
Inhaltsverzeichnis

0	Voraussetzungen aus den Grundvorlesungen	1
0.1	Äquivalenzklassen, Gruppen, Ringe	1
0.2	Polynomring	5
0.3	Ergänzung: Formale Potenzreihen	13
	Übungen	14
1	Natürliche und ganze Zahlen	15
1.1	Axiomatik bzw. Konstruktion	15
1.2	Zahldarstellungen	19
	Übungen	22
2	Teilbarkeit und Primzahlen	23
2.1	Teilbarkeit in Integritätsbereichen	23
2.2	Fundamentalsatz der Arithmetik	29
2.3	Unendlichkeit der Primzahlmenge	32
2.4	Ergänzung: Primzahlsatz und Riemannsche Zetafunktion	33
2.5	Sieb des Eratosthenes	34
	Übungen	36
3	Hauptidealringe, euklidischer Algorithmus und diophantische Gleichungen	39
3.1	Größter gemeinsamer Teiler	39
3.2	Eindeutige Primfaktorzerlegung	43
3.3	Euklidischer Algorithmus und euklidische Ringe	45
3.4	Lineare diophantische Gleichungen	49
3.5	Ergänzung: Multiplikative Funktionen	51
	Übungen	54
4	Kongruenzen und Ideale	57
4.1	Kongruenzen	57
4.2	Restklassenring und Homomorphiesatz	63

4.3	Simultane Kongruenzen und chinesischer Restsatz	68
4.4	Lineare Kongruenzen und prime Restklassengruppe	75
4.5	Ergänzung: Polynomiale Kongruenzen	79
4.6	Ergänzung: Gauß'sche Primzahlen	83
	Übungen	86
5	Gruppen	89
5.1	Grundbegriffe	89
5.2	Nebenklassen, Faktorgruppe und Homomorphiesatz	101
5.3	Isomorphiesätze und direktes Produkt	110
5.4	Ergänzung: Semidirektes Produkt	115
	Übungen	116
6	Operationen von Gruppen auf Mengen	119
6.1	Grundbegriffe	119
6.2	Bahnformel und Klassengleichung	123
6.3	Ergänzung: Sätze von Sylow	126
	Übungen	129
7	Abelsche Gruppen und Charaktere	131
7.1	Abelsche Gruppen und der Hauptsatz	131
7.2	Charaktergruppe	138
7.3	Diskrete Fouriertransformation	143
7.4	Ergänzung: Moduln über Hauptidealringen	148
	Übungen	157
8	Prime Restklassengruppe und quadratische Reste	161
8.1	Struktur der primen Restklassengruppe	161
8.2	Primitivwurzeln und Potenzreste	168
8.3	Das quadratische Reziprozitätsgesetz	174
8.4	Ergänzung: Primzahltests	186
	Übungen	192
9	Körper und Körpererweiterungen	195
9.1	Konstruktion von Körpern	195
9.2	Körpererweiterungen	200
9.3	Nullstellen von Polynomen in Erweiterungskörpern	207
9.4	Zerfällungskörper und algebraischer Abschluss	211
9.5	Ergänzung: Konstruktionen mit Zirkel und Lineal	218
	Übungen	221
10	Endliche Körper	223
10.1	Konstruktion und Klassifikation	223
10.2	Erweiterungen endlicher Körper und Automorphismen	230
10.3	Endliche Körper und quadratisches Reziprozitätsgesetz	232
10.4	Ergänzung: Zyklische lineare Codes	235

Übungen	243
11 Faktorisierung von Polynomen	245
11.1 Gauß'sches Lemma und Irreduzibilitätskriterien	245
11.2 Ergänzung: Algorithmische Faktorzerlegung über endlichen Körpern	250
Übungen	259
12 Ergänzung: Galoistheorie	261
Übungen	271
Sachverzeichnis	273