

# Inhaltsverzeichnis

|          |                                                                                      |           |
|----------|--------------------------------------------------------------------------------------|-----------|
| <b>0</b> | <b>Voraussetzungen aus den Grundvorlesungen</b> .....                                | <b>1</b>  |
| 0.1      | Äquivalenzklassen, Gruppen, Ringe .....                                              | 1         |
| 0.2      | Polynomring .....                                                                    | 5         |
| 0.3      | Ergänzung: Formale Potenzreihen .....                                                | 13        |
|          | Übungen .....                                                                        | 14        |
| <b>1</b> | <b>Natürliche und ganze Zahlen</b> .....                                             | <b>15</b> |
| 1.1      | Axiomatik bzw. Konstruktion .....                                                    | 15        |
| 1.2      | Zahldarstellungen .....                                                              | 19        |
|          | Übungen .....                                                                        | 22        |
| <b>2</b> | <b>Teilbarkeit und Primzahlen</b> .....                                              | <b>23</b> |
| 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        |
| <b>3</b> | <b>Hauptidealringe, euklidischer Algorithmus und diophantische Gleichungen</b> ..... | <b>39</b> |
| 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 .....                                                                        | 53        |
| <b>4</b> | <b>Kongruenzen und Ideale</b> .....                                                  | <b>55</b> |
| 4.1      | Kongruenzen .....                                                                    | 55        |
| 4.2      | Restklassenring und Homomorphiesatz .....                                            | 61        |

|           |                                                             |     |
|-----------|-------------------------------------------------------------|-----|
| 4.3       | Simultane Kongruenzen und chinesischer Restsatz .....       | 66  |
| 4.4       | Lineare Kongruenzen und prime Restklassengruppe .....       | 72  |
| 4.5       | Ergänzung: Polynomiale Kongruenzen .....                    | 77  |
| 4.6       | Ergänzung: Gauß'sche Primzahlen .....                       | 81  |
|           | Übungen .....                                               | 84  |
| <b>5</b>  | <b>Gruppen</b> .....                                        | 87  |
| 5.1       | Grundbegriffe .....                                         | 87  |
| 5.2       | Nebenklassen, Faktorgruppe und Homomorphiesatz .....        | 99  |
| 5.3       | Isomorphiesätze und direktes Produkt .....                  | 108 |
| 5.4       | Ergänzung: Semidirektes Produkt .....                       | 113 |
|           | Übungen .....                                               | 114 |
| <b>6</b>  | <b>Operationen von Gruppen auf Mengen</b> .....             | 117 |
| 6.1       | Grundbegriffe .....                                         | 117 |
| 6.2       | Bahnformel und Klassengleichung .....                       | 121 |
| 6.3       | Ergänzung: Sätze von Sylow .....                            | 124 |
|           | Übungen .....                                               | 127 |
| <b>7</b>  | <b>Abelsche Gruppen und Charaktere</b> .....                | 129 |
| 7.1       | Abelsche Gruppen und der Hauptsatz .....                    | 129 |
| 7.2       | Charaktergruppe .....                                       | 136 |
| 7.3       | Diskrete Fouriertransformation .....                        | 140 |
| 7.4       | Ergänzung: Moduln über Hauptidealringen .....               | 146 |
|           | Übungen .....                                               | 155 |
| <b>8</b>  | <b>Prime Restklassengruppe und quadratische Reste</b> ..... | 157 |
| 8.1       | Struktur der primen Restklassengruppe .....                 | 157 |
| 8.2       | Primitivwurzeln und Potenzreste .....                       | 164 |
| 8.3       | Das quadratische Reziprozitätsgesetz .....                  | 170 |
| 8.4       | Ergänzung: Primzahltests .....                              | 182 |
|           | Übungen .....                                               | 188 |
| <b>9</b>  | <b>Körper und Körpererweiterungen</b> .....                 | 191 |
| 9.1       | Konstruktion von Körpern .....                              | 191 |
| 9.2       | Körpererweiterungen .....                                   | 196 |
| 9.3       | Nullstellen von Polynomen in Erweiterungskörpern .....      | 202 |
| 9.4       | Zerfällungskörper und algebraischer Abschluss .....         | 207 |
| 9.5       | Ergänzung: Konstruktionen mit Zirkel und Lineal .....       | 214 |
|           | Übungen .....                                               | 217 |
| <b>10</b> | <b>Endliche Körper</b> .....                                | 219 |
| 10.1      | Konstruktion und Klassifikation .....                       | 219 |
| 10.2      | Erweiterungen endlicher Körper und Automorphismen .....     | 225 |
| 10.3      | Endliche Körper und quadratisches Reziprozitätsgesetz ..... | 227 |
|           | Übungen .....                                               | 230 |

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| <b>11 Endliche Körper und Faktorisierung von Polynomen</b>               | 233 |
| 11.1 Gauß'sches Lemma und Irreduzibilitätskriterien                      | 233 |
| 11.2 Ergänzung: Algorithmische Faktorzerlegung über endlichen<br>Körpern | 237 |
| Übungen                                                                  | 245 |
| <b>Sachverzeichnis</b>                                                   | 247 |