

- of Finitely Generated Modules over a P.I.D., 462, 464, 466
 - of Galois Theory, 574ff.
 - on Symmetric Functions, 608
- G**
- G -invariant, 843
 - G -module, 798
 - G -stable, 843
 - Galois closure, 594
 - Galois cohomology groups, 809ff.
 - Galois conjugates, 573
 - Galois extension, 562, 572ff.
 - Galois group, 562ff., 574ff.
 - of \mathbb{F}_{p^n} , 566, 586
 - of $\mathbb{Q}(2^{1/8}, i)$ or $x^8 - 2$, 577ff.
 - of $\mathbb{Q}(2^{1/8}, i)$ over quadratic subfields, 581
 - of $\mathbb{Q}(\sqrt{(2 + \sqrt{2})(3 + \sqrt{3})})$, 584
 - of $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$, 582
 - of $\mathbb{Q}(\sqrt{2})$, 563
 - of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, 563ff., 567, 576
 - of $\mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$, 582
 - of $\mathbb{Q}(\zeta_{13})$, 598ff.
 - of $\mathbb{Q}(\zeta_5)$, 597
 - of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, 601, 603
 - of $\mathbb{Q}(\zeta_n)$, 596ff.
 - of $\mathbb{Q}(\zeta_p)$, 597
 - of $x^3 - 2$, 564ff., 568, 576
 - of $x^4 + 1$, 579ff.
 - of $x^4 - 2x^2 - 2$, 582
 - of $x^6 - 2x^3 - 2$, 623, 644
 - of $x^n - a$, 636
 - of $x^p - x - a$, 589
 - of a biquadratic, 582
 - of a composite extension, 592
 - of a cubic, 612
 - of a cyclotomic field, 599
 - of a general polynomial, 609
 - of a quadratic, 563
 - of a quartic, 615, 618
 - Galois groups, of polynomials, 606ff.
 - infinite, 651ff.
 - over \mathbb{Q} , 640ff.
 - Galois Theory, 14, 105, 558ff.
 - Gaschütz's Theorem, 838
 - Gauss' Lemma, 303, 530, 819, 824
 - Gauss–Jordan elimination, 327, 424ff.
 - Gauss sum, 637
 - Gaussian integers, 229ff., 271, 278, 289ff., 377
 - general linear group, 35, 89, 236, 413, 418
 - general polynomial, 607, 609, 629, 646
 - general polynomial division, 320ff., 331
 - generalized associative law, 18
 - generalized character, 898
 - generalized eigenspace, 501
 - generalized quaternion group, 178
 - generating set, 61ff.
 - generator, 25ff., 54, 218ff.
 - of S_n , 64, 107ff., 219
 - of S_p , 111
 - of a cyclic group, 57
 - of a free module, 354
 - of a subgroup, 61ff.
 - of a submodule, 351
 - of an ideal, 251
 - generic point, 733
 - germs of continuous functions, 269
 - $GL_3(\mathbb{F}_2)$, 211ff., 489, 644
 - global sections, 740
 - globally asymptotically stable, 508
 - Going-down Theorem, 694, 728
 - Going-up Theorem, 694, 720
 - graded, ordering, 331
 - ring, 443
 - graded ideal, 443
 - graded lexicographic ordering (grlex), 331
 - graph, 210, 669, 687
 - coloring, 335ff.
 - greatest common divisor (g.c.d.), 4, 252, 274ff., 287
 - of ideals, 767
 - grevlex monomial ordering, 331
 - Gröbner basis, 315ff., 319ff., 664ff., 702, 712
 - in field extensions, 672
 - group, 13, 16ff.
 - of n^{th} roots of unity — see root of unity
 - of units in a ring, 226
 - group extensions, 824ff.
 - group ring, 236ff., 798, 840
 - group table, 21
 - groups, of order 12, 144, 182
 - of order 30, 143, 182
 - of order 56, 185
 - of order 60, 145ff., 186
 - of order 75, 185
 - of order 147, 185
 - of order 168, 207ff.
 - of order $3^3 \cdot 7 \cdot 13 \cdot 409$, 212ff., 898ff.
 - of order p^2 , 125, 137
 - of order p^3 , 179, 183, 198, 199ff., 886
 - of order $2p^2$, 186
 - of order $4p$, 186
 - of order pq , 143, 179, 181
 - of order p^2q , 144
 - groups, table of small order, 167ff.

H

$H^n(G; A)$ — see cohomology group
 Hall subgroup, 101, 200, 829, 890
 Hall's Theorem, 105, 196, 890
 Hamilton Quaternions, 224ff., 231, 237, 249, 299
 Harmonic Analysis, 875
 Heisenberg group, 35, 53, 174, 179, 187
 Hilbert's Basis Theorem, 316, 334, 657
 Hilbert's Nullstellensatz, 675, 700ff.
 Hilbert's Specialization Theorem, 648
 Hilbert's Theorem 90, 583, 814
 additive form, 584, 815
 Hilbert's Zahlbericht, 815
 Hölder Program, 103ff.
 holomorph, 179, 186
 Hom, of direct products, 404
 of direct sums, 388, 388, 404
 $\text{Hom}_F(V, W)$, 416
 $\text{Hom}_R(M, N)$, 345ff., 385ff.
 homeomorphism, 738
 homogeneous cochains, 810
 homogeneous component, of a polynomial, 297
 of a graded ring, 443
 homogeneous ideal, 299
 homogeneous of degree m , 621
 homogeneous polynomial, 297
 homological algebra, 391, 655, 776ff.
 homology groups, 777
 homomorphism, of algebras, 343, 657
 of complexes, 777
 of fields, 253, 512
 of graded rings, 443
 of groups, 36, 73ff., 215
 of modules, 345ff.
 of rings, 239ff.
 of short exact sequences, 381ff.
 of tensor algebras, 450
 homotopic, 792
 hypernilpotent group, 191
 hypersurface, 659

I

icosahedron — see Platonic solids
 ideal quotient, 333, 691
 ideal, 242ff.
 generated by set, 251
 idempotent, 267, 856
 idempotent linear transformation, 423
 identity, of a group, 17
 matrix, 236
 of a ring, 223
 image, of a map, 2

 of a k -algebra homomorphism, computing, 665ff.
 of a linear transformation, computing, 429
 implicitization, 678
 incidence relation, 210
 indecomposable module, 847
 independence of characters, 569, 872
 independent transcendentals, 645
 index, of a subgroup, 90ff.
 of a field extension, 512
 induced, character, 892ff., 898
 module, 363, 803, 811, 812, 893
 representation, 893
 inductive limit — see direct limit
 inequivalent extensions, 379ff.
 inert prime, 749, 775
 infinite cyclic group, 57, 811
 infinite Galois groups, 651ff.
 inflation homomorphism, 806
 inhomogeneous cochains, 810
 injective envelope — see injective hull
 injective hull, 398, 405, 405
 injective map, 2
 injective module, 395ff., 403ff., 784
 injective resolution, 786
 injectively equivalent, 407
 inner automorphism, 134
 inner product of characters, 870ff.
 inseparable degree, of a polynomial, 550
 of a field extension, 650
 inseparable extension, 551, 566
 inseparable polynomial, 546
 insolubility of the quintic, 625, 629
 integer, 1, 695ff.
 integers mod n — see $\mathbb{Z}/n\mathbb{Z}$
 integral basis, 698, 775
 integral closure, 229, 691ff.
 integral domain, 228, 235
 integral element, 691
 integral extension, 691ff.
 integral group ring ($\mathbb{Z}G$), 237, 798
 integral ideal, 760
 integral Quaternions, 229
 integrally closed, 691ff.
 internal, direct product, 172
 direct sum, 354
 intersection of ideals, computing, 330ff.
 intertwine, 847
 invariant factor, 159ff., 464, 774
 decomposition, 159ff., 462ff.
 of a matrix, 475, 477
 Invariant Factor Decomposition Algorithm, 480
 invariant subspace, 341, 843
 inverse, of a map, 2
 of an element in a group, 17

- inverse image, 2
- inverse limit, 268, 358, 652ff.
- inverse of a fractional ideal, 760
- inverse of matrices, 427, 440
- invertible fractional ideal, 760
- irreducibility, criteria, 307ff.
 - of a cyclotomic polynomial, 310
- irreducible algebraic set, 679
- irreducible character, 866, 870, 873
- irreducible element, 284
 - in $\mathbb{Z}[i]$, 289ff.
- irreducible ideal, 683
- irreducible module, 356, 847
- irreducible polynomial, 287, 512ff., 572
 - of degree n over \mathbb{F}_p , 301, 586
- irreducible topological space, 733
- isolated prime ideal, 685
- isomorphism, classes, 37
 - of algebras, 343
 - of cyclic groups, 56
 - of groups, 37
 - of modules, 345
 - of rings, 239
 - of short exact sequences, 381
 - of vector spaces, 408
- Isomorphism Theorems, for groups, 97ff.
 - for modules, 349
 - for rings, 243, 246
- isomorphism type, 37
- isotypic component, 869

J

- Jacobson radical, 259, 750
- join, 67, 88
- Jordan block, 492
- Jordan canonical form, 457, 472, 492ff.
- Jordan–Hölder Theorem, 103ff.

K

- k -stage Euclidean Domains, 294
- k -tensors, 442
- kernel, of a group action, 43, 51, 112ff.
 - of a homomorphism, 40, 75, 239, 345
 - of a k -algebra homomorphism, computing, 665ff.
 - of a k -algebra homomorphism, 678
 - of a linear transformation, computing, 429
- Klein 4-group (Viergruppe), 68, 136, 155
- Kronecker product, 421ff., 431
- Kronecker–Weber Theorem, 600
- Krull dimension, 704, 750ff., 754
- Krull topology, 652

- Krull's Theorem, 652
- Kummer extensions, 627, 817
- Kummer generators for cyclic extensions, 636
- Kummer theory, 626, 816, 823

L

- Lagrange resolvent, 626
- Lagrange's Theorem, 13, 45, 89ff., 460
- lattice of subfields, 574
 - of $\mathbb{Q}(\sqrt[3]{2}, \rho)$, 568
 - of $\mathbb{Q}(\zeta_{13})$, 598
 - of $\mathbb{Q}(2^{1/8}, i)$, 581
- lattice of subgroups, 66ff.
 - of A_4 , 111
 - of D_8 , 69, 99
 - of D_{16} , 70
 - of Q_8 , 69, 99
 - of QD_{16} , 72, 580
 - of S_3 , 69
 - of $\mathbb{Z}/2\mathbb{Z}$, 67
 - of $\mathbb{Z}/4\mathbb{Z}$, 67
 - of $\mathbb{Z}/6\mathbb{Z}$, 68
 - of $\mathbb{Z}/8\mathbb{Z}$, 67
 - of $\mathbb{Z}/12\mathbb{Z}$, 68
 - of $\mathbb{Z}/n\mathbb{Z}$, 67
 - of $\mathbb{Z}/p^n\mathbb{Z}$, 68
 - of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (Klein 4-group), 68
 - of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, 71ff.
 - of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, 72
 - of the modular group of order 16, 72
- lattice of subgroups for quotient group, 98ff.
- Laurent series — see formal Laurent series
- leading coefficient, 234, 295
- leading term, 234, 295, 318
 - ideal of, 318ff.
- least common multiple (l.c.m.), 4, 279, 293
- least residue, 9
- left derived functor, 788
- left exact, 391, 395, 402
- left group action, 43
- left ideal, 242, 251, 256
- left inverse, in a ring, 233
 - of a map, 2
- left module, 337
- left multiplication, 44, 118ff., 531
- left Principal Ideal Domain, 302
- left regular representation, 44, 120
- left translation, 44
- left zero divisor, 233
- Legendre symbol, 818
- length of a cycle, 30
- lexicographic monomial ordering, 317ff., 622
- Lie groups, 505, 876

- lifts, 386
- linear algebraic sets, 659
- linear character, 569
- linear combination, 5, 275, 280, 408
- linear equations, solving, 425ff.
- linear functional, 431
- linear representation, 840
- linear transformation, 340ff., 346, 408
- linearly independent, characters, 569, 872
 - vectors, 409
- local homomorphism, 723, 744
- local ring, 259, 717, 752ff., 755
 - of an affine variety, 721ff.
- localization, 706ff., 795, 796
 - at a point in a variety, 722
 - at a prime, 708ff., 718
 - of a module, 714ff.
- locally ringed spaces, 745
- locus, 659
- Long Exact Sequence, 778, 789
 - in Group Cohomology, 802
- lower central series, 193
- Lüroth's Theorem, 647

M

- map, 1, 215
- Maschke's Theorem, 453, 849
- matrix, 34, 235, 415ff.
 - of a composition, 418
 - of a linear transformation, 415ff.
- matrix representation, 840
- matrix ring, 235ff., 418
 - ideals of, 249
- maximal ideal, 253ff., 280, 512
- maximal order, 232
- maximal real subfield of a cyclotomic field, 603
- maximal spectrum, 731
 - of $k[x]$, 735
 - of $k[x, y]$, 735
 - of $\mathbb{Z}[i]$, 735
 - of $\mathbb{Z}[x]$, 736
- maximal subgroup, 65, 117, 131, 188, 198
 - of solvable groups, 200
- middle linear map — see balanced map
- minimal element, 4
- minimal Gröbner basis, 325ff.
- minimal normal subgroup, 200
- minimal polynomial, 474
 - of a field element, 520
 - of a field element, computing, 667
- minimal prime ideal, 298, 688
- minimal primary decomposition, 683
- minimum condition, 855

- Minkowski's Criterion, 441
- minor, 439
- Möbius inversion formula, 555, 588
- modular arithmetic, 9, 224
- modular group of order 16, 72, 186
- modular representations, 846
- module, 337ff.
 - over \mathbb{Z} , 339, 456ff.
 - over $F[x]$, 340ff., 456ff.
 - over a Dedekind Domain, 769ff.
 - over a group ring, 798ff., 843ff.
 - over a P.I.D., 456ff.
 - sheaf of, 748
- module of fractions, 714
- monic, 234
- monomial, 297
- monomial ideal, 318, 332, 334
- monomial ordering, 317
- monomial part, 297
- monomial term, 297
- Monster simple group, 865
- morphism, 911
 - of affine algebraic sets, 662
 - of affine schemes, 743
- multidegree, 297, 318
- multilinear form, 435
- multilinear map, 372, 435
- multiple, 252, 274
- multiple root of a polynomial, 312, 545, 547
- multiplicative field norm, 230, 582
- multiplicative function, 7, 267
- multiplicative subgroup of a field, 314
- multiplicativity of extension degrees, 523, 529
- multiplicity of a root, 313, 545

N

- Nakayama's Lemma, 751
- natural, 83, 167, 432, 911ff.
 - projection, 83, 243, 348, 916
- Newton's Formulas, 618
- nilpotence class, 190
- nilpotent, element, 231, 250, 596, 689
 - group, 190ff., 198
 - ideal, 251, 258, 674
 - matrix, 502
- nilradical, 250, 258, 673, 674
- Noetherian, module, 458, 469
 - ring, 316, 458, 656ff., 793
- Noether's Normalization Lemma, 699ff.
- noncommutative polynomial algebra, 302, 443
- nonfinitely generated ideal, 298, 657
- nongenerator, 199
- nonpivotal, 425