

- Integral domain, 196  
     associates in, 276  
     Euclidean norm on, 286  
     prime element of, 280  
     field of quotients of, 211, 215  
     unit in, 276  
 Intermediate field, 344  
 Internal direct product, 91  
 Intersection, 60, 71  
 Interval, closed, 8  
 Invariant factors, 93  
 Invariant series, 157  
 Invariant subgroup, 118  
 Inverse  
     of an element, 20  
     left, 25  
     multiplicative, 190  
 Inverse function, 4  
 Inverse map, 4  
 Irreducible element, 276  
 Irreducible polynomial, 231  
     for  $\alpha$  over  $F$ , 315, 319  
     in  $F[x]$ , 231  
 Isometry, 22, 105  
 Isomorphic  $G$ -sets, 139  
 Isomorphic groups, 26  
 Isomorphic presentations, 180  
 Isomorphic rings, 189  
 Isomorphic series, 157  
 Isomorphism  
     conjugation, 345  
     of a  $G$ -set, 139  
     of a group, 26  
     of a ring, 189  
     up to, 92  
     of a vector space, 274  
 Isomorphism extension theorem, 351  
 Isomorphism theorems, 145–148  
 Isosceles triangle, 2  
 Isotropy subgroup, 135  
  
 Join  
     of extension fields, 371  
     of subgroups, 146  
 Jordan, Camille, 21, 162  
 Jordan-Hölder theorem, 161  
  
 $k$ -cycle, 44  
 Kernel, 78, 188, 247  
     of a linear transformation, 275  
 Khayyam, Omar, 224  
 Klein 4-group, 32, 53  
 Kronecker, Leopold, 92, 191, 312  
 Kronecker's theorem, 312  
 Kummer, Ernst, 92, 244, 277  
  
 Lagrange, Joseph-Louis, 21, 42, 385  
     theorem of, 99, 123  
 Lame, Gabriel, 277  
 Law  
     antisymmetric, 324  
     cancellation, 23, 196  
     distributive, 185  
     reflexive, 324  
     transitive, 324  
  
 Least common multiple, 69, 90, 291  
 Left cancellation law, 23  
 Left coset, 98  
 Left distributive law, 185  
 Left ideal, 258  
 Left identity, 25  
 Left inverse, 25  
 Left  $R$ -module, 272  
 Left regular representation, 80  
 Length of a code word, 238  
 Letter, 172  
 Levi ben Gerson, 42  
 Levinson, Norman, 339  
 Lexicographical order, 304  
 Lindemann, Ferdinand, 334  
 Linear code, 238  
 Linear combination, 269  
 Linear group, special, 115  
 Linear transformation, 275  
     kernel of, 275  
 Linearly dependent vectors over  $F$ , 269  
 Linearly independent vectors over  $F$ , 269  
 Liouville, Joseph, 277  
  
 Main diagonal of a matrix, 28  
 Main theorems of Galois theory, 364  
 Map, 3  
     extension of, 351  
     image under, 78  
     injection, 214  
     inverse of, 4  
     range of, 3  
 Matrix  
     determinant of, 28  
     diagonal, 28  
     main diagonal of, 28  
     orthogonal, 57  
     transpose of, 57  
     upper-triangular, 28  
 Maximal element, 325  
 Maximal ideal, 251  
 Maximal normal subgroup, 127  
 Maximum condition, 286  
 Mersenne prime, 201  
 Minimal polynomial for  $\alpha$  over  $F$ , 315, 319  
 Minimal subset, 55n  
 Minimum condition, 286  
 Monic polynomial, 314  
 Monoid, 25  
 Multiple, least common, 69, 90, 291  
 Multiplication  
     by components, 88  
     modulo  $n$ , 187  
     permutation, 41  
 Multiplicative identity, 14  
 Multiplicative inverse, 190  
 Multiplicative norm, 294  
 Multiplicity of a zero, 358  
  
 Nilpotent element, 193, 250  
 Nilradical, 250  
 Noether, Emmy, 186  
  
 Noetherian ring, 278  
 Nontrivial ideal, proper, 251  
 Nontrivial subgroup, 52  
 Norm  
     Euclidean, 286  
     Gaussian, 292  
     multiplicative, 294  
     over  $F$ , 370  
 Normal extension, finite, 362  
 Normal series, 157  
 Normal subgroup, 114, 118, 248  
     maximal, 127  
 Normalizer of a subgroup, 150  
 Nullstellensatz, 257  
 Number(s)  
     algebraic, 314  
     Betti, 92  
     commensurable, 223  
     complex, 3, 33  
     constructible, 329  
     imaginary, 34  
     rational, 2  
     real, 2  
     transcendental, 314  
 Number theory, algebraic, 294  
  
 Octic group, 182  
 Odd permutation, 83  
 One-to-one correspondence, 4  
 One-to-one function, 4  
 Onto function, 4  
 Operation  
     associative, 13, 20  
     binary, 11  
     commutative, 13  
     induced, 12  
     well-defined, 16  
 Orbit, 51, 82, 135  
 Order  
     of a group, 41  
     of an element, 61  
     infinite, 61  
     of ring, 192  
     term, 304  
 Ordering  
     lexicographical, 304  
     partial, 324  
     of power products, 303  
 Orientation, 106  
 Orthogonal matrix, 57  
  
 $p$ -group, 137  
 $p$ -subgroup, 137  
 Partial ordering, 324  
 Partition, 5  
     cells of, 5  
 Pattern, periodic, 108  
 Peano, Giuseppe, 268  
 Perfect field, 359  
 Periodic pattern, 108  
 Permutation, 41  
     even, 83  
     groups of, 77, 79  
     movement of elements in, 87  
     multiplication, 41

- odd, 83
- orbits of, 82
- sign of, 84
- Phi-function, 105, 202
- Plane
  - isometry of, 22
  - translation of, 105
- Plane crystallographic group, 108
- Plane isometry, 105
- Point, fixed, 110
- Polygon, constructible, 380
- Polynomial(s), 219
  - coefficients of, 219
  - constant, 219
  - content of, 237, 281
  - cyclotomic, 234, 378
  - degree of, 219
  - discriminant of, 378
  - divisor of, 234, 300
  - Eisenstein, 233
  - factor of, 300
  - general of degree  $n$ , 372
  - group of, 365
  - irreducible for  $\alpha$  over  $F$ , 315, 319
  - irreducible over  $F$ , 231
  - irreducible, 231
  - minimal for  $\alpha$  over  $F$ , 319
  - monic, 314
  - primitive, 237, 281
  - reducible, 231
  - ring of, 220
  - separable over  $F$ , 359
  - solvable by radicals over  $F$ , 384
  - splitting field of, 347, 349, 353
  - term ordering of, 304
  - zero of, 223, 298
- Polynomial code, 241
- Polynomial extension, 350
- Polynomial function on  $F$ , 227
- Power product, 303
  - ordering of, 303
- Power set, 8
- Presentation, 178, 179
  - finite, 179
  - generators for, 179
  - isomorphic, 180
- Prime, 280
  - Fermat, 381
  - Mersenne, 201
  - relatively, 291
- Prime field, 254
- Prime ideal, 252
- Primitive element, 360
- Primitive element theorem, 360
- Primitive  $n$ th root of unity, 69, 336
- Primitive polynomial, 237, 281
- Principal ideal, 254
  - generator of, 254
- Principal ideal domain, 276
- Principal series, 161
- Private key, 206
- Product
  - Cartesian, 2, 88
  - direct, 89, 187
- of ideals, 258
- power, 303
- Projection homomorphism, 246
- Proper nontrivial ideal, 251
- Proper subgroup, 52
- Proper subset, 2
- Public key, 206, 207
- Pythagorean theorem, 224
- Qin Jiushao, 288
- Quaternion group, 183
- Quaternions, 262
- Quotient
  - in the division algorithm, 62
  - of ideals, 258
- Quotient group, 115
- Quotient space, 275
- Rabin, Michael, 180
- Radical(s)
  - extension by, 384
  - of an ideal, 250
- Range of a map, 3
- Rank, 168, 174
- Rate of linear code, 238
- Rational function, 221
- Rational integer, 292
- Rational number, 2
- Real number, 3
- Reduced word, 173
- Reducible polynomial, 231
- Reduction modulo  $n$ , 116
- Refinement of a series, 157
- Reflection, 105
  - axis of, 105
  - glide, 106
- Reflexive law, 324
- Reflexive relation, 6, 7
- Regular representation, 80
  - left, 80
  - right, 81
- Relation(s), 3, 75, 179
  - consequence of, 179
  - equality, 3
  - equivalence, 6
  - reflexive, 6, 7
  - symmetric, 6, 7
  - transitive, 6, 7
- Relatively prime, 64, 291
- Relator, 179
- Remainder in the division algorithm, 62
- Representation
  - left regular, 80
  - right regular, 81
- Residue class modulo  $n$ , 6
- Ribet, Ken, 277
- Right cancellation law, 23
- Right coset, 100
- Right distributive law, 185
- Right ideal, 258
- Right  $R$ -module, 273
- Right regular representation, 81
- Ring(s), 185
  - additive group of, 186
  - Boolean, 194
  - characteristic of, 198
  - commutative, 189
  - division, 190
  - of endomorphisms, 258
  - factor, 245
  - group, 261
  - homomorphism, 188, 245
  - ideal of, 248
  - isomorphic, 189
  - isomorphism of, 189
  - maximal ideal of, 251
  - modules over, 272
  - nilradical of, 250
  - Noetherian, 278
  - order of, 192
  - of polynomials, 220
  - prime ideal of, 252
  - quotient, 245
  - radical of, 250
  - simple, 257
  - subring of, 190
  - unit in a, 190, 276
  - with unity, 189
  - zero, 189
- Roots of unity, 37
  - $n$ th, 37
  - primitive  $n$ th, 69, 336
- Rotation, 105
- RSA encryption, 206
- Ruffini, Paolo, 385
- Scalar, 267
- Schreier theorem, 160
- Sefer Yetzirah*, 42
- Semigroup, 25
- Separable element over  $F$ , 359
- Separable extension, 347, 359
- Separable polynomial over  $F$ , 359
- Series
  - ascending central, 163
  - chief, 161
  - composition, 161
  - invariant, 157
  - isomorphic, 157
  - normal, 157
  - principal, 161
  - refinement of, 157
  - subnormal, 157
- Set(s), 1
  - binary operation on, 11
  - cardinality of, 3
  - Cartesian product of, 2, 88
  - closed under an operation, 12
  - disjoint, 5
  - element of, 1
  - empty, 1
  - finite generating, 286
  - $G$ -, 132
  - generating, 70, 71
  - infinite, 4
  - intersection of, 60, 71
  - partial ordering of, 324

- Set(s) (*cont.*)  
 partition of, 5  
 permutation of, 41  
 power, 8  
 subset of, 2  
 union of, 278  
 well-defined, 1
- Shimura, Goro, 277
- Sign of a permutation, 84
- Simple extension, 315
- Simple group, 126
- Simple ring, 257
- Skew field, 190
- Smallest subset,  $55n$
- Solvable group, 163
- Solvable polynomial over  $F$ , 384
- Span, 269
- Special linear group, 115
- Splitting field, 347, 349, 353
- Square matrix  
 determinant of, 28  
 main diagonal of, 28
- Squaring the circle, 333
- Standard form of dihedral group  
 element, 48
- Strictly skew field, 190
- Sub- $G$ -set, 139
- Subfield, 190
- Subgroup(s), 52  
 commutator, 120, 128  
 conjugate, 119, 120  
 cyclic, 55, 61  
 improper, 52, 59  
 index of, 99  
 invariant, 118  
 isotropy, 135  
 join of, 146  
 maximal normal, 127  
 nontrivial, 52  
 normal, 114, 118, 248  
 normalizer of, 150  
 $p$ -, 137  
 proper, 52  
 torsion, 96  
 trivial, 52
- Subgroup diagram, 53
- Subnormal series, 157
- Subring, 190  
 generated by  $a$ , 193
- Subset, 2  
 improper, 2  
 minimal,  $55n$   
 proper, 2  
 smallest,  $55n$
- upper bound for, 325
- Subspace of a vector space, 274
- Sum  
 direct, 89  
 of ideals, 257  
 modulo  $n$ , 65
- Surjection, 4
- Syllable, 172
- Sylow, Peter Ludvig Mejdell, 150
- Sylow  $p$ -subgroup, 151
- Sylow theorems, 150
- Symmetric function, 372  
 elementary, 372
- Symmetric group on  $n$  letters, 43
- Symmetric relation, 6, 7
- Symmetries, group of, 105
- Table, group, 25  
 properties of, 27
- Taniyama, Yutaka, 277
- Tartaglia, Niccolo, 385
- Taylor, Richard, 277
- Term ordering, 304
- Thompson, John G., 127, 152
- Torsion coefficient, 93, 96
- Torsion free, 96, 119
- Torsion group, 119
- Torsion subgroup, 96
- Tower of fields, 311
- Trace over  $F$ , 370
- Transcendental element over  $F$ , 313
- Transcendental number, 314
- Transitive action, 133
- Transitive  $G$ -set, 133
- Transitive law, 324
- Transitive relation, 6, 7
- Translation, 105
- Transpose of a matrix, 57
- Transposition, 45, 81
- Trap door functions, 206
- Triangle, isosceles, 2
- Trisection of an angle, 333
- Trivial ideal, 251
- Trivial subgroup, 52
- Two-to-two function, 9
- Union  
 of sets, 278  
 of  $G$ -sets, 140
- Unique factorization domain, 276
- Unit, 190, 276
- Unit circle, 37
- Unity, 189
- nth* root of, 37, 336  
 primitive *nth* root of, 69, 336
- Upper bound for a subset, 325
- Upper-triangular matrix, 28
- Variety, algebraic, 298
- Vector(s), 267  
 linear combination of, 269  
 linearly dependent over  $F$ , 269  
 linearly independent over  $F$ , 269
- Vector space(s), 267  
 basis for, 270  
 dimension over  $F$ , 272  
 direct sum of, 274  
 finite-dimensional, 269  
 isomorphism of, 274  
 linear transformation of, 275  
 subspace of, 274
- Vertex/vertices  
 of a digraph, 72  
 of graph, 308
- Viete, Francois, 218
- Von Dyck, Walther, 21, 81
- Wallpaper group, 108
- Wantzel, Pierre, 334
- Weber, Heinrich, 21, 191
- Wedderburn, Joseph Henry Maclagan, 262
- Wedderburn theorem, 263
- Weierstrass, Karl, 312
- Weight of a string, 238
- Well-defined operation, 16
- Well-defined set, 1
- Weyl, Hermann, 268
- Weyl algebra, 260
- Wiles, Andrew, 277
- Wilson's theorem, 205
- Word(s), 172  
 empty, 172  
 reduced, 173
- Word problem, 180
- Zassenhaus, Hans, 158
- Zassenhaus lemma, 158
- Zermelo, Ernst, 326
- Zero  
 multiplicity of, 358  
 of a polynomial, 223, 298
- Zero divisors, 194
- Zero ring, 189
- Zorn, Max, 325
- Zorn's lemma, 324, 325

*This page is intentionally left blank*

*This page is intentionally left blank*