



Inhaltsverzeichnis

Rolf Socher

Algebra für Informatiker

Mit Anwendungen in der Kryptografie und Codierungstheorie

ISBN (Buch): 978-3-446-43257-4

ISBN (E-Book): 978-3-446-43312-0

Weitere Informationen oder Bestellungen unter

<http://www.hanser-fachbuch.de/978-3-446-43257-4>

sowie im Buchhandel.

Inhalt

1	Gruppen	9
1.1	Die Gruppenaxiome	9
1.2	Homomorphismen und Isomorphismen	17
1.3	Untergruppen, Nebenklassen und der Satz von Lagrange	24
1.4	Normalteiler und Faktorgruppen	30
1.5	Die Ordnung von Gruppenelementen	35
1.6	Zyklische Gruppen	41
2	Ringe, Körper und Polynome	45
2.1	Ringe	45
2.2	Körper	54
2.3	Polynome	56
3	Elementare Zahlentheorie	67
3.1	Lineare Gleichungen in \mathbb{Z}_m und der chinesische Restsatz	67
3.2	Die eulersche φ -Funktion	74
4	Endliche Körper und Körpererweiterungen	79
4.1	Ein Körper mit neun Elementen	79
4.2	Charakterisierung endlicher Körper	81
4.3	Konstruktion endlicher Körper	85
4.4	Existenz endlicher Körper	90
5	Kryptografie	95
5.1	Grundbegriffe	95
5.2	Symmetrische Verfahren – Die AES-Verschlüsselung	95
5.3	Public-Key-Verschlüsselung	99
5.4	Digitale Signaturen	106
5.5	Kryptografische Hashfunktionen	108
5.6	Elliptische Kurven	113
5.7	Primzahlerzeugung	116
6	Fehlerkorrigierende Codes	123
6.1	Grundbegriffe	123
6.2	Lineare Codes	132
6.3	Kontrollmatrix und Generatormatrix	135
6.4	Zyklische Codes	147

7 Anhang	157
7.1 Teilbarkeit und euklidischer Algorithmus	157
7.2 Primzahlen und Primfaktorzerlegung	160
7.3 Modulare Arithmetik	162
 Weiterführende Literatur	 167
 Symbolverzeichnis	 169
 Sachwortverzeichnis	 173