{Q})$: Dazu verwenden wir die Zerlegung von $K \mid \mathbb{Q}$ in $\mathbb{Q}(\zeta_3) \mid \mathbb{Q}$ und $K \mid \mathbb{Q}(\zeta_3)$ und gehen dann wie folgt vor:
  1. Wir zeigen, dass die Einschränkung auf $\mathbb{Q}(\zeta_3)$ einen wohldefinierten Gruppenhomomorphismus $\mathrm{Gal}(K, \mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q})$ liefert.
  2. Wir bestimmen die Gruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q})$ mit dem Konjugationsprinzip.
  3. Wir bestimmen für jedes Element von $\mathrm{Gal}(\mathbb{Q}(\zeta_3), \mathbb{Q})$ alle möglichen Fortsetzungen zu Elementen von $\mathrm{Gal}(K, \mathbb{Q})$ mit dem Konjugationsprinzip. Damit erhalten wir $\mathrm{Gal}(K, \mathbb{Q})$ als Menge.
  4. Wir bestimmen die Gruppenstruktur auf $\mathrm{Gal}(K, \mathbb{Q})$ durch Berechnung der Werte von Verknüpfungen auf ζ_3 und α.

  Zu 1. Sei $\sigma \in \mathrm{Gal}(K, \mathbb{Q})$. 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 $\sigma(\mathbb{Q}(\zeta_3)) \subset \mathbb{Q}(\zeta_3)$. 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.

  Zu 2. Wegen $\zeta_3^2 = \overline{\zeta}_3$ erhalten wir mit dem Konjugationsprinzip (Korollar 3.2.29, Beispiel 3.2.19), dass

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_3), \mathbb{Q}\big) = \{\mathrm{id}, c\}$$

  ist, 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):

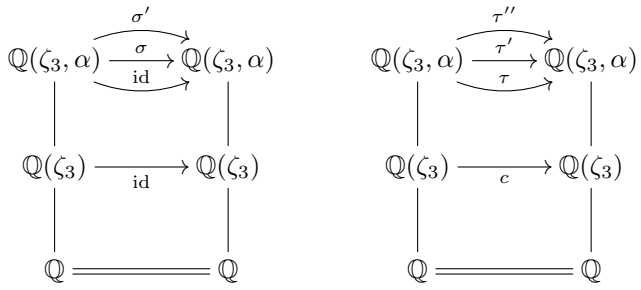


Abbildung 3.4.: Die Elemente von $\mathrm{Gal}(K, \mathbb{Q})$, schematisch

– 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 $\zeta_3 \longmapsto \zeta_3$):

$$\sqrt[3]{2} \longmapsto \sqrt[3]{2} \qquad \text{(dies liefert die Identität auf } K\text{)}$$
$$\sqrt[3]{2} \longmapsto \zeta_3 \cdot \sqrt[3]{2} \qquad \text{(diesen Automorphismus nennen wir } \sigma\text{)}$$
$$\sqrt[3]{2} \longmapsto \zeta_3^2 \cdot \sqrt[3]{2} \qquad \text{(diesen Automorphismus nennen wir } \sigma'\text{)}$$

– Fortsetzungen von c: Es gibt genau drei solche Fortsetzungen und diese sind jeweils eindeutig durch die folgenden Zuordnungen bestimmt (zusätzlich zu $\zeta_3 \longmapsto \zeta_3^2$):

$$\sqrt[3]{2} \longmapsto \sqrt[3]{2} \qquad \text{(diesen Automorphismus nennen wir } \tau'\text{)}$$
$$\sqrt[3]{2} \longmapsto \zeta_3 \cdot \sqrt[3]{2} \qquad \text{(diesen Automorphismus nennen wir } \tau\text{)}$$
$$\sqrt[3]{2} \longmapsto \zeta_3^2 \cdot \sqrt[3]{2} \qquad \text{(diesen Automorphismus nennen wir } \tau''\text{)}$$

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:

$$\sigma^2 = \sigma', \quad \mathrm{ord}(\sigma) = 3, \quad \mathrm{ord}(\tau) = 2, \quad \tau \circ \sigma \circ \tau = \sigma^2 = \sigma^{-1}, \quad \ldots$$

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 $\mathrm{Gal}(K, \mathbb{Q})$

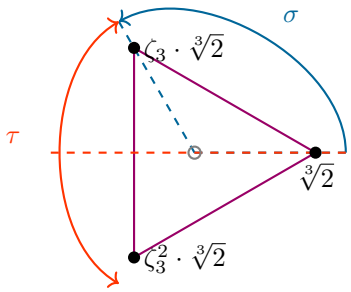


Abbildung 3.6.: Geometrie der Operation der Galoisgruppe $\mathrm{Gal}(K, \mathbb{Q})$ auf den Nullstellen $\{\sqrt[3]{2}, \zeta_3 \cdot \sqrt[3]{2}, \zeta_3^3 \cdot \sqrt[3]{2}\}$ von $T^3 - 2$ in K

Eine einfache Rechnung zeigt nun, dass $\mathrm{Gal}(K, \mathbb{Q})$ das semi-direkte Produkt von $\langle\sigma\rangle_{\mathrm{Gal}(K,\mathbb{Q})} \cong \mathbb{Z}/3$ mit $\langle\tau\rangle_{\mathrm{Gal}(K,\mathbb{Q})} \cong \mathbb{Z}/2$ ist, wobei letztere Gruppe auf der ersten durch Inversion operiert. Also ist (Abbildung 3.6)

$$\mathrm{Gal}(K, \mathbb{Q}) \cong D_3 \cong S_3.$$

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 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. Wir zeigen zunächst die folgende Aussage:

(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 $L \mid K$ 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 genügt also, die Aussage (Z) zu beweisen. Wir gehen dazu induktiv vor: Ist $\deg f \leq 1$, so hat die Erweiterung $K \mid K$ die gewünschte Eigenschaft.

Wir nehmen nun an, dass $\deg f > 1$ ist und dass (Z) für Polynome von kleinerem Grad bereits bewiesen ist. Wir unterscheiden zwei Fälle:

- 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 $N \mid M$, so dass g in M und h in N in Linearfaktoren zerfällt. Dann zerfällt f in N in Linearfaktoren.
- Ist f irreduzibel, so ist $M := K[T]/(f)$ ein Körper mit kanonischer Inklusion $K \subset M$. Außerdem besitzt f in M eine Nullstelle (nach Konstruktion nämlich die Restklasse von T im Restklassenring M). Damit ist f reduzibel über M und wir können den reduziblen Fall 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. Wir beweisen 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 n.

Induktionsschritt. Sei nun $\sigma\colon K \longrightarrow K'$ 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:

- 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

$$\widetilde{\sigma}|_K = \tau|_K = \sigma.$$

- 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.

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 werden die Auflösbarkeitseigenschaften der zugehörigen Galoisgruppen eine entscheidende Rolle spielen (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 3.5.29) 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).
- 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 *nicht* algebraisch abgeschlossen: zum Beispiel besitzt das Polynom $X^2 - T$ *keine* Nullstelle in $K(T)$ (nachrechnen oder mit dem Eisensteinschein Irreduzibilitätskriterium (Satz 2.2.52) 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 2.2.48).

Satz 3.2.50 (Existenz algebraischer Abschlüsse)**.** *Jeder Körper besitzt einen algebraischen Abschluss.*

Beweis. 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. □

Bemerkung 3.2.51. In der obigen Konstruktion ist sogar bereits $C(K)$ ein algebraischer Abschluss von K [7, Aufgabe 11 in Kapitel 3.7].

Beispiel 3.2.52. Insbesondere gibt es algebraisch abgeschlossene Körper positiver Charakteristik, z.B. ein algebraischer Abschluss von $\mathbb{F}_2$.

Beispiel 3.2.53 (Jordansche Normalform)**.** Sei K ein Körper und $n \in \mathbb{N}$ und sei $L \mid K$ ein algebraischer Abschluss von K. Ist $A \in M_{n\times n}(K)$, 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 3.2.54 (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 Körpermorphismus $\sigma\colon M \longrightarrow M$ 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. Zu 1. Dies folgt mit dem Lemma von Zorn (Satz I.3.3.19) aus dem Konjugationsprinzip (Proposition 3.2.28): Wir betrachten dazu die Menge

$$\begin{aligned} F := \big\{(Z, f) \;\big|\; & Z \text{ ist ein Zwischenkörper von } L \mid K \\ & \text{und } f\colon Z \longrightarrow M \text{ ist ein Körpermorphismus} \\ & \text{mit } f|_K = \mathrm{id}_K\big\}. \end{aligned}$$

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 gibt es ein $\alpha \in L \setminus Z$. 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 3.1.6). 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 Körpermorphismen $f\colon M \longrightarrow N$ 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 $\cong \mathbb{F}_p$) des Polynoms*
$$T^{p^k} - T.$$

2. *Sei F ein Körper mit $|F| = p^k$ und Primkörper $K \cong \mathbb{F}_p$. 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 1.1.48) 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 2.2.49). 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 $\mathbb{F}_p$.

Bestimmung der Galoisgruppe. Mithilfe von $\operatorname{char} F = p$ folgt, dass der Frobeniusendomorphismus $\sigma \colon F \longrightarrow F$ tatsächlich ein Körperisomorphismus mit $\sigma|_K = \mathrm{id}_K$ ist (Übungsaufgabe).

Warum ist σ ein Erzeuger von $\operatorname{Gal}(F, K)$? Dafür genügt es zu zeigen, dass $|\operatorname{Gal}(F, K)| \leq k$ und $\operatorname{ord} \sigma \geq k$ ist:

Die Einheitengruppe $F^\times$ ist zyklisch (Korollar 3.1.8). 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

$$\big|\operatorname{Gal}(F, K)\big| \leq \big[K(\alpha) : K\big] = [F : K] = \log_p p^k = k.$$

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 2.2.49)

$$p^k = |F| \leq \deg(T^{p^m} - T) = p^m,$$

und damit $k \leq m$. Also ist σ ein Erzeuger von $\operatorname{Gal}(F, K)$ und induziert somit einen Gruppenisomorphismus $\mathbb{Z}/k \cong \operatorname{Gal}(F, K)$.

Existenz. Sei F ein Zerfällungskörper von f über $\mathbb{F}_p$. Wir zeigen nun, 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

$$|F| = |N| \leq \deg f = p^k.$$

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

$$Df = p^k \cdot T^{p^k-1} - 1 \cdot T^0 = -1$$

hat f in F somit 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 2.2.48 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* $\mathrm{ggT}(f, Df) \neq 1$ *(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 2.2.25) 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 natürlich *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.

Beispiel 3.3.8 (ein Körper mit 256 Elementen)**.** Sei F ein endlicher Körper der Charakteristik p. Wir wissen bereits, dass die Einheitengruppe $F^\times$ zyklisch ist (Korollar 3.1.8). Sei $\alpha \in F^\times$ ein Erzeuger dieser Einheitengruppe und sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über dem Primkörper $K \cong \mathbb{F}_p$ 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

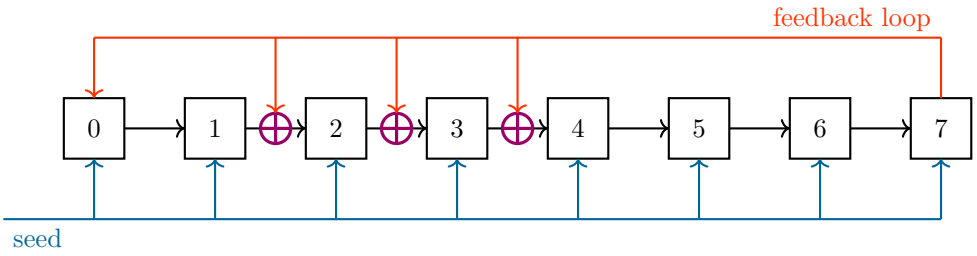


Abbildung 3.7.: Das LFSR zum Polynom $T^8 + T^4 + T^3 + T^2 + 1 \in \mathbb{F}_2[T]$

$$\big(K[T]/(\mu_\alpha)\big)^\times = \big\{[T^j] \;\big|\; j \in \{0, \dots, |F| - 1\}\big\}.$$

Wir geben nun 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 1.1.48) 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 3.3.9 (LFSR)**.** Sei $f \in \mathbb{F}_2[T]$ das Polynom aus Beispiel 3.3.8 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 $\mathbb{F}_2$-Vektorraumisomorphismus

$$F \longrightarrow {\mathbb{F}_2}^8.$$

Multiplikation mit $[T]$ in F liefert unter diesem Isomorphismus die Abbildung

$$R\colon \mathbb{F}_2{}^8 \longrightarrow \mathbb{F}_2{}^8$$
$$x \longmapsto \begin{pmatrix} x_7 \\ x_0 \\ x_1 + x_7 \\ x_2 + x_7 \\ x_3 + x_7 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}$$

(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 3.7, 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 3.7 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 2.2.28).

Beispiel 3.3.10 (RAID(6))**.** Eine Anwendung von LFSRs (Beispiel 3.3.9) ist bei der praktischen Umsetzung von RAID(6): Möchte man große Mengen

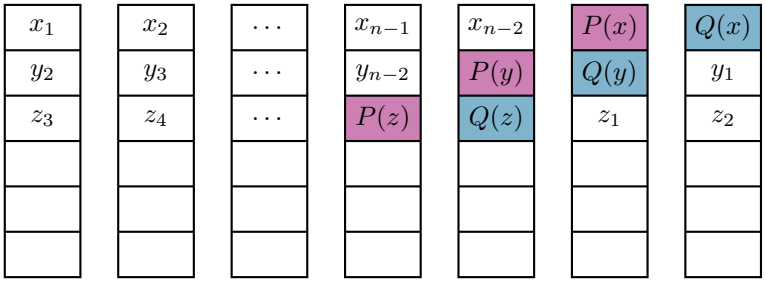


Abbildung 3.8.: RAID(6), schematische Verteilung von Datenblöcken und Kontrollblöcken

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 3.8 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 3.3.8, sei

$$F := \mathbb{F}_2[T]/(f)$$

und sei $\alpha := [T] \in F$. Dann ist α ein Erzeuger von $F^\times$ (Beispiel 3.3.8) und die Potenzen von α können effizient mithilfe eins LFSR berechnet werden (Beispiel 3.3.9). Wir betrachten nun die Abbildungen

$$\begin{aligned} P\colon F^{n-2} &\longrightarrow F \\ x &\longmapsto \sum_{j=1}^{n-2} x_j \end{aligned}$$

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) eindeu-

tige 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.

Außerdem werden endliche Körper auch bei der Untersuchung von Kreisteilungspolynomen bzw. Kreisteilungskörpern über $\mathbb{Q}$ eine wichtige Rolle spielen (Kapitel 3.5.1).

3.4 Galoiserweiterungen

Für gutartige endliche Körpererweiterungen $L \mid K$ erwarten wir folgendes:

- Es gilt $\left|\mathrm{Gal}(L,K)\right| = [L:K]$
- und $K = L^{\mathrm{Gal}(L,K)} := \{x \in L \mid \forall_{f \in \mathrm{Gal}(L,K)} \quad f(x) = x\}$.
- Die Struktur (der Untergruppen) von $\mathrm{Gal}(L,K)$ beschreibt die 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 dann:

① Wenn das Minimalpolynom μ_α über L *nicht* in Linearfaktoren zerfällt, ist $\left|\mathrm{Gal}(L,K)\right| < \deg \mu_\alpha = [L:K]$.

② Wenn μ_α über L zwar in Linearfaktoren zerfällt, aber mehrfache Nullstellen besitzt, ist $\left|\mathrm{Gal}(L,K)\right| < \deg \mu_\alpha = [L:K]$.

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).

3.4.1 Normale Körpererweiterungen

Definition 3.4.1 (normale Körpererweiterung)**.** Eine algebraische Körpererweiterung $L \mid K$ ist *normal*, wenn für jedes $\alpha \in L$ das Minimalpolynom $\mu_\alpha \in K[T]$ von α über K bereits in L in Linearfaktoren zerfällt.

Die Bezeichnung solcher Körpererweiterungen als „normal“ hängt mit dem Normalteilerbegriff für Gruppen zusammen (wie wir in Satz 3.4.23 sehen werden).

Beispiel 3.4.2 (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 3.4.3. 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 enthalten sind).

Man erinnere sich bei dieser Gelegenheit daran, dass auch die Normalteilereigenschaft in der Gruppentheorie im allgemeinen *nicht* transitiv ist (Caveat 1.3.26).

Die folgenden beiden Kriterien helfen in vielen Fällen, Normalität nachzuweisen:

Proposition 3.4.4 (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 Körpermorphismus $\sigma\colon L \longrightarrow M$ 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 Körpermorphismus mit $\sigma|_K = \mathrm{id}_K$. Wegen $L = K(S)$ genügt es zu zeigen, dass $\sigma(S) \subset L$

ist (nachrechnen). 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 nun 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 dann ein Körpermorphismus $\sigma\colon K(\alpha) \longrightarrow M$ mit $\sigma|_K = \mathrm{id}_K$ und $\sigma(\alpha) = \beta$.

Analog zum Beweis von Satz 3.2.54 können wir mithilfe des Konjugationsprinzips und des Zornschen Lemmas den Körpermorphismus σ zu einem Körpermorphismus $\widetilde{\sigma}\colon L \longrightarrow M$ mit $\widetilde{\sigma}|_{K(\alpha)} = \sigma$ fortsetzen. Nach Voraussetzung ist dann

$$\beta = \sigma(\alpha) = \widetilde{\sigma}(\alpha) \in \widetilde{\sigma}(L) \subset L. \qquad \square$$

Zum Beispiel liefern Zerfällungskörper also normale Körpererweiterungen.

Beispiel 3.4.5. 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 3.4.4). Dann ist auch $M \mid K$ normal (nachrechnen).

3.4.2 Separable Körpererweiterungen

Definition 3.4.6 (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 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

$$[L : K]_s := \big|\{\sigma\colon L \longrightarrow M \mid \sigma \text{ ist ein Körpermorphismus und } \sigma|_K = \mathrm{id}_K\}\big|$$

der Einbettungen von $L \mid K$ nach $M \mid K$ als *Separabilitätsgrad* der Erweiterung $L \mid K$.

Bemerkung 3.4.7. Die obigen Begriffe sind unabhängig vom gewählten algebraischen Abschluss, da algebraische Abschlüsse bis auf Isomorphie eindeutig bestimmt sind (Satz 3.2.54) und die obigen Eigenschaften unter Isomorphie von Körpererweiterungen erhalten bleiben (nachrechnen).

Beispiel 3.4.8 (Separabilität)**.** Mit dem Ableitungskriterium für mehrfache Nullstellen (Proposition 3.3.3) folgt:

- Ist K ein Körper mit $\operatorname{char} K = 0$ und ist $f \in K[T]$ 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 Polynom

  $$X^p - T \in \mathbb{F}_p(T)[X]$$

  über $\mathbb{F}_p(T)$ irreduzibel (nach dem Eisensteinschen Irreduzibilitätskriterium; Satz 2.2.52) 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 3.4.9 (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 3.4.10 (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). □

Satz 3.4.11 (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 3.4.10 aus dem ersten Teil.

Zu 1. Ist K endlich, so ist auch L endlich, und damit ist $L^\times$ zyklisch (Korollar 3.1.8). Insbesondere hat dann jeder Erzeuger α von $L^\times$ die Eigenschaft, dass $L = K(\alpha)$ ist. Wir nehmen daher im folgenden an, dass K unendlich ist.

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 $\sigma_1, \ldots, \sigma_n$ die n Körpermorphismen $L \longrightarrow M$. Wir betrachten dann das Polynom

$$f := \prod_{j,k \in \{1,\ldots,n\}, j<k} \Big(\big(\sigma_j(\beta) - \sigma_k(\beta)\big) + \big(\sigma_j(\gamma) - \sigma_k(\gamma)\big) \cdot T \Big) \in M[T].$$

Da die $\sigma_1, \ldots, \sigma_n$ alle verschieden sind und wegen $L = K(\beta, \gamma)$ durch ihre Werte auf $\{\beta, \gamma\}$ eindeutig bestimmt sind, ist f *nicht* das Nullpolynom. Also besitzt f in K nur endlich viele Nullstellen (Korollar 2.2.49). Da K unendlich ist, gibt es somit ein $x \in K$ mit $f(x) \neq 0$. Wir betrachten nun

$$\alpha := \beta + x \cdot \gamma \in L.$$

Wegen $f(x) \neq 0$ sind die Elemente $\alpha_1, \ldots, \alpha_n$ mit

$$\forall_{j \in \{1,\ldots,n\}} \quad \alpha_j := \sigma_j(\beta) + x \cdot \sigma_j(\gamma) = \sigma_j(\alpha)$$

alle verschieden. Sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K. Mit dem Konjugationsprinzip (Proposition 3.2.28) folgt dann, dass μ_α in L mindestens die n Nullstellen $\alpha_1, \ldots, \alpha_n$ besitzt. Also ist

$$\big[K(\alpha) : K\big] = \deg \mu_\alpha \geq n.$$

Zu ②. Angenommen, es wäre $K(\alpha) \neq L$. Dann gibt es ein $\beta \in L \setminus K(\alpha)$. Mit dem Konjugationsprinzip und ① erhalten wir dann

$$\begin{aligned}
n &= [L : K]_s && \text{(Definition von } n\text{)} \\
&\geq \big[K(\alpha,\beta) : K\big]_s && \text{(Wegen } K(\alpha,\beta) \subset L\text{; Konjugationsprinzip)} \\
&\geq \big[K(\alpha,\beta) : K(\alpha)\big]_s \cdot \big[K(\alpha) : K\big]_s && \text{(Konjugationsprinzip)} \\
&= \big[K(\alpha,\beta) : K(\alpha)\big]_s \cdot \big[K(\alpha) : K\big] && \text{(Proposition 3.4.10)} \\
&\geq \big[K(\alpha)(\beta) : K(\alpha)\big]_s \cdot n. && \text{(Teil ①)}
\end{aligned}$$

Da $\beta \notin K(\alpha)$ gilt und da das Minimalpolynom von β über K (bzw. dann auch über $K(\alpha)$) nach Voraussetzung separabel ist, folgt mit Proposition 3.4.10

$$\big[K(\alpha)(\beta) : K(\alpha)\big]_s = \big[K(\alpha)(\beta) : K(\alpha)\big] > 1.$$

Also ist

$$n = [L : K]_s > 1 \cdot n = n,$$

was nicht sein kann. Somit folgt $K(\alpha) = L$. □

Bemerkung 3.4.12. Man beachte, dass der Beweisschritt ① im Satz vom primitiven Element (Satz 3.4.11) eine Anleitung gibt, mit der man (induktiv) primitive Elemente finden kann.

Beispiel 3.4.13 (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 nun 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 3.4.11 erhalten wir dann 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 3.4.11).

3.4.3 Galoiserweiterungen

Wie bereits angekündigt, werden wir uns nun mit algebraischen Körpererweiterungen beschäftigen, die „genug Nullstellen“ enthalten:

Definition 3.4.14 (Galoiserweiterung)**.** Eine *Galoiserweiterung* ist eine algebraische Körpererweiterung, die normal und separabel ist.

Bemerkung 3.4.15 (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. Diese Erkenntnisse hat er in wenigen Tagen vor seinem fatalen Duell(!) am 30. Mai 1832 in Briefen an Chevalier skizziert ...

Beispiel 3.4.16 (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 3.4.4).
- Endliche Erweiterungen von endlichen Körpern sind Galoiserweiterungen (Beispiel 3.4.5, Beispiel 3.4.9).
- Es ist $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ *keine* Galoiserweiterung, da diese Erweiterung *nicht* normal ist (Beispiel 3.4.2).
- 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 3.4.9).

Wir zeigen nun, dass für Galoiserweiterungen tatsächlich der angestrebte Zusammenhang zwischen Grad, Galoisgruppe und Fixkörpern besteht.

Proposition 3.4.17 (Grad endlicher Galoiserweiterungen)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung. Dann ist*

$$[L : K] = [L : K]_s = \big|\mathrm{Gal}(L, K)\big|.$$

Beweis. Nach dem Satz vom primitiven Element (Satz 3.4.11) gibt es $\alpha \in L$ mit $L = K(\alpha)$ und

$$[L : K] = [L : K]_s = \big[K(\alpha) : K\big]_s.$$

Da die Körpererweiterung $L \mid K$ normal ist, erhalten wir aus dem Konjugationsprinzip (Proposition 3.2.28 und Proposition 3.4.4) auch

$$\big[K(\alpha) : K\big]_s = \big|\mathrm{Gal}(L, K)\big|.$$

Zusammen liefern diese Beobachtungen die behauptete Gleichungskette. □

Satz 3.4.18 (Fixkörper). *Sei $L \mid K$ eine Körpererweiterung, sei G eine endliche Untergruppe von* $\mathrm{Gal}(L, K)$ *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*
$$[L : L^G] = |G| \quad \textit{und} \quad \mathrm{Gal}(L, L^G) = G.$$

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: Sei $\alpha \in L$ und sei $(\sigma_1, \ldots, \sigma_m)$ eine maximale Familie in G, für die $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$ 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. Um $[L : L^G]$ und $\mathrm{Gal}(L, L^G)$ zu bestimmen, zeigen wir zunächst: Für jede endliche Teilmenge $S \subset L$ gilt

$$\big[L^G(S) : L^G\big] \leq |G|,$$

denn: Da $L \mid L^G$ separabel ist, ist auch die Erweiterung $L^G(S) \mid L^G$ separabel (nachrechnen). Da diese Erweiterung aufgrund der Endlichkeit von S und der Gradabschätzung aus dem Beweis von 2. endlich ist (nachrechnen; mithilfe

von Proposition 3.2.12), erhalten wir aus dem Satz vom primitiven Element (Satz 3.4.11) ein $\alpha \in L$ mit $L^G(S) = L^G(\alpha)$. Mit den Überlegungen aus dem ersten Teil folgt somit

$$\big[L^G(S) : L^G\big] = \big[L^G(\alpha) : L^G\big] \leq |G|.$$

Es gibt somit ein $\alpha \in L$, dessen Grad über L^G maximal ist. Daraus folgt dann bereits $L = L^G(\alpha)$ (nachrechnen) und somit

$$[L : L^G] \leq |G|.$$

Nach Definition ist $G \subset \mathrm{Gal}(L, L^G)$. Also erhalten wir mit Proposition 3.4.17 das Ungleichungs-Sandwich

$$|G| \leq \big|\mathrm{Gal}(L, L^G)\big| = [L : L^G] \leq |G|,$$

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 3.4.19 (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 3.4.17); andererseits gilt $[L : L^G] = |G|$ (Satz 3.4.18). Mit der Multiplikativität des Grades (Proposition 3.2.10) erhalten wir also

$$[L^G : K] = \frac{[L : K]}{[L : L^G]} = \frac{|G|}{|G|} = 1,$$

und damit $L^G = K$. □

Bemerkung 3.4.20. Auch für unendliche Galoiserweiterungen $L \mid K$ ist $L^{\mathrm{Gal}(L,K)} = K$ (Übungsaufgabe).

Korollar 3.4.21 (Realisierung von endlichen Gruppen als Galoisgruppen)**.** *Sei G eine endliche Gruppe. Dann gibt es eine Galoiserweiterung $L \mid K$ mit*

$$\mathrm{Gal}(L, K) \cong G.$$

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 zu einer Untergruppe H von S isomorph.

Nach Satz 3.4.18 ist dann $L \mid L^H$ eine endliche Galoiserweiterung mit

$$\mathrm{Gal}(L, L^H) = H \cong G \qquad \square$$

Caveat 3.4.22. 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 3.4.21 haben wir kaum Kontrolle über den entstehenden Grundkörper.)

3.4.4 Der Hauptsatz der Galoistheorie

Wir fassen nun die Ergebnisse zu Galoiserweiterungen zusammen:

Satz 3.4.23 (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.

Beweis von Satz 3.4.23. Zu 1. Sei $H \subset \mathrm{Gal}(L,K)$ eine Untergruppe; da $\mathrm{Gal}(L,K)$ endlich ist (Proposition 3.4.17), ist H eine endliche Gruppe. Dann ist L^H ein Zwischenkörper von $L \mid K$ und Satz 3.4.18 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 3.4.19), 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).

  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 $\mathrm{Gal}(L,K)/\mathrm{Gal}(L,M) \cong \mathrm{Gal}(M,K)$.

- 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. Durch mehrfache Anwendung des Konjugationsprinzips (Proposition 3.2.28) erhalten wir einen Körperisomorphismus $\sigma \in \mathrm{Gal}(L,K)$ mit

  $$\sigma(\alpha) = \beta.$$

  Wir zeigen nun $\beta \in L^H$: Da H ein Normalteiler in $\mathrm{Gal}(L,K)$ ist, gilt $H = \sigma \cdot H \cdot \sigma^{-1}$. Wegen

  $$\forall_{\tau \in H \subset \mathrm{Gal}(L,L^H)} \quad \sigma \circ \tau \circ \sigma^{-1}(\beta) = \sigma \circ \tau(\alpha) = \sigma(\alpha) = \beta$$

  ist $\beta \in L^{\sigma \cdot H \cdot \sigma^{-1}} = L^H$. Nach dem ersten Teil ist also $\beta \in L^H = M$. □

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 3.4.24 (Überlagerungstheorie)**.** In der algebraischen Topologie gibt es das folgende Analogon des Hauptsatzes der Galoistheorie [21, Kapitel 2.5]: Dort wird die Struktur von (Zwischen-)Überlagerungen durch die Strukture 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 dann 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 3.4.25 (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.6).

Dabei bezeichnen $\mathsf{Subgroup}\,\mathrm{Gal}(L,K)$ und $\mathsf{Subext}(L,K)$ die folgenden Kategorien: Jede partiell geordnete Menge $(X,\leq)$ liefert wie folgt 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

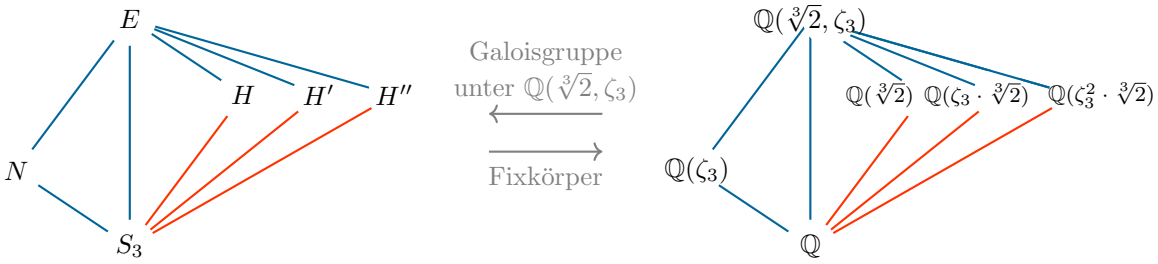


Abbildung 3.9.: Der Hauptsatz der Galoistheorie für $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \mid \mathbb{Q}$; normale Erweiterungen/Untergruppen sind blau, die nicht-normalen rot, dargestellt

von“. Wir betrachten dann 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 nun die Aussagen des Hauptsatzes der Galoistheorie an einem einfachen Beispiel. Man sollte dabei auch nachverfolgen, wie der Hauptsatz mit den Argumenten/Berechnungen in Beispiel 3.2.41 zusammenpasst.

Beispiel 3.4.26. Wir betrachten die Erweiterung $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \mid \mathbb{Q}$ aus Beispiel 3.2.41. Diese Körpererweiterung ist eine Galoiserweiterung, denn:

- 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, Proposition 3.4.4).

- Die Erweiterung ist separabel, da es sich um eine Erweiterung in Charakteristik 0 handelt (Beispiel 3.4.9).

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):

$$\begin{aligned} G &:= \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{Q}) \cong S_3, \\ H &:= \langle \tau \rangle_G \cong \mathbb{Z}/2, \\ H' &:= \langle \tau \circ \sigma \rangle_G \cong \mathbb{Z}/2, \\ H'' &:= \langle \tau \circ \sigma^2 \rangle_G \cong \mathbb{Z}/2, \\ N &:= \langle \sigma \rangle_G \cong \mathbb{Z}/3, \\ E &:= \{\mathrm{id}\}. \end{aligned}$$

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 3.9 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 3.4.27 (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 3.4.23) gibt es dann eine Gruppenerweiterung (Caveat 1.1.60) 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 nun 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 soll natürlich an die geometrische Lage der n-ten Einheitswurzeln auf dem Einheitskreis in $\mathbb{C}$ erinnern.

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 $\mathbb{C}$.

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*

$$\begin{aligned} \mathrm{Gal}(K, \mathbb{Q}) &\longrightarrow \big(\mathbb{Z}/(n)\big)^\times \\ f &\longmapsto [k], \text{ wobei } k \in \mathbb{Z} \text{ mit } f(\zeta_n) = {\zeta_n}^k \end{aligned}$$

   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 3.4.9); es genügt daher zu zeigen, dass f und Φ_n dieselben Nullstellen in $\mathbb{C}$ besitzen.

Mit dem Konjugationsprinzip (Proposition 3.2.28) folgt: Ist $\alpha \in \mathbb{C}$ eine Nullstelle von f, so gibt es ein $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})$ mit $\sigma(\zeta_n) = \alpha$, und damit

$$\operatorname{ord} \alpha = \operatorname{ord} \sigma(\zeta_n) = \operatorname{ord} \zeta_n = n.$$

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 geeigneten 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 $\operatorname{ggT}(k, n) = 1$ (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 also $p \in \mathbb{N}$ 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 2.2.44), dass $g \in \mathbb{Z}[T]$ liegt.

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 2.2.44) 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

$$\begin{aligned}
\big(\pi(g)\big)^p &= \pi(g^p) \\
&= \pi\big(g(T^p)\big) \qquad \text{(da in Charakteristik } p\text{; Frobenius auf } \mathbb{F}_p(T)) \\
&= \pi(f \cdot h) \qquad\qquad\qquad\qquad\qquad\qquad \text{(Konstruktion von } h) \\
&= \pi(f) \cdot \pi(h).
\end{aligned}$$

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

$$[K : \mathbb{Q}] = \deg \Phi_n = \big|U_n(\mathbb{C})^\times\big| = \varphi(n).$$

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 2.2.22) 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

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{11}), \mathbb{Q}\big) \cong \big(\mathbb{Z}/(11)\big)^\times.$$

Da 11 prim ist, enthält diese (abelsche) Gruppe genau zehn Elemente. Da $\mathbb{Z}/(11)$ ein Körper ist, ist $(\mathbb{Z}/(11))^\times$ eine zyklische Gruppe mit genau 10 Elementen. Somit erhalten wir

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_{11}), \mathbb{Q}\big) \cong \big(\mathbb{Z}/(11)\big)^\times \cong \mathbb{Z}/10.$$

Alternativ kann man auch mit dem Chinesischen Restsatz (Satz 2.2.22) oder mit dem Klassifikationssatz für endliche abelsche Gruppen (Satz 1.3.1) argumentieren; oder direkt nachrechnen, dass $[2] \in \mathbb{Z}/(11)$ die multiplikative Ordnung 10 besitzt und auf diese Weise auf $(\mathbb{Z}/(11))^\times \cong \mathbb{Z}/10$ schließen.

Beispiel 3.5.3 (Prim-Einheitswurzeln)**.** Allgemeiner gilt: Ist $p \in \mathbb{N}$ prim, so ist

$$T^p - 1 = (T-1) \cdot (T^{p-1} + \cdots + T + 1),$$

und wir wissen bereits (Beispiel 2.2.53), dass der zweite Faktor in $\mathbb{Q}[T]$ irreduzibel ist. Also ist

$$\Phi_p = \sum_{j=0}^{p-1} T^j.$$

Dabei ist $\mathrm{Gal}(\mathbb{Q}(\zeta_p), \mathbb{Q})) \cong (\mathbb{Z}/(p))^\times \cong \mathbb{Z}/(p-1)$.

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

$$\big[\mathbb{Q}(\zeta_7) : \mathbb{Q}\big] = \varphi(7) = 6 \quad \text{und} \quad \mathrm{Gal}\big(\mathbb{Q}(\zeta_7), \mathbb{Q}\big) \cong \big(\mathbb{Z}/(7)\big)^\times \cong \mathbb{Z}/6.$$

Andererseits ist (Beispiel 3.2.41)

$$\big[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}\big] = 6 \quad \text{und} \quad \mathrm{Gal}\big(\mathbb{Q}(\zeta_3, \sqrt[3]{2}), \mathbb{Q})\big) \cong S_3.$$

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

$$\big[\mathbb{Q}(\zeta_3) : \mathbb{Q}\big] = \varphi(3) = 2 \quad \text{und} \quad \mathrm{Gal}\big(\mathbb{Q}(\zeta_3), \mathbb{Q}\big) \cong \big(\mathbb{Z}/(3)\big)^\times \cong \mathbb{Z}/2.$$

Außerdem ist auch

$$\big[\mathbb{Q}(\sqrt{2}), \mathbb{Q}\big] = 2 \quad \text{und} \quad \mathrm{Gal}\big(\mathbb{Q}(\sqrt{2}), \mathbb{Q}\big) \cong \mathbb{Z}/2.$$

Aber es gilt $\mathbb{Q}(\zeta_3) \ncong \mathbb{Q}(\sqrt{2})$ (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 $\mathrm{Gal}(L, \mathbb{Q}) \cong \mathbb{Z}/3$ zu konstruieren: Nach dem Hauptsatz der Galoistheorie (Satz 3.4.23) genügt es dafür, eine endliche Galoiserweiterung von $\mathbb{Q}$ zu finden, deren Galoisgruppe G einen Normalteiler N mit $G/N \cong \mathbb{Z}/3$ 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 $H \subset \mathrm{Gal}(\mathbb{Q}(\zeta_7), \mathbb{Q}) \cong \mathbb{Z}/6$ die (normale) Untergruppe, die unter diesem Isomorphismus der Untergruppe $\{[0], [3]\} \subset \mathbb{Z}/6$ entspricht. Dann ist

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_7), \mathbb{Q}\big)/H \cong (\mathbb{Z}/6)/\{[0], [3]\} \cong \mathbb{Z}/3.$$

Nach dem Hauptsatz der Galoistheorie ist somit $L := \mathbb{Q}(\zeta_7)^H$ ein Zwischenkörper mit

$$\mathrm{Gal}(L, \mathbb{Q}) \cong \mathrm{Gal}\big(\mathbb{Q}(\zeta_7), \mathbb{Q}\big)/H \cong \mathbb{Z}/3.$$

Ausblick 3.5.8 (abelsche Erweiterungen von $\mathbb{Q}$)**.** Allgemeiner gilt nach dem Satz von Kronecker-Weber [30, 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 nun 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 $\operatorname{char} K = 0$.

- 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 $j \in \{1, \ldots, n\}$ 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

$$T^2 + b \cdot T + c \in K[T]$$

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)

$$f = \Big(T - \frac{-b + \alpha}{2}\Big) \cdot \Big(T - \frac{-b - \alpha}{2}\Big).$$

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 diesen Satz beweisen, verwenden wir ihn, um zu zeigen, dass Aufgabe 4 aus der Einführung *nicht* durch iteriertes Wurzelziehen lösbar ist:

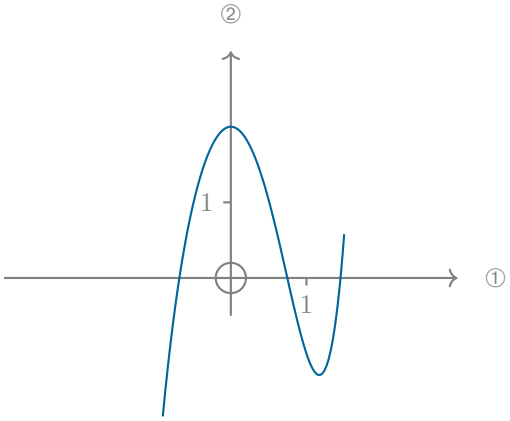


Abbildung 3.10.: Die reelle Polynomfunktion zu $T^5 - 4 \cdot T^2 + 2$

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 $G := \mathrm{Gal}(L, \mathbb{Q})$ 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 1.3.24).

Die Galoisgruppe G operiert effektiv auf der (fünf-elementigen) Menge X der komplexen Nullstellen von f (Korollar 3.2.29). Da 5 prim ist, genügt es zu 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 3.10). 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 3.4.17)

$$|G| = \big|\mathrm{Gal}(L, \mathbb{Q})\big| = [L : \mathbb{Q}].$$

Das Polynom f ist über $\mathbb{Q}$ irreduzibel (nach dem Eisensteinschen Irreduzibilitätskriterium; Satz 2.2.52). 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 1.3.35) bzw. dem Satz von Cauchy (Korollar 1.3.36) 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 [7, 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

$$\mathrm{Gal}(L, \mathbb{Q}) = [L : \mathbb{Q}] \leq 24$$

(Proposition 3.4.17). Daher handelt es sich bei $\mathrm{Gal}(L, \mathbb{Q})$ um eine auflösbare Gruppe (Bemerkung A.4.6). Also ist f durch Radikale auflösbar (Satz 3.5.11). Dies kann auch explizit gemacht werden [7, 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 geben nun den 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 $\mathrm{char}\, K = 0$, 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 $\mathrm{Gal}(L,K) \cong \mathbb{Z}/n$, so ist $L \mid K$ eine Wurzelerweiterung.*

Beweis. Zu 1. $\Longrightarrow$ 2. Ist $\alpha \in L$ und gilt $L = K(\alpha)$ sowie $\alpha^n = c$, so ist $L = K(\alpha)$ ein Zerfällungskörper von $T^n - c$ über K, denn

$$T^n - c = \prod_{k=0}^{n} (T - \zeta^k \cdot \alpha).$$

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 3.4.4, Proposition 3.4.10). 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. $\Longrightarrow$ 1. Sei umgekehrt $L \mid K$ eine Galoiserweiterung mit $\mathrm{Gal}(L,K) \cong \mathbb{Z}/n$. Sei $\sigma \in \mathrm{Gal}(L,K) \cong \mathbb{Z}/n$ ein Erzeuger.

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.3.3.23). 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). Mit Bemerkung 3.4.27 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 1.3.23) 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 $N := \big\{x \in \mathbb{C} \mid x^n = \sigma(c) \text{ und } \sigma \in \mathrm{Gal}(K, \mathbb{Q})\big\} \subset \mathbb{C}$ 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 3.4.19) 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 3.4.4). □

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

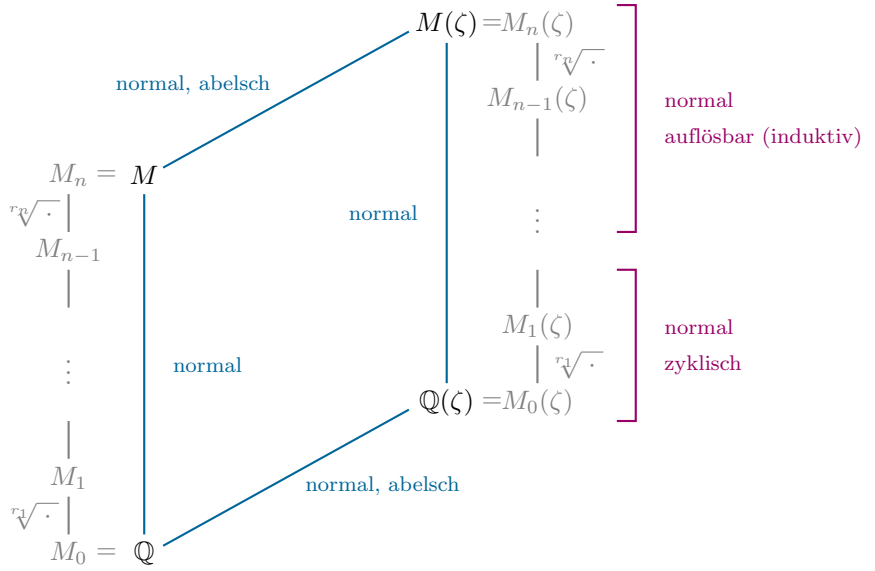


Abbildung 3.11.: Durch Radikale auflösbare Polynome haben auflösbare Galoisgruppe, schematisch

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 3.4.27) und den Vererbungseigenschaften auflösbarer Gruppen (Proposition 1.3.23) folgt induktiv (von unten nach oben, mit einer leicht allgemeineren Induktionsbehauptung) wie in Abbildung 3.11 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 1. $\Longrightarrow$ 2. 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 1.3.27) und die Anzahl der Elemente von $\overline{G}$ ist ein Teiler von $|G|$ (nachrechnen). Mit dem Hauptsatz der Galoistheorie (Satz 3.4.23) 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, 10].

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. 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 3.5.19 (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

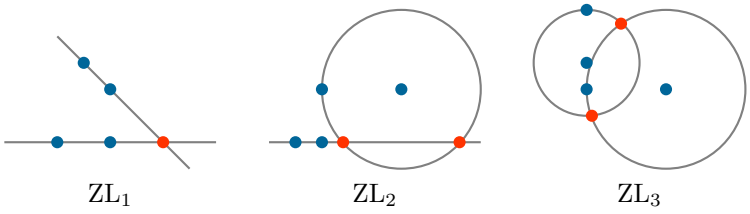


Abbildung 3.12.: Die elementaren Konstruktionsschritte mit Zirkel und Lineal: bereits konstruierte Punkte (blau), Hilfsgeraden/-kreise (grau), neue Punkte (rot)

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 3.12)

- $\mathrm{ZL}_1(M)$ für die Menge aller Schnittpunkte zweier verschiedener Geraden aus $G(M)$,
- $\mathrm{ZL}_2(M)$ für die Menge aler Schnittpunkte von Geraden aus $G(M)$ mit Kreisen aus $C(M)$,
- $\mathrm{ZL}_3(M)$ für die Menge aller Schnittpunkte zweier verschiedener Kreise aus $C(M)$.

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 $\mathbb{C}$.

Der Vollständigkeit halber geben wir ein Beispiel für die Lösung eines Konstruktionsproblems mit Zirkel und Lineal in der ebenen Geometrie [22, Kapitel 2.4].

Beispiel 3.5.20 (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 3.13)

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.

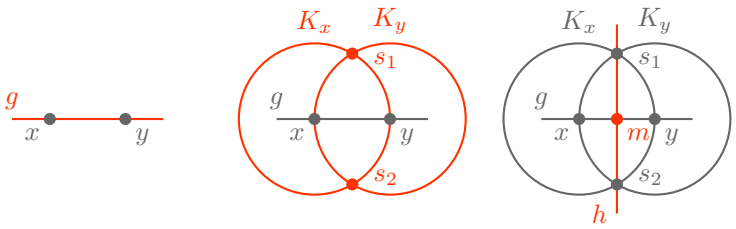


Abbildung 3.13.: Konstruktion des Mittelpunktes von x und y

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
$$m = \frac{1}{2} \cdot (s_1 + s_2).$$

Satz 3.5.21 (der Körper der konstruierbaren Punkte). *Die Menge* $\mathrm{ZL} \subset \mathbb{C}$ *ist ein Zwischenkörper von* $\mathbb{C} \mid \mathbb{Q}$*, der im folgenden Sinne unter Quadratwurzeln abgeschlossen ist: 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 schreiben wir z in Polarkoordinaten, d.h. $z = e^{i\cdot\varphi} \cdot r$ mit $\varphi \in \mathbb{R}$ und $r \in \mathbb{R}_{>0}$. Dann gilt (nachrechnen):

> Der Punkt z liegt genau dann in ZL, wenn $|z| \in \mathrm{ZL}$ ist und der durch φ gegebene Winkel aus $\{0, 1\}$ konstruierbar ist (in dem Sinne, dass wir ihn als Winkel zwischen zwei konstruierbaren Geraden erhalten).

Indem wir in Polarkoordinaten rechnen, folgt, dass es genügt die folgenden Aussagen zu zeigen:

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 $\varphi, \psi \in \mathbb{R}$ 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 zeigen dies mithilfe des Strahlensatzes (Abbildung 3.14): Es ist $i \in \mathrm{ZL}$, da wir die zur reellen Achse orthogonale Gerade durch 0 mit Zirkel und Lineal aus $\{0, 1\}$ konstruieren können (nachrechnen), und diese Gerade mit dem Einheitskreis (dieser ist aus $\{0, 1\}$ konstruierbar) schneiden.

Konstruktion von $x \cdot y$: Wir konstruieren nun die Gerade durch x und i sowie die dazu parallele Gerade durch $i \cdot y$ (konstruierbar). Sei z der Schnittpunkt 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

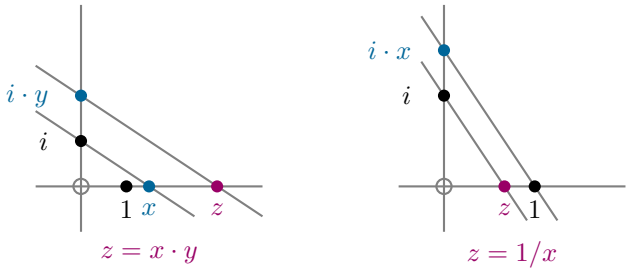


Abbildung 3.14.: Produkte und Quotienten, geometrisch

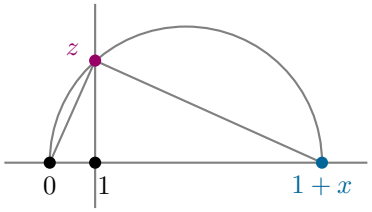


Abbildung 3.15.: Reelle Quadratwurzeln, geometrisch

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 3.15): 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 zuerst konstruierten Halbkreis. Nach dem Satz von Thales sind dann 0, z und $1 + x$ die Ecken eines rechtwinkligen Dreiecks und nach dem Höhensatz ist

$$1 \cdot x = |z - 1|^2.$$

Mit z ist dann auch die Wurzel $|z - 1|$ aus x konstruierbar. □

Satz 3.5.22 (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 $\mathrm{ZL}(\mathrm{ZL}^{n-1}(\{0,1\}))$ 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 nun die folgende essentielle Beobachtung: Sei $L \subset \mathrm{ZL}$ ein Teilkörper. Dann gilt (nachrechnen [7, 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

$$[\mathbb{Q}(M)(z) : \mathbb{Q}(M)] \leq 2$$

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 3.5.21), 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 1.3.27, dass $\mathrm{Gal}(L, \mathbb{Q})$ eine Normalreihe mit Faktoren isomorph zu $\mathbb{Z}/2$ besitzt. Der Hauptsatz der

Galoistheorie (Satz 3.4.23) übersetzt eine solche Normalreihe in eine Erweiterungskette wie in Aussage 2.

Zu 3. $\Longleftrightarrow$ 4. Die Aussagen 3. und 4. sind via Proposition 3.4.17 äquivalent. □

Mit dieser Theorie können wir Aufgabe 1, Aufgabe 2 und Aufgabe 3 aus der Einführung behandeln:

Beispiel 3.5.23 (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 3.5.22 im Widerspruch zu $\sqrt{\pi} \in \mathrm{ZL}$.

Beispiel 3.5.24 (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

$$\big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big] = 3$$

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 3.5.22 im Widerspruch zu $\sqrt[3]{2} \in \mathbb{Z}$.

Beispiel 3.5.25 (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

$$\big[\mathbb{Q}(\zeta_9) : \mathbb{Q}\big] = \varphi(9) = 6$$

(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 3.5.22 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

$$\big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big] = \varphi(17) = |17 - 1| = 2^4$$

(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 3.5.26 (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 3.5.27. 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 3.5.28 (Origami-Konstruierbarkeit)**.** Ähnlich zur Konstruierbarkeit mit Zirkel und Lineal kann man auch die Konstruierbarkeit durch elementare Origami-Operationen formalisieren 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 3.5.29 (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 natürlich davon auszugehen, dass analytische Eigenschaften in den Beweis eingehen müssen. 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 3.4.4; Separabilität ist in Charakteristik 0 automatisch erfüllt: Beispiel 3.4.9). 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 verfolgen nun 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 1.3.35) enthält G eine 2-Sylowgruppe H. Also gilt

$$[L : L^H] = |H| = 2^k$$

(Satz 3.4.18), 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 3.4.11) 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 3.4.23)

$$L^H = \mathbb{R}(\alpha) = \mathbb{R} \quad \text{und} \quad H = G.$$

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 3.4.23)

$$\frac{|G|}{|N|} = |G/N| = \big|\mathrm{Gal}(\mathbb{C}, \mathbb{R})\big| = 2.$$

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 1.3.33 per Induktion über $|N|$). Insbesondere ist N' ein Normalteiler von N (Übungsaufgabe). Nach dem Hauptsatz der Galoistheorie ist dann

$$[L^{N'} : \mathbb{C}] = \big|\mathrm{Gal}(L^{N'}, \mathbb{C})\big| = |N/N'| = [N : N'] = 2.$$

Dies ist aber ein Widerspruch zu ④ (nachrechnen).

Also ist $\mathrm{Gal}(L, \mathbb{C}) = N = \{e\}$ und, da $L \mid \mathbb{C}$ eine Galoiserweiterung ist, erhalten wir $L = \mathbb{C}$, wie gewünscht. □

Bemerkung 3.5.30 (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?
  - 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	Formalisierte Algebra	A.3
A.2	Kategorien	A.7
A.3	Freie Gruppen	A.11
A.4	Sylow-Zoo	A.15
A.5	Euklidische Ringe	A.19
A.6	Funktoren	A.25

A.1 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, Konstruktionen und Beweise 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 Coq [11] und Isabelle [18].

Auf den folgenden Seiten geben wir ein Beispiel für eine Formalisierung in Isabelle des Beginns dieser Algebra-Vorlesung, d.h. eine Formalisierung der gruppentheoretischen Grundbegriffe. Auch ohne mit den Details von Isabelle vertraut zu sein, ist die Nähe zur „gewöhnlichen“ Formulierung dieser Definitionen, Sätze und Beweise deutlich zu erkennen.

Die folgende Implementation zeigt nur, dass es prinzipiell möglich ist, mathematische Theorien, Definitionen, Sätze und Beweise zu formalisieren. Bei einer systematischen Implementation der Algebra würde man anders vorgehen:

- Man würde die Definition von Gruppen auf einfacheren algebraischen Strukturen (z.B. Halbgruppen) aufbauen, die auch in anderen algebraischen Strukturen auftreten (z.B. um die Multiplikation in Ringen beschreiben).
- Man würde entsprechend auch Eigenschaften wie Eindeutigkeit des neutralen Elements für diese einfacheren algebraischen Strukturen nachweisen.
- Man würde Homomorphismen bereits auch für die einfacheren algebraischen Strukturen definieren und untersuchen.
- Man würde systematisch alle nützlichen Lemmata formulieren und beweisen, um später bei komplexeren Beweisen darauf zurückgreifen zu können.
- ...
- Und man würde den Code natürlich vernünftig kommentieren bzw. dokumentieren!

Ein Gruppentheorie-Fragment in Isabelle

```
theory Basic-Groups

  imports Main

begin

no-notation Groups.times (infixl * 70)
no-notation Groups.one (1)

class verbose-group =
  fixes composition :: 'a ⇒ 'a ⇒ 'a  (infixl * 70)
  fixes unit :: 'a (1)
  fixes inverse :: 'a ⇒ 'a
  assumes group-assoc: x * (y * z) = (x * y) * z
  assumes group-neutral-right: x * 1 = x
  assumes group-neutral-left:  1 * x = x
  assumes group-inverse-right: x * inverse x = 1
  assumes group-inverse-left:  inverse x * x = 1

theorem (in verbose-group) inverse-is-unique: x * y = 1 ⟹ x = inverse y

proof −
  assume x-is-inverse: x * y = 1
  have x = x * 1
    by (simp only: group-neutral-right)
  also have ... = x * (y * inverse y)
    by (simp only: group-inverse-right)
  also have ... = (x * y) * inverse y
    by (simp only: group-assoc)
  also have ... = 1 * inverse y
    by (simp only: x-is-inverse)
  also have ... = inverse y
    by (simp only: group-neutral-left)
  finally show ?thesis by simp
qed

theorem (in verbose-group) double-inverse: inverse (inverse x) = x

proof −
  have x * inverse x = 1
    by (rule group-inverse-right)
  thus ?thesis by (rule inverse-is-unique [of x inverse x, symmetric])
qed

theorem (in verbose-group) neutralelement-is-unique: e * x = x ⟹ e = 1

proof −
  assume e-is-xneutral: e * x = x
  have e = e * 1
```

```
    by (simp only: group-neutral-right)
  also have ... = e * (x * inverse x)
    by (simp only: group-inverse-right)
  also have ... = (e * x) * inverse x
    by (simp only: group-assoc)
  also have ... = x * inverse x
    by (simp only: e-is-xneutral)
  also have ... = 1
    by (simp only: group-inverse-right)
  finally show ?thesis .
qed

class abelian-group = verbose-group +
  assumes group-abelian: x * y = y * x

locale homomorphism =
  fixes f :: 'a :: verbose-group ⇒ 'b :: verbose-group
  assumes composition-compatible: f(x * y) = f(x) * f(y)

theorem homomorphism-is-compatible-with-unit:
  fixes f :: 'a :: verbose-group ⇒ 'b :: verbose-group
  assumes hom: homomorphism f
  shows f(1) = 1

proof −
  have f(1) = f(1 * 1)
    by (simp only: group-neutral-left)
  also have ... = f 1 * f 1
    by (rule homomorphism.composition-compatible [of f 1 1], rule hom)
  finally have f(1) = f(1) * f(1) by simp
  then have f(1) * f(1) = f(1) by simp
  then have f(1) = 1
    by (rule neutralelement-is-unique[of f 1])
  thus ?thesis .
qed

theorem homomorphism-is-compatible-with-inverse:
  fixes f :: 'a :: verbose-group ⇒ 'b :: verbose-group
  assumes hom: homomorphism f
  shows f(inverse x) = inverse (f(x))

proof −
  have f(inverse x) * f(x) = 1
      proof −
        have f(inverse x) * f(x) = f(inverse x * x)
          by (rule homomorphism.composition-compatible[of f inverse x x, symmetric],
              rule hom)
        also have ... = f(1)
          by (simp only: group-inverse-left)
        also have ... = 1
          by (rule homomorphism-is-compatible-with-unit, rule hom)
        finally show ?thesis by simp
      qed
```

```
  then have f(inverse x) = inverse (f(x))
    by (rule inverse-is-unique [of f(inverse x) f(x)])
  thus ?thesis .
qed

theorem homomorphism-is-injective-if-kernel-is-trivial:
  fixes f :: 'a :: verbose-group ⇒ 'b :: verbose-group
  assumes hom: homomorphism f
  assumes kernel-trivial: ⋀ x. f(x) = 1 ⟹ x = 1
  shows   f(x) = f(y) ⟹ x = y

proof −
  fix x
  fix y
  assume equal-image: f(x) = f(y)
  then have x = y
      proof −
        have f(x * inverse y) = 1
            proof −
              have f(x * inverse y) = f(x) * f(inverse y)
                by (rule homomorphism.composition-compatible [of f x (inverse y)],
                    rule hom)
              also have ... = f(x) * inverse (f(y))
                by (simp only: homomorphism-is-compatible-with-inverse [of f y] hom)
              also have ... = f(x) * inverse (f(x))
                by (simp only: equal-image [symmetric])
              finally show ?thesis by (simp only: group-inverse-right)
            qed

        then have x * inverse y = 1
          by (rule kernel-trivial)
        then have x = inverse (inverse y)
          by (rule inverse-is-unique)
        also have ... = y
          by (rule double-inverse)
        finally show x = y by simp
      qed

  then show f(x) = f(y) ⟹ x = y by simp

qed

end
```

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 [24, 6]:

Definition A.2.1 (Kategorie)**.** Eine *Kategorie* C besteht aus den folgenden Komponenten:

- Eine Klasse $\mathrm{Ob}(C)$; 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

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

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 (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.2.5 (Mengenlehre)**.** Die Kategorie Set der Mengen besteht aus:

- Objekte: Es sei Ob(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.2.6 (lineare Algebra)**.** Sei K ein Körper. Die Kategorie Vect_K der K-Vektorräume besteht aus:

- Objekte: Es sei Ob(Vect_K) die Klasse aller K-Vektorräume.
- Morphismen: Sind V und W Vektorräume über K, so sei $\mathrm{Mor}_K(V,W)$ die Menge aller K-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, ...

Beispiel A.2.7 (Ringtheorie)**.** Die Kategorie Ring der Ringe besteht aus:

- Objekte: Es sei $\mathrm{Ob}(\mathsf{Ring})$ die Klasse aller Ringe.
- Morphismen: Sind R und S Ringe, so sei $\mathrm{Mor}_{\mathsf{Ring}}(R,S)$ die Menge aller Ringhomomorphismen $R \longrightarrow S$.
- Verknüpfungen: Die Verknüpfung sei durch die gewöhnliche Abbildungskomposition gegeben.

Beispiel A.2.8 (Algebren)**.** Sei K ein Körper. Die Kategorie Alg_K der K-Algebren besteht aus:

- Objekte: Es sei $\mathrm{Ob}(\mathsf{Alg}_K)$ die Klasse aller K-Algebren.
- Morphismen: Sind A und B Algebren über K, so sei $\mathrm{Mor}_{\mathsf{Alg}_K}(A,B)$ die Menge aller K-Algebrenhomomorphismen $A \longrightarrow B$.
- Verknüpfungen: Die Verknüpfung sei durch die gewöhnliche Abbildungskomposition gegeben.

Beispiel A.2.9 (Modultheorie)**.** Sei R ein Ring. Die Kategorie Mod_R der (Links-)R-Moduln besteht aus:

- Objekte: Es sei $\mathrm{Ob}(\mathsf{Mod}_R)$ die Klasse aller R-Moduln.
- Morphismen: Sind V und W Moduln über R, so sei $\mathrm{Mor}_{\mathsf{Mod}_R}(V,W)$ die Menge aller R-Modulhomomorphismen $V \longrightarrow W$.
- Verknüpfungen: Die Verknüpfung sei durch die gewöhnliche Abbildungskomposition gegeben.

Beispiel A.2.10 (Topologie)**.** Die Kategorie Top der topologischen Räume besteht aus:

- Objekte: Es sei $\mathrm{Ob}(\mathsf{Top})$ 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.2.11 (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.2.12 (Isomorphismenbegriffe)**.**

- Objekte in Set sind genau dann isomorph, wenn sie gleichmächtig sind.
- Sei K ein Körper und sei R ein Ring. Objekte in Group, Ab, Vect_K, Ring, Alg_K, Mod_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.

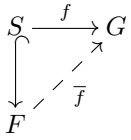
Definition A.2.13 (Automorphismengruppe)**.** Sei C eine Kategorie und sei $X \in \mathrm{Ob}(C)$. Dann bildet die Menge $\mathrm{Aut}(X)$ aller Isomorphismen $X \longrightarrow X$ in C bezüglich der Komposition von Morphismen in C eine Gruppe, die *Automorphismengruppe von* X *in* C.

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 charakterisiserten Objekten (*Brüderchen, komm tanz mit mir. Einmal hin, einmal her; rundherum, das ist nicht schwer* ..., Abbildung I.4.6). □

Satz A.3.4 (Existenz freier Gruppen). *Sei S eine Menge. Dann gibt es eine Gruppe, die frei von S erzeugt ist.*

Beweis. 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^*.

- Als zweiten Schritt definieren wir
$$F(S) := A^* / \sim,$$
wobei $\sim$ die Äquivalenzrelation auf A^* ist, die von
$$\begin{aligned} &\forall_{x,y \in A^*} \quad \forall_{s \in S} \quad x s \widehat{s} y \sim xy, \\ &\forall_{x,y \in A^*} \quad \forall_{s \in S} \quad x \widehat{s} s y \sim xy \end{aligned}$$
erzeugt wird. Das heißt, $\sim$ ist die kleinste (bezüglich Inklusion) Äquivalenzrelation auf A^*, die die obigen Bedingungen erfüllt.

  Dann erzeugt das Hintereinanderschreiben von Wörtern eine wohldefinierte Abbildung $\cdot : F(S) \times F(S) \longrightarrow F(S)$ (Übungsaufgabe).

Die Menge $F(S)$ bildet bezüglich der obigen Verknüpfung eine Gruppe (Übungsaufgabe). 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 (Übungsaufgabe). □

Insbesondere folgt aus der obigen Konstruktion und der Eindeutigkeit freier Gruppen, dass freie Erzeugendensysteme tatsächlich *erzeugend* sind.

A.4 Sylow-Zoo

Die folgenden Beispiele zu Gruppen mit gegebenen Anzahlen demonstrieren ein paar Handgriffe, die bei der Verwendung der Sylowsätze für Klassifikationsfragen nützlich sind.

Beispiel A.4.1 (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 dann

$$s_{37} \mid 333 \quad \text{und} \quad s_{37} \equiv 1 \mod 37.$$

Aus diesen beiden Bedingungen erhalten wir bereits (wie im Beweis von Korollar 1.3.38), dass $s_{37} = 1$ ist und damit, dass die (eindeutig bestimmte) 37-Sylowgruppe S von G ein Normalteiler in G ist. 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.4.2 (33)**.** Ist G eine Gruppe mit $|G| = 33$, so ist G bereits zyklisch: 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 dann

$$s_3 \mid 33 \quad \text{und} \quad s_3 \equiv 1 \mod 37.$$

Aus diesen beiden Bedingungen erhalten wir bereits (wie im Beweis von Korollar 1.3.38), dass $s_3 = 1$ ist und damit, dass die (eindeutig bestimmte) 3-Sylowgruppe S von G ein Normalteiler in G ist. Dabei gilt $S \cong \mathbb{Z}/3$; sei $g \in S \setminus \{e\}$ (insbesondere ist $\operatorname{ord} g = 3$).

Da 11 ein Primteiler von $|G|$ ist, gibt es außerdem ein Element $h \in G$ mit $\operatorname{ord} h = 11$ (Korollar 1.3.36). 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 nun:

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 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

$$g = \mathrm{id}(g) = f^{11}(g) = g^{2^{11}} = g^{2048} = (g^3)^{682} \cdot g^2 = g^2 \neq g,$$

was nicht sein kann. 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 1.1.24) und den Isomorphiesätzen (Satz 1.1.50) 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

$$G \cong \mathbb{Z}/3 \times \mathbb{Z}/11.$$

Mit dem Chinesischen Restsatz (oder durch Berechnung von $\mathrm{ord}(g \cdot h)$) erhalten wir daraus, dass $G \cong \mathbb{Z}/33$ ist. Insbesondere ist G zyklisch.

Beispiel A.4.3 (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 kann mit den Sylowsätzen darauf kommen? Wie in Korollar 1.3.38 kann man zeigen, dass es genau eine 7-Sylowgruppe T in G gibt (die daher ein Normalteiler in G ist) und dass $T \cong \mathbb{Z}/7$ ist. Außerdem gibt es eine 3-Sylowgruppe S und wegen $|G| = 21 = 3 \cdot 7$ folgt $|S| = 3$, und damit $S \cong \mathbb{Z}/3$.

Wie in Beispiel A.4.2 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 1.1.59). Also ist

$$G \cong \mathbb{Z}/7 \rtimes_\varphi \mathbb{Z}/3$$

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.4.4 (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 1.3.35) 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 nun, 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 $S \cong \mathbb{Z}/3$. 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 1.1.24) 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. Wegen

$$\frac{12}{3} = 4 = 2^2 \quad \text{und} \quad \frac{12}{4} = 3$$

sind die zugehörigen Quotientengruppen auflösbar (Satz 1.3.33). Da die Sylowgruppen auch auflösbar sind (Satz 1.3.33), erhalten wir mit Proposition 1.3.23, dass auch 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.4.5 (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 1.3.35) 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). 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). Also ist $N \neq G$.

Also 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.4.6. Mit den bisher entwickelten Techniken kann man nachweisen, dass jede Gruppe G mit $|G| < 60$ auflösbar ist.

A.5 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 werden dies nun formalisieren:

Definition A.5.1 (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.5.2 (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.5.3 (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 sogenannte *Polynomdivision*, die wie folgt algorithmisch durchgeführt werden kann: Seien $x, y \in K[T]$

mit $y \neq 0$. Wir zeigen per Induktion über $\delta(x) \in \mathbb{N}$, dass es $r, s \in K[T]$ mit $x = s \cdot y + r$ und $\delta(r) < \delta(y)$ (oder sogar $r = 0$) gibt.

- *Induktionsanfang.* Ist $x = 0$, so ist $x = 0 \cdot y + 0$ eine Darstellung der gewünschten Form. Ist $\delta(x) < \delta(y)$, so ist $x = 0 \cdot y + x$ eine Darstellung der gewünschten Form.
- *Induktionsvoraussetzung.* Sei $\delta(x) > 0$ und für alle $x' \in K[T]$ mit $\delta(x') < \delta(x)$ gebe es $r', s' \in K[T]$ mit $x' = s' \cdot y + r'$ und $\delta(r') < \delta(y)$ (oder sogar $r' = 0$).
- *Induktionsschritt.* Wir schreiben $y = \sum_{j=0}^{n} b_j \cdot T^j$ und $x = \sum_{j=0}^{m} a_j \cdot T^j$ mit $a_0, \ldots, a_m, b_0, \ldots, b_n \in K$ und $a_m \neq 0 \neq b_n$. Wegen $b_n \neq 0$ können wir das Polynom (Elimination der höchsten T-Potenz aus x)

  $$x' := x - \frac{a_m}{b_n} \cdot T^{m-n} \cdot y \in K[T]$$

  definieren; nach Konstruktion ist $\delta(x') < m = \delta(x)$ und

  $$x = x' + \frac{a_m}{b_n} \cdot T^{m-n} \cdot y.$$

  Nach Induktionsvoraussetzung gibt es $r', s' \in K[T]$ mit $x' = s' \cdot y + r'$ und $\delta(r') < \delta(y)$ (oder sogar $r' = 0$). Damit ist

  $$x = \left(s' + \frac{a_m}{b_n} \cdot T^{m-n}\right) \cdot y + r'$$

  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.5.4 (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:

$$\begin{array}{rl}
 & T^3 + 0 \cdot T^2 + 0 \cdot T - 1 = (T+2) \cdot (1 \cdot T^2 - 2 \cdot T + 4) - 9 \\
- & (\ T^3 + 2 \cdot T^2\ ) \\
\hline
 & \quad - 2 \cdot T^2 + 0 \cdot T - 1 \\
 & - (\ - 2 \cdot T^2 - 4 \cdot T\ ) \\
\hline
 & \quad + 4 \cdot T - 1 \\
 & - (\ + 4 \cdot T + 8\ ) \\
\hline
 & \quad - 9
\end{array}$$

Proposition A.5.5 (euklidische Ringe sind Hauptidealringe)**.** *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei R ein euklidischer Ring mit eukildischer Gradfunktion $\delta\colon R \longrightarrow \mathbb{N}$ und sei $a \subset R$ ein Ideal. Ohne Einschränkung sei $a \neq \{0\}$. Wir betrachten ein Element $y \in a$ mit

$$\delta(y) = \min\bigl\{\delta(x) \bigm| x \in a \setminus \{0\}\bigr\} \in \mathbb{N};$$

ein solches Element existiert, da $a \setminus \{0\}$ nicht-leer ist und $\mathbb{N}$ wohlgeordnet ist. Dann gilt

$$a = (y),$$

denn: Wegen $y \in a$ ist $(y) \subset a$. Sei umgekehrt $x \in a$. Da δ eine euklidische Gradfunktion ist, gibt es $r, s \in R$ mit

$$x = s \cdot y + r \quad \text{und} \quad \bigl[\delta(r) < \delta(y) \text{ oder } r = 0\bigr].$$

Wegen $r = x - s \cdot y$ und $x, y \in a$ folgt auch $r \in a$. Aufgrund der Minimalität von y bezüglich δ erhalten wir daraus $r = 0$. Also ist $x = s \cdot y \in (y)$. □

Korollar A.5.6.

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.5.2, Proposition A.5.3). Also sind diese Ringe insbesondere auch Hauptidealringe (Proposition A.5.5). □

Caveat A.5.7 (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.5.5 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.5.8 (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.5.9 (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.5.10 (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.5.11. 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.6 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“.

Definition A.6.1 (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 $X, Y, Z \in \mathrm{Ob}(C)$ 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.6.2 (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.6.3 (Vergissfunktor)**.** Der Vergissfunktor $\mathsf{Vect}_{\mathbb{R}} \longrightarrow \mathsf{Set}$ ist wie folgt definiert:

- Auf Objekten betrachten wir die Abbildung $\mathrm{Ob}(\mathsf{Vect}_{\mathbb{R}}) \longrightarrow \mathrm{Ob}(\mathsf{Set})$, die einem $\mathbb{R}$-Vektorraum die unterliegende Menge zuordnet.
- Auf Morphismen: Für alle $\mathbb{R}$-Vektorräume X, Y betrachten wir
$$\begin{aligned} \mathrm{Mor}_{\mathsf{Vect}_{\mathbb{R}}}(X,Y) = \mathrm{Hom}_{\mathbb{R}}(X,Y) &\longrightarrow \mathrm{Mor}_{\mathsf{Set}}(X,Y) \\ f &\longmapsto f. \end{aligned}$$

Analog erhält man Vergissfunktoren $\mathsf{Top} \longrightarrow \mathsf{Set}$, $\mathsf{Vect}_{\mathbb{R}} \longrightarrow \mathsf{Ab}$, ...

Beispiel A.6.4 (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

$$\begin{aligned} F\colon \mathrm{Ob}(\mathsf{Set}) &\longrightarrow \mathrm{Ob}(\mathsf{Vect}_{\mathbb{R}}) \\ X &\longmapsto \bigoplus_X \mathbb{R}. \end{aligned}$$

  (Dabei ist $\bigoplus_X \mathbb{R}$ eine Verallgemeinerung der direkten Summe zweier Vektorräume (s. Lineare Algebra II). Wir betrachten 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. Dabei gilt für alle Mengen X und alle $\mathbb{R}$-Vektorräume V, dass

$$\begin{aligned} \mathrm{Mor}_{\mathsf{Vect}_{\mathbb{R}}}\big(F(X), V\big) &\longrightarrow \mathrm{Mor}_{\mathsf{Set}}(X, V) \\ f &\longrightarrow f|_X \end{aligned}$$

eine Bijektion ist (universelle Eigenschaft von Basen). Dies zeigt, dass der Funktor F und der Vergissfunktor $\mathsf{Vect}_{\mathbb{R}} \longrightarrow \mathsf{Set}$ sogenannte zueinander adjungierte Funktoren sind.

Beispiel A.6.5 (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.4.1.8):

- 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.6.6 (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.4.1.12).

In vielen Situationen benötigt man Funktoren, die „die Richtung der Pfeile umdrehen“, also sogenannte kontravariante Funktoren:

Definition A.6.7 (kontravarianter Funktor)**.** Seien C und D Kategorien. Ein *kontravarianter 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

$$F\colon \mathrm{Mor}_C(X,Y) \longrightarrow \mathrm{Mor}_C\big(F(Y), F(X)\big).$$

Dabei müssen folgende Bedingungen erfüllt sein:

- Für alle $X \in \mathrm{Ob}(C)$ ist $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$.
- Für alle $X, Y, Z \in \mathrm{Ob}(C)$ und alle $f \in \mathrm{Mor}_C(X,Y)$, $g \in \mathrm{Mor}_C(Y,Z)$ gilt

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

Beispiel A.6.8 (Dualraum)**.** Man kann die Konstruktion des Dualraums als kontravarianten Funktor $\cdot^*\colon \mathsf{Vect}_{\mathbb{R}} \longrightarrow \mathsf{Vect}_{\mathbb{R}}$ auffassen:

- Auf Objekten verwenden wir

$$\begin{aligned} \mathrm{Ob}(\mathsf{Vect}_{\mathbb{R}}) &\longrightarrow \mathrm{Ob}(\mathsf{Vect}_{\mathbb{R}}) \\ X &\longmapsto X^* = \mathrm{Hom}_{\mathbb{R}}(X, \mathbb{R}). \end{aligned}$$

- Auf Morphismen: Für alle $\mathbb{R}$-Vektorräume X, Y betrachten wir

$$\begin{aligned} \mathrm{Mor}_{\mathsf{Vect}_{\mathbb{R}}}(X,Y) = \mathrm{Hom}_{\mathbb{R}}(X,Y) &\longrightarrow \mathrm{Hom}_{\mathbb{R}}(Y^*, X^*) \\ f &\longmapsto f^*. \end{aligned}$$

Allgemeiner liefern Objekte in Kategorien Funktoren, die beschreiben wie die entsprechende Kategorie aus dem Blickwinkel dieses Objekts aussieht:

Beispiel A.6.9 (darstellbare Funktoren)**.** Sei C eine Kategorie und $X \in \mathrm{Ob}(C)$. Dann erhalten wir einen kontravarianten Funktor

$$\mathrm{Mor}_C(\,\cdot\,, X)\colon C \longrightarrow \mathsf{Set},$$

den *von X dargestellten kontravarianten Funktor*. Dieser Funktor ist wie folgt definiert:

- Auf Objekten: Sei

$$\begin{aligned} \mathrm{Mor}_C(\,\cdot\,, X)\colon \mathrm{Ob}(C) &\longrightarrow \mathrm{Ob}(\mathsf{Set}) \\ Y &\longmapsto \mathrm{Mor}_C(Y, X). \end{aligned}$$

- Auf Morphismen: Sind $Y, Z \in \mathrm{Ob}(C)$, so definieren wir

$$\begin{aligned} \mathrm{Mor}_C(\,\cdot\,, X)\colon\ \mathrm{Mor}_C(Y,Z) &\longrightarrow \mathrm{Mor}_{\mathsf{Set}}\big(\mathrm{Mor}_C(Z,X), \mathrm{Mor}_C(Y,X)\big) \\ f &\longmapsto (g \mapsto g \circ f). \end{aligned}$$

Analog erhält man einen kovarianten Funktor $\mathrm{Mor}_C(X, \,\cdot\,)\colon C \longrightarrow \mathsf{Set}$.

Eine wesentliche Eigenschaft von (kovarianten wie kontravarianten) Funktoren ist, dass sie – da sie mit Verknüpfungen und Identitätsmorphismen verträglich sind – Isomorphie erhalten und somit ein geeignetes Konzept für Invarianten liefern:

Proposition A.6.10 (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. 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.6.11. 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

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 0 vom 20. Oktober 2017

Aufgabe 1 (Gruppenhomomorphismen)**.** Seien G, H Gruppen, sei $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Für alle $g \in G$ gilt $f(g^{-1}) = \big(f(g)\big)^{-1}$.
2. Für alle $g, h \in G$ gilt $f(g \cdot h) = f(h) \cdot f(g)$.

Aufgabe 2 (Inversion)**.** Sei $(G, \cdot\,)$ eine Gruppe.

1. Zeigen Sie: Für alle $g \in G$ ist $(g^{-1})^{-1} = g$.
2. Zeigen Sie: Für alle $g, h \in G$ ist $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.
3. Zeigen Sie: Die Abbildung

$$\begin{aligned} G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned}$$

   ist genau dann ein Automorphismus von G, wenn G abelsch ist.

Aufgabe 3 (Linksnebenklassen)**.** Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe.

1. Zeigen Sie, dass die durch

$$\forall_{g_1, g_2 \in G} \quad g_1 \sim_H g_2 \iff g_1^{-1} \cdot g_2 \in H$$

   gegebene Relation $\sim_H$ auf G eine Äquivalenzrelation ist.
2. Zeigen Sie: Für alle $g \in G$ ist $g \cdot H = \{g' \in G \mid g \sim_H g'\}$.

Aufgabe 4 (Isometriegruppe)**.** Bestimmen Sie die Isometriegruppe der Teilmenge

$$L := \big\{(x, 0) \;\big|\; x \in [0,1]\big\} \cup \big\{(0, x) \;\big|\; x \in [0,1]\big\}$$

bezüglich der euklidischen Metrik d_2 auf $\mathbb{R}^2$. Machen Sie das Resultat nicht nur anschaulich plausibel, sondern führen Sie alle Details aus!

Bonusaufgabe (mathematische Allgemeinbildung)**.** Wer war Vladimir Voevodsky? Warum wird diese Aufgabe gerade jetzt gestellt?

---

keine Abgabe; diese Aufgaben werden in den Übungen
in der zweiten Vorlesungswoche besprochen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 1 vom 20. Oktober 2017

Aufgabe 1 (Gruppenhomomorphismen)**.** Seien G, H Gruppen, sei $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Ist $K \subset H$ eine Untergruppe von H, so ist das Urbild $f^{-1}(K)$ eine Untergruppe von G.
2. Ist $K \subset G$ eine Untergruppe von G, so ist $f(K)$ eine Untergruppe von H.

Aufgabe 2 (Verknüpfungstabellen)**.** Sei $(G, \cdot\,)$ eine Gruppe.

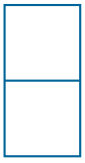
1. Zeigen Sie: Ist $g \in G$, so ist die folgende Abbildung bijektiv:
$$\begin{aligned} G &\longrightarrow G \\ h &\longmapsto g \cdot h \end{aligned}$$
2. Folgern Sie: Die untenstehende Verknüpfungstabelle definiert *keine* Gruppenstruktur auf $\{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$:

	♣	♠	♡	♢
♣	♣	♠	♡	♢
♠	♠	♣	♢	♡
♡	♡	♢	♣	♠
♢	♣	♡	♠	♣

Aufgabe 3 (Konjugation)**.** Sei $(G, \cdot\,)$ eine Gruppe.

1. Zeigen Sie: Ist $g \in G$, so ist die folgende Abbildung ein Automorphismus 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.

Aufgabe 4 (Isometriegruppe)**.** Bestimmen Sie die Isometriegruppe von
$$B := \big([0,1] \times \{0,1,2\}\big) \cup \big(\{0,1\} \times [0,2]\big) \subset \mathbb{R}^2$$
bezüglich der euklidischen Metrik d_2 auf $\mathbb{R}^2$.



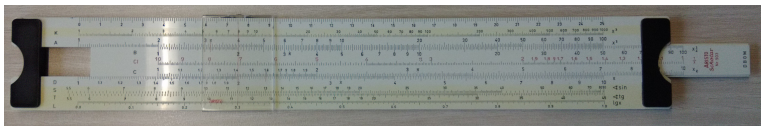
Hinweis. Es genügt, wenn Sie alle Elemente dieser Gruppe und ihre Verknüpfungen explizit beschreiben und die wichtigsten Beweisschritte skizzieren.

Bitte wenden

Bonusaufgabe (Isabelle)**.** Formulieren Sie den untenstehenden Satz und seinen Beweis auf die „gewöhnliche“ menschenfreundliche Weise. Was hat das mit Gruppentheorie zu tun?

```
theory Groups-Exercise

  imports Main

begin

class blubb =
  fixes argh :: 'a ⇒ 'a ⇒ 'a  (infixl ## 70)
  fixes iik :: 'a (e)
  fixes oink :: 'a ⇒ 'a
  assumes drei: x ## (y ## z) = (x ## y) ## z
  assumes iik-nix: x ## e = x
  assumes oink-iik: x ## oink x = e
  assumes iik-oink:  oink x ## x = e

theorem (in blubb) nix-iik: e ## x = x

proof −

  have e ## x = (x ## oink x) ## x
    by (simp only: oink-iik)
  also have ... = x ## (oink x ## x)
    by (simp only: drei)
  also have ... = x ## e
    by (simp only: iik-oink)
  also have ... = x
    by (simp only: iik-nix)
  finally show ?thesis by simp

qed

theorem (in blubb) blorx: oink x = oink y ⟹ x = y

proof −

  assume slurp: oink x = oink y
  have x = x ## e
    by (simp only: iik-nix)
  also have ... = x ## (oink y ## y)
    by (simp only: iik-oink)
  also have ... = (x ## oink y) ## y
    by (simp only: drei)
  also have ... = (x ## oink x) ## y
    by (simp only: slurp)
  also have ... = e ## y
    by (simp only: oink-iik)
  also have ... = y
    by (simp only: nix-iik)
  finally show ?thesis by simp

qed

end
```

Bonusaufgabe (Rechenschieber; für Lehrämtler (als optionale Alternative zur obigen Bonusaufgabe))**.** Wie funktionieren Rechenschieber? Was hat das mit dem Gruppenisomorphismus $\exp\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot\,)$ zu tun?



Abgabe bis zum 27. Oktober 2017, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 2 vom 27. Oktober 2017

Aufgabe 1 (Gruppenhomomorphismen)**.** Seien G, H Gruppen, sei $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

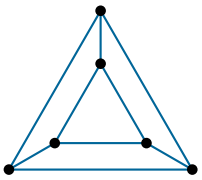
1. Ist $K \subset H$ ein Normalteiler von H, so ist das Urbild $f^{-1}(K)$ ein Normalteiler von G.
2. Ist $K \subset G$ ein Normalteiler von G, so ist $f(K)$ ein Normalteiler von H.

Aufgabe 2 (Untergruppen vom Index 2)**.**

1. Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe vom Index 2. Zeigen Sie, dass H dann bereits ein Normalteiler in G ist.
2. Äußerst nützliche (?!) Folgerung: Sei G eine Gruppe mit $|G| = 4034$. Zeigen Sie, dass alle Untergruppen von G, die mindestens 42 Elemente enthalten, Normalteiler sind.

Aufgabe 3 (S_3, anschaulich)**.** Sei $\tau := (1\ 2) \in S_3$ und sei $\sigma := (1\ 2\ 3) \in S_3$ die Permutation, die die Elemente $1,\ 2,\ 3$ zyklisch vertauscht.

1. Zeigen Sie, dass $\{\sigma, \tau\}$ ein Erzeugendensystem von S_3 ist.
2. Beschriften Sie die Knoten des abgebildeten Graphen so, dass klar wird, dass es sich dabei um den Cayleygraphen $\mathrm{Cay}(S_3, \{\sigma, \tau\})$ handelt.



Aufgabe 4 (kleine/große symmetrische Gruppen)**.** Sei X eine Menge.

1. Zeigen Sie: Ist X endlich, so ist S_X endlich erzeugt.
2. Zeigen Sie: Ist X unendlich, so ist S_X *nicht* endlich erzeugt.

   Hinweis. Es ist nützlich, sich zu überlegen, dass endlich erzeugte Gruppen (höchstens) abzählbar sind …

Bonusaufgabe (Freiheit)**.** Lesen Sie den Anhang über freie Gruppen im Skript.

1. Zeigen Sie, dass die Gruppen $\mathbb{Z}/2$ und $\mathbb{Z}^2$ *nicht* frei sind.
2. Sei S eine Menge. Lesen Sie die Konstruktionsskizze für die Gruppe $F(S)$ und ergänzen Sie die fehlenden Details. (Warum ist die Verknüpfung wohldefiniert? Warum handelt es sich um eine Gruppe? Warum ist diese Gruppe frei von S erzeugt?)

Abgabe bis zum 3. November 2017, 10:00 Uhr, in die Briefkästen

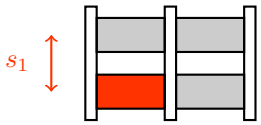
Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 3 vom 3. November 2017

Aufgabe 1 (Quotientengruppen)**.** 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 (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Ist $N \cong N'$ und $G/N \cong G'/N'$, so folgt $G \cong G'$.
2. Ist $G \cong G'$ und $N \cong N'$, so folgt $G/N \cong G'/N'$.

Aufgabe 2 (H 31)**.** In H 31 gibt es vier Tafeln, die unabhängig voneinander auf- und abbewegt werden können; der Einfachheit halber nehmen wir an, dass sich jede Tafel nur in zwei Positionen befinden kann, nämlich oben oder unten. Die vier Schalter an den Tafeln erlauben es, die Tafeln jeweils einzeln nach oben bzw. unten zu bewegen.



Die vier Schalter können somit durch die Elemente

$$s_1 := \big([1],[0],[0],[0]\big)$$
$$s_2 := \big([0],[1],[0],[0]\big)$$
$$s_3 := \big([0],[0],[1],[0]\big)$$
$$s_4 := \big([0],[0],[0],[1]\big)$$

in der Gruppe $G := \prod_{j=1}^{4} \mathbb{Z}/2$ modelliert werden.

1. Zeigen Sie, dass $\{s_1 + s_2 + s_3 + s_4, s_1 + s_2 + s_4, s_1 + s_2, s_2\}$ ein Erzeugendensystem von G ist. Wäre dies ein praktisches Erzeugendensystem?!
2. Gibt es ein Erzeugendensystem von G, das nur drei Elemente enthält? Begründen Sie Ihre Antwort!

Aufgabe 3 (semi-direkte Produkte)**.** Seien N, Q Gruppen und $\varphi\colon Q \longrightarrow \mathrm{Aut}(N)$ ein Gruppenhomomorphismus.

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 $\big(\varphi(q^{-1})(n^{-1}), q^{-1}\big)$ das Inverse von (n, q) in $N \rtimes_\varphi Q$.

Aufgabe 4 (spaltende Erweiterungen)**.**

1. Sei G eine Gruppe, sei $N \subset G$ ein Normalteiler und sei $Q := G/N$, mit kanonischer Projektion $\pi\colon G \longrightarrow G/N = Q$. 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
$$G \cong N \rtimes_\varphi Q.$$
2. Folgern Sie: Für jedes $n \in \mathbb{N}_{\geq 2}$ gibt es einen Gruppenhomomorphismus $\varphi\colon \mathbb{Z}/2 \longrightarrow \mathrm{Aut}(A_n)$ mit $S_n \cong A_n \rtimes_\varphi \mathbb{Z}/2$.

Bitte wenden

Bonusaufgabe (Schröder-Bernstein?!)**.** Gilt auch die gruppentheoretische Variante des Satzes von Schröder-Bernstein? Genauer: Seien G und H Gruppen und es gebe injektive Gruppenhomomorphismen $G \longrightarrow H$ und $H \longrightarrow G$; folgt dann bereits $G \cong H$?
Hinweis. Produkte?!

Bonusaufgabe (Spiegelei; für Lehrämtler (als optionale Alternative zur obigen Bonusaufgabe))**.**

1. Zeigen Sie, dass $\mathrm{Isom}(\mathbb{R}^2, d_2)$ von der Menge aller Spiegelungen (an affinen Geraden) erzeugt wird.
2. Wann/Wie geht dies in den Schulunterricht ein?

Hinweis. Sie dürfen verwenden, dass

$$\begin{aligned} \mathbb{R}^2 \rtimes_\varphi \mathrm{O}(2) &\longrightarrow \mathrm{Isom}(\mathbb{R}^2, d_2) \\ (x, A) &\longmapsto (v \mapsto A \cdot v + x) \end{aligned}$$

ein Gruppenisomorphismus ist, wobei

$$\begin{aligned} \varphi\colon \mathrm{O}(2) &\longrightarrow \mathrm{Aut}(\mathbb{R}^2) \\ A &\longmapsto (x \mapsto A \cdot x). \end{aligned}$$

Abgabe bis zum 10. November 2017, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 4 vom 10. November 2017

Aufgabe 1 (Bahnen und Stabilisatoren)**.** 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 2 (Konjugationsoperation)**.** Sei G eine Gruppe und sei

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

(s. Aufgabe 3 von Blatt 1).

1. Zeigen Sie, dass ϱ eine Operation von G auf G definiert.
2. Sei $g \in G$. Zeigen Sie, dass der Stabilisator von g unter dieser Operation die folgende Menge ist:
$$Z_G(g) := \{h \in G \mid h \cdot g = g \cdot h\}.$$
3. Bestimmen Sie $Z_{S_3}(g)$ für alle $g \in S_3$.
4. Bestimmen Sie für jedes $g \in S_3$ die S_3-Bahn von g unter dieser Operation von S_3 auf S_3.

Aufgabe 3 (Triforce-Münzen)**.** 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)

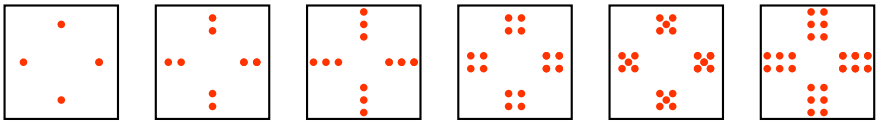
Um verschiedene Sorten Münzen zu ermöglichen, können aus den vier Dreiecken noch Kreise oder seitenparallele Dreiecke ausgestanzt werden. Wieviele essentiell verschiedene solcher Münzen gibt es? Begründen Sie Ihre Antwort!
Hinweis. Die Münzen in Abbildung (b) und (c) sind essentiell verschieden, aber die Münzen in Abbildung (c) und (d) *nicht*.

Aufgabe 4 (Fixpunktnonsens)**.** 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.

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.

Bitte wenden

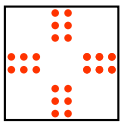
Bonusaufgabe (Würfel)**.** Ein Casino-Betreiber verwendet Würfel, bei denen jede Seite mit einem der folgenden Symbole dekoriert ist:



Dabei können manche Symbole auch auf mehreren Seiten vorkommen (und andere Symbole dafür gar nicht).

1. Wieviele essentiell verschiedene solcher Würfel gibt es? Begründen Sie Ihre Antwort!

2. Wieviele essentiell verschiedene solcher Würfel gibt es, wenn jeder Würfel höchstens auf einer Seite das Symbol



enthalten darf? Begründen Sie Ihre Antwort!

Hinweis. Die relevante Gruppe enthält genau 24 Elemente.

Abgabe bis zum 17. November 2017, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 5 vom 17. November 2017

Aufgabe 1 (Zykelsalat)**.** 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.

Aufgabe 2 (endliche abelsche Gruppen)**.** Seien $p, q \in \mathbb{N}$ Primzahlen mit $p \neq q$.

1. Bestimmen Sie ein Repräsentantensystem für die Isomorphieklassen abelscher Gruppen A mit $|A| = p^2 \cdot q^2$.
2. Zeigen Sie, dass jede abelsche Gruppe A mit $|A| = p^2 \cdot q^2$ ein zweielementiges Erzeugendensystem besitzt.

Aufgabe 3 (Zykelzerlegung)**.** Begründen Sie jeweils Ihre Antwort!

1. Gibt es einen injektiven Gruppenhomomorphismus $\mathbb{Z}/10 \longrightarrow S_7$?
2. Gibt es einen injektiven Gruppenhomomorphismus $\mathbb{Z}/8 \longrightarrow S_7$?

Aufgabe 4 (14/15-Puzzle)**.** Beim 14/15-*Puzzle* sind fünfzehn numerierte Plättchen und eine „Lücke“ auf einem quadratischen Brett verteilt (siehe linke Abbildung). Modellieren Sie die Situation geeignet in S_{16} und zeigen Sie mithilfe des Signums, dass es *nicht* möglich ist, durch Verschieben der Plättchen die Position in der rechten Abbildung zu erreichen.

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	

Bonusaufgabe (GAP)**.** 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 zum 24. November 2017, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 6 vom 24. November 2017

Aufgabe 1 (Sylowlogie)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Es gibt eine einfache Gruppe G mit $|G| = 42$.
2. Jede Gruppe G mit $|G| = 200$ ist auflösbar.

Aufgabe 2 (Diedergruppen)**.**

1. Sei $n \in \mathbb{N}_{\geq 3}$. Zeigen Sie, dass $[D_n, D_n]$ zyklisch ist. Wieviele Elemente enthält diese Gruppe?
2. Bestimmen Sie alle 2-Sylowgruppen und alle 3-Sylowgruppen in D_6 und skizzieren Sie die entsprechenden Isometrien eines regulären Sechsecks.

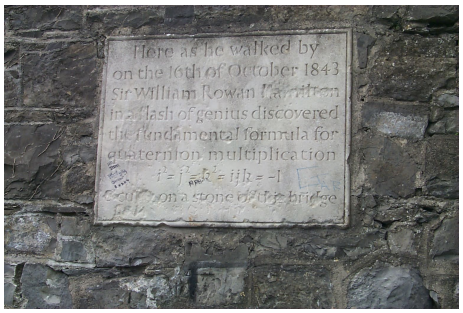
Aufgabe 3 (Primquadrate)**.**

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)**.** Sei G eine Gruppe mit $|G| = 1001$. Zeigen Sie, dass es einen surjektiven Gruppenhomomorphismus $G \longrightarrow \mathbb{Z}/13$ gibt.
Hinweis. Sylow!

Bonusaufgabe (Quaternionen)**.**

1. Wie sind die Quaternionen definiert?
2. Welche algebraischen Eigenschaften besitzen die Quaternionen?
3. Geben Sie eine Verknüpfungstabelle für die (acht-elementige) Quaternionengruppe an.



Abgabe bis zum 1. Dezember 2017, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 7 vom 1. Dezember 2017

Aufgabe 1 (Funktionenringe). Sei $R := C([0,1], \mathbb{R})$ der Ring der stetigen Funktionen $[0,1] \longrightarrow \mathbb{R}$ (bezüglich punktweiser Addition und Multiplikation). Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Die Abbildung $\int_0^1 dx \colon R \longrightarrow \mathbb{R}$ ist ein Ringhomomorphismus.
2. Die Menge $\{f \in R \mid \forall_{n \in \{0,1\}} \quad f(n) = 0\}$ ist ein Ideal in R.

Aufgabe 2 (vierte Potenzen).

1. Bestimmen Sie alle vierten Potenzen in $\mathbb{Z}/(8)$.
2. Folgern Sie, dass die Gleichung
$$x^{2020} - y^{44} - x^{2016} \cdot y^{200} - 88 \cdot x \cdot y^{2017} \cdot z = 555556$$
keine Lösungen $x, y, z \in \mathbb{Z}$ besitzt.

Aufgabe 3 (Körper).

1. Zeigen Sie: Ist R ein endlicher Integritätsring, so ist R bereits ein Körper.
Hinweis. Injektive Selbstabbildungen einer endlichen Menge sind bereits surjektiv.
2. Zeigen Sie: Ein Ring $R \ncong \{0\}$ ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale von R sind.

Aufgabe 4 (Ringe mit $p \cdot q$ Elementen). Seien $p, q \in \mathbb{N}$ prim mit $p \neq q$ und sei R ein Ring mit $|R| = p \cdot q$. Zeigen Sie, dass 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?

Bonusaufgabe (Nikolausaufgabe). Alle Jahre wieder lässt sich der Nikolaus auf ein Wettrennen mit seinem grazilen Rentier Ruprecht ein.

Ruprecht legt pro Schritt einen Meter zurück, der Nikolaus – trotz des viel zu langen Barts – hingegen beeindruckende eineinhalb Meter; jedoch kann der etwas füllige Nikolaus in der Zeit, in der Ruprecht drei Schritte tänzelt, nur zwei Schritte gehen.

Ruprecht schlägt für dieses Jahr folgende Streckenführung vor: Vom Haus des Nikolaus bis zum hundert Meter entfernten Pool und wieder zurück.

Wer wird gewinnen? Warum?

Abgabe bis zum 8. Dezember 2017, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 8 vom 8. Dezember 2017

Aufgabe 1 (komplexe Zahlen?!)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Es gilt $\mathbb{R}[T]/(T^2+1) \cong \mathbb{C}$.
2. Es ist $\mathbb{F}_7[T]/(T^2+1)$ ein Körper.

Aufgabe 2 (Adventskalender)**.** 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!

Aufgabe 3 (gaußsche Primzahlen)**.** 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 $\mathbb{Z}[i] \subset \mathbb{C}$.

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!

Aufgabe 4 (reelle Zahlen)**.** Sei Q die Menge aller Cauchyfolgen mit Folgengliedern in $\mathbb{Q}$ und sei $N \subset Q$ die Menge aller Nullfolgen. Dann bildet Q einen Ring bezüglich gliedweiser Addition bzw. Multiplikation.

1. Zeigen Sie, dass N ein maximales Ideal in Q ist.
2. Folgern Sie, dass der Restklassenring Q/N ein Körper ist und geben Sie einen injektiven Ringhomomorphismus $\mathbb{Q} \longrightarrow Q/N$ an.

Auf diese Weise kann man $\mathbb{R}$ aus $\mathbb{Q}$ konstruieren!

Bitte wenden

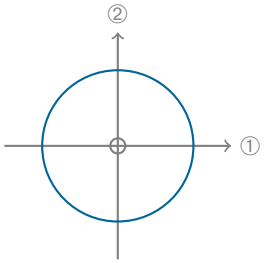
Bonusaufgabe (Kreis-Ring)**.** Wir betrachten den Ring

$$R := \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$$

zur Kreisgleichung „$x^2 + y^2 = 1$“.

1. Zeigen Sie, dass $R \cong \mathbb{C}[T, T^{-1}]$. Dabei bezeichnet $\mathbb{C}[T, T^{-1}]$ den Unterring von $\mathbb{C}(T)$, der von $\mathbb{C}[T]$ und $1/T$ erzeugt wird.
2. Zeigen Sie, dass $\mathbb{C}[T, T^{-1}] \ncong \mathbb{C}[T]$ und folgern Sie $R \ncong \mathbb{C}[T]$.

   Hinweis. Einheiten!



Abgabe bis zum 15. Dezember 2017, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 9 vom 15. Dezember 2017

Aufgabe 1 (Fermat?!)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Ist $p \in \mathbb{N}$ prim und $x \in \mathbb{Z}$, so gilt $x^p \equiv x \mod p$.
2. Ist $m \in \mathbb{N}_{>1}$ und $x \in \mathbb{Z}$, so gilt $x^{\varphi(m)+1} \equiv x \mod m$.

Aufgabe 2 (Primpolynome)**.** Sei R ein faktorieller Ring. Zeigen Sie, dass der Polynomring $R[T]$ unendlich viele Primelemente enthält.
Hinweis. Was würde Euklid tun?!

Aufgabe 3 (RSA)**.**

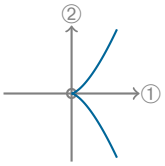
1. Bestimmen Sie einen passenden privaten Schlüssel zu dem öffentlichen Schlüssel $(6661, 8051)$.
2. Entschlüsseln Sie mit diesem privaten Schlüssel den folgenden mit dem öffentlichen Schlüssel $(6661, 8051)$ verschlüsselten Klassiker (Goethe!):

   937, 2978, 87, 4201, 4969, 1713, 4201, 7677, 2356, 6087, 2948, 3371, 449, 2978, 3207, 2789, 5702, 201, 1569, 7241, 4380, 4642, 4741, 6636, 1535, 7118, 7677, 2356, 4395, 900, 7902, 3371, 2978, 3207, 2789, 2974, 3371, 7058, 7061, 854, 3211, 4201, 4264, 7136, 672, 6350, 2789, 3574, 7757, 2788, 2177, 308, 4957, 3179, 1713, 1, 87, 2431, 6009, 3578, 1569, 7241, 7061, 6216, 3352, 7061, 854, 3369, 6292, 4264, 2788, 6093, 6040, 2978, 3207, 2789, 1743, 7252, 878, 1569, 7241, 1, 7058, 2773, 356, 4356, 4201, 2948, 4252, 959, 2595, 3207, 7180, 1569, 7241, 5938, 2170, 2356, 1518, 2773, 3371, 449, 1569, 7241, 4380, 7677, 2356, 1518, 2773, 977, 84, 2948, 6761, 2948, 1518, 2773, 6761, 2948, 6310, 4007, 5288, 84, 4715, 472, 84, 2948

   Hinweis. Das Leerzeichen wird durch 0 repräsentiert, die Buchstaben A, ..., Z des Alphabets durch $1, \dots, 26$. Die Zahlen x, y zu zwei aufeinanderfolgenden Buchstaben werden zu $[100 \cdot x + y] \in \mathbb{Z}/(8051)$ zusammengefasst. Dies wurde dann mit RSA verschlüsselt.

Aufgabe 4 (noch eine Kurve)**.** Sei K ein Körper. Sei $R := K[X, Y]/(Y^2 - X^3)$ der Ring zur Gleichung „$y^2 = x^3$“. Wir schreiben $x, y \in R$ für die von X bzw. Y repräsentierten Restklassen. Bearbeiten Sie zwei der folgenden vier Aufgaben:

1. Zeigen Sie, dass $Y^2 - X^3$ in $K[X, Y]$ prim ist und folgern Sie, dass R ein Integritätsring ist.
2. Zeigen Sie $x, y, x^3, y^2 \notin \{0\} \cup R^\times$.
   Hinweis. Wie kommen Sie via „$X \mapsto T^2$, $Y \mapsto T^3$“ von R nach $R[T]$?
3. Zeigen Sie, dass x und y in R irreduzibel sind, indem Sie passende Gleichungen in $K[X, Y]$ betrachten.
4. Folgern Sie, dass R *nicht* faktoriell ist und insbesondere $R \ncong K[X]$ gilt.



Bitte wenden

Bonusaufgabe (Kauderwelsch)**.** Entschlüsseln Sie folgenden deutschen Text:

> WMJXQNQRHQYDVYNZRPQR ZRC URAVBNQ. CUQ
> IFAZQBQYURRQR ZRC IFAZQBQY ... KVWNMYUIUQYQR
> RVNZQYBUFAQ HVABQR ZRC QYJUNNQBR CQYQR
> XYUJKVWNMYHQYBQPZRP, DMLQU IUQ IUFA CQY
> QURCQZNUPWQUN CUQIQY HQYBQPZRP LQDZIIN IURC; LQUJ
> KVWNMYUIUQYQR DQRCQR IUQ VZFA YQPQBR KZQY CUQ
> NQUBLVYWQUN CZYFA HDQU, CYQU, KZQRK ZRC HQAR
> HUQBPQYUFANQN VR. IUQ RZNHQR CUQIQ WQRRNRUIIQ VZFA
> KZQY VYPZJQRNVNUMRQR, HZJ LQUIXUQB UJ YVAJQR CQY
> LQVRNDMYNZRP VBBNVPIRVAQY KYVPQINQBBZRPQR.

Hinweis. Jedes Zeichen steht dabei immer für denselben Buchstaben. Satzzeichen bleiben unverschlüsselt. Welche Buchstaben sind im Deutschen am häufigsten?

Abgabe bis zum 22. Dezember 2017, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 10 vom 22. Dezember 2017

Aufgabe 1 (Irreduzibilität)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Das Polynom $T^3 + 2019 \cdot T^2 + 42 \cdot T + 9 \in \mathbb{Z}[T]$ ist irreduzibel in $\mathbb{Z}[T]$.
2. Das Polynom $X^2 \cdot Y + Y^2 \cdot X^{2018} + X + Y + 1$ ist irreduzibel in $\mathbb{F}_2[X, Y]$.

Aufgabe 2 (Restklassenkörper)**.** Zu $a \in \mathbb{Z}$ sei $f_a := T^4 + a \cdot T + 2 \in \mathbb{Q}[T]$.

1. Zeigen Sie: Es gibt unendlich viele $a \in \mathbb{Z}$, für die $\mathbb{Q}[T]/(f_a)$ ein Körper ist.
2. Bestimmen Sie alle $a \in \mathbb{Z}$, für die $\mathbb{Q}[T]/(f_a)$ *kein* Körper ist.

   Hinweis. Diese Polynome sind primitiv in $\mathbb{Z}[T]$. Warum hilft das?

Aufgabe 3 (Primkörper)**.** 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 (Binomi für Dummies)**.** 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 (invariant und irreduzibel)**.** 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. Das obige 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 ...

Bitte wenden

Die folgenden Aufgaben bieten die Gelegenheit, den bisher gelernten Stoff zu Gruppen, Ringen und Körpern zu wiederholen und zu vertiefen; für jede dieser Aufgaben können Sie bis zu vier Zusatzpunkte bekommen.

Bonusaufgabe (Gruppen für Schüler)**.** Wie kann man Schülern (der Mittelstufe) anhand eines Pappquadrats erklären, was eine (Symmetrie)Gruppe ist? Wie könnte man das Pappquadrat dafür markieren/dekorieren?

Bonusaufgabe (Struktur endlicher Gruppen)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Ist G eine Gruppe mit $|G| = 2018$, so ist jede 2-Sylowgruppe in G normal.
2. Je zwei Untergruppen von S_5 mit genau acht Elementen sind isomorph.

Bonusaufgabe (Sylowmatrizen)**.** Sei $p \in \mathbb{N}$ prim und $n \in \mathbb{N}_{\geq 1}$. Zeigen Sie, dass

$$\left\{ \begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ 0 & \dots & 0 & 1 \end{pmatrix} \middle| \, a_{12}, a_{13}, \dots, a_{n-1,n} \in \mathbb{F}_p \right\} \subset \mathrm{GL}_n(\mathbb{F}_p)$$

eine p-Sylowgruppe in $\mathrm{GL}_n(\mathbb{F}_p)$ ist.
Hinweis. Zählen!

Bonusaufgabe (kleiner Fermat für Schüler)**.**

1. Sei $p \in \mathbb{N}$ prim. Beweisen Sie induktiv (natürlich ohne den kleinen Satz von Fermat zu verwenden), dass $x^p - x$ für jedes $x \in \mathbb{Z}$ durch p teilbar ist. Schreiben Sie den Beweis so auf, dass er für einen Mittelstufenschüler verständlich ist.
2. Wie könnte man aufbauend darauf das RSA-Verfahren Schülern erklären?

Bonusaufgabe (Kubismus)**.** Zeigen Sie: Es gibt *keine* ganzen Zahlen x, y, z mit

$$x^3 + y^3 + z^3 = 2020.$$

Hinweis. Reduktion!

Bonusaufgabe (noch ein Körper)**.** Zeigen Sie, dass

$$\mathbb{Z}[T]/(T^4 - T^3 - T^2 - 3 \cdot T + 5, T^3 + T^2 + T - 1)$$

ein Körper ist.
Hinweis. Kann man dieses Ideal einfacher darstellen?

Bonusaufgabe (Skript)**.** Finden Sie so viele Fehler im Skript wie möglich!

Abgabe bis zum 12. Januar 2018, 10:00 Uhr, in die Briefkästen

Frohe Weihnachten und ein Gutes Neues Jahr!

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 11 vom 12. Januar 2018

Aufgabe 1 (Charakteristik)**.** Seien K und L Körper. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort!

1. Gibt es einen Körperhomomorphismus $K \longrightarrow L$, so ist $\operatorname{char} K = \operatorname{char} L$.
2. Ist $\operatorname{char} K = \operatorname{char} L$, so gibt es einen Körperhomomorphismus $K \longrightarrow L$.

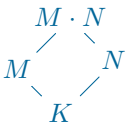
Aufgabe 2 (ungerade Grade)**.** Sei $L \mid K$ eine Körpererweiterung und sei $\alpha \in L$ mit $[K(\alpha) : K] = 2019$. Zeigen Sie, dass $K(\alpha) = K(\alpha^2)$.

Aufgabe 3 (ein Zerfällungskörper von $T^4 - 42$ über $\mathbb{Q}$)**.** 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 $\mathbb{Q}(\sqrt[4]{42})$?
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 $\operatorname{Gal}(K, \mathbb{Q})$ *kein* Element der Ordnung 8 enthält.
   Hinweis. Wieviele Nullstellen haben $T^4 - 42$ bzw. $T^2 + 1$ in K ?

Aufgabe 4 (Grade von Komposita)**.** 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 $\operatorname{ggT}\big([M : K], [N : K]\big) = 1$, so ist
$$[M \cdot N : K] = [M : K] \cdot [N : K].$$



Bonusaufgabe (Transzendenz)**.** Zeigen Sie, dass die reelle Zahl
$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.11000100000000000000000001\ldots$$
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 zum 19. Januar 2018, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 12 vom 19. Januar 2018

Aufgabe 1 (algebraische Zahlen)**.** 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 2 (algebraische Erweiterungen)**.** 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 3 (Wurzeln)**.** Sei $n \in \mathbb{N}_{\geq 2}$, sei K ein Körper, der ein Zerfällungskörper von $T^n - 1 \in K[T]$ über K ist, 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.

Aufgabe 4 (Fixkörper)**.** Sei $L \mid K$ eine Körpererweiterung, sei $G \subset \mathrm{Gal}(L, K)$ eine endliche Untergruppe und sei

$$M := L^G := \{x \in L \mid \forall_{\sigma \in G} \quad \sigma(x) = x\}$$

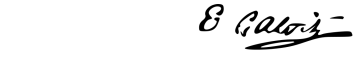
der *Fixkörper von $L \mid K$ bezüglich G*. Sei $\alpha \in L$.

1. Zeigen Sie, dass M ein Zwischenkörper von $L \mid K$ ist.
2. Sei $(\sigma_1, \dots, \sigma_m)$ eine maximale Familie in G, für die $\sigma_1(\alpha), \dots, \sigma_m(\alpha)$ 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.

Bonusaufgabe (Galois)**.** Wo hängt Galois im Mathematikgebäude? Wer sind seine Nachbarn? Warum sieht Galois auf allen Bildern so jung aus?



Abgabe bis zum 26. Januar 2018, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 13 vom 26. Januar 2018

Aufgabe 1 (algebraischer Abschluss)**.** Sei K ein Körper. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort!

1. Gilt für jede Körpererweiterung $L \mid K$, dass $[L : K] \in \{1, \infty\}$, so ist K algebraisch abgeschlossen.
2. Ist K algebraisch abgeschlossen, so gilt für jede Körpererweiterung $L \mid K$, dass $[L : K] \in \{1, \infty\}$.

Aufgabe 2 (Galoisgruppen von Gleichungen)**.**

1. Bestimmen Sie die Galoisgruppe des Polynoms $T^4+T^3+T^2+T+1$ über $\mathbb{Q}$.

   Hinweis. Was hat das mit ζ_5 und Eisenstein zu tun?
2. Bestimmen Sie die Galoisgruppe des Polynoms $T^3 - 2$ über $\mathbb{F}_5$.

Aufgabe 3 (Ableitungskriterium)**.** 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.

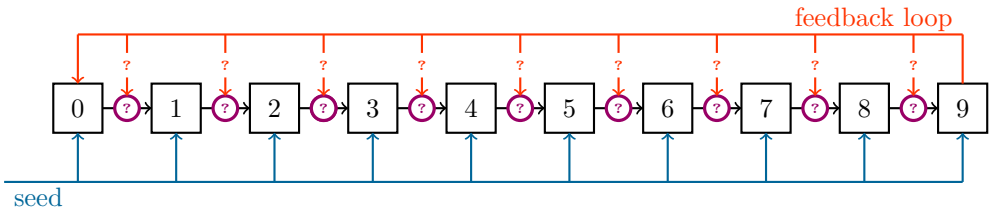
1. Zeigen Sie, dass f genau dann eine mehrfache Nullstelle in L besitzt, wenn $\mathrm{ggT}(f, Df) \neq 1$ (in $L[T]$; Bonusaufgabe: in $K[T]$) ist.
2. Zeigen Sie: Ist f in $K[T]$ irreduzibel, so besitzt f genau dann eine mehrfache Nullstelle in L, wenn $Df = 0$ ist.

Aufgabe 4 (Klassifikation endlicher Körpererweiterungen von endlichen Körpern)**.** 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 (LFSR)**.** Konstruieren Sie ein LFSR mit Periodenlänge 1023. Schreiben Sie dazu ein Programm, das ein geeignetes Polynom in $\mathbb{F}_2[T]$ findet und zeigt, dass dieses Polynom die gewünschten Eigenschaften besitzt. Vervollständigen Sie dann die untenstehende Skizze:



Abgabe bis zum 2. Februar 2018, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 14 vom 2. Februar 2018

Aufgabe 1 (normal/separabel und Zwischenkörper)**.** Sei $L \mid K$ eine Körpererweiterung und sei M ein Zwischenkörper von $L \mid K$. Welche der folgenden Aussagen sind in dieser Situation immer wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

1. Ist $L \mid K$ normal, so sind auch $L \mid M$ und $M \mid K$ normal.
2. Ist $L \mid K$ separabel, so sind auch $L \mid M$ und $M \mid K$ separabel.

Aufgabe 2 (Fünfzehn)**.** Sei $\zeta_{15} := e^{2 \cdot \pi \cdot i/15} \in \mathbb{C}$.

1. Konstruieren Sie einen Isomorphismus $\big(\mathbb{Z}/(15)\big)^\times \cong \mathbb{Z}/4 \times \mathbb{Z}/2$.
2. Bestimmen Sie alle Untergruppen von $\mathbb{Z}/4 \times \mathbb{Z}/2$.
3. Bestimmen Sie $\mathrm{Gal}\big(\mathbb{Q}(\zeta_{15}), \mathbb{Q}\big)$ möglichst explizit.
4. 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?!

Aufgabe 3 (schon wieder Fünfzehn)**.** 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 (Fixkörper)**.** Sei $L \mid K$ eine Galoiserweiterung. Zeigen Sie, dass

$$L^{\mathrm{Gal}(L,K)} = K.$$

Hinweis. Konjugationsprinzip, was sonst?

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 $\mathrm{Gal}(L, K) \cong \mathbb{Z}/n$. Zeigen Sie, dass es dann ein $c \in K$ gibt, so dass L ein Zerfällungskörper von $T^n - c$ über K ist.

Hinweis. Sei $\sigma \in \mathrm{Gal}(L, K) \cong \mathbb{Z}/n$ 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 (die Argumente aus Beispiel II.3.3.23 helfen dabei!). 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 12.3).
4. Zeigen Sie, dass $L = K(\alpha)$ ist (Grade?!).

Frewillige Abgabe bis zum 9. Februar 2018, 10:00 Uhr, in die Briefkästen

Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 15 vom 9. Februar 2018

Aufgabe 1 (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 2 (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 3 (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.

Aufgabe 4 (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 $n \to \infty$?!

Bonusaufgabe (Skript)**.** Finden Sie so viele Fehler im Skript wie möglich!

keine Abgabe

C

Fingerübungen

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 0 vom 16. Oktober 2017

Aufgabe 1 (Gruppen).

1. Wie sind Gruppen definiert?
2. Welche der folgenden Strukturen sind Gruppen?
   (a) Die Menge $\mathbb{Z}$ bezüglich Addition.
   (b) Die Menge $\mathbb{Z}$ bezüglich Multiplikation.
   (c) Die Menge $\{1/n \mid n \in \mathbb{N}_{>0}\}$ bezüglich Multiplikation.
   (d) Die Menge $\{n^2 \mid n \in \mathbb{N}_{>0}\}$ bezüglich Multiplikation.
3. Sei $(G, \cdot\,)$ eine Gruppe. Welche der folgenden Aussagen sind wahr?
   (a) Ist $g \in G$ mit $g \cdot g = g$, so ist g das neutrale Element e.
   (b) Ist $g \in G$ mit $g \cdot g = e$, so ist $g = e$.

Aufgabe 2 (Untervektorräume).

1. Wie sind Untervektorräume definiert?
2. Wie kann man überprüfen, ob ein Untervektorraum vorliegt?
3. Sind Durchschnitte von Untervektorräumen Untervektorräume?
4. Sind Vereinigungen von Untervektorräumen Untervektorräume?
5. Welche der folgenden Mengen sind Untervektorräume von $\mathbb{R}^3$?
   (a) $\{x \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}$
   (b) $\{x \in \mathbb{R}^3 \mid x_1 = {x_2}^2\}$
   (c) $\{x \in \mathbb{R}^3 \mid x_3 \geq 0\}$
   (d) $\{x \in \mathbb{R}^3 \mid x_1 \cdot x_2 = 0\}$
6. Sei $U := \{x \in \mathbb{R}^2 \mid 2 \cdot x_1 = -x_2\}$. Skizzieren Sie die folgenden Mengen in $\mathbb{R}^2$:
$$\begin{pmatrix}0\\0\end{pmatrix} + U, \quad \begin{pmatrix}1\\1\end{pmatrix} + U, \quad \begin{pmatrix}1\\0\end{pmatrix} + U, \quad \begin{pmatrix}2\\-2\end{pmatrix} + U.$$

Aufgabe 3 (Ringe und Körper).

1. Wie sind Ringe definiert?
2. Wie sind Körper definiert?
3. Wie sind Polynomringe über Körpern definiert?

Aufgabe 4 (Lücken). Welche Begriffe/Sätze aus der Linearen Algebra I/II haben Sie vergessen? Welche Beweise/Rechentechniken aus der Linearen Algebra I/II finden Sie dubios? Füllen Sie diese Lücken!

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 1 vom 23. Oktober 2017

Aufgabe 1 (zyklische Gruppen)**.** Sei G eine der Gruppen $\mathbb{Z}/7$, $\mathbb{Z}/8$, $\mathbb{Z}/9$, $\mathbb{Z}/10$.

1. Berechnen Sie für jede dieser Möglichkeiten in G den Ausdruck
$$[2] + [7] - [42] + [5] + [-2017].$$
2. Überlegen Sie jeweils, ob es ein $x \in G$ mit $x + x + x = [5]$ gibt.
3. Bestimmen Sie jeweils alle Untergruppen von G.

Aufgabe 2 (symmetrische Gruppen)**.**

1. Listen Sie alle Elemente von S_3 auf.
2. Bestimmen Sie alle Untergruppen von S_3.
3. Besitzt S_3 eine Untergruppe, die $\mathbb{Z}/3$ isomorph ist?
4. Besitzt S_3 eine Untergruppe, die $\mathbb{Z}/4$ isomorph ist?

Aufgabe 3 (Quotientenvektorräume)**.**

1. Wie werden Quotientenvektorräume konstruiert?
2. Welche universelle Eigenschaft besitzen Quotientenvektorräume?
3. Welche weiteren Eigenschaften von Quotientenvektorräumen kennen Sie?
4. Welche der folgenden Terme liefern wohldefinierte $\mathbb{R}$-lineare Abbildungen $\mathbb{R}^3/\{x \in \mathbb{R}^3 \mid x_2 + x_3 = 0\} \longrightarrow \mathbb{R}$?
   (a) $[x] \mapsto x_1$
   (b) $[x] \mapsto x_2$
   (c) $[x] \mapsto x_1 + x_3$
   (d) $[x] \mapsto x_1 + x_2 + x_3$

Aufgabe 4 (Matrixgruppen)**.**

1. An welche Matrixgruppen können Sie sich aus der Linearen Algebra erinnern?
2. Was wissen Sie über die algebraischen und geometrischen Eigenschaften von $\mathrm{O}(n)$ und $\mathrm{SO}(n)$?

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 2 vom 30. Oktober 2017

Aufgabe 1 (symmetrische Gruppen)**.**

1. Bestimmen Sie alle Normalteiler von S_3.
2. Bestimmen Sie die zugehörigen Quotientengruppen.
3. Bestimmen Sie alle $n \in \mathbb{N}$, für die die Gruppe S_n zyklisch ist.

Aufgabe 2 (Normalteilerbuchhaltung)**.** Sei G eine endliche Gruppe und sei $N \subset G$ ein Normalteiler mit $N \neq \{e\}$ und $N \neq G$. Welche der folgenden Situationen können eintreten?

1. $|G| = |N| \cdot |N|$
2. $|G| = |N| \cdot |G/N| \cdot |G/N|$
3. $G/N \cong G$
4. $G/N \cong N$
5. $|G| = |N| + |G/N|$
6. $|G/N| = |G| + |N|$

Aufgabe 3 (Quotientengruppen und Gruppenhomomorphismen)**.** Welche der folgenden Abbildungen sind wohldefinierte Gruppenhomomorphismen?

$$\begin{aligned} \mathbb{Z}/2 &\longrightarrow \mathbb{Z} \\ [n] &\longmapsto n \\ \mathbb{Z}/2 &\longrightarrow \mathbb{Z}/2 \\ [n] &\longmapsto [n^2] \\ S_3/A_3 &\longrightarrow \mathbb{Z}/2 \\ [\sigma] &\longmapsto \big[\operatorname{sgn}(\sigma) + 1\big] \\ S_3/A_3 &\longrightarrow \mathbb{Z}/3 \\ [\sigma] &\longmapsto \big[\sigma(1)\big] \end{aligned}$$

Aufgabe 4 (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?

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 3 vom 6. November 2017

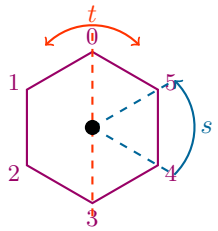
Aufgabe 1 (Produkte). Untersuchen Sie für alle Gruppen G und H aus der folgenden Liste, ob es einen injektiven Gruppenhomomorphismus $G \longrightarrow H$ gibt:

$$\mathbb{Z}/2, \quad \mathbb{Z}/2 \times \mathbb{Z}/3, \quad S_3, \quad \mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{Z} \times \mathbb{Q}, \quad \mathbb{Q} \times \mathbb{Q}$$

Aufgabe 2 (semi-direkte Produkte). Seien N, Q Gruppen, sei $\varphi\colon Q \longrightarrow \mathrm{Aut}(N)$ ein Gruppenhomomorphismus und seien $n \in N$, $q \in Q$. Vereinfachen Sie die folgenden Terme in $N \rtimes_\varphi Q$:

1. $(n, e) \cdot (e, q)$
2. $(e, q) \cdot (n, e)$
3. $(n, q) \cdot (n^{-1}, q^{-1})$
4. $(n, q)^3$

Aufgabe 3 (Isometrien des regulären Sechsecks). Wir betrachten ein reguläres Sechseck X in $(\mathbb{R}^2, d_2)$, dessen Ecken rundherum mit $0, \dots, 5$ durchnumeriert sind. Sei $s \in \mathrm{Isom}(X, d_2)$ die Rotation um $2 \cdot \pi/6$ (um den Mittelpunkt von X, gegen den Uhrzeigersinn) und sei $t \in \mathrm{Isom}(X, d_2)$ die Spiegelung an der Diagonalen durch die Ecken 0 und 3:



1. Beschreiben Sie die folgenden Kompositionen geometrisch auf möglichst einfache Weise:
$$s^2, \quad s^3, \quad s^6, \quad s^{11}, \quad s \circ t, \quad t \circ s, \quad t \circ s \circ t^{-1}.$$
2. Wie kann man die Spiegelung an der Diagonalen durch 2 und 5 als Komposition von s und t ausdrücken?

Aufgabe 4 (universelle Eigenschaften).

1. An welche universellen Eigenschaften können Sie sich aus der Linearen Algebra erinnern?
2. Finden Sie eine universelle Eigenschaft für semi-direkte Produkte!

   Hinweis. Obwohl semi-direkte Produkte Varianten von Produkten sind, hat ihre universelle Eigenschaft etwas mit Homomorphismen *aus* semi-direkten Produkten *heraus* zu tun.

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 4 vom 13. November 2017

Aufgabe 1 (Gruppenoperationen?!)**.** Welche der unten angegebenen Abbildungen $\mathrm{GL}_2(\mathbb{R}) \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ definieren eine Gruppenoperation von $\mathrm{GL}_2(\mathbb{R})$ auf $\mathbb{R}^2$?

1. $(A, x) \longmapsto A \cdot x$
2. $(A, x) \longmapsto A^{-1} \cdot x$
3. $(A, x) \longmapsto A + x$
4. $(A, x) \longmapsto \det(A) \cdot x$

Aufgabe 2 (Satz von Cayley)**.** Geben Sie jeweils eine Untergruppe von S_6 an, die zu der gegebenen Gruppe isomorph ist:

1. $\mathbb{Z}/6$
2. S_3
3. $\mathbb{Z}/4$
4. $\mathbb{Z}/2 \times \mathbb{Z}/2$

Aufgabe 3 (Isometrien des regulären Sechsecks)**.** Wir betrachten ein reguläres Sechseck X in $(\mathbb{R}^2, d_2)$ und die kanonische Operation der zugehörigen Isometriegruppe $G := \mathrm{Isom}(X, d_2)$ auf X.

1. Was ist der Stabilisator des Mittelpunkts von X?
2. Was ist der Stabilisator einer Ecke von X?
3. Welche Punkte von X haben welche Stabilisatoren?
4. Bestimmen Sie für jedes $g \in G$ die zugehörige Fixpunktmenge X^g.
5. Bestimmen Sie für jedes $x \in X$ die zugehörige Bahn $G \cdot x$.

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 1.1; orientieren Sie sich dabei an den folgenden Fragen:

1. Was sind die grundlegenden Begriffe der Gruppentheorie?
2. Welche Beispiele für Gruppen bzw. Konstruktionen von Gruppen kennen Sie? Wozu verwendet man diese?
3. Was sind grundlegende Sätze und Beweismethoden der Gruppentheorie?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen ...

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 5 vom 20. November 2017

Aufgabe 1 (endliche abelsche Gruppen)**.** Bestimmen Sie für jede der folgenden Zahlen $n \in \mathbb{N}$ die Klassifikation der abelschen Gruppen mit genau n Elementen:

$$2017, \quad 2018, \quad 2019, \quad 2020, \quad 8$$

Wieviele Elemente der Ordnung 2 enthalten diese Gruppen?

Aufgabe 2 (Permutationen)**.** Berechnen Sie die folgenden Permutationen in S_5:

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. $(1\ 2) \cdot (2\ 3) \cdot (1\ 2) \cdot (2\ 3)$

Aufgabe 3 (Zykelzerlegungen)**.** Bestimmen Sie Zykelzerlegungen und die Ordnungen der folgenden Permutationen in S_6:

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. $1 \mapsto 6,\ 2 \mapsto 5,\ 3 \mapsto 2,\ 4 \mapsto 1,\ 5 \mapsto 3,\ 6 \mapsto 4$

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 1.2; orientieren Sie sich dabei an den folgenden Fragen:

1. Was sind die grundlegenden Begriffe zu Gruppenoperationen?
2. Welche Beispiele für Gruppenoperationen kennen Sie? Wozu verwendet man diese?
3. Was sind grundlegende Sätze und Beweismethoden für Gruppenoperationen?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen ...

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 6 vom 27. November 2017

Aufgabe 1 (Auflösbarkeit?)**.** Untersuchen Sie, für welche der folgenden Zahlen n alle Gruppen G mit $|G| = n$ auflösbar sind:

1. 2017
2. 2018
3. 2040
4. 2048

Aufgabe 2 (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. $D_5 \times \mathbb{Z}/2$

Aufgabe 3 (Sylowzahlen)**.** Sei n jeweils eine der folgenden Zahlen. Gibt es dann eine Gruppe G mit $|G| = n$ mit genau fünf 2-Sylowgruppen?

1. 5
2. 8
3. 10
4. 30

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 1.3; orientieren Sie sich dabei an den folgenden Fragen:

1. Was ist die allgemeine Klassifikationsstrategie für endliche Gruppen?
2. Was sind die atomaren Bausteine?
3. Welche Gruppen lassen sich gut zerlegen?
4. Was sind grundlegende Sätze und Beweismethoden?
5. Welche Rolle spielen die Sylowsätze in diesem Kontext?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen ...

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 7 vom 4. Dezember 2017

Aufgabe 1 (Ringe). Welche der folgenden Teilmengen von $\mathbb{C}$ sind Ringe (bezüglich komplexer Addition und Multiplikation)?

1. $\{z \in \mathbb{C} \mid \operatorname{Im} z \geq 0\}$
2. $\{z \in \mathbb{C} \mid |z| \leq 1\}$
3. $\{z \in \mathbb{C} \mid \operatorname{Re} z \in \mathbb{Z},\ \operatorname{Im} z \in \mathbb{Z}\}$
4. $\{z \in \mathbb{C} \mid \operatorname{Re} z \in \mathbb{Z} + \sqrt{2} \cdot \mathbb{Z},\ \operatorname{Im} z = 0\}$

Aufgabe 2 (Ringhomomorphismen). Welche dieser Abbildungen $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]$ sind Ringhomomorphismen?

1. $f \longmapsto f(2017)$
2. $f \longmapsto f^2$
3. $f \longmapsto f + 1$
4. $f \longmapsto 2017 \cdot f$

Aufgabe 3 (Restklassenringe). Welche der folgenden Ringe sind isomorph zueinander?

$$\mathbb{Z}/(4), \quad \mathbb{Z}/(2) \times \mathbb{Z}/(2), \quad \mathbb{Z}/(2,4), \quad \big(\mathbb{Z}/(4)\big)/([2018])$$

Aufgabe 4 (Quotientenkörper). Zeigen Sie, dass die Quotientenkörperkonstruktion wirklich funktioniert. An welcher Stelle benötigen Sie welche Voraussetzungen?

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 8 vom 11. Dezember 2017

Aufgabe 1 (größter gemeinsamer Teiler)**.**

1. Gilt $\mathrm{ggT}(2017, 88) = \mathrm{ggT}(17, 8888)$ in $\mathbb{Z}$?
2. Gilt $\mathrm{ggT}(44, 88) = \mathrm{ggT}(444, 888)$ in $\mathbb{Z}$?
3. Gilt $\mathrm{ggT}(T^4 + T^3 + T + 1, T^4 + T^2 + 1) = T^2 + T + 1$ in $\mathbb{F}_2[T]$?
4. Gilt $\mathrm{ggT}(T^4 + T^3 + T + 1, T^4 + T^2 + 1) = -5 \cdot T^2 + 5 \cdot T - 5$ in $\mathbb{Q}[T]$?

Aufgabe 2 (Idealrechnerei)**.** Welche der folgenden Ideale sind gleich?

1. (12), $(3, 4)$, $(2, 6)$, $(2) \cap (6)$, $(3) \cap (4)$ in $\mathbb{Z}$.
2. $(T^3 + T^2)$, $(T + 1, T^2)$, $(T, T^2 + T)$, $(T) \cap (T^2 + T)$, $(T + 1) \cap (T^2)$ in $\mathbb{Q}[T]$.

Aufgabe 3 (Primideale, maximale Ideale)**.** Welche der folgenden Ideale sind prim? Welche maximal?

1. (4242) in $\mathbb{Z}$
2. $(T^2 + 2)$ in $\mathbb{Q}[T]$
3. $(T^2 + 1)$ in $\mathbb{F}_2(T)$
4. $(T^2 + 1)$ in $\mathbb{F}_2[T]$
5. $(2, T)$ in $\mathbb{Z}[T]$
6. (X, Y) in $\mathbb{Q}[X, Y]$
7. (X, Y) in $\mathbb{Z}[X, Y]$
8. $([0])$ in $\mathbb{Z}/(2018)$

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 2.1; orientieren Sie sich dabei an den folgenden Fragen:

1. Was sind die grundlegenden Begriffe der Ringtheorie?
2. Welche Beispiele für Ringe bzw. Konstruktionen von Ringen kennen Sie? Wozu verwendet man diese?
3. Was sind grundlegende Sätze und Beweismethoden?
4. Welche Parallelen zur Gruppentheorie können Sie entdecken?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen ...

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 9 vom 18. Dezember 2017

Aufgabe 1 (letzte Ziffern).

1. Bestimmen Sie die letzte Ziffer von 2017^{888} im Zehnersystem.
2. Bestimmen Sie die letzte Ziffer von 888^{2017} im Zehnersystem.
3. Bestimmen Sie die letzte Ziffer von 888^{2017} im Zwölfersystem.
4. Bestimmen Sie die letzte Ziffer von 2017^{2019} im Hexadezimalsystem.

Aufgabe 2 (modulare Gleichungen).

1. Bestimmen Sie ein multiplikatives Inverses zu $[5]$ in $\mathbb{Z}/(12)$.
2. Bestimmen Sie ein multiplikatives Inverses zu $T^2 + 1$ in $\mathbb{Q}[T]/(T + 1)$.
3. Bestimmen Sie alle $x \in \mathbb{Z}$ mit $x^7 \equiv 3 \mod 7$.
4. Bestimmen Sie alle $x \in \mathbb{Z}$ mit $x^9 \equiv 6 \mod 7$.

Aufgabe 3 (Primbewertungen). Berechnen Sie jeweils die folgenden Bewertungen zu den angegebenen Primelementen in den angegebenen Ringen:

- $\nu_3(\frac{42}{99})$ in $Q(\mathbb{Z})$ für $3 \in \mathbb{Z}$.
- $\nu_3(\frac{99}{42})$ in $Q(\mathbb{Z})$ für $3 \in \mathbb{Z}$.
- $\nu_3(3 \cdot T^3 + \frac{1}{3} \cdot T^2 - 7 \cdot T + 99)$ in $Q(\mathbb{Z})[T]$ für $3 \in \mathbb{Z}$.
- $\nu_T(3 \cdot T^3 + \frac{1}{3} \cdot T^2 - 7 \cdot T + 99)$ in $\mathbb{Z}[T]$ für $T \in \mathbb{Z}[T]$.

Aufgabe 4 (Wiederholung). Erstellen Sie eine Tabelle mit den wichtigsten Ringeigenschaften (als Zeilen) und den wichtigsten Beispielen von Ringen (als Spalten) und überlegen Sie bzw. schlagen Sie nach, welche Beispielringe welche Eigenschaften erfüllen.

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 10 vom 8. Januar 2018

Aufgabe 1 (Irreduzibilität, konkret)**.** Welche der folgenden Polynome sind irreduzibel?

1. $T^2 - 2$ in $\mathbb{F}_3[T]$
2. $T^3 + 2 \cdot T + 1$ in $\mathbb{Z}[T]$
3. $T^{2018} + 2017 \cdot T^{2017} - 2017 \in \mathbb{Z}[T]$
4. $5 \cdot T^3 + 555 \cdot T^2 - 555555 \cdot T + 2019 \in \mathbb{Z}[T]$
5. $\frac{1}{2} \cdot T^3 + 1 \in \mathbb{Q}[T]$

Aufgabe 2 (Irreduzibilität, abstrakt)**.** Welche der folgenden Aussagen sind wahr?

1. Jedes irreduzible Polynom in $\mathbb{Z}[T]$ ist auch irreduzibel in $\mathbb{Q}[T]$.
2. Jedes Polynom in $\mathbb{Z}[T]$, das in $\mathbb{Q}[T]$ irreduzibel ist, ist auch irreduzibel in $\mathbb{Z}[T]$.
3. Jedes irreduzible Polynom in $\mathbb{Q}[T]$ ist auch irreduzibel in $\mathbb{Q}(T)$.
4. Jedes Polynom in $\mathbb{Q}[T]$, das in $\mathbb{Q}(T)$ irreduzibel ist, ist auch in $\mathbb{Q}[T]$ irreduzibel.

Aufgabe 3 (Restklassenringe)**.** 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.
3. Ist $p \in \mathbb{Q}[X, Y]$ prim, so ist $\mathbb{Q}[X, Y]/(p)$ ein Körper.
4. Ist $p \in \mathbb{F}_2[T]$ prim, so ist $\mathbb{F}_2[T]/(p)$ isomorph zu $\mathbb{F}_2(T)$.

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 2.2; orientieren Sie sich dabei an den folgenden Fragen:

1. Was bedeutet „prim“ und „irreduzibel“? Was sind Primideale, maximale Ideale? Warum sind diese Begriffe so definiert, wie sie definiert sind?
2. Welche Beispiele für Primelemente, irreduzible Elemente, Primideale, maximale Ideale kennen Sie? Wozu verwendet man diese?
3. Was sind grundlegende Sätze und Beweismethoden?
4. Wie kann man testen, ob Polynome irreduzibel sind? Wie kann man testen, ob Ideale prim bzw. maximal sind?
5. Was besagt der kleine Satz von Fermat? Wozu verwendet man ihn?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen ...

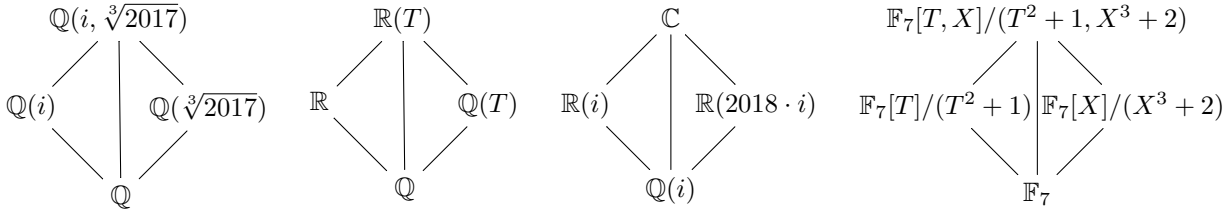
---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 11 vom 15. Januar 2018

Aufgabe 1 (Grade)**.** Bestimmen Sie zu jeder der folgenden Körpererweiterungen den Grad:



Aufgabe 2 (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 $1, \alpha, \alpha^2, \alpha^3, \alpha^4$:

1. α^5
2. α^6
3. $1/\alpha$
4. Gilt $\alpha^4 = 42 \cdot \alpha^3 - 2018$?

Aufgabe 3 (Minimalpolynome)**.** Bestimmen Sie für die folgenden komplexen Zahlen das Minimalpolynom über den angegebenen Grundkörpern:

1. von $\sqrt{2018}$ über $\mathbb{Q}$ bzw. $\mathbb{Q}(\sqrt[3]{2017})$
2. von $i \cdot \sqrt{2018}$ über $\mathbb{Q}$ bzw. $\mathbb{R}$ bzw. $\mathbb{Q}(i)$
3. von $1 + \sqrt{2}$ über $\mathbb{Q}$
4. von $\sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$
5. von $1/2 \cdot (1 + \sqrt{5})$ über $\mathbb{Q}$

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 3.1; orientieren Sie sich dabei an den folgenden Fragen:

1. Was sind die grundlegenden Begriffe der Körpertheorie?
2. Welche Beispiele für Körper bzw. Konstruktionen von Körpern kennen Sie? Wozu verwendet man diese?
3. Wie gehen die Erkenntnisse aus der Gruppen- und Ringtheorie dabei ein?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen ...

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 12 vom 22. Januar 2018

Aufgabe 1 (algebraische Erweiterungen)**.** Welche der folgenden Körpererweiterungen (in $\mathbb{C} \mid \mathbb{Q}$ bzw. $\mathbb{C}(T) \mid \mathbb{Q}$) sind algebraisch?

$$\mathbb{Q}(\zeta_{2020}) \mid \mathbb{Q}(i), \qquad \mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}(\sqrt{3}), \qquad \mathbb{C}(T) \mid \mathbb{Q}, \qquad \mathbb{C}(T) \mid \mathbb{R}(T).$$

Aufgabe 2 (Zerfällungskörper)**.**

1. Ist $\mathbb{Q}(\sqrt[2018]{2017}) \subset \mathbb{C}$ ein Zerfällungskörper von $T^{2018} - 2017$ über $\mathbb{Q}$?
2. Ist $\mathbb{Q}(\zeta_2) \subset \mathbb{C}$ ein Zerfällungskörper von $T^4 - 1$ über $\mathbb{Q}$?
3. Ist $\mathbb{Q}(\zeta_4) \subset \mathbb{C}$ ein Zerfällungskörper von $T^2 - 1$ über $\mathbb{Q}$?
4. Ist $\mathbb{Q}(\zeta_3, \zeta_6) \subset \mathbb{C}$ ein Zerfällungskörper von $(T^3 - 1) \cdot (T^6 - 1)$ über $\mathbb{Q}$?
5. Ist $\mathbb{Q}(\zeta_6) \subset \mathbb{C}$ ein Zerfällungskörper von $(T^3 - 1) \cdot (T^6 - 1)$ über $\mathbb{Q}$?
6. Ist $\mathbb{R}(\zeta_3) \subset \mathbb{C}$ ein Zerfällungskörper von $T^3 - 2$ über $\mathbb{R}$?
7. Ist $\mathbb{F}_3[T]/(T^2 + 1)$ ein Zerfällungskörper von $T^2 + 1$ über $\mathbb{F}_3$?
8. Ist $\mathbb{F}_7$ ein Zerfällungskörper von $T^3 - 1$ über $\mathbb{F}_7$?

Aufgabe 3 (Konjugationsprinzip für algebraische Zahlen)**.** Wir betrachten den Zwischenkörper $K := \mathbb{Q}(\sqrt[5]{2018}, i, \zeta_5)$ von $\mathbb{C} \mid \mathbb{Q}$. Sei $\sigma \in \mathrm{Gal}(K, \mathbb{Q})$. Welche der folgenden Gleichungen sind möglich?

1. $\sigma(\sqrt[5]{2018}) = -i$
2. $\sigma(i) = -i$
3. $\sigma(\zeta_5) = -\zeta_5$
4. $\sigma(\zeta_5) = {\zeta_5}^4$

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 3.2; orientieren Sie sich dabei an den folgenden Fragen:

1. Was sind die grundlegenden Begriffe über Körpererweiterungen?
2. Welche Beispiele für Körpererweiterungen bzw. Konstruktionen von Körpererweiterungen kennen Sie? Wozu verwendet man diese? Was wissen Sie über die zugehörigen Galoisgruppen?
3. Was sind grundlegende Sätze und Beweismethoden?
4. Wie gehen die Erkenntnisse aus der Gruppen- und Ringtheorie dabei ein?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen ...

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 13 vom 29. Januar 2018

Aufgabe 1 (algebraischer Abschluss)**.**

1. Ist $\mathbb{Q}(i) \mid \mathbb{Q}$ ein algebraischer Abschluss von $\mathbb{Q}$?
2. Ist $\mathbb{R} \mid \mathbb{Q}$ ein algebraischer Abschluss von $\mathbb{Q}$?
3. Ist $\mathbb{Q}(i, \sqrt{2}) \mid \mathbb{Q}$ ein algebraischer Abschluss von $\mathbb{Q}$?
4. Ist $\mathbb{C} \mid \mathbb{Q}(i)$ ein algebraischer Abschluss von $\mathbb{Q}(i)$?
5. Ist $\mathbb{C}(T) \mid \mathbb{Q}(T)$ ein algebraischer Abschluss von $\mathbb{Q}(T)$?
6. Ist $\mathbb{C} \mid \mathbb{C}$ ein algebraischer Abschluss von $\mathbb{C}$?

Aufgabe 2 ($\mathbb{F}_4$)**.** Bestimmen Sie die Verknüpfungstabellen für Addition und Multiplikation auf $\mathbb{F}_4$.
Hinweis. Überlegen Sie sich zunächst eine geeignete Beschreibung der Elemente von $\mathbb{F}_4 \cong \mathbb{F}_2[T]/(T^2 + T + 1)$.

Aufgabe 3 ($\mathbb{F}_{16}$)**.** Beantworten Sie die folgenden Fragen mithilfe des Klassifikationssatzes für endliche Körper:

1. Wie kann man $\mathbb{F}_{16}$ aus $\mathbb{F}_2$ konstruieren?
2. Wie sieht der Frobeniusendomorphismus $\sigma\colon \mathbb{F}_{16} \longrightarrow \mathbb{F}_{16}$ in dieser Beschreibung aus?
3. Warum besitzt $\mathbb{F}_{16} \mid \mathbb{F}_2$ genau einen Zwischenkörper K mit $|K| = 4$?
4. Welche Potenzen von σ liegen in $\mathrm{Gal}(\mathbb{F}_{16}, K)$?
5. Warum besitzt $\mathbb{F}_8 \mid \mathbb{F}_2$ *keinen* Zwischenkörper K mit $|K| = 4$?

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 3.3; orientieren Sie sich dabei an den folgenden Fragen:

1. Welche Klassifikationsresultate gibt es für endliche Körper bzw. endliche Körpererweiterungen von endlichen Körpern?
2. Welche Konstruktionsprinzipien kennen Sie für endliche Körper?
3. Wie können Sie möglichst explizit mit endlichen Körpern rechnen?
4. Wie gehen die Erkenntnisse aus der Gruppen- und Ringtheorie dabei ein?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen ...

---

keine Abgabe!

Fingerübungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — Blatt 14 vom 5. Februar 2018

Aufgabe 1 (normal)**.** Welche der folgenden Körpererweiterungen (in $\mathbb{C} \mid \mathbb{Q}$) sind normal?

1. $\mathbb{Q}(\sqrt{2018}) \mid \mathbb{Q}$
2. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2018}) \mid \mathbb{Q}(\sqrt{2018})$
3. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2018}) \mid \mathbb{Q}(\sqrt[3]{2})$
4. $\mathbb{Q}(i \cdot \sqrt{2}) \mid \mathbb{Q}$
5. $\mathbb{Q}(i, \sqrt{2}) \mid \mathbb{Q}$

Aufgabe 2 (primitive Elemente)**.** Bestimmen Sie ein primitives Element für die Körpererweiterung $\mathbb{Q}(\zeta_3, \sqrt{2}) \mid \mathbb{Q}$.

Aufgabe 3 (Galoiskorrespondenz)**.** Sei $L \mid K$ eine endliche Galoiserweiterung mit $\mathrm{Gal}(L, K) \cong A_5$. Welche der folgenden Aussagen treffen zu?

1. Es gilt $[L : K] = 5$.
2. Es gibt einen Zwischenkörper M von $L \mid K$ mit $\mathrm{Gal}(L, M) \cong \mathbb{Z}/30$.
3. Es gibt einen Zwischenkörper M von $L \mid K$ mit $[M : K] = 2$.
4. Es gibt einen Zwischenkörper M von $L \mid K$ mit $|\mathrm{Gal}(L, M)| = 5$.

Aufgabe 4 (Wiederholung)**.** Schreiben Sie eine Übersicht/Zusammenfassung von Kapitel 3.4; orientieren Sie sich dabei an den folgenden Fragen:

1. Was besagt der Hauptsatz der Galoistheorie?
2. Wozu braucht man Normalität? Wozu braucht man Separabilität?
3. Wie beweist man den Hauptsatz der Galoistheorie?
4. Wie gehen die Erkenntnisse aus der Gruppen- und Ringtheorie dabei ein?

Alles, was Sie jetzt sicher beherrschen, müssen Sie nicht mühsam vor der Klausur unter Zeitdruck lernen …

---

keine Abgabe!

D
Allgemeine Hinweise

Algebra im WS 2017/18
Organisatorisches

Prof. Dr. C. Löh/D. Fauser/J. Witzig Oktober 2017

Homepage. Alle aktuellen Informationen zur Vorlesung, zu den Übungen, zu Sprechstunden, Literaturangaben, sowie die Übungsblätter finden Sie auf der Homepage zur Vorlesung bzw. in GRIPS:

http://www.mathematik.uni-regensburg.de/loeh/teaching/algebra_ws1718

https://elearning.uni-regensburg.de

Vorlesung. Die Vorlesung findet jeweils dienstags (10:15–12:00; H 31) und freitags (10:15–12:00; H 31) statt.

Es wird ein (Kurz)Skript zur Vorlesung geben, das eine Übersicht über die wichtigsten Themen der Vorlesung enthält. Dieses Skript wird jeweils auf den obigen Homepages aktualisiert. Beachten Sie bitte, dass dieses Skript keineswegs geeignet ist, den Besuch der Vorlesung, der Zentralübung oder der Übungen zu ersetzen!

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 10:00 Uhr in die entsprechenden Briefkästen in der Mathematik abzugeben.

Auf jedem Übungsblatt gibt es vier reguläre Aufgaben (je 4 Punkte) und herausforderndere Bonusaufgaben (je 4 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 an der Tafel zu präsentieren (andernfalls werden die Punkte aberkannt).

Die Übungen beginnen in der zweiten Vorlesungswoche; in diesen ersten Übungen wird Blatt 0 besprochen.

Zentralübung. Zusätzlich zur Vorlesung und den Übungen bietet die Zentralübung die Gelegenheit, Fragen zu stellen und den Stoff der Vorlesung zu wiederholen und zu vertiefen. Die Zentralübung findet voraussichtlich jeweils montags (12:15–14:00; H 32) statt und wird von Daniel Fauser und Johannes Witzig geleitet; die Zentralübung beginnt in der *ersten* Vorlesungswoche.

Außerdem werden wir auf der Homepage Fingerübungen anbieten, mit denen grundlegende Begriffe, Handgriffe und Rechentechniken eingeübt werden können. Diese Aufgaben werden nicht abgegeben bzw. korrigiert. Sie dürfen und sollen aber gerne in der Zentralübung Fragen dazu stellen, falls Sie mit diesen grundlegenden Aufgaben Schwierigkeiten haben.

Einteilung in die Übungsgruppen. Die Einteilung in die Übungsgruppen erfolgt über GRIPS:

https://elearning.uni-regensburg.de

Sie können sich bis Mittwoch, den 18. Oktober 2017, um 10:00 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.

Falls Sie noch keine Kennung des Rechenzentrums haben, wenden Sie sich bitte an Daniel Fauser oder Johannes Witzig.

Die endgültige Einteilung der Übungsgruppen wird spätestens am Freitag, den 20. April 2017, in GRIPS bekanntgegeben. Ein Wechsel in volle Übungsgruppen ist dann nur durch Tausch mit einem Tauschpartner möglich.

Bei Fragen zur Einteilung der Übungsgruppen und zum Übungsbetrieb wenden Sie sich bitte an Daniel Fauser (daniel.fauser@ur.de) oder Johannes Witzig (johannes.witzig@ur.de).

Leistungsnachweise. Diese Vorlesung kann wie in den einzelnen Modulkatalogen spezifiziert in die Studiengänge eingebracht werden.

- *Studienleistung*: Regelmäßige und aktive Teilnahme an den Übungen, mindestens 50% der (in den regulären Aufgaben) möglichen Punkte, mindestens einmal zufriedenstellend vorrechnen.
- *Prüfungsleistung (für den Leistungsnachweis zur Algebra)*: Zweistündige Klausur (s.u.). Die Modulnote ergibt sich wie im jeweiligen Modulkatalog angegeben.

Klausur. Die Klausur findet am Freitag, den 16.02.2018, von 9:00 bis 11:00 Uhr, statt. Die Wiederholungsklausur ist voraussichtlich am Ende der Semesterferien; der genaue Termin wird so bald wie möglich bekanntgegeben. 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 Algebra-Vorlesung.

Sie müssen sich in FlexNow für die Studienleistung und die Prüfungsleistung anmelden. Bitte informieren Sie sich frühzeitig. Wir werden rechtzeitig Einträge in FlexNow vorbereiten. Berücksichtigen Sie bitte auch (implizite) Fristen der entsprechenden Prüfungsordnungen bis wann (Wiederholungs-)Prüfungen abgelegt werden müssen.

Wichtige Informationen im Krankheitsfall finden Sie unter:

http://www.uni-regensburg.de/mathematik/fakultaet/studium/studierende-und-studienanfaenger/index.html

Hinweise für Wiederholer. Studenten, die bereits in einem vorangegangenen Semester die Klausurzulassung erhalten haben, aber im entsprechenden

Semester die Klausur nicht bestanden haben oder nicht an der Klausur teilgenommen haben, können mit dieser Zulassung auch an den oben genannten Klausurterminen teilnehmen. Informieren Sie sich rechtzeitig über den Stoffumfang dieser Vorlesung (z.B. über das Kurzskript). Außerdem kann es je nach Kenntnisstand sinnvoll sein, nochmal an den Übungen oder der Vorlesung teilzunehmen.

Für den Drittversuch besteht alternativ zur Klausur auch wahlweise die Möglichkeit, die Prüfung als mündliche Prüfung abzulegen.

Falls Sie an den Übungen teilnehmen möchten, ohne dass Ihre Lösungen korrigiert werden sollen, schreiben Sie bitte eine email an Daniel Fauser oder Johannes Witzig mit Ihren Wunschterminen (damit die Übungsgruppen einigermaßen gleichmäßig besucht sind).

Ansprechpartner.

- Bei Fragen zur Organisation des Übungsbetriebs wenden Sie sich bitte an Daniel Fauser oder Johannes Witzig (Büro M 205):

  daniel.fauser@ur.de
  johannes.witzig@ur.de

- Bei Fragen zu den Übungsaufgaben wenden Sie sich bitte an Ihren Übungsleiter oder an Daniel Fauser oder Johannes Witzig.
- Bei mathematischen Fragen zur Vorlesung wenden Sie sich bitte an Ihren Übungsleiter, an Daniel Fauser, Johannes Witzig oder an Clara Löh.
- Bei Fragen zur Planung Ihres Studiums bzw. zur Prüfungsordnung wenden Sie sich bitte an die zuständige Studienberatung oder das zuständige Prüfungsamt:

http://www.uni-regensburg.de/mathematik/fakultaet/studium/ansprechpersonen/index.html

Bei vielen Fragen kann Ihnen auch die Fachschaft weiterhelfen:

http://www-cgi.uni-regensburg.de/Studentisches/FS_MathePhysik/cmsms/

Algebra im WS 2017/18
Hinweise zur Prüfungsvorbereitung

Prof. Dr. C. Löh/D. Fauser/J. Witzig Oktober 2017

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.

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.

Erreichen dieses Ziels. Während der Vorlesungszeit:

- aktive Auseinandersetzung mit den Übungsaufgaben
- Erlernen des Fachwissens (Definitionen, Sätze), notfalls mit Karteikarten
- weiteres aktives Üben mit zusätzlichen Aufgaben und Vertiefung der Kenntnisse durch Selbststudium (Bibliothek!)
- Bei Fragen: Betreuungsangebote nutzen!

Kurz vor der Prüfung:

- Kann ich mein Wissen präzise und verständlich präsentieren? (Das kann man einfach an anderen Kommilitonen ausprobieren ...)
- Was könnten typische Prüfungsfragen sein? Was sind gute Lösungen zu diesen Fragen?
- Wie belastbar sind meine Fähigkeiten? Was muss ich noch verbessern?

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

Viel Erfolg bei der Prüfung!

Algebra im WS 2017/18
Hinweise zu den Übungsaufgaben

Prof. Dr. C. Löh/D. Fauser/J. Witzig Oktober 2017

Ziel der Übungsaufgaben. Ziel der Übungsaufgaben ist, sich aktiv mit den behandelten Definitionen, Sätzen, Beispielen und Beweistechniken auseinanderzusetzen und zu lernen, damit umzugehen.

Das Punkteminimum für die Klausurzulassung ist das *Minimum*. Sie sollten versuchen, möglichst viele Punkte zu erreichen und nicht nach Erreichen dieser Minimalzahl die Übungen schleifen lassen!

Wie bearbeitet man eine Übungsaufgabe?

- Beginnen Sie mit der Bearbeitung 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 alle auftretenden Begriffe? Verstehen Sie, was in den Aufgaben verlangt wird?
- Was sind die Voraussetzungen? Was ist zu zeigen? Wie könnten diese Dinge zusammenhängen? Gibt es Sätze 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?
- Versuchen Sie, das Problem in kleinere Teilprobleme aufzuteilen. Können Sie diese Teilprobleme lösen?
- Verwenden Sie viel Schmierpapier und geben Sie sich genug Zeit, an der Aufgabe herumzuexperimentieren! Selbst wenn Sie die Aufgabe nicht vollständig lösen, werden Sie auf diese Weise viel lernen, da Sie sich aktiv mit den Begriffen und Sätzen auseinandersetzen.
- Wenn Sie nicht weiterwissen, diskutieren Sie die Aufgabe mit Kommilitonen. Lassen Sie sich aber auf keinen Fall dazu verleiten, einfach Lösungen irgendwo abzuschreiben oder ausschließlich in Gruppen zu arbeiten. Mathematik kann man nur lernen, wenn man aktiv damit arbeitet und seine Gedanken selbst formuliert!

Wie schreibt man eine Lösung auf?

- Gliedern Sie Ihre Lösung sauber in Voraussetzung, Behauptung und Beweis.

- Teilen Sie Ihre Beweise in sinnvolle Zwischenschritte auf.
- 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.

Bewertungskriterien. Bei der Bewertung der abgegebenen Lösungen wird auf folgendes geachtet:

- Wurde die gestellte Aufgabe vollständig gelöst?
- Wurden Voraussetzung, Behauptung, Beweis deutlich 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?

Viel Erfolg und viel Spass bei den Übungen!

Literaturverzeichnis

Bitte beachten Sie, dass das Literaturverzeichnis im Laufe der Vorlesung wachsen wird und sich daher auch die Nummern der Quellen ändern werden!

[1] Manindra Agrawal, Neeraj Kayal, Nitin Saxena. PRIMES is in P, *Ann. of Math. (2)*, 160(2), pp. 781–793, 2004. Zitiert auf Seite: 94

[2] Martin Aigner, Günter M. Ziegler, *Proofs from The Book*, dritte Auflage, Springer, 2004. Zitiert auf Seite: 87

[3] W.R. Alford, Andrew Granville, Carl Pomerance. There are infinitely many Carmichael numbers, *Ann. of Math. (2)*, 139(3), pp. 703–722, 1994. Zitiert auf Seite: 94

[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. Zitiert auf Seite: 54

[5] ATLAS of finite group representations, version 3. http://brauer.maths.qmul.ac.uk/Atlas/v3/ Zitiert auf Seite: 54

[6] Martin Brandenburg. *Einführung in die Kategorientheorie: Mit ausführlichen Erklärungen und zahlreichen Beispielen*, Springer Spektrum, 2015. Zitiert auf Seite: A.7

[7] Siegfried Bosch. *Algebra*, sechste Auflage, Springer Spektrum, 2006. Zitiert auf Seite: 92, 109, 114, 138, 168, 177

[8] Kenneth S. Brown. *Cohomology of Groups*, Graduate Texts in Mathematics, 87, Springer, 1982. Zitiert auf Seite: 34

[9] Daniel Bump. *Lie Groups*, Graduate Texts in Mathematics, 225, zweite Auflage, Springer, 2013. Zitiert auf Seite: 68

[10] Brian Conrad. Impossibility theorems for elementary integration, http://www2.maths.ox.ac.uk/cmi/library/academy/LectureNotes05/Conrad.pdf Zitiert auf Seite: 172

[11] The Coq Proof Assistant. https://coq.inria.fr/ Zitiert auf Seite: A.3

[12] David A. Cox. *Galois Theory*, Wiley, 2004. Zitiert auf Seite: 179

[13] A. Crans, T. Fiore, R. Satyendra. Musical Actions of Dihedral Groups, *American Mathematical Monthly* 116(6), S. 479–495, 2009. Zitiert auf Seite: 37

[14] David M. Evans, Zaniar Ghadernezhad, Katrin Tent. Simplicity of the automorphism groups of some Hrushovski constructions, *Ann. Pure Appl. Logic* 167(1), S. 22–48, 2016. Zitiert auf Seite: 54

[15] Walter Feit, John G. Thompson. A solvability criterion for finite groups and some consequences, *Proc. Nat. Acad. Sci. U.S.A.* 48, S. 968–970, 1962. Zitiert auf Seite: 59

[16] Eberhard Freitag, Rolf Busam. *Funktionentheorie 1*, vierte Auflage, Springer, 2006. Zitiert auf Seite: 87

[17] Georges Gonthier, Andrea Asperti, Jeremy Avigad et al.. A machine-checked proof of the odd order theorem, *Interactive theorem proving*, S. 163179, *Lecture Notes in Comput. Sci.* 7998, Springer, 2013. Zitiert auf Seite: 59

[18] Isabelle, https://www.cl.cam.ac.uk/research/hvg/Isabelle/ Zitiert auf Seite: 7, A.3

[19] K. Jänich. *Lineare Algebra*, 11. Auflage, Springer, 2013. Zitiert auf Seite: 50

[20] Clara Löh. *Geometric Group Theory. An Introduction*, book draft, 2017.
http://www.mathematik.uni-r.de/loeh/ggt_book/ggt_book_draft.pdf
Universitext, Springer, 2018. Zitiert auf Seite: 20, 29, 35, A.12

[21] Clara Löh. *Algebraische Topologie I*, Kurzskript zur Vorlesung, 2014.
http://www.mathematik.uni-r.de/loeh/teaching/topologie1_ws1516/lecture_notes.pdf
Zitiert auf Seite: 159

[22] Clara Löh. *Geometrie*, Vorlesungsskript, 2015.
http://www.mathematik.uni-r.de/loeh/teaching/geometrie_ss15/lecture_notes.pdf
Zitiert auf Seite: 11, 173

[23] Falko Lorenz. *Einführung in die Algebra I*, dritte Auflage, Spektrum Akademischer Verlag, 1996. Zitiert auf Seite: 68

[24] Saunders MacLane. *Categories for the Working Mathematician*, zweite Auflage, Springer, 1998. Zitiert auf Seite: A.7

[25] Ronald L. Rivest, Adi Shamir, Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2), pp. 120–126, 1978. Zitiert auf Seite: 95, 97

[26] Maxwell Rosenlicht. Integration in finite terms, *The American Mathematical Monthly*. 79(9), pp. 963–972, 1972. Zitiert auf Seite: 172

[27] Joseph J. Rotman. *An Introduction to the Theory of Groups*, Graduate Texts in Mathematics, 148, vierte Auflage, Springer, 1995. Zitiert auf Seite: 20, 53, 56

[28] Michael Spivak. *Calculus*, dritte Auflage, Cambridge University Press, 2006. Zitiert auf Seite: 121

[29] Simon Singh. *Fermat's Last Theorem: The Story Of A Riddle That Confounded The World's Greatest Minds For 358 Years*, Walker & Co, 1997. Zitiert auf Seite: 97

[30] Lawrence C. Washington. *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, 83, Springer, 1982 Zitiert auf Seite: 165

Symbolverzeichnis

Symbole

(A)	von A erzeugtes Ideal, 78
$\lvert \cdot \rvert$	Mächtigkeit,
$\cap$	Durchschnitt von Mengen,
$\cup$	Vereinigung von Mengen,
$\sqcup$	disjunkte Vereinigung von Mengen,
$\subset$	Teilmengenrelation (Gleichheit ist erlaubt),
$\cong$	isomorph (Gruppen), 9
$<$	ist Untergruppe von, 13
$\lhd$	ist Normalteiler in, 21
$\times$	kartesisches Produkt,
$\rtimes$	semi-direktes Produkt,

A

Ab	Kategorie der abelschen Gruppen, A.8
Alg_K	Kategorie der K-Algebren, A.9
A_n	alternierende Gruppe, 22
Aut	Automorphismengruppe, 12
Aut_K	Automorphismengruppe, 11

C

$\mathbb{C}$	Menge der komplexen Zahlen,
$\mathrm{Cay}(G, S)$	Cayleygraph von G bezüglich S, 20
c_g	Konjugationsabbildung zu g, 12
char	Charakteristik eines Körpers, 112

D

D	formale Ableitung von Polynomen, 142
D_n	Diedergruppe, 32

E

e	neutrales Element, 7

F

$\mathbb{F}_p$	der Körper $\mathbb{Z}/(p)$, 90
$\mathbb{F}_{p^k}$	„der“ endliche Körper mit p^k Elementen, 142

G

g^{-1}	inverses Element zu g, 6
$[G : H]$	Index von H in G, 15
Gal	Galoisgruppe, 12, 120
ggT	größter gemeinsamer Teiler, 84
G/H	Menge der Linksnebenklassen von H in G, 16
$g \cdot H$	Linksnebenklasse, 15
GL_n	allgemeine lineare Gruppe, 11
Group	Kategorie der Gruppen, A.8
$G \setminus X$	Bahnenraum, 40
$G \cdot x$	Orbit von x, 40
G_x	Standgruppe von x, 40

I

id	Identitätsmorphismus, A.7
Im	Imaginärteil,
im f	Bild von f, 9
Isom	Isometriegruppe, 11

K

$K(S)$	von $S \subset L$ erzeugter Zwischenkörper von $L \mid K$, 116
$K(T)$	rationaler Funktionenkörper über K, 77
$\ker f$	Kern von f, 9
kgV	kleinstes gemeinsames Vielfaches, 85

L

$[L : K]$	Grad von $L \mid K$, 117
$L \mid K$	Körperweiterung L über K, 114

M

$M \cdot N$	Kompositum von M und N in $L \mid K$, 116
Mod_R	Kategorie der (Links-)R-Moduln, A.9
Mor_C	Morphismen in der Kategorie C, A.7

N

$\mathbb{N}$	Menge der natürlichen Zahlen: $\{0, 1, 2, \dots\}$,
$\nu_p(x)$	Vielfachheit von p in x, 97, 100

O

Ob	Klasse der Objekte einer Kategorie, A.7
$\mathrm{O}(n)$	orthogonale Gruppe, 12
ord	Ordnung, 25

P

ϕ	eulersche φ-Funktion, 94
Φ_n	n-tes Kreisteilungspolynom über $\mathbb{Q}$, 162
Φ_n	das n-te Kreisteilungspolynom, 125
$\prod$	Produkt,

Q

$\mathbb{Q}$	Menge der rationalen Zahlen,
$Q(R)$	Quotientenkörper, 76

R

$\mathbb{R}$	Menge der reellen Zahlen,
R/a	Restklassenring von R modulo a, 78

$R[T]$ Polynomring über R, 73
Re Realteil,
Ring Kategorie der Ringe, A.9

S

S^1 der Einheitskreis in $\mathbb{C}$, 24
Set Kategorie der Mengen, A.8
$\langle S \rangle_G$ von S erzeugte Untergruppe in G, 18
sgn Signumsabbildung, 22
SL_n spezielle lineare Gruppe, 11
S_n symmetrische Gruppe von $\{1, \ldots, n\}$, 8
Subext(L, K) Menge der Zwischenkörper von $L \mid K$, 157
Subgroup(G) Menge der Untergruppen von G, 157
S_X symmetrische Gruppe von X, 8

T

Top Kategorie der topologischen Räume, A.9

V

Vect_K Kategorie der K-Vektorräume, A.8

X

X^g Fixpunktmenge von g, 40

Z

$\mathbb{Z}$ Menge der ganzen Zahlen,
$Z(G)$ Zentrum von G, 44
$Z_G(g)$ Zentralisator von g in G, 44
ZL Menge der konstruierbaren Punkte, 173
ZL_i elementare Konstruktionsschritte mit Zirkel und Lineal, 172

Index

Symbole

14/15-Puzzle, 2, 51

A

Abelianisierung, 56
    universelle Eigenschaft, 56
abelsche Erweiterung, 165
abelsche Gruppe, 6
    Klassifikation endlicher, 46
Ableitung, 142
Ableitungskriterium, 142
adjungierte Funktoren, A.26
Adjunktion, 116
affine Gerade, 18
affiner Unterraum, 18
Algebra
    Anwendungen, 2
    warum?, 1
algebraisch, 121
algebraisch abgeschlossen, 136
algebraische Geometrie, 81
algebraische Körpererweiterung, 127
algebraischer Abschluss, 136
    von endlichen Körper, 143
Algorithmus
    euklidischer, A.22
allgemeine lineare Gruppe, 11
alternierende Gruppe, 22, 50
    Einfachheit, 53
    Erzeugendensystem, 51
arithmetic overflow, 80
assoziiert, 82
auflösbar
    durch Radikale, 166
auflösbare Gruppe, 57
    p-Gruppe, 61
Auflösung durch Radikale, 2
auflösbare Gruppe, 59
Automorphismengruppe, 12
    in einer Kategorie, A.10
    in Kategorien, 12
Automorphismus
    innerer, 12
    von Gruppen, 12

B

Bahn, 40
Bahnengleichung, 41
Bahnenraum, 40
Beweis
    formalisiert/verifiziert, 7, A.3
Bewertungstest, 101
Bibliothek, 4
Bild, 9

byte, 145

C

Carmichael-Zahl, 94
Cauchy
    Satz von, 62
Cayley
    Satz von, 39
Cayleygraph, 20
Charakteristik, 112
Chinesischer Restsatz, 91

D

darstellbarer Funktor, A.27
Determinante, 25
Diedergruppe, 31
    Musik, 37
Distributivitätsgesetz, 70
Division mit Rest, A.19
Duelle, 154

E

einfache Gruppe, 53
    alternierende Gruppe, 53
Einheit, 82
Einheitengruppe, 82, 113
Einheitswurzel, 124, 162
    primitiv, 124
    primitive, 168
Eisensteinsches Irreduzibilitätskriterium, 109
elementare Zahlentheorie, 80
endlich erzeugt
    Gruppe, 19
endlich erzeugte Körpererweiterung, 118
endliche Körper, 90
endliche Körpererweiterung, 117
endlicher Körper, 140
    Einheitengruppe, 114
    Klassifikation, 140
    Körpererweiterungen, 143
erster Isomorphiesatz, 27
Erzeugendensystem
    frei, A.11
    von Gruppen, 18
erzeugte Untergruppe, 18
    explizite Beschreibung, 19
erzeugter Zwischenkörper, 115
euklidische
    Isometriegruppe, 33
euklidische Gradfunktion, A.19
euklidischer Algorithmus, A.22
euklidischer Ring, A.19
eulersche ϕ-Funktion, 94

F

Faktoren
    einer Normalreihe, 58
faktorieller Ring, 97
Feit-Thompson Theorem, 59
Fermat
    großer Satz, 97
    kleiner Satz, 92, 95
Fixkörper, 155
Fixpunktmenge, 40
formale Ableitung, 142
formalisierter Beweis, 7, A.3
freie Gruppe, A.11
freie Gruppenoperation, 38
freies Erzeugendensystem, A.11
Frobeniusendomorphismus, 140
Fundamentalsatz der Algebra, 179
Funktionenkörper, 77
Funktor, A.25
    adjungiert, A.26
    darstellbar, A.27
    Dualraum, A.27
    erhält Isomorphie, A.28
    Identitätsfunktor, A.25
    kontravariant, A.27
    kovariant, A.25
    Tensorprodukt, A.26
    Vergissfunktor, A.25

G

Galois, 154
Galoiserweiterung, 148, 154
    Fixkörper, 156
    Grad, 154

Galoisgruppe, 12, 120
einer Gleichung, 136
Fixkörper, 156
Größe, 154
induktive Berechnung, 161
Realisierung als, 156
Galoistheorie
Hauptsatz, 157
kategoriell, 159
Gauß
Lemma von, 101
Satz von, 100
Gaußsche ganze Zahlen, 71
Geometrische Gruppentheorie, 20
Gerade
affin, 18
ggT, 84, A.23
Grad einer Körpererweiterung, 117
Gradfunktion
euklidische, A.19
großer Satz von Fermat, 97
größter gemeinsamer Teiler, 84, 99, A.23
Gruppe, 5, 6
Abelianisierung, 56
abelsch, 6
allgemeine lineare, 11
als Automorphismengruppe, 12
als Kategorie, A.8
alternierende, 22
auflösbar, 57, 59
Cayleygraph, 20
Dieder-, 31
einfach, 53
endlich erzeugt, 19
Erzeugendensystem, 18
frei, A.11
Galois-, 12
inverses Element, 6
Isometrie-, 11
Kommutator, 55
Koprodukt, 29
neutrales Element, 6
Normalisator, 67
Normalreihe, 58
Normalteiler, 21
orthogonale, 11
p-Gruppe, 60
Produkt, 28
Quaternionen, 62
Quotientengruppe, 22
semi-direktes Produkt, 30
spezielle lineare, 11
Sylowgruppe, 60
symmetrische, 8
triviale, 10
Unter-, 13
Wortproblem, 20
Zentralisator, 44
Zentrum, 44
zyklisch, 19, 26
Gruppenautomorphismus, 12
Gruppenelement
Konjugationsklasse, 45
Ordnung, 25
Gruppenerweiterung, 34, 52
semi-direktes Produkt, 34
Gruppenhomomorphismus, 8
Gruppenisomorphismus, 9, 10
Gruppenkohomologie, 34
Gruppenoperation, 35
Bahn, 40
Bahnengleichung, 41
Bahnenraum, 40
explizit, 36
Fixpunktmenge, 40
freie, 38
in der Musik, 37
Isotropiegruppe, 40
Klassengleichung, 45
Konjugationsoperation, 44
Linkstranslation, 36, 39
Orbit, 40
Orbitraum, 40
Rotationsoperation, 38
Rubik's Cube, 38
Stabilisator, 40
Standgruppe, 40
transitive, 38
trivial, 36

Zählproblem, 43

H

Hauptideal, 83
Hauptidealring, 83
Hauptsatz der Galoistheorie, 157
Homomorphiesatz, 24
für Ringe, 81

I

Ideal, 77
erzeugt von, 78
Hauptideal, 83
koprim, 91
maximal, 88
prim, 88
Identitätsfunktor, A.25
Identitätsmorphismus, A.7
Index
Ideal in Körpern, 78
innerer Automorphismus, 12
int, 80
Integritätsring, 72
inverses Element
Gruppe, 6
irreduzibel, 85, 106
Irreduzibilitätskriterien, 106
Isabelle, A.3
Isometriegruppe, 11
euklidische, 33
isomorph
Gruppentheorie, 9
Isomorphiesätze
für Ringe, 81
Isomorphiesatz, 27
Isomorphismus
in einer Kategorie, A.10
Isotropiegruppe, 40

K

Körper
endlich, 90
kanonische Projektion, 23
Kaplansky-Vermutung, 72
Kategorie, A.7
der Algebren, A.9
der Gruppen, 6, A.8
der Körpererweiterungen, 119
der Mengen, A.8
der Moduln, A.9
der Ringe, A.9
der topologischen Räume, A.9
der Vektorräume, A.8
leere, A.8
Morphismus, A.7
Objekt, A.7
Kern, 9
kgV, 85
Klassengleichung, 45
Klassifikation
zyklischer Gruppen, 26
kleiner Satz von Fermat, 92, 95
kleinstes gemeinsames Vielfaches, 84, 99
Kommutator, 55
Kommutatoruntergruppe, 55
komplexe Zahlen, 106
Kompositum, 115
Konjugationsabbildung, 12
Konjugationsklasse, 45
Konjugationsoperation, 44
Konjugationsprinzip, 125
konjugierte Nullstellen, 125
Konstruierbarkeit, 172
Konstruierbarkeit mit Zirkel und Lineal, 1
kontravarianter Funktor, A.27
koprim, 91
Koprodukt
von Gruppen, 29
Körper, 112
algebraisch abgeschlossen, 136
Charakteristik, 112
Einheitengruppe, 113
endliche, 140
Fixkörper, 155
Funktionenkörper, 77
Kompositum, 115
Kreisteilungskörper, 162
perfekt, 151

Primkörper, 112
Quotientenkörper, 76
Zerfällungskörper, 130
Körpererweiterung, 114
abelsche, 165
algebraisch, 127
endlich erzeugt, 118
endliche, 117
erzeugter Zwischenkörper, 115
Galoiserweiterung, 154
Galoisgruppe, 120
Grad, 117
Kategorie, 119
Kompositum, 115
Morphismen von, 119
normal, 148
separabel, 150
transzendent, 127
unendliche, 117
von endlichen Körpern, 143
Wurzelerweiterung, 166
Zwischenkörper, 114
zyklische, 169
Körperhomomorphismus, 112, 113
kovarianter Funktor, A.25
Kreisteilungskörper, 162
Kreisteilungspolynom, 125, 162

L

Länge
eines Zykels, 49
Lagrange
Satz von, 16, 17, 26
Standard-Argumente, 27
leere Kategorie, A.8
LFSR, 144
Lineal, 172
linear feedback shift register, 144
Linksnebenklasse, 15
Linkstranslationsoperation, 36, 39

M

maximales Ideal, 88
mehrfache Nullstelle, 142
Minimalpolynom, 122
Mitternachtsformel, 166
Morphismus, A.7
Morphismus von Körpererweiterungen, 119

N

neutrales Element
Gruppe, 6
noetherscher Ring, 98
normale Hülle, 170
normale Körpererweiterung, 148
Normalisator, 67
Normalreihe, 58
Normalteiler, 21
normiertes Polynom, 101
Nullring, 71
Nullstelle
konjugiert, 125
mehrfache, 142

O

Orbit, 40
Orbitraum, 40
Ordnung, 25
Satz von Lagrange, 26, 27
orthogonale Gruppe, 11

P

perfekter Körper, 151
Perlenketten, 43
p-Gruppe, 60
auflösbar, 61
Polynom
Auflösbarkeit, 166
irreduzibles, 106
Kreisteilungspolynom, 125, 162
normiertes, 101
primitives, 103
separables, 150
Polynomdivision, A.20
polynomiale Gleichung
Auflösbarkeit, 136, 166
Polynomring, 73, 138
als euklidischer Ring, A.19
universelle Eigenschaft, 75

prim, 82, 85
Primfaktorzerlegung, 98
Primideal, 88
primitive Einheitswurzel, 124, 168
primitives Element, 152
primitives Polynom, 103
Primkörper, 112
Primzahl
    2017, 87
    unendlich viele, 87
    Verteilung, 87
Primzahlsatz, 87
Primzahltest, 94
    probabilistischer, 94
probabilistischer Primzahltest, 94
Produkt
    universelle Eigenschaft, 29
    von Gruppen, 28
Produktring, 72
proof assistant, 7, A.3
Pseudozufallszahlen, 145
public key cryptography, 95

Q

Quaternionengruppe, 62
Quotientengruppe, 22
    universelle Eigenschaft, 23
Quotientenkörper, 76
    universelle Eigenschaft, 77

R

Radikal
    Auflösbarkeit, 166
RAID(6), 145
rationaler Funktionenkörper, 77
Rechenschieber, 10
Rechtsnebenklasse, 16
Reduktionskriterium, 107
Referenzen zur LA, 4
Restklassenkörper, 90
Restklassenring, 78
    universelle Eigenschaft, 80
Ring, 70
    Einheit, 82
    Einheitengruppe, 82
    euklidisch, A.19
    faktoriell, 97
    Gaußsche ganze Zahlen, 71
    ggT, 84
    Hauptidealring, 83
    Homomorphismus, 71
    Ideal, 77
    Integritätsring, 72
    Isomorphismus, 71
    kgV, 84
    noethersch, 98
    Nullring, 71
    Polynomring, 73
    Produktring, 72
    Restklassenring, 78
    Teilbarkeit, 82
Ringhomomorphismus, 71
Ringisomorphismus, 71
Rotationsoperation, 38
RSA, 95
Rubik's Cube, 38

S

Satz
    Ableitungskriterium, 142
    Bahnengleichung, 41
    Chinesischer Restsatz, 91
    Eisensteinsches Irreduzibilitätskriterium, 109
    Feit-Thompson, 59
    Fundamentalsatz der Algebra, 179
    großer Satz von Fermat, 97
    Hauptsatz der Galoistheorie, 157
    Homomorphiesatz, 24
    Isomorphiesatz, 27
    Klassengleichung, 45
    Klassifikation endlicher abelscher Gruppen, 46
    Klassifikation endlicher Körper, 140
    kleiner Satz von Fermat, 92, 95
    Lemma von Gauß, 101

Primzahlsatz, 87
Reduktionskriterium, 107
Sylowsätze, 62, A.15
vom primitiven Element, 152
von Cauchy, 62
von Cayley, 39
von Gauß, 100
von Lagrange, 16
Satz von Lagrange
für endliche Gruppen, 17
für Ordnungen, 26
Standard-Argumente, 27
seed, 145
semi-direktes Produkt, 30, 33
separabel, 150
Signum, 25, 50
Spalt, 30
spezielle lineare Gruppe, 11
Stabilisator, 40
Standard-Argument
Klassifikation endlicher abelscher Gruppen, 48
Satz von Lagrange, 27
Standgruppe, 40
Sylowgruppe, 60
Sylowsätze, 62, A.15
symmetrische Gruppe, 8, 11
Erzeugendensystem, 49
Signum, 50
Zykel, 48
Zykelzerlegung, 49

T

Teilbarkeit, 82
teilt, 82
Träger
eines Zykels, 49
transitive Gruppenoperation, 38
transzendent, 121
transzendente Körpererweiterung, 127
triviale Gruppe, 10
triviale Gruppenoperation, 36
triviale Untergruppe, 14

U

Überlagerungstheorie, 159
unendliche Körpererweiterung, 117
universelle Eigenschaft
Abelianisierung, 56
Polynomring, 75
Produkt, 29
Quotientengruppe, 23
Quotientenkörper, 77
Restklassenring, 80
Untergruppe, 13
erzeugte, 18
normal, 21
Sylowgruppe, 60
triviale, 14
Unterraum
affin, 18

V

Vergissfunktor, A.25
verifizierter Beweis, 7, A.3
Verknüpfung, 6
Verknüpfungstabelle, 8
Verschlüsselung, 95
vollkommener Körper, 151
Vorlesung
Überblick, 2

W

warum Algebra?, 1
Wortproblem, 20
Wurzel, 121
Wurzelerweiterung, 166

Z

Zählproblem, 43
Zahlentheorie, 80
Zauberwürfel, 38
Zentralisator, 44
Zentrum, 44
Zerfällungskörper, 130
Zirkel, 172
zweiter Isomorphiesatz, 27
Zwischenkörper, 114

erzeugter Zwischenkörper, 115
Zykel, 48
Länge, 49
Träger, 49
Zykelzerlegung, 49
zyklische Erweiterung, 169
zyklische Gruppe, 19, 26