

Bibliography

Groups and Fields

Alperin, J. L.; Bell, Rowen B. *Groups and representations*. Graduate Texts in Mathematics, 162. Springer-Verlag, New York, 1995.

Artin, Michael *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

Dummit, David S.; Foote, Richard M. *Abstract algebra*. Third edition. John Wiley and Sons, Inc., Hoboken, NJ, 2004.

Herstein, I. N. *Abstract algebra*. Third edition. With a preface by Barbara Cortzen and David J. Winter. Prentice Hall, Inc., Upper Saddle River, NJ, 1996.

Humphreys, John F. *A course in group theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1996.

Rotman, Joseph J. *An introduction to the theory of groups*. Fourth edition. Graduate Texts in Mathematics, 148. Springer-Verlag, New York, 1995.

van der Waerden, B. L. *Modern Algebra. Vol. I*. Translated from the second revised German edition by Fred Blum. With revisions and additions by the author. Frederick Ungar Publishing Co., New York, N. Y., 1949.

Matrix Theory

Gantmacher, F. R. *The theory of matrices. Vol. I*. Translated from the Russian by K. A. Hirsch. Reprint of the 1959 translation. AMS Chelsea Publishing, Providence, RI, 1998.

Herstein, I. N.; Winter, David J. *Matrix theory and linear algebra*. Macmillan Publishing Company, New York; Collier Macmillan Publishers, London, 1988.

Strang, Gilbert *Linear algebra and its applications*. Second edition. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1980.

Determinants

Lang, Serge *Linear algebra*. Reprint of the third edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1989.

Muir, Thomas *A treatise on the theory of determinants*. Revised and enlarged by William H. Metzler Dover Publications, Inc., New York 1960.

Shilov, Georgi E. *Linear algebra*. Revised English edition. Translated from the Russian and edited by Richard A. Silverman. Dover Publications, Inc., New York, 1977.

Turnbull, H. W. *The theory of determinants, matrices, and invariants*. 3rd ed. Dover Publications, Inc., New York 1960.

Vector Spaces

Artin, Michael *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

Birkhoff, Garrett; MacLane, Saunders *A Survey of Modern Algebra*. Macmillan Company, New York, 1941.

Halmos, Paul R. *Finite-dimensional vector spaces*. Reprinting of the 1958 second edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1974.

Hoffman, Kenneth; Kunze, Ray *Linear algebra*. Second edition Prentice-Hall, Inc., Englewood Cliffs, N.J. 1971.

Lang, Serge *Linear algebra*. Reprint of the third edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1989.

Samelson, Hans *An introduction to linear algebra*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley and Sons], New York-London-Sydney, 1974.

Herstein, I. N.; Winter, David J. *Matrix theory and linear algebra*. Macmillan Publishing Company, New York; Collier Macmillan Publishers, London, 1988.

Linear Transformations

Coxeter, H. S. M. *Introduction to geometry*. Reprint of the 1969 edition. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1989.

Gelfand, I. M. *Lectures on linear algebra*. With the collaboration of Z. Ya. Shapiro. Translated from the second Russian edition by A. Shenitzer. Reprint of the 1961 translation. Dover Books on Advanced Mathematics. Dover Publications, Inc., New York, 1989.

Herstein, I. N.; Winter, David J. *Matrix theory and linear algebra*. Macmillan Publishing Company, New York; Collier Macmillan Publishers, London, 1988.

Weyl, H. *Symmetry*. Reprint of the 1952 original. Princeton Science Library. Princeton University Press, Princeton, NJ, 1989.

Eigentheory

Lax, Peter D. *Linear algebra*. Pure and Applied Mathematics (New York). A Wiley-Interscience Publication. John Wiley and Sons, Inc., New York, 1997.

Strang, Gilbert *Linear algebra and its applications*. Second edition. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1980.

Unitary Diagonalization and Quadratic Forms

Gelfand, I. M. *Lectures on linear algebra*. With the collaboration of Z. Ya. Shapiro. Translated from the second Russian edition by A. Shenitzer. Reprint of the 1961 translation. Dover Books on Advanced Mathematics. Dover Publications, Inc., New York, 1989.

Samelson, Hans *An introduction to linear algebra*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley and Sons], New York-London-Sydney, 1974.

Strang, Gilbert *Linear algebra and its applications*. Second edition. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1980.

Theory of Linear Mappings

Birkhoff, Garrett; MacLane, Saunders *A Survey of Modern Algebra*. Macmillan Company, New York, 1941.

Gelfand, I. M. *Lectures on linear algebra*. With the collaboration of Z. Ya. Shapiro. Translated from the second Russian edition by A. Shenitzer. Reprint of the 1961 translation. Dover Books on Advanced Mathematics. Dover Publications, Inc., New York, 1989.

Hoffman, Kenneth; Kunze, Ray *Linear algebra*. Second edition Prentice-Hall, Inc., Englewood Cliffs, N.J. 1971.

Strang, Gilbert *Linear algebra and its applications*. Second edition. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1980.

Linear Algebraic Groups

Alperin, J. L.; Bell, Rowen B. *Groups and representations*. Graduate Texts in Mathematics, 162. Springer-Verlag, New York, 1995.

Dieudonné, Jean; Carrell, James B. *Invariant Theory, Old and New*. Academic Press, New York-London, 1971.

Humphreys, James E. *Linear algebraic groups*. Graduate Texts in Mathematics, No. 21. Springer-Verlag, New York-Heidelberg, 1975.

Humphreys, James E. *Reflection groups and Coxeter groups*. Cambridge Studies in Advanced Mathematics, 29. Cambridge University Press, Cambridge, 1990.

Malle, Gunter; Testerman, Donna *Linear algebraic groups and finite groups of Lie type*. Cambridge Studies in Advanced Mathematics, 133. Cambridge University Press, Cambridge, 2011.

Index

Symbols

G -set, 339
 k -cycle, 345
 m -frame, 161
 p -ary linear code of length n , 187
 p -group, 344

A

Abelian group, 12
Adjoint, 133, 282
Adjoint map, 236
Algebraically closed field, 45
Algebraic torus, 386
Alternating group, 121
Angle between vectors, 172
Associative law, 12

B

Basic codewords, 187
Basic null vectors, 79
Basis, 147
Bijective, 3
Binary operation, 2
Birkhoff decomposition, 340
Borel sgn, 392
Bounded set, 286
Bruhat cell, 396
Bruhat decomposition, 340, 395

C

Center, 344
Centralizer, 343
Characteristic equation, 240
Characteristic of a field, 50

Characteristic polynomial, 243
Cipher, 375
Closed subgroup, 384
Code, 187
Codewords, 187
Commutator subgroup, 367
Complete flag, 161
Completely reducible, 398
Complex conjugate, 43
Complex exponential, 43
Complex number, 42
Complex polynomial, 45
Composition series, 365
Congruent matrices, 306
Conjugacy class, 339
Conjugation, 20
Conjugation action, 343
Connected group, 385
Convex polyhedron, 286
Convex set, 286
Coordinates, 222
Corner entry, 68
Coset, 23
Coset of a subspace, 183
Cross product, 143, 200
Cyclic group, 16
Cyclic subspaces, 320

D

Daily key, 379
Derivative of a polynomial, 53
Derived series, 366
Diagonalizable matrix, 252
Direct sum, 165
Domain of a mapping, 2
Dot product, 62

Double coset, 340
 Double dual, 236
 Dual basis, 233
 Dual space, 232
 Dynamical system, 256

E

Eigenpair, 239
 Eigenvalue, 239
 Eigenvector, 239
 Equivalence class, 4
 Equivalence relation, 4
 Equivalent linear systems, 77
 Euler's theorem, 32
 Extended Hamming code, 191
 External direct product, 359
 External direct sum, 167

F

Fermat's little theorem, 51
 Fibonacci numbers, 256
 Field, 36
 Finite-dimensional vector space, 147
 Fixed point, 344
 Flag variety, 161, 394
 Fourier expansion, 177
 Free variables, 78
 Frobenius map, 204
 Fundamental theorem of algebra, 45

G

Galois field, 47
 Galois group, 371
 General linear group, 93
 General solution vector, 79
 Golden ratio, 353
 Greatest common divisor, 21, 32
 Group, 12
 Group action, 338

H

Hamming distance, 61, 189
 Hermitian inner product, 173
 Hermitian matrix, 128
 Hermitian transpose, 173
 Homomorphism, 19

I

Idempotent, 377

Imaginary numbers, 41
 Imaginary part, 42
 Inconsistent system, 79
 Index of a subgroup, 26
 Injective, 3
 Inner automorphism, 20
 Inner product, 169
 Inner product space, 169
 Internal direct product, 360
 Invariant subspace, 320
 Inverse image, 3
 Irreducible polynomial, 294
 Irreducible subspace, 398
 Isomorphism, 19
 Isomorphism of vector spaces, 207

J

Jordan block, 328
 Jordan–Chevalley decomposition, 321

K

Kernel, 19
 Kernel of a linear mapping, 205
 Killing form, 170
 Klein 4-group, 356
 Kronecker delta, 64

L

Length of a Weyl group element, 392
 Lie bracket, 326
 Linear algebraic group, 384
 Linear combination, 60, 137
 Linear function, 198
 Linear mapping, 20
 Linear subspace, 141
 Linearly independence, 145
 Linearly reductive, 398

M

Mapping, 2
 Matrix, 58
 Matrix linear mapping, 200
 Metric, 181
 Minimal polynomial, 271
 Modular group, 134
 Multiplicative unit, 33

N

Negative definite matrix, 309

Nilpotent matrix, 269
 Nilpotent part, 321
 Noncollinear vectors, 142
 Nonsingular matrix, 75
 Normal matrix, 299
 Normal subgroup, 24
 Null space, 78

O

Orbit, 339
 Order of a group, 13
 Order of an element, 26
 Orthogonal complement, 177
 Orthogonal group, 95
 Orthogonal group over \mathbb{F} , 95
 Orthogonal mapping, 211
 Orthogonal projection, 172
 Outer automorphism, 20

P

Pairings, 377
 Parabolic subgroup, 396
 Partial permutation matrix, 101
 Partition, 334
 Perfect code, 192
 Perfect field, 54
 Permutation, 14
 Phi function, 32
 Plaintext, 61, 375
 Plane, 142
 Platonic solid, 286
 Polar decomposition, 315
 Polar orbit, 350
 Pole, 349
 Polyhedral group, 349
 Polynomial, 52
 Positive definite matrix, 309
 Prime field, 47
 Primitive element, 35
 Projection, 213
 Projective linear group, 368

Q

Quadratic form, 305
 Quadratic variety, 308
 Quotient, 5
 Quotient group, 29

R

Radical of a group, 385

Rank of a matrix, 74
 Real part, 42
 Reductive group, 385
 Reflection, 213, 215
 Relation, 4
 Relative maximum, 310
 Relative minimum, 310
 Ring, 40
 Roots of unity, 44
 Rotation of \mathbb{R}^3 , 283

S

Scalar multiplication, 42
 Schubert cell, 396
 Self adjoint, 274
 Semidirect product, 363
 Semisimple group, 385
 Semisimple linear mapping, 200
 Semisimple part, 321, 322
 Signature of a permutation, 119
 Signature of a quadratic form, 313
 Signed permutation matrix, 98
 Similar matrices, 128, 228
 Simple group, 364
 Simple reflection, 389, 397
 Simple root, 53
 Simple transposition, 97
 Skew-Hermitian matrix, 301
 Skew-symmetric matrix, 128
 Solution set, 77
 Solvable group, 365
 Span, 60
 Spanning set, 142
 Special linear group, 115
 Splitting field, 294
 Stabilizer, 339
 Standard basis, 147
 String basis, 329
 Subfield, 38
 Subgroup, 18
 Subnormal series, 364
 Sum of subspaces, 162
 Surjective, 3
 Sylow subgroup, 354
 Symplectic group, 386

T

Target, 2
 Telegram key, 379
 Torus, 31
 Trace of a matrix, 170

Transitive action, [339](#)
Transpose, [64](#)
Triangle inequality, [189](#)

U

Unipotent, [322](#)
Unipotent matrix, [100](#)

Unipotent part, [322](#)
Unitary matrix, [128](#), [179](#)

W

Weight of a codeword, [189](#)
Weyl group, [388](#)