

# Inhaltsverzeichnis

<b>I</b>	<b>Algebraische Strukturen</b>	<b>1</b>
<b>1</b>	<b>Einführung</b>	<b>5</b>
<b>2</b>	<b>Halbgruppen und Monoide</b>	<b>13</b>
2.1	Definitionen und Beispiele . . . . .	13
2.2	Unterhalbgruppen . . . . .	15
2.3	Halbgruppen- und Monoidhomomorphismen . . . . .	16
2.4	Kongruenzrelationen . . . . .	19
2.5	Der Homomorphiesatz für Halbgruppen . . . . .	24
2.6	Übungen . . . . .	27
<b>3</b>	<b>Gruppen</b>	<b>29</b>
3.1	Gruppenisomorphismen . . . . .	31
3.2	Zyklische Gruppen . . . . .	35
3.3	Untergruppen . . . . .	36
3.3.1	Permutationsgruppen . . . . .	37
3.3.2	Der Satz von Lagrange . . . . .	39
3.3.3	Normalteiler . . . . .	43
3.3.4	Kerne von Homomorphismen . . . . .	45
3.3.5	Der Homomorphiesatz für Gruppen . . . . .	47
3.3.6	Elementordnungen . . . . .	48
3.4	Übungen . . . . .	50
<b>4</b>	<b>Ringe, Körper und Integritätsbereiche</b>	<b>55</b>
4.1	Grundlegende Definitionen . . . . .	55
4.1.1	Ringe . . . . .	55
4.1.2	Körper . . . . .	56
4.1.3	Unterringe, Unterkörper, Ring- und Körperhomomorphismen . . . . .	59
4.1.4	Körpererweiterungen . . . . .	60
4.2	Integritätsbereiche . . . . .	62
4.3	Polynomringe . . . . .	63

4.4	Ideale . . . . .	65
4.5	Die Einheitengruppe eines Rings und der Satz von Euler . . . . .	67
4.6	Übungen . . . . .	69
<b>II Einführung in die Zahlentheorie</b>		<b>71</b>
<b>5</b>	<b>Teilbarkeit, Irreduzibilität und prime Elemente</b>	<b>75</b>
5.1	Teilbarkeit . . . . .	75
5.2	Irreduzible und prime Elemente . . . . .	76
5.3	Übungen . . . . .	79
<b>6</b>	<b>Teilbarkeit ganzer Zahlen</b>	<b>81</b>
6.1	Größter gemeinsamer Teiler . . . . .	82
6.2	Euklidischer Algorithmus für ganze Zahlen . . . . .	84
6.3	Primzahlen . . . . .	88
6.4	Der Kleine Satz von Fermat . . . . .	94
6.5	Effizientes Potenzieren . . . . .	96
6.6	Übungen . . . . .	99
<b>7</b>	<b>Teilbarkeit von Polynomen</b>	<b>101</b>
7.1	Größter gemeinsamer Teiler von Polynomen . . . . .	101
7.2	Polynomringe und Irreduzibilität . . . . .	104
7.3	Nullstellen . . . . .	107
7.4	Übungen . . . . .	109
<b>8</b>	<b>Kongruenzgleichungen</b>	<b>111</b>
8.1	Lineare Kongruenzen . . . . .	111
8.2	Chinesischer Restsatz . . . . .	114
8.3	Übungen . . . . .	118
<b>9</b>	<b>Die Eulersche <math>\varphi</math>-Funktion</b>	<b>119</b>
9.1	Eigenschaften und Berechnung . . . . .	119
9.2	Modulare Arithmetik . . . . .	122
<b>10</b>	<b>Primzahltests</b>	<b>127</b>
10.1	Pseudoprimzahlen . . . . .	129
10.2	Carmichael-Zahlen . . . . .	132
10.3	Miller-Rabin-Test . . . . .	135
10.4	Übungen . . . . .	141
<b>11</b>	<b>Primitivwurzeln und diskrete Logarithmen</b>	<b>143</b>

<b>III</b>	<b>Einführung in die Kryptologie</b>	<b>149</b>
<b>12</b>	<b>Einfache Chiffriersysteme</b>	<b>153</b>
12.1	Verschiebe- und Tauschchiffren . . . . .	153
12.1.1	Cäsar-Chiffre . . . . .	153
12.1.2	Tauschchiffren . . . . .	155
12.2	Kryptoanalyse . . . . .	156
12.3	Weitere Tauschchiffren. Vigenère-Chiffre . . . . .	158
<b>13</b>	<b>Perfekte Sicherheit und One time pad-Verfahren</b>	<b>163</b>
13.1	Perfekte Sicherheit . . . . .	164
13.2	One-Time-Pad . . . . .	165
13.3	Lineare Schieberegister . . . . .	167
13.4	Übung . . . . .	170
<b>14</b>	<b>Public key-Systeme</b>	<b>171</b>
14.1	Einwegfunktionen . . . . .	171
14.2	Das RSA-Verfahren . . . . .	173
14.3	Der Diffie-Hellman-Schlüsselaustausch . . . . .	180
14.4	Das ElGamal-Verfahren . . . . .	181
14.5	Signaturen . . . . .	182
<b>IV</b>	<b>Lineare Algebra</b>	<b>187</b>
<b>15</b>	<b>Vektorräume</b>	<b>191</b>
15.1	Grundlegende Definitionen und Eigenschaften . . . . .	191
15.2	Lineare Unabhängigkeit . . . . .	196
15.3	Basis und Dimension eines Vektorraums . . . . .	199
15.4	Lineare Abbildungen . . . . .	202
15.5	Orthogonalräume . . . . .	208
15.6	Übungen . . . . .	211
<b>16</b>	<b>Lineare Gleichungssysteme und Matrizen</b>	<b>213</b>
16.1	Matrizen . . . . .	213
16.2	Lineare Gleichungssysteme . . . . .	220
16.3	Determinanten . . . . .	227
16.4	Invertierbare Matrizen . . . . .	233
16.5	Übungen . . . . .	239
<b>V</b>	<b>Einführung in die Codierungstheorie</b>	<b>241</b>
<b>17</b>	<b>Einfache Codes</b>	<b>247</b>
17.1	Block-Codes . . . . .	247

17.1.1	Repetitionscode . . . . .	248
17.1.2	Codes mit Paritätsbit . . . . .	249
17.1.3	Codes mit Blocksicherung . . . . .	250
17.2	Linearcodes . . . . .	251
17.3	Übungen . . . . .	258
<b>18</b>	<b>Perfekte Codes</b>	<b>261</b>
18.1	Triviale perfekte Codes . . . . .	263
18.2	Hamming-Codes . . . . .	264
18.3	Übungen . . . . .	266
<b>19</b>	<b>Präfixcodes</b>	<b>267</b>
<b>20</b>	<b>Information, Entropie und Sätze von Shannon</b>	<b>273</b>
20.1	Huffman-Code . . . . .	275
20.2	Information . . . . .	281
20.3	Entropie . . . . .	283
20.4	Quellencodierung . . . . .	285
20.5	Kanalcodierung . . . . .	288
20.6	Übungen . . . . .	299
<b>21</b>	<b>Prüfzeichencodierung</b>	<b>301</b>
21.1	Prüfzeichenverfahren: Definition und allgemeine Eigenschaften . .	302
21.2	Prüfziffercodierung in additiven Restklassen . . . . .	303
21.2.1	ISBN-Codierung . . . . .	304
21.2.2	EAN-Codierung . . . . .	307
21.3	Fehlererkennung mit abelschen Gruppen . . . . .	309
21.4	Prüfziffercodierung in Diedergruppen . . . . .	312
21.5	Übungen . . . . .	316
<b>22</b>	<b>Zyklische Codes</b>	<b>319</b>
22.1	Generatorpolynome und -matrizen . . . . .	321
22.2	Kontrollpolynome und -matrizen . . . . .	324
22.3	Erweiterungen endlicher Körper . . . . .	325
22.3.1	Beispiele . . . . .	325
22.3.2	Grundlegende Definitionen und Eigenschaften . . . . .	329
22.3.3	Minimalpolynome . . . . .	330
22.3.4	Einheitengruppen endlicher Körper . . . . .	331
22.3.5	Charakteristik von Körpern . . . . .	332
22.3.6	Automorphismen endlicher Körper . . . . .	336
22.4	Hamming-Codes . . . . .	338
22.5	BCH-Codes . . . . .	346
22.6	Reed-Solomon-Codes . . . . .	348
22.7	Übungen . . . . .	350

*Inhalt*

xv

**Literaturverzeichnis**

**353**

**Index**

**357**

# Abbildungsverzeichnis

6.1	Euklidischer Algorithmus. . . . .	85
13.1	Zwei lineare Schieberegister . . . . .	168
13.2	Zustandsfolgen beim Startzustand 1000 der beiden Schieberegister aus Abbildung 13.1 . . . . .	168
13.3	Allgemeiner Aufbau eines Schieberegisters der Länge 4 . . . . .	169
19.1	Codebaum $T_C$ zu $C = \{ 1, 00, 01, 10, 010, 011, 111 \}$ . . . . .	269
19.2	1. Codebaum zu Beispiel 19.2 . . . . .	271
19.3	2. Codebaum zu Beispiel 19.2 . . . . .	271
20.1	Beispiel für eine Huffman-Codierung der Quelle $Q$ aus dem Beispiel 20.2 . . . . .	277
20.2	BMC: binärer gedächtnisloser Kanal . . . . .	289
20.3	BSC: binärer symmetrischer Kanal . . . . .	290

# Tabellenverzeichnis

6.1	Berechnung von $(42, 27)$ mit dem Euklidischen Algorithmus aus Abbildung 6.1. . . . .	85
21.1	Verknüpfungstafel für die Diedergruppe $D_5$ . . . . .	314
22.1	Multiplikations- und Logarithmentafel für $\mathbb{F}_2[x]/(x^2 + x + 1)$ . . .	326
22.2	Multiplikations- und Logarithmentafel für $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$ . . .	327
22.3	Multiplikations- und Logarithmentafel für $\mathbb{F}_2[x]/(x^3 + x + 1)$ . . .	338
22.4	Alle zyklischen Codes der Länge 7 . . . . .	343