Volker Diekert, Manfred Kufleitner, Gerhard Rosenberger
Diskrete algebraische Methoden
De Gruyter Studium

Volker Diekert, Manfred Kufleitner,
Gerhard Rosenberger

Diskrete algebraische Methoden

Arithmetik, Kryptographie, Automaten und Gruppen

DE GRUYTER

Mathematics Subject Classification 2010
11-01, 11Y11, 12-01, 14H52, 20E06, 20M05, 20M35, 68Q45, 68Q70, 68R15, 94A60

Autoren
Volker Diekert
Universität Stuttgart
Institut für Formale Methoden der Informatik (FMI)
Abteilung Theoretische Informatik
Universitätsstraße 38
70569 Stuttgart
volker.diekert@fmi.uni-stuttgart.de

Manfred Kufleitner
Universität Stuttgart
Institut für Formale Methoden der Informatik (FMI)
Abteilung Theoretische Informatik
Universitätsstraße 38
70569 Stuttgart
manfred.kufleitner@fmi.uni-stuttgart.de

Gerhard Rosenberger
Universität Hamburg
Fachbereich Mathematik
Bereich AZ
Bundesstraße 55 (Geomatikum)
20146 Hamburg
gerhard.rosenberger@math.uni-hamburg.de

Gerhard Rosenberger
Universität Passau
Fakultät für Informatik und Mathematik
Innstraße 33
94032 Passau
rosenber@fim.uni-passau.de

ISBN 978-3-11-031260-7
e-ISBN 978-3-11-031261-4

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Satz: le-tex publishing services GmbH, Leipzig
Druck und Bindung: Hubert & Co.GmbH & Co. KG, Göttingen
♾ Gedruckt auf säurefreiem Papier
Printed in Germany

www.degruyter.com

Vorwort

Über den Inhalt. Dieses Buch basiert auf verschiedenen Vorlesungen, die an den Universitäten Stuttgart und Dortmund über viele Jahre hinweg von den Autoren erfolgreich gehalten wurden. Hieraus entstanden die beiden Bücher *Elemente der diskreten Mathematik* [23] und das vorliegende Buch *Algebraische Methoden der diskreten Mathematik*. Unser erster Band [23] wendet sich an einen Leserkreis ohne spezifische Vorkenntnisse. Bei dem vorliegenden Buch über algebraische Methoden wird durch den Titel ein veränderter Fokus klar. Zunächst ist es keine Fortsetzung von [23], sondern ein unabhängiges Buch. Es wendet sich weniger an Studierende im Grundstudium, sondern an Leser mit fortgeschrittenen Kenntnissen in Mathematik, wie man sie im Hauptstudium (oder bei Masterstudenten) in Mathematik oder Informatik voraussetzen kann. Die Zielgruppe umfasst auch Doktoranden und Dozenten, die sich auf einem modernen Gebiet zwischen Mathematik und Informatik fortbilden möchten.

Bei der Stoffauswahl spielte natürlich die persönliche Neigung der Autoren eine Rolle. Wir beginnen mit einem allgemeinen Kapitel *Algebraische Strukturen*, welches die Grundlage für das gesamte Buch bereitstellt. In der tabellarischen Zusammenfassung kann der Leser erkennen, welche Tatsachen er bereits kennt, auffrischen oder neu lernen kann. Die folgenden Kapitel können prinzipiell unabhängig voneinander gelesen werden, aber es gibt bewusst diverse Querbezüge. So ist der Bezug vom Kapitel *Kryptographie* zu den später behandelten kryptographischen Verfahren bei elliptischen Kurven gewollt und offensichtlich.

In gewisser Weise ist *algebraische Kryptographie* ein Leitmotiv. Kryptographie ist in der Internetgesellschaft des einundzwanzigsten Jahrhunderts allgegenwärtig. Die Vermittlung von Grundkenntnissen in Kryptographie sollte selbstverständlicher Standard jeder Mathematik- und Informatikausbildung sein. Für uns stehen asymmetrische kryptographische Verfahren im Vordergrund. Auch deshalb, weil sie häufig mathematisch spannender sind als rein auf *Performance* ausgerichtete symmetrische Verfahren. Wir behandeln auch Shamirs Angriff auf das Merkle-Hellman-Verfahren. Dieser Angriff ist ein mathematisches Glanzstück! Das Merkle-Hellman-Verfahren spielt durch diesen Angriff keine praktische Rolle mehr; es bleibt aber ein Lehrstück, wie skeptisch wir gegenüber unbewiesenen Sicherheitsbeteuerungen bleiben sollten. Auch die eigentliche Frage, ob man sichere Kryptosysteme überhaupt auf **NP**-schwierigen Problemen aufbauen kann, bleibt hochaktuell. Die „philosophische" rein spekulative Antwort, zu der wir tendieren, ist „Nein". Aber leider ist *der Rand zu schmal*, um die Begründung zu fassen.[1]

Das Kapitel über zahlentheoretische Algorithmen ist wichtig für das Erzeugen von Kryptosystemen, für die beispielsweise große „zufällige" Primzahlen benötigt werden. Es ist auch wichtig für die Sicherheit der Verfahren. Wenn man sich auf das

1 Frei nach Pierre de Fermat.

Diffie-Hellman-Verfahren zum sicheren Schlüsselaustausch verlassen möchte, so mag es beruhigend sein, zu verstehen, warum die bekannten Algorithmen bei dem Problem, diskrete Logarithmen zu berechnen, bei moderaten Eingabegrößen versagen. Beim Rechnen mit großen Zahlen bauen viele Analysen darauf auf, dass man Zahlen in fast-linearer Zeit multiplizieren kann. Dies ist ohne den Algorithmus von Schönhage und Strassen nicht zu verstehen. Das Verfahren ist technisch anspruchsvoll und basiert auf brillianten Ideen. Der hier wiedergegebene Korrektheitsbeweis präsentiert dennoch alle Details auf wenigen Seiten.

In dem Kapitel über Primzahlerkennung in Polynomialzeit stellen wir den deterministischen Polynomialzeittest von Agrawal, Kayal und Saxena vor. Dieser nach den Autoren benannte AKS-Test wurde 2002 entdeckt und ist ein Paradebeispiel der erfolgreichen Anwendung diskreter algebraischer Methoden in der Mathematik. In der Darstellung des AKS-Tests folgen wir über weite Strecken der Darstellung des Originalartikels, berücksichtigen allerdings zwei wesentliche Vereinfachungen. So benutzen wir keine tiefliegenden Sätze zur Primzahldichte, sondern nur die Aussage, dass das kleinste gemeinsame Vielfache der ersten n Zahlen schneller als 2^n wächst. Dies hat nach Nair einen elementaren Beweis mittels einer Integralabschätzung. Im Gegensatz zum Originalartikel benutzen wir auch keine Kenntnisse über Kreisteilungspolynome. Dies wird ersetzt durch die viel elementarere Aussage, dass Zerfällungskörper existieren. Durch diese Aufarbeitung ist es möglich, den AKS-Test in einer Mathe-AG an Gymnasien mit einer engagierten Lehrkraft und interessierten Schülern lückenlos zu besprechen. Wir möchten Lehrer zu einem solchen Schulprojekt ermutigen!

In dem Abschnitt über elliptische Kurven stehen wieder die zahlentheoretischen und kryptographischen Anwendungen im Vordergrund. Kryptographie über elliptischen Kurven hat sich in der Praxis etabliert; und dieses Gebiet wird in der Zukunft weiter an Bedeutung gewinnen. Wir stellen dafür die notwendige Mathematik bereit. Ein großes Problem für die Akzeptanz elliptischer Kurven ist, dass Anwender gar nicht verstehen, warum das, was sie ausrechnen, korrekt ist. Dies trifft in weit geringerem Umfang auf RSA-basierte Verfahren zu, denn das Rechnen modulo n ist elementar verständlich. Im Vergleich dazu sind elliptische Kurven inhärent komplizierte mathematische Objekte. Es ist für einen Anwender im Prinzip sehr einfach, die benötigten Operationen auf elliptischen Kurven zu implementieren. Es reichen die Grundrechenarten. Der Formalismus steht damit in Form von Kochrezepten zur Verfügung, aber Kochrezepte (und viele Bücher, die sie enthalten) verraten nicht, warum sie „funktionieren“. Dies führt berechtigterweise zu Berührungsängsten und einer damit verbundenen Skepsis gegenüber elliptischen Kurven. Wir treten dieser Skepsis entgegen, indem wir den schwierigen Teil nicht umschiffen. Der Beweis der Gruppenstruktur wird vollständig geführt und basiert ausschließlich auf dem Kapitel über algebraische Strukturen. Wir verlangen vom Leser insbesondere keine Vorkenntnisse aus der algebraischen Geometrie oder Funktionentheorie.

Mit den beiden Kapiteln *Kombinatorik auf Wörtern* und *Automatentheorie* begeben wir uns in das Teilgebiet der theoretischen Informatik, in dem die Halbgruppentheorie eine zentrale Rolle spielt. Wir behandeln reguläre Sprachen in einem allgemeinen Kontext, der wesentlich für das Verständnis von deterministischen und nichtdeterministischen Automaten ist. Zwei fundamentale Resultate auf diesem Gebiet sind Schützenbergers Charakterisierung sternfreier Sprachen und das Zerlegungstheorem von Krohn und Rhodes. Für beide stellen wir neue und vereinfachte Beweise vor.

Das letzte Kapitel widmet sich diskreten unendlichen Gruppen. Die ausgewählten Themen gehören zur algorithmisch-kombinatorischen Gruppentheorie, wie sie in dem Klassiker von Lyndon und Schupp [55] geprägt wurde. Wir behandeln den Zugang, Standardkonstruktionen durch die systematische Verwendung konfluenter Wortersetzungssysteme zu erklären. Dies führt zu mathematisch präzisen Aussagen und vielfach direkt zu Algorithmen. In dem Abschnitt über freie Gruppen wird der Einfluss von Stallings auf die moderne Gruppentheorie unmittelbar sichtbar. Einige seiner Ideen wurden unabhängig und bereits früher von Benois entwickelt. Dies wird hier dargestellt. Eine besonders schöne Anwendung von Stallings' Ideen ist der geometrische Beweis, dass die Automorphismengruppe endlich erzeugter freier Gruppen von (endlich vielen) Whitehead-Automorphismen erzeugt wird.

Wir sind davon überzeugt, dass es sich bei diskreten algebraischen Methoden um ein zukunftsweisendes Gebiet handelt und dass die Grundlagen in diesem Bereich weiter an Bedeutung gewinnen werden. Das Buch ergänzt und vertieft Grundlagen und zeigt Anwendungen auf. Es werden auch viele Themen behandelt, die über den Standardstoff hinausgehen. Wie in [23] favorisieren wir flüssige gegenüber allzu langatmigen Erklärungen; so soll Freiraum für eigene Überlegungen bleiben. Am Ende eines jeden Kapitels haben wir kurze Zusammenfassungen als Lern- und Merkhilfe hinzugefügt. Erwähnen wir Mathematiker namentlich, so finden sich biographische Angaben, sofern es uns sinnvoll erschien und die Daten öffentlich zugänglich waren oder wir das Einverständnis zur Nennung der Geburtsjahre erhielten. Mit anderen Worten, teilweise fehlen diese Angaben. Bei notwendigen Umschriften von Namen haben wir die international übliche englische Umschrift bevorzugt. Bei lebenden Mathematikern haben wir, falls uns bekannt, auf ihre selbst verwendete Umschrift zurückgegriffen. Schließlich möchten wir darauf hinweisen, dass wir Satzzeichen am Ende von abgesetzten Formeln unterdrückt haben.

Über die Autoren lässt sich berichten, dass sie sowohl in der Mathematik als auch in der Informatik zu Hause sind:

Volker Diekert hatte das große Glück, dass er bei Alexander Grothendieck in Montpellier (Frankreich) eine Abschlussarbeit anfertigen und bei Ernst Witt in Hamburg regelmäßig Seminare besuchen konnte. Diese beeindruckenden Persönlichkeiten haben nachhaltigen Einfluss auf seine Entwicklung gehabt.

Manfred Kufleitner hat beim ersten Autor in Stuttgart in Informatik promoviert und dann ebenfalls in Frankreich (Bordeaux) ein Auslandsjahr verbracht. Mathematik und Schachspielen begeistern ihn seit frühester Jugend. Die genaue Vorausschau, durch welche Züge ein Ziel erreicht werden kann, findet sich durchgehend beim Planen der Beweise im Text.

Gerhard Rosenberger verfügt über die größte Lebenserfahrung, die Erfahrungen Mathematik zu unterrichten und Lehrbücher zu verfassen. Geprägt in seiner Lehre und Forschung sowie bei seiner Präsentation von Vorträgen wurde er insbesondere durch längere Aufenthalte in Russland und den USA. In seinen Forschungsarbeiten kann er auf Koautoren aus mehr als 25 verschiedenen Ländern verweisen.

Danksagung

Das Buch wäre ohne Unterstützung nicht zustande gekommen. Für eine gewisse Strecke war die ganze Abteilung *Theoretische Informatik*, zu der die beiden ersten Autoren gehören, bei der Erstellung des Manuskripts miteinbezogen. Ohne die engagierte Mitarbeit beim Korrekturlesen und der Hilfe beim Lösen von Aufgaben, wäre das Projekt nicht termingerecht fertiggestellt worden. Zum inhaltlichen Gelingen haben insbesondere Ulrich Hertrampf, Jonathan Kausch, Jürn Laun, Alexander Lauser, Tobias Walter und Armin Weiß beigetragen. Hilfe erfuhren wir auch von Horst Prote und Martin Seybold. Die verbliebenen mathematischen Fehler gehen zu Lasten der Autoren.

Unser Dank gilt auch dem Verlag Walter de Gruyter und insbesondere der für uns zuständigen Akquise-Lektorin Friederike Dittberner, die sich spontan bereit erklärte, aus einem Buchprojekt gleich zwei zu machen.

Stuttgart und Hamburg, Januar 2013

Volker Diekert
Manfred Kufleitner
Gerhard Rosenberger

Inhalt

1 Algebraische Strukturen

Die ursprüngliche Aufgabe der Algebra war es, Gleichungen und Gleichungssysteme zu lösen. Die Anwendungen hiervon waren das Vermessungswesen, die Architektur, die Steuererhebung oder auch die Kalenderrechnung. Methoden zum Lösen von linearen und quadratischen Gleichungen sowie zum Wurzelziehen waren den Babyloniern schon mehrere hundert Jahre v. Chr. bekannt. Die ersten allgemeinen Lösungsverfahren für Gleichungen dritten Grades wurden erst im 16. Jahrhundert durch Scipione del Ferro (1465–1526) und später nochmals durch Niccolò Fontana Tartaglia (1500–1557) entdeckt und von Gerolamo Cardano (1501–1576) veröffentlicht. Noch etwas später fand Lodovico Ferrari (1522–1565), ein Schüler Cardanos, entsprechende Lösungsformeln für Gleichungen vierten Grades.

In unmittelbarem Zusammenhang mit den jeweils zur Verfügung stehenden Methoden wurden auch die Zahlenbereiche, mit denen man rechnete, regelmäßig erweitert. Die Entdeckung komplexer Zahlen wird beispielsweise häufig Cardano und Rafael Bombelli (1526–1573) zugeschrieben, wohingegen die (positiven) rationalen Zahlen schon den alten Ägyptern bekannt waren. Bereits in der Antike hatte man verstanden, dass $\sqrt{2}$ keine rationale Zahl war. Der Beweis soll auf Theaitetos (ca. 415–369 v. Chr.) zurückgehen und wurde in Buch X der *Elemente* durch Euklid niedergeschrieben. Dennoch hat $\sqrt{2}$ als Lösung von $X^2 = 2$ eine einfache Beschreibung und, in der Antike wichtiger, als Länge in einem rechtwinkligen Dreieck mit Katheten der Länge 1 eine unmittelbare geometrische Interpretation. Die ersten reellen Zahlen, die nicht als Lösungen von Gleichungssystemen mit rationalen Koeffizienten auftreten, wurden erst 1844 von Joseph Liouville (1809–1882) angegeben. Solche Zahlen nennt man *transzendent*, wohingegen Zahlen *algebraisch* heißen, wenn sie Lösungen eines polynomiellen Gleichungssystems sind. Die beiden bekanntesten Vertreter transzendenter Zahlen sind die Euler'sche Zahl e (nach Leonhard Euler, 1707–1783) und die Kreiszahl π. Den Nachweis der Transzendenz von e erbrachte Charles Hermite (1822–1901) im Jahr 1872. Das entsprechende Resultat für π im Jahr 1882 geht auf Carl Louis Ferdinand von Lindemann (1852–1939) zurück. Für die Euler'sche Konstante $\gamma = 0{,}57772\cdots$ ist es noch offen, ob sie transzendent ist.

Die Methoden, um die „Nicht-Durchführbarkeit" von Dingen zu zeigen, sind häufig abstrakter als die Methoden, die man für die „Durchführbarkeit" braucht. Wenn man zeigen wollte, dass π algebraisch ist, würde es genügen, ein entsprechendes Polynom anzugeben. Aber wie zeigt man, dass kein Polynom mit rationalen Koeffizienten die Zahl π als Nullstelle besitzt? Wie zeigt man, dass es keine Lösungsformeln für Gleichungen fünften Grades gibt? Wie zeigt man, dass das antike Problem der Dreiteilung von Winkeln nur mit Zirkel und Lineal nicht möglich ist?

Solche Fragestellungen haben die moderne Algebra geprägt. Zum einen versuchte man, die Struktur von Zahlen besser zu verstehen. Zum anderen motivierte die Verbreitung von Vektoren und Matrizen die Untersuchung von verallgemeinerten arith-

metischen Operationen. Niels Henrik Abel (1802–1829) zeigte 1824, dass keine Lösungsformeln für Gleichungen fünften Grades existieren. Auf den Ideen Abels aufbauend untersuchte Évariste Galois (1811–1832) allgemeine Gleichungen und erkannte, dass die Weiterentwicklung der Gruppentheorie hierfür von großem Wert war. Vorangetrieben von David Hilbert (1862–1943) wurde Ende des 19. Jahrhunderts der sogenannte axiomatische Ansatz bei den Mathematikern immer populärer. Die Idee war es, interessante Objekte (z. B. Zahlen) nicht direkt zu erforschen. Stattdessen stützten sich Untersuchungen auf ein paar wenige vorgegebene Voraussetzungen (die Axiome), die unter anderem auf die Objekte zutreffen, an denen man interessiert ist. Dadurch begann die Erforschung von allgemeineren Zahlkörpern. Ernst Steinitz (1871–1928) veröffentlichte 1910 die erste axiomatische Studie zu abstrakten Körpern. In den ersten Jahren des 20. Jahrhunderts kam das Konzept von Ringen auf. Amalie Emmy Noether (1882–1935) legte 1921 die Grundlagen für die Untersuchung von kommutativen Ringen.

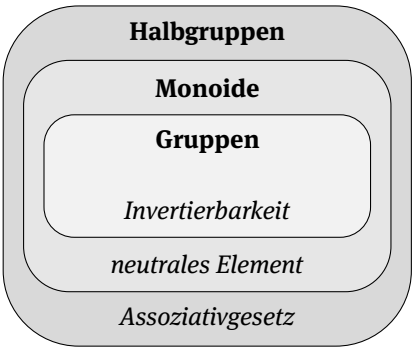
Die Theorie von Halbgruppen und Monoiden wurde vergleichsweise spät entwickelt. Dies liegt vor allem an der intuitiven Idee, dass je mehr Struktur ein Objekt aufweist, desto mehr Eigenschaften lassen sich für diese Objekte herleiten. Viele Mathematiker hielten Halbgruppen für zu allgemein, als dass dafür nichttriviale Strukturaussagen gelten. Als Erste haben Kenneth Bruce Krohn und John Lewis Rhodes (geb. 1937) diese Ansicht 1965 widerlegt. Sie haben eine Zerlegung von endlichen Halbgruppen in einfache Gruppen und Flipflops beschrieben (siehe Satz 7.30). Dieses Ergebnis gilt als Grundstein der Halbgruppentheorie. Eine größere Bedeutung wurde Halbgruppen erst mit der Verbreitung der Informatik beigemessen. Hierzu trägt insbesondere der enge Zusammenhang zwischen Halbgruppen und Automaten bei.

Auf einen allgemeineren Standpunkt stellt sich die universelle Algebra – manchmal spricht man auch von allgemeiner Algebra. Begründet wurde sie 1935 von Garrett Birkhoff (1911–1996). Hier werden beliebige algebraische Strukturen untersucht und häufig auftretende Begriffsbildungen – wie z. B. Homomorphismen und Unterstrukturen – in einem einheitlichen Zusammenhang dargestellt. Die Idee der Verallgemeinerung wird in der Kategorientheorie sogar noch etwas weiter getrieben. Samuel Eilenberg (1913–1998) und Saunders MacLane (1909–2005) entwickelten das Konzept der Kategorien und Funktoren im Jahr 1942. Die Kategorientheorie hat aufgrund ihrer Allgemeinheit viele Erscheinungsformen. Beispielsweise kann man damit die Semantik von Programmiersprachen in einem mathematischen Rahmen darstellen.

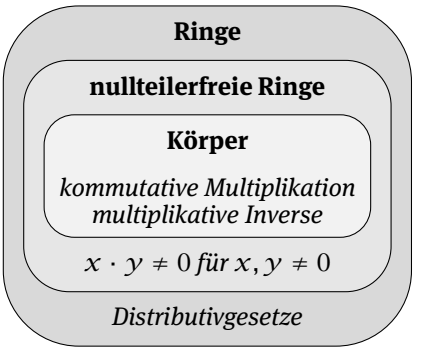
Die heutige Algebra ist durch eine starke Verwebung mit den anderen mathematischen Disziplinen gekennzeichnet. Zu betonen ist hierbei die enge und historisch bedingte Beziehung zur Geometrie und zur Zahlentheorie. Entsprechend sind die Anwendungen der Algebra außerordentlich vielfältig. Nennen wollen wir hiervon die Automatentheorie, algebraische Codierungstheorie und Codes variabler Länge, Kryptographie, Symmetriebetrachtungen in der Chemie und der Physik, Computer-Algebra-Systeme und die Graphentheorie. Die moderne Algebra ist auch von vielen

Begriffsbildungen geprägt. Tatsächlich ist gerade dies einer der Beiträge der jeweiligen Theorien, da hierdurch wichtige Eigenschaften, Zusammenhänge und Unterscheidungskriterien entwickelt und beschrieben werden können.

In diesem Kapitel widmen wir uns einem genaueren Studium der Gruppen, danach behandeln wir Ringe, Polynome und die Körpertheorie soweit, wie es zum Rahmen des Buches passt oder zum Verständnis der anderen Kapitel notwendig ist. Einen kleinen Überblick über die verschiedenen algebraischen Strukturen geben die folgenden Diagramme.



Eine Verknüpfung



Zwei Verknüpfungen

Wir geben nun einen groben Überblick über einige elementare Grundbegriffe der Algebra. Für (binäre) *Verknüpfungen* $\circ : M \times M \to M$ wird häufig die Infixschreibweise $x \circ y$ anstelle von $\circ(x, y)$ verwendet, und wenn die zugrundeliegende Verknüpfung klar ist, dann schreiben wir dafür kurz xy. Eine Verknüpfung auf M ist *assoziativ*, wenn für alle $x, y, z \in M$ die Rechenregel $(xy)z = x(yz)$ gilt, und sie ist *kommutativ* oder auch *abelsch* (nach Niels Henrik Abel), wenn $xy = yx$ für alle $x, y \in M$ ist. Ein Element $e \in M$ ist *neutral*, falls $xe = ex = x$ für alle $x \in M$ gilt. Neutrale Elemente bezeichnet man oft auch als *Einselemente*. Ganz ähnlich ist $n \in M$ ein *Nullelement*, wenn $xn = nx = n$ für alle $x \in M$ gilt. Eine Menge M zusammen mit einer assoziativen Verknüpfung bildet eine *Halbgruppe*. Eine Halbgruppe mit einem neutralen Element wird als *Monoid* bezeichnet. Wenn in einem Monoid M mit neutralem Element e jedes Element x ein *Inverses* y mit $xy = yx = e$ besitzt, dann bildet M eine *Gruppe*. Bei zwei Verknüpfungen $+$ und $\cdot$ kann man auch Rechengesetze zwischen diesen beiden Operationen formulieren. Dies führt auf die Begriffe *Ring* und *Körper*, auf die wir später eingehen.

Etwas grob gesprochen bildet eine Teilmenge $Y \subseteq X$ einer algebraischen Struktur X eine *Unterstruktur*, wenn Y selbst auch wieder dieselben Struktureigenschaften erfüllt, wie sie bei X gefordert werden. Betrachten wir beispielsweise die Halbgruppe $M = \{1, 0\}$ mit der Multiplikation; hier sind $\{1\}$ und $\{0\}$ Unterhalbgruppen. Die Halbgruppe M ist auch ein Monoid, aber nur $\{1\}$ ist ein Untermonoid, da $\{0\}$ zwar ein

Monoid bildet, aber nicht die 1 von M enthält. Die von $X \subseteq Y$ *erzeugte* Unterstruktur von Y ist die kleinste Unterstruktur, welche die Menge X enthält; diese Unterstruktur wird mit $\langle X \rangle$ bezeichnet.

Eine Abbildung zwischen zwei algebraischen Strukturen, die mit den jeweiligen Operationen verträglich ist (wie $+$ und $\cdot$) sowie neutrale Elemente aufeinander abbildet, heißt *Homomorphismus*. So werden für einen Homomorphismus $\varphi : M \to N$ zwischen Monoiden M und N die beiden Eigenschaften $\varphi(xy) = \varphi(x)\varphi(y)$ und $\varphi(1_M) = 1_N$ gefordert; hierbei bezeichnen 1_M und 1_N die jeweiligen neutralen Elemente. Eine Bijektion φ besitzt stets eine Umkehrabbildung φ^{-1}. Sind beide Abbildungen φ und φ^{-1} Homomorphismen, so nennt man φ einen *Isomorphismus*. In vielen Fällen ist ein bijektiver Homomorphismus bereits ein Isomorphismus.

Für Zahlen $k, \ell \in \mathbb{Z}$ schreiben wir $k \mid \ell$, falls $m \in \mathbb{Z}$ existiert mit $km = \ell$; in diesem Fall ist k ein *Teiler* von ℓ. Wir sagen, k ist kongruent ℓ modulo n (und schreiben $k \equiv \ell \bmod n$), falls eine Zahl $m \in \mathbb{Z}$ existiert mit $k = \ell + mn$.

1.1 Gruppen

Der Begriff einer Gruppe entstammt einer umgangssprachlichen Sprechweise und geht wesentlich auf Galois zurück. Er untersuchte die Lösungen polynomieller Gleichungen über den rationalen Zahlen und fasste diese in *Gruppen* auflösbarer Gleichungen zusammen. Den überlieferten Manuskripten nach schrieb er wesentliche mathematische Erkenntnisse erst in der Nacht vor einem Duell auf, bei dem er auf tragische Weise umkam. Die Bedeutung seiner Werke wurde erst posthum ab Mitte des 19. Jahrhunderts erkannt.

Wir untersuchen Gruppen vom abstrakten Standpunkt aus. Eine Gruppe G ist eine Menge mit einer binären Operation $(g, h) \mapsto g \cdot h$, welche assoziativ ist und damit der Gleichung $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ genügt. Ferner gibt es ein *neutrales Element* $1 \in G$ mit $1 \cdot x = x \cdot 1 = x$, und zu jedem $x \in G$ gibt es ein *Inverses* y mit $x \cdot y = y \cdot x = 1$. Tatsächlich reicht es, die Existenz von Linksinversen zu verlangen, da diese dann automatisch auch rechtsinvers sind; siehe Aufgabe 1.7. (a). Außerdem sind die Inversen dann eindeutig bestimmt und wir schreiben x^{-1} für das Inverse y von x. Für eine Teilmenge $X \subseteq G$ bezeichnen wir mit $\langle X \rangle$ die von X *erzeugte* Untergruppe von G. In $\langle X \rangle$ sind damit genau die Gruppenlemente, die sich als Produkt von Elementen x und x^{-1} mit $x \in X$ schreiben lassen. Für $X = \{x_1, \ldots, x_n\}$ schreiben wir auch $\langle x_1, \ldots, x_n \rangle$ anstelle von $\langle \{x_1, \ldots, x_n\} \rangle$.

Im Folgenden sei G eine Gruppe, $g, g_1, g_2 \in G$ seien beliebige Gruppenelemente und H eine Untergruppe von G. Die Menge $gH = \{gh \mid h \in H\}$ nennen wir die *(Links-)Nebenklasse* von g bezüglich H. Analog ist Hg die *Rechts-Nebenklasse* von g. Die Menge der Nebenklassen bezeichnen wir mit G/H, d. h.

$$G/H = \{\, gH \mid g \in G \,\}$$

Analog ist $H\backslash G = \{Hg \mid g \in G\}$ die Menge der Rechts-Nebenklassen.

Lemma 1.1. *Es gelten folgende Eigenschaften:*

(a) $|H| = |gH| = |Hg|$

(b) $g_1H \cap g_2H \neq \emptyset \;\Leftrightarrow\; g_1 \in g_2H \;\Leftrightarrow\; g_1H \subseteq g_2H \;\Leftrightarrow\; g_1H = g_2H$

(c) $|G/H| = |H\backslash G|$

Beweis. Zu (a): Die Abbildung $g\cdot : H \to gH,\ x \mapsto gx$ ist eine Bijektion mit der Umkehrabbildung $g^{-1}\cdot : gH \to H,\ x \mapsto g^{-1}x$. Dies zeigt $|H| = |gH|$. Symmetrisch folgt $|H| = |Hg|$.
Zu (b): Sei $g_1h_1 = g_2h_2$ mit $h_1, h_2 \in H$. Dann gilt $g_1 = g_2h_2h_1^{-1} \in g_2H$. Aus $g_1 \in g_2H$ folgt $g_1H \subseteq g_2H \cdot H = g_2H$. Nun folgt aus $g_1H \subseteq g_2H$ sofort $g_1H \cap g_2H \neq \emptyset$. Hieraus können wir jetzt symmetrisch $g_2H \subseteq g_1H$ schließen. Also sind alle vier Aussagen in (b) äquivalent. Zu (c): Es ist $g_1 \in g_2H$ genau dann, wenn $g_1^{-1} \in Hg_2^{-1}$ gilt. Nach (b) liefert daher die Zuordnung $gH \mapsto Hg^{-1}$ eine Bijektion zwischen den Mengen G/H und $H\backslash G$. □

Aus Lemma 1.1 (b) folgt, dass verschiedene Nebenklassen von H disjunkt sind. Jedes Element $g \in G$ liegt in der Nebenklasse gH. Zusammen bedeutet dies, dass die Einteilung in Nebenklassen eine Partition von G ist, in der nach (a) alle Klassen gleichmächtig sind. Mit $[G : H]$ bezeichnen wir die Anzahl der Nebenklassen von H und nennen $[G : H] = |G/H|$ den *Index* von H in G. Die Mächtigkeit $|G|$ von G heißt *Ordnung* (oder *Gruppenordnung*) von G. Mit Lemma 1.1 (c) gilt dann auch $[G : H] = |H\backslash G|$. Die *Ordnung* eines Elements g ist die Ordnung von $\langle g\rangle$. Falls $\langle g\rangle$ endlich ist, dann ist die Ordnung von g die kleinste positive Zahl n, für die $g^n = 1$ gilt. Der folgende Satz (benannt nach Joseph Louis Lagrange, 1736–1813) ist fundamental.

Satz 1.2 (Lagrange). $|G| = [G : H] \cdot |H|$

Beweis. Für jede Nebenklasse gH wählen wir genau einen Repräsentanten $r \in gH$. Diese Repräsentanten fassen wir in der Menge R zusammen. Es gilt nun $|R| = |G/H|$ und $G/H = \{rH \mid r \in R\}$. Zu zeigen ist $|G| = |R| \cdot |H|$. Nach Lemma 1.1 ist die Menge G die disjunkte Vereinigung $\bigcup\{rH \mid r \in R\}$ und alle Nebenklassen rH haben die Mächtigkeit von H, siehe Abbildung 1.1. Hieraus folgt die Behauptung. □

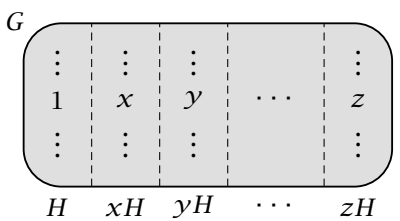


Abb. 1.1: Die Gruppe G als disjunkte Vereinigung von Nebenklassen.

Für endliche Gruppen G ergeben sich aus dem Satz von Lagrange folgende Folgerungen. Die Ordnung einer Untergruppe H ist ein Teiler der Ordnung von G. Mit $H = \langle g \rangle$ folgt, dass die Ordnung von g ein Teiler der Gruppenordnung von G ist. Falls K eine Untergruppe von H und H eine Untergruppe von G ist, dann gilt $[G : K] = [G : H][H : K]$.

Satz 1.3. *Sei $g \in G$ mit Ordnung $d \in \mathbb{N}$. Dann gilt $g^n = 1 \Leftrightarrow d \mid n$.*

Beweis. Für die eine Richtung sei $n = kd$. Dann gilt $g^n = (g^d)^k = 1^k = 1$. Für die Umkehrung sei $g^n = 1$ und $n = kd + r$ mit $0 \leq r < d$. Dann gilt $1 = g^n = (g^d)^k g^r = 1 \cdot g^r = g^r$ und damit $r = 0$. Also ist n ein Vielfaches von d. □

Korollar 1.4. *Sei G endlich. Für alle $g \in G$ gilt $g^{|G|} = 1$.*

Beweis. Sei d die Ordnung von $g \in G$. Aus dem Satz von Lagrange 1.2 folgt, dass d ein Teiler von $|G|$ ist. Mit Satz 1.3 ergibt sich $g^{|G|} = 1$. □

Eine Gruppe G heißt *zyklisch*, falls G von einem Element x erzeugt wird; dies bedeutet $G = \langle x \rangle$. Wir nennen dann x ein *erzeugendes Element*. Zyklische Gruppen sind entweder endlich oder isomorph zu $(\mathbb{Z}, +, 0)$. Falls $|\langle x \rangle| = |\langle y \rangle|$ für zyklische Gruppen $\langle x \rangle$ und $\langle y \rangle$ gilt, definiert $x^i \mapsto y^i$ einen Gruppenisomorphismus. Deshalb sind zyklische Gruppen durch die Anzahl ihrer Elemente (bis auf Isomorphie) eindeutig bestimmt. Für alle $n \geq 1$ ist $\{1, x, x^2, \ldots, x^{n-1}\}$ mit der Verknüpfung $x^i \cdot x^j = x^{(i+j) \bmod n}$ eine von x erzeugte zyklische Gruppe mit n Elementen. Dies wird in Abbildung 1.2 veranschaulicht.

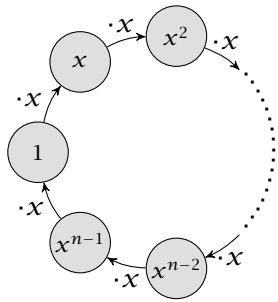


Abb. 1.2: Von x erzeugte Gruppe der Ordnung n.

Satz 1.5. *Gruppen von Primzahlordnung sind zyklisch.*

Beweis. Sei $|G|$ eine Primzahl und $g \in G \setminus \{1\}$. Nun gilt $|\langle g \rangle| \geq 2$ und nach dem Satz von Lagrange 1.2 ist $|\langle g \rangle|$ ein Teiler von $|G|$. Da $|G|$ eine Primzahl ist, folgt $|\langle g \rangle| = |G|$ und damit erzeugt g die Gruppe G. □

Satz 1.6. *Untergruppen von zyklischen Gruppen sind zyklisch.*

Beweis. Sei $G = \langle g \rangle$ und U eine Untergruppe von G. Da die triviale Untergruppe $\{1\}$ zyklisch ist, können wir im Folgenden $U \neq \{1\}$ annehmen. Nun existiert $n > 0$ mit $g^n \in U$. Sei n minimal mit dieser Eigenschaft. Betrachte ein beliebiges Element $g^k \in U$, dann ist $g^{k \bmod n} \in U$. Da n minimal ist, folgt $k \equiv 0 \bmod n$, also wird U von g^n erzeugt. □

Satz 1.7. *Sei G eine abelsche Gruppe und seien $g, h \in G$ mit teilerfremden Ordnungen $n, m \in \mathbb{N}$. Dann hat gh die Ordung nm.*

Beweis. Sei d die Ordnung von gh. Wegen $(gh)^{nm} = (g^n)^m (h^m)^n = 1 \cdot 1 = 1$ folgt mit Satz 1.3, dass d ein Teiler von nm ist. Falls $d \neq nm$ gilt, existiert ein Primteiler p von nm mit $d \mid \frac{nm}{p}$. Wegen $\mathrm{ggT}(m, n) = 1$ gilt entweder $p \mid n$ oder $p \mid m$ (aber nicht beides gleichzeitig). Ohne Einschränkung nehmen wir $p \mid n$ und $p \nmid m$ an. Es gilt nun $(gh)^{\frac{n}{p}m} = g^{\frac{n}{p}m} \cdot 1 \neq 1$, da $\frac{n}{p}m$ kein Vielfaches von n ist. Dies ist ein Widerspruch zu $d \mid \frac{nm}{p}$. Also gilt $d = nm$. □

Der folgende Satz ist nach Augustin Louis Cauchy (1789–1857) benannt. Der hier vorgestellte Beweis ist von James H. McKay (1923–2012) [58].

Satz 1.8 (Cauchy). *Sei G endlich und sei p eine Primzahl, welche die Ordnung von G teilt. Dann gibt es in G ein Element der Ordnung p.*

Beweis. Sei $n = |G|$ und $S = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = 1 \text{ in } G\}$. Da in jedem p-Tupel $(g_1, \ldots, g_p) \in S$ die Elemente $g_1, \ldots, g_{p-1} \in G$ beliebig gewählt werden können und g_p dann durch $g_p = (g_1 \cdots g_{p-1})^{-1}$ eindeutig bestimmt ist, gilt $|S| = n^{p-1}$. Wir definieren $\sim$ durch $(g_1, \ldots, g_p) \sim (g_{i+1}, \ldots, g_p, g_1, \ldots g_i)$ für $1 \leq i \leq p$. Dies ist eine Äquivalenzrelation auf G^p. Die Äquivalenzklasse von $(g_1, \ldots, g_p)$ besteht aus allen zyklischen Vertauschungen. Aus $(g_1 \cdots g_i)(g_{i+1} \cdots g_p) = 1$ folgt $(g_{i+1} \cdots g_p)(g_1 \cdots g_i) = 1$. Also ist $\sim$ auch eine Äquivalenzrelation auf S. Angenommen, es gilt $(g_1, \ldots, g_p) = (g_{i+1}, \ldots, g_p, g_1, \ldots g_i)$ für ein $1 \leq i < p$. Dann gilt $g_1 = g_{i+1} = g_{2i+1} = \cdots = g_{(p-1)i+1}$. Bei dieser Schreibweise rechnen wir im Index modulo p. Da $ki + 1 \equiv \ell i + 1 \bmod p$ äquivalent ist zu $k \equiv \ell \bmod p$, sind alle Indizes $\ell i + 1$ für $0 \leq \ell \leq p - 1$ verschieden, und es gilt $g_1 = g_2 = \cdots = g_p$. Dies zeigt, dass jede Äquivalenzklasse von $\sim$ entweder aus einem Element oder aus p Elementen besteht. Die Klassen mit nur einem Element sind genau die von der Form $\{(g, \ldots, g)\}$. Sei s die Anzahl der Äquivalenzklassen mit einem Element und sei t die Anzahl der Äquivalenzklassen mit p Elementen. Die Einteilung in Äquivalenzklassen liefert $s + pt = |S| = n^{p-1}$. Aus $p \mid n$ folgt $s \equiv 0 \bmod p$. Wegen $(1, \ldots, 1) \in S$ gilt $s \geq 1$ und damit $s \geq p$. Also existiert $g \in G \setminus \{1\}$ mit $(g, \ldots, g) \in S$, d. h. $g^p = 1$ und $g \neq 1$. Aus Satz 1.3 folgt, dass $g \in G$ die Ordnung p hat. □

Zum Abschluss dieses Abschnitts behandeln wir den Homomorphiesatz der Gruppentheorie. Wie wir später sehen werden, ist dieser die Grundlage für einen analogen

Satz der Ringtheorie. Sei $\varphi : G \to K$ ein Gruppenhomomorphismus, d. h., es gilt $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ für alle $g_1, g_2 \in G$. Wir definieren folgende Mengen:

$$\begin{aligned} \ker(\varphi) &= \{ g \in G \mid \varphi(g) = 1 \} \\ \operatorname{im}(\varphi) &= \varphi(G) = \{ \varphi(g) \in K \mid g \in G \} \end{aligned}$$

Wir bezeichnen $\ker(\varphi)$ als den *Kern* von φ und $\operatorname{im}(\varphi)$ als das *Bild* (engl. *image*) von φ. Eine Untergruppe H von G ist ein *Normalteiler* von G, wenn die Links-Nebenklassen von H gleich den Rechts-Nebenklassen von H sind, d. h., falls $gH = Hg$ für alle $g \in G$ gilt. Dies ist gleichbedeutend damit, dass die Einteilung in Links-Nebenklassen und die Einteilung in Rechts-Nebenklassen dieselben Partitionen liefern. Wenn G kommutativ ist, dann sind alle Untergruppen auch Normalteiler.

Satz 1.9. *Für jede Untergruppe H von G sind die folgenden Aussagen äquivalent:*

(a) *H ist ein Normalteiler von G.*

(b) *G/H ist eine Gruppe bezüglich der Verknüpfung $g_1H \cdot g_2H = g_1g_2H$ mit neutralem Element H.*

(c) *H ist der Kern eines Homomorphismus $\varphi : G \to K$.*

(d) *H ist eine Untergruppe und für alle $g \in G$ gilt $gHg^{-1} \subseteq H$.*

Beweis. (a) ⇒ (b): Die Mengen g_1Hg_2H und g_1g_2H sind gleich, denn es gilt $g_1(Hg_2)H = g_1(g_2H)H = g_1g_2H$. Dies zeigt, dass die Verknüpfung auf G/H wohldefiniert und assoziativ ist und dass H das neutrale Element ist. Wohldefiniertheit bedeutet, dass die Operation unabhängig von den Repräsentaten g_1 und g_2 ist. Das Inverse von gH ist $g^{-1}H \in G/H$.
(b) ⇒ (c): Betrachte die Abbildung $\varphi : G \to G/H,\ g \mapsto gH$. Es gilt $\varphi(g_1g_2) = g_1g_2H = g_1Hg_2H = \varphi(g_1)\varphi(g_2)$. Also ist φ ein Homomorphismus. Der Kern von φ ist $\ker(\varphi) = \{g \in G \mid gH = H\} = H$.
(c) ⇒ (d): Sei $\varphi : G \to K$ ein Gruppenhomomorphismus mit $\ker(\varphi) = H$. Es gilt $1 \in H$, da $\varphi(1) = 1$. Seien $g_1, g_2 \in H$, dann ist $\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = 1 \cdot 1 = 1$. Daraus folgt $g_1g_2^{-1} \in \ker(\varphi) = H$. Dies zeigt, dass H eine Untergruppe ist; siehe Aufgabe 1.8. (a) Für alle $g \in G$ und alle $h \in H$ gilt $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$ und damit $gHg^{-1} \subseteq H = \ker(\varphi)$.
(d) ⇒ (a): Aus $gHg^{-1} \subseteq H$ folgt $gH \subseteq Hg$ und $Hg^{-1} \subseteq g^{-1}H$ für alle $g \in G$. Da sich alle Gruppenelemente in G als Inverses darstellen lassen, gilt damit auch $Hg \subseteq gH$ für alle $g \in G$. Insgesamt haben wir $gH = Hg$ für alle $g \in G$. □

Falls H ein Normalteiler ist, bezeichnet man die Gruppe aus Satz 1.9 (b) als die *Faktorgruppe* von G *modulo* H. Die Abbildung $G \to G/H,\ g \mapsto gH$ ist ein Homomorphismus mit Kern H. Im Falle von zyklischen Gruppen kann man Faktorgruppen durch „Aufwickeln“ interpretieren. Betrachten wir die endliche zyklische Gruppe $C_6 = \{0, 1, 2, 3, 4, 5\}$ mit der Addition modulo 6 als Verknüpfung. Dann ist $\{0, 3\}$ eine Untergruppe. Da in kommutativen Gruppen jede Untergruppe ein Normalteiler

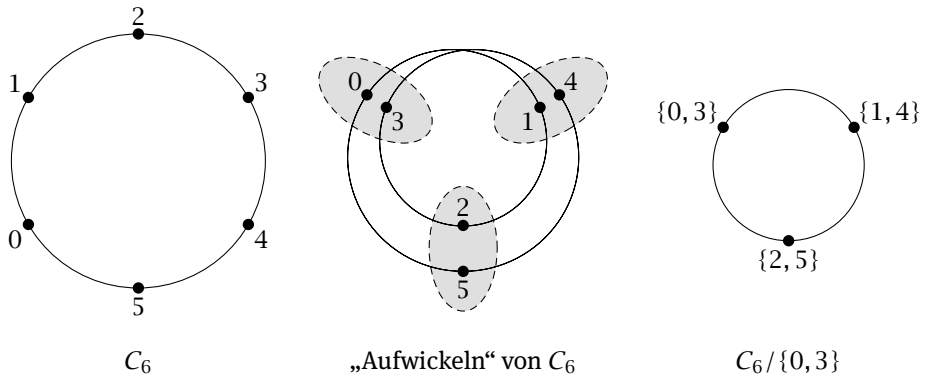


Abb. 1.3: Übergang von C_6 zu $C_6/\{0,3\}$.

ist, und da jede zyklische Gruppe kommutativ ist, ist $\{0,3\}$ ein Normalteiler von C_6 und wir können die Faktorgruppe $C_6/\{0,3\}$ bilden, siehe Abbildung1.3. Am Beispiel der unendlichen zyklischen Gruppe $(\mathbb{Z},+,0)$ und ihrem Normalteiler $4\mathbb{Z}$ ergibt sich eine analoge Zeichnung, siehe Abbildung 1.4. Hierbei identifizieren wir $\mathbb{Z}/4\mathbb{Z}$ durch Wahl von Repräsentanten mit der Menge $\{0,1,2,3\}$. Jedes Element dieser Menge entspricht der Nebenklasse in der es vorkommt, z. B. entspricht das Element 3 der Nebenklasse $3+4\mathbb{Z}=\{\ldots,-1,3,7,\ldots\}$. Dieselbe Deutung funktioniert ganz analog für die unendliche und nicht zyklische Gruppe $(\mathbb{R},+,0)$ und ihren Normalteiler $4\mathbb{Z}$.

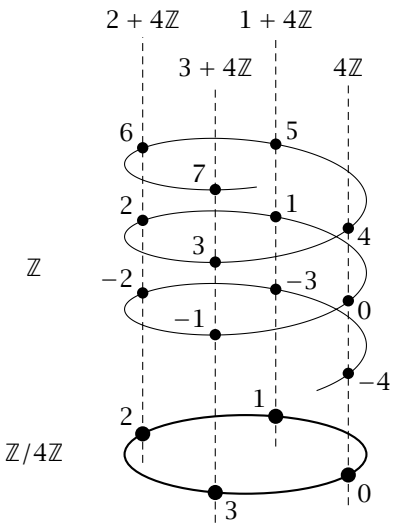


Abb. 1.4: Übergang von $\mathbb{Z}$ zu $\mathbb{Z}/4\mathbb{Z}$.

Dies liefert eine Veranschaulichung der unendlichen Gruppe $\mathbb{R}/4\mathbb{Z}$ als Kreis der Länge 4.

Satz 1.10. *Untergruppen von Index 2 sind Normalteiler.*

Beweis. Sei $[G : H] = 2$. Dann gilt:

$$gH = \left\{ \begin{array}{ll} H & \text{falls } g \in H \\ G \setminus H & \text{falls } g \notin H \end{array} \right\} = Hg$$

Also ist H ein Normalteiler. □

Satz 1.11 (Homomorphiesatz der Gruppentheorie)**.** *Seien G, K Gruppen und sei $\varphi : G \to K$ ein Homomorphismus. Dann induziert φ den Isomorphismus:*

$$\begin{aligned} \overline{\varphi} : G/\ker(\varphi) &\to \operatorname{im}(\varphi) \\ g\ker(\varphi) &\mapsto \varphi(g) \end{aligned}$$

Beweis. Sei $H = \ker(\varphi)$. Die Abbildung $\overline{\varphi}$ ist wohldefiniert: Sei $g_1H = g_2H$. Dann ist $g_1 = g_2h$ für $h \in H$. Damit gilt $\overline{\varphi}(g_1H) = \varphi(g_1) = \varphi(g_2h) = \varphi(g_2)\varphi(h) = \varphi(g_2) = \overline{\varphi}(g_2H)$, da $\varphi(h) = 1$. Aus der Wohldefiniertheit folgt nun unmittelbar, dass $\overline{\varphi}$ ein Homomorphismus ist.

Nach Konstruktion ist $\overline{\varphi}$ surjektiv. Zu zeigen bleibt, dass $\overline{\varphi}$ injektiv ist. Sei $\overline{\varphi}(g_1H) = \overline{\varphi}(g_2H)$. Es folgt $\varphi(g_1) = \varphi(g_2)$ und $\varphi(g_1^{-1}g_2) = \varphi(g_2^{-1}g_1) = 1$. Dies zeigt schließlich $g_1^{-1}g_2$, $g_2^{-1}g_1 \in H$ und damit $g_1H = g_2H$. □

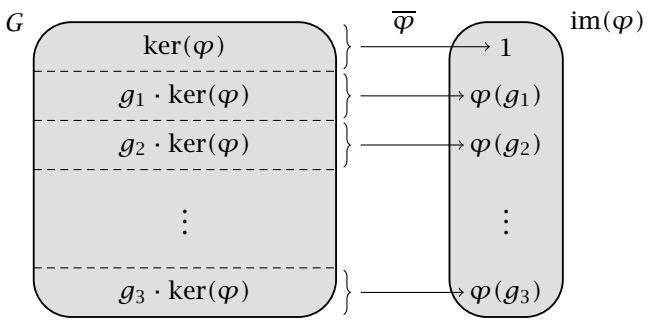
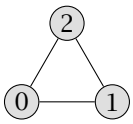


Abb. 1.5: Veranschaulichung des Homomorphiesatzes der Gruppentheorie.

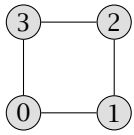
Bemerkung 1.12. Aus dem Homomorphiesatz der Gruppentheorie 1.11 und Satz 1.9 folgt, dass es gleichwertig ist, Faktorgruppen oder homomorphe Bilder von Gruppen zu betrachten. Außerdem sehen wir, dass ein Gruppenhomomorphismus φ genau dann injektiv ist, wenn $\ker(\varphi) = \{1\}$ gilt. ◊

1.2 Bewegungsgruppen regelmäßiger Vielecke

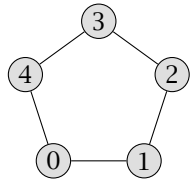
In diesem Abschnitt wollen wir die oben eingeführten Konzepte anhand von Abbildungen von regelmäßigen Vielecken auf sich selbst veranschaulichen. Ein *regelmäßiges n-Eck* ist ein ungerichteter Graph $C_n = (V, E)$ mit $V = \mathbb{Z}/n\mathbb{Z}$ und der Kantenmenge $E = \{\{i, i+1\} \mid i \in \mathbb{Z}/n\mathbb{Z}\} \subseteq \binom{V}{2}$. Die Fälle $n = 0$, $n = 1$ und $n = 2$ entarten und sind für uns uninteressant. Für $n \geq 3$ hat ein n-Eck stets n Kanten.



Dreieck



Viereck



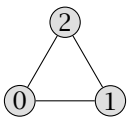
Fünfeck

Ein *Automorphismus* eines Graphen $G = (V, E)$ ist eine bijektive Abbildung $\varphi : V \to V$ mit

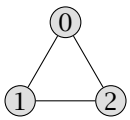
$$\forall x, y \in V\colon \{x, y\} \in E \;\Leftrightarrow\; \{\varphi(x), \varphi(y)\} \in E$$

Die Menge der Automorphismen $\mathrm{Aut}(G) \subseteq V^V$ eines Graphen $G = (V, E)$ bildet eine Gruppe mit der Hintereinanderausführung von Abbildungen als Verknüpfung und dem neutralen Element id_V. Man bezeichnet $\mathrm{Aut}(G)$ als die *Automorphismengruppe* oder *Bewegungsgruppe* von G. Im Folgenden wollen wir die Gruppen $D_n = \mathrm{Aut}(C_n)$ untersuchen, die Bewegungsgruppen von regelmäßigen n-Ecken.

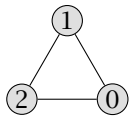
Sei $\varphi \in D_n$, dann ist φ eindeutig durch die Werte $\varphi(0)$ und $\varphi(1)$ bestimmt. Sei $\varphi(0) = i$ mit $i \in \mathbb{Z}/n\mathbb{Z}$. Dann gibt es für $\varphi(1)$ nur die Möglichkeiten $\varphi(1) = i + 1$ und $\varphi(1) = i - 1$, denn der Knoten i ist nur mit den Knoten $i - 1$ und $i + 1$ verbunden. In dem für uns interessanten Fall $n \geq 3$ sind $i + 1$ und $i - 1$ zwei verschiedene Knoten. Falls $\varphi(1) = i + 1$, dann folgt $\varphi(2) = i + 2$, da i und $i + 2$ die einzigen Nachbarn von $i + 1$ sind, und weil $\varphi(2) \neq i = \varphi(0)$ wegen der Bijektivität von φ gilt. Wenn wir so fortfahren, erhalten wir $\varphi(j) = \varphi(0) + j$. Im anderen Fall $\varphi(1) = i - 1$ erhalten wir symmetrisch $\varphi(j) = \varphi(0) - j$ für alle $j \in \mathbb{Z}/n\mathbb{Z}$. Dies bedeutet $|D_n| = 2n$ für $n \geq 3$, da wir für $\varphi(0)$ genau n Möglichkeiten haben und zwei mögliche Orientierungen in Frage kommen. Die 6 Elemente von D_3 lassen sich wie folgt veranschaulichen:



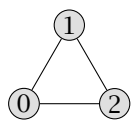
id



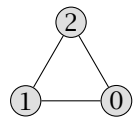
δ



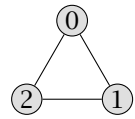
δ^2



σ



$\delta\sigma$



$\delta^2\sigma$

Wegen $6 = 3!$ ergibt sich, dass D_3 alle Permutationen der Ecken 0, 1 und 2 enthält. Wir zeigen jetzt, dass für $n \geq 3$ die Gruppe D_n in Drehungen und Spiegelungen zerfällt. Definiere die Drehung $\delta \in D_n$ durch:

$$\delta(j) = j + 1 \quad \text{für } j \in \mathbb{Z}/n\mathbb{Z}$$

Dann gilt $\delta^k(j) = j + k$ für alle $k, j \in \mathbb{Z}/n\mathbb{Z}$ und damit $\delta^n = \mathrm{id}$. Insbesondere folgt daraus $\delta^k = \delta^m$, falls $k \equiv m \bmod n$. Es gibt n Drehungen $\mathrm{id} = \delta^0, \delta = \delta^1, \delta^2, \ldots, \delta^{n-1}$. Dabei gilt für jede Drehung $(\delta^k)^{-1} = \delta^{n-k} = \delta^{-k}$ falls $k \in \mathbb{Z}/n\mathbb{Z}$. Wir definieren die Spiegelung $\sigma \in D_n$ durch

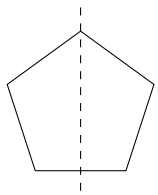
$$\sigma(j) = -j \quad \text{für } j \in \mathbb{Z}/n\mathbb{Z}$$

Wir können σ durch die Spiegelung an der Achse durch den Punkt $0 \in \mathbb{Z}/n\mathbb{Z}$ und den Mittelpunkt des n-Ecks visualisieren. Das Verhalten für ungerade n und gerade n ist unterschiedlich. Für gerade n hat σ zwei Fixpunkte. Es gilt $\sigma(0) = 0$ und $\sigma(\frac{n}{2}) = \frac{n}{2}$. Für ungerade n ist 0 der einzige Fixpunkt.

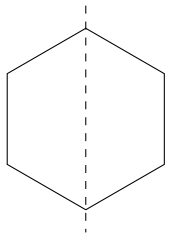
Sei $i \in \mathbb{Z}/n\mathbb{Z}$ ein beliebiger Eckpunkt. Betrachte die Spiegelung σ_i an der Achse durch i und den Mittelpunkt des n-Ecks. Dann gilt $\sigma_i(j) = -(j - i) + i = 2i - j = \delta^{2i}(\sigma(j))$. Das heißt, die Spiegelungen haben mit $\sigma = \sigma_0$ alle die Gestalt $\sigma_i = \delta^{2i}\sigma$. Für ungerade n sind alle σ_i verschieden, und wir erhalten

$$D_n = \{\mathrm{id}, \delta, \delta^2, \ldots, \delta^{n-1}, \sigma_0, \sigma_1, \ldots, \sigma_{n-1}\}$$

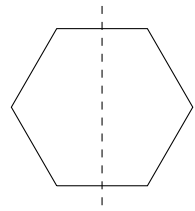
Für gerade n geht die Spiegelungsachse durch i und den Mittelpunkt auch durch den Punkt $\frac{n}{2} + i$ und es gilt $\sigma_i = \sigma_{\frac{n}{2}+i}$. Es gibt dann aber $\frac{n}{2}$ weitere Spiegelungsachsen durch je zwei gegenüberliegende Kanten.



n ungerade



n gerade, Spiegelungsachse durch 2 Knoten



n gerade, Spiegelungsachse durch 2 Kanten

Betrachte die Abbildung $\delta^i\sigma$ mit i ungerade. Dann gilt $\delta^i\sigma(j) = i - j$. Man beachte, für n gerade und i ungerade gibt es kein j mit $i - j \equiv j \bmod n$, d. h., $\delta^i\sigma$ besitzt keine Fixpunkte. Die Spiegelungsachse teilt genau zwei Kanten. Um diese Kanten zu berechnen, betrachten wir die Gleichung $\delta^i\sigma(j) = j+1$. Es ergibt sich die Kongruenz

$i - j \equiv j + 1 \bmod n$. Dies ist gleichbedeutend mit $i - 1 \equiv 2j \bmod n$. Für gerades n und ungerades i hat dies die beiden Lösungen:

$$j = \frac{i-1}{2} \quad \text{und} \quad j = \frac{n+i-1}{2}$$

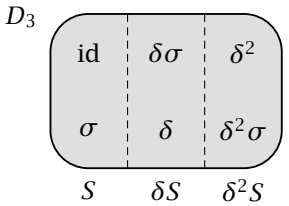
Daraus folgt, dass $\delta^i\sigma$ an folgenden Kanten spiegelt:

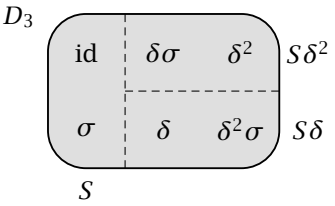
$$\left\{\frac{i-1}{2}, \frac{i-1}{2}+1\right\} \quad \text{und} \quad \left\{\frac{n+i-1}{2}, \frac{n+i-1}{2}+1\right\}$$

Unabhängig davon, ob n gerade oder ungerade ist, können wir D_n schreiben als $D_n = \{\mathrm{id}, \delta, \delta^2, \ldots, \delta^{n-1}, \sigma, \delta\sigma, \delta^2\sigma, \ldots, \delta^{n-1}\sigma\}$. Damit kennen wir alle $2n$ Elemente aus D_n. Als Nächstes stellen wir einige Identitäten für D_n zusammen:

$$\sigma^2 = \mathrm{id}, \quad \delta^n = \mathrm{id}, \quad \delta\sigma = \sigma\delta^{-1}$$

Die Ordnung von σ ist 2 und die Ordnung von δ ist n. Die Untergruppe $S = \langle\sigma\rangle = \{\mathrm{id}, \sigma\}$ von $D_n = \langle\delta, \sigma\rangle$ enthält 2 Elemente und besitzt nach dem Satz von Lagrange 1.2 genau n Nebenklassen. Es gilt $G/S = \{S, \delta S, \ldots, \delta^{n-1}S\}$. Aus $\delta\sigma = \sigma\delta^{-1} \notin S\delta$ für $n \geq 3$ folgt $\delta S \neq S\delta$. Damit ist S kein Normalteiler für $n \geq 3$. Im Fall von $n = 3$ liefert die Einteilung in Links-Nebenklassen und Rechts-Nebenklassen von S die folgenden Partitionen von D_3:





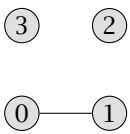
Betrachten wir die Untergruppe $N = \langle\delta\rangle = \{\mathrm{id}, \delta, \delta^2, \ldots, \delta^{n-1}\}$ mit Ordnung n. Dann hat N den Index 2 in D_n. Die beiden Nebenklassen dieser Gruppe sind N und $\sigma N = \{\sigma, \sigma\delta, \sigma\delta^2, \ldots, \sigma\delta^{n-1}\}$. Nach Satz 1.10 ist N ein Normalteiler von D_n. Dies folgt auch aus der Beziehung $\sigma\delta^i = \delta^{-i}\sigma$.

Für $n \geq 2$ betrachte D_{2n}. Dann enthält die Untergruppe $E_n = \langle\delta^2\rangle = \{\mathrm{id}, \delta^2, \delta^4, \ldots, \delta^{2n-2}\}$ genau n Elemente. Der Index von $E = E_n$ in D_{2n} ist damit 4. Die vier Nebenklassen von E sind E, δE, σE und $\sigma\delta E$. Es gilt $\sigma\delta^{2i} = \delta^{2n-2i}\sigma$; insbesondere ist $2n - 2i$ gerade. Daraus folgt $\sigma E = E\sigma$. Zusammen mit $\delta E = E\delta$ können wir schließen, dass E ein Normalteiler von D_{2n} ist. Damit ist D_{2n}/E eine Gruppe mit 4 Elementen. Wir wählen das Repräsentantensystem $\{\mathrm{id}, \delta, \sigma, \sigma\delta\}$ für die vier Nebenklassen bezüglich E. Für die Nebenklassen gilt nun zusätzlich zu den Rechenregeln aus D_{2n} die Beziehung $\delta^2 = \mathrm{id}$, da alle Elemente aus E dem Repräsentanten id entsprechen.

Anstatt mit den Nebenklassen zu rechnen, definieren wir auf dem Repräsentantensystem die Gruppenstruktur direkt durch die folgende Multiplikationstabelle.

$\cdot$	**id**	$\boldsymbol{\delta}$	$\boldsymbol{\sigma}$	$\boldsymbol{\sigma\delta}$
id	id	δ	σ	$\sigma\delta$
$\boldsymbol{\delta}$	δ	id	$\sigma\delta$	σ
$\boldsymbol{\sigma}$	σ	$\sigma\delta$	id	δ
$\boldsymbol{\sigma\delta}$	$\sigma\delta$	σ	δ	id

Die Tabelle ist symmetrisch und auf der Diagonalen steht jeweils id. Die Gruppe ist daher abelsch und alle nichttrivialen Elemente haben die Ordnung 2. Deshalb kann die Gruppe nicht zyklisch sein. Man bezeichnet sie als die *Klein'sche Vierergruppe* nach Felix Christian Klein (1849–1925). Sie ist isomorph zum direkten Produkt $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und zur Automorphismengruppe des folgenden Graphen mit vier Knoten:



1.3 Symmetrische Gruppen

Mit S_n bezeichnen wir die Permutationen auf der Menge $\{1,\dots,n\}$. Die Permutationen S_n bilden bezüglich der Hintereinanderausführung von Abbildungen eine Gruppe, dabei sei $\pi\sigma$ durch $(\pi\sigma)(i) = \pi(\sigma(i))$ für $1 \le i \le n$ definiert. Man nennt S_n die *symmetrische Gruppe* einer n-elementigen Menge. Sie enthält alle Gruppen der Ordnung n als Untergruppe, denn jedes Element g einer Gruppe G definiert durch $x \mapsto gx$ eine Permutation auf der Menge G. Für $|G| = n$ können wir also G in die Gruppe S_n einbetten. In diesem Abschnitt wollen wir die Elemente von S_n näher betrachten. Sei π eine Permutation auf $\{1,\dots,n\}$. Dann ist ein Paar $(i,j) \in \{1,\dots,n\}^2$ mit $i < j$ eine *Fehlstellung* von π, wenn $\pi(i) > \pi(j)$ gilt. Die Anzahl der Fehlstellungen von π bezeichnen wir mit $I(\pi)$. Eine Permutation aus S_n hat maximal $\binom{n}{2}$ Fehlstellungen, und die Permutation $\pi = (n,\dots,1)$ mit $\pi(i) = n - i + 1$ nimmt diese obere Schranke an. Die identische Abbildung ist die einzige Permutation ohne Fehlstellungen. Das *Vorzeichen* („Signum") von π ist $\operatorname{sgn}(\pi) = (-1)^{I(\pi)}$; es ist ein Element der multiplikativen Gruppe $\{1,-1\}$.

Lemma 1.13. *Sei $\pi : \{1,\dots,n\} \to \{1,\dots,n\}$ eine Permutation. Dann gilt:*

$$\operatorname{sgn}(\pi) = \prod_{1 \le i < j \le n} \frac{\pi(j) - \pi(i)}{j - i}$$

Beweis. Sei $\mathcal{F} \subseteq \{1,\dots,n\}^2$ die Menge der Fehlstellung von π, und sei $\mathcal{G} = \{(i,j) \mid 1 \le i < j \le n,\ (i,j) \notin \mathcal{F}$ das Komplement von $\mathcal{F}$. Dann gilt:

$$\prod_{i<j} \frac{\pi(j)-\pi(i)}{j-i} = \prod_{(i,j)\in\mathcal{F}} \frac{\pi(j)-\pi(i)}{j-i} \cdot \prod_{(i,j)\in\mathcal{G}} \frac{\pi(j)-\pi(i)}{j-i}$$
$$= (-1)^{|\mathcal{F}|} \prod_{(i,j)\in\mathcal{F}} \frac{\pi(i)-\pi(j)}{j-i} \cdot \prod_{(i,j)\in\mathcal{G}} \frac{\pi(j)-\pi(i)}{j-i} = (-1)^{|\mathcal{F}|} = \operatorname{sgn}(\pi)$$

Hierbei gilt $\prod_{(i,j)\in\mathcal{F}} \frac{\pi(i)-\pi(j)}{j-i} \cdot \prod_{(i,j)\in\mathcal{G}} \frac{\pi(j)-\pi(i)}{j-i} = 1$, da jedes Paar (i,j) mit $1 \le i < j \le n$ genau einmal über dem Bruchstrich und einmal unter dem Bruchstrich den Faktor $j-i$ beiträgt. □

Satz 1.14. *Die Abbildung* $\operatorname{sgn} : S_n \to \{1,-1\}$ *ist ein Homomorphismus.*

Beweis. Sei $T = \binom{\{1,\dots,n\}}{2}$ die Menge aller zweielementigen Teilmengen von $\{1,\dots,n\}$. Für alle $\pi \in S_n$ und alle $i \neq j$ gilt $\frac{\pi(j)-\pi(i)}{j-i} = \frac{\pi(i)-\pi(j)}{i-j}$. Also kommt es nicht auf die Reihenfolge von i und j an, sodass der Ausdruck $\prod_{\{i,j\}\in T} \frac{\pi(j)-\pi(i)}{j-i}$ wohldefiniert ist und mit $\operatorname{sgn}(\pi)$ übereinstimmt. Für $\pi, \sigma \in S_n$ gilt

$$\operatorname{sgn}(\pi\sigma) = \prod_{\{i,j\}\in T} \frac{\pi(\sigma(j))-\pi(\sigma(i))}{j-i} = \prod_{\{i,j\}\in T} \frac{\pi(\sigma(j))-\pi(\sigma(i))}{\sigma(j)-\sigma(i)} \cdot \frac{\sigma(j)-\sigma(i)}{j-i}$$
$$= \prod_{\{i,j\}\in T} \frac{\pi(j)-\pi(i)}{j-i} \cdot \prod_{\{i,j\}\in T} \frac{\sigma(j)-\sigma(i)}{j-i} = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$$

wobei die vorletzte Gleichheit $\{\{\sigma(i),\sigma(j)\} \mid \{i,j\} \in T\} = T$ verwendet. □

Eine *Transposition* ist eine Permutation, welche genau zwei Elemente miteinander vertauscht und alle anderen Elemente unverändert lässt. Die Anzahl der Fehlstellungen einer Transposition σ, die i mit j vertauscht, ist für $i < j$ die Zahl $2(j-i)-1$. Denn schreiben wir σ als Tupel $(\sigma(1),\dots,\sigma(n))$, so ergibt sich die folgende Darstellung, in der wir alle Fehlstellungen erkennen:

$$\sigma = (1,\dots,i-1,\ j\,,i+1,\dots,j-1,\ i\,,j+1,\dots,n)$$

Die $j-i-1$ Elemente zwischen i und j haben jeweils eine Fehlstellung mit i und mit j; hinzu kommt noch die Fehlstellung von i und j selbst. Das Vorzeichen einer Transposition ist daher stets -1.

Korollar 1.15. *Wenn sich eine Permutation* π *auf* $\{1,\dots,n\}$ *als Produkt von* m *Transpositionen schreiben lässt, dann gilt* $\operatorname{sgn}(\pi) = (-1)^m$.

Beweis. Jede Transposition hat das Vorzeichen -1. Nach Satz 1.14 ist $\operatorname{sgn} : S_n \to \{-1,1\}$ ein Homomorphismus. Daraus folgt $\operatorname{sgn}(\pi) = (-1)^m$. □

Als Nächstes überzeugen wir uns davon, dass die Gruppe S_n von Transpositionen erzeugt wird. Etwas genauer zeigen wir, dass hierfür Transpositionen ausreichen, welche jeweils nur benachbarte Elemente i und $i+1$ vertauschen.

Satz 1.16. *Jedes Element der symmetrischen Gruppe S_n kann als Produkt von höchstens $\binom{n}{2}$ Transpositionen geschrieben werden, so dass jede dieser Transpositionen nur benachbarte Elemente vertauscht.*

Beweis. Sei $\pi \in S_n$. Wir machen eine Induktion nach der Anzahl der Fehlstellungen $I(\pi)$. Wenn π keine Fehlstellungen hat, dann gilt stets $\pi(i) = i$, und π ist die Identität. Insbesondere ist π dann das Produkt von 0 Transpositionen. Wenn π eine Fehlstellung enthält, dann gibt es einen Index i mit $\pi(i) > \pi(i+1)$. Sei σ die Transposition, die i und $i+1$ vertauscht; dann hat $\pi\sigma$ eine Fehlstellung weniger als π. Mit Induktion lässt sich $\pi\sigma$ als Produkt von Transpositionen $\sigma_1 \cdots \sigma_m$ schreiben, wobei $m = I(\pi\sigma)$ gilt und jede Transposition σ_i nur benachbarte Elemente vertauscht. Es folgt $\pi = \sigma_1 \cdots \sigma_m \sigma$. □

Aufgrund von Korollar 1.15 sehen wir, dass die Definition des Vorzeichens unabhängig von der Wahl der Anordnung der Elemente in $\{1, \ldots, n\}$ ist, denn die Definition einer Transposition ist davon unabhängig. Ist also X eine endliche Menge und π eine Permutation von X, so können wir das Vorzeichen $\operatorname{sgn}(\pi)$ definieren. Insbesondere können wir bei einer endlichen Gruppe G mit einer beliebigen Anordnung der Elemente beginnen, und jede solche Anordnung definiert für alle $g \in G$ dasselbe Vorzeichen $\operatorname{sgn}(g) \in \{1, -1\}$; hierzu betrachtet man die von g induzierte Permutation $x \mapsto gx$ auf G.

Bemerkung 1.17. Der Kern des Homomorphismus $\operatorname{sgn} : S_n \to \{1, -1\}$ ist die *alternierende Gruppe* A_n über n Elementen. Es sind die Permutationen mit positivem Vorzeichen. Man spricht auch von der Menge der *geraden Permutationen*, während die Elemente mit Vorzeichen -1 als *ungerade Permutationen* bezeichnet werden. Nach Korollar 1.15 werden gerade (bzw. ungerade) Permutationen von einer geraden (bzw. ungeraden) Anzahl von Transpositionen erzeugt. Bemerkenswert ist auch, dass die Gruppen A_n ab $n = 5$ keine nichttrivialen Normalteiler haben. Diese Eigenschaft führte zu der Erkenntnis, dass Polynomgleichungen fünften oder höheren Grades im Allgemeinen nicht mit sogenannten Wurzelausdrücken auflösbar sind. Der entsprechende Satz ist nach Paolo Ruffini (1765–1822) und Niels Henrik Abel benannt, und seine Entdeckung steht am Anfang der *Galois-Theorie*. ◊

1.4 Ringe

Wir erinnern uns, dass ein Ring durch ein Tupel $(R, +, \cdot, 0, 1)$ gegeben ist, wobei $(R, +, 0)$ eine abelsche Gruppe und $(R, \cdot, 1)$ ein Monoid ist. Der Ring heißt *kommutativ*, wenn die Multiplikation kommutativ ist. Ferner gelten die Distributivgesetze:

$$\begin{aligned}(x + y) \cdot z &= x \cdot z + y \cdot z \\ z \cdot (x + y) &= z \cdot x + z \cdot y\end{aligned}$$

Gilt in einem Ring $0 = 1$, so folgt $R = \{0\}$ und R ist der *Nullring*. In allen anderen Ringen gilt $0 \neq 1$. Die Menge der multiplikativ invertierbaren Elemente $\{r \in R \mid \exists s\colon rs = sr = 1\}$ ist die *Einheitengruppe* oder *multiplikative Gruppe* von R und wird mit R^* bezeichnet. Es gilt $1 \in R^*$. Ein Ring R ist ein *Schiefkörper*, wenn nur die Null nicht invertierbar ist, also $R^* = R \setminus \{0\}$ gilt. Wir behandeln hier nur kommutative Schiefkörper, dies sind genau die *Körper*.

Eine Teilmenge S eines Rings R heißt *Unterring*, falls S bezüglich der Addition eine Untergruppe und bezüglich der Multiplikation ein Untermonoid bildet. Insbesondere haben Unterringe dieselbe Null und dieselbe Eins. Damit ist S mit den Einschränkungen der Operationen von R selbst ein Ring. Ein Unterring S eines Körpers R ist ein *Unterkörper*, falls S selbst ein Körper ist.

Beispiel 1.18. Ist R ein Ring, so bildet die Menge der Abbildungen

$$R^R = \{ f : R \to R \mid f \text{ ist Abbildung} \}$$

einen Ring mit der punktweisen Addition und Multiplikation. Formal sind für $f, g \in R^R$ die Abbildungen $f + g \in R^R$ und $f \cdot g \in R^R$ definiert durch:

$$\begin{aligned}(f + g)(r) &= f(r) + g(r)\\ (f \cdot g)(r) &= f(r) \cdot g(r)\end{aligned}$$

Auch wenn R ein Körper ist, so ist R^R kein Körper. ◊

Wir nennen eine Abbildung $\varphi : R \to S$ zwischen Ringen einen Homomorphismus oder genauer einen *Ringhomomorphismus*, falls die folgenden Bedingungen für alle $x, y \in R$ erfüllt sind.

(a) $\varphi(x + y) = \varphi(x) + \varphi(y)$

(b) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

(c) $\varphi(1) = 1$

Die erste Eigenschaft bedeutet, dass φ ein Gruppenhomomorphismus bezüglich der Addition ist. Es gilt deshalb auch $\varphi(0) = 0$. Die beiden letzten Eigenschaften besagen, dass φ ein Monoidhomomorphismus bezüglich der Multiplikation ist. Insbesondere folgt (c) nicht aus (b). Ein bijektiver Ringhomomorphismus ist ein *Ringisomorphismus*, denn aufgrund der Bijektivität ist die Umkehrabbildung auch ein Homomorphismus.

Beispiel 1.19. Sei R ein Ring und $r \in R$. Dann ist die Zuordnung $R^R \to R$ mit $f \mapsto f(r)$ ein Ringhomomorphismus. ◊

Eine Teilmenge $I \subseteq R$ heißt *Ideal*, wenn I eine additive Untergruppe von R ist und wenn $R \cdot I \cdot R \subseteq I$ gilt. Eine Teilmenge $I \subseteq R$ ist eine additive Untergruppe von R, wenn $(I, +, 0)$ eine Untergruppe von $(R, +, 0)$ ist. Ein Ideal kann nur dann ein Unterring sein, wenn $1 \in I$ gilt. Dann gilt aber schon $I = R$. Die Menge der additiven

Nebenklassen von I ist $R/I = \{r + I \mid r \in R\}$. Aufgrund der Kommutativität der Addition in R bildet die Menge der Nebenklassen R/I selbst eine abelsche Gruppe. Für die Addition gilt dann:

$$(r + I) + (s + I) = r + s + I$$

Wir definieren jetzt eine Multiplikation durch:

$$(r + I) \cdot (s + I) = rs + I$$

Die Definition hängt nicht von der Wahl der Repräsentanten ab, wie die folgende Rechnung mit Teilmengen von R zeigt:

$$(r + I)(s + I) = rs + Is + rI + II \subseteq rs + I$$

Die Assoziativität der Multiplikation und das Distributivgesetz auf R/I folgen nun aus den entsprechenden Gesetzen auf R und wir erhalten einen kanonischen surjektiven Homomorphismus $R \to R/I$. Wir nennen R/I den *Restklassenring* von R *modulo* I. Die Elemente von R/I werden *Restklassen* genannt. Wir sagen „r ist kongruent s modulo I“, falls $r + I = s + I$ gilt. Beim Rechnen modulo I können wir wie üblich zwischen Repräsentanten und Klassen hin und her wechseln.

Sei $\varphi : R \to S$ ein Ringhomomorphismus, dann ist der *Kern* $\ker(\varphi)$ definiert durch das Ideal $\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\}$ von R. Das *Bild* von φ ist der Unterring $\mathrm{im}(\varphi) = \{\varphi(r) \mid r \in R\}$ von S. Im Gegensatz zu $\mathrm{im}(\varphi)$ ist das Ideal $\ker(\varphi)$ nur dann ein Unterring, wenn $\mathrm{im}(\varphi) = \{0\}$ gilt. Analog zu Satz 1.9 kann man zeigen, dass I genau dann ein Ideal ist, wenn I der Kern eines Ringhomomorphismus $\varphi : R \to S$ ist. Dies sei dem interessierten Leser überlassen.

Beispiel 1.20. Für den Ringhomomorphismus $\varphi : \mathbb{R}^{\mathbb{R}} \to \mathbb{R} : f \mapsto f(0)$ gilt $\ker(\varphi) = \{f : \mathbb{R} \to \mathbb{R} \mid f(0) = 0\}$. Die Abbildungen mit einer Nullstelle bei 0 bilden damit ein Ideal in $\mathbb{R}^{\mathbb{R}}$. ◊

Es gibt Abbildungen zwischen Ringen, die nur Gruppenhomomorphismen bezüglich der Addition sind.

Beispiel 1.21. Betrachte den *Ableitungsoperator*

$$D : \{ f : \mathbb{R} \to \mathbb{R} \mid f \text{ ist differenzierbar } \} \to \mathbb{R}^{\mathbb{R}},\ f \mapsto f'$$

Dann gilt $(f + g)' = f' + g'$, aber D ist kein Ringhomomorphismus, denn der Kern $\ker(D) = \{f \mid f \text{ ist konstant}\}$ ist kein Ideal. ◊

Lässt sich für eine Teilmenge $S \subseteq I$ jedes Element $r \in I$ als endliche Summe $r = \sum_{s \in S} r_s s r'_s$ mit $r_s, r'_s \in R$ schreiben, wobei fast alle r_s, r'_s gleich 0 sind, so sagt man, dass I von S *erzeugt* wird. Existiert eine endliche erzeugende Menge, so heißt das Ideal *endlich erzeugt*. Ideale der Form $I = R \cdot r \cdot R$ für ein $r \in R$ nennt

man *Hauptideale*. In $\mathbb{Z}$ ist jedes Ideal ein Hauptideal, denn es wird von dem größten gemeinsamen Teiler über alle seine Elemente erzeugt. Jedes Ideal in $\mathbb{Z}$ hat also die Form $n\mathbb{Z}$ für eine natürliche Zahl $n \in \mathbb{N}$, siehe Satz 1.31. Der folgende Satz ist analog zum Homomorphiesatz der Gruppentheorie 1.11.

Satz 1.22 (Homomorphiesatz der Ringtheorie). *Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann induziert φ den Ringisomorphismus*

$$\begin{aligned} R/\ker(\varphi) &\to \operatorname{im}(\varphi) \\ r + \ker(\varphi) &\mapsto \varphi(r) \end{aligned}$$

Beweis. Die Menge $\varphi(r + \ker(\varphi))$ besteht genau aus dem einen Element $\varphi(r)$. Daher definiert $r + \ker(\varphi) \mapsto \varphi(r)$ einen Ringhomomorphismus. Aus Satz 1.11 folgt, dass dies eine Bijektion ist, und bijektive Ringhomomorphismen sind Isomorphismen. □

Aus dem Homomorphiesatz der Ringtheorie folgt leicht, dass Homomorphismen von endlichen Körpern in sich selbst bijektiv sind. Wir zeigen eine etwas allgemeinere Aussage.

Korollar 1.23. *Ringhomomorphismen von einem Körper in einen Ring mit $0 \neq 1$ sind injektiv. Insbesondere sind alle Homomorphismen zwischen Körpern injektiv.*

Beweis. Sei φ ein Homomorphismus und $\varphi(z) = 0$. Angenommen, es wäre $z \neq 0$. Dann würde $1 = \varphi(1) = \varphi(z^{-1}z) = \varphi(z^{-1}) \cdot \varphi(z) = \varphi(z^{-1}) \cdot 0 = 0$ gelten, was ausgeschlossen wurde. Also gilt $z = 0$, und damit ist $\ker(\varphi) = \{0\}$, was nach Satz 1.22 die Injektivität zeigt. □

Ein Ideal $M \subseteq R$ heißt *maximal*, falls $M \neq R$ und es kein Ideal I mit $M \subsetneq I \subsetneq R$ gibt. Man beachte, dass R selbst ein Ideal ist und damit das „größte“ Ideal R kein maximales Ideal von R ist.

Satz 1.24. *Ein Ideal $M \subseteq R$ in einem kommutativen Ring R ist genau dann maximal, wenn R/M ein Körper ist.*

Beweis. Sei $M \subseteq R$ maximal und $x + M \in R/M$ eine Restklasse mit $x \notin M$. Wir zeigen, dass $x + M$ in R/M invertierbar ist. Da M maximal und $x \notin M$ ist, folgt $M + xR = R$. Also finden wir eine Darstellung $m + xy = 1$ mit $m \in M$. Damit ist das Produkt xy kongruent zu 1 modulo M, und $y + M$ ist das multiplikative Inverse. Dies zeigt, dass jede Klasse $x + M$ aus R/M, die nicht dem Nullelement M entspricht, invertierbar ist. Also ist R/M ein Körper.

Sei jetzt R/M ein Körper. Dann ist $1 \notin M$, da $0 \neq 1$ in jedem Körper gilt. Sei $I \subseteq R$ ein Ideal mit $M \subsetneq I$ und $x \in I \setminus M$. Dann ist $x + M \neq 0 + M$ und da R/M ein Körper ist, existiert ein $r \in R$, so dass $(x + M) \cdot (r + M) = 1 + M$. Es folgt $1 \in xR + M$ und daher auch $R = xR + M \subseteq I$, da $xR + M$ ein Ideal ist. Dies zeigt $I = R$, und M ist maximal. □

In dem Ring $\mathbb{Z}$ entsprechen die maximalen Ideale $n\mathbb{Z}$ genau den Primzahlen in $\mathbb{N}$ und für eine natürliche Zahl $n \in \mathbb{N}$ ist der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.

Ein Element r eines Rings R heißt *Nullteiler*, falls ein $s \in R \setminus \{0\}$ existiert mit $rs = 0$ oder $sr = 0$. Beispielsweise ist 2 im Ring $\mathbb{Z}/6\mathbb{Z}$ ein Nullteiler. Ein Ring ist *nullteilerfrei*, wenn 0 der einzige Nullteiler ist. Nach dieser Definition gilt in nullteilerfreien Ringen $0 \neq 1$. Invertierbare Elemente sind keine Nullteiler. In jedem Ring $(R, +, \cdot, 0_R, 1_R)$ lassen sich ganze Zahlen $k \in \mathbb{Z}$ durch

$$k \cdot 1_R = \underbrace{1_R + \cdots + 1_R}_{k \text{ mal}}$$

interpretieren. Für eine ganze Zahl $k \in \mathbb{Z}$ schreiben wir daher auch $k \in R$ und meinen das Element $k \cdot 1_R$. In dieser Schreibweise ergeben sich für $0, 1 \in \mathbb{Z}$ z. B. die Identitäten $0 = 0_R \in R$ und $1 = 1_R \in R$. Es gibt jetzt zwei Fälle. Entweder alle positiven Zahlen sind in R von Null verschieden, oder es gibt eine kleinste positive Zahl n mit $n = 0$ in R. Im ersten Fall sagen wir, dass R die *Charakteristik* 0 hat, im zweiten Fall ist die Charakteristik n mit $n > 0$. In jedem Fall bezeichnen wir die Charakteristik von R mit $\operatorname{char}(R)$. Das Ideal $\operatorname{char}(R) \cdot \mathbb{Z}$ ist der Kern des Homomorphismus $\mathbb{Z} \to R,\ k \mapsto k \cdot 1_R$. Nach dem Homomorphiesatz der Ringtheorie 1.22 ist $\mathbb{Z}/\operatorname{char}(R)\mathbb{Z}$ isomorph zu einem Unterring von R. Aus der Definition der Charakteristik folgt, dass jeder Unterring S von R die gleiche Charakteristik hat wie R.

Lemma 1.25. *Sei R nullteilerfrei. Dann gilt* $\operatorname{char}(R) = 0$ *oder* $\operatorname{char}(R)$ *ist eine Primzahl.*

Beweis. Da R nullteilerfrei ist, ist sein Unterring $\mathbb{Z}/\operatorname{char}(R)\mathbb{Z}$ ebenfalls nullteilerfrei. Ein Ring $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}$ ist genau dann nullteilerfrei, wenn $n = 0$ oder n eine Primzahl ist. □

Körper sind nullteilerfrei und damit ist ihre Charakteristik entweder Null oder eine Primzahl. Körper mit Charakteristik Null enthalten $\mathbb{Z}$ als Unterring und damit können alle Brüche $\frac{r}{s} = rs^{-1}$ mit $r, s \in \mathbb{Z}$ und $s \neq 0$ interpretiert werden. Sie enthalten also die rationalen Zahlen $\mathbb{Q}$ als eindeutig bestimmten Unterkörper. Weitere Körper der Charakteristik Null sind z. B. $\mathbb{R}$, $\mathbb{C}$ oder auch $\{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\} \subsetneq \mathbb{C}$. Körper mit einer Primzahlcharakteristik p enthalten den Körper $\mathbb{Z}/p\mathbb{Z}$. Für einen nullteilerfreien Ring R gibt es also einen eindeutig bestimmten Unterkörper $\mathbb{Q}$ bzw. $\mathbb{Z}/p\mathbb{Z}$. Diesen nennen wir den *Primkörper* von R.

Der *Binomialkoeffizient* $\binom{x}{k}$ für $x \in \mathbb{C}$ und $k \in \mathbb{Z}$ ist definiert durch

$$\binom{x}{k} = \begin{cases} \frac{x \cdot (x-1) \cdots (x-k+1)}{k!} & \text{für } k \geq 0 \\ 0 & \text{für } k < 0 \end{cases}$$

Für $k \geq 0$ stehen über dem Bruchstrich genau k Faktoren; insbesondere steht für $k = 0$ sowohl über als auch unter dem Bruchstrich das leere Produkt, welches sich

zum neutralen Element 1 auswertet. Für $n, k \in \mathbb{N}$ ist damit $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$. Für alle $x \in \mathbb{C}$ und $k \in \mathbb{Z}$ gilt das *Additionstheorem*:

$$\binom{x}{k} = \binom{x-1}{k} + \binom{x-1}{k-1}$$

Dies sieht man wie folgt. Für $k < 0$ sind beide Seiten 0, und für $k = 0$ werten sich beide Seiten zu 1 aus. Sei also $k > 0$. Dann ist $\binom{x}{k} = \frac{x}{k}\binom{x-1}{k-1} = \frac{x-k}{k}\binom{x-1}{k-1} + \frac{k}{k}\binom{x-1}{k-1} = \binom{x-1}{k} + \binom{x-1}{k-1}$. Für $n \in \mathbb{N}$ gilt $\binom{n}{0} = \binom{n}{n} = 1$. Mit Induktion folgt nun aus dem Additionstheorem, dass der Binomialkoeffizient $\binom{n}{k}$ für $n, k \in \mathbb{N}$ stets ganzzahlig ist. Insbesondere lassen sich Binomialkoeffizienten für $n \in \mathbb{N}$ und $k \in \mathbb{Z}$ als Vielfaches des neutralen Elements 1_R in beliebigen Ringen R interpretieren.

Satz 1.26 (Binomialsatz). *Sei R ein kommutativer Ring. Für alle $x, y \in R$ und alle $n \in \mathbb{N}$ gilt $(x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k}$.*

Beweis. Die Summe auf der rechten Seite läuft dabei über alle $k \in \mathbb{Z}$, wobei aber fast alle Summanden Null sind. Durch diese Konvention gestalten sich Indexverschiebungen oft etwas einfacher. Der Beweis ist mit Induktion nach n. Für $n = 0$ steht auf beiden Seiten das neutrale Element 1_R. Sei nun $n > 0$. Dann gilt:

$$\begin{aligned}
(x+y)^n &= (x+y)(x+y)^{n-1} = (x+y)\sum_k \binom{n-1}{k} x^k y^{n-1-k} \\
&= \left(\sum_k \binom{n-1}{k} x^{k+1} y^{n-1-k}\right) + \left(\sum_k \binom{n-1}{k} x^k y^{n-k}\right) \\
&= \left(\sum_k \binom{n-1}{k-1} x^k y^{n-k}\right) + \left(\sum_k \binom{n-1}{k} x^k y^{n-k}\right) \\
&= \sum_k \left(\binom{n-1}{k-1} + \binom{n-1}{k}\right) x^k y^{n-k} = \sum_k \binom{n}{k} x^k y^{n-k}
\end{aligned}$$

□

Der Binomialsatz ist ein wichtiges Hilfmittel für die Betrachtung der Abbildung $r \mapsto r^p$ in kommutativen Ringen.

Satz 1.27. *Sei R ein kommutativer Ring mit Primzahlcharakteristik p. Dann definiert $r \mapsto r^p$ einen Ringhomomorphismus.*

Beweis. Es gilt $1^p = 1$ und $(rs)^p = r^p s^p$. Es bleibt zu zeigen $(r+s)^p = r^p + s^p$. Nach dem Binomialsatz gilt $(r+s)^p = \sum_k \binom{p}{k} r^k s^{p-k}$. Alle Binomialkoeffizienten $\binom{p}{k}$ für $1 \le k \le p-1$ sind durch p teilbar. Da R die Charakteristik p hat, sind diese Binomialkoeffizienten alle Null in R. Es folgt $(r+s)^p = \binom{p}{0} r^0 s^p + \binom{p}{p} r^p s^0 = s^p + r^p$. □

Den Homomorphismus aus Satz 1.27 bezeichnet man als den *Frobenius-Homomorphismus* nach Ferdinand Georg Frobenius (1849–1917). Er ist vor allem für Körper

interessant, denn in diesem Fall ist er nach Korollar 1.23 injektiv und bei endlichen Körpern damit notwendigerweise bijektiv. Als Anwendung von Satz 1.27 beweisen wir den kleinen Satz von Fermat. Insbesondere ist der Frobenius-Homomorphismus auf Primkörpern die Identität.

Satz 1.28 (Kleiner Satz von Fermat für Ringe). *Es sei R ein kommutativer Ring mit Primzahlcharakteristik p und $a \in \mathbb{Z}$ eine ganze Zahl. Dann gilt in R:*

$$a^p = a$$

Beweis. Für $p = 2$ gilt $-1 = 1$ in R. Daher gilt $(-a)^p = (-1)^p a^p = -a^p \in R$ für alle Primzahlen p. Es reicht also $a \in \mathbb{N}$ zu betrachten. Wir zeigen die Aussage mit Induktion. Für $a = 0$ gilt die Aussage. Betrachte nun $(a+1)^p = a^p + 1^p = a+1 \in R$. Die erste Gleichheit folgt aus Satz 1.27, die zweite gilt nach Induktion. □

Insbesondere gilt in der Situation von Satz 1.28 für Elemente $a \in \mathbb{Z}$, welche in R invertierbar sind, die Gleichung $a^{p-1} = 1$ in R.

1.5 Modulare Arithmetik

Den *größten gemeinsamen Teiler* von zwei ganzen Zahlen k und ℓ bezeichnen wir mit $\mathrm{ggT}(k, \ell)$; es ist die größte natürliche Zahl, die sowohl k als auch ℓ teilt. Den größten gemeinsamen Teiler von k und 0 definieren wir als die Zahl $|k|$. Zwei Zahlen heißen *teilerfremd*, wenn ihr größter gemeinsamer Teiler 1 ist. Für das Rechnen im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ hat sich für ganze Zahlen k, ℓ und n die Schreibweise

$$k \equiv \ell \mod n$$

etabliert; sie bedeutet nichts anderes als $k + n\mathbb{Z} = \ell + n\mathbb{Z}$. Wir sagen dann, k ist kongruent ℓ modulo n. Es gilt genau dann $k \equiv \ell \bmod n$, wenn sich k und ℓ um ein Vielfaches von n unterscheiden. Mit $k \bmod n$ meinen wir die eindeutig bestimmte Zahl $r \in \{0, \ldots, |n| - 1\}$ mit $k \equiv r \bmod n$. Häufig zieht man $k \bmod n$ als Repräsentant der Restklasse $k + n\mathbb{Z}$ heran. Mit $(\mathbb{Z}/n\mathbb{Z})^*$ bezeichnen wir die Gruppe der *Einheiten* des Rings $\mathbb{Z}/n\mathbb{Z}$. Dies sind die Restklassen, die ein multiplikatives Inverses besitzen.

1.5.1 Der euklidische Algorithmus

Der *euklidische Algorithmus* (Euklid von Alexandria, Wirken um 300 v. Chr.) ist ein effizientes Verfahren zur Berechnung des größten gemeinsamen Teilers. Da $\mathrm{ggT}(k, \ell) = \mathrm{ggT}(-k, \ell) = \mathrm{ggT}(\ell, k)$ gilt, genügt es natürliche Zahlen k und ℓ zu betrachten. Sei $0 < k \leq \ell$ und schreibe $\ell = qk + r$, wobei $0 \leq r < k$ der *Rest* ist. Es gilt $r = \ell \bmod k$. Jede Zahl, die k und den Rest r teilt, teilt auch die Summe $\ell = qk + r$. Jede Zahl, die