
Index

- Abelian group, 107
 - $(ab)^2 = a^2b^2$ in, 110
 - finite, 262
- Action
 - faithful, 253
 - group, 253
 - induced, 253
- Alternating group, 204, 239
 - cyclic subgroups of A_4 , 216
 - list of elements of A_4 , 215
 - subgroups of A_4 , 229
- Angle, 275
- Associativity, 21, 96–97
 - and grouping of factors, 97
 - Light’s test for, 104 *ex*
- Automorphism, 181, 254
 - of cyclic group, 255
 - group, 190 *ex*
 - inner, 189 *ex*
- Axioms for the integers, 37

- Basis of a free Abelian group, 269
- Beer-drinking logicians, 6
- Bézout’s identity, 129
- Bijection, 52
- Binary operation, 93
 - associativity of, 96, 104 *ex*
 - Cayley table of, 94
 - closed under, 95
 - commutativity of, 99
 - direct product of, 104
 - identity element, 97
 - uniqueness of, 97
 - induced, 95
 - inverse elements, 98
 - uniqueness of, 100 *ex*
 - set equipped with, 93
 - on two-element set, 105
- Binomial
 - coefficient, 83
 - theorem, 84–86
- Boolean function, 58
- Boost transformation, 190 *ex*
 - group law for, 123 *ex*

- Cancellation law, 40, 108
- Cantor diagonal argument, 54
- Cartesian
 - plane, 117
 - vector space, 159
- Cartesian product, 48
 - of empty set, 48
- Cat and mouse, 126
- Cayley table, 94
 - and isomorphism, 183
 - of the orthogonal group, 282
- Cayley’s theorem, 207 *ex*
- Center of a group, 244, 258
- Centralizer of a subgroup, 244
- Chinese remainder theorem, 154
- Class formula of a group, 258
- Closed under
 - a binary operation, 95, 112
 - addition, 18

- inversion, 112
- multiplication, 22
- Codomain of a mapping, 49
- Commutativity, 21
- Complex numbers
 - argument of, 21
 - conjugate of, 17, 178 *ex*, 188 *ex*
 - groups of, 117–119, 188 *ex*
 - imaginary part of, 17
 - lattice subgroup of, 118
 - magnitude of, 21
 - non-real, 17
 - product of, 19
 - real part of, 17
 - roots of unity, 65 *ex*, 108
 - square roots of, 22, 29 *ex*
 - unit, 22
- Composition, 54–58
 - associativity of, 55
- Congruence mod n , 126
- Congruences
 - systems of, 154
- Conjugacy class of a group, 254
- Conjugate subgroups, 255
- Constant mapping, 50
- Contrapositive, 7
 - advantages of, 7–8, 12 *ex*
- Coprime integers, 136
- Correspondence principle, 248
- Counterexample, 7
- Cranial blows
 - effect mod 2, 126
- Cube
 - symmetry group of, 218, 250
- Cycle notation for permutations, 194
- Cyclic group, 110, 228
 - automorphism of, 187, 255
 - classification of, 186
 - generators of, 187
 - homomorphic image of, 240
 - homomorphism into an arbitrary group, 241
 - as symmetries of an n -gon, 211
- Cyclic subgroup, 114
- De Morgan's laws, 4, 30
- Diagonal matrix, 176 *ex*
- Dicyclic group, 214
- Dihedral group, 211, 221 *ex*
 - generators and relations for, 211
- Direct product
 - of binary operations, 104
- Discrete group, 286
- Distributivity, 21
- Division algorithm, 40–42
- Divisor, 125
 - proper, 135
- Domain of a mapping, 49
- Double factorial, 88
- Empty set, 16
- Equipped with a binary operation, 93
- Equivalence classes, 59
 - mod n , 126
 - the space of, 61
- Equivalence relation, 59–63
 - stronger than, 68
- Equivalent group actions, 289
- Escher, M. C., 289
- Euclid's algorithm, 131
- Euler totient function, 144 *ex*
- Euler's formula, 21, 66 *ex*, 90 *ex*, 119, 297
- Even function, 65 *ex*
- Even integer, 42, 59, 94, 111
- Exact sequence, 250
- Existential quantification, 5
 - negation of, 5
- Exponentiation, 78–86
 - in a group, 109
- Factorial, 76
 - double, 88
 - table of, 76
- Faithful action, 253
- Fermat's Little Theorem, 157
- Fibonacci numbers, 76
- Finite Abelian groups, 262
- Finitely-generated group, 115, 261
- First isomorphism theorem, 244
- Free Abelian group, 269
 - rank of, 270
- Friendship as a binary relation, 59
- Frieze group, 288, 292 *ex*
- Fundamental domain, 289
- Fundamental theorem of arithmetic, 137
- Gaussian integers, 19, 249

- as subgroup, 118
- Generators and relations, 123 *ex*
- Geometric series, 87 *ex*
- $GL(2, \mathbf{R})$, 167
 - center of, 175 *ex*
- Glide reflection, 284
- Gödel, K., 3
- Greatest common divisor, 134, 140
 - definition of, 129
 - Euclid's algorithm, 131
- Group
 - Abelian, 107
 - action, 209, 253
 - equivalence of, 289
 - orbit of, 256
 - stabilizer, 206 *ex*, 257
 - automorphism of, 254
 - cancellation law, 108
 - center of, 244, 258
 - class formula of, 258
 - conjugacy class of, 254
 - cyclic, 110, 185, 228
 - dicyclic, 214
 - finitely-generated, 115, 261
 - free Abelian, 269
 - law of exponents in, 109
 - order 12, 266
 - order 8, 221 *ex*, 266
 - order 9, 228
 - order of, 107
 - order p^3 , 274 *ex*
 - power of a product in, 110
 - of prime order, 228
 - product of subsets, 117
 - reverse order law, 122 *ex*
 - simple, 264
 - word in, 115
- Groups
 - direct product of, 116, 134
 - direct sum of, 117
 - semidirect product of, 273 *ex*
- Hackers, 77
- Heisenberg group, 177 *ex*
- Hexagon
 - lattice, 294
 - symmetry group of, 213, 247
- Homomorphic image, 237, 241
- Homomorphisms
 - from a cyclic group, 241
 - definition of, 237
 - exact sequence of, 250
 - existence of, 240
 - kernel of, 237
 - and left cosets, 239
 - trivial, 238
- Hyperbolic functions, 66–67, 190 *ex*
- Identified by a mapping, 51, 68 *ex*
- Identity element
 - of a subgroup, 111–112
 - uniqueness of, 38, 97
- Identity mapping, 50
- Identity matrix, 163, 170
- Image of a set, 49
- Implication, 2
 - converse, 7
 - vacuous, 3, 16
- Inconsistent, 3
- Index of a subgroup, 257
- Induced
 - action, 253
 - binary operation, 95
 - mapping, 62, 186
- Induction, 71–84
- Inductively true, 73
- Injective mapping, 51
- Inner automorphism, 189 *ex*, 255
- Integers
 - additive group of, 107
 - axioms for, 37
 - cancellation law, 40
 - composite, 135
 - coprime, 136
 - even, 16, 42, 59, 94
 - odd, 16, 42
 - positive, 16
 - prime, 135
 - proper divisor of, 135
 - residue classes of, 126
 - unique factorization of, 137
- Internal direct product of subgroups, 248
- Inverse
 - uniqueness of, 38
- Inverse mapping, 56
- Isolated point, 286

- Isometry, 276
 - proper, 283
- Isometry group
 - structure of, 279
- Isomorphism, 181
 - as a commutative diagram, 95
 - and law of exponents, 182
 - natural logarithm as, 182
 - properties of, 182
 - of quotient group, 244
 - theorem
 - first, 244
 - second, 245
 - third, 245
- Jacobi identity, 176 *ex*
- Joke
 - all-you-can-eat buffet, 82
 - beer-drinking logicians, 6
 - black sheep, 61
 - double feature, 169, 172 *ex*
 - negative numbers, 34
 - parallelogram, 160
 - printing all primes, 143 *ex*
 - tuples, 82
- Kernel of a homomorphism, 237
 - is a normal subgroup, 238
- Klein 4-group, 104 *ex*, 120 *ex*, 172 *ex*, 206 *ex*, 220 *ex*, 228, 243, 290
 - automorphisms of, 255
- Kronecker δ symbol, 170
- Lagrange's theorem, 227
- Lattice
 - symmetries of, 292 *ex*
- Lattice subgroup, 118, 286
- Law of exponents, 109
 - and distributive law, 110
 - integer power, 78
 - as morphism condition, 182, 238
- Least common multiple, 134, 140
- Left cosets
 - and homomorphisms, 239
- Left cosets, 225
 - number of, 227
 - as orbits of right translation, 256
 - product of, 231
- Left inverse of a mapping, 56
- Length, 275
- Librarian's nightmare, 201
- Light's test for associativity, 104 *ex*
- Line, 277
- Linear combination, 160–162, 269
- Linear transformation, 161
 - matrix of, 163, 168
- Logarithmic spiral, 119
- Logical
 - contradiction, 3
 - equivalence, 6
 - implication, 2
 - counterexample to, 7
 - quantification, 4–6
- Mapping, 49
 - bijective, 52
 - with empty domain, 49
 - factors through the quotient, 62
 - image of a set under, 49
 - inversion, 56
 - level set of, 68 *ex*
 - parity of, 65 *ex*
 - preimage of a set under, 49, 64 *ex*
 - restriction of, 64 *ex*
 - well-defined mod R , 62
- Matrix
 - columns, meaning of, 163
 - complex, 167, 177 *ex*
 - determinant of, 166
 - invertibility of, 166
 - of a linear transformation, 163
 - multiplication, 163, 169
 - computational procedure for, 168
 - geometric interpretation of, 164, 173 *ex*
 - mapping interpretation of, 165–166
 - orthogonal, 177 *ex*, 281
 - of reflection, 164
 - of rotation, 164
 - transpose of, 169
- Maximal p -subgroup, 258
- Millennium problems, 144
- Modular arithmetic, 127–129
- Morphism condition, 181, 237
 - commutative diagram for, 95
- Motion, 276
 - proper, 283

- Multiplication diagram, 151–152
- Natural numbers, 36, 71
- Normal subgroup, 230
 product of left cosets, 231
- Normalizer, 244, 245, 257
- n th roots of unity, 22, 65 *ex*, 88 *ex*, 119, 183
- Number of mappings between finite sets, 80–84
- Odd function, 65 *ex*
- Odd integer, 42, 94
- 1 is the smallest positive integer, 40
- Orbit of a group action, 256
- Order
 of a group element, 114, 186
 of a group, 107
- Ordered set, 81
- Orthogonal group, 177 *ex*
 Cayley table for, 282
 composition rules, 282
 matrices of elements, 174 *ex*
- Orthogonal matrix, 164, 281
- Outer automorphism, 255
- Parallel postulate, 277
- Parallelogram, 160
- Partition of a set, 24
 defined by an equivalence relation, 60
- Pascal's triangle, 85–86
- Pauli matrices, 177 *ex*
- Permutations
 algorithm for multiplying, 197–199
 conjugacy, 199
 cycle decomposition of, 196
 cycle notation, 194
 disjoint cycle structure of, 193
 disjointly supported, 195
 fixed point of, 195
 order of, 199
 parity of, 202
 versus order of, 204
 support of, 195
 of vertices of an n -gon, 213
- Pigeonhole Principle, 64 *ex*
- Playing cards, 82
- Polarization identity, 276
- Power set, 24
 no surjection to, 54
- Preimage of a set, 49
- Primes
 paper required to print all, 143
- Principle of mathematical induction, 72
- Product of chords in unit circle, 90 *ex*
- Proper motion, 283
- Public-key encryption, 157 *ex*
- Push poll, 11 *ex*
- Quantification
 existential, 5
 universal, 4
- Quaternion group, 214
 as matrices, 178 *ex*
 quotients of, 242
- Quaternions, 177 *ex*
- Quotient
 group, 241
 torus as, 287
 mapping, 62
 of a set by an equivalence relation, 61
- \mathbf{R}^n , 159
- Rank of a free Abelian group, 270
- Ray, 277
- Recursive definition, 75
 songs, 77
- Reflection matrix, 164, 174 *ex*, 281
- Relation on a set, 58
- Residue classes, 25, 44 *ex*, 67 *ex*, 126
 arithmetic of, 127
 group of units, 146
 automorphisms of, 185
 generators of, 187
 invertible, 146
 multiplying, 151–152
 visualizing, 126
 zero divisor, 150
- Restriction of a mapping, 64 *ex*
- Reverse order law, 122 *ex*
- Reverse triangle inequality, 43
- Riemann hypothesis, 144
- Right inverse of a mapping, 57
- Roots of unity, 22, 65 *ex*, 119, 183
- Rotation matrix, 164, 174 *ex*, 176 *ex*, 281
- RSA (Rivest, Shamir, Adleman) algorithm, 157
- Rubik's cube, 219

- Russell's paradox, 16
- Scalar matrix, 176 *ex*
- Second isomorphism theorem, 245
- Semidirect product of groups, 273 *ex*
- Sequence, 75
 - partial sums of, 75
- Set
 - binary relation on, 58
 - complement of, 23
 - empty, 16
 - ordered, 81
 - partition of, 24
 - by an equivalence relation, 60
 - power set of, 24
 - subsets of, 15
- Sets
 - Cartesian product of, 48
 - difference of, 31
 - disjoint, 24
 - equality of, 15
 - intersection of, 23
 - product of, 29
 - sum of, 28
 - union of, 23
- Sheep, 33, 61
- Short exact sequence, 250
- Sieve of Eratosthenes, 143
 - implementation warning, 143 *ex*
- Simple group, 264
- Skew-symmetric matrix, 170
- $SL(2, \mathbf{R})$, 167
- Special relativity, 123 *ex*, 190 *ex*
- Spirograph, 152
- Square integer, 42
- Stabilizer, 257
- Standard basis, 159
- Subgroup
 - centralizer of, 244
 - correspondence principle for, 248
 - cyclic, 114
 - generated by a set, 114
 - identity element of, 111–112
 - index of, 257
 - of $(\mathbf{Z}, +)$, 116
 - normal, 230
 - normalizer of, 244, 245
- Subgroups
 - conjugate, 255
 - internal direct product of, 248
 - intersection of, 113
- Summation notation, 75
- Surjection, 51
- Sylow theorems, 261
- Symmetric group, 193
 - Cayley's theorem, 207 *ex*, 209
 - generators for, 200
 - list of elements of S_4 , 214
- Symmetric matrix, 170
- Symmetries
 - of Platonic solids, 216
 - of a regular n -gon, 211
 - of Rubik's cube, 219
- Third isomorphism theorem, 245
- Torsion subgroup, 270
- Tower of Hanoi, 73–75
- Translation, 281
- Triangle inequality, 43
- Trivial
 - conjugacy class, 254
 - homomorphism, 238
- Truth tables, 6
- Unit circle
 - product of chord lengths in, 90 *ex*
- Unitary matrix, 178 *ex*
- Units
 - group of, 146
- Universal quantification, 4
 - negation of, 5
- Vacuous implication, 3, 16
- Vector addition, 160, 276
- Video game, 287
- Wallpaper group, 288, 292–294
- Wason selection task, 9
- Well-defined, 62, 127
- Zero divisor, 150
- Zero matrix, 163
- $0! = 1$, 76
- $0^0 = 1$, 78
 - rationale, 80