Inhalt

1 **Ganze Zahlen, Teilbarkeit** 1
1.1 Natürliche und ganze Zahlen 1
1.2 Größter gemeinsamer Teiler, euklidischer Algorithmus 3
1.3 Primfaktorzerlegung 6
1.4 Primzahlen 8
1.5 Kongruenzen und Reste 14
1.6 Aufgaben 20

2 **Gruppen** 23
2.1 Definition, Beispiele, elementare Eigenschaften 23
2.2 Untergruppen und Homomorphismen 29
2.3 Index und Ordnung 34
2.4 Normalteiler und Faktorgruppen 36
2.5 Isomorphiesätze 37
2.6 Operation von Gruppen auf Mengen 40
2.7 Sylowuntergruppen 43
2.8 Produkte und universelle Eigenschaften 48
2.9 Endliche abelsche Gruppen 51
2.10 Aufgaben 54

3 **Ringe** 57
3.1 Grundbegriffe 57
3.2 Ideale und Restklassenringe 62
3.3 Polynome 67
3.4 Euklidische und faktorielle Ringe 71
3.5 Diophantische Probleme für Zahlen und Polynome 79
3.6 Aufgaben 84

4 **Arithmetik modulo n** 86
4.1 Multiplikative zahlentheoretische Funktionen 86
4.2 Die Struktur der primen Restklassengruppe 91

4.3 Quadratische Reste 97
4.4 Das quadratische Reziprozitätsgesetz 100
4.5 Das Jacobisymbol 101
4.6 Verzweigung von Primzahlen 105
4.7 Aufgaben 109

5 Primzahltests und Primfaktorzerlegung **110**
5.1 Das RSA-Schema 110
5.2 Der Kleine Fermatsche Satz als Primzahltest 112
5.3 Riemannsche Vermutung und probabilistische Primzahltests 117
5.4 Faktorisierungsverfahren 124
5.5 Ein Ausblick auf elliptische Kurven 128
5.6 Aufgaben 134

6 Körper und Körpererweiterungen **135**
6.1 Grundbegriffe 135
6.2 Algebraische Körpererweiterungen 138
6.3 Der algebraische Abschluß 144
6.4 Normalität und Separabilität 147
6.5 Transzendente Körpererweiterungen 151
6.6 Aufgaben 155

7 Galoistheorie **157**
7.1 Der Hauptsatz der Galoistheorie 157
7.2 Kreisteilungskörper 161
7.3 Endliche Körper 168
7.4 Quadratische Gaußsche Summen 170
7.5 Nochmals das quadratische Reziprozitätsgesetz 175
7.6 Konstruktionen mit Zirkel und Lineal 177
7.7 KUMMER-Theorie. Auflösung algebraischer Gleichungen 180
7.8 Einfache Gruppen 190
7.9 Einfache lineare Gruppen 194
7.10 Arithmetik der Werte der e-Funktion 201
7.11 Aufgaben 209

Literaturverzeichnis **213**

Index **218**