Index

Abel, Niels Henrik, 39
abelian extension of $\mathbb{Q}$ is cyclotomic, 267
abelian group, 39
   all orders divide largest order, 192, 367
   conjugacy classes of, 453
   elliptic curve is, 460
   endomorphism ring, 87
   every subgroup normal, 129
   finite is product of cyclic groups, 354
   finitely generated is product of cyclic groups, 353
   has no inner automorphisms, 388, 395
   inversion is homomorphism, 58, 390
   is $\mathbb{Z}$-module, 328
   number of a given order, 368
   of fractional ideals of a number field, 466
   of order twelve, 396
   order of product of elements, 53, 192, 367
   order $p^2$ is abelian, 139
   representation of, 453
   simple iff prime order, 380
   structure theorem, 52, 353, 392, 485
action
   conjugation, 138
   group, 133
   transitive, 136, 152
addition, 63
additive group, 41
additive polynomial, 494
adjugate, 411
Adleman, Leonard, 499
affine algebraic set, 470
   ideal of, 471, 514
of an ideal, 471
affine line, 470
affine linear group, 396
affine plane, 470
affine space, 470
   projective space $\mathbb{P}^n$ covered by $n + 1$
      copies of $\mathbb{A}^n$, 514
affine variety, 470, 471
   affine algebraic set is union of, 471
   coordinate ring of, 471
   field of rational functions of, 471
algebra
   commutative, 426
   elements integral over a subring, 433
   extension of scalars, 509
   finite over a ring, 432
   finitely generated, 362, 432
   Hilbert Basis Theorem, 432
   integrality criterion, 433
   of finite type over a ring, 432
   over a ring, 431
   sum and product of integral elements are integral, 433
algebraic closure, 227, 286
   of $\mathbb{F}_p$, 227, 290
   of $\mathbb{Q}$, 227
algebraic extension, 221, 223
   of infinite degree, 286
algebraic geometry, 470
   Bezout’s Theorem, 476
   Nullstellensatz, 471, 514
algebraic number, 187
   approximated by rational number, 215
algebraic number \((continued)\)

- iff \(\dim F[\alpha]\) finite, 224
- iff \(F[\alpha] = F(\alpha)\), 188, 222, 224
- minimal polynomial, 225
- set of is a field, 224

algebraic number theory, 464

fundamental exact sequence, 514

algebraic set

- affine, 470
- projective, 474
- union of varieties, 471

algebraic variety, 471

coordinate ring of, 471

field of rational functions of, 471, 514

algebraically closed field, 124, 226, 286, 290, 355

\(\mathbb{C}\) is, 226, 251

- iff polynomials split completely, 226, 286, 308
- linear operator has eigenvector in, 308, 451

Alice, 496

alternating form

- bilinear, 362
- \(D^B\) is an \(R\)-basis, 403
- expansion as a sum, 323, 402
- map induced by endomorphism, 401, 410
- map induced by linear operator, 312, 323
- on \(R^n\) has rank one, 401, 410
- sign change formula, 400
- space of has dimension one, 323
- swap variables changes sign, 312, 323
- top non-trivial space has rank one, 401, 410

alternating group, 379, 400

- has index 2 in \(S_n\), 379
- is normal subgroup of \(S_n\), 379
- of order twelve, 396
- simple for \(n \geq 5\), 381

alternating property, 311

\(A^n\), see affine space

angle bisector, 209

angle trisection problem, 208

annihilator ideal, 349, 365, 366

antisymmetry property, 29, 418

arrow in a category, 436

Artin’s conjecture, 193

Artin, Emil, 193

Artinian ring, 363

associative axiom, 133, 436

associative law, 39

as commutative diagram, 430

module, 327

ring, 64

vector space, 93

\(au + bv = \gcd\) theorem, 18, 364

Euclidean algorithm, 32

Aut, see automorphism group

automorphism

- conjugation, 388
- in a category, 436
- inner, 154, 388
- linear independence of field, 282
- of polynomial ring, 230
- outer, 154, 388

automorphism group, 154

- homomorphism from group to, 389
- in a category, 437
- of a group, 388
- of a module, 490
- of cyclic group, 389, 396
- of symmetric group, 389
- of \(\mathbb{Z}^n\), 395
- vector space, 296

axiom

- field, 105
- group, 39
- module, 327
- ring, 63
- vector space, 93
- what is an, 1, 2

Axiom of Choice, 227, 319, 336, 414, 417, 418

existence of maximal ideal, 79, 506

existence of vector space basis, 98, 318, 421, 506

Babai’s Closest Vector Algorithm, 481, 499, 500

Babylonia, 221

babystep-giantstep method, 520

ball, formula for volume, 517

base, group over a, 441

basis, 95

- all have same size, 98, 334, 336
- change of for free module, 359, 361
- finite, 95
- for direct product, 325
- for direct sum, 325
- fundamental domain associated to, 478
- iff \(\delta(v_1, \ldots, v_n) \neq 0\), 312
- iff spans and linearly independent, 96, 318, 332
basis (continued)
  infinite, 98
  not every module has a, 332, 333, 359
  of polynomial ring, 325
  standard, 95
Bezout’s Theorem, 211, 476
bijective, 12
  iff invertible, 13
bijective function, 36
bilinear form
  alternating, 362
  module of, 361, 362
  symmetric, 361, 362
bilinear map, 424
  module of, 361
binary relation, 29
  antisymmetric, 29
  reflexive, 29
  symmetric, 29
  transitive, 29
Binet’s formula, 370
binomial coefficient, 23
  \( \binom{n}{k} \) divisible by \( p \), 33
  \( \binom{p}{k} \) divisible by \( p \), 24
  \( \binom{p^n}{m} \) not divisible by \( p \), 142
binomial theorem, 24, 76
bisect angle, 209
block Jordan matrix, 355
Bob, 496
Burnside’s theorem on groups of order \( p^i q^j \), 381
\( \mathbb{C} \), see field of complex numbers
calculus, 94
  fundamental theorem, 95
cancellation property, 70
canonical isomorphism, 405
Cantor’s diagonalization method, 415
Cantor, Georg, 187
Cardano’s formula, 105, 269
cardinality, 415, 506
  equal, 415
  strictly smaller, 415, 506
  unequal, 415, 506
category, 435, 436
  arrow, 436
  associative axiom, 436
  automorphism in a, 436
  composition map, 436
  fiber product, 439, 509
  functor, 437
group in a, 441
  group of automorphisms, 437
  homomorphism functor, 438, 509, 510
  identity axiom, 436
  inverse of a morphism, 436, 509
  isomorphism in a, 436, 509
  map, 436
  morphism, 436
  object, 436
  small, 436
  subcategory, 437
  tensor product functor, 510
Cayley graph, 446
  connected iff set generates group, 447
  of a group, 446
  of dihedral group, 446, 510
  of quaternion group, 510
Cayley’s Theorem, 379, 394
Cayley–Hamilton Theorem, 292, 368
center
  of a group, 60, 138
  of a group ring, 494, 518
  of a ring, 83
  of \( p \)-group is non-trivial, 138
  permutation group has trivial, 393
  central element in group ring, 494, 518
  centralizer of a subgroup, 60, 140, 388
  chain, 419
    descending, 363
    maximal element, 419
    of modules, 426
    of submodules stabilizes, 337
    upper bound, 419
  chain rule, 196
  change of basis, 359, 361
    elementary operation, 348
    formula, 303, 322
  change of generating set, 361
  character
    1-dimensional, 294
    group of, 455
    inner product equals multiplicity, 456
    inner product of, 455
    irreducible, 453
    is invariant under conjugation, 454
    is sum of roots of unity, 454, 511
    linear independence of, 294
    not a homomorphism, 454
    of a representation, 453
    of direct sum is sum, 454
    of regular representation, 455
Index

character (continued)
- orthogonality relation, 456
- table, 454
- value at e is rank, 455
- value at power, 511
character group, 455
- inner product equals multiplicity, 456
- inner product on, 455
character table, 454
- of dihedral group, 454
- of quaternion group, 511
characteristic
- of a ring, 75
- of finite field, 117
- zero, 75
characteristic polynomial, 315, 316
- Cayley–Hamilton Theorem, 368
- is unique, 323
- of inverse operator, 324
- roots are eigenvalues, 316
- trace is next-to-top coefficient, 324
characteristic value, see eigenvalue
characteristic zero field extension always separable, 238, 239, 242, 287
char, see characteristic of a ring/field
Chebotarev density theorem, 204
Chebyshev polynomial, 220
China, 221
Chinese Remainder Theorem, 52, 168, 169, 183, 351, 353
- application to Euler phi function, 171
- history, 168
circle, 207
- squaring the, 208
class field theory, 267
class number, 466
- of quadratic extension, 467
classification theorem for finite simple groups, 387
closest vector problem, 481, 499
- Babai’s Algorithm, 481, 499, 500
- Gaussian heuristic, 517
- has a solution, 515
- to find NTRU plaintext, 521
closure
- algebraic, 227
- integral, 433
$C_n$, see cyclic group
coefficient, leading, 341, 362
Cohen, Paul, 504
column and row reduction, 343, 365
column rank, 363
column span, 363
- has same dimension as row span, 363
combination, 23
combinatorial symbol, 23
combinatorics, 21
commutative algebra, 426
commutative diagram, 429
- associative law as a, 430
- Five Lemma, 430, 508
- proof by diagram chase, 430
- tensor product, 423
commutative group, 39
commutative law, 39
- ring, 64
commutative ring, 64
- module over a, 327
commutative square, 430
commutative diagram, 174
comparability property, 418
compass and ruler construction, 207
complement, 11
- of intersection, 27
- of union, 27
complete bipartite graph, 444, 510
complete graph, 444, 510
complex embedding, 468
- conjugate of, 468
complex number, square root of, 252, 289
component of a graph, 445, 505
composition, 12
composition map, 436
composition quotients do not determine group uniquely, 387, 395
composition series, 386
dihedral group, 395
does not determine group uniquely, 387, 395
for group of prime power order, 395
groups with more than one, 386
Jordan–Hölder Theorem, 386, 395
length, 386
quaternion group, 395
quotients, 386
symmetric group, 395
compositum, 291
Galois group of, 291
congruence, 66
- linear, 21
congruent, 20, 73
conic in $\mathbb{P}^2$, 474

conjunctive class  
   abelian group, 453  
   dihedral group, 453  
   number of equals number of irreducible representations, 453  
conjunctive complex embedding, 468  
conjunctive of matrix, 303  
conjunctive subgroup, 289  
   is isomorphic to original subgroup, 130  
   is subgroup, 130  
conjunctive action, 138  
conjunctive automorphism, 388  
conjunctive, 4  
   distributes over disjunction, 6  
connected component,  
   graph is disjoint union of, 445  
   of a graph, 445, 505  
connected graph, 445  
constructibility versus solubility, 271  
constructible number, 210, 271  
   17th-root of unity is, 293  
   is algebraic, 211  
constructible point, 210, 271  
continuous hypothesis, 504  
contradiction, proof by, 4, 27  
contravariant functor, 437  
   Hom, 509  
convex open set, 486  
coordinate, 95  
coordinate ring of affine variety, 471  
corps, 108  
coset, 48, 73, 127  
   all have same size, 49  
   double, 148  
   equal or disjoint, 49  
   equals $gH$ iff $g$ is in coset, 60, 127  
   multiplication algorithm, 128  
countable set, 413, 414  
   product of is countable, 504  
   $\mathbb{Q}$ is, 504  
covariant functor, 437  
   Hom, 438  
cryptography, 496  
   contradictory goals, 499  
   Diffie–Hellman problem, 499, 520  
   efficiency versus security, 499  
   Elgamal, 500, 520  
   GGH, 500, 503  
   hard problems used for, 498  
   lattice-based, 500, 501, 520  
   NTRU, 520  
   pseudo-random number, 503  
   public key, 497  
   random number, 503  
   RSA, 499, 504  
   trapdoor function, 497  
   true random number, 503  
cubic doubling problem, 208  
cubic formula, 105, 269  
curve in $\mathbb{P}^2$, 474  
CVP, see closest vector problem  
cycle, 373  
   and transposition generate $S_n$, 278, 394  
   disjoint, 372  
   disjoint cycles commute, 373, 393  
   length of, 372  
   number of cycles in a power of, 393  
   of a permutation, 372  
   permutation is product of disjoint, 374  
   sign of, 379  
   sign of product of, 379  
   transposition, 375  
cyclic Galois group, 283  
cyclic graph, 444, 510  
cyclic group, 41  
   automorphism group of, 389, 396  
   finite abelian group is product of, 354, 392  
   finitely generated abelian group is product of, 353  
   generator, 41, 47, 55  
   group ring of, 493, 519  
   of prime order, 50  
   product of, 367  
   representation of, 449, 453  
   semidirect product of, 392, 396  
   simple iff prime order, 380  
cyclic module, 333  
cyclic submodule, 331, 358  
   is cyclic group if $R = \mathbb{Z}$, 331  
cyclotomic field, 264  
   contains quadratic extensions, 292  
   Galois group, 265, 513  
   Galois theory, 264  
   ring of integers, 464  
cyclotomic polynomial, 206, 218, 267, 293  
   is separable, 265  
Dalek, 8  
definition, what is a, 1  
degree  
   multiplication rule, 109, 222, 225, 238, 247
degree (continued)
of a homogeneous polynomial, 473
of a hypersurface, 474, 476
of a polynomial, 84, 110
of extension field, 109
of extension field is one, 122
of extension field is prime, 122
of field generated by root of irreducible
polynomial, 115, 189, 222
of minimal polynomial, 226
of polynomial bounds number of roots,
190
of product of polynomials, 110, 122
of splitting field, 194, 223
of zero polynomial, 110
dehomogenization, 476
Deligne, Pierre, 464
derivative
equal to zero, 196
formal, 83, 196
implicit formal, 462
descending chain of ideals, 363
determinant, 309, 315, 405
definition of, 313
definition via action on $\mathfrak{A}_n(M)$, 405
expansion as a sum, 323, 402, 406
is a unit iff endomorphism is invertible,
406
is multiplicative, 314
multiplication formula, 405
non-zero iff linear operator is invertible,
314
DHP, see Diffie–Hellman problem
diagonal matrix, 307
eigenvalues, 322
eigenvectors, 322
Smith normal form, 343
diagonalizable, 307, 354
commuting operators, 322
if $\dim(V)$ distinct eigenvalues, 322
diagram chase, 430
diagram, commutative, 174
difference, 11
differentiation is linear transformation, 94
Diffie, Whitfield, 499
Diffie–Hellman problem, 499
can be used to break Elgamal, 520
dihedral group, 43, 44
Cayley graph, 446, 510
character table, 454
composition series, 395
conjugacy classes of, 453
$D_4$, 38
Galios group, 234, 244, 248, 287, 288
generalization to $C_n \times C_m$, 396
is semidirect product, 392
normal subgroup, 130
(not) isomorphic to symmetric group, 58
of order twelve, 396
representation of, 449, 453, 510
dimension
infinite, 318
of a representation, 448
of a representation is value at $e$, 455
of Jordan block, 355
of module, 334, 336
of vector space, 98
Rank-Nullity Theorem, 304, 429
dimension formula for representations, 456
Diophantine approximation, 215
direct product
basis for, 325
of groups, 389
of infinitely many modules, 332, 359
of infinitely many vector spaces, 319,
325
tensor product distributes over, 507
direct sum
basis for, 325
of a representation, 450
of infinitely many modules, 332, 359
of infinitely many vector spaces, 320,
325
directed graph, 444
commutative diagram is, 429
Dirichlet Unit Theorem, 469
discrete logarithm problem, 498
babystep-giantstep method, 520
discrete subgroup, 477
is finitely generated free abelian group,
478, 516
of maximal rank, 478
rank at most rank of vector space, 516
discriminant
of a lattice, 478, 486, 516
polynomial, 179, 376, 393
disjoint cycles, 372
commute, 373, 393
disjoint union, 14
gives equivalence relation, 15, 374
disjunction, 4
distributes over conjunction, 6
distributive law
  for and/or, 6
  for negation, 6
module, 327
ring, 64
vector space, 93
divisibility, 17, 158
  and congruences, 20
  equivalent to ideal inclusion, 158
division ring, 108
division with remainder, 18, 31, 88, 111, 159
DLP, see discrete logarithm problem
$D_n$, see dihedral group
domain, 12, see also integral domain
divisibility, 158
Euclidean, 159
field of fractions, 172, 434
principal ideal, 159
unique factorization, 158
unique factorization is integrally closed, 434
double-and-add algorithm, 502, 522
double coset, 148
equivalence relation, 148
double negation, 5
doubling cube problem, 208
e is transcendental, 187
ECDLP, see elliptic curve discrete logarithm problem
domain, 443
Egypt, 221
eigenvalue, 306, 315
  at most $\dim(V)$ distinct, 316, 322
diagonal matrix, 322
  distinct have linearly independent eigenvectors, 322
equal to zero, 306, 308
  is root of characteristic polynomial, 316
  of finite-order linear operator is root of unity, 324
  of inverse operator, 324
  of Jordan block, 355
  permutation matrix, 394
  sum is trace, 324
eigenvector, 306
  basis of, 307, 322, 354
diagonal matrix, 322
  exists over algebraically closed field, 308, 451
  is a non-zero vector, 306
  linearly independent if distinct eigenvalues, 322
  Eisenstein irreducibility criterion, 200, 205, 267, 279
element of a set, 9
elementary change-of-basis operation, 348
elementary divisor, 346
elementary matrix operation, 343, 365
  reduce to Smith normal form, 344, 365
  elementary symmetric polynomial, 178, 185, 246, 275, 468
  of roots gives coefficient, 178, 246
Elgamal cryptosystem, 500
  Diffie–Hellman problem will break, 520
Elgamal, Taher, 500
Elkies, Noam, 463
elliptic curve, 457, 459, 498
  associative law is hard to prove, 461
  computing large multiples, 502, 522
  defined over finite field, 463
  defined over $\mathbb{Q}$, 462
  discrete logarithm problem, 498
  group law, 458, 460
  group of $\mathbb{Q}$-rational points, 462
  Hasse’s Theorem, 464, 513
  intersection with a line, 458
  intersection with tangent line, 458
  intersection with vertical line, 459
  Mazur’s Theorem, 463
  Mordell–Weil Theorem, 462
  multiplication by $n$ map, 461
  number of points defined over a finite field, 464, 513
  $\mathcal{O}$, 459
  of rank at least 28, 463
  point at infinity, 459
  points form an abelian group using $\oplus$, 460
  rank is unbounded?, 463
  rank is uniformly bounded?, 463
  rank of group of rational points, 463
  reflection map, 459
  tangent line, 458
  torsion subgroup, 463
  uniform bound for torsion subgroup, 463
  elliptic discrete logarithm problem, 498
  empty set, 10
  is subset of every set, 10
  maps to every set, 420
End, see endomorphism ring
endomorphism
  adjugate, 411
endomorphism (continued)
  induced map on multilinear form, 401, 410
  induced map on multilinear map, 409
  invertible iff determinant is unit, 406
endomorphism ring, 87
  commutative iff dimension one, 320
  dimension of, 299, 321
  isomorphic to ring of matrices, 336, 360
  of a module, 334, 360, 397, 490
  of a vector space, 101, 296, 320
  of rank one module, 405
  rank of, 336, 360
  units, 490
epimorphism, see surjective
equal cardinality, 415
equivalence class, 15
equal or disjoint, 15, 374
equivalence relation, 13, 14, 29
  breaks set into disjoint union, 15, 374
  congruence is a, 20
  connected components of a graph, 445
  double coset, 148
  equivalence class, 15
  reflexive property, 14
  symmetry property, 14
  transitive property, 14
Euclid, 1, 19, 32
Euclidean algorithm, 18, 31, 167, 198, 498, 520, 521
  \( au + bv = \gcd \) theorem, 32
Euclidean domain, 159
every element is product of irreducibles,
  165
  \( F[x] \) is a, 161
  is a PID, 160
  is Noetherian, 338
  matrix with entries in, 342, 344
  size function, 159, 344
  structure theorem for finitely generated
  module, 346, 350
  torsion submodule trivial iff module is
  free, 366
  \( \mathbb{Z} \) is a, 161
  \( \mathbb{Z}[i] \) is a, 161
Euclidean geometry, 472
Euclidean lattice, 477
Euler characteristic, 508
Euler phi function, 171, 183, 499
Euler’s criterion, 216
Euler, Leonhard, 27
evaluation homomorphism, 67, 81, 82, 90,
  94, 226, 357, 362, 432
  image of, 187
Eve, 496
even function, 360
even permutation, 378, 400
exact functor, 443
exact sequence, 359, 366, 426
  additivity of rank in, 429
  annihilator ideals of, 366
  Euler characteristic, 508
  exact functor, 443
  finite generation of modules in, 359, 429,
  508
  Five Lemma, 430, 508
  free modules in, 429, 508
  ideal class group in, 514
  left-exact functor, 443, 508
  long, 508
  of torsion submodules, 508
  right-exact functor, 443
  torsion submodules of, 366
  unit group in, 514
exclusive disjunction, 4
exclusive or, 4
exists, see there exists
extension field, 108
  algebraic of infinite degree, 286
  degree, 109, 122
  extension of isomorphism of, 230
  finite, 109
  finite implies algebraic, 224
  Galois, 235
  infinite, 109
  Primitive Element Theorem, 239
extension of scalars, 507, 509
factorial, 22
  \( 0! = 1, 23 \)
  power of \( p \) dividing, 33
  \( F[\alpha] = F(\alpha) \) iff \( \alpha \) is algebraic, 188, 222,
  224
  Fermat's Last Theorem, 280
  Fermat's Little Theorem, 24, 61, 85
fiber product, 439
  of sets, 509
  of sets is intersection, 509
  universal mapping property, 439, 509
Fibonacci sequence, 30, 369, 370
field, 69, 92, 105
  algebraic number, 187
  algebraic of infinite degree, 286
field (continued)
  algebraically closed, 124, 226, 286, 308, 355
  algebraic closure of, 227, 286
  degree multiplication rule for extensions, 109, 222, 225, 238, 247
  degree of extension, 109, 122
  extension, 108
  extension generated by $\alpha_1, \ldots, \alpha_n$, 108
  extension viewed as vector space, 109
  finite, 69, 70, 92, 107, 117, 119, 200, 233, 254
  finite subgroup of multiplicative group is cyclic, 192, 265, 468
  fixed, 243
  generated by root of irreducible polynomial, 115, 189, 222
  generated by roots, 270
  homomorphism is injective, 106
  iff quotient by maximal ideal, 78
  inseparable extension, 200, 238, 239, 290
  is a domain, 83
  matrix with entries in, 343
  number field, 464
  of algebraic numbers, 224
  of complex numbers, 92, 107
  of complex numbers is algebraically closed, 226, 251
  of fractions of, 172, 434
  of rational functions, 175, 176, 275, 276, 287
    of affine variety, 471
    of projective space, 473
    of projective variety, 514
  of rational numbers, 92, 107
  of real numbers, 92, 107
  of symmetric rational functions, 275, 276
  $\mathbb{Q}(\sqrt{2})$, 107, 109
  $\mathbb{Q}(i)$, 107, 109
  quotient by irreducible element is, 164
  quotient by irreducible polynomial is, 113, 222
  radical extension, 270
  skew, 108
  splitting, 124, 194, 223
  splitting in characteristic zero, 238, 287
  subfield, 108
  transcendental number, 187
  field automorphism, linear independence of, 282

field extension
  algebraic, 221, 223
  always separable in characteristic zero, 238, 239, 242, 287
  compositum of, 291
  conjugate subfields, 289
  cyclotomic, 264
  extension of isomorphism of, 230
  finite implies algebraic, 224
  Galois, 235, 242
  Galois group of, 228
  Galois group of intermediate field, 243
  generated by finitely many elements, 122, 239
  intermediate, 243
  Kummer, 264, 267, 268, 392
  norm, 291
  normal, 258
  Primitive Element Theorem, 239
  radical, 270
  separable, 239, 287
  trace, 291
  with cyclic Galois group, 283

field of fractions, 172, 434
  generalized, 184

field of rational numbers
  algebraic closure of, 227
  Fields Medal, 215
  finite abelian group
    is product of cyclic groups, 392
    structure theorem, 52
  finite algebra over a ring, 432
  finite basis, 95
  finite degree field extension, 109
    is algebraic, 224
  finite field, 69, 70, 92, 107, 117
    algebraic closure of, 227, 290
    characteristic, 117
    contains $\mathbb{F}_p$, 117
    elliptic curve defined over, 463
    exists for all prime powers, 119, 200, 254
    Galois theory of, 254, 255
    irreducible element in polynomial ring, 118
    isomorphic if same order, 119, 200, 233, 254
    multiplicative group is cyclic, 192, 468
    order is prime power, 117
    primitive root, 193
    product of non-zero elements, 121
    squares in, 216
Index

finite group
  abelian is product of cyclic groups, 354
  classification of simple, 387
  sporadic simple, 387
finite set, 10, 414
  map is injective iff surjective if same size,
  13, 29
finite type, 432
finite-dimensional vector space
  left-inverse iff right-inverse, 322
  linear operator injective iff surjective, 305
finitely generated abelian group
  of points on an elliptic curve, 462
  structure theorem, 353, 485
  unit group of a number field is, 469
finitely generated algebra, 362, 432
  Hilbert Basis Theorem, 432
  over Noetherian ring is Noetherian, 432
finitely generated free module
  bases all have same size, 334
  rank of, 334, 336
  right-inverse equals left-inverse, 490
finitely generated ideal, 337
finitely generated module, 332, 333, 359, 429, 508
  algebra that is a, 432
  change of generating set, 361
  free of n-tuples, 333
  multilinear map of, 398, 409
  rank of, 346
  structure theorem, 346, 350, 463
first-order logic, 419
Five Lemma, 430, 508
fixed field, 243
  Galois group of, 245, 247
  of Galois group is base field, 258
  of Galois group is intermediate field, 245, 247
floor, 33
F-module, see module over field
F^n, see vector space of n-tuples
for all, 7
forgetful functor, 438, 507
form
  alternating, 399
  multilinear, 398
  symmetric, 399
  symmetrization of, 410
formal derivative, 83, 196
  equal to zero, 196
  implicit, 462
  rules for, 196
fizzle, 9
F_p, see finite field
fractional ideal, 466
  group of, 466
  principal, 466
free module, 332, 333, 429, 508
  bases all have same size, 334
  change of basis, 359, 361
  determinant, 405
  finitely generated of n-tuples, 333
  iff torsion submodule is trivial, 366
  multilinear map of, 398, 409
  rank additive in exact sequence, 429
  rank of, 334, 336
Frey, Gerhard, 280
Frobenius homomorphism, 76, 255, 496
Frost, Robert, 429
function, 12
  bijective, 12, 36
  bijective iff invertible, 13
  composition of, 12
  composition of in a category, 436
  domain, 12
  even, 360
  formal definition, 12
  injective, 12, 414
  injective iff surjective for finite equal size
    sets, 13, 29, 53
  invertible, 13
  invertible iff bijective, 13
  odd, 360
  one-way, 503
  range, 12
  set of from S to T, 415
  surjective, 12, 414
  trapdoor, 497
functor, 437
  contravariant, 437
  covariant, 437
  exact, 443
  forgetful, 438, 507
  Hom, see homomorphism functor
  homomorphism, 438, 509, 510
  left-exact, 443, 508
  on the category of modules, 442
  right-exact, 443
  tensor product, 442, 443, 510
fundamental domain, 478
  sum of lattice vector and vector in, 479, 515
fundamental domain (continued)
  volume of, 478, 486, 516
  Voronoi cell, 486, 487
  weak, 486
Fundamental Theorem of Algebra, 250, 251
Fundamental Theorem of Arithmetic, 157
Fundamental Theorem of Galois Theory, 247
$F$-vector space, 93
$F[x]$-module, 329, 355

Galois extension, 235, 242
  abelian of $\mathbb{Q}$, 267
  radical extension contained in, 270
Galois group, 228
  as permutation group, 242
  cyclic, 283
  cyclotomic field, 265, 513
  dihedral group, 234, 244, 248, 287, 288
  fixed field of conjugate of subgroup, 289
  fixed field of subgroup, 243
  is a group, 228
  Kummer field, 268
  linear independence of field automorphisms, 282
  of compositum, 291
  of conjugate of intermediate field, 289
  of fixed field is subgroup, 245, 247
  of intermediate field, 243
  of splitting field, 235
  of $X^4 - 2$, 233, 244, 248, 287, 288
  order equals degree of $K/F$, 235
  permutes roots of polynomial, 228
  radical extension has solvable, 273
  semidirect product, 268, 292, 392
  solvable iff polynomial solvable by radicals, 274, 294
  trivial, 229, 286

Galois theory, 221
  cyclotomic field, 264
  $H = G(K/K^H)$, 245, 247
  equivalent formulations, 257, 258
  finite field, 254, 255
  Fundamental Theorem of, 247
  $H = G(K/K^H)$, 245, 247
  inclusion reversing correspondence, 247
  Kummer field, 268, 292
  normal subgroup iff Galois, 247, 262
  gamma function, 480, 517
  Gauss’s Lemma, 202, 467
  Gauss, Carl, 20, 193
  Gaussian heuristic, 517, 522
Gaussian integers, 66
  are a Euclidean domain, 161
  are a PID, 161
  are a UFD, 165
  unit group, 70
gcd, see greatest common divisor
general linear group, 42, 56, 57, 296, 448
generating set
  of a group, 59, 446
  of a group iff Cayley graph connected, 447
  of an ideal, 73, 517
generator of cyclic group, 41, 47, 55
GGH cryptosystem, 500, 503
$g^{-1}Hg$, see conjugate subgroup
GL$_n$, see general linear group
Goldbach’s Conjecture, 27
Goldbach, Christian, 27
Goldreich, Oded, 500
Goldwasser, Shafi, 500
graph, 443
  commutative diagram is directed, 429
  complete, 444, 510
  complete bipartite, 444, 510
  connected, 445
  connected component, 445, 505
  cyclic, 444, 510
  directed, 444
  disjoint union of connected components, 445
  isomorphism, 446
  isomorphism problem, 446
  morphism, 446
  path, 444, 510
  path in a, 445
  set of edges, 443
  set of vertices, 443
  subgraph of, 446
  undirected, 444
greatest common divisor, 18
  equals $au + bv$, 18, 364
  equal to one, 18
  Euclidean algorithm, 31
  in polynomial ring, 288
  in principal ideal domain, 364
Greece, 221
group, 39
  abelian, 39
  additive, 41
  affine linear, 396
  automorphism, 154
  automorphism group of a, 388
### Index

**group  (continued)**

- axioms, 39
- Cayley graph, 446
- center, 60, 138
- centralizer of a subgroup, 60, 140, 388
- character, 294
- character group of, 455
- classification of finite simple, 387
- commutative, 39
- composition quotient, 386
- composition series, 386, 395
- computing large powers, 502, 522
- conjugation action, 138
- coset, 48, 127
- cyclic, 41
- dihedral, 43, 44
- discrete logarithm problem, 498, 520
- double coset, 148
- elliptic curve, 458, 460
- elliptic discrete logarithm problem, 498
- equals semidirect product of subgroups, 391
- Galois, 228
- homomorphism from group to
  - automorphism group of normal subgroup, 388
- ideal class, 466
- in a category, 441
- index multiplication rule, 60
- infinite, 41
- inner automorphism, 388
- inversion is homomorphism iff abelian, 58, 390
- irreducible representation, 451
- isomorphism, 45
- Jordan–Hölder Theorem, 386, 395
- kernel of homomorphism, 47
- Lagrange’s Theorem, 50, 499
- Maschke’s Theorem, 452, 511
- matrix, 42
- maximal normal subgroup, 387, 395
- monster, 387
- multiplicative, 41
- normal subgroup, 129
- normalizer of a subgroup, 140, 145
- number of abelian groups of a given order, 368
- number of conjugacy classes equals
  - number of irreducible representations, 453
- number of conjugates of subgroup, 145
- of fractional ideals of a number field, 466
- of Lie type, 387
- of order $p^2$ is abelian, 139
- of order $p^n$, see Sylow subgroup
- of order $p^n$ has non-trivial center, 138
- of order $pq$, 144, 395
- of order ten, 143
- of order twelve, 396
- of prime order is cyclic, 50
- of units of a number field, 467
- Orbit-Stabilizer Counting Theorem, 136
- order of, 40
- order of an element, 40
- order of element divides order of group, 50, 499
- outer automorphism, 388
- permutation, 371
- product of, 51, 389
- product of subgroups, 147
- quaternion, 43
- quotient by normal subgroup, 132
- quotient map, 132
- regular representation, 449
- representation of, 448
- ring of invariants for action by, 180
- Schur’s Lemma, 451
- semidirect product, 268, 292, 389, 390
- simple, 129, 380
- simple abelian, 380
- simple of prime power order is cyclic, 380
- solvable, 272, 381, 387
- sporadic finite simple, 387
- subgroup generated by element, 47
- subgroup generated by subset, 59, 394, 446
- subgroup of a, 46
- subgroup of index two is normal, 151
- subset generates iff Cayley graph connected, 447
- Sylow subgroup, 142
- Sylow’s Theorem, 140, 253, 278
- symmetric, 42
- transitive action, 136, 152
- trivial, 47
- group action, 133
- orbit, 134
- permutation representation, 449
- stabilizer, 134
- group homomorphism, 44
- kernel is normal subgroup, 130
- group of units, see unit group
group representation, see representation
group ring, 493
  abelian iff group is abelian, 493, 519
central element associated to normal subgroup, 494, 518
idempotent associated to subgroup, 494, 518
left ideal is invariant subspace, 494, 518
multiplication formula, 493
of cyclic group, 493, 519
regular representation of group, 494, 518
\( G \times x \), see orbit
\( G_x \), see stabilizer

\( \mathbb{H} \), see quaternion ring
Hadamard’s inequality, 480
Halevi, Shai, 500
Hamilton, William, 67
Hasse’s Theorem, 464, 513
Hasse, Helmut, 464
Helleougarch, Yves, 280
Hellman, Martin, 499
Hermite’s constant, 479
  upper bound for, 480
Hermite, Charles, 187
Hermite–Minkowski Theorem, 479, 488, 516
higher-order logic, 416
Hilbert Basis Theorem, 340, 432, 471
Hilbert Finiteness Theorem, 180
Hilbert Irreducibility Theorem, 277
Hilbert Theorem “90”, 283
Hom, see homomorphism space
Hom functor, see homomorphism functor
homogeneous coordinates, 472
homogeneous ideal of projective algebraic set, 474
homogeneous polynomial, 186, 473
homomorphism
  Frobenius, 76, 255, 496
group, 44
group has normal kernel, 130
  inclusion, 52
kernel is ideal, 75, 518
kernel is submodule, 330, 358
logarithm, 45
matrix associated to, 335
matrix of composition, 336, 360
module, 328
  of a representation, 450
of fields is injective, 106
of polynomial ring, 82
projection, 52
ring, 65
  ring from \( \mathbb{Z} \), 68
to quotient group, 132
to quotient module, 330, 358
to quotient ring, 75, 518
vector space, 93, 295
homomorphism functor, 438, 509, 510
covariant, 438
is left-exact, 443
on modules is left-exact, 510
on the category of modules, 442, 443, 510
homomorphism space
  dimension of, 299, 321
isomorphic to space of matrices, 299, 335, 360
  of a module, 334, 397
  rank of, 336, 360
  vector space, 101, 295, 320
hyperplane, 474
  boundary of Voronoi cell, 487
hypersurface, 475
  degree of, 474, 476
  multiplicity at intersection of, 476
  transversal intersection, 476, 477
ideal, 72
affine algebraic set associated to, 471
annihilator, 349, 365, 366
congruence, 73
coset of an, 73
descending chain, 363
finitely generated, 337
generated by a set, 73, 517
generated by irreducible element is maximal, 164
generated by irreducible element is prime, 164
generated by irreducible polynomial is maximal, 113, 222
generators for, 73, 517
in polynomial ring is principal, 112, 222
is \( R \)-module, 329, 358, 359
kernel is a two-sided, 518
kernel is an, 75
left, 489
maximal, 77
of affine algebraic set, 471, 514
of projective algebraic set, 474
prime, 77
principal, 73, 112, 159
ideal (continued)
  product of, 88
radical of, 88, 471
right, 489
sum of, 88
two-sided, 489
unique factorization a product of prime
  ideals, 465
unit, 73
zero, 73
ideal class group, 465, 466
  class number, 466
  in exact sequence with unit group, 514
  is finite, 466
  of quadratic extension, 467
idempotent, 84, 86, 494, 518
  element, 518
  in group ring, 494, 518
identity axiom, 39, 133, 436
identity law
  module, 327
  vector space, 93
identity permutation, 36
if and only if, 5
iff, see if and only if
IFP, see integer factorization problem
image
  is finitely generated free module, 366
  is vector subspace, 322
  of linear transformation, 304
  rank of, 366
implication, 4
implicit differentiation, 461, 462
inclusion reversing correspondence, 247
inclusion/exclusion principle, 25, 26, 120
  for three sets, 25
  for two sets, 25
index, 50
  multiplication rule, 60
India, 221
induction, 16
  proof that all horses have the same color, 30
  proof using well-ordering principle, 16
infinite degree field extension, 109
  algebraic, 286
infinite set, 414
  countable, 414
  uncountable, 414
infinite-dimensional vector space, 98, 318
  linear operator injective and not surjective, 319, 325
  linear operator surjective and not injective, 319, 325
  one-sided inverse, 319, 325
  shift operator, 319, 325
infinitely many variables, 185, 338
injective, 12, 414
  iff surjective, 53
  iff surjective for finite same size sets, 13, 29
inner automorphism, 154, 388
  abelian group has no, 388, 395
  quaternion group, 396
inner product
  equals multiplicity, 456
  of characters, 455
inseparable, 197, 223
  field extension, 200, 238, 239, 290
  irreducible polynomial that is, 200, 238, 290
insolubility by radicals, 271
  generally if degree \( \geq 5 \), 277
  iff Galois group not solvable, 274, 294
insolubility versus non-constructibility, 271
integer factorization problem, 498
integers, 41
  \( au + bv = \text{gcd} \) theorem, 18
  congruence, 20, 66
  divisibility, 17
  division with remainder, 18, 31
  greatest common divisor, 18
  modulo \( m \), 21, 41
  prime, 19
  prime divides product, 19
  relatively prime, 18
  ring of, 17, 63
  square-free, 198
integers modulo \( m \), 21, 41, 65
  unit group, 70
integral closure, 433
  is a ring, 433
  number field, 464
integral domain, 69
  cancellation property, 70
  divisibility, 158
  Euclidean, 159
  field of fractions, 172, 434
  finite is a field, 83
  iff quotient by prime ideal, 78
integral domain (continued)
  principal ideal, 159
  unique factorization, 434
integral element
  criterion for, 433
  sum and product are integral, 433
integral extension
  of a field same as algebraic, 433
  of a ring, 433
integrality criterion, 433
integally closed ring, 434
  UFD is, 434
integration is linear transformation, 95
intermediate field, 243
  fixed field of Galois group is, 245, 247
  Galois group of, 243
  Galois group of conjugate, 289
  Galois of normal subgroup, 247, 262
  of \(X^4 - 2, 248, 287, 288\)
Intermediate Value Theorem, 250
intersection, 10
  Bezout’s Theorem, 476
  complement of, 27
  multiplicity of, 476
  of infinitely many sets, 28
  of subsets is fiber product, 509
  transversal, 476, 477
intersection of lines in \(\mathbb{P}^2\), 474
intersection theory, 474
invariant subspace, 450
  is left ideal of group ring, 494, 518
  projection map to, 511
  trivial, 451
inverse
  axiom, 39
  left, 489
  of morphism in a category, 436, 509
  right, 489
  two-sided, 489
invertible, 13
  iff 0 not eigenvalue, 308
  iff bijective, 13
  iff determinant is unit, 406
  linear operator, 296
irreducible element, 158
  divides product, 165
  generates maximal ideal, 164
  generates prime ideal, 164
  in a ring, 158
irreducible polynomial, 113, 222
  degree of field generated by root, 115, 189, 222
  Eisenstein irreducibility criterion, 205
  example of inseparable, 200, 238, 290
  generates maximal ideal, 113, 222
  minimal polynomial is, 226
  over finite field, 118
  product over all, 120
  separable if characteristic zero, 199, 223, 239
  separable if derivative is non-zero, 199, 223
irreducible representation, 451
  abelian group, 453
  finitely many, 453
  Maschke’s Theorem, 452, 511
  multiplicity in regular representation, 452, 456
  multiplicity of, 452
  Schur’s Lemma, 451
  sum of dimensions, 453
isomorphism, see also bijective
  canonical, 405
  extension of field, 230
  group, 45
  in a category, 436, 509
  of a representation, 450
  of graphs, 446
  ring, 65
joke, math fruit, 39, 419
Jordan block, 355
  has only one eigenvalue, 368
  has only one eigenvector direction, 368
  is sum of diagonal plus nilpotent, 368
Jordan normal form, 354, 355, 368
  blocks are unique, 368
  theorem, 355
Jordan–Hölder Theorem, 386, 395

\(k\)-cycle, 372
kernel, 47, 65, 304, 328
  is a two-sided ideal, 518
  is a subgroup, 47
  is a submodule, 330, 358
  is an ideal, 75

\(\sqrt{n}\) is, 32
\(\sqrt{p}\) is, 20
irreducibility theorem of Hilbert, 277
irreducible character, 453
  orthogonality relation, 456
kernel (continued)
  is finitely generated free module, 366
  is normal subgroup, 130
  is subspace, 304
  is trivial iff map is injective, 47, 75, 304, 330, 358
  is vector subspace, 322
  linear transformation, 304, 328
  of a group homomorphism, 47
  of a ring homomorphism, 65
  of map to quotient module, 358
  of quotient map of groups, 132
  of quotient map of modules, 330
  of quotient map of rings, 74
  rank of, 366
  Rank-Nullity Theorem, 304, 429
  zero iff injective, 322
key, public/private, 497
Körper, 108
Kronecker’s theorem, 267
  for quadratic extensions, 292
Kummer extension, 267, 268, 392
Kummer field, 264, 267, 268, 392
  Galois group, 268
  Galois theory, 268, 392
Kummer homomorphism, 268

Lagrange’s Theorem, 50, 125, 136, 499
lattice, 478
  Babai’s Closest Vector Algorithm, 481, 499, 500
  bases related by $\text{SL}_n(\mathbb{Z})$, 516
  closest vector problem, 481, 499
  covolume, 478, 486, 516
  discriminant, 478, 486, 516
  Euclidean, 477
  fundamental domain, 478, 486
  Gaussian heuristic, 517, 522
  Hadamard’s inequality, 480
  has a short basis, 480
  has a short vector, 479, 488, 516
  Hermite’s constant, 479
  intersection with ball is finite, 515
  LLL reduction algorithm, 483
  Minkowski Theorem, 480
  NTRU, 521
  shortest vector problem, 481
  sum of vector in fundamental domain and vector in, 479, 515
  volume of fundamental domain, 478, 486, 516
  Voronoi cell, 486, 487
lattice reduction, 483
  LLL algorithm, 483
lattice-based cryptosystem, 500, 501, 520
  GGH, 500
  NTRU, 520
law of the excluded middle, 4, 27
leading coefficient, 341, 362
least common multiple, 53
left coset, see coset
left-exact functor, 443, 508
  homomorphism functor is, 443, 510
left ideal, 489
left principal ideal, 490
left-inverse, 87, 319, 322, 325, 489
  equals right-inverse, 86, 489, 490
  of morphism in a category, 436, 509
left-shift operator, 319, 322, 325
length of a cycle, 372
length of composition series, 386
Lenstra, Arjen, 483
Lenstra, Hendrik, 483
less than, 10
Lindemann, Ferdinand von, 187
line, 2, 207
  affine, 470
  in $\mathbb{F}^2$, 474
  intersect in projective plane, 474
  projective, 472
linear combination, 95
linear congruence, 21
linear form
  alternating, 311, 362, 399
  bilinear, 361
  multilinear, 311, 398
  symmetric, 361, 399
linear independence, 96, 318, 332
  of characters, 294
  of field automorphisms, 282
linear operator, 101, 296, 320
Cayley–Hamilton Theorem, 368
  characteristic polynomial is unique, 323
  characteristic polynomial of inverse, 324
  commuting simultaneously diagonalizable, 322
determinant, 313
determinant is multiplicative, 314
diagonalizable, 307, 354
diagonalizable if $\dim(V)$ distinct eigenvalues, 322
eigenvalue, 306
eigenvalue of inverse, 324
linear operator (continued)
eigenvector, 306
finite order ⇒ eigenvalues are roots of
unity, 324
has eigenvector over algebraically closed
field, 308, 451
induced map on alternating $n$ forms, 312,
323
injective and not surjective, 319, 325
injective iff surjective, 305
inverse is linear operator, 297, 320
invertible, 296
invertible iff 0 not eigenvalue, 308
invertible iff determinant non-zero, 314
is root of characteristic polynomial, 368
Jordan normal form, 354, 355, 368
left-inverse iff right-inverse on
finite-dimensional vector space, 322
of dimension one vector space, 310
one-sided inverse, 319, 325
shift, 319, 325
singular, 296
surjective and not injective, 319, 325
linear recursion, 368
closed formula, 369
matrix associated to, 369
linear transformation, 93, 295
change-of-basis formula, 303, 322
composition defines matrix multiplication,
302
differentiation, 94
image is vector subspace, 322
injective iff ker $= \{0\}$, 322
integration, 95
kernel, 304, 328
kernel is vector subspace, 322
matrix of, 298, 335
matrix of composition, 301
module, 328
null space, 304
scalar product, 101, 295, 320, 334, 360
sum of, 101, 295, 320, 334, 360
linearly independent set, 96, 332
contained in basis, 97, 318
module, 322
no larger than spanning set, 99
of eigenvectors if distinct eigenvalues, 322
vector space, 96, 318
Liouville’s number, 187, 215
Liouville, Joseph, 187
LLL algorithm, 483
local ring, 89, 184
of $\mathbb{P}^n$ at a point, 475, 515
of projective space, 515
logarithm, 45
discrete, 498
logic, 3
logical equivalence, 5
logical operation, 3
conjunction, 4
disjunction, 4
exclusive disjunction, 4
exclusive or, 4
for all, 7
if and only if, 5
implication, 4
logical equivalence, 5
negation, 3
there exists, 7
there exists a unique, 8
long exact sequence, 508
loop, 55
Lovász, László, 483
Lucas sequence, 30, 370
magic
differentiation, 198
field containing root of polynomial, 112
irreducibility criterion, 204
proof that looks like, 173
property of Noetherian ring, 340
universal mapping property, 424
vector space of alternating forms, 309
magma, 55
map, 12
in a category, 436
sending maps to maps-of-maps, 401, 410
Maschke’s Theorem, 452, 511
false over field of characteristic $p$, 512
mathematical induction, 16
mathematical cryptography, 496
hard problems used for, 498
mathematical logic, 3
matrix, 298, 334
adjugate, 411
associated to a linear recursion, 369
associated to a module homomorphism,
335
basis for $\text{Mat}_{m \times n}$, 321, 335
Cayley–Hamilton Theorem, 368
change-of-basis formula, 303, 322
column span, 363
commuting pair of, 368
matrix (continued)

commuting simultaneously diagonalizable, 322
conjugate of, 303
diagonal, 307
diagonalizable, 307, 354
dimension of $\text{Mat}_{m \times n}$, 299, 300, 321
elementary operation, 343, 364, 365
endomorphism attached to a, 299, 335, 360
is root of characteristic polynomial, 368
Jordan block, 355
Jordan normal form, 354, 355, 368
nilpotent, 368
of linear transformation relative to basis, 298, 335
permutation, 394, 449
product formula for, 301
rank, 363
rank of $\text{Mat}_{m \times n}$, 335, 336, 360
ring, 68, 83
ring is not domain, 81
row and column reduction, 343, 365
row span, 363
Smith normal form, 343, 344, 365
trace, 324
with entries in a Euclidean domain, 342, 344
with entries in a field, 298, 343
with entries in a principal ideal domain, 342, 344, 365
with entries in a ring, 334
matrix group, 42, see also general linear group
matrix multiplication, 42, 56, 57, 68, 301, 336
is composition of linear transformation, 302
origin of horrible formula, 301
pictorial mnemonic, 302
matroid, 55
matryoshka nesting dolls, 107
maximal element, 337, 418
of a chain, 419
maximal ideal, 77
exists, 79, 506
generated by irreducible element, 164
generated by irreducible polynomial, 113, 222
iff quotient is field, 78
is prime, 79
ring with unique, 89, 184
maximal normal subgroup, 387, 395
quotient is simple, 387, 395
Mazur’s Theorem, 463
meromorphic function, 515
minimal element, 11, 419
minimal polynomial, 225
degree of, 226
is irreducible, 226
separable, 239, 287
Minkowski Theorem, 479, 480, 488
lattice points in compact convex symmetric regions, 516
$M_n$, see matrix ring
module, 327
algebra that is a finitely generated, 432
annihilator ideal, 349, 365, 366
associative law, 327
automorphism group, 490
bases all have same size, 334
basis iff spans and linearly independent, 332
bilinear form, 361, 362
bilinear map, 361
chain of, 426
change of basis for free, 359, 361
change of generating set, 361
cyclic, 333
cyclic submodule, 331, 358
determinant map on free, 405
dimension of, 334, 336
direct product of infinitely many, 332, 359
direct sum of infinitely many, 332, 359
distributive laws, 327
elementary divisor, 346
End, 334, 397, 490
determinant map on multilinear form, 401, 409, 410
determinant map on endomorphism ring, 334, 360, 490
Euler characteristic, 508
even function, 360
exact functor, 443
exact sequence, 359, 366, 426
extension of scalars, 509
finitely generated, 332, 333, 359, 429, 508
finitely generated over Noetherian ring is Noetherian, 340
finitely generated submodule, 337
free, 332, 333, 429, 508
functor on the category of, 442
Hom, 334, 397
module (continued)
  homomorphism, 328
  homomorphism functor on the category of, 442, 443, 510
  homomorphism kernel is submodule, 330, 358
  identity law, 327
  image is finitely generated free module, 366
  kernel is finitely generated free module, 366
  kernel of linear transformation, 328
  left-exact functor, 443, 508
  linear transformation, 328
  linearly independent set, 332
  matrix associated to homomorphism, 335
  matrix of composition of homomorphisms, 336, 360
  maximal element of collection of submodules, 337
  multilinear form, 361, 362
  multilinear map, 361, 397, 422
  need not have a basis, 332, 333, 359
  Noetherian, 337
  odd function, 360
  of matrices Mat_{n \times s} (R), 334
  of matrices is free, 335
  of n-tuples, 328, 331, 333, 357
  is Noetherian, 340
  over Euclidean domain, 346
  over field is vector space, 329
  over \( F[x] \), 329, 355
  over \( \mathbb{Z}[x] \), 333, 359
  \( \pi \)-primary part, 351, 367
  principal submodule, 331, 358
  product, 330
  product of linear transformations, 334, 360
  quotient is module for quotient ring, 331, 358
  quotient map, 330
  quotient module, 330, 358
  rank of End, 336, 360
  rank of finitely generated, 346
  rank of Hom, 336, 360
  rank one, 405
  right-exact functor, 443
  right-inverse equals left-inverse, 490
  span of subset, 330, 332, 359
  structure theorem, 346, 350

  submodule generated by a set, 330, 332, 359
  submodule of, 330
  sum of linear transformations, 334, 360
  tensor product, 422
  tensor product functor on the category of, 442, 443, 510
  torsion submodule, 349, 365, 366, 427, 508
  modulo, 20, 21
  monic polynomial, 110, 433
  monoid, 55, 64
  monomorphism, see injective
  monster group, 387
  moon made of green cheese, 5
  Mordell, Louis, 462
  Mordell–Weil Theorem, 462
  morphism, see also homomorphism
    in a category, 436
    inverse in a category, 436, 509
    of graphs, 446
  Moufang loop, 55
  multilinear algebra, 422
  multilinear form, 398
    alternating, 399
    map induced by endomorphism, 401, 410
    module, 361, 362
    sign change formula for alternating, 400
    symmetric, 399
    symmetrization of, 410
  multilinear map, 397, 422
    is not homomorphism, 409
    map induced by endomorphism, 409
    module of, 361
    of free modules is free, 398, 409
    rank of space of, 398, 409
    space of, 398, 422
    space of is \( R \)-module, 398
    space of is tensor product homomorphism space, 507
  multilinearity property, 311
  multiplication, 63
  multiplication by \( \alpha \) map, 291
  multiplicative group, 41
    computing large powers, 502, 522
    of field is cyclic, 192, 265, 468
  multiplicatively closed set, 184
  multiplicity
    formula for representations, 456
    of an irreducible representation, 452
multiplicity (continued)
of point in intersection in projective space, 476

multivariate polynomial ring, 176, 470
action of symmetric group, 176, 376
is a UFD, 159
of infinitely many variables, 185, 338
symmetric polynomial, 177

Munroe, Randall, xvii

N, see natural numbers

Napier, John, 45

natural numbers, 7, 10, 413
axiomatic definition, 10
induction, 16
less than, 10
well-ordering principle, 11, 16, 18

negation, 3
distributes over conjunction, 6
distributes over disjunction, 6
double, 5

n-form, see multilinear form; alternating form

$N_G(H)$, see normalizer of a subgroup

nilpotent, 84, 89, 184
matrix, 368
nilradical, 89, 90

Noether, Emmy, 337
Noetherian module, 337
finitely generated module over Noetherian ring is, 340
iff submodule and quotient module
Noetherian, 339

Noetherian ring, 337
Euclidean domain is, 338
example of non-Noetherian ring, 338
finitely generated module over is
Noetherian, 340
Hilbert Basis Theorem, 340, 432
polynomial ring over a field is, 338, 342, 471
polynomial ring over a Noetherian ring is, 340, 342, 432, 471
principal ideal domain is, 338
non-commutative polynomial ring, 491
non-commutative ring, 67, 489
center, 83
endomorphism ring of a module, 490
group ring, 493
homomorphism kernel is two-sided ideal, 518
ideal generated by a set, 517

idempotent element, 518
left ideal, 489
left-inverse, 489
polynomial, 491
polynomial with infinitely many roots, 216
principal ideal, 490
quotient by two-sided ideal, 489, 518
right ideal, 489
right-inverse, 489
right-inverse equals left-inverse, 490
two-sided ideal, 489
two-sided inverse, 489
two-sided inverses are equal, 86, 489
two-sided unit, 296
unit group, 489

non-constructibility versus insolubility, 271
non-residue, 216
non-unique factorization, 167
non-Euclidean geometry, 2
non-Noetherian ring, 338

norm for field extension, 291
normal field extension, 258

normal subgroup, 129
homomorphism from group to
automorphism group of, 388
index two is, 151
intermediate field Galois iff, 247, 262
kernel is, 130
maximal iff quotient is simple, 387, 395
of symmetric group, 381
quotient by is group, 132
simple group if no non-trivial, 380
normalizer of a subgroup, 140, 145

normal field extension, 258

nth cyclotomic polynomial, 206, 218, 267
NTRU cryptosystem, 520
NTRU lattice, 521
null space, 304
is subspace, 304
is trivial iff map is injective, 304
Rank-Nullity Theorem, 304, 429

Nullstellensatz, 471, 514

number field, 464
class number, 466
complex embedding, 468
Dirichlet Unit Theorem, 469
fractional ideal, 466
group of fractional ideals, 466
ideal class group, 465, 466
ideal class group is finite, 466

number field (continued)
  ideal class group of quadratic extension, 467
  real embedding, 468
  ring of integers, 464
  torsion subgroup, 467, 513
  unique factorization of ideal, 465
  unit group, 467
  unit group of quadratic extension, 469
number theory, 17
  algebraic, 464

object in a category, 436
odd function, 360
odd permutation, 378, 400
one-to-one, see injective
one-way function, 503
onto, see surjective
orbit, 134
  equal or disjoint, 134
orbit-stabilizer formula, 135, 261, 374
Orbit-Stabilizer Counting Theorem, 136
order
  of a group, 40
  of a group element, 40
  of group element divides order of group, 50, 499
  of product of elements in abelian group, 53, 192, 367
  of subgroup divides order of group, 50
  of symmetric group, 53, 371
ordered list, 22
ordered pair, 11
ordered set, 10, 418
  partially, 418
orthogonality relation for irreducible characters, 456
outer automorphism, 154, 388
parallel postulate, 2
partial order, 29
partially ordered set, 29, 418
  antisymmetry property, 418
  chain, 419
  comparability property, 418
  maximal element, 337, 418
  maximal element of chain, 419
  minimal element, 419
  reflexive property, 418
  transitive property, 418
  upper bound of chain, 419
path graph, 444, 510
path in a graph, 445
Peano arithmetic, 10
Pell’s equation, 469
permutation, 22, 35, 36, 42
  action on polynomial ring is homomorphism, 177, 185, 376
  cycle, 373
  cycle of an element, 372
  equals product of disjoint cycles, 374
  equals product of transpositions, 375, 400
  even, 378, 400
  identity, 36
  inverse of a, 36
  length of a cycle, 372
  matrix associated to a, 394, 449
  odd, 378, 400
  parity of number of transpositions as product, 376
  representation, 449
  set with n elements has n!, 22
  sign, 378, 400
  sign of product of cycles, 379
  transitive, 372, 393
  transposition, 375
permutation group, see also symmetric group, 371
  Cayley’s Theorem, 379
  center is trivial, 393
  every group a subgroup of some, 379
  Galois group is, 242
  homomorphism to $GL_n$ by permutation matrices, 394
  number of cycles in a power of a cycle, 393
permutation matrix, 394, 449
  determinant is sign, 394
  eigenvalues are roots of unity, 394
permuted polynomial, 176, 376
Persia, 221
$p$-group has non-trivial center, 138
phi function, 171, 183, 499
philosopher’s stone, 130
$\pi$ is transcendental, 187
$\pi$-cycle, 372
PID, see principal ideal domain
pigs with wings, 5
$\pi$-primary part of module, 351, 367
plane, 2
  affine, 470
  lines and circles in, 207
  of complex numbers, 161
plane (continued)
  projective, 472
  vectors in, 91
\IP^n, see projective space
point in projective space, 472
polyhedron, 487
polynomial
  additive, 494
  coefficient is elementary symmetric
    polynomial of roots, 178, 246
  degree, 84, 110
  degree of product, 84, 122
  discriminant, 179, 376, 393
  distinct roots, 197, 223
division with remainder, 31, 88, 111
Eisenstein irreducibility criterion, 205
elementary symmetric, 178, 185, 246,
  275, 468
example of inseparable irreducible, 200,
  238, 290
factorization by roots, 190
factors with integer coefficients, 202
field containing root of, 115, 189, 222
formal derivative, 83, 196
generally insoluble by radicals if degree is
  at least five, 277
homogeneous, 186, 473
implicit formal derivative, 462
inseparable, 197, 223
irreducible, 113, 222
leading coefficient, 341, 362
monic, 110, 433
non-commuting, 491
number of roots at most the degree, 190
permutated, 176, 376
quadratic, 223
reducible, 113, 222
repeated roots, 197, 223
roots permuted by field automorphism,
  228
separable, 197, 223, 235
separable if irreducible and characteristic
  zero, 199, 223, 239
separable if irreducible and derivative is
  non-zero, 199, 223
separable iff f and f' relatively prime,
  198
solution by radicals, 269, 271
solvable by radicals iff Galois group is
  solvable, 274, 294
splits completely, 194, 223
splitting field, 194, 223
symmetric, 177, 376
with infinitely many roots, 216
with more roots than degree, 192, 215
with zero derivative, 196
polynomial ring, 66, 110
action of permutation is homomorphism,
  177, 185, 376
action of symmetric group, 176, 376
automorphism of, 230
basis as vector space, 325
evaluation homomorphism, 67, 82, 90, 94,
  226, 357, 362, 432
greatest common divisor, 288
homomorphism of, 82
irreducible element of, 118
is a Euclidean domain, 161
is a PID, 112, 161, 222
is a UFD, 159, 165
is infinite-dimensional vector space, 98,
  103, 319, 325
is vector space, 94
multivariate, 176, 376, 470
non-commutative, 491
of infinitely many variables, 185, 338
over a field is Noetherian, 338, 342, 471
over a Noetherian ring is Noetherian, 340,
  342, 432, 471
quotient by irreducible polynomial is
  field, 113, 222
polytope, 487
poset, see partially ordered set
power set, 416
powering algorithm, 502, 522
powers generate unit ideal, 182, 351, 366
p-power map, see Frobenius homomorphism
prime, 19
  defined by a logical expression, 8
  divides product, 19
  ideal, 77
  infinitely many, 19, 32
  power dividing factorial, 33
prime ideal, 77
generated by irreducible element, 164
iff quotient is domain, 78
unique factorization as a product of, 465
Primitive Element Theorem, 239, 245, 258,
  261, 287
primitive root, 193
primitive root of unity, 264
Index

principal ideal, 73, 112, 159
fractional, 466
in polynomial ring, 112, 222
left, 490
right, 490
two-sided, 490
principal ideal domain, 159
$au + bv = \gcd$ theorem, 364
column and row operations, 365
Euclidean domain is, 160, 165
every element is product of irreducibles, 182
$F[x]$ is a, 161
irreducible element, 164
irreducible element divides product, 165
is integrally closed, 434
is Noetherian, 338
matrix with entries in, 342, 344, 365
quotient by irreducible element is field, 164
torsion submodule trivial iff module is free, 366
$\mathbb{Z}$ is a, 161
$\mathbb{Z}[i]$ is a, 161
principal submodule, 331, 358
is principal ideal if $M = R$, 331
private key, 497
PRNG, 504
product
divisible by irreducible, 165
divisible by prime, 19
fiber, 439, 509
inclusion homomorphism, 52
module, 330
of countable sets is countable, 504
of cyclic groups, 367
of groups, 51, 389
of ideals, 88
of infinitely many sets, 28
of matrices, 301, 336, 360
of sets, 11, 418
of sets is non-empty, 418
projection homomorphism, 52
projection map, 12
ring, 71, 87
semidirect, 268, 292, 389, 390
tensor, 422
Zorn’s Lemma, 417
product ring, 71, 87
Chinese Remainder Theorem, 169, 351, 353
unit group, 72, 86
product rule, 196
projection map, 12
projection algebraic set, 474
ideal of, 474
projection line, 472
projection plane, 472
conic in, 474
curve in, 474
line in, 474
lines intersect in a point, 474
projection space, 472
Bezout’s Theorem, 476
covered by affine spaces, 514
field of rational functions of, 473
hyperplane, 474
hypersurface, 474, 475
intersection theory, 474
is disjoint union of affine spaces, 473, 514
local ring at a point, 475, 515
multiplicity at intersection of hypersurfaces, 476
$\mathbb{P}^n$ covered by $n + 1$ copies of $\mathbb{A}^n$, 514
point in, 472
rational function is function on, 473, 514
projective variety, 474
field of rational functions of, 514
meromorphic function, 515
proof, 1
by contradiction, 4, 27
by induction, 16, 17
magic explained, 173
techniques, 3
what is a, 1
pseudo-random number generator, 504
$p$-Sylow subgroup, see Sylow subgroup
$p$th cyclotomic polynomial, 206, 267
public key, 497
public key cryptography, 497
contradictory goals, 499
Diffie–Hellman problem, 499, 520
efficiency versus security, 499
hard problems used for, 498
pseudo-random number, 503
trapdoor function, 497
true random number, 503
public key cryptosystem
Elgamal, 500, 520
GGH, 500, 503
lattice-based, 500, 501, 520
NTRU, 520
public key cryptosystem (continued)
  random number, 503
  RSA, 499, 504
Pythagorean theorem, 162

Q, see field of rational numbers
Q, see quaternion group
Q(√2), 107, 109
Q(i), 107, 109
quadratic extension
  ideal class group, 467
  in cyclotomic field, 292
  ring of integers, 464, 513
  unit group, 469
quadratic formula, 105, 221, 269
quadratic polynomial, 223
quadratic residue, 216
quandle, 55
quantifier, 7
  order is important, 9
quantum computer, 198, 501
quartic formula, 105, 270
quaternion group, 43
  Cayley graph, 510
  character table, 511
  composition series, 395
  inner automorphism, 396
quaternion ring, 67, 83, 108, 121, 192, 216
quintic polynomial generally insoluble by radicals, 277
quotient, 18
quotient group, 132
  simple iff subgroup is maximal normal, 387, 395
quotient map
  of groups, 132
  of modules, 330
  of rings, 74
quotient module, 330, 358
  is module for quotient ring, 331, 358
  kernel of map to, 330, 358
  of Noetherian module is Noetherian, 339
quotient ring, 73
  domain iff by prime ideal, 78
  field iff by maximal ideal, 78
  is field, 113, 164, 222
  is \( R \)-module, 329, 359
  non-commutative, 518
  tensor product with, 424
quotient vector space, 305, 322

\( \mathbb{R} \), see field of real numbers

rabbit-out-of-a-hat proof, 173
radical extension, 270
  contained in Galois extension, 270
  has solvable Galois group, 273
radical of an ideal, 88, 471
radical solution of polynomial, 271
\( R \)-algebra, 431
random number, 503
  pseudo, 503
  true, 503
range, 12
rank
  in exact sequence, 429
  of a matrix, 363
  of a representation, 448
  of a representation is value at \( e \), 455
  of elliptic curve, 463
  of elliptic curve is bounded/unbounded?, 463
  of module, 334, 336, 346
  of unit group of number field, 469
Rank-Nullity Theorem, 304, 366, 429
rational function
  field of, 175, 287
  field of on affine variety, 471
  field of on projective space, 473
  field of on projective variety, 514
  gives function on projective space, 473, 514
  multivariable, 176, 275, 276
rationalizing the denominator, 107
\( R \)-basis, 333
real embedding, 468
real vector space
  discrete subgroup, 477
  discrete subgroup is finitely generated free abelian group, 478, 516
  discrete subgroup of maximal rank, 478
  lattice in, 478
reducible element in a ring, 158
reducible polynomial, 113, 222
reduction mod \( m \), 66
reflection map, 459
reflexive property, 14, 29, 418
regular representation, 449
  character value, 455
  multiplicities of irreducible pieces, 452, 456
  relation to group ring, 498, 518
relatively prime, 18
remainder, 18
representation, 448
1-dimensional, 448
abelian group, 453
cracter, 453
is invariant under conjugation, 454
is not a homomorphism, 454
is sum of roots of unity, 511
of direct sum, 454
value of regular, 455
character is sum of roots of unity, 454
character group, 455
character table, 454
dimension, 448
direct sum, 450
finitely many irreducible, 453
group, 448
homomorphism, 450
identity, 448
inner product of characters, 455
inner product of characters equals
multiplicity, 456
invariant subspace, 450
invariant subspace is left ideal of group
ring, 494, 518
irreducible, 451
isomorphism, 450
Maschke’s Theorem, 452, 511
multiplicity of an irreducible
representation in, 452
multiplicity of irreducible in regular
representation, 452, 456
of cyclic group, 449, 453
of dihedral group, 449, 453, 510
of symmetric group, 448
orthogonality relation for irreducible
characters, 456
over field of characteristic $p$, 512
permutation, 449
projection map to invariant subspace, 511
rank, 448
rank one, 448
regular, 449
Schur’s Lemma, 451
sum of dimensions of irreducible, 453
representation theory, 448
$R/I$, see quotient ring
right coset, see coset
right-exact functor, 443
tensor product is, 443, 510
right ideal, 489
right principal ideal, 490
right-inverse, 87, 319, 322, 325, 489
equals left-inverse, 86, 489, 490
of morphism in a category, 436, 509
right-shift operator, 319, 322, 325
ring, 63
$a, b$ generate $R$ implies $a^n, b^n$ generate
$R$, 182, 351, 366
addition, 63
algebra over $a$, 431
Artinian, 363
associative law, 64
cancellation property, 70
center, 83
characteristic, 75
commutative law, 64
congruence, 73
coordinate ring of affine variety, 471
coset of ideal, 73
distributive law, 64
divisibility, 158
division, 108
element integral over, 433
endomorphism, 87
Euclidean domain, 159
evaluation homomorphism, 67, 81, 226,
357, 362, 432
field, 69, 105
finitely generated algebra over, 362, 432
finitely generated ideal, 337
Gaussian integers, 66
group ring, 493
homomorphism, 65
homomorphism from $\mathbb{Z}$, 68
homomorphism kernel is ideal, 75, 518
ideal, 72
ideal generated by a set, 73, 517
ideal is $R$-module, 329, 358, 359
idempotent element, 84, 494, 518
integers modulo $n$, 65
integral closure, 433
integral domain, 69
integrality criterion, 433
integrrally closed, 433
invariant by group action, 180
irreducible element, 158
isomorphism, 65
kernel of homomorphism, 65
left ideal, 489
left principal ideal, 490
left/right-inverse, 87, 319, 322, 325, 489
local, 89, 184, 515
ring (continued)
  matrix, 68, 83
  maximal ideal, 77
  module, 327
  multiplication, 63
  multiplicatively closed set, 184
  nilpotent element, 84, 184
  nilradical, 89
  Noetherian, 337
  non-commutative, 67, 489
  of additive polynomials, 494
  of elements integral over base ring, 433
  of invariants, 180
  polynomial, 66, 110
  prime ideal, 77
  principal ideal domain, 159
  product, 71, 87, 169
  quaternion, 67, 83, 108, 121, 192, 216
  quotient, 73
  quotient by maximal ideal, 78
  quotient by prime ideal, 78
  quotient is \( R \)-module, 329, 359
  quotient map, 74
  quotient of non-commutative, 518
  radical of an ideal, 88, 471
  reduction modulo \( m \), 66
  right ideal, 489
  right principal ideal, 490
  right-inverse, 489
  subring, 65
  sum and product of integral elements are integral, 433
  two-sided ideal, 489
  two-sided inverse, 489
  two-sided inverses are equal, 86, 489
  two-sided principal ideal, 490
  unipotent element, 84
  unit group, 70, 106, 158, 489
  unit group of product, 72, 86
  unit ideal, 73
  with unique maximal ideal, 89, 184
  zero divisor, 69
  zero ideal, 73
ring of integers, 17, 63
  class number, 466
  cyclotomic field, 464
  Dirichlet Unit Theorem, 469
  fractional ideal, 466
  group of fractional ideals, 466
  ideal class group, 466
  ideal class group is finite, 466
ideal class group of quadratic extension, 467
  is a Euclidean domain, 161
  is a PID, 161
  is a UFD, 20, 165
  of a number field, 464
  of quadratic extension, 464, 513
  torsion subgroup, 467, 513
  unique factorization of ideal, 465
  unit group of quadratic extension, 469
Rivest, Ron, 499
\( R \)-linearly independent, 333
\( R \)-module, see module
\( R \)-multilinear map, see multilinear map
\( R^n \), see module of \( n \)-tuples
root
  inseparable if repeated, 197, 223
  number of bounded by degree, 190
  of polynomial permuted by Galois group, 228
  separable if distinct, 197, 223
  root of unity, see also cyclotomic field
character is sum of, 454, 511
eigenvalue of finite-order linear operator, 324
field generated by, 264
  primitive, 264
  roots modulo \( m \) problem, 498
Rose’s song, 157
Roth, Klaus, 215
row and column reduction, 343, 365
  over a Euclidean domain, 344
  over a field, 343
  over a principal ideal domain, 365
row rank, 363
row span, 363
  has same dimension as column span, 363
RSA cryptosystem, 499
  incorporating randomness, 504
\( R \)-span, 333
ruler and compass construction, 207
Russell’s paradox, 417
\( R[x] \), see polynomial ring
scalar, 93
Schröder–Bernstein Theorem, 415, 504
Schur’s Lemma, 451
semidirect product, 268, 292, 389, 390
affine linear group, 396
  dihedral group is, 392
  group decomposition into, 391
  group law has inverses, 396
semidirect product (continued)
  group law is associative, 390
  is a group, 390
  of cyclic groups, 392, 396
  of order twelve, 396
semigroup, 55
separable, 197, 223
  if irreducible and characteristic zero, 199, 223
  if irreducible and derivative is non-zero, 199, 223
  iff \( f \) and \( f' \) relatively prime, 198
separable field extension, 239, 287
  always in characteristic zero, 238, 239, 242, 287
separable polynomial, 197
  Galois group, 235
  splitting field, 235
set, 9
  Axiom of Choice, 418
  binary relation, 29
  Cantor’s diagonalization method, 415
  cardinality, 415
  complement, 11
  countable, 413, 414
  difference, 11
  disjoint union of, 14
  element of, 9
  empty, 10
  empty set is always subset of, 10
  equivalence relation, 14, 29
  existence of uncountable, 416
  fiber product of, 509
  finite, 10, 414
  group action on, 133
  infinite, 414
  injective function, 414
  intersection, 10
  intersection is fiber product, 509
  is subset of itself, 10
  not an element of, 9
  number of ordered lists of specified size, 23
  number of subsets of specified size, 23
  of all sets, 416
  of functions from \( S \) to \( T \), 415
  of sets, 127, 416–418
  orbit under group action, 134
  partially ordered, 29, 418
  permutation of, 22
  power set of, 416
product is non-empty, 418
product of, 11
product of arbitrarily many, 418
product of countable is countable, 504
projection map on product of, 12
\( \#S = \#T \) iff \( \#S \leq \#T \) and \( \#T \leq \#S \), 415, 504
Schröder–Bernstein Theorem, 415, 504
  set of subsets of, 415, 416
  stabilizer under group action, 134
  subset, 10
  surjective function, 414
  symmetric difference, 27
  symmetric group of, 42, 134
  totally ordered, 10, 418
  uncountable, 413, 414
  unequal cardinality, 415, 506
  union, 10
  well-ordered, 419
set theory, 9, 413
  continuum hypothesis, 504
  Russell’s paradox, 417
  Well-Ordering Theorem, 419
  Zermelo–Frankel axioms, 419
  Zorn’s Lemma, 419
Shamir, Adi, 499
Shanks, Dan, 520
shift operator, 319, 325
Shor, Peter, 198, 501
short exact sequence, 359, 366, 426
  built from long exact sequence, 508
  iff satisfies four conditions, 426
  of quotient modules, 427
  tensor product by \( R/I \), 427
  with product in middle, 426
shortest vector problem, 481
  Gaussian heuristic, 517, 522
  to find NTRU private key, 521
sign, 378, 400
  is determinant of permutation matrix, 394
  is homomorphism, 378
  is surjective, 378
  of a cycle, 379
  of a product of cycles, 379
simple group, 129, 380
  abelian, 380
  alternating group is, 381
  cannot have order \( p^i q^j \), 381
classification of finite, 386
  composition series, 387
simple group \((continued)\)
  of prime power order is cyclic, 380
  sporadic finite, 387
singular linear operator, 296
singular value, see eigenvalue
size function, 159, 344
  on \(F[x]\), 161
  on \(\mathbb{Z}\), 161
  on \(\mathbb{Z}[i]\), 161
\(s_k\), see elementary symmetric polynomial
skew field, 108, 121
\(SL_n\), see special linear group
small category, 436
Smith normal form, 343
  elementary operations to reduce to, 344, 365
\(S_n\), see symmetric group
solubility by radicals, 271
  iff Galois group solvable, 274, 294
solubility versus constructibility, 271
solvable group, 272, 381, 387
  quotient group of, 272, 293
  radical extension Galois group is, 273
\(S_n\) not solvable for \(n \geq 5\), 275, 381
subgroup of, 272, 293
Sondheim, Stephen, 157
span
  notation for, 333
  of elements of a module, 330, 332, 359
  of set of vectors, 96, 318
spanning set
  contains basis, 97, 318
  is larger than linearly independent set, 99
  vector space, 96, 318
special linear group, 57
splits completely, 194, 223
splitting field, 124, 194, 223, 258
  degree, 194, 223
  exists, 194, 223
  Galois group order equals degree, 235
  in characteristic zero always Galois, 238
  in characteristic zero always separable, 287
  is unique, 232
  of \(X^4 - 2\), 233, 244, 248, 287, 288
sporadic finite simple group, 387
square-and-multiply algorithm, 502, 522
square, commutative, 340
square-free integer, 198
square root
  of complex number, 252, 289
  of \(n\) is irrational, 32
  of \(p\) is irrational, 20
square, symmetry of, 38
stabilize, 337
stabilizer, 134
  orbit counting theorem, 136
stabilizer-orbit formula, 135, 261, 374
standard basis, 95
  coordinates in, 95
Stirling’s formula, 480, 517
structure theorem
  finite abelian groups, 52
  finitely generated abelian groups, 353, 485
  finitely generated modules, 346, 350, 463
subcategory, 437
subfield, 108
subgraph, 446
  isomorphism problem, 446
subgroup, 46
  conjugate, 129
  coset of a, 48, 127
  double coset, 148
  generated by element, 47
  index of, 50
  Lagrange’s Theorem, 50
  normal, 129
  number of conjugates, 145
  of index two is normal, 151
  order divides order of group, 50
  product of two, 147
  semidirect product of, 391
  trivial, 47
submodule, 330
  chain stabilizes, 337
  cyclic, 331, 358
  finitely generated, 337
  generated by a set, 330, 332, 359
  kernel is a, 330, 358
  maximal element of collection of, 337
  of Noetherian module is Noetherian, 339
  principal, 331, 358
  torsion, 349, 365, 366, 427, 508
subring, 65, 431
subset, 10
  intersection is fiber product, 509
  set of, 415, 416
subspace of a vector space, 303
  quotient by, 305, 322
sum
  of cubes, 30
  of ideals, 88
sum (continued)
of squares, 17
rule for derivatives, 196
Sun Tzu Suan Ching, 168
surjective, 12, 414
  iff injective, 53
  iff injective for finite same size sets, 13, 29
SVP, see shortest vector problem
swap, 375
  lemma, 98
  rows/columns of a matrix, 343
$S_X$, see symmetric group
Sylow subgroup, 142
  are conjugates, 143, 149
  number of, 143, 149
  of symmetric group, 380
Sylow’s Theorem, 140, 143, 149, 253, 278, 380
symmetric bilinear form, 361, 362
symmetric difference, 27
symmetric form, 399
  map induced by endomorphism, 401, 410
symmetric function field, 275, 276
symmetric group, 42, 134, 371
  action on multivariate polynomial ring, 176, 376
  acts on field of rational functions, 275, 276
  alternating group is normal subgroup of, 379
  alternating subgroup, 379, 400
  automorphism group of, 389
  Cayley’s Theorem, 379
  composition series, 386, 395
  cycle, 373
  disjoint cycles commute, 373, 393
even permutation, 378, 400
every group a subgroup of some, 379
generated by cycle and transposition, 278, 394
is non-abelian, 371
$n$-cycle in $S_n$, 372, 393
normal subgroup of, 381
(not) isomorphic to dihedral group, 58
not solvable for $n$ at least five, 275, 381
odd permutation, 378, 400
order of, 53, 371
permutation is product of disjoint cycles, 374
permutation is product of transpositions, 375, 400
representation of, 448
sign is homomorphism, 378
sign of a permutation, 378, 400
sign of product of cycles, 379
Sylow subgroup of, 380
transitive permutation, 372, 393
transposition, 375
symmetric polynomial, 177, 376
  is polynomial of elementary symmetric polynomials, 179
symmetric rational function, 275, 276
symmetrization of a multilinear form, 410
symmetry property, 14, 29
tangent line, 458
tensor product, 422
  commutative diagram, 423
distributes over direct product, 507
  exists and is unique, 423, 506
extension of scalars, 507, 509
functor is right-exact, 443, 510
functor on the category of modules, 442, 443, 510
  homomorphism space is space of multilinear maps, 507
  is commutative, 507
  of short exact sequence by $R/I$, 427
universal mapping property, 422, 424
  with quotient ring, 424
tensor product functor, 510
covariant, 510
  on modules is right-exact, 510
tensor product functor, 510
covariant, 510
torsion submodule, 349, 365, 366, 427
  exact sequence of, 508
  trivial iff module is free, 366
totally ordered set, 10, 418
trace, 291, 324, 453
  for field extension, 291
  is conjugation invariant, 324
  is linear, 324
  of a linear operator, 324
  of a matrix, 324
  of a representation, 453
Index

trace (continued)
  sum of diagonal entries, 324
  sum of eigenvalues, 324
transcendental number, 187, 215
e, 187
π, 187
uncountably many, 187
transitive
  group action, 136, 152
  permutation, 372, 393
transitive property, 14, 29, 418
transposition, 375
  and cycle generate $S_n$, 278, 394
  parity of number in a product, 376
  permutation is product of, 375, 400
transversal intersection, 476, 477
trapdoor function, 497
trisection problem, 208
trivial invariant subspace, 451
truth table, 3, 6
truth value, 3
two-sided ideal, 489
two-sided inverse, 489
two-sided principal ideal, 490
two-sided unit, 86, 296

UFD, see unique factorization domain
uncountable set, 413, 414
  Cantor’s diagonalization method, 415
  existence of, 416
  $\mathbb{R}$ is, 504
undirected graph, 444
unequal cardinality, 415, 506
union, 10
  complement of, 27
  disjoint, 14
  of infinitely many sets, 28
unipotent, 84
unique factorization domain, 158
  Euclidean domain is a, 165
  $F[x]$ is a, 165
  is integrally closed, 434
  PID is a, 165
  polynomial ring is, 159
  ring that is not a, 167
  $\mathbb{Z}$ is a, 20, 165
  $\mathbb{Z}[i]$ is a, 165
unit, 70, 106, 158
  in endomorphism ring, 490
  two-sided, 86, 296
  unit group, 70, 106, 158, 489
  Gaussian integers, 70
  in exact sequence with ideal class group, 514
  of a number field, 467
  of quadratic extension, 469
  of $\mathbb{Z}/m\mathbb{Z}$, 70
  product ring, 72, 86
  unit ideal, 73
  generated by powers, 182, 351, 366
Unit Theorem of Dirichlet, 469
universal mapping property
  fiber product, 439
  fiber product of sets, 509
tensor product, 422, 424
unordered pair, 443
upper bound of a chain, 419

variety, 470, 471, 474
  algebraic set is union of, 471
vector, 93
  coordinates for standard basis, 95
  linear combination of, 95
  zero, 93
vector space, 93
  alternating $n$-form, 311, 323
  associative law, 93
  bases all have same size, 98, 336
  basis, 95
  basis iff $\delta(v_1, \ldots, v_n) \neq 0$, 312
  basis iff spans and linearly independent, 96, 318
  basis iff spans iff linearly independent, 102
  basis of eigenvectors, 307, 322, 354
  column span of a matrix, 363
  commuting matrices, 368
  contains basis, 98, 421, 506
  determinant non-zero, 314
  determinant of linear operator, 313
diagonalizable linear operator, 307, 322, 354
dimension of, 98
dimension one, 310
  direct product of infinitely many, 319, 325
direct sum of infinitely many, 320, 325
discrete subgroup in $\mathbb{R}^n$, 477
discrete subgroup is finitely generated free
  abelian group, 478, 516
discrete subgroup of maximal rank, 478
distributive laws, 93
eigenvalue, 306
eigenvector, 306
vector space (continued)
eigenvector exists over algebraically closed field, 308, 451
endomorphism ring, 101, 296, 320
extension of scalars, 507
general linear group, 296, 448
Hom, 295
homomorphism, 93, 295
identity law, 93
image is subspace, 322
infinite-dimensional, 98, 318, 325
invertible linear operator, 296
is module over field, 329
isomorphic to space of \( n \)-tuples, 102
Jordan normal form of linear operator, 354, 355
kernel is subspace, 322
lattice in \( \mathbb{R}^n \), 478
linear combination of vectors, 95
linear operator, 101, 296, 320
linear operator on finite-dimensional, 305
linear operator on infinite-dimensional, 325
linear transformation, 93, 295
linearly independent set, 96, 318
of \( n \)-tuples, 94
of polynomials, 94
quotient, 305, 322
rank of discrete subgroup is at most rank of, 516
Rank-Nullity Theorem, 304, 366, 429
row span of a matrix, 363
scalar, 93
shift operator, 319, 325
singular linear operator, 296
span of set of vectors, 96, 318
spanning set, 96, 318
standard basis of \( F^n \), 95
subspace, 303
Swap Lemma, 98

Venn diagram, 25
vertex, 443
volume
doubling volume of cube, 208
of a ball in \( \mathbb{R}^n \), 517
of a lattice, 478, 486, 516
Voronoi cell, 486
boundary is contained in hyperplanes, 487
boundary is polyhedron, 487
is fundamental domain, 487

Wedderburn’s Theorem, 108
Weil, André, 462, 464
well-ordering principle, 11, 16, 18
Well-Ordering Theorem, 417, 419
Wiles, Andrew, 280
Wilson’s formula, 121
wizzle, 9

xkcd, xvii, 7, 66

\( \mathbb{Z} \), see ring of integers
Zermelo–Fraenkel axioms, 419
zero divisor, 69
zero ideal, 73
zero vector, 93
\( \mathbb{Z}(G) \), see center of a group
\( \mathbb{Z}_G(H) \), see centralizer of a subgroup
\( \mathbb{Z}[i] \), see Gaussian integers
\( \mathbb{Z} \)-module, 328
is abelian group, 328
need not have a basis, 333
\( \mathbb{Z}/m\mathbb{Z} \), see integers modulo \( m \)
Zorn’s Lemma, 417, 419
existence of maximal ideal, 506
existence of vector space basis, 421, 506
implies the Axiom of Choice, 419
\( \mathbb{Z}[x] \)-module, 333, 359
Zyglx theory, 1