

Inhaltsverzeichnis

1	Einleitung	1
2	Zahlen	5
2.1	Die ganzen Zahlen und Division mit Rest	5
2.2	Fundamentalsatz der Arithmetik	10
2.3	Euklidischer Algorithmus	13
2.4	Der Chinesische Restsatz	16
2.5	Übungsaufgaben	18
3	Gruppen	23
3.1	Übersicht	23
3.2	Gruppen und Operationen	25
3.2.1	Grundbegriffe	25
3.2.2	Gruppenoperationen	35
3.2.3	Operation durch Translation	47
3.2.4	Operation durch Konjugation	50
3.2.5	Bahnengleichung	55
3.3	Normalteiler	62
3.3.1	Normalteiler und Quotientengruppe	62
3.3.2	Konjugationsklassen von Untergruppen	66
3.3.3	Homomorphiesatz und Isomorphiesätze	69
3.3.4	Semidirektes Produkt	78
3.3.5	Klassengleichung	80
3.4	Sylowsätze	83
3.4.1	Existenz von p -Gruppen	85
3.4.2	Sylowuntergruppen	89
3.4.3	Anwendung der Sylowsätze	95
3.5	Übungsaufgaben	100

4 Ringe	117
4.1 Übersicht	117
4.2 Grundbegriffe	120
4.3 Ideale	126
4.4 Integritätsringe	129
4.4.1 Einheiten und Nullteiler	129
4.4.2 Primideale und maximale Ideale	132
4.5 Ideale und affine Varietäten	134
4.6 Computeralgebra in Polynomringen	142
4.7 Noethersche Ringe	145
4.8 Faktorielle Ringe	149
4.8.1 Teilbarkeit und Zerlegung in irreduzible Elemente	149
4.8.2 Zerlegung in Primelemente	151
4.8.3 Größter gemeinsamer Teiler	154
4.9 Hauptidealringe	156
4.10 Euklidische Ringe	160
4.11 Der Chinesische Restsatz	166
4.12 Übungsaufgaben	172
5 Moduln und der Elementarteilersatz	181
5.1 Übersicht	181
5.2 Der Elementarteiler-Algorithmus	182
5.3 Moduln und Präsentationen	190
5.4 Endlich erzeugte Moduln über Hauptidealringen	197
5.5 Der Hauptsatz über endlich erzeugte abelsche Gruppen	202
5.6 Die Jordansche Normalform	203
5.7 Übungsaufgaben	209
6 Die prime Restklassengruppe	213
6.1 Übersicht	213
6.2 Die Einheitengruppe von $\mathbb{Z}/n$	214
6.3 Die Eulersche Phi-Funktion und der kleine Satz von Fermat	215
6.4 Die Struktur von zyklischen Gruppen	217
6.5 Der Fermatsche Primzahltest	223
6.6 Primfaktorisation und das Verfahren von Pollard	225
6.7 Der Primzahlsatz von Dirichlet	228
6.8 RSA	228
6.8.1 Setup	229
6.8.2 Nachrichtenübertragung	230
6.9 Diffie-Hellman Schlüsselaustausch	231
6.10 Wann ist die prime Restklassengruppe zyklisch?	233
6.11 Übungsaufgaben	235

7 Körper	239
7.1 Übersicht	239
7.2 Körpererweiterungen	242
7.3 Charakteristik und Primkörper	244
7.4 Maximale Ideale in Hauptidealringen	245
7.5 Algebraische Körpererweiterungen	246
7.6 Der Zerfällungskörper	252
7.6.1 Konstruktion und Eindeutigkeit	252
7.6.2 Normale Körpererweiterungen	257
7.6.3 Beispiele von Zerfällungskörpern	258
7.7 Algebraisch abgeschlossene Körper	261
7.8 Endliche Körper	262
7.8.1 Konstruktion und Klassifikation	262
7.8.2 Die Einheitengruppe eines endlichen Körpers	266
7.8.3 Die Unterkörper eines endlichen Körpers	268
7.8.4 Die Automorphismengruppe eines endlichen Körpers	273
7.8.5 Die Galoiskorrespondenz	274
7.9 Separable Erweiterungen	279
7.10 Allgemeine Galoiskorrespondenz	284
7.11 Übungsaufgaben	294
8 Quadratische Reste	299
8.1 Übersicht	299
8.2 Die Anzahl der Punkte einer elliptischen Kurve über $\mathbb{F}_p$	301
8.3 Das Legendre-Symbol	304
8.4 Quadratische Kongruenzen für beliebige Moduli	308
8.5 Das Jacobi-Symbol	312
8.6 Beweis des quadratischen Reziprozitätsgesetzes	315
8.7 Solovay-Strassen Primzahltest	319
8.8 Übungsaufgaben	321
9 Konstruktionen mit Zirkel und Lineal	325
9.1 Übersicht	325
9.2 Elementare Konstruktionsschritte	325
9.3 Irreduzibilität über dem Quotientenkörper	332
9.4 Nicht-Konstruierbarkeit des regelmäßigen 9-Ecks	336
9.5 Wann ist das regelmäßige n -Eck konstruierbar?	337
9.6 Übungsaufgaben	338
Literaturverzeichnis	341
Sachverzeichnis	343