

- free, 218, 354
 of a field extension, 513
 of a vector space, 408
Bass' Characterization of Noetherian Rings, 793
 belongs to an ideal, 682
Berlekamp's Factorization Algorithm, 311, 589ff.
 Betti number, 159, 464
Bezout Domain, 274, 283, 294, 302, 307, 775
 bijection, 2
 bilinear, 368ff., 372, 436
 bimodule, 366, 404
 binary, operation, 16
 relation, 3
 Binomial Theorem, 60, 249, 548
 biquadratic, extension, 530, 582, 589
 polynomial, 617
 block, 117
 diagonal, 423, 475
 upper triangular, 423
 Boolean ring, 231, 232, 249, 250, 258, 267
 Brauer group, 836
 Buchberger's Algorithm, 324ff.
 Buchberger's Criterion, 324ff., 332
 building, 212
 Building-Up Lemma, 411
 Burnside's Basis Theorem, 199
 Burnside's Lemma, 877
 Burnside's N/C -Theorem, 213
 Burnside's p^aq^b Theorem, 196, 886ff.
- C**
- $C^n(G; A)$ — see cochains
 cancellation laws, 20
 canonical forms, 457, 472
 canonical model, 734
 Cardano's Formulas, 630ff., 638ff.
 cardinality, 1
 Cartesian product, 1, 905ff.
 Castelnuovo's Theorem, 646
 Casus irreducibilis, 633, 637
 category, 391, 911ff.
 Cauchy's Theorem, 93, 96, 102, 146
 Cayley–Hamilton Theorem, 478
 Cayley's Theorem, 118ff.
 center, of a group, 50, 84, 89, 124, 134, 198
 of a group ring, 239
 of a matrix ring, 239, 834, 856
 of a p -group, 125, 188
 of a ring, 231, 231, 344, 832ff., 856
 central idempotent, 357, 856
 central product, 157, 169
 central simple algebra, 832ff.
 centralize, 94
- centralizer, 49ff., 123ff., 133ff.
 of a cycle, 173
 of a representation, 853
 chain complex, 777
 homotopy, 782
 change of basis, 40, 419
 changing the base — see extension of scalars
 character, of a group, 568, 866
 of a representation, 866
 character table, 880ff.
 of A_4 , 883
 of D_8 , 881
 of Q_8 , 882
 of S_3 , 881
 of S_4 , 883
 of S_5 , 884
 of $\mathbb{Z}/2\mathbb{Z}$, 880
 of $\mathbb{Z}/3\mathbb{Z}$, 881
 characteristic, of a field, 510
 of a ring, 250
 characteristic function, 249
 characteristic p fields, 510
 characteristic polynomial, 473
 characteristic subgroup, 135ff., 174
 Chinese Remainder Theorem, 246, 265ff., 313, 357,
 768
 choice function, 905
 class equation, 122ff., 556
 class field theory, 600
 class function, 866, 870
 class group, 761, 774
 class number, 761
 Classical Greek Problems, 531ff.
 classification theorems, 38, 142ff., 181ff.
 closed, topologically, 676
 under an operation, 16, 242, 528
 closed points, 733
 coboundaries, 800
 cochain, 777, 799, 808
 cochain complex, 777
 cochain homotopy, 792
 cocycle, 800
 codomain, 1
 coefficient matrix, 424
 cofactor, 439
 Expansion Formula, 439
 Formula for the Inverse of a Matrix, 440
 coherent module sheaf, 748
 cohomologically trivial, 802, 804, 812
 cohomology group, 777, 798ff.
 coinduced module, 803, 811, 812
 cokernel, 792
 coloring graphs, 335
 column rank, 418, 427, 434

- comaximal ideals, 265
 commutative, 16, 223
 diagram, 100
 commutator, 89, 169
 commutator series — see derived series
 commutator subgroup, 89, 169, 195ff.
 commute, diagram, 100
 compact, 688
 support, 225
 companion matrix, 475
 compatible homomorphisms, 805
 complement, 180, 453, 454, 820, 829, 890
 complete, 759ff.
 complete preimage, 83
 completely reducible, 847
 completion, 759ff.
 complex conjugation, 345, 567, 603, 618, 654, 872
 complex numbers, 1, 512, 515, 654
 component of a direct product, 155, 338
 composite extensions, 529, 591ff.
 of fields, 528
 composition factors, 103
 composition series, 103ff.
 computing k -algebra homomorphisms, 664ff.
 computing Galois groups, 640ff.
 congruence class, 8ff.
 congruent, 8
 conjugacy class, 123ff., 489, 860
 conjugate, algebraic, 573
 field, 573
 of a field element, 573
 of a group element, 82, 123ff.
 of a set, 123ff.
 of a subgroup, 134, 139ff.
 conjugation, 45, 52, 122ff., 133
 in A_n , 127, 131
 in S_n , 125ff.
 connected, 687
 connecting homomorphisms, 778, 791
 constituent of a module, 847
 constructible, 532ff.
 constructibility of a regular n -gon, 534ff., 601ff.
 construction of cube roots, 535
 construction of the regular 17-gon, 602ff.
 continuous cohomology groups, 809
 continuous group action, 808ff.
 contracting homomorphisms, 809
 contraction of ideals, 693, 708ff.
 contravariant, 659
 converge, 503
 coordinate ring, 661
 coprime — see relatively prime
 corestriction homomorphism, 806, 807
 corresponding group actions, 129
 coset, 77ff., 89ff.
 representatives, 77
 Cramer's Rule, 438
 Criterion for the Solvability of a Quintic, 639
 crossed homomorphisms, 814ff.
 crossed product algebra, 833ff.
 cubic equations, formulas for roots, 630ff.
 curve, 726
 cycle, 29, 30, 33, 106ff., 173
 cycle decomposition, 29, 30, 115ff., 641
 algorithm, 30ff.
 cycle type, 126ff.
 of automorphisms, 640
 cyclic extensions, 625, 636
 cyclic group, 22, 54ff., 90, 149, 192, 198, 539
 characters of, 880, 881
 cohomology of, 801, 811
 cyclic module, 351, 462
 cyclotomic extensions, 552ff., 596ff.
 cyclotomic field, 540ff., 698
 cyclotomic polynomial, 310, 489, 552ff.
 cyclotomy, 598

D

- D.C.C. — see descending chain condition
 decomposable module, 847
 Dedekind Domain, 764ff.
 modules over, 769ff.
 Dedekind–Hasse Criterion, 281
 Dedekind–Hasse norm, 281, 289, 294
 degree, of a character, 866
 of a field element, 520
 of a field extension, 512
 of a monomial, 621
 of a polynomial, 234, 295, 297
 of a representation, 840
 of a symmetric group, 29
 degree ordering, 331
 dense, 677, 687
 density of primes, 642
 derivative, of a polynomial, 312, 546
 of a power series, 505
 derived functors, 785
 derived series, 195ff.
 descending chain condition (D.C.C.), 331, 657, 751
 855
 determinant, 248, 435ff., 450, 488
 computing, 441
 determinant ideal, 671
 diagonal subgroup, 49, 89
 diagonalizable matrices criterion, 493, 494
 Dickson's Lemma, 334
 differential, 723

- of a morphism, 728
 dihedral group, 23ff.
 as Galois group, 617ff.
 characters of, 881, 885
 commutator subgroup of, 171
 conjugacy classes in, 132
 dimension, of a ring, 750, 754ff.
 of a tensor product, 421
 of a variety, 681, 729
 of a vector space, 408, 411
 of $S^k(V)$, 446
 of $T^k(V)$, 443
 of $\Lambda^k(V)$, 449
 dimension shifting, 802
 Diophantine Equations, 14, 245, 276, 278
 direct factor, 455
 direct limit, 268, 358, 741
 direct product, characters of, 879
 infinite, 157, 357, 414
 of free modules, 358
 of groups, 18, 152ff., 385, 593
 of injective modules, 793
 of injective resolutions, 793
 of modules, 353, 357, 358, 385
 of rings, 231, 233, 265ff.
 direct sum, infinite, 158, 357, 414
 of injective modules, 403
 of modules, 351ff., 357, 385
 of projective modules, 392, 403, 793
 of projective resolutions, 793
 of rings, 232
 direct summand, 373, 385, 451
 directed set, 268
 Dirichlet's Theorem on Primes in Arithmetic Progressions, 557
 discrete G -module, 808
 discrete cohomology groups, 808ff.
 discrete valuation, 232, 238, 272, 755
 Discrete Valuation Ring, 232, 272, 755ff., 762
 discriminant, 610
 as resultant, 621
 of a cubic, 612
 of a polynomial, 610
 of a quadratic, 611
 of a quartic, 614
 of p^{th} cyclotomic polynomial, 621
 distributive laws, 34, 223
 divides, 4, 252, 274
 divisibility of ideals, 767
 divisible, group, 66, 86, 167
 module, 397
 Division Algorithm, 4, 270, 299
 division ring, 224, 225, 834
 divisor, 274
- domain, 1
 double coset, 117
 double dual, 432, 823, 914
 Doubling the Cube impossibility of, 531ff.
 doubly transitive, 117, 877
 dual basis, 432
 dual group, 167, 815, 823
 dual module, 404, 404
 dual numbers, 729
 dual vector space, 431

E

- echelon, 425
 eigenspace, 473
 eigenvalue, 414, 423, 472
 eigenvector, 414, 423, 472
 Eisenstein's Criterion, 309ff., 312
 elementary abelian group, 136, 155, 339, 654
 elementary divisor, 161ff., 465ff.
 decomposition, 161ff., 464
 decomposition algorithm, 495
 elementary Jordan matrix, 492
 elementary row and column operations, 424, 470ff., 479ff.
 elementary symmetric functions, 607
 elimination ideal, 328ff.
 elimination theory, 327ff.
 elliptic, curve, 14
 function, 600
 function field, 653
 integral, 14
 embedded prime ideal, 685
 embedding, 83, 359, 569
 endomorphism, 347
 ring, 347
 equivalence class, 3, 45, 114
 equivalence of categories, 734, 916
 equivalence of short exact sequences, 381
 equivalence relation, 3, 45, 114
 equivalent extensions, 381, 787, 824
 equivalent representations, 846, 869
 Euclidean Algorithm, 5, 271
 Euclidean Domain, 270ff., 299
 modules over, 470, 490
 Euler φ -function, 7, 8, 11, 267, 315, 539ff., 589
 Euler's Theorem, 13, 96
 evaluation homomorphism, 244, 255, 432ff.
 exact, functor, 391, 396
 sequence, 378
 exactness, of Hom, 389ff., 393ff.
 of tensor products, 399
 exceptional characters, 901
 exponent of a group, 165ff., 626

- exponential map, 86
 exponential notation, 20, 22
 exponential of a matrix, 503ff.
 $\text{Ext}_R^n(A, B)$, 779ff.
 extension, of a map, 3, 386, 393
 - of ideals, 693, 708ff.
 - of modules, 378
 - of scalars, 359ff., 363ff., 369, 373
 extension field, 511ff.
 extension problem, 104, 378, 776
 Extension Theorem, for Isomorphisms of Fields, 519, 541
 exterior algebra, 446
 exterior power, 446
 exterior product — see wedge product
 external, direct product, 172
 - direct sum, 353
- F**
- F -algebra — see algebra
 factor group — see quotient group
 factor set, 824ff.
 factor through, homomorphism, 100, 365
 factorial variety, 726
 factorization, 283ff.
 faithful, action, 43, 112ff.
 - functor, 914
 - representation, 840
 Fano Plane, 210
 Feit–Thompson Theorem, 104, 106, 149, 196, 212, 899
 Fermat primes, 601
 Fermat’s Little Theorem, 96
 Fermat’s Theorem on sums of squares, 291
 fiber, 2, 73ff., 240ff.
 fiber product of homomorphisms, 407
 fiber sum of homomorphisms, 407
 field, 34, 224, 226, 510ff.
 - of fractions, 260ff.
 - of p -adic numbers, 759
 - of rational functions, 264, 516, 530, 567, 585, 647ff., 681, 721
 field extension, 511ff.
 field generated by, 511, 516
 field norm, 229
 finite covering, 704
 finite dimensional, 408, 411
 finite extensions, 512ff., 521, 526
 finite fields, 34, 301, 529
 - algebraic closure of, 588
 - existence and uniqueness of, 549ff.
 - Galois groups of, 566, 586
 - of four elements, 516, 653
 subfields of, 588
 finite group, 17
 finitely generated, field extension, 524ff., 646
 - group, 65, 158, 218ff.
 - ideal, 251, 317
 - k -algebra, 657
 - module, 351ff., 458
 finitely presented, group, 218ff.
 - module, 795ff.
 First Order Diophantine Equation, 276, 278
 First Orthogonality Relation, 872
 Fitting ideal, 671
 Fitting’s Lemma, 668
 fixed, element, 558
 - field, 560
 - set, 131, 798
 fixed point free, 41, 132
 flat module, 400ff., 405ff., 790, 795
 form, 297
 formal Laurent series, 238, 265, 756, 759
 formal power series, 238, 258, 265, 668
 formally real fields, 530
 Fourier Analysis, 875ff.
 fractional ideal, 760ff.
 fractional linear transformations, 567, 647
 Frattini subgroup, 198ff.
 Frattini’s Argument, 193
 free, abelian group, 158, 355
 - group, 215ff.
 - module, 338, 352, 354ff., 358, 400
 nilpotent group, 221
 free generators, 218
 - of a module, 354
 free rank, 159, 218, 355, 460, 464
 Frobenius automorphism, 549, 556, 566, 586, 589, 604
 Frobenius group, 168, 638, 643ff., 896
 - as Galois group, 638
 - characters of, 896
 Frobenius kernel, 896
 Frobenius Reciprocity, 904
 full functor, 914
 function, 1
 function field, 646, 653
 functor, 391, 396, 398, 913
 - contravariant, 395, 913
 - covariant, 391, 398, 913
 fundamental matrix, 506
 Fundamental Theorem, of Algebra, 545, 615ff.
 of Arithmetic, 6, 289
 of Finitely Generated Abelian Groups, 158ff., 196, 468
 of Finitely Generated Modules over a Dedekind Domain, 769ff.