Index

A-construction, 103
acoustic
– power, 383
– pressure, 384
action
– faithful, 669
– finite, 34
– fixed point, 59, 171
– graph, 670
– induced, 688
– kernel, 207
– kernel of, 33
– lattice, 625
– left regular, 38
– of a group, 33
– orbit, 33
– poset, 625
– restriction, 38
– right regular, 38
– similar, 174, 666
– stabilizer, 170
– transitive, 38
– trivial, 54
additive representation
– Galois field, 204
affine
– $q$-polynomial, 198
– multiple, 198
– transformations, 245
affine geometry, 355
galois, 215
algebraic, 159
algebraic closure, 159, 229, 237
algebraically closed, 159
algorithm
– Berlekamp, 192
– Chien search, 395
– construct a normal element, 559
– CRC-decoding, 402
– decoding of errors and erasures with a BCH-code, 396
– Dixon–Wilf, 527
– Euclidean, 145, 147
– Extended Euclidean, 393
– Forney, 395
– generate a normal element, 558
– lattice point enumeration, 601
– $L^3$, 588
– LLL, 588
– minimum distance, 70–77, 605
– orbits on points, 673
– orbits on subsets, 709
– order of a group element, 199
– orderly generation, 691
– orderly generation by canonical augmentation, 693
– pre-Lyndon, 187
– primitive element of $\mathbb{F}_q$, 200
– sift, 724
– Zassenhaus, 196
aliasing, 380
alphabet, 11, 178, 179
annihilator, 219, 223
– left, 219
– right, 218
anti-isomorphism
– of lattices, 161
– order-, 161
antichain, 627
generation, 102, 126
– ideal, 329
– mapping, 322
automorphism
– group, 626
– doubly transitive, 251
– of a blocking set, 637
– of extension set, 708
– projective, 641
B-construction, 103
backtracking algorithm, 564
band limited signal, 376
barcode, 9
base $b$ representation, 22
base of a group, 717
basic orbit, 718
basis, 566
- $\delta$-reduced, 591
- Korkine–Zolotarev-reduced, 587, 596
- LLL-reduced, 588, 591
- Minkowski-reduced, 586
BCH
- -bound, 238
- -code, 239
Berlekamp algorithm, 192
Bézout’s Identity, 145, 147
binary code, 20
binomial
- formula, 154
- theorem, 154
binomial tree, 683
Blichfeldt, 585, 587
- lemma of, 582
block, 305
- code, 7, 36
- length, 12
blocking set, 622
blow up, 108
Book
- Red, 423
- Yellow, 435
Boolean function, 119
Bose–distance, 241
bound
- BCH-, 238
- Gilbert-, 90
- Griesmer-, 89
- Hamming-, 82
- Plotkin-, 85
- Reiger-, 403
- Singleton-, 82
- Square-Root-, 262
- Varshamov-, 91
bounds, 82–93
breadth first search, 684
Brouwer, 70
burst error, 401
- correcting efficiency, 404
- location, 401
- pattern, 401
- wrap around, 401
Butterworth filter, 382
canonical
- actions, 34, 35
- basis of $\mathbb{F}^G$, 214
- form of a critical code, 522
- generators, 482
- labelings of field elements, 203
- projection, 301
- representative, 145, 148, 222
- transversal, 179, 690
cardinal sine function, 377
Cauchy–Frobenius
- Lemma, 171
- weighted form, 454
Cayley-graph, 725
CD-ROM, 435
center, 206, 458
centralizer, 181
centrally-primitive, 283
channel, 3
- symmetric, 4
character
- modular, 54
- of finite action, 54
- of representation, 54
- one-dimensional, 54
- ordinary, 54
characteristic, 139
- polynomial, 481
check
- bits, 65
- matrix, 20
- polynomial, 221
- symbols, 227
Chien search, 395
Chinese Remainder Theorem, 190, 192, 202
Cholesky decomposition, 576
CIRC, 412
classification, metric, 445
CLV, 424
code, 5
  - A-construction, 103
  - Alternant-, 285
  - BCH-, 75, 239
  - in the narrow sense, 239
  - primitive, 239
  - B-construction, 103
  - binary, 20
  - Golay-, 106, 264
  - block, 36
  - block length, 12
  - concatenated
  - diagonally, 98
  - critical, 511, 512
  - cyclic, 215
  - annihilator, 223
  - indecomposable, 304
  - root, 233
  - variety, 233
  - decomposable, 463
  - defect, 90
  - dimension, 12
  - dual, 21
  - EAN, 8
  - equidistant, 87
  - generator matrix, 696
  - Golay-, 264, 343, 527, 606
  - binary, 77, 106, 264
  - ternary, 264, 606
  - Goppa-, 287
  - MDS-, 282
  - group algebra, 213, 215
  - Hamming-, 23, 83, 126, 452, 525, 698
  - extended, 95
  - hexacode, 132
  - homomorphism, 511
  - indecomposable, 464, 511
  - critical, 511
  - injective, 452
  - inner, 407
  - ISBN-, 5, 7
  - isometric, 29
  - linearly, 30, 444
  - permutationally, 30
  - semilinearly, 49
  - isometry classes, 741
  - isomorphism, 512
  - ISSN-, 8
  - length, 12
  - linear, 7, 12
  - linearly isometric, 444
  - MDS-, 82, 128–135
  - trivial, 82
  - minimum weight, 15
  - (n,k)-, 12
  - (n,k,d)-, 16
  - (n,k,d,q)-, 16
  - nonredundant, 448
  - optimal, 81
  - orderly generation, 688–698
  - outer, 407
  - parity check, 21, 27
  - perfect, 83
  - projective, 28, 452, 515
  - punctured, 96
  - QR-, 257
  - quadratic-residue-, 257
  - quaternary, 20
  - r-divisible, 60
  - reduced, 452, 515
  - Reed–Muller, 526
  - binary, 123
  - Reed–Muller-, 120
  - Reed–Solomon-, 239
  - repetition, 5
  - restricted, 108
  - self-dual, 21
  - self-orthogonal, 21
  - semi-simple, 308
  - simplex-, 83, 126, 452, 619
  - spectrum, 524
  - stabilizer type of a, 642
  - ternary, 20
  - Golay-, 264
  - t-error-correcting, 16
- t-error-detecting, 16
- type of, 16
- (u | u + v)-construction, 100, 122
- (u, v)-construction, 98
- (u + w | v + w | u + v + w)-constr., 105
- visible, 313
- X-construction, 104
- Y1-construction, 103
- codevector, 12
- codeword, 4, 12
- colexicographical order, 178
- collineation, 206
- column
  - code, 407
  - critical, 515
  - decoder, 407
- communication system, 3
- compact disc read only memory, 435
- companion matrix, 327, 480
- comparable, 161
- composition series, 298, 304
  - length, 299
- concatenated code, 98
- conjugacy class, 181
- conjugates, 168
- conjugation, 181
- construction
  - A-, 103
  - B-, 103
  - (u | u + v)-, 100, 122
  - (u, v)-, 98
  - (u + w | v + w | u + v + w), 105
  - X-, 104
  - Y1-, 103
- content, 451, 455, 457, 460
- convergence
  - in energy, 371
  - mean, 371
  - mean quadratic, 371
  - pointwise, 371
  - uniform, 371
- convolution, 214
- coset leader, 23
  - algorithm, 20
- covering
  - polynomial, 344
  - radius, 90
- critical
  - code, 511, 512
  - column, 515
- cross
  - interleaved Reed–Solomon-codes, 412
  - interleaving, 412
- cross section, 550
- cycle
  - index, 455
  - of the symmetric group, 498
  - PGLk(q), 493
  - Sn, 498
  - type, 454
  - of n, 477
- cyclic
  - code, 215
  - module, 293
  - vector space, 293
- cyclotomic coset, 231
- decoder
  - column, 407
  - Kasami-, 344
- decoding, 4
  - CRC, 402
  - cyclic redundancy check, 402
  - inner, 407
  - outer, 407
  - permutation-, 341
  - row, 407
  - with error-correcting pairs, 346
- decoding tree, 354
- Decomposition Theorem, 467
- Dedekind number, 178
- defect, 90
- degree
  - formulae, 147
  - of a multinomial, 120
  - of a polynomial, 140
  - of nilpotency, 329
- delta function, 166
- depth first search, 683
Index

derivative, 188
design, 366, 624
designed distance, 239
determinant, 574
DFT, 273
digital sum, 432
digraph, 670
dimension
  – maximal, 82
  – of representation, 53
Diophantine linear equations, 563
direct sum of modules, 294
directed graph, 670
Discrete Fourier
  – Transform, 56, 63, 273, 375
discrete subgroup, 566
discriminant, 555
distance
  – minimum, 6, 14
dither, 387
division
  – ring, 235
  – shift register, 336
  – theorem, 145, 147
Dixon–Wilf-algorithm, 527
down-and-up process, 703, 714
downstep, 703
dual group, 634
EAN-code, 8
EFM, 431
eight-to-fourteen modulation, 431
elementary symmetric polynomial, 60
empty word, 179
encoder, 11
encoding, 4
  – systematic, 65
enumeration, weighted, 454
equidistant code, 87
equivalence relation, 29
equivalent representations, 53
erasure, 389
  – location polynomial, 391
error
  – bits, 351
  – concealment, 407
  – correcting
    – – pair, 348
  – evaluation polynomial, 391
  – location polynomial, 391
  – random, 389, 401
  – trapping, 342
  – vector, 15, 351
error-correction rate, 6
Euclidean Algorithm
  – Extended, 393
  – for polynomials, 147
  – number theoretic version, 145
Euler function, 177
evaluation map, 141
exponent
  – of a group, 63
  – of a polynomial, 486
extension, 701
F1-frame, 439
F2-frame, 439
F3-frame, 439
factor
  – action, 39
  – module, 293
family
  – decomposable, 464
  – indecomposable, 464
  – independent, 464
Fano-plane, 621
field
  – algebraically closed, 159
  – extension, 140
    – algebraic, 159
    – finite, 140
  – multiplicative group, 149
  – splitting, 157
filter, 381
  – Butterworth-, 382
  – ideal low-pass, 381
  – realizable, 382
finite field cf. Galois field, 139
finite group action, 34
fixed
- field, 167
- point, 59, 171
formal sum, 214
formula, binomial, 154
Fourier
- coefficients, 373
- matrix, 273
- series, 373
- Transform, 273, 375
  -- Discrete, 56, 63, 375
  -- Inverse, 376
- vector, 273
f-reducing polynomial, 190
Frobenius
- automorphism, 155, 229
  -- over $\mathbb{F}_p$, 155
  -- over $\mathbb{F}_q$, 155
- mapping, 154
full monomial group, 35
fundamental parallelootope, 574
fusion
- element, 709
- node, 709
Galois
- field, 154
  -- additive representation, 204
  -- multiplicative representation, 203
- group, 167
Gauss, 576, 586
- Criterion, 255
general
- linear group, 18, 53
- semilinear group, 208
general position, 668
generating
- function, 455, 456
  -- ordinary, 456
- unit, 269, 283
generator
- idempotent, 268
- matrix, 12
  -- decomposable, 464
  -- indecomposable, 464
  -- systematic, 65
- polynomial, 221
generators of a group, 670
group
  -- action, 33
    -- finite, 34
  -- affine linear group, 245
  -- algebra, 214
    -- code, 215
    -- codes, 213
  -- base, 678, 717
    -- base and strong generating set, 717–727
  -- dual, 634
    -- exponent, 63
    -- extension, 704
  -- general linear, 18, 53
  -- general semilinear, 208
Golay-code, 264, 343, 527, 606
- binary, 106, 264
- ternary, 264, 606
Goppa
- code, 287
- MDS-code, 282
- polynomial, 287
G-orbit, 33
Gram–Schmidt
- coefficient, 578
- orthogonalization, 577
- vector, 578
Gram-matrix, 579
granulation noise, 387
graph
- action, 670
  -- Cayley-, 725
  -- connected component, 670
  -- directed, 670
  -- loop, 670
greatest common divisor, 145, 147
group
  -- action, 33
  -- finite, 34
  -- affine linear group, 245
  -- algebra, 214
  -- code, 215
  -- codes, 213
  -- base, 678, 717
  -- base and strong generating set, 717–727
  -- dual, 634
  -- exponent, 63
  -- extension, 704
  -- general linear, 18, 53
  -- general semilinear, 208
Gleason and Prange Theorem, 262
geometry
- affine, 355
- projective, 206
geometry, projective, 206
Goppa–code, 287
G–orbit, 33
Gram–Schmidt
- generators, 670
- of linear isometries, 32
- of Rubik’s cube, 719
- of semilinear isometries, 49
- projective linear, 727–738
- projective semilinear, 738–741
- projective special linear group, 260
- rank function, 724
- stabilizer chain, 717
- strong generators, 681, 718
- symmetric, 30, 725

Hadamard inequality, 580
Hamming
- code, 23, 83, 126, 452, 525
- distance, 6, 13
- metric, 13
- space, 13
- weight, 15
hereditary condition, 689
Hermite, 576, 580, 585, 586
- constant, 585
hexacode, 132
homogeneous coordinates, 266
homomorphism theorem, 163
hyper companion matrix, 480
hyperplane, 616
ideal, 141, 215
- indecomposable, 304
- maximal, 304
- minimal, 304
- relatively prime, 191
- two-sided, 215
ideal low-pass filter, 381
idempotent, 282
- central, 282
- centrally-primitive, 283
- generator, 268
- orthogonal, 283
- primitive, 283
identity
- representation, 54
Identity of Bézout, 145, 147
incidence matrix, 623
incomparable, 161
indecomposability, 469
induced
- action, 688
- permutation, 33
- permutation group, 33
infimum, 161
- of two subgroups, 172
information
- place, 65
- rate, 6
- set, 65
- symbols, 227
injective code, 452
inner
- code, 407
- decoding, 407
integral
- domain, 140
- element, 485, 488
integral domain, 301
interleaving, 404
- cross, 412
- with delay, 413
invariant, 59
Inverse Fourier Transform, 376
inversion formula
- Fourier, 376
- general, 166
- M"{o}bius, 166
ISBN-code, 5, 7
isometric
- code, 29
- linearly, 30
- permutationally, 30
- semilinearly, 49
isometry, 29
- linear, 30
- -- global, 549
- -- local, 549
- local, 549
- permutational, 30
- semilinear, 45
- -- global, 549
isomorphic normal series, 297
isomorphism
  – lattice, 161
  – order-, 161
Isomorphism Theorem
  – First
    – for modules, 295
    – for rings, 296
  – Second
    – for modules, 296
    – for rings, 296
ISSN-code, 8
Jacobi normal form, 480
Jennings
  – basis, 312, 328
  – weight, 328
kernel, 163
  – of action, 33
knapsack problem, 564, 593
Korkine, 576, 587
Krawtchouk polynomial, 64
Lagarias, 568, 587
Lagarias-Odlyzko lattice, 568
Lagrange, 576, 586
  – Theorem, 38
λ-way interleave, 405
land, 430
lattice, 161, 566
  – action, 625
  – anti-isomorphism, 161
  – basis, 566
    – reduction, 586, 587
  – determinant, 574
  – dual, 599
  – generator matrix, 566
  – isomorphism, 161
  – Lagarias-Odlyzko, 568
  – linear, 625
  – low-density, 593
  – of subgroups, 172, 675
  – rank, 566
  – successive minima, 575
lattice point enumeration, 601
leading coefficient
  – of a polynomial, 141
  – of a vector, 677
least length, 82
left
  – annihilator, 219
  – coset, 38
  – module, 292
Legendre, 576
  – symbol, 255
Lehmann’s Lemma, 448
  – generalized, 535
Leiterspiel, 700
lemma
  – Cauchy–Frobenius, 171
    – weighted form, 454
  – Euler’s, 255
  – Lehmann’s, 448
    – generalized, 535
length, least, 82
Lenstra, 587
lexicographical order, 178, 682–688
linear
  – code, 7
    – combination
      – irreducible, 464
      – reducible, 464
    – group
      – projective, 260
      – special, 260
    – isometry, 30, 444
      – group, 444
      – local, 549
    – lattice, 625
    – representation, 53
linearized polynomial, 197
linearly isometric, 30
L3-algorithm, 588
LLL-algorithm, 588
LLL-reduced, 588
local
  – isometry, 549
  – linear isometry, 549
Index

- semilinear isometry, 549
- locally finite, 629
- Lovász, 587
- lower bound, 161
- Lyndon
  - decomposition, 180
  - length, 180
  - set, 179
  - theorem of, 180
  - word, 179
- MacWilliams-identity, 58
- majority logic decoding, 350–366
- matrix
  - generator, 566
  - Gram, 574, 579, 590
  - Möbius, 173, 628
  - Plesken, 630
  - projective, 452
  - representation, 53
  - unimodular, 574
  - zeta, 173, 628
- Mattson–Solomon polynomial, 273
- maximal
  - dimension, 82
  - minimum distance, 82
  - module, 294
- maximum weight, 102
- maximum-likelihood-decoding, 15
- MDS-code, 128–135
  - trivial, 128
- merging bits, 432
- message, 4
- metric classification, 445
- minihyper, 620
- minimal
  - polynomial, 142, 143, 481
    - of a matrix, 478
    - of a vector, 478
- minimum
  - distance, 6, 14, 605
    - maximal, 82
    - relative, 6, 326
  - weight, 15
- Minkowski, 567, 575, 576, 582, 584–586
  - fundamental theorem of, 582
  - second theorem of, 585
- minterm, 120
- modular
  - character, 54
  - representation, 54
- module
  - cyclic, 293
  - factor, 293
  - finitely generated, 293
  - isomorphic, 294
  - left, 292
    - maximal, 294
  - natural projection, 294
  - right, 293
  - semi-simple, 307
  - simple, 294
- modules, direct sum, 294
- Möbius
  - function
    - general, 166
    - number theoretic, 162, 165
  - inversion, 163
    - general, 166
    - number theoretic, 165
  - matrix, 173, 628
- multibase representation, 722
- multiplicative representation
  - Galois field, 203
- multiset, 618
- necklace, 179
- $n$-fold
  - product, 63
  - sum, 62
  - $(n,k)$-code, 12
  - $(n,k,d)$-code, 16
  - $(n,k,d,q)$-code, 16
- nonredundant
  - code, 448
  - subspace, 452
- nonsquare modulo $n$, 253
- normal
  - basis, 169
- element, 555
- form, 480, 663
- in $GL_k(q)$, 478
- Jacobi, 480
- of endomorphism, 478
- series, 297
- factors, 297
- isomorphic, 297
- subgroup, 69, 181
- normalizer, 181
- number, Dedekind, 178
- Nyquist
  - frequency, 380
  - rate, 380
- Odlyzko, 568
- optimal code, 81
- orbit, 33, 669
  - basic-, 718
  - computing, 700–716
  - data structure, 675
  - of type $U$, 172
  - representatives, 689
  - Schreier-tree, 672
- order
  - anti-isomorphism, 161
  - colexicographical, 178
  - isomorphism, 161
  - lexicographical, 178
  - of a formal series, 456
  - of a group, 149
  - of a group element, 149
  - of a polynomial, 486
- order tree, 682
- orderly generation, 688–698
- ordinary
  - character, 54
  - representation, 54
- orthogonal, 577
  - projection, 578
- orthogonality
  - defect, 580
  - relation, 63
- orthogonality defect, 593
- outer
  - code, 407
  - decoding, 407
  - direct sum, 97
- Pólya, 455
- packing radius, 14
- parallelootope, fundamental, 574
- parity
  - check bit, 21
  - extension, 95
- partial
  - order, 161
  - syndrome, 391
- polynomial, 391
- partially ordered set, 161
- partition of a set, 34
- PCM, 385
- PD-set, 342
- perfect code, 83
- period of a polynomial, 486
- permutation
  - decoding, 342
  - group
  - induced, 33
  - induced, 33
  - representation, 33
- permutational isometry, 30
- permutationally isometric, 30
- pit, 430
- Plesken matrix, 630
- Plotkin construction, 100
- point, 617
- pointwise stabilizer, 207, 717
- polynomial
  - affine $q$, 198
  - check, 221
  - covering, 344
  - degree, 140
  - divisor, 141
  - elementary symmetric, 60
  - exponent, 486
  - $f$-reducing, 190
  - generating, 51
- generator, 221
- irreducible, 141
- Krawtchouk, 64
- leading coefficient, 141
- linearized, 197
- Mattson–Solomon, 273
- minimal, 142, 143
- monic, 141
- order, 486
- period, 486
- primitive, 152
- \( q \)-, 197
- reciprocal, 224
- reducible, 141
- root of, 141
- splitting field, 157
- subexponent, 488
- symmetric, 60
- -- elementary, 60
poset, 161
- action, 625
- automorphism, 626
- interval, 161
- locally finite, 161
power set, 682
pre-Lyndon
- algorithm, 187
- word, 179
pre-order traversal, 683
primary
- components, 479
- decomposition, 479
prime field, 140
primitive
- element, 152
- polynomial, 152
principal
- ideal, 149
- -- domain, 141, 301
projection, 512
- orthogonal, 578
projective
- automorphism, 641
- code, 28
- dimension, 206
- geometry, 206, 617
- hyperplane, 206
- line, 206, 259
- linear group, 207, 260, 458, 476, 681, 727–738
- matrix, 452
- plane, 206
- point, 206
- semilinear group, 209, 738–741
- space, 205, 450, 676
- standard vector, 677
projective code, 452, 515
prolongation, 102
pulse code modulation, 385
punctured
- code, 96
- space, 205
puncturing, 126
\( q \)-binomial numbers, 460
\( q \)-polynomial, 197
- affine, 198
quadratic
- form, 576
- residue, 253
Quadratic Reciprocity, 256
quantization, 384
quasicanonical form of a critical code, 519
quaternary code, 20
radius, covering, 90
random error, 389, 401
rank, 566
rank function
- for \( \mathbb{F}_q^k \), 677
- for group elements, 724
- for subsets, 685
- projective geometry, 728
\( r \)-divisible code, 60
realizable filter, 382
recoupling polynomial, 336
Red Book, 423
reduced code, 452, 515
redundancy
– places, 65
– set, 65
Reed–Muller-code, 120, 526
– canonical generator matrix, 125
Reed–Solomon-code, 438
refinement, 297
Reiger-bound, 403
repeated
– doubling and adding, 183
– squaring and multiplying, 183
representation
– character of, 54
– dimension of, 53
– linear, 53
– modular, 54
– ordinary, 54
– space, 53
– trivial, 54
representative, canonical, 222
residue class, 145, 252
– ring, 140
– modulo n, 146
restriction
– of a code, 108
– of an action, 38
reversed sequence, 723
right
– annihilator, 218
– coset, 38
– module, 293
ring
– associate elements, 301
– divisor, 301
– free of zero divisors, 144
– irreducible element, 301
– prime element, 301
– relatively prime elements, 301
– semi-simple, 307
– unit, 301
R-linear closure, 293
R-module homomorphism, 294
– kernel, 294
root, 141
– multiple, 141
– multiplicity, 141
– of unity, 229
– simple, 141
row
– code, 407
– decoding, 407
RSPC, 438
Rubik’s cube, 719
sampling, 370, 378
– frequency, 378
– rate, 378
Schnorr, 587, 596
Schreier
– generator, 673
– tree, 672
scrambling, 439
sector, 436
– address bytes, 436
– ECC, 437
– EDC, 437
– header field, 436
– mode byte, 436
– Mode 0, 436
– Mode 1, 437
– Mode 2, 437
– RSPC, 437
– scrambled, 439
– synchronization word, 436
Seeber, 586
self
– dual code, 21
– orthogonal code, 21
semidirect sum, 100
semilinear
– isometries, group of, 49
– isometry, 45, 49
– classes, 49
– local, 549
– mapping, 45
semilinearly isometric, 49
set partition, 34
shortening, 101
sift algorithm, 724
Index

signal-to
  – error ratio, 385
  – noise ratio, 385
similar actions, 174
simple module, 294
simplex-code, 83, 126, 452, 619
Sims chain, 717
Slepian, 663
snakes and ladders, 700
sound
  – intensity, 384
  – power, 383
  – pressure, 384
space
  – projective, 205
  – punctured, 205
special linear group, 260
spectrum, 524
sphere, 584
splitting field, 157
square modulo $n$, 253
stabilizer, 170, 669
  – chain, 717
  – pointwise, 207, 688, 717
  – setwise, 688
stabilizer type, 642
standard bilinear form, 21
strong generators, 681, 718
subcode, 104, 434
  – bits, 434
  – block, 434
subcycle, 485
  – expression, 486
  – index, 486
  – index, 492
  – length, 486
  – type, 486
subdeterminant, 590
subexponent of a polynomial, 488
subgroups, lattice of, 172
submodule, 293
subset sum problem, 564
subspace, nonredundant, 452
successive minima, 575
sum
  – outer direct, 97
  – semidirect, 100
summable family, 456
support, 61, 371, 511
supremum, 161
  – of two subgroups, 172
switching function, 119
symbol
  – check, 227
  – information, 227
  – Legendre, 255
symmetric
  – channel, 4
  – difference, 61
  – group, 30
  – cycle index, 498
  – polynomial, 60
syndrome, 24
  – decoding, 24
$\tau$-order, 558
tensor, 114
  – product, 108, 114
ternary code, 20
theorem
  – binomial, 154
  – First Isomorphism-
    – for modules, 295
    – for rings, 296
  – homomorphism, 163
  – Lyndon’s, 180
  – of Berman, 318
  – of Gleason and Prange, 262
  – of Lagrange, 38
  – of Pólya, 455
  – Second Isomorphism-
    – for modules, 296
    – for rings, 296
  – Structure of cyclic codes, 305
topological sorting, 628
total order, 161
totally ordered set, 161
trace function, 555
transfer function, 381
transitive, 38, 245
transporter
– element, 669, 689, 709
– map, 675
transversal, 33, 689
– canonical, 690, 709
trap decoding, 342
tree
– binomial tree, 683
– breadth first search, 684
– depth first search, 683
– distance from root, 683
– fusion node, 709
– level, 683
– order tree, 682
– pre-order traversal, 683
– root, 683
– Schreier, 672
– spanning, 672
trigonometric polynomial, 372
trivial
– action, 54
– representation, 54
two-sided ideal, 215
type
– of a code, 16
– of an orbit, 172
unimodular, 574
uniqueness of finite fields, 149
unit
– generating, 269, 283
– sphere, 584
upper bound, 161
upstep, 703
\((u \mid u + v)\)-construction, 100, 122
\((u, v)\)-construction, 98
\((u + w \mid v + w \mid u + v + w)\)-constr., 105
Vandermonde matrix, 134
variety, 229, 237
– consecutive, 238
– irreducible, 237
vector, 565
– \(\ell_q\)-shortest, 567
– column, 565
– directly connected with itself, 465
– space, cyclic, 293
vectors
– connected, 465
– directly connected, 465
– orthogonal, 577
– proportional, 550
visible, 313
volume of a set, 574
weight, 15
– enumerator, 52, 757
– function, 56, 453
– general, 455
– multiplicative, 454
weighted enumeration, 454
word, 4, 178
– concatenation, 179
– empty, 179
– length, 179
– Lyndon, 179
– prefix, 179
– suffix, 179
wrap around burst, 401
wreath product, 34
– generalized, 533
X-construction, 104
Y1-construction, 103
Yellow Book, 435
Zassenhaus algorithm, 196
Zech logarithm, 203
zeta
– function
– general, 165
– number theoretic, 162
– matrix, 173, 628
Zolotarev, 576, 587