



Sachwortverzeichnis

Rolf Socher

Algebra für Informatiker

Mit Anwendungen in der Kryptografie und Codierungstheorie

ISBN (Buch): 978-3-446-43257-4

ISBN (E-Book): 978-3-446-43312-0

Weitere Informationen oder Bestellungen unter

<http://www.hanser-fachbuch.de/978-3-446-43257-4>

sowie im Buchhandel.

Sachwortverzeichnis

A

abgeschlossen **9**
AddKey 98
Adjunktion 87
AES-Algorithmus 96
Äquivalenzklasse 163
Äquivalenzrelation 163
Assoziativgesetz 10
assoziiert **60**
Auswertung eines Polynoms 62
Automorphismus **18**
 von Körpern **56**

B

Bézout-Koeffizienten 61, 159
Bild **20**
Binärcode **125**
Blockcode **125**

C

Carmichael-Zahl 119
Cäsar-Code 95
Charakteristik **81**
Code **125**
 äquivalenter **141**
 dualer **145**
 fehlererkennender **127**
 fehlerkorrigierender **127**
 linearer **132**
 optimaler **131**
 perfekter **130, 134**
 zyklischer **147**

D

DES-Algorithmus 96
Diedergruppe **40**
Diffie-Hellman-Schlüsselaustausch 103
direktes Produkt **21**
diskreter Logarithmus 101
Distributivgesetz 45
Dreiecksungleichung 126
dualer Code **145**

E

Einheitengruppe **48**
Einwegfunktion 100
Element
 inverses **10**
 neutrales **10**
elliptische Kurve 113
Erweiterungskörper 86
erzeugende Relation 39
erzeugendes Element
 einer zyklischen Gruppe **41**
eulersche Phi-Funktion **43, 74, 101**

F

Faktor **60**
Faktorgruppe **31**
Faktoring **51**
Fehlererkennung 126
Fehlerkorrektur 126
Fermat-Test 118
formale Nullstelle 87
führender Koeffizient 57

G

Gauß-Jordan-Form 137
Generatormatrix 136, **136, 145**
Generatorpolynom 149, 152
Gewicht **133**
gewichtserhaltend **141**
Gilbert-Varshamov-Schranke **131**
Grad eines Polynoms 57
Gradformel 58
größter gemeinsamer Teiler **60, 158**
Gruppe **10**
 abelsche **10, 45**
 allgemeine lineare 11
 isomorphe **18**
 kommutative **10**
 zyklische **41, 83**
Gruppenaxiome **10**

H

Hamming-Abstand **125**
Hamming-Code **141**
Hamming-Matrix **140**
Hamming-Schranke **130, 134**

Hashfunktion 108, 110
 kollisionsresistente 109

Hauptideal 50

Hauptidealring **51**, 149

Homomorphismus
 von Gruppen **18**
 von Körpern **56**
 von Ringen **48**

I

Ideal **49**, 148

triviales 49

Index **29**

Integritätsbereich **45**, 54, 55, 58

inverses Element **10**

invertierbar **47**

Involution 20

isomorph **18**, **48**

Isomorphiesatz
 für Gruppen **32**
 für Ringe **52**

Isomorphismus
 von Gruppen **18**
 von Körpern **56**
 von Ringen **48**

K

Kanalcodierung 124

Kern **20**

Klein'sche Vierergruppe 20

Kollision 108, 109

kollisionsresistent 109

Kompressionsfunktion 109

kongruent ... modulo **162**

Kontrollmatrix 135, **136**, 145

Kontrollpolynom **149**

Körper **54**

L

Lagrange 39, 74

lateinisches Quadrat 15

Lemma von Bézout **159**

Linksnebenklasse **27**

M

Matrix

Generator- 136

MDS-Code **130**

Miller-Rabin-Test 120

Minimalabstand **125**

Minimaldistanz 134, 139

Minimalgewicht **133**

Minimalpolynom **88**

MixColumns 98

Möbiusfunktion 78

Modul **162**

Monom 57

N

Nebenklassenanführer 143

neutrales Element **10**

Normalteiler **31**

Nullpolynom 57

Nullstelle eines Polynoms 62

nullteilerfrei **45**

O

Ordnung

einer Gruppe **10**

eines Gruppenelements **36**

orthogonal 144

orthogonales Komplement **144**

P

Paritätsprüfcode 133

Phi-Funktion **43**, **74**, 101

Polynom 57

Auswertung 62

irreduzibles 62

konstantes 57

lineares 62

normiertes 60

Nullstelle 62

Primfaktorzerlegung 62

primitives Element 84

Primzahl **160**

Prinzip des nächsten Nachbarn 124

Produkttring **49**

Projektion 24

Q

Quaternionengruppe 44

Quellencodierung 124

R

Rechtsnebenklasse 27

Rijndael 96

Ring 45

der ganzen gaußschen Zahlen 48

kommutativer 45

nullteilerfreier 45, 47

Ringaxiome 45

RSA-Verfahren 101

S

Satz

chinesischer Restsatz 70

kleiner Fermat 75

Primzahlsatz von Hadamard und de la Vallée

Poussin 117

von Euklid 161

von Euler 74

von Lagrange 29, 82, 89

von Wilson 117

selbstdual 145

ShiftRows 98

Signatur

ElGamal 107

RSA 106

Simplex-Code 145

Singleton-Schranke 130, 134

Skalarprodukt 144

spezielle lineare Gruppe 29

SubBytes 97

Symmetriegruppe 12

Syndrom 143

Syndromdecodierung 142

T

teilbar 157

Teiler 60, 157

größter gemeinsamer 60, 158

Ternärcode 125

U

Untergruppe 24

triviale 25

von g erzeugte 39 UpdateKey 99**V**

Verschlüsselung

symmetrische 95

Vielfaches 157

Vigenère-Code 95

W

Wiederholungscode 133

Z

Zerfallungskörper 90

Zeuge 118

zyklisch 147