Let $A$ be an $n \times n$ matrix and consider a matrix equation of the form $AX = B$, where $A$ and $B$ are known but $X$ is unknown. If we can find an $n \times n$ matrix $A^{-1}$ such that $A^{-1}A = AA^{-1} = I_n$, then we can conclude that

$$A^{-1}(AX) = A^{-1}B, \qquad (A^{-1}A)X = A^{-1}B, \qquad I_nX = A^{-1}B, \qquad X = A^{-1}B,$$

and we have found the desired matrix $X$. Such a matrix $A^{-1}$ acts like the reciprocal of a number: $A^{-1}A = I_n$ and $(1/r)r = 1$. This is the reason for the notation $A^{-1}$.

If $A^{-1}$ exists, the square matrix $A$ is **invertible** and $A^{-1}$ is the **inverse** of $A$. If $A^{-1}$ does not exist, then $A$ is said to be **singular**. It can be shown that if there exists an $n \times n$ matrix $A^{-1}$ such that $A^{-1}A = I_n$, then $AA^{-1} = I_n$ also, and furthermore, there is only one matrix $A^{-1}$ having this property.

**A5 Example** Let

$$A = \begin{bmatrix} 2 & 9 \\ 1 & 4 \end{bmatrix}.$$

We can check that

$$\begin{bmatrix} -4 & 9 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 2 & 9 \\ 1 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 9 \\ 1 & 4 \end{bmatrix}\begin{bmatrix} -4 & 9 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus,

$$A^{-1} = \begin{bmatrix} -4 & 9 \\ 1 & -2 \end{bmatrix}. \qquad \blacktriangle$$

We leave the problems of determining the existence of $A^{-1}$ and its computation to a course in linear algebra.

Associated with each square $n \times n$ matrix $A$ is a number called the *determinant* of $A$ and denoted by $\det(A)$. This number can be computed as sums and differences of certain products of the numbers that appear in the matrix $A$. For example, the determinant of the $2 \times 2$ matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $ad - bc$. Note that an $n \times 1$ matrix with real number entries can be viewed as giving coordinates of a point in $n$-dimensional Euclidean space $\mathbb{R}^n$. Multiplication of such a single column matrix on the left by a real $n \times n$ matrix $A$ produces another such single column matrix corresponding to another point in $\mathbb{R}^n$. This multiplication on the left by $A$ thus gives a map of $\mathbb{R}^n$ into itself. It can be shown that a piece of $\mathbb{R}^n$ of volume $V$ is mapped by this multiplication by $A$ into a piece of volume $|\det(A)| \cdot V$. This is one of the reasons that determinants are important.

The following properties of determinants for $n \times n$ matrices $A$ and $B$ are of interest in this text:

1. $\det(I_n) = 1$
2. $\det(AB) = \det(A)\det(B)$
3. $\det(A) \neq 0$ if and only if $A$ is an invertible matrix
4. If $B$ is obtained from $A$ by interchanging two rows (or two columns) of $A$, then $\det(B) = -\det(A)$
5. If every entry of $A$ is zero above the *main diagonal* from the upper left corner to the lower right corner, then $\det(A)$ is the product of the entries on this diagonal. The same is true if all entries below the main diagonal are zero.

## EXERCISES A

In Exercises 1 through 9, compute the given arithmetic matrix expression, if it is defined.

**1.** $\begin{bmatrix} -2 & 4 \\ 1 & 5 \end{bmatrix} + \begin{bmatrix} 4 & -3 \\ 1 & 2 \end{bmatrix}$

**2.** $\begin{bmatrix} 1+i & -2 & 3-i \\ 4 & i & 2-i \end{bmatrix} + \begin{bmatrix} 3 & i-1 & -2+i \\ 3-i & 1+i & 0 \end{bmatrix}$

**3.** $\begin{bmatrix} i & -1 \\ 4 & 1 \\ 3 & -2i \end{bmatrix} - \begin{bmatrix} 3-i & 4i \\ 2 & 1+i \\ 3 & -i \end{bmatrix}$

**4.** $\begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ -1 & 3 \end{bmatrix}$

**5.** $\begin{bmatrix} 3 & 1 \\ -4 & 2 \end{bmatrix} \begin{bmatrix} 1 & 5 & -3 \\ 2 & 1 & 6 \end{bmatrix}$

**6.** $\begin{bmatrix} 4 & -1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 7 \\ 3 & 1 \end{bmatrix}$

**7.** $\begin{bmatrix} i & 1 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 3i & 1 \\ 4 & -2i \end{bmatrix}$

**8.** $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^4$

**9.** $\begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}^4$

**10.** Give an example in $M_2(\mathbb{Z})$ showing that matrix multiplication is not commutative.

**11.** Find $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^{-1}$, by experimentation if necessary.

**12.** Find $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -1 \end{bmatrix}^{-1}$, by experimentation if necessary.

**13.** If $\mathrm{A} = \begin{bmatrix} 3 & 0 & 0 \\ 10 & -2 & 0 \\ 4 & 17 & 8 \end{bmatrix}$, find det (A).

**14.** Prove that if $A, B \in M_n(\mathbb{C})$ are invertible, then $AB$ and $BA$ are invertible also.

# Bibliography


## Classic Works

1. N. Bourbaki, *Eléments de Mathématique,* Book II of Part I, *Algèbre*. Paris: Hermann, 1942–58.
2. N. Jacobson, *Lectures in Abstract Algebra*. Princeton, NJ: Van Nostrand, vols. I, 1951, II, 1953, and III, 1964.
3. O. Schreier and E. Sperner, *Introduction to Modern Algebra and Matrix Theory* (English translation), 2nd Ed. New York: Chelsea, 1959.
4. B. L. van der Waerden, *Modern Algebra* (English translation). New York: Ungar, vols. I, 1949, and II, 1950.

## General Algebra Texts

5. M. Artin, *Algebra*. (Classic Version), 2nd Edition, London: Pearson, 2018.
6. A. A. Albert, *Fundamental Concepts of Higher Algebra*. Chicago: University of Chicago Press, 1956.
7. G. Birkhoff and S. MacLane, *A Survey of Modern Algebra,* 3rd Ed. New York: Macmillan, 1965.
8. J. A. Gallian, *Contemporary Abstract Algebra,* 8th Ed. Boston, MA: Brook/Cole, 2013.
9. I. N. Herstein, *Topics in Algebra*. New York: Blaisdell, 1964.
10. T. W. Hungerford, *Algebra*. New York: Springer, 1974.
11. S. Lang, *Algebra*. Reading, MA: Addison-Wesley, 1965.
12. S. MacLane and G. Birkhoff, *Algebra*. New York: Macmillan, 1967.
13. N. H. McCoy and G. J. Janusz, *Introduction to Modern Algebra*. Cambridge, MA: Academic Press, 2001.
14. G. D. Mostow, J. H. Sampson, and J. Meyer, *Fundamental Structures of Algebra*. New York: McGraw-Hill, 1963.
15. W. W. Sawyer, *A Concrete Approach to Abstract Algebra*. Mineola, NY: Dover, 1978.

## Group Theory

16. W. Burnside, *Theory of Groups of Finite Order,* 2nd Ed. Cambridge, UK: Cambridge University Press, 2012.
17. H. S. M. Coxeter and W. O. Moser, *Generators and Relations for Discrete Groups,* 2nd Ed. Berlin: Springer, 1965.
18. M. Hall, Jr., *The Theory of Groups*. Mineola, NY: Dover, 2018.
19. A. G. Kurosh, *The Theory of Groups* (English translation). New York: Chelsea, vols. I, 1955, and II, 1956.
20. W. Ledermann, *Introduction to the Theory of Finite Groups,* 4th rev. Ed. New York: Interscience, 1961.

21. J. G. Thompson and W. Feit, "Solvability of Groups of Odd Order." *Pac. J. Math*., **13** (1963), 775–1029.
22. M. A. Rabin, "Recursive Unsolvability of Group Theoretic Problems." *Ann. Math*., **67** (1958), 172–194.

## Ring Theory

23. W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases* (Graduate Studies in Mathematics, vol. 3). Providence, RI: American Mathematical Society, 1994.
24. E. Artin, C. J. Nesbitt, and R. M. Thrall, *Rings with Minimum Condition*. Ann Arbor: University of Michigan Press, 1964.
25. N. H. McCoy, *Rings and Ideals* (Carus Monograph No. 8), 5th Ed. Buffalo: The Mathematical Association of America, 1971.
26. N. H. McCoy, *The Theory of Rings*. New York: Macmillan, 1964.

## Field Theory

27. E. Artin, *Galois Theory* (Notre Dame Mathematical Lecture No. 2), 2nd Ed. Notre Dame, IN: University of Notre Dame Press, 1944.
28. O. Zariski and P. Samuel, *Commutative Algebra*. Princeton, NJ: Van Nostrand, vol. I, 1958.

## Number Theory

29. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* 6th Ed. Oxford: Oxford University Press, 2008.
30. S. Lang, *Algebraic Numbers*. Reading, MA: Addison-Wesley, 1964.
31. W. J. LeVeque, *Elementary Theory of Numbers,* Mineola, NY: Dover, 1990.
32. W. J. LeVeque, *Topics in Number Theory*. Mineola, NY: Dover, 2002.
33. T. Nagell, *Introduction to Number Theory*, 2nd Ed. Providence, RI: American Mathematical Society, 2001.
34. I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, 5th Ed. New York: Wiley, 1991.
35. H. Pollard, *The Theory of Algebraic Numbers* (Carus Monograph No. 9). Buffalo: The Mathematical Association of America; New York: Wiley, 1950.
36. D. Shanks, *Solved and Unsolved Problems in Number Theory*. Washington, DC: Spartan Books, vol. I, 1962.
37. B. M. Stewart, *Theory of Numbers,* 2nd Ed. New York: Macmillan, 1964.
38. J. V. Uspensky and M. H. Heaslet, *Elementary Number Theory*. New York: McGraw-Hill, 1939.
39. E. Weiss, *Algebraic Number Theory*. Mineola, NY: Dover, 1998.

## Homological Algebra

40. J. P. Jans, *Rings and Homology*. New York: Holt, 1964.
41. S. MacLane, *Homology*. Berlin: Springer, 1963.

## Other References

42. A. A. Albert (ed.), *Studies in Modern Algebra* (MAA Studies in Mathematics, vol. 2). Buffalo: The Mathematical Association of America; Englewood Cliffs, NJ: Prentice-Hall, 1963.
43. E. Artin, *Geometric Algebra*. New York: Interscience, 1957.
44. R. Courant and H. Robbins, *What Is Mathematics*? Oxford University Press, 1941.
45. H. S. M. Coxeter, *Introduction to Geometry,* 2nd Ed. New York: Wiley, 1969.
46. R. H. Crowell and R. H. Fox, *Introduction to Knot Theory*. New York: Ginn, 1963.
47. H. B. Edgerton, *Elements of Set Theory*. San Diego: Academic Press, 1977.
48. C. Schumacher, *Chapter Zero*. Reading, MA: Addison-Wesley, 1996.

# Notations

| | |
|---|---|
| $\in, a \in S$ | membership, 1 |
| $\varnothing$ | empty set, 1 |
| $\notin, a \notin S$ | nonmembership, 1 |
| $\{x \mid P(x)\}$ | set of all $x$ such that $P(x)$, 1 |
| $B \subseteq A$ | set inclusion, 2 |
| $B \subset A$ | subset $B \neq A$, 2 |
| $A \times B$ | Cartesian product of sets, 2 |
| $\mathbb{Z}$ | integers, 2 |
| $\mathbb{Q}$ | rational numbers, 2 |
| $\mathbb{R}$ | real numbers, 3 |
| $\mathbb{C}$ | complex numbers, 3 |
| $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ | positive elements of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, 3 |
| $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ | nonzero elements of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, 3 |
| $\mathscr{R}$ | relation, 3 |
| $\lvert A \rvert$ | number of elements in $A$, 3; as order of group, 41 |
| $\phi : A \to B$ | mapping of $A$ into $B$ by $\phi$, 3 |
| $\phi(a)$ | image of element $a$ under $\phi$, 4 |
| $\phi[A]$ | image of set $A$ under $\phi$, 4 |
| $\leftrightarrow$ | one-to-one correspondence, 4 |
| $\phi^{-1}$ | the inverse function of $\phi$, 4 |
| $\aleph_0$ | cardinality of $\mathbb{Z}^+$, 4 |
| $\bar{x}$ | cell containing $x \in S$ in a partition of $S$, 6 |
| $\mathbb{Z}/n\mathbb{Z}$ | residue classes modulo $n_\iota$, 6 |
| $\equiv_n, a \equiv b (\mathrm{mod}\ n)$ | congruence modulo $n$, 6 |
| $\mathscr{P}(A)$ | power set of $A$, 8 |
| $U$ | set of all $z \in \mathbb{C}$ such that $\lvert z \rvert = 1$, 36 |
| $\mathbb{R}_c$ | set of all $x \in \mathbb{R}$ such that $0 \leq x < c$, 33 |
| $+_c$ | addition modulo $c$, 33 |
| $U_n$ | group of $n$th roots of unity, 37 |

| | |
|---|---|
| $\mathbb{Z}_n$ | $\{0, 1, 2, \cdots, n-1\}$, 32 |
| | cyclic group $\{0, 1, \cdots, n-1\}$ under addition modulo $n$, 38 |
| | ring $\{0, 1, \cdots, n-1\}$ under addition and multiplication modulo $n$, 189 |
| $*, a * b$ | binary operation, 11 |
| $\circ, f \circ g, \sigma\tau$ | function composition, 14, 41 |
| $e$ | identity element, 20 |
| $M_{m\times n}(S)$ | $m \times n$ matrices with entries from $S$, 22, 393 |
| $M_n(S)$ | $n \times n$ matrices with entries from $S$, 22, 393 |
| $GL(n, \mathbb{R})$ | general linear group of degree $n$, 22, 23 |
| $\det(A)$ | determinant of square matrix $A$, 28, 395 |
| $a^{-1}, -a$ | inverse of $a$, 15 |
| $H \leq G; K \leq L$ | subgroup inclusion, 52; substructure inclusion, 192 |
| $H < G; K < L$ | subgroup $H \neq G$, 52; substructure $K \neq L$, 192 |
| $\langle a \rangle$ | cyclic subgroup generated by $a$, 56 |
| | principal ideal generated by $a$, 256 |
| $n\mathbb{Z}$ | subgroup of $\mathbb{Z}$ generated by $n$, 56 |
| | subring (ideal) of $\mathbb{Z}$ generated by $n$, 245 |
| $A^T$ | transpose of $A$, 57 |
| gcd | greatest common divisor, 63, 283, 304 |
| $\cap_{i\in I} S_i$, $S_1 \cap S_2 \cap \cdots \cap S_n$ | intersection of sets, 71 |
| $S_A$ | group of permutations of $A$, 43 |
| $\iota$ | identity map, 43 |
| $S_n$ | symmetric group on $n$ letters, 43 |
| $n!$ | $n$ factorial, 43 |
| $D_n$ | $n$th dihedral group, 47 |
| $A_n$ | alternating group on $n$ letters, 84 |
| $aH, a + H$ | left coset of $H$ containing $a$, 98 |
| $Ha, H + a$ | right coset of $H$ containing $a$, 100 |
| $(G : H)$ | index of $H$ in $G$, 137 |
| $\varphi$ | Euler phi-function, 105, 204 |
| $\prod_{i=1}^n B_i$, $B_1 \times B_2 \times \cdots \times B_n$ | Cartesian product of sets, 88 |
| $\prod_{i=1}^n G_i$ | direct product of groups, 88, 89 |
| $\oplus_{i=1}^n G_i$ | direct sum of groups, 89 |
| lcm | least common multiple, 90 |
| $\overline{G}_i$ | natural subgroup of $\prod_{i=1}^n G_i$, 91 |
| $H \leq G$ | $H$ normal subgroup of $G$, 116 |
| $\mathrm{SL}(n, \mathbb{R})$ | special linear group, 117 |
| $\phi_a$ | evaluation homomorphism, 191 |
| $\pi_i$ | projection onto $i$th component, 248 |
| $\phi^{-1}[B]$ | inverse image of the set $B$ under $\phi$, 78 |
| $\mathrm{Ker}(\phi)$ | kernel of homomorphism $\phi$, 78 |
| $G/N; R/N$ | factor group, 117; factor ring, 247 |
| $\gamma$ | canonical residue class map, 118, 119 |
| $i_g$ | inner automorphism, 120 |
| $Z(G)$ | center of the group $G$, 130 |
| $C$ | commutator subgroup, 130 |
| $X_g$ | subset of elements of $X$ fixed by $g$, 136 |
| $G_x$ | isotropy subgroup of elements of $G$ leaving $x$ fixed, 137 |
| $Gx$ | orbit of $x$ under $G$, 143 |
| $R[x]$ | polynomial ring with coefficients in $R$, 220 |
| $R[x_1, x_2, \cdots, x_n]$ | polynomials in $n$ indeterminates, 299 |
| $F(x)$ | field of quotients of $F[x]$, 222 |
| $\mathrm{F}(x_1, \cdots, x_n)$ | field of rational functions in $n$ indeterminates, 223 |

| | |
|---|---|
| $\Phi_p(x)$ | cyclotomic polynomial of degree $p-1$, 236 |
| $\mathrm{End}(A)$ | endomorphisms of $A$, 260 |
| $RG$ | group ring, 262 |
| $FG$ | group algebra over the field $F$, 263 |
| $\mathbb{H}$ | quaternions, 264, 265 |
| ACC | ascending chain condition, 280 |
| $F^n$ | Cartesian product, 299 |
| $F[\mathbf{x}]$ | ring of polynomials in $x_1, \cdots, x_n$ over $F$, 299 |
| $V(S)$ | algebraic variety of polynomials in $S$, 300 |
| $\langle b_1, \cdots, b_r \rangle$ | ideal generated by elements $b_1, \cdots, b_r$, 300 |
| $\mathrm{lt}(f)$ | leading term of the polynomial $f$, 306 |
| $\mathrm{lp}(f)$ | power product of $\mathrm{lt}(f)$, 306 |
| $\mathrm{irr}(\alpha, F)$ | irreducible polynomial for $\alpha$ over $F$, 317 |
| $\deg(\alpha, F)$ | degree of $\alpha$ over $F$, 317 |
| $F(\alpha)$ | field obtained by adjoining $\alpha$ to field $F$, 317 |
| $[E : F]$ | degree of $E$ over $F$, 321 |
| $F(\alpha_1, \cdots, \alpha_n)$ | field obtained by adjoining $\alpha_1, \cdots, \alpha_n$ to $F$, 323 |
| $\overline{F_E}$ | algebraic closure of $F$ in $E$, 325 |
| $\bar{F}$ | an algebraic closure of $F$, 325, 326 |
| $\mathrm{GF}(p^n)$ | Galois field of order $p^n$, 337 |
| $HN$ | product set, 148 |
| $H \vee N$ | subgroup join, 148 |
| $N[H]$ | normalizer of $H$, 152 |
| $F[A]$ | free group on $A$, 175 |
| $(x_j : r_i)$ | group presentation, 181 |
| $a \mid b$ | $a$ divides (is a factor of) $b$, 278 |
| UFD | unique factorization domain, 278 |
| PID | principal ideal domain, 278 |
| $\cup_{i \in I} S_i$, $S_1 \cup S_2 \cup \cdots \cup S_n$ | union of sets, 280 |
| $\nu$ | Euclidean norm, 288 |
| $N(\alpha)$ | norm of $\alpha$, 294, 296 |
| $\psi_{\alpha,\beta}$ | conjugation isomorphism of $F(\alpha)$ with $F(\beta)$, 347 |
| $E_{\{\sigma_i\}}, E_H$ | subfield of $E$ fixed by all $\sigma_i$ or all $\sigma \in H$, 345 |
| $G(E/F)$ | automorphism group of $E$ over $F$, 346 |
| $\lambda(E)$ | automorphisms that fix $E$, 367 |