

nonprincipal ideal, 252, 273, 298
 nonsimple field extension, 595
 nonsingular, point, 725, 742, 763
 variety, 725
 nonsingular, linear transformation, 413
 matrix, 417
 nonsingular curve, 775
 nonsingular model, 726
 norm, 232, 270, 299
 of a character, 872
 of an element in a field, 582, 585
 normal basis, 815
 normal complement, 385
 normal extension, 537, 650
 normal ring, 691
 normal subgroup, 82ff.
 normal variety, 726
 normalization, 691, 726
 normalize, 82, 94
 normalized, cocycle, 827
 factor set, 825
 section, 825
 normalizer, 50ff., 123ff., 134, 147, 206ff.
 null space, 413
 nullity, 413
 number fields, 696

O

object, 911
 opposite algebra, 834
 orbit, 45, 115ff., 877
 order, of a permutation, 32
 of a set, 1
 of an element in a group, 20, 55, 57, 90
 order of conductor f , 232
 order of zero or pole, 756, 763
 ordered basis, 409
 orthogonal characters, 872
 orthogonal idempotents, 377, 856, 870
 orthogonality relations, 872
 outer automorphism group, 137

P

p -adic integers, 269, 652, 758ff.
 p -adic Laurent series, 759
 p -adic valuation, 759
 p -extensions, 596, 638
 p -group, 139, 188
 characters of, 886
 representations of, 854, 864
 p -primary component, 142, 358, 465
 p^{th} -power map, 166, 174

P.I.D. — see Principal Ideal Domain
 parabolic subgroup, 212
 partition, of a set, 3
 of n , 126, 162
 Pell's equation, 230
 perfect field, 549
 perfect group, 174
 periods in cyclotomic fields, 598, 602, 604
 permutation, 3, 29, 42
 even, 108ff.
 odd, 108ff.
 sign of, 108ff., 436ff.
 permutation character, 866, 877, 895
 permutation group, 116, 120
 permutation matrix, 157
 permutation module, 803
 permutation representation, 43, 112ff., 203ff., 840,
 844, 852, 877
 pivotal element, 425
 Platonic solids, symmetries of, 28, 45, 92, 111, 148
 pole, 756
 polynomial, 234
 map, 299, 662
 ring, 234ff., 295ff.
 polynomials with S_n as Galois group, 642ff.
 Pontriagin dual group, 787
 positive norm, 270
 Postage Stamp Problem, 278
 power of an ideal, 247
 power series of matrices, 502ff.
 power set, 232
 preimage, 2
 presentation, 26ff., 39, 218ff., 380
 primary component — see p -primary component
 Primary Decomposition Theorem, for abelian
 groups, 161
 for ideals, 681ff., 716ff.
 for modules, 357, 465, 772
 primary ideal, 260, 298, 748
 prime, 6
 prime element in a ring, 284
 prime factorization, 6
 for ideals, 765ff.
 prime ideal, 255ff., 280, 674
 algorithm for determining, 710ff.
 prime spectrum, 731ff.
 prime subfield, 264, 511, 558
 primes associated, to a module, 670
 to an ideal, 670
 primitive central idempotent, 856, 870
 primitive element, 517, 594
 Primitive Element Theorem, 595
 primitive idempotent, 856
 primitive permutation group, 117

primitive roots of unity, 539ff.
 principal character, 866
 principal crossed homomorphisms, 814
 principal fractional ideal, 760
 principal ideal, 251
 Principal Ideal Domain (P.I.D.), 279ff., 284, 459
 characterization of, 281, 289, 294
 that is not Euclidean, 282
 principal open set, 687, 738
 product, of ideals, 247, 250
 of subgroups, 93ff.
 profinite, 809, 813
 projection, 83, 423, 453
 homomorphism, 153ff.
 projections of algebraic sets, 679
 projective limit — see inverse limit
 projective module, 390ff., 400, 403ff., 761, 773, 786
 projective plane, 210
 projective resolution, 779
 projectively equivalent, 407
 Public Key Code, 279
 pullback of a homomorphism, 407
 purely inseparable, 649
 purely transcendental, 646
 pushout of a homomorphism, 407
 Pythagoras' equation rational solutions, 584

Q

\mathbb{Q} , subgroups of, 65, 198
 \mathbb{Q}/\mathbb{Z} , 86
 quadratic, equation, 522, 533
 extensions, 522, 533
 field, 227, 698
 subfield of cyclic quartic fields, criterion, 638
 subfield of $\mathbb{Q}(\zeta_p)$, 621, 637
 quadratic integer rings, 229ff., 248, 271, 278, 286,
 293ff., 698, 749
 that are Euclidean, 278
 that are P.I.D.s, 278
 Quadratic Reciprocity Law, 819
 quadratic residue symbol, 818
 quartic equations, formulas for roots, 634ff.
 quasicontract, 688, 738, 746
 quasidihedral group, 71ff., 186
 as Galois group, 579
 quaternion group, 36
 as Galois group, 584
 characters of, 882
 generalized, 178
 representations of, 845, 852
 Quaternion ring, 224, 229, 258
 (see also Hamilton Quaternions)
 quintic, insolvability, 625, 629

quotient, computations in k -algebras, 672
 group, 15, 73ff., 76, 574
 module, 348
 ring, 241ff.
 vector space, 408, 412
 quotient field, 260ff.

R

radical extension, 625ff.
 radical ideal, 258, 673, 689
 radical of an ideal, 258, 673ff., 701
 computing, 701
 radical of a zero-dimensional ideal, 706ff.
 radicals, 625
 ramified prime, 749, 775
 range, 2
 rank, of a free module, 338, 354, 356, 358, 459
 of a group, 165, 218, 355
 of a linear transformation, 413
 of a module, 460, 468, 469, 471, 719, 773
 rational canonical form, 457, 472ff.
 computing, 481ff.
 rational functions — see field of rational functions
 rational group ring, 237
 rational numbers, 1, 260
 rational valued characters, 879
 real numbers, 1
 modulo 1, 21, 86
 reciprocity, 229, 621
 recognition theorem, 171, 180
 reduced Gröbner basis, 326ff.
 reduced row echelon form, 425
 reduced word, 216ff.
 reducible character, 866
 reducible element, 284
 reducible module, 847
 reduction homomorphism, 245, 296, 300, 586
 reduction mod n , 10, 243, 296, 640
 reduction of polynomials mod p , 586, 589
 reflexive, 3
 regular at a point, 721
 regular local ring, 725, 755
 regular map, 662, 722
 regular representation, 844, 862ff.
 relations, 25ff., 218ff., 380
 relations matrix, 470
 relative Brauer group, 836
 relative degree of a field extension, 512
 relative integral basis, 775
 relatively prime, 4, 282
 remainder, 5, 270, 320ff.
 Replacement Theorem, 410, 645
 representation, 840ff.

- permutation, 43, 112*ff.*, 203*ff.*, 840, 844, 852,
 877
 representative, 3, 9, 77
 residue class, 8
 resolvent cubic, 614, 623
 resolvent polynomials, 642
 restricted direct product, 158
 restriction homomorphism, 269, 805, 807
 restriction maps, 269, 740
 restriction of scalars, 359
 resultant, 619*ff.*
 reverse of a polynomial, 312
 right derived functor, 785
 right Euclidean Domain, 302
 right exact, 400, 402
 right group action, 43, 128, 844, 852
 right ideal, 242, 251
 right inverse, in a ring, 233
 of a map, 2
 right module, 337
 right regular representation, 132
 right zero divisor, 233
 ring, 223
 of algebraic integers, 695*ff.*
 of continuous functions, 225, 227, 259
 of dual numbers, 729
 of fractions, 260*ff.*, 708
 of integers, 229
 of sets, 232
 root, 310, 521
 root extension, 627
 root of a polynomial, 307*ff.*, 512
 root of unity, 22, 66, 86, 539*ff.*, 552
 row equivalent, 425
 row rank, 418, 427, 434
 row reduced, 424
 ruler and compass constructions, 534
- S**
- saturated, 710
 saturation of an ideal, 710*ff.*
 scalar, 408
 scalar matrix, 236
 scalar transformations, 348
 Schanuel's Lemma, 407
 scheme, 745
 Schur multiplier, 838
 Schur's Lemma, 356, 853, 856
 Schur's Theorem, 829
 second dual — see double dual
 Second Orthogonality Relation, 872
 section, 384, 740
 semidihedral group — see quasidihedral group
- semidirect product, 175*ff.*, 383, 385, 821, 829
 semisimple, 855
 separable, 551
 extension, 551, 572, 594*ff.*
 polynomial, 546, 562, 572
 separable degree, of a field extension, 650
 of a polynomial, 550
 separating transcendence base, 650
 Shapiro's Lemma, 804
 short exact sequence, 379
 of complexes, 778
 Short Five Lemma, 383
 similar, linear transformations, 419, 476
 matrices, 419, 476, 493*ff.*
 similar central simple algebras, 835
 similar representations, 846
 similarity, 40
 simple algebra, 832
 simple extensions, 517, 586, 594
 simple group, 91, 102*ff.*, 149*ff.*, 201*ff.*, 212
 classification of, 103, 212
 of order 168, 207*ff.*
 sporadic, 104, 865
 simple module — see irreducible module
 simple radical extension, 625
 simple ring, 253, 863
 simple tensor, 360
 Simultaneous Resolution, 783
 singular point, 725
 skew field — see division ring
 skew-symmetrization, 452
 Smith Normal Form, 479
 smooth, 725, 742
 Snake Lemma, 792
 solution, of cubic equations, 630
 of quartic equations, 634*ff.*
 solvability of a quintic, criterion, 630, 639
 solvability of groups of odd order — see
 Feit-Thompson Theorem
 solvable by radicals, 627*ff.*
 solvable extensions, 625*ff.*
 solvable group, 105, 149, 196*ff.*, 628, 886, 890
 solvable length, 195*ff.*
 solving algebraic equations, 327*ff.*
 solving linear equations, 425*ff.*
 span, 62, 351, 408, 427
 special linear group, 48, 89, 101, 669
 specialization, 648
 spectral sequences, 808
 spectrum — see also prime spectrum and maximal
 spectrum
 of $k[x]$, 735
 of $k[x, y]$, 735
 of $\mathbb{Z}/\mathbb{Z}[2\mathbb{Z}]$, 747

- of $\mathbb{Z}[i]$, 735
 of $\mathbb{Z}[x]$, 736
split algebra, 835
split exact sequence, 384, 388ff.
split extension, 384
split prime, 749, 775
 splits completely, 536
splitting field, 513, 536ff., 562, 572
 - of $(x^2 - 2)(x^2 - 3)$, 537
 - of $x^2 - 2$, 537
 - of $x^2 - t$ over $k(t)$, 516
 - of $x^2 + 1$, 515
 - of $x^2 + x + 1$ over \mathbb{F}_2 , 516
 - of $x^3 - 2$, 537
 - of $x^4 - px + q$, 618
 - of $x^4 - px^2 + q$, 618
 - of $x^4 + 4$, 538
 - of $x^4 + 8$, 581
 - of $x^4 - 2x^2 - 2$, 582
 - of $x^6 - 2x^3 - 2$, 623
 - of $x^8 - 2$, 577ff.
 - of $x^n - 1$, 539ff.
 - of $x^p - 2$, 541
 - of $x^p - x - a$ over \mathbb{F}_p , 589
- splitting homomorphism**, 384
- splitting of polynomials in Galois extensions**, 572, 584, 595
- sporadic simple group**—see **simple group, sporadic**
- square root of a matrix**, 502
- squarefree part**, 227
- Squaring the Circle**, impossibility of, 531ff.
- stability group**, 819
- stabilizer**, 44, 51ff., 112ff., 123ff.
- stable subspace**, 341, 843
- stalk**, 741
- standard bimodule structure**, 367
- standard resolution**, 799
- steady states**, 507
- Steinitz class**, 773
- Stone-Čech compactification**, 259
- straightedge and compass constructions**, 531ff., 602
- structure sheaf**, 740ff.
- Sturm's Theorem**, 624
- subfield**, 511, 516
- subgroup**, 22, 46ff.
 - criterion, 47
 - of cyclic groups, 58ff.
 - of index 2, 91, 120, 122
- sublattice**, 70
- submodule**, 337
 - criterion, 342
- subring**, 228
- subspace topology**, 677
- sum**, of ideals, 247, 250
- of submodules**, 349, 351
- support**, 729ff.
- surjective**, 2
- Sylow p -subgroup**, 101, 139ff., 161
- Sylow's Theorem**, 93, 105, 139ff., 617
- symmetric algebra**, 444
- symmetric function**, 436, 608
- symmetric group**, 29ff.
 - as Galois group, 642ff., 649ff.
 - characters of, 879, 881, 883, 884
 - conjugation in — see conjugation
 - isomorphisms between, 37, 40
 - Sylow p -subgroups of, 168, 187
- symmetric polynomials**, 608, 621ff.
- symmetric relation**, 3
- symmetric tensor**, 451
- symmetrization**, 452

T

- table, group**, 21
- tangent space**, 724ff., 741ff.
- Tchebotarov Density Theorem**, 642
- tensor algebra**, 443
- tensor product**, 359ff., 788ff.
 - associativity of, 371
 - of algebras, 374
 - of direct products, 376
 - of direct sums, 373, 376
 - of fields, 377, 531, 596
 - of free modules, 404
 - of homomorphisms, 370
 - of ideals, 377
 - of matrices, 421
 - of projective modules, 402, 404
 - of vector spaces, 420
- tensors**, 360, 364
- tetrahedron** — see **Platonic solids**
- Thompson subgroup**, 139
- Thompson Transfer Lemma**, 822
- Thompson's Theorem**, 196
- topological space**, 676ff.
- $\text{Tor}_n^R(A, B)$, 788ff.
- torsion**, element, 344
 - module, 356, 460, 463
 - subgroup, 48
 - submodule, 344
- torsion free**, 406, 460
- trace**, of a field element, 583, 585
 - of a matrix, 248, 431, 431, 488, 866
- trace ideal of a group ring**, 846
- transcendence base**, 645
- transcendence degree**, 645
- transcendental**, element, 520, 527, 534