

Index

- Abelian, 43
- action, 137
- addition modulo n , 28, 58
- adelic group, 152
- adjacency matrix, 55
- affine group, 55, 71, 99, 150
- affine space, 284
- algebra of quaternions, 222
- algebra word origin, xvi
- algebraic closure, 232
- algebraic extension field, 230
- algebraic topology, 152
- algebraically closed field, 232, 239
- alternating function, 224
- alternating group, 87
- antisymmetric, 34
- Archimedean solids, 122
- arithmetic–geometric mean inequality, 12
- Artin conjecture on primitive roots, 79
- associative, 10, 43
- associative algebra, 223
- autocorrelation, 255
- automorphism, 92, 189, 238, 239
- axiom of choice, 232

- Banach–Tarski paradox, 233
- basis, 215
- BCH code, 262
- benzene, xiii, 132, 133
- Bézout’s identity, 23, 184, 199
- bijective, 37
- binary operation, 42, 43
- binomial theorem, 40
- Boolean functions, 120, 264
- Bourbaki, xviii, 218, 222
- buckyball, 152
- Burnside, 114, 117
- Burnside’s lemma, 117, 146

- cancellation law, 10
- Cantor, 6

- Cartesian product, 7, 232
- Cauchy, 13, 114, 118, 228, 243
- Cauchy sequence, 13
- Cauchy’s theorem on elements of prime order in a group, 118
- Cauchy–Binet formula, 228
- Cayley, 28, 36, 43, 52
- Cayley graph, 52, 55, 258
- Cayley table, 28
- Cayley’s theorem, 91
- Cayley–Hamilton theorem, 242
- center, 70
- centralizer, 118
- character, 129
- characteristic, 169
- characteristic polynomial of a linear recurrent sequence, 251
- characteristic polynomial of a matrix, 242
- chemistry, xiii, 55, 114, 133, 273
- Chinese remainder theorem, 110, 193
- circular reasoning, 22
- class equation, 118
- classification of finite simple groups, 101, 152
- Clay Mathematics Institute problems, 153
- closure, 43
- code, 257
- combinations of n objects k at a time, 39
- combinatorics, 38
- commutative, 10, 43, 159
- commutator subgroup, 101
- companion matrix, 213, 253
- complement, 6
- complete graph, 153
- complex conjugate, 222
- complex conjugation, 192
- complex numbers, xiii, 3, 5, 102, 104, 105, 129, 158, 168, 175, 192, 229, 232, 236, 272, 287
- composition of functions, 35
- congruence, 27
- congruence class, 28

- congruent, 27
 congruent number problem, 287
 conjugacy class, 92, 118
 conjugate, 92, 93, 266
 conjugation, 116, 118
 conjugation in fields, 222, 238, 240, 254
 conjugation in groups, 92
 connected graph, 54
 conservation of energy, 141
 containment, 6
 contrapositive, 4
 converse, 4
 convolution, 129
 coset, 94, 99, 117, 174, 185, 200, 229, 232, 259
 countable set, 38
 Coxeter group, 145
 Cramer's rule, 228
 cryptanalysis, 124
 cryptography, 124, 186, 269, 282, 293, 296
 cryptology, 124
 crystallography, 72, 134
 cube, 8, 56
 cycle, 82
 cycle diagram, 80
 cyclic code, 259
 cyclic group, 47, 69, 73
 cyclobutadiene, 133

 Dedekind, 174
 degree of a field extension, 230
 degree of a polynomial, 163, 165
 Delenn, 295
 denumerable set, 38
 derivative, 41, 104, 136, 236, 289
 determinant, 61, 88, 104, 224
 dicyclic group, 149
 difference equation, 251
 dihedral group, 46, 55, 66
 dimension, 111, 215, 222
 Diophantine equations, xvi
 direct sum or product, 108, 179, 212
 directed graph, 52
 discrete logarithm problem, 75, 296
 discriminant of a quadratic, 201
 discriminant of an elliptic curve, 284
 disjoint, 7
 disjoint cycle notation, 82
 distributive, 10, 159
 divides, 19
 division algebra, 223
 division algorithm, 21, 182
 divisor, 19, 181

 DNA, 134
 dodecahedron, 56, 122, 150, 269
 double coset, 98
 double helix, 134
 Dr. Who, 295
 dual group, 129

 echelon form, 206
 eigenvalue, 97, 133, 213, 233, 239, 240, 268, 272, 273
 eigenvector, 272, 273
 Eisenstein series, 288
 elementary divisor, 211
 elementary matrix, 209
 elementary row operations, 206
 elementary symmetric polynomials, 117, 204
 ElGamal cryptosystem, 295
 elliptic curve, 282
 empty set, 6
 encryption, 124
 energy, 133, 137, 140, 141
 equivalence class, 32
 equivalence relation, 31
 error-correcting code, 258
 Euclid, xv
 Euclid's lemma, 23
 Euclidean algorithm, 22, 180, 184
 Euclidean domain, 184
 Euler, xvii, 26, 135
 Euler phi-function, 60, 64
 Euler's criterion, 202
 Euler's identity, 104
 Euler-Lagrange equation, 136
 even permutation, 85
 expander graph, 269
 expansion by minors, 227, 229
 exponent, 65
 extension field, 171
 external direct product, 113
 extremal, 136

 factor group, 99
 factor ring, 174
 feedback shift register, 185, 186, 251
 Fermat's last theorem, xvi
 Fermat's little theorem, 95
 Fibonacci numbers, 17, 254
 field, 167
 field generated by an element of a larger field, 230
 field of fractions or quotients, 203
 field of rational functions, 204

- finite-dimensional vector space, 215
 finite field, xvi, xvii, 168, 175, 185, 221, 232, 233, 236
 finite logarithm, 73
 finite subgroup test, 69
 finite upper half plane, 266
 finitely generated group, 211
 first principal of mathematical induction, 14
 fixed point set, 116
 floor, 20
 formal power series, 164
 Fourier, 106, 130
 Fourier transform, 130, 263, 265
 fractional linear transformation, 266
 free group, 56, 153
 free module, 217
 Frobenius, 114, 223, 238, 280
 Frobenius automorphism, 238
 function, 35
 functional, 136
 fundamental group of a graph, 152
 fundamental theorem of Abelian groups, 212
 fundamental theorem of algebra, 232
 fundamental theorem of arithmetic, 23, 180
 fundamental theorem of Galois theory, 240
 fundamental theorem on symmetric polynomials, 117, 204

 Gödel incompleteness theorem, 3, 197
 Galois, 243
 Galois field, xvii, 222
 Galois group, xv, 92, 101, 204, 239
 Gauss, xiii, xvii, 5, 15, 24, 26, 106, 206, 222, 232
 Gaussian elimination, 206, 210
 Gaussian integers, 12, 161
 general linear group, 61, 70, 97, 104, 116, 150, 210, 221, 229, 253, 266, 273
 generator matrix, 258
 generators of a group, 49, 52, 55, 69, 73, 79
 geodesic, 135, 266
 Golay code, 264
 golden ratio, 254
 golden rectangle, 254
 Google bombing, 280
 Google matrix, 278
 Gram–Schmidt process, 273
 graph, 55
 graphs of Lubotzky, Phillips, and Sarnak, 270
 greatest common divisor, 21, 23, 83, 184
 group, 43
 group action on a set, 114
 group algebra, 131, 223
 group of an elliptic curve, 285
 groups of order less than or equal to 15, 148

 Hadamard matrix, 262
 Hamilton, 112, 222
 Hamming, 257
 Hamming code, 260
 Hamming weight, 257
 Hasse diagram, 34
 Hasse’s theorem on the number of points on an elliptic curve, 292
 Heisenberg group, 151
 Hermitian matrix, 273
 Hilbert, 153, 174, 272
 Hilbert’s problems, 153
 homogeneous linear recurrent sequence, 251
 homomorphism, 102, 104, 189, 190

 icosahedron, 56, 63
 ideal, 173
 ideal generated by a set, 174
 identity, 10, 37, 43, 63, 159, 160, 162, 169, 221, 224, 227, 258, 285
 identity matrix, 57, 61
 image, 35, 91, 104, 105, 190, 220, 258
 imaginary numbers, 5
 impulse response sequence, 251
 inclusion–exclusion principle, 41
 indeterminate, 86, 115, 163, 164, 180, 199
 induction hypothesis, 15
 inductive definition, 16
 infinite dimensional vector space, 215
 infinite set, 37
 injective, 36
 inner automorphism, 92
 inner product, 130
 integers, xv, 10–12
 integers modulo n , 28, 58, 98
 integral domain, 166
 internal direct product, 113
 intersection, 6
 invariance under a transformation, 138
 inverse, 10, 43, 159
 inverse function, 37
 inverse image, 39, 192
 inversion of Fourier transform, 132, 265
 irreducible polynomial, 181
 isomorphism, 89, 90, 104, 107, 170, 189, 190, 218, 222, 235, 238

 Jacobi identity, 165
 Jordan form, 213

- kernel, 102, 103, 190, 220, 259
- kinetic energy, 137
- Klein, 50
- Klein 4-group, 54, 60, 96, 108, 147
- Krawtchouk polynomial, 265
- Kronecker delta, 228

- Lagrange's theorem, 95
- Lagrangian, 137
- Laplace expansion of determinant, 228
- Latin square, 54
- lattice in the plane, 288
- leading coefficient of a polynomial, 181
- least common multiple, 82, 109
- left group action, 114
- Legendre symbol, 291
- Lehmer, 244, 250
- Lie bracket, 165
- Lie group, 152
- line at infinity, 284
- linear combination, 23, 133, 215
- linear congruence, 29, 75, 77, 194
- linear congruential random number generator, 245
- linear function or mapping, 36, 62, 93, 103, 218
- linear map, 218
- linear recurrent sequence, 251
- linearly independent vectors, 215
- Lorentz group, 142
- Lubotzky, Phillips, and Sarnak graphs, 271

- majority rule, 265
- mapping or map, 35
- Markov chain, 274
- Markov chain Monte Carlo methods, 244
- Markov matrix, 274
- mathematical induction, 14, 16
- mathematics as a language, 5
- matrix exponential, 107
- matrix multiplication, 36
- matrix of a linear mapping, 219
- maximal ideal, 177, 183
- Maxwell's equations, 138, 141
- Mersenne prime, 4
- methane, 57, 88
- metric, 258
- minimal polynomial, 231, 232
- minor, 227
- modular arithmetic, 26
- modular form, 266, 271, 288
- modular group, 51, 266
- module, 217

- momentum, 140
- monic polynomial, 181
- monomial, 165
- monster group, 101, 152
- Mordell's theorem on elliptic curves, 287
- multilinear function, 224
- multiple, 19
- multiplication modulo n , 28, 59
- multiplicative group of finite field is cyclic, 79, 202, 238
- multiplicity of a root of a polynomial, 183

- n factorial, 16
- natural numbers, 9, 12, 24
- natural projection, 105
- Newton's law, 137
- Noether, xvii, 104, 131, 135, 174
- Noether's theorem, 139
- non-Euclidean geometry, 5, 266
- non-singular elliptic curve, 284
- non-singular square matrix, 62, 107, 207, 229
- norm, 129, 134, 222, 266
- normal subgroup, 95
- normalizer, 119
- nullity, 220
- nullspace, 220
- number of elements in a finite set, 37

- octahedron, 56, 122, 151, 267
- odd permutation, 85
- one-parameter group, 107, 141
- one-step subgroup test, 68
- one-to-one, 36
- onto, 36
- orbit, 83, 116
- orbit/stabilizer theorem, 117
- order, 11
- order of a finite group, 65
- order of an element in a group, 66, 77
- orientation of the coordinates, 227
- orthogonal group, 57
- orthogonality, 131
- outer automorphism, 92

- p -group, 119
- Pólya enumeration theory, 120
- page rank, 279
- parallelepiped, 227
- parallelotope, 227
- parity check matrix, 259
- partial order, 34
- partition, 33
- Pascal's triangle, 40

- period of a linear recurrent sequence, 252
 permutation, 44, 81, 83
 permutation matrix, 92, 209
 permutation notation, 44
 Perron theorem, 280
 photo number 51, 134
 physics, 50, 135, 152, 273
 pigeonhole principle, 39
 pivot, 206, 217
 Platonic solids, 56
 Poincaré, 266, 270
 point at infinity, 284
 polynomial in two indeterminates, 165
 polynomial in n indeterminates, 86, 115
 polynomial ring, 163, 175, 180
 poset, 34
 poset diagram, 34
 potential energy, 137
 power method to find dominant
 eigenvector, 279
 power series, 18, 164
 powers of group elements, 64
 presentation, 55, 153
 prime, 20
 prime ideal, 176
 primitive polynomial, 185, 186, 238
 primitive root, 79
 primitive root of unity, 233, 261, 264
 principal ideal, 174, 210, 260
 principal ideal domain, 210
 principle of least action, 137
 product of ideals, 179
 projection, 105, 112
 projective general linear group, 270
 projective space, 284
 projective special linear group, 152
 proof by contradiction, 4
 proper ideal, 173
 proper subgroup, 67
 proper symmetry, 56
 pseudo random numbers, 244
 public-key cryptography, 124, 125,
 293, 295
 Pythagoreans, 5, 24

 quadratic formula, 101, 201
 quadratic reciprocity law, 311, 312
 quadratic residue code, 264
 quantum physics, 50
 quaternion, xvi, 112, 222
 quaternion group, 112, 147
 quintic equation, 101, 241

 quotient group, 99
 quotient ring, 174

 Ramanujan, 272
 Ramanujan graph, 269, 270
 random number generator, 245
 range, 220
 rank of a free module, 217
 rank of a linear map, 220
 rank of an Abelian group, 287
 rational canonical form, 213
 rational functions, 203, 204, 230
 rational numbers, xvi, 5, 12, 15, 158, 167, 202,
 231, 241, 254, 286
 real numbers, xiii, xvi, 5, 8, 12, 102, 105, 141,
 158, 168, 226, 231, 247, 273
 reciprocal polynomial, 241
 reducible polynomial, 181
 Reed–Muller code, 262
 Reed–Solomon code, 262
 reflexive, 31, 34
 relation, 30
 relation between group elements, 49, 55
 relation between rank and nullity, 220
 relatively prime, 21
 restriction of a function, 38
 resultant, 285
 right group action, 114
 ring, 159
 ring generated by an element of a larger
 ring, 187, 230
 ring of polynomials in several indeterminates,
 204
 roots of a polynomial, xv, 101, 164
 rotation group, 141
 row operations, 206
 row rank of a matrix, 217, 258
 row-reduced echelon form, 206
 RSA cryptography, 124, 125
 ruler and compass constructions, 241
 Russell’s paradox, 6

 scalar, 214
 Schreier graph, 96
 Schroedinger equation, 138
 Schur decomposition, 273
 second principle of mathematical induction, 16
 semi-direct product, 148
 shidoku or junior sudoku, 143
 sign of a permutation, 86
 similar matrices, 93, 213, 214, 221, 273
 simple algebra, 223

- simple field extension, 239
- simple group, 100
- Smith normal form of a matrix, 211
- solvable group, 241
- space group, 72, 152
- span of set of vectors, 215
- spanning tree, 153
- special linear group, 152
- special orthogonal group, 56, 57
- special relativity, 142
- spectral theorem, 133, 273
- spectroscopy, 134, 273
- spectrum, 133, 134, 142, 268, 272
- splat, 129
- splitting field of a polynomial, 234
- sporadic group, 101
- stabilizer, 116
- state vector of linear recurrent sequence, 253
- statistical tests, 255
- subfield, 171
- subfield test, 171
- subgroup, 67
- subring, 161
- subring test, 161
- subset, 6
- subspace, 216
- sudoku, 143
- sum of ideals, 179
- surjective, 36
- switching functions, 120, 264
- Sylow p -subgroup, 119
- Sylow theorems, 119
- symmetric, 31
- symmetric group, 81
- symmetric matrix, 55
- symmetric polynomial, 117
- symmetry, xiii, 47, 48, 50, 54, 152, 154
- system of Euler–Lagrange equations, 137
- tessellation, 270
- tesseract, 9, 108
- tetrahedral group, 87
- tetrahedron, 56, 87, 153
- torsion subgroup, 287
- torus, 111, 195, 288
- transcendental extension field, 230
- transitive, 11, 31, 34
- translation-invariant metric, 258
- transpose of a matrix, 57, 97, 141, 143, 219, 226, 272, 281
- transposition, 85
- triangle inequality, 12, 258
- trichotomy, 11
- truncated icosahedron, 152
- two-step subgroup test, 68
- undirected graph, 55
- union, 6
- unique factorization into primes, 23
- unit, 20, 59, 162, 180
- unitary matrix, 273
- Vandermonde determinant, 88
- vector, 214
- vector space, xiii, 61, 108, 130, 131, 185, 214
- very useful polynomial, 86
- vibrating system, 133, 142
- viruses, 58
- volume function, 227
- voting, 244, 264
- webpages, 276
- websites, 276
- Wedderburn theory, 224
- Wedderburn’s theorem on finite division rings, 173
- Wedderburn’s theorem on simple algebras, 223
- Weierstrass function, 287
- well defined, 28, 35
- well-ordering axiom, 12
- Wilson’s theorem, 64
- word problem, 153
- X-ray diffraction spectroscopy, 134
- zero divisor, 10
- Zorn’s lemma, 232