Index

We generally indicate the first occurrence only. The data include the typical notation (if any), the serial number of the definition, theorem, etc. explaining the notion or denomination, and finally the page number in parentheses.

D2.1.6 means Definition 2.1.6, and letters T, L, E instead of D refer to the theorem, lemma, and exercise with the given number. P1.3.3 stands for the proof of Theorem 1.3.3, 4.1.E3 denotes Example 3 in Section 4.1, 5.7 means Section 5.7, and A.7/2 refers to Subsection 2 in Section A.7.

We add a sign "−" or "+" to the number of definition, theorem, etc., if the notion is introduced not in the given definition, theorem, etc., but just before or after it, without a new serial number. E.g., DA.10.6+ indicates at the phrase "transcendental number" that it is explained *after* Definition A.10.6.

In some cases, we include an important theorem besides the definition. E.g., for "subspace" we refer both to Definition 4.2.1 and Theorem 4.2.2.

For information about notation used in the book, please consult part "Technical details" in the Introduction. The phrasing of a definition or theorem is closed by a ♣ sign, the end of a proof is denoted by ■. We add that as mentioned in another part of the Introduction, exercises marked with one or two asterisks are considered hard or extra hard by our judgement, and the boldface serial number indicates that a detailed solution can be found at `bookstore.ams.org/amstext-66`.

C = complex numbers
F = generally denotes a field
F_p = finite field of p elements
$F[x]$ = polynomials over F
Q = rational numbers
R = real numbers
Z = integers
$\mathbf{Z}[x]$ = polynomials with integer coefficients
2-repetition code, 10.1.E1, (231)
3-repetition code, 10.1.E2, (231)

A-orthogonal, D7.2.4, (161)
Abelian group, DA.8.1+, (277)
absolute value of a complex number, $|z|$, DA.3.2, (255)
absolute value of a vector, $\|\mathbf{x}\|$, D8.2.1, (182)
accompanying transformation, T5.8.1, (127)

addition
  complex numbers, DA.3.1, (254)
  linear map, $\mathcal{A}+\mathcal{B}$, D5.5.1, (113)
  matrix, $A+B$, D2.1.1, (30)
  polynomials, A.7/3, (269)
  vector, $\mathbf{v}+\mathbf{w}$, D4.1.1, (73)
adjacency matrix of a graph, A, P9.5.1, (214)
adjoint of a matrix, D2.1.6, (33)
adjoint transformation, $\mathcal{A}^*$, T8.4.1, (189)
adjugate matrix, $\hat{A}$, L2.2.3, (37)
algebra, D5.6.5, (117)
algebraic element, DA.10.6, (286)
  degree, $\deg\Theta$, DA.10.9, (287)
algebraic form of a complex number, $a+bi$, TA.3.4+, (255)
algebraic number, DA.10.6+, (286)
algebraically closed field, EA.10.17, (290)
angle in a Euclidean space, D8.2.7, (183)
antisymmetric bilinear function, E7.2.1, (168)
antisymmetric matrix, E1.3.13, (20)
argument of a complex number, $\arg(z)$, DA.3.2, (255)
associate, A.7/12, (272)
associative law, DA.4.2, (259)
augmented matrix, $A \mid \mathbf{b}$, 3.1, (42)
axioms of vector spaces, D4.1.1, (73)

basis, D4.5.1, T4.5.2, (91)
  Hamel, T4.5.7+, (93)
  orthonormal, D8.1.4, (178)
BCH code, t-error correcting, T10.4.2, (242)
BCH code, 2-error correcting, T10.4.1, (241)
Bessel inequality, E8.2.15, (186)
bilinear function, **A**, D7.1.1, (157)
  antisymmetric, E7.2.1, (168)
  complex, D7.4.1, (173)
  Hermitian, T7.4.4+, (174)
  matrix, [**A**], D7.1.3, (159)
  real, **A**, D7.1.1, (157)
  self-adjoint, T7.4.4+, (174)
  skew-Hermitian, E7.4.8, (176)
  skew-symmetric, E7.2.1, (168)
  symmetric, D7.2.1, (161)
  zero, **0**, 7.1.E4, (158)
binomial coefficient, $\binom{n}{k}$, A.1/2, (246)
binomial theorem, TA.1.1, (246)
block of a matrix, T6.6.1+, (148)
Bolyai–Gerwien theorem, E9.7.1, (224)

Cauchy's functional equation, E9.1.8, (202)
Cauchy–Bunyakovsky–Schwarz inequality = CBS, T8.2.8, (183)
Cayley–Hamilton theorem, T6.3.5, (139)
CBS = Cauchy–Bunyakovsky–Schwarz inequality, T8.2.8, (183)
characteristic of a ring, EA.11.5, (294)
characteristic polynomial, $k_{\mathcal{A}}$, D6.2.2, (135)
Chevalley's theorem, E9.3.2, (208)
Chinese remainder theorem, TA.2.10A, (253)
code, C, D10.1.1, (230)
  2-repetition, 10.1.E1, (231)
  3-repetition, 10.1.E2, (231)
  BCH, t-error correcting, T10.4.2, (242)
  BCH, 2-error correcting, T10.4.1, (241)
  cyclic, E10.4.9, (244)
  dimension, n, D10.1.6, (231)
  dual, $C^\perp$, E10.3.10, (239)
  error correcting, D10.1.3, T10.1.5, (230)
  error detecting, D10.1.2, T10.1.5, (230)
  generator matrix, G, D10.2.3, (233)
  generator polynomial, g, E10.2.8(a), D10.4.3, (236), (242)
  Hamming, D10.3.4, (238)
  length, k, D10.1.6, (231)
  linear, D10.2.1, (233)

parity-check matrix, P, D10.3.1, (237)
parity-check, 10.1.E3, (231)
polynomial, E10.2.8(a), D10.4.3, (236), (242)
quasi-parity-check matrix, Q, 10.4, (240)
Reed–Muller, E10.4.11, (244)
systematic, T10.3.2–, (237)
codeword, **c**, D10.1.1, (230)
coefficient matrix, A, 3.1, (42)
cofactor, D1.4.1, (21)
expansion, T1.4.2, (22)
column rank of a matrix, D3.4.1/C, (62)
column space of a matrix, Im A, 4.2.E4, (80)
column vector, D3.1.5, (48)
component, D3.1.5, (48)
coordinate, D3.1.5, (48)
commutative
field, F, DA.5.1, (263)
group, DA.8.1+, (277)
law, DA.4.3, (259)
ring, DA.6.1+, (266)
complement of a 0–1 vector, E10.3.13, (239)
complex
bilinear function, D7.4.1, (173)
Euclidean space, 8.3, (187)
inner product, D8.3.1, T8.3.2, (187)
number, $z = a + bi$, DA.3.1, (254)
nth root, $\sqrt[n]{z}$, TA.3.5, (256)
absolute value, $|z|$, DA.3.2, (255)
addition, DA.3.1, (254)
algebraic form, $a + bi$, TA.3.4+, (255)
argument, $\arg(z)$, DA.3.2, (255)
conjugate, $\overline{z} = a - bi$, DA.3.2, (255)
Euler's form, $z = |z|e^{i\varphi}$, TA.3.4+, (255)
imaginary part, Im z, DA.3.1, (254)
modulus, $|z|$, DA.3.2, (255)
multiplication, DA.3.1, (254)
real part, Re z, DA.3.1, (254)
trigonometric form, $|z|(\cos\varphi + i\sin\varphi)$, TA.3.4+, (255)
root of unity, DA.3.6, (256)
order, $o(w)$, DA.3.6, (256)
component of a column vector, D3.1.5, (48)
congruence mod m, $\equiv$, DA.2.3, (251)
conjugate of a complex number, $\overline{z} = a - bi$, DA.3.2, (255)
consistent system of equations, T3.1.1+, (46)
coordinate of a column vector, D3.1.5, (48)
coordinate vector, 5.1.E5, (105)
coordinates in a basis, D4.7.1, (100)
coprime, DA.2.1, (250)
coset, gH, DA.8.5, (279)
of a subgroup, gH, DA.8.5, (279)
of a subspace, $\mathbf{v} + W$, E4.2.16, (83)
of an ideal, $c + I$, TA.9.5, (282)
cyclic code, E10.4.9, (244)
cyclic group, $\langle g\rangle$, DA.8.3, (279)
generator, DA.8.3, (279)
cyclotomic polynomial, Φ_m, A.7/13, (274)

decoding table, 10.2, (234)
degree
of a field extension, $\deg(M : L)$, DA.10.2, (285)
of a polynomial, deg, A.7/5, (270)
of a vertex in a graph, E9.5.1–, (215)
of an algebraic element, $\deg\Theta$, DA.10.9, (287)
Dehn-invariant, P9.7.1, (223)
dependent, D4.4.1, (88)
in F^k, D3.3.2, (56)
derivative of a polynomial, f', A.7/10, (272)
determinant, D1.2.2, (12)
Vandermonde, D1.5.1, T1.5.2, (26)
determinant rank of a matrix, D3.4.1/D, (62)

diagonal matrix, E4.2.2(h), (80)
dihedral group, D_n, A.8.E7, (278)
dimension of a code, n, D10.1.6, (231)
dimension of a vector space, dim, D4.6.1, (96)
dimension theorem, T5.4.1, (112)
direct sum of matrices, T6.6.1+, (148)
direct sum of subspaces, $W \oplus Z$, D4.3.7, (85)
disjoint subspaces, D4.3.7−, (85)
distance in a normed space, δ, D8.2.4, (183)
distance of 0–1 vectors, δ, D10.1.4, (230)
distributive laws, DA.6.1, (266)
divisibility, $a \mid b$, DA.2.1, (250)
division algorithm for integers, TA.2.2, (250)
division algorithm for polynomials, A.7/12, (273)
dot product, $\mathbf{u} \cdot \mathbf{v}$, D8.1.1, T8.1.2, (177, 178)
  in $\mathbf{R}^k$, 7.1.E2, (158)
  in the plane and space, 7.1.E1, (158)
dual code, $C^\perp$, E10.3.10, (239)
dual space, E8.1.13, (181)

echelon form, 3.1, (44)
  reduced, 3.1, (45)
eigenbasis, (132)
eigenspace, T6.1.3, (132)
eigenvalue, D6.1.1, (131)
eigenvector, D6.1.2, (131)
elementary equivalent transformation, 3.1, (42)
elimination, Gaussian, 3.1, (42)
encoding function, φ, $\mathcal{A}$, D10.1.1, (230)
equidissectible, 9.7, (222)
equivalence class, TA.1.4+, (248)
equivalence relation, DA.1.3, TA.1.4, (248)
error correcting code, D10.1.3, T10.1.5, (230)
error detecting code, D10.1.2, T10.1.5, (230)
error vector, $\mathbf{e}$, 10.2, (234)
Euclidean
  algorithm, TA.2.2+, (250)
  domain, A.7/12, (273)
  space, complex, 8.3, (187)
  space, D8.1.3, (178)
  space, real, D8.1.3, (178)
Euler's form of a complex number, $z = |z|e^{i\varphi}$, TA.3.4+, (255)
Euler's function, $\varphi(n)$, DA.2.4, TA.2.5, (251)
Euler–Fermat theorem, TA.2.6, (252)
even permutation, D1.1.2, (8)
Eventown, T9.4.2, (210)
expansion, 1.4, (21)
  cofactor, T1.4.2, (22)
  Laplace, E1.4.15, (26)
  skew, T1.4.3, (24)

factor ring, R/I, TA.9.5, (282)
factorization of integers, 9.3, (207)
Fermat's little theorem, TA.2.6A, (252)
Fibonacci number, φ_n, E4.6.8, 9.2, (99), (202)
field, F, DA.5.1, (263)
  algebraically closed, EA.10.17, (290)
  axioms, DA.5.1, (263)
  commutative, F, DA.5.1, (263)
  extension, $M : L$, DA.10.1, (285)
    degree, $\deg(M : L)$, DA.10.2, (285)
    simple, $L(\Theta)$, DA.10.4, TA.10.5, (286)
    tower theorem, TA.10.3, (286)
  finite, M, F_p, A.11, (290)
  isomorphism, EA.5.4, (265)
  of modulo p residue classes, F_p, $\mathbf{Z}_p$, A.5.E2, (264)
  skew, DA.5.1+, (263)
finite field, M, F_p, A.11, (290)
  primitive element, Δ, TA.11.3+, (291)
finite projective plane, E9.5.11, (216)
finitely generated ideal, $(a_1, \ldots, a_k)$, EA.9.7, (284)

$F^{k\times n}$ = the set of $k \times n$ matrices, D2.1.1−, (29)
forbidden row, 3.1, (45)
form
  algebraic, of a complex number, $a + bi$, TA.3.4+, (255)
  echelon, 3.1, (44)
  Euler's, of a complex number, $z = |z|e^{i\varphi}$, TA.3.4+, (255)
  Jordan, T6.6.6, (152)
  quadratic, $\tilde{\mathbf{A}}$, D7.3.1, (169)
  reduced echelon, 3.1, (45)
  trigonometric, of a complex number, $|z|(\cos\varphi + i\sin\varphi)$, TA.3.4+, (255)
F^q = set of column vectors, D3.1.5, (48)
free parameter, 3.1, (45)
free variable, 3.1, (45)
Frobenius theorem, 5.6.E5, (118)
function
  bilinear, $\mathbf{A}$, D7.1.1, (157)
  encoding, φ, $\mathcal{A}$, D10.1.1, (230)
  polynomial, A.7/2, (269)
  real bilinear, $\mathbf{A}$, D7.1.1, (157)
fundamental theorem of algebra, A.7/8, (271)

Gauss's lemmas for polynomials, A.7/13, (274)
Gaussian elimination, 3.1, (42)
Gaussian integers, A.6.E2, (267)
gcd = greatest common divisor, (a, b), DA.2.1, (250)
generator
  matrix of a code, G, D10.2.3, (233)
  of a cyclic group, DA.8.3, (279)
  of a subspace, D4.3.3+, (84)
  polynomial of a code, g, E10.2.8(a), D10.4.3, (236), (242)
Gram–Schmidt orthogonalization, P7.2.3, (162)
greatest common divisor of integers, (a, b), DA.2.1, (250)
greatest common divisor of polynomials, A.7/12, (273)
group, G, DA.8.1, (277)
  Abelian, DA.8.1+, (277)
  commutative, DA.8.1+, (277)
  cyclic, $\langle g\rangle$, DA.8.3, (279)
  dihedral, D_n, A.8.E7, (278)
  isomorphism, $\cong$, TA.8.6+, (280)
  of symmetries of a figure, A.8.E7, (278)
  order of an element, $o(g)$, DA.8.2, (278)
  symmetric, S_n, A.8.E5, (278)

Hamel basis, T4.5.7+, (93)
Hamming code, D10.3.4, (238)
Hamming distance, δ, D10.1.4, (230)
Hamming weight, w, D10.1.4, (230)
Hermitian bilinear function, T7.4.4+, (174)
Hilbert's third problem, T9.7.1, (223)
Hoffman–Singleton theorem, T9.5.1, (214)
Hom V, T5.5.3, (114)
Hom(V_1, V_2), T5.5.3, (114)
homogeneous coordinates, EA.11.13, (295)
homogeneous system of equations, D3.1.3, (47)
  trivial solution, D3.1.3+, (47)

ideal, I, DA.9.1, (281)
  coset, $c + I$, TA.9.5, (282)
  finitely generated, $(a_1, \ldots, a_k)$, EA.9.7, (284)
  principal, (a), DA.9.2, TA.9.3, (282)
  tightest, TA.9.3+, (282)
  trivial, DA.9.1+, (281)
ideal line, EA.11.13, (295)
ideal point, EA.11.13, (295)
identity, e, DA.4.4, (259)
  left, e_L, DA.4.4, (259)
  map, $\mathcal{I}$, 5.1.E3, (105)
  matrix, I, P2.2.1, (35)
  right, e_R, DA.4.4, (259)
image
  linear map, Im $\mathcal{A}$, D5.1.3, (104)
  matrix, Im A, 4.2.E4, (80)

imaginary number, DA.3.1, (254)
imaginary part of a complex number, Im z, DA.3.1, (254)
incidence matrix of a graph, E9.5.1−, (215)
incidence matrix of a set system, E9.4.4, (211)
inclusion-exclusion formula, TA.1.2, (247)
indefinite, D7.3.2, (171)
independent, D4.4.2, (88)
  in F^k, D3.3.3, (56)
index of a subgroup, $|G : H|$, DA.8.5+, (279)
inner product, $\mathbf{u} \cdot \mathbf{v}$, D8.1.1, T8.1.2, (177, 178)
  complex, D8.3.1, T8.3.2, (187)
  in $\mathbf{R}^k$, 7.1.E2, (158)
  in the plane and space, 7.1.E1, 7.1.E2, (158)
integral domain, A.6.E1−, (267)
interpolation polynomial, T3.2.4, (53)
  Lagrange, E3.2.11, (55)
  Newton, E3.2.10, (55)
invariant subspace, D6.4.1, (142)
inverse, a^{-1}, DA.4.5, (260)
  left, a_L, DA.4.5, (260)
  matrix, A^{-1}, T2.2.2, (36)
  operation, DA.4.6, (261)
  right, a_R, DA.4.5, (260)
inversion in a permutation, D1.1.1, (8)
irreducible integer, DA.2.1, (250)
irreducible polynomial, A.7/12, (273)
isomorphic vector spaces, $\cong$, D5.2.1, T5.2.5, (108)
isomorphism
  field, EA.5.4, (265)
  group, $\cong$, TA.8.6+, (280)
  vector space, $\cong$, D5.2.1, T5.2.2, (108)

J = matrix where all entries are 1, (214)
Jordan form, T6.6.6, (152)

kernel
  linear map, Ker $\mathcal{A}$, D5.1.4, (104)
  matrix, Ker A, 4.2.E4, (80)

Lagrange's interpolation polynomial, E3.2.11, (55)
Lagrange's theorem on the size of a subgroup, TA.8.6, (280)
Laplace expansion, E1.4.15, (26)
law of inertia, T7.2.6, (167)
leader, 3.1, (44)
leading coefficient of a polynomial, A.7/5, (270)
left identity, e_L, DA.4.4, (259)
left inverse, a_L, DA.4.5, (260)
length of a code, k, D10.1.6, (231)
length of a vector, $\|\mathbf{x}\|$, D8.2.1, (182)
length of an orbit, D6.6.4, (150)
linear
  code, D10.2.1, (233)
  combination
    trivial, D3.3.1+, (56)
  congruence, $ax \equiv b \pmod{m}$, TA.2.9, (252)
  Diophantine equation, $Ax + By = C$, TA.2.8−, (252)
  equations, system of, 3.1, (41)
  functional, 7.1.9, (160)
  map, $\mathcal{A}$, D5.1.1, (103)
    addition, $\mathcal{A} + \mathcal{B}$, D5.5.1, (113)
    identity, $\mathcal{I}$, 5.1.E3, (105)
    image, Im $\mathcal{A}$, D5.1.3, (104)
    kernel, Ker $\mathcal{A}$, D5.1.4, (104)
    matrix, $[\mathcal{A}]$, D5.7.1, (122)
    multiplication by a scalar, $\lambda\mathcal{A}$, D5.5.2, (114)
    multiplication, $\mathcal{A}\mathcal{B}$, D5.6.1, (116)
    null space, Ker $\mathcal{A}$, D5.1.4, (104)
    range space, Im $\mathcal{A}$, D5.1.3, (104)
    zero, $\mathcal{O}$, 5.1.E2, (105)
  transformation, $\mathcal{A}, \mathcal{B}, \ldots$, D5.1.6, (105)
    characteristic polynomial, $k_{\mathcal{A}}$, D6.2.2, (135)
    minimal polynomial, $m_{\mathcal{A}}$, D6.3.1, (137)
linearly dependent, D4.4.1, (88)
  in F^k, D3.3.2, (56)

linearly independent, D4.4.2
in F^k, D3.3.3, (56)

magic square, E4.6.9, (99)
magnitude of a vector, $\|\mathbf{x}\|$, D8.2.1, (182)
mathematical induction, A.1/1, (245)
matrix, D1.2.1, (10)
addition, $A + B$, D2.1.1, (30)
adjacency, of a graph, A, P9.5.1, (214)
adjoint, D2.1.6, (33)
adjugate, $\hat{A}$, L2.2.3, (37)
antisymmetric, E1.3.13, (20)
augmented, $A \mid \mathbf{b}$, 3.1, (42)
block, T6.6.1+, (148)
coefficient, A, 3.1, (42)
column space, Im A, 4.2.E4, (80)
diagonal, E4.2.2(h), (80)
direct sum, T6.6.1+, (148)
generator, of a code, G, D10.2.3, (233)
identity, I, P2.2.1, (35)
image, Im A, 4.2.E4, (80)
incidence, of a graph, E9.5.1−, (215)
incidence, of a set system, E9.4.4, (211)
inverse, A^{-1}, T2.2.2, (36)
kernel, Ker A, 4.2.E4, (80)
multiplication by a scalar, λA, D2.1.1+, (30)
multiplication, AB, D2.1.3, (31)
nilpotent, E4.2.2(d), (80)
non-singular, D3.5.1, (67)
null space, Ker A, 4.2.E4, (80)
of a bilinear function, $[\mathbf{A}]$, D7.1.3, (159)
of a linear map, $[\mathcal{A}]$, D5.7.1, (122)
parity-check, of a code, P, D10.3.1, (237)
quasi-parity-check, of a code, Q, 10.4, (240)
rank, rk(A), T3.4.2, (63)
similar, D6.1.6, (133)
singular, D3.5.1, (67)
skew-symmetric, E1.3.13, (20)
square, D1.2.1+, (11)
symmetric, E4.2.2(j), (80)
trace, E5.1.3(c), (106)
transpose, D2.1.5, (33)
upper triangular, 2.2.6, (39)
zero, 0, T2.1.2, (30)
message word, D10.1.1, (230)
metric space, D8.2.6, (183)
minimal polynomial
of a linear transformation, $m_{\mathcal{A}}$, D6.3.1, (137)
of an algebraic element, m_Θ, DA.10.7, (287)
minor, E1.4.15, (26)
signed, D1.4.1, (21)
complementary, E1.4.15, (26)
modulus of a complex number, $|z|$, DA.3.2, (255)
modulus of a congruence, m, DA.2.3, (251)
Moivre's formula, TA.3.4+, (256)
monic polynomial, A.7/5, (270)
multiple root, A.7/7, (271)
multiplication
complex numbers, DA.3.1, (254)
linear map, $\mathcal{AB}$, D5.6.1, (116)
matrix, AB, D2.1.3, (31)
polynomials, A.7/3, (270)
multiplication by a scalar
linear map, $\lambda\mathcal{A}$, D5.5.2, (114)
matrix, λA, D2.1.1+, (30)
vector, $\lambda\mathbf{v}$, D4.1.1, (74)
multiplicity of a root of a polynomial, A.7/7, (271)

negative, $-a$, DA.4.5+, (260)
negative definite, D7.3.2, (171)
negative semidefinite, D7.3.2, (171)
Newton's interpolation polynomial, E3.2.10, (55)
nilpotent matrix, E4.2.2(d), (80)
non-singular matrix, D3.5.1, (67)
norm of a vector, $\|\mathbf{x}\|$, D8.2.1, (182)
normal transformation, D8.5.1, T8.5.2, (191)
normed space, D8.2.3, (183)

nth root of a complex number, $\sqrt[n]{z}$, TA.3.5, (256)
null space of a linear map, $\mathrm{Ker}\,\mathcal{A}$, D5.1.4, (104)
null space of a matrix, $\mathrm{Ker}\,A$, 4.2.E4, (80)
nullity of a linear map, T5.4.1+, (112)
number of check digits, s, D10.1.6, (231)
number of inversions, $I(\sigma)$, D1.1.1, (8)

odd permutation, D1.1.2, (8)
Oddtown, T9.4.1, (210)
operation, DA.4.1, (258)
orbit of a vector, D6.6.4, (150)
order
  modulo m, $o_m(c)$, $o(c)$, DA.2.7, (252)
  of a complex root of unity, $o(w)$, DA.3.6, (256)
  of a vector, $o_{\mathcal{A}}(\mathbf{u})$, D6.5.1, (144)
  of an element in a group, $o(g)$, DA.8.2, (278)
orthogonal, $\perp$, D8.1.5, (179)
  complement, $()^{\perp}$, D8.1.6, (179)
  projection, T8.1.7+, (179)
  transformation, D8.6.3, (196)
  vectors, $\perp$, D8.1.5, (179)
orthonormal basis, D8.1.4, (178)
orthonormal system, D8.1.4, (178)

parallelepiped (n-dimensional), 9.8, (225)
parallelepiped volume, D, 9.8, (225)
parameter, free, 3.1, (45)
parity-check code, 10.1.E3, (231)
parity-check matrix of a code, P, D10.3.1, (237)
Parseval formula, E8.2.14, (186)
permutation, σ, 1.1, (7)
  even, D1.1.2, (8)
  inversion, D1.1.1, (8)
  number of inversions, $I(\sigma)$, D1.1.1, (8)
  odd, D1.1.2, (8)
perpendicular vectors, $\perp$, D8.1.5, (179)
Petersen graph, E9.5.1, (215)

$\varphi(n)$ = Euler's function, DA.2.4, TA.2.5, (251)
pivot, 3.1, (44)
polynomial, A.7/1, (269)
  addition, A.7/3, (269)
  characteristic, $k_{\mathcal{A}}$, D6.2.2, (135)
  code, E10.2.8(a), D10.4.3, (236), (242)
  cyclotomic, Φ_m, A.7/13, (274)
  degree, deg, A.7/5, (270)
  derivative, f', A.7/10, (272)
  function, A.7/2, (269)
  Gauss's lemmas, A.7/13, (274)
  generator of a code, g, E10.2.8(a), D10.4.3, (236), (242)
  interpolation, T3.2.4, (53)
  irreducible, A.7/12, (273)
  Lagrange interpolation, E3.2.11, (55)
  leading coefficient, A.7/5, (270)
  minimal, of a linear transformation, $m_{\mathcal{A}}$, D6.3.1, (137)
  minimal, of an algebraic element, m_{Θ}, DA.10.7, (287)
  monic, A.7/5, (270)
  multiple root, A.7/7, (271)
  multiplication, A.7/3, (270)
  Newton interpolation, E3.2.10, (55)
  primitive in $\mathbf{Z}[x]$, A.7/13, (274)
  primitive over F_p, TA.11.6+, (292)
  reducible, A.7/12, (273)
  relation between roots and coefficients, A.7/11, (272)
  repeated root, A.7/7, (271)
  root, A.7/6, (270)
positive definite, D7.3.2, (171)
positive semidefinite, D7.3.2, (171)
prime property, TA.2.2+, (250)
primitive nth root of unity, DA.3.6, (256)
primitive element of a finite field, Δ, TA.11.3+, (291)
primitive polynomial in $\mathbf{Z}[x]$, A.7/13, (274)

primitive polynomial over F_p, TA.11.6+, (292)
primitive root mod p, DA.8.3+, (279)
principal axis theorem, T8.6.2, (195)
principal ideal, (a), DA.9.2, TA.9.3, (282)
  domain, TA.9.4+, (282)
projection, $\mathcal{P}$, E5.6.18, (121)
  orthogonal, T8.1.7+, (179)
projective plane, E9.5.11, (216)
  finite, E9.5.11, (216)
  real, EA.11.13, (295)

quadratic form, $\tilde{\mathbf{A}}$, D7.3.1, (169)
quasi-parity-check matrix, Q, 10.4, (240)
quaternion, 5.6.E5, (118)

range space of a linear map, Im $\mathcal{A}$, D5.1.3, (104)
rank of a
  linear map, rk $\mathcal{A}$, T5.4.1+, (112)
  matrix, rk(A), T3.4.2, (63)
    column, D3.4.1/C, (62)
    determinant, D3.4.1/D, (62)
    row, D3.4.1/R, (62)
  system of vectors, (97)
rational root test, A.7/9, (271)
real
  bilinear function, $\mathbf{A}$, D7.1.1, (157)
  Euclidean space, D8.1.3, (178)
  part of a complex number, Re z, DA.3.1, (254)
  projective plane, EA.11.13, (295)
reciprocal, $1/a$, DA.4.5+, (260)
recursion, E4.6.8, 9.2, (99)
reduced echelon form, 3.1, (45)
reduced residue class, A.6.E5, (267)
reducible polynomial, A.7/12, (273)
redundant row, 3.1, (45)
Reed–Muller code, E10.4.11, (244)
REF = reduced echelon form, 3.1, (45)
reflexive relation, DA.1.3, (248)
regular graph, E9.5.1–, (215)
relation, R, DA.1.3–, (248)
  between roots and coefficients of a polynomial, A.7/11, (272)
  equivalence, DA.1.3, TA.1.4, (248)
  reflexive, DA.1.3, (248)
  symmetric, DA.1.3, (248)
  transitive, DA.1.3, (248)
relatively prime, DA.2.1, (250)
repeated root, A.7/7, (271)
replacement theorem, L4.5.5, (92)
residue class, DA.2.3+, (251)
  reduced, A.6.E5, (267)
right identity, e_R, DA.4.4, (259)
right inverse, a_R, DA.4.5, (260)
ring, R, DA.6.1, (266)
  axioms, DA.6.1, (266)
  characteristic, EA.11.5, (294)
  commutative, DA.6.1+, (266)
  factor, R/I, TA.9.5, (282)
  of modulo m residue classes, $\mathbf{Z}_m$, A.6.E5, (267)
root factor, A.7/6, (271)
root of a polynomial, A.7/6, (270)
  multiplicity, A.7/7, (271)
root of unity, DA.3.6, (256)
  primitive, DA.3.6, (256)
row rank of a matrix, D3.4.1/R, (62)

scalar, D2.1.1+, (30)
Schönemann–Eisenstein criterion of irreducibility, A.7/13, (273)
self-adjoint bilinear function, T7.4.4+, (174)
self-adjoint transformation, D8.5.4, (192)
Sidon set, 9.6, (217)
signed complementary minor, E1.4.15, (26)
signed minor, D1.4.1, (21)
signed volume of a parallelepiped, D, 9.8, (225)
similar matrices, D6.1.6, (133)
simple extension, $L(\Theta)$, DA.10.4, TA.10.5, (286)
simultaneous system of congruences, TA.2.10, (252)
singular matrix, D3.5.1, (67)

skew expansion, T1.4.3, (24)
skew field, DA.5.1+, (263)
skew-Hermitian bilinear function, E7.4.8, (176)
skew-symmetric bilinear function, E7.2.1, (168)
skew-symmetric matrix, E1.3.13, (20)
span of
  a subset, $\langle H \rangle$, D4.3.8, (85)
  a vector and a transformation, $\langle \mathbf{u}, \mathcal{A} \rangle$, D6.4.2, (142)
  subspaces, $\langle W, Z \rangle$, D4.3.5, (84)
  vectors, $\langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$, D4.3.3, T4.3.4, (84)
spanning set, D4.3.2, (83)
spectrum of a graph, E9.5.1−, (215)
square matrix, D1.2.1+, (11)
standard form of integers, TA.2.2, (250)
subfield, EA.5.5, (265)
  tightest, $L(\Theta)$, TA.10.5, (286)
subgroup, DA.8.4, (279)
  coset, gH, DA.8.5, (279)
  index, $|G : H|$, DA.8.5+, (279)
  trivial, DA.8.5−, (279)
subring, EA.6.10, (268)
subspace, D4.2.1, T4.2.2, (79)
  coset, $\mathbf{v} + W$, E4.2.16, (83)
  generator, D4.3.3+, (84)
  invariant, D6.4.1, (142)
  tightest, T4.3.4, (84)
  translate, $\mathbf{v} + W$, E4.2.16, (83)
  trivial, 4.2.E1, (80)
sum of subspaces, $W + Z$, D4.3.5, (84)
symmetric
  bilinear function, D7.2.1, (161)
  difference, EA.4.1(f), (262)
  group, S_n, A.8.E5, (278)
  matrix, E4.2.2(j), (80)
  relation, DA.1.3, (248)
  transformation, D8.6.1, (195)
symmetry group of a figure, A.8.E7, (278)
syndrome, $\mathbf{z}$, T10.3.2−, (237)
system of linear equations, 3.1, (41)
  consistent, T3.1.1+, (46)
  homogeneous, D3.1.3, (47)
systematic code, T10.3.2−, (237)

tightest
  ideal, TA.9.3+, (282)
  subfield, $L(\Theta)$, TA.10.5, (286)
  subspace, T4.3.4, (84)
tower theorem for field extensions, TA.10.3, (286)
trace of a matrix, E5.1.3(c), (106)
transcendental element, TA.10.11+, (288)
transcendental number, DA.10.6+, (287)
transformation, T5.8.1
  accompanying, (127)
  adjoint, $\mathcal{A}^*$, T8.4.1, (189)
  elementary equivalent, 3.1, (42)
  linear, $\mathcal{A}, \mathcal{B}, \ldots$, D5.1.6, (105)
  normal, D8.5.1, T8.5.2, (191)
  orthogonal, D8.6.3, (196)
  self-adjoint, D8.5.4, (192)
  symmetric, D8.6.1, (195)
  unitary, D8.5.5, (192)
transitive relation, DA.1.3, (248)
translate of a subspace, $\mathbf{v} + W$, E4.2.16, (83)
transpose of a matrix, D2.1.5, (33)
triangle inequality, T8.2.2, (183)
trigonometric form of a complex number, $|z|(\cos\varphi + i\sin\varphi)$, TA.3.4+, (255)
trivial
  ideal, DA.9.1+, (281)
  linear combination, D3.3.1+, (56)
  solution of a homogeneous system, D3.1.3+, (47)
  subgroup, DA.8.5−, (279)
  subspace, 4.2.E1, (80)

unique factorization of integers, TA.2.2, (250)
unique factorization of polynomials, A.7/12, (273)

unit (related to divisibility), A.7/12, (272)
unit vector, 3.4, (68)
unitary transformation, D8.5.5, (192)
unknown in equations, 3.1, (41)
upper triangular matrix, E2.2.6, (39)

Vandermonde determinant, D1.5.1, T1.5.2, (26)
variable, free, 3.1, (45)
vector, **v**, D4.1.1+, (74)
  absolute value, $||\mathbf{x}||$, D8.2.1, (182)
  addition, $\mathbf{v} + \mathbf{w}$, D4.1.1, (73)
  column, D3.1.5, (48)
  length, $||\mathbf{x}||$, D8.2.1, (182)
  magnitude, $||\mathbf{x}||$, D8.2.1, (182)
  multiplication by a scalar, $\lambda\mathbf{v}$, D4.1.1, (74)
  norm, $||\mathbf{x}||$, D8.2.1, (182)
  orbit, D6.6.4, (150)
  orthogonal, $\perp$, D8.1.5, (179)
  perpendicular, $\perp$, D8.1.5, (179)
  unit, 3.4, (68)
  zero, **0**, E3.1.1−, (48)
vector depending linearly on vectors, D4.4.4, (89)
vector space, V, D4.1.1, (73)
  axioms, D4.1.1, (73)
  basis, D4.5.1, T4.5.2, (91)
  dimension, dim, D4.6.1, (96)
  isomorphic, $\cong$, D5.2.1, T5.2.5, (108)
  isomorphism, $\cong$, D5.2.1, T5.2.2, (108)
  normed, D8.2.3, (183)
  spanning set, D4.3.2, (83)
Vieta formulas, A.7/11, (272)
volume of a parallelepiped, D, 9.8, (225)

Wedderburn's theorem, EA.6.8, (268)
weight of a 0–1 vector, w, D10.1.4, (230)

zero
  bilinear function, **0**, 7.1.E4, (158)
  divisor, DA.6.2, (266)
    left, DA.6.2, (266)
    right, DA.6.2, (266)
  element, 0, DA.4.4+, (260)
  map, $\mathcal{O}$, 5.1.E2, (105)
  matrix, 0, T2.1.2, (30)
  of a polynomial, A.7/6, (270)
  vector, **0**, E3.1.1−, (48)
$\mathbf{Z}_m$ = ring of modulo m residue classes, A.6.E5, (267)