
Algebraische und zahlentheoretische Grundlagen für die Informatik

Kurt-Ulrich Witt

Algebraische und zahlentheoretische Grundlagen für die Informatik

Gruppen, Ringe, Körper, Primzahltests,
Verschlüsselung

 Springer Vieweg

Kurt-Ulrich Witt
Fachbereich Informatik
Hochschule Bonn-Rhein-Sieg
Sankt Augustin, Deutschland

ISBN 978-3-658-04074-1
DOI 10.1007/978-3-658-04075-8

ISBN 978-3-658-04075-8 (eBook)

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

Springer Vieweg
© Springer Fachmedien Wiesbaden 2014

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-vieweg.de

Vorwort

Dieses Buch stellt mathematische Grundlagen sowie Anwendungen von Rechenstrukturen vor. Es beginnt im Kapitel 1 mit der Rechenstruktur der ganzen Zahlen, die uns aus der Schule und dem täglichen Leben bekannt ist. Anhand dieser Struktur werden viele Begriffe und Eigenschaften betrachtet, die in späteren Kapiteln verallgemeinert und abstrakt untersucht werden. Dabei haben endliche Strukturen, die in der Praxis allerdings sehr groß sein können, eine besondere Bedeutung. Ausgangspunkt dafür ist das Einteilen der ganzen Zahlen in endlich viele Restklassen. Dementsprechend beschäftigen wir uns zunächst mit der Teilbarkeit von Zahlen, mit Primzahlen, mit dem größten gemeinsamen Teiler sowie mit dem kleinsten gemeinsamen Vielfachen von Zahlen. Wir untersuchen schrittweise wesentliche Eigenschaften dieser Begriffe. Diese Eigenschaften spielen im Verlaufe des Buches an vielen Stellen eine bedeutende Rolle bei der Untersuchung und Anwendung algebraischer Strukturen.

In den Kapiteln 2 und 3 werden abstrakte Rechenstrukturen wie Gruppen, Ringe, Integritätsbereiche und Körper betrachtet. Insbesondere wird das Rechnen mit endlichen Strukturen auf ein mathematisch solides Fundament gestellt. Außerdem lernen wir mit den Polynomen eine weitere Rechenstruktur kennen, die zum einen Bedeutung für Anwendungen, wie z.B für die fehlertolerante Codierung von Daten hat und die zum anderen im Kapitel 4 Ausgangspunkt für die Betrachtung endlicher Körper und deren Erweiterungen ist. Sie helfen dabei, alle endlichen Körper zu identifizieren und zu charakterisieren.

In den Kapiteln 5, 6 und 7 werden praxisrelevante Probleme betrachtet, die mithilfe der in den vorangehenden Kapiteln erarbeiteten Konzepte und Methoden gelöst werden können. Wir lernen ein Verfahren zur Lösung von linearen Kongruenzgleichungssystemen kennen, was uns zum einen bei der modularen Addition und Multiplikation hilft und mit dem wir zum anderen die Fehlerwahrscheinlichkeit des probabilistischen Miller-Rabin-Primzahltests bestimmen können. In Kapitel 7 stellen wir mehr oder weniger beispielhaft in der Praxis verwendete Verschlüsselungsverfahren vor. Diese benötigen sehr große Primzahlen. Da deterministische Primzahltests bei derzeitigen Stand des Wissens zu viel Zeit benötigen, um sie in der Praxis einzusetzen, spielen effiziente probabilistische Tests eine große Rolle. Wir stellen die Grundidee des Miller-Rabin-Tests vor und untersuchen, wie bereits erwähnt, seine Fehlerwahrscheinlichkeit.

Das Buch richtet sich an Bachelor-Studierende in Informatik-Studiengängen aller Art sowie an Bachelor-Studierende der Mathematik im Haupt- oder Nebenfach. Das Studium dieses Buches vermittelt nicht nur Wissen zu den oben genannten Gebieten, sondern die Auseinandersetzung mit seinen Inhalten schult die Fähigkeiten, abstrakt und logisch zu denken, Zusammenhänge zu erkennen, sich klar und präzise auszudrücken, neue Probleme anzugehen und zu wissen, wann ein Problem noch nicht vollständig gelöst ist. Es liefert ein zeitinvariantes methodisches Rüstzeug für die Beschreibung und die Lösung von Problemen.

Das Buch ist als Begleitlectüre zu entsprechenden Lehrveranstaltungen an Hochschulen aller Art und insbesondere zum Selbststudium geeignet. Jedes Kapitel beginnt mit einer seinen Inhalt motivierenden Einleitung und der Auflistung von Lernzielen, die durch das Studium des Kapitels erreicht werden sollen. Die meisten Beweise sind vergleichsweise ausführlich und mit Querverweisen versehen, die die Zusammenhänge aufzeigen. Eingestreut sind über sechzig Aufgaben, deren Bearbeitung zur Festigung des Wissens und zum Üben der dargestellten Methoden und Verfahren dienen. Zu fast allen Aufgaben sind am Ende des Buches oder im Text Musterlösungen aufgeführt. Die Aufgaben und Lösungen sind als integraler Bestandteil des Buches konzipiert. Wichtige Begriffe sind als Marginalien aufgeführt; der Platz zwischen den Marginalien bietet Raum für eigene Notizen.

Das Schreiben und das Publizieren eines solchen Buches ist nicht möglich ohne die Hilfe und ohne die Unterstützung von vielen Personen, von denen ich an dieser Stelle allerdings nur einige nennen kann: Als Erstes erwähne ich die Autoren der Publikationen, die ich im Literaturverzeichnis aufgeführt habe. Alle dort aufgeführten Werke habe ich für den einen oder anderen Aspekt verwendet. Ich kann sie allesamt für weitere ergänzende Studien empfehlen. Zu Dank verpflichtet bin ich auch vielen Studierenden, deren kritische Anmerkungen in meinen Lehrveranstaltungen zu Themen dieses Buches ich beim Schreiben berücksichtigt habe. Trotz dieser Hilfen wird das Buch Fehler und Unzulänglichkeiten enthalten. Diese verantworte ich allein – für Hinweise zu deren Beseitigung bin ich dankbar.

Die Publikation eines Buches ist nicht möglich ohne einen Verlag, der es herausgibt. Ich danke dem Springer-Verlag für die Bereitschaft der Publikation und insbesondere Frau Schmickler-Hirzebruch für ihre Ermunterung zur und ihre Unterstützung bei der Publikation des Buches.

Bedburg, im Juni 2014

K.-U. Witt

Inhaltsverzeichnis

1	Die Menge der ganzen Zahlen	1
1.1	Die Rechenstruktur \mathbb{Z}	1
1.2	Teilbarkeit	3
1.2.1	Division mit Rest	3
1.2.2	Division ohne Rest	5
1.2.3	Restklassen	9
1.3	Größter gemeinsamer Teiler	12
1.3.1	Definitionen und elementare Eigenschaften	12
1.3.2	Das Lemma von Bézout	14
1.3.3	Algorithmen zur Berechnung des größten gemeinsamen Teilers	16
1.4	Primzahlen	21
1.5	Kleinstes gemeinsames Vielfaches	27
2	Gruppen	31
2.1	Grundlegende Eigenschaften von Rechenstrukturen	33
2.2	Definitionen und Beispiele	35
2.3	Elementordnungen	41
2.4	Untergruppen	44
2.4.1	Elementare Eigenschaften	44
2.4.2	Zyklische Gruppen	46
2.5	Faktorisierung von Gruppen	48
2.5.1	Nebenklassen	49
2.5.2	Faktorgruppen	50
2.5.3	Satz von Lagrange	52
2.6	Gruppenhomomorphismen	55
2.6.1	Beispiele und Definitionen	55
2.6.2	Kerne von Homomorphismen	61
2.6.3	Der Homomorphiesatz für Gruppen	64
3	Ringe, Integritätsbereiche und Körper	69
3.1	Ringe	69
3.2	Integritätsbereiche	72
3.3	Körper	75
3.4	Unterringe, Unterkörper, Ring- und Körperhomomorphismen	78
3.5	Körpererweiterungen	79
3.6	Restklassengruppen und die Sätze von Euler und Fermat	83
3.7	Polynomringe	86
3.8	Irreduzible und prime Elemente	88
3.9	Teilbarkeit von Polynomen	91
3.9.1	Größter gemeinsamer Teiler von Polynomen	91
3.9.2	Polynomringe und Irreduzibilität	95
3.9.3	Nullstellen	99

4	Erweiterungen endlicher Körper	105
4.1	Beispiele	105
4.2	Grundlegende Definitionen und Eigenschaften	109
4.3	Minimalpolynome	111
4.4	Einheitengruppen endlicher Körper	112
4.5	Charakteristik von Körpern	113
5	Modulare Arithmetik	119
5.1	Chinesischer Restsatz	119
5.2	Modulare Addition und Multiplikation	124
5.3	Effizientes Potenzieren	126
5.4	Primitivwurzeln und diskrete Logarithmen	129
6	Primzahltests	137
6.1	Das Sieb des Eratosthenes	137
6.2	Wilson-Test	139
6.3	Lucas-Test	140
6.4	Fermat-Test	141
6.5	Carmichael-Zahlen	147
6.6	Miller-Rabin-Test	151
6.7	Der AKS-Test	159
7	Asymmetrische Verschlüsselung	165
7.1	Einwegfunktionen	166
7.2	Das RSA-Verfahren	168
7.3	Der Diffie-Hellman-Schlüsselaustausch	175
7.4	Das ElGamal-Verfahren	176
7.5	Signaturen	177
A	Anhang	181
A.1	Zahlenmengen	181
A.2	Alphabete, Wörter, Sprachen	181
A.3	Relationen und Funktionen	182
A.4	Spezielle Funktionen sowie Summen und Produkte	183
A.5	Vektorräume	185
	Lösungen zu den Aufgaben	187
	Literatur	215
	Stichwortverzeichnis	217