

Bücher und Computersoftware

Objektyp: **Group**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **48 (1993)**

PDF erstellt am: **25.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

<http://www.e-periodica.ch>

Bücher und Computersoftware

J. H. Silverman, J. Tate: Rational Points on Elliptic Curves. 34 Abb., 281 Seiten, DM 58,-. Undergraduate Texts in Mathematics, Springer-Verlag 1992; ISBN 3-540-97825-9.

Im hier zu besprechenden Werk führen J. Silverman und J. Tate den Leser mit elementarsten Methoden in die interessanten und tiefliegenden Ergebnisse der Arithmetik über den rationalen Zahlen definierter elliptischer Kurven ein. Wir fassen im Folgenden kurz den Inhalt dieses Buches, welcher in sechs Kapitel und einen Anhang gegliedert ist, zusammen.

Im ersten Kapitel werden zunächst Geraden und Kurven zweiten Grades in der projektiven Ebene betrachtet. Danach wird ausführlich die Geometrie ebener, nicht-singulärer kubischer Kurven

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \tag{1}$$

$(a, b, c, d, e, f, g, h, i, j \in \mathbb{Q})$

diskutiert; dabei wird auf den Kubiken (1) eine kommutative Gruppenstruktur eingeführt. Damit ist der Hauptgegenstand des Buches, die elliptische Kurve, definiert. Indem die Autoren geschickt die Intuition des Lesers ansprechen, gelingt es ihnen, dieses Thema mit einem Minimum an Kenntnissen aus der Theorie algebraischer Kurven zu behandeln. Diejenigen, welche eine mathematisch präzise Diskussion des Sachverhalts wünschen, finden diese im Anhang am Schluss des Buches. Zum Abschluss des Kapitels werden die Weierstrass'sche Normalform

$$y^2 = x^3 + ax^2 + bx + c \tag{2}$$

$(a, b, c \in \mathbb{Z})$

einer elliptischen Kurve C/\mathbb{Q} und explizite Formeln zur Gruppenstruktur (Additionstheorem) hergeleitet.

In den folgenden Kapiteln interessieren nun die rationalen Lösungen (x, y) von (2); dazu wird die abelsche Gruppe $C(\mathbb{Q})$ der rationalen Punkte von C untersucht. Im zweiten Kapitel wird der Satz von Nagell-Lutz bewiesen, welcher besagt, dass die Elemente (x, y) endlicher Ordnung von $C(\mathbb{Q})$ sogar ganz sind, d.h. $x, y \in \mathbb{Z}$ erfüllen. Im dritten Kapitel folgt ein Beweis des Satzes von Mordell, welcher zeigt, dass die Gruppe $C(\mathbb{Q})$ eine endlich erzeugte abelsche Gruppe ist. Der Beweis ist äusserst übersichtlich gegliedert, und die wesentlichen Beweisideen (siehe z.B. "Descent Theorem", p. 65) werden klar hervorgehoben; um den Aufwand gering zu halten, muss allerdings die (unwesentliche) Einschränkung $c = 0$ gemacht werden. Illustrativ sind die Beispiele am Ende dieses Kapitels, bei denen der Rang der Gruppe $C(\mathbb{Q})$ bestimmt wird.

Im vierten Kapitel werden elliptische Kurven C über dem endlichen Körper \mathbb{F}_p (p eine ungerade Primzahl) betrachtet. Bezeichnet N_p die Anzahl der Elemente von $C(\mathbb{F}_p)$, d.h. die Anzahl der Lösungen von (2) modulo p plus den "unendlich fernen" Punkt, so gilt nach Hasse die Abschätzung

$$|N_p - (p + 1)| \leq 2\sqrt{p}.$$

Stellvertretend für dieses Ergebnis wird folgender Satz von Gauss bewiesen. Die Anzahl M_p der projektiven Lösungen der Gleichung

$$x^3 + y^3 + z^3 = 0$$

mit $x, y, z \in \mathbb{F}_p$ ist im Fall $p \equiv 1 \pmod{3}$ wie folgt gegeben: Es gibt eindeutig bestimmte ganze Zahlen A, B mit

$$A \equiv 1 \pmod{3}, 4p = A^2 + 27B^2,$$

so dass

$$M_p = p + 1 - A$$

gilt. Am Ende des Kapitels wird kurz auf den Nutzen elliptischer Kurven C/\mathbb{F}_p in der Kryptographie hingewiesen.

Im fünften Kapitel wird der Satz von Siegel, dass nämlich die Anzahl der *ganzzahligen* Lösungen (x, y) von (2) endlich ist, diskutiert. Der Beweis wird anhand des Beispiels

$$ax^3 + by^3 = c \quad (a, b, c \in \mathbb{Z} \setminus \{0\})$$

illustriert. Dabei werden systematisch die Methoden der diophantischen Approximation (Konstruktion eines "kleinen" nicht-trivialen Hilfspolynoms) entwickelt.

Im sechsten Kapitel wird ein neuer Themenkreis angeschnitten. Es geht um die Konstruktion abelscher Erweiterungen quadratischer Zahlkörper mit Hilfe von elliptischen Kurven mit komplexer Multiplikation. Es wird gezeigt, dass man durch Adjunktion (der Koordinaten) der n -Torsionspunkte $C[n]$ der Kurve

$$C : y^2 = x^3 + x$$

abelsche Erweiterungen $\mathbb{Q}(C[n])$ von $\mathbb{Q}(i)$ erhält.

Dieser hervorragende Band der Reihe "Undergraduate Texts in Mathematics" ist einem Publikum zu empfehlen, das sich ohne grosse Vorkenntnisse in ein aktuelles Gebiet der Zahlentheorie einarbeiten möchte. Für den Dozenten bietet die ausgezeichnete Darstellung der ausgewählten Kapitel und Übungsaufgaben wertvolle Anregungen zur eigenen Unterrichtstätigkeit.

J. Kramer, Zürich

Kunz, Ernst: Algebra. 254 pages, DM 36,-. Vieweg Studium, Aufbaukurs Mathematik, Vol. 43. 1991. ISBN 3-528-07243-1.

This book gives a concrete and attractive introduction to algebra. Most algebra textbooks start by discussing the fundamental concepts of algebra (groups, rings, fields, ...) and then present some examples and applications. By contrast, this book starts with some of the concrete problems that motivated the development of modern algebra: ruler and compass constructions, solution of algebraic equations. This way, the abstract algebraic concepts appear in a natural and motivated way. The book also contains many interesting exercises.

The contents of the book are as follows: ruler and compass constructions, solution of algebraic equations, algebraic and transcendental field extensions, divisibility in rings, irreducibility criteria, ideals and residue fields, separable and inseparable algebraic extensions, normal and Galois extensions, the main theorem of Galois theory, group theory, cyclotomic fields, finite fields, solution of algebraic equations by radicals.

The prerequisites for reading this book are: linear algebra, basic facts on groups and rings.

Eva Bayer Fluckiger, Besançon.

Egorov, Yu. V. and Shubin, M.A. (Eds.): Partial Differential Equations I. 250 Seiten, DM 128,-. Encyclopedia of Math. Sciences, Vol 30; Springer Verlag 1991. ISBN 3-540-52002-3.

Auf knappem Raum tragen Egorov und Shubin sehr viel Grundsätzliches und Wesentliches aus der Theorie der partiellen Differentialgleichungen zusammen, angefangen von der Klassifikation partieller Differentialgleichungen, den Sätzen von Cauchy-Kovalevskaya und Holmgren, der Lösung von Gleichungen mit konstanten Koeffizienten mittels Fouriertransformation und Distributionen über elliptische Randwertprobleme und Sobolevräume bis hin zu Evolutionsproblemen, Außenraumproblemen und Streutheorie. Die Konzepte werden anhand einfacher Beispiele gut verständlich erklärt und ein ausgezeichneter Überblick über den Stand der Technik in den einzelnen Teilgebieten dieses überaus umfangreichen Themas vermittelt.

Das Buch bereitet Freude beim Lesen und weckt die Neugier für vertiefte Studien. Dabei stößt man dann auf den vielleicht einzigen Mangel aus der Sicht dieses Lesers: Die zahlreichen Hinweise auf russische Lehrbücher und Übersichtsartikel sind zwar für das Zielpublikum der russischen Originalausgabe als Referenz sehr nützlich; im Westen sind diese Publikationen hingegen wohl kaum zu finden, und der Leser ist auf vergleichsweise wenige Standardwerke verwiesen.

Michael Struwe, Zürich

Robert Ineichen/Hansjürg Stocker: Stochastik; Einführung in die elementare Statistik und Wahrscheinlichkeitsrechnung. 8. überarbeitete Auflage, 164 Seiten. Rieber Verlag, Luzern und Stuttgart, 1992; ISBN 3-7239-0042-9.

Ein Lehrbuch, das über Jahrzehnte hinweg sein Grundkonzept beibehalten kann, ist ein besonderer Glücksfall in der heutigen Lehrmittellandschaft. Dem Autor Robert Ineichen gelang es, ein Buch der Stochastik zu schreiben, das noch heute modernen Anforderungen des Unterrichts gerecht wird. Er verstand es, bei Neuauflagen stets sein Lehrbuch zu aktualisieren und später zusammen mit Hansjürg Stocker massvoll zu überarbeiten. Der Zeit entsprechend erhielt das Buch bei der 8. Auflage einen grünen Farbtupfer. Zudem wurden einige Beispiele und Aufgaben ersetzt.

Mit dem Lehrmittel können Schülerinnen und Schüler die Grundlagen der Stochastik selbständig erarbeiten. Es lässt zudem Lehrerinnen und Lehrer einen grossen Freiraum für die persönliche Gestaltung der Lektionen. Das Studium der Begriffe, die mit vielen Beispielen aus dem breiten Anwendungsbereich veranschaulicht werden, ist anregend und zeigt deutlich die grosse Bedeutung der Stochastik als wissenschaftliches Werkzeug. Besonders geglückt ist die Entwicklung der mathematischen Modelle aus realen Problemen; ein Vorgehen, das an allgemeinbildenden Schulen nicht nur wünschbar, vielmehr geradezu unabdingbar ist. Die Strukturtafel am Anfang des Buches erleichtert jungen Lehrerinnen und Lehrern die Auswahl für einen Grundkurs; diese zeigt nämlich graphisch geschickt die Zusammenhänge und Erweiterungsmöglichkeiten der Themenbereiche auf.

Gegliedert ist das Buch in vier Kapitel: Einführung in die beschreibende Statistik, Einführung in die Wahrscheinlichkeitsrechnung, Ausbau der Wahrscheinlichkeitsrechnung, Von der Normalverteilung.

Einführung in die beschreibende Statistik. Die Grundbegriffe der elementaren Statistik werden leicht verständlich dargestellt, mit wesentlichen Beispielen illustriert und durch ein reichhaltiges Aufgabenmaterial ergänzt. Bei der Arbeit mit diesem Lehrmittel kann man immer wieder feststellen, dass die Vielfalt der Probleme Schülerinnen und Schüler zu eigenen originellen Untersuchungen animiert. Eines Hinweises bedarf das Kleingedruckte: Dieses ist wie in andern Bereichen äusserst wichtig und sollte sorgfältig studiert werden. Nur ein kleiner Wunsch bleibt in diesem Kapitel offen: Würde der Abschnitt 4.2 Regressionsrechnung ergänzt mit der elementaren Herleitung der optimalen Schätzwerte, könnte dieses Thema viel früher behandelt werden.

Einführung in die Wahrscheinlichkeitsrechnung. Didaktisch hervorragend gestaltet ist die schrittweise Einführung der Begriffe der Wahrscheinlichkeitsrechnung. Das Axiomensystem von Kolmogoroff wird anschaulich erarbeitet, und die Grundlagen werden bis zur bedingten Wahrscheinlichkeit — durch praktische Beispiele motiviert — erweitert. Dabei wird erfreulicherweise auf die Kombinatorik verzichtet, die Schülerinnen und Schülern das Verstehen erschweren kann. Sie wird erst im 2. Kapitel ausführlich behandelt. Abgeschlossen wird dieser Abschnitt mit Anwendungen aus der Technik, der Genetik und der Physik. Hier und im Aufgabenteil sind echte Perlen der Stochastik zu finden. Die historischen Anmerkungen verdienen ebenfalls Beachtung. Sie zeigen die tiefen Kenntnisse von R. Ineichen, die im Unterricht ausgenützt werden sollten.

Ausbau der Wahrscheinlichkeitsrechnung. Das Kapitel setzt folgende Schwerpunkte: Testen einer Hypothese, Masszahlen von diskreten Verteilungen, Satz von Bernoulli — Ein Gesetz der grossen Zahlen. Alle diese Themen wären für das tiefere Verständnis der Stochastik notwendig; die Praxis wird jedoch Lehrerinnen und Lehrer zwingen, eine vernünftige Auswahl zu treffen, die im Unterricht sorgfältig zu studieren ist.

Von der Normalverteilung. Im Schlusskapitel wird ein Einblick in das Gebiet der stetigen, normalverteilten Zufallsvariablen gegeben. Das Angebot befriedigt mit Bestimmtheit das, was in diesem Bereich der Stochastik am Gymnasium noch behandelt werden kann.

Das Buch wird abgerundet durch einen Anhang mit den Lösungen der Aufgaben, einer Tabelle mit Zufallszahlen und einer Wertetafel zur Normalverteilung.

Fazit. Die Stochastik von Robert Ineichen und Hansjürg Stocker ist ein aussergewöhnliches Buch und ein in jeder Hinsicht überzeugendes Lehrmittel, das Schülerinnen und Schülern einen leichten Einstieg in einen interessanten und wesentlichen Mathematikbereich ermöglicht. Darüber hinaus erhalten selbst erfahrene Lehrerinnen und Lehrer immer wieder neue Anregungen für den Unterricht.

E. Holzherr