

# Literaturverzeichnis

## Lehrbücher der Algebra

- [ArE] ARTIN, E.: *Galoissche Theorie*. Harri Deutsch 1965
- [ArM] ARTIN, M.: *Algebra*. Birkhäuser 1993
- [Bo] BOSCH, S.: *Algebra*. Springer 2009<sup>7</sup>
- [F-S] FISCHER, G., SACHER, R.: *Einführung in die Algebra*. Teubner 1983<sup>3</sup>
- [Fr] FRICKE, R.: *Lehrbuch der Algebra I*. Vieweg 1924
- [Ku] KUNZ, E.: *Algebra*. Vieweg 1994<sup>2</sup>
- [K-M] KARPFINGER, C., MEYBERG, K.: *Algebra*. Springer 2013<sup>3</sup>
- [La] LANG, S.: *Algebra*. Addison Wesley 1965
- [Ro] ROTMAN, J.J.: *An Introduction to the Theory of Groups*. Springer 1995<sup>4</sup>
- [W<sub>1</sub>] VAN DER WAERDEN, B.L.: *Moderne Algebra*. Springer 1931; neu aufgelegt als *Algebra I*. Springer 1966<sup>7</sup>
- [We<sub>1</sub>] WEBER, H.: *Lehrbuch der Algebra*. 3 Bände. Vieweg 1896 - 1908
- [Wü] WÜSTHOLZ, G.: *Algebra*. Vieweg 2004

## Weitere Literatur

- [A] ABEL, N.H.: *Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden, als dem vierten, allgemein aufzulösen*. J. Reine Angew. Math. **1**, 65-85 (1826)
- [Ab] ABHYANKAR, S.: *On Macaulay's Example*. In: Springer Lecture Notes in Math. 423 (1974), 1-16
- [Ba] BANACH, S.: *Théorie des opérations linéaires*. Warschau, 1932
- [B-R-K] BARTHOLOMÉ, A., J. RUNG und H. KERN: *Zahlentheorie für Einsteiger*. Vieweg 2006<sup>5</sup>
- [B-E-O'B] BESCHKE, H.U., B. EICK, E.A. O'BRIEN: *A millennium project: constructing small groups*. Internat. J. Algebra Comput. **12**, 623-644 (2002)
- [Be] BEWERSDORFF, J.: *Algebra für Einsteiger*. Vieweg 2007<sup>3</sup>
- [Bi] BIEBERBACH, L.: *Theorie der geometrischen Konstruktionen*. Birkhäuser 1952
- [Bl] BLUMENTHAL, O.: *Lebensgeschichte*. In: D. HILBERT, *Gesammelte Abhandlungen*, Band 3, 388-429. SPRINGER, 1935
- [B-O] BRUINIER, J.H., K. ONO: *An algebraic formula for the partition function*. Preprint 2011
- [Can] CANTOR, G.: *Beiträge zur Begründung der transfiniten Mengenlehre*. Math. Ann. **5**, 123-132, 1872
- [C] CARDANO, G.: *Artis magna sive de regulis algebraicis liber unus*. Nürnberg 1545
- [Ca] CARMICHAEL, R.D.: *Introduction to the theory of groups of finite order*. Ginn 1937
- [Ca<sub>1</sub>] CAYLEY, A.: *On the Theory of Groups, as Depending on the Symbolic Equation  $\vartheta^n = 1$* . Collected Papers 2, p. 123, 1854
- [Ca<sub>2</sub>] CAYLEY, A.: *Desiderata and Suggestions*. Am. Journal of Math. **1**, 50 - 52, 1877
- [C-L-O'S] COX, D., J. LITTLE, D. O'SHEA: *Ideals, Varieties and Algorithms*. Springer 1991
- [De] DEDEKIND, R.: *Beweis für die Irreduzibilität der Kreisteilungsgleichung*. J. Reine Angew. Math. **54**, 27-30 (1857)
- [De<sub>1</sub>] DEDEKIND, R.: *Vorlesung über Differential- und Integralrechnung*. Dokumente zur Geschichte der Mathematik, Band 1. Vieweg, 1985
- [De<sub>2</sub>] DEDEKIND, R.: *Stetigkeit und Irrationalzahlen*. Vieweg, 1872
- [De<sub>3</sub>] DEDEKIND, R.: *Was sind und was sollen die Zahlen*. Vieweg, 1888
- [DMV] *Ein Jahrhundert Mathematik, 1890-1990. Festschrift zum Jubiläum der DMV*. Vieweg, 1990
- [Dü] DÜRER, A.: *Underweysung der messung mit dem zirckel un richt scheyt in Linien ebnen unnd gantzen corporen*. Nürnberg, 1525
- [Eb] EBBINGHAUS, H.-D. et al.: *Zahlen*. Springer 1992<sup>3</sup>
- [Eu] EUKLID: *Die Elemente*. Hrsg. C. Thaeer, Wiss. Buchgesellschaft 1980
- [F-T] FEIT, W., J.G. THOMPSON: *Solvability of groups of odd order*. Pac. J. Math. **13**, 775-1029 (1963)
- [Fi<sub>1</sub>] FISCHER, G.: *Lineare Algebra*. Vieweg 2014<sup>18</sup>
- [Fi<sub>2</sub>] FISCHER, G.: *Analytische Geometrie*. Vieweg 2001<sup>7</sup>
- [Fi<sub>3</sub>] FISCHER, G.: *Plane Algebraic Curves*. AMS 2001
- [Fi<sub>4</sub>] FISCHER, G.: *Lernbuch Lineare Algebra und Analytische Geometrie*. Springer 2017<sup>3</sup>
- [F-L] FISCHER, W., I. LIEB: *Funktionentheorie*. Vieweg 2005<sup>9</sup>
- [G] GALOIS, É.: *Écrits et mémoires mathématiques*. Gauthier-Villars 1962

- [Ga<sub>1</sub>] GAUSS, C.F.: *Demonstratio nova theorematis omnem functionem algebraicam rationalem integrum unius variabilis in factores reales primi vel secundi gradus resolvi posse*. In: Werke, Band III, 1-30
- [Ga<sub>2</sub>] GAUSS, C.F.: *Die vier Gauss'schen Beweise für die Zerlegung ganzer algebraischer Funktionen*. Herausgegeben von E. NETTO. Oswald's Klassiker der exakten Wissenschaften Nr. 14. Akademische Verlagsgesellschaft 1913
- [Ga<sub>3</sub>] GAUSS, C.F.: *Disquisitiones arithmeticae*, 1801. Gesammelte Werke, Band I. Deutsche Übersetzung: *Untersuchungen über höhere Arithmetik*, 1889
- [Ga<sub>4</sub>] GAUSS, C.F.: *Theoria residuorum biquadraticorum, Commentatio secunda* 1831. In: Gesammelte Werke, Band II. Deutsche Übersetzung im Anhang zu: *Untersuchungen über höhere Arithmetik*, 1889
- [Gr] GRASSMANN, H.: *Die Ausdehnungslehre*. Enslin, 1862
- [Ham] HAMILTON, W.: *Researches Representing Quaternions, First Series*. In: *Collected Papers* Vol. III, Part II.
- [Har] HARTSHORNE, R.: *Geometry: Euclid und Beyond*. Springer, 2000
- [Ha] HASSE, H.: *Vorlesungen über Zahlentheorie*. Springer 1950
- [He] HERMES, J.: *Über die Teilung des Kreises in 65537 gleiche Teile*. Nachrichten von der Königl. Ges. d. Wiss. zu Göttingen, Math.-phys. Kl. 1894, 170-186
- [Her] HERMITE, C.: *Sur la fonction exponentielle*. C.R.Acad.Sci. Paris **77**, (1873)
- [Hi<sub>1</sub>] HILBERT, D.: *Die Theorie der algebraischen Zahlkörper*. Jahresber. DMV **4**, 175-546, 1897
- [Hi<sub>2</sub>] HILBERT, D.: *Grundlagen der Geometrie*. Teubner, 1899
- [Hi<sub>3</sub>] HILBERT, D.: *Über den Zahlbegriff*. Jahresber. DMV **8**, 180-184, 1900
- [Hi<sub>4</sub>] HILBERT, D.: *Mathematische Probleme*. Nachr. Kgl. Ges. d. Wiss. Göttingen, math.-phys. Klasse, **3**, 253-297, 1900
- [Hi<sub>5</sub>] *Die Hilbertschen Probleme*. Akademische Verlagsgesellschaft, 1971
- [H-C] HILBERT, D., S. COHN-VOSSEN: *Anschauliche Geometrie*. Springer 1932
- [Hou] HOUZEL, C.: *Le rôle de Bourbaki dans les mathématiques du vingtième siècle*. Gazette de la SMF, **100**, 53-63, 2004
- [Hu] HULEK, K.: *Elementare Algebraische Geometrie*. Vieweg 2000
- [J] JUNGnickel, D.: *Finite Fields*. Bibl. Inst. 1993
- [Ka] KANT, I.: *Versuch den Begriff der negativen Größen in die Weltweisheit einzuführen*. J. Kanter, 1763. Werkausgabe 2, Suhrkamp, 1977
- [Ke] KEMPER, G.: *Algebra*. Vorlesungsskript, TU München 2011
- [Kl] KLEIN, F.: *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert*. Springer, 1926
- [Kl<sub>1</sub>] KLEIN, F.: *Vorlesungen über das Ikosaeder und die Auflösung von Gleichungen vom fünften Grade*. Teubner 1884. Kommentierte Neuauflage Birkhäuser 1993
- [Kl<sub>2</sub>] KLEIN, F.: *Vorträge über ausgewählte Fragen der Elementargeometrie*, ausgearbeitet von F. Tägert. Teubner 1895
- [Kli] KLINE, M.: *Why Johnny Can't Add*. Random House, 1973
- [Kn] KNÖRRER, H.: *Geometrie*. Vieweg 2006<sup>2</sup>
- [K-R] KOECHER, M. UND R. REMMERT: *HAMILTONSche Quaternionen*. In: *Zahlen*. Springer 1992<sup>3</sup>

- [Kö] KÖNIGSBERGER, K.: *Analysis I*. Springer 2001<sup>5</sup>
- [Kr] KRONECKER, L.: *Über einige Anwendungen der Modulsysteme auf elementare algebraische Fragen*. Journ. r. u. a. Math. **99**, 329-371, 1886
- [K-S] KURZWEIL, H. UND B. STELLMACHER: *The Theory of Finite Groups*. Springer, 2004
- [Le] LEAVITT, W. G.: *A Theorem on Repeating Decimals*. Am. Math. Monthly **74**, 669-673, 1967.
- [L-N] LIDL, L., NIEDERREITER, H.: *Introduction to finite fields and their applications*. Cambridge University Press, 1986
- [Li] LINDEMANN, F.: *Über die Zahl  $\pi$* . Math. Ann. **20**, 213-225
- [Lip] LIPSCHITZ, L.: *Briefwechsel mit Cantor, Dedekind, Helmholtz, Kronecker, Weierstrass und anderen*. Bearbeitet von W. Scharlau, Vieweg, 1986
- [M] MACAULAY, F.S.: *Algebraic Theory of Modular Systems*. Cambridge 1916
- [Ma] MATZAT, B.H.: *Konstruktive Galoistheorie*. Lecture Notes in Mathematics 1284. Springer 1987
- [Mi] MICHLER, G.O.: *Vom Hilbertschen Basissatz bis zur Klassifikation der endlichen einfachen Gruppen*. In: Ein Jahrhundert Mathematik, 1890-1990. Vieweg 1990
- [M-P] MÜLLER-STACH, S., J. PIONTKOWSKI: *Elementare und algebraische Zahlentheorie*. Vieweg 2007
- [Ne] NEUKIRCH, J.: *Algebraische Zahlentheorie*. Springer 1992
- [N-S-T] NEUMANN, P.M., G.A. STOY, E.C. THOMPSON: *Groups and geometry*. Oxford Univ. Press 1994
- [Pe<sub>1</sub>] PEANO, G.: *Calcolo Geometrico secondo l'Ausdehnungslehre di H. Grassmann, preceduto dalle operazioni della logica detuttiva*. Frat. Bocca, 1888, Englische Übersetzung *Geometric Calculus* von L. C. KANNENBERG. Birkhäuser, 2000
- [Pe<sub>2</sub>] PEANO, G.: *Arithmetices principia nova exposita*. Frat. Bocca, 1889
- [Pe] PERRON, O.: *Eine neue Winkeldreiteilung des Schneidermeisters KOPF*. Sitzungsber. bayr. Akad. d. Wiss., math.-nat. Abt. 1933, 439-445
- [R-U] REMMERT, R. und P. ULLRICH: *Elementare Zahlentheorie*. Birkhäuser 1995
- [Ri] RICHELOT, F.: *De resolutione algebraica aequationis  $X^{257} = 1$ , sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata*. J. Reine Angew. Math. **9** (1832)
- [S] SARGES, H.: *Ein Beweis des Hilbertschen Basissatzes*. J. Reine Angew. Math. **283/ 284**, 436-437 (1976)
- [Sa] ŠAFAREVIČ, I.R.: *Construction of fields of algebraic numbers with given solvable Galois group*. Izv. Akad. Nauk. SSSR. Ser. Math. **18**, 525-578 (1954); AMS Translation, Ser. 2, Vol. 4, 185-237 (1956)
- [Sl] SŁODOWY, P.: *Das Ikosaeder und die Gleichungen fünften Grades*. In: Mathematische Miniaturen 3. Birkhäuser 1986
- [St] STEINITZ, E.: *Algebraische Theorie der Körper*. J. Reine Angew. Math. **137**, 167-309 (1910)
- [Sy] SYLOW, M.L.: *Théorèmes sur les groupes de substitutions*. Math. Ann. **5**, 584-594 (1872)
- [W<sub>2</sub>] VAN DER WAERDEN, B.L.: *A history of Algebra. From al-Khwarizmi to Emmy Noether*. Springer 1985
- [We<sub>2</sub>] WEBER, H.: *Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie*. Math. Ann. **43**, 521-549, 1893
- [We<sub>3</sub>] WEBER, H.: *Theorie der Abel'schen Zahlkörper*. Acta Math. **8**, 193-263 (1886)

- [Wey] WEYL, H.: *Raum-Zeit-Materie. Vorlesungen über allgemeine Relativitätstheorie*. Springer, 1918
- [Wi] WIELANDT, H.: *Ein Beweis für die Existenz der Sylowgruppen*. Arch. Math. 10, 401-402 (1959).
- [Wu] WUSSING, H.: *Die Genesis des abstrakten Gruppenbegriffs*. Deutscher Verlag der Wissenschaften, 1969
- [Wu<sub>1</sub>] WUSSING, H.: *6000 Jahre Mathematik*. Springer 2008 .
- [Za] ZADDACH, A.: *Grassmanns Algebra in der Geometrie*. Bibliographisches Institut, 1994

Ein „Exponent“ an der Jahreszahl gibt die Nummer der Auflage an.

# Index

- Abbildung
  - kanonische, 46
- Ableitung
  - formale, 332
- Abschluss
  - algebraischer, 311, 328, 345
  - relativer algebraischer, 308
- Absolutbetrag, 178
- Adjunktion, 175, 295
  - symbolische, 313
- Algorithmus
  - euklidischer, 77
- Anordnung
  - lexikografische, 197
- Anteil
  - homogener, 195
- Assoziativgesetz, 8
- Auswahlaxiom, 233
- Auswertung, 229
- Automorphismengruppe, 30, 90, 364
- Automorphismus
  - innerer, 34, 106
  - relativer, 364
  - von Gruppen, 28
  - von Ringen, 175
  
- Bahn, 104
- Bahn-Lemma, 104
- Bahngleichung, 105
- Bahnenraum, 104
- Bahnsumme, 428
- Basis, 100
- Basissatz von HILBERT, 220
- Berechnung des Inversen, 301
- Bild, 28, 175
  
- CARDANO-Formel, 393
- casus irreducibilis, 393
- CAUCHY-Produkt, 183
- CAYLEYSche Kubik, 357
- Charakter, 418
- Charakteristik, 292
- Chinesischer Restsatz, 75, 223
- Codierung, 97
  
- Delisches Problem, 437
- Diedergruppe, 66, 154
- Diskriminante, 353, 387
- Distributivgesetze, 171
- Division mit Rest, 14, 188, 190, 215
- Divisionsalgebra, 179
- Dodekaeder, 123, 455
- Don Giovanni Gruppen, 159
- Dualität, 456
  
- Einbettung
  - von Halbgruppen, 201
- Einbettungssatz, 330
- Einheit, 86, 173, 187, 207, 211, 272
- Einheitengruppe, 86, 173
- Einheitswurzel, 22, 192, 404, 411
  - primitive, 22, 404
- Einselement, 172
- Einsetzungshomomorphismus, 185, 187, 297
- EISENSTEIN-Kriterium, 257
- Element
  - algebraisches, 297
  - assoziiertes, 235
  - inverses, 6, 8
  - invertierbares, 6
  - irreduzibles, 236
  - linksinverses, 9

- linksneutrales, 6, 9
- maximales, 233
- neutrales, 6, 8
- primes, 237
- primitives, 296, 346, 347
- rechtsneutrales, 6
- reduzibles, 236
- separables, 335
- transzendentes, 297
- Elementarmatrix, 114
- Elementarteiler, 132
- Endlichkeits-Satz, 372
- Endomorphismenring, 180
- Endomorphismus
  - von Gruppen, 28
  - von Ringen, 175
- Epimorphismus
  - von Gruppen, 28
  - von Ringen, 175
- Ergänzung
  - quadratische, 391
- Erweiterung
  - eines Zahlbereichs, 200
- EUKLIDISCHER Algorithmus, 77, 248
- EUKLIDISCHER Ring, 215, 255, 276
- EULERSche  $\phi$ -Funktion, 87
- Exponent
  - einer Gruppe, 130
  - eines Primfaktors, 247
- Faktorgruppe, 46, 166
- Faktorisierungssatz, 50, 209
- Faltung, 183
- Familie
  - freie, 98
- Fehlstand, 32
- FERMATkurve, 260
- FIBONACCI-Folge, 80
- Fixkörper, 370
- formale Potenzreihe, 186, 194, 218
- Formel
  - von CARDANO, 393
- Fortsetzungssatz
  - für Körperisomorphismen, 319
- freshman's dream, 337
- FROBENIUS
  - Homomorphismus, 337
  - Regel, 337
- Fundamentalsatz der Algebra, 310, 383, 384
- Funktion
  - holomorphe, 179, 264
  - meromorphe, 204
  - rationale, 204
  - stetige, 219
- GALOIS-Erweiterung, 373
- GALOISgruppe, 364
- Ganzheitsring, 269
- GAUSSsche Periode, 428
- Gebiet, 179
- Gleichung
  - PELLsche, 272
  - allgemeine, 423
  - DIOPHANTische, 272
  - fünften Grades, 424
  - kubische, 391
  - quadratische, 391
  - vierten Grades, 397
- goldener Schnitt, 449, 454
- Grad
  - einer Körpererweiterung, 294
  - eines Polynoms, 186, 195–197
  - gewichteter, eines Polynoms, 361
  - totaler, eines Polynoms, 196
- Gradformel
  - für Körper, 294
  - für Polynome, 186
- GRASSMANN-Varietäten, 467
- GRÖBNERbasis, 221
- Gruppe, 8
  - abelsche, 8
  - allgemeine lineare, 20
  - alternierende, 33
  - auflösbare, 167
  - der relativen Automorphismen, 364
  - einfache, 162
  - endlich erzeugte, 13
  - frei-abelsche, 98
  - invertierbarer Matrizen, 20
  - kommutative, 8
  - orthogonale, 20, 48
  - spezielle lineare, 42, 48
  - spezielle orthogonale, 32, 48
  - symmetrische, 19, 63
  - torsionsfreie, 143
  - triviale, 18
  - zyklische, 16, 19, 47, 69, 198

- Halbgruppe, 6
- Halbgruppenring, 195
- Halbordnung, 233
- Hauptideal, 206, 214
- Hauptidealring, 214, 216, 242, 255
- Hauptsatz
  - der GALOIS-Theorie, 376, 390
  - der elementaren Zahlentheorie, 244
  - symmetrische Polynome, 361
- HILBERTscher Nullstellensatz, 232
- Homomorphismus
  - von Gruppen, 28
  - von Ringen, 175
- Ideal, 206, 226
  - Korrespondenzsatz, 209
  - Produkt, 222
  - Summe, 222
  - coprime, 223
  - erzeugtes, 214
  - maximales, 228, 231, 234
  - primes, 228
  - triviales, 206
- Idealkette
  - stationäre, 214
- Ikosaeder, 123, 454
  - gestutztes, 457
- Ikosaedergleichung, 426
- Ikosaedergruppe, 123
- Imaginärteil, 266
- Index
  - einer Untergruppe, 38
- Inhalt
  - eines Polynoms, 250, 251
- Inklusion, 34
- Integritätsring, 173, 255
- Interpolationsformel
  - von LAGRANGE, 192
- Interpolationspolynom, 192
- Invarianten, 132
- Inversion, 35
- Irrationalteil, 267
- Irreduzibilität, 236
- Irreduzibilitäts-Satz, 253
- Isomorphiesatz
  - dritter, 52
  - erster, 51, 209
  - zweiter, 62, 223
- Isomorphismus
  - von Gruppen, 28
  - von Ringen, 175
- Isotropiegruppe, 104
- Kern, 28, 175
- Kette, 233
- Klassengleichung, 107
  - der Ikosaedergruppe, 127
- Klassifikation
  - endlicher abelscher Gruppen, 131, 141
  - von Gruppen, 50
  - von zyklischen Gruppen, 70
- KLEINSche Vierergruppe, 19, 30, 62
- Koeffizient, 183, 194
  - allgemeiner, 423
- Körper, 174, 255
  - PLATONischer, 453
  - algebraisch abgeschlossener, 309
  - der meromorphen Funktionen, 204
  - der rationalen Funktionen, 204
  - endlicher, 340
  - vollkommener, 338
- Körpererweiterung, 174, 293
  - algebraische, 306
  - biquadratische, 397
  - einfache, 296
  - endliche, 294
  - GALOISSche, 373
  - normale, 323
  - separable, 335
  - transzendente, 306
  - zyklische, 417
- Körpergrad, 294
- Kommutator, 164
- Kommutatorgruppe, 164
  - höhere, 166
- Kongruenz, 15, 37, 208
  - simultane, 75
- Konjugation, 34, 103, 106, 267
- Konjugationsklasse, 112
- Konstruktion
  - mit Zirkel und Lineal, 438
- Konstruktionsschritte
  - elementare, 438
- Korrespondenzsatz
  - für Ideale, 209
- Kreisteilungskörper, 408
- Kreisteilungspolynom, 405, 411
- KRONECKER-Verfahren, 258



- Kürzungsregeln, 10
- Kummerring, 237, 286, 287
- LAGRANGESche Resolvente, 419
- Leitkoeffizient, 186
- Leitterm, 186
- Lemma
  - von ARTIN, 418
  - von GAUSS, 251
  - von ZORN, 234
- Linkstranslation, 10, 103
- Matrixdarstellung, 181
- Matrizenring, 181
- Menge
  - induktiv geordnete, 233
- Minimalpolynom, 269, 299
- Monom, 183, 194, 196, 328
  - primitives, 183, 195, 328
- Monomorphismus
  - von Gruppen, 28
  - von Ringen, 175
- Multiindex, 194
- $n$ -Eck
  - regelmäßiges, 115, 437
- Nebenklasse
  - linke, 36
  - rechte, 36
- Negatives, 8
- NEILSche Parabel, 357
- Norm, 178, 217, 237, 267
- Normalisator, 60
- Normalreihe, 166
- Normalteiler, 44
- Normalteiler-Satz, 153
- Nullelement, 8, 171
- Nullring, 172
- Nullstelle, 186
  - allgemeine, 423
  - einfache, 332
  - mehrfache, 332
- Nullstellenmenge, 226
- Nullteiler, 172, 187
- Oberkörper, 174
- Oktaeder, 120, 454
- Oktaven, 179
- Operation, 102
  - effektive, 103
  - einfach transitive, 103
  - transitive, 103
- Ordnung
  - einer Gruppe, 38
  - einer Menge, 233
  - einer Potenzreihe, 218
  - eines Elements, 38
- $p$ -Gruppe, 137, 148
- $p$ -Sylowgruppe, 149
- $p$ -Untergruppe, 149
- Partition, 137, 139
- Pentagon, 449
- Permutation
  - gerade, 32
  - ungerade, 32
- Permutationsgruppe, 19
- Permutationsmatrix, 113
- Polyeder
  - konvexes, 458
  - reguläres, 453
- Polyederformel, 456
- Polynom, 183, 194, 195
  - allgemeines, 423
  - durch Radikale lösbares, 419
  - elementarsymmetrisches, 360
  - homogenes, 197
  - normiertes, 187
  - primitives, 250
  - reines, 414, 415
  - separables, 335
  - symmetrisches, 360
- Polynomfunktion, 185
- Polynomring, 184, 328, 329
- Potenzreihe
  - formale, 186, 194, 218
- Primärkomponente, 137, 138
- Primelement, 237
  - träges, 281
  - unverzweigtes, 281
  - verzweigtes, 281
- Primideal, 228
- Primitivzahl, 428
- Primkörper, 211, 292
- Primrestklassengruppe, 86, 211, 412
- Primzahl, 242
  - FERMATSCHE, 448
  - MERSENNEsche, 345

## Produkt

- äußeres semidirektes, 58
- äußeres direktes, 53
- inneres direktes, 55–57
- inneres semidirektes, 61
- von Idealen, 222
- zyklischer Gruppen, 81

## Produkttring, 179

## Progression

- arithmetische, 435

## Prüfziffer, 25

## Punkt

- konstruierbarer, 439

## Punktgitter, 21

## pythagoreische Tripel, 2

## Quadratur des Kreises, 437

## Quaternionen, 181, 465

## Quaternionengruppe, 21, 49, 183

## Quersumme, 23

## Quotient, 188

## Quotientenkörper, 202

## Quotientenvektorraum, 47

## Radikal, 414

## Radikalerweiterung, 419

## Rang, 100

## Rationalteil, 267

## Realteil, 266

## Rechteck

- goldenes, 454

## Rechtstranslation, 10, 103

## Reduktions-Kriterium, 257

## Regel

- von FROBENIUS, 337

## Reihe

- hypergeometrische, 426

## Relation, 97

- von BÉZOUT, 72, 248

## Resolvente, 426

- LAGRANGESche, 419
- irrationale, 427
- kubische, 398
- quadratische, 392

## Rest, 14, 188

## Restklasse, 15

- primitive, 199

## Restklassenring, 208

## Resultante, 349

## Ring, 171

- der formalen Potenzreihen, 186, 218
- der stetigen Funktionen, 219
- EUKLIDischer, 215, 255, 276
- faktorieller, 246, 254, 255
- kommutativer, 172
- NOETHERscher, 214, 219
- nullteilerfreier, 172

## RSA-Kryptosystem, 95

## Satz

- Fortsetzung von Körperisomorphismen, 319
- Produkt zyklischer Gruppen, 82
- Untergruppen von  $\mathbb{Z}$ , 13
- Untergruppen zyklischer Gruppen, 83
- endliche Untergruppen von  $O(2)$ , 118
- kleiner, von FERMAT, 24
- symbolische Adjunktion von Nullstellen, 313
- über vollkommene Körper, 338
- vom primitiven Element, 346
- von CAUCHY, 147
- von CAYLEY, 35
- von DIRICHLET, 435
- von EULER, 282
- von FERMAT-EULER, 88
- von GAUSS, 254
- von KRONECKER und WEBER, 436
- von LAGRANGE, 38, 112
- von SYLOW, 150

## Schiefkörper, 174

- der Quaternionen, 183

## Schnitt

- goldener, 449, 454

## Schranke

- obere, 233

## Sieb des ERATOSTHENES, 245

## Signum, 32

## Sphäre, 453

## Spur, 267

## Stabilisator, 104

## Standgruppe, 104

## Struktursatz

- Primrestklassengruppen, 87
- endlich erzeugte abelsche Gruppen, 146
- endliche Körper, 340
- endliche abelsche  $p$ -Gruppen, 137
- endliche abelsche Gruppen, 132, 136
- konstruierbare Punkte, 441

## Substitutionshomomorphismus, 185

- Summe
  - direkte, 57
  - von Idealen, 222
- Sylowgruppe, 149
- Symmetrie, 19, 115
- Symmetriegruppe, 115
- Teilbarkeits-Lemma, 73
- Teilbarkeitssatz
  - von EUKLID, 243
- Teiler, 71, 235
  - echter, 235
  - gemeinsamer, 72
  - größter gemeinsamer, 72, 247, 334
- Teilerkette, 240
  - stationäre, 240
- Teilerkettensatz, 240
- Teilersummen-Formel, 89, 405
- Tetraeder, 119, 453
- Tetraedergruppe, 119
- Theorem
  - von FEIT und THOMPSON, 169
- Torsionsuntergruppe, 143
- Translation, 34
- Transposition, 33
- TSCHIRNHAUS-Transformation, 354
- Unbestimmte, 183
- Unendlichkeitssatz von EUKLID, 244
- Untergruppe, 11
  - erzeugte, 12
  - triviale, 12
  - von  $\mathbb{Z}$ , 13
- Unterkörper, 174
  - erzeugter, 295
- Unterring, 174
  - erzeugter, 175, 295
- Verknüpfung
  - abelsche, 8
  - assoziative, 5, 8
  - innere, 5
  - kommutative, 5
- Verknüpfungstafel, 5
- Verschlüsselung, 97
- Vertretersystem, 105, 247
- Vielfaches, 72, 235
  - gemeinsames, 72
  - kleinstes gemeinsames, 72, 248
- Vielfachheit
  - einer Nullstelle, 191, 332
- Winkeldreiteilung, 437
- Wohldefiniertheit, 16
- Würfel, 120, 454
- Würfelgruppe, 120
- Würfelverdoppelung, 437
- Wurzel, 414
- Wurzelsatz von VIETA, 360
- Zahl
  - ganze, 13, 269
  - ganze GAUSSsche, 21, 178, 217
  - ganzrationale, 13, 269
  - ideale, 287
  - komplex konjugierte, 178
  - paarweise teilerfremde, 73
  - quadratfreie, 266
  - teilerfremde, 73
- Zahlenebene, 177, 301
- Zahlkörper, 266
  - algebraischer, 266
  - imaginär-quadratischer, 205, 266
  - quadratischer, 266
  - reell-quadratischer, 266
- Zahlring
  - quadratischer, 269
- Zentralisator, 106
- Zentrum, 106, 114
- Zerfällungskörper, 320
- Zwischenkörper, 177, 293
- Zyklusstruktur, 112
- Zykluszerlegung, 108
- Zyklus, 108
  - elementfremder, 108

# Symbolverzeichnis

$\mathbb{N}$	natürliche Zahlen, 6	$S_p$	$p$ -Sylowgruppe, 150
$\mathbb{Z}$	ganze Zahlen, 6, 13	$\sigma_g$	Einsetzungshomomorphismus, 187
$\mathbb{Q}$	rationale Zahlen, 8, 177	$Z_n, Z(n)$	zyklische Gruppe, 16, 84
$\mathbb{R}$	reelle Zahlen, 8	$Z_n^\times$	Primrestklassengruppe, 86
$\mathbb{C}$	komplexe Zahlen, 21, 177	$\zeta_n$	primitive $n$ -te Einheitswurzel, 22
$\mathbb{H}$	Quaternionen, 181	$\text{Abb}(M, N)$	Menge von Abbildungen, 7
$\mathbb{F}_q$	Körper mit $q$ Elementen, 18, 340	$\text{Aut}(G), \text{Aut}(K)$	Automorphismengruppe, 29, 364
$A_n$	alternierende Gruppe, 33	$\text{Aut}(K; k)$	relative Automorphismen, 364
$C_n$	$n$ -te Einheitswurzeln, 22	$\mathcal{C}(M, \mathbb{R})$	stetige Funktionen, 179
$D_n$	Diedergruppe, 66	$\text{char}(R)$	Charakteristik, 292
$e$	Eulersche Zahl, 301	$\text{deg}(f)$	Grad eines Polynoms, 186
$f_a$	Minimalpolynom von $a$ , 299	$\text{dis}(f), \Delta(f)$	Diskriminante, 353
$G_p$	Primärkomponente von $G$ , 137	$\text{End}(G)$	Endomorphismenring von $G$ , 180
$i$	imaginäre Einheit, 21, 177	$\text{Erz}(M)$	Erzeugnis von $M$ , 12, 175
$\iota$	Inklusion, 34	$\text{exp}(G)$	Exponent von $G$ , 130
$\bar{k}$	algebraischer Abschluss von $k$ , 311	$\text{Fix}(K; G)$	Fixkörper, 370
$K^*$	Körper ohne Null, 65	$G(x)$	Bahn von $x$ , 104
$\kappa_a$	Konjugation, 34	$G/H$	linke Nebenklassen, 37
$\mathcal{K}_4$	Kleinsche Vierergruppe, 19	$H \setminus G$	rechte Nebenklassen, 37
$l_a$	Linkstranslation, 10, 34, 174	$G/N$	Faktorgruppe von $G$ nach $N$ , 46
$\mathcal{O}_d$	quadratischer Zahlring, 269	$\text{Gal}(f; k)$	Galoisgruppe, 364
$P_n$	regelmäßiges $n$ -Eck, 115	$\text{ggT}$	größter gemeinsamer Teiler, 72, 248
$\Phi_n, \Phi_n^{(p)}$	Kreisteilungspolynom, 405, 411	$\text{GL}(n; K)$	allgemeine lineare Gruppe, 20
$Q$	Quaternionengruppe, 21, 49	$aH$	linke Nebenklasse von $a$ bzgl. $H$ , 36
$r_a$	Rechtstranslation, 10, 34	$Ha$	rechte Nebenklasse von $a$ bzgl. $H$ , 36
$R^\times$	Einheitengruppe von $R$ , 173	$\text{im}(\alpha)$	Imaginärteil, 266
$R^*$	Ring ohne Null, 173	$\text{Im } \varphi$	Bild von $\varphi$ , 28, 175
$S_n$	symmetrische Gruppe, 19	$\text{ind}(G : H)$	Index von $G$ in $H$ , 38
$s_p$	Anzahl der $p$ -Sylowgruppen, 150	$\text{inh}(f)$	Inhalt eines Polynoms, 250

$\text{ir}(\alpha)$	Irrationalteil, 267	$Z(G)$	Zentrum, 106
$k(A)$	Körperadjunktion, 295	$\mathbb{Z}[i]$	ganze GAUSSsche Zahlen, 204, 217
$K \supset k$	Körpererweiterung, 176, 293	$k + n\mathbb{Z}$	Restklasse modulo $n$ , 15
$\text{Ker } \varphi$	Kern von $\varphi$ , 28, 175	$\mathbb{Z}/n\mathbb{Z}$	Menge der Restklassen, 15
$\text{kgV}$	kleinstes gemeinsames Vielfaches, 73, 248	$\text{Zen}_G(x)$	Zentralisator, 106
$\text{Kom}(G)$	Kommutatorgruppe, 164	$(A)$	erzeugtes Ideal, 214
$\text{Kon}(M)$	konstruierbare Punkte, 439	$(a_1, \dots, a_n)$	erzeugtes Ideal, 214
$M(n \times n; K)$	Matrizenring, 182	$(N_0, \dots, N_k)$	Normalreihe, 166
$\mu(f; x)$	Vielfachheit einer Nullstelle, 332	$(x_1, \dots, x_n)$	$n$ -Zyklus, 108
$N(\alpha)$	Norm, 217, 267	$[a, b]$	Kommutator, 164
$\text{Nor}_G(H)$	Normalisator, 60	$[K : k]$	Körpergrad, 294
$O(n)$	orthogonale Gruppe, 20	$\#M$	Anzahl der Elemente, 38
$\text{ord}(a)$	Ordnung eines Elements $a$ , 38	$\mathfrak{a} + \mathfrak{b}$	Summe von Idealen, 222
$\text{ord}(G)$	Ordnung einer Gruppe $G$ , 38	$\mathfrak{a} \cdot \mathfrak{b}$	Produkt von Idealen, 222
$P(n)$	Anzahl der Partitionen von $n$ , 140	$a b$	$a$ teilt $b$ , 71, 235
$\varphi(n)$	Eulersche $\varphi$ -Funktion, 87	$a \sim b$	$a$ assoziiert $b$ , 235
$Q(R)$	Quotientenkörper von $R$ , 203	$\leq$	Halbordnung, 233, 331
$R[a]$	Ringadjunktion, 175	$<$	Untergruppe, 11
$R[X]$	Polynomring, 183	$\triangleleft$	Normalteiler, 44
$R[[X]]$	Ring der formalen Potenzreihen, 186	$\equiv$	kongruent, 15, 37, 208
$R[X_1, \dots, X_n]$	Polynomring in $n$ Veränderlichen, 194	$\cong$	isomorph, 28
$Ra, (a)$	von $a$ erzeugtes Hauptideal, 206	$\oplus$	direkte Summe, 57
$R/\mathfrak{a}$	Restklassenring, 208	$\times$	direktes Produkt, 53
$\text{ra}(\alpha)$	Rationalteil, 267	$\times_{\Phi}$	äußeres semidirektes Produkt, 58
$\text{rang } G$	Rang, 100	$\times$	inneres semidirektes Produkt, 61
$\text{re}(\alpha)$	Realteil, 266		
$\text{res}(f, g)$	Resultante, 349		
$S(\alpha)$	Spur, 267		
$\text{sign } \sigma$	Signum einer Permutation, 32		
$\text{SL}(n; K)$	spezielle lineare Gruppe, 42, 48		
$\text{SO}(n)$	spezielle orthogonale Gruppe, 32		
$\text{Sta}_G(x)$	Standgruppe von $x$ , 104		
$T(G)$	Torsionsuntergruppe, 143		
$v_p(a)$	Exponent von $p$ bezüglich $a$ , 247		