

Personen- und Sachverzeichnis

A

Abakus, 53
Abel, Niels Henrik, 272, 330
abelsche Gruppe, 271
abzählbare Menge, 254
Achse einer Spiegelung, 264
Addition modulo n , 86
Addition natürlicher Zahlen, 37
Addition von Restklassen, 97
Additionsverfahren, 151
Adjunktion einer Zahl, 227
Adleman, Leonard, 118
Ägyptische Zahlen, 51
Algebra, 178
algebraisch abgeschlossen, 320
algebraische Zahl, 222
algebraische Zahlen sind abzählbar, 256
algebraischer Körper, 233
Algorithmus, 178
allgemeine Endstellenregel, 72
allgemeine Gleichung, 328
allgemeine Quersummenregel, 75
allgemeiner Satz von Vieta, 328
alternierende Gruppe, 264
alternierende Quersumme, 76
al-Chwarizmi, Muhammad ibn Musa, 63, 178
al-Chwarizmi Methode, 178
al-K-ashi, 169
al-Uqlidisi, 169
Anaximander, 1
Anzahl der Nullstellen eines Polynoms, 202
äquivalente Brüche, 126
äquivalente Gleichungen, 146
Äquivalenz von Brüchen, 127
Äquivalenzklasse, 128
Äquivalenzumformung, 146

Aspekte des Polynombegriffs, 190
auflösbare Gruppe, 332
Auflösbarkeit durch Radikale, 330
Automorphismus von C , 311

B

Berechnung der phi-Funktion, 108
Berechnung des ggT, 32
Bézout, Étienne, 22
Binärsystem, 61
Binärzahl, 61
Boethius, 63
Bombelli, Rafael, 308, 324
Brahmagupta, 57
Briefkastenmodell, 117
Bruch, 124
Bruchzahl, 128
b-adische Darstellung, 61

C

Cantor, Georg, 254
Cardano, Gerolamo, 307, 320, 326
Cardanosche Formel, 322
casus irreduzibilis, 324
Cauchy, Augustin-Louis, 13, 283
Charakterisierung konstruierbarer Zahlen, 240
Charakteristik eines Körpers, 213
Charakteristik p , 216
chinesischer Restsatz, 103
Code, 293
Code der DM-Scheine, 302
Code der Euro-Banknoten, 296
Codewort, 293

D

de La Vallée Poussin, Charles-Jean, 34
Dedekind, Richard, 35

del Ferro, Scipione, 320
 del Fior, Antonia Maria, 320
 Delisches Problem, 235
 Demokrit, 3
 Descartes, René, 143, 180, 202, 236, 312
 Dezimalbruch, 170
 Dezimalbrüche sind reelle Zahlen, 170
 Dezimalbrüche und rationale Zahlen, 175
 Dezimalsystem, 61
 Dezimalzahl, 61
 Diagonale eines Fünfecks, 156
 dicht, 138
 Diedergruppe, 271
 Diffie, Whitfield, 116
 Diophant, 114
 direktes Produkt, 104
 Diskriminante, 183
 Division mit Rest, 19
 Drehung, 264
 Dreieckszahl, 9
 Dreiteilung des Winkels, 236
 Dualsystem, 61
 Dualzahl, 61
 Durchschnitt von Unterkörpern, 227
 d'Alembert, Jean-Baptist le Rond, 319

E

EAN-Code, 300
 Effizienz des Sieb des Eratosthenes, 28
 einfache Gruppe, 333
 Einsetzen, 198
 Einsetzungshomomorphismus, 198
 Einsetzungsverfahren, 150
 Eisenstein, Gotthold Max, 207
 Eisensteinkriterium, 207
 elementarsymmetrisches Polynom, 328
 Elemente der Ordnung 2, 282
 Elemente der Ordnung 3, 282
 endliche Dezimalbrüche und rationale Zahlen, 173
 endliche Erweiterungen sind algebraisch, 233
 endliche geometrische Reihe, 166
 endliche Gruppe, 276
 endlicher Dezimalbruch, 173
 Endstellenregeln, 70
 Entschlüsselung des RSA-Algorithmus, 119
 Eratosthenes, 27
 Erdős, Paul, 34
 Erkennung von Vertauschungsfehlern, 299

Erweitern, 126
 Erweiterter Euklidischer Algorithmus, 24
 erzeugendes Element, 285
 Erzeugnis eines Elements, 285
 Euklid, 17, 33, 163
 Euklidischer Algorithmus, 22
 Euler, Leonhard, 106, 166, 308
 Eulersche phi-Funktion, 108
 explizite Beschreibung von $Q(a)$, 228

F

Faktorgruppe, 289
 fehlererkennender Code, 294
 Fehlererkennung, 294
 fehlerkorrigierender Code, 304
 Fermat, Pierre de, 12, 106, 113
 Fermatsche Primzahl, 247
 Ferrari, Ludovico, 326
 Fibonacci, 40, 63
 figurierte Zahl, 4, 39
 Fourier, Joseph, 166
 Fundamentalsatz der Algebra, 317
 Fundamentalsatz für reelle Polynome, 318

G

Galois, Évariste, 219, 330, 335
 Galoisfeld, 219
 Galoisgruppe, 330
 Galoisgruppe einer einfachen
 Radikalerweiterung, 331
 Galoisgruppe und Nullstellen, 333
 ganze Zahl, 13, 43
 Gauß, Carl Friedrich, 11, 34, 244, 319
 Gauß-Algorithmus, 153
 geometrische Reihe, 165
 gerade Permutation, 263
 gerade plus gerade, 5
 gerade Zahl, 4
 ggT und Division mit Rest, 21
 Girard, Albert, 313
 Gleichheitszeichen, 143
 gleichnamige Brüche, 129
 Gleichsetzungsverfahren, 150
 Gleichung, 144
 Gleichungen und auflösbare Gruppen, 333
 Gleitspiegelung, 264
 goldener Schnitt, 157
 goldener Schnitt im Fünfeck, 158
 Grad der Summe von Polynomen, 191

Grad einer Erweiterung, 229
 Grad einer konstruierbaren Zahl, 241
 Grad eines Polynoms, 190
 Grad eines Unterkörpers, 232
 Grad Erweiterung = Grad Minimalpolynom, 230
 Gradformel, 195
 Gradsatz, 230
 Griechische Zahlen, 52
 größter gemeinsamer Teiler, 16
 Gruppe, 271

H

Hadamard, Jacques, 34
 Hamilton, Willam Rowan, 308
 Hamming-Code, 306
 Hauptsatz der elementaren Zahlentheorie, 30
 Hauptsatz über elementarsymmetrische Funktionen, 329
 Hau-Methode, 142
 Hellman, Martin, 116
 Heraklit, 2
 Hermite, Charles, 33
 Hilbert, David, 242
 Hippiasos von Metapont, 158
 Höhe eines Polynoms, 256
 Homomorphie modulo n , 91

I

IBAN, 295
 imaginäre Einheit, 309
 Imaginärteil, 309
 Induktionsaxiom, 35
 Inverse modulo p , 89
 invertierbare Polynome, 195
 invertierbare Restklasse, 99
 irrationale Zahl, 160
 Irrationalität des goldenen Schnitts, 159
 Irrationalität von e , 166
 Irrationalität von $\sqrt{2}$, 160
 Irrationalität von \sqrt{p} , 161
 irreduzibles Polynom, 203
 ISBN, 302
 ISBN-Code, 301
 Ishango-Knochen, 25
 Isometrie, 264
 isomorphe Gruppen, 287
 Isomorphie und direktes Produkt, 105
 Isomorphismus von Gruppen, 287

K

Klassifikation zyklischer Gruppen, 287
 Kleiner Satz von Fermat, 106
 Kleiner-gleich-Relation von Bruchzahlen, 137
 Koeffizienten eines Polynoms, 186
 kommutativer Ring, 193
 komplexe Zahl, 309
 Komplexität der Addition, 66
 Komplexität der Multiplikation, 68
 konjugiert komplexe Zahl, 311
 konstruierbare Zahl, 237
 konstruierbarer Punkt, 236
 Konstruierbarkeit von \sqrt{n} , 163
 Konstruktion regulärer n -Ecke, 247
 Konstruktion regulärer p -Ecke, 246
 Konstruktion von Körpern, 212
 Kontrollgleichung, 294, 305
 Kontrollsymbol, 293
 Konvergenz der geometrischen Reihe, 166
 konvexes Vieleck, 269
 Körper, 90, 135
 Körper der algebraischen Zahlen, 234
 Körper der komplexen Zahlen, 310
 Körper der konstruierbaren Zahlen, 237
 Körper mit 4 Elementen, 214, 218
 Kriterium für die Gleichheit von Restklassen, 96
 Kriterium für Invertierbarkeit von Restklassen, 99
 Kriterium zur Gleichheit von Nebenklassen, 275
 Kürzen, 126

L

Lagrange, Joseph-Louis, 13, 277
 Lambert, Heinrich, 166
 Länge eines Codes, 293
 Leibniz, Gottfried Wilhelm, 66, 143
 Lemma von Bézout, 23
 Lemma von Bézout für Polynome, 211
 Lemma von Euklid, 29
 Lemma von Gauß, 206
 Lindemann, Ferdinand, 242
 lineare Gleichung, 146
 lineares Gleichungssystem, 149
 Liouville, Joseph, 177
 Liouvillesche Konstante, 248
 Liouvillesche Konstante ist transzendent, 251
 Liouvillesche Zahl, 177

Lösbarkeit linearer Gleichungen, 148
 Lösung der kubischen Gleichung, 326
 Lösung einer Gleichung, 145

M

Mächtigkeit endlicher Körper, 216
 Malkreuz, 143
 Malpunkt, 143
 Mayakalender, 101
 Mielsds, Rune, 27
 Minimalpolynom, 223
 Minimalpolynom = irreduzibles Polynom, 224
 Mobilfunk, 116
 modulo, 84
 Multiplikation komplexer Zahlen, 310
 Multiplikation modulo n , 86
 Multiplikation natürlicher Zahlen, 39
 Multiplikation von Restklassen, 98

N

natürliche Zahlen, 13
 Nebenklasse, 275
 Nenner, 124
 Neunerprobe, 90
 Neunerrest, 91
 Normalreihe einer Radikalerweiterung, 332
 Normalteiler, 290
 Nullpolynom, 190
 Nullstelle eines Polynoms, 200, 201
 nullteilerfrei, 195
 n -Eck, 268
 n -te Einheitswurzel, 325

O

öffentlicher Schlüssel, 116
 Ordnung einer Gruppe, 276
 Ordnung eines Elements, 279
 Ordnung eines Gruppenelements, 281
 Oughtred, William, 143

P

p, q -Formel, 184
 Papyrus Rhind, 124, 142
 Paritätscode, 294
 Paritätscode mit Gewichten, 299
 Paritätscode mit Permutationen, 298
 Peano, Giuseppe, 35
 Peano-Axiome, 35
 Periodenlänge, 174
 periodischer Dezimalbruch, 174

Permutation, 261
 Pluszeichen, 143
 Polynom, 186
 Polynomdivision, 196
 Polynomring, 193
 Positionssystem, 61
 Primkörper, 215
 Primzahl, 26
 Primzahlsatz, 33
 privater Schlüssel, 116
 Produkt ganzer Zahlen, 46
 Produkt modulo f , 212
 Produkt natürlicher Zahlen, 38
 Produkt von Bruchzahlen, 133
 Produkt von Polynomen, 192
 Public-Key-Verschlüsselung, 116
 Pythagoras, 1, 63

Q

quadratische Ergänzung, 183
 Quadratur des Kreises, 235
 Quadratwurzelschnecke, 162
 Quadratzahl, 7
 Qualität des ISBN-Codes, 301
 Quersumme, 73
 Quersummenregeln, 70
 Quotientenkörper, 135

R

Radikalerweiterung, 330
 rationale Zahl, 128
 rationale Zahlen sind abzählbar, 254
 Realteil, 309
 Rechentisch, 54
 Rechentuch, 54
 Rechnen auf den Linien, 54
 Rechteckzahl, 9
 Recorde, Robert, 143
 Reduktion kubischer Gleichungen, 322
 reduzibles Polynom, 203
 reelle Zahlen sind nicht abzählbar, 257
 reguläres Fünfeck, 156
 reguläres Vieleck, 244
 Reisch, Gregor, 63
 Rest bei Division durch n , 84
 Restklasse, 94
 Ries, Adam, 54, 93
 Ring, 193
 Ring mit Eins, 193

- Rivest, Ronald, 118
 Römische Zahlen, 52
 Roth, Peter, 312
 RSA-Algorithmus, 118
 Rudolff, Christoph, 169
 Ruffini, Paolo, 200, 330
- S**
 Satz vom Minimalpolynom, 222
 Satz von Abel-Ruffini, 334
 Satz von Cauchy, 283
 Satz von der Faktorgruppe, 289, 290
 Satz von Euler, 111
 Satz von Lagrange, 277
 Satz von Ruffini, 200
 Satz von Sylow, 284
 Satz von Vieta, 181
 Schlüssel, 115
 Schlüssellänge, 121
 Schönemann, Theodor, 207
 Schönemann-Eisenstein-Kriterium, 207
 Selberg, Atle, 34
 Shamir, Adi, 118
 Sicherheit von RSA, 120
 Sieb des Eratosthenes, 27
 Siebzehneck, 244
 Skalar, 189
 Spiegelung, 264
 Square-and-multiply-Algorithmus, 120
 starrer Körper, 311
 Stellen im Stellenwertsystem, 61
 Stellenwertsystem, 57, 60, 61
 Stevin, Simon, 169
 Stifel, Michael, 40
 Struktur der Diedergruppe, 291
 Struktur der Nebenklassen, 276
 Summe aufeinanderfolgender Zahlen, 6
 Summe gleichnamiger Brüche, 129
 Summe im Stellenwertsystem, 65
 Summe natürlicher Zahlen, 36
 Summe und Differenz ganzer Zahlen, 44
 Summe ungerader Zahlen, 8
 Summe von Bruchzahlen, 130
 Summe von Dreieckszahlen, 10
 Summe von Polynomen, 187
 Sylow, Ludwig, 284
 Symmetrieabbildung, 266
 Symmetriegruppe, 268
 Symmetrien eines n -Ecks, 270
 symmetrische Gruppe, 261
- T**
 Tartaglia, Niccoló, 320
 Teilbarkeit durch 2, 71
 Teilbarkeit durch 3, 74
 Teilbarkeit durch 4, 71
 Teilbarkeit durch 7, 80
 Teilbarkeit durch 9, 74
 Teilbarkeit durch 11, 78
 Teilbarkeit durch eine Primzahl, 30
 Teilbarkeit von Summe und Differenz, 15
 Teiler, 14
 Teiler eines Polynoms, 210
 teilerfremde Polynome, 211
 teilerfremde Zahlen, 17
 Tennenbaum, Stanley, 163
 Term, 144
 Thales von Milet, 1
 Translation, 264
 Transposition, 262
 transzendente Zahl, 248, 251
- U**
 überabzählbar, 257
 ultimative Quersumme, 76
 Unendlichkeit der Primzahlen, 33
 ungerade Permutation, 263
 ungerade Zahl, 4
 Unmöglichkeit der Dreiteilung des Winkels, 242
 Unmöglichkeit der Quadratur des Kreises, 242
 Unmöglichkeit der Verdoppelung des Würfels, 242
 Untergruppe, 273
 Untergruppen zyklischer Gruppen, 288
 Untergruppenkriterium, 273
 Unterkörper, 225
- V**
 Vektorraum, 189
 Vektorraum der Polynome, 189
 Verdoppelung des Würfels, 235
 Verschlüsselung, 115
 Vielfaches, 14
 Vielfachheit einer Nullstelle, 200
 Viète, François, 143, 169, 180, 185
 vollständige Induktion, 36
 von-Ansatz, 132
 Vorperiode, 174

Vorzeichenregel von Descartes, [314](#)
Vorzeichenwechsel eines Polynoms, [313](#)

W

Wantzel, Pierre, [241](#)
Wechselwegnahme, [17](#)
Wessel, Caspar, [308](#)
Widmann, Johannes, [143](#)
Wiles, Andrew, [114](#)
wohldefiniert, [130](#)
Wohldefiniertheit der Addition von
Bruchzahlen, [130](#)
Wohldefiniertheit der Kleiner-gleich-Relation,
[137](#)

Wohldefiniertheit der Multiplikation von
Bruchzahlen, [133](#)

Wolfsknochen, [49](#)

Wurzeln aus natürlichen Zahlen, [161](#)

Z

Zähler, [124](#)
Zentrum einer Drehung, [264](#)
Ziffern eines Dezimalbruchs, [170](#)
 \mathbf{Z}_p ist Körper, [100](#)
zyklische Gruppe, [285](#)
zyklische Permutation, [262](#)
Zyklus, [262](#)