
Inhaltsverzeichnis

0	Voraussetzungen aus den Grundvorlesungen	1
0.1	Äquivalenzklassen, Gruppen, Ringe	1
0.2	Polynomring	6
0.3	Ergänzung: Formale Potenzreihen	14
0.4	Übungen	16
1	Natürliche und ganze Zahlen	17
1.1	Axiomatik bzw. Konstruktion	17
1.2	Zahldarstellungen	21
1.3	Übungen	25
2	Teilbarkeit und Primzahlen	27
2.1	Teilbarkeit in Integritätsbereichen	27
2.2	Fundamentalsatz der Arithmetik	35
2.3	Unendlichkeit der Primzahlmenge	38
2.4	Ergänzung: Primzahlsatz und Riemannsche Zetafunktion	40
2.5	Sieb des Eratosthenes	42
2.6	Übungen	44
3	Hauptidealringe, euklidischer Algorithmus und diophantische Gleichungen	47
3.1	Größter gemeinsamer Teiler	47
3.2	Eindeutige Primfaktorzerlegung	52
3.3	Euklidischer Algorithmus und euklidische Ringe	55
3.4	Lineare diophantische Gleichungen	61
3.5	Ergänzung: Multiplikative Funktionen	62
3.6	Übungen	66
4	Kongruenzen und Ideale	69
4.1	Kongruenzen	69
4.2	Restklassenring und Homomorphiesatz	76
4.3	Simultane Kongruenzen und chinesischer Restsatz	86

4.4	Lineare Kongruenzen und prime Restklassengruppe	94
4.5	Ergänzung: Polynomiale Kongruenzen	100
4.6	Ergänzung: Gauß'sche Primzahlen	104
4.7	Übungen	107
5	Gruppen	111
5.1	Grundbegriffe	111
5.2	Nebenklassen, Faktorgruppe und Homomorphiesatz	125
5.3	Zyklische Gruppen und Ordnung eines Elements	134
5.4	Isomorphiesätze und direktes Produkt	138
5.5	Ergänzung: Semidirektes Produkt	143
5.6	Ergänzung: Der Satz von Jordan-Hölder	145
5.7	Übungen	147
6	Operationen von Gruppen auf Mengen	151
6.1	Grundbegriffe	151
6.2	Bahnformel und Klassengleichung	155
6.3	Ergänzung: Sätze von Sylow	160
6.4	Übungen	163
7	Abelsche Gruppen und Charaktere	169
7.1	Abelsche Gruppen und der Hauptsatz	169
7.2	Charaktergruppe	176
7.3	Diskrete Fouriertransformation	182
7.4	Ergänzung: Moduln über Hauptidealringen	188
7.5	Ergänzung: Jordan'sche und rationale Normalform	197
7.6	Übungen	201
8	Prime Restklassengruppe und quadratische Reste	207
8.1	Struktur der primen Restklassengruppe	207
8.2	Primitivwurzeln und Potenzreste	215
8.3	Das quadratische Reziprozitätsgesetz	222
8.4	Ergänzung: Primzahltests	234
8.5	Übungen	240
9	Körper und Körpererweiterungen	245
9.1	Konstruktion von Körpern	246
9.2	Körpererweiterungen	250
9.3	Nullstellen von Polynomen in Erweiterungskörpern	256
9.4	Zerfällungskörper und algebraischer Abschluss	261
9.5	Ergänzung: Konstruktionen mit Zirkel und Lineal	269
9.6	Übungen	274

10	Endliche Körper	277
10.1	Konstruktion und Klassifikation	277
10.2	Erweiterungen endlicher Körper und Automorphismen	284
10.3	Endliche Körper und quadratisches Reziprozitätsgesetz	287
10.4	Ergänzung: Zyklische lineare Codes	289
10.5	Übungen	298
11	Faktorisierung von Polynomen	301
11.1	Gauß'sches Lemma und Irreduzibilitätskriterien	301
11.2	Ergänzung: Algorithmische Faktorzerlegung über endlichen Körpern	306
11.3	Übungen	314
12	Ergänzung: Galoistheorie	317
12.1	Übungen	328
	Sachverzeichnis	331