

Inhaltsverzeichnis

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	9
1.5	Kongruenzen und Reste	15
1.6	Aufgaben	21
2	Gruppen	25
2.1	Definition, Beispiele, elementare Eigenschaften	25
2.2	Untergruppen und Homomorphismen	31
2.3	Index und Ordnung	36
2.4	Normalteiler und Faktorgruppen	38
2.5	Isomorphiesätze	40
2.6	Operation von Gruppen auf Mengen	42
2.7	Sylowuntergruppen	46
2.8	Produkte und universelle Eigenschaften	51
2.9	Endliche abelsche Gruppen	54
2.10	Aufgaben	57
3	Ringe	61
3.1	Grundbegriffe	61
3.2	Ideale und Restklassenringe	66
3.3	Polynome	71
3.4	Euklidische und faktorielle Ringe	75
3.5	Diophantische Fragen zu Zahlen und Polynomen	84
3.6	Aufgaben	89
4	Arithmetik modulo n	91
4.1	Multiplikative zahlentheoretische Funktionen	91
4.2	Die Struktur der primen Restklassengruppe	96
4.3	Quadratische Reste	103
4.4	Das quadratische Reziprozitätsgesetz	106
4.5	Das Jacobisymbol	108
4.6	Verzweigung von Primzahlen	111

4.7 Aufgaben	115
5 Primzahltests und Primfaktorzerlegung	117
5.1 Das RSA-Schema	117
5.2 Der Kleine Fermatsche Satz als Primzahltest	119
5.3 Riemannsche Vermutung und probabilistische Primzahltests	124
5.4 Faktorisierungsverfahren	131
5.5 Ein Ausblick auf elliptische Kurven	137
5.6 Aufgaben	142
6 Körper und Körpererweiterungen	145
6.1 Grundbegriffe	145
6.2 Algebraische Körpererweiterungen	148
6.3 Der algebraische Abschluss	154
6.4 Normalität und Separabilität	157
6.5 Transzendenten Körpererweiterungen	162
6.6 Aufgaben	166
7 Galoistheorie	169
7.1 Der Hauptsatz der Galoistheorie	169
7.2 Kreisteilungskörper	174
7.3 Endliche Körper	181
7.4 Quadratische Gaußsche Summen	183
7.5 Nochmals das quadratische Reziprozitätsgesetz	188
7.6 Konstruktionen mit Zirkel und Lineal	190
7.7 KUMMER-Theorie. Auflösung algebraischer Gleichungen	194
7.8 Einfache Gruppen	204
7.9 Einfache lineare Gruppen	208
7.10 Arithmetik der Werte der e-Funktion	215
7.11 Aufgaben	224
8 Gitter	227
8.1 Grundbegriffe	227
8.2 Untergitter und Elementarteiler	230
8.3 Der Minkowskische Gitterpunktsatz	235
8.4 Anwendungen des Gitterpunktsatzes	239
8.5 Das Kreis- und Kugelproblem	242
8.6 Der Satz von MINKOWSKI-HLAWKA	245
8.7 Packungsdichte	251
8.8 Packungsdichte und Codierungstheorie	258
8.9 Golay-Code und Leech-Gitter	264
8.10 Reduktionstheorie	267
8.11 Binäre quadratische Formen: Reduktion und Klassenzahl	273

8.12 Der LLL-Algorithmus	279
8.13 Aufgaben	284
Lösungshinweise zu den Aufgaben	287
Literaturverzeichnis	295
Index	300