

---

# Sachverzeichnis

## A

abelsch, 2, 111  
abgeleitete Reihe, 131  
abgeschlossen  
  algebraisch, 259, 263  
Abschluss  
  algebraischer, 263  
Abschluss in  $L$   
  algebraischer, 259  
adjungiert, 253  
Adjunktion, 253  
Algebra, 5  
algebraisch abgeschlossen, 259, 263  
algebraische  
  Körpererweiterung, 251  
algebraischer  
  Abschluss, 263  
  Abschluss in  $L$ , 259  
algebraisches  
  Element, 251  
Algebrenhomomorphismus, 5  
Algorithmus, euklidischer, 57  
Alice, 209, 218  
allgemeine lineare Gruppe, 113  
alternierende Gruppe, 116  
Anwendungen  
  kryptographische, 218  
Arithmetik, modulare, 92  
arithmetische Progression, 2  
Artin'sche Vermutung, 215  
Assoziativgesetz, 2  
assoziiert, 29  
asymptotisch gleich, 24  
auflösbar, 131  
Automorphismen  
  äußere, 149

Automorphismengruppe  
  einer Gruppe, 120  
  eines Rings, 117  
Automorphismus  
  eines Rings, 78  
  innerer, 122  
   $K$ -, 262

## B

Bahn, 153  
Bahnengleichung, 159  
Bahnformel, 155  
Basis  
  eines  $R$ -Moduls, 189  
BCH-Code, 295  
Begleitmatrix, 199  
Betrag  
   $p$ -adischer, 45  
Bewertung  
   $p$ -adische, 36  
Bild, 119  
Binärdarstellung, 21  
biquadratische Erweiterung, 324  
Block-Code, 289  
Bob, 209, 218

## C

Carmichael-Zahl, 210  
Cauchy, Satz von, 161  
Cayley, 123  
  Satz von, 123  
ceiling, 20  
Charakter, 176  
  -gruppe, 177

unitärer, 177  
 Charakteristik, 249  
 chinesischer Restsatz, 86  
 Code  
   dualer, 291  
   linearer, 289  
   selbstdualer, 291  
   zyklischer, 291

## D

Darstellung  
   primitive, 106  
   treue, 151  
 Darstellung zur Basis, 21  
 Darstellung, lineare, 122  
 Darstellung, Permutations-, 123  
 Determinantenteiler, 193  
 Dezimaldarstellung, 21  
 Diagramm, kommutatives, 132  
 Diedergruppe, 117  
 Diffie-Hellman, 218  
 Digitale Signatur, 218  
 diophantisch, 61  
 direkte Summe, 170  
   von Ringen, 86  
 direktes Produkt  
   von Gruppen, 86, 142  
   von Ringen, 86  
 Dirichlet-Charakter, 204  
 Dirichletreihe, 64  
 Dirichlets Primzahlsatz, 99  
 discrete logarithm, 218  
 diskreter Logarithmus, 218  
 Diskriminante, 328  
 Divisionsalgebra, 3  
 double precision integers, 23  
 duale Gruppe, 178  
 dualer Code, 291

## E

Einbettung  
   in den Quotientenkörper, 246  
 einfach, 131  
 einfache  
   Erweiterung, 253  
 Einheit, 5  
 Einheitengruppe, 5

Einheitswurzel, 171, 178  
   primitive  $n$ -te, 212  
 Einselement, 3  
 Einsetzungshomomorphismus, 10  
 Eisenstein  
   Irreduzibilitätskriterium, 304  
 El Gamal, 218  
 Element  
   inverses, 2  
   neutrales, 2  
   primitives, 321  
 Elementarteiler, 191, 194  
 Elementarteilerbasen, 194  
 Elementarteilersatz, 191  
 endlich erzeugt, 34  
 endlich erzeugter Modul, 189  
 Ergänzungssatz zum quadratischen  
   Reziprozitätsgesetz  
   Erster, 225  
   Zweiter, 225  
 Erster Ergänzungssatz zum quadratischen  
   Reziprozitätsgesetz, 225  
 Erweiterung, 250  
   biquadratische, 324  
   einfache, 253  
   quadratische, 254  
   separable, 319  
 Erzeugendensystem  
   eines  $R$ -Moduls, 189  
 Erzeugermatrix, 290  
 Erzeugerpolynom (eines zyklischen Codes), 291  
 euklidische Funktion, 55  
 euklidischer Algorithmus, 57  
 euklidischer Ring, 55  
 Euler-Faktoren, 64  
 Euler-Kriterium, 223  
 Euler-Produkt, 64  
 Euler-Pseudoprimzahl, 234  
 Euler'sche  $\varphi$ -Funktion, 98  
 Exponent, 169

## F

Faktorgruppe, 128  
 faktoriell, 54  
 faktorisiert, 84  
 Faktorkommutatorgruppe, 133  
 Faktoring, 71  
 Faltung, 185

- multiplikativer Funktionen, 63
  - Faser, 128
  - fast Fourier transform, 187
  - Feit-Thompson, Satz von, 131
  - Fermat, kleiner Satz von, 208
  - Fermat-Euler, Satz von, 208
  - Fermat'sche Primzahlen, 43
  - Fermat-Zahlen, 43
  - Fibonacci-Zahlen, 67
  - Fixgruppe, 319
  - Fixkörper, 319
  - Fixpunkt, 153
  - floating point numbers, 23
  - floor, 20
  - formale Potenzreihe, 14
  - Fourier transform
    - fast, 187
  - Fourieranalysis
    - diskrete, 178
  - Fourier'sche Umkehrformel, 184
  - Fouriertransformation
    - diskrete, 178
    - schnelle, 187
  - Fourier-Transformierte, 183
  - freie Gruppe, 119
  - freier Modul, 189
  - Friendly Giant, 132
  - Funktion
    - euklidische, 55
    - Möbius'sche, 63
    - multiplikative zahlentheoretische, 62
    - zahlentheoretische, 62
- G**
- Galoiserweiterung, 317
  - Galoisgruppe, 317
  - ganze Zahlen, 17
  - ganzer Anteil, 20
  - Gauß
    - Lemma über primitive Polynome, 302
    - Lemma über quadratische Reste, 243
  - Gauß-Klammer, 20
  - Gauß'sche ganze Zahlen, 30, 56
  - gebrochener Anteil, 20
  - gerade Permutation, 116
  - ggT, 47
  - Gleichungen
    - diophantische, 61
  - Gleitkommazahlen, 23
  - Goldbach'sche Vermutung, 40
  - goldener Schnitt, 59
  - Grad
    - einer Körpererweiterung, 250
    - eines Elements, 251
    - eines Monoms, 31
    - eines Polynoms, 6
  - Gradsatz, 255
  - Green, 40
  - größter gemeinsamer Teiler, 47
    - von Idealen, 77
  - Gruppe, 2, 111
    - abelsche, 2
    - alternierende, 116
    - Charakter-, 177
    - freie, 119
    - kommutative, 2
    - perfekte, 125
    - sporadische, 132
    - symmetrische, 114
    - Torsions-, 170
- H**
- Halbgruppe, 5
  - Hamming-Abstand, 290
  - Hamming-Gewicht, 290
  - Hauptideal, 33
  - Hauptidealring, 34
  - Hauptraumzerlegung
    - verallgemeinerte, 198
  - Hauptsatz
    - über endlich erzeugte abelsche Gruppen, 175
    - über endliche abelsche Gruppen, 172
  - Helfgott, 40
  - Hensels Lemma, 102
  - Hermite
    - Satz von, 252
  - Hermite-Normalform, 192
  - Hierarchie der Ringe, 57
  - Hölder
    - Satz von Jordan-, 145
  - homogen, 31
  - Homomorphiesatz, 83, 132
  - Homomorphismus
    - von Algebren, 5
    - von Gruppen, 119

von Ringen, 78  
 Hülle  
 normale, 268

## I

Ideal, 33  
 maximales, 81  
 Index, 125, 216  
 einer Untergruppe, 126  
 Indexrechnung, 217  
 innerer Automorphismus, 122  
 inseparabel, 319  
 Integritätsbereich, 3, 19, 27  
 Interpolationspolynom  
 von Lagrange, 92  
 inverses Element, 2  
 irreduzibel, 32  
 Irreduzibilitätskriterium von Eisenstein, 304  
 irreduzibles Polynom, 32  
 isomorph  
 (Subnormalreihen), 131  
 Isomorphiesatz  
 Zweiter, 140  
 Isomorphismus, 5  
 $K$ -, 262  
 von Gruppen, 119  
 von Ringen, 78  
 von  $R$ -Moduln, 189  
 Isotropiegruppe, 153

## J

Jacobi-Symbol, 232  
 Jordan-Hölder  
 Satz von, 131, 145  
 Jordan'sche Normalform, 188, 199

## K

$K$ -Algebra, 5, 262  
 Kern, 119  
 key exchange, 218  
 kgV, 47  
 Klassengleichung, 159  
 kleiner Satz von Fermat, 208  
 Kleinsche Vierergruppe, 116  
 kleinstes gemeinsames Vielfaches, 47  
 von Idealen, 77

kommutative Gruppe, 19  
 kommutative Halbgruppe, 19  
 kommutativer Ring, 3, 19  
 kommutatives Diagramm, 132  
 Kommutativgesetz, 2  
 Kommutatoren, 125  
 Kommutatorgruppe, 125  
 Kompositionsfaktoren, 131  
 Kompositionsreihe, 131  
 kongruent, 69  
 kongruent modulo  $n$ , 1  
 Kongruenzen  
 simultane, 87  
 Konjugation, 123  
 Konjugationsklasse, 154  
 konjugiert, 123  
 Konstruierbarkeit mit Zirkel und Lineal, 269  
 Kontrollmatrix, 290  
 Kontrollpolynom, 291  
 Konvolution, 185  
 Körper, 3  
 der Brüche, 246  
 Prim-, 249  
 Zerfallungs-, 261  
 Körpererweiterung, 250  
 normale, 268  
 Kreisteilungskörper, 325  
 Kreisteilungspolynom, 255  
 Kryptographie, 209, 218  
 public key, 209

## L

Lagrange  
 Interpolationssatz, 92  
 Satz über Summen von vier Quadraten, 75  
 Satz von (Gruppentheorie), 127  
 Lagrange'sches Interpolationspolynom, 14, 92  
 Legendre-Symbol, 222  
 Leitkoeffizient, 6  
 Lemma von Gauß (über primitive Polynome),  
 302  
 Lemma von Gauß (über quadratische Reste),  
 243  
 Lindemann  
 Satz von, 252  
 linear, 18  
 linearer Code, 289  
 Logarithmus

diskreter, 218  
 Lucas-Zahlen, 67

## M

maximaler zyklischer Code, 294  
 maximales Ideal, 81  
 Maynard, 40  
 Mersenne-Zahlen, 43  
 Miller-Rabin, Primzahltest, 236  
 Minimalabstand, 290  
 minimaler zyklischer Code, 294  
 Minimalgewicht, 290  
 Minimalpolynom, 251  
 Möbius-Funktion, 63  
 Modul, 188  
   endlich erzeugter, 189  
   freier, 189  
 modulare Arithmetik, 92  
 Modulhomomorphismus, 189  
 Monoid, 5, 19  
 Monom, 31  
 monoton, 18  
 Monstergruppe, 132  
 multiplikative zahlentheoretische Funktion, 62

## N

$n$ -ter Potenzrest, 218  
 Nachfolgerabbildung, 18  
 natürliche Zahlen, 17  
 Nebenklasse, 125  
 neutrales Element, 2  
 Nichtrest, 218  
 noethersch, 34  
 Norm, 250  
 normale  
   Körpererweiterung, 268  
   Untergruppe, 124  
 normale Hülle, 268  
 Normalform  
   Jordan'sche, 188, 199  
   rationale, 189, 199  
 Normalisator, 148, 155  
 normalisiert, 138  
 Normalreihe, 131  
 Normalteiler, 124  
 normiertes Polynom, 6  
 Nullstelle

einfache, 12  
 mehrfache, 12  
 Nullteiler, 3, 27  
 nullteilerfrei, 3, 19, 27

## O

$O(x)$ , 23  
 $o(x)$ , 23  
 Oberkörper, 250  
 Operation, 151  
 operieren, 151  
 Orbit, 153  
 Ordnung  
   modulo  $m$ , 210  
 Ordnungsrelation, 18  
 orthogonale Gruppe, 117  
 Orthogonalitätsrelation, 181

## P

$p$ -adische Bewertung, 36  
 Peano-Axiome, 17  
 perfekt, 260  
 perfekte Gruppe, 125  
 Permutation, 114  
   gerade, 116  
   ungerade, 116  
   zyklische, 114  
 Permutationen, 114  
 $p$ -Gruppe, 160  
 Phi-Funktion, Euler'sche, 98  
 Poisson'sche Summenformel, 185  
 Polynom  
   homogenes, 31  
   Inhalt, 301  
   irreduzibles, 32  
   Kreisteilungs-, 255  
   normiertes, 6  
   primitives, 301  
 Polynomdivision, 11  
 Polynomfunktion, 10  
 Polynomring, 6  
   in mehreren Variablen, 30  
   in unendlich vielen Variablen, 31  
 Potenzreihe, formale, 14  
 Potenzrest,  $n$ -ter, 218  
 Präsentation  
   einer Gruppe, 130

praxisnah, 89  
 prime Restklassen, 97  
 prime Restklassengruppe, 97  
 Primelement, 32  
 Primideal, 81  
 primitive Darstellung, 106  
 primitive  $n$ -te Einheitswurzel, 212  
 primitives Element, 321  
 Primitivwurzel, 211  
 Primkörper, 249  
 Primzahl, 32  
 Primzahlen  
     Fermat'sche, 43  
     Mersenne'sche, 43  
 Primzahlsatz, 39  
     von Dirichlet, 99  
 Primzahltest  
     Miller-Rabin, 236  
     Solovay-Strassen, 235  
 Primzahlzwillinge, 39  
 principal ideal domain, 34  
 Produkt  
     direktes, 86, 142  
     semidirektes, 144  
 Progression  
     arithmetische, 2  
 Projektionsabbildung, 79  
 pseudoprime  
     strong, 236  
 Pseudoprимzahl, 210  
     Euler-, 234  
     starke, 236  
 $p$ -Sylowgruppe, 160  
 public key, 209

## Q

quadratfrei, 44, 306  
 quadratfreie Zerlegung, 309  
 quadratische Erweiterung, 254  
 quadratischer Rest, 218  
 Quadratische-Reste-Code, 296  
 quadratisches Reziprozitätsgesetz, 224  
 Quadratur des Kreises, 252  
 Quasicharakter, 177  
 Quaternionengruppe, 149  
 Quotientenkörper, 246  
     Einbettung in den, 246

## R

Rang, 175  
     eines endlich erzeugten Moduls, 195  
 reduzibel, 32  
 Reed-Solomon-Code, 294  
 Reihe  
     (Sub-)Normal-, 131  
     abgeleitete, 131  
     Kompositions-, 131  
 rein transzendent, 259  
 Relationen  
     definierende, 129  
 relativ prim, 47  
 Repräsentantensystem, 70  
 Rest, 20  
 Restklasse, 70, 71  
     modulo  $n$ , 1  
 Restklassen  
     prime, 97  
 Restklassengruppe  
     prime, 97  
 Restklassenring, 71  
 Restsatz, chinesischer, 86  
 Restsystem  
     absolut kleinstes, 71  
 Reziprozitätsgesetz, quadratisches, 224  
 Riemann'sche Vermutung, 41  
 Riemann'sche Zetafunktion, 40  
 Ring, 3  
     euklidischer, 55  
     faktorieller, 54  
     kommutativer, 3  
     noetherscher, 34  
 Ringhomomorphismus, 78  
 RSA-Verfahren, 209

## S

Satz  
     Grad-, 255  
     von Cauchy, 161  
     von Feit-Thompson, 131  
     von Fermat-Euler, 208  
     von Green und Tao, 40  
     von Hermite, 252  
     von Jordan-Hölder, 131  
     von Lindemann, 252  
     von Sylow, 161  
 Schiefkörper, 3

Schlüssel  
 Austausch von, 218  
 Schmetterlingslemma  
 (Zassenhaus), 146  
 Schnitt  
 goldener, 59  
 Schreier  
 Satz von, 145  
 selbstdualer Code, 291  
 semidirektes Produkt, 144  
 separabel, 319  
 separable Erweiterung, 319  
 Signatur  
 digitale, 218  
 signum, 114  
 simultane Kongruenzen, 87  
 single precision integer, 22  
 Smith-Normalform, 191  
 Solovay-Strassen  
 Primzahltest von, 235  
 spezielle lineare Gruppe, 117  
 spezielle orthogonale Gruppe, 118  
 Spur, 250  
 Stabilisator, 153  
 Standgruppe, 153  
 Subnormalreihe, 131  
 summatorische Funktion, 63  
 Summe  
 direkte, 86, 170  
 Summen von Quadraten, 75  
 Sylow, Satz von, 161  
 Sylowgruppe, 160  
 symmetrische Gruppe, 114

**T**

Tao, 40  
 Taylor-Entwicklung, 101  
 Teiler, 27  
 teilerfremd, 47  
 Teilerketten, 52  
 Torsion, 171  
 Torsionselement, 170  
 torsionsfrei, 170  
 Torsionsgruppe, 170  
 total, 18  
 träge, 104  
 transitiv, 153  
 transzendent, 251

rein, 259  
 treue Darstellung, 151

**U**

Umkehrformel  
 Möbius'sche, 65  
 ungerade Permutation, 116  
 unitärer Charakter, 177  
 Untergrad, 16  
 Untergruppe, 3, 115  
 Unterraum  
*f*-zyklischer, 199  
 unzerlegbar, 32

**V**

Vektorraum, 2  
 Verfeinerung  
 (Subnormalreihen), 145  
 Vermutung  
 Artin'sche, 215  
 Riemann'sche, 41  
 von Goldbach, 40  
 Verschwindungsideal, 80  
 verzweigt, 104  
 Vielfachheit, 12  
 Vierergruppe, 116  
 Vinogradov, 40  
 Viéta'scher Wurzelsatz, 252  
 vollkommene Zahl, 27, 68  
 vollkommener Körper, 260  
 Vorzeichen (einer Permutation), 114

**W**

Wohlordnung, 19

**Z**

zahlentheoretische Funktion, 62  
 Zassenhaus  
 Lemma von, 146  
 Zentralisator, 149  
 Zentrum  
 einer Gruppe, 122, 123  
 Zerfällungskörper, 261  
 Zerlegung  
 quadratfreie, 309

Zetafunktion

  Riemann'sche, [40](#)

Zhang, [39](#)

ZPE-Ring, [54](#)

Zweiter Ergänzungssatz zum quadratischen  
  Reziprozitätsgesetz, [225](#)

Zykel, [114](#)

zyklische Permutation, [114](#)

zyklischer Code, [291](#)

zyklischer Unterraum, [199](#)