Abstract Algebra

G. V. V. Sharma

Contents

1 Things Familiar and Less Familiar

1.1 Introduction

1. let S be a set having an operation * which assigns an element a*b of S for any $a, b \in S$. Let us assume that the following two rules hold:
   a) If a, b are any objects in S, then $a * b = a$.
   b) If a, b are any objects in S, then $a * b = b * a$.

   Show that S can have at most one object.
   Solution: From condition 1.1.1a, interchanging a, b,
   $$b * a = b \tag{1.1.1}$$
   and from condition 1.1.1b,
   $$b * a = a * b \tag{1.1.1}$$
   But from condition 1.1.1a,
   $$a * b = a \implies a = b \tag{1.1.1}$$
   Thus, S can have at most one object.
2. Let S be the set of all integers $0, \pm 1, \pm 2, \dots, \pm n, \dots$. For $a, b \in S$, define * by
   $$a * b = a - b \tag{1.1.2}$$
   Verify the following
   a) $a * b \neq b * a$ unless $a = b$
   b) $(a * b) * c \neq a * (b * c)$ in general. Under what conditions on a, b, c is
   $$(a * b) * c \neq a * (b * c) \quad ? \tag{1.1.2}$$
   c) The integer a has the property that $a * 0 = a$ for every $a \in S$.
   d) For $a \in S, a * a = 0$.

   Solution:
   a)
   $$a * b = b * a \tag{1.1.2}$$
   $$\implies a - b = b - a \tag{1.1.2}$$
   $$\text{or, } a = b \tag{1.1.2}$$
   b) Let $a = 1, b = 2, c = 4$. Then,
   $$a * b = -1, (a * b) * c = -1 - 4 = -5 \tag{1.1.2}$$
   $$b * c = -2, a * (b * c) = 1 + 2 = 3 \neq -5 \tag{1.1.2}$$
   Thus, for the given condition to be satisfied,
   $$(a - b) - c = a - (b - c) \tag{1.1.2}$$
   $$\implies c = 0 \tag{1.1.2}$$
   c)
   $$a * 0 = a - 0 = a \tag{1.1.2}$$
   d)
   $$a * a = a - a = 0 \tag{1.1.2}$$
3. Let S consist of the two objects $\square$ and $\triangle$. We define the operatin * on S by subjecting $\square$ and $\triangle$ to the following conditions.
   a) $\square * \triangle = \triangle = \triangle * \square$
   b) $\square * \square = \square$
   c) $\triangle * \triangle = \square$

   Verify by explicit calculation that if a, b, c are any elements of S, (i.e. a, b, c can be any of $\square$ or $\triangle$), then

a) $a * b$ is in S
b) $(a * b) * c = a * (b * c)$
c) $a * b = b * a$
d) There is a particular a in S such that $a * b = b * a = b$ for all $b \in S$
e) Given $b \in S, b * b = a$, where a is the particular element in Part 1.1.3d.

Solution: Let $\square = 1, \triangle = -1$. These satisfy all the given conditions.

a) $a * b \in [1, -1] \in S$.
b) Writing the truth table, $(a * b) * c = a * (b * c)$.
c) $a * b = b * a$ can be verified by writing the truth table.
d) For $a = 1, a * b = b * a = b$, for all $b \in S$.
e) For $a = 1$, if $b = -1, b * b = 1 = a$. This can be shown to be true for $b = 1$ as well.

1.2 Set Theory

1. Describe the following sets verbally
   a) $S = \{\text{Mercury, Venus, Earth, } \dots, \text{ Pluto}\}$
   b) $S = \{\text{Andhra Pradesh, Uttar Pradesh, } \dots, \text{ Assam}\}$

   Solution:
   a) Planets
   b) Indian states
2. Describe the following sets verbally
   a) $S = \{2, 4, 6, 8, \dots\}$
   b) $S = \{2, 4, 8, 16, \dots\}$
   c) $S = \{1, 4, 9, 16, 25, 36 \dots\}$

   Solution:
   a) Even numbers
   b) Powers of 2
   c) Squares of positive integers
3. If A is the set of all residents of India, B the set of all Sri Lankan citizens, and C the set of all women in the world, describe the sets $ABC, A - B, A - C, C - A$ verbally.

   Solution:
   a) ABC is the set of all women residents of India who are citizens of Sri Lanka.
   b) $A - B = AB'$ is the set of all residents of India who are not Sri Lankan citizens.
   c) $A - C = AC'$ is the set of all male residents of India.
   d) $C - A = CA'$ is the set of all women who are not residing in India.
4. If $A = \{1, 4, 7, a\}$ and $B = \{3, 4, 9, 11\}$ and you have been told that $AB = \{4, 9\}$, then what must a be?

   Solution: $a = 9$
5. If $A \subset B, B \subset C$, prove that $A \subset C$

   Solution: From the given information,

$$A + P = B, AP = 0, B + Q = C, BQ = 0 \tag{1.2.5.1}$$

$$\implies B + Q = A + P + Q = C, \tag{1.2.5.2}$$

$\because BQ = 0$,

$$AQ + PQ = 0 \implies AQ = 0, PQ = 0 \tag{1.2.5.3}$$

Hence,

$$A(P + Q) = 0 \implies A \subset C \tag{1.2.5.4}$$

6. If $A \subset B$ prove that $A \cup C \subset B \cup C$ for any set C.

   Solution: From the given information, there exists P such that

$$A + P = B, AP = 0 \tag{1.2.6.1}$$

Also,

$$B + C = A + P + C \tag{1.2.6.2}$$
$$\implies A + C \subset B + C \tag{1.2.6.3}$$

7. Show that

$$A \cup B = B \cup A \tag{1.2.7.1}$$
$$A \cap B = B \cap A \tag{1.2.7.2}$$

8. Prove that

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B) \tag{1.2.8.1}$$

Solution: Since

$$A - B = AB', \tag{1.2.8.2}$$
$$(A - B) \cup (B - A) = AB' + BA' \tag{1.2.8.3}$$

Also,

$$(A \cup B) - (A \cap B) = (A + B)(AB)' \tag{1.2.8.4}$$
$$= (A + B)(A' + B') \tag{1.2.8.5}$$
$$= AB' + BA' \tag{1.2.8.6}$$

9. Prove that

$$(A) \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{1.2.9.1}$$

Solution:

$$LHS = A(B+C) = AB + AC = RHS \tag{1.2.9.2}$$

10. Prove that

$$(A) \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{1.2.10.1}$$

Solution:

$$LHS = A + BC \tag{1.2.10.2}$$
$$RHS = (A+B)(A+C) \tag{1.2.10.3}$$
$$= A + A(B+C) + BC \tag{1.2.10.4}$$
$$= A(1+B+C) + BC \tag{1.2.10.5}$$
$$= LHS \tag{1.2.10.6}$$

11. Write down all the subsets of $S = \{1,2,3,4\}$.
Solution: Write a program for this.
12. If C is a subset of S, let C' denote the complement of C in S. Prove the *De Morgan Rules* for subsets A, B of S, namely,
a) $(A \cup B)' = A' \cap B'$
b) $(A \cap B)' = A' \cup B'$
Solution:
a)

$$(A+B)A'B' = AA'B' + BA'B' \tag{1.2.12.1}$$
$$= 0 \tag{1.2.12.2}$$

b) Substituting $A = A', B = B'$ in the above, the second result is obtained.
13. Let S be a set. For any to subsets of S, we define

$$A \oplus B = (A - B) \cup (B \cup A) \tag{1.2.13.1}$$

Prove that
a) $A \oplus B = B \oplus A$.
b) $A \oplus \Phi = A$.
c) $A \cdot A = A$.
d) $A \oplus A = \Phi$.
e) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.
f) If $A \oplus B = A \oplus C$, then $B = C$.
g) $A \cdot (B + C) = A \cdot B + A \cdot C$.
Solution: All can be proved using boolean logic.
14. If C is a finite set, let $m(C)$ denote the number of elements in C. If A, B are finite sets, prove that

$$m(A \cup B) = m(A) + m(B) - m(A \cap B) \tag{1.2.14.1}$$

Solution:

$$A'B' = (A+B)' \tag{1.2.14.2}$$
$$\implies m(A'B') = m((A+B)') \tag{1.2.14.3}$$
$$= 1 - m(A+B) \tag{1.2.14.4}$$

$$\because A + B = A(B+B') + B \tag{1.2.14.5}$$
$$= B(A+1) + AB' \tag{1.2.14.6}$$
$$= B + AB' \tag{1.2.14.7}$$
$$\implies m(A+B) = m(B+AB') \tag{1.2.14.8}$$
$$= m(B) + m(AB') \tag{1.2.14.9}$$
$$\because B(AB') = 0 \tag{1.2.14.10}$$

$$A = A(B+B') = AB + AB' \tag{1.2.14.11}$$

and

$$(AB)(AB') = 0, \because BB' = 0 \tag{1.2.14.12}$$

Hence, AB and AB' are mutually exclusive and

$$m(A) = m(AB) + m(AB') \tag{1.2.14.13}$$
$$\implies m(AB') = m(A) - m(AB) \tag{1.2.14.14}$$

Substituting (1.2.14.14) in (1.2.14.10),

$$m(A+B) = m(A) + m(B) - m(AB) \tag{1.2.14.15}$$

15. For three finite sets A, B, C, find a formula for $m(A \cup b \cup C)$. **Solution:** Extend the above.
16. Take a shot at finding $m\left(\cup_{i=1}^{n} A_i\right)$.
17. Show that if 80% of all Indians have gone to high school and 70% of all Indians read a daily newspaper, then *at least* 50% of all Indians have both gone to high school and read a daily newspaper.
Solution: Let A represent high school and B represent newspaper. Then,

$$\Pr(AB) = \Pr(A) + \Pr(B) - \Pr(A+B) \tag{1.2.17.1}$$

Since

$$\Pr(A+B) \le 1, \tag{1.2.17.2}$$
$$\Pr(A) + \Pr(B) - \Pr(A+B) \ge \Pr(A) + \Pr(B) - 1 \tag{1.2.17.3}$$
$$\implies \Pr(AB) \ge 0.8 + 0.7 - 1 \tag{1.2.17.4}$$
$$= 0.5 \tag{1.2.17.5}$$

18. A public opinion poll shows that 90% of the population agreed with the government on the first decision, 84% on the second, and 74% on the third, for three decisions made by the government. At least what percentage of the population agreed with the government on all three decisions.

Solution: Let the decisions be A, B, C. Then,

$$\Pr(AB) \geq \Pr(ABC), \tag{1.2.18.1}$$
$$\Pr(BC) \geq \Pr(ABC), \tag{1.2.18.2}$$
$$\Pr(CA) \geq \Pr(ABC) \tag{1.2.18.3}$$

Since

$$\begin{aligned} \Pr(A+B+C) &= \sum \Pr(A) \\ &\quad - \sum \Pr(AB) + \Pr(ABC), \\ \implies \Pr(A+B+C) &+ \sum \Pr(AB) \\ &= \sum \Pr(A) + \Pr(ABC), \end{aligned} \tag{1.2.18.4}$$

from (1.2.18.1),

$$\begin{aligned} &\Pr(A+B+C) + 3\Pr(ABC) \\ &\quad \geq \sum \Pr(A) + \Pr(ABC), \\ \implies &2\Pr(ABC) \geq \sum \Pr(A) - \Pr(A+B+C) \end{aligned} \tag{1.2.18.5}$$

Since

$$\Pr(A+B+C) \leq 1, \tag{1.2.18.6}$$
$$-\Pr(A+B+C) \geq -1 \tag{1.2.18.7}$$
$$\implies 2\Pr(ABC) \geq \sum \Pr(A) - 1 \tag{1.2.18.8}$$
$$\text{or} \Pr(ABC) \geq \frac{\sum \Pr(A) - 1}{2} \tag{1.2.18.9}$$
$$= 0.74 \tag{1.2.18.10}$$

19. In his book *A Tangled Tale*, Lewis Caroll proposed the following riddle about a group of disabled veterans. "Say that 70% have lost an eye, 75% an ear, 80% an arm, 85% a leg. What percentage, at least, must have lost all four?" Solve Lewis Caroll's problem.

Solution: Let A_i represent the events. Then,

$$\begin{aligned} \Pr\left(\sum_{i=1}^{4} A_i\right) &= \sum_{i=1}^{4} \Pr(A_i) - \sum_{i,j} \Pr\left(A_i A_j\right) \\ &+ \sum_{i,j,k} \Pr\left(A_i A_j A_k\right) - \Pr\left(\prod_{i=1}^{4} A_i\right) \end{aligned} \tag{1.2.19.1}$$

Now,

$$\Pr(A_1A_2) \geq \Pr(A_1A_2A_3) \geq \Pr(A_1A_2A_3A_4) \tag{1.2.19.2}$$

which, upon substitution in (1.2.19.1) yields

$$\Pr\left(\sum_{i=1}^{4} A_i\right) \geq \frac{\sum_{i=1}^{4} \Pr(A_i) - 1}{1 + {}^4C_2 - {}^4C_3} \tag{1.2.19.3}$$
$$= 70\% \tag{1.2.19.4}$$

20. Show, for finite sets A, B, that $m(A \times B) = m(A) \times m(B)$.

Solution: Basic principle of counting.

21. If S is a set having five elements,
   a) How many subsets does S have?
   b) How many subsets having four elements does S have?
   c) How many subsets having two elements does S have?

   Solution:
   a) $2^5 = 32$.
   b) ${}^5C_4 = 5$.
   c) ${}^5C_2 = 10$.

22. a) Show that a set having n elements has 2^n subsets.
   b) If $0 < m < n$, how many subsets are there that have exactly m elements?

   Solution:
   a) The number of subsets is

$$\sum_{k=0}^{n} {}^nC_k = 2^n \tag{1.2.22.1}$$

   using the binomial theorem.
   b) The number of subsets having exactly m elements are ${}^nC_m$.

1.3 Mappings

1. For the given sets S, T determine if a mapping $f : S \to T$ is clearly and unambiguously defined; if not, say why not.
   a) S = set of all women, T = set of all men, $f(s)$ = husband of s.
   b) S = set of all positive integers, $T = S$, $f(s) = s - 1$.
   c) S = set of positive integers, T = set of nonnegative integers, $f(s) = s - 1$.
   d) S = set of nonnegative integers, $T = S$, $f(s) = s - 1$.

e) S = set of all integers, $T = S, f(s) = s - 1$.
f) S =set of all real numbers, $T = S, f(s) = \sqrt{s}$.
g) S = set of all positive real numbers, $T = S, f(s) = \sqrt{s}$.

Solution:

a) Not all women have husbands. So the mapping is not clearly defined.
b) For every integer $s, s-1$ is an integer. So the mapping is defined.
c) $0 \notin S$, so the mapping is defined.
d) $f(0) = -1 \notin S$. So the mapping is not defined.
e) $f(-1) \notin S$, so the mapping is not defined.
f) $f(s) \in S \forall S$. So the mapping is defined.

2. In those parts of Problem 1.3.1 where f does define a function, determine if it is 1-1, onto, or both. **Solution:**

a) For $f(s) = s - 1, s \in \mathbb{Z}$, the mapping is a bijection.
b) For $s \in \mathbb{N}, f(s) = s - 1 \in \mathbb{W}$, the mapping is a bijection.
c) For $s \in S, f(s) \in S$ and vice-versa. So the mapping is a bijection.

3. If f is a 1-1 mapping of S onto T, prove that f^{-1} is a 1-1 mapping of T onto S.
Solution: By definition,

$$s_1 = s_2 \in S \implies f(s_1) = f(s_2) \in T$$
$$t_1 = t_2 \in T \implies \exists s_1 = s_2 \in S \ni f(s_1) = f(s_2). \tag{1.3.3.1}$$

Let $g = f^{-1}$. Then,

$$f(s_i) = t_i \implies g(t_i) = s_i. \tag{1.3.3.2}$$

From (1.3.3.1),

$$\begin{aligned} g(t_1) = g(t_2) \in S &\implies t_1 = t_2 \in T \\ t_1 = t_2 \in T &\implies \exists g(t_1) = g(t_2) \in S \end{aligned} \tag{1.3.3.3}$$

(1.3.3.3) shows that $g = f^{-1}$ is also 1-1.

4. If f is a 1-1 mapping of S onto T, prove that $f^{-1} \circ f = i_S$.
Solution: For $s \in S, t \in T$,

$$f(s) = t \implies g(t) = s \tag{1.3.4.1}$$
$$\text{or, } g \circ f(s) = s \implies (g \circ f) = i_S \quad \square \tag{1.3.4.2}$$

5. If $g : S \to T$ and $f : T \to U$ are both onto, then $f \circ g : S \to U$ is also onto.

Solution: From the given information,

$$g(S) = T, f(T) = U \tag{1.3.5.1}$$
$$\implies (f \circ g)(S) = U \quad \square \tag{1.3.5.2}$$

6. If $f : S \to T$ is onto and $g : T \to U$ and $h : T \to U$ are such that $g \circ f = h \circ f$, prove that $g = h$.
Solution: From the given information,

$$g \circ f - h \circ f = 0 \tag{1.3.6.1}$$
$$\implies (g - h) \circ f = 0 \tag{1.3.6.2}$$
$$\text{or, } g = h \tag{1.3.6.3}$$

7. If $g : S \to T, h : S \to T$, and if $f : T \to U$ is 1-1, show that if $f \circ g = f \circ h$, then $g = h$.
8. Let S be the set of all integers and $T = \{1, -1\}$; $f : S \to T$ is defined by

$$f(s) = \begin{cases} 1 & s \text{ even} \\ -1 & s \text{ odd} . \end{cases} \tag{1.3.8.1}$$

a) Does this define a function from S to T?
b) Show that

$$f(s_1 + s_2) = f(s_1) f(s_2) \tag{1.3.8.2}$$

What does this say about the integers?
c) Is $f(s_1 s_2) = f(s_1) f(s_2)$ also true?

Solution:

a) Yes, f is a function.
b) See Table 1.3.8.

$f(s_1)$	$f(s_2)$	$f(s_1) + f(s_2)$
1	1	1
1	-1	-1
-1	-1	1
-1	1	-1

TABLE 1.3.8

c) No. If s_1, s_2 are odd,

$$s_1 s_2 \text{ odd} \tag{1.3.8.3}$$
$$f(s_1 s_2) = -1 \neq f(s_1) f(s_2) \tag{1.3.8.4}$$

9. Let S be the set of all real numbers. Define

$$f : S \to S | f(s) = s^2, \tag{1.3.9.1}$$
$$g : S \to S | g(s) = s + 1, \tag{1.3.9.2}$$

a) Find $f \circ g$.

b) Find $g \circ f$.
c) Is $f \circ g = g \circ f$?

Solution:

a)

$$(f \circ g)(s) = (s+1)^2 \tag{1.3.9.3}$$

b)

$$(g \circ f)(s) = s^2 + 1 \tag{1.3.9.4}$$

c) From (1.3.9.4) and (1.3.9.4) $f \circ g \neq g \circ f$.

10. Let S be the set of all real numbers and for $a, b \in S$, where $a \neq 0$; define $f_{a,b}(s) = as + b$.
   a) Show that $f_{a,b} \circ f_{c,d} = f_{u,v}$ for some real u, v. Give explicit values for u, v in terms of a, b, c and d.
   b) Is $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b}$ always?
   c) Find all $f_{a,b}$ such that $f_{a,b} \circ f_{1,1} = f_{1,1} \circ f_{a,b}$.
   d) Show that f^{-1} exists and find its form.

   Solution:

   a)

$$f_{a,b} \circ f_{c,d} = c\,(as+b) + d \tag{1.3.10.1}$$
$$= cas + cb + d \tag{1.3.10.2}$$
$$= us + v \tag{1.3.10.3}$$
$$\implies u = ca, v = bc + d \tag{1.3.10.4}$$

   b) From (1.3.10.1),

$$f_{c,d} \circ f_{a,b} = cas + ad + b \tag{1.3.10.5}$$

   Thus, from (1.3.10.1) and (1.3.10.5)

$$f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b} \tag{1.3.10.6}$$
$$\implies bc + d = ad + b \tag{1.3.10.7}$$

   c) From (1.3.10.7),

$$f_{a,b} \circ f_{1,1} = f_{1,1} \circ f_{a,b} \tag{1.3.10.8}$$
$$\implies as + b + 1 = as + a + b \tag{1.3.10.9}$$
$$\text{or, } a = 1. \tag{1.3.10.10}$$

   Thus,

$$f_{a,b} = s + b \tag{1.3.10.11}$$

   d) From the definition,

$$f_{a,b}(s) = as + b \tag{1.3.10.12}$$
$$\implies s = \frac{f_{a,b}(s) - b}{a} \tag{1.3.10.13}$$
$$\text{or, } f_{a,b}^{-1}(s) = \frac{s-b}{a} \tag{1.3.10.14}$$

11. Let S be the set of all positive integers. Define $f : S \to S$ by $f(1) = 2, f(2) = 3, f(3) = 1$ and $f(s) = s$ for any other $s \in S$. Show that $fofof = i_S$. What is f^{-1} in this case?

   Solution: For $s \in \{1, 2, 3\}$, it is obvious. For $s \notin \{1, 2, 3\}$,

$$(f \circ f)(s) = f(s) = s \tag{1.3.11.1}$$
$$\implies (f \circ f \circ f)(s) = s \quad \square \tag{1.3.11.2}$$

   It is easy to verify that

$$f^{-1}(s) = f(s) = ss \notin (1, 2, 3) \tag{1.3.11.3}$$

   Also,

$$f^{-1}(2) = f(1), f^{-1}(3) = f(2), f^{-1}(1) = f(3), \tag{1.3.11.4}$$

1.4 $A(S)$ (The set of 1-1 mappings of S onto itself)

1. If $s1 \neq s_2$ are in S, show that there is an $f \in A(S)$ such that $f(s_1) = s_2$.

   Solution: By definition of a 1-1 mapping, it is obvious.

2. If $s_1 \in S$, let $H = \{f \in A(S) \mid f(s_1) = s_1\}$. Show that:
   a) $i \in H$.
   b) If $f, g \in H$, then $fg \in H$.
   c) If $f \in H$, then $f^{-1} \in H$.

   Solution:

   a) $\because i(s_1) = s_1, i \in H$.
   b) $fg(s_1) = f(s_1) = s_1$.
   c) $f(s_1) = s_1 \implies f^{-1}(s_1) = s_1 \implies f^{-1} \in H$.

3. Suppose that $s_1 \neq s_2$ are in S and $f(s_1) = s_2$, where $f \in A(S)$. Then if H is as in Problem 1.4.2 and $K = \{g \in A(S) \mid g(s_2) = s_2\}$, show that:
   a) If $g \in K$, then $f^{-1}gf \in H$.
   b) If $h \in H$, then there is some $g \in K$ such that $h = f^{-1}gf$.

   Solution:

   a) From the given information,

$$f^{-1}gf(s_1) = f^{-1}g(s_2) = f^{-1}(s_2) = s_1 \tag{1.4.3.1}$$

Hence,

$$f^{-1}gf \in H \qquad (1.4.3.2)$$

b) The h was found in the previous part.

4. If $f, g, h \in A(S)$, show that $(f^{-1}gf)(f^{-1}hf) = f^{-1}(gh)f$. What can you say about $(f^{-1}gf)^n$?
Solution: From the given information,

$$(f^{-1}gf)(f^{-1}hf) = f^{-1}g\left(ff^{-1}\right)hf \qquad (1.4.4.1)$$
$$= f^{-1}(gh)f \qquad (1.4.4.2)$$

Similarly,

$$\left(f^{-1}gf\right)^n = f^{-1}g^n f \qquad (1.4.4.3)$$

5. If $f, g \in A(S)$ and $fg = gf$, show that:
a) $(fg)^2 = f^2g^2$.
b) $(fg)^{-1} = f^{-1}g^{-1}$.
Solution: From the given information,
a)

$$(fg)^2 = (fg)(fg) \qquad (1.4.5.1)$$
$$= (fg)(gf) = fg^2f \qquad (1.4.5.2)$$
$$= f\left(fg^2\right) = f^2g^2 \qquad (1.4.5.3)$$

b) Since

$$(fg)^{-1}fg = i, \qquad (1.4.5.4)$$
$$(fg)^{-1}fgg^{-1} = g^{-1} \qquad (1.4.5.5)$$
$$\implies (fg)^{-1}f = g^{-1} \qquad (1.4.5.6)$$
$$\implies (fg)^{-1}ff^{-1} = g^{-1}f^{-1} \qquad (1.4.5.7)$$
$$\text{or, } (fg)^{-1} = g^{-1}f^{-1} \qquad (1.4.5.8)$$

6. Push the result of Problem 1.4.5 , for the same f and g, to show that

$$(fg)^m = f^mg^m \qquad (1.4.6.1)$$

for all integers m.
Solution: Using induction,

$$(fg)^{m+1} = (fg)^m(fg) \qquad (1.4.6.2)$$
$$= f^mg^mfg = f^mg^mgf \qquad (1.4.6.3)$$
$$= ff^mg^mg \qquad (1.4.6.4)$$

yielding (1.4.6.1).

7.

8. If $f, g \in A(S)$ and $(fg)^2 = f^2g^2$, prove that $fg = gf$.
Solution:

$$(fg)^2 = f^2g^2 \qquad (1.4.8.1)$$
$$\implies fgfg = ffgg \qquad (1.4.8.2)$$
$$\implies f^{-1}fgfg = f^{-1}ffgg \qquad (1.4.8.3)$$
$$\implies gfg = fgg \qquad (1.4.8.4)$$
$$\implies gfgg^{-1} = fggg^{-1} \qquad (1.4.8.5)$$

yielding the desired result.

1.5 The Integers

1. Find (a, b) and express (a, b) as $ma + nb$ for
a) $(116, -84)$
b) $(85, 65)$
c) $(72, 26)$
d) $(72, 25)$
Solution:
a) Using the extended Euclid algorithm,

$$\begin{pmatrix} 116 & 1 & 0 \\ -84 & 0 & 1 \end{pmatrix} \qquad (1.5.1.1)$$
$$\xleftrightarrow{R_3 \leftarrow R_1 + R_2} \begin{pmatrix} 32 & 1 & 1 \end{pmatrix} \qquad (1.5.1.2)$$
$$\xleftrightarrow{R_4 \leftarrow R_2 + 2R_3} \begin{pmatrix} -20 & 2 & 3 \end{pmatrix} \qquad (1.5.1.3)$$
$$\xleftrightarrow{R_5 \leftarrow R_4 + R_3} \begin{pmatrix} 12 & 3 & 4 \end{pmatrix} \qquad (1.5.1.4)$$
$$\xleftrightarrow{R_6 \leftarrow R_5 + R_4} \begin{pmatrix} -8 & 5 & 7 \end{pmatrix} \qquad (1.5.1.5)$$
$$\xleftrightarrow{R_7 \leftarrow R_6 + R_5} \begin{pmatrix} 4 & 8 & 11 \end{pmatrix} \qquad (1.5.1.6)$$
$$\xleftrightarrow{R_8 \leftarrow R_7 + 2R_6} \begin{pmatrix} 0 & 21 & 29 \end{pmatrix} \qquad (1.5.1.7)$$

Thus,

$$4 = (8)116 + 11(-84) \qquad (1.5.1.8)$$

b)

$$\begin{pmatrix} 85 & 1 & 0 \\ 65 & 0 & 1 \end{pmatrix} \qquad (1.5.1.9)$$
$$\xleftrightarrow{R_3 \leftarrow R_1 - R_2} \begin{pmatrix} 20 & 1 & -1 \end{pmatrix} \qquad (1.5.1.10)$$
$$\xleftrightarrow{R_4 \leftarrow R_2 - 3R_3} \begin{pmatrix} 5 & -3 & 4 \end{pmatrix} \qquad (1.5.1.11)$$
$$\xleftrightarrow{R_5 \leftarrow R_3 - 4R_4} \begin{pmatrix} 0 & 13 & -17 \end{pmatrix} \qquad (1.5.1.12)$$

Thus,

$$5 = (-3)85 + 4(65) \qquad (1.5.1.13)$$

c)

$$\begin{pmatrix} 72 & 1 & 0 \\ 26 & 0 & 1 \end{pmatrix} \quad (1.5.1.14)$$

$$\xleftrightarrow{R_3 \leftarrow R_1 - 2R_2} \begin{pmatrix} 20 & 1 & -2 \end{pmatrix} \quad (1.5.1.15)$$

$$\xleftrightarrow{R_4 \leftarrow R_2 - R_3} \begin{pmatrix} 6 & -1 & 3 \end{pmatrix} \quad (1.5.1.16)$$

$$\xleftrightarrow{R_5 \leftarrow R_3 - 3R_4} \begin{pmatrix} 2 & 4 & -11 \end{pmatrix} \quad (1.5.1.17)$$

$$\xleftrightarrow{R_6 \leftarrow R_4 - 3R_5} \begin{pmatrix} 0 & -13 & 36 \end{pmatrix} \quad (1.5.1.18)$$

Thus,

$$2 = (4)72 + (-11)26 \quad (1.5.1.19)$$

d)

$$\begin{pmatrix} 72 & 1 & 0 \\ 25 & 0 & 1 \end{pmatrix} \quad (1.5.1.20)$$

$$\xleftrightarrow{R_3 \leftarrow R_1 - 2R_2} \begin{pmatrix} 22 & 1 & -2 \end{pmatrix} \quad (1.5.1.21)$$

$$\xleftrightarrow{R_4 \leftarrow R_2 - R_3} \begin{pmatrix} 3 & -1 & 3 \end{pmatrix} \quad (1.5.1.22)$$

$$\xleftrightarrow{R_5 \leftarrow R_3 - 7R_4} \begin{pmatrix} 1 & 8 & -23 \end{pmatrix} \quad (1.5.1.23)$$

Thus,

$$1 = (8)72 + (-23)25 \quad (1.5.1.24)$$

2. Show that the following are true
   a) $1 \mid n$ for all n .
   b) If $m \neq 0$, then $m \mid 0$.
   c) If $m \mid n$ and $n \mid q$, then $m \mid q$.
   d) If $m \mid n$ and $n \mid q$, then $m \mid (un + vq)$ for all v, u.
   e) If $m \mid 1$, then $m = 1$ or $m = -1$.
   f) If $m \mid n$, and $n \mid m$, then $m = \pm n$.

   Solution:
   a) $n = 1 \times n$.
   b) $0 = 0 \times m$.
   c) Let

   $$n = cm, q = dn. \quad (1.5.2.1)$$

   Then

   $$q = (cdn)m \implies m \mid q \quad (1.5.2.2)$$

   d) Let

   $$n = cm, q = dn. \quad (1.5.2.3)$$

   Then

   $$un + vq = ucm + vdn \quad (1.5.2.4)$$
   $$= (uc + vdc)m \quad (1.5.2.5)$$
   $$\implies m \mid (un + vq) \quad (1.5.2.6)$$

   e) If

   $$1 = cm, \quad (1.5.2.7)$$
   $$c = 1, m = 1 \quad (1.5.2.8)$$
   $$c = -1, m = -1 \quad (1.5.2.9)$$

   f)

   $$n = cm, m = dn \quad (1.5.2.10)$$
   $$\implies mn = cdmn \quad (1.5.2.11)$$
   $$\text{or, } cd = 1 \quad (1.5.2.12)$$

   Thus, either

   $$c = d = 1, \implies n = m, \quad (1.5.2.13)$$
   $$\text{or, } c = d = -1, \implies n = -m \quad (1.5.2.14)$$

3. Show that

   $$(ma, mb) = m\,(a, b) \quad m > 0. \quad (1.5.3.1)$$

   Solution: Let

   $$(a, b) = xa + yb \quad (1.5.3.2)$$

   Then,

   $$(ma, mb) = xma + ymb = m\,(xa + yb) \quad (1.5.3.3)$$
   $$= m\,(a, b) \quad (1.5.3.4)$$

4. Show that if $a \mid m$ and $b \mid m$, and $(a, b) = 1$, then $(ab) \mid m$.
   Solution: From the given information,

   $$\begin{aligned} m &= ac, \\ m &= bd, \end{aligned} \quad (1.5.4.1)$$
   $$ax + by = 1 \quad (1.5.4.2)$$

   Multiplying both sides of (1.5.4.2) by m

   $$max + mby = m \quad (1.5.4.3)$$
   $$\implies ab\,(dx + cy) = m \quad (1.5.4.4)$$

   upon substituting from (1.5.4.1). Hence, $(ab) \mid m$.

5. Factor the following into primes
   a) 36
   b) 120

c) 720
d) 5040

Solution:

a) $36 = 2^2 \times 3^2$.
b) $120 = 2^3 \times 3 \times 5$.
c) $720 = 2^4 \times 3^2 \times 5$.
d) $5040 = 2^2 \times 3^2 \times 5 \times 7$.

6. If $m = p_1^{a_1} \dots p_k^{a_k}$, and $n = p_1^{b_1} \dots p_k^{b_k}$, where p_i are distinct primes and a_i, b_i are nonnegative, express (m, n) as $p_1^{c_1} \dots p_k^{c_k}$ by describing the cs in terms of the as and bs.
Solution: Let

$$m = 36 = 2^2 \times 3^2 \tag{1.5.6.1}$$
$$n = 720 = 2^4 \times 3^2 \times 5 \tag{1.5.6.2}$$

Then,

$$k = 3 \tag{1.5.6.3}$$
$$p_1 = 2, p_2 = 3, p_3 = 5 \tag{1.5.6.4}$$
$$a_1 = 2, a_2 = 2, a_3 = 0 \tag{1.5.6.5}$$
$$b_1 = 4, b_2 = 2, b_3 = 1 \tag{1.5.6.6}$$

and

$$(36, 720) = 2^2 \times 3^2 \tag{1.5.6.7}$$
$$\implies c_i = \min(a_i, b_i) \tag{1.5.6.8}$$

7. Define the least common multiplie (LCM) of positive integers m and n to be the smallest positive integer v such that both $m \mid v$ and $n \mid v$.
a) Show that
$$v = \frac{mn}{(m, n)} \tag{1.5.7.1}$$
b) In terms of the factorization of m and n given in problem 1.5.6 what is v?

8. Find the least common multiples of the following pairs
a) $(116, -84)$
b) $(85, 65)$
c) $(72, 26)$
d) $(72, 25)$

Solution:

a) 2436.
b) 1105.
c) 936.
d) 1800.

9. If $m, n > 0$ are two integers, show that we can find integers u, v with $-\frac{n}{2} \leq v \leq \frac{n}{2}$ such that $m = un + v$.

10. To check that a given integer $n > 1$ is a prime, prove that it is enough to show that n is not divisible by any prime p with $p \leq \sqrt{n}$.

1.6 Mathematical Induction

1. Prove that
$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6} \tag{1.6.1.1}$$
by induction.
Solution: $P(n+1)$ is
$$\begin{aligned} &1^2 + 2^2 + 3^2 + \dots + n^2 + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= (n+1)\left(\frac{2n^2 + 7n + 7}{6}\right) \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned} \tag{1.6.1.2}$$
which is true. Hence, the given proposition is true for all $n \geq 1$

2. Prove that
$$1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2}\right]^2 \tag{1.6.2.1}$$
by induction.
Solution: $P(n+1)$ is
$$\begin{aligned} &1^3 + 2^3 + 3^3 + \dots + n^3 + (n+1)^3 \\ &= \left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 \\ &= (n+1)^2\left(\frac{n^2 + 4n + 4}{4}\right) \\ &= \left[\frac{(n+1)(n+2)}{2}\right]^2 \end{aligned} \tag{1.6.2.2}$$
which is true. Hence, the given proposition is true for all $n \geq 1$.

3. Prove that a set having $n \geq 2$ elements has $\frac{n(n-1)}{2}$ subsets having exactly 2 elements.
4. Prove that a set having $n \geq 3$ elements has $\frac{n(n-1)(n-2)}{3}$ subsets having exactly 3 elements.
5. If $n \geq 4$ and S is a set having n elements, guess how many subsets having exactly 4 elements are there in S. Then verify your guess using mathematical induction.

6. If p is a prime and $p \mid (a_1 a_2 a_3 \ldots a_n)$, then prove using induction that $p \mid a_i$ for some i with $1 \leq i \leq n$.
7. If $a \neq 1$, prove that
$$1 + a + a^2 + \cdots + a^n = \frac{\left(a^{n+1} - 1\right)}{a - 1} \quad (1.6.7.1)$$
by induction.
Solution: $P(n+1)$ can be expressed as
$$\begin{aligned} 1 + a + a^2 + \cdots + a^n + a^{n+1} \\ &= \frac{\left(a^{n+1} - 1\right)}{a - 1} + a^{n+1} \\ &= \frac{\left(a^{n+2} - 1\right)}{a - 1} \quad (1.6.7.2) \end{aligned}$$
upon simplification. Hence, the given proposition is true for all $n \geq 1$.
8. By induction, show that
$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1} \quad (1.6.8.1)$$
Solution: $P(n+1)$ can be expressed as
$$\begin{aligned} \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n \cdot (n+1)} + \frac{1}{(n+1) \cdot (n+2)} \\ &= \frac{n}{n+1} + \frac{1}{(n+1) \cdot (n+2)} \\ &= \frac{1}{n+1}\left[n + \frac{1}{n+2}\right] \\ &= \frac{n+1}{n+2} \quad (1.6.8.2) \end{aligned}$$
upon simplification. Hence, the given proposition is true for all $n \geq 1$.
9. Suppose that $P(n)$ is a proposition about positive integers n such that $P(n_0)$ is valid, and if $P(k)$ is true, so must be $P(k+1)$. What can you say about $P(n)$? Prove your statement.
10. Let $P(n)$ be a proposition about integers n such that $P(1)$ is true and such that if $P(j)$ is true for all positive integers $j < k$, then $P(k)$ is true. Prove that $P(n)$ is true for all positive integers n.
11. Given an example of a proposition that is *not* true for any positive integer, yet for which the induction step holds.
12. Prove by induction that a set having n elements has exactly 2^n subsets.
Solution: Let $S = \{1, 2\}$. Then the subsets are
$$\{\phi\}, \{1\}, \{2\}, \{1, 2\} \quad (1.6.12.1)$$
For $S = \{1, 2, 3\}$, the subsets are
$$\{\phi\}, \{1\}, \{2\}, \{1, 2\} \quad (1.6.12.2)$$
$$\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \quad (1.6.12.3)$$
Thus $P(n+1)$ can be expressed as
$$2^n + 2^n = 2^{n+1} \quad (1.6.12.4)$$
Hence, the given proposition is true for all $n \geq 1$.
13. Prove by induction on n that $n^3 - n$ is always divisible by 3.
Solution: $P(n+1)$ can be expressed as
$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 \quad (1.6.13.1)$$
$$= n^3 - n + 3\left(n^2 + n\right) \quad (1.6.13.2)$$
which is divisible by 3. Hence, the given proposition is true for all $n \geq 1$.
14. If p is a prime number, then prove that $n^p - n$ is always divisible by p.
Solution: $P(n+1)$ can be expressed as
$$(n+1)^p - (n+1) = n^p - n + p \sum_{k=1}^{n-1} {}^nC_k p^{k-1} \quad (1.6.14.1)$$
$$\implies p \mid \left[(n+1)^p - (n+1)\right] \quad (1.6.14.2)$$
Hence, the given proposition is true for all $n \geq 1$
15. Prove by induction that for a set having n elements the number of $1-1$ mappings of this set onto itself is $n!$.
Solution: Let $S = \{a, b, c\}$. Then the possible 1-1 onto mappings are
$$\begin{cases} a \mapsto b \\ b \mapsto c \\ c \mapsto a \end{cases} \begin{cases} a \mapsto b \\ b \mapsto a \\ c \mapsto c \end{cases} \begin{cases} a \mapsto c \\ b \mapsto b \\ c \mapsto a \end{cases} \begin{cases} a \mapsto a \\ b \mapsto c \\ c \mapsto b \end{cases} \begin{cases} a \mapsto a \\ b \mapsto b \\ c \mapsto c \end{cases} \begin{cases} a \\ b \\ c \end{cases} \quad (1.6.15.1)$$

1.7 Complex Numbers

1. Multiply
   a) $(6-7\jmath)(8+\jmath)$
   b) $\left(\frac{2}{3}+\frac{3}{2}\jmath\right)\left(\frac{2}{3}-\frac{3}{2}\jmath\right)$
   c) $(6+7\jmath)(8-\jmath)$

   Solution:

   a)
$$(6-7\jmath)(8+\jmath) = \begin{pmatrix} 6 & 7 \\ -7 & 6 \end{pmatrix}\begin{pmatrix} 8 \\ 1 \end{pmatrix} \tag{1.7.1.1}$$
$$= \begin{pmatrix} 53 \\ -50 \end{pmatrix} = 53 - 50\jmath \tag{1.7.1.2}$$

   b)
$$\left(\frac{2}{3}+\frac{3}{2}\jmath\right)\left(\frac{2}{3}-\frac{3}{2}\jmath\right) = \begin{pmatrix} \frac{2}{3} & -\frac{3}{2} \\ \frac{3}{2} & \frac{2}{3} \end{pmatrix}\begin{pmatrix} \frac{2}{3} \\ -\frac{3}{2} \end{pmatrix} \tag{1.7.1.3}$$
$$= \begin{pmatrix} \frac{97}{36} \\ 0 \end{pmatrix} = \frac{97}{36} \tag{1.7.1.4}$$

   c)
$$(6+7\jmath)\,8-\jmath = \left[(6-7\jmath)\,8+\jmath\right]^* \tag{1.7.1.5}$$
$$= (53-50\jmath)^* = 53+50\jmath \tag{1.7.1.6}$$

2. Find z^{-1} for
   a) $z = 6+8\jmath$
   b) $z = 6-8\jmath$
   c) $z = \frac{1}{\sqrt{2}}(1+\jmath)$

   Solution:

   a)
$$z^{-1} = \frac{z^*}{|z|^2} = \frac{6-8\jmath}{100} \tag{1.7.2.1}$$

   b)
$$z^{-1} = \frac{6+8\jmath}{100} \tag{1.7.2.2}$$

   c)
$$z^{-1} = \frac{1-\jmath}{\sqrt{2}} \tag{1.7.2.3}$$

3. Show that
$$(z^*)^{-1} = \left(z^{-1}\right)^* \tag{1.7.3.1}$$

   Solution: Since
$$zz^{-1} = 1, \tag{1.7.3.2}$$
$$\left(zz^{-1}\right)^* = 1 \tag{1.7.3.3}$$
$$\implies (z)^*\left(z^{-1}\right)^* = 1 \tag{1.7.3.4}$$

   yielding (1.7.3.1).

4. Find
$$(\cos\theta + \jmath\sin\theta)^{-1} \tag{1.7.4.1}$$

   Solution:
$$(\cos\theta + \jmath\sin\theta)^{-1} = \cos\theta - \jmath\sin\theta \tag{1.7.4.2}$$

5. Verify the following
   a) $(z^*)^* = z$
   b) $(z+w)^* = z^* + w^*$
   c) $z + z^* = 2\text{Re}\,(z)$
   d) $z - z^* = 2\jmath\text{Im}\,(z)$

   Solution:

   a) For
$$z = a + \jmath b, \tag{1.7.5.1}$$
$$z^* = a - \jmath b, \tag{1.7.5.2}$$
$$\implies (z^*)^* = a + \jmath b = z \tag{1.7.5.3}$$

   b) For
$$\begin{aligned} z &= z_1 + \jmath z_2 \\ w &= w_1 + \jmath w_2, \end{aligned} \tag{1.7.5.4}$$
$$(z+w)^* = (z_1 + \jmath z_2 + w_1 + \jmath w_2)^* \tag{1.7.5.5}$$
$$= (z_1 - \jmath z_2) + (w_1 - \jmath w_2) \tag{1.7.5.6}$$
$$= z^* + w^* \tag{1.7.5.7}$$

   c) For
$$z = a + \jmath b, \tag{1.7.5.8}$$
$$z^* = a - \jmath b, \tag{1.7.5.9}$$
$$\implies (z + z^*) = a + \jmath b + a - \jmath b \tag{1.7.5.10}$$
$$= 2a = 2\text{Re}\,(z) \tag{1.7.5.11}$$

   d) For
$$z = a + \jmath b, \tag{1.7.5.12}$$
$$z^* = a - \jmath b, \tag{1.7.5.13}$$
$$\implies (z - z^*) = a + \jmath b - a + \jmath b \tag{1.7.5.14}$$
$$= 2\jmath b = 2\text{Im}\,(z) \tag{1.7.5.15}$$

6. Show that z is real if and only if $z^* = z$ and is purely imaginary if and only if $z^* = -z$.
Solution: Let

$$z = a + \jmath b. \tag{1.7.6.1}$$

Then

$$z^* = a - \jmath b. \tag{1.7.6.2}$$

If

$$z^* = z, \tag{1.7.6.3}$$
$$a + \jmath b = a - \jmath b \tag{1.7.6.4}$$
$$\implies b = 0 \tag{1.7.6.5}$$

and z is real. If z is real,

$$z = a \tag{1.7.6.6}$$
$$\implies z^* = a \tag{1.7.6.7}$$
$$\text{or, } z = z^* \tag{1.7.6.8}$$

Similarly, the other property can be proved.

7. Verify the commutative law of multiplication $zw = wz$ in $\mathbb{C}$.
Solution: Let

$$z = a + \jmath b \tag{1.7.7.1}$$
$$w = x - \jmath y \tag{1.7.7.2}$$

Then

$$zw = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{1.7.7.3}$$
$$= \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \tag{1.7.7.4}$$
$$= wz \tag{1.7.7.5}$$

8. Show that for $z \neq 0$, $|z|^{-1} = \frac{1}{|z|}$.
Solution: Let

$$z = re^{\jmath\theta}. \tag{1.7.8.1}$$

Then

$$z^{-1} = \frac{1}{r}e^{-\jmath\theta} \tag{1.7.8.2}$$
$$\implies \left|z^{-1}\right| = \frac{1}{r} \tag{1.7.8.3}$$

9. Find
   a) $|6 - 4\jmath|$.
   b) $\left|\frac{1}{2} + \frac{2}{3}\jmath\right|$.
   c) $\left|\frac{1}{\sqrt{2}}(1 + \jmath)\right|$

Solution:

a)

$$|6 - 4\jmath| = \sqrt{6^2 + 4^2} = 2\sqrt{13} \tag{1.7.9.1}$$

b)

$$\left|\frac{1}{2} + \frac{2}{3}\jmath\right| = \frac{5}{6} \tag{1.7.9.2}$$

c)

$$\left|\frac{1}{\sqrt{2}}(1 + \jmath)\right| = \frac{1}{\sqrt{2}}|(1 + \jmath)| = 1 \tag{1.7.9.3}$$

10. Show that $|z^*| = |z|$.
Solution: Let

$$z = re^{\jmath\theta} \tag{1.7.10.1}$$

Then

$$z^* = re^{-\jmath\theta} \tag{1.7.10.2}$$
$$\implies |z^*| = r = |z|. \tag{1.7.10.3}$$

11. Find the polar form for
   a) $z = \frac{\sqrt{2}}{2} - \frac{1}{\sqrt{2}}\jmath$.
   b) $z = 4\jmath$.
   c) $z = \frac{6}{\sqrt{2}} + \frac{6}{\sqrt{2}}\jmath$.
   d) $z = -\frac{13}{2} + \frac{39}{2\sqrt{3}}\jmath$.

Solution:

a)

$$|z| = \sqrt{\left(\frac{\sqrt{2}}{2}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2}. \tag{1.7.11.1}$$
$$= 1 \tag{1.7.11.2}$$

and

$$\angle z = -\tan^{-1}\frac{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}} \tag{1.7.11.3}$$
$$= \frac{\pi}{4} \tag{1.7.11.4}$$

b)

$$|z| = 4, \angle z = \frac{\pi}{2}. \tag{1.7.11.5}$$

c)

$$|z| = \frac{6}{\sqrt{2}}, \angle z = \frac{\pi}{4}. \tag{1.7.11.6}$$

d)

$$|z| = \frac{13}{2}\sqrt{1 + 3} \tag{1.7.11.7}$$
$$= 13 \tag{1.7.11.8}$$

and

$$\angle z = \pi - \tan^{-1} \frac{\frac{39}{2\sqrt{3}}}{\frac{13}{2}} \quad (1.7.11.9)$$

$$= \pi - \tan^{-1} \sqrt{3} = \frac{2\pi}{3} \quad (1.7.11.10)$$

12. Prove that

$$\left(\cos\left(\frac{\theta}{2}\right) + \jmath \sin\left(\frac{\theta}{2}\right)\right)^2 = \cos(\theta) + \jmath \sin(\theta) \quad (1.7.12.1)$$

Solution: The L.H.S can be expressed as

$$\left(e^{\jmath\theta}\right)^2 = e^{\jmath\theta} \quad (1.7.12.2)$$

13. Show that

$$\left(\frac{1}{2} + \frac{\sqrt{3}}{2}\jmath\right)^3 = -1 \quad (1.7.13.1)$$

Solution:

$$\frac{1}{2} + \frac{\sqrt{3}}{2}\jmath = e^{\frac{\jmath\pi}{3}} \quad (1.7.13.2)$$

$$\implies \left(e^{\frac{\jmath\pi}{3}}\right)^3 = e^{\jmath\pi} = -1 \quad (1.7.13.3)$$

14. Show that

$$(\cos(\theta) + \jmath \sin(\theta))^m = \cos(m\theta) + \jmath \sin(m\theta) \quad (1.7.14.1)$$

for all integers m. **Solution:** It is easy to verify that

$$(\cos(\theta) + \jmath \sin(\theta))^2 = \cos(2\theta) + \jmath \sin(2\theta) \quad (1.7.14.2)$$

Then

$$(\cos(\theta) + \jmath \sin(\theta))^{k+1} = (\cos(\theta) + \jmath \sin(\theta))^k$$
$$(\cos(m\theta) + \jmath \sin(m\theta))$$
$$= \cos\left[(k+1)\theta + \jmath \sin((k+1)\theta)\right] \quad (1.7.14.3)$$

By induction, (1.7.14.1) is proved.

15. Show that

$$(\cos(\theta) + \jmath \sin(\theta))^r = \cos(r\theta) + \jmath \sin(r\theta) \quad (1.7.15.1)$$

for all rational numbers r. **Solution:** Let

$$r = \frac{m}{n}, (\cos(\theta) + \jmath \sin(\theta))^{\frac{1}{n}} = \cos(\alpha) + \jmath \sin(\alpha) \quad (1.7.15.2)$$

Then

$$(\cos(\alpha) + \jmath \sin(\alpha))^n = (\cos(\theta) + \jmath \sin(\theta)) \quad (1.7.15.3)$$

$$\implies \cos(n\alpha) + \jmath \sin(n\alpha) = (\cos(\theta) + \jmath \sin(\theta)) \quad (1.7.15.4)$$

$$\text{or, } \alpha = \frac{\theta}{n} \quad (1.7.15.5)$$

yielding

$$(\cos(\theta) + \jmath \sin(\theta))^{\frac{1}{n}} = \cos\left(\frac{\theta}{n}\right) + \jmath \sin\left(\frac{\theta}{n}\right) \quad (1.7.15.6)$$

Using (1.7.14.1) and (1.7.15.6),

$$(\cos(\theta) + \jmath \sin(\theta))^{\frac{m}{n}} = \cos\left(\frac{m\theta}{n}\right) + \jmath \sin\left(\frac{m\theta}{n}\right) \quad (1.7.15.7)$$

16. If $z \in \mathbb{C}$ and $n \geq 1$ is any positive integer, show that there are n distinct complex numbers such that $z = w^n$. **Solution:** Let

$$z = \cos(\theta) + \jmath \sin(\theta) \quad (1.7.16.1)$$

then using (1.7.15.6),

$$w = \cos\left(\frac{2\pi k + \theta}{n}\right) + \jmath \sin\left(\frac{2\pi k + \theta}{n}\right), k = 0, \dots, n-1 \quad (1.7.16.2)$$

which are the distinct roots.

17. Find the necessary and sufficient condition on k such that

$$\left(\cos\left(\frac{2\pi k}{n}\right) + \jmath \sin\left(\frac{2\pi k}{n}\right)\right)^n = 1 \quad \text{and} \quad (1.7.17.1)$$

$$\left(\cos\left(\frac{2\pi k}{n}\right) + \jmath \sin\left(\frac{2\pi k}{n}\right)\right)^m \neq 1 \quad 0 < m < n \quad (1.7.17.2)$$

Solution: From the above equations, using (1.7.14.1),

$$\frac{mk}{n} \notin \mathbb{Z} \quad (1.7.17.3)$$

18. Viewing the $x-y$ plane as the set of all complex numbers $x + \jmath y$, show that multiplication by $\jmath$ induces as 90° rotation of the $x - y$ plan in counterclockwise direction.
Solution: The given multiplication can be expressed using matrices as

$$\begin{pmatrix} \cos 90^\circ & -\sin 90^\circ \\ \sin 90^\circ & \cos 90^\circ \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \quad (1.7.18.1)$$

which is the multiplication of $\begin{pmatrix} x \\ y \end{pmatrix}$ with a 90° rotation matrix.

19. In problem (1.7.18), interpret geometrically what multiplication by the complex number $a + \jmath b$ does to the $x - y$ plane.
Solution: The multiplication can be represented as
$$\sqrt{a^2+b^2}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \tag{1.7.19.1}$$
where
$$\cos\theta = \frac{a}{\sqrt{a^2+b^2}} \sin\theta \qquad = \frac{b}{\sqrt{a^2+b^2}} \tag{1.7.19.2}$$
Geometrically, multiplication by $a + \jmath b$ results in rotation by θ and scaling by $\sqrt{a^2+b^2}$.
20. Prove that
$$|z+w|^2 + |z-w|^2 = 2\left(|z|^2 + |w|^2\right) \tag{1.7.20.1}$$
Solution: Since
$$|z+w|^2 = (z+w)^*(z+w) \tag{1.7.20.2}$$
$$= |z|^2 + |w|^2 + 2z^*w \tag{1.7.20.3}$$
and
$$|z-w|^2 = (z+w)^*(z-w) \tag{1.7.20.4}$$
$$= |z|^2 + |w|^2 - 2z^*w, \tag{1.7.20.5}$$
$$|z+w|^2 + |z-w|^2 = 2\left(|z|^2 + |w|^2\right) \tag{1.7.20.6}$$
21. Consider the set $A = a + b\jmath, a, b \in \mathbb{Z}$. Prove that there is 1-1 correspondence of A onto $\mathbb{N}$.
22. If a is a (complex) root of the polynomial
$$x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1}x + \alpha_n, \tag{1.7.22.1}$$
where the α_i are real, show that $\bar{a}$ must also be a root.
Solution: From the given information,
$$\bar{a}^n + \alpha_1\bar{a}^{n-1} + \cdots + \alpha_{n-1}\bar{a} + \alpha_n = 0 \tag{1.7.22.2}$$
Thus, $\bar{a}$ is also a root of the given polynomial.
23. Find the necessary and sufficient conditions on z and w in order that
$$|z+w| = |z| + |w| \tag{1.7.23.1}$$
Solution:
$$|z+w|^2 = |z|^2 + |w|^2 + 2z^*w \tag{1.7.23.2}$$
$$(|z| + |w|)^2 = |z|^2 + |w|^2 + 2|z||w| \tag{1.7.23.3}$$
If the above expressions are equal,
$$z^*w = |z||w| \tag{1.7.23.4}$$
which is the desired condition.
24. Find the necessary and sufficient conditions on z_i in order that
$$\left|\sum_{i=1}^{k} z_i\right| = \sum_{i=1}^{k} |z_i| \tag{1.7.24.1}$$
Solution:
$$\left|\sum_{i=1}^{k} z_i\right|^2 = \sum_{i=1}^{k} |z_i|^2 + 2\sum_{\substack{i=1,j=1\\ i\neq j}}^{k} {z_i}^* z_j \tag{1.7.24.2}$$
$$\left(\sum_{i=1}^{k} |z_i|\right)^2 = \sum_{i=1}^{k} |z_i|^2 + 2\sum_{\substack{i=1,j=1\\ i\neq j}}^{k} |z_i|\left|z_j\right| \tag{1.7.24.3}$$
From (1.7.24.2) and (1.7.24.3),
$$\sum_{i=1}^{k} |z_i|^2 + 2\sum_{\substack{i=1,j=1\\ i\neq j}}^{k} {z_i}^* z_j$$
$$= \sum_{i=1}^{k} |z_i|^2 + 2\sum_{\substack{i=1,j=1\\ i\neq j}}^{k} |z_i|\left|z_j\right|$$
$$\implies \sum_{\substack{i=1,j=1\\ i\neq j}}^{k} {z_i}^* z_j$$
$$= \sum_{\substack{i=1,j=1\\ i\neq j}}^{k} |z_i|\left|z_j\right| \tag{1.7.24.4}$$
which is the desired condition.
25. The complex number θ is said to have *order* $n \geq 1$ if $\theta^n = 1$ and $\theta^m \neq 1$ for $0 < m < n$. Show that if θ has order n and $\theta^k = 1$, where $k > 0$, then $n|k$.
Solution: From the given information,
$$\theta^n = \theta^k = 1, k \geq n \tag{1.7.25.1}$$
If $n \nmid k, k = mn + p, 0 < p < n$, Then,
$$\theta^k = \theta^{mn+p} = \theta^p \neq 1, \tag{1.7.25.2}$$
which is a contradiction, Hence, $n \mid k$.
26. Find all complex numbers θ having order n.
Solution: If
$$\theta^n = 1, \tag{1.7.26.1}$$
$$\theta^n = e^{\jmath 2\pi r}, 0 \leq r < n \tag{1.7.26.2}$$

yielding

$$\theta = \exp\left(\jmath\frac{2\pi r}{n}\right) 0 \le r < n \tag{1.7.26.3}$$

2 Groups

2.1 Definitions and Examples of Groups

1. Determine if the following sets G with the operation indicated form a group. If not, point out which of the group axioms fail.
   a) G = set of all integers, $a * b = a - b$.
   b) G = set of all integers, $a * b = a + b + ab$
   c) G = set of nonnegative integers, $a*b = a+b$.
   d) G = set of all rational numbers $\neq -1, a * b = a + b + ab$.
   e) G = set of all rational numbers with denominator divisible by 5 (written so that numerator and denominator are relatively prime), $a * b = a + b$.
   f) G a set having more than one element, $a*b = a \forall a, b \in G$.

   Solution: The properties of a group are
   a) $a, b \in G \implies a * b \in G$.
   b) $a, b, c \in G \implies a * (b * c) = (a * b) * c \in G$.
   c) $\exists\, e \in G \ni a * i = i * a = a \,\forall\, a \in G$.
   d) $a \in G \implies \exists b \in G \ni a * b = b * a = i$.

   a) From 2.1.1b,

$$a * (b * c) = a - (b - c) = a - b + c \tag{2.1.1.1}$$

$$(a * b) * c = (a - b) - c = a - b - c \tag{2.1.1.2}$$

$$\implies a * (b * c) \neq (a * b) * c \tag{2.1.1.3}$$

   Thus, G is not a group.

   b) i) From property 2.1.1b,

$$a * (b * c) = a * (b + c + bc) \tag{2.1.1.4}$$

$$= a + b + c + bc + a(b + c + bc) \tag{2.1.1.5}$$

$$= a + b + c + ab + bc + ca + abc \tag{2.1.1.6}$$

$$(a * b) * c = (a + b + ab) + c + c\,(a + b + ab) \tag{2.1.1.7}$$

$$= a + b + c + ab + bc + ca + abc \tag{2.1.1.8}$$

   Thus, property 2.1.1b is satisfied.

   ii) Since

$$a * i = a + i + ai \tag{2.1.1.9}$$

$$i * a = a + i + ai \tag{2.1.1.10}$$

   property 2.1.1c is satisfied.

   iii)

$$a * i = a + i + ai \tag{2.1.1.11}$$

$$i * a = a + i + ai \tag{2.1.1.12}$$

   Thus, for property 2.1.1c to be satisfied,

$$i * a = a \tag{2.1.1.13}$$

$$\implies a + i + ai = a \tag{2.1.1.14}$$

$$\text{or, } i\,(1 + a) = 0 \tag{2.1.1.15}$$

$$\implies i = 0 \tag{2.1.1.16}$$

   iv) If

$$a * b = b * a = i, \tag{2.1.1.17}$$

$$a + b + ab = 0 \tag{2.1.1.18}$$

$$\implies b = -\frac{a}{1 + a} \tag{2.1.1.19}$$

   which is not finite for $a = -1$. Also, $b \notin G$ for $a = 1$. Thus, property 2.1.1d is violated and G is not a group.

   c) In this case, for property 2.1.1c to be satisfied,

$$a * i = i * a = a, \tag{2.1.1.20}$$

$$\implies a + i = a \tag{2.1.1.21}$$

$$\text{or, } i = 0 \tag{2.1.1.22}$$

   From property 2.1.1c,

$$a + b = 0 \implies b = -a \tag{2.1.1.23}$$

   Thus, G is a group.

   d) From problem 2.1.1b, it is easy to verify that G is a group, since we are now considering rational numbers.

   e) From property 2.1.1c,

$$a * i = a, i * a = i \tag{2.1.1.24}$$

$$\implies a = i \tag{2.1.1.25}$$

   From property 2.1.1d,

$$a * b = b * a = i \tag{2.1.1.26}$$

$$\implies i * b = i, b * i = b = i \tag{2.1.1.27}$$

Thus, G has only a single element i which is a contradiction. So G is not a group.

2. Let G be the set of all mappings

$$T_{a,b} \mid T_{a,b}(r) = ar + b, \quad a \neq 0, b, r \in \mathbb{R}, \tag{2.1.2.1}$$

show that the set $H = T_{a,b} \mid a = \pm 1, b \in \mathbb{R}$ forms a group under the $*$ of G.
Solution:

a)

$$\left(T_{a,b} * T_{a,c}\right)(r) = a\,(ar + c) + b \tag{2.1.2.2}$$
$$= a^2 r + ac + b = r + ac + b \tag{2.1.2.3}$$
$$= T_{1,ac+b} \in G \tag{2.1.2.4}$$

Similarly,

$$\left(T_{a,c} * T_{a,b}\right)(r) = r + ab + c \tag{2.1.2.5}$$

b) If

$$\left(T_{a,b} * T_{a,c}\right)(r) = T_{a,b}, \tag{2.1.2.6}$$
$$r + ab + c = ar + b \tag{2.1.2.7}$$
$$\implies a = 1, c = 0 \tag{2.1.2.8}$$

Thus,

$$i = T_{1,0} \tag{2.1.2.9}$$

c) If

$$\left(T_{a,b} * T_{a,c}\right)(r) = \left(T_{a,c} * T_{a,b}\right)(r) = T_{1,0}, \tag{2.1.2.10}$$
$$r + ab + c = r + ac + b = r \tag{2.1.2.11}$$
$$\implies b = \pm c \tag{2.1.2.12}$$

d) From (2.1.2.4),

$$T_{a,b} * \left(T_{a,c}(r) * T_{a,d}\right)(r) = T_{a,b} * T_{1,ad+c} \tag{2.1.2.13}$$
$$= a\,(r + ad + b + c) + b \tag{2.1.2.14}$$
$$= ar + ab + ac + b + d \tag{2.1.2.15}$$

Similalrly,

$$\left(T_{a,b} * T_{a,c}\right)(r) * T_{a,d}(r) = T_{1,ac+b} * T_{a,d} \tag{2.1.2.16}$$
$$= (ar + d) + ac + b \tag{2.1.2.17}$$
$$= ar + ab + ac + b + d \tag{2.1.2.18}$$

which satisfies the associativity property.
Thus, $T_{a,b}^{-1} = T_{a,\pm b}$. and G is a group.

3. Let $H \subset G$, for G in problem 2.1.2d and $H = \{T_{a,b} \in G \mid a \text{ is rational}, b \text{ any real}\}$. Show that H is also a group.
4. Let $K \subset G$, for G in problem 2.1.2d and $K = \{T_{1,b} \in G \mid b \in \mathbb{R}\}$. Show that K is an Abelian group.
Solution: From (2.1.2.4),

$$T_{1,b} * T_{1,c} = T_{1,b+c} \tag{2.1.4.1}$$
$$= T_{1,c+b} \tag{2.1.4.2}$$

Thus, K is an Abelian group.

5. Let $S = \{(x, y) \mid x, y \in \mathbb{R}\}$ and consider $f, g \in A(S)$ defined by $f(x, y) = (-x, y)$ and $g(x, y) = (-y, x)$; f is the reflection about the y-axis and g is the rotation through 90° in a counterclockwise direction about the origin. We then define $G = f^i g^j \mid i = 0, 1; j = 0, 1, 2, 3$, and let $*$ in G be the product of elements in $A(S)$. Clearly, $f^2 = g^4 =$ identity mapping; $(f * g)(x, y) = (fg)(x, y) = f(g(x, y) = f(-y, x) = (y, x)$ and $(g * f)(x, y) = g(f(x, y) = g(-x, y) = (-y, -x)$. Prove that $g * f = f * g^{-1}$, and that G is a group, is nonabelian, and is of order 8.
Solution: Let

$$\mathbf{x} = \begin{pmatrix} x \\ y \end{pmatrix}. \tag{2.1.5.1}$$

Then

$$f\,(\mathbf{x}) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\mathbf{x} = \mathbf{f}\mathbf{x} \tag{2.1.5.2}$$
$$g\,(\mathbf{x}) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\mathbf{x} = \mathbf{g}\mathbf{x} \tag{2.1.5.3}$$

and

$$\mathbf{g}\mathbf{f} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \mathbf{f}\mathbf{g}^{-1} \tag{2.1.5.4}$$

Let

$$\mathbf{G}_1 = \mathbf{f}^i \mathbf{g}^j \in G \tag{2.1.5.5}$$
$$\mathbf{G}_2 = \mathbf{f}^k \mathbf{g}^l \in G \tag{2.1.5.6}$$

a) The identity element is

$$\mathbf{i} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.1.5.7}$$

b) It is easy to verify that

$$\mathbf{f}^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad (2.1.5.8)$$

$$\mathbf{g}^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (2.1.5.9)$$

Also,

$$\mathbf{f}^i\mathbf{g}^j g^{-j} f^{-i} = \mathbf{i} \quad (2.1.5.10)$$

and

$$\mathbf{g}^{-j}\mathbf{f}^{-i}\mathbf{f}^i\mathbf{g}^j = \mathbf{i} \quad (2.1.5.11)$$

which implies that all elements in G have an inverse.

c) The product

$$\mathbf{G}_1\mathbf{G}_2 = \mathbf{f}^i\mathbf{g}^j\mathbf{f}^k\mathbf{g}^l \in G \quad (2.1.5.12)$$

For $j > k$,

$$\mathbf{f}^i\mathbf{g}^{j-k}\mathbf{g}^k\mathbf{f}^k\mathbf{g}^l = \mathbf{f}^i\mathbf{g}^{j-k}\mathbf{f}^k\mathbf{g}^{l-k} \quad (2.1.5.13)$$

if $l > k$.

6.
7.
8. If G is an Abelian group, prove that $(a * b)^n = a^n * b^n$ for all integers n.
Solution: For $n = 1$, the above result is valid. For $n = 2$,

$$(a * b)^2 = a * b * a * b = a * a * b * b = a^2 * b^2 \quad (2.1.8.1)$$

Let $P(n)$ be true. Then, $P(n+1)$ can be expressed as

$$(a * b)^{n+1} = (a * b)^n * a * b \quad (2.1.8.2)$$
$$= a^n * b^n * a * b = a^n * a * b^n * b \quad (2.1.8.3)$$
$$= a^{n+1}b^{n+1} \quad (2.1.8.4)$$

9. If G is a group in which $a^2 = e$ for all $a \in G$, show that G is abelian.
Solution:

$$\because e \in G, e^2 = e \quad (2.1.9.1)$$
$$\implies e = I \quad (2.1.9.2)$$

Also, for $b \in G, ab \in G$ using the property of a group. Hence,

$$b^2 = I \quad (2.1.9.3)$$
$$\implies (ab)^2 = a^2b^2 = I \quad (2.1.9.4)$$
$$\implies a\,(ba)\,b = a(ab)b \quad (2.1.9.5)$$
$$\implies a^{-1}a\,(ba)\,bb^{-1} = a^{-1}a(ab)bb^{-1} \quad (2.1.9.6)$$
$$\text{or, } ab = ba \quad (2.1.9.7)$$

Hence, G is Abelian.

10.
11.
12.
13. Show that a group of order 4 or less is Abelian.
Solution:
a) Let $a, I \in G$ be a group of order 2. Then

$$a^2 = I \quad (2.1.13.1)$$

Hence, G is Abelian.

b) Considering a group of order 3 with $a, b, I \in G$, If $b = a^{-1}$,

$$ab = ba = I \quad (2.1.13.2)$$

and the group is Abelian. Alternatively,

$$a = a^{-1} \implies a^2 = b^2 = I \quad (2.1.13.3)$$

and from problem 2.1.9, G is Abelian.

c) Considering a group of order 4 with $a, b, c, I \in G$, if

$$a^2 = b^2 = c^2 = I \quad (2.1.13.4)$$

from problem 2.1.9, G is Abelian. Alternatively, if, without loss of generality, only $a^2 = I$,

$$bc = cb = I \quad (2.1.13.5)$$

and the group is Abelian.

These are the only two possibilities, so any group of order 4 or less is always an Abelian group.

14. If G is any group and $a, b, c \in G$, show that if $a * b = a * c$, then $b = c$, and if $b * a = c * a$, then $b = c$.
Solution: $\because a \in G, \ni a^{-1} \in G | aa^{-1} = a^{-1}a = I$. Using the associativity property of G,

$$a^{-1}\,(ab) = a^{-1}\,(ac) \quad (2.1.14.1)$$
$$\implies \left(a^{-1}a\right)b = \left(a^{-1}a\right)c \quad (2.1.14.2)$$
$$\implies Ib = Ic \quad (2.1.14.3)$$

and the proof is complete. The second property can be proved similarly.

15. Express $(a * b)^{-1}$ in terms of a^{-1} and b^{-1}.
Solution:

$$(ab)^{-1}(ab) = I \qquad (2.1.15.1)$$
$$\implies (ab)^{-1} abb^{-1}a^{-1} = b^{-1}a^{-1} \qquad (2.1.15.2)$$
$$\implies (ab)^{-1} = b^{-1}a^{-1} \qquad (2.1.15.3)$$

16. Using the result of Problem 2.1.15, prove that a group G in which $a = a^{-1}$ for every $a \in G$ must be abelian.
Solution: See Problem 2.1.9.
17. In any group G, prove that $\left(a^{-1}\right)^{-1} = a$ for all $a \in G$.
Solution: Let $ab = ba = I$. Then $a^{-1} = b$ and

$$\left(a^{-1}\right)^{-1} = (b)^{-1} \qquad (2.1.17.1)$$
$$= a \qquad (2.1.17.2)$$

18. If G is a finite group of *even* order, show that there must be an element $a \neq I$ such that $a = a^{-1}$. (Hint: Try to use the result ofProblem 17.)
Solution: If G is of order 2, the elements of G are a, I. Thus,

$$a^2 = I \qquad (2.1.18.1)$$

From the proof of 2.1.13c, it can be shown that for even order,

$$a^2 = I \implies a = a^{-1} \qquad (2.1.18.2)$$