Elementare Galois-Theorie

Marc Nieper-Wißkirchen

Elementare Galois-Theorie

Ein konstruktiver Zugang

Springer Spektrum

Marc Nieper-Wißkirchen
Lehrstuhl Algebra & Zahlentheorie
University of Augsburg
Augsburg, Deutschland

ISBN 978-3-662-60933-0 ISBN 978-3-662-60934-7 (eBook)
https://doi.org/10.1007/978-3-662-60934-7

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

Planung/Lektorat: Iris Ruhmann
Springer Spektrum ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Für Konrad, Karla und Irmgard

Vorwort

Die galoissche Theorie, welche mit einigem Recht sicherlich zu den Perlen der reinen Mathematik gezählt werden kann, nimmt eine zentrale Stellung in den Algebrakursen für Bachelor- oder Lehramtsstudenten in Mathematik ein.

Ausgangspunkt ist die Frage, ob sich Lösungen von Polynomgleichungen mithilfe von Wurzelausdrücken beschreiben lassen können. Dazu werden Symmetrien zwischen den Lösungen einer solchen Gleichung untersucht. Es zeigt sich, dass aus diesen Symmetrien wesentliche Informationen über das Polynom erhalten werden können und dass diese insbesondere Antworten auf die ursprüngliche Frage nach der Auflösbarkeit durch Wurzeln geben.

Der Stellenwert der galoisschen Theorie ist auch deswegen so hoch, weil sich aus ihr die drei wichtigsten Strukturen der Algebra entwickelt haben: Die Symmetrien der Lösungen einer Gleichung lassen sich zu einer *Gruppe* zusammenfassen. Die Koeffizienten der Polynomgleichungen nehmen Werte in einem *Körper* an, etwa den rationalen oder den komplexen Zahlen. Schließlich bilden die Polynome in ihrer Gesamtheit einen *Ring,* welcher in vielerlei Hinsicht Ähnlichkeiten mit dem Ring der ganzen Zahlen hat.

Ziel dieses Buches ist es, ohne Verwendung höherer Konzepte einen elementaren, klassischen Einstieg in die galoissche Theorie zu vermitteln und dabei gleichzeitig die Früchte der Theorie in Form von Anwendungen auf Jahrtausende alte Probleme zu ernten.

Der Stoff dieses Bandes ist so konzipiert, dass er im Rahmen einer einsemestrigen Algebravorlesung auch direkt schon zu Beginn des Studiums behandelt werden kann. Da es um die Grundlagen der Theorie geht, ist die gesamte behandelte Materie relevant für (Staatsexamens-)Prüfungen in Algebra.

Im Anhang sind für die Algebra wichtige Ergebnisse aus der Linearen Algebra und der Analysis zusammengestellt. Dieses Material bietet sich natürlich besonders an, wenn dieses Buch Grundlage einer Erst- oder Zweitsemestervorlesung ist oder im Selbststudium durchgearbeitet wird.

Das Buch wird durch einen zweiten Band fortgesetzt werden, in dem die modernere, abstraktere Sichtweise auf die galoissche Theorie betont wird und die abstrakten

Strukturen Gruppe, Ring und Körper motiviert, definiert und dann im Detail studiert werden.

Was den vorliegenden Band betrifft, ist darauf Wert gelegt worden, dass auch das alleinige Studium dieses Buches einen wesentlichen Beitrag für die mathematische Allgemeinbildung eines interessierten Laiens oder eines Studenten liefert, welcher sich nicht weiter in den Bereich der Algebra vertiefen möchte.

Es sind schon viele einführende Lehrbücher der Algebra und speziell über die galoissche Theorie geschrieben worden. Der Autor dieses Buches hat zum Beispiel viel aus dem Buch von Serge Lang [4] gelernt, und auch in deutscher Sprache gibt es viele bewährte Lehrbücher wie zum Beispiel das von Siegfried Bosch [1]. Was sind also die Besonderheiten des vorliegenden Buches, dessen Inhalt auch Grundlage von Vorlesungen des Autors ist?

Eine Reihe von Prinzipien sind bei der Erstellung der „Galois-Theorie“ verfolgt worden:

Abstrakte Theorien und Definitionen werden aus konkreten Problemstellungen und Lösungen abgeleitet und nicht umgekehrt das Konkrete als Spezialfall des Abstrakten angesehen. Auch wenn die abstrakte Theorie am Ende das ist, was die eigentliche Weiterentwicklung der Mathematik darstellt, kann sie doch nur mit Wissen des ursprünglichen konkreten Rahmens ausreichend gewürdigt und verstanden werden.

Weiter besteht bei jeder fortschrittlichen mathematischen Theorie die Gefahr, dass die großen Sätze am Ende zwar elegant aus einer Kette von Abstraktionen und Lemmata folgen, der eigentliche Grund für ihre Wahrheit aber nicht mehr gesehen wird. Erklärtes Ziel des Buches ist es daher auch, dafür zu sorgen, dass der rote Faden im Kopf des Lesers nicht abreißt und dieser zu jeder Zeit in der Lage ist, jemandem, der die Theorie nicht kennt, zumindest grob erklären zu können, was die Inhalte der Theorie sind, und ungefähre Begründungen für ihre Aussagen liefern zu können. In dieser Hinsicht wichtig ist dem Autoren auch, dass schon frühzeitig auf Anwendungen der Theorie eingegangen wird und nicht erst am Ende, nachdem ein riesiges Theoriegebäude scheinbar unmotiviert hochgezogen worden ist.

Das vorliegende Buch enthält drei Elemente, die unterstützen sollen, dieses selbstgesteckte Ziel auch zu erreichen:

Erstens wird der Fließtext regelmäßig durch grau unterlegte Boxen unterbrochen. In diesen Boxen werden schlagwortartig jeweils wichtige Tatsachen aus dem Haupttext aufgegriffen. Zum einen sollen sie beim ersten Lesen dazu anregen, innezuhalten und zu reflektieren, ob die wesentlichen Punkte des eigentlichen Inhalts verstanden worden sind; zum anderen erlauben sie bei der (Prüfungs-)Wiederholung, sich auf die wichtigsten Punkte fokussieren zu können.

Zweitens gibt es am Ende der jeweiligen Kapitel grau unterlegte Zusammenfassungen in Form von Aufzählungslisten. In diesen Zusammenfassungen werden noch einmal Schritt für Schritt die wesentlichen mathematischen Argumente des jeweiligen Kapitels nachvollzogen.

Drittens schließen sich jeweils zahlreiche Übungsaufgaben an diese Zusammenfassungen an. Denn es ist die überzeugte Meinung des Autors, dass Mathematik genauso wenig wie Schwimmen oder das Spielen eines Instrumentes nur durch das passive Studium eines Buches gelernt werden kann. Das Niveau der Übungsaufgaben beginnt absichtlich bei sehr einfachen Fragen. Anhand dieser ist eine einfache Überprüfung des Lernerfolges möglich. Das Niveau der Aufgaben steigt jeweils an und geht hin bis zu schweren Kopfnüssen, die auch die Begnadeten unter den Lesern animieren sollen.

Etwas, wovon sich dieses Buch von den meisten, wenn auch nicht von allen Lehrbüchern der Algebra – wir denken da an das von Harold Edwards [3] – unterscheidet, ist, dass konsequent der Standpunkt eines konstruktiven Mathematikers eingenommen worden ist:

Konstruktive Mathematik heißt Folgendes: Um die Existenz eines mathematischen Objektes zu beweisen, ist eine Konstruktionsvorschrift für dieses anzugeben. Ein abstrakter Existenzbeweis ohne Angabe einer solchen Konstruktionsvorschrift wird abgelehnt.

Damit muss zwar auf das Gesetz des ausgeschlossenen Dritten und das Auswahlaxiom, welche beide nicht konstruktiv sind, verzichtet werden (das heißt, die klassische Logik muss durch die intuitionistische ersetzt werden), allerdings erlaubt dies nicht nur eine schärfere Sicht auf die Dinge, sondern verhindert auch, dass wir Aussagen ableiten, welche zwar logische Konsequenz der Axiome sind, aber für sich genommen keine praktische Relevanz haben:

So besagt der klassische Fundamentalsatz der Algebra, dass jede nichttriviale Polynomgleichung über den komplexen Zahlen eine Nullstelle hat. Jedoch gibt es kein allgemeines Verfahren, eine solche Nullstelle zu berechnen, was im Wesentlichen daran liegt, dass es für eine beliebige komplexe Zahl unentscheidbar ist, ob sie verschwindet oder nicht.

Viele heutige Mathematiker kommen im Laufe ihrer Ausbildung mit konstruktiver Mathematik nicht in Berührung und empfinden Konstruktivismus oder intuitionistische Logik vielleicht als esoterische Mathematik. Dem ist allerdings vehement zu widersprechen: Zum einen ist jede konstruktiv bewiesene Aussage auch klassisch (d. h. nicht konstruktiv) wahr; zum anderen kann jeder klassische Beweis einer Aussage in einen konstruktiven einer entsprechend umformulierten Aussage übersetzt werden. Außerdem taucht intuitionistische Logik auch in der klassischen Mathematik auf, etwa beim Studium von Garben über einem topologischen Raum.

Im Gegensatz zu anderen Büchern über konstruktive Algebra wie etwa [5] wird in diesem Buch der konstruktive Standpunkt jedoch nicht betont. Jemandem, dem der Konstruktivismus bisher fremd gewesen ist und der dieses Buch liest, wird im Wesentlichen auffallen, dass einige Aussagen etwas vorsichtiger als klassisch üblich formuliert sind – so werden wir den Fundamentalsatz der Algebra nur für Gleichungen beweisen, deren Koeffizienten algebraische Zahlen sind (in diesem Falle gibt es nämlich ein effektives Verfahren, Nullstellen zu finden!) – und vielleicht, dass einige Beweise zwar aufwendiger, dafür aber mit größerer Klarheit geführt worden sind.

Genug der Vorrede, jetzt kommt die Algebra zu Wort. Ich wünsche viel Spaß beim Stöbern und Durcharbeiten der Kapitel (Abb. 1).

Abb. 1 Évariste Galois, 25.10.1811–31.05.1832 [2]

Augsburg
Februar 2020

Marc Nieper-Wißkirchen

Literatur

1. Bosch S (2009) Algebra. (Algebra.), 7th revised Aufl. Springer-Lehrbuch, Berlin
2. Dupuy P (1896) La vie d'Évariste Galois. Annales scientifiques de l'École Normale Supérieure, 3(13):197–266
3. Edwards HM (1984) Galois theory. Graduate texts in mathematics, 101. Springer, New York
4. Lang S (2002) Algebra, 3rd revised Aufl. Graduate texts in mathematics, 211. Springer, New York
5. Mines R, Richman F, Ruitenburg W (1988) A course in constructive algebra. Universitext. Springer, New York

Danksagungen

Dieses Buch basiert auf Vorlesungen zur Einführung in die Algebra, die ich unter anderem im Wintersemester 2010 und im Sommersemester 2013 an der Universität Augsburg gehalten habe. Das Buch wäre ohne die hilfreichen Kommentare und Verbesserungsvorschläge der Hörerinnen und Hörer dieser Vorlesungen in dieser Form sicherlich nicht zustande gekommen, sodass mein Dank ihnen allen, insbesondere aber Frau Caren Schinko, Frau Gesa Scupin und Herrn Moritz Meisel gebührt. Außerdem möchte ich den Herren Franz Vogler und Ingo Blechschmidt danken, die als Assistenten zu den beiden Vorlesungen wertvolle Hinweise gegeben haben und die Übungsaufgaben in der Praxis erprobt haben. Zudem hat Herr Blechschmidt die den Beweisen in diesem Buch zugrunde liegenden Algorithmen im Rahmen eines Softwareprojektes in die Programmiersprache Haskell praktisch umgesetzt.

Inhaltsverzeichnis

Symbole

A_n	Alternierende Gruppe
C	Bereich der komplexen Zahlen
C_n	Zyklische Gruppe
D_n	Dieder-Gruppe
$e_k(X_1,\ldots,X_n)$	Elementarsymmetrische Funktion
$G\sigma$	Zentralisator des Gruppenelementes σ
$[G:1]$	Gruppenordnung
$[G:G\sigma]$	Anzahl der zu σ konjugierten Gruppenelemente
$[G:H]$	Index einer Untergruppe
$\mathrm{Gal}_K(x_1,\ldots,x_n)$	Galoissche Gruppe
$\mathrm{Gal}_Q(x_1,\ldots,x_n)$	Galoissche Gruppe über den rationalen Zahlen
ggT	Größter gemeinsamer Teiler
$H \cdot N$	Komplexprodukt einer Untergruppe mit einem Normalteiler
$K[X]$	Bereich von Polynomen in der Unbestimmten X
$K[X_1,\ldots,X_n]$	Bereich von Polynomen in den Unbestimmten $X_1,\ldots,X_n$
$K(x_1,\ldots,x_n)^{\sigma_1,\ldots,\sigma_m}$	Invarianten unter der galoisschen Wirkung
$\Phi_n(X)$	Kreisteilungspolynom
$\mathbf{Q}$	Bereich der rationalen Zahlen
$\bar{\mathbf{Q}}$	Bereich der algebraischen Zahlen
$\mathbf{Q}_+$	Menge der positiven rationalen Zahlen
$\mathbf{Q}(t_1,\ldots,t_n)$	Menge der in $t_1,\ldots,t_n$ rationalen Zahlen
$\mathbf{Q}[X]$	Bereich der Polynome mit rationalen Koeffizienten in der Unbestimmten X
$\mathbf{Q}[X_1,\ldots,X_n]$	Bereich der Polynome mit rationalen Koeffizienten in den Unbestimmten $X_1,\ldots,X_n$
$\mathbf{R}$	Bereich der reellen Zahlen
S_n	Permutationsgruppe
sgn σ	Signum einer Permutation
Z	Bereich der ganzen Zahlen
ζ_n	Primitive Einheitswurzel
V_4	Kleinsche Vierergruppe