

Vorwort zur zweiten Auflage

Ich freue mich, dass die zweite Auflage schon ein Jahr nach dem Erscheinen der erste Auflage möglich wurde. Dies gab mir die Gelegenheit, einige Fehler zu korrigieren und den Text in Teilen umzuformulieren. Dabei habe ich Anregungen gerne aufgegriffen und hoffe, dass Studierende und mathematisch Interessierte nun noch besser endliche Körper verstehen und anwenden können.

Von Kollegen erfuhr ich, dass sie dieses Buch auch als Leitfaden für eine elementare Einführung in die Algebra verwenden. Die Grundbegriffe der Algebra dienen hier nämlich einem klaren und greifbaren Ziel: Die Bestimmung der endlichen Körper.

Ich würde mich sehr freuen, wenn Mathematiker wie „Anwender“ gleichermaßen mit dem vorliegenden Buch ihre Freude an diesem aktuellen mathematischen Thema entdecken würden.

Erlangen,
Juli 2008

Hans Kurzweil

Einleitung

Ein endlicher Körper \mathbb{F} ist ein Zahlbereich mit nur endlich vielen Zahlen, in dem die vier Grundrechnungsarten ausgeführt werden können, man kann addieren, subtrahieren, multiplizieren und dividieren. Dabei ist die Anzahl $|\mathbb{F}|$ der Elemente immer eine Primzahlpotenz p^n . Man nennt \mathbb{F} auch *Galoisfeld*, und schreibt

$$\mathbb{F} = \text{GF}(p^n)$$

nach Evariste Galois (1811–1832), der zum ersten Mal solche Zahlbereiche angegeben hat.¹

Bekanntlich hat eine komplexe Zahl ($\in \mathbb{C}$) die Form

$$a_0 + a_1 i \quad \text{mit} \quad a_0, a_1 \in \mathbb{R}, \quad 1 + i^2 = 0;$$

hier ist i die imaginäre Einheit, $i^2 = -1$. Ausgehend von dieser Darstellung definiert Galois $\text{GF}(p^n)$ als die Menge aller Ausdrücke der Form

$$a_0 + a_1 i + a_2 i^2 + \dots + a_{n-1} i^{n-1}.$$

Hier sind die Koeffizienten a_0, a_1, \dots, a_{n-1} ganze Zahlen, die modulo einer Primzahl p gerechnet werden, und die „imaginäre“ Zahl $i \in \mathbb{F}$ genügt einer Gleichung

$$b_0 + b_1 i + \dots + b_{n-1} i^{n-1} + i^n = 0.$$

Dabei ist diese Relation *minimal*, d. h. sie gilt für keine kleinere natürliche Zahl m anstelle von n ; Galois spricht von einer *irreduziblen Kongruenz*.

Diese exotischen Zahlen waren lange Zeit nur aus innermathematischen Gründen von Interesse, ganz im Gegensatz zu den komplexen Zahlen, die von Anfang an via Differential- und Integralrechnung in Anwendungen der Mathematik unentbehrlich waren. Die innermathematische Sicht bettet die Theorie der endlichen Körper als Spezialfall in die sogenannte *Erweiterungstheorie* von Körpern ein, so dass in Lehrbüchern der Algebra endliche Körper nur auf ganz wenigen Seiten abgehandelt werden, und zwar mit einer dem allgemeinen Fall angemessenen „Maschinerie“, welche aber den direkten Zugang für den Nicht-Fachmann erschwert.

Mit dem Aufkommen der digitalen Datenverarbeitung hat sich die Situation geändert. Der Computer ist ein *diskretes* Werkzeug, d. h. er kann endlich viele Zeichen in einer endlichen Zeit bearbeiten; er kann mit diesen Zeichen exakt

¹E. Galois: SUR LA THÉORIE DES NOMBRES, Bulletin des sciences mathématiques de Férussac XIII, 1830, § 218

rechnen, wenn sie mit den Elementen eines Galoisfelds $\text{GF}(p^n)$ identifiziert werden können. Zum Beispiel besteht $\text{GF}(2)$ aus den bits 0, 1 und $\text{GF}(2^8)$ aus *Bytes* – acht bits definieren ein Byte.

Ich skizziere ein typisches Beispiel aus der Nachrichtenübertragung. Es liegt ein „Alphabet“ mit $2^8 = 256$ Zeichen (Buchstaben) vor, welche als Bytes interpretiert werden, die Zeichen sind also die Elemente von $\text{GF}(2^8)$. Eine Information a sei ein Wort mit 231 Zeichen und diese Information wird durch Hinzufügen von 24 Zeichen (*Redundanz*) in ein Codewort x der Länge 255 ($= 2^8 - 1$) *codiert*. In einem fehlerbehafteten Übertragungskanal verändere sich x infolge von technischen Störungen, der Empfänger erhält statt x ein gestörtes Wort \tilde{x} mit ebenfalls 255 Buchstaben; dabei ist vorausgesetzt, dass sich \tilde{x} in höchstens $12 = \frac{255-231}{2}$ Stellen von x unterscheidet. Der Empfänger *decodiert* nun \tilde{x} , berechnet also aus \tilde{x} das Codewort x und dann die Information a . Dazu muss blitzschnell ein lineares Gleichungssystem über dem Körper $\text{GF}(2^8)$ gelöst werden, bestehend aus 13 Gleichungen in 12 Unbekannten. Dies leistet ein Chip, welcher in jedem Handy, Computer oder CD-Player installiert ist. Im letzten Kapitel rechne ich dazu zwei Beispiele. Anstatt den großen Körper $\text{GF}(2^8)$ nehme ich zunächst den Körper $\text{GF}(7)$ und dann den Körper $\text{GF}(2^3)$, denn in ihnen kann noch per Hand gerechnet werden. Eigentlich können diese Beispiele schon ab Kap. 1 bzw. Kap. 2 gelesen werden, wenn man den *erweiterten Euklidische Algorithmus* (Kap. 4) sowie die *diskrete Fouriertransformation* (Kap. 7) übernimmt.

Natürlich gibt es nun Monographien speziell über endliche Körper, z. B. [3], [4]. Diese gehen weit über den vorliegenden Text hinaus, und sind in ihrem mathematischen Niveau einem mathematisch nicht sehr geschulten Leser nicht ohne weiteres zugänglich.

Dieses Buch entstand aus einer einsemestrigen Vorlesung für den neu eingerichteten Studiengang *Informations- und Kommunikationstechnologie* in Erlangen. Es setzt eine gewisse Vertrautheit mit den Grundbegriffen der linearen Algebra voraus, wie sie z. B. in jeder Vorlesung *Ingenieurmathematik* erklärt werden. Natürlich sind endliche Körper abstrakte Gebilde, die exakte Definitionen und den Einsatz der mathematischen Sprache (Mengen, Abbildungen, ...) erfordern. Ich habe mich bemüht, den formalen Apparat nur als Mittel zum Zweck erscheinen zu lassen. Zum Beispiel habe ich den für den Ungeübten schwierigen Begriff der *Faktorbildung* vermieden, weil in dem hier betrachteten Kontext immer natürliche *Repräsentantensysteme* existieren.

In Kap. 1 erkläre ich den Ring \mathbb{Z} der ganzen Zahlen, sowie den Ring \mathbb{Z} modulo n , $n \in \mathbb{N}$, welchen ich mit \mathbb{Z}_n bezeichne. Ist hier $n = p$ Primzahl, so ist \mathbb{Z}_p ein Körper mit p Elementen, $\mathbb{Z}_p = \text{GF}(p)$. In Kap. 2 definiere ich sorgfältig

den Polynomring $\mathbb{F}[X]$ über einem Körper \mathbb{F} , sowie den Ring $\mathbb{F}[X]$ *modulo* einem Polynom $N \in \mathbb{F}[X]$, den ich mit \mathbb{F}_N bezeichne. Ist hier N Primelement, also irreduzibles Polynom in $\mathbb{F}[X]$, so ist \mathbb{F}_N Körper. Im Fall $\mathbb{F} = \mathbb{Z}_p$ erhält man so den endlichen Körper $\text{GF}(p^n)$, $n = \text{grad } N$. Damit sind in Kap. 2 bis auf Isomorphie schon alle endlichen Körper definiert, ihre Existenz, also die Existenz von N , und die Eindeutigkeit klären wir allerdings erst in Kap. 10. Am Ende von Kap. 2 diskutiere ich die Beispiele $\text{GF}(2^2)$, $\text{GF}(2^3)$, $\text{GF}(2^4)$ und $\text{GF}(3^2)$, auf die ich immer wieder zurückkomme. Das den Körpern $\text{GF}(p^n)$ zugrundeliegende Rechenkalkül entwickle ich in Kap. 8. Dieses kann gleich nach Kap. 2 gelesen werden, wenn man mehr theoretische Sachverhalte aus den Kapiteln 3–6 übernimmt.

Die Teilbarkeitslehre im Polynomring $\mathbb{F}[X]$ ist völlig analog zu der im Ring \mathbb{Z} . Sie bedarf allerdings in dem abstrakten Gebilde $\mathbb{F}[X]$ einer genauen Begründung; diese wird in den Kapiteln 3–5 gegeben. In den Kapiteln 6, 7 klären wir die Struktur einer zyklischen Gruppe und beweisen den fundamentalen Satz, dass die multiplikative Gruppe eines endlichen Körpers eine zyklische Gruppe ist. Dieser Satz und die Rechnungen im letzten Kapitel sind der Anlass, am Schluss von Kap. 7 auch die *diskrete Fouriertransformation* vorzustellen. In Kap. 9 führe ich den Begriff des *Minimalpolynoms* ein und betrachte endliche Körper als *Erweiterungskörper* von \mathbb{Z}_p , bereite somit die theoretischen Sätze in Kap. 10 vor, also den Existenz- und Eindeutigkeitsatz. Mit den Ergebnissen aus Kap. 10 erhalten wir in Kap. 11 einen Überblick über sämtliche irreduziblen Polynome in $\mathbb{Z}_p[X]$, welche ja letztendlich die endlichen Körper definieren. So haben wir in Kap. 2 angefangen und so steht es auch bei Galois.

Im gesamten Text finden sich viele konkrete Beispiele und nach jedem Kapitel stelle ich ein paar Übungsaufgaben, die in der Regel das Vorhergehende anhand konkreter Rechnungen üben.

Ich betone, dass der Text auch eine elementare Einführung in die Algebra bietet. Anders als in manchen „College-Einführungen“ dienen hier die Grundbegriffe der Algebra – *Gruppen, Vektorräume, Ringe, Körper, Polynome* – einem klaren Ziel, nämlich endliche Körper zu erklären.

Für die Fertigstellung des Manuskripts bedanke ich mich bei Frau Irmgard Moch und Herrn dott. Raffaello Caserta.

Die Zahl der Ungenauigkeiten und Fehler, die mein Freund und Kollege Hans Günter Weidner durch geduldiges und genaues Lesen aufspürte, war eindrucksvoll!



<http://www.springer.com/978-3-540-79597-1>

Endliche Körper

Verstehen, Rechnen, Anwenden

Kurzweil, H.

2008, XIII, 178 S., Softcover

ISBN: 978-3-540-79597-1