

# Inhalt

<b>1</b>	<b>Gruppen</b>	<b>9</b>
1.1	Die Gruppenaxiome	9
1.2	Homomorphismen und Isomorphismen	17
1.3	Untergruppen, Nebenklassen und der Satz von Lagrange	24
1.4	Normalteiler und Faktorgruppen	30
1.5	Die Ordnung von Gruppenelementen	35
1.6	Zyklische Gruppen	41
<b>2</b>	<b>Ringe, Körper und Polynome</b>	<b>45</b>
2.1	Ringe	45
2.2	Körper	54
2.3	Polynome	56
<b>3</b>	<b>Elementare Zahlentheorie</b>	<b>67</b>
3.1	Lineare Gleichungen in $\mathbb{Z}_m$ und der chinesische Restsatz	67
3.2	Die eulersche $\varphi$ -Funktion	74
<b>4</b>	<b>Endliche Körper und Körpererweiterungen</b>	<b>79</b>
4.1	Ein Körper mit neun Elementen	79
4.2	Charakterisierung endlicher Körper	81
4.3	Konstruktion endlicher Körper	85
4.4	Existenz endlicher Körper	90
<b>5</b>	<b>Kryptografie</b>	<b>95</b>
5.1	Grundbegriffe	95
5.2	Symmetrische Verfahren – Die AES-Verschlüsselung	95
5.3	Public-Key-Verschlüsselung	99
5.4	Digitale Signaturen	106
5.5	Kryptografische Hashfunktionen	108
5.6	Elliptische Kurven	113
5.7	Primzahlerzeugung	116
<b>6</b>	<b>Fehlerkorrigierende Codes</b>	<b>123</b>
6.1	Grundbegriffe	123
6.2	Lineare Codes	132
6.3	Kontrollmatrix und Generatormatrix	135
6.4	Zyklische Codes	147

<b>7 Anhang</b>	<b>157</b>
7.1 Teilbarkeit und euklidischer Algorithmus .....	157
7.2 Primzahlen und Primfaktorzerlegung .....	160
7.3 Modulare Arithmetik .....	162
 <b>Weiterführende Literatur</b>	 <b>167</b>
 <b>Symbolverzeichnis</b>	 <b>169</b>
 <b>Sachwortverzeichnis</b>	 <b>173</b>