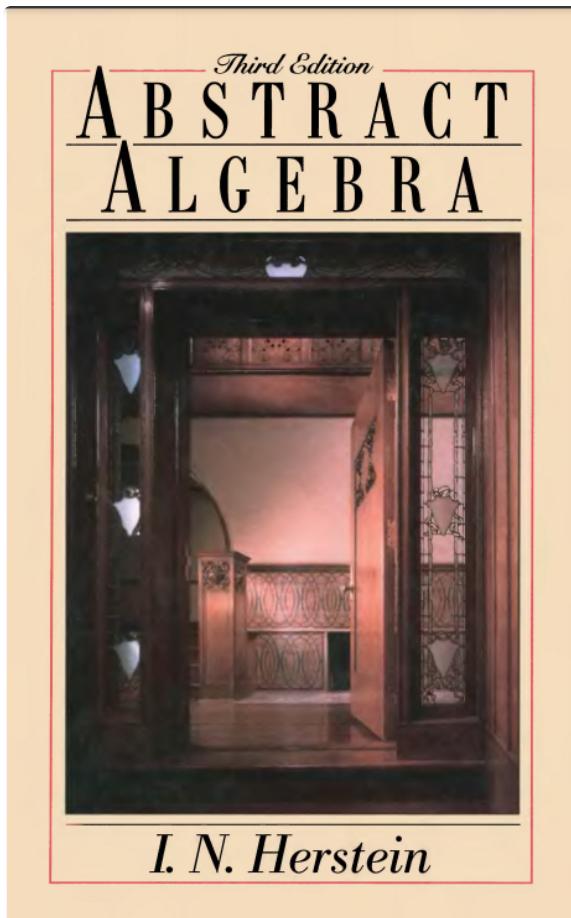


# Table of Contents

Chapter 1	4
Section 1-1	4
Section 1-2	6
Section 1-3	19
Section 1-4	34
Section 1-5	60
Section 1-6	75
Section 1-7	83
Chapter 2	94
Section 2-1	94
Section 2-2	110
Section 2-3	115
Section 2-4	145
Section 2-5	181
Section 2-6	214
Section 2-7	226
Section 2-8	233
Section 2-9	242
Section 2-10	247
Section 2-11	249
Chapter 3	265
Section 3-1	265
Section 3-2	270
Section 3-3	289
Chapter 4	298
Section 4-1	298
Section 4-2	328
Section 4-3	338
Section 4-4	368
Section 4-5	377
Section 4-6	403
Section 4-7	412

Chapter 5	415
Section 5-1	415
Section 5-2	425
Section 5-3	449
Section 5-4	462
Section 5-5	464
Section 5-6	466
Chapter 6	476
Section 6-1	476
Section 6-2	483
Section 6-3	489
Section 6-5	494

# Abstract Algebra by I.N. Herstein 3ed



- Complete solution guide to almost every exercise of Abstract Algebra by I.N. Herstein 3ed.  
from slader(quizlet)

# Chapter 1

## Section 1–1

1. a

Suppose  $S$  has (at least) two distinct objects  $x$  and  $y$ . Then we see that  $x = x * y = y * x = y$ . But this says that the two objects  $x$  and  $y$  are the same. Contradiction. Hence  $S$  cannot have at least two distinct elements -- equivalently,  $S$  has at most one object.

2. a

(a) Suppose that  $a \neq b$ . Then

$$a * b = a - b = -(b - a) = -b * a$$

So the only way that  $a * b = b * a$  is if  $b * a = -b * a$ . This implies that  $2b * a = 0$  which says that  $b * a = b - a = 0$ . Hence  $a = b$ . Contradiction. So  $a \neq b \implies a * b \neq b * a$ .

### Step 2

2 of 4

(b) To show that  $(a * b) * c = a * (b * c)$  does not hold in general, we need only provide one counterexample. Here's one: let  $a = 1 = c$  and  $b = 2$ . Then  $(a * b) * c = (a - b) - c = -2$  and  $a * (b * c) = a - (b - c) = 0$ .

For this property to hold we need

$$\begin{aligned} (a - b) - c &= a - (b - c) \\ \implies (a - b) - a &= c - (b - c) \\ \implies -b &= 2c - b \\ \implies 0 &= 2c \\ \implies c &= 0 \end{aligned}$$

So  $(a - b) - c = a - (b - c) \implies c = 0$ . Alternatively, we immediately see that  $c = 0 \implies (a - b) - c = a - (b - c)$ . Hence  $(a - b) - c = a - (b - c) \iff c = 0$ . So, in particular, if  $c = 0$ , then the property does happen to hold.

(c) Let  $a \in S$ . Then

$$a * 0 = a - 0 = a$$

### Step 4

(d) Let  $a \in S$ . Then

$$a * a = a - a = 0$$

### 3. a

(a) 1, 2, and 3 give every possible product of the elements  $\square$  and  $\triangle$  and all of them are either  $\square$  or  $\triangle$  themselves. So  $a * b \in S$ .

(b) (Note after writing this part I realized it would have been shorter just to write up all 8 combinations of  $a, b, c$  and verify the identity for each. You can do it in 8 lines. Oh well. This works, too.) Suppose  $a = b$ . Then  $a * b = \square$  and

$$(a * b) * c = \square * c = c$$

Also

$$b * c = \begin{cases} \square, & b = c \\ \triangle, & b \neq c \end{cases}$$

and hence

$$a * (b * c) = \begin{cases} a * \square, & b = c \\ a * \triangle, & b \neq c \end{cases} = \begin{cases} \square, & b = c \text{ and } a = \square \\ \triangle, & b = c \text{ and } a = \triangle \\ \triangle, & b \neq c \text{ and } a = \square \\ \square, & b \neq c \text{ and } a = \triangle \end{cases} = \begin{cases} \square, & a = b = c = \square \\ \triangle, & a = b = c = \triangle \\ \triangle, & a = b = \square \text{ and } c = \triangle \\ \square, & a = b = \triangle \text{ and } c = \square \end{cases}$$

By inspection we see that here too  $a * (b * c) = c$ .

Now suppose  $a \neq b$ . Then  $a * b = \triangle$  and

$$(a * b) * c = \triangle * c \neq c$$

i.e.  $(a * b) * c$  is the opposite element as  $c$ .

We also see that

$$b * c = \begin{cases} \square, & b = c \\ \triangle, & b \neq c \end{cases}$$

and hence

$$a * (b * c) = \begin{cases} a * \square, & b = c \\ a * \triangle, & b \neq c \end{cases} = \begin{cases} \square, & b = c \text{ and } a = \square \\ \triangle, & b = c \text{ and } a = \triangle \\ \triangle, & b \neq c \text{ and } a = \square \\ \square, & b \neq c \text{ and } a = \triangle \end{cases} = \begin{cases} \square, & b = c = \triangle \text{ and } a = \square \\ \triangle, & b = c = \square \text{ and } a = \triangle \\ \triangle, & b = \triangle \text{ and } a = c = \square \\ \square, & b = \square \text{ and } a = c = \triangle \end{cases}$$

By inspection we see that here too  $a * (b * c)$  is the opposite element as  $c$ .

Hence, regardless of whether  $a = b$  or not, we find that  $(a * b) * c = a * (b * c)$ , as desired.

(c) Notice that if  $a \neq b$ , then  $a * b = \triangle = b * a$  and if  $a = b$ , then  $a * b = \square = b * a$ . Hence, regardless of whether  $a = b$  or not, we find that  $a * b = b * a$ .

(d) Notice that  $\square * \square = \square$  and  $\square * \triangle = \triangle = \triangle * \square$ . Hence multiplying by  $\square$  doesn't change your object. In symbols,  $a * b = b * a = b$  for all  $b \in S$ .

(e) Note that if  $b = \square$ , then  $b * b = \square * \square = \square$  and if  $b = \triangle$ , then  $b * b = \triangle * \triangle = \square$ . Hence the "square" of any element in  $b$  is always  $\square$ . In symbols,  $b * b = a$  for all  $b$ .

## Section 1–2

1. a

(a) This is the set of all planets in the solar system plus one big snow ball in the Kuiper belt that used to be called a planet.

(b) This is the set of all states in the United States.

2. a

(a) The set of all positive even integers.

(b) The set of all positive integer powers of two. (That is,  $2^1, 2^2$ , etc.)

(c) The set of all square numbers. That is, the set of numbers which are themselves the square of a positive integer.

3. a

$A \cap B \cap C$  is the set of all Canadian women who currently live in the US.

$A - B$  is the set of all people who currently live in the US but are *not* citizens of Canada.

$A - C$  is the set of all men (/non-women) living in the US.

$C - A$  is the set of all women who *don't* live in the US.

4. a

$A \cap B = \{4, 9\}$  says that 4 and 9 are both elements of  $A$  and  $B$ . It's clear that 4 is an element of both  $A$  and  $B$  but the only way for 9 to be as well is if  $a = 9$ .

**Result**

2 of 2

9

5. a

!!!

6. a

Let  $A$ ,  $B$ , and  $C$  be sets such that  $A \subset B$ . There are no restrictions on  $C$ . Let  $x \in A \cup C$ . Then either  $x \in A$  or  $x \in C$ . If  $x \in A$ , then  $x \in B$  because  $A \subset B$ . Otherwise  $x \in C$ . Hence  $x \in B$  or  $x \in C$ . Thus we see that  $x \in B \cup C$ . We thus showed that  $x \in A \cup C \implies x \in B \cup C$ . Hence  $A \cup C \subset B \cup C$ .

7. a

**Unions:** Let  $x \in A \cup B$ . Then  $x \in A$  or  $x \in B$ . Then  $x \in B$  or  $x \in A$ . Hence  $x \in B \cup A$ . i.e.  $A \cup B \subset B \cup A$ . Reverse the roles of  $A$  and  $B$  in the argument just given to show that likewise  $B \cup A \subset A \cup B$ . Hence

$$A \cup B = B \cup A$$

as desired.

## Step 2

2 of 2

**Intersections:** Let  $x \in A \cap B$ . Then  $x \in A$  and  $x \in B$ . Then  $x \in B$  and  $x \in A$ . Hence  $x \in B \cap A$ . i.e.  $A \cap B \subset B \cap A$ . Reverse the roles of  $A$  and  $B$  in the argument just given to show that likewise  $B \cap A \subset A \cap B$ . Hence

$$A \cap B = B \cap A$$

as desired.

## 8. a

Suppose  $x \in (A - B) \cup (B - A)$ . Then either  $x \in A - B$  or  $x \in B - A$ . If  $x \in A - B$ , then  $x \in A$  and  $x \notin B$ . Because  $A \subset A \cup B$ , we see that  $x \in A \cup B$  and because  $A \cap B \subset B$ , we see that  $x \notin A \cap B$ . Thus  $x \in (A \cup B) - (A \cap B)$ . Reversing the roles of  $B$  and  $A$  in the previous argument we likewise show that if  $x \in B - A$  then  $x \in (A \cup B) - (A \cap B)$ . Hence, either way we find that  $x \in (A \cup B) - (A \cap B)$ . Thus

$$(A - B) \cup (B - A) \subset (A \cup B) - (A \cap B)$$

## Step 2

2 of 3

Now suppose that  $x \in [(A \cup B) - (A \cap B)]$ . Then  $x \in A \cup B$  and  $x \notin A \cap B$ . So  $x \in A$  or  $x \in B$  and it's not true that  $x \in A$  and  $x \in B$ . Hence if  $x \in A$ , then  $x \notin B$  and likewise if  $x \in B$ , then  $x \notin A$ . Thus either  $x \in A - B$  or  $x \in B - A$ . i.e.  $x \in (A - B) \cup (B - A)$ . Hence

$$(A \cup B) - (A \cap B) \subset (A - B) \cup (B - A)$$

We therefore see that

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

as desired.

For the pictorial representation look back at the Venn diagrams on page 5. Our identity says that if you take the area shaded in 1 and remove the area shaded in 2 then you get the combination of the areas shaded in 3 and 4.

## 9. a

Suppose  $x \in A \cap (B \cup C)$ . Then  $x \in A$  and  $x \in B \cup C$ . Thus  $x \in A$  and  $x$  is either in  $B$  or  $C$ . I.e.  $x \in A$  and  $x \in B$  or  $x \in A$  and  $x \in C$ . Thus  $x \in (A \cap B) \cup (A \cap C)$ . Hence

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$$

### Step 2

2 of 3

Now suppose that  $x \in (A \cap B) \cup (A \cap C)$ . Then  $x \in A \cap B$  or  $x \in A \cap C$ . I.e.  $x \in A$  and  $x \in B$  or  $x \in A$  and  $x \in C$ . So  $x \in A$  either way, but then also  $x \in B$  or  $x \in C$ . Hence  $x \in A$  and  $x \in B \cup C$ . Thus  $x \in A \cap (B \cup C)$ . Hence

$$(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$$

### Step 3

3 of 3

We therefore see that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

as desired.

## 10. a

Suppose that  $x \in A \cup (B \cap C)$ . Then  $x \in A$  or  $x \in B \cap C$ . I.e.  $x \in A$  or it's true that  $x \in B$  and  $x \in C$ . If  $x \in A$ , then  $x \in A \cup B$  and  $x \in A \cup C$  because  $A \subset A \cup B$  and  $A \subset A \cup C$ . Hence  $x \in (A \cup B) \cap (A \cup C)$ . Alternatively, if  $x \in B$  and  $x \in C$ , then  $x \in A \cup B$  and  $x \in A \cup C$  because  $B \subset A \cup B$  and  $C \subset A \cup C$ . Hence  $x \in (A \cup B) \cap (A \cup C)$ . Thus, either way, we see that  $x \in (A \cup B) \cap (A \cup C)$  and hence

$$A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$$

### Step 2

2 of 3

Conversely, suppose that  $x \in (A \cup B) \cap (A \cup C)$ . Then  $x \in A \cup B$  and  $x \in A \cup C$ . I.e.  $x \in A$  or  $x \in B$  but also  $x \in A$  or  $x \in C$ . If  $x \in A$  then it satisfies both conditions. If  $x \notin A$ , then  $x \in B$  and  $x \in C$ . Hence, in that case,  $x \in B \cap C$ . So in all  $x \in A \cup (B \cap C)$ . Thus

$$(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$$

We therefore see that

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

as desired.

## 11. a

First, remember to include the trivial cases: we know that  $\emptyset$  is a subset of every set and  $S \subset S$  always holds. The others are fairly easy to construct if you go about it systematically. Here is the full list:

- $\emptyset$
- $\{1, 2, 3, 4\}$
- $\{1\}$
- $\{2\}$
- $\{3\}$
- $\{4\}$
- $\{1, 2\}$
- $\{1, 3\}$
- $\{1, 4\}$
- $\{2, 3\}$
- $\{2, 4\}$
- $\{3, 4\}$
- $\{1, 2, 3\}$
- $\{1, 2, 4\}$
- $\{1, 3, 4\}$
- $\{2, 3, 4\}$

Note: One thing to keep in mind is that order doesn't matter in sets so things like  $\{1, 2\}$  and  $\{2, 1\}$  are the same set and thus only once in my above list.

## 12. a

### De Morgan's Laws.

- $(A \cap B)' = A' \cup B'$ .
- $(A \cup B)' = A' \cap B'$ .

**Proof:** (b) Let us consider  $P = (A \cup B)'$ , and  $Q = A' \cap B'$ .

Let  $x$  be an element of  $P$ .

Then

$$\begin{aligned} x \in P &\implies x \notin A \cup B \\ &\implies x \notin A \text{ and } x \notin B \\ &\implies x \in A' \text{ and } x \in B' \\ &\implies x \in A' \cap B'. \end{aligned}$$

Thus  $P \subset Q$ .

Let  $y$  be an element of  $Q$ .

Then

$$\begin{aligned} y \in Q &\implies y \in A' \cap B' \\ &\implies y \in A' \text{ and } y \in B' \\ &\implies y \notin A \text{ and } y \notin B \\ &\implies y \notin A \cup B \\ &\implies y \in (A \cup B)'. \end{aligned}$$

Therefore  $Q \subset P$ .

Consequently,  $P = Q$  i.e.,  $(A \cup B)' = A' \cap B'$ .

(a) Let us consider the subsets  $A'$  and  $B'$  of  $S$ .

Then by above argument it follows that

$$\begin{aligned}(A' \cup B')' &= (A')' \cap (B')' \\ \implies (A' \cup B')' &= A \cap B, \text{ since } (A')' = A \\ \implies \{(A' \cup B')'\}' &= (A \cap B)', \text{ taking complements} \\ \implies A' \cup B' &= (A \cap B)', \text{ since } (A')' = A\end{aligned}$$

This completes (a).

**Note:**  $(A)'$  is the complement of  $A$  in  $S$ .

3 of 3

## Result

First we prove (b) by considering an element  $x$  in  $(A \cup B)'$ , we show that  $x \in A' \cap B'$ , and vice versa, again by help of (b) we proved (a) directly.

[Click for the complete proof.](#)

## 13. a

**Given:**  $A$  and  $B$  are two subsets of a set  $S$ . Let us define

$$A + B := (A - B) \cup (B - A) \text{ and } A.B := A \cap B.$$

**To Prove:**\

- (a)  $A + B = B + A$
- (b)  $A + \phi = A$
- (c)  $A.A = A$
- (d)  $A + A = \phi$
- (e)  $A + (B + C) = (A + B) + C$
- (f) If  $A + B = A + C$  then  $B = C$
- (g)  $A.(B + C) = A.B + A.C$

Before proving we will state the **De Morgans Rule** for subsets  $A$  and  $B$  of  $S$  as

$$\begin{aligned}(A \cup B)' &= A' \cap B' \\ (A \cap B)' &= A' \cup B'.\end{aligned}$$

**Proof:**

(a) We have by definition

$$A + B := (A - B) \cup (B - A).$$

Then we have

$$\begin{aligned} B + A &= (B - A) \cup (A - B) \\ &= (A - B) \cup (B - A), \text{ since union is a commutative operator} \\ &= A + B. \end{aligned}$$

(b) Note that  $\phi$  is the empty set, which is contained in every set. So, according to the question

$$A + \phi = (A - \phi) \cup (\phi - A).$$

We know that by definition

$$A - B := \{x \mid x \in A \text{ but } x \notin B\}.$$

SO,

$$(A - \phi) = A \text{ and } (\phi - A) = \phi \text{ and } A \cup \phi = A.$$

Hence

$$A + \phi = A.$$

(c) Now we know that

$$A \cap B := \{x \mid x \in A \text{ and } x \in B\}.$$

So by the given condition,

$$A \cdot A = A \cap A = \{x \mid x \in A \text{ and } x \in A\} = A.$$

(d) Now we have

$$\begin{aligned} A + A &= (A - A) \cup (A - A) \\ &= \phi \cup \phi = \phi. \end{aligned}$$

(e) Let us consider three subsets of  $S$  given by  $A$ ,  $B$  and  $C$ . We need to show

$$A + (B + C) = (A + B) + C.$$

Since for any two sets  $X$  and  $Y$

$$X - Y = X \cap Y'$$

then we have

$$\begin{aligned} B + C &= (B - C) \cup (C - B) = (B \cap C') \cup (C \cap B') \\ A + B &= (A - B) \cup (B - A) = (A \cap B') \cup (B \cap A') \end{aligned}$$

Now,

$$\begin{aligned} A + (B + C) &= [A - (B + C)] \cup [(B + C) - A] \\ &= [A - ((B \cap C') \cup (C \cap B'))] \cup [((B \cap C') \cup (C \cap B')) - A] \\ &= [A \cap ((B \cap C') \cup (C \cap B'))'] \cup [((B \cap C') \cup (C \cap B')) \cap A'] \\ &= [A \cap ((B \cap C')' \cap (C \cap B'))'] \cup [((B \cap C') \cup (C \cap B')) \cap A'] \\ &= [A \cap ((B' \cup C) \cup (C' \cup B))] \cup [(B \cap C' \cap A') \cup (C \cap B' \cap A')] \\ &= [(A \cap (B' \cup C)) \cup (A \cap (C' \cup B))] \cup [(B \cap C' \cap A') \cup (C \cap B' \cap A')] \\ &= (A \cap B') \cup (A \cap C) \cup (A \cap C') \cup (A \cap B) \cup [(B \cap C' \cap A') \cup (C \cap B' \cap A')] \end{aligned}$$

Again by similar calculation and using **De Morgans Rule** we have

$$(A + B) + C = A \cap B' \cup (A \cap C) \cup (A \cap C') \cup (A \cap B) \cup [(B \cap C' \cap A') \cup (C \cap B' \cap A')].$$

(f) By the given condition

$$A + B = A + C.$$

Then we have

$$(A - B) \cup (B - A) = (A - C) \cup (C - A).$$

Now, we need to show that  $B = C$ .

Let us assume that  $x \in A$ . Then

$$x \in A - C \text{ or } x \in A \cap C.$$

If  $x \in A - C$ . Then,

$$A + C = B + C = (B - C) \cup (C - B), \quad x \in B - C, \quad x \notin C.$$

In particular,

$$x \in B.$$

If  $x \in A \cap C$ . Again,

$$A - C = B - C, \quad x \notin B + C.$$

That is,  $x \in B \cap C$  or  $x \notin B \cup C$ . Since  $x \in C$ , it must be the case that  $x \in B \cap C$ . In particular,  $x \in B$ .

Hence,  $A \subseteq B$ .

Similarly by the aforesaid argument we proceed in the other direction. Consequently,

$$B = C.$$

(g) Now

$$\begin{aligned} A.(B + C) &= A \cap [(B - C) \cup (C - B)] \\ &= A \cap [(B \cap C') \cup (C \cap B')] \\ &= (A \cap B \cap C') \cup (A \cap B' \cap C). \end{aligned}$$

Again we have

$$\begin{aligned} A.B + A.C &= [(A \cap B) - (A \cap C)] \cup [(A \cap C) - (A \cap B)] \\ &= [(A \cap B) \cap (A \cap C)'] \cup [(A \cap C) \cap (A \cap B)'] \\ &= [(A \cap B) \cap (A' \cup C')] \cup [(A \cap C) \cap (A' \cup B')] \\ &= (A \cap B \cap C') \cup (A \cap B' \cap C), \text{ since } A \cap A' = \emptyset. \end{aligned}$$

Therefore,

$$A.(B + C) = A.B + A.C.$$

This completes the proof.

## Result

6 of 6

Considering three arbitrary subsets  $A$ ,  $B$  and  $C$  of  $S$  and using the aforesaid definitions and a little bit use of DE Morgans Rule of sets we have proved all the above mentioned problems. Click for the complete solution.

## 14. a

If  $A$  and  $B$  are disjoint sets, then we have

$$m(A \cup B) = m(A) + m(B)$$

and since  $m(A \cap B) = 0$ , we have  $m(A \cup B) = m(A) + m(B) - m(A \cap B)$ . We have

$$A = (A \cap B) \cup (A \cap B^c)$$

Since  $(A \cap B)$  and  $(A \cap B^c)$  are disjoint, we have

$$m(A) = m(A \cap B) + m(A \cap B^c)$$

Similarly,

$$m(B) = m(A \cap B) + m(A^c \cap B)$$

This gives

$$m(A) + m(B) = 2m(A \cap B) + m(A \cap B^c) + m(A^c \cap B)$$

We have

$$A \cup B = (A \cap B^c) \cup (A^c \cap B) \cup (A \cap B)$$

This gives

$$m(A \cup B) = m(A \cap B^c) + m(A^c \cap B) + m(A \cap B)$$

Therefore

$$m(A \cup B) = m(A) + m(B) - m(A \cap B)$$

## 15. a

Let  $D = B \cup C$ , we get

$$m(A \cup B \cup C) = m(A) + m(D) - m(A \cap D)$$

This gives

$$m(D) = m(B) + m(C) - m(B \cap C)$$

and

$$m(A \cap D) = m((A \cap B) \cup (A \cap C))$$

Using the formula from (14) again gives

$$\begin{aligned} m((A \cap B) \cup (A \cap C)) &= m(A \cap B) + m(A \cap C) - m((A \cap B) \cap (A \cap C)) \\ &= m(A \cap B) + m(A \cap C) - m(A \cap B \cap C) \end{aligned}$$

Therefore

$$m(A \cup B \cup C) = m(A) + m(B) + m(C) - m(A \cap B) - m(A \cap C) - m(C \cap B) + m(A \cap B \cap C)$$

## 16. a

For finite sets,  $A_1, A_2, \dots, A_n$ , we have

$$m(A_1 \cup A_2 \cup \dots \cup A_n) = \sum_{S \subseteq \{1, \dots, n\}; S \neq \emptyset} (-1)^{m(S)-1} m(\cap_{j \in S} A_j)$$

This can be proven by induction. For  $n = 1$ , this is trivially true as

$$m(A_1) = \sum_{\emptyset \neq S \subseteq \{1\}} (-1)^{m(S)-1} m(\cap_{j \in S} A_j) = (-1)^0 m(A_1) = m(A_1)$$

For our inductive step, we assume

$$m(A_1 \cup \dots \cup A_{n-1}) = \sum_{S \subseteq \{1, \dots, n-1\}; S \neq \emptyset} (-1)^{m(S)-1} m(\cap_{j \in S} A_j)$$

This gives

$$\begin{aligned} m(A_1 \cup \dots \cup A_{n-1} \cup A_n) &= m((A_1 \cup \dots \cup A_{n-1}) \cup A_n) \\ &= m(A_1 \cup \dots \cup A_{n-1}) + m(A_n) - m((A_1 \cup \dots \cup A_{n-1}) \cap (A_n)) \\ &= \sum_{S \subseteq \{1, \dots, n-1\}; S \neq \emptyset} (-1)^{m(S)-1} m(\cap_{j \in S} A_j) + m(A_n) \\ &\quad - m((A_1 \cap A_n) \cup \dots \cup (A_{n-1} \cap A_n)) \\ &= \sum_{S \subseteq \{1, \dots, n-1\}; S \neq \emptyset} (-1)^{m(S)-1} m(\cap_{j \in S} A_j) + m(A_n) \\ &\quad - \sum_{S \subseteq \{1, \dots, n-1\}; S \neq \emptyset} (-1)^{m(S)-1} m((\cap_{j \in S} A_j) \cap A_n) \\ &= \sum_{S \subseteq \{1, \dots, n\}; S \neq \emptyset} (-1)^{m(S)-1} m(\cap_{j \in S} A_j) \end{aligned}$$

Thus by induction, we have

$$m(A_1 \cup \dots \cup A_n) = \sum_{S \subseteq \{1, \dots, n\}; S \neq \emptyset} (-1)^{m(S)-1} m(\cap_{j \in S} A_j)$$

## 17. a

Let  $A$  represent the set of Americans gone to high school and  $B$  represent who reads a newspaper. Then  $p(A) = 80\%$  and  $p(B) = 70\%$ . Then

$$p(A \cup B) = p(A) + p(B) - p(A \cap B)$$

Since  $p(A \cup B)$  at max can represent all Americans, i.e. 100%. This gives

$$p(A \cap B) = 70 + 80 - 100 = 50\%$$

Therefore, at least 50% Americans have gone to high school or reads a daily newspaper.

## 18. a

**Solution:** As we are dealing with percentages, let us consider the **total population** be 100. Let us consider  $A, B, C$  be three sets of people such that

$A$  = population agreed with the government on the first decision

$B$  = population agreed with the government on the second decision

$C$  = population agreed with the government on the third decision.

Then by the given condition

$$m(A) = 93\%, \quad m(B) = 84\% \text{ and } m(C) = 74\%.$$

**According to the question we need to find the least value** for  $m(A \cap B \cap C)$ .

Now by Formula

$$m(A \cap B \cap C) = m(A \cup B \cup C) + m(A \cap B) + m(B \cap C) + m(A \cap C) - m(A) - m(B) - m(C).$$

Since

$$m(A \cap B) = m(A) + m(B) - m(A \cup B),$$

it follows that

$$m(A \cap B \cap C) = m(A \cup B \cup C) + m(A) + m(B) + m(C) - m(A \cup B) - m(B \cup C) - m(A \cup C).$$

Now

$$m(A \cup B \cup C) \geq m(A) \implies m(A \cup B \cup C) \geq 93\%.$$

And since the total population is considered to be 100, we have

$$m(A \cup B) \leq 100$$

$$m(A \cup C) \leq 100$$

$$m(C \cup B) \leq 100.$$

Consequently, we have

$$m(A \cap B \cap C) \geq 93 - 100 - 100 - 100 + 93 + 84 + 74 = 44\%.$$

Hence, the least percentage of the population agreed with the government on all three decisions is 44%.  
This completes our solution.

## Result

3 of 3

Result: The least percentage of the population agreed with the government on all three decisions is 44%. Click for the detailed solution.

## 19. a

Let  $A$  and  $B$  are two arbitrary sets, then we have

$$\begin{aligned} A \cap B &= \{s \in S | s \in A \text{ and } s \in B\} \\ &= \{s \in S | s \in A \text{ and } s \notin B'\} \\ &= \{s \in A | s \notin B'\} = A - B' \end{aligned}$$

Further, let consider the sets :

$$\begin{aligned} \textit{Arm} &\equiv \text{set of soldiers who have lost an arm} \\ \textit{Ear} &\equiv \text{set of soldiers who have lost an ear} \\ \textit{Eye} &\equiv \text{set of soldiers who have lost an eye} \\ \textit{Leg} &\equiv \text{set of soldiers who have lost an leg} \end{aligned}$$

Set of soldiers who lost both ear and eye is represented by  $\textit{Ear} \cap \textit{Eye}$ , then using the identity above we obtain that  $\textit{Ear} \cap \textit{Eye} = \textit{Ear} - \textit{Eye}' = \textit{Eye} - \textit{Ear}'$ . Therefore, minimum number of elements of the set  $\textit{Ear} \cap \textit{Eye}$  we obtain if  $\textit{Ear} \subset \textit{Eye}$  or  $\textit{Eye} \subset \textit{Ear}$ .

Hence, at least  $75\% - 30\% = 45\%$  of soldiers have lost both ear and eye.

Analogously, the set of soldiers who lost ear, eye and arm is represented by  $\textit{Ear} \cap \textit{Eye} \cap \textit{Arm}$  then using the identity above we obtain that  $\textit{Ear} \cap \textit{Eye} \cap \textit{Arm} = \textit{Ear} \cap \textit{Eye} - \textit{Arm}'$ .

Hence, at least  $45\% - 20\% = 25\%$  of soldiers have lost ear, eye and arm.

Finally, the set of soldiers who lost ear, eye, arm and leg is represented by  $\textit{Ear} \cap \textit{Eye} \cap \textit{Arm} \cap \textit{Leg}$  then using the identity above we obtain that  $\textit{Ear} \cap \textit{Eye} \cap \textit{Arm} \cap \textit{Leg} = \textit{Ear} \cap \textit{Eye} \cap \textit{Arm} - \textit{Leg}'$ .

Hence, at least  $25\% - 15\% = 10\%$  of soldiers have lost ear, eye and arm.

## Result

Use the identity  $A \cap B = A - B'$ .

## 20. a

Let  $m(A) = k$ , and  $m(B) = n$ .

Let  $A = \{a_1, \dots, a_k\}$  and  $B = \{b_1, \dots, b_n\}$ .

Then each element  $b_i$  of  $B$  produces  $k$  number of ordered pairs corresponding to the  $k$  elements of  $A$ , given by:

$(a_1, b_i), (a_2, b_i), \dots, (a_k, b_i)$ .

Since  $B$  has  $n$  number of elements, and each element of  $B$  produces  $k$  number of ordered pairs, the total number of such ordered pairs equals,

$$k + k + \dots + k \text{ (n times)} = k \times n.$$

Thus,  $m(A \times B) = m(A)m(B)$ .

21. a

**Given:**  $S$  is a set with 5 elements.

**Claim:**

- (a)  $S$  has  $2^5 (= 32)$  subsets.
- (b)  $S$  has 5 subsets containing 4 elements.
- (c)  $S$  has 10 subsets containing 2 elements.

**Proof:** Let  $A$  be the set defined by

$$A := \{X \subset S \mid X \text{ has } k \text{ elements}\}.$$

Then, the cardinality of  $A$  is given by

$$\binom{5}{k} = \frac{5!}{(k!)(5-k)!}.$$

(c) Then, the number of subsets of  $S$  having 2 elements is

$$\binom{5}{2} = \frac{5!}{(2!)(5-2)!} = 10.$$

(b) Similarly, the number of subsets of  $S$  having 4 elements is

$$\binom{5}{4} = \frac{5!}{(4!)(5-4)!} = 5.$$

(a) Now, the number of subsets of  $S$  is equal to the sum of the number of subsets of  $S$  having  $k$  elements, where  $k$  varies from 0 to 5.

Note that,  $\phi$  and  $S$  are the only subsets of  $S$  having 0 and 5 elements respectively.

Let  $n$  be the number of subsets of  $S$ .

Then,

$$\begin{aligned} n &= \sum_{k=0}^5 \binom{5}{k} \\ &= (1+1)^5, \text{ by binomial theorem} \\ &= 32. \end{aligned}$$

This completes our claim.

### Result

4 of 4

- (a)  $S$  has 32 subsets.
- (b)  $S$  has 5 subsets containing 4 elements.
- (c)  $S$  has 10 subsets containing 2 elements.

## 22. a

(a) We have to prove that a set with  $n$  elements has  $2^n$  subsets.

We will prove this using the principle of mathematical induction.

When  $n = 1$ , i.e, the set has only one element, the possible subsets are the empty set, and the set itself. Thus, when  $n = 1$ , the set has  $2^1 = 2$  subsets.

Now, assume that if a set has  $n$  elements, it has  $2^n$  subsets (Induction hypothesis).

To complete the proof by induction, we need to show that a set with  $n + 1$  elements has  $2^{n+1}$  subsets.

Let  $S$  be a set with  $n + 1$  elements, and let  $a$  be an element of  $S$ .

Then the set  $S - \{a\}$  has  $n$  elements. By the Induction hypothesis,  $S - \{a\}$  has  $2^n$  subsets.

Now, all subsets of  $S - \{a\}$  are subsets of  $S$ . Thus  $S$  already has  $2^n$  subsets.

The other subsets of  $S$  all contain  $a$ . Thus, each of them is of the form  $A \cup \{a\}$ , where  $A$  is a subset of  $S - \{a\}$ .

The number of such subsets equal the number of subsets of  $S - \{a\}$ , i.e,  $2^n$ .

Thus the total number of subsets of  $S$  is  $2^n + 2^n = 2^{n+1}$ .

Hence, by induction, a set with  $n$  elements has  $2^n$  elements.

(b) Given a set with  $n$  elements, we need to find the number of subsets it has with exactly  $m$  elements.

This is equivalent to the number of distinct ways we can select  $m$  elements from  $n$  elements;

i.e, the number of possible combinations of  $m$  items from  $n$  items, given by the formula  $\binom{n}{m} = \frac{n!}{m!(n-m)!}$

## Section 1–3

### 1. a

- (a) **NOT** a function. Since every woman is not married, so for every  $s \in S$ ,  $f(s)$  is not defined.
- (b) **NOT** a function. As,  $f(1) = 0 \notin T \implies 1$  does not have any image.
- (c) **YES**, it is a function, as it is well defined, i.e, given any  $s \in S$  we have only one image and for every  $s \in S$  we have an image in  $T$ .
- (d) **NOT** a function. Since,  $f(0) = -1 \notin T$ .
- (e) **YES**, it is a function, as it is well defined, i.e, given any  $s \in S$  we have only one image and for every  $s \in S$  we have an image in  $T$ .
- (f) **NOT** a function. Since square root of a negative real number is not defined.
- (g) **YES**, it is a function, as it is well defined, i.e, given any  $s \in S$  we have only one image and for every  $s \in S$  we have an image in  $T$ .

### Result

See the solution.

### 2. a

- (c) The function is 1 – 1 and onto. For 1 – 1,

$$\begin{aligned} f(s_1) &= f(s_2) \implies s_1 - 1 = s_2 - 1 \\ &\implies s_1 = s_2. \end{aligned}$$

For onto, let  $t \in T \implies t \geq 0$  and  $t \in \mathbb{Z}$ . Define  $s = 1 + t \in \mathbb{Z}^+$  and  $f(s) = t$ .

- (e) The function is 1 – 1 and onto. For 1 – 1,

$$\begin{aligned} f(s_1) &= f(s_2) \implies s_1 - 1 = s_2 - 1 \\ &\implies s_1 = s_2. \end{aligned}$$

For onto, let  $t \in T \implies t \in \mathbb{Z}$ . Define  $s = 1 + t \in \mathbb{Z}$  and  $f(s) = t$ .

- (g) The function is 1 – 1 and onto. For 1 – 1,

$$\begin{aligned} f(s_1) &= f(s_2) \implies \sqrt{s_1} = \sqrt{s_2} \\ &\implies s_1 = s_2. \end{aligned}$$

For onto, let  $t \in T \implies t \in \mathbb{R}^+$ . Define  $s = t^2 \in \mathbb{R}^+$  and  $f(s) = \sqrt{t^2} = t$ .

### Result

See the solution.

### 3. a

Let  $f : S \rightarrow T$  be one to one and onto mapping. Then  $f^{-1} : T \rightarrow S$  is one to one and onto from  $T$  to  $S$ .

Since  $f$  is onto, for all  $y \in T$ , there is  $x \in S$  such that  $f(x) = y$ . And  $f$  is one to one as well,  $f(a) = f(b) \implies a = b$ . Since  $a$  and  $b$  are domain of  $f^{-1}$ , the map is well defined.

Since  $f$  is well defined,  $f^{-1}$  is onto. This also gives  $a = b \implies f(a) = f(b)$ . Since  $f(a)$  and  $f(b)$  are domain of  $f^{-1}$ , it is one to one as well.

#### 4. a

Let  $s \in S$ .

Let  $f(s) = t$ , where  $t \in T$ .

Now,  $f^{-1} \circ f(s) = f^{-1}(f(s)) = f^{-1}(t)$ .

Since  $f$  is a  $1 - 1$  function,

if  $f(s_1) = t = f(s)$  for some  $s_1$  in  $S$ ,

then  $s_1 = s$ .

Thus,  $f^{-1}(t)$  takes only one value in  $S$ , which is  $s$ .

Or,  $f^{-1} \circ f(s) = f^{-1}(t) = s$ .

Hence,

$$f^{-1} \circ f = i_s.$$

#### 5. a

We have to show that if  $g : S \rightarrow T$  and  $f : T \rightarrow U$  are onto,  $f \circ g : S \rightarrow U$  is onto.

Equivalently, by the definition of onto, we need to show that for any element  $u \in U$ , there is an element in  $S$ , say  $s$ , such that  $f \circ g(s) = u$ .

Let  $u \in U$ . Since  $f : T \rightarrow U$  is onto, there exists some  $t \in T$  such that  $f(t) = u$ .

Also, since  $g : S \rightarrow T$  is onto, given  $t$ , there exists some  $s \in S$  such that  $g(s) = t$ .

Now,  $f \circ g(s) = f(g(s)) = f(t) = u$ .

That is, if  $u \in U$ , there exists an  $s \in S$  such that  $f \circ g(s) = u$ .

Or,  $f \circ g : S \rightarrow U$  is onto.

#### 6. a

We have to prove that if  $f : S \rightarrow T$  is onto, and  $g : T \rightarrow U$  and  $h : T \rightarrow U$  are such that  $g \circ f = h \circ f$ ,

then,  $g = h$ .

We start by observing that both  $g$  and  $h$  are defined from  $T$  into  $U$ .

Let  $t$  be an element in  $T$ .

Since  $f$  is onto, there exists  $s \in S$  such that  $f(s) = t$ .

$$g \circ f = h \circ f$$

$$\implies g \circ f(s) = h \circ f(s)$$

Or,  $g(f(s)) = h(f(s))$

$$\implies g(t) = h(t).$$

Since this holds for arbitrary  $t \in T$ , we have that  $g = h$ .

## 7. a

We have to prove that if  $f : T \rightarrow U$  is 1 – 1, and  $g : S \rightarrow T$  and  $h : S \rightarrow T$  are such that  $f \circ g = f \circ h$ ,

then,  $g = h$ .

Let  $s$  be an element in  $S$ .

Let  $t_1 = g(s)$  and  $t_2 = h(s)$  where  $t_1$  and  $t_2$  are elements of  $T$ .

$$\text{Now, } f \circ g = f \circ h$$

$$\implies f \circ g(s) = f \circ h(s).$$

Or,  $f(g(s)) = f(h(s))$

$$\implies f(t_1) = f(t_2).$$

Since  $f$  is 1 – 1, this implies that  $t_1 = t_2$ .

Or,  $g(s) = h(s)$ .

Since this holds for arbitrary  $s \in S$ , we have that  $g = h$ .

## 8. a

**Given:** Let  $S$  be the set of all integers and  $T$  be the set  $\{-1, 1\}$ .

Now we define  $f : S \rightarrow T$  by the following assignment :

$$\begin{cases} f(s) = 1, & \text{if } s \text{ is even.} \\ f(s) = -1, & \text{if } s \text{ is odd.} \end{cases}$$

**To Prove:**

a)  $f$  is a function from  $S$  to  $T$ .

b)  $f(s_1 + s_2) = f(s_1)f(s_2)$ .

c) Is  $f(s_1s_2) = f(s_1)f(s_2)$ ?

**Proof:**

a) Now by the definition of  $f$ ,

$$\begin{cases} f(s) = 1, & \text{if } s \text{ is even.} \\ f(s) = -1, & \text{if } s \text{ is odd.} \end{cases}$$

So, for each element  $s$  in  $S$  there exists a unique image in  $T$ , as an element from  $S$  can either be even or be odd.

So,  $f$  defines a function from  $S$  to  $T$ .

b) Let  $s_1, s_2 \in S$ .

Now, **three** cases arise.

**Case 1:** Both  $s_1$  and  $s_2$  are even.

Then  $s_1 + s_2$  is even.

So,  $f(s_1 + s_2) = 1 = f(s_1)f(s_2)$ . **Done.**

**Case 2:** Both  $s_1$  and  $s_2$  are odd.

Then  $s_1 + s_2$  is even.

So,  $f(s_1 + s_2) = 1$  and  $f(s_1)f(s_2) = (-1) \times (-1) = 1$

Therefore,  $f(s_1 + s_2) = f(s_1)f(s_2)$  in this case.

**Case 3:** One of  $s_1, s_2$  is odd and other is even.

Without loss of generality, let us take  $s_1$  be odd and  $s_2$  be even.

Then,  $f(s_1) = -1$  and  $f(s_2) = 1$  also  $s_1 + s_2$  is odd, so  $f(s_1 + s_2) = -1$ .

Therefore,  $f(s_1 + s_2) = f(s_1)f(s_2) = -1$

**Hence we are done.**

c) Let us take  $s_1$  and  $s_2$  **both odd** in  $S$ .

Then, obviously  $s_1s_2$  is odd.

So,  $f(s_1s_2) = -1$  but  $f(s_1)f(s_2) = (-1) \times (-1) = 1$ .

Therefore,

$f(s_1s_2) \neq f(s_1)f(s_2)$

If both of  $s_1$  and  $s_2$  are odd

in  $S$ .

Hence, generally  $f(s_1s_2) = f(s_1)f(s_2)$  is not true in  $S$ .

### Result

Click for the answer.

9. a

**Given:** Let  $S$  be a set of all Real numbers.

Let us define two functions  $f : S \rightarrow S$  by  $f(s) = s^2$

and  $g : S \rightarrow S$  by  $g(s) = s + 1$ .

## Step 2

a) We now find  $f \circ g$ .

Observe that  $f \circ g$  is a function from  $S$  to  $S$ .

Now, for  $s \in S$

$$f \circ g(s) = f(g(s)) = f(s + 1) = (s + 1)^2$$

So,  $f \circ g(s) = (s + 1)^2$ , for all  $s \in S$

## Step 3

b) We have to find  $g \circ f$ .

Observe that  $g \circ f$  is a function from  $S$  to  $S$ .

Now, for  $s \in S$

$$g \circ f(s) = g(f(s)) = g(s^2) = s^2 + 1$$

So,  $g \circ f(s) = s^2 + 1$ , for all  $s \in S$ .

c) Now from the foregoing activities it yield's that

for any  $s \in S$

$$f \circ g(s) = (s + 1)^2 \text{ and } g \circ f(s) = s^2 + 1$$

Consequently,  $f \circ g \neq g \circ f$  in general.

## Result

Click for the answer.

10. a

**Given:**  $S$  is a set of Real numbers with  $a, b \in S$ , where  $a \neq 0$  and define  $f_{a,b}$  as

$$f_{a,b}(s) = as + b.$$

**Solution:**

(a) Let us consider two elements  $c$  and  $d$  from the set  $S$  different from  $a, b$ . Then by the given condition

$$f_{c,d}(s) = cs + d.$$

Now for any element  $s \in S$  we have

$$\begin{aligned} f_{a,b} \circ f_{c,d}(s) &= f_{a,b}(f_{c,d}(s)) \\ &= f_{a,b}(cs + d) \\ &= a(cs + d) + b \\ &= (ac)s + (ad + b) \\ &= us + v, \text{ taking } ac = u \text{ and } ad + b = v \\ &= f_{u,v}(s). \end{aligned}$$

Hence

$$f_{a,b} \circ f_{c,d} = f_{u,v}, \text{ where } ac = u \text{ and } ad + b = v.$$

(b) If possible, let us assume

$$f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b}.$$

Then by the above problem

$$\begin{aligned} a(cs + d) + b &= c(as + b) + d \implies acs + ad + b = acs + cb + d \\ &\implies d(a - 1) = b(c - 1). \end{aligned}$$

But this is not possible for every value of  $c$  and  $d$ . Therefore

$$f_{a,b} \circ f_{c,d} \neq f_{c,d} \circ f_{a,b}$$

can not be possible always.

(c) Let us consider Two elements  $a$  and  $b$  from the set  $S$ . Then

$$f_{a,b}(s) = as + b.$$

Now,

$$\begin{aligned} f_{a,b} \circ f_{1,1}(s) &= f_{1,1} \circ f_{a,b}(s) \implies f_{a,b}(f_{1,1}(s)) = f_{1,1}(f_{a,b}(s)) \\ &\implies f_{a,b}(s+1) = f_{1,1}(as+b) \\ &\implies a(s+1) + b = 1.(as+b) + 1 \\ &\implies a = 1. \end{aligned}$$

Let us now construct the set  $X$  by

$$X := \{f_{a,b} \mid a = 1\}.$$

Therefore,

$$f_{a,b} \circ f_{1,1} = f_{1,1} \circ f_{a,b} \text{ holds if } f_{a,b} \in X.$$

(d) We have

$$f_{a,b}(s) = as + b.$$

Let us assume  $f_{a,b}(s) = t$  for some  $t$  in  $S$ .

Then we have

$$as + b = t \implies s = \frac{t - b}{a}.$$

Since  $a \neq 0$ ,  $s$  is well defined. Therefore  $f_{a,b}^{-1}$  exists for all  $a, b \in S$ .

And

$$f_{a,b}^{-1}(s) = \frac{s - b}{a} = us + v, \text{ where } u = \frac{1}{a} \text{ and } v = \frac{-b}{a}.$$

## Result

- (a)  $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b}$ .
- (b)  $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b}$  can not be possible always.
- (c)  $f_{a,b} \circ f_{1,1} = f_{1,1} \circ f_{a,b}$  holds if  $a = 1$ .
- (d)  $f_{a,b}^{-1}$  exists for all  $a, b \in S$  and

$$f_{a,b}^{-1}(s) = \frac{s - b}{a} = us + v, \text{ where } u = \frac{1}{a} \text{ and } v = \frac{-b}{a}.$$

Click for the complete solution.

Let  $s$  be a positive integer greater than 3.

Then, by definition,  $f(s) = s$ .

Hence  $f \circ f \circ f(s) = f(f(f(s))) = f(f(s)) = f(s) = s$ .

Now,  $f \circ f \circ f(1) = f(f(f(1))) = f(f(2)) = f(3) = 1$ .

Also,  $f \circ f \circ f(2) = f(f(f(2))) = f(f(3)) = f(1) = 2$ .

And,  $f \circ f \circ f(3) = f(f(f(3))) = f(f(1)) = f(2) = 3$ .

Thus we have showed that for all positive integers, i.e, for all  $x \in S$ ,

$$f \circ f \circ f(x) = x.$$

Thus,  $f \circ f \circ f = i_S$ .

For any positive integer  $s > 3$ ,  $f(s) = s$ .

$$\implies f^{-1}(s) = s \text{ for all such } s.$$

Now,

$$f(1) = 2 \implies f^{-1}(2) = 1.$$

$$f(2) = 3 \implies f^{-1}(3) = 2.$$

$$f(3) = 1 \implies f^{-1}(1) = 3.$$

Thus,  $f^{-1}$  is a function from  $S$  to  $S$ , given by,

$$f^{-1}(x) = \begin{cases} 3 & \text{if } x = 1 \\ 1 & \text{if } x = 2 \\ 2 & \text{if } x = 3 \\ x & \text{if } x > 3 \end{cases}$$

## 12. a

(a) Let  $x = \frac{2}{3} = \frac{4}{6}$ . Then

$$f(2/3) = 2^2 3^3 = 108$$

and

$$f(4/6) = 2^4 3^3 = 11664$$

the map is not well defined so it is not legitimate function.

(b) To make it legitimate function, define  $f$  by

$$f(m/n) = 2^{(\frac{n}{\gcd(m,n)})} 3^{(\frac{m}{\gcd(m,n)})}$$

This makes  $f$  a legitimate function as rational number can be written in different ratios, but for numerator and denominator having gcd equals 1, ratio is always uniquely written.

## 13. a

Let  $s$  be an element of  $S$ .

We need to show that  $f(s)$  takes a unique value in  $T$ .

From the definition of  $S$ , we get that  $s = 2^m 3^n$  for some positive integers  $m, n$ .

Since  $m/n$  is rational,  $f(s)$  takes at least one value in  $T$ , given by

$$f(s) = f(2^m 3^n) = m/n.$$

Now, assume  $s = 2^{m_1} 3^{n_1}$ , where  $m_1$  and  $n_1$  are positive integers.

By the fundamental theorem of arithmetic,

$s$  has a unique prime factorization.

Thus  $m_1 = m$  and  $n_1 = n$ .

Therefore  $f(s)$  takes only one value in  $T$ .

Since  $s$  was an arbitrary element of  $S$ , we have showed that

$f : S \rightarrow T$  takes one and only one value for each element in  $S$ .

In other words,  $f$  defines a function from  $S$  to  $T$ .

#### 14. a

For set of integers  $S$ ,  $f : S \rightarrow S$  be defined by  $f(s) = as + b$ . Then

$$\begin{aligned}f(f(s)) &= f(as + b) \\&= a(as + b) + b \\&= a^2s + ab + b\end{aligned}$$

For  $f \circ f = i_s$ , we have  $a^2s + ab + b = s$ . This gives  $a^2 = 1 \implies a = \pm 1$ . And we must also have

$$ab + b = 0 \implies b(a + 1) = 0$$

if  $a = -1$ , then  $b$  can be any number. If  $a = 1$ , then  $b = 0$ .

#### 15. a

For set of integers  $S$ ,  $f : S \rightarrow S$  be defined by  $f(s) = as + b$ . Then

$$\begin{aligned}f(f(f(s))) &= f(f(as + b)) \\&= f(a(as + b) + b) \\&= f(a^2s + ab + b) \\&= a(a^2s + ab + b) + b \\&= a^3s + b(a^2 + a + 1)\end{aligned}$$

For  $f \circ f \circ f = i_s$ , we have  $a^3s + b(a^2 + a + 1) = s$ . This gives  $a^3 = 1$  and  $b(a^2 + a + 1) = 0$ . Thus  $a = 1$  and  $b = 0$  is the required condition.

#### 16. a

Let us denote  $f^{-1}$  by  $g$ .

Since  $f$  is a 1-1 function from  $S$  onto itself,

by Problem 3,  $f^{-1} = g$  is also a 1-1 function from  $S$  onto itself.

For the same reason,  $g^{-1}$  is also a 1-1 function from  $S$  onto itself.

We have to show that if  $s \in S$ , then

$$g^{-1}(s) = f(s).$$

Let  $g^{-1}(s) = s_1$ .

By the defintion of inverse,

$$g(s_1) = s.$$

But  $g = f^{-1}$ .

Hence,  $f^{-1}(s_1) = s$ .

$$\implies f(s) = s_1.$$

Since  $s_1 = g^{-1}(s)$ ,

we have that  $(f^{-1})^{-1}(s) = f(s)$ .

Since this holds for any  $s \in S$ ,

$$(f^{-1})^{-1} = f.$$

## 17. a

For each element of  $S$ , there are  $m$  choices in codomain for any map. Since there are  $m$  elements in the domain, there must be  $m^m$  such mappings.

## 18. a

If the mapping is one to one, it should be onto as well since the mapping maps to itself which is finite set. Each map is a particular permutation of its elements. There are  $m$  elements in  $S$ , therefore the number of such one to one mapping is  $m!$ .

## 19. a

Let  $S$  be a set of real number and  $f : S \rightarrow S$  be a map defined by  $f(s) = s^2 + as + b$ . Then,

$$f(s_1) = f(s_2) \implies s_1^2 + as_1 + b = s_2^2 + as_2 + b$$

This gives  $s_1 = \pm s_2$  therefore the map is not one to one. Completion of square gives

$$f(s) = (s + \frac{a}{2})^2 + b - \frac{a^2}{4}$$

For no values of  $s$ , there is  $f(s)$  in  $S$  such that  $f(s) < b - \frac{a^2}{4}$ . Therefore  $f$  cannot be onto.

## 20. a

**Given:**  $S$  is a set of positive real numbers with  $a, c > 0$  and  $b, d$  are non-negative real numbers and define a mapping  $f : S \rightarrow S$  by the assignment

$$f(s) = \frac{as + b}{cs + d}.$$

**Solution:** Let us consider an element  $s$  in  $S$  such that

$$f(s) = t, \text{ for some } t \in S.$$

This implies

$$t = \frac{as + b}{cs + d}.$$

Therefore,  $t$  is positive, since  $a, c > 0$  and  $b, d$  are non-negative real numbers and  $s \in S$ . Hence,  $f(t)$  is well defined.

Now

$$f(f(s)) = f(t).$$

Let us concentrate on  $f(t)$ . Let us consider the equation

$$f(t) = s, \text{ that is } f \circ f = i_S.$$

So,

$$\begin{aligned} f(t) = s &\implies \frac{at + b}{ct + d} = s \\ &\implies at + b = cst + ds \\ &\implies a\left(\frac{as + b}{cs + d}\right) + b = cs\left(\frac{as + b}{cs + d}\right) + ds \\ &\implies a(as + b) + b(cs + d) = cs(as + b) + ds(cs + d) \\ &\implies s^2(a + d)c - s(a - d)(a + d) - b(a + d) = 0 \\ &\implies (a + d)(cs^2 - s(a - d) - b) = 0. \end{aligned}$$

Since  $a > 0$  and  $d$  is non-negative

$$cs^2 - s(a - d) - b = 0.$$

This equation holds for every  $s \in S$ . Hence we have

$$b = 0, c = 0, \text{ and } a = d.$$

**Which is an Impossibility, since  $c$  is positive real number.**

Hence our assumption that the existence of  $f$  such that  $f \circ f = i_S$  is wrong.

Therefore there does not exist any  $f$  such that  $f \circ f = i_S$  holds.

This completes our proof.

## Result

3 of 3

Considering any element  $s$  in  $S$  and taking  $f(s) = t$  we have contradict the fact that  $f(t) \neq i_S$  for any chosen  $a, b, c, d$  on  $f$  such that  $f \circ f = i_S$  holds. Click for the complete proof.

21. a

**Given:**  $S$  is the set of all Rational numbers and  $f_{a,b} : S \rightarrow S$  is defined by

$$f_{a,b}(s) = as + b, \text{ where } a \neq 0 \text{ and } b \text{ are rational numbers.}$$

**Solution:** We have

$$\begin{aligned} f_{c,d} \circ f_{a,b} &= f_{a,b} \circ f_{c,d} \implies f_{c,d}(f_{a,b}(s)) = f_{a,b}(f_{c,d}(s)) \\ &\implies f_{c,d}(as + b) = f_{a,b}(cs + d) \\ &\implies c(as + b) + d = a(cs + d) + b \\ &\implies bc - b = ad - d \\ &\implies b(c - 1) = d(a - 1). \end{aligned}$$

Now we have to find all the rational pairs  $(c, d)$  for which

$$b(c - 1) = d(a - 1) \text{ holds.}$$

**Now the only solution to hold the above equation** is  $c = 1$  and  $d = 0$ . Thus  $f_{1,0}$  the only function such that

$$f_{1,0} \circ f_{a,b} = f_{a,b} \circ f_{1,0} \text{ holds.}$$

## Result

Result:  $\{f_{c,d} \mid f_{c,d} \circ f_{a,b} = f_{a,b} \circ f_{c,d}\} = \{f_{1,0}\}$ . Click for the complete solution.

22. a

$f$  is defined by

$$f(s) = as^2 + bs + c,$$

where  $s$  is an integer, and  $a, b, c$  are rationals.

We have to find necessary and sufficient conditions on  $a, b, c$  so that  $f(s)$  is an integer (for all values of  $s$ ).

To find the necessary conditions on  $a, b, c$ , we substitute values for  $s$ .

Since  $a, b, c$  are fixed coefficients, necessary conditions obtained on them using a particular value of  $s$  will hold for all values of  $s$ .

Let  $s = 0$ .

$$f(0) = a \times 0^2 + b \times 0 + c = c.$$

So,  $f(0)$  is an integer

$$\implies c \text{ is an integer.}$$

Let  $s = 1$ .

$$f(1) = a + b + c.$$

Since we have found that  $c$  is an integer,

$$f(1) \text{ is an integer}$$

$\implies f(1) - c = a + b$  is integer valued.

Now, let  $s = 2$ .

$$f(2) = 4a + 2b + c.$$

Since  $c$  is an integer, and  $a + b$  is an integer,

we get that  $2(a + b) + c$  is an integer.

Then,  $f(2)$  is an integer

$\implies f(2) - c - 2(a + b) = 2a$  is integer valued.

Since  $a + b$  and  $2a$  are integer valued,

$$2(a + b) - 2a = 2b \text{ is integer valued.}$$

Also, since  $a + b$  is integer valued,

$a, b$  are either both integers, or both odd multiples of  $\frac{1}{2}$ .

We have obtained the necessary conditions on  $a, b, c$  as:

(1)  $c$  is an integer.

(2)  $a$  and  $b$  are both integers or both odd multiples of  $\frac{1}{2}$ .

We will now show that these conditions are sufficient for  $f(s)$  to be integer valued.

If  $a$  and  $b$  are both integer valued,

$$f(s) = as^2 + bs + c \text{ is integer valued.}$$

Take  $a, b$  to be both odd multiples of  $\frac{1}{2}$ .

$$f(s) = as^2 + bs + c.$$

If  $s$  is even valued,  $as^2$  and  $bs$  are both integers.

Then  $f(s)$  is integer valued.

If  $s$  is odd,  $f(s) = as^2 + bs + c = s(as + b) + c$  is integer valued,

because  $as + b =$  sum of two odd multiples of  $\frac{1}{2}$ , which is an integer.

Thus we have proved that conditions (1) and (2) are necessary and sufficient for  $f$  to be a function on  $S$ .

23. a

Arrange the elements of  $S$  in ascending order.

$$S = \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, \dots\}$$

Define  $f : S \rightarrow T$  by

$$f(s) = (\text{number of elements of } S \text{ which are smaller than } s) + 1.$$

For example,  $f(1) = 1$ ,

$$f(9) = 6 + 1 = 7,$$

$$f(16) = 8 + 1 = 9, \text{ and so on.}$$

We will prove that  $f$  is a 1-1 function from  $S$  onto  $T$ .

To prove that  $f$  is 1-1,

assume that  $s_1, s_2$  are elements of  $S$  such that

$$f(s_1) = f(s_2).$$

Denote  $f(s_1) = f(s_2)$  by  $n$ .

By definition,  $f(s_1) = n$

$\implies$  there are  $n - 1$  elements in  $S$  which are smaller than  $s_1$ .

Or,  $s_1$  is the  $n$ th element in  $S$ , in ascending order.

Also,  $f(s_2) = n$

$\implies$  there are  $n - 1$  elements in  $S$  smaller than  $s_2$ .

Or  $s_2$  is the  $n$ th element of  $S$ , in ascending order.

Hence,  $s_1 = s_2$ .

Therefore  $f$  is a 1-1 function.

To prove that  $f$  maps  $S$  onto  $T$ ,

consider an element  $m$  in  $T$ .

Arrange  $S$  in ascending order,

and find the  $m$ th smallest element in  $S$ . Call it  $s$ .

Then,

$$f(s) = (m - 1) + 1 = m.$$

Hence  $f$  is an onto function.

Thus, we have proved that the function  $f$ , as defined above,

is a 1-1 correspondence from  $S$  onto  $T$ .

24. a

We want to find a  $1 - 1$  correspondence between  $\mathbb{Z}^+$  and  $\mathbb{Q}^+$ . First we observe that by the *Fundamental Theorem of Arithmetic*, any positive integer can be written as  $2^{m-1} \cdot (2n - 1)$ , a product of power of 2 and an odd number. Now we define a map

$$\phi : \mathbb{Q}^+ \rightarrow \mathbb{Z}^+, \frac{m}{n} \mapsto 2^{m-1}(2n - 1)$$

where we are considering that  $m$  and  $n$  are relatively prime. Similarly, we define the inverse mapping as

$$\begin{aligned}\phi^{-1}(k) &= \phi^{-1}(2^{m-1} \cdot (2n - 1)), \text{ for some } m, n \in \mathbb{Z}^+ \\ &= \frac{m}{n}\end{aligned}$$

### Result

A bijection between  $\mathbb{Q}^+$  and  $\mathbb{Z}^+$ .

### 25. a

Let  $S$  be set of real numbers and  $T$  be set of positive reals. Choose  $a > 1$  and define a map  $f : S \rightarrow T$  by  $f(s) = a^s$ . Then

$$f(s_1 + s_2) = a^{s_1+s_2} = a^{s_1}a^{s_2} = f(s_1)f(s_2)$$

Since  $a > 1$ , the range is  $(0, \infty)$  therefore  $f$  is onto on  $T$ . This is clearly one to one as

$$a^{s_1} = a^{s_2} \implies a^{s_1-s_2} = 0 \implies s_1 - s_2 = 0 \implies s_1 = s_2$$

### 26. a

Let  $S$  be set of real numbers and  $T$  be set of positive reals, and  $a > 1$ . Define  $\log_a s = k$  if  $s = a^k$ . Then

$$f^{-1}(f(s)) = f^{-1}(a^s) = a$$

and

$$f(f^{-1}(a^s)) = f(s) = a^s$$

Thus,  $f^{-1}(s) = \log_a(s)$ .

### 27. a

(a) If  $g$  is onto function, then  $g$  is one to one as well. Since  $\{g(s) : s \in S\} = S$ , then  $\{f(g(s)) : g(s) \in S\} = \{\text{constant}\}$ . This implies  $f$  must be a constant function.

(b) If  $f$  is one to one of  $S$  into itself, for  $s_1, s_2 \in S$ ,  $f(s_1) = f(s_2) \implies s_1 = s_2$ . Or, using contraposition logic,  $s_1 \neq s_2 \implies f(s_1) \neq f(s_2)$ . Since  $f \circ g$  is constant function,  $g(s) = s_1 = s_2$  for all  $s \in S$  i.e.  $g$  must be a constant function.

### 28. a

Given  $S$  is a finite set and  $f$  is mapping of  $S$  onto itself i.e. for every  $s' \in S$ , there is  $s \in S$  such that  $f(s) = s'$ . Suppose  $s_1, s_2 \in S$  such that  $s_1 \neq s_2$  and  $f(s_1) = f(s_2)$  then domain of  $f$  is greater than co-domain of  $f$ . This contradicts that  $f$  is mapping of  $S$  onto itself. Therefore  $f(s_1) = f(s_2) \implies s_1 = s_2$ . Hence the mapping is one to one.

29. a

Let  $S$  be a finite set and  $f$  is one to one mapping of  $S$  into itself. i.e.  $f(b) = f(a) \implies b = a$ . Each element on set  $\{f(s) : s \in S\}$  is distinct as  $s_1 \neq s_2 \implies f(s_1) \neq f(s_2)$ . Therefore  $\{f(s) : s \in S\} = S$  and  $f$  is onto.

30. a

Let  $S$  be a finite set having  $m$  elements and  $f$  is one to one mapping of  $S$ . Let  $a, b \in S$  such that  $f(a) = b$ , if  $f^2(a) \neq b$  then  $f^2$  maps  $a$  to some other element other than  $b$  (bijective mapping). Similarly if  $f^3(a) \neq b$ , then  $f^3$  maps  $a$  to some element other than  $b$  and  $f^2(a)$ . Continuing this way, since element of  $S$  is finite,  $f^k(a) = b$  for some  $k \geq 1$ . For every element  $a_i \in S$ , there is a positive integer  $k_i$  such that  $f^{k_i}(a_i) = f(a_i)$ . Then  $f^{k_i-1}(a_i) = a_i$  for all  $a_i \in S$ . Take  $n = \text{lcm}(k_1 - 1, k_2 - 1, \dots, k_m - 1)$ , then

$$f^n(a) = i_S(a) = a$$

for all  $a \in S$ .

31. a

**Solution:** By the given condition  $S$  is a finite set of  $m$  elements and let us consider an arbitrary  $1 - 1$  mapping  $f$  on  $S$ .

**Claim:**  $f$  is surjective.

**Proof of the Claim:** Since  $f$  is  $1 - 1$  mapping from  $S$  onto itself, we have

$$f(a) = f(b) \implies a = b, \text{ for any } a, b \in S.$$

Now

**the set  $\{f(s) \mid s \in S\}$  is finite and each element of the set  $\{f(s) \mid s \in S\}$  is distinct**

since

$$s_1 \neq s_2 \implies f(s_1) \neq f(s_2).$$

Therefore,

$$\{f(s) \mid s \in S\} = S$$

and this implies  $S$  is surjective. This completes our Claim.

Let us now consider an element  $s$  in  $S$  and arrange

$$f(s) = s_1, f(s_1) = s_2, \dots, f(s_{m-1}) = s_m.$$

Since  $S$  has only  $m$  elements, at least one element among  $\{s_1, s_2, \dots, s_m\}$  must equal to  $s$ . Let us assume  $s = s_k$  where  $k \in \{1, 2, \dots, m\}$ .

Then,

$$f \circ f \circ \dots \circ f(s) = s, \text{ where } f \text{ is taken } k \text{ times.}$$

That is

$$f^k(s) = s.$$

Now

$$f^{2k}(s) = f^k(f^k(s)) = f^k(s) = s.$$

**Using induction** we have

$$f^{dk}(s) = s, \text{ for any positive integer } d.$$

Thus corresponding to each  $s$  in  $S$  we get a positive integer  $k$  such that

$$f^k(s) = s, \text{ and } 1 \leq k \leq m.$$

Now we have

$$f^{m!}(s) = s \quad \forall s \in S$$

since every integers  $k$  divides  $m!$ , where  $1 \leq k \leq m$ . Then

$$f^{m!} = f \circ f \circ \dots \circ f = i_s, \text{ where } f \text{ is taken } m! \text{ times.}$$

Since  $f$  is an arbitrary  $1 - 1$  function from  $S$  to itself, the aforesaid result holds for every  $1 - 1$  functions from  $S$  to itself.

Hence, the required integer  $n$  is  $m!$ .

This completes our solution.

### Result

The required integer  $n$  is  $m!$ . Click for the complete solution.

## Section 1–4

### 1. a

By definition  $A(S)$  is the set of all maps that permutes elements of  $S$ . As there are  $n!$  permutations of  $S$ , there must be  $n!$  maps in  $A(S)$ . For  $s_1 \neq s_2$ ,  $s_1 \rightarrow s_2$  represents a permutation of set  $S$ . Therefore there must exists a map  $f \in A(S)$  such that  $f(s_1) = s_2$ .

### 2. a

Let  $s_1 \in S$  and  $H = \{f \in A(S) | f(s_1) = s_1\}$ .

(a)  $i(s) = s$  for all  $s \in S$  so  $i(s_1) = s_1 \implies i \in H$

(b) Let  $f, g \in H$ , then  $f(s_1) = s_1$  and  $g(s_1) = s_1$ . Then

$$g \circ f(s_1) = g(f(s_1)) = g(s_1) = s_1$$

Therefore  $gf \in H$ .

(c) If  $f \in H$  then  $f^{-1} \in A(S)$  such that  $f^{-1}f = ff^{-1} = i$ . This gives

$$f^{-1} \circ f(s_1) = s_1 \implies f^{-1}(s_1) = s_1$$

Therefore  $f^{-1} \in H$ .

### 3. a

Suppose  $s_1 \neq s_2$  are in  $S$  and  $f(s_1) = s_2$ , where  $f \in A(S)$  and  $H = \{h \in A(S) | h(s_1) = s_1\}$  and  $K = \{g \in A(S) | g(s_2) = s_2\}$ .

(a) If  $g \in K$  then

$$f^{-1} \circ g \circ f(s_1) = f^{-1}(g(f(s_1))) = f^{-1}(g(s_2)) = f^{-1}(s_2) = s_1$$

This shows that  $f^{-1}gf \in H$ .

(b) Applying  $h$  to  $f$  and  $f^{-1}$  to  $hf$ , we get

$$fhf^{-1} = ff^{-1}gff^{-1} = g$$

This is equivalent to showing that for any  $h \in H$ ,  $fhf^{-1} \in K$ .

$$fhf^{-1}(s_2) = fh(s_1) = f(s_1) = s_2$$

This shows that  $f hf^{-1} = g \in K$ .

### 4. a

If  $f, g, h \in A(S)$ , then using associativity of maps

$$\begin{aligned} (f^{-1}gf)(fhf^{-1}) &= (f^{-1}g)(ff^{-1})(hf) \\ &= (f^{-1}g)(hf) \\ &= f^{-1}(gh)f \end{aligned}$$

This shows that

$$(f^{-1}gf)^2 = f^{-1}g^2f$$

One can show that using induction hypothesis  $(f^{-1}gf)^k = f^{-1}g^kf$ ,

$$(f^{-1}gf)^{k+1} = (f^{-1}g^kf)(f^{-1}gf) = f^{-1}g^{k+1}f$$

Thus, by induction, we have

$$(f^{-1}gf)^n = f^{-1}g^n f$$

### 5. a

Given  $g, f \in A(S)$ , and  $gf = fg$ .

(a) Using the associativity property of maps and the given assumption, we get

$$(fg)^2 = (fg)(fg) = f(gf)g = f(fg)g = (ff)(gg) = f^2g^2$$

(b) We use the property that  $(fg)^{-1} = g^{-1}f^{-1}$  and the given assumption. This gives

$$(fg)^{-1} = (gf)^{-1} = f^{-1}g^{-1}$$

### 6. a

Let us prove this by using mathematical induction. This is trivially true for  $n = 1$  as  $(fg)^1 = fg$ . Let this be true for some natural number  $k$ . Then, as induction hypothesis, let this be true for some integer  $k$ . i.e.

$(fg)^k = f^k g^k$ . Then this implies

$$\begin{aligned}(fg)^{k+1} &= (fg)^k (fg) \\&= f^k g^k fg \\&= f^k g^{k-1} (gf) g \\&= f^k g^{k-1} (fg) g \\&= f^k g^{k-1} fg^2\end{aligned}$$

Continuing this way, we get  $f^k f g g^k = f^{k+1} g^{k+1}$ . By induction this works for all natural number  $n$ . To show that this holds for all integers, we show that this result holds for  $(fg)^{-n}$  as well. Using result from 5(b)

$$(fg)^{-1} = f^{-1} g^{-1}$$

we get

$$(fg)^{-n} = (f^{-1} g^{-1})^n$$

Since  $fg = gf \implies g^{-1} f^{-1} = f^{-1} g^{-1}$ , we have

$$(f^{-1} g^{-1})^n = f^{-n} g^{-n}$$

which shows that

$$(fg)^n = f^n g^n$$

for all integers.

## 7. a

**To Prove:**  $f^r f^s = f^{r+s}$  and  $(f^r)^s = f^{rs}$ , for  $f \in A(S)$  and positive integers  $r, s$ .

**Proof:** We will use induction on  $s$  to prove the above.

**Step-1:** Let us consider  $s = 1$ .

Then,

$$f^r f^1 = f^r f = f^{r+1}.$$

Also,

$$(f^r)^1 = f^r = f^{r \cdot 1}.$$

Hence, the statement is true for  $s = 1$ .

**Step-2:** Let us assume that our statement is true for all positive integers less than  $s$ . Then it suffices to show that our statement is true for  $s$ .

Now,

$$\begin{aligned}f^r f^s &= f^r f^{s-1} f^1, \text{ by Step-1} \\&= f^{r+s-1} f^1, \text{ by inductive hypothesis} \\&= f^{(r+s-1)+1}, \text{ by Step-1} \\&= f^{r+s}.\end{aligned}$$

Again,

$$\begin{aligned}(f^r)^s &= (f^r)^{s-1}(f^r)^1 \\&= f^{r(s-1)}f^r, \text{ by inductive hypothesis} \\&= f^{r(s-1)+r} = f^rs.\end{aligned}$$

Hence, we have proved that our statement is true for  $s$ , whenever it is true for all positive integers less than  $s$ .

So, by law of induction it's done.

This completes the proof.

## Result

3 of 3

We use the law of induction on  $s$  to prove that  $f^r f^s = f^{r+s}$  and  $(f^r)^s = f^{rs}$ , for  $f \in A(S)$  and positive integers  $r, s$ .

Click for the detailed proof.

### 8. a

Let  $f, g \in A(S)$  and  $(fg)^2 = f^2g^2$ . Applying  $f^{-1}$  on both sides from left, we get

$$f^{-1}(fg)^2 = f^{-1}f^2g^2 \implies f^{-1}(fg)(fg) = fg^2 \implies gfg = fg^2$$

Applying  $gfg = fg^2$  to  $g^{-1}$  from left side, we get

$$gfgg^{-1} = fg^2g^{-1} \implies gf = fg$$

### 9. a

!!!

### 10. a

Let  $S = \{x_1, x_2, x_3\}$  and  $f \in S_3$  and  $f(x_1) \neq x_1$ . Since there are only finite number of choices in  $S$ , either  $f^2(x_1) = x_1$  or  $f^3(x_1) = x_1$ . Similarly for other members  $x_2$  and  $x_3$ ,  $f$  satisfies  $f^2(x) = x$  or  $f^3(x) = x$ . This gives  $f^6(x) = x$  for all members of  $S$  since  $6 = 3 \cdot 2$ .

### 11. a

For  $m = 24$ ,  $f^m = i$  for all  $f \in S_4$ . This is because, for any particular element  $f \in S_4$  and some  $x \in S$ ,  $f(x) \neq x \implies f^i(x) = x$  for some  $i = 2, 3, 4$  because there are only finite choices in  $S$  (only other three remaining).

This shows that  $f^{24}(x) = x$  for all  $x \in S$  because each of 2,3,4 cycles that would map  $x$  to itself would be complete on 24 as 24 is multiple of all.

### 12. a

Let  $f \in S_n$ . Consider the positive powers of  $f$  i.e.  $f^1, f^2, f^3, \dots, f^n$ . Since there are finite number of elements in  $S_n$ , the sequence  $f^1, f^2, f^3, \dots, f^m$  must repeat itself at certain say  $k + 1$ . Let  $f^{k+1} = f$ . This gives  $f^k = i$ .

### 13. a

From problem 12, we know that for  $f \in S_n$  there exists some  $k$  such that  $f^k = i$ . Let  $t$  be the least common multiple of all such  $k$ 's for all  $f$ . Then for all  $f \in S_n$ , we have  $f^t = i$  because  $f$  is a multiple of  $k$  and  $(k^k)^m = i$  where  $t = mk$ .

#### 14. a

Let  $f \in S_m$ .

Define  $f_1 \in S_n$ , corresponding to  $f$ , by:

$$f_1(s) = \begin{cases} f(s) & \text{if } s \leq m \\ s & \text{if } s > m \end{cases}$$

where  $s$  takes integer values from 1 to  $n$ .

Let  $F(f) = f_1$  for each  $f \in S_m$ .

To prove that  $F$  is 1-1, consider  $f, g \in S_m$ .

Let  $f_1 = F(f)$ ,  $g_1 = F(g)$ .

If  $F(f) = F(g)$ , i.e.,  $f_1 = g_1$ ,

Then for  $1 \leq s \leq n$ ,

$$f_1(s) = g_1(s).$$

$$\implies f(s) = g(s) \text{ for } s \leq m.$$

$$\implies f = g.$$

Thus,  $F$  is a 1-1 function.

Given  $f, g \in S_m$ ,

denote  $g(s)$  by  $s_1$  for all  $s \leq m$ .

Note that  $s_1 \leq m$  because  $g(s) \in \{1, 2, \dots, m\}$ .

If  $s > m$ ,

then, by definition,  $F(fg)(s) = s$ .

$$F(f)F(g)(s) = f_1g_1(s) = f_1(g_1(s)) = f_1(s) = s.$$

If  $s \leq m$ , then,

$$F(fg)(s) = F(f(g(s))) = F(f(s_1)) = f(s_1).$$

$$\begin{aligned} F(f)F(g)(s) &= F(f)[F(g(s))] = F(f)(g_1(s)) \\ &= F(f)(g(s)) = F(f)(s_1) = f_1(s_1) = f(s_1). \end{aligned}$$

Thus  $F(fg)(s) = F(f)F(g)(s)$  for all  $s \leq n$ .

Since  $f, g$  were arbitrary elements in  $S_m$ , we have that

$$F(fg) = F(f)F(g) \text{ for all } f, g \in S_m.$$

#### 15. a

**Given:**  $S$  is a set of 3 or more elements.

**To Construct:** Two elements  $f, g$  in  $A(S)$  such that  $fg \neq gf$ .

**Construction:** Let us fix three elements of  $S$ , say  $x_1, x_2, x_3$ .

Let us now define  $f : S \rightarrow S$  by

$$f(x_1) = x_2, f(x_2) = x_3, f(x_3) = x_1 \text{ and } f(x) = x, \text{ for all other } x \text{ in } S.$$

Let us define  $g : S \rightarrow S$  by

$$g(x_1) = x_2, g(x_2) = x_1 \text{ and } g(x) = x, \text{ for all other } x \text{ in } S.$$

Then clearly by definition it follows that both of  $f, g$  are belongs to  $A(S)$ .

Now,

$$fg(x_1) = f(g(x_1)) = f(x_2) = x_3.$$

And,

$$gf(x_1) = g(f(x_1)) = g(x_2) = x_1.$$

This implies,

$$fg(x_1) \neq gf(x_1).$$

Hence,

$$fg \neq gf, \text{ where } f, g \in A(S).$$

Here we are done.

## Result

2 of 2

Constructing two elements  $f, g \in A(S)$  by fixing 3 elements on  $S$ , we have constructed  $f$  and  $g$  in such a way that  $fg \neq gf$ .

Click for the complete proof.

## 16. a

**Given:**  $S$  is an infinite set and  $M$  is a subset of  $A(S)$  given by

$$M := \{f \in A(S) \mid f(s) \neq s \text{ at most at finite number of points } s \in S\}.$$

**To Prove:**  $M$  forms a group under multiplication.

**Proof:** We need to show that

$$f, g \in M \implies fg \in M \text{ and } f \in M \implies f^{-1} \in M.$$

Let us assume that  $S_f$  be a finite subset of  $S$  with  $n$  elements (without loss of generality) such that

$$f(s) = s, \text{ for all } s \in S - S_f.$$

Similarly, again assume that  $S_g$  be a

**finite subset of  $S$  with  $m$  elements**

such that

$$g(s) = s, \text{ for all } s \in S - S_g.$$

Let us consider

$$S_{fg} = S_f \cup S_g.$$

Then

$$S - (S_f \cup S_g) = (S - S_f) \cap (S - S_g).$$

Therefore,

$$s \in S - (S_f \cup S_g) \text{ if and only if } s \in (S - S_f) \text{ and } s \in (S - S_g).$$

Thus if  $s \in S - (S_f \cup S_g)$ ,

$$f(s) = s \text{ and } g(s) = s.$$

This implies,

$$fg(s) = f(s) = s.$$

Since  $S_f \cup S_g$  has

**atmost  $n + m$  elements**

we have

$$fg(s) \neq s, \text{ for at most at finitely many } s$$

$$\implies fg \in M.$$

Now we show that  $f^{-1} \in M$ .

Let  $S_f$  be an finite subset of  $S$  with  $n$  elements such that

$$f(s) = s, \text{ for all } s \in S - S_f.$$

Since  $f$  is a bijective function

$$f(s) = s \implies f^{-1}(s) = s.$$

Therefore,

$$f^{-1}(s) = s, \text{ for all } s \in S - S_f.$$

Hence,

$$f^{-1}(s) \neq s, \text{ at most } n \text{ number of elements of } S.$$

Thence,

$$f^{-1} \in M.$$

This completes the proof.

## Result

3 of 3

Considering two elements  $f$  and  $g$  in  $M$  we have shown that  $fg(s) \neq s$  for at most a finite number of elements of  $S$  and then for  $f^{-1}$  too, to show that  $fg$  and  $f^{-1}$  belongs to  $M$ . Click for the detailed proof.

17. a

**To Prove:**  $fMf^{-1} = M$  if  $f \in A(S)$ .

**Proof:** Let us consider an element  $g$  in  $M$ . Let  $S_g \subset S$  with  $n$  elements such that

$$g(s) = s, \text{ for all } s \in S - S_g.$$

We will propose to prove that  $fMf^{-1} = M$ . We will first show that

$$fMf^{-1} \subset M.$$

Let us assume  $x \in fMf^{-1}$ . Then there exists an element  $g$  in  $M$  such that

$$x = fgf^{-1}.$$

Let us define

$$S_x := \{f^{-1}(s) \mid s \in S_g\}.$$

Then  $t \in S_x$  if and only if  $f(t) \in S_g$ .

Equivalently,

$$t \in S - S_x \text{ if and only if } f(t) \in S - S_g.$$

Thus if  $t \in S - S_x$  then

$$g(f(t)) = f(t).$$

Hence,

$$f^{-1}(g(f(t))) = f^{-1}(f(t)) = t.$$

Therefore,

$$h(t) = f^{-1}gf(t) = t, \text{ for all } t \in S - S_x.$$

Since  $S_x$  has only  $n$  elements

$$\begin{aligned} h &= f^{-1}gf \in M, \text{ for all } g \in M \\ \implies f^{-1}Mf &\subset M. \end{aligned}$$

Now we will show the other side, that is,

$$M \subset f^{-1}Mf.$$

Let us consider an element  $g$  in  $M$ . Then take

$$h = fgf^{-1}.$$

Then,

$$hf = fg \implies g = f^{-1}hf.$$

Let us atke

$$S_h := \{f(s) \mid s \in S_g\}.$$

Then

$$t \in S_h \text{ if and only if } f^{-1}(t) \in S_g.$$

Thence,

$$t \in S - S_h \text{ if and only if } f^{-1}(t) \in S - S_g.$$

Therefore, if  $t \in S - S_h$  then we have

$$h(t) = fgf^{-1}(t) = f[g(f^{-1}(t))] = f[f^{-1}(t)] = t.$$

This gives

$$h \in M.$$

Therefore,

$$g = f^{-1}hf \in f^{-1}Mf.$$

Hence

$$M \subset f^{-1}Mf.$$

Consequently we have

$$M = f^{-1}Mf.$$

This completes the proof.

### Result

3 of 3

In order to show that  $M = f^{-1}Mf$  we have proved that for any element  $h$  in  $M$ ,  $h$  also belongs to  $f^{-1}Mf$  and vice-versa. Click for the complete proof.

## 18. a

**Given:**  $U(T)$  is a subset of  $A(S)$  given by

$$U(T) := \{f \in A(s) \mid f(t) \in T \text{ for every } t \in T\},$$

where  $T \subset S$ .

**To Prove:**

$$(a) \ i \in U(T).$$

$$(b) \ f, g \in U(T) \implies fg \in U(T).$$

**Proof:**

(a) Let us consider any  $t \in T$ .

Then,

$$i(t) = t, \text{ by definition.}$$

So we have,

$$i(t) \in T \text{ for every } t \in T.$$

This implies,

$$i \in U(T).$$

(b) Let us take  $f, g$  in  $U(T)$ . Let  $t \in T$ .

Then,

$$f(t), g(t) \in T \text{ for every } t \in T.$$

Let us denote,  $g(t) = t' \in T$ .

Then,

$$fg(t) = f(g(t)) = f(t') = t'',$$

for some  $t'' \in T$  since  $f \in U(T)$ .

Since,  $t$  is chosen arbitrary it follows that  $fg \in U(T)$  for  $f, g \in U(T)$ .

This completes the proof.

**Result**

3 of 3

Being  $i$  is the identity map, trivially  $i \in U(T)$  and considering an arbitrary  $t \in T$  we have proved that  $fg(t) \in T$ , follows the result.

[Click for the detailed proof.](#)

**19. a**

**Solution:** By the given condition  $S$  has  $n$  elements and  $T$  has  $m$  elements. Let us consider

$$S = \{x_1, x_2, \dots, x_m, \dots, x_n\} \text{ and } T = \{x_1, x_2, \dots, x_m\}.$$

Let us assume  $f \in U(T)$ .

**Then  $f(x_1) \in T$ . Therefore  $f$  has  $m$  choices for  $x_1$ .**

Similarly,  $f$  has  $m - 1$  choices for  $x_2$ , again  $f$  has  $m - 2$  choices for  $x_3$  and so on upto  $x_m$ , for which  $f$  has only one choice. Now all the  $m$  elements get exhausted, so there is no choice left for the element  $x_{m+1}$ . Therefore, we have only  $n - m$  elements in the set  $S - T$ . So,  $f(x_{m+1})$  have  $n - m$  choices.

Similarly,  $f(x_{m+2})$  have  $n - m - 1$  choices to fulfill. Continuing successively, we have only one choice for  $f(x_n)$ .

Therefore,

**Number of elements of  $U(T)$  = Total number of ways we can construct  $f$**

$$\begin{aligned} &= m.(m-1)\dots2.1.(n-m)(n-m-1)\dots2.1 \\ &= (m!).(n-m)! \end{aligned}$$

Therefore  $U(T)$  has  $(m!).(n-m)!$  elements.

Now we will prove **the existence of a mapping**  $F : U(T) \rightarrow S_m$  such that  $F$  is onto on  $S_m$  and

$$F(fg) = F(f)F(g), \text{ for } f, g \in U(T).$$

Let us consider an element  $f$  in  $U(T)$ . And define  $F(f)$  by the assignment

$$F(f)(t) = f(t), \text{ for all } t \in T.$$

Then we have

$$F(fg)(t) = fg(t), \text{ for all } t \in T.$$

Again for all  $t \in T$  we have

$$F(f)F(g)(t) = F(f)[F(g)(t)] = F(f)[g(t)] = f(g(t)) = fg(t).$$

Therefore,

$$F(fg) = F(f)F(g).$$

So, enough to prove now,  $F$  is onto on  $S_m$ .

To prove  $F$  is onto on  $S_m$  let us consider an element  $h$  in  $S_m$ .

Now define  $f_h : S \rightarrow S$  by the assignment

$$f_h(t) = \begin{cases} h(t) & \text{if } t \in T \\ t & \text{if } t \in S - T. \end{cases}$$

Then trivially

$$f_h \in U(T)$$

and

$$F(f_h(t)) = h(t), \text{ for all } t.$$

Therefore for each  $h$  in  $S_m$ , we can find a pre-image  $f_h$  of  $h$  in  $U(T)$ . Hence  $F$  is onto on  $S_m$ .

This completes the proof of existence of the function  $F$ .

## Result

4 of 4

Firstly we have proved that  $U(T)$  has  $m!(n-m)!$  elements, and then by defining  $F$  by  $F(f)(t) = f(t)$  in  $U(T)$  we have proved the existence of a mapping  $F : U(T) \rightarrow S_m$  such that  $F$  is onto on  $S_m$  and  $F(fg) = F(f)F(g)$ , for  $f, g \in U(T)$ . Click for the complete proof.

20. a

**Solution:**  $F$  will be  $1 - 1$  if  $m = n - 1$ . We will propose to prove it below.

Let us consider two elements  $f, g \in U(T)$  such that

$$F(f) = F(g).$$

It follows that

$$\begin{aligned} F(f)(t) &= F(g)(t), \text{ for all } t \in T \\ \implies f(t) &= g(t), \text{ for all } t \in T. \end{aligned}$$

Since  $S$  has  $n$  elements,  $T$  has  $m$  elements and  $n = m + 1$ ,  $S - T$  is a **singleton set**, say

$$S - T := \{x\}.$$

**Since  $f$  is an injective function and all values of  $T$  are already taken**

, we must have  $f(x) \in S - T$ . This implies

$$f(x) = x.$$

Similarly, by aforesaid argument we can conclude that

$$g(x) = x.$$

Hence,

$$f(x) = g(x).$$

Therefore, we have

$$f(s) = g(s), \text{ for all } s \in S.$$

Hence for any two elements  $f, g \in U(T)$ ,

$$F(f) = F(g) \implies f = g.$$

Therefore,  $F$  is  $1 - 1$ , when  $m = n - 1$ .

This completes the proof.

## Result

$F$  will be  $1 - 1$  when  $m = n - 1$ . Click for the detailed proof.

21. a

**Solution:** Let us consider a mapping  $g_i : S \rightarrow S$  by the assignment

$$g_i(x) = \begin{cases} x_{i+1}, & x = x_i \\ x_i, & x = x_{i+1} \\ x, & \text{otherwise} \end{cases}$$

Then it follows that  $g_1$  takes  $x_1$  to  $x_2$  and  $x_2$  to  $x_1$  and leaves other elements unaltered. Similarly,  $g_2$  takes  $x_2$  to  $x_3$  and  $x_3$  to  $x_2$  and leaves other elements unaltered. Proceeding like this way, we came across a decision that,  $g_{n-1}$  takes  $x_{n-1}$  to  $x_n$  and  $x_n$  to  $x_{n-1}$  and leaves other elements unchanged.

Now it follows that

$$\begin{aligned} g_1g_2\dots g_{n-2}g_{n-1}(x_1) &= g_1g_2\dots g_{n-2}(g_{n-1}(x_1)) \\ &= g_1g_2\dots g_{n-3}g_{n-2}((x_1)) \\ &= g_1g_2\dots g_{n-4}g_{n-3}((x_1)) \\ &= \dots = g_1(x_1) = x_2 = f(x_1). \end{aligned}$$

Again, we have

$$\begin{aligned} g_1g_2\dots g_{n-2}g_{n-1}(x_n) &= g_1g_2\dots g_{n-2}(g_{n-1}(x_n)) \\ &= g_1g_2\dots g_{n-3}(g_{n-2}(x_{n-1})) \\ &= g_1g_2\dots g_{n-4}(g_{n-3}(x_{n-2})) \\ &= \dots = g_1(g_2(x_3)) \\ &= g_1(x_2) = x_1 = f(x_n). \end{aligned}$$

Now for  $1 < i < n$ ,

$$\begin{aligned} g_1g_2\dots g_{n-2}g_{n-1}(x_i) &= g_1g_2\dots g_i(x_i) \\ &= g_1g_2\dots g_{i-1}(x_{i+1}) \\ &= x_{i+1} = f(x_i). \end{aligned}$$

Hence,

$$f = g_1g_2\dots g_{n-2}g_{n-1}.$$

This completes the proof.

## Result

2 of 2

Considering a mapping  $g_i$  as sending  $x_i$  to  $x_{i+1}$  and  $x_{i+1}$  to  $x_i$  and unchanged for others we have shown that  $f$  can be written as  $f = g_1g_2\dots g_{n-1}$ , for some  $g_i$  in  $S_n$ . Click for the complete proof.

22. a

**Given:**  $f$  is an element of  $S_n$ .

**To Prove:**  $f = h_1 h_2 \dots h_m$  for some  $h_j \in S_n$  such that  $h_j^2 = i$ .

**Proof:** Let us consider the set of elements

$$S := \{x_1, x_2, \dots, x_n\}.$$

Now for some  $k \leq n$  let us define  $f$  by the assignment

$$f(x_i) = \begin{cases} x_{i+1} & 1 \leq i \leq k-1 \\ x_1 & i = k \end{cases}$$

Then  $\{x_1, x_2, \dots, x_k\}$  forms a cycle by the element  $f$  in  $S$ .

If  $k$  is strictly less than  $n$ , then consider an element from the set  $\{x_1, x_2, \dots, x_k, \dots, x_n\}$ , as  $x_{k+1}$  enumerated, and defined  $f$  by  $f(x_{k+1}) = x_{k+2}, f(x_{k+2}) = x_{k+3}$  and so on.

Then we form another cycle given by  $\{x_{k+1}, x_{k+2}, \dots, x_m\}$ , for some  $m \leq n$ . We will continue to proceed this assignment until all the  $n$  elements get exhausted, that is, until we can form  $f$  like function for  $x_n$ .

Now corresponding to the elements of  $S$ , let us define  $h_j$  by the assignment

$$h_j(x) = \begin{cases} x_{j+1} & x = x_j \\ x_j & x = x_j + 1 \\ x & \text{otherwise} \end{cases}$$

Now from the above construction we have

$$h_j^2 = i.$$

## Step 2

2 of 3

Also we have

$$h_1 h_2 \dots h_{k-1}(x_j) = f(x_j), \text{ for } 1 \leq j \leq k.$$

Similarly, for each such cycle let us define  $h_j$  like above one.

**Since each cycle affects only the elements of the same cycle,** it follows that  $h_1 h_2 \dots h_{k-1} h_k \dots h_m$  affects each elements say  $x_j$  as

$$h_1 h_2 \dots h_{k-1} h_k \dots h_m(x_j) = x_{j+1} = f(x_j).$$

This conclude that

$$f = h_1 h_2 \dots h_m.$$

This completes our proof.

## Result

3 of 3

Considering any cycle of  $k$  elements  $\{x_1, x_2, \dots, x_k\}$ , and extending this cycle until all the  $n$  elements get exhausted we define  $h_j$  such a way that  $h_j^2 = i$  and using the condition  $h_1 h_2 \dots h_{k-1}(x_j) = f(x_j)$  we have proved that  $f = h_1 h_2 \dots h_m$ . Click for the complete proof.

23. a

**To Prove:** Any element in  $S_n$  can be written as a product of transpositions.

**Proof:** First we will propose to prove the following Lemma.

**Lemma:** Every permutation of a finite set can be written as a product of disjoint cycles.

**Proof of the Lemma:** Let  $\alpha$  be a permutation on  $A = \{1, 2, \dots, n\}$ . Pick any element of the set  $A$ , say  $a_1$ . Let us consider

$$\alpha(a_1) = a_2, \alpha(a_2) = \alpha^2(a_1) = a_3, \text{ and so on.}$$

Since the set  $A$  is a finite set, the constructing sequence  $a_1, \alpha(a_1), \alpha^2(a_1), \dots$  must be finite and therefore there is a repetition, that is there exist  $i > j$  for which

$$\begin{aligned} \alpha^i(a_1) &= \alpha^j(a_1) \\ \implies \alpha^{i-j} &= a_1. \end{aligned}$$

Let us say,  $i - j = m$ . Then we can write

$$\alpha = (a_1, a_2, \dots, a_m) \dots$$

**where the dots indicate we may not have exhausted all the elements of  $A$ .**

If we did not, we pick  $b_1$  among the elements of  $A$  which do not appear in  $(a_1, a_2, \dots, a_m)$  and repeat the same process to get a cycle  $(b_1, b_2, \dots, b_k)$ .

Notice that  $(a_1, a_2, \dots, a_m)$  and  $(b_1, b_2, \dots, b_k)$  are two disjoint cycles. Otherwise for some  $i$  and  $j$  we have

$$\alpha^i(a_1) = \alpha^j(b_1) \implies b_1 = \alpha^{i-j}(a_1),$$

but

this would imply  $b_1$  is an element of the cycle  $(a_1, a_2, \dots, a_m)$ , which is an impossibility.

Now we have

$$\alpha = (a_1, a_2, \dots, a_m)(b_1, b_2, \dots, b_k) \dots$$

where the cycles appearing so far are disjoint and the dots indicate we may not have exhausted all the elements of  $A$ . If there are elements of  $A$  left, we repeat the procedure again. We know this must end since  $A$  has a finite number of elements.

This proves our Lemma.

Now we Claim that

**any cycle in  $S_n$  with  $n > 1$  can be written as the product of transposition.**

**Proof of the Claim:** If we consider any 1-cycle, call the identity, then we can write

$$(a_i) = (a_i, a_{i+1})(a_{i+1}, a_i).$$

Then let us assume an  $r$ -cycle with  $r \geq 2$ , then

$$(a_1, a_2, \dots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2).$$

This completes our Claim.

Now consequently from the above Lemma and the Claim we can propose that

**any element in  $S_n$  can be written as product of transposition.**

This completes the proof.

## Result

3 of 3

First we prove that "every permutation of a finite set can be written as a product of disjoint cycles" and "any cycle in  $S_n$  with  $n > 1$  can be written as the product of transposition" and combining these two conditions we have proved our required result. Click for the detailed proof.

24. a

**Given:**  $S_n$  is the **symmetric group** of order  $n$ , where  $n \geq 3$ .

**To Prove:** There exists some element  $f$  in  $S_n$ , such that  $f$  cannot be expressed as

$$f = g^3, \text{ for any } g \in S_n.$$

**Proof:** Let us consider a map  $\gamma : S_n \rightarrow S_n$  by the assignment

$$\gamma(\sigma) = \sigma^3, \text{ for } \sigma \in S_n.$$

In order to show the existence of such  $f$  in  $S_n$ , it suffices to show that the mapping  $\gamma$  is not surjective.

We will propose to prove that  $\gamma$  is not injective even.

Let us consider two distinct  $3 - \text{cycle}$  in  $S_n$ , existence of a  $3 - \text{cycle}$  in  $S_n$  is obvious, implies the existence of another three cycle (just interchange consecutive two elements in the cycle). Let us assume two distinct  $3 - \text{cycles}$  say,  $\sigma$  and  $\alpha$  in  $S_n$ . Then

$$\sigma^3 = \text{id}, \text{ and } \alpha^3 = \text{id}.$$

Then

$$\gamma(\alpha) = \alpha^3 = \sigma^3 = \gamma(\sigma).$$

This follows that  $\gamma$  is not injective. Since  $S_n$  is finite, then  $\gamma$  is not surjective, otherwise  $\gamma$  will be injective. Since  $\gamma$  is not surjective there exists an element  $f$  in  $S_n$  such that

$$f \notin \text{Image}(\gamma).$$

Then we have

$$f \neq g^3, \text{ for any } g \in S_n.$$

This completes our proof.

## Result

2 of 2

Considering a mapping  $\gamma : S_n \rightarrow S_n$  by  $\gamma(\sigma) = \sigma^3$  for  $\sigma \in S_n$ , we have proved that  $\gamma$  is not surjective, implies the existence of such  $f$ . Click for the complete proof.

25. a

Assume that  $f \in S_n$  such that  $f \neq i$  but  $f = i^3$ , then we have that there is a  $x$  such that  $f(x) \neq x$ . Let  $M$  be subset of  $S$  such that  $f(y) \neq y$  for each  $y \in M$ . Let  $x_1$  be an arbitrary element from  $M$ , then we obtain  $f^2(x_1) \neq x_1$  (

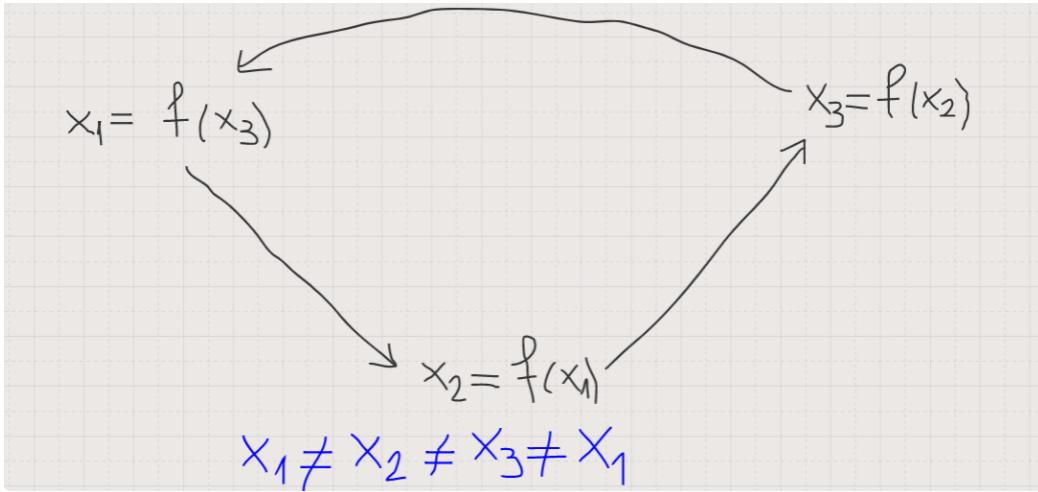
$$\text{if } f^2(x_1) = x_1, \text{ then } x_1 = f^3(x_1) = f(x_1)$$

) and

$$f(x_1) = x_2 \neq x_1$$

$$f(x_2) = f^2(x_1) = x_3 \neq x_2$$

$$f(x_3) = f^3(x_1) = x_1 \neq x_3$$



Therefore, using results above we can conclude that set  $M$  can be splitted onto part of three elements, i.e. number of elements is divisible by 3.

Further, we can choose an arbitrary element from  $M - \{x_1, x_2, x_3\}$  for  $x_4$ , then  $x_5$  and  $x_6$  can be used as  $x_5 = f(x_4)$  and  $x_6 = f(x_5)$ .

Continuing the process we are obtaining the groups we need.

When the process is done, the rest elements we can numbering easily.

## Result

4 of 4

Note that  $f(x) \neq x$  and  $f^3(x) = x$  implies  $f^2(x) \neq x$ .

## 26. a

Let  $x_1, x_2, \dots, x_{52}$  be the initial orders of cards in the deck. And let  $f \in S_{52}$  be the fixed shuffle of the deck, that is  $f(x_1), f(x_2), \dots, f(x_{52})$  form the new order of the deck. Now we prove a Claim.

**Claim:** If  $f \in S_n$ , then there is some positive integer  $k$ , depending on  $f$ , such that

$$f^k = i.$$

**Proof of the Claim:** Let  $f \in S_n$ . Let us consider the positive powers of  $f$ , that is,

$$f, f^2, f^3, \dots, f^n.$$

Since there are finite number of elements in  $S_n$ , then the above sequence must repeat itself after certain terms, say after  $k + 1$  elements.

That is,

$$f^{k+1} = f.$$

This implies

$$f^k = i.$$

This proves our Claim.

Now back to our main problem.

By the above claim there exists a positive integer  $k$  such that

$$f^k = i.$$

This implies

$$f^k(x_m) = x_m, \text{ for } 1 \leq m \leq 52.$$

Therefore, if we repeat the fixed shuffle  $f$   $k$ -times we will get the original order of the deck. And this complete our requirement.

## Result

3 of 3

Considering  $x_1, x_2, \dots, x_{52}$  be the initial orders of cards in the deck and using the statement that, if  $f \in S_n$ , then there is some positive integer  $k$ , depending on  $f$ , such that  $f^k = i$ , we have proved that by repeating a fixed shuffle a finite number of times will bring the deck back to its original order.

27. a

**To Prove:** If  $s, t \in S$  then either  $O(s) \cap O(t) = \phi$  or  $O(s) = O(t)$ .

**Definition:** If  $f \in A(S)$ , call, for  $s \in S$ , the **orbit** of  $s$  (relative to  $f$ ) the set

$$O(s) = \{f^j(s) \mid \text{all integers } j\}.$$

**Proof:** For  $s, t \in S$ , either  $O(s) \cap O(t) = \phi$  or  $O(s) \cap O(t) \neq \phi$ . If  $O(s) \cap O(t) = \phi$ , then partially we are done.

So,

**let us assume**  $O(s) \cap O(t) \neq \phi$ .

Then for some  $x$  in  $S$  we have

$$x = f^m(s) \text{ and } x = f^n(t), \text{ where } m, n \text{ are integers.}$$

Now,

$$\begin{aligned} x = f^m(s) &\implies s = f^{-m}(x) \\ &\implies s = f^{-m}[f^n(t)] \\ &\implies s = f^{n-m}(t) \\ &\implies f^{m-n}(s) = t. \end{aligned}$$

Now if we take an element  $y$  in  $O(s)$ , then

$$y = f^j(s).$$

Therefore,

$$y = f^j(s) \implies y = f^j[f^{n-m}(t)] \implies y = f^{j+n-m}(t) \implies y \in O(t).$$

Now if we take an element  $y$  in  $O(t)$ , then

$$y = f^j(t).$$

Now,

$$y = f^j(t) \implies y = f^j[f^{m-n}(s)] \implies y = f^{j+m-n}(s) \implies y \in O(s).$$

Consequently, we have

$$O(s) = O(t).$$

Hence,

$$O(s) \cap O(t) \neq \emptyset \implies O(s) = O(t).$$

This completes the proof.

## Result

2 of 2

Considering  $O(s) \cap O(t) \neq \emptyset$  we have shown that for any element  $y \in O(s)$ ,  $y$  also belongs to the set  $O(t)$  and vice-versa, and follows the result. Click for the complete proof.

## 28. a

**Given:**  $S := \{x_1, x_2, \dots, x_{12}\}$  is a set of 12 elements and  $f \in S_{12}$  is defined by

$$f(x_t) = x_{t+1}, \text{ if } i = 1, 2, \dots, 11 \text{ and } f(x_{12}) = x_1.$$

**We need to find the orbits of all the elements of  $S$ .**

**Solution:** First of all notice that

$$f^0(x_k) = i(x_k) = x_k, \text{ for all } 1 \leq k \leq 12.$$

This implies

$$x_k \in O(x_k), \text{ for all } 1 \leq k \leq 12.$$

Now by the given condition,

$$x_2 = f(x_1) \implies x_2 \in O(x_1).$$

Now,

$$\begin{aligned} x_2 \in O(x_2) \text{ also } x_2 \in O(x_1) &\implies x_2 \in O(x_1) \cap O(x_2) \\ &\implies O(x_1) \cap O(x_2) \neq \emptyset. \end{aligned}$$

**Now we know that for any elements  $s, t \in S$**

either  $O(s) \cap O(t) = \emptyset$  or  $O(s) = O(t)$ .

But we have

$$O(x_1) \cap O(x_2) \neq \emptyset, \text{ for } x_1, x_2 \in S.$$

Therefore,

$$O(x_1) = O(x_2).$$

Again we have

$$x_3 = f(x_2).$$

**Proceeding like above we can conclude that**

$$O(x_3) = O(x_2) = O(x_1).$$

Hence, by **succeeding step of enumeration** we have

$$O(x_k) = O(x_1), \text{ for } 2 \leq k \leq 12.$$

Also,

$$\begin{aligned} x_k \in O(x_k) &\implies x_k \in O(x_1), \text{ for } 1 \leq k \leq 12 \\ \implies S \subset O(x_1) &\implies O(x_1) = S = \{x_1, x_2, \dots, x_{12}\}. \end{aligned}$$

Therefore,

$$O(x_1) = O(x_2) = \dots = O(x_{12}) = S.$$

This completes the proof.

## Result

3 of 3

Being  $x_k \in O(x_k)$  and  $f(x_k) = x_{k+1}$  for all  $1 \leq k \leq 11$  and  $f(x_{12}) = x_1$ , we have shown that  $O(x_k) = O(x_1)$  for all  $1 \leq k \leq 12$  follows the result as  $O(x_1) = O(x_2) = \dots = O(x_{12}) = S$ . Click for the detailed solution.

29. a

**Given:**  $f \in A(S)$  such that  $f^3 = i$ .

**To Prove:** The orbit of any element of  $S$  has 1 or 3 elements.

**Proof:** Let us consider  $s \in S$ .

Now, two cases arise.

**Case-1:**  $f(s) = s$  in  $S$ .

Then,

$$f^n(s) = f^{n-1}(s) = \dots = f(s) = s, \text{ for all integers } n.$$

Then orbit of  $s$  consists of only one element  $s$  itself, i.e.,  $O(s) = \{s\}$ .

**Case-2:**  $f(s) \neq s$  in  $S$ .

Let us assume  $f(s) = s'$ , for some  $s' \in S$ .

Now,

$$f^2(s) = f(s') = s'', \text{ for some } s'' \in S.$$

According to the question,

$$f^3 = i \implies f^3(s) = f(s'') = i(s) = s.$$

If,  $s = s''$ .

Then by above argument we lead a contradiction as  $f(s) = s$ .

So,

$$s \neq s''.$$

If,  $s'' = s'$ .

Then,

$$f(s') = s' \text{ and also } f(s) = s',$$

contradict the fact that  $f$  is one-one.

So,

$$s' \neq s''.$$

And, by our assumption  $s \neq s'$  as  $f(s) = s'$ .

Therefore, orbit of  $s$  contains three elements as  $s, s', s''$ .

That is  $O(s) = \{s, s', s''\}$ .

This completes our proof.

## Result

3 of 3

Considering an element  $s \in S$  and dividing in two cases on as  $f(s) = s$  and  $f(s) \neq s$ , we have shown that either

$$O(s) = \{s\} \text{ or } O(s) = \{s, f(s), f^2(s)\}.$$

Click for the complete proof.

30. a

**Given:**  $f$  is an element in  $A(S)$  satisfying  $f^p = i$ , for some prime  $p$ .

**We need to find the size of the elements of  $S$  relative to  $f$ .**

Let us consider an element  $x \in S$ .

If  $f(x) = x$  then orbit of  $x$  is a singleton set, that is

$$O(x) = \{x\}.$$

Let us now consider  $f(x) \neq x$ .

Let us assume  $m$  is the smallest positive integer greater than 1 such that

$$f^m(x) = x.$$

Therefore,

$$f^m = i \implies p \leq m.$$

Then by **the method of Division algorithm there exist integers**  $q$  and  $r$  such that

$$p = qm + r, \text{ where } 0 \leq r < m.$$

Now,

$$\begin{aligned} f^p(x) = x &\implies f^{qm+r}(x) = x \\ &\implies f^{qm}(x) \cdot f^r(x) = x \\ &\implies \{f^m(x)\}^q \cdot f^r(x) = x \\ &\implies f^r(x) = x. \end{aligned}$$

**This is a contradiction to the minimality of the integer  $m$  such that**

$$f^m(x) = x.$$

So,  $r$  must be 0.

Hence,

$$p = qm.$$

Since  $p$  is a prime, either  $q = 1$  or  $m = 1$ . But  $m$  can not be equals 1, since  $f(x) \neq x$ . Therefore,  $m = p$  and  $q = 1$ .

So, if  $f(x) \neq x$ ,  $O(x)$  has size  $p$ .

Consequently,  $O(x)$  has size 1 or size  $p$ .

This completes the proof.

## Result

2 of 2

Considering any arbitrary element  $x$  and separated by cases as if  $f(x) = x$  and  $f(x) \neq x$ , we have shown that orbit of  $x$  has size 1 or  $p$  respectively. Click for the complete proof.

31. a

**To Prove:** If  $S$  has more than two elements, then the only elements  $f_0$  in  $A(S)$  such that

$$ff_0 = f_0f, \text{ for all } f \in A(S)$$

must satisfy

$$f = i.$$

**Proof:** Let us assume  $x_1, x_2, x_3 \in S$ . Let us define an element  $f_1 \in A(S)$  by the assignment

$$f_1(x_1) = x_2, f_1(x_2) = x_1 \text{ and } f_1(s) = s \text{ if } s \neq x_1, x_2.$$

Now define another element  $f_2$  in  $A(S)$  by the assignment

$$f_2(x_1) = x_3, f_2(x_3) = x_1 \text{ and } f_2(s) = s \text{ if } s \neq x_1, x_3.$$

Now we will prove the following Claim.

**Claim:** Given an element  $f : S \rightarrow S$  in  $A(S)$  is defined by

$$f(x) = y, f(y) = x \text{ and } f(s) = s, \text{ if } s \neq x, y.$$

Then the only elements in  $A(S)$  commutes with  $f$  are identity and  $f$  itself.

**Proof of the Claim:** Let us consider an element  $g \in A(S)$  such that  $g$  commutes with  $f$ .

Let us assume  $s \neq x, y$ . Then we have,

$$fg(s) = gf(s) = g(f(s)) = g(s).$$

Again,

$$\begin{aligned} f[g(s)] &= g(s) \implies g(s) \neq x, y. \\ &\implies g \text{ takes } S \setminus \{x, y\} \text{ to } S \setminus \{x, y\}. \end{aligned}$$

**Since  $g$  is 1-1, we can conclude that**

$$g(x) \in \{x, y\} \text{ and } g(y) \in \{x, y\}.$$

Now,

$$fg(x) = gf(x) = g(f(x)) = g(y).$$

If  $g(x) = x$  then  $g(y) = y$ , since  $g \in A(S)$ .

Now

$$fg(x) = f(g(x)) = f(x) = y = g(y) = g(f(x)) = gf(x)$$

$$fg(y) = f(g(y)) = f(y) = x = g(x) = g(f(y)) = gf(y).$$

Therefore it follows that

$$fg = gf.$$

Now if we consider  $g(x) = y$  then  $g(y) = x$ , since  $g \in A(S)$ .

Now,

$$fg(x) = f(g(x)) = f(y) = x = g(y) = g(f(x)) = gf(x)$$

$$fg(y) = f(g(y)) = f(x) = y = g(x) = g(f(y)) = gf(y).$$

Therefore,

$$fg = gf.$$

Hence, If  $g$  in  $A(S)$  commutes with given  $f$  then

either  $g = \text{id}$  or  $g = f$ .

### Step 3

3 of 4

Hence by the above Claim it follows that

$$f_0 f_1 = f_1 f_0 \implies f_0 = i \text{ or } f_0 = f_1.$$

Also,

$$f_0 f_2 = f_2 f_0 \implies f_0 = i \text{ or } f_0 = f_2.$$

By our construction

$$f_1 \neq f_2.$$

Hence

$$f_0 = i.$$

This completes our proof.

### Result

4 of 4

Considering three elements  $x_1, x_2, x_3$  in  $A(S)$  and defining two different elements in  $A(S)$  we have shown that  $f_0$  must be identity. Click for the complete proof.

32. a

**Given:** An element  $f : S \rightarrow S$  in  $A(S)$  is defined by

$$f(x_1) = x_2, f(x_2) = x_1 \text{ and } f(s) = s, \text{ if } s \neq x_1, x_2.$$

**We need to find all the elements of  $A(S)$  that commute with the given  $f$ .**

**Solution:** Let us consider an element  $g \in A(S)$  such that  $g$  commutes with  $f$ .

Let us assume  $s \neq x_1, x_2$ . Then we have,

$$fg(s) = gf(s) = g(f(s)) = g(s).$$

Again,

$$\begin{aligned} f[g(s)] &= g(s) \implies g(s) \neq x_1, x_2. \\ &\implies g \text{ takes } S \setminus \{x_1, x_2\} \text{ to } S \setminus \{x_1, x_2\}. \end{aligned}$$

**Since  $g$  is 1-1, we can conclude that**

$$g(x_1) \in \{x_1, x_2\} \text{ and } g(x_2) \in \{x_1, x_2\}.$$

Now,

$$fg(x_1) = gf(x_1) = g(f(x_1)) = g(x_2).$$

If  $g(x_1) = x_1$  then  $g(x_2) = x_2$ , since  $g \in A(S)$ .

Now

$$fg(x_1) = f(g(x_1)) = f(x_1) = x_2 = g(x_2) = g(f(x_1)) = gf(x_1)$$

$$fg(x_2) = f(g(x_2)) = f(x_2) = x_1 = g(x_1) = g(f(x_2)) = gf(x_2).$$

Therefore it follows that

$$fg = gf.$$

Now if we consider  $g(x_1) = x_2$  then  $g(x_2) = x_1$ , since  $g \in A(S)$ .

Now,

$$fg(x_1) = f(g(x_1)) = f(x_2) = x_1 = g(x_2) = g(f(x_1)) = gf(x_1)$$

$$fg(x_2) = f(g(x_2)) = f(x_1) = x_2 = g(x_1) = g(f(x_2)) = gf(x_2).$$

Therefore,

$$fg = gf.$$

**Hence, If  $g$  in  $A(S)$  commutes with given  $f$  then**

$$\text{either } g = \text{id} \text{ or } g = f.$$

Here we are done.

## Result

3 of 3

For the given element  $f$  in  $A(S)$ , only identity and  $f$  itself commutes with  $f$ . Click for the detailed solution.

### 33. a

We have that  $f \in S_n$  is defined as  $f(x_i) = x_{i+1}$ , for  $i = 1, \dots, n-1$  and  $f(x_n) = x_1$ , then it is not hard to conclude that for each  $k = 0, 1, \dots, n-1$  function  $f^k$  is given by

$$f(x_i) = x_{k+i}, \quad i = 1, \dots, n-k$$

and

$$f(x_{k+i}) = x_i, \quad i = 1, \dots, k$$

In this task we need to show that if function  $g \in S_n$  commutes with  $f$ , then it must equal to  $f^k$  for some  $k$ .

Therefore, assume that  $g \in S_n$  such that  $gf = fg$ . There is an  $j \in \{1, 2, \dots, n\}$  such that  $x_j = g(x_1)$ , from our assumption we have that

$$f(x_j) = g(x_1) = g(f(x_n)) = f(g(x_n))$$

and from that  $f$  is bijection we obtain  $g(x_n) = x_j = f^{j-1}(x_1)$ .

Let show that  $g = f^j$  by proving that  $g(x_i) = f^j(x_i)$  for each  $j = 1, \dots, n$ :

$$\begin{aligned}g(x_1) &= g(f(x_n)) = f(g(x_n)) = f(f^{j-1}(x_1)) = f^j(x_1) \\g(x_2) &= g(f(x_1)) = f(g(x_1)) = f(f^j(x_1)) = f^j(f(x_1)) = f^j(x_2) \\g(x_3) &= g(f(x_2)) = f(g(x_2)) = f(f^j(x_2)) = f^j(f(x_2)) = f^j(x_3)\end{aligned}$$

...

$$g(x_n) = g(f(x_{n-1})) = f(g(x_{n-1})) = f(f^j(x_{n-1})) = f^j(f(x_{n-1})) = f^j(x_n)$$

Therefore, for an arbitrary  $g \in S_n$  which commuting with it is proven that  $g$  must be equal to some power of  $f$ !

### Result

(HINT:) For each  $k = 0, 1, \dots, n - 1$  function  $f^k$  is given by

$$f(x_i) = x_{k+i}, \quad i = 1, \dots, n - k$$

and

$$f(x_{k+i}) = x_i, \quad i = 1, \dots, k$$

34. a

(a) Given  $g, h \in C(f)$ , we want to prove that  $gh \in C(f)$ . Consider,

$$\begin{aligned}f(gh) &= (fg)h = (gf)h \\&= g(fh) = g(hf) \\&= (gh)f\end{aligned}$$

Therefore,  $gh \in C(f)$ .

(b) Given  $g \in C(f)$  we want to prove that  $g^{-1} \in C(f)$ . Since,

$$\begin{aligned}fg = gf &\implies g^{-1}(fg) = g^{-1}(gf) \\&\implies (g^{-1}f)g = (g^{-1}g)f \\&\implies (g^{-1}f)g = f \\&\implies g^{-1}f = fg^{-1}\end{aligned}$$

Therefore,  $g^{-1} \in C(f)$ .

(c) We want to prove that  $C(f) \neq \emptyset$ . Observe that  $i \in A(S)$ , where  $i$  is the identity map, i.e.,  $i(s) = s$ ,  $\forall s \in S$ . Clearly,

$$fi = f = if.$$

### Result

$$gh \in C(f), g^{-1} \in C(f) \text{ and } C(f) \neq \emptyset.$$

## Section 1–5

1. a

solution 1)

$$(a) (116, -84) = 4$$

$$116 = 84 \times 1 + 32$$

$$84 = 32 \times 2 + 20$$

$$32 = 20 \times 1 + 12$$

$$20 = 12 \times 1 + 8$$

$$12 = 8 \times 1 + 4$$

## System of Equations

$$\Rightarrow 4 = 12 - 8 \times 1$$

$$= 12 - (20 - 12)$$

$$= (32 - 20) \times 2 - 20 \times 1$$

$$= 32 \times 2 - 20 \times 3$$

$$= 32 \times 2 - (84 - 32 \times 2) \times 3$$

$$= 32 \times 2 - 84 \times 3 + 32 \times 6$$

$$= 32 \times 8 - 84 \times 3$$

$$= (116 - 84) \times 8 - 84 \times 3$$

$$= 116 \times 8 - 84 \times 1$$

$$= 116 \times 8 + (-84) \times 11.$$

Using the  
above  
equations.

(b)

$$(85, 65) = 5$$

$$85 = 65 \times 1 + 20$$

$$65 = 20 \times 3 + 5$$

$$S = 65 - 20 \times 3$$

$$\Rightarrow S = \{S - CS - CS\}$$

$$= 65 - 85 \times 3 + 55 \times 3$$

$$= 65 \times 4 + (-3) \times 85$$

## Equations

## Result

- a)  $m=8, n=11$   
 b)  $m=-3, n=4$

2. a

Lemma 1.5.2

(a)  $1 \mid n$  for all  $n$ .

Proof:

$$n = n \times 1 = c \times 1, \text{ where } c = n$$

$$\Rightarrow 1 \mid n, \text{ by definition.}$$

(b)  $0 = 0 \times m$ .

Since  $0$  is an integer,  
we have

$$m \mid 0$$

(c)  $m \mid n \Rightarrow n = c_1 m$  for some integer  $c_1$

$$n \mid q \Rightarrow q = c_2 n \text{ for some integer } c_2$$

$$\Rightarrow q = c_2 n = c_2(c_1 m)$$

$$= (c_2 c_1)m$$

Since  $c_2 c_1$  is an integer  
we have that  $m \mid q$ .

(d)  $m \mid 1$

$$\Rightarrow 1 = c m \text{ for some integer } c.$$

$$\Rightarrow c = \frac{1}{m}, \text{ where } m \neq 0.$$

Assume that  $m > 1$ .

Then  $0 < \frac{1}{m} < 1 \Rightarrow c$  is not an integer.

Since this is a contradiction,

$$\Rightarrow m \leq 1.$$

Assume that  $m < -1$ .

Then  $-1 < \frac{1}{m} < 0 \Rightarrow c$  is not an integer.

Again a contradiction.

$$\Rightarrow m \geq -1.$$

Since  $m$  is a non zero integer,  
we have

$$\underline{\underline{m = -1 \text{ or } m = 1}}$$

f) Let  $m = nc_1$  and  $n = mc_2$ ,  
where  $c_1$  and  $c_2$  are integers.

$$\Rightarrow m = nc_1 = (mc_2)c_1$$

$$\Rightarrow m(c_2c_1 - 1) = 0.$$

$$\Rightarrow m = 0 \quad \text{or} \quad c_2c_1 = 1.$$

if  $m = 0$ ,  
then  $n = 0$   
 $\Rightarrow m = \pm n$

$\left| \begin{array}{l} \text{if } c_2c_1 = 1, \\ \text{by (e), } c_2 = \pm 1, c_1 = \pm 1 \\ \Rightarrow n = mc_2 = \pm m \\ m = nc_1 = \pm n \end{array} \right.$

3. a

**To Prove:**  $(ma, mb) = m(a, b)$ , if  $m > 0$ .

**Proof:** Let us first assume that  $(a, b) = d$ . Then

**It suffices to proof that**  $(ma, mb) = md$ .

Since,

$$(a, b) = d \implies d \text{ divides both } a \text{ and } b.$$

It is given that  $m > 0$ . Hence,  $md$  divides both  $ma$  and  $mb$ .

Let us take  $c > 0$  such that  $c$  divides both  $ma$  and  $mb$ .

**We will propose to prove that  $c$  divides  $md$ .**

Now,  $(a, b) = d$  implies there exist integers  $p$  and  $q$  such that

$$d = ap + bq.$$

Hence,

$$md = map + mbq.$$

Now,  $c$  divides both  $ma$  and  $mb$  implies  $c$  divides both of  $map$  and  $mbq$ .

$$\implies c \text{ divides } md.$$

Hence, **by the definition of GCD** we have

$$md = (ma, mb).$$

This implies,

$$m(a, b) = (ma, mb), \text{ since } (a, b) = d.$$

This completes the proof.

### Result

2 of 2

Considering  $(a, b) = d$  we have proved that for any  $c > 0$  divides both  $ma$  and  $mb$  implies  $c$  divides  $md$ , follows the result.

Click for the detailed proof.

4. a

**Given:**  $a$  divides  $m$  and  $b$  divides  $m$  and  $(a, b) = 1$ .

**To Prove:**  $ab$  divides  $m$ .

**Proof:** Since,  $a$  divides  $m$  and  $b$  divides  $m$  then there exist integers  $x$  and  $y$  such that

$$m = ax \text{ and } m = by.$$

This implies

$$ax = by.$$

Now,  $(a, b) = 1$ . Then there exist integers  $p$  and  $q$  such that

$$ap + bq = 1.$$

Now,

$$\begin{aligned} ap + bq = 1 &\implies axp + bxq = x \\ &\implies byp + bxq = x, \text{ since } ax = by \\ &\implies b(yp + xq) = x. \end{aligned}$$

Again we have  $m = ax$ .

Then,

$$m = ax \implies m = ab(yp + xq)$$

Since,  $yp + xq$  is an integer it follows that  $ab$  divides  $m$ .

This completes the proof.

## Result

2 of 2

Considering  $m = ax = by$  for some integers  $x$  and  $y$  and using the fact  $(a, b) = 1$  we have proved that  $m = (ab)k$ , for some integer  $k$ , implies the result.

[Click for the detailed proof.](#)

## 5. a

### Prime factorization of 36, 120, 720 and 5040

(a)  $36 = 4 \times 9 = 2^2 \times 3^2$ .

(b)  $120 = 24 \times 5 = 8 \times 3 \times 5 = 2^3 \times 3 \times 5$ .

(c)  $720 = 120 \times 6 = (2^3 \times 3 \times 5) \times (2 \times 3) = 2^4 \times 3^2 \times 5$ .

(d)  $5040 = 720 \times 7 = 2^4 \times 3^2 \times 5 \times 7$ .

## Result

2 of 2

Prime factorization of 36 is  $2^2 \times 3^2$ , 120 is  $2^3 \times 3 \times 5$ , 720 is  $2^4 \times 3^2 \times 5$  and of 5040 is  $2^4 \times 3^2 \times 5 \times 7$ .

## 6. a

**Given:**  $m$  and  $n$  are two integers given by

$$m = p_1^{a_1} \dots p_k^{a_k} \text{ and } n = p_1^{b_1} \dots p_k^{b_k},$$

where  $p_1, p_2, \dots, p_k$  are distinct primes and  $a_1, a_2, \dots, a_k$  are non-negative and  $b_1, b_2, \dots, b_k$  are non-negative.

We need to express  $(m, n)$  as  $p_1^{c_1} \dots p_k^{c_k}$ , where  $c_i$ 's are described in terms of  $a_i$ 's and  $b_i$ 's.

Let us consider  $d := (m, n)$ . Then it follows that,

**$d$  divides both  $m$  and  $n$  simultaneously.**

That is,

$$d|m \text{ and } d|n$$

$$\implies d = p_1^{c_1} \dots p_k^{c_k}, \text{ where } c_i \leq a_i, b_i$$

$$\implies c_i \leq \min(a_i, b_i).$$

We will propose to prove that  $c_i = \min(a_i, b_i)$ .

If possible, let us assume that  $c_i \neq \min(a_i, b_i)$ . Then by the above argument it yield's that

$$c_i < \min(a_i, b_i).$$

Let us now consider,

$$x = p_1^{e_1} \dots p_k^{e_k}, \text{ where } e_i = \min(a_i, b_i).$$

Then it follows that

$$x|a \text{ and } x|b.$$

Also,

$$c_i < e_i \implies d|x,$$

**which is an impossibility**, since  $d = (m, n)$ .

Therefore

$$d = x.$$

Hence,

$$(m, n) = p_1^{e_1} \dots p_k^{e_k}, \text{ where } e_i = \min(a_i, b_i), \forall i = 1, 2, \dots, k.$$

This completes our solution..

## Result

3 of 3

The result we have that  $(m, n) = p_1^{e_1} \dots p_k^{e_k}$ , where  $e_i = \min(a_i, b_i), \forall i = 1, 2, \dots, k$ . Click for the complete solution.

7. a

First we propose to show that

$$v = \frac{mn}{(m, n)}.$$

For our simplicity let us assume that

$$(m, n) = d.$$

Now, it suffices to show that

$$vd = mn$$

that is,  $vd$  divides  $mn$  as well as  $mn$  divides  $vd$ .

By the given condition we have

$$\begin{aligned} m, n \text{ divides } v &\implies mn \text{ divides both } mv \text{ and } nv \\ &\implies mn \text{ divides } (mv, nv) \\ &\implies mn \text{ divides } (m, n)v \\ &\implies mn \text{ divides } vd. \end{aligned}$$

Now we show the other side.

Now  $d = (m, n)$ , implies  $d$  divides both of  $m$  and  $n$ . Then we have

$$m \text{ divides } m \cdot \frac{n}{d} \text{ and } n \text{ divides } n \cdot \frac{m}{d}.$$

This follows that  $\frac{mn}{d}$  is a common multiple of  $m$  and  $n$ . Since  $v$  is the least common multiple of  $m, n$ , we have

$$v \text{ divides } \frac{mn}{d}.$$

Consequently we have

$$vd \text{ divide } mn.$$

Therefore,

$$mn = vd.$$

This completes our proof.

For the second question let us assume

**the prime factorization of  $m$  and  $n$  are respectively**

as

$$m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \text{ and } n = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k},$$

where  $a_i$ 's and  $b_j$ 's are non-negative integers. Since  $v$  is the LCM of  $m$  and  $n$  then we can write

$$v = p_1^{c_1} p_2^{c_2} \dots p_k^{c_k},$$

where  $c_i$ 's are **non-negative integers** such that

$$c_i = \max\{a_i, b_i\}.$$

This completed our proof.

## Result

3 of 3

Considering  $(m, n) = d$ , we first proved that  $mn$  divides  $vd$  and vice-versa, and follows the result. And for the second one maximum of the prime power of  $m$  and  $n$  is the required prime power of their LCM. Click for the complete proof.

## 8. a

The least

**common multiple of positive integers  $m$  and  $n$**

is the

smallest positive integer  $v$  such that both  $m|v$  and  $n|v$ . Therefore, if the integers  $m$  and  $n$  are given by

$$m = p_1^{\ell_1} \cdot \dots \cdot p_k^{\ell_k}$$

$$n = p_1^{\mu_1} \cdot \dots \cdot p_k^{\mu_k}$$

the least common multiple  $lcm$  is given by

$$lcm(m, n) = p_1^{\epsilon_1} \cdot \dots \cdot p_k^{\epsilon_k}$$

$$\epsilon_i = \min(\mu_i, \ell_i)$$

Therefore, we first need to represent numbers using the prime factorization, then **least common multiple** easily found. If one of  $m$  and  $n$  are negative (assume that is  $n$ ), the least common multiple of  $n$  and  $m$  is the least common multiple of  $-n$  and  $m$ .

- [a)] The integers 116 and 84 can be represent as

$$116 = 2^2 \cdot 3^0 \cdot 7^0 \cdot 29^1$$

$$84 = 2^2 \cdot 3^1 \cdot 7^1 \cdot 29^0$$

then using results above we conclude that

$$\text{lcm}(116, -84) = 2^2 \cdot 3^1 \cdot 7^0 \cdot 29^0 = 4$$

- [b)] The integers 85 and 65 can be represent as

$$85 = 5^1 \cdot 13^0 \cdot 17^1$$

$$65 = 5^1 \cdot 13^1 \cdot 17^0$$

then using results above we conclude that

$$\text{lcm}(85, 65) = 5^1 \cdot 13^0 \cdot 17^0 = 5$$

- [c)] The integers 72 and 26 can be represent as

$$72 = 2^3 \cdot 3^2 \cdot 13^0$$

$$26 = 2^1 \cdot 3^0 \cdot 13^1$$

then using results above we conclude that

$$\text{lcm}(72, 26) = 2^1 \cdot 3^0 \cdot 13^0 = 2$$

- [d)] The integers 72 and 25 can be represent as

$$72 = 2^3 \cdot 3^2 \cdot 5^0$$

$$25 = 2^0 \cdot 3^0 \cdot 5^2$$

then using results above we conclude that

$$\text{lcm}(72, 25) = 2^0 \cdot 3^0 \cdot 5^0 = 1$$

## Result

If the integers  $m$  and  $n$  are given by

$$m = p_1^{\ell_1} \cdot \dots \cdot p_k^{\ell_k}$$

$$n = p_1^{\mu_1} \cdot \dots \cdot p_k^{\mu_k}$$

the least common multiple  $\text{lcm}$  is given by

$$\text{lcm}(m, n) = p_1^{\epsilon_1} \cdot \dots \cdot p_k^{\epsilon_k}$$

$$\epsilon_i = \min(\mu_i, \ell_i)$$

9. a

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

**Proof:** Since  $m, n > 0$ , by Euclidean algorithm there exist integers  $q$  and  $r$  such that

$$m = nq + r, \text{ where } 0 \leq r < n.$$

Now we arrived at two cases.

**Case-1:**  $r \leq \frac{n}{2}$ .

Then take  $v = r$  and  $u = q$ . So, we are done in this case.

**Case-2:**  $r > \frac{n}{2}$ .

Now we have,

$$m = nq + r \implies m = nq + n - n + r \implies (q+1)n + (r-n).$$

Now,

$$r > \frac{n}{2} \implies -\frac{n}{2} \leq (r-n) \leq \frac{n}{2}.$$

So, consider  $v = r - n$  and  $u = q + 1$ . So, we are done in this case.

Consequently, we have proved our required condition.

This completes our proof.

## Result

2 of 2

Using Euclidean algorithm and considering two cases  $r \leq \frac{n}{2}$  and  $r > \frac{n}{2}$  we have shown that there exist integers  $u$  and  $v$  with  $-\frac{n}{2} \leq v \leq \frac{n}{2}$  such that  $m = un + v$ .

Click for the complete proof.

## 10. a

**Given:**  $n$  is a given integer such that  $n$  is not divisible by any prime  $p$  with  $p \leq \sqrt{n}$ .

**To Prove:**  $n$  is a prime.

**Proof:** We will prove it by contradiction.

If possible, let  $n$  is a composite number, that is,  $n$  is not a prime.

Then there exist primes  $p_1, p_2, \dots, p_k$  such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Now  $p_1$  divides  $n$  and  $p_2$  divides  $n$ , where  $p_1, p_2$  are primes.

It follows that

$$p_1 > \sqrt{n} \text{ and } p_2 > \sqrt{n}.$$

This implies

$$p_1 p_2 > n.$$

This contradicts the fact of prime decomposition of  $n$ .

So our assumption that  $n$  is composite is wrong. Therefore  $n$  is a prime.

This completes the proof.

**Result**

2 of 2

Considering  $n$  is composite and its prime factorization, we have shown that multiplication of any two primes from its decomposition forms a larger number than  $n$ , which is absurd and hence contradict the composite term. Click for the complete proof.

**11. a**

(a)  $301 = 7 \cdot 43$ .

Hence 301 is not prime.

(b)  $1001 = 7 \cdot 143$ .

Hence 1001 is not prime.

(c)  $473 = 11 \cdot 43$ .

Hence 473 is not prime.

**Result**

None are prime.

**12. a**

$$1 + 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30031.$$

But  $30031 = 59 \cdot 509$ .

That is, 30031 is not a prime.

**Result**

No!

**13. a**

**To Prove:** If  $p$  is an odd prime then,  $p$  is of the form

(a)  $4n + 1$  or  $4n + 3$  for some  $n$ .

(b)  $6n + 1$  or  $6n + 5$  for some  $n$ .

**Proof:** (a) By the given condition  $p$  is an odd prime.

If,  $p = 3$  then  $p = 4 \times 0 + 3$ . So for  $p = 3$  we are done.

If  $p \geq 5$ .

Then by **division algorithm there exist integers**  $n$  and  $r$  such that

$$p = 4n + r, \text{ where } 0 \leq r < 4.$$

So, the **possible forms** of  $p$  are  $4n$ ,  $4n + 1$ ,  $4n + 2$  and  $4n + 3$ .

Now, if  $p = 4n$  then  $p$  is an **even number**, so cannot be an odd prime.

If,  $p = 4n + 2$  then also  $p$  is even, and cannot be an odd prime.

So, the only possibilities for  $p$  be an odd prime are if  $p$  has form  $4n + 1$  or  $4n + 3$  for some  $n$ .

(b) By the given condition  $p$  is an odd prime.

If,  $p = 3$  then  $p = 6 \times 0 + 3$ , and if  $p = 5$  then  $p = 6 \times 0 + 5$ .

So for  $p = 3, 5$  we are done.

If  $p \geq 7$ .

Then by **division algorithm there exist integers**  $n$  and  $r$  such that

$$p = 6n + r, \text{ where } 0 \leq r < 6.$$

So, **the possible forms of**  $p$  are  $6n$ ,  $6n + 1$ ,  $6n + 2$ ,  $6n + 3$ ,  $6n + 4$  and  $6n + 5$ .

Now, if  $p = 6n$  then  $p$  is an **even number**, so cannot be an odd prime.

If,  $p = 6n + 2$  then  $p$  is an **even number, so cannot be an odd prime**. Again, if  $p = 6n + 4$  then  $p$  is an even number, so cannot be an odd prime. If,  $p = 6n + 3$  then  $p$  is divisible by 3, so can be a prime number, as  $n \geq 1$ .

So, the only possibilities for  $p$  be an odd prime are if  $p$  has form  $6n + 1$  or  $6n + 5$  for some  $n$ .

This completes the proof.

## Result

3 of 3

In both the cases we have used division algorithm to initiate the form of  $p$  and then we eliminate all such forms of  $p$  which are even and not prime, and follows the result.

Click for the complete proof.

14. a

**To Prove:**

- (a) There are infinitely many primes of the form  $4n + 3$ .  
 (b) There are infinitely many primes of the form  $6n + 5$ .

**Proof:**

(a) We will use Euclid's argument for the existence of infinitely many primes.

If possible, let there are finitely many primes of the form  $4n + 3$  and they are exactly  $\{p_1, p_2, \dots, p_l\}$ .

Let us now consider

$$N = (p_1 p_2 \dots p_l)^2 + 2.$$

Then,

$$N \equiv 3 \pmod{4}.$$

That is,

***N leaves a remainder 3 when divided by 4.***

On the other hand  $N$  is odd, since

***each  $p_i$  is an odd prime and  $N$  is not divisible by any  $p_i$ .***

Therefore, all prime divisors of  $N$  must be of the form  $4n + 1$ , for some integers  $n$ .

It follows that,  $N$  leaves a remainder 1 when divided by 4, which is a contradiction. Hence, our assumption that there exist only a finitely many primes of the form  $4n + 3$ , is wrong.

***Therefore, there are infinitely many primes of the form  $4n + 3$ .***

This completes our proof.

(b)

***We know that any odd prime is of the form  $6n + 1$  or  $6n + 5$ , where  $n$  is an integer.***

We will show that there are infinitely many primes of the form  $6n + 5$ .

If possible, let there are finitely many primes of the form  $6n + 5$  and they are exactly  $\{p_1, p_2, \dots, p_l\}$ .

Let us now consider

$$N = (p_1 p_2 \dots p_l)^2 + 4.$$

Then,

$$N \equiv 5 \pmod{6}.$$

That is,

***N leaves a remainder 5 when divided by 6.***

On the other hand  $N$  is odd, since

***each  $p_i$  is an odd prime and  $N$  is not divisible by any  $p_i$ .***

Therefore, all prime divisors of  $N$  must be of the form  $6n + 1$ , where  $n$  is an integer.

It follows that,  $N$  leaves a remainder 1 when divided by 6, which is a contradiction. Hence, our assumption that there exist only a finitely many primes of the form  $6n + 5$ , is wrong.

***Therefore, there are infinitely many primes of the form  $6n + 5$ .***

This completes our proof.

**Result**

3 of 1

We have used Euclid's argument to show that there exist infinite number of primes of the respective forms, by contradict the fact of finite set of primes of the given forms.

Click for the complete proof.

## 15. a

**To Prove:** There exists no integer  $u = 4n + 3$  can be written as  $u = a^2 + b^2$ , where  $a$  and  $b$  are integers.

**Proof:** First we start with a claim.

**Claim:**  $a^2$  is divisible by 4 or leaves a remainder 1 when divisible by 4, where  $a$  is an integer.

**Proof of the Claim:** Let us consider an integer  $a$ . Then we have two cases.

Case-1:  $a$  is an odd integer.

Then we can write

$$a = 2k + 1, \text{ for some integer } k.$$

Then,

$$a^2 = (2k + 1)^2 = 4(k^2 + k) + 1.$$

Since  $k$  is an integer,  $k^2 + k$  is an integer. This implies  $a^2$  leaves remainder 1 when divided by 4. Since,  $a$  is arbitrary, square of any odd integer leaves remainder 1 when divided by 4.

Case-2:  $a$  is an even integer.

Then

$$a = 2l, \text{ for some integer } l.$$

Now,

$$a^2 = 4l^2.$$

Therefore,  $a^2$  is divided by 4, as  $l^2$  is an integer. Since  $a$  is arbitrary, square of any even integer is divisible by 4.

Consequently,

**$a^2$  is divisible by 4 or leaves a remainder 1 when divisible by 4, where  $a$  is an integer.**

This completes our Claim.

Now back to our problem. We need to show that there exists no integer  $u = 4n + 3$  such that  $u$  can be written as sum of square of two integers.

**If possible, there exists such an integer  $u$ .**

Then, for some integers  $a, b$  we have

$$u = a^2 + b^2.$$

By our claim,

$$a^2 \equiv 0 \text{ or } 1 \pmod{4}$$

$$b^2 \equiv 0 \text{ or } 1 \pmod{4}.$$

Therefore,

$$u = a^2 + b^2 \equiv 0 \text{ or } 1 \text{ or } 2 \pmod{4}.$$

It follows that,

**the possible remainder of  $u$  when divided by 4 are 0 or 1 or 2.**

So,  $u$  can not be of the form  $4n + 3$ , where  $n$  is an integer. So, we arrived at a contradiction.

Hence, there exists no integer  $u = 4n + 3$  can be written as  $u = a^2 + b^2$ , where  $a$  and  $b$  are integers.

This completes our proof.

## Result

3 of 3

Considering any integer  $a$  we claim that  $a^2$  leaves remainder 0 or 1 when divided by 4 and then we have proved that for any integers  $a, b$ ,  $a^2 + b^2$  leaves remainder 0 or 1 or 2 when divided by 4, and follows the result. Click for the complete proof.

16. a

**Given:**  $T$  is an infinite subset of  $\mathbb{N}$ .

**To Prove:** Existence of an one-one mapping of  $T$  onto  $\mathbb{N}$ .

**Proof:** Since,  $\mathbb{N}$  is **countable** and  $T$  is an infinite subset of  $\mathbb{N}$ , it yield's that  $T$  is **countable**.

Then elements of  $T$  can be represents as  $\{x_1, x_2, x_3, \dots, x_n, \dots\}$ , where  $x_i < x_j$  if  $i < j$ .

Now, let us define a mapping  $f : T \rightarrow \mathbb{N}$  by

$$f(x_i) = i.$$

This map is **well defined by definition**, i.e.,

$$i = j \implies f(x_i) = f(x_j).$$

We now prove that  $f$  is one-one.

Let  $f(x_i) = f(x_j)$ , for some  $i, j \in \mathbb{N}$ .

Then,

$$f(x_i) = f(x_j) \implies i = j \implies x_i = x_j.$$

**Contrapositively,**

$$x_i \neq x_j \implies f(x_i) \neq f(x_j).$$

Hence,  $f$  is one-one.

In order to show that  $f$  is onto, let  $k$  be an arbitrary element in  $\mathbb{N}$ . Then, by our hypothesis  $x_k$  is an element in  $T$

**corresponding to  $k$  under  $f$**

. Hence,  $f$  is onto.

Therefore,  $f$  is the required mapping.

---

## Result

3 of 3

Enumerating  $T$  as  $\{x_1, x_2, x_3, \dots, x_n, \dots\}$ , where  $x_i < x_j$  if  $i < j$  and define the mapping  $f : T \rightarrow \mathbb{N}$  by  $f(x_i) = i$ , we have shown that  $f$  is one-one between  $T$  onto  $\mathbb{N}$ .

Click for the complete proof.

17. a

**To Prove:** For a prime  $p$  there cannot exist non-zero integers  $a$  and  $b$  such that

$$a^2 = pb^2 \text{ holds.}$$

**Proof:** First we claim that  $\sqrt{p}$  is irrational for every prime  $p$ .

**Proof of the Claim:** If possible,  $\sqrt{p}$  is a rational number. Then there exist integers  $x$  and  $y$  satisfying  $\text{GCD}(x, y) = 1$  and  $y \neq 0$  such that

$$\sqrt{p} = \frac{x}{y}.$$

Then by squaring both side we have

$$p = \frac{x^2}{y^2} \implies p \cdot y^2 = x^2 \implies y^2 = \frac{x^2}{p}.$$

Since  $y$  is an integer,  $p$  divides  $x^2$ . As  $p$  is a prime,  $p$  divides  $x$ . Then there exists an integer  $l$  such that

$$x = pl.$$

Then squaring both side

$$x^2 = p^2 l^2 \implies p \cdot y^2 = p^2 l^2 \implies l^2 = \frac{y^2}{p}.$$

This implies  $p$  divides  $y^2$ , since  $l$  is an integer.

But  $p$  is a prime, so  $p$  divides  $y$ .

Consequently,

**$p$  divides both of  $x$  and  $y$  simultaneously.**

Which contradicts the fact that  $\text{GCD}(x, y) = 1$ . Hence our assumption is wrong.

Therefore,

**$\sqrt{p}$  is an irrational number.**

This completes our Claim.

Now back to our question.

If possible, let us assume that there exist non-zero integers  $a$  and  $b$  such that

$$a^2 = pb^2 \text{ holds for any prime } p.$$

Then

$$a^2 = pb^2 \implies p = \frac{a^2}{b^2} \implies \sqrt{p} = \pm \frac{a}{b}.$$

**Since  $a, b$  are non-zero integers,  $\sqrt{p}$  defined to be a rational number, which is an impossibility by our above proved Claim.**

Hence, for a prime  $p$  there cannot exist non-zero integers  $a$  and  $b$  such that

$$a^2 = pb^2 \text{ holds.}$$

This completes our proof.

## Result

3 of 3

Considering a prime  $p$  we have shown that  $\sqrt{p}$  is irrational, and by using this we have shown that there cannot exist non-zero integers  $a$  and  $b$  such that  $a^2 = pb^2$  holds. Click for the complete proof.

## Section 1–6

### 1. a

Let  $P(n)$  be the proposition that the statement

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$$

For  $n = 1$ , we have

$$1^2 = \frac{1}{6} \cdot 1(1+2)(2 \cdot 1 + 1)$$

which is certainly true. Suppose  $P(k)$  be true. i.e.

$$1^2 + 2^2 + \cdots + k^2 = \frac{1}{6}k(k+1)(2k+1)$$

Then

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\ &= \frac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\ &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1) \end{aligned}$$

Therefore the proposition  $P(k+1)$  is also true. By induction,  $P(n)$  is true for all  $n \geq 1$ .

### 2. a

Let  $P(n)$  be the proposition that the statement

$$1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$$

For  $n = 1$ , we have

$$1^3 = \frac{1}{4} \cdot 1^2(1+1)^2$$

which is certainly true i.e  $P(1)$  is true. Suppose  $P(k)$  be true. i.e.

$$1^3 + 2^3 + \cdots + k^3 = \frac{1}{4}k^2(k+1)^2$$

Then

$$\begin{aligned} 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \frac{1}{4}k^2(k+1)^2 + (k+1)^3 \\ &= \frac{1}{4}(k+1)^2(k^2 + 4k + 4) \\ &= \frac{1}{6}(k+1)^2(k+2)^2 \end{aligned}$$

Therefore the proposition  $P(k+1)$  is also true. By induction,  $P(n)$  is true for all  $n \geq 1$ .

### 3. a

Let  $P(n)$  be the proposition that the set having  $n \geq 2$  elements has  $\frac{1}{2}n(n - 1)$  subsets having only 2 elements. For  $n = 2$ , we have  $\frac{1}{2} \cdot 2(2 - 1) = 1$  therefore  $P(2)$  is true. Suppose  $P(k)$  be true. i.e. Set having  $k$  elements exactly has  $\frac{1}{2}k(k - 1)$  subsets with two elements. Suppose an element is added to set with  $k$  elements, then  $k$  new subsets with two elements can be formed. Thus the total number of elements in set having  $k + 1$  elements is

$$\frac{1}{2}k(k - 1) + k = \frac{1}{2}k(k - 1 + 2) = \frac{1}{2}k(k + 1)$$

Thus the proposition  $P(k)$  is true. Therefore  $P(n)$  is true for all  $n \geq 2$ .

### 4. a

Let  $P(n)$  be the proposition that for a set with  $n \geq 3$  elements, number of subsets having 3 elements is  $n(n - 1)(n - 2)/3!$ . For  $n = 3$ , we get

$$3(3 - 1)(3 - 2)/3! = 1$$

A set with 3 elements can have only one subset with three elements i.e. itself. Therefore  $P(1)$  is true. Let  $P(k)$  be true. i.e. A set with  $k$  elements has  $k(k - 1)(k - 2)/3!$  subsets with three elements.

A set with  $k + 1$  elements can be made by adding one element to it. Choose any two elements from set with  $k$  elements. It can be done in  $k(k - 1)/2$  ways. Adding new element not in this set gives new  $k(k - 1)/2$  subsets with three elements. Therefore the total number of subsets (with three elements) is

$$\frac{1}{3!}k(k - 1)(k - 2) + \frac{1}{2}k(k - 1) = k(k - 1)\left(\frac{1}{6}(k - 2) + \frac{1}{2}\right) = \frac{1}{6}(k + 1)k(k - 1)$$

Therefore  $P(k + 1)$  is true. By induction,  $P(n)$  is true for all  $n \geq 3$ .

### 5. a

Proposition 1. The set with  $n \geq 4$  elements can have

$$\binom{n}{4} = \frac{n(n - 1)(n - 2)(n - 3)}{4!}$$

subsets with 4 elements.

Proof: Let  $P(n)$  be proposition 1. For  $n = 4$ , we have

$$\frac{4(4 - 1)(4 - 2)(4 - 3)}{4!} = 1$$

which is trivially true since only one subset (itself) with 4 elements is possible. Let  $P(k)$  be true i.e. set with  $k$  elements can have  $\binom{k}{4}$  subsets with 3 elements. Then in set with  $k + 1$  elements, there are  $\binom{k}{3}$  new subsets with four elements (adding new element to subsets with 3 elements). The total number of subsets is

$$\binom{k}{4} + \binom{k}{3} = \binom{k+1}{4}$$

Therefore  $P(n)$  is true for all  $n \geq 4$ .

### 6. a

Let  $P(n)$  be the proposition that if  $p \mid (a_1 a_2 \dots a_n)$  for prime  $p$  then  $p \mid a_i$  for some  $1 \leq i \leq n$ . For  $n = 1$ , this is trivially true. Suppose for  $n = k$ , the statement is true i.e.  $p \mid (a_1 a_2 \dots a_k)$  then  $p \mid a_i$  for some  $1 \leq i \leq k$ . Suppose  $p \mid (a_1 a_2 \dots a_{k+1})$  then  $p \mid ((a_1 a_2 \dots a_k) a_{k+1})$ . If  $p \mid a_{k+1}$ , then this is trivially true. If  $p \nmid a_{k+1}$  then  $p \mid (a_1 \dots a_k)$  which is true by proposition  $P(k)$ . Therefore  $P(k+1)$  is true and  $P(n)$  is true for all  $n \geq 1$ .

## 7. a

Let  $P(n)$  be the proposition that

$$1 + a + \dots + a^n = \frac{a^{n+1} - 1}{a - 1}$$

for  $a \neq 1$ . For  $n = 1$ , we have

$$1 + a = \frac{a^2 - 1}{a - 1}$$

which is true. Therefore  $P(1)$  be true. Let  $P(k)$  be true. i.e.

$$1 + a + \dots + a^k = \frac{a^{k+1} - 1}{a - 1}$$

Then

$$\begin{aligned} 1 + a + \dots + a^k + a^{k+1} &= \frac{a^{k+1} - 1}{a - 1} + a^{k+1} \\ &= a^{k+1} \left( \frac{1}{a - 1} + 1 \right) - \frac{1}{a - 1} \\ &= a^{k+1} \left( \frac{a}{a - 1} \right) - \frac{1}{a - 1} \\ &= \frac{a^{k+2} - 1}{a - 1} \end{aligned}$$

Therefore  $P(k+1)$  is true. Therefore, by induction  $P(n)$  is true for all  $n \geq 1$ .

## 8. a

Let  $P(n)$  be proposition that

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}$$

For  $n = 1$ , this is trivially true. Suppose  $P(k)$  be true. i.e.

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{k \cdot (k+1)} = \frac{k}{k+1}$$

Then

$$\begin{aligned} \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(k+1) \cdot (k+2)} &= \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1) \cdot (k+2)} \\ &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{1}{k+1} \left( k + \frac{1}{k+2} \right) \\ &= \frac{1}{k+1} \left( \frac{(k+1)^2}{k+2} \right) \\ &= \frac{k+1}{k+2} \end{aligned}$$

Therefore  $P(k+1)$  is also true. By induction  $P(n)$  is true for all  $n \geq 1$ .

## 9. a

We will prove that  $P(n)$  is true for all  $n \geq n_0$ .

Let  $m = n - n_0 + 1$ .

Then  $m$  takes all positive integer values ( i.e,  $m \geq 1$  ).

Let  $Q(m) = P(m + n_0 - 1) = P(n)$ .

Then,  $Q(m)$  is a statement about positive integers.

Now,  $Q(1) = P(1 + n_0 - 1) = P(n_0)$ .

Thus,  $P(n_0)$  is true  $\implies Q(1)$  is true.

Now, assume that  $Q(j)$  is true.

$\implies P(j + n_0 - 1)$  is true.

But this implies that  $P(j + n_0)$  is true (as given in the problem).

That is,  $Q(j + 1)$  is true.

Thus, by the principle of mathematical induction,  $Q(m)$  is true for all positive integers  $m$ . i.e., for  $m \geq 1$ .

But  $m = n - n_0 + 1$ .

So,  $m \geq 1 \implies n \geq n_0$ .

$\implies P(n)$  is true for all  $n \geq n_0$

## Result

$P(n)$  is true for all  $n \geq n_0$

## 10. a

- Given:**  $P(n)$  is a proposition about integers  $n$  such that
- (1)  $P(1)$  is true;
  - (2) if  $P(j)$  is true for all positive integers  $j < k$ , then  $P(k)$  is true.

**To Prove:**  $P(n)$  is true for all positive integers  $n$ .

**Proof:** We will proof our problem by the way to contradiction.

If possible, let us assume that there exists a positive integer  $n_0$  for which the proposition  $P(n)$  is false.

Let us now consider

**the set  $S$  of all those positive integers  $k$  for which the proposition  $P(n)$  is false.**

In other words,

$$S := \{k \in \mathbb{N} \mid k \geq 1 \text{ and } P(k) \text{ is false}\}.$$

Clearly  $S$  is a non-empty subset of  $\mathbb{N}$ , since  $n_0 \in S$ . Then by

**Well ordering property of the set  $\mathbb{N}$ ,**

there exists a least element in  $S$ , say  $r$ .

Clearly,  $r \neq 1$ , by the given condition (1).

Therefore,

$$1 \notin S \text{ and } r > 1.$$

Now it follows that,  $P(j)$  is true for all positive integers  $j$ , which are less than  $r$ . But by the given condition (2),  $P(r)$  is true, that is,  $r \notin S$ . This is a contradiction,

**since  $r$  is the smallest element of the set  $S$ .**

Hence our assumption is wrong.

Therefore, the proposition  $P(n)$  is true for all positive integers  $n$ .

This completes the proof.

2 of 2

## Result

Considering the non-empty set  $S := \{k \in \mathbb{N} \mid k \geq 1 \text{ and } P(k) \text{ is false}\}$ , we have contradict the fact (2) in the given condition by using Well ordering property of the set  $\mathbb{N}$ , follows that  $S$  is empty. Click for the complete proof.

11. a

Let us consider the proposition  $P(n)$  is given by the assignment

" $2n + 1$  is an even number".

Here the proposition is taken over all positive integers  $n$ .

It is well known to us that,

**for any positive integer  $n$ ,  $2n + 1$  is always odd.**

So, our proposition is vacuously wrong.

But we will show that,  $P(n + 1)$  is true whenever  $P(n)$  is true.

So, let us consider the proposition  $P(n + 1)$ .

We have

$$2(n + 1) + 1 = (2n + 1) + 2.$$

Therefore,  $(2n + 1) + 2$  is even if and only if  $2n + 1$  is even, which is true by our induction hypothesis. Hence we have conclude that  $2(n + 1) + 1$  is even. Therefore, the proposition  $P(n + 1)$  is true whenever  $P(n)$  is true.

Hence, the induction step holds for our considered proposition  $P(n)$ , even though  $P(n)$  is false for all  $n$ .

This completes our proof.

## Result

2 of 2

Considering the proposition that, " $2n + 1$  is an even number", we have proved that the induction step hold for this proposition, even though  $P(n)$  is false for all  $n$ .

[Click for the complete proof.](#)

## 12. a

We have to prove that a set with  $n$  elements has  $2^n$  subsets, using the principle of mathematical induction.

Let  $P(n)$  be the statement that a set with  $n$  elements has  $2^n$  subsets.

When  $n = 1$ , i.e, the set has only one element, the possible subsets are the empty set, and the set itself. Thus, when  $n = 1$ , the set has  $2^1 = 2$  subsets. i.e,  $P(1)$  is true.

Now, assume that  $P(k)$  is true. That is, if a set has  $k$  elements, it has  $2^k$  subsets (Induction hypothesis). To complete the proof by induction, we need to show that a set with  $k + 1$  elements has  $2^{k+1}$  subsets.

Let  $S$  be a set with  $k + 1$  elements, and let  $a$  be an element of  $S$ .

Then the set  $S - \{a\}$  has  $k$  elements. By the Induction hypothesis,  $S - \{a\}$  has  $2^k$  subsets.

Now, all subsets of  $S - \{a\}$  are subsets of  $S$ . Thus  $S$  already has  $2^k$  subsets.

The other subsets of  $S$  all contain  $a$ . Thus, each of them is of the form  $A \cup \{a\}$ , where  $A$  is a subset of  $S - \{a\}$ .

The number of such subsets equal the number of subsets of  $S - \{a\}$ , i.e,  $2^k$ .

Thus the total number of subsets of  $S$  is  $2^k + 2^k = 2^{k+1}$ .

Thus we have that  $P(k)$  is true  $\implies P(k + 1)$  is true.

Hence, by induction,  $P(n)$  is true for all positive integers  $n$ . i.e, a set with  $n$  elements has  $2^n$  elements.

## 13. a

**To Prove:**  $n^3 - n$  is divisible by 3.

**Proof:** We will use induction on  $n$  to show that  $n^3 - n$  is divisible by 3.

**Step-1:** Let us take  $n = 1$ . Then trivially our statement is true, since 0 is always divisible by 3.

**Step-2:** Let us assume that our statement is true for some  $m$ , where  $m$  is a positive integer.

We will propose to prove that, our statement is true for  $m + 1$ .

That is, we need to show that  $(m + 1)^3 - (m + 1)$  is divisible by 3 whenever  $m^3 - m$  is divisible by 3.

Now,

$$(m + 1)^3 - (m + 1) = (m^3 + 3m^2 + 3m + 1) - (m + 1) = (m^3 - m) + 3(m^2 + m).$$

By our inductive hypothesis,  $m^3 - m$  is divisible by 3 and the later term of the above expression is a multiple of 3, consequently  $(m + 1)^3 - (m + 1)$  is divisible by 3.

Therefore our statement is true for  $m + 1$  whenever it is true for  $m$ .

Hence by law of induction we have proved that

$$n^3 - n \text{ is divisible by 3 for all positive integers } n.$$

This completes the proof.

## Result

2 of 2

Using Induction on  $n$  we have proved that the statement is true for  $m + 1$  whenever it is true for  $m$ , for any positive integer  $m$ , follows our result.

[Click for the detailed proof.](#)

## 14. a

**Question:** Using induction on  $n$ , generalize the result in Problem 13 to: If  $p$  is a prime number, then  $n^p - n$  is always divisible by  $p$ . (Hint: The binomial theorem.)

### Step 2

Let  $P(n)$  be the statement, where

$$P(n) : n^p - n \text{ is divisible by } p, \text{ for all } n \geq 1.$$

Clearly  $P(1)$  is true. As  $1^p - 1 = 0$  is divisible by  $p$ .

Now assume  $P(n)$  is true. It means that  $n^p - n$  is divisible by  $p$ .

Thus there exist an a natural number  $k$  such that

$$(n+1)^p - (n+1) = (n^p + kp + 1) - (n+1) = (n^p - n) + kp$$

Now using induction hypothesis, there exist natural number  $s$  such that  $n^p - n = sp$ . Therefore  $(n+1)^p - (n+1) = (k+s)p$  and hence divisible by  $p$ . Therefore  $P(n+1)$  is true. Now using binomial theorem we have,

$$(n+1)^p - (n+1) = \left( n^p + \binom{p}{1} n^{p-1} + \dots + \binom{p}{k} n^{p-k} + \dots + 1 \right) - (n+1)$$

Notice that for any  $1 < k < p$ , we have

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{(p-1)\cdots(p-k+1)}{k!} = \frac{p}{k} \binom{p-1}{k-1} \implies k \binom{p}{k} = pt,$$

where  $t = \binom{p-1}{k-1} \in \mathbb{N}$ . Since  $p$  is prime, and  $1 < k < p$ , so  $k$  and  $p$  are coprime. Thus  $\binom{p}{k}$  is divisible by  $p$ .

Thus there exist an a natural number  $r$  such that

$$(n+1)^p - (n+1) = (n^p + rp + 1) - (n+1) = (n^p - n) + rp$$

Now using induction hypothesis, there exist natural number  $s$  such that  $n^p - n = sp$ . Therefore  $(n+1)^p - (n+1) = (r+s)p$  and hence divisible by  $p$ . Therefore  $P(n+1)$  is true.

## Result

5 of 5

Thus by principle of mathematical induction we have

$$n^p - n \text{ is divisible by } p, \text{ for all } n \geq 1.$$

15. a

**To Prove:** The number of  $1 - 1$  mapping from a set of  $n$  elements to itself is  $n!$ .

**Proof:** Let  $S$  be a set of  $n$  elements. We will use induction on  $n$  to show that the number of  $1 - 1$  mapping from  $S$  to itself is  $n!$ .

If  $n = 1$ . Then  $S$  will be a singleton set  $\{a\}$ , say, and the only  $1 - 1$  mapping exists is

$$f(a) = a.$$

Let us assume that our statement holds for the set  $S$  having  $k$  elements for some natural number  $k$ , that is,

that is, the number of  $1 - 1$  mapping from  $S$  to  $S$  is  $k!$ , whenever  $S$  contains  $k$  elements for some positive integer  $k$ .

We will show that our statement is true for  $k + 1$  elements.

Let us consider an arbitrary element  $a$  from  $S$ . Now consider the set  $S \setminus \{a\}$ , say  $T$ . Then  $T$  contains  $k$  elements and by induction hypothesis the number of  $1 - 1$  map between  $T$  to itself is  $k!$ .

Now if we consider the whole set  $S$ , that is  $T \cup \{a\}$ , then we can send  $a$  to any of  $k + 1$  elements of  $S$ , including to  $a$  also.

**Since there are  $(k + 1)$  elements and already  $k!$   $1 - 1$  mapping from  $S \setminus \{a\}$  to itself,**

the number of  $1 - 1$  mapping can be constructed are  $(k + 1) \times k! = (k + 1)!$ .

Therefore, the number of possible  $1 - 1$  mapping from  $S$  (having  $k + 1$  elements) to itself is  $(k + 1)!$ .

Hence the statement is true for  $k + 1$  whenever it is true for  $k$ . Hence by method of induction on  $n$ , we have proved that

**"The number of  $1 - 1$  mapping from a set of  $n$  elements to itself is  $n!$ ", for every positive integer  $n$ .**

This completes the proof.

## Result

2 of :

By considering a set  $S$  having  $n$  elements we have proved by using induction on  $n$  that, the number of  $1 - 1$  mapping from  $S$  to itself is  $n!$ .

Click for the complete proof.

# Section 1–7

1. a

(a)

$$\begin{aligned}(6 - 7i)(8 + i) &= 6(8 + i) - 7i(8 + i) \\&= 48 + 6i - 56i - 7i^2 \\&= 48 - 7(-1) - 50i \\&= 55 - 50i\end{aligned}$$

(b)

$$\begin{aligned}(2/3 + 3/2i)(2/3 - 3/2i) &= 2/3(2/3 - 3/2i) + 3/2i(2/3 - 3/2i) \\&= 2/3 \cdot 2/3 - 2/3 \cdot 3/2i + 3/2i \cdot 2/3 - 3/2i \cdot 3/2 \\&= (2/3)^2 + 0 - (3/2)^2i^2 \\&= (2/3)^2 - (3/2)^2(-1) \\&= 4/9 + 9/4 \\&= 97/36\end{aligned}$$

(c)

$$\begin{aligned}(6 + 7i)(8 - i) &= 6(8 - i) + 7i(8 - i) \\&= 48 - 6i + 56i - 7i^2 \\&= 48 - 7(-1) + 50i \\&= 55 + 50i\end{aligned}$$

2. a

We know  $z\bar{z} = |z|^2$  where  $|z|$  is defined as  $|z| = \sqrt{a^2 + b^2}$  for  $z = a + ib$ . This gives

$$z \cdot \frac{\bar{z}}{|z|^2} = 1$$

Therefore inverse of  $z$  is  $\bar{z}/|z|^2$ .

(a) For  $z = 6 + 8i$

$$\begin{aligned} z^{-1} &= \frac{\bar{z}}{|z|^2} \\ &= \frac{6 - 8i}{6^2 + 8^2} \\ &= \frac{6}{100} - \frac{8}{100}i \\ &= \frac{3}{50} - \frac{2}{25}i \end{aligned}$$

(b) For  $z = 6 - 8i$ ,

$$\begin{aligned} z^{-1} &= \frac{\bar{z}}{|z|^2} \\ &= \frac{6 + 8i}{6^2 + 8^2} \\ &= \frac{6}{100} + \frac{8}{100}i \\ &= \frac{3}{50} + \frac{2}{25}i \end{aligned}$$

(c) For  $z = (1/\sqrt{2}) + (1/\sqrt{2})i$

$$\begin{aligned} z^{-1} &= \frac{\bar{z}}{|z|^2} \\ &= \frac{(1/\sqrt{2}) - (1/\sqrt{2})i}{1/2 + 1/2} \\ &= \frac{(1/\sqrt{2}) - (1/\sqrt{2})i}{1} \\ &= (1/\sqrt{2}) - (1/\sqrt{2})i \end{aligned}$$

## Result

[see answers](#)

### 3. a

We need to prove  $\bar{z}^{-1} = \overline{z^{-1}}$ . Now, Let  $z = a + ib$ . So  $\bar{z} = a - ib$ . Hence  $\bar{z}^{-1} = \frac{1}{a - ib} = \frac{a + ib}{(a + ib)(a - ib)} = \frac{a + ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} + i \frac{b}{a^2 + b^2}$ . Again  $\overline{z^{-1}} = \overline{\frac{1}{a + ib}} = \overline{\frac{a - ib}{a^2 + b^2}} = \overline{\frac{a}{a^2 + b^2} - i \cdot \frac{b}{a^2 + b^2}} = \frac{a}{a^2 + b^2} - i \cdot \frac{b}{a^2 + b^2}$ . So we are done hence there is equality from both sides.

## Result

[2 of 2](#)

[See the proof](#)

### 4. a

$$(\cos(\theta) + i\sin(\theta))^{-1} = \frac{\cos(\theta) - i\sin(\theta)}{(\cos(\theta) + i\sin(\theta))(\cos(\theta) - i\sin(\theta))} = \frac{\cos(\theta) - i\sin(\theta)}{\cos^2(\theta) + \sin^2(\theta)} = \cos(\theta) - i\sin(\theta).$$

## Result

See the proof

5. a

Suppose  $z = a + ib$ . Then  $w = \bar{z} = a - ib$ . Again  $\bar{\bar{z}} = \bar{w} = a + ib$ . So,  $\bar{\bar{z}} = z$ . Now, Let  $w = c + id$ . Then  $\bar{z} + w = \overline{a + ib + c + id} = \overline{(a+c) + i(b+d)} = (a+c) - i(b+d)$ . And  $\bar{z} + \bar{w} = (a - ib) + (c - d) = (a+c) - i(b+d) = \bar{z} + w$ .

Also,  $z + \bar{z} = a + ib + a - ib = 2a$ , hence twice the real part. And,  $z - \bar{z} = a + ib - (a - ib) = (2b)i$ , hence twice the imaginary part times  $i$ .

## Result

2 of 2

See the result

6. a

Let  $z$  be real, then  $z = a + 0i$  and  $\bar{z} = a + 0i$ . This shows  $z = \bar{z}$ . Conversely, if  $z = \bar{z}$ , then  $\mathbf{Re}(z) = \frac{1}{2}(z + \bar{z}) = z$ . Therefore  $z$  must be real.

Similarly, suppose  $z = -\bar{z}$ , then  $\mathbf{Im}(z) = \frac{1}{2i}(z - \bar{z}) = \frac{z}{i}$ . This gives  $i\mathbf{Im}(z) = z$ . Since  $\mathbf{Im}(z) \in \mathbb{R}$ ,  $z = \mathbf{Im}(z)i$  must be purely imaginary. Conversely, if  $z$  is purely imaginary, then  $\frac{1}{2}(z + \bar{z}) = \mathbf{Re}(z) = 0$ . This gives  $z = -\bar{z}$ .

Method 2.

## Step 1

1 of 2

Let  $z \in \mathbb{R}$ . Then  $z = \bar{z}$  is very obvious. In the other direction, if  $z = \bar{z}$ , then if  $z = a + ib$ , we have  $a + ib = a - ib \implies b = 0 \implies \mathbf{Im}(z) = 0 \implies z = a \in \mathbb{R}$ . Now if  $z = ib$ , then  $\bar{z} = -ib = -z$ . In the other direction, if  $\bar{z} = -z$ , and if  $z = a + ib$ , then  $a - ib = -a - ib \implies 2a = 0 \implies a = 0$ . So  $z = ib$ , and hence is purely imaginary.

## Result

2 of 2

See the proof

7. a

Let  $z = a + ib$  and  $w = c + id$  where  $a, b, c, d \in \mathbb{R}$ , then

$$\begin{aligned} zw &= (a + ib)(c + id) \\ &= a(c + id) + ib(c + id) \\ &= ac + iad + ibc + ibid \\ &= ac + i^2bd + iad + ibd \\ &= ac - bd + i(ad + bc) \end{aligned}$$

Since multiplication of real numbers is commutative, we have

$$\begin{aligned} zw &= ac - bd + i(ad + bc) \\ &= ca - bd + i(da + cb) \\ &= (c + id)(a + ib) \\ &= wz \end{aligned}$$

## 8. a

Let  $z = a + ib$ . Now  $\bar{z} = a - ib$ . We have  $\frac{1}{\bar{z}} = \frac{1}{a - ib} = \frac{a+ib}{(a-ib)(a+ib)} = \frac{a+ib}{a^2+b^2} = \frac{a}{a^2+b^2} - i \cdot \frac{b}{a^2+b^2}$ . Then  $|\frac{1}{\bar{z}}| = |\frac{a}{a^2+b^2} - i \cdot \frac{b}{a^2+b^2}| = \sqrt{\frac{a^2}{(a^2+b^2)^2} + \frac{b^2}{(a^2+b^2)^2}} = \frac{1}{a^2+b^2} = \frac{1}{|z|}$ .

### Result

2 of 2

See the proof

## 9. a

(a)

$$\begin{aligned} |6 - 4i| &= \sqrt{6^2 + 4^2} \\ &= \sqrt{36 + 16} \\ &= 2\sqrt{13} \end{aligned}$$

(b)

$$\begin{aligned} |1/2 + (2/3)i| &= \sqrt{(1/2)^2 + (2/3)^2} \\ &= \sqrt{\frac{1}{4} + \frac{4}{9}} \\ &= \sqrt{\frac{25}{36}} \\ &= \frac{5}{6} \end{aligned}$$

(c)

$$\begin{aligned} \left| \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \right| &= \sqrt{(1/\sqrt{2})^2 + (1/\sqrt{2})^2} \\ &= \sqrt{\frac{1}{2} + \frac{1}{2}} \\ &= \sqrt{1} \\ &= 1 \end{aligned}$$

## 10. a

To show  $|\bar{z}| = |z|$ . Let  $z = a + ib$ . We know  $|z| = a^2 + b^2$ . Then  $|\bar{z}| = a^2 + (-b)^2 = a^2 + b^2$ . So we have the result

## Result

2 of 2

[See the proof](#)

## Method 2.

Another possible way:

We have  $\overline{(\bar{z})} = z$ . Since the multiplication of complex number is commutative.

$$|z| = \sqrt{z\bar{z}} = \sqrt{(\bar{z})\bar{z}} = \sqrt{\bar{z}(\bar{z})} = |\bar{z}|$$

## 11. a

We use the Euler's formula  $e^{i\theta} = \cos \theta + i \sin \theta$

(a)

$$\begin{aligned} z &= \frac{\sqrt{2}}{2} - \frac{1}{\sqrt{2}}i \\ &= \cos(-\pi/4) + i \sin(-\pi/4) \\ &= e^{-i\frac{\pi}{4}} \end{aligned}$$

(b)

$$\begin{aligned} z &= 4i \\ &= 0 + 4 \sin(\pi/2)i \\ &= 4 \cos(\pi/2) + 4 \sin(\pi/2)i \\ &= 4e^{i\pi/2} \end{aligned}$$

(c)

$$\begin{aligned} z &= \frac{6}{\sqrt{2}} + \frac{6}{\sqrt{2}}i \\ &= 6 \left( \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i \right) \\ &= 6(\cos(\pi/4) + i \sin(\pi/4)) \\ &= 6e^{i\pi/4} \end{aligned}$$

(d)

$$\begin{aligned} z &= -\frac{13}{2} + \frac{39}{2\sqrt{3}}i \\ &= 13 \left( -\frac{1}{2} + i \frac{\sqrt{3}}{2} \right) \\ &= 13(\cos(2\pi/3) + i \sin(2\pi/3)) \\ &= 13e^{i\frac{2\pi}{3}} \end{aligned}$$

## 12. a

This can be shown directly as follows

$$\begin{aligned}
 \cos \theta + i \sin \theta &= \cos^2\left(\frac{\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) + i2 \sin\left(\frac{\theta}{2}\right) \cos\left(\frac{\theta}{2}\right) \\
 &= \cos^2\left(\frac{\theta}{2}\right) + (i \sin^2\left(\frac{\theta}{2}\right))^2 + i2 \sin\left(\frac{\theta}{2}\right) \cos\left(\frac{\theta}{2}\right) \\
 &= \left( \cos\left(\frac{\theta}{2}\right) + i \sin\left(\frac{\theta}{2}\right) \right)^2
 \end{aligned}$$

Also, using polar form,

$$\begin{aligned}
 \left( \cos\left(\frac{\theta}{2}\right) + i \sin\left(\frac{\theta}{2}\right) \right)^2 &= \left( e^{i\frac{\theta}{2}} \right)^2 \\
 &= e^{i\theta} \\
 &= \cos \theta + i \sin \theta
 \end{aligned}$$

13. a

$$\begin{aligned}
 \left( \frac{1}{2} + \frac{1}{2}\sqrt{3}i \right)^3 &= (\cos(\pi/3) + i \sin(\pi/3))^3 \\
 &= \left( e^{i\pi/3} \right)^3 \\
 &= e^{i\pi} \\
 &= \cos(\pi) + i \sin(\pi) \\
 &= -1
 \end{aligned}$$

14. a

From De Moivre's Theorem, we have

$$(\cos \theta + i \sin \theta)^n = \cos(n\theta) + i \sin(n\theta)$$

for all integers  $n \geq 1$ . For  $n = 0$ , it follows trivially. For  $-n$ , we have

$$\begin{aligned}
 (\cos \theta + i \sin \theta)^{-n} &= \frac{1}{(\cos \theta + i \sin \theta)^n} \\
 &= \frac{1}{\cos(n\theta) + i \sin(n\theta)} \\
 &= \frac{1}{\cos(n\theta) + i \sin(n\theta)} \times \frac{\cos(n\theta) - i \sin(n\theta)}{\cos(n\theta) - i \sin(n\theta)} \\
 &= \frac{\cos(n\theta) - i \sin(n\theta)}{\cos^2(n\theta) + \sin^2(n\theta)} \\
 &= \cos(n\theta) - i \sin(n\theta) \\
 &= \cos(-n\theta) + i \sin(-n\theta)
 \end{aligned}$$

Therefore it follows  $(\cos \theta + i \sin \theta)^n = \cos(n\theta) + i \sin(n\theta)$  for all integers  $n$ .

15. a

From above problem

$$(\cos \theta + i \sin \theta)^n = \cos(n\theta) + i \sin(n\theta)$$

for all integers  $n$ . For rational number  $r = \frac{m}{n}$ , we have

$$\begin{aligned} \cos(r\theta) + i \sin(r\theta) &= \cos\left(n \frac{\theta}{m}\right) + i \sin\left(n \frac{\theta}{m}\right) \\ &= (\cos(\theta/m) + i \sin(\theta/m))^n \end{aligned}$$

We have

$$\left( \cos\left(\frac{\theta}{m}\right) + i \sin\left(\frac{\theta}{m}\right) \right)^m = \cos \theta + i \sin \theta$$

This gives

$$\cos\left(\frac{\theta}{m}\right) + i \sin\left(\frac{\theta}{m}\right) = \cos \theta + i \sin \theta^{1/m}$$

This gives

$$\begin{aligned} (\cos \theta + i \sin \theta)^r &= \cos\left(\frac{m}{n}\theta\right) + i \sin\left(\frac{n}{m}\theta\right) \\ &= \cos(r\theta) + i \sin(r\theta) \end{aligned}$$

## 16. a

Let  $w_0 = r^{1/n} e^{i\theta/n}$ , and suppose

$$z = w_0^n = r e^{i\theta}$$

Set  $w_k = r^{1/n} e^{i(2\pi k + \theta)/n}$  where  $k = 0, 1, \dots, n-1$ , then we get

$$w_k^n = (r^{1/n})^n e^{i(2\pi k + \theta)} = r e^{i\theta} \cdot e^{i2\pi k}$$

But  $e^{i2\pi k} = \cos(2\pi k) + i \sin(2\pi k) = 1$ . This gives  $w_k^n = r$ . This shows there are  $n$  distinct complex numbers  $w$  such that  $z = w^n$ .

## 17. a

From De Moivre's theorem, we have

$$\left( \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \right)^n = \cos(2\pi k) + i \sin(2\pi k)$$

Suppose  $\cos(2\pi k) + i \sin(2\pi k) = 1$ , then we get  $\cos(2\pi k) = 1$  and  $\sin(2\pi k) = 0$ . This gives  $k = \dots, -2, -1, 0, 1, 2, \dots$  i.e.  $k \in \mathbb{Z}$ .

Given  $0 < m < n$ , we have

$$\left( \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \right)^m = \cos\left(\frac{2mk\pi}{n}\right) + i \sin\left(\frac{2mk\pi}{n}\right)$$

Suppose  $\cos\left(\frac{2mk\pi}{n}\right) + i \sin\left(\frac{2mk\pi}{n}\right) = 1$  this gives  $\cos\left(\frac{2mk\pi}{n}\right) = 1$  and  $\sin\left(\frac{2mk\pi}{n}\right) = 0$ . This gives  $k = j \frac{n}{m}$  where  $j \in \mathbb{Z}$ . Thus if  $k$  is not integer multiple of  $\frac{n}{m}$ , then

$$\left( \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right) \right)^m \neq 1$$

## 18. a

We know  $i = e^{i\frac{\pi}{2}}$ . Suppose  $z = re^{i\theta}$  be any complex number, then

$$iz = e^{i\frac{\pi}{2}}re^{i\theta} = re^{i(\theta+\frac{\pi}{2})}$$

This shows that multiplication induces  $90^\circ$  anticlockwise rotation. Moreover for  $z = x + iy$ ,  $iz = -y + ix$ .  $(x, y) \rightarrow (-y, x)$  represents  $90^\circ$  rotation.

## 19. a

Let  $z = re^{i\theta}$ . Writing  $a + ib$  in polar form, we get  $a + ib = \sqrt{a^2 + b^2}e^{i\tan^{-1}(b/a)}$ . Multiplying, we get

$$z(a + ib) = r\sqrt{a^2 + b^2}e^{i(\theta + \tan^{-1}(b/a))}$$

This can be interpreted as the absolute value of  $z$  is magnified by  $\sqrt{a^2 + b^2}$  and the resulting point is rotated by  $\tan^{-1}(b/a)$  anticlockwise.

## 20. a

We use the following result  $z\bar{z} = |z|^2$ . Now,  $|z + w|^2 + |z - w|^2 = (z + w)(\bar{z} + \bar{w}) + (z - w)(\bar{z} - \bar{w}) = (z + w)(\bar{z} + \bar{w}) + (z - w)(\bar{z} - \bar{w}) = 2(z\bar{z} + w\bar{w}) = 2(|z|^2 + |w|^2)$ .

### Result

2 of 2

See the proof

## 21. a

For finding out a  $1 - 1$  correspondence between the set  $A$  and  $\mathbb{N}$ , we should first observe the following:

$$a + ib \in A \iff (a, b) \in \mathbb{Z} \times \mathbb{Z}.$$

Therefore, it is enough to find a  $1 - 1$  correspondence between  $\mathbb{Z} \times \mathbb{Z}$  to  $\mathbb{N}$ . At first we will find a bijection between  $\mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ . By the *Fundamental Theorem of Arithmetic*, any positive integer can be written as product of powers of 2 and an odd number, i.e., given any  $m \in \mathbb{Z}^+$ ,  $m = 2^k \cdot r$  where  $k \in \mathbb{Z} \cup \{0\}$  and  $r$  is a positive odd integer. Define a bijection,

$$f : \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+, (m, n) \mapsto 2^{m-1}(2n-1).$$

Define a map

$$f^{-1} : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ \times \mathbb{Z}^+,$$

as given any  $m \in \mathbb{Z}^+$  we can write  $m = \underbrace{2^{n-1}}_{\text{Powers of 2}} \cdot \underbrace{(2k-1)}_{\text{odd number}}$ . Define

$f^{-1}(m) = (n, k)$ . Clearly,  $f$  and  $f^{-1}$  are inverses of each other and therefore,  $\mathbb{Z}^+ \times \mathbb{Z}^+$  has a  $1 - 1$  correspondence with  $\mathbb{Z}^+$ . Similarly,

$$g : \mathbb{Z}^- \times \mathbb{Z}^- \rightarrow \mathbb{Z}^-, (m, n) \mapsto 2^{-(m+1)}(2n+1)$$

is a bijection between  $\mathbb{Z}^- \times \mathbb{Z}^-$  and  $\mathbb{Z}^-$ . Therefore, we have a bijection between  $\mathbb{Z} \times \mathbb{Z}$  and  $\mathbb{Z}$  namely,

$$h(m, n) = \begin{cases} 2^{m-1}(2n-1), & (m, n) \in \mathbb{Z}^+ \times \mathbb{Z}^+, \\ 0, & (m, n) = (0, 0), \\ 2^{-(m+1)}(2n+1), & (m, n) \in \mathbb{Z}^- \times \mathbb{Z}^-. \end{cases}$$

Now we define a bijection between  $\mathbb{Z}$  and  $\mathbb{N}$  as

$$\phi : \mathbb{Z} \rightarrow \mathbb{N},$$

$$\phi(m) = \begin{cases} 2m, & m \in \mathbb{Z}^+ \\ -2m + 1, & m \in \mathbb{Z}^- \cup \{0\} \end{cases}$$

Therefore,  $\phi \circ h$  is a bijection between  $\mathbb{Z} \times \mathbb{Z}$  and  $\mathbb{N}$  being a composition of bijection functions.

## Result

1 – 1 correspondence between  $A$  and  $\mathbb{N}$ .

22. a

We know that  $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$  and  $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$ . Let  $a$  be root of polynomial

$$x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1} x + \alpha_n$$

Then, we have

$$a^n + \alpha_1 a^{n-1} + \cdots + \alpha_{n-1} a + \alpha_n = 0$$

taking conjugate, we get

$$\overline{a^n + \alpha_1 a^{n-1} + \cdots + \alpha_{n-1} a + \alpha_n} = 0$$

Or,

$$\overline{a^n} + \overline{\alpha_1 a^{n-1}} + \cdots + \overline{\alpha_{n-1} a} + \bar{\alpha}_n = 0$$

Or,

$$\bar{a}^n + \alpha_1 \bar{a}^{n-1} + \cdots + \alpha_{n-1} \bar{a} + \alpha_n = 0$$

This shows that  $\bar{a}$  is also root of the polynomial

$$x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1} x + \alpha_n$$

23. a

Let  $z = a + ib$  and  $w = c + id$ , then

$$|z + w| = |(a + c) + i(b + d)| = \sqrt{(a + c)^2 + (b + d)^2}$$

We have  $|z| = \sqrt{a^2 + b^2}$  and  $|w| = \sqrt{c^2 + d^2}$ . Thus, we get

$$\sqrt{(a + c)^2 + (b + d)^2} = \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}$$

squaring both sides, we get

$$(a + c)^2 + (b + d)^2 = (a^2 + b^2) + (c^2 + d^2) + 2\sqrt{(a^2 + b^2)(c^2 + d^2)}$$

Simplification gives

$$ac + bd = \sqrt{(a^2 + b^2)(c^2 + d^2)}$$

Again, squaring gives

$$a^2c^2 + 2abcd + b^2d^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$

Simplifying, we get

$$2abcd = a^2d^2 + b^2c^2$$

Or,

$$(ad - bc)^2 = 0 \implies \frac{a}{c} = \frac{b}{d} = k$$

where  $k \geq 0$  is some constant. This gives  $a = ck$  and  $b = dk$  thus  $z = kw$  which is the necessary condition.

The condition is sufficient as  $z = kw$  gives

$$\begin{aligned} |z + w| &= |kw + w| \\ &= |k + 1||w| \\ &= k|w| + |w| \\ &= |kw| + |w| \\ &= |z| + |w| \end{aligned}$$

## 24. a

Suppose  $z_1 + \dots + z_{k-1} = z'$ , then  $|z' + z_k| = |z'| + |z_k|$  if and only if  $z' = c_k z_k$  for some  $c_k > 0$ . Suppose  $z_1 + \dots + z_{k-2} = z''$ . Then  $|z_1 + \dots + z_{k-2} + z_{k-1}| = |z'' + z_{k-1}| = |z''| + |z_{k-1}|$  if and only if  $z'' = c_{k-1} z_{k-1}$  for some  $c_{k-1} > 0$ . Continuing this way, we get

$$|z_1 + \dots + z_n| = |z_1| + \dots + |z_k|$$

if  $c_1 z_1 = c_2 z_2 = c_3 z_3 = \dots = c_k z_k$  where  $c_1, \dots, c_k > 0$  which is necessary condition.

The condition is sufficient. Suppose  $z_1 = c_2 z_2 = c_3 z_3 = \dots = c_k z_k$  where  $c_1, \dots, c_k \geq 0$

$$\begin{aligned} |z_1 + \dots + z_n| &= \left| z_1 \left( 1 + \frac{c_1}{c_2} + \dots + \frac{c_1}{c_k} \right) \right| \\ &= |z_1| \left( 1 + \frac{c_1}{c_2} + \dots + \frac{c_1}{c_k} \right) \\ &= |z_1| + \left( \left| z_1 \frac{c_1}{c_2} \right| + \left| z_k \frac{c_1}{c_1} \right| \right) \\ &= |z_1| + |z_2| + \dots + |z_k| \end{aligned}$$

Therefore the condition is sufficient.

## 25. a

We must have  $k \geq n$  since  $k < n$  implies  $\theta^k \neq 1$ . Using division algorithm,  $k = nq + r$  where  $0 \leq r < n$ . This gives

$$\theta^k = \theta^{nq+r} = (\theta^n)^q \theta^r = \theta^r = 1$$

Since  $0 \leq r < n$ , we must have  $r = 0$  thus  $k = nq \implies n \mid k$ .

## 26. a

We know

$$e^{2k\pi i} = \cos(2k\pi) + i \sin(2k\pi)$$

where  $k \in \mathbb{Z}$ . Suppose  $\theta^n = 1$  then  $\theta^n = e^{2k\pi i}$ . This gives

$$\theta = e^{\frac{2\pi ki}{n}}$$

where  $k = 1, \dots, n-1$ .

## Chapter 2

### Section 2–1

1. a

(a) The only axiom which doesn't fail is closure. Not a group.

(b) This structured set is closed, associative, and 0 is the identity element. But it fails having an inverse for each element. For instance, there is no integer  $b$  such that  $1 * b = 0$ .

(c) This structured set is closed, associative, and 0 is the identity element. But it fails having an inverse for each element. For instance, there is no integer  $b$  such that  $1 * b = 0$ .

(d) This one is a group. The group identity is 0 and the inverse of any element  $a$  is  $\frac{-a}{1-a}$ , which clearly is always defined because  $a$  can't equal  $-1$  and it can be shown to never equal  $-1$  itself (try it).

(e) Not closed as  $\frac{1}{5}, \frac{4}{5}$  are both in the set but  $\frac{1}{5} + \frac{4}{5} = \frac{1}{1}$  where 1 is not divisible by 5.

2. a

Closure: It was shown in example 6 that

$$T_{a,b} * T_{c,d} = T_{ac,ad+b}$$

If  $a$  is restricted to  $\pm 1$  and  $b$  can be anything then clearly  $T_{ac,ad+b} = T_{\pm 1,ad+b}$  is an element of  $H$ . Hence  $H$  is closed under  $*$ .

Associativity: The elements of  $H$  are functions and we know that composition of functions is associative.

Identity: Note that  $T_{1,0} = i$  is in  $H$  and we know that it acts as an identity under function composition.

Inverses: Let  $c = a$  and  $d = -\frac{b}{a}$ . From  $T_{a,b} * T_{c,d} = T_{ac,ad+b}$ , we conclude that  $ac = a^2 = (\pm 1)^2 = 1$  and  $a\left(-\frac{b}{a}\right) + b = 0$ . Hence  $T_{ac,ad+b} = i$ , as required. Thus for any  $T_{a,b} \in H$ ,  $T_{a,-\frac{b}{a}}$  is its inverse.

Thus, by definition,  $H$  is a group under  $*$ .

3. a

Note: It must be assumed that Herstein means for the  $a \neq 0$  restriction to still hold here. Or else this isn't a group. So we shall assume this.

Closure: It was shown in example 6 that

$$T_{a,b} * T_{c,d} = T_{ac,ad+b}$$

Note that if  $a, c$  are rational, then  $ac$  is too. Also  $ad + b$  must be real. Hence  $H$  is closed under  $*$ .

Associativity: The elements of  $H$  are functions and we know that composition of functions is associative.

Identity: Note that  $T_{1,0} = i$  is in  $H$  and we know that it acts as an identity under function composition.

Inverses: Let  $c = \frac{1}{a}$  and  $d = -\frac{b}{a}$ . From  $T_{a,b} * T_{c,d} = T_{ac,ad+b}$ , we conclude that  $ac = a\frac{1}{a} = 1$  and  $a\left(-\frac{b}{a}\right) + b = 0$ . Hence  $T_{ac,ad+b} = i$ , as required. Thus for any  $T_{a,b} \in H$ ,  $T_{\frac{1}{a}, -\frac{b}{a}}$  is its inverse.

Thus, by definition,  $H$  is a group under  $*$ .

#### 4. a

Closure: It was shown in example 6 that

$$T_{a,b} * T_{c,d} = T_{ac,ad+b}$$

If  $a = 1$  and  $b$  can be any real number then clearly  $T_{ac,ad+b} = T_{1,d+b}$  is an element of  $H$ . Hence  $H$  is closed under  $*$ .

Associativity: The elements of  $H$  are functions and we know that composition of functions is associative.

Identity: Note that  $T_{1,0} = i$  is in  $H$  and we know that it acts as an identity under function composition.

Inverses: Let  $c = 1$  and  $d = -b$ . From  $T_{a,b} * T_{c,d} = T_{ac,ad+b}$ , we conclude that  $ac = 1^2 = 1$  and  $a(-b) + b = -b + b = 0$ . Hence  $T_{ac,ad+b} = i$ , as required. Thus for any  $T_{a,b} \in H$ ,  $T_{1,-b}$  is its inverse.

Thus, by definition,  $H$  is a group under  $*$ .

#### 5. a

**To Prove:**  $g * f = f * g^{-1}$  and  $G$  which is defined in

Example 9

is a non-abelian group of order 8.

$$(a) \{g * f = f * g^{-1}\}.$$

First we observe that (and also stated in the

**Example 9**

)  $g$  is the counter clockwise rotation about the origin. It is also given that  $g^4 = e$ , where  $e$  denotes the identity mapping. Since,

$$\begin{aligned} g^4 = e &\implies g^{-1} = g^3 \implies g^{-1}(x, y) = g * g * g(x, y) \\ &= g(g(-y, x)) \\ &= g(-x, -y) \\ &= (y, -x) \end{aligned}$$

Therefore, we got

$$g^{-1}(x, y) = (y, -x)$$

Now,

$$\begin{array}{lll} (g * f)(x, y) &= (gf)(x, y) & (f * g^{-1})(x, y) &= (fg^{-1})(x, y) \\ &= g(f(x, y)) & &= f(g^{-1}(x, y)) \\ &= g(-x, y) & &= f(y, -x) \\ &(-y, -x) & &(-y, -x) \end{array}$$

Therefore,

$$g * f = f * g^{-1}.$$

We can even generalize this as

$$g^i * f = f * g^{-i} \implies g^i * f * g^i = f \quad (1)$$

which can be proved by induction easily. Observe that,

$$\begin{aligned} g * f = f * g^{-1} &\implies g * (g * f) = g * (f * g^{-1}) \\ &\implies g^2 * f = (g * f) * g^{-1} \\ &\implies g^2 * f = (f * g^{-1}) * g \\ &\implies g^2 * f = f * g^{-2} \end{aligned}$$

Moreover,

$$(f * g^i) * (f * g^j) = (f * f) * (g^{-i} * g^j) = g^{j-i} \quad (2)$$

(b) For proving it a non-abelian group of order 8 we will write its group table (Cayley Table) keeping the result (l) and (2) in our mind.

	$e$	$f$	$g$	$g^2$	$g^3$	$f * g$	$f * g^2$	$f * g^3$
$e$	$e$	$f$	$g$	$g^2$	$g^3$	$f * g$	$f * g^2$	$f * g^3$
$f$	$f$	$e$	$f * g$	$f * g^2$	$f * g^3$	$g$	$g^2$	$g^3$
$g$	$g$	$g * f = f * g^{-1} = f * g^3$	$g^2$	$g^3$	$e$	$f$	$f * g$	$f * g^2$
$g^2$	$g^2$	$f * g^2$	$g^3$	$e$	$g$	$fg^3$	$f$	$fg$
$g^3$	$g^3$	$f * g$	$e$	$g$	$g^2$	$f * g^2$	$f * g^3$	$f$
$f * g$	$f * g$	$g^3$	$f * g^2$	$f * g^3$	$f$	$e$	$g$	$g^2$
$f * g^2$	$f * g^2$	$g^2$	$f * g^3$	$f$	$f * g$	$g^3$	$e$	$g$
$f * g^3$	$f * g^3$	$g$	$f$	$f * g$	$f * g^2$	$g^2$	$g^3$	$e$

(c) See that

$$(f * g)(x, y) = f(g(x, y)) = f(-y, x) = (-x, -y)$$

whereas,

$$(g * f)(x, y) = g(f(x, y)) = g(-x, y) = (-y, -x).$$

Hence, the group is non-abelian.

(d) It has 8 elements which are listed in the above table.

## Result

See the proof.

## 6. a

**To Prove:** Given  $T_{a,b} \in G$  and  $V \in H$ ,  $T_{a,b} * V * T_{a,b}^{-1} \in H$ .

### Step 2

2 of 3

From the [Exercise 6](#),

$$T_{a,b} * T c, d = T_{ac,ad+b}.$$

So at first we need to compute the inverse of  $T_{a,b}$ . We want  $T_{c,d}$  such that

$$\begin{aligned} T_{a,b} * T_{c,d} &= T_{1,0} \\ \implies T_{ac,ad+b} &= T_{1,0} \end{aligned}$$

So we should take  $c = \frac{1}{a}$  and  $d = \frac{-b}{a}$ . This is well defined since  $a \neq 0$ . Let  $V \in H \implies V = T_{c,d}$  for some  $c \in \mathbb{Q}$  and  $d \in \mathbb{R}$ . Now Let us compute  $T_{a,b} * V * T_{a,b}^{-1}$ .

$$\begin{aligned} T_{a,b} * V * T_{a,b}^{-1} &= T_{a,b} * T_{c,d} * T_{a,b}^{-1} \\ &= T_{ac,ad+b} * T_{\frac{1}{a}, \frac{-b}{a}} \\ &= T_{ac \cdot \frac{1}{a}, (ad+b) \cdot \frac{-b}{a}} \\ &= T_{c, \frac{-b(ad+b)}{a}} \end{aligned}$$

Since,  $c \in \mathbb{Q} \implies T_{c, \frac{-b(ad+b)}{a}} \in H$ . Therefore,

$$T_{a,b} * V * T_{a,b}^{-1} \in H$$

## Result

See the proof.

7. a

**To Prove:** Given  $T_{a,b} \in G$  and  $V \in K$ ,  $T_{a,b} * V * T_{a,b}^{-1} \in K$ .

2 of 3

### Step 2

From the [Exercise 6](#),

$$T_{a,b} * T_{c,d} = T_{ac,ad+b}.$$

So at first we need to compute the inverse of  $T_{a,b}$ . We want  $T_{c,d}$  such that

$$\begin{aligned} T_{a,b} * T_{c,d} &= T_{1,0} \\ \implies T_{ac,ad+b} &= T_{1,0} \end{aligned}$$

So we should take  $c = \frac{1}{a}$  and  $d = \frac{-b}{a}$ . This is well defined since  $a \neq 0$ . Let  $V \in K \implies V = T_{1,d}$  for some  $d \in \mathbb{R}$ . Now Let us compute  $T_{a,b} * V * T_{a,b}^{-1}$ .

$$\begin{aligned} T_{a,b} * V * T_{a,b}^{-1} &= T_{a,b} * T_{1,d} * T_{a,b}^{-1} \\ &= T_{a,ad+b} * T_{\frac{1}{a}, \frac{-b}{a}} \\ &= T_{a, \frac{1}{a}, (ad+b) \cdot \frac{-b}{a}} \\ &= T_{1, \frac{-b(ad+b)}{a}} \end{aligned}$$

Since,  $c \in \mathbb{Q} \implies T_{1, \frac{-b(ad+b)}{a}} \in H$ . Therefore,

$$T_{a,b} * V * T_{a,b}^{-1} \in K$$

## Result

See the proof.

8. a

Suppose that  $G$  is an abelian group under  $*$ . Then, for all  $a, b \in G$ , we have  $a * b = b * a$ . We now show that  $(a * b)^n = a^n * b^n$  for positive integers by induction.

## Step 2

2 of 3

Note: To avoid a bunch of steps where we're just moving around parentheses, I will not show every step involving associativity. All other steps will be shown, though.

Base Step: Let  $n = 1$ . Then it's trivially true that

$$(a * b)^n = a * b = a^n * a^n$$

Inductive Hypothesis: Now suppose that  $(a * b)^n = a^n * b^n$  for some  $n \geq 1$ .

Induction Step: Then

$$\begin{aligned} (a * b)^{n+1} &= (a * b)^n * (a * b) \\ &= a^n * b^n * a * b \\ &\stackrel{(1)}{=} a^n * a * b^n * b \\ &= a^{n+1} * b^{n+1} \end{aligned}$$

where (1) is due to the fact that  $G$  is abelian. Hence, by the principle of mathematical induction,  $(a * b)^n = a^n * b^n$  for all positive integers  $n$ .

If  $n = 0$ , then clearly  $(a * b)^n = e = a^n * b^n$  where  $e$  is the identity element of  $G$ . Now suppose  $n$  is a negative integer. Then

$$(a * b)^n = (a * b)^{-(-n)} = [(a * b)^{-n}]^{-1} \stackrel{(2)}{=} [a^{-n} * b^{-n}]^{-1} \stackrel{(3)}{=} b^{-(-n)} * a^{-(-n)} = b^n * a^n = a^n * b^n$$

where (2) uses the result of the above proof by induction because  $-n$  is a positive integer and (3) uses the result of exercise 15.

Thus we've proven that the result holds for positive integers, 0, and negative integers. Hence  $(a * b)^n = a^n * b^n$  for all integers  $n$ .

## 9. a

Note that by multiplying both sides of  $a^2 = e$  by  $a^{-1}$  we find that  $a = a^{-1}$ . Hence every element of  $G$  is its own inverse.

Let  $a, b \in G$ . Then we see that

$$a * b \stackrel{(1)}{=} (a * b)^{-1} \stackrel{(2)}{=} b^{-1} * a^{-1} \stackrel{(1)}{=} b * a$$

where (1) (both of them) is due to the fact that  $a, b, a * b \in G$  and hence are all equal to their own inverses and (2) uses the result of exercise 15.

## 10. a

We want to find all  $T_{a,b} \in G$  such that  $T_{a,b} * T_{1,x} = T_{1,x} * T_{a,b}$  for all  $x \in \mathbb{R}$ .

From the [Exercise 6](#),

$$T_{a,b} * T_{c,d} = T_{ac,ad+b}.$$

So, for any  $x \in \mathbb{R}$ ,

$$\begin{aligned} T_{a,b} * T_{1,x} &= T_{a,ax+b} \\ T_{1,x} * T_{a,b} &= T_{a,b+x} \end{aligned}$$

We want  $T_{a,ax+b} = T_{a,b+x}$  for any  $x \in \mathbb{R}$ . It is same as

$$ax + b = b + x \iff ax - x = 0 \iff x(a - 1) = 0 \iff a = 1 \text{ or } x = 0.$$

Therefore, for  $x \neq 0$ ,  $\boxed{T_{a,b} * T_{1,x} = T_{1,x} * T_{a,b} \iff a = 1}$ , and they are always same if  $x = 0$ .

## Result

2 of 2

For  $x \neq 0$ ,  $\boxed{T_{a,b} * T_{1,x} = T_{1,x} * T_{a,b} \iff a = 1}$ , and they are always same if  $x = 0$ .

## 11. a

It is non-abelian because  $g * f = f * g^{-1} = f * g^2$ . Since,  $g$  is the rotation of an equilateral triangle (as this is the group of all symmetries of an equilateral triangle) so  $g^2 \neq g$ . Therefore,  $g * f \neq f * g$ .

It has 6 elements that is easy to see, after proving the above two facts. The elements are

$$\{e, f, g, g^2, f * g, g * f = f * g^2\}.$$

## Result

3 of 3

The group has 6 elements and is non-abelian.

## 12. a

First the things that we are given with are

$$\boxed{f^2 = h^n = e \text{ and } fh = h^{-1}f \implies fh^i = h^{-i}f},$$

where  $e$  denotes the identity function. Now we want to compute  $(f^i h^j) *$

$(f^s h^t)$ . Since  $f^2 = e \implies f^i = \begin{cases} f & \text{if } i \text{ is odd} \\ e & \text{if } i \text{ is even.} \end{cases}$

So

$$(f^i h^j) * (f^s h^t) = \begin{cases} h^j * h^t = h^{j+t} & \text{if } i \text{ and } s \text{ are even,} \\ (fh^j) * h^t = fh^{j+t} & \text{if } i \text{ is odd and } s \text{ is even,} \\ h^j * (fh^t) = fh^{-j} * h^t = fh^{t-j} & \text{if } i \text{ is even and } s \text{ is odd,} \\ (fh^j) * (fh^t) = f^2 h^{-j} h^t = h^{t-j} & \text{if } i \text{ and } s \text{ are odd.} \end{cases}$$

It is non-abelian because  $g * f = f * g^{-1} = f * g^3$ . Since,  $g$  is the rotation of a square (as this is the group of all symmetries of a square) so  $g^3 \neq g$ . Therefore,  $g * f \neq f * g$ .

It has 8 elements that is easy to see, after proving the above two facts. The elements are

$$\{e, f, g, g^2, g^3, f * g, g * f = f * g^3, f * g^2 = g^2 * f\}.$$

In the above listed elements, I have written  $f * g^2 = g^2 * f$  because,  $g^2 = g^{-2}$ .

## Result

3 of 3

The group has 8 elements and is non-abelian.

### 13. a

Note: Just to give a name to the result of switching the order in a product we'll say that  $x * y$  and  $y * x$  are the "reverse" of one another for the duration of this exercise.

Case 1: Suppose that  $G$  is a group of order 1. Then  $G$  is trivially abelian.

Case 2: Suppose  $G$  is a group of order 2. Then  $G = \{e, a\}$  where  $e$  is the identity and  $a \neq e$ .  $e * e$  and  $a * a$  are equal to their reverses by symmetry, but also  $a * e = a = e * a$ . Hence all products are equal to their reverses.

Case 3: Suppose  $G$  is a group of order 3. Then  $G = \{e, a, b\}$  where  $e, a, b$  are all distinct. We know that  $e * e$ ,  $a * a$ ,  $b * b$ ,  $e * a$ ,  $a * e$ ,  $e * b$ , and  $b * e$  are clearly equal to their reverses. The ones that're left are  $a * b$  and  $b * a$ . Suppose  $a * b = a$  or  $a * b = b$  then either  $b = e$  or  $a = e$ , respectively. But this contradicts the fact that  $e, a, b$  are all distinct. Hence  $a * b = e$ . But then  $a$  and  $b$  are inverses and hence  $a * b = e = b * a$ . Thus every product is equal to its reverse.

Case 4: Suppose  $G$  is a group of order 4. Then  $G = \{e, a, b, c\}$  where each of those four elements are distinct. First note that  $e$  commutes with everything and hence we really only care about products made from only pairs of the other 3 elements.

Suppose that  $a * b \neq b * a$ . Then clearly  $a * b \neq e, a, b$  for the same reasons as in case 3. So then  $a * b = c$ . But for the same reasons  $b * a$  can't equal  $e, a$ , or  $b$ . So it must equal  $c$ . Hence  $a * b = b * a$ . Contradiction. So  $a * b = b * a$ . Replacing the roles of  $a$  and  $b$  with any other combination of  $a, b$ , and  $c$  shows that all products are equal to their reverses.

Thus we have proven that every group of order 4 or less is abelian.

### 14. a

Suppose  $a, b, c \in G$  such that  $a * b = a * c$ . Let  $e$  denote the identity in  $G$ . Then, because  $G$  is a group,  $a^{-1} \in G$ . We then multiply both sides on the left by  $a^{-1}$ :

$$\begin{aligned} a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c \\ e * b &= e * c \\ b &= c \end{aligned}$$

We therefore see that if  $a * b = a * c$ , then  $b = c$ . Similarly (the proof works nearly exactly the same, but with multiplying  $a^{-1}$  on the right), we find that if  $b * a = c * a$ , then  $b = c$ . Note that if  $a * b = c * a$ , then we can make no conclusions (unless the group happens to be abelian, of course).

### 15. a

**Claim:** Let  $a$  and  $b$  be elements of a group  $G$ . Then

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

**Proof:** We just need to check that  $b^{-1} * a^{-1}$  satisfies the defining condition of the inverse of  $a * b$ :

$$\begin{aligned}(a * b) * (b^{-1} * a^{-1}) &= ((a * b) * b^{-1}) * a^{-1} \\&= (a * (b * b^{-1})) * a^{-1} \\&= (a * e) * a^{-1} \\&= a * a^{-1} \\&= e \\(b^{-1} * a^{-1}) * (a * b) &= b^{-1} * (a^{-1} * (a * b)) \\&= b^{-1} * ((a^{-1} * a) * b) \\&= b^{-1} * (e * b) \\&= b^{-1} * b \\&= e\end{aligned}$$

Hence  $(a * b)^{-1} = b^{-1} * a^{-1}$ , as desired.

## 16. a

Let  $a, b \in G$ . Then we see that

$$a * b \stackrel{(1)}{=} (a * b)^{-1} \stackrel{(2)}{=} b^{-1} * a^{-1} \stackrel{(1)}{=} b * a$$

where (1) (both of them) is due to the fact that  $a, b, a * b \in G$  and hence are all equal to their own inverses and (2) uses the result of exercise 15.

## 17. a

We know that the inverse of  $a$  is the element  $a^{-1}$  which satisfies

$$a * a^{-1} = e = a^{-1} * a \tag{1}$$

So the inverse of  $a^{-1}$  must be the element  $(a^{-1})^{-1}$  which satisfies

$$(a^{-1})^{-1} * a^{-1} = e = a^{-1} * (a^{-1})^{-1} \tag{2}$$

Comparing equations (1) and (2), we immediately see that  $a = (a^{-1})^{-1}$ .

## 18. a

First note that  $a = a^{-1}$  is the same as saying  $a^2 = e$ , where  $e$  is the identity. I.e. the statement is that there exists at least one element of order 2 in  $G$ .

Every element  $a$  of  $G$  of order at least 3 has an inverse  $a^{-1}$  that is not itself -- that is,  $a \neq a^{-1}$ . So the subset of all such elements has an even cardinality (/size). There's exactly one element with order 1: the identity  $e^1 = e$ . So  $G$  contains an even number of elements -- call it  $2k$  -- of which an even number are elements of order 3 or above -- call that  $2n$  where  $n < k$  -- and exactly one element of order 1. Hence the number of elements of order 2 is

$$2k - 2n - 1 = 2(k - n) - 1$$

This cannot equal 0 as  $2(k - n)$  is even and 1 is odd. Hence there's at least one element of order 2 in  $G$ , which concludes the proof.

## 19. a

Let  $\phi$  denote the permutation  $(1\ 2)$ , i.e. permutation of first and second elements and  $\psi$  denote the permutation  $(1\ 2\ 3)$  cyclic permutation of first, second and third elements. Elements of  $S_3$  are

$$S_3 = \{e, \phi, \psi, \psi^2, \phi\psi, \phi\psi^2\}$$

It is clear that elements  $e, \psi, \psi^2$  form subgroup of  $S_3$  of order 3 and all elements satisfy  $x^3 = e$ . Also  $\phi^2 = e$ . We need to show that elements  $\phi\psi$  and  $\phi\psi^2$  have order two. Now,

$$\begin{aligned} (\phi\psi)^2 &= (\phi\psi)(\phi\psi) \\ &= \phi(\psi\phi)\psi \\ &= \phi(\phi\psi^2)\psi \\ &= \phi^2\psi^3 \\ &= e \end{aligned}$$

Now again,

$$\begin{aligned} (\phi\psi^2)^2 &= (\phi\psi^2)(\phi\psi^2) \\ &= \phi(\psi^2\phi)\psi^2 \\ &= \phi(\phi\psi)\psi^2 \\ &= \phi^2\psi^3 \\ &= e \end{aligned}$$

Therefore elements  $e, \phi, \phi\psi, \phi\psi^2$  have order 2. These elements represents the transposition of two elements  $(1\ 2), (2\ 3)$ , and  $(1\ 3)$ .

## 20. a

**Elements of  $S_4$  satisfying  $x^4 = e$ .**

$S_4$  is the group of all permutations of the set  $\{1, 2, 3, 4\}$ . There are 24 elements including identity in  $S_4$ . Let us consider  $x \in S_4$  such that

$$x^4 = e, \text{ } e \text{ being the identity element of } S_4.$$

**Then order of  $x$  will divide 4. Then the possible order of  $x$  are 1 or 2 or 4.**

There is only one element of order 1, the identity element.

The order 2 elements in  $S_4$  are all transpositions and elements like  $\sigma_1\sigma_2$  where  $\sigma_1$  and  $\sigma_2$  are disjoint transpositions.

And the 4 order elements in  $S_4$  are the 4 cycles. There are precisely 6 elements in  $S_4$  whose order is 4. That is, all the four cycles in  $S_4$  are

$$(1, 2, 3, 4), (1, 2, 4, 3), (1, 3, 2, 4), (1, 3, 4, 2), (1, 4, 2, 3), (1, 4, 3, 2).$$

Let us now consider the sets below as:

$$H_1 := \{(a, b) \mid a, b \in \{1, 2, 3, 4\} \text{ and } a \neq b\}$$

$$H_2 := \{(a, b)(c, d) \mid a, b, c, d \in \{1, 2, 3, 4\} \text{ and } a \neq b \neq c \neq d\}$$

$$H_3 := \{(1, 2, 3, 4), (1, 2, 4, 3), (1, 3, 2, 4), (1, 3, 4, 2), (1, 4, 2, 3), (1, 4, 3, 2)\}.$$

**Then the elements of  $S_4$  satisfying  $x^4 = e$  are precisely the set**

$$A = \{e\} \cup H_1 \cup H_2 \cup H_3.$$

The elements of  $S_4$  satisfying  $x^4 = e$  are precisely the identity element, the transpositions, product of disjoint transpositions and order 4 elements. Click for the complete proof.

## 21. a

Suppose  $G$  is a group of order 5 which is not abelian. Then there exist two non-identity elements  $a, b \in G$  such that  $a * b \neq b * a$ . Further we see that  $G$  must equal  $\{e, a, b, a * b, b * a\}$ . To see why  $a * b$  must be distinct from all the others, note that if  $a * b = e$ , then  $a$  and  $b$  are inverses and hence  $a * b = b * a$ . Contradiction. If  $a * b = a$  (or  $= b$ ), then  $b = e$  (or  $a = e$ ) and  $e$  commutes with everything. Contradiction. We know by supposition that  $a * b \neq b * a$ . Hence all the elements  $\{e, a, b, a * b, b * a\}$  are distinct.

Now consider  $a^2$ . It can't equal  $a$  as then  $a = e$  and it can't equal  $a * b$  or  $b * a$  as then  $b = a$ . Hence either  $a^2 = e$  or  $a^2 = b$ .

Now consider  $a * b * a$ . It can't equal  $a$  as then  $b * a = e$  and hence  $a * b = b * a$ . Similarly it can't equal  $b$ . It also can't equal  $a * b$  or  $b * a$  as then  $a = e$ . Hence  $a * b * a = e$ .

So then we additionally see that  $a^2 \neq e$  because then  $a^2 = e = a * b * a$  and consequently  $a = b * a$  (and hence  $b = e$ ). So  $a^2 = b$ . But then  $a * b = a * a^2 = a^2 * a = b * a$ . Contradiction.

Hence starting with the assumption that there exists an order 5 abelian group  $G$  leads to a contradiction. Thus there is no such group.

## 22. a

Applying a reflection twice gives us the identity and applying a rotation of  $2\pi/n$  radians  $n$  times also gives us the identity, so  $f^2 = h^n = id$ . We also have that

$$\begin{aligned} fh(x, y) &= f(\cos(2\pi/n)x - \sin(2\pi/n)y, \sin(2\pi/n)x + \cos(2\pi/n)y) \\ &= (-\cos(2\pi/n)x + \sin(2\pi/n)y, \sin(2\pi/n)x + \cos(2\pi/n)y) \\ &= h^{-1}(-x, y) \\ &= h^{-1}f(x, y) \end{aligned}$$

so  $fh = h^{-1}f$ . We can then compute that

$$(f^i h^j) * (f^s h^t) = f^{i+s \bmod 2} h^{(-1)^s j+t \bmod n}$$

The element  $f^0 h^0$  is a unit for this product:

$$\begin{aligned} (f^i h^j) * (f^0 h^0) &= f^{i+0 \bmod 2} h^{(-1)^0 j+0 \bmod n} \\ &= f^i h^j \\ &= f^{0+i \bmod 2} h^{(-1)^i 0+j \bmod n} \\ &= (f^0 h^0) * (f^i h^j) \end{aligned}$$

Associativity is satisfied:

$$\begin{aligned}
 ((f^i h^j) * (f^s h^t)) * (f^u h^v) &= (f^{i+s \bmod 2} h^{(-1)^s j + t \bmod n}) * (f^u h^v) \\
 &= (f^{i+s+u \bmod 2} h^{(-1)^{s+u} j + (-1)^u t + v \bmod n}) \\
 &= (f^i h^j) * (f^{s+u \bmod 2} h^{(-1)^u t + v \bmod n}) \\
 &= (f^i h^j) * ((f^s h^t) * (f^u h^v))
 \end{aligned}$$

and  $f^i h^{(-1)^i j}$  is the inverse of  $f^i h^j$ :

$$\begin{aligned}
 (f^i h^j) * (f^i h^{(-1)^i j}) &= f^{i+i \bmod 2} h^{(-1)^i j + (-1)^i j \bmod n} \\
 &= f^0 h^0 \\
 &= f^{i+i \bmod 2} h^{(-1)^i (-1)^i j + j \bmod n} \\
 &= (f^i h^{(-1)^i j}) * (f^i h^j)
 \end{aligned}$$

Therefore the set forms a group. Since  $fh = h^{-1}f$  and  $n > 2$  we have that this group is not abelian. Since the elements are of the form  $f^i h^j$  with  $i = 0, 1$  and  $j = 0, 1, \dots, n - 1$  we have that this set has at most  $2n$  elements. It could be the case that two expressions  $f^i h^j$  and  $f^s h^t$  represent the same function on  $S$  for distinct pairs  $(i, j)$  and  $(s, t)$ . But note that

$$\begin{aligned}
 f^i h^j &= f^s h^t \\
 (f^i h^j) * (f^s h^{(-1)^s t}) &= f^0 h^0 \\
 f^{i+s \bmod 2} h^{(-1)^s j + (-1)^s t \bmod n} &= f^0 h^0
 \end{aligned}$$

which implies  $i = s$  and  $j = t$ . So indeed this set has  $2n$  elements.

## Result

3 of 3

All properties can be verified using the formula

$$(f^i h^j) * (f^s h^t) = f^{i+s \bmod 2} h^{(-1)^s j + t \bmod n}.$$

## 23. a

From the [Example 6](#),

$$T_{a,b} * T_{c,d} = T_{ac,ad+b}$$

and

$$T_{c,d} * T_{a,b} = T_{ca,cb+d}.$$

We want to find  $T_{c,d}$  such that

$$T_{a,b} * T_{c,d} = T_{c,d} * T_{a,b}.$$

Since,  $a, c \in \mathbb{R} \implies ac = ca$ . We want to find relation between  $a, b, c, d$  such that

$$\begin{aligned}
 ad + b &= cb + d \\
 \implies ad + b - cb - d &= 0 \\
 \implies -b(c-1) + d(a-1) &= 0 \\
 \implies b(c-1) &= d(a-1)
 \end{aligned}$$

Therefore,  $U \in \{T_{c,d} \in G : b(c-1) = d(a-1)\}$ .

## Result

$$U \in \left\{ T_{c,d} \in G : b(c-1) = d(a-1) \right\}.$$

24. a

**Given:**  $G$  is the Dihedral group of order  $2n$ , i.e.  $G = D_{2n}$ .

**To Prove:**

- (1) If  $n$  is odd and  $a \in G$  is such that  $a * b = b * a$  for all  $b \in G$  then  $a = e$ .
- (2) If  $n$  is even show that there is an  $a \in G$ ,  $a \neq e$  such that  $a * b = b * a$  for all  $b \in G$ .
- (3) If  $n$  is even, find all the elements  $a \in G$  such that  $a * b = b * a$  for all  $b \in G$ .

**Proof:** Here we will consider all the cases when  $n > 2$ , otherwise if  $n = 1$  or  $n = 2$  then  $G$  is an **commutative group** and for a particular element  $a \in G$

$$a * b = b * a, \text{ for all } b \in G.$$

So without loss of generality we assume that  $n > 2$ .

By definition, we have

$$D_{2n} = \{f^i h^j : i = 0, 1, j = 0, 1, \dots, n-1\},$$

where

**f is an element of order 2, h is an element of order n and f, h are related by the relation**

$$hf = fh^{-1}.$$

It then follows that

$$h^2 f = hfh^{-1} = fh^{-2}$$

and in general

$$h^r f = fh^{-r}, \text{ for all integers } r \geq 0.$$

**Now, since f and g together generate G(= D<sub>2n</sub>) an element a of G is such that a \* b = b \* a for all b ∈ G**

**If and only If It commutes with both f and h.**

Let us consider an element  $a \in G$  such that

$$a * f = f * a \text{ and } a * h = h * a.$$

Since  $a \in D_{2n}$ , there exist integers  $i$  and  $j$  such that

$$a = f^i h^j.$$

Now,

$$\begin{aligned} a * h &= h * a \implies f^i h^{j+1} = h f^i h^j. \\ &\implies f^i h = h f^i. \end{aligned}$$

Now by the definition of  $D_{2n}$ , either  $i = 0$  or  $i = 1$ .

If  $i = 1$ .

Then,

$$fh = hf \implies fh = fh^{-1} \implies h^2 = e.$$

This is an impossibility, since  $n > 2$ .

Therefore we have  $i = 0$ . Then  $a = h^j$ .

Now,

$$a * f = f * a \implies h^j f = fh^j.$$

But by definition we have

$$h^r f = fh^{-r}, \text{ for all integers } r \geq 0.$$

Hence,

$$h^j f = fh^j \implies fh^{-j} = fh^j \implies h^{2j} = e.$$

Since order of  $h$  is  $n$  and  $h^{2j} = e$ ,  $e$  being the identity element in  $G$ ,

$n$

**divides  $2j$ .**

Therefore, either  $j = 0$  or  $2j = n$ , since  $0 \leq j \leq n - 1$ .

If  $j = 0$  Then  $a = e$ .

And if  $2j = n$ , then  $n$  is **even** and

$$a = h^{2j} = h^{n/2}.$$

(1) Therefore we have proved that if  $n$  is odd then for  $a \in G$  such that  $a * b = b * a$  for all  $b \in G$  implies  $a = e$ ,  $e$  being the identity element of  $G$ .

(2) If  $n$  is even, then consider an element  $a = h^{n/2}$  in  $G$ . Then by the above argument

$$a * b = b * a, \text{ for all } b \in G.$$

(3) Here  $G = D_{2n}$ , where  $n$  is even. Let  $H$  be the set defined by

$$H := \{a \in G \mid a * b = b * a, \text{ for all } b \in G\}.$$

Now the only element in  $G$  satisfies the above condition is  $h^{n/2}$  and the identity element.

Therefore

$$H = \{e, h^{n/2}\}.$$

This completes the proof.

## Result

5 of 5

Considering any element  $a \in G$  we have shown that if  $n$  is odd identity is the only element such that  $e * b = b * e$  for all  $b \in G$ , and if  $n$  is even there exists an element  $a = h^{n/2}$  in  $G$  and this is the only non-identity element in  $G$  satisfying  $a * b = b * a$  for all  $b \in G$ . Click for the complete proof.

25. a

**(a)** Suppose that  $e$  and  $f$  are identity elements of  $G$ . Then  $e = e * f$  because  $f$  is an identity. But also  $e * f = f$  because  $e$  is an identity. Thus, by the transitive property,  $e = f$ . Hence  $e$  is the unique identity of  $G$ .

## Step 2

2 of 2

**(b)** Suppose that  $b$  and  $c$  are both inverses of  $a \in G$ . Then

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

Hence there is only one inverse of  $a$  and we can thus give a special notation for that element: say  $a^{-1}$ .

## 26. a

Because there are only a finite number of elements of  $G$ , it's clear that the set  $\{a, a^2, a^3, \dots\}$  must be a finite set and in particular, there should exist some  $i$  and  $j$  such that  $i \neq j$  and  $a^i = a^j$ . WLOG suppose further that  $i > j$  (just reverse the roles of  $i$  and  $j$  otherwise). Then multiply both sides by  $(a^j)^{-1} = a^{-j}$  to get

$$a^i * a^{-j} = a^{i-j} = e$$

Thus the  $n = i - j$  is a positive integer such that  $a^n = e$ .

## 27. a

Let  $n_1, n_2, \dots, n_k$  be the orders of all  $k$  elements of  $G = \{a_1, a_2, \dots, a_k\}$ . Let  $m = \text{lcm}(n_1, n_2, \dots, n_k)$ . Then, for any  $i = 1, \dots, k$ , there exists an integer  $c$  such that  $m = n_i c$ . Thus

$$a_i^m = a_i^{n_i c} = (a_i^{n_i})^c = e^c = e$$

Hence  $m$  is a positive integer such that  $a^m = e$  for all  $a \in G$ .

## 28. a

From (3) we have there exists element  $e$  such that for every  $x \in G$ ,  $e * x = x$ . From (4), we have there exists element  $y$  such that  $y * x = e$ .

$$y * (x * e) = (y * x) * e = e * e = e = y * x$$

This shows  $x * e = e * x = x$ .

$$x * (y * x) = (x * y) * x = x = e * x$$

This shows  $x * y = y * x = e$ .

## 29. a

To show that  $G$  is a group, we need to show the existence of inverse and identity. Given that for  $a, b, c \in G$

$$a * b = a * c \implies b = c$$

and

$$b * a = c * a \implies b = c$$

Since the group is finite, for any  $y \in G$ , there is unique  $x \in G$  such that  $x * a = y$ . If it were not, then it would contradict the cancellation laws. Choose  $y = a$ , this gives  $x * a = a$ . Let  $x = e$  be that element.

$G$  is finite, then for  $x \in G$ , there exists a  $y \in G$  such that  $y * x = e$ . The set  $G$  satisfies two properties on problem no 28. Therefore  $G$  is a group.

### 30. a

Choose  $G = \mathbb{Z} - \{0\}$  with operation of multiplication  $\times$ . All properties defined on problem no 29 holds but this is not group as all elements except  $\pm 1$  does not have multiplicative inverse.

#### Result

2 of 2

see example

### 31. a

**Given:**  $G$  is a group of all non-zero real numbers under the operation  $*$ , that is, under multiplication and  $H$  is a group of all real numbers under  $\#$  which is addition of real numbers.

**To Prove:**

- (1) Show that there is a mapping  $F : G \rightarrow H$  of  $G$  onto  $H$  which satisfies  $F(a * b) = F(a) \# F(b)$  for all  $a, b \in G$ .
- (2) Show that no such mapping can be 1 – 1.

**Proof:** By the given condition

$$(G, *) := (\mathbb{R} \setminus \{0\}, \cdot) \text{ and } (H, \#) := (\mathbb{R}, +).$$

- (1) Let us consider the mapping  $F : G \rightarrow H$  given by

$$F(g) := 0, \text{ for all } g \in G.$$

Then clearly for any  $a, b \in G$  we have

$$F(a * b) = F(a) \# F(b).$$

(2) If possible let us assume that, there exists a mapping  $F : G \rightarrow H$  with  $F(a * b) = F(a) \# F(b)$  for all  $a, b \in G$  such that  $F$  is 1 – 1.

**Without loss of generality loss us consider  $a = 1$  and  $b = -1$ .**

Then,

$$F(a * b) = F(a) \# F(b) \implies F(-1) = F(-1) + F(1) \implies F(1) = 0.$$

Again let  $a = b = -1$ . Then,

$$\begin{aligned} F(a * b) &= F(a) \# F(b) \implies F(1) = F(-1) + F(-1) \\ &\implies 2F(-1) = 0 \\ &\implies F(-1) = 0. \end{aligned}$$

Hence we have

$$F(1) = F(-1) = 0.$$

Since  $F$  is

**Injective, It follows that  $1 = -1$ , which is an impossibility.**

So, assumption that "there exists a mapping  $F : G \rightarrow H$  with  $F(a * b) = F(a) \# F(b)$  for all  $a, b \in G$  such that  $F$  is 1 – 1" is wrong. **Therefore there cannot exist such map.**

This completes the proof.

## Result

3 of 3

For (1) consider the zero map, and for the (2) one consider the image of 1 and  $-1$  under such map  $F$  is  $F$  is 1 – 1. Click for the detailed proof.

## Section 2–2

### 1. a

Choose  $y = a$  in (1) and  $w = a$  in (2). This gives  $ax = a$  and  $ua = a$ . We need to show that  $x = u$ . Again choose  $a = u$  in (1) and  $a = x$  in (2). This gives  $ux = u$  and  $ux = x$ . This shows  $u = x$ . Let this element by  $e$ , the identity element.

Choose  $y = e$  in (1) and  $w = e$  in (2), we get  $ax = e$  and  $ua = e$ . We need to show  $x = u$ .

$$u(ax) = ue = u$$

also

$$u(ax) = (ua)x = ex = x$$

This shows the existence of inverse.

### 2. a

Let consider an arbitrary element  $a \in G$ , using the given condition we can prove that for an arbitrary element  $b \in G$  there are  $x, y \in G$  such that

$$ax = b \quad \text{and} \quad ya = b$$

This result follows from the fact that sets  $\{ax \mid x \in G\}$  and  $\{ya \mid y \in G\}$  have the same number of elements as  $G$  (

$$au = aw \text{ implies } u = w, \text{ and } ca = da \text{ implies } c = d$$

).

From the result above, we obtain that there are  $e_1, e_2 \in G$  such that

$$ae_1 = a \tag{1}$$

$$e_2a = a \tag{2}$$

and for an arbitrary  $b \in G$  there are  $c, d \in G$  such that

$$ac = b \tag{3}$$

$$da = b \tag{4}$$

Further, we are proving that  $e_2 = e_1$  and  $be_1 = e_1b = b$ :

$$be_1 \stackrel{(4)}{=} (da)e_1 = d(ae_1) = da \stackrel{(4)}{=} b \tag{5}$$

$$e_2b \stackrel{(3)}{=} e_2(ac) = (e_2a)c = ac \stackrel{(3)}{=} b \tag{6}$$

Substituting  $b = e_2$  in (5) and (6) we obtain that  $e_2e_1 = e_2e_2$  and from the given conditions

$$e_1 = e_2$$

Therefore, there is the identity element  $e = e_2 = e_1$  in  $G$ . If we prove that each element in  $G$  has inverse element, then we have that  $G$  is a group.

For an arbitrary  $b \in G$  there are  $b', b'' \in G$  such that  $b'b = e = bb''$ .

Further, from

$$bb'' = e \Rightarrow b'(bb'') = b'e \Rightarrow (b'b)b'' = b' \Rightarrow eb'' = b' \Rightarrow b'' = b'$$

Hence, we obtain that  $b^{-1} = b'' = b'$  and from the fact that  $b$  is an arbitrary element we obtain that  $G$  is group.

## Result

3 of 3

(HINT:) Consider the sets  $\{ax \mid x \in G\}$  and  $\{ya \mid y \in G\}$  to prove that for an arbitrary element  $b \in G$  there are  $x, y \in G$  such that

$$ax = b \quad \text{and} \quad ya = b$$

3. a

Let  $G$  be a group,  $a, b \in G$  and  $i$  be any integer. Then from given condition,

$$\begin{aligned}(ab)^i &= a^i b^i \\ (ab)^{i+1} &= a^{i+1} b^{i+1} \\ (ab)^{i+2} &= a^{i+2} b^{i+2}\end{aligned}$$

From first and second, we get

$$a^{i+1} b^{i+1} = (ab)^i (ab) = a^i b^i ab \implies b^i a = ab^i$$

From first and third, we get

$$a^{i+2} b^{i+2} = (ab)^i (ab)^2 = a^i b^i ab ab \implies a^2 b^{i+1} = b^i aba$$

This gives

$$a^2 b^{i+1} = a(ab^i)b = ab^i ab = b^i a^2 b$$

Finally, we get

$$b^i aba = b^i a^2 b \implies ba = ab$$

This shows that  $G$  is Abelian.

#### 4. a

**Given:**  $G$  is a group such that

$$(ab)^i = a^i b^i$$

holds for two consecutive integers  $i$ .

Now we need to find a non-abelian group in which this holds.

Let us consider the group  $Q_8$ , the **Quaternion group**.

Then

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

where  $i^2 = j^2 = k^2 = -1$  and  $ij = k, jk = i, ji = -k, ik = j, ki = -j, kj = -i$ .

In  $Q_8$  notice that

$$(a.b)^i = a^i \cdot b^i \text{ holds for } i = 4, 5.$$

But  $Q_8$  is **non-Abelian**, since  $ij \neq ji$ .

Hence we are done.

#### Result

2 of 2

Take the group  $Q_8$  and consider all its elements and look that  $(a.b)^i = a^i \cdot b^i$  for  $i = 4, 5$  but group itself is non-abelian. Click for the result.

#### 5. a

**Given:**  $G$  be a group such that

$$(ab)^3 = a^3 b^3 \text{ and } (ab)^5 = a^5 b^5, \text{ for all } a, b \in G.$$

**To Prove:**  $G$  is an abelian group.

**Proof:** We have

$$\begin{aligned}
 (ab)^3 &= a^3b^3, \text{ for all } a, b \in G \\
 \implies (ab)(ab)(ab) &= a(a^2b^2)b \\
 \implies a(ba)(ba)b &= a(a^2b^2)b \\
 \implies (ba)^2 &= a^2b^2, \text{ by cancellation law.}
 \end{aligned}$$

Again,

$$\begin{aligned}
 (ab)^5 &= a^5b^5, \text{ for all } a, b \in G \\
 \implies (ab)(ab)(ab)(ab)(ab) &= a(a^4b^4)b \\
 \implies a(ba)(ba)(ba)(ba)b &= a(a^4b^4)b \\
 \implies (ba)^4 &= a^4b^4, \text{ by cancellation law.}
 \end{aligned}$$

Now by combining two cases we have

$$\begin{aligned}
 (ba)^4 &= a^4b^4 \\
 \implies ((ba)^2)^2 &= a^2(a^2b^2)b^2 \\
 \implies (a^2b^2)^2 &= a^2(a^2b^2)b^2 \\
 \implies (a^2b^2)(a^2b^2) &= a^2(a^2b^2)b^2 \\
 \implies a^2(b^2a^2)b^2 &= a^2(a^2b^2)b^2 \\
 \implies b^2a^2 &= a^2b^2, \text{ by cancellation law.} \\
 \implies b^2a^2 &= (ba)^2, \text{ since } (ba)^2 = a^2b^2 \\
 \implies b(ba)a &= (ba)(ba) \\
 \implies b(ba)a &= b(ab)a \\
 \implies ba &= ab, \text{ by cancellation law.}
 \end{aligned}$$

This follows that,  $ab = ba$  for all  $a, b \in G$ . Hence  $G$  is abelian.

## Result

3 of 3

Simplifying  $(ab)^3 = a^3b^3$  and  $(ab)^5 = a^5b^5$  and by left and right cancellation law we have proved that  $ab = ba$  for all  $a, b \in G$ , follows that  $G$  is abelian.

Click for the complete proof.

6. a

**Given:**  $G$  is a group in which  $(ab)^n = a^n b^n$  for some fixed integers  $n > 1$  for all  $a, b \in G$ .

**To Prove:** For all  $a, b \in G$ ,

$$(1) (ab)^{n-1} = b^{n-1}a^{n-1}.$$

$$(2) a^n b^{n-1} = b^{n-1} a^n.$$

$$(3) (aba^{-1}b^{-1})^{n(n-1)} = e.$$

**Proof:**

(1) By the given condition for all  $a, b \in G$

$$(ba)^n = b^n a^n, \text{ for some fixed integers } n > 1.$$

Then,

$$\begin{aligned} (ba)^n = b^n a^n &\implies b.(ab)(ab)\dots(ab).a = b(b^{n-1}a^{n-1})a, \text{ where } (ab) \text{ occurs } n-1 \text{ times} \\ &\implies (ab)^{n-1} = b^{n-1}a^{n-1}, \text{ by cancellation law.} \end{aligned}$$

Hence, for all  $a, b \in G$

$$(ab)^{n-1} = b^{n-1}a^{n-1}.$$

(2) By the given condition for all  $a, b \in G$

$$(ba)^n = b^n a^n, \text{ for some fixed integers } n > 1.$$

Then we have

$$\begin{aligned} (ba)^n &= b^n a^n \\ &\implies b.(ab)(ab)\dots(ab).a = b(b^{n-1}a^{n-1})a, \text{ where } (ab) \text{ occurs } n-1 \text{ times} \\ &\implies (ab)^{n-1} = b^{n-1}a^{n-1}, \text{ by cancellation law} \\ &\implies (ab)^{n-1}(ab) = (b^{n-1}a^{n-1})(ab) \\ &\implies (ab)^n = b^{n-1}a^n \\ &\implies a^n b^n = b^{n-1}a^n b, \text{ given condition} \\ &\implies a^n b^{n-1} = b^{n-1}a^n, \text{ by cancellation law.} \end{aligned}$$

Therefore for all  $a, b \in G$  we have

$$a^n b^{n-1} = b^{n-1} a^n.$$

(3) To prove this we will use above solved problems (1) and (2). So for all  $a, b \in G$  we have

$$(ab)^{n-1} = b^{n-1}a^{n-1} \tag{1}$$

$$a^n b^{n-1} = b^{n-1} a^n \tag{2}$$

In order to show that

$$(aba^{-1}b^{-1})^{n(n-1)} = e, \text{ for all } a, b \in G$$

it is enough to show that

$$(ab)^{n(n-1)} = (ba)^{n(n-1)}, \quad \forall x, y \in G.$$

This is because of

$$\begin{aligned}
 (ab)^{n(n-1)} &= (ba)^{n(n-1)} \implies (ba)^{-1})^{n(n-1)}(ab)^{n(n-1)} = e \\
 &\implies (a^{-1}b^{-1})^{n(n-1)}(ab)^{n(n-1)} = e \\
 &\implies ((a^{-1}b^{-1})^n)^{n-1}((ab)^n)(n-1) = e \\
 &\implies ((ab)^n(a^{-1}b^{-1})^n)^{n-1} = e, \text{ by (1)} \\
 &\implies (aba^{-1}b^{-1})^{n(n-1)} = e, \text{ ( given condition).}
 \end{aligned}$$

**Now, It suffices to show that**

$$(ab)^{n(n-1)} = (ba)^{n(n-1)}, \forall x, y \in G.$$

Now, we have

$$\begin{aligned}
 (ab)^{n(n-1)} &= (a^n b^n)^{n-1}, \text{ by the given condition} \\
 &= (a^n b^{n-1} b)^{n-1} \\
 &= (b^{n-1} a^n b)^{n-1}, \text{ by (2)} \\
 &= (a^n b)^{n-1} (b^{n-1})^{n-1}, \text{ by (1)} \\
 &= b^{n-1} (a^n)^{n-1} (b^{n-1})^{n-1}, \text{ by (1)} \\
 &= (b^{n-1} (a^{n-1})^n) (b^{n-1})^{n-1} \\
 &= (a^{n-1})^n b^{n-1} (b^{n-1})^{n-1}, \text{ by (2)} \\
 &= (a^{n-1})^n (b^{n-1})^n \\
 &= (a^{n-1} b^{n-1})^n, \text{ by (1)} \\
 &= (ba)^{n(n-1)}, \text{ by (1).}
 \end{aligned}$$

This completes our proof.

## Result

4 of 4

We have proved (1) by simply expanding the given condition that  $(ab)^n = a^n b^n$  for some fixed integers  $n > 1$  for all  $a, b \in G$ , and by using (1) we have proved (2) and lastly we have used all three conditions to prove (3).

Click for the complete proof.

## Section 2–3

1. a

**Given:**  $G$  is a group and  $A, B$  are two subgroups of  $G$ .

**To Prove:**  $A \cap B$  is a subgroup of  $G$ .

**Proof:**  $A \cap B$  is a non-empty subset of  $G$  since  $e$  belongs to both  $A$  and  $B$ ,  $e$  being the identity element.

Let  $a, b \in A \cap B$ .

Then,

$$a, b \in A \text{ and } a, b \in B.$$

Since  $A$  is a subgroup,

$$a, b \in A \implies ab^{-1} \in A.$$

Since  $B$  is a subgroup,

$$a, b \in B \implies ab^{-1} \in B.$$

Therefore

$$a \in A \cap B, b \in A \cap B \implies ab^{-1} \in A \cap B$$

and this proves that  $A \cap B$  is a subgroup of  $G$ .

## Result

3 of 3

Considering any two elements  $a, b$  in  $A \cap B$ , we have shown that  $ab^{-1} \in A \cap B$ , followed that  $A \cap B$  is a subgroup of  $G$ .

Click for the detailed proof.

## 2. a

Note that  $\mathbb{Z}$  is an infinite cyclic group. We claim that, if  $H$  is a cyclic subgroup of  $\mathbb{Z}$  generated by  $-1$ , then  $H = \mathbb{Z}$ .

**Proof of the claim:** Let  $x$  be an arbitrary element of  $\mathbb{Z}$ .

Then,

$$m = 1 \cdot m = (-1) \cdot (-m) = (-1) \cdot m_1, \text{ where } m_1 \in \mathbb{Z}.$$

So,  $m$  can be expressed as  $(-1) \cdot m_1$  for some integer  $m_1$ . Since  $m$  is an arbitrary element of  $\mathbb{Z}$ , it follows that

$$\mathbb{Z} = \langle -1 \rangle = H.$$

therefore we are done.

## Result

2 of 2

The cyclic subgroup of  $\mathbb{Z}$  generated by  $-1$  is  $\mathbb{Z}$  itself. Click for the complete solution.

## 3. a

### All the subgroups of $S_3$

The elements of the group  $S_3$  are given by

$$\rho_0 = id, \rho_1 = (1, 2, 3), \rho_2 = (1, 3, 2), \rho_3 = (2, 3), \rho_4 = (1, 3), \rho_5 = (1, 2).$$

now,

$$\langle \rho_0 \rangle = \{\rho_0\}$$

$$\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}, \text{ since } \rho_1^2 = \rho_2, \rho_1^3 = \rho_0;$$

$$\langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}, \text{ since } \rho_2^2 = \rho_1, \rho_2^3 = \rho_0;$$

$$\langle \rho_3 \rangle = \{\rho_0, \rho_3\}, \text{ since } \rho_3^2 = \rho_0;$$

$$\langle \rho_4 \rangle = \{\rho_0, \rho_4\}, \text{ since } \rho_4^2 = \rho_0;$$

$$\langle \rho_5 \rangle = \{\rho_0, \rho_5\}, \text{ since } \rho_5^2 = \rho_0.$$

Hence all the subgroups of  $S_3$  are precisely

$$\langle \rho_0 \rangle, \langle \rho_1 \rangle, \langle \rho_2 \rangle, \langle \rho_3 \rangle, \langle \rho_4 \rangle, \langle \rho_5 \rangle \text{ and } S_3.$$

**Result**

2 of 2

All the subgroups of  $S_3$  are precisely the cyclic subgroups generated by each element and  $S_3$  itself. Click for the complete solution.

**4. a**

**To Prove:**  $Z(G)$  is a subgroup of the group  $G$ .

**Proof:** The centre

$$Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}$$

is a **non-empty subset** of  $G$ , since  $e \in Z(G)$ ,  $e$  being the **identity element**.

Let  $p, q \in Z(G)$ .

Then,

$$pg = gp, \quad qg = gq \text{ for all } g \in G.$$

Now,

$$(pq)g = p(qg) = (pg)q = (gp)q = g(pq), \text{ for all } g \text{ in } G.$$

This shows that  $pq \in Z(G)$ .

Therefore,

$$p \in Z(G), q \in Z(G) \implies pq \in Z(G).$$

Let  $p \in Z(G)$ . Then

$$pg = gp \text{ for all } g \text{ in } G.$$

Hence,

$$gp^{-1} = p^{-1}(pg)p^{-1} = p^{-1}(gp)p^{-1} = p^{-1}g, \text{ for all } g \text{ in } G.$$

This shows that  $p^{-1} \in Z(G)$ .

Therefore,

$$p \in Z(G) \implies p^{-1} \in Z(G).$$

Consequently  $Z(G)$  is a subgroup of  $G$ .

This completes the proof.

**Result**

2 of 2

Considering elements  $p, q \in Z(G)$  we have shown that  $pq \in Z(G)$  and  $p^{-1} \in Z(G)$ , follows that  $Z(G)$  is a subgroup of  $G$ .

Click for the proof.

**5. a**

**Given:**  $G$  is a group and  $C(a)$  is the centralizer of  $a$  in  $G$ .

**To Prove:**  $Z(G) = \cap_{a \in G} C(a)$ .

**Proof:** Let us take  $x \in Z(G)$ .

Then

$$xg = gx, \text{ for all } g \in G.$$

Then clearly,

$$\begin{aligned} & xa = ax, \text{ for all } a \in G. \\ \implies & x \in C(a), \text{ for all } a \in G. \\ \implies & x \in \cap_{a \in G} C(a) \\ \implies & Z(G) \subset \cap_{a \in G} C(a). \end{aligned}$$

Now, let us take  $y \in \cap_{a \in G} C(a)$ . Then,

$$\begin{aligned} & y \in C(a), \text{ for all } a \in G \\ \implies & ay = ya, \text{ for all } a \in G \\ \implies & y \in Z(G), \text{ by definition of } Z(G) \\ \implies & \cap_{a \in G} C(a) \subset Z(G). \end{aligned}$$

Consequently,  $Z(G) = \cap_{a \in G} C(a)$ .

This completes the proof.

## Result

2 of

Considering an element in  $Z(G)$  we have showed that the element belongs to  $\cap_{a \in G} C(a)$  and vice versa.

[Click for the complete proof.](#)

## 6. a

**To Prove:**  $G$  is a group then for an element  $a$  in  $G$

$$a \in Z(G) \text{ if and only if } C(a) = G.$$

**Proof:** The subgroup

$$Z(G) := \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

is the **centre** of  $G$ .

Let  $a \in Z(G)$ . Then

$$ax = xa \text{ for all } x \in G.$$

This follows that

$$x \in C(a) \text{ for all } x \in G >$$

Hence,  $G \subset C(a) \implies G = C(a)$ .

Conversely, let  $C(a) = G$ .

Then

$$ax = xa \text{ for all } x \in G$$

This implies  $a \in Z(G)$ .

Hence we conclude that

$$a \in Z(G) \text{ if and only if } C(a) = G.$$

This completes the proof.

## Result

3 of 3

Considering any element in  $G$  we show that its already in  $C(a)$  and then considering  $G = C(a)$  we have proved that  $a \in Z(G)$ .

Click for the complete proof.

## 7. a

$$C(a) \text{ for each } a \in S_3.$$

Let us arrange the elements of  $S_3$  as:

$$\rho_0 = id, \rho_1 = (2\ 3), \rho_2 = (1\ 2), \rho_3 = (1\ 2\ 3), \rho_4 = (1\ 3\ 2), \rho_5 = (1\ 3).$$

Now the composition table:

## Step 2

2 of 3

$S_3$	$\rho_0$	$\rho_1$	$\rho_2$	$\rho_3$	$\rho_4$	$\rho_5$
$\rho_0$	$\rho_0$	$\rho_1$	$\rho_2$	$\rho_3$	$\rho_4$	$\rho_5$
$\rho_1$	$\rho_1$	$\rho_0$	$\rho_4$	$\rho_5$	$\rho_2$	$\rho_3$
$\rho_2$	$\rho_2$	$\rho_3$	$\rho_0$	$\rho_1$	$\rho_5$	$\rho_4$
$\rho_3$	$\rho_3$	$\rho_2$	$\rho_5$	$\rho_4$	$\rho_0$	$\rho_1$
$\rho_4$	$\rho_4$	$\rho_5$	$\rho_1$	$\rho_0$	$\rho_3$	$\rho_2$
$\rho_5$	$\rho_5$	$\rho_4$	$\rho_3$	$\rho_2$	$\rho_1$	$\rho_0$

Now form the above table it follows that,

$$C(\rho_0) = S_3, C(\rho_1) = \{\rho_0, \rho_1\}, C(\rho_2) = \{\rho_0, \rho_2\}, C(\rho_3) = \{\rho_0, \rho_3, \rho_4\}, C(\rho_4) = \{\rho_0, \rho_4, \rho_3\}, C(\rho_5) = \{\rho_0, \rho_5\},$$

Result:  $C(\rho_0) = S_3, C(\rho_1) = \{\rho_0, \rho_1\}, C(\rho_2) = \{\rho_0, \rho_2\}, C(\rho_3) = \{\rho_0, \rho_3, \rho_4\}, C(\rho_4) = \{\rho_0, \rho_4, \rho_3\}, C(\rho_5) = \{\rho_0, \rho_5\}$ , where  $\rho_0 = id, \rho_1 = (2\ 3), \rho_2 = (1\ 2), \rho_3 = (1\ 2\ 3), \rho_4 = (1\ 3\ 2), \rho_5 = (1\ 3)$ .

Click for the complete solution.

## 8. a

3 of

**Given:**  $G$  is an abelian group and  $H$  is a subset of  $G$  defined by

$$H := \{a \in G \mid a^2 = e\}.$$

**To Prove:**  $H$  is a subgroup of  $G$ .

**Proof:**

Clearly  $H$  is a non-empty subset of  $G$ , since  $e^2 = e \implies e \in H$ .

Let,  $x, y \in H$ .

Then,

$$x^2 = e \text{ and } y^2 = e.$$

Since  $G$  is abelian we have

$$xy = yx.$$

Now,

$$(xy)^2 = (xy)(xy) = x(yx)y = x(xy)y = x^2y^2 = e \cdot e = e.$$

This implies,

$$\text{for } x, y \in H \implies xy \in H.$$

Now,

$$(x^{-1})^2 = (x^2)^{-1} = e^{-1} = e.$$

This implies,

$$\text{for } x \in H \implies x^{-1} \in H.$$

Consequently,  $H$  is a subgroup of  $G$ .

This completes the proof.

## Result

3 of 3

Considering the elements  $x, y$  in  $H$  we have proved that  $xy$  and  $x^{-1}$  in  $H$  by using abelian property of  $G$ , follows that  $H$  is a subgroup of  $G$ .

[Click for the detailed proof.](#)

9. a

**Given:**  $G$  is a group and define a subset  $H$  of  $G$  by

$$H := \{a \in G \mid a^2 = e\}.$$

We need to find a non-abelian group such that  $H$  cannot be a subgroup of  $G$ .

**Let us now consider the symmetric group of order 3, that is  $S_3$ .**

The elements of the set are

$$\rho_0 = id, \rho_1 = (1, 2, 3), \rho_2 = (1, 3, 2), \rho_3 = (2, 3), \rho_4 = (1, 3), \rho_5 = (1, 2).$$

Now order of the elements are as

$$o(\rho_0) = 1, o(\rho_1) = o(\rho_2) = 3, o(\rho_3) = o(\rho_4) = o(\rho_5) = 2.$$

Then notice that,

**the only elements of  $S_3$  belongs to  $H$  are  $\rho_0, \rho_3, \rho_4, \rho_5$ .**

That is,

$$H := \{\rho_0, \rho_3, \rho_4, \rho_5\}.$$

Now the order of  $H$  is 4 but  $S_3$  is 6, and 4 does not divide 6, hence by **Lagrange's Theorem**,  $H$  is not a subgroup of  $G$ .

This complete the solution.

## Result

2 of 2

Take  $G$  as the symmetric group  $S_3$  and  $H$  as the subset of all elements in  $S_3$  of order 2. Click for the solution.

## 10. a

**Given:**  $G$  is an abelian group, and  $n > 1$  an integer and define a set

$$A_n := \{a^n : a \in G\}.$$

**To Prove:**  $A_n$  is a subgroup of  $G$ .

**Proof:**

$A_n$  is a subset of  $G$  containing all elements like  $a^n$  for  $a \in G$ .

We prove that  $A_n$  is a subgroup of  $G$ .

Let us assume  $G$  is non-trivial group. Then  $A_n$  contains the identity element  $e$ , since

$$e^n = e \in A_n.$$

Let  $p \in A_n$ ,  $q \in A_n$ .

Then

$$p = a^n, q = b^n \text{ for some elements } a, b \in G.$$

Now,

$$pq = a^n b^n = (ab)^n \in A_n, \text{ since } G \text{ is abelian.}$$

Also,

$$p^{-1} = a^{-n} = (a^{-1})^n \in A_n, \text{ since } a^{-1} \in G.$$

Therefore

$$p \in A_n, q \in A_n \implies pq \in A_n$$

and

$$p \in A_n \implies p^{-1} \in A_n.$$

Consequently,  $A_n$  is a subgroup of  $G$ .

This completes the proof.

**Result**

3 of 3

Considering any two elements  $p, q$  in  $A_n$ , we have shown that  $pq$  and  $p^{-1}$  belongs to  $A_n$  implies  $A_n$  is a subgroup of  $G$ .

[Click for the detailed proof.](#)

11. a

**Given:**  $G$  is an abelian group and  $H$  is a subset of  $G$  given by

$$H := \{a \in G \mid a^{n(a)} = e, \text{ for some } n(a) \geq 1 \text{ depending on } a\}.$$

**To Prove:**  $H$  is a subgroup of  $G$ .

**Proof:** Trivially  $H$  is a non-empty subset of  $G$ , since  $e^{n(e)} = e \in H$ ,  $e$  being the identity element in  $G$ .

Let us consider  $p \in H$  and  $q \in H$ .

Then,

$$p^{n(p)} = e \text{ and } q^{n(q)} = e.$$

Let us now assume  $\text{lcm}(n(p), n(q))$  and denoted by  $[n(p), n(q)]$ .

Since,  $n(p)$  and  $n(q)$  both divides  $[n(p), n(q)]$ , we have

$$p^{[n(p), n(q)]} = q^{[n(p), n(q)]} = e.$$

**Since  $G$  is abelian**

$$(pq)^{[n(p), n(q)]} = (p^{[n(p), n(q)]})(q^{[n(p), n(q)]}) = e \cdot e = e.$$

Let us call  $[n(p), n(q)] = n(pq)$ .

Then

$$(pq)^{n(pq)} = e.$$

This follows that

$$p \in H, q \in H \implies pq \in H.$$

Also,

$$(p^{-1})^{n(p)} = (p^{n(p)})^{-1} = e^{-1} = e.$$

And call  $n(p) = n(p^{-1})$ . This follows that

$$p \in H \implies p^{-1} \in H.$$

Hence  $H$  is a subgroup of  $G$ .

This complete the proof.

## Result

2 of 2

Considering two elements in  $H$  we have shown that their inverse and composition are also in  $H$ , which follows that  $H$  is a subgroup of  $G$ . Click for the complete proof.

12. a

**To Prove:** A cyclic group is abelian.

**Proof:** Let  $G$  be a cyclic group and  $a$  be a generator of  $G$ .

We prove that  $G$  is abelian.

Let  $p, q \in G$ .

Then,

$$p = a^r, q = a^s \text{ for some integers } r \text{ and } s.$$

Now,

$$pq = a^r a^s = a^{r+s};$$

$$qp = a^s a^r = a^{s+r}.$$

Since  $r + s = s + r$ , it follows that

$$pq = qp \text{ for all } p, q \in G.$$

Therefore  $G$  is abelian.

This completes the proof.

## Result

2 of 2

Being  $G$  is cyclic and  $a$  is a generator of  $G$  every element of  $G$  can be written as power of  $a$ , and using these we have proved that  $G$  is abelian.

13. a

**To Prove:** Every subgroup of a cyclic group  $G$  is cyclic.

**Proof:** Let  $G$  be a cyclic group generated by  $a$  and let  $H$  be a subgroup of  $G$ . We consider the following cases.

**Case-1:**  $H = G$ .

Clearly,  $H$  is a cyclic group.

**Case-2:**  $H = \{e\}$ .

Since  $e^n = e$  for all  $n \in \mathbb{Z}$ ,

$$H = \{e^n : n \in \mathbb{Z}\}.$$

Therefore  $H$  is the cyclic group  $\langle e \rangle$ .

**Case-3:**  $H$  is a proper subgroup of  $G$  other than the trivial subgroup  $\{e\}$ .

Then there is an element  $x$  in  $H$  such that  $x \neq e$ .

Since  $x \in G$ ,

$$x = a^k \text{ for some integer } k \neq 0.$$

Since  $H$  is a subgroup,  $x^{-1} \in H$  and  $x^{-1} = a^{-k}$ .

So,  $a^k$  and  $a^{-k}$  both belong to  $H$  for some integer  $k \neq 0$ .

Therefore

**there is some positive integral powers of  $a$  in  $H$**

Let  $m$  be the **least positive integer** such that  $a^m \in H$ . Such an  $m$  exists by

**well ordering property of the set  $\mathbb{N}$**

We prove that  $a^m$  is a generator of  $H$ .

Let  $h$  be an element of  $H$ .

Then

$$h = a^p \text{ for some integer } p.$$

By **division algorithm**, there exist integers  $q$  and  $r$  such that

$$p = qm + r, \text{ where } 0 \leq r < m.$$

Since  $H$  is a subgroup,

$$a^m \in H \implies a^{-qm} \in H.$$

Also

$$a^p \in H \text{ and } a^{-qm} \in H \implies a^{p-qm} \in H, \text{ i.e., } a^r \in H.$$

But  $0 \leq r < m$  and  $a^r \in H$  are both satisfied only if  $r = 0$ , because, otherwise  $m$

**fails to be the smallest positive integral power** of  $a$  in  $H$ .

Consequently,  $p = qm$  and therefore  $h = (a^m)^q$  where  $q$  is an integer.

Hence  $H = \langle a^m \rangle$  and the proof is complete.

---

**Result**

3 of 3

Considering a generator of  $G$ , say  $a$  we have proved that  $a^m$  is a generator of the subgroup  $H$  for some  $m$ , by

Division Algorithm.

Click for the detailed proof.

14. a

**Given:**  $G$  is a group such that  $G$  has no proper subgroup.

**To Prove:**  $G$  has no proper subgroup.

**Proof:** There are two cases arise.

**Case-1:**  $G = \{e\}$ ,  $e$  being the identity element in  $G$ .

Then trivially  $G$  is cyclic.

**Case-2:**  $G \neq \{e\}$ .

**Then there exists an non-identity element in  $G$ .**

Let us consider an non-identity element in  $G$ , say  $a (\neq e)$ .

Now look at the cyclic subgroup generated by  $a$ , that is,  $\langle a \rangle$ .

Since

$$a (\neq e) \in G, \langle a \rangle \text{ is a subgroup of } G.$$

If  $G \neq \langle a \rangle$  then  $\langle a \rangle$  is a **proper non-trivial subgroup** of  $G$ , which is an impossibility.

Therefore we must have

$$G = \langle a \rangle.$$

This implies,  $G$  is a cyclic group generated by  $a$ .

This completes the proof.

## Result

2 of 2

Considering a non-identity element  $a$  in  $G$ , we have shown that  $G = \langle a \rangle$ , follows that  $G$  is cyclic. Click for the complete proof.

## 15. a

**Given:**  $G$  is a group and  $H$  is a non-empty subset of  $G$  such that given  $a, b \in H$ , then  $ab^{-1} \in H$ .

**To Prove:**  $H$  is a subgroup of  $G$ .

**Proof:** Let  $H$  be a non-empty subset of  $G$  such that

$$a \in H, b \in H \implies ab^{-1} \in H.$$

Let  $\in H$ . Then

$$a \in H, a \in H \implies aa^{-1} = e \in H.$$

Therefore

**$H$  contains the identity element.**

Now,

$$e \in H, a \in H \implies e(a)^{-1} = a^{-1} \in H, \text{ by the condition.}$$

Hence,  $a \in H$  implies  $a^{-1}$  in  $H$ . Therefore

**the inverse of each element in  $H$  exists in  $H$ .**

Let  $a, b \in H$ . Then  $a \in H$  and  $b^{-1} \in H$ ; and by the given condition

$$a(b^{-1})^{-1} = ab \in H.$$

Hence,

$$a \in H, b \in H \implies ab \in H.$$

Therefore

**$H$  is closed.**

Since  $H$  is non-empty subset of  $G$  and composition is associative on  $G$ , is associative on  $H$ .

Therefore,  $H$  is a group and hence  $H$  is a subgroup of  $G$ .

This completes the proof.

## Result

3 of 3

Being  $H$  is a non-empty subset of  $G$  with  $a, b \in H \implies ab^{-1} \in H$  we have shown that  $H$  contains identity element and the inverse of each element in  $H$  exists in  $H$  and  $H$  is closed, follows that  $H$  is a subgroup.

Click for the detailed proof.

16. a

**Given:**  $G$  is a group such that  $G$  has no proper subgroups.

**To Prove:**  $G$  is a cyclic group of prime order.

**Proof:** There are two cases arise.

**Case-1:**  $G = \{e\}$ ,  $e$  being the identity element in  $G$ .

Then trivially  $G$  is cyclic.

**Case-2:**  $G \neq \{e\}$ .

**Then there exists an non-identity element in  $G$ .**

Let us consider an non-identity element in  $G$ , say  $a (\neq e)$ .

Now look at the cyclic subgroup generated by  $a$ , that is,  $\langle a \rangle$ .

Since

$$a (\neq e) \in G, \langle a \rangle \text{ is a subgroup of } G.$$

If  $G \neq \langle a \rangle$  then  $\langle a \rangle$  is a **proper non-trivial subgroup** of  $G$ , which is an impossibility.

Therefore we must have

$$G = \langle a \rangle.$$

This implies,  $G$  is a cyclic group generated by  $a$ .

Then

**It follows that every non-identity element of  $G$  is a generator of  $G$ .**

**Now we claim that  $G$  is finite.**

**Proof of the claim:** If possible, let  $G$  be an infinite cyclic group that is generated by an element  $a$ .

**We will show that  $a$  and  $a^{-1}$  are the only generators of  $G$ , which will contradict the fact that every non-identity element of  $G$  is a generator of  $G$ .**

Let  $b$  be a generator of the group  $G$ , such that  $b \neq a$ .

Now,  $a \in G$  and  $b$  is a generator of the group  $G$ , so

$$a = b^p, \text{ for some integer } p.$$

Again,  $b \in G$  and  $a$  is a generator of the group  $G$ , so

$$b = a^m, \text{ for some integer } m.$$

So,

$$a = b^p = (a^m)^p.$$

This implies

$$a^{mp-1} = e, \text{ } e \text{ being the identity element of } G.$$

Since  $G = \langle a \rangle$  and  $o(G)$  is infinite,  $o(a)$  is infinite.

Since  $o(a)$  is infinite and  $a^{mp-1} = e$  it follows that

$$mp = 1.$$

So,

$$\text{either } m = 1 \text{ and } p = 1, \text{ or } m = -1 \text{ and } p = -1.$$

Therefore,

$$\text{either } b = a \text{ or } b = a^{-1}.$$

But our hypothesis  $b \neq a$ . So,  $b = a^{-1}$ .

It follows that,  $a$  and  $a^{-1}$  are the only generators of  $G$ .

Now in our case if  $G$  is of infinite order, then

**every element of  $G$  must be a generator,**

but which is an impossibility by our above argument. Hence  $G$  is a group of finite order.

This proves the claim.

Now we assert that order of  $G$  is  $p$ , for some prime  $p$ .

If possible let the order of  $G$  be composite, that is, there exists a positive integer  $d$  other than 1 such that  $d$  divides  $p$ .

**Since  $G$  is cyclic, and  $d$  divides the order of  $G$  then  $G$  must have a subgroup of order  $D$ ,**

which is a contradiction to the fact that,  $G$  has no proper subgroups. So, our assumption that  $p$  is composite is wrong. Hence  $p$  is prime.

Consequently,  $G$  is a cyclic group of order  $p$ , for some prime  $p$ .

This completes the proof.

## Result

4 of 4

First we proved that  $G$  is cyclic and followed by contradiction that  $G$  is a finite cyclic group of order  $p$ , for some prime  $p$ . Click for the complete proof.

## 17. a

**Given:**  $G$  is a group and  $a, x \in G$ .

**To Prove:**  $C(x^{-1}ax) = x^{-1}C(a)x$ .

**Proof:** Note that

$$C(a) := \{x \in G \mid xa = ax\}.$$

Let us assume  $p \in C(x^{-1}ax)$ .

Then,

$$\begin{aligned} p(x^{-1}ax) &= (x^{-1}ax)p \\ \implies (px^{-1}a)x &= x^{-1}(axp) \\ \implies x(px^{-1}a) &= (axp)x^{-1} \\ \implies (xpx^{-1})a &= a(xpx^{-1}) \\ \implies xpx^{-1} &\in C(a). \end{aligned}$$

Therefore,

$$p \in C(x^{-1}ax) \implies xpx^{-1} \in C(a).$$

Thus,

$$C(x^{-1}ax) \subset x^{-1}C(a)x.$$

Let us assume

$$q \in x^{-1}C(a)x.$$

**Then there exists an element**  $y$  in  $C(a)$  such that

$$q = x^{-1}yx.$$

Now,

$$y \in C(a) \implies ya = ay.$$

Also,

$$q(x^{-1}ax) = (x^{-1}yx)(x^{-1}ax) = x^{-1}(ya)x = x^{-1}(ya)x = (x^{-1}yx)(x^{-1}ax) = (x^{-1}yx)q.$$

Therefore,

$$q(x^{-1}ax) = (x^{-1}yx)q.$$

So,

$$q \in C(x^{-1}ax).$$

Consequently we have

$$x^{-1}C(a)x \subset C(x^{-1}ax).$$

It follows from the aforesaid argument

$$C(x^{-1}ax) = x^{-1}C(a)x.$$

This completes the proof.

## Result

3 of

Considering an element  $q$  in  $x^{-1}C(a)x$ , we have proved that  $q \in C(x^{-1}ax)$  and vice-versa. Click for the complete proof.

18. a

Assume that  $X$  is finite.

We need to show that  $T(X)$  is a subgroup of  $A(S)$ .

First, observe that the identity function  $i : S \rightarrow S$  is in  $T(X)$ :

For,  $i(x) = x$  for all  $x \in X$ . Hence,  $i(X) = X$ .

That is, the identity element of  $A(S)$  is in  $T(X)$ .

Let  $f, g \in T(X)$ .

Then, by definition  $f, g \in A(S)$  and  $f(X) \subset X, g(X) \subset X$ .

Let  $x \in X$ . Put  $g(x) = y$ . Then  $y \in X$ .  $fg$  is given by:

$$\begin{aligned} fg(x) &= f(g(x)) \\ &= f(y) \in X. \end{aligned}$$

Thus,  $T(X)$  is closed.

Let  $f$  in  $T(X)$ .

Since  $X$  has finite elements,  $f$  is a 1-1 and onto function from  $X \rightarrow X$ .

Therefore,  $f^{-1}(X) \subset X$ .

Thus,  $T(X)$  is a subgroup of  $A(S)$ .

## 19. a

**Given:**  $A$  and  $B$  are subgroups of an abelian group  $G$ , where  $AB = \{ab : a \in A, b \in B\}$ .

**To Prove:**  $AB$  is a subgroup of  $G$ .

**Proof:** Since  $G$  is an abelian group the we have

$$AB = BA, \text{ for the given subgroups } A \text{ and } B \text{ in } G.$$

Now let  $p$  and  $q$  be two distinct elements in  $AB$ .

Let,

$$p = a_1 b_1 \text{ and } q = a_2 b_2.$$

Then,

$$\begin{aligned} pq &= (a_1 b_1)(a_2 b_2) \\ &= a_1(b_1 a_2)b_2 \\ &= a_1(a_3 b_3)b_2, \text{ since } AB = BA \\ &= (a_1 a_3)(b_3 b_2) \in AB. \end{aligned}$$

Therefore,

$$p, q \in AB \implies pq \in AB.$$

Also,

$$p^{-1} = (a_1 b_1)^{-1} = b_1^{-1} a_1^{-1} \in BA = AB.$$

Therefore,

$$p \in AB \implies p^{-1} \in AB.$$

Consequently,  $AB$  is a subgroup of  $G$ .

This completes the proof.

## Result

3 of 3

Considering  $AB = BA$  since  $G$  is abelian, and using the subgroup criterion we have proved that  $AB$  is a subgroup of  $G$ .

[Click for the detailed proof.](#)

## 20. a

**Given:**  $G$  is a group and  $A, B$  are two subgroups of  $G$ .

We need to show that  $AB$  is not a subgroup of  $G$  by giving a counter-example.

### Step 2

The set  $AB$  is defined by

$$AB = \{ab : a \in A, b \in B\}.$$

For example, let us consider  $G = S_3$ ,  $A = \{(2\ 3), id\}$ , and  $B = \{(1\ 3), id\}$ .

Then,

$$AB = \{(2\ 3)(1\ 3), (1\ 3), (2\ 3), id\} = \{(1\ 2\ 3), (2\ 3), (1\ 3), id\}.$$

Now,

$$(1\ 3)(2\ 3) = (1\ 3\ 2).$$

But  $(1\ 3\ 2) \notin AB$  implies that  $AB$  is not a subgroup of  $G (= S_3)$ .

Considering  $G = S_3$ ,  $A = \{(2\ 3), id\}$ , and  $B = \{(1\ 3), id\}$ . we have shown that  $AB$  is not a subgroup of  $G$

[Click for the detailed solution.](#)

## 21. a

**Given:**  $G$  is a group and  $A, B$  are two subgroups of  $G$  such that

$$b^{-1}Ab \subset A, \text{ for all } b \in B.$$

**To Prove:**  $AB$  is a subgroup of  $G$ .

**Proof:** Let us consider any two elements  $p$  and  $q$  in  $AB$ . Then there exist elements  $a_1, a_2 \in A$  and  $b_1, b_2 \in B$  such that

$$p = a_1b_1 \text{ and } q = a_2b_2.$$

Now,

$$\begin{aligned} pq^{-1} &= (a_1b_1)(a_2b_2)^{-1} \\ &= (a_1b_1)(b_2^{-1}a_2^{-1}) \\ &= a_1(b_1b_2^{-1}a_2^{-1}b_2b_1^{-1})b_1b_2^{-1}. \end{aligned}$$

Since  $b^{-1}Ab \subset A$ , for all  $b \in B$ , we have

$$b_1b_2^{-1}a_2^{-1}b_2b_1^{-1} \in A.$$

Therefore,  $a_1b_1b_2^{-1}a_2^{-1}b_2b_1^{-1} \in A$  and consequently

$$a_1(b_1b_2^{-1}a_2^{-1}b_2b_1^{-1})b_1b_2^{-1} \in AB.$$

Therefore,

$$p, q \in AB \implies pq^{-1} \in AB.$$

Hence,  $AB$  is a subgroup of  $G$ .

This completes the proof.

## Result

Considering  $p$  and  $q$  in  $AB$ , we have proved that  $pq^{-1} \in AB$  by using the hypothesis that  $b^{-1}Ab \subset A$  for all  $b \in B$ . Click for the detailed proof.

## 22. a

**Given:** Let  $A$  and  $B$  are finite subgroups of order  $m$  and  $n$ , of an abelian group  $G$  respectively.

**To Prove:**  $AB$  is a subgroup of order  $mn$  if  $m$  and  $n$  are relatively prime.

**Proof:** Firstly we show that  $AB$  forms a subgroup of the abelian group  $G$ .

Let us consider  $p \in AB, q \in AB$  and  $p = a_1b_1, q = a_2b_2$ , for some  $a_1, a_2 \in A$  and  $b_1, b_2 \in B$ . Then,

$$\begin{aligned} pq &= (a_1b_1)(a_2b_2) \\ &= a_1(b_1a_2)b_2 \\ &= a_1(a_2b_1)b_2, \text{ since } G \text{ is abelian} \\ &= (a_1a_2)(b_1b_2) \in AB. \end{aligned}$$

Therefore,

$$p, q \in AB \implies pq \in AB.$$

Also,

$$p^{-1} = (a_1b_1)^{-1} = (b_1)^{-1}(a_1)^{-1} = (a_1)^{-1}(b_1)^{-1} \in AB.$$

**So,  $AB$  is a subgroup of  $G$ .**

**Now we claim that**  $o(AB) = \frac{m \cdot n}{o(A \cap B)}$

**Proof of the claim:** Let us assume  $o(A \cap B) = p$  and  $A \cap B = \{t_1, t_2, \dots, t_p\}$ . Since  $o(A) = m$  and  $o(B) = n$ , consider

$$A = \{a_1, a_2, \dots, a_m\} \text{ and } B = \{b_1, b_2, \dots, b_n\}.$$

Then,

$$AB := \{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}.$$

**Now the elements  $a_i b_j$  in the list may not be all distinct.**

Let us find how many times an element, say  $a_1 b_1$ , appears in the list.

Let us consider,

$$a_1 b_1 = a_r b_s, \text{ for some } r, s.$$

Then,

$$a_1^{-1} a_r = b_1 b_s^{-1} = t, \text{ say.}$$

Since

$$a_1^{-1} a_r \in A \text{ and } b_1 b_s^{-1} \in B, \text{ so } t \in A \cap B.$$

Now,

$$a_r = a_1 t \text{ and } b_s = b_1 t^{-1}.$$

Thus any  $a_r b_s$  which equals  $a_1 b_1$  is of the form  $(a_1 t)(b_1 t^{-1})$  for some  $t \in A \cap B$ .

Conversely, for any  $t_i \in A \cap B$ , the element  $(a_1 t_i)(b_1 t_i^{-1}) = a_1 b_1$ .

**Thus  $a_1 b_1$  appears in the list  $p$  times.**

Therefore the number of elements in  $AB$  is  $\frac{m.n}{p}$ .

That is,

$$o(AB) = \frac{m.n}{o(A \cap B)}.$$

**This completes the proof of the claim.**

Now by the given condition  $m$  and  $n$  are relatively prime.

Actually we can conclude

$$A \cap B \subset A \text{ and } A \cap B \subset B.$$

**Therefore,  $A \cap B$  is a subgroup of both  $A$  and  $B$  and thence by Lagrange's Theorem**

$$o(A \cap B) \text{ divides both of } o(A) \text{ and } o(B).$$

That is,

$$o(A \cap B) \text{ divides both of } m \text{ and } n.$$

Since  $m$  and  $n$  are relatively prime,

$$o(A \cap B) = 1.$$

Hence,

$$o(AB) = m.n, \text{ when } m \text{ and } n \text{ are relatively prime.}$$

This completes the proof.

## Result

4 of 4

Being  $G$  is abelian  $AB$  is a subgroup, and using  $o(A) = m$  and  $o(B) = n$  we have shown that  $o(AB) = \frac{m.n}{o(A \cap B)}$ , and  $m$  and  $n$  being relatively prime we get that  $o(AB) = m.n$ . Click for the complete proof.

23. a

**Given:** Let  $A$  and  $B$  are finite subgroups of order  $m$  and  $n$ , of an abelian group  $G$  respectively.

**Claim:**  $o(AB) = \frac{m \cdot n}{o(A \cap B)}$ .

**Proof of the claim:** Let us assume  $o(A \cap B) = p$  and  $A \cap B = \{t_1, t_2, \dots, t_p\}$ . Since  $o(A) = m$  and  $o(B) = n$ , consider

$$A = \{a_1, a_2, \dots, a_m\} \text{ and } B = \{b_1, b_2, \dots, b_n\}.$$

Then,

$$AB := \{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}.$$

**Now the elements  $a_i b_j$  in the list may not be all distinct.**

Let us find how many times an element, say  $a_1 b_1$ , appears in the list.

Let us consider,

$$a_1 b_1 = a_r b_s, \text{ for some } r, s.$$

Then,

$$a_1^{-1} a_r = b_1 b_s^{-1} = t, \text{ say.}$$

Since

$$a_1^{-1} a_r \in A \text{ and } b_1 b_s^{-1} \in B, \text{ so } t \in A \cap B.$$

Now,

$$a_r = a_1 t \text{ and } b_s = b_1 t^{-1}.$$

Thus any  $a_r b_s$  which equals  $a_1 b_1$  is of the form  $(a_1 t)(b_1 t^{-1})$  for some  $t \in A \cap B$ .

Conversely, for any  $t_i \in A \cap B$ , the element  $(a_1 t_i)(b_1 t_i^{-1}) = a_1 b_1$ .

**Thus  $a_1 b_1$  appears in the list  $p$  times.**

Therefore the number of elements in  $AB$  is  $\frac{m \cdot n}{p}$ .

That is,

$$o(AB) = \frac{m \cdot n}{o(A \cap B)}.$$

This completes the proof.

## Result

3 of 3

If  $m$  and  $n$  are not relatively prime, then  $o(AB) = \frac{m \cdot n}{o(A \cap B)}$ . Click for the detailed solution.

24. a

**Given:**  $H$  is a subgroup of a group  $G$  and  $N := \cap_{x \in G} x^{-1} H x$ .

**To Prove:**  $N$  is a subgroup of  $G$  such that  $y^{-1} N y = N$  for all  $y \in G$ .

**Proof:** In order to show that  $N$  is a subgroup of  $G$ , it suffices to show that  $x^{-1} H x$  is a subgroup of  $G$  for every  $x \in G$ .

Let us consider two elements  $s, t \in x^{-1} H x$ . Then **there exist elements**  $h_1$  and  $h_2$  in  $H$  such that

$$s = x^{-1} h_1 x \text{ and } t = x^{-1} h_2 x.$$

Now consider  $st^{-1}$ . So,

$$\begin{aligned} st^{-1} &= (x^{-1} h_1 x)(x^{-1} h_2 x)^{-1} \\ &= (x^{-1} h_1 x)(x^{-1} h_2^{-1} x) \\ &= x^{-1} (h_1 h_2^{-1}) x \in x^{-1} H x. \end{aligned}$$

Hence,

$$s, t \in x^{-1} H x \implies st^{-1} \in x^{-1} H x.$$

Therefore,  $x^{-1} H x$  is a subgroup of  $G$ , and since  $x$  is arbitrary  $x^{-1} H x$  is a subgroup of  $G$  for every  $x$  in  $G$ .

**Since intersection of an arbitrary family of subgroups of a group  $G$  is a subgroup of  $G$ ,  $N (= \cap_{x \in G} x^{-1} H x)$  is a subgroup of  $G$ .**

**Now it sufficient to show that, intersection of an arbitrary family of subgroups of a group  $G$  is a subgroup of  $G$ .**

Let  $H_\alpha$  arbitrary be an family of subgroups of  $G$ , where  $\alpha$  belongs to an index set  $I$ . We need to show that  $\cap H_\alpha$  is a **subgroup** of  $G$ .

Clearly  $\cap H_\alpha$  is a

**non-empty subset of  $G$  since the identity element  $e$  belongs to  $H_\alpha$  for every  $\alpha \in I$ .**

Let us now consider  $a, b \in \cap H_\alpha$ . Then

$$a, b \in H_\alpha, \text{ for every } \alpha \in I.$$

Since for each  $\alpha$ ,  $H_\alpha$  is a subgroup of  $G$ ,

$$a, b \in H_\alpha \implies ab^{-1} \in H_\alpha.$$

Therefore,

$$a, b \in \cap H_\alpha \implies ab^{-1} \in \cap H_\alpha.$$

Thence,  $\cap H_\alpha$  is a subgroup of  $G$ . This completes the proof.

Now we show that  $y^{-1}Ny = N$  for every  $y$  in  $G$ .

Let us take  $g \in y^{-1}Ny$ . Then there exists an element  $n$  in  $N$  such that

$$g = y^{-1}ny.$$

Now

$$n \in N \implies n = x^{-1}hx, \text{ for some } h \in H.$$

Then,

$$g = y^{-1}ny = y^{-1}x^{-1}hxy = (xy)^{-1}h(xy).$$

Since this holds for every  $x$  and  $y$  in  $G$ , it follows that

$$g = y^{-1}ny \in N.$$

Hence,

$$y^{-1}Ny \subset N.$$

Let us take an element  $n$  in  $N$ . Now for every  $y \in G$  we can write

$$n = y^{-1}(yny^{-1})y.$$

Since by the above argument  $y^{-1}Ny \subset N$ , it follows that

$$yny^{-1} \in N.$$

This implies,

$$n = y^{-1}(yny^{-1})y \in y^{-1}Ny.$$

Therefore,

$$n \in N \implies n \in y^{-1}Ny.$$

Therefore,

$$N \subset y^{-1}Ny.$$

Consequently,

$$N = y^{-1}Ny.$$

This completes the proof.

## Result

4 o

Being  $H$  is a subgroup of  $G$ ,  $\cap_{x \in G} x^{-1}Hx$  is a subgroup of  $G$ , since intersection of an arbitrary family of subgroups of a group  $G$  is a subgroup of  $G$ , and follows the result. Click for the complete proof.

25. a

Let  $S$  be the set of all integers and let  $X$  be the set of all positive integers.

Let  $f : S \rightarrow S$  be the function defined by:

$$f(x) = x + 1.$$

Then  $f \in A(S)$ .

If  $x \in X$ , then  $x \geq 1$

$$\implies f(x) = x + 1 \geq 2.$$

Thus  $f(x) \in X$ .

Now,  $f^{-1} : S \rightarrow S$  is given by:

$$f^{-1}(x) = x - 1.$$

$$f^{-1}(1) = 1 - 1 = 0 \notin X.$$

But  $1 \in X$ .

$$\implies f^{-1}(X) \not\subset X. \text{ i.e., } f^{-1} \notin T(X).$$

Since  $f^{-1}$  is the unique inverse of  $f$  in  $A(S)$ , this implies that  $f$  does not have an inverse in  $T(X)$ , which is a subset of  $A(S)$ .

Thus,  $T(X)$  is not a group, and hence not a subgroup.

## 26. a

**Given:**  $G$  is a group and  $H$  is a subgroup of  $G$ . Define a set

$$Hx := \{hx \mid h \in H\}.$$

**To Prove:** For  $a, b \in G$ , either  $Ha = Hb$  or  $Ha \cap Hb = \phi$ .

**Proof:** Let us consider the sets  $Ha$  and  $Hb$  in  $G$ . Then either  $Ha \cap Hb = \phi$  or  $Ha \cap Hb \neq \phi$ .

Let  $Ha \cap Hb \neq \phi$  and let  $p \in Ha \cap Hb$ .

Then

$$p \in Ha \text{ and } p \in Hb.$$

Now,

$$p \in Ha \implies p = h_1a \text{ for some } h_1 \in H.$$

$$p \in Hb \implies p = h_2b \text{ for some } h_2 \in H.$$

Hence  $h_1a = h_2b$ . That is,

$$a = h_1^{-1}h_2b \text{ and } b = h_2^{-1}h_1a.$$

Let  $x \in Ha$ .

Then

$$x = h_3a \text{ for some } h_3 \in H.$$

$$= h_3h_1^{-1}h_2b$$

$$= h_4b, \text{ for some } h_4 \in H.$$

Thus  $x \in Ha \implies x \in Hb$  and therefore  $Ha \subset Hb$ .

Let  $y \in Hb$ .

Then

$$\begin{aligned}y &= h_5b \text{ for some } h_5 \text{ in } H. \\&= h_5h_2^{-1}h_1a. \\&= h_6a \text{ for some } h_6 \text{ in } H.\end{aligned}$$

Thus  $y \in Hb \implies y \in Ha$  and therefore  $bH \subset Ha$ .

Consequently,  $Ha = Hb$ .

Therefore, either  $Ha = Hb$  or,  $Ha$  and  $Hb$  are disjoint.

This completes the proof.

## Result

3 of 3

Considering  $Ha$  and  $Hb$  are not disjoint, we have shown that every element of  $Ha$  must coincide with the elements with  $Hb$  and vice versa.

[Click for the complete proof.](#)

27. a

**Given:**  $H$  is a finite subgroup of a group  $G$  and  $Ha$  and  $Hb$  be two cosets of  $H$  in  $G$ .

**To Prove:**  $Ha$  and  $Hb$  have same number of elements.

**Proof:** First we claim that,

**any two cosets of  $h$  in  $G$  have the same cardinality.**

**Proof of the claim:** Let  $Ha$  and  $Hb$  are two cosets of  $H$  in  $G$ . Let us define a mapping  $f : Ha \rightarrow Hb$  by the assignment

$$f(ha) = hb, \text{ for every } h \text{ in } H.$$

**To prove  $f$  is injective, let us take two distinct elements**

$h_1a$  and  $h_2a$  in  $Ha$ . Then,

$$f(h_1a) = h_1b, \quad f(h_2a) = h_2b.$$

Now,

$$\begin{aligned}f(h_1a) &= f(h_2a) \implies h_1b = h_2b \\&\implies h_1 = h_2, \text{ by left cancellation law} \\&\implies h_1a = h_2a.\end{aligned}$$

So,

$$h_1a \neq h_2a \implies f(h_1a) \neq f(h_2a)$$

and this implies  $f$  is injective.

To prove  $f$  is surjective, let us take an element  $hb$  in  $Hb$ .

Then,

$$f(ha) = hb$$

shows that  $ha$  is a pre-image of  $hb$ . Therefore,  $f$  is surjective.

**Consequently,  $f$  is a bijection and therefore  $Ha$  and  $Hb$  have the same cardinality.**

Hence,  $Ha$  and  $Hb$  have the same number of elements.

2 of 3

## Step 2

Now notice that  $H$  **itself is a coset** of  $H$  in  $G$ , since  $H = He$ ,  $e$  being the identity element of  $G$ . Since every cosets of  $H$  in  $G$  have same number of elements and  $H$  is a finite subgroup of  $G$ ,

**every cosets of  $H$  in  $G$  has  $o(H)$  elements, that is, as many elements as  $H$  has.**

3 of 3

## Result

Considering two cosets of  $H$  in  $G$  we have shown that there is a bijection between them, hence having same number of elements and since  $H$  itself is a coset of  $H$  in  $G$ , every cosets of  $H$  in  $G$  has  $o(H)$  elements. Click for the complete proof.

28. a

**Given:**  $M$  and  $N$  are two subgroups of a group  $G$  such that

$$x^{-1}Mx \subset M \text{ and } x^{-1}Nx \subset N \text{ for all } x \in G.$$

**To Prove:**  $MN$  is a subgroup of  $G$  and  $x^{-1}(MN)x \subset MN$ .

**Proof:** First we assert that  $MN$  is a subgroup of  $G$ .

Let us consider two elements

$$x, y \in MN.$$

Then, **there exists**  $m_1, m_2 \in M$  and  $n_1, n_2 \in N$  such that

$$x = m_1n_1 \text{ and } y = m_2n_2.$$

Now

**we need to show that**  $xy^{-1} \in MN$ .

Now,

$$\begin{aligned} xy^{-1} &= m_1 n_1 (m_2 n_2)^{-1} \\ &= m_1 n_1 n_2^{-1} m_2^{-1} \\ &= m_1 m_2^{-1} (m_2 n_1 n_2^{-1} m_2^{-1}). \end{aligned}$$

Since,

$$n_1, n_2 \in N, \text{ then } n_1 n_2^{-1} \in N \text{ and this implies } m_2 n_1 n_2^{-1} m_2^{-1} \in N.$$

Consequently,

$$xy^{-1} = m_1 m_2^{-1} (m_2 n_1 n_2^{-1} m_2^{-1}) \in MN.$$

Thus,

$$x, y \in MN \implies xy \in MN.$$

Hence,  $MN$  is a subgroup of  $G$ .

Now we shall endeavor to show that  $x^{-1}(MN)x \subset MN$ .

Let,  $y \in x^{-1}(MN)x$ . Then,

**there exist elements  $m$  in  $M$  and  $n$  in  $N$  such that**

$$y = x^{-1}(mn)x.$$

Then we have,

$$y = x^{-1}(mn)x = (x^{-1}mx)(x^{-1}nx) \in MN$$

as  $x^{-1}Mx \subset M$  and  $x^{-1}Nx \subset N$  for all  $x \in G$ .

Therefore,

$$y \in x^{-1}(MN)x \implies y \in MN.$$

So,

$$x^{-1}(MN)x \subset MN.$$

This completes the proof.

## Result

3 of 3

Being  $x^{-1}Mx \subset M$  and  $x^{-1}Nx \subset N$  for all  $x \in G$ , we have proved that for any  $x, y \in MN$ ,  $xy^{-1} \in MN$  and later  $x^{-1}(MN)x \subset M$ . Click for the complete proof.

29. a

**Given:**  $G$  is a group and  $M$  is a subgroup of  $G$  such that

$$x^{-1}Mx \subset M, \text{ for all } x \in G.$$

**To Prove:**  $x^{-1}Mx = M$ .

**Proof:** To prove  $x^{-1}Mx = M$ , it suffices to show that

$$M \subset x^{-1}Mx.$$

Let us consider an element  $m$  in  $M$ .

Then,

$$m = x^{-1}(xmx^{-1})x, \text{ for any } x \in G.$$

Since  $G$  is a group,

$$x \in G \implies x^{-1} \in G.$$

So,

$$xmx^{-1} = (x^{-1})^{-1}mx^{-1} \in x^{-1}Mx (\subset M) \implies xmx^{-1} \in M.$$

It follows that

$$m = x^{-1}(xmx^{-1})x \in x^{-1}Mx.$$

Thus,

$$m \in M \implies m \in x^{-1}Mx.$$

Consequently,

$$M \subset x^{-1}Mx.$$

Thence,

$$M = x^{-1}Mx.$$

This completes the proof.

## Result

2 of 2

Considering any  $m$  in  $M$  we have proved by using  $x^{-1}Mx \subset M$ , that  $M \subset x^{-1}Mx$ , consequently  $x^{-1}Mx = M$ . Click for the complete proof.

30. a

**Given:**  $M$  and  $N$  are two subgroups of a group  $G$  such that

$$x^{-1}Mx = M \text{ and } x^{-1}Nx = N.$$

**To Prove:** If  $M \cap N = (e)$ , then  $mn = nm$  for any  $m \in M$  and  $n \in N$ ,  $e$  being the identity element of  $G$ .

**Proof:** Let us consider arbitrary elements  $m \in M$  and  $n \in N$ . Now consider the element  $m^{-1}n^{-1}mn$  in  $G$ . Considering  $m \in M$  and  $n \in N$  we have

$$n^{-1}mn \in n^{-1}Mn (= M) \implies n^{-1}mn \in M.$$

Now,

$$m \in M \implies m^{-1} \in M.$$

So,

$$m^{-1}, n^{-1}mn \in M \implies m^{-1}n^{-1}mn \in M.$$

Again,

$$n \in N \implies n^{-1} \in N.$$

Similarly, considering  $n \in N$  and  $m \in M$  we have,

$$m^{-1}n^{-1}m \in m^{-1}Nm (= N) \implies m^{-1}n^{-1}m \in N.$$

Therefore,

$$m^{-1}n^{-1}m, n \in N \implies m^{-1}n^{-1}mn \in N.$$

Hence,

$$m^{-1}n^{-1}mn \in M \text{ as well as } m^{-1}n^{-1}mn \in N \implies m^{-1}n^{-1}mn \in M \cap N.$$

But

$$M \cap N = (e), e \text{ being the identity element in } G.$$

Hence,

$$m^{-1}n^{-1}mn = e \implies mn = nm.$$

Since  $n$  and  $m$  were arbitrary, it follows that

$$mn = nm, \text{ for all } m \in M, n \in N.$$

This completes the proof.

## Result

2 of 2

Considering  $m \in M$  and  $n \in N$  and using  $n^{-1}Mn = M$  we have shown that  $m^{-1}n^{-1}mn \in M$ , similarly using  $m^{-1}Nm = N$ , we have shown that  $m^{-1}n^{-1}mn \in N$  and being  $M \cap N = (e)$ ,  $nm = mn$  comes. click for the detailed proof.

## Section 2-4

1. a

(a) Refl: For all  $a \in \mathbb{R}$  we have  $a - a = 0 \in \mathbb{Q}$ .

Sym: If  $a \sim b$  then  $a - b \in \mathbb{Q}$ , so  $b - a = -(a - b) \in \mathbb{Q}$  and therefore  $b \sim a$ .

Trans: If  $a \sim b$  and  $b \sim c$  then  $a - b, b - c \in \mathbb{Q}$ , so  $a - c = (a - b) + (b - c) \in \mathbb{Q}$  and therefore  $a \sim c$ .

(b) Refl: For all  $a \in \mathbb{C}$  we have  $|a| = |a|$ .

Sym: If  $a \sim b$  then  $|a| = |b|$ , so  $|b| = |a|$  and therefore  $b \sim a$ .

Trans: If  $a \sim b$  and  $b \sim c$  then  $|a| = |b|$  and  $|b| = |c|$ , so  $|a| = |c|$  and therefore  $a \sim c$ .

(c) Refl: For all  $a \in S$  we have that  $a$  parallel to itself.

Sym: If  $a \sim b$  then  $a$  is parallel to  $b$ , so  $b$  is parallel to  $a$  and therefore  $b \sim a$ .

Trans: If  $a \sim b$  and  $b \sim c$  then  $a$  is parallel to  $b$  and  $b$  is parallel to  $c$ , so  $a$  is parallel to  $c$  and therefore  $a \sim c$ .

(d) Refl: For all  $a \in S$  we have that  $a$  has the same eye color as themselves.

Sym: If  $a \sim b$  then  $a$  has the same eye color as  $b$ , so  $b$  has the same eye color as  $a$  and therefore  $b \sim a$ .

Trans: If  $a \sim b$  and  $b \sim c$  then  $a$  has the same eye color as  $b$  and  $b$  has the same eye color as  $c$ , so  $a$  has the same eye color as  $c$  and therefore  $a \sim c$ .

## Result

In each case the reflective, symmetry and transitivity conditions can be directly verified.

## 2. a

**Given:** The relation  $\sim$  on the real line  $\mathbb{R}$  is defined by

$$a \sim b \text{ if and only if } a > b \text{ and } b < a.$$

We need to show that this is not an equivalence relation.

### Step 2

2 of 3

Let us examine the reflexiveness of the relation.

If  $a$  be an element in  $\mathbb{R}$ , then  $a$  does not satisfy any of the above given condition as,  $a > a$  nor  $a < a$ . This implies  $\sim$  is not reflexive, implies not an equivalence relation.

## Result

3 of 3

Since the given relation does not satisfies the reflexive property, its not an equivalence relation.

## 3. a

It is not the case in general that for each element in  $a \in S$  there is  $b \in S$  such that  $a \sim b$ . Therefore, without this assumption the given proof is not correct!

**Example :** Let consider set  $\{1, 2, 3\}$  and relation given by

$$x \sim y \text{ if and only if } (x, y) \in \{(1, 1), (1, 2), (2, 1), (2, 2)\}$$

This is well-defined relation on  $\{1, 2, 3\}$  and it satisfies the *symmetry* and *transitivity* condition, but it is not *reflexive*.

## Result

2 of 2

It is not the case in general that for each element in  $a \in S$  there is  $b \in S$  such that  $a \sim b$

### 4. a

Define the following relation: For  $a, b \in S$  let  $a \sim b$  if there is some  $\alpha$  such that  $a, b \in S_\alpha$ .

This is indeed an equivalence relation:

Refl.: For all  $a \in S$  since  $S = \bigcup_\alpha S_\alpha$  there is some  $\alpha$  such that  $a \in S_\alpha$  and so  $a \sim a$ .

Sym.: If  $a \sim b$  then  $a, b \in S_\alpha$ , so  $b, a \in S_\alpha$  and so  $b \sim a$ .

Trans.: If  $a \sim b$  and  $b \sim c$  then  $a, b \in S_\alpha$  and  $b, c \in S_\beta$ . Since  $b \in S_\alpha \cap S_\beta$  by assumption ( $S_\alpha \cap S_\beta = \emptyset$  for  $\alpha \neq \beta$ ) we have that  $\alpha = \beta$ , so we have that  $a, c \in S_\alpha$  and therefore  $a \sim c$ .

By definition all elements in  $S_\alpha$  are in the same equivalence class, and since  $S_\alpha \cap S_\beta = \emptyset$  we have that elements in distinct subsets  $S_\alpha$  are in distinct equivalence classes.

## Result

2 of 2

Define the following relation: For  $a, b \in S$  let  $a \sim b$  if there is some  $\alpha$  such that  $a, b \in S_\alpha$ .

### 5. a

**Given:**  $G$  is a group and  $H$  is a subgroup of  $G$ . A relation  $\sim$  is defined on  $G$  by the assignment

$$\text{for } a, b \in G, a \sim b \text{ if and only if } a^{-1}b \in H.$$

**To Prove:**  $\sim$  defines an equivalence relation on  $G$ .

**Proof:** Let us consider three elements  $a, b, c$  in  $G$ . We will now check the equivalence relation of  $\sim$  on  $G$ .

#### Reflexivity

$a \in G$  then  $a^{-1}a = e \in H$ ,  $e$  being the identity element in  $G$ .

So,  $a \sim a$ .

#### Symmetry

$a, b \in G$  such that  $a^{-1}b \in H$ .

Since  $H$  is a subgroup

$$(a^{-1}b)^{-1} \in H \implies b^{-1}a \in H.$$

This follows that  $b \sim a$ .

### **Transitivity**

$a, b, c \in G$  such that  $a \sim b$  and  $b \sim c$ .

That is,

$$a^{-1}b \in H \text{ and } b^{-1}c \in H.$$

Since  $H$  is a subgroup

$$a^{-1}b \in H \text{ and } b^{-1}c \in H \implies (a^{-1}b)(b^{-1}c) = a^{-1}c \in H.$$

This follows that  $a \sim c$ .

Hence  $\sim$  defines an equivalence relation on  $G$ .

Since  $\sim$  is an equivalence relation we have

$$\begin{aligned}[a] &= \{b \in G \mid a^{-1}b \in H\} \\ &= \{b \in G \mid aH = bH\} \\ &= aH.\end{aligned}$$

Hence we are done.

### **Result**

3 of 3

In order to show that  $\sim$  defines an equivalence relation on  $G$ , we have shown that for any three elements  $a, b, c \in G$  all three conditions Reflexivity, Symmetry and Transitivity satisfied. Click for the complete solution.

## 6. a

**Given:**  $G = S_3$ , where  $S_3$  is the set of all permutations on the set  $\{x_1, x_2, x_3\}$ . And  $H = \{i, f\}$ , where  $f : S \rightarrow S$  is a mapping is defined by

$$f(x_1) = x_2, f(x_2) = x_1, f(x_3) = x_3.$$

We will now find the list of all left and right cosets of  $H$  in  $G$ . For our simplicity we would like to write  $f$  as  $f = (x_1, x_2)$ .

Let us introduce the set  $S_3$  as

$$S_3 := \{i, f_1, f_2, f_3, f_4, f\},$$

where  $f_1 = (x_1, x_2, x_3)$ ,  $f_2 = (x_1, x_3, x_2)$ ,  $f_3 = (x_2, x_3)$ , and  $f_4 = (x_1, x_3)$ .

Now the left cosets of  $H$  in  $G$  are

$$\begin{aligned}iH &= \{i, f\} = H \\ f_1H &= \{f_1, f_4\} \\ f_2H &= \{f_2, f_3\} \\ f_3H &= \{f_3, f_2\} \\ f_4H &= \{f_4, f_1\} \\ fH &= \{f, i\}.\end{aligned}$$

**There are three distinct left cosets of  $H$  in  $G$ .**

They are

$$H, \{f_2, f_3\}, \{f_1, f_4\}.$$

Now the right cosets of  $H$  in  $G$  are

$$\begin{aligned} Hi &= \{i, f\} = H \\ Hf_1 &= \{f_1, f_3\} \\ Hf_2 &= \{f_2, f_4\} \\ Hf_3 &= \{f_3, f_1\} \\ Hf_4 &= \{f_4, f_2\} \\ Hf &= \{f, i\}. \end{aligned}$$

**There are three distinct left cosets of  $H$  in  $G$ .**

They are

$$H, \{f_2, f_4\}, \{f_1, f_3\}.$$

These are the complete list of left and right cosets of  $H$  in  $G$ .

## Result

3 of 3

Complete list of left cosets of  $H$  in  $G$  are  $H, \{f_2, f_3\}, \{f_1, f_4\}$  and right cosets are  $H, \{f_2, f_4\}, \{f_1, f_3\}$ .

## 7. a

**Given:**  $G = S_3$ , where  $S_3$  is the set of all permutations on the set  $\{x_1, x_2, x_3\}$ . And  $H = \{i, f\}$ , where  $f : S \rightarrow S$  is a mapping is defined by

$$f(x_1) = x_2, f(x_2) = x_1, f(x_3) = x_3.$$

We will now find the list of all left and right cosets of  $H$  in  $G$ . For our simplicity we would like to write  $f$  as  $f = (x_1, x_2)$ .

Let us introduce the set  $S_3$  as

$$S_3 := \{i, f_1, f_2, f_3, f_4, f\},$$

where  $f_1 = (x_1, x_2, x_3)$ ,  $f_2 = (x_1, x_3, x_2)$ ,  $f_3 = (x_2, x_3)$ , and  $f_4 = (x_1, x_3)$ .

Now the left cosets of  $H$  in  $G$  are

$$\begin{aligned} iH &= \{i, f\} = H \\ f_1H &= \{f_1, f_4\} \\ f_2H &= \{f_2, f_3\} \\ f_3H &= \{f_3, f_2\} \\ f_4H &= \{f_4, f_1\} \\ fH &= \{f, i\}. \end{aligned}$$

**There are three distinct left cosets of  $H$  in  $G$ .**

They are

$$H, \{f_2, f_3\}, \{f_1, f_4\}.$$

Now the right cosets of  $H$  in  $G$  are

$$\begin{aligned} Hi &= \{i, f\} = H \\ Hf_1 &= \{f_1, f_3\} \\ Hf_2 &= \{f_2, f_4\} \\ Hf_3 &= \{f_3, f_1\} \\ Hf_4 &= \{f_4, f_2\} \\ Hf &= \{f, i\}. \end{aligned}$$

**There are three distinct left cosets of  $H$  in  $G$ .**

They are

$$H, \{f_2, f_4\}, \{f_1, f_3\}.$$

These are the complete list of left and right cosets of  $H$  in  $G$ .

Then not every right coset of  $H$  in  $G$  is a left coset of  $H$  in  $G$ . For example, consider the right coset  $Hf_1 = \{f_1, f_3\}$ , from above, which is not a left coset of  $H$  in  $G$ .

## Result

3 of 3

Not every right coset of  $H$  in  $G$  is a left coset of  $H$  in  $G$ . For example, consider the right coset  $Hf_1 = \{f_1, f_3\}$ , which is not a left coset of  $H$  in  $G$ . Click for the detailed proof.

## 8. a

**Given:**  $H$  is a subgroup of the group  $G$  with the property that every left coset of  $H$  in  $G$  is also a right coset of  $H$  in  $G$ .

**To Prove:**  $aHa^{-1} = H$ , for all  $a \in G$ .

**Proof:** We have

$$Ha = bH, \text{ for } a, b \in G.$$

Then there exist  $h_1, h_2 \in H$  such that

$$h_1a = bh_2.$$

Hence,

$$\begin{aligned} h_1a = bh_2 &\implies b = h_1ah_2^{-1} \\ &\implies bH = h_1ah_2^{-1}H \\ &\implies Ha = h_1ah_2^{-1}H \\ &\implies Ha = h_1aH \\ &\implies h_1^{-1}Ha = aH \\ &\implies Ha = aH. \end{aligned}$$

Therefore,

$$\begin{aligned} Ha &= aH, \text{ for all } a \in G \\ \implies H &= aHa^{-1}. \end{aligned}$$

This completes the proof.

### Result

2 of 2

Considering  $Ha = bH$  for  $a, b \in H$  we have proved that  $H = aHa^{-1}$ . Click for the complete proof.

### 9. a

We have

$$\mathbb{Z}_{16} = \{[0], [1], [2], \dots, [14], [15]\}.$$

By the given condition

$$H = \{[0], [4], [8], [12]\}.$$

Then the list of all cosets (left) of  $H$  in  $\mathbb{Z}_{16}$  are given by

$$\begin{aligned} [0] + H &= H; \\ [1] + H &= \{[1], [5], [9], [13]\}; \\ [2] + H &= \{[2], [6], [10], [14]\}; \\ [3] + H &= \{[3], [7], [11], [15]\}. \end{aligned}$$

### Result

2 c

The list of all left cosets of  $H$  in  $\mathbb{Z}_{16}$  are  $[0] + H = H$ ;  $[1] + H = \{[1], [5], [9], [13]\}$ ;  $[2] + H = \{[2], [6], [10], [14]\}$ ;  $[3] + H = \{[3], [7], [11], [15]\}$ .

### 10. a

We have

$$\mathbb{Z}_{16} = \{[0], [1], [2], \dots, [14], [15]\}.$$

By the given condition

$$H = \{[0], [4], [8], [12]\}.$$

Then the list of all cosets (left) of  $H$  in  $\mathbb{Z}_{16}$  are given by

$$\begin{aligned}[0] + H &= H; \\ [1] + H &= \{[1], [5], [9], [13]\}; \\ [2] + H &= \{[2], [6], [10], [14]\}; \\ [3] + H &= \{[3], [7], [11], [15]\}. \end{aligned}$$

Now we know that

$$\text{The number of left cosets of } H \text{ in } \mathbb{Z}_{16} = \text{The number of right cosets of } H \text{ in } \mathbb{Z}_{16} = 4$$

Hence the index of  $H$  in  $\mathbb{Z}_{16}$  is 4. That is,

$$[\mathbb{Z}_{16} : H] = 4.$$

## Result

The index of  $H$  in  $\mathbb{Z}_{16}$  is 4.

11. a

**Given:**  $G$  is a finite group and  $H$  is a subgroup of  $G$ .

**To Prove:** The number of left cosets of  $H$  in  $G$  is equal to the number of right cosets of  $H$  in  $G$ .

### Proof:

It suffices to show that

**the set of all distinct left cosets of  $H$  in  $G$  and the set of all distinct right cosets of  $H$  in  $G$  have the same cardinality.**

Let  $L$  and  $R$  be the set of all distinct left and right cosets of  $H$  in  $G$  respectively.

Let us consider an element  $a$  in  $G$ .

Let us define a mapping

$$f : L \rightarrow R$$

by the assignment

$$f(aH) = Ha^{-1}, \quad aH \in L.$$

First we show that the mapping  $f$  is **well defined** in the sense that if

$$xH = aH \quad \text{then} \quad Hx^{-1} = Ha^{-1}.$$

Now,

$$\begin{aligned}xH = aH &\implies x \in aH \\&\implies a^{-1}x \in H \\&\implies a^{-1}(x^{-1})^{-1} \in H \\&\implies a^{-1} \in Hx^{-1} \\&\implies Ha^{-1} = Hx^{-1}.\end{aligned}$$

Therefore

$f$  assigns a unique coset in  $R$  to a unique coset in  $L$

We now prove that  $f$  is **injective**.

Let  $aH, bH \in L$  and  $aH \neq bH$ .

Then,

$$\begin{aligned}f(aH) = f(bH) &\implies Ha^{-1} = Hb^{-1} \\&\implies a^{-1} \in Hb^{-1} \\&\implies a^{-1}(b^{-1})^{-1} \in H \\&\implies a^{-1}b \in H \\&\implies b \in aH \implies bH = aH.\end{aligned}$$

So,

$$aH \neq bH \implies f(aH) \neq f(bH).$$

This proves that

$f$  is injective.

In order to prove the  $f$  is **surjective**, let us take an element  $Ha$  in  $R$ .

The pre-image of  $Ha$  is  $a^{-1}H$  in  $L$ , since

$$f(a^{-1}H) = H(a^{-1})^{-1} = Ha.$$

Therefore,

$f$  is surjective.

Consequently,  $f$  is a **bijection** from  $L$  to  $R$ .

Hence the sets  $L$  and  $R$  have the **same cardinality**.

#### Step 4

4 of 5

Since  $G$  is a

**finite group, the sets  $L$  and  $R$  are finite.**

Since  $f$  is a bijection from  $L$  to  $R$ ,

**the number of elements of  $L$  and  $R$  must be same.**

Thus we have proved that the number of left cosets of  $H$  in  $G$  is equal to the number of right cosets of  $H$  in  $G$ .

Hence we are done.

## Result

5 of 5

Being  $G$  is a finite group the number of left and right cosets of  $H$  in  $G$  must be finite. In order to show that the number of left cosets of  $H$  in  $G$  is equal to the number of right cosets of  $H$  in  $G$ , we have proved the existence of a bijection between them.  
Click for the detailed proof.

## 12. a

If we consider abelian group  $G$ , then must be  $aH = Ha$  and  $bH = Hb$ . Therefore, this implies that

$$Ha = aH \neq bH = Hb$$

Considering the nonabelian symmetry group  $S_3$  an its subgroup  $H = \{Id, f\}$  where

$$Id(1) = 1 \quad Id(2) = 2 \quad Id(3) = 3$$

$$f(1) = 2 \quad f(2) = 1 \quad f(3) = 3$$

we can conlude that for  $a$  given by  $a(1) = 1, a(2) = 3$  and  $a(3) = 2$  and  $b = fa$  we obtain that

$$aH = \{a, af\} \neq \{af, afa\} = bH$$

and

$$Ha = \{a, fa\} = \{f^2a, fa\} = Hb$$

Therefore, in the case where  $G$  is non-abelian it is not neccesary that  $aH \neq bH$  implies that  $Ha \neq Hb$ .

## Result

(HINT:) Consider the non-abelian group  $S_3$ .

## Method 2.

Consider the group  $D_4$  of symmetries of a square and let  $f$  be the vertical reflection and  $r$  the  $90^\circ$  counterclockwise rotation. Let  $H = \{e, f\}$  We then have that

$$rH = \{r, rf\} \neq \{e, f\} = rfH$$

Consider the group  $D_4$  of symmetries of a square and let  $f$  be the vertical reflection and  $r$  the  $90^\circ$  counterclockwise rotation. Let  $H = \{e, f\}$  We then have that

$$rH = \{r, rf\} \neq \{fr, frf = r^3\} = frH$$

and

$$Hr = \{r, fr\} = \{fr, r\} = Hfr.$$

## Result

2 of 2

A counter example can be constructed by consider the group  $D_4$  of symmetries of a square and the subgroup  $H = \{e, f\}$  consisting of the identity and a reflection.

## 13. a

We have the following elements of  $U(18)$  and their orders can be directly computed:

element	order
[1]	1
[5]	6
[7]	3
[11]	6
[13]	3
[17]	2

For example,

$$[13]^1 = [13] \neq [1]$$

$$[13]^2 = [169] = [7] \neq [1]$$

$$[13]^3 = [2197] = [1]$$

Thus, the order of [13] is 3. Similarly for the rest of the elements.

Since  $U(18)$  has order 6 and elements of order 6 it is cyclic.

## Result

$U(18)$  has order 6 and an element of order 6, so it is cyclic.

## Method 2.

Group  $U_{18}$  is given by

$$U_{18} = \{[a] \in \mathbb{Z}_{18} | (a, 18) = 1\}$$

i.e.

$$U_{18} = \{[1], [5], [7], [11], [13], [17]\}$$

Order of this group is 6, so that let's prove that there is some element of order 6. From the facts

$$5 \equiv 5 \pmod{18} \quad (1)$$

$$5^2 \equiv 7 \pmod{18} \quad (2)$$

$$5^3 \equiv 17 \pmod{18} \quad (3)$$

$$5^4 \equiv 13 \pmod{18} \quad (4)$$

$$5^5 \equiv 11 \pmod{18} \quad (5)$$

$$5^6 \equiv 1 \pmod{18} \quad (6)$$

So,  $[5]^6 = [1]$ , and we obtain that  $o([5]) = 6$ .

Therefore, group  $U_{18}$  is cyclic!

## Result

2 of 2

(HINT:) Find the order of [5].

14. a

Group  $U_{20}$  is given by

$$U_{20} = \{[a] \in \mathbb{Z}_{20} \mid (a, 20) = 1\}$$

i.e.

$$U_{20} = \{[1], [3], [7], [9], [11], [13], [17], [19]\}$$

Order of this group is 8, so let's see if there is some element of order 8. From the facts

$$3^4 \equiv 1 \pmod{20} \quad (1)$$

$$7^4 \equiv 1 \pmod{20} \quad (2)$$

$$9^2 \equiv 1 \pmod{20} \quad (3)$$

$$11^2 \equiv 1 \pmod{20} \quad (4)$$

$$13^4 \equiv 1 \pmod{20} \quad (5)$$

$$17^4 \equiv 1 \pmod{20} \quad (6)$$

$$19^2 \equiv 1 \pmod{20} \quad (7)$$

we obtain that there is no element of order 8.

Therefore, group  $U_{20}$  is **not cyclic!**

## Result

2 of 2

(HINT:) Consider the order of each element.

## Method 2.

We have the following elements of  $U(20)$  and their orders can be directly computed:

element	order
[1]	1
[3]	4
[7]	4
[9]	2
[11]	2
[13]	4
[17]	4
[19]	2

For example,

$$[3]^1 = [3] \neq [1]$$

$$[3]^2 = [9] \neq [1]$$

$$[3]^3 = [27] = [7] \neq [1]$$

$$[3]^4 = [81] = [1]$$

Thus, the order of [3] is 4. Similarly for the rest of the elements.

Since  $U(20)$  has order 8 and no element of order 8 it is not cyclic.

## Result

$U(20)$  has order 8 and no element of order 8, so it is not cyclic.

15. a

Given that  $p$  is a prime number.

We need to show that the only solutions of the equation  $x^2 \equiv 1 \pmod{p}$  are  $x \equiv 1 \pmod{p}$  or  $x \equiv -1 \pmod{p}$

Since we have  $x^2 \equiv 1 \pmod{p}$ . Then

**there exists integer  $k$  such that**

$$x^2 = 1 + kp.$$

Therefore,

$$x^2 - 1 = kp \implies (x+1)(x-1) = kp.$$

It follows that  $p$  divides  $(x+1)(x-1)$ . Since  $p$  is a prime,  $p$  either divides  $(x+1)$  or  $(x-1)$ .

Thus

$$x \equiv 1 \pmod{p} \text{ or } x \equiv -1 \pmod{p}.$$

Hence the only solutions of the equation  $x^2 \equiv 1 \pmod{p}$  are  $x \equiv 1 \pmod{p}$  or  $x \equiv -1 \pmod{p}$ .

This completes the proof.

## Result

2 of 2

Considering the equation  $x^2 \equiv 1 \pmod{p}$  and factorize  $x^2 - 1$  as  $(x+1)(x-1)$  we have proved that the only solutions of the equation  $x^2 \equiv 1 \pmod{p}$  are  $x \equiv 1 \pmod{p}$  or  $x \equiv -1 \pmod{p}$ . Click for the complete proof.

## 16. a

**Given:**  $G$  is a finite abelian group with  $a_1, a_2, a_3, \dots, a_n$  are all its elements.

**To Prove:** If  $x = a_1 a_2 a_3 \dots a_n$  then  $x$  must satisfy  $x^2 = e$ ,  $e$  being the identity element of  $G$ .

**Proof:** Since  $G$  is a finite group with all its elements are precisely  $a_1, a_2, a_3, \dots, a_n$ ,  
then the inverses of these elements are in the set  $\{a_1, a_2, a_3, \dots, a_n\}$ .

Since  $G$  is abelian

$$a_k \cdot a_m = a_m \cdot a_k, \text{ for } 1 \leq m, k \leq n.$$

Now  $x = a_1 a_2 a_3 \dots a_n$ . So,

$$\begin{aligned} x^2 &= (a_1 a_2 a_3 \dots a_n)^2 \\ &= (a_1 a_2 a_3 \dots a_n)(a_1 a_2 a_3 \dots a_n) \end{aligned}$$

Since  $G$  is

abelian, the product  $(a_1 a_2 a_3 \dots a_n)(a_1 a_2 a_3 \dots a_n)$  can arrange them according as  $(a_i a_j)$  where  $a_i$  is the inverse of  $a_j$  in  $G$ .

It follows that

$$x^2 = e \cdot e \cdot e \dots \cdot e, \text{ up to } n \text{ terms.}$$

Hence,

$$x^2 = e.$$

This completes the proof.

### Result

Being  $G$  is finite and abelian, we arrange each element to its inverse in the product  $(a_1 a_2 a_3 \dots \dots a_n)(a_1 a_2 a_3 \dots \dots a_n)$  and get the identity. Click for the complete proof.

17. a

**Given:**  $G$  is a group of odd order such that there exists an element with

$$x^2 = e, \text{ } e \text{ being the identity element of } G.$$

**Claim:**  $x$  is the identity element in  $G$ .

**Proof of the claim:** We have

$$x^2 = e.$$

This follows that order of  $x$  divides 2. Hence order of  $x$  must be 1 or 2.

If order of  $x$  be 2 in  $G$ , then 2 must divide the order of  $G$ , which is an impossibility since  $G$  is an group of odd order.

Hence, order of  $x$  is 1 in  $G$ .

Therefore,  $x = e$ .

This completes our proof.

### Result

2 of 2

$G$  being an odd order group and  $x^2 = e$  in  $G$ ,  $x$  must be the identity element in  $G$ . Click for the detailed proof.

18. a

**To prove:** If  $p$  is an odd prime, then  $(p - 1)! \equiv -1 \pmod{p}$ .

**Proof:** Let us consider the group of integers modulo  $p$ ,  $\mathbb{Z}_p$ . Since  $p$  is odd prime,  $\mathbb{Z}_p - \{0\}$  forms a group under multiplication, that is,  $(\text{modulo } p)$ .

Now order of the group  $(\mathbb{Z}_p - \{0\}, \cdot)$  is  $p - 1$ , which is even. As mentioned in the question, from Question.16 we have

$$\begin{aligned} ((p - 1)!)^2 &\equiv 1 \pmod{p} \\ \implies (p - 1)! &\equiv 1 \pmod{p} \text{ or } (p - 1)! \equiv -1 \pmod{p}. \end{aligned}$$

Since each element have inverse in the group formed above we have

$$\begin{aligned} ((p - 1)!)^2 &\equiv 1 \pmod{p} \\ \implies 1 \cdot 2 \cdot 3 \dots (p - 2) &\equiv 1 \pmod{p}. \end{aligned}$$

Therefore,

$$(p - 1)! \equiv -1 \pmod{p}.$$

This completes the proof.

## Result

2 of 2

Considering the group  $\mathbb{Z}_p - \{0\}$  under multiplication modulo( $p$ ) we have proved that  $1 \cdot 2 \cdot 3 \dots (p - 2) \equiv 1 \pmod{p}$ , which follows the result. Click for the complete proof.

## 19. a

### Conjugacy classes in $S_3$

The elements of  $S_3$  are  $\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ , where

$$\rho_0 = id, \rho_1 = (1 \ 2 \ 3), \rho_2 = (1 \ 3 \ 2), \rho_3 = (2 \ 3), \rho_4 = (1 \ 3), \text{ and } \rho_5 = (1 \ 2).$$

The centre of  $S_3$  is  $\{\rho_0\}$ . Therefore  $\rho_0$  is a self conjugate element.

The conjugacy class

$$cl(\rho_0) = \{\rho_0\}.$$

Now,

$$\rho_3 \rho_1 \rho_3^{-1} = \rho_3 \rho_1 \rho_3 = \rho_2.$$

Hence  $\rho_2$  is conjugate to  $\rho_1$ .

Since every conjugate to an element  $a$  must have the same order as that of  $a$ , and the order of  $\rho_1$  is 3, it follows that  $\rho_3, \rho_4, \rho_5$  each being of order 2, cannot be conjugate to  $\rho_1$ .

So the conjugacy class

$$\begin{aligned} cl(\rho_1) &= \{\rho_1, \rho_2\}. \\ \rho_4 \rho_3 \rho_4^{-1} &= \rho_4 \rho_3 \rho_4 = \rho_5. \end{aligned}$$

Hence  $\rho_5$  is conjugate to  $\rho_3$ .

$$\rho_5 \rho_3 \rho_5^{-1} = \rho_5 \rho_3 \rho_5 = \rho_4.$$

Hence  $\rho_4$  is conjugate to  $\rho_3$ .

The conjugacy class

$$cl(\rho_3) = \{\rho_3, \rho_4, \rho_5\}.$$

Therefore,

$$S_3 = cl(\rho_0) \cup cl(\rho_1) \cup cl(\rho_3).$$

Therefore, the distinct conjugacy classes of  $S_3$  are precisely

$$\{\rho_0\}, \{\rho_1, \rho_2\}, \{\rho_3, \rho_4, \rho_5\}.$$

## Result

2 of

The distinct conjugacy classes of  $S_3$  are precisely  $\{\rho_0\}, \{\rho_1, \rho_2\}, \{\rho_3, \rho_4, \rho_5\}$ .

[Click for the detailed solution.](#)

## 20. a

It is not hard to conclude that inverse element for  $T_{c,d}$  is given by  $T_{c^{-1},dc^{-1}}$ .

Therefore, the conjugacy class of  $T_{a,b}$  is given by

$$\begin{aligned} [T_{a,b}] &= \{T_{c^{-1},dc^{-1}} * T_{a,b} * T_{c,d} | c, d \in \mathbb{R} \text{ and } c \neq 0\} \\ &= \{T_{c^{-1},dc^{-1}} * T_{ac,ad+b} | c, d \in \mathbb{R} \text{ and } c \neq 0\} \\ &= \{T_{a,(b+d(a-1))c^{-1}} | c, d \in \mathbb{R} \text{ and } c \neq 0\} \end{aligned}$$

Let consider next cases

⊕. In the case  $a = 1, b = 0$ , the conjugacy class has only one element  $T_{1,0}$ .

⊕. In the case  $a \neq 1, b = 0$ , for an arbitrary number  $s$  we can choose  $c = 1$  and  $d = s(a-1)^{-1}$  to obtain that  $s = b + d(a-1)c^{-1}$ .

Therefore, the conjugacy class of  $T_{a,0}$  is given by

$$[T_{a,0}] = \{T_{a,s} | s \in \mathbb{R}\}$$

⊕. In the case  $a = 1, b \neq 0$ , for an arbitrary number  $s \neq 0$  we can choose  $c = bs^{-1}$  to obtain that  $s = b + d(a-1)c^{-1}$ , but we can not choose  $c$  and  $d$  such that  $0 = b + d(a-1)c^{-1} = bc^{-1}$ .

Therefore, the conjugacy class of  $T_{1,b}$  is given by

$$[T_{1,b}] = \{T_{1,s} | s \in \mathbb{R} \text{ and } s \neq 0\}$$

⊕. Finally, the case  $a \neq 1, b \neq 0$ , for an arbitrary number  $s \neq 0$  we can choose  $c = bs^{-1}$  and  $d = 0$  to obtain that  $s = b + d(a-1)c^{-1}$ , and we can choose  $d = -b(a-1)^{-1}$  to obtain  $0 = b + d(a-1)c^{-1}$ .

Therefore, the conjugacy class of  $T_{a,b}$  is given by

$$[T_{a,b}] = \{T_{a,s} | s \in \mathbb{R}\}$$

## Result

(HINT:) Use the fact that  $(T_{c,d})^{-1}T_{a,b}T_{c,d} = T_{a,(b+d(a-1))c^{-1}}$ .

21. a

### Conjugacy classes of Dihedral group of order 8

Let  $G$  be the Dihedral group of order 8 i.e.,  $G := \langle s, r \rangle$ .

Then for element  $s \in G$ , the

**centralizer of  $s$  has order 4**

, and is  $\{1, r^4, s, sr^4\}$ .

Therefore

the conjugacy class of  $s$  in  $G$  has size 4.

Now we have

$$s^r = rsr = ssrsr = sr^2$$

and

$$s^{rs} = sr^6 \text{ and } s^{rsr} = sr^2r^2 = sr^4$$

Thus the **conjugacy class** of  $s$  is  $\{s, sr^2, sr^4, sr^6\}$ .

Now

$t = sr$  and the centralizer of  $sr$  at least contains  $1, sr, r^2$  and  $sr^3$  so the conjugacy class of  $t$  has size at most 2.

Notice that

$$t^s = sts = rs = sr^{-1} = sr^3.$$

Thus the **conjugacy class** of  $t$  ( $= sr$ ) is

$$\{sr, sr^3, sr^5, sr^7\}.$$

The centre  $Z(G)$  of  $G$  is  $\{1, r^2\}$  and so each of the elements of this set is in a conjugacy class of size 1.

Finally, the elements  $r$  and  $r^3$  are

**non-central and therefore are in conjugacy classes of size greater than 1.**

The remaining conjugacy class is therefore

$$\{r, r^3\}.$$

Now let us consider the cyclic subgroup  $\langle t \rangle$ .

The elements of  $\langle t \rangle$  are all centralized by  $\langle t \rangle$  and so are either central, or are in conjugacy classes of size 2. Each element of  $\langle t \rangle$  is conjugate to its inverse.

**Hence the list of all conjugacy classes of  $G$  are given as:**

$$\{s, sr^2, sr^4, sr^6\}, \{sr, sr^3, sr^5, sr^7\}, \{1\}, \{r^4\}, \{r, r^7\}, \{r^2, r^6\}, \text{ and } \{r^3, r^5\}.$$

## Result

2 of 2

The conjugacy classes of  $G$  are  $\{s, sr^2, sr^4, sr^6\}, \{sr, sr^3, sr^5, sr^7\}, \{1\}, \{r^4\}, \{r, r^7\}, \{r^2, r^6\}, \text{ and } \{r^3, r^5\}$ .

Click for the complete solution.

22. a

#### Verification of Euler's Theorem

Given,  $n = 14$  and  $a = 3$ .

Then we have

$$(a, n) = (3, 14) = 1.$$

Now,

$$\phi(n) = \phi(14) = \phi(2 \times 7) = 14 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right) = 6.$$

Now,

$$\begin{aligned} a^{\phi(n)} \pmod{n} &= (3)^6 \pmod{14} \\ &= 729 \pmod{14} \\ &= (52 \times 14 + 1) \pmod{14} \\ &= 1 \pmod{14}. \end{aligned}$$

Given,  $n = 14$  and  $a = 5$ .

Then we have

$$(a, n) = (5, 14) = 1..$$

Now,

$$\phi(n) = \phi(14) = \phi(2 \times 7) = 14 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right) = 6.$$

Now,

$$\begin{aligned} a^{\phi(n)} \pmod{n} &= (5)^6 \pmod{14} \\ &= 15625 \pmod{14} \\ &= (1116 \times 14 + 1) \pmod{14} \\ &= 1 \pmod{14}. \end{aligned}$$

Hence we have verified Euler's Theorem.

#### Result

2 of 2

For given  $n = 14$  and  $a = 3$ , we have shown that  $a^{\phi(n)} \pmod{n} = 1 \pmod{n}$ , and so for  $n = 14$  and  $a = 5$ .

Click for the solution.

23. a

We know that

$$U_{41} := \{x \in \mathbb{N} \mid GCD(x, 41) = 1\}.$$

Since 41 is a **prime** we have

$$U_{41} = \{1, 2, 3, 4, \dots, 40\} = \mathbb{Z}_{41} \setminus \{0\}.$$

We need to show that there exists an element  $a \in U_{41}$  such that

$$a^2 \equiv -1 \pmod{41}.$$

By **Fermat's theorem**,

$$\text{for any } x \in U_{41}, \quad x^{40} \equiv 1 \pmod{41}.$$

It follows that order of  $x$  in  $U_{41}$  divides 40. Then **the possible orders** of  $x$  in  $U_{41}$  are 1, 2, 4, 5, 8, 10, 20, 40.

We will be done if we show that there exists an element  $a$  in  $U_{41}$  such that order of  $a$  is 4.

Let us take the element 9 in  $U_{41}$ . Then,

$$9^4 \equiv 1 \pmod{41} \text{ and } 9^2 = 81 \equiv -1 \pmod{41}.$$

Hence 9 in  $U_{41}$  is the required element.

## Result

2 of 2

Let us look at 9 in  $U_{41}$ , we have  $9^2 \equiv -1 \pmod{41}$ . Click for the complete proof.

24. a

**Given:**  $p$  is a prime of the form  $4n + 3$ , where  $n$  is an integer.

**To Prove:** The equation

$$x^2 \equiv -1 \pmod{p}$$

has no solution.

**Proof:** Given that  $p = 4n + 3$ .

Note that if  $x$  is not divisible by  $p$ , then by **Fermat's Theorem** we have

$$(x^2)^{2n+1} = x^{4n+2} \equiv 1 \pmod{p}$$

If possible let us assume that the equation  $x^2 \equiv -1 \pmod{p}$  has a solution.

Then

$$(x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}.$$

But this is an impossibility, since we cannot have  $-1 \equiv 1 \pmod{p}$  and this contradicts our fact.

Hence, the equation

$$x^2 \equiv -1 \pmod{p}$$

has no solution.

This completes the proof.

## Result

3 of 3

Being  $p$  is a prime of the form  $4n + 3$  we have shown a contradiction through Fermat's Theorem to conclude that

the given equation is not solvable.

[Click for the complete proof.](#)

## 25. a

We have given the group  $\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$ .

**To Prove:**  $\mathbb{Z}_n - \{0\}$  forms a group under multiplication if and only if  $n$  is prime.

**Proof:** Let us consider that  $n$  is a prime. We will show that  $(\mathbb{Z}_n - \{0\}, \cdot)$  is a group.

Trivially closure and associative property are clear, since they are basically elements from  $\mathbb{Z}$ .

**Claim:** [1] is the identity element of  $\mathbb{Z}_n - \{0\}$ .

**Proof of the Claim:** Let  $x$  be an arbitrary element of  $\mathbb{Z}_n - \{0\}$ .

Then

$$[1] \cdot [x] = [x] \cdot [1] = [x].$$

This proves the Claim.

Now **we show the existence of the inverse for each element in  $\mathbb{Z}_n - \{0\}$ .**

Let us assume  $a \in \mathbb{Z}_n - \{0\}$ . We will show the existence of an element  $b$  in  $\mathbb{Z}_n - \{0\}$  such that

$$[a][b] = [b][a] = [1].$$

Let us now define a function  $f_a : \mathbb{Z}_n - \{0\} \rightarrow \mathbb{Z}_n - \{0\}$  by the assignment

$$f_a(x) = a \cdot x.$$

Since  $\cdot$  is closed in  $\mathbb{Z}_n - \{0\}$ ,  $f_a$  is well defined.

We now show that  $f_a$  is 1 - 1.

Let us assume two elements  $x, y$  from  $\mathbb{Z}_n - \{0\}$ .

Then

$$\begin{aligned} f_a(x) &= f_a(y) \\ \implies a \cdot x &\equiv a \cdot y \pmod{n} \\ \implies a \cdot (x - y) &\equiv 0 \pmod{n} \\ \implies n | d \text{ or } n | (x - y). \end{aligned}$$

Since  $a \in \mathbb{Z}_n - \{0\}$ , we have  $n$  divides  $x - y$ . It follows that

$$x - y \equiv 0 \pmod{n} \implies [x] = [y].$$

This shows that  $f_a$  is 1 - 1.

**Since  $\mathbb{Z}_n - \{0\}$  is a finite set  $f_a$  is onto.**

Hence  $f_a$  is a bijection.

Therefore there exists an element  $b$  in  $\mathbb{Z}_n - \{0\}$ , such that

$$a \cdot b \equiv 1 \pmod{n}.$$

That is

$$[a][b] = [1].$$

This completes the proof. Hence  $(\mathbb{Z}_n - \{0\}, \cdot)$  forms a group.

## Result

3 of 3

Closure, associativity and identity property are all trivial so we have proved the existence of the inverse for each element in  $\mathbb{Z}_n - \{0\}$  by showing that for any element  $a$  in  $\mathbb{Z}_n - \{0\}$  there exists an element  $b \in \mathbb{Z}_n - \{0\}$  such that  $a \cdot b = 1 \pmod{n}$ . Click for the complete proof.

## 26. a

**Given:**  $G$  is a group and  $H$  is a subgroup of  $G$ . Let  $S$  be the set of all right cosets of  $H$  in  $G$  and  $T$  be the set of all left cosets of  $H$  in  $G$ .

**To Prove:** There is an one-one mapping from  $S$  onto  $T$ .

**Proof:**

It suffices to show that

**there is a bijection between the set of all distinct left cosets of  $H$  in  $G$  and the set of all distinct right cosets of  $H$  in  $G$**

Let us consider an element  $a$  in  $G$ .

Let us define a mapping

$$f : S \rightarrow T$$

by the assignment

$$f(Ha) = a^{-1}H, \quad Ha \in S.$$

First we show that the mapping  $f$  is **well defined** in the sense that if

$$Hx = Ha \text{ then } x^{-1}H = a^{-1}H.$$

Now,

$$\begin{aligned} Hx = Ha &\implies x \in Ha \\ &\implies xa^{-1} \in H \\ &\implies (x^{-1})^{-1}a^{-1} \in H \\ &\implies a^{-1} \in x^{-1}H \\ &\implies a^{-1}H = x^{-1}H. \end{aligned}$$

Therefore

$f$  assigns a unique coset in  $T$  to a unique coset in  $S$

We now prove that  $f$  is **one-one**.

Let  $Ha, Hb \in S$  and  $Ha \neq Hb$ .

Then,

$$\begin{aligned} f(Ha) = f(Hb) &\implies a^{-1}H = b^{-1}H \\ &\implies a^{-1} \in b^{-1}H \\ &\implies (b^{-1})^{-1}a^{-1} \in H \\ &\implies ba^{-1} \in H \\ &\implies b \in Ha \implies Hb = Ha. \end{aligned}$$

So,

$$Ha \neq Hb \implies f(Ha) \neq f(Hb).$$

This proves that

$f$  is **one-one**.

In order to prove the  $f$  is **onto**, let us take an element  $aH$  in  $T$ .

The pre-image of  $aH$  is  $Ha^{-1}$  in  $S$ , since

$$f(Ha^{-1}) = (a^{-1})^{-1}H = aH.$$

Therefore,

***f* is onto.**

Consequently,  $f$  is a **bijection** from  $S$  to  $T$ .

Hence we get an one-one mapping  $S$  onto  $T$ .

This completes the proof.

## Result

4 of 4

Considering a mapping  $f$  from  $S$  to  $T$  by  $f(Ha) = a^{-1}H$ ,  $Ha \in S$ , we have proved that  $f$  is an one-one mapping from  $S$  onto  $T$ .

[Click for the complete proof.](#)

## 27. a

**Given:**  $G$  is a group and  $H$  is a subgroup of  $G$  and  $aH = bH \implies Ha = Hb$  in  $G$ .

**To Prove:**  $aHa^{-1} = H$  for every  $a \in G$ .

**Proof:** By the given condition we have  $aH = bH$ .

Let  $x \in aH$ , then there exists  $h_1 \in H$  such that

$$x = ah_1.$$

Then,  $x \in bH$ . So there exists  $h_2 \in H$  such that

$$x = bh_2.$$

Now,

$$ah_1 = bh_2 \implies b^{-1}a = h_2h_1^{-1} \implies b^{-1}a \in H \implies (b^{-1}a)^{-1} \in H \implies a^{-1}b \in H.$$

Thus,

$$aH = bH \implies a^{-1}b \in H.$$

Now we have  $Ha = Hb$ . **Similarly by the aforesaid argument** it follows that

$$Ha = Hb \implies ab^{-1} \in H.$$

So,  $a^{-1}b \in H$  forces  $ab^{-1} \in H$ .

We need to show that  $aHa^{-1} = H$  for every  $a \in G$ .

Let us take an element  $x \in aHa^{-1}$ . Then there exists an element  $h$  in  $H$  such that

$$x = aha^{-1}.$$

Now, we have

$$\begin{aligned} x = aha^{-1} &\implies h = a^{-1}xa \\ &\implies (x^{-1}a)^{-1}a \in H \\ &\implies (x^{-1}a)a^{-1} \in H \\ &\implies x^{-1} \in H \implies x \in H. \end{aligned}$$

Therefore,

$$aHa^{-1} \subset H.$$

Now let  $y \in H$ . Then we have

$$a^{-1}xa \in a^{-1}Ha \subset H \implies a^{-1}xa = h, \text{ for some } h \text{ in } H.$$

So,

$$a^{-1}xa = h \implies x = aha^{-1} \implies x \in aHa^{-1}.$$

It yields that

$$H \subset aHa^{-1}.$$

Consequently,

$$aHa^{-1} = H, \text{ for every } a \in G.$$

This completes the proof.

## Result

3 of 3

By considering  $aH = bH$  forces  $Ha = Hb$  in  $G$  we have proved that  $a^{-1}b \in H$  forces  $ab^{-1} \in H$  and then using this we have proved that  $aHa^{-1} \subset H$  and vice versa. Click for the complete proof.

## 28. a

**Given:**  $G$  is a cyclic group of order  $n$ .

**To prove:** There are  $\phi(n)$  generators of  $G$ .

**Proof:** Let us consider  $G$  be generated by  $x$ , i.e.

$$G := \{1, x, x^2, \dots, x^{n-1}\}.$$

Assume any element  $a$  from  $G$ . Then

$$a = x^i, \text{ for some } 1 \leq i \leq n - 1.$$

**Claim:**  $a$  is a generator of  $G$  if and only if  $\text{GCD}(i, n) = 1$ .

**Proof of the claim:** Let  $a$  be a generator of  $G$ . Then  $1 \leq r < n$ .

Since  $x^i$  is a generator and  $x \in G$ ,

$$x = (x^i)^k, \text{ for some integer } k.$$

Hence,

$$x^{ik-1} = 1, \text{ 1 being the Identity element of } G.$$

Since the order of  $x$  is  $n$ ,  $n$  is a divisor of  $ik - 1$ . So,

$$ik - 1 = -sn, \text{ for some integer } s.$$

That is,

$$ik + sn = 1, \text{ where } k \text{ and } s \text{ are integers}$$

and this implies

$$\text{GCD}(i, n) = 1.$$

Conversely, let  $\text{GCD}(i, n) = 1$ .

Then

**there exist integers  $k$  and  $l$  such that**

$$ik + nl = 1.$$

Then,

$$x^{ki} = x \implies x^i \text{ is a generator of } G.$$

Hence,  $a$  is a generator of  $G$ . And this proves the Claim.

Since there are  $\phi(n)$  elements which are less than  $n$  and prime to  $n$ . So, there exists  $\phi(n)$  generators of  $G$ , and they are precisely

$$\{x^i \mid \text{GCD}(i, n) = 1\}.$$

This completes the proof.

## Result

3 of 3

$G$  being cyclic with generator  $x$ , we have shown that for a positive integer  $i$ ,  $x^i$  is also a generator of  $G$  iff  $i$  is less than  $n$  and prime to  $n$ . Click for the complete proof.

29. a

**Given:** Let  $G$  be a group and for elements  $a, b \in G$  we have

$$aba^{-1} = b^i.$$

**To Prove:**  $a^rba^{-r} = b^{i^r}$  for all positive integers  $r$ .

**Proof:** We will use induction on  $r$  to prove this.

If  $r = 1$  then our statement is trivially true.

Let us assume that our statement true for all integers  $n$  less than  $r$ . We will show that, the statement is true for  $r$ .

It suffices to show that

$$a^rba^{-r} = b^{i^r}.$$

Now by Induction hypothesis we have

$$a^{r-1}ba^{-(r-1)} = b^{i^{r-1}}.$$

This implies

$$\begin{aligned} & (a^{r-1}ba^{-(r-1)})^i = b^{i^r} \\ \implies & a^{r-1}b^i a^{-(r-1)} = b^{i^r} \\ \implies & a^{r-1}aba^{-1}a^{-(r-1)} = b^{i^r}, \text{ since } b^i = aba^{-1} \\ \implies & a^rba^{-r} = b^{i^r}. \end{aligned}$$

Therefore,

**our statement is true for  $r$  whenever it is true for all integers less than  $r$ .**

Hence, by **Principle of Induction** we proved that

$$a^rba^{-r} = b^{i^r}, \text{ for all integers } r.$$

This completes the proof.

## Result

2 of 2

We have used induction on  $r$  to show that  $a^rba^{-r} = b^{i^r}$  for all positive integers  $r$ .

[Click for the complete proof.](#)

## 30. a

**Given:**  $G$  is a group and  $a, b$  are elements of  $G$  such that

$$a^5 = e \text{ and } aba^{-1} = b^2.$$

**To Find:** Order of  $b$  if  $b \neq e$ .

**Solution:** We have

$$a^5 = e \text{ and } aba^{-1} = b^2 \text{ for } a, b \in G.$$

Now,

$$\begin{aligned} a^2ba^{-2} &= a(aba^{-1})a^{-1} \\ &= ab^2a^{-1} \\ &= aba^{-1}aba^{-1} \\ &= (aba^{-1})(aba^{-1}) \\ &= b^2b^2 = b^2. \end{aligned}$$

Again,

$$\begin{aligned} a^3ba^{-3} &= a(a^2ba^{-2})a^{-1} \\ &= ab^4a^{-1} \\ &= aba^{-1}aba^{-1}aba^{-1}aba^{-1} \\ &= (aba^{-1})(aba^{-1})(aba^{-1})(aba^{-1}) \\ &= b^2b^2b^2 = b^2. \end{aligned}$$

By similar way we will get,

$$a^4ba^{-4} = b^2 \text{ and } a^5ba^{-5} = b^2.$$

Therefore,

$$\begin{aligned} a^5ba^{-5} &= b^2 \\ \implies ebe^{-1} &= b^{32}, \text{ since } a^5 = e \\ \implies b^{31} &= e. \end{aligned}$$

Since  $b \neq e$  and 31 is a prime, it follows that order of  $b$  must be 31.

Here we are done.

## Result

Hence the order of the element  $b$  is 31.

[Click for the detailed solution.](#)

31. a

**Given:**  $o(a) = m$  and  $a^s = e$ ,  $e$  being the identity element.

**To Prove:**  $m$  divides  $s$ .

**Proof:** We have integers  $m$  and  $s$ . So by **Division Algorithm** there exist integers  $q$  and  $r$  such that

$$s = qm + r, \text{ where } 0 \leq r < m.$$

We will propose to prove that  $r = 0$ .

If possible, let  $r \neq 0$ .

Now,

$$a^s = e \implies a^{qm+r} = e \implies a^{qm} \cdot a^r = e \implies (a^m)^q \cdot a^r = e \implies a^r = e.$$

But by the given condition,

$$o(a) = m$$

that is,  $m$  is the **least positive integer** such that

$$a^m = e.$$

So,  $a^r = e$  can not be possible, since  $r < m$ .

So, we arrive at a contradiction. It follows that  $r = 0$ .

Therefore,

$$s = qm \implies m | s.$$

This completes the proof.

## Result

$m$  and  $s$  being integers, we have used division algorithm to show that  $m$  divides  $s$ .

[Click for the detailed proof.](#)

## 32. a

**Given:**  $G$  is a finite group,  $H$  is a subgroup of  $G$   $f(a)$  be a least positive  $m$  such that

$$a^m \in H.$$

**To Prove:**  $f(a) | o(a)$ .

**Prove:** Let us assume that

$$o(a) = n.$$

Then by **Division Algorithm**, there exist  $q$  and  $r$  such that

$$n = qf(a) + r, \text{ where } 0 \leq r < f(a).$$

Since  $o(a) = n$ , we have

$$\begin{aligned} a^n &= e \implies (a)^{qf(a)} \cdot a^r = e \\ &\implies (a^{f(a)})^q \cdot a^r = e \end{aligned}$$

Now,

$$a^{f(a)} \in H \implies (a^{f(a)})^q \in H \implies a^r \in H, \text{ as } e \in H.$$

The **minimality** of  $f(a)$  that  $a^{f(a)} \in H$ , forced  $r = 0$ .

It follows that

$$n = qf(a).$$

Therefore,

$$f(a) \mid o(a).$$

This completes the proof.

## Result

2 of 2

Considering  $o(a) = n$  and applying Division algorithm we have shown that  $a^r \in H$  for some  $r < f(a)$ , contradicts the minimality of  $f(a)$ , hence the result follows by  $r = 0$ .

Click for the complete proof.

### 33. a

We have that

$$s = f^p(s) = f^{p-j}(f^j(s)) = f^{p-j}(s) = f^{-j}(f^p(s)) = f^{-j}(s)$$

and

$$s = i(s) = f^{-p}(f^p(s)) = f^{-p}(s)$$

then we obtain that for the arbitrary integers  $m$  and  $n$

$$f^{mp+nj}(s) = s(1)$$

Further, from the fact that  $j$  and  $p$  are relatively prime and **Theorem 1.5.4.** we have that there are integers  $m_0$  and  $n_0$  such that  $1 = m_0 p + n_0 j$ .

Therefore, from (1) and preceding result we obtain

$$f(s) = f^{m_0 \cdot p + n_0 \cdot j}(s) = s$$

## Result

2 of 2

(HINT:) Use **Theorem 1.5.4.**

### 34. a

Let consider two cases

I. Assume that  $s \in S$  arbitrary such that  $f(s) = s$ . In this case we have that for an arbitrary integer  $j$   $f^j(s) = s$ .

**Therefore, in this case the orbit of  $s$  under  $f$  has only one element  $s$ .**

II. Assume that  $s \in S$  arbitrary such that  $f(s) \neq s$ . From the fact that  $f$  has order  $p$ , we obtain that for an arbitrary  $j = 1, \dots, p$

$$f^{p+j}(s) = f^j(f^p(s)) = f^j(s)$$

Therefore, in this case the orbit of  $s$  under  $f$  has less or equal  $p$  elements. If the number of elements is less than  $p$ , then there are the integers  $1 \leq i < j \leq p$  such that  $f^i(s) = f^j(s)$ . From here we obtain that

$$f^i(s) = f^j(s) = f^i(f^{j-i}(s))$$

and from the fact that  $f^i$  is bijection, must be  $f^{j-i}(s) = s$ . Now, the fact that  $1 \leq j - i < p$  and preceding problem implies  $f(s) = s$  (**CONTRADICTION!**).

**Therefore, in this case the orbit of  $s$  under  $f$  has  $p$  elements.**

## Result

2 of 2

Use the preceding problem result.

### 35. a

Note, the fact that the orbits of elements  $s_1$  and  $s_2$  under  $f$  have non empty intersection implies that they must be equal.

Preceding problem result implies that orbit of  $s$  under  $f$  has  $p$  elements if  $f(s) \neq s$ . Therefore, if  $f(s) \neq s$ , for each  $s \in S$ , then we can separate into groups of  $p$  elements, which implies  $p|n$ . (**contradiction!**)

**Hence, there exists some  $s \in S$  such that  $f(s) = s$ !**

## Result

2 of 2

Use the preceding problem results.

### 36. a

**Given:**  $a$  is an integer greater than 1 and  $\phi$  is the Euler  $\phi$ -function.

**To Prove:**  $n$  divides  $\phi(a^n - 1)$ .

**Proof:** We have  $a > 1$ . First we propose to prove that

$$\text{Gcd}(a, a^n - 1) = 1.$$

If possible, let us assume that

$$\text{Gcd}(a, a^n - 1) = d, \text{ where } d > 1.$$

Then

$$d \text{ divides } a \text{ as well as } a^n - 1.$$

Now,

$$d \text{ divides } a \implies d \text{ divides } a^n.$$

This is an impossibility, since  $d$  divides  $a^n - 1$  by our assumption. Consequently,  $d$  divides 1, which implies  $d = 1$ .

Hence we are contradict to the fact that  $d > 1$ . Therefore

$$\text{Gcd}(a, a^n - 1) = 1.$$

Then  $a \in U_{a^n - 1}$ , where  $U_n$  is a group defined by

$$U_n := \{\bar{a} \in \mathbb{Z}_n \mid \text{Gcd}(a, n) = 1\}.$$

We know that **order of an element divides the order of the group**. Here order of the group  $U_{a^n - 1}$  is  $\phi(a^n - 1)$  and  $a \in U_{a^n - 1}$ . This follows that

$$\text{o}(a) \text{ divides } \phi(a^n - 1).$$

Now in the group  $U_{a^n - 1}$  we have

$$a^n - 1 \equiv 0 \pmod{a^n - 1} \implies a^n \equiv 1 \pmod{a^n - 1}.$$

This implies

$$\text{o}(a) \text{ divides } n.$$

In order to prove the problem, it suffices to show that  $\text{o}(a) = n$ .

Let **there exists a positive integer**  $k$  with  $0 < k < n$  such that

$$a^k \equiv 1 \pmod{a^n - 1}.$$

That is

$$a^k - 1 \equiv 0 \pmod{a^n - 1}.$$

This follows that

$$a^n - 1 \text{ divides } a^k - 1,$$

which is an impossibility since  $k < n$ .

**So our assumption of the existence of such  $k$  is wrong.**

Hence  $\text{o}(a) = n$ .

Consequently we have

$$n \text{ divides } \phi(a^n - 1).$$

This completes the proof.

Considering  $a$  and  $a^n - 1$  we have proved that  $\text{Gcd}(a, a^n - 1) = 1$ , that is,  $a \in U_{a^n - 1}$  and then proved that  $\text{o}(a) = n$  which follows the result that  $n$  divides  $\phi(a^n - 1)$ . Click for the complete proof.

### 37. a

**Given:** Let  $G$  be a cyclic group of order  $n$  and  $m$  is a divisor of  $n$ .

**to Prove:** There are  $\phi(m)$  elements of order  $m$  in  $G$ .

**Proof:** To prove this, we will start with a Claim.

**Claim:** A cyclic group of finite order  $n$  has one and only one subgroup of order  $m$  for every positive divisor  $m$  of  $n$ .

**Proof of the Claim:** Let  $G = \langle a \rangle$  be a finite cyclic group of order  $n$  generated by  $a$ . Then we have

$$\text{o}(a) = n \text{ and } G = \{a, a^2, \dots, a^{n-1}, a^n (= e)\}.$$

The

**trivial group  $\{e\}$  is the only subgroup of  $G$  of order 1,**

$e$  being the identity element of  $G$ . And the **improper subgroup**  $G$  is the only subgroup of  $G$  of order  $n$ . Therefore, the claim holds for the divisors 1 and  $n$ .

Let us now assume  $1 < m < n$ . Then there exists some positive integer  $d$  satisfying  $1 < d < n$  such that

$$md = n.$$

Now,

$$a^d \in G \text{ and } \text{o}(a^d) = \frac{n}{\text{gcd}(d, n)} = \frac{n}{d} = m.$$

Therefore the cyclic subgroup  $\langle a^d \rangle$  is of order  $m$ . Let us take  $H = \langle a^d \rangle$ .

Let  $K$  be another subgroup of  $G$  such that  $\text{o}(K) = m$ .

**Since  $G$  is cyclic,  $K$  must be cyclic.**

Let  $a^p$  be a generator of  $K$ .

Then we have

$$\circ(a^p) = m.$$

But,

$$\circ(a^p) = \frac{n}{\gcd(p, n)}.$$

Therefore,

$$\gcd(p, n) = \frac{n}{m} = d.$$

This follows that

$$p = td, \text{ for some positive integer } t.$$

Therefore,

$$a^p = (a^d)^t.$$

Since  $t$  is an integer, it follows that

$$\langle a^p \rangle \subset \langle a^d \rangle \text{ that is, } K \subset H.$$

Since  $\circ(H) = \circ(K)$ ,  $K = H$  and

**this proves that  $H$  is unique.**

This proves our Claim.

Now by the given condition,  $m|n$  and  $G$  is a cyclic group of order  $n$ . Then  $G$  has a subgroup  $H$ , say, of order  $m$ .

Since  $G$  is cyclic,  $H$  is also a cyclic group of order  $m$ .

**Then  $H$  must have  $\phi(m)$  generators, that is,  $H$  has  $\phi(m)$  elements of order  $m$ .**

**Since  $H$  is the unique subgroup of  $G$  of order  $m$ , by the Claim,  $G$  has  $\phi(m)$  elements of order  $m$ .**

This completes the proof.

3 of 3

## Result

Considering  $G$  is a cyclic group of order  $n$ , we first show that  $G$  has one and only one subgroup of order  $m$  for every positive divisor  $m$  of  $n$ . Since a cyclic group of order  $M$  has  $\phi(m)$  elements of order  $m$ , follows the result that  $G$  has  $\phi(m)$  elements of order  $m$ . Click for the detailed proof.

## 38. a

We have to show that

$$\sum_{m|n} \phi(m) = n, \text{ the sum being taken for all positive divisors } m \text{ of } n.$$

Let  $m_1, m_2, \dots, m_k$  be a **complete list of positive divisors** of  $n$ .

Let us consider a cyclic group  $G$  of order  $n$ .

Since  $G$  is a finite group,

**the order of each element of  $G$  is a divisor of  $n$**

and since  $G$  is cyclic,

**for every positive divisor  $m_i$  of  $n$  there is some element in  $G$  of order  $m_i$ .**

Let us define a relation  $\rho$  on the set  $G$  by

" $a \rho b$  if and only if  $a, b \in G$  and  $o(a) = o(b)$ ".

Then clearly  $\rho$  is an **equivalence relation** on  $G$ .

$G$  is partitioned into distinct and disjoint  $\rho$  – equivalence classes

$cl(m_1), cl(m_2), \dots, cl(m_k)$ , where  $cl(m_i) = \{x \in G : o(x) = m_i\}$ .

Now,

$$G = \bigcup_{i=1}^k cl(m_i).$$

Each element of  $cl(m_i)$

**generates a cyclic subgroup of order  $m_i$**

As there is only one subgroup  $H_i$  of order  $m_i$  in  $G$  and the number of generators of the subgroup of order  $m_i$  is  $\phi(m_i)$ , it follows that

**the number of elements in  $cl(m_i)$  is  $\phi(m_i)$ .**

Thus,

$$G = \bigcup_{i=1}^k cl(m_i) \text{ gives } n = \sum_{i=1}^k \phi(m_i), \text{ i.e. } n = \sum_{m|n} \phi(m).$$

This completes the proof.

## Result

Click for the proof.

### 39. a

**Given:**  $G$  is a finite abelian group of order  $n$  in which the number of solutions in  $G$  of the equation  $x^m = e$  is at most  $m$  for every positive integer  $m$  dividing  $n$ .

**To Prove:**  $G$  is cyclic.

#### Step 2

2 of 4

**Proof:** We first define **exponent** of  $G$ .

In a finite group  $G$ , each element is of finite order. The highest possible of an element of  $G$  is called the **exponent** of  $G$ .

**Lemma:** The order of every element of a finite abelian group  $G$  is a divisor of the **exponent** of  $G$ .

**Proof of the lemma:** Let the **exponent** of  $G$  be  $k$ .

Let  $a \in G$  and order of  $a$  is  $d$ .

Clearly,  $d \leq k$ .

If  $d$  is not a divisor of  $k$  then the *l.c.m* of  $d, k$  is greater than  $k$ .

Since  $G$  is abelian, there exists an element  $c$  in  $G$  such that order of  $c$  is *l.c.m* of  $d, k$ .

This implies order of  $c$  is greater than the exponent of  $G$ , an impossibility.

Therefore  $d$  is a divisor of  $k$ .

**This proves the Lemma.**

Now back to the main question.

Given that order of  $G$  is  $n$  and let us assume  $n_1$  be the **exponent** of  $G$ .

Then  $n_1 \leq n$ .

$G$  will be cyclic if there exists an element  $b$  in  $G$  such that order of  $b$  is  $n$ .

Because  $n_1$  is the exponent of  $G$ , the order of every element of  $G$  is a divisor of  $n_1$ .

Therefore, for every  $x \in G$ ,  $x^{n_1} = e$  holds.

So the equation  $x^{n_1} = e$  has  $n$  solutions in  $G$ .

By the given condition  $n \leq n_1$ .

Consequently,  $n = n_1$ .

Therefore there exists an element  $c$  in  $G$  such that

*order of  $c = n_1 = n$ .*

Now *order of  $c = n$*  implies  $G$  is a cyclic group generated by  $c$ .

This completes the proof.

## Result

Click for the proof.

### 40. a

We have that  $U_p$  is a finite abelian group of order  $p - 1$ . By **exercise 39** if the equation  $x^m \equiv 1 \pmod{p}$  has at most  $m$  solutions in  $U_p$  for all divisors  $m$  of  $p - 1$  then  $U_p$  is cyclic.

We prove in general that for a polynomial  $f(x)$  of degree  $m$  the equation  $f(x) \equiv 0 \pmod{p}$  has at most  $m$  solutions modulo  $p$ . This is obvious for  $m = 1$ . Suppose that for all polynomials  $g(x)$  of degree  $d < m$  we have that  $g(x) \equiv 0 \pmod{p}$  has at most  $d$  solutions, and let  $a$  be a solution for  $f(x) \equiv 0 \pmod{p}$ . We then have that  $f(x) \equiv (x - a)g(x) \pmod{p}$  for some  $g(x)$  of degree  $m - 1$ . Since for  $m, n \in \mathbb{Z}_p$  we have that  $mn = 0$  if and only if  $a = 0$  or  $b = 0$  the solutions to  $f(x) \equiv 0 \pmod{p}$  are either  $a$  or a solution to  $g(x) \equiv 0 \pmod{p}$ . By assumption  $g(x)$  has at most  $m - 1$  solutions so  $f(x)$  must have at most  $m$  solutions.

Applying the above results to the polynomial  $f(x) = x^m - 1$  we reach our desired conclusion.

## Result

2 of 2

This follows from **exercise 39** and the fact that polynomials of degree  $m$  over  $\mathbb{Z}_p$  have at most  $m$  roots.

### 41. a

By **exercise 40** since  $p$  is prime there is some element  $a \in U_p$  of order  $p - 1$ , ie a generator for  $U_p$ . We then have that  $p - 1$  is the smallest positive integer that satisfies  $a^{p-1} \equiv 1 \pmod{p}$ . Now using the assumption that  $p = 4n + 1$  we get that  $a^{4n} \equiv 1 \pmod{p}$ . Since the square roots of  $1 \pmod{p}$  are either  $1$  or  $-1$  (because  $y^2 \equiv 1 \pmod{p}$  means that  $p$  divides  $y^2 - 1 = (y - 1)(y + 1)$ , so  $p$ , being prime, divides either  $y - 1$  or  $y + 1$ ) then  $a^{2n} \equiv \pm 1 \pmod{p}$ . But note that since  $2n < 4n = p - 1$  by the minimality of  $p - 1$  we have that  $a^{2n} \not\equiv 1 \pmod{p}$  and so  $a^{2n} \equiv -1 \pmod{p}$ . Therefore  $a^n$  is a solution for the equation  $x^2 \equiv -1 \pmod{p}$ .

## Result

2 of 2

If  $a$  is a generator of  $U_p$  then  $a^n$  is a solution for  $x^2 \equiv -1 \pmod{p}$ .

### 42. a

By Wilson's theorem (**exercise 18**) for every prime  $p$  we have that  $(p-1)! \equiv -1 \pmod{p}$ . If  $p = 4n+1$  this implies that  $(4n)! \equiv -1 \pmod{p}$ . Note also that for all  $0 \leq i < p$  we have that  $-i \equiv p-i \pmod{p}$ .

$$\begin{aligned} -1 &\pmod{p} = (4n)! \pmod{p} \\ &= \prod_{i=1}^{4n} i \pmod{p} \\ &= \prod_{i=1}^{2n} i(p-i) \pmod{p} \\ &= (-1)^{2n} \prod_{i=1}^{2n} i^2 \pmod{p} \\ &= ((2n)!)^2 \end{aligned}$$

Since  $y$  is defined as  $\left(\frac{p-1}{2}\right)!$  then  $y = (2n)!$  is a solution for the equation  $x^2 \equiv -1 \pmod{p}$ .

## Result

2 of 2

This follows from **exercise 18** and the fact that  $-i \equiv p-i \pmod{p}$  for all  $i$ .

### 43. a

**Given:**  $G = \{a_1, a_2, \dots, a_n\}$  is a finite abelian group of order  $n$  and consider an element  $x$  as

$$x = a_1 a_2 \dots a_n.$$

**To Prove:**

- (a) If  $G$  has exactly one element  $b \neq e$  such that  $b^2 = e$ , then  $x = b$ .
- (b) If  $G$  has more than one element  $b \neq e$  such that  $b^2 = e$ , then  $x = b$ .
- (c) If  $n$  is odd then  $x = e$ .

**Proof:**

- (a) By the given condition  $G$  is an abelian group and

$$G := \{a_1, a_2, \dots, a_n\}.$$

Now we have  $x = a_1 a_2 \dots a_n$ . Then

$$x^2 = (a_1 a_2 \dots a_n)^2 = (a_1 a_2 \dots a_n)(a_1 a_2 \dots a_n) = e,$$

since

**$x$  is the product of all elements of  $G$  and  $x^2$  is the product of all elements of  $G$  twice,**

**which implies inverse of each element is also there which cause the cancellation of their pairs and gives the identity.**

Therefore

$$x^2 = e.$$

Now according to the question there exists only one  $b \neq e$  in  $G$  such that  $b^2 = e$ . This follows that

$$x = b,$$

since  $x$  is not the identity element in  $G$ .

(b) According to the question  $G$  has more than one element  $b \neq e$  such that  $b^2 = e$ . Let us assume  $a \in G$  with  $a \neq b$  such that  $a^2 = e$ .

Since  $G$  is abelian, we have

$$(ab)^2 = (ab)(ab) = a^2b^2 = e.$$

If  $ab = e$  then we have

$$a = b^{-1} \implies a = b,$$

which is an impossibility.

So,  $ab \neq e$  but  $(ab)^2 = e$ .

In this way we can construct new elements like above property. By proceeding like this way we can conclude that

$$\text{for every } g \text{ in } G, g^2 = e.$$

That is,

$$g = g^{-1}, \text{ for all } g \in G.$$

Now by the given condition  $x = a_1a_2..a_n$ , product of all the elements of  $G$ .

We will propose to prove that  $x = e$ .

If possible, let us assume  $x \neq e$ . That is, there exists an element  $a_k$  in  $G$  such that  $x = a_k$ .

Then

$$\begin{aligned} x &= a_1a_2....a_n \\ \implies a_k &= a_1a_2..a_{k-1}a_k a_{k+1}...a_n \\ \implies e &= a_1a_2...a_{k-1}a_{k+1}...a_n, \end{aligned}$$

Which is an impossibility, **since each element is inverse of itself**. So our assumption is wrong. Hence

---


$$x = e.$$

(c) According to the question we have

$$x = a_1a_2....a_n.$$

Then

$$\begin{aligned} x^2 &= (a_1a_2....a_n)^2 \\ &= (a_1a_2....a_n)(a_1a_2....a_n) \\ &= e, \text{ by (a).} \end{aligned}$$

we will endeavor to show that  $x = e$ .

If possible, let  $x \neq e$  in  $G$ .

Since  $x^2 = e$  in  $G$  and  $x \neq e$ , it follows that order of  $x$  is 2.

By the given condition, order of the group  $G$  is odd, that is,  $n$  is odd. Now we know that,

**order of each element in a group must divide the order of the group.**

Here,  $x \in G$  has order 2 and order of  $G$  is odd. Which contradict our fact that 2 divides an odd integer. So our assumption that  $x \neq e$  is wrong.

Hence  $x = e$ . This completes the proof.

## Result

4 of 4

For three problems the main idea is to show  $x^2 = e$ , the identity element. Then we have proved the by considering the main fact  $x = a_1a_2...a_n$ . Click for the detailed proof.

## Section 2–5

1. a

(a)  $\varphi$  is a homomorphism:

$$\begin{aligned}\varphi(a+b) &= [a+b] \\ &= [a] + [b] \\ &= \varphi(a) + \varphi(b)\end{aligned}$$

Kernel of  $\varphi$  is  $n\mathbb{Z} = \{a \in \mathbb{Z} \mid n|a\}$ . If  $a \in n\mathbb{Z}$  then  $a \equiv 0 \pmod{n}$  and so  $\varphi(a) = [a] = [0]$ . On the other hand if  $a \in \text{Ker } \varphi$  then  $[a] = [0]$  so that  $a \equiv 0 \pmod{n}$  and so  $a \in n\mathbb{Z}$ .

Since  $0 \neq n$  but  $\varphi(0) = \varphi(n)$  this homomorphism is not 1-to-1, and since for all  $[a] \in \mathbb{Z}_n$  we have  $\varphi(a) = [a]$  we have that  $\varphi$  is onto.

(b)  $\varphi$  is not in general a homomorphism:

$$\begin{aligned}\varphi(a * b) &= (a * b)^{-1} \\ &= b^{-1} * a^{-1} \\ \varphi(a) * \varphi(b) &= a^{-1} * b^{-1}\end{aligned}$$

Therefore  $\varphi$  is a homomorphism if and only if  $a^{-1} * b^{-1} = b^{-1} * a^{-1}$  which is equivalent to  $ab = ba$ , ie if and only if  $G$  is abelian.

(c) As seen in the last item, if  $G$  is assumed to be abelian then  $\varphi$  is a homomorphism. If  $\varphi(a) = \varphi(b)$  then  $a^{-1} = b^{-1}$  which is equivalent to  $a = b$ , therefore  $\varphi$  is 1-to-1 and its kernel is  $\{e\}$ . Since for all  $a \in G$  we have  $\varphi(a^{-1}) = (a^{-1})^{-1} = a$  this homomorphism is onto.

(d)  $\varphi$  is a homomorphism. Let  $a, b \in \mathbb{R} - \{0\}$ . If  $\varphi(a) = \varphi(b)$  then  $a$  and  $b$  have the same sign and so  $ab$  is positive. Since  $1^2 = 1 = (-1)^2$  we have that  $\varphi(ab) = 1 = \varphi(a)\varphi(b)$ . If  $\varphi(a) \neq \varphi(b)$  then  $a$  and  $b$  have opposite signs and so  $ab$  is negative. Since  $(-1)1 = -1 = 1(-1)$  we have that  $\varphi(ab) = -1 = \varphi(a)\varphi(b)$ .

$\varphi(a) = 1$  if and only if  $a > 0$ , so the kernel of  $\varphi$  is the set  $\mathbb{R}_+$  of positive real numbers. Therefore  $\varphi$  is not 1-to-1. Since  $\varphi(1) = 1$  and  $\varphi(-1) = -1$  we have that  $\varphi$  is onto.

(e)  $\varphi$  is not in general a homomorphism. Consider for instance the group  $D_4$  of symmetries of a square,  $r$  the 90 counterclockwise rotation,  $f$  the vertical reflection and  $n = 2$ . Then  $(rf)^2 = id$  and  $r^2f^2 = r^2$  so  $\varphi(x) = x^2$  is not a homomorphism.

### Result

Only the pairings in (a), (c) and (d) are homomorphisms.

2. a

**Given:**  $G_1$ ,  $G_2$  and  $G_3$  are three groups.

**To Prove:**

- (a)  $G_1 \simeq G_1$
- (b)  $G_1 \simeq G_2 \implies G_2 \simeq G_1$ .
- (c)  $G_1 \simeq G_2$  and  $G_2 \simeq G_3 \implies G_1 \simeq G_3$ .

**Proof:**

(a) Let us consider the identity homomorphism on  $G_1$  as

$$id : G_1 \rightarrow G_1.$$

Trivially an identity map is 1 – 1 and onto in  $G_1$ . So,  $id : G_1 \rightarrow G_1$  is an isomorphism between  $G_1$  to itself. Hence,

$$G_1 \simeq G_1.$$

(b) Since,  $G_1 \simeq G_2$  there exists an isomorphism between  $G_1$  and  $G_2$

say,  $\phi$ .

$\phi : G_1 \rightarrow G_2$  is an isomorphism  $\implies \phi^{-1}$  exists and it's also a bijective homomorphism, hence an isomorphism. Therefore,

$$\phi^{-1} : G_2 \rightarrow G_1$$

is an isomorphism implies

$$G_2 \simeq G_1.$$

(c) According to the question,

$$G_1 \simeq G_2 \text{ and } G_2 \simeq G_3.$$

So, there exist isomorphisms  $\phi : G_1 \rightarrow G_2$  and  $\psi : G_2 \rightarrow G_3$ .

Let us now consider the map

$$\rho : G_1 \rightarrow G_3$$

by the assignment  $\rho = \psi\phi$ , composition of  $\phi$  and  $\psi$ .

Now,

$$\rho(ab) = (\psi\phi)(ab) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi\phi)(a)(\psi\phi)(b)$$

for all  $a, b \in G_1$ .

Hence  $\psi\phi$  is a **group homomorphism**.

Since, both of  $\psi$  and  $\phi$  are

**bijective, it follows that  $\psi\phi$  is bijective.**

Consequently,  $\psi\phi$  is an isomorphism, i.e.  $\rho$  is an isomorphism from  $G_1$  to  $G_3$ .

Hence,

$$G_1 \simeq G_3.$$

This completes the proof.

## Result

4 of 4

(a) Considering identity map from  $G_1$  to itself, we have proved that  $G_1 \simeq G_1$ .

(b) Being  $G_1 \simeq G_2$  and  $\phi$  being an isomorphism, we consider the map  $\phi^{-1}$  to show that  $G_2 \simeq G_1$ .

(c) Since  $G_1 \simeq G_2$ ,  $G_2 \simeq G_3$  and  $\phi, \psi$  be the respective isomorphism, we consider the composition map  $\psi\phi$  to show that  $G_1 \simeq G_3$ .

Click for the detailed proof.

## 3. a

(a)

The function  $L_a$  by definition has domain and codomain  $G$ , we need to further show that it is one-on-one and onto.

To prove that it is one-to-one, let  $g_1, g_2 \in G$ , now if we have  $L_a(g_1) = L_a(g_2)$  then  $g_1a^{-1} = g_2a^{-1}$ , and so by cancellation property in groups we have  $g_1 = g_2$ , showing that  $L_a$  is one-to-one.

To show that it is onto, let  $g$  be an arbitrary element of  $G$ . Then since  $a$  is also in  $G$ , we have that  $ga \in G$ , so  $L_a(ga) = gaa^{-1} = g$ , showing that  $g$  is in the image of  $G$ .

(b) We have

$$\begin{aligned} L_a L_b(x) &= L_a(L_b(x)) \\ &= L_a(xb^{-1}) \\ &= xb^{-1}a^{-1} \\ &= x(ab)^{-1} \\ &= L_{ab}(x) \end{aligned}$$

for all  $x \in G$ , where we used the fact that  $(ab)^{-1} = b^{-1}a^{-1}$ .

**Step 3**

3 of 4

(c) Recall that a **monomorphism is a one-to-one homomorphism**. To show that  $\psi$  is one-to-one, suppose that  $\psi(a) = \psi(b)$ , i.e.  $L_a = L_b$ , so  $L_a$  and  $L_b$  are equal as functions, and in particular they're equal at all the points of their domain, including the identity  $1_G \in G$ , so that

$$a^{-1} = 1_G a^{-1} = L_a(1_G) = L_b(1_G) = 1_G b^{-1} = b^{-1},$$

where  $a^{-1} = b^{-1}$  implies that  $a = b$ . The fact that  $\psi$  is a homomorphism follows directly from the (b) part, where we proved that  $\psi(ab) = \psi(a)\psi(b)$ .

**Result**

4 of 4

- Cancellation property of groups is used to prove it is one-to-one, while considering  $L_a(ga) = g$  for any  $g \in G$  gives us surjectivity.
  - We write out the composition and note that the equality holds.
- We use (b) where it was proved that  $\psi$  is a homomorphism as well as give a proof of one-to-oneness by considering functions values at the identity of  $G$ .

[Click for more details.](#)

4. a

Let  $a, b \in G$  be two arbitrary elements, then for an arbitrary  $x \in G$  we have that

$$T_a L_b(x) = T_a(L_b(x)) = T_a(xb^{-1}) = axb^{-1} \quad (1)$$

and

$$L_b T_a(x) = L_b(T_a(x)) = L_b(ax) = axb^{-1} \quad (2)$$

Therefore, (1), (2) and the fact that  $x \in G$  is arbitrary gives us that

$$L_b T_a = T_a L_b$$

Hence, the proof!

### Result

For an  $x \in G$  arbitrary prove that  $L_b T_a(x) = T_a L_b(x)$

## 5. a

For an arbitrary  $a \in G$ , acting on identity element  $e \in G$  we obtain

$$aV(e) = T_a(V(e)) = V(T_a(e)) = V(a) \quad (1)$$

Therefore, if  $V = L_b$  for some  $b \in G$ , identity (1) gives that must be

$$b = (V(e))^{-1} \quad (2)$$

Let  $x \in G$  be an arbitrary element, then using (1) we obtain

$$V(x) = V(ex) = V(xx^{-1}x) = xV(x^{-1}x) = xV(e) = L_{(V(e))^{-1}}(x)$$

Therefore, the fact that  $x \in G$  is an arbitrary element gives

$$V = L_{(V(e))^{-1}}$$

The proof!

### Result

Conclude that  $b = (V(e))^{-1}$ .

## 6. a

**Given:**  $G$  and  $G'$  are two groups and

$$\phi : G \rightarrow G'$$

is a homomorphism.

**To Prove:**  $\phi(G)$  is a subgroup of  $G'$ .

**Proof:**  $\phi(G)$  is a non-empty subset of  $G'$ , since  $e_{G'} (= \phi(e_G)) \in \phi(G)$ .

Let  $a' \in \phi(G)$  and  $b' \in \phi(G)$ .

Then there exists elements  $a, b$  in  $G$  such that

$$\phi(a) = a' \text{ and } \phi(b) = b'.$$

Also we have,

$$ab^{-1} \in G.$$

Now,

$$\begin{aligned} a'(b')^{-1} &= \phi(a)\phi(b)^{-1} \\ &= \phi(a)\phi(b^{-1}) \\ &= \phi(ab^{-1}) \in \phi(G) \end{aligned}$$

Therefore,

$$a', b' \in \phi(G) \implies a'b'^{-1} \in \phi(G).$$

Hence,  $\phi(G)$  is a subgroup of  $G'$ .

This completes the proof.

## Result

Considering  $a', b'$  in  $\phi(G)$  we have proved that  $a'b'^{-1} \in \phi(G)$ .

[Click for the detailed proof.](#)

## 7. a

**Given:**  $G$  and  $G'$  are two groups with

$$\phi : G \rightarrow G'$$

is a homomorphism.

**To Prove:**  $\phi$  is a monomorphism if and only if  $\text{Ker}(\phi) = (e)$ .

**Proof:** Let us assume  $\phi$  is a **monomorphism**.

Then,

$$\phi(x) = \phi(y) \implies x = y, \text{ for any } x, y \in G.$$

Now,

$$\text{Ker}(\phi) := \{g \in G \mid \phi(g) = e_{G'}\}.$$

Let,  $x \in \text{Ker}(\phi)$ .

Then

$$\phi(x) = e_{G'} = \phi(e_G) \implies x = e_G, \text{ as } \phi \text{ is 1-1.}$$

So,  $\text{Ker}(\phi) = (e)$ .

Conversely, let us assume  $\text{Ker}(\phi) = (e)$ .

**We need to show that  $\phi$  is 1 - 1.**

Let us consider two elements  $x, y \in G$  such that  $\phi(x) = \phi(y)$ .

Then,

$$\phi(x) = \phi(y) \implies \phi(xy^{-1}) = e_{G'}, \text{ as } \phi \text{ is a homomorphism.}$$

This yield's that

$$\begin{aligned} xy^{-1} &\in \text{Ker}(\phi) \\ \implies xy^{-1} &= e, \text{ since } \text{Ker}(\phi) = (e) \\ \implies x &= y. \end{aligned}$$

Hence,

$$\phi(x) = \phi(y) \implies x = y.$$

So,  $\phi$  is 1 – 1. Hence a monomorphism.

This completes the proof.

## Result

Considering  $\phi$  is 1 – 1 we have proved that  $\text{Ker}(\phi) = (e)$ , and vice-versa.

[Click for the complete proof.](#)

## 8. a

Let  $G$  be a group of real numbers with " + " as operation. Let  $G'$  be the group of positive real number with " ." as operation. We need to give an isomorphism between  $G$  and  $G'$ . Let  $\phi : G \rightarrow G'$  as follows :  $\phi(x) = e^x$ . This is clearly homomorphism. Because,  $\phi(x + y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$ . Clearly  $e^x$  is one-one and onto. so, this is the required isomorphism.

## 9. a

Question 2.5.9 Verify that if  $G$  is the group  $G = \{T_{a,b} | a, b \in \mathbb{R}, a \neq 0\}$ , and  $H = \{T_{a,b} \in G | a \in \mathbb{Q}\}$ , then  $H \triangleleft G$ , the dihedral group of order 8.

### Step 2

2 of 6

SOLUTION

To show something is a normal subgroup, we must show it is a subgroup (closed under multiplication and closed under inverses) and we must prove that for any  $h \in H$  and any  $g \in G$ ,  $h^g = g^{-1}hg \in H$ .

### Step 3

3 of 6

(Closed Under Multiplication)

*proof.* Let  $x, y \in H$ , then there exists  $a, c \in \mathbb{Q} - \{0\}$  and  $b, d \in \mathbb{R}$  such that  $x = T_{a,b}$  and  $y = T_{c,d}$ . Thus  $T_{a,b} \cdot T_{c,d} = T_{ac,ad+b}$ . Since  $a, c \in \mathbb{Q} - \{0\}$  and they are closed under multiplication,  $ac \in \mathbb{Q} - \{0\}$ . Therefore  $T_{ac,ad+b} \in H$ .

(Closed Under Inverses)

*proof.* Let  $x \in H$ , then there exists  $a \in \mathbb{Q} - \{0\}$  and  $b \in \mathbb{R}$  such that  $x = T_{a,b}$ . Since  $\mathbb{Q} - \{0\}$  is a group under multiplication, there exists an  $a^{-1}$ . Pick  $T_{a^{-1}, -a^{-1}b}$ . Then  $T_{a,b} \cdot T_{a^{-1}, -a^{-1}b} = T_{aa^{-1}, a(-a^{-1}b)+b} = T_{1,0}$ .

### Step 5

5 of 6

(Normal)

*proof.* Let  $h \in H$  and  $g \in G$ , then there exists  $a \in \mathbb{Q} - \{0\}$  and  $b \in \mathbb{R}$  such that  $h = T_{a,b}$  and there exists  $c, d \in \mathbb{R}$  such that  $a \neq 0$  and  $g = T_{c,d}$ . Thus  $h^g = g^{-1}hg = T_{c^{-1}, -c^{-1}d} \cdot T_{a,b} \cdot T_{c,d} = T_{c^{-1}a, c^{-1}b - c^{-1}d} \cdot T_{c,d} = T_{c^{-1}ac, c^{-1}ad + c^{-1}b - c^{-1}d} = T_{a, c^{-1}(ad + c - d)}$  with  $a \in \mathbb{Q} - \{0\}$  and  $c^{-1}(ad + c - d) \in \mathbb{R}$ . Therefore  $h^g \in H$  for arbitrary  $h, g$ . Thus  $H \triangleleft G$ .

### Result

6 of 6

See proof.

## 10. a

All elements of  $G$  are of the form  $f^i g^j$  for  $i = 0, 1$  and  $j = 0, 1, 2, 3$ . The group operation is  $(f^i g^j)(f^k g^l) = f^{i+k \text{ mod } 2} g^{(-1)^k j + l \text{ mod } 4}$  and inverses are given by  $(f^i g^j)^{-1} = f^i g^{(-1)^{i+1} j}$ . We then have that for any  $f^i g^j \in G$  and  $g^l \in H$

$$\begin{aligned} (f^i g^{(-1)^{i+1} j})g^l(f^i g^j) &= f^{i+i \text{ mod } 2} g^{(-1)^i l \text{ mod } 4} \\ &= g^{(-1)^i l \text{ mod } 4} \in H \end{aligned}$$

So  $H$  is normal in  $G$ .

### Result

2 of 2

The normal subgroup condition can be directly verified using that all elements of  $G$  are of the form  $f^i g^j$  for  $i = 0, 1$  and  $j = 0, 1, 2, 3$ , that the group operation is  $(f^i g^j)(f^k g^l) = f^{i+k \text{ mod } 2} g^{(-1)^k j + l \text{ mod } 4}$  and inverses are given by  $(f^i g^j)^{-1} = f^i g^{(-1)^{i+1} j}$ .

## 11. a

All elements of  $G$  are of the form  $f^i g^j$  for  $i = 0, 1$  and  $j = 0, 1, 2, \dots, n - 1$ . The group operation is  $(f^i g^j)(f^k g^l) = f^{i+k \bmod 2} g^{(-1)^k j + l \bmod n}$  and inverses are given by  $(f^i g^j)^{-1} = f^i g^{(-1)^{i+1} j}$ . We then have that for any  $f^i g^j \in G$  and  $g^l \in H$

$$\begin{aligned}(f^i g^{(-1)^{i+1} j})(g^l)(f^i g^j) &= f^{i+i \bmod 2} g^{(-1)^i l \bmod n} \\ &= g^{(-1)^i l \bmod n} \in H\end{aligned}$$

So  $H$  is normal in  $G$ .

## Result

2 of 2

The normal subgroup condition can be directly verified using that all elements of  $G$  are of the form  $f^i g^j$  for  $i = 0, 1$  and  $j = 0, 1, 2, 3$ , that the group operation is  $(f^i g^j)(f^k g^l) = f^{i+k \bmod 2} g^{(-1)^k j + l \bmod n}$  and inverses are given by  $(f^i g^j)^{-1} = f^i g^{(-1)^{i+1} j}$ .

12. a

### The Centre $Z(G)$ of a group $G$ is a normal subgroup of $G$ .

**Proof:** The centre

$$Z(G) := \{x \in G \mid xg = gx \text{ for all } g \in G\}$$

is a **subgroup** of  $G$ .

Let  $H = Z(G)$  and let  $a \in G$ .

We prove that  $aH = Ha$ .

Let  $p \in aH$ .

Then

$$\begin{aligned}p &= ah_1 \text{ for some } h_1 \in H \\ &= h_1 a, \text{ since } h_1 \in Z(G).\end{aligned}$$

So

$$p \in aH \implies p \in Ha$$

and therefore

$$aH \subset Ha.$$

Let  $q \in Ha$ .

Then

$$\begin{aligned}q &= h_2 a \text{ for some } h_2 \in H \\ &= ah_2, \text{ since } h_2 \in Z(G).\end{aligned}$$

So,

$$q \in Ha \implies q \in aH$$

and therefore

$$Ha \subset aH.$$

Consequently, we have  $aH = Ha$ . Hence  $Z(G)$  is normal in  $G$ .

This completes the proof.

2 of 2

## Result

For any element  $a \in G$ , we have proved that  $aZ(G) = Z(G)a$ , conclude  $Z(G)$  is a normal subgroup of  $G$ .

[Click for the detailed proof.](#)

## 13. a

Since  $G$  is assumed to be abelian  $\varphi$  is always homomorphism:

$$\varphi(ab) = (ab)^m = a^m b^m = \varphi(a)\varphi(b).$$

Since  $G$  is finite (has order  $n$ )  $\varphi$  is an isomorphism if and only if it is a monomorphism, which in its turn is equivalent to having trivial kernel. We will prove that  $\ker \varphi$  is trivial if and only if  $\gcd(m, n) = 1$ .

Suppose  $a \in \ker \varphi$ . This means  $a^m = e$ , so the order  $o(a)$  of  $a$  divides  $m$ . Note that  $o(a)$  also divides  $|G| = n$ , so  $o(a) | \gcd(m, n)$ .

If we assume now that  $\gcd(m, n) = 1$  we conclude then that every element of  $\ker \varphi$  has order 1, which means the only element of the kernel is the identity and so  $\varphi$  is an isomorphism.

For the other implication we show first by induction on the number of prime divisors (counting repeated primes) of  $|G| = n$  that for all prime divisor  $p$  of  $n$  there is some  $a \in G$  such that  $o(a) = p$ . If there is only one prime divisor  $p$  of  $n$  then  $G$  is cyclic of order  $p$  and the conclusion is trivial.

For the inductive step let  $a \in G$  be any non-identity element. If  $p$  divides  $o(a)$  then  $o(a^{\frac{o(a)}{p}}) = p$  and we are done. If  $p$  does not divide the order of  $a$  then by Lagrange's theorem it divides the number of cosets of the subgroup  $(a)$  generated by  $a$ , which has strictly less prime factors than  $n$ . Since the operation  $b(a) \cdot c(a) = bc(a)$  defines an abelian group structure on the set of cosets of  $(a)$ , so by the inductive hypothesis this group has an element of order  $p$ , in other words there is some  $b \in G$  such that  $b^p(a) = (a)$ . Now note that  $b^{o(b)}(a) = e(a) = (a)$ , which means  $p$  divides  $o(b)$  and as before we have that  $o(b^{\frac{o(b)}{p}}) = p$ . We can therefore conclude that if  $p$  is a prime that divides  $n = |G|$  then some element  $a \in G$  has order  $p$ .

Now suppose that there is some prime  $p$  that divides  $\gcd(m, n)$ . Let  $a \in G$  be an element of order  $p$ . By assumption  $p | m$ , so we have that  $\frac{m}{p} \in \mathbb{Z}_+$  and  $a^m = (a^p)^{\frac{m}{p}} = e^{\frac{m}{p}} = e$ , so  $a \in \ker \varphi$  and so  $\varphi$  is not an isomorphism. Therefore if  $\varphi$  is an isomorphism then  $\gcd(m, n) = 1$ .

2 of

## Result

$\varphi$  is an isomorphism if and only if  $\gcd(m, n) = 1$ . This requires proving that if  $G$  is an abelian group and  $p$  is a prime number that divides  $|G|$  then  $G$  has some element of order  $p$ .

## 14. a

**Given:**  $G$  and  $G'$  are two groups and  $\phi$  is an onto homomorphism as

$$\phi : G \rightarrow G'.$$

**To Prove:** If  $G$  is abelian, then  $G'$  is abelian.

## Step 2

**Proof:** Let  $a', b'$  be two elements in  $G'$ .

Since  $\phi$  is an onto homomorphism there exist elements  $a, b$  in  $G$  such that

$$\phi(a) = a' \text{ and } \phi(b) = b'.$$

Now,

$$\begin{aligned} a'b' &= \phi(a)\phi(b) = \phi(ab) \text{ since } \phi \text{ is a homomorphism} \\ &= \phi(ba) \text{ since } G \text{ is abelian} \\ &= \phi(b)\phi(a) = b'a'. \end{aligned}$$

Therefore,

$$\text{for any elements } a', b' \in G' \implies a'b' = b'a'.$$

So,  $G'$  is abelian. This completes the proof.

## Result

3 of 3

Considering any two elements  $a', b' \in G'$  we have proved that  $a'b' = b'a'$ , follows that  $G'$  is abelian.

[Click for the detailed proof.](#)

## 15. a

**Given:**  $G$  and  $G'$  are two groups and  $N$  is a normal subgroup of  $G$  and

$$\phi : G \rightarrow G'$$

is an onto homomorphism.

**To Prove:**  $\phi(N)$  is normal in  $G'$ .

**Proof:**

Since  $N$  is a subgroup of  $G$ ,  $\phi(N)$  is a **subgroup** of  $G'$ .

Let us assume  $\phi(N) = N'$ .

Let  $x' \in G'$  and  $h' \in N'$ .

Since  $\phi$  is **onto, there exist elements**  $x \in G$  and  $h \in N$   
such that

$$\phi(x) = x' \text{ and } \phi(h) = h'.$$

Now,

$$\begin{aligned} x'h'(x')^{-1} &= \phi(x)\phi(h)[\phi(x)]^{-1} \\ &= \phi(x)\phi(h)\phi(x^{-1}), \text{ since } \phi \text{ is a homomorphism} \\ &= \phi(xhx^{-1}). \end{aligned}$$

Since  $N$  is a **normal subgroup** of  $G$ ,

$$x \in G, h \in N \implies xhx^{-1} \in N$$

and therefore

$$\phi(xhx^{-1}) \in \phi(N).$$

Thus,

$$x' \in G', h' \in \phi(N) \implies x'h'(x')^{-1} \in \phi(N).$$

This proves that  $\phi(N)$  is a normal subgroup of  $G'$ .

**Result**

3 of 3

Considering elements  $x' \in G'$  and  $h' \in \phi(N)$  we have proved that  $x'h'(x')^{-1} \in \phi(N)$ , follows that  $\phi(N)$  is a normal subgroup of  $G'$ .

[Click for the complete proof.](#)

**16. a**

**Given:**  $M$  and  $N$  are two normal subgroups of a group  $G$  and define the subset  $MN$  of  $G$  as

$$MN := \{mn \mid m \in M, n \in N\}.$$

**To Prove:**  $MN$  is a normal subgroup of  $G$ .

**Proof:** Clearly,  $MN$  is a **non-empty subset** of  $G$  since

$$e \in MN, e \text{ being the identity element in } G.$$

Let us take,  $mn$  and  $m'n'$  in  $MN$ , where  $m, m' \in M$  and  $n, n' \in N$ .

Now,

$$(mn)^{-1}(m'n') = n^{-1}m^{-1}m'n' = n^{-1}m^{-1}m'nn^{-1}n' \in MN.$$

Since,  $M$  is **normal** in  $G$

$$n^{-1}m^{-1}m'n \in M.$$

Therefore,

$$mn, m'n' \in MN \implies (mn)^{-1}(m'n') \in MN.$$

So,  $MN$  is **subgroup** of  $G$ .

Now, we will show that  $MN$  is normal in  $G$ .

Let us consider  $g \in G$  and  $mn \in MN$ , where  $m \in M$  and  $n \in N$ .

Now,

$$g(mn)g^{-1} = gmeng^{-1} = (gmg^{-1})(gng^{-1}) \in MN.$$

As,  $M$  and  $N$  are **normal** in  $G$

$$gmg^{-1} \in M \text{ and } gng^{-1} \in N.$$

Therefore,

$$g \in G, mn \in MN \implies g(mn)g^{-1} \in MN.$$

Hence,  $MN$  is normal in  $G$ .

This completes the proof.

## Result

3 of 3

Firstly we have proved that  $MN$  is a subgroup of  $G$  and then considering any elements  $g$  in  $G$  and  $mn$  in  $MN$  we have shown that  $g(mn)g^{-1}$  in  $MN$ , follows the result.

Click for the complete proof.

17. a

**Given:**  $G$  is a group and  $M, N$  are two normal subgroups of  $G$ .

**To Prove:**  $M \cap N$  is a normal subgroup of  $G$ .

**Proof:** Firstly, we know that the intersection of two subgroups of  $G$  is a subgroup of  $G$ .

Hence,  $M \cap N$  is a subgroup of  $G$ . We need to show that  $M \cap N$  is normal in  $G$ .

Let us consider  $g \in G$  and  $x \in M \cap N$ .

Then

$$x \in M \text{ and } x \in N.$$

Since  $M$  is normal in  $G$ ,

$$x \in M, g \in G \implies gxg^{-1} \in M.$$

Again, since  $N$  is normal in  $G$ ,

$$x \in N, g \in G \implies gxg^{-1} \in N.$$

This follows that  $gxg^{-1} \in M \cap N$ .

Hence,

$$x \in M \cap N, g \in G \implies gxg^{-1} \in M \cap N.$$

Consequently,  $M \cap N$  is normal in  $G$ .

This completes the proof.

## Result

3 of 3

Considering  $x \in M \cap N$ ,  $g \in G$  we have proved that  $gxg^{-1} \in M \cap N$ , follows that  $M \cap N$  is normal in  $G$ .

[Click for the detailed proof.](#)

## 18. a

**Given:**  $H$  is a subgroup of a group  $G$  and  $N$  is a subset of  $G$  given by

$$N := \bigcap_{a \in G} aHa^{-1}.$$

**To Prove:**  $N$  is a normal subgroup of  $G$ .

**Proof:** Since  $H$  is a subgroup of  $G$  and  $a \in G$ ,  $aHa^{-1}$  is a subgroup of  $G$ . This implies trivially  $N$  is a subgroup of  $G$ , since **Intersection of subgroups form a subgroup**.

So, it suffices to show that  $N$  is normal in  $G$ .

Let,  $n$  in  $N$  and  $g$  in  $G$ .

Then,

$$n \in N \implies n \in \bigcap_{a \in G} aHa^{-1} \implies n \in aHa^{-1}, \text{ for all } a \in G.$$

Since,  $e \in G$  being the identity element,

$$n \in eHe^{-1} = H.$$

Now,

$$gng^{-1} \in aHa^{-1}, \text{ for all } a \in G \implies gng^{-1} \in \bigcap_{a \in G} aHa^{-1}.$$

Therefore,

$$g \in G, n \in N \implies gng^{-1} \in N.$$

So,  $N$  is a **normal subgroup** of  $G$ .

This completes the proof.

Considering arbitrary elements  $g$  in  $G$  and  $n$  in  $N$  we have proved that  $gng^{-1}$  in  $N$ , follows that  $N$  is normal in  $G$ .  
[Click for the complete proof.](#)

## 19. a

Let  $G$  be a group and  $H$  is a subgroup of  $G$ . Define  $N(H) = \{ a \in G | a^{-1}Ha = H \}$ . We have prove that  $N(H)$  is a subgroup and  $H \subset N(H)$ . Clearly  $H \subset N(H)$  because  $h^{-1}Hh \subset H$  by closure property and hence  $h^{-1}Hh = H$ . So  $h \in N(H)$ . Let  $a, b \in N(H) \implies a^{-1}Ha = H, b^{-1}Hb = H$ . Now  $(ab^{-1})^{-1}H(ab^{-1}) = b(a^{-1}Ha)b^{-1} = bHb^{-1} = H$ . So  $ab^{-1} \in N(H)$ . So  $N(H)$  is a subgroup. To prove:  $H$  is normal in  $N(H)$ . But that is by definition , because if  $a \in N(H) \implies a^{-1}Ha = H$ . So  $H$  is normal in  $N(H)$ . The last result: If  $H$  is normal in  $K$ , then we need to prove that  $K \subset N(H)$ . Now Let  $k \in K$ . We have , $k^{-1}Hk = H$  as  $H$  is normal in  $K$ . But then by definition  $K \subset N(H)$ . So we are done. So  $ab^{-1} \in N(H)$ . So  $N(H)$  is a subgroup. To prove:  $H$  is normal in  $N(H)$ . But that is by definition , because if  $a \in N(H) \implies a^{-1}Ha = H$ . So  $H$  is normal in  $N(H)$ . The last result: If  $H$  is normal in  $K$ , then we need to prove that  $K \subset N(H)$ . Now Let  $k \in K$ . We have ,  $k^{-1}Hk = H$  as  $H$  is normal in  $K$ . But then by definition  $K \subset N(H)$ . So we are done.

## Result

[See the proof](#)

## 20. a

**Given:**  $M$  and  $N$  are two normal subgroup of a group  $G$  and  $M \cap N = (e)$ .

**To Prove:**  $mn = nm$  for all  $m \in M, n \in N$ .

**Proof:** In order to show that  $mn = nm$  for all  $m \in M, n \in N$ ,  
**we will prove that**  $mnm^{-1}n^{-1} = e$  for all  $m \in M, n \in N$ .

Since  $G$  is a group  $mnm^{-1}n^{-1} \in G$ . Now  $M$  is a **normal subgroup** of  $G$  and  $m \in M$ , then

$$nm^{-1}n^{-1} \in M, \text{ since } n \in N \subset G.$$

Again,  $N$  is a **normal subgroup** of  $G$  and  $n \in N$ , then

$$mnm^{-1} \in N, \text{ since } m \in M \subset G.$$

Therefore,

$$mnm^{-1}n^{-1} = m(nm^{-1}n^{-1}) \in M, \text{ since } M \text{ is a group}$$

and

$$mnm^{-1}n^{-1} = (mnm^{-1})n^{-1} \in N, \text{ since } N \text{ is a group}$$

Hence,

$$mnm^{-1}n^{-1} \in M \cap N = (e) \implies mnm^{-1}n^{-1} = e.$$

Consequently,  $mn = nm$  for all  $m \in M$  and  $n \in N$ .

This completes the proof.

**Result**

2 of 2

Considering the element  $mnm^{-1}n^{-1}$  in  $G$ , where  $m \in M$  and  $n \in N$ , we have proved that  $mnm^{-1}n^{-1} \in M \cap N$  implies  $mnm^{-1}n^{-1} = e$ , follows that  $mn = nm$ .

[Click for the detailed proof.](#)

21. a

So we have  $|S| > 2$ . Let  $s \in S$ . Consider  $H(s) = \{f \in A(S) | f(s) = s\}$ . Clearly  $H(s) \subset A(S)$ , more generally  $H(s)$  is a subgroup of  $A(S)$ . But we want to prove that that  $H(s)$  can never be normal in  $A(S)$ . Since  $|S| > 2$ . So there exists  $a, b$  distinct such that none of them are equal to  $s$ . Consider  $f \in A(S)$  such that  $f(s) = s, f(a) = b, f(n) = n \quad \forall n \in S, n \neq a, s$ . clearly  $f \in H(s)$ . Now consider  $g \in A(S)$  such that  $g(a) = s$ . Now  $g \circ f \circ g^{-1}(s) = g(f(a)) = g(b) \neq s$  as  $g$  is bijective and  $g(a) = s$ . So,  $g \circ f \circ g^{-1} \notin H(s)$ , and hence  $H(s)$  is not normal in  $A(S)$ .

**Result**

[See the proof](#)

22. a

Let  $r \in S_3$  where  $r(x_1) = x_2, r(x_2) = x_3$  and  $r(x_3) = x_1$ . We have that  $S_3 = \{e, r, r^2, f, fr, fr^2\}$  and  $rf = f^2r$ . Leting  $H = \{e, f\}$  we have:

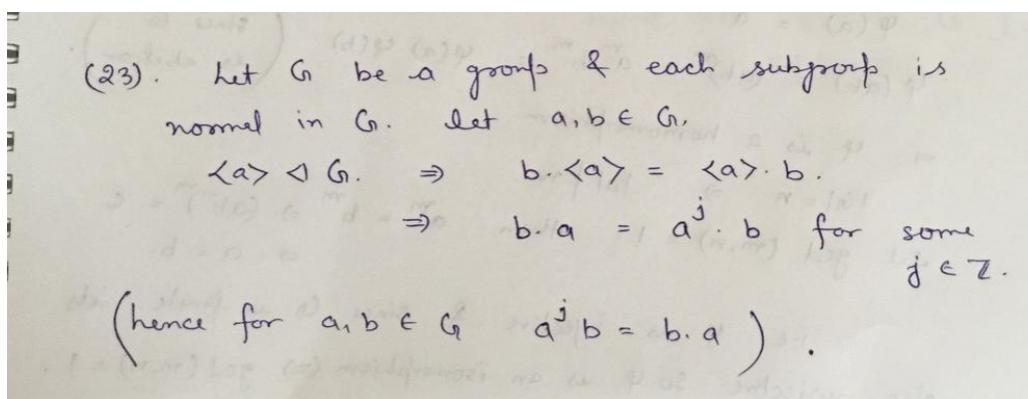
- (a) The left cosets of  $H$  are  $\{e, f\} = H, \{r, fr^2\} = rH$  and  $\{r^2, fr\} = r^2H$ .
- (b) The right cosets of  $H$  are  $\{e, f\} = H, \{r, fr\} = Hr$  and  $\{r^2, fr^2\} = Hr^2$ .
- (c) No, for instance  $rH$  is not a right coset since the only right coset that contains  $r$  is  $Hr$ , but  $fr^2 \notin Hr$ .

**Result**

2 of 2

Let  $r \in S_3$  where  $r(x_1) = x_2, r(x_2) = x_3$  and  $r(x_3) = x_1$ . We have that  $S_3 = \{e, r, r^2, f, fr, fr^2\}$  and  $rf = f^2r$ . From this we can compute the left and right cosets. We can see some left cosets are not right cosets.

23. a



## 24. a

(a) We prove the axioms for a group directly:

assoc.

$$\begin{aligned}(a_1, a_2)((b_1, b_2)(c_1, c_2)) &= (a_1, a_2)(b_1c_1, b_2c_2) \\ &= (a_1b_1c_1, a_2b_2c_2) \\ &= (a_1b_1, a_2b_2)(c_1, c_2) \\ &= ((a_1, a_2)(b_1, b_2))(c_1, c_2)\end{aligned}$$

ident.

$$\begin{aligned}(a_1, a_2)(e_1, e_2) &= (a_1e_1, a_2e_2) \\ &= (a_1, a_2) \\ (e_1, e_2)(a_1, a_2) &= (e_1a_1, e_2a_2) \\ &= (a_1, a_2)\end{aligned}$$

inv.

$$\begin{aligned}(a_1, a_2)(a_1^{-1}, a_2^{-1}) &= (a_1a_1^{-1}, a_2a_2^{-1}) \\ &= (e_1, e_2) \\ (a_1^{-1}, a_2^{-1})(a_1, a_2) &= (a_1^{-1}a_1, a_2^{-1}a_2) \\ &= (e_1, e_2)\end{aligned}$$

(b) We can see that as described  $\varphi_1$  is a homomorphism:

$$\begin{aligned}\varphi_1(a_1b_1) &= (a_1b_1, e_2) \\ &= (a_1, e_2)(b_1, e_2) \\ &= \varphi_1(a_1)\varphi_1(b_1)\end{aligned}$$

The kernel is the  $a_1 \in G_1$  such that  $\varphi_1(a_1) = (a_1, e_2)$  equals  $(e_1, e_2)$ , which is only the case if  $a_1 = e_1$  and so  $\ker \varphi_1 = \{e_1\}$ . Therefore  $\varphi_1$  is a monomorphism.

The elements of  $\varphi_1(G_1)$  are the elements of the form  $(a_1, e_2)$  for some  $a_1 \in G_1$ . Now letting  $(b_1, b_2) \in G_1 \times G_2$  we have that

$$\begin{aligned}(b_1^{-1}, b_2^{-1})(a_1, e_2)(b_1, b_2) &= (b_1^{-1}a_1b_1, e_2) \\ &= \varphi_1(b_1^{-1}a_1b_1)\end{aligned}$$

so  $\varphi_1(G_1)$  is a normal subgroup.

(c) Defining

$$\begin{aligned}\varphi_2 : G_2 &\rightarrow G_1 \times G_2 \\ a_2 &\mapsto (e_1, a_2)\end{aligned}$$

a proof analogous to the one in (b) shows  $\varphi_2$  is a monomorphism with normal image.

(d) For every  $(a_1, a_2) \in G_1 \times G_2$  we have that

$$(a_1, a_2) = (a_1, e_2)(e_1, a_2) = \varphi_1(a_1)\varphi_2(a_2)$$

so  $G = \varphi_1(G_1)\varphi_2(G_2)$ . Now suppose  $(a_1, a_2) \in \varphi_1(G_1) \cap \varphi_2(G_2)$ . The second coordinate of elements in  $\varphi_1(G_1)$  is  $e_2$ , and the first coordinate of elements in  $\varphi_2(G_2)$  is  $e_1$ , therefore  $(a_1, a_2) = (e_1, e_2)$ . Therefore the identity element is the only element in  $\varphi_1(G_1) \cap \varphi_2(G_2)$ .

(e) Define

$$\begin{aligned}\tau : G_1 \times G_2 &\rightarrow G_2 \times G_1 \\ (a_1, a_2) &\mapsto (a_2, a_1)\end{aligned}$$

This map is a homomorphism:

$$\begin{aligned}\tau((a_1, a_2)(b_1, b_2)) &= (a_2 b_2, a_1 b_1) \\ &= (a_2, a_1)(b_2, b_1) \\ &= \tau(a_1, a_2)\tau(b_1, b_2)\end{aligned}$$

It is a monomorphism since  $\tau(a_1, a_2) = (e_2, e_1)$  if and only if  $(a_1, a_2) = (e_1, e_2)$ . This monomorphism is also onto since for any  $(a_2, a_1) \in G_2 \times G_1$  we have that  $\tau(a_1, a_2) = (a_2, a_1)$ .

## Result

All conditions can be directly verified.

25. a

(a) We can verify that  $\varphi$  is a homomorphism:

$$\begin{aligned}\varphi(ab) &= (ab, ab) \\ &= (a, a)(b, b) \\ &= \varphi(a)\varphi(b)\end{aligned}$$

Also if  $\varphi(a) = \varphi(b)$  then  $(a, a) = (b, b)$ , and this is equivalent to  $a = b$ . Therefore  $\varphi$  is a monomorphism.

(b) Suppose first that  $\varphi(G)$  is normal. Let  $a, b \in G$  be any pair of elements.

Since  $\varphi(G)$  is normal we have that

$$(a^{-1}, b^{-1})\varphi(a)(a, b) = (a, b^{-1}ab)$$

is in  $\varphi(G)$ . Therefore by structure of  $\varphi(G)$  (to be precise, all elements of  $\varphi(G)$  are of the form  $(g, g)$  for some  $g \in G$ ) we have that  $a = b^{-1}ab$ , which is equivalent to  $ba = ab$ . Since  $a$  and  $b$  were chosen arbitrarily we have that  $G$  is abelian.

Now suppose  $G$  is abelian and  $a, b_1, b_2 \in G$ , then

$$\begin{aligned}(b_1^{-1}, b_2^{-1})\varphi(a)(b_1, b_2) &= (b_1^{-1}ab_1, b_2^{-1}ab_2) \\ &= (b_1^{-1}b_1a, b_2^{-1}b_2a) \\ &= (a, a) \\ &= \varphi(a)\end{aligned}$$

which is an element of  $\varphi(G)$ , therefore  $\varphi(G)$  is normal in  $W$ .

## Result

All conditions can be directly verified.

## 26. a

(a) We can verify directly that  $\psi$  is a homomorphism by computing for  $a, b \in G$  the application of  $\psi(ab)$  on an arbitrary element  $g \in G$ :

$$\begin{aligned}\psi(ab)(g) &= \sigma_{ab}(g) \\ &= abgb^{-1}a^{-1} \\ &= \sigma_a(\sigma_b(g)) \\ &= \psi(a)(\psi(b)(g)) \\ &= (\psi(a) \circ \psi(b))(g)\end{aligned}$$

which proves that  $\psi(ab) = \psi(a) \circ \psi(b)$ , and so  $\psi$  is a homomorphism.

(b) First let's prove that  $\ker \psi \subset Z(G)$ . Suppose  $a \in \ker \psi$ . This means that  $\psi(a) = id_G$  and so that for all  $g \in G$  we have that  $g = \psi(a)(g) = \sigma_a(g) = aga^{-1}$ , which is equivalent to  $ga = ag$  and so that  $a \in Z(G)$ .

Now we prove that  $Z(G) \subset \ker \psi$ . Let  $a \in Z(G)$ . As mentioned before this means that for all  $g \in G$  we have that  $ga = ag$  which is equivalent to  $g = aga^{-1} = \sigma_a(g) = \psi(a)(g)$ , therefore  $\psi(a) = id_G$  and so  $a \in \ker \psi$ .

## Result

All conditions can be directly verified.

## 27. a

**Given:**  $\theta$  is an automorphism of a group  $G$  and  $N$  is a normal subgroup of  $G$ .

**To Prove:**  $\theta(N)$  is a normal subgroup of  $G$ .

**Proof:** Let us consider the elements  $g$  in  $G$  and  $n$  in  $\theta(N)$ .

We need to show that  $gng^{-1} \in \theta(N)$ .

Since  $\theta$  is an

**automorphism of  $G$ , there exists element  $x$  in  $G$  such that  $\theta(x) = g$ .**

And, since  $n \in \theta(N)$ , there exists an element  $y$  in  $N$  such that  $\theta(y) = n$ .

Now,

$$\begin{aligned} gng^{-1} &= \theta(x)\theta(y)\theta(x)^{-1} \\ &= \theta(xyx^{-1}), \text{ since } \theta \text{ is an automorphism} \end{aligned}$$

Since,  $N$  is **normal** in  $G$

$$x \in G, y \in N \implies x y x^{-1} \in N.$$

This implies,  $\theta(xyx^{-1}) \in \theta(N) \implies gng^{-1} \in \theta(N)$ .

Hence,

$$g \in G, n \in \theta(N) \implies gng^{-1} \in \theta(N).$$

So,  $\theta(N)$  is a normal subgroup of  $G$ .

This completes the proof.

## Result

2 of 2

Considering arbitrary elements  $g$  in  $G$  and  $n$  in  $\theta(N)$ , we have shown that  $gng^{-1}$  in  $\theta(N)$  by using automorphism  $\theta$ , follows the result.

Click for the complete proof.

28. a

### The set of all automorphism of the group $G$ forms a group

Given that,  $G$  is a group.

Now,

$$\text{Aut}(G) = \{f : G \rightarrow G \mid f \text{ is an isomorphism of } G\}.$$

Let us now consider two automorphisms  $\theta, \psi \in \text{Aut}(G)$ , and consider the composition  $\theta\psi$ .

We will prove that  $\text{Aut}(G)$  is a group under the aforesaid composition.

Firstly we show that  $\theta\psi$  is a **homomorphism**. Moreover,

$$(\theta\psi)(ab) = \theta(\psi(ab)) = \theta(\psi(a)\psi(b)) = \theta(\psi(a))\theta(\psi(b)) = (\theta\psi)(a)(\theta\psi)(b)$$

for all  $a, b \in G$ .

Hence  $\theta\psi$  is a **group homomorphism**.

Since, both of  $\theta$  and  $\psi$  are **bijective**, it follows that  $\theta\psi$  is **bijective**.  
Consequently,  $\theta\psi \in \text{Aut}(G)$ .

Secondly, due to the **associativity** of  $G$ , this composition is also associative in  $\text{Aut}(G)$ .

Now, we need to check the identity element in  $\text{Aut}(G)$ .

Clearly  $Id_G : G \rightarrow G : a \mapsto a$  is an automorphism.

Since,

$$\theta Id_G = Id_G \theta, \text{ for all } \theta \in \text{Aut}(G), Id_G \text{ is the identity element.}$$

So, **the existence of the identity element** in  $\text{Aut}(G)$  is proved.

Lastly, we have to check that each  $\theta \in \text{Aut}(G)$  has an inverse in  $\text{Aut}(G)$ .

Consider the **inverse function**  $\theta^{-1}$ .

Clearly

$$\theta^{-1} \theta = Id_G = \theta \theta^{-1}.$$

So it remains to show that  $\theta^{-1}$  is a group homomorphism.

We have  $\theta : G \rightarrow G$  is a group isomorphism.

Let us consider  $a, b \in G$ . By definition there exist a unique  $x, y \in G$  such that

$$\theta(x) = a \text{ and } \theta(y) = b.$$

Hence

$$\theta^{-1}(ab) = \theta^{-1}(\theta(x) \theta(y)) = \theta^{-1}(\theta(xy)) = xy.$$

Similarly

$$\theta^{-1}(a)\theta^{-1}(b) = \theta^{-1}(\theta(x))\theta^{-1}(\theta(y)) = xy.$$

Hence

$$\theta^{-1}(ab) = \theta^{-1}(a)\theta^{-1}(b).$$

Consequently,  $\text{Aut}(G)$  forms a **group**.

This completes our proof.

## Result

3 of 3

Considering two arbitrary automorphisms  $\theta$  and  $\psi$  of  $G$  we have proved that  $\theta\psi$  and  $\theta^{-1}$  are also automorphisms,

and follows that  $\text{Aut}(G)$  is a group.

Click for the complete proof.

29. a

- [(a)] It is proven ([page 65. \(9\)](#)) that for an arbitrary group  $\mathbb{G}$  and arbitrary  $x \in \mathbb{G}$  the mapping  $\psi : \mathbb{G} \rightarrow \mathbb{G}$  defined as

$$\psi_x(g) = x^{-1}gx, g \in G$$

is an isomorphism of  $\mathbb{G}$  onto itself. So that, for an arbitrary  $x \in G$  we have that  $\psi_x(M) \subset M$ , i.e.  $x^{-1}Mx \subset M$ , and this implies that

$M$  is normal in  $\mathbb{G}$

- [(b)] We have that for an arbitrary automorphism  $\varphi$  of  $\mathbb{G}$

$$\varphi(M) \subset M \text{ and } \varphi(N) \subset N$$

this implies that

$$\varphi(M)\varphi(N) \subset MN$$

Further, we need to prove that  $\varphi(MN) = \varphi(M)\varphi(N)$ :

$$\begin{aligned}\varphi(M)\varphi(N) &= \{\varphi(m)\varphi(n) | m \in M, n \in N\} \\ &= \{\varphi(mn) | m \in M, n \in N\} = \varphi(MN)\end{aligned}$$

(c)

Let consider the Klein four group  $\mathbb{A}$  given as

$\odot$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

and its normal subgroup determine by  $N = \{e, a\}$ .

Further, we are defining mapping  $F$  of  $A$  onto itself as:

$$F(e) = e \quad F(a) = b \quad F(b) = a \quad F(c) = c$$

It is not hard to prove that  $F$  is a bijection of  $A$  onto itself, but we need to prove that it is homomorphism. Therefore, from

$$\begin{aligned}F(a \odot b) &= F(c) = c = b \odot a = F(a) \odot F(b) \\ F(a \odot e) &= F(a) = b = b \odot e = F(a) \odot F(e) \\ F(a \odot c) &= F(b) = a = b \odot c = F(a) \odot F(c) \\ F(a \odot a) &= F(e) = e = a \odot a = F(a) \odot F(a) \\ F(b \odot a) &= F(a \odot b) = F(a) \odot F(b) = F(b) \odot F(a) \\ F(b \odot e) &= F(b) = a = a \odot e = F(b) \odot F(e) \\ F(b \odot c) &= F(a) = b = a \odot c = F(b) \odot F(c) \\ F(b \odot b) &= F(e) = e = a \odot a = F(b) \odot F(b)\end{aligned}$$

we can conclude that  $F$  is homomorphism and we already have that  $F$  is bijection, this implies  $F$  is automorphism on  $\mathbb{A}$ .

We have that

$$F(N) = \{e, b\} \not\subset N$$

therefore, the normal subgroup  $N$  it is not characteristic!

## Result

(HINT:) c) Consider the Klein four group.

### 30. a

Let  $G$  be a group of order  $pm$ , such that  $p \nmid m$ . Now, Given that  $H$  is a normal subgroup of order  $p$ . Now we want to prove that  $H$  is a characteristic subgroup, that is  $\phi(H) = H$  for any automorphism  $\phi$  of  $G$ . Now consider  $\phi(H)$ . Clearly  $|\phi(H)| = p$ . Suppose  $\phi(H) \neq H$ , then  $H \cap \phi(H) = \{e\}$ . Consider  $H\phi(H)$ , this is a subgroup of  $G$  as  $H$  is normal. Also  $|H\phi(H)| = p^2$ . By lagrange's theorem then  $p^2 \mid pm \implies p \mid m$ - contradiction. So  $\phi(H) = H$ , and  $H$  is characteristic subgroup of  $G$ .

#### Result

See the proof

### 31. a

Let  $G$  be an abelian group of order  $p^n m$ , such that  $p \nmid m$ . Now, Given that  $H$  is a subgroup of order  $p^n$ . Since  $G$  is abelian  $H$  is normal. Now we want to prove that  $H$  is a characteristic subgroup, that is  $\phi(H) = H$  for any automorphism  $\phi$  of  $G$ . Now consider  $\phi(H)$ . Clearly  $|\phi(H)| = p^n$ . Suppose  $\phi(H) \neq H$ , then  $|H \cap \phi(H)| = p^s$ , where  $s < n$ . Consider  $H\phi(H)$ , this is a subgroup of  $G$  as  $H$  is normal. Also  $|H\phi(H)| = \frac{|H||\phi(H)|}{|H \cap \phi(H)|} = \frac{p^n p^n}{p^s} = p^{2n-s}$ , where  $2n - s > n$ . By lagrange's theorem then  $p^{2n-s} \mid p^n m \implies p^{n-s} \mid m \implies p \mid m$ - contradiction. So  $\phi(H) = H$ , and  $H$  is characteristic subgroup of  $G$ .

#### Result

2 of 2

See the proof

### 32. a

Let  $G$  be a group of order  $p^n m$ , such that  $p \nmid m$ . Now, Given that  $H$  is a normal subgroup of order  $p^n$ . Now we want to prove that  $H$  is a characteristic subgroup, that is  $\phi(H) = H$  for any automorphism  $\phi$  of  $G$ . Now consider  $\phi(H)$ . Clearly  $|\phi(H)| = p^n$ . Suppose  $\phi(H) \neq H$ , then  $|H \cap \phi(H)| = p^s$ , where  $s < n$ . Consider  $H\phi(H)$ , this is a subgroup of  $G$  as  $H$  is normal. Also  $|H\phi(H)| = \frac{|H||\phi(H)|}{|H \cap \phi(H)|} = \frac{p^n p^n}{p^s} = p^{2n-s}$ , where  $2n - s > n$ . By lagrange's theorem then  $p^{2n-s} \mid p^n m \implies p^{n-s} \mid m \implies p \mid m$ - contradiction. So  $\phi(H) = H$ , and  $H$  is characteristic subgroup of  $G$ .

#### Result

2 of 2

See the proof

### 33. a

Given that  $G$  is a group.  $N$  is a normal subgroup of  $G$ .  $M \subset N$ , is a characteristic subgroup of  $N$ . We need to prove that  $M$  is normal in  $G$ . So we need to prove  $gMg^{-1} = M$  for every  $g \in G$ . Consider  $\sigma_g : G \rightarrow G$  defined as  $\sigma_g(a) = gag^{-1}$ . This is an automorphism of  $G$ , popularly known as an inner automorphism. Now as  $N$  is normal in  $G$ ,  $\sigma_g$  restricted to  $N$  is a well defined map, and hence an automorphism of  $N$ , that is  $\sigma_g : N \rightarrow N$  is an automorphism of  $N$ . But  $M$  is characteristic in  $N$ , so  $\sigma_g(M) = M \implies gMg^{-1} = M$ . Since  $g$  is arbitrary,  $M$  is normal in  $G$ .

## Result

2 of 2

See the proof

### 34. a

Let  $\sigma_a \in I(G)$  and  $\phi \in \mathcal{A}(G)$ . We verify that  $\phi\sigma_a\phi^{-1} \in I(G)$  by verifying how this automorphism acts on an arbitrary element  $g \in G$ :

$$\begin{aligned}\phi\sigma_a\phi^{-1}(g) &= \phi(a\phi^{-1}(g)a^{-1}) \\ &= \phi(a)(\phi\phi^{-1}(g))\phi(a)^{-1} \\ &= \phi(a)g\phi(a)^{-1} \\ &= \sigma_{\phi(a)}(g)\end{aligned}$$

We then have that  $\phi\sigma_a\phi^{-1} = \sigma_{\phi(a)} \in I(G)$  and so  $I(G)$  is a normal subgroup of  $\mathcal{A}(G)$ .

## Result

2 of 2

For all  $\sigma_a \in I(G)$  and  $\phi \in \mathcal{A}(G)$  we have that  $\phi\sigma_a\phi^{-1} = \sigma_{\phi(a)}$ .

### 35. a

#### $Z(G)$ is a characteristic subgroup of $G$

**Proof:** We know that, the center

$$Z(G) := \{x \in G \mid xg = gx \ \forall g \in G\}$$

is a **subgroup** of  $G$ .

In order to show that  $Z(G)$  is a characteristic subgroup of  $G$ , we need to prove

$$\phi(Z(G)) \subset Z(G), \text{ for all automorphisms } \phi \text{ of } G.$$

Let us take  $g \in G$ .

Since  $\phi$  is an automorphism of  $G$ , **there exists an element**  $h$  in  $G$  such that  $\phi(h) = g$ .

Let us take,  $x \in Z(G)$ .

We will show that  $\phi(x) \in Z(G)$ .

Now,

$$\begin{aligned}g\phi(x) &= \phi(h)\phi(x), \text{ since } g = \phi(h) \\ &= \phi(hx), \text{ since } \phi \text{ is an automorphism} \\ &= \phi(xh), \text{ since } x \in Z(G) \\ &= \phi(x)\phi(h), \text{ since } \phi \text{ is an automorphism} \\ &= \phi(x)g, \text{ since } g = \phi(h).\end{aligned}$$

Hence,

$$g\phi(x) = \phi(x)g, \forall g \in G.$$

So,  $\phi(x) \in Z(G)$ .

This follows that

$$\phi(Z(G)) \subset Z(G).$$

Hence  $Z(G)$  is a characteristic subgroup of  $G$ .

This completes the proof.

## Result

2 of 2

Considering any element  $g$  in  $G$  and  $x$  in  $Z(G)$ , we have shown that  $g\phi(x) = \phi(x)g$  for all automorphisms  $\phi$  of  $G$ , follows the result that  $\phi(Z(G)) \subset Z(G)$  for all automorphisms  $\phi$  of  $G$ .

[Click for the complete proof.](#)

## 36. a

**Given:**  $G$  is a group,  $H$  is a subgroup of  $G$  and  $N$  is a normal subgroup of  $G$ .

**To Prove:**  $H \cap N$  is a normal subgroup of  $H$ .

**Proof:** Since intersection of two subgroups of a group is a subgroup, therefore  $H \cap N$  is a subgroup of  $G$ . Now,

$$H \cap N \subset H \text{ and } H \text{ is a subgroup of } G.$$

It follows that  $H \cap N$  is a subgroup of  $H$ .

It suffices to prove that  $H \cap N$  is normal in  $H$ .

Let us take,  $h \in H$  and  $\alpha \in H \cap N$ .

Then,

$$\alpha \in N \text{ and } \alpha \in H.$$

Since  $N$  is normal in  $G$ , then by normality we have

$$h\alpha h^{-1} \in N, \text{ considering } h \text{ an element of } G.$$

Again,  $H$  is a subgroup, then

$$h \in H, \alpha \in H \implies hah^{-1} \in H.$$

Consequently we have,

$$h \in H, \alpha \in H \cap N \implies hah^{-1} \in H \cap N.$$

This implies,  $H \cap N$  is a normal subgroup of  $H$ .

This completes the proof.

## Result

2 of

Considering  $h \in H$  and  $\alpha \in H \cap N$  and using the normality condition of  $N$  we have proved that  $h\alpha h^{-1} \in H \cap N$ , follows that  $H \cap N$  is normal in  $H$ .

[Click for the complete proof.](#)

## 37. a

Suppose  $G$  is a non-abelian group of order 6. We need to prove that  $G \cong S_3$ . Since  $G$  is non-abelian, we conclude that there is no element of order 6. Now all the non-identity element has order either 2 or 3. All elements cannot be order 3. This is because except the identity elements there are 5 elements, but order 3 elements occur in pair, that is  $a, a^2$ , both have order 3, and  $a \neq a^2$ . So, this is a contradiction, as there are only 5 elements. So, there must be an element of order 2. All elements of order 2 will imply that  $G$  is abelian, hence there is also element of order 3. Let  $a$  be an element of order 2, and  $b$  be an element of order 3. So we have  $e, a, b, b^2$ , already 4 elements. Now  $ab \neq e, , b, b^2$ . So  $ab$  is another element distinct from the ones already constructed.  $ab^2 \neq e, b, ab, b^2, a$ . So, we have got another element distinct from the other. So, now  $G = \{e, a, b, b^2, ab, ab^2\}$ . Also,  $ba$  must be equal to one of these elements. But  $ba \neq e, a, b, b^2$ . Also if  $ba = ab$ , the group will become abelian. so  $ba = ab^2$ . So what we finally get is  $G = \langle a, b | a^2 = e = b^3, ba = ab^2 \rangle$ . Hence  $G \cong S_3$ .

### Result

[See the proof](#)

### 38. a

- (a) We verify that  $T_{bc} = T_b T_c$  for all  $b, c \in G$  by computing the application on an arbitrary element  $Ha$  of  $S$ :

$$\begin{aligned} T_{bc}(Ha) &= Hac^{-1}b^{-1} \\ &= T_b(Hac^{-1}) \\ &= T_b(T_c(Ha)) \\ &= (T_b T_c)(Ha) \end{aligned}$$

- (b) We prove that  $\ker \psi = \{b \in G \mid \forall a \in G : aba^{-1} \in H\}$ . Suppose  $b \in \ker \psi$ , then for all  $Ha \in S$  we have that  $Ha = Hab^{-1}$ , which is equivalent to  $Haba^{-1} = H$ . Therefore if  $b \in \ker \psi$  then for all  $a \in G$  we have that  $aba^{-1} \in H$ .

Now suppose that  $b \in G$  is such that for all  $a \in G$  we have that  $aba^{-1} \in H$ . Then  $Haba^{-1} = H$ , which implies  $Ha = Hab^{-1}$  and so  $\psi(b)(Ha) = Hab^{-1} = Ha$ . Therefore  $b \in \ker \psi$ .

- (c) Note in particular that taking  $a = e$  the previous item gives us that  $\ker \psi \subset H$ . We also have that  $\ker \psi$  is normal in  $G$ . To see this let  $b \in \ker \psi$  and  $g \in G$ , then by the previous item we have that  $gbg^{-1} \in \ker \psi$  since for all  $a \in G$  we have that  $a(gbg^{-1})a^{-1} = (ag)b(ag)^{-1} \in H$ . We therefore have that  $\ker \psi$  is a normal subgroup of  $G$  contained in  $H$ .

Let  $N$  be a normal subgroup of  $G$  contained in  $H$ . For any  $b \in N$  and  $a \in G$  we have that  $aba^{-1} \in N \subset H$ , so by the previous item  $N \subset \ker \psi$ . Therefore  $\ker \psi$  is the largest normal subgroup of  $G$  contained in  $H$ .

### Result

2 of 2

In item (b) we can verify that  $\ker \psi = \{b \in G \mid \forall a \in G : aba^{-1} \in H\}$ . All other conditions can be directly verified from the definitions.

### 39. a

In problem 38, we saw that if  $G$  is a group, with  $H$  a subgroup and  $S$  be the set of right cosets, then  $T : G \rightarrow A(S)$  defined as  $b \mapsto T_b$ , where  $T_b : S \rightarrow S$  given by  $T_b(Ha) = Hab^{-1}$ , is a homomorphism from  $G$  to  $A(S)$ , where  $A(S)$  is the set of bijective maps from  $S$  onto itself.  $\text{Ker}(T) \subset H$ . Now we are given that  $G$  is a non-abelian group of order 6 and we need to prove that  $G \cong S_3$  using the above result. We already proved this in problem 37, and in that solution we argued that  $G$  must contain an element of order 2, call it  $a$ . Consider  $H = \langle a \rangle$ . So  $|H| = 2$ . Now apply the theorem above with  $H$  as described. So  $|S| = 3$  and hence  $A(S)$  is nothing but  $S_3$ . Now we intend to show that the map  $T$  is injective. If we prove that then as  $|G| = |A(S)|$ , so  $G \cong S_3$ . So if we prove that  $T$  is injective. Consider  $\text{Ker}(T)$ .  $\text{Ker}(T) \subset H$ . So either  $\text{Ker}(T) = \{e\}$  or  $\text{Ker}(T) = H$ . If  $a \in \text{Ker}(T) \implies T_a = \text{id} \implies Hxa^{-1} = Hx$  for every  $x \in G$ , in particular we  $Hba^{-1} = Hb$ , where  $b$  is an element of order 3, whose existence we proved in problem 37. This implies that  $bab^{-1} \in H$ . Now,  $bab^{-1} \neq e$  is clear. Also  $bab^{-1} = a \implies ab = ba$ . This implies  $G$  is abelian a contradiction. So  $a \notin \text{Ker}(T)$ . So,  $\text{Ker}(T) = \{e\}$ . Hence  $T$  is injective which is what we needed. So we have  $G \cong S_3$ .

### Result

[See the proof](#)

40. a

As we saw in problem 38, given a group  $G$ , and a subgroup  $H$ , if we consider  $S$  to be the set of right cosets of  $H$  in  $G$ , we get a homomorphism  $T : G \rightarrow A(S)$ , where  $A(S)$  is the set of all bijective map from  $S$  onto  $S$ , which is a group under composition. Also we proved that  $\text{Ker}(T) \subset H$ , and  $\text{Ker}(T)$  is the largest normal subgroup of  $G$  contained in  $H$ . We use this result to prove this problem which is as follows : given that  $G$  is a group and  $H$  a subgroup, such that  $|G| = n$  and  $n \nmid i_G(H)!$ . We need to prove that there exists a normal subgroup  $K \subset H$  and  $K \neq \{e\}$ . We consider  $S$  as above. So we have the above group homomorphism  $T$  from  $G \rightarrow A(S)$ . Now, If  $\text{Ker}(T) = \{e\}$ , then  $T$  is injective, so  $T(G)$  is a subgroup of  $A(S)$ , and  $|T(G)| = |G| = n$ . By, lagrange's theorem  $n \mid |A(G)| = i_G(H)!$ , contradiction. So,  $\text{Ker}(T) \neq \{e\} \subset H$ . So  $\text{Ker}(T)$  is the required non-trivial normal subgroup contained in  $H$ .

### Result

[See the proof](#)

41. a

We use the result from problem 40 which is as follows: Suppose  $G$  is a group,  $H$  is a subgroup and  $|G| = n$  and  $n \nmid (i_G(H))!$ . Then there exists a normal subgroup  $K \neq \{e\}$  and  $K \subseteq H$ .

So, we have now a group  $G$  of order 21, and there exists an element  $a$  of order 7, and  $A = \langle a \rangle$ . Now  $i_G(A) = 3$ , so  $21 \nmid 3!$ , hence by the above result there is a normal subgroup  $K$ , non-trivial and  $K \subseteq A$ . But  $|A| = 7$ , a prime order subgroup, hence has no non-trivial subgroup, so  $K = A$ . So  $A$  is normal subgroup.

### Result

[See the proof](#)

42. a

We use the result from problem 40 which is as follows: Suppose  $G$  is a group,  $H$  is a subgroup and  $|G| = n$  and  $n \nmid (i_G(H))!$ . Then there exists a normal subgroup  $K \neq \{e\}$  and  $K \subseteq H$ .

So, we have now a group  $G$  of order 36, and there exists a subgroup of order 9, call it  $A$ . Now  $i_G(A) = 4$ , so  $36 \nmid 4!$ , hence by the above result there is a normal subgroup  $K$ , non-trivial and  $K \subseteq A$ . But  $|A| = 9$ . So either  $A$  itself is normal or contains a normal subgroup of order 3.

43. a

We use the result from problem 40 which is as follows: Suppose  $G$  is a group,  $H$  is a subgroup and  $|G| = n$  and  $n \nmid (i_G(H))!$ . Then there exists a normal subgroup  $K \neq \{e\}$  and  $K \subseteq H$ .

So, we have now a group  $G$  of order 9. Suppose that  $G$  is cyclic, then  $G$  is abelian and there is nothing more to prove. Suppose that  $G$  is not cyclic, then there exists an element  $a$  of order 3, and  $A = \langle a \rangle$ . Now  $i_G(A) = 3$ , now  $9 \nmid 3!$ , hence by the above result there is a normal subgroup  $K$ , non-trivial and  $K \subseteq A$ . But  $|A| = 3$ , a prime order subgroup, hence has no non-trivial subgroup, so  $K = A$ . So  $A$  is normal subgroup. Now since  $G$  is not cyclic any non-identity element is of order 3. So Let  $a (\neq e) \in G$ . Consider  $A = \langle a \rangle$ . As shown before  $A$  is normal.  $a$  commutes with any of its powers. Now Let  $b \in G$  such that  $b \notin A$ . Then  $bab^{-1} \in A$  and hence  $bab^{-1} = a^i$ . This implies  $a = b^3ab^{-3} = a^{i^3} \implies a^{i^3-1} = e$ . So, 3 divides  $i^3 - 1$ . Also by fermat's little theorem 3 divides  $i^2 - 1$ . So 3 divides  $i - 1$ . But  $0 \leq i \leq 2$ . So  $i = 1$ , is the only possibility and hence  $ab = ba$ . So  $a \in Z(G)$  as  $b$  was arbitrary. Since  $a$  was arbitrary  $G = Z(G)$ . Hence  $G$  is abelian.

### Result

[See the proof](#)

44. a

We use the result from problem 40 which is as follows: Suppose  $G$  is a group,  $H$  is a subgroup and  $|G| = n$  and  $n \nmid (i_G(H))!$ . Then there exists a normal subgroup  $K \neq \{e\}$  and  $K \subseteq H$ .

So, we have now a group  $G$  of order  $p^2$ . Suppose that the group is cyclic, then it is abelian and any subgroup of order  $p$  is normal. Now let us suppose that  $G$  is not cyclic, then there exists an element  $a$  of order  $p$ , and  $A = \langle a \rangle$ . Now  $i_G(A) = p$ , so  $p^2 \nmid p!$ , hence by the above result there is a normal subgroup  $K$ , non-trivial and  $K \subseteq A$ . But  $|A| = p$ , a prime order subgroup, hence has no non-trivial subgroup, so  $K = A$ . So  $A$  is normal subgroup.

### Result

See the proof.

## 45. a

Let  $G$  be a group of order  $p^2$ . We have to show that  $G$  is abelian. Now, Suppose that  $G$  is cyclic, then  $G$  is abelian. Let us now suppose that  $G$  is not cyclic. Then every non-identity element has order  $p$ . Let  $a \in G$  be of order  $p$ . Consider  $A = \langle a \rangle$ . We proved in the previous problem that it is normal subgroup. Now  $a$  commutes with all its powers. Now Let  $b \neq e \in G$  such that  $b \notin A$ . Since  $A$  is normal,  $bab^{-1} \in A \implies bab^{-1} = a^i$ . Now  $a = b^p ab^{-p} = a^{ip} \implies a^{ip-1} = e$ . Hence  $p \mid i^p - 1$ . Also by Fermat's little theorem,  $p \mid i^{p-1} - 1$ . This together implies  $p \mid i - 1$ . Hence  $i = 1$ . Thus we get  $ab = ba$  for arbitrary  $b$ . Hence  $a \in Z(G)$ . But  $a$  is arbitrary, so  $Z(G) = G$ , hence  $G$  is abelian.

## 46. a

We may prove this by contradiction. Remember that by Lagrange's theorem (**theorem 2.4.2**) we have that the order of any element  $a \in G$  divides  $|G| = 15$ . Therefore The order of elements of  $G$  can only be 1, 3, 5 and 15.

Suppose that no element of  $G$  has order 3. The only element of a group of order 1 is the identity, so all non-identity elements of  $G$  may only have order 5 or 15. Note however that if  $a$  has order 15 then  $a^5$  is an element of order 3, which contradicts our assumption. Therefore we conclude that if no element of  $G$  has order 3 then all non-identity elements of  $G$  have order 5. Note however that there are 14 non-identity elements of  $G$ . If we take an arbitrary element  $b \in G - \{e\}$  we have that the elements of  $\{b, b^2, b^3, b^4\}$  are all distinct. Also if  $c \in G - \{e, b, b^2, b^3, b^4\}$  then for all  $1 \leq i, j \leq 4$  we have that  $b^i \neq c^j$  since otherwise there would be some  $k$  such that  $c = (c^j)^k = (b^i)^k \in \{e, b, b^2, b^3, b^4\}$ , a contradiction. Therefore the 14 elements in  $G - \{e\}$  are partitioned in subsets of 4 elements, which is clearly impossible since  $4 \nmid 14$ . Therefore some element of  $G$  must have order 3.

Let  $a \in G$  be an element of order 3 and  $S$  be the set of right cosets of the subgroup  $H = \{e, a, a^2\}$ . Consider  $\psi : G \rightarrow A(S)$  the homomorphism of **exercise 38**. Note that the coset  $H$  is always fixed by  $\psi(a)$ , and since  $\psi(a)$  must have order 3 and there are 4 other cosets at least one of them must be fixed, say  $Hx$ . We then have that  $S = \{H, Hx, Hx^2, Hx^3, Hx^4\}$ , and so  $x^5 \in H$  and this can only be the case if  $x^5 = e$ , ie  $x$  is an element of order 5.

### Result

2 of 2

We can prove by contradiction that there is an element of order 3. Then analyzing the right cosets of a subgroup of order 3 we see there must be some element of order 5.

## 47. a

Taking  $H = \{e, b, b^2, b^3, b^4\}$  since there are 3 cosets of  $H$  by **exercise 40** we have that  $H$  is a normal subgroup. Since  $H$  is normal  $a^{-1}ba \in H$ , so it must then be the case that  $ba = ab^i$  for some  $i = 0, 1, 2, 3, 4$ . Since  $a$  has order 3 it must be the case that  $b = ba^3 = a^3b^{i^3} = b^{i^3}$ , and so that  $i^3 \equiv 1 \pmod{5}$ . Therefore the only possible value for  $i$  is  $i = 1$ . Therefore  $a$  and  $b$  commute. We can conclude that all elements of  $G$  can be written in the form  $a^i b^j$  for some  $i = 0, 1, 2$  and  $j = 0, 1, 2, 3, 4$  with  $(a^i b^j)(a^k b^l) = a^{i+k} b^{j+l}$ , and it is easily verifiable that  $\{e, a, a^2\}$  is a normal subgroup.

### Result

2 of 2

From **exercise 40** we have that the subgroup generated by  $b$  is normal. From this we can conclude that  $a$  and  $b$  commute, from which it easily follows that  $G$  is abelian, and in particular the subgroup generated by  $a$  is normal.

### 48. a

As proved in **exercise 47**  $G$  is an abelian group with elements of the form  $a^i b^j$  for  $i = 0, 1, 2$  ad  $j = 0, 1, 2, 3, 4$ , with operation given by  $(a^i b^j)(a^k b^l) = a^{i+k} b^{j+l}$ . From the fact that 3 and 5 are relatively prime it follows that  $ab$  has order 15, and so  $G$  is generated by  $ab$  and is therefore cyclic.

### Result

2 of 2

This follows from the fact that  $G$  must be abelian and 3 and 5 are relatively prime.

### 49. a

Let  $S$  be the set of right cosets of  $H$  and  $\psi : G \rightarrow A(S)$  be as in **exercise 38**. As proved there  $\ker \psi$  is a normal subgroup of  $G$  contained in  $H$ . All we need to prove is that  $i_G(\ker \psi)$  is finite. Note that  $\psi$  induces a well defined map

$$\begin{aligned}\bar{\psi} : \{(\ker \psi)g \mid g \in G\} &\rightarrow A(S) \\ (\ker \psi)g &\mapsto \psi(g)\end{aligned}$$

which is one-to-one since if  $\psi(g) = \psi(g')$  then  $g'g^{-1} \in \ker \psi$  and so  $(\ker \psi)g = (\ker \psi)g'g^{-1}g = (\ker \psi)g'$ . Therefore  $i_G(\ker \psi) \leq |A(S)| = i_G(H)!$  is finite.

### Result

2 of 2

This follows from **exercise 38** and the fact that by assumption  $i_G(H)!$  is finite.

### 50. a

Consider the Dihedral group of order 8, popularly denoted by  $D_8$ .  $D_8 = \{r, s | r^4 = e = s^2, sr = rs^{-1}\}$ . The subgroup generated by  $r$ , that is,  $H = \{e, r^2, s, sr^2\}$  is of order 4, hence of index 2, so normal in  $D_8$ , again consider  $K = \{e, s\}$ ,  $K$  is normal in  $H$  because it is of index 2 in  $H$ , but  $K$  is not normal in  $G$ ,

### Result

See the example

51. a

$\phi: h \rightarrow h$  is an automorphism of  $h$ .

$\phi(x) = x \neq x \in h$

and  $\phi(e) = e \Rightarrow e = e$ .

Consider  $x^{-1}\phi(x) \in h$ .

$$\begin{aligned} \phi(x^{-1}\phi(x)) &= \phi(x^{-1})\phi^2(x) \\ &= \phi(x^{-1}).x = (\phi(x))^{-1}x \\ &= (x^{-1}\phi(x))^{-1} \end{aligned}$$

$$\Rightarrow \phi(x^{-1}\phi(x)) = (x^{-1}\phi(x))^{-1}.$$

Now we show that for every  $g \in h \exists x \in h$

such that  $g = x^{-1}\phi(x)$ .

Consider the set  $h' = \{x^{-1}\phi(x) | x \in h\}$

then  $h'$  is a subset of  $h$ .

We show that for  $x \neq y$

$$x^{-1}\phi(x) \neq y^{-1}\phi(y).$$

Let  $y \neq x$

$$\begin{aligned} &x^{-1}\phi(x) = y^{-1}\phi(y) \\ \Rightarrow \quad &\phi(x^{-1}\phi(x)) = \phi(y^{-1}\phi(y)) \\ \phi(x^{-1})\phi^2(x) &= \phi(y^{-1})\phi^2(y) = \phi(y^{-1})y \\ \Rightarrow (\phi(x^{-1}))^{-1}\phi(x) &= yx^{-1} \\ \Rightarrow \phi(y)\phi(x^{-1}) &= yx^{-1} \\ \Rightarrow \phi(yx^{-1}) &= yx^{-1} \\ \Rightarrow yx^{-1} &= e \quad [\because \phi(x) = x \Rightarrow x = e] \\ \Rightarrow y &= x \\ \text{which is a contradiction} \end{aligned}$$

$\Rightarrow$  for  $x \neq y$

$$x^{-1}\phi(x) \neq y^{-1}\phi(y)$$

$$\Rightarrow |h'| = |\{x^{-1}\phi(x) | x \in h\}| = |h|$$

$$\Rightarrow h' = h$$

$\Rightarrow$  for every  $g \in h$ ,  $\exists x \in h$  such that  $g = x^{-1}\phi(x)$

$$\Rightarrow \phi(g) = \phi(x^{-1}\phi(x)) = (x^{-1}\phi(x))^{-1}g^{-1}$$

$$\Rightarrow \phi(g) = g^{-1} \neq g \in h.$$

Now to show G is abelian.

Let  $x, y \in G$  s.t.,  $x, y \neq e$ .

$$\phi(xy) = \phi(x)\phi(y)$$

$$\Rightarrow (xy)^+ = x^+y^+$$

$$\Rightarrow y^+x^+ = x^+y^+$$

$$\Rightarrow xy = yx$$

$\Rightarrow$  G is abelian.

52. a

Let us consider the following set

$$A = \{x \in G : \phi(x) = x^{-1}\}$$

It is given that  $|A| > (3/4)|G|$ . We prove that G is abelian and  $A = G$ . For better understanding, we will divide the given problem into few smaller subproblems.

---

### Step 2

2 of 17

Let us start with considering  $b$  to be an arbitrary element in  $A$ .

1. Show that  $|A \cap (b^{-1}A)| > \frac{|G|}{2}$ , where

$$b^{-1}A = \{b^{-1}a \mid a \in A\}$$

First notice that if we consider a map  $f : A \rightarrow b^{-1}A$  defined by  $f(a) = b^{-1}a$ , for all  $a \in A$ , then  $f$  is a 1-1 map and so  $|b^{-1}A| \geq |A| > \frac{3}{4}|G|$ . Now using inclusion-exclusion principle we have

$$|A \cap (b^{-1}A)| = |A| + |b^{-1}A| - |A \cup (b^{-1}A)| > \frac{3}{4}|G| + \frac{3}{4}|G| - |G| = \frac{1}{2}|G|$$

#### Step 4

4 of 17

- 2.** Argue that  $A \cap (b^{-1}A) \subseteq C(b)$ , where  $C(b)$  is the centralizer of  $b$  in  $G$ .

#### Step 5

5 of 17

Suppose  $x \in A \cap (b^{-1}A)$ , that means,  $x \in A$  and  $x \in b^{-1}A$ . Thus there exist an element  $a \in A$  such that  $x = b^{-1}a$ , which gives us  $xb = a \in A$ .

Now notice that  $x, b \in A$  and  $xb \in A$ , therefore we get

$$\phi(xb) = (xb)^{-1} \implies \phi(x)\phi(b) = (xb)^{-1} \implies x^{-1}b^{-1} = b^{-1}x^{-1} \implies xb = bx$$

Therefore, we get  $xb = bx$ , for any  $x \in A \cap (b^{-1}A)$ , that means,  $x \in C(b)$ .

- 3.** Argue that  $C(b) = G$ .

#### Step 7

7 of 17

We know that centralizer of an element in a group  $G$  is a subgroup (See Page 53). Therefore  $C(b)$  is a subgroup of  $G$ . From statements **1** and **2**, we have

$$|C(b)| \geq |A \cap (b^{-1}A)| > \frac{|G|}{2}.$$

#### Step 8

8 of 17

We need to use the following remark to argue  $C(b) = G$  from the above step.

**Remark.** Let  $G$  be a finite group and  $H$  be a subgroup with more than  $|G|/2$  elements then  $H = G$ .

**Proof of Remark.** Suppose  $|H| = p$ . Then by Lagrange Theorem, there exist an  $n \in \mathbb{N}$ , such that  $|G| = np$ , as  $|H|$  divide  $|G|$ . Now by hypothesis  $p > \frac{|G|}{2}$  gives us,

$$p > \frac{|G|}{2} \implies np > \frac{n|G|}{2} \implies n < 2 \implies n = 1$$

Therefore we get  $H = G$ .

## Step 10

10 of 17

Now notice that  $C(b)$  is a subgroup of  $G$  with  $C(b)$  having more than  $|G|/2$  elements. Therefore,  $C(b) = G$ .

## Step 11

11 of 17

4. Show that  $A \subseteq Z(G)$ .

We know that from Problem 2.3.6,  $x \in Z(G)$  if and only if  $C(x) = G$ . Now notice that, for any  $b \in A$  we have  $C(b) = G$ . Therefore, every element of  $A$  is in the center of  $G$ , that means,  $A \subseteq Z(G)$ .

## Step 13

13 of 17

5. Show that  $Z(G) = G$ .

## Step 14

14 of 17

As it is given that  $|A| > \frac{3|G|}{4}$  and  $A \subseteq |Z(G)|$ , therefore we get

$$|Z(G)| > \frac{3}{4}|G| > \frac{1}{2}|G|.$$

As  $Z(G)$  is a subgroup of  $G$ , so by the above Remark we have  $Z(G) = G$ . Hence  $G$  is abelian.

6. Finally show that  $A = G$ .

## Step 16

16 of 17

First notice that  $A$  is a subgroup of  $G$ . To show this let  $p, q \in A$ . Then we have

$$\phi(pq) = \phi(p)\phi(q) = p^{-1}q^{-1} = (qp)^{-1} = (pq)^{-1}, \quad \text{As } G \text{ is abelian.}$$

## Step 17

17 of 17

Therefore,  $pq \in A$  and so by Lemma 2.3.2. we have  $A$  is a subgroup of  $G$ . Again by applying the above remark we get  $A = G$ . Therefore we have

$$\phi(y) = y^{-1}, \quad \text{for all } y \in G$$

## Section 2–6

1. a

We have that for  $G = \mathbb{R} - \{0\}$  and  $N = \mathbb{R}_+$  then  $G/N = \{N, -1N\}$ . We then have that  $N$  is the identity in  $G/N$  and  $-1N \cdot -1N = N$ .

**Result**

2 of 2

$$G/N = \{N, -1N\}$$

2. a

The cosets of  $N$  in  $G$  are of the form  $rN = r\{1, -1\} = \{r, -r\}$  where  $r$  is a real number. Define the map

$$\begin{aligned}\phi : G/N &\rightarrow \mathbb{R}_+ \\ \{r, -r\} &\mapsto |r|\end{aligned}$$

which is a homomorphism since

$$\begin{aligned}\phi(\{r, -r\}\{s, -s\}) &= \phi(\{rs, -rs\}) \\ &= |rs| \\ &= |r||s| \\ &= \phi(\{r, -r\})\phi(\{s, -s\})\end{aligned}$$

We have that  $\phi$  is onto since for all  $r \in \mathbb{R}_+$  then  $\phi(\{r, -r\}) = r$ . We also have that  $\phi$  is a monomorphism since  $\phi(\{r, -r\}) = 1$  if and only if  $|r| = 1$  and so  $\{r, -r\} = N$ . Then  $\phi$  is an isomorphism which gives the desired identification.

**Result**

2 of 2

The identification is given by the isomorphism

$$\begin{aligned}\phi : G/N &\rightarrow \mathbb{R}_+ \\ \{r, -r\} &\mapsto |r|\end{aligned}$$

3. a

Assume that  $x, y \in M$  are the arbitrary elements, then definition of the set  $M$  implies  $Nx, Ny \in \overline{M}$ . Using the fact that  $\overline{M} < G/N$  we obtain that

$$Nxy = Nx \odot Ny \in \overline{M}$$

so that  $xy \in M$  for the arbitrary  $x, y \in M$ , i.e.  $M$  is closed under the product in  $G$ .

Also, for an arbitrary  $x \in M$ , the fact that  $\overline{M} < G/N$  and the definition of set  $M$  implies  $Nx^{-1} \in \overline{M}$ . Therefore, from the last result we obtain that  $x^{-1} \in M$ .

It is proven that  $M$  is closed under the product in  $G$  and for an arbitrary  $x \in M$  we have that  $x^{-1} \in M$ . Now, the fact  $M \subset G$  and last result implies  $M < G$ .

Note that  $Nn = N \in \overline{M}$  for each  $n \in N$ , so that  $N \subset M$ .

## Result

2 of 2

Use the fact that  $\overline{M} < G/N$ .

4. a

## Result

Use the fact that  $\overline{M}$  is normal subgroup of  $G/N$

5. a

Note that the definition of the set  $M$  gives us that  $Nm \in \overline{M}$  for each  $m \in M$ .

Therefore,

$$M/N = \{Nm \mid m \in M\} \subset \overline{M}$$

Furthermore, if  $Nm \in \overline{M}$ , then  $m$  must be an element of the set  $M$  and  $Nm$  must be an element of  $M/N$ .

**Hence, using the results above we obtain the proof!**

## Result

2 of 2

Use the definition of the set  $M$

6. a

Let  $X$  be the square  $[0, 1] \times [0, 1]$  with the identification  $(t, 0) \sim (t, 1)$  and  $(0, s) \sim (1, s)$ , so that  $X$  is the torus. We define

$$\begin{aligned}\phi : G/N &\rightarrow X \\ (a \pmod{\mathbb{Z}}, b \pmod{\mathbb{Z}}) &\mapsto (a - \lfloor a \rfloor, b - \lfloor b \rfloor)\end{aligned}$$

with  $\lfloor x \rfloor$  the largest integer less than the real number  $x$ . Due to the identifications of  $X$  this is a well defined map. It is surjective since for  $(a, b) \in X$  we have that  $\phi(a \pmod{\mathbb{Z}}, b \pmod{\mathbb{Z}}) = (a, b)$  and is one to one since by definition if  $(a \pmod{\mathbb{Z}}, b \pmod{\mathbb{Z}}) = (c \pmod{\mathbb{Z}}, d \pmod{\mathbb{Z}})$  then  $c - a$  and  $d - b$  are integers which implies

$$\begin{aligned}\phi(a \pmod{\mathbb{Z}}, b \pmod{\mathbb{Z}}) &= (a - \lfloor a \rfloor, b - \lfloor b \rfloor) \\ &= (c - \lfloor c \rfloor, d - \lfloor d \rfloor) \\ &= \phi(c \pmod{\mathbb{Z}}, d \pmod{\mathbb{Z}}).\end{aligned}$$

## Result

2 of 2

This is similar to the argument in [example 2](#).

## 7. a

**Given:**  $N$  is a subgroup of a cyclic group  $G$ .

**To Prove:** The quotient group  $G/N$  is cyclic.

**Proof:** First we prove a Lemma.

**Lemma:** Every subgroup of an abelian group  $G$  is a normal subgroup of  $G$ .

**Proof of the Lemma:** Let  $H$  be a subgroup of an abelian group  $G$ .

Let  $a \in G$ .

Then

$$aH := \{ah : h \in H\}$$

and

$$Ha := \{ha : h \in H\}.$$

Since  $G$  is **abelian group**,

$$ah = ha \text{ for all } h \in H$$

and therefore

$$aH = Ha \text{ holds for all } a \in G.$$

Hence,

$$H \text{ is normal in } G$$

This proves our Lemma.

Now back to our question.

Since  $G$  is cyclic,  $G$  is an **abelian group**.

Therefore,  $N$  is a **normal subgroup** of  $G$  and the quotient group  $G/N$  exists.

Let us assume

$$G = \langle a \rangle.$$

Since  $N$  is a subgroup of  $G$ ,  $N$  is also **cyclic** and

$$N = \langle a^m \rangle$$

where  $m$  is the **least positive integer** such that  $a^m \in N$ .

First we prove that  $N, aN, a^2N, \dots, a^{m-1}N$  is a

#### complete list of distinct cosets of $N$ in $G$

Let  $x \in G$ . Then

$$x = a^p \text{ for some integer } p.$$

By **division algorithm**, there exist integers  $q$  and  $r$  such that

$$p = qm + r, \text{ where } 0 \leq r \leq m - 1.$$

Therefore,

$$a^p = a^{qm+r} = a^r(a^m)^q = a^r h \text{ for some } h \in N.$$

Since  $0 \leq r \leq m - 1$ ,  $x$  belongs to one of the cosets  $N, aN, a^2N, \dots, a^{m-1}N$ .

**No two of these cosets are equal**,

since

$$\begin{aligned} a^iN &= a^jN \text{ with } 0 \leq i < j \leq m - 1 \\ \implies (a^i)^{-1}a^j &\in N \text{ i.e., } a^{j-i} \in N, \end{aligned}$$

which is contradiction, since  $0 < j - i < m$ .

Therefore the **distinct cosets** of  $N$  in  $G$  are  $N, aN, a^2N, \dots, a^{m-1}N$ .

Now,

$$\begin{aligned} a^rN &= (a.a...a)N \\ &= (aN)(aN)...(aN) \text{ (r factors)} \\ &= (aN)^r. \end{aligned}$$

Thus  $G/N$  is a

#### finite group of $m$ elements

$N, aN, (aN)^2, \dots, (aN)^{m-1}$ .

Hence,  $G/N$  is a **cyclic group**,  $aN$  being a **generator**.

This completes our proof.

## Result

5 of 5

Being  $G$  is cyclic,  $N$  is cyclic and considering all the distinct cosets of  $N$  in  $G$  and by applying division algorithm we have proved the existence of an element in  $G/N$  which generates  $G/N$ , and hence  $G/N$  is cyclic.

Click for the detailed proof.

## 8. a

**Given:**  $G$  is an abelian group and  $N$  be a subgroup of  $G$ .

**To Prove:** The quotient group  $G/N$  is abelian.

**Proof:** First we start with a Lemma.

**Lemma:** Every subgroup of an abelian group  $G$  is a normal subgroup of  $G$ .

**Proof of the Lemma:** Let  $H$  be a subgroup of an abelian group  $G$ .

Let  $a \in G$ .

Then

$$aH := \{ah : h \in H\}$$

and

$$Ha := \{ha : h \in H\}.$$

Since  $G$  is **abelian group**,

$$ah = ha \text{ for all } h \in H$$

and therefore

$$aH = Ha \text{ holds for all } a \in G.$$

Hence,

$$H \text{ is normal in } G$$

This proves our Lemma.

Now back to the question.

Since  $G$  is an abelian group,  $N$  is a **normal subgroup** of  $G$ .

Therefore  $G/N$  exists.

Let us assume  $aN, bN \in G/N$ .

Then  $a, b \in G$ .

Now,

$$(aN)(bN) = abN \text{ and } (bN)(aN) = baN.$$

Since  $G$  is **abelian**,

$$ab = ba.$$

Therefore,

$$(aN)(bN) = (bN)(aN) \text{ for all } aN, bN \in G/N.$$

Thus,  $G/N$  is an **abelian group**.

This completes our proof.

### Result

4 of 4

Considering any two elements of the quotient group  $G/N$ , we have proved that they commutes by the help of the given condition that  $G$  is abelian.

Click for the detailed proof.

## 9. a

We have that

$$\begin{aligned}\phi : G &\rightarrow G/N \\ g &\mapsto gN\end{aligned}$$

is surjective. If  $G$  is generated by  $x \in G$  then for all  $g \in G$  there is  $i \in \mathbb{Z}_+$  such that  $g = x^i$ . Therefore  $\phi(x) = xN$  generates  $G/N$  since for any  $gN \in G/N$  we have that  $gN = x^iN = (xN)^i$ .

Suppose now that  $G$  is abelian. We then have that for all  $gN, hN \in G/N$  that

$$\begin{aligned}(gN)(hN) &= ghN \\ &= \phi(gh) \\ &= \phi(hg) \\ &= hgN \\ &= (hN)(gN)\end{aligned}$$

so  $G/N$  is abelian.

### Result

2 of 2

Both properties follows easily using the surjective homomorphism

$$\begin{aligned}\phi : G &\rightarrow G/N \\ g &\mapsto gN\end{aligned}$$

## 10. a

Let  $i$  be an arbitrary integer such that  $1 \leq i \leq k$ . If  $a_i = 1$ , then Cauchy's theorem gives us that there is the element  $g \in G$  of order  $p_i$  and the cyclic group generated by  $g$  is of order  $G$ .

Further, we assuming that for  $a_i < n$  there is an subgroup of  $G$  such that its order is equal to  $p_i^{a_i}$ . Using this assumption we need to prove that, if  $a_i = n$  we can found the subgroup of order  $p_i^n$  and then mathematical induction principle gives us the proof!

Therefore, let consider  $a_i = n$ , Cauchy's theorem gives that there is  $g \in G$  of order  $p_i$  and the cyclic group generated by  $g$  is of order  $G$ , let denote it by  $\mathbf{N}$ . Fact that  $G$  is an abelian group gives that  $\mathbf{N}$  is normal in  $\mathbf{G}$ . So that, we can consider factor group  $\mathbf{G}/\mathbf{N}$  of order

$$\frac{|G|}{|\mathbf{N}|} = p_1^{a_1} \cdot \dots \cdot p_i^{n-1} \cdot \dots \cdot p_k^{a_k}$$

The assumption we made gives us that there is subgroup  $\overline{\mathbf{S}_i}$  of  $\mathbf{G}/\mathbf{N}$  which has order  $p_i^{n-1}$ . Let define the set  $S_i$  as

$$S_i = \{s \in G | Ns \in \overline{\mathbf{S}_i}\}$$

Finaly, fact that factor group  $\mathbf{G}/\mathbf{N}$  is abelian ( $\mathbf{G}$  is abelian), results from **Problem 3.**, **Problem 4.** and **Problem 5.**, and the result above gives that  $\mathbf{S}_i < \mathbf{G}$  and

$$\mathbf{S}_i/\mathbf{N} = \overline{\mathbf{S}_i}$$

Therefore, order of  $\mathbf{S}_i$  is equal to product  $|\mathbf{N}| \cdot |\overline{\mathbf{S}_i}| = p_i^n$ .

THE PROOF!

### Result

Prove by induction and the Cauchy's theorem.

## 11. a

**Given:**  $G$  is a group and  $Z(G)$  is the center of  $G$  such that the quotient group  $G/Z(G)$  is cyclic.

**To Prove:**  $G$  is an abelian group.

**Proof:**

Since  $Z(G)$  is a

**commutative subgroup of  $G$ , it is a normal subgroup**

of  $G$ .

Hence, the quotient group  $G/Z(G)$  exists.

Let us assume that  $G/Z(G)$  is cyclic.

Then,

$$G/Z(G) = \langle aZ(G) \rangle \text{ for some } a \in G.$$

**So each element of  $G/Z(G)$  is of the form  $(aZ(G))^i$ , i.e., of the form  $a^i Z$  for some integer  $i$ .**

Let  $p, q$  be arbitrary elements of  $G$ .

Let the **cosets** of  $Z(G)$  to which they belong be  $a^r Z(G), a^s Z(G)$  respectively, where  $r$  and  $s$  are integers.

Then

$$p = a^r z_1 \text{ and } q = a^s z_2 \text{ for some } z_1, z_2 \in Z(G).$$

Now,

$$\begin{aligned} pq &= (a^r z_1)(a^s z_2) \\ &= a^r a^s z_1 z_2 \quad (z_1 \text{ commutes with } a^s, \text{ since } z_1 \in Z(G)) \\ &= a^{r+s} z_1 z_2; \end{aligned}$$

and

$$\begin{aligned} qp &= (a_s z_2)(a^r z_1) \\ &= a^s a^r z_2 z_1 \quad (z_2 \text{ commutes with } a^r, \text{ since } z_2 \in Z(G)) \\ &= a^{r+s} z_1 z_2. \end{aligned}$$

Hence,

$$pq = qp \text{ for all } p, q \in Z(G).$$

This proves that  $G$  is **abelian**.

### Result

3 of 3

Being  $G/Z(G)$  is cyclic, we consider the generator of  $G/Z(G)$  and two arbitrary elements of  $G$ , to show that they commute.

Click for the detailed proof.

## 12. a

**Given:**  $N$  is a normal subgroup of a group  $G$  such that  $G/N$  is abelian.

**To Prove:**  $aba^{-1}b^{-1} \in N$  for all  $a, b \in G$ .

**Proof:** Let us consider two arbitrary elements  $a, b \in G$ .

Then  $aN, bN \in G/N$ .

Since,  $G/N$  is abelian

$$(aN)(bN) = (bN)(aN).$$

Now,

$$\begin{aligned}(aN)(bN) &= (bN)(aN) \\ \implies abN &= baN, \text{ by definition} \\ \implies b^{-1}a^{-1}ba &\in N.\end{aligned}$$

It follows that,

$$b^{-1}a^{-1}ba \in N, \text{ for all } a, b \in G.$$

So, we can conclude from here that

$$aba^{-1}b^{-1} \in N, \text{ for all } a, b \in G.$$

This completes our proof.

## Result

2 of 2

Considering any elements  $a, b \in G$  and using the fact that  $G/N$  is abelian, we have proved that  $aba^{-1}b^{-1} \in N$ , for all  $a, b \in G$ .

Click for the complete proof.

## 13. a

**Given:**  $G$  is a group and  $N$  is a normal subgroup of  $G$  such that

$$aba^{-1}b^{-1} \in N \text{ for all } a, b \in G.$$

**To Prove:**  $G/N$  is abelian.

**Proof:** Since  $N$  is normal in  $G$ , the existence of the quotient group  $G/N$  is well defined.

We will propose to prove that  $G/N$  is abelian.

Let us consider elements  $aN, bN \in G/N$ , where  $a, b \in G$ .

Then,

$$(aN)(bN) = abN, \text{ by the definition of quotient group}$$

Now by the given condition,

$$\begin{aligned} aba^{-1}b^{-1} &\in N \text{ for all } a, b \in G \\ \implies b^{-1}a^{-1}(b^{-1})^{-1}(a^{-1})^{-1} &\in N \text{ for all } a, b \in G \\ \implies b^{-1}a^{-1}ba &\in N \text{ for all } a, b \in G \\ \implies baN &= abN \\ \implies (bN)(aN) &= (aN)(bN), \text{ for all } a, b \in G. \end{aligned}$$

Therefore,  $G/N$  is abelian.

This completes the proof.

## Result

3 of 3

Considering any two elements  $aN, bN \in G/N$  and using the fact that  $aba^{-1}b^{-1} \in N$  for all  $a, b \in G$ , we have proved that  $(bN)(aN) = (aN)(bN)$ , for all  $a, b \in G$ .

[Click for the complete proof.](#)

## 14. a

**Given:**  $G$  is an abelian group of order  $p_1 p_2 \dots p_k$ , where  $p_1, p_2, \dots, p_k$  are all distinct primes.

**To Prove:**  $G$  is a cyclic group.

**Proof:** We will use **Cauchy's theorem for group theory** in this context.

It states that,

**Let  $G$  be a finite group and  $p$  be a prime. If  $p$  divides the order of  $G$ , then  $G$  has an element of order  $p$ .**

Since,  $G$  is an abelian group of order  $p_1 p_2 \dots p_k$ , where  $p_1, p_2, \dots, p_k$  are all distinct primes,  $G$  is finite.

Also,

$p_i$  divides the order of  $G$ , for all  $1 \leq i \leq k$ .

Hence, by **Cauchy's theorem** there exists  $g_i$  in  $G$  such that

order of  $g_i$  is  $p_i$ , for all  $1 \leq i \leq k$ .

Let us now consider the element  $g$  in  $G$  defined as

$$g := g_1 g_2 \dots g_k.$$

Then  $g \in G$ , and the order of  $g$  is  $\text{lcm}(p_1, p_2, \dots, p_k)$ .

Since,  $p_1, p_2, \dots, p_k$  are all distinct primes, it follows that

$$\text{lcm}(p_1, p_2, \dots, p_k) = p_1 p_2 \dots p_k.$$

Hence, order of  $g$  in  $G$  is  $p_1 p_2 \dots p_k$ , which is equal to the order of the group  $G$ .

Therefore,  $G$  is a finite abelian group having an element  $g$  such that order of  $g$  is equal to the order of  $G$ .

Hence  $G$  is cyclic.

This completes the proof.

Using Cauchy's theorem we have considered the elements  $g_i$  in  $G$  whose order is  $p_i$  for all  $i$ , and considering the element  $g_1g_2\dots g_k$  and showing that the order of this elements equals the order of  $G$ , follows the result.

[Click for the detailed proof.](#)

## 15. a

**Given:**  $G$  is an abelian group.  $G$  has an element of order  $m$  and an element of order  $n$ , where  $m$  and  $n$  are relatively prime.

**To Prove:**  $G$  has an element of order  $mn$ .

### Proof:

Let us consider the elements  $a$  and  $b$  in  $G$  such that  $o(a) = m$  and  $o(b) = n$ , where  $o(x)$  denotes the order of the element  $x$  in  $G$ .

Let us consider the element  $ab$  in  $G$ .

**Claim:** Order of  $ab$  in  $G$  is  $mn$ , i.e.,  $o(ab) = mn$ .

**Proof of the Claim:** Let us assume, order of  $ab$  in  $G$  be  $k$ .

Since

$$o(a) = m, \quad o(b) = n \text{ and } o(ab) = k$$

it follows that

$$a^m = e, \quad b^n = e \text{ and } (ab)^k = e,$$

$e$  being the **Identity element** of  $G$ .

Now,

$$\begin{aligned} (ab)^{mn} &= a^{mn} b^{mn} \quad (\text{since } G \text{ is abelian}) \\ &= e \cdot e = e. \end{aligned}$$

Therefore,

**$k$  is a divisor of  $mn$ .**

Again,

$$\begin{aligned} (ab)^k &= e \implies a^k b^k = e, \quad (\text{since } G \text{ is abelian}) \\ &\implies a^k = b^{-k} \\ &\implies a^{nk} = e, \quad (\text{since } b^{-nk} = e) \\ &\implies m \text{ is a divisor of } nk \\ &\implies m \text{ is a divisor of } k, \quad \text{since } \gcd(m, n) = 1. \end{aligned}$$

Also,

$$\begin{aligned}
 (ab)^k &= e \implies b^k a^k = e, (\text{ since } G \text{ is abelian}) \\
 \implies b^k &= a^{-k} \\
 \implies b^{mk} &= e, (\text{ since } a^{-mk} = e) \\
 \implies n &\text{ is a divisor of } mk \\
 \implies n &\text{ is a divisor of } k, \text{ since } \gcd(m, n) = 1.
 \end{aligned}$$

It follows that

***mn is a divisor of k***

, since  $\gcd(m, n) = 1$ . ....(ii)

Consequently, from (i) and (ii) it yield's that  $k = mn$ .

Hence,  $ab$  has order  $mn$  in  $G$ .

This proves the claim.

Consequently, we have proved that,

***there exists an element, say c (= ab) in G such that o(c) = mn.***

This completes our proof.

## Result

4 of 4

Considering the elements  $a$  and  $b$  in  $G$  of orders  $m$  and  $n$  respectively, we have shown that the element  $ab$  has order  $mn$  in  $G$  provided  $m$  and  $n$  are relatively prime.

[Click for the detailed proof.](#)

## 16. a

a)

For each  $k$  we have that  $e^{b^k} = e$ , so that  $e \in \mathbb{P}$ .

Let  $a, b \in \mathbb{P}$  be the arbitrary element, then  $a^{p^m} = e$  and  $b^{p^\ell} = e$  for some  $m$  and  $\ell$ . Further, considering  $(ab)^{p^{m+\ell}}$  we obtain that

$$(ab)^{p^{m+\ell}} = (a^{p^m})^{p^\ell} (b^{p^\ell})^{p^m} = e$$

For an arbitrary  $b \in \mathbb{P}$  there is  $k$  such that  $b^{p^k} = e$ , then it is not hard to conclude that  $(b^{-1})^{p^k} = e^{-1} = e$ .

Therefore, from the preceding results we obtain that  $\mathbb{P}$  is subgroup of  $\mathbb{G}$ .

b)

Assume that there is an element in  $\mathbb{G}/\mathbb{P}$  of order  $p$ , then must be

$a^p \mathbb{P} = \mathbb{P}$ , i.e.  $a^p \in \mathbb{P}$ . Therefore, definition of the set  $P$  gives us that  $e = (a^p)^{p^\ell} = a^{p^{\ell+1}}$ , i.e.  $a \in P$  (contradiction!- because  $aP$  has order  $p$ ).

c)

Using result from part b), we can conclude that  $p^n$  divides the order of group  $\mathbb{P}$ , because if not then  $p$  divides the order of  $\mathbb{G}/\mathbb{P}$  and there is an element in  $\mathbb{G}/\mathbb{P}$  of order  $p$  (Cauchy's theorem).

Hence, order of  $\mathbb{P}$  has a form  $p^n \cdot k$  and  $k$  divides  $m$ .

Assume that  $k > 1$ , there is prime divisor  $q$  of  $k$  and using the Cauchy's theorem there is  $a \in P$  such that  $o(a) = q$ . The definition of the set  $P$  gives us that prime  $q$  divides  $p$  (contradiction!  $p$  not divides  $m$ ). Therefore, the order of  $\mathbb{P}$  is equal to  $p^n$ .

## Result

2 of 2

(HINT:) Use the definition of  $P$ .

17. a

- a) It is well-known that  $e^m = e$ , so that  $e \in M$ . For an arbitrary  $a \in M$  we have that

$$(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$$

and then  $a^{-1} \in M$ .

Further, let consider the arbitrary  $a, b \in M$ , we need to show that  $(ab)^m = e$ :

$$(ab)^m = \underbrace{a^m b^m}_{\mathbb{G} \text{ is abelian group}} = e \cdot e = e$$

Therefore,  $M$  is subgroup of  $\mathbb{G}$

- b) There is  $g \in G$  such that  $Mg = x$ . From the fact that

$$M = x^m = (Mg)^m = Mg^m$$

we obtain that  $g^m \in M$  and this gives that  $g^{m^2} = e$ . Therefore, the order of  $g$  must divide  $m^2$  and the order of the group  $M$ , but the fact that  $m$  and  $n$  are relatively prime implies that  $o(g)$  divide  $m$ , i.e. there is an integer  $k$  such that  $k \cdot o(g) = m$

Finally,

$$g^m = g^{k \cdot o(g)} = \left( g^{o(g)} \right)^k = e^k = e$$

and then  $g \in M$ , so  $M = Mg = x$ .

## Result

Use the fact that  $m$  and  $n$  are relatively prime.

18. a

a)

For each  $m$  we have that  $e^m = e$ , so that  $e \in \mathbb{T}$ .

Let  $a, b \in \mathbb{T}$  be the arbitrary element, then  $a^m = e$  and  $b^\ell = e$  for some  $m$  and  $\ell$ . Further, considering  $(ab)^{m\ell}$  we obtain that

$$(ab)^{m\ell} = (a^m)^\ell (b^\ell)^m = e$$

For an arbitrary  $b \in \mathbb{P}$  there is  $k$  such that  $b^k = e$ , then it is not hard to conclude that  $(b^{-1})^k = e^{-1} = e$ .

Therefore, from the preceding results we obtain that  $\mathbb{T}$  is subgroup of  $\mathbb{G}$ .

b)

Assume that  $aT \in \mathbb{G}/\mathbb{T}$  is an arbitrary element of finite order  $m$ , then must be

$a^m \mathbb{T} = \mathbb{T}$ , i.e.  $a^m \in \mathbb{T}$ . Therefore, definition of the set  $T$  gives us that  $e = (a^m)^\ell = a^{m\ell}$  for some  $\ell$ , i.e.  $a \in T$ .

Hence, we obtained that  $aT = T$ .

THE PROOF!

## Result

2 of 2

(HINT:) Use the definition of  $T$ .

## Section 2–7

1. a

There is slight typo in this question. In the question it is asking that `` Show that  $M \supset N$  in the proof of Theorem 2.7.3." but there is no proof given for Theorem 2.7.3 in the book, instead if we read the proof of Theorem 2.7.4, there author have shown the part  $M \subset N$  and left the part  $M \supset N$  to the reader. Thus this question is related to the Theorem 2.7.4.

## Step 2

2 of 5

Let us first describe the problem properly.

**Question:** Suppose the map  $\phi : G \rightarrow G'$  is a homomorphism of  $G$  onto  $G'$  with  $N' \triangleleft G'$  and  $N = \{a \in G \mid \phi(a) \in N'\}$ . Let  $\Psi : G \rightarrow G'/N'$  be map defined by

$$\Psi(a) = N'\phi(a), \quad \text{for all } a \in G.$$

If kernal of  $\Psi$  is  $M$ , then show that  $M \supset N$ .

## Step 3

3 of 5

**Answer:**

Suppose  $a \in N$ . Then by definition of  $N$  we have  $\phi(a) \in N'$ . Notice that

$$\begin{aligned} \Psi(a) &= N'\phi(a), && [\text{By definition of } \Psi] \\ &= N' && [\text{As } \phi(a) \in N'] \end{aligned}$$

Therefore, we get  $a \in Ker(\Psi) = M$  and so for all  $a \in N \implies a \in M$ .

## Result

Hence we prove:  $M \supset N$ .

## 2. a

**Question:** Let  $G$  be the group of all real-valued functions on the unit interval  $[0, 1]$ , where we define, for  $f, g \in G$ , addition by  $(f + g)(x) = f(x) + g(x)$  for every  $x \in [0, 1]$ . If  $N = \{f \in G \mid f(\frac{1}{4}) = 0\}$ , prove that  $G/N \cong$  real numbers under  $+$ .

## Step 2

2 of 6

Let us consider  $\mathbb{R}$  be the set of real number under addition. Our aim is to apply First Homomorphism Theorem (Theorem 2.7.1). In order to apply First Homomorphism Theorem we have to find a homomorphism  $\phi$  from  $G$  onto  $\mathbb{R}$  such that  $Ker(\phi) = N$ . Thus the obvious choice for the homomorphism is as follows.

## Step 3

3 of 6

Consider the map  $\phi : G \rightarrow \mathbb{R}$  defined as

$$\phi(f) = f\left(\frac{1}{4}\right), \quad \text{for all } f \in G.$$

Clearly  $\phi$  is an homomorphism, because for any  $f, g \in G$  we have

$$\phi(f+g) = (f+g)\left(\frac{1}{4}\right) = f\left(\frac{1}{4}\right) + g\left(\frac{1}{4}\right) = \phi(f) + \phi(g).$$

### Step 5

5 of 6

Also  $\phi$  is onto  $\mathbb{R}$ , as for any real number  $r \in \mathbb{R}$ , we can take the constant function  $f(x) = r$ , for all  $x \in [0, 1]$ , and then  $\phi(f) = f\left(\frac{1}{4}\right) = r$ .

Clearly  $N = \text{Ker}(\phi)$ .

### Result

6 of 6

Therefore, by the first homomorphism theorem  $G/N \cong \mathbb{R}$ .

### 3. a

**Question:** Let  $G$  be the group of nonzero real numbers under multiplication and let  $N = \{1, -1\}$ . Prove that  $G/N \cong$  positive real numbers under multiplication.

### Step 2

2 of 6

Let us consider  $\mathbb{R}^+$  be the set of real number under multiplication. Our aim is to apply First Homomorphism Theorem (Theorem 2.7.1). In order to apply First Homomorphism Theorem we have to find a homomorphism  $\phi$  from  $G$  onto  $\mathbb{R}^+$  such that  $\text{Ker}(\phi) = N$ . Thus the obvious choice for the homomorphism is as follows.

### Step 3

3 of 6

Consider the map  $\phi : G \rightarrow \mathbb{R}^+$  defined as

$$\phi(r) = |r|, \quad \text{for all } r \neq 0.$$

Clearly  $\phi$  is an homomorphism, because for any  $p, q \in \mathbb{R} \setminus \{0\}$  we have

$$\phi(p \cdot q) = |p \cdot q| = |p| \cdot |q| = \phi(p) \cdot \phi(q).$$

### Step 5

Also  $\phi$  is onto  $\mathbb{R}^+$ , as for any positive real number  $r \in \mathbb{R}^+$ , we have  $\phi(r) = |r| = r$ .

Now notice that  $\text{Ker}(\phi) = \{r \in \mathbb{R} \setminus \{0\} \mid \phi(r) = 1\}$  and so  $\text{Ker}(\phi) = \{1, -1\} = N$ .

### Result

Therefore by first homomorphism theorem  $G/N \cong \mathbb{R}^+$ .

#### 4. a

**Question:** If  $G_1, G_2$  are two groups and  $G = G_1 \times G_2 = \{(a, b) \mid a \in G_1, b \in G_2\}$ , where we define  $(a, b)(c, d) = (ac, bd)$ , show that:

- sep=0em
  - a.  $N = \{(a, e_2) \mid a \in G_1\}$ , where  $e_2$  is the unit element of  $G_2$ , is a normal subgroup of  $G$ .
  - b.  $N \cong G_1$ .
  - a.  $G/N \cong G_2$ .

#### Step 2

2 of

**Answer for (a):** Let us consider the map  $\varphi : G \rightarrow G_2$ , defined by

$$\varphi(a, b) = b, \quad \text{for all } (a, b) \in G.$$

To show  $\varphi$  is a homomorphism, let us take  $(a, b), (c, d) \in G$ . Then we get

$$\varphi((a, b)(c, d)) = \varphi(ac, bd) = bd = \varphi(a, b)\varphi(c, d)$$

Therefore,  $\varphi((a, b)(c, d)) = \varphi(a, b)\varphi(c, d)$ , for all  $(a, b), (c, d) \in G$  and so  $\varphi$  is a homomorphism.

Note that  $Ker(\varphi) = \{(a, b) \in G \mid \varphi(a, b) = e_2\}$ . Now we have

$$\varphi(a, b) = e_2 \implies b = e_2 \text{ and } a \in G_1.$$

Therefore we get  $N = Ker(\varphi)$ .

Now from Theorem 2.5.5, we know that  $Ker(\varphi)$  is normal subgroup of  $G$ , as  $\varphi$  is an homomorphism from  $G$  into  $G_2$ . Hence the part (a) proved.

#### Step 4

4 of

**Answer for (b):** Now in order to see  $N \cong G_1$ , let us consider  $\Psi : N \rightarrow G_1$  defined as

$$\Psi(a, e_2) = a, \quad \text{for all } a \in G_1.$$

Clearly,  $\Psi$  is an homomorphism, as for  $(a, e_2), (c, e_2) \in N$ ,

$$\Psi((a, e_2)(c, e_2)) = \Psi(ac, e_2) = ac = \Psi(a, e_2)\Psi(c, e_2)$$

Also  $\Psi$  is onto  $G_1$ , as for any  $a \in G_1$ , we have  $\Psi(a, e_2) = a$ .

Clearly  $\Psi$  is an one-one map, as

$$Ker(\Psi) = \{(a, e_2) \in N \mid \Psi(a, e_2) = e_1\} = \{e_1\}$$

Hence  $\Psi$  is an isomorphism and so  $N \cong G_1$ .

**Answer for (c):** From part (a), we know that  $\text{Ker}(\varphi) = N$  and  $\varphi$  is an homomorphism. Now in-order to apply first homomorphism theorem we need to verify  $\varphi$  is onto.

Let  $b \in G_2$ , then for any  $a \in G_1$ , we get  $\varphi(a, b) = b$  and so  $\varphi$  is onto  $G_2$ .

Therefore, by first homomorphism theorem,  $G/N \cong G_2$ .

## Result

6 of 6

[Click Here To See Complete Solution.](#)

## 5. a

**Question:** If  $G$  be a group,  $H$  a subgroup of  $G$  and  $N \triangleleft G$ . Let the set  $HN = \{hn \mid h \in H, n \in N\}$ . Prove that:

- sep=0em
  - a.  $H \cap N \triangleleft H$ .
  - b.  $HN$  is a subgroup of  $G$ .
  - c.  $N \subset HN$  and  $N \triangleleft HN$ .
  - d.  $(HN)/N \cong H/(H \cap N)$ .

## Step 2

2 of 9

**Answer for (a):** We need to prove  $H \cap N \triangleleft H$ . Let  $h \in H$  and  $x \in H \cap N$ . We have to show  $h^{-1}xh \in H \cap N$

Clearly  $x \in H$  as  $H \cap N \subset H$  and  $x \in N$  as  $H \cap N \subset N$ . Thus we have

$$\begin{aligned} h^{-1}xh &\in H, \quad \text{as } x, h \in H \\ h^{-1}xh &\in N, \quad \text{as } g^{-1}Ng \subset N, \forall g \in G \text{ and } h \in H \subset G. \end{aligned}$$

This give us  $h^{-1}xh \in H \cap N$ , for all  $x \in H \cap N$ .

Therefore, we have  $h^{-1}(H \cap N)h \subset H \cap N$ , for all  $h \in H$  and so  $H \cap N \triangleleft H$ .

**Answer for (b):** We have to show  $HN$  is a subgroup of  $G$ .

**Step 1:** To show  $HN$  closed under multiplication. Let  $h_1, h_2 \in H$  and  $n_1, n_2 \in N$ . We have to show  $(h_1n_1)(h_2n_2) \in HN$ .

Since  $N$  is normal subgroup of  $G$ , therefore  $h_2^{-1}n_1h_2 \in N$ , as  $h_2^{-1}Nh_2 \subset N$ .

Thus  $n_1h_2 = h_2n_3$ , for some  $n_3 \in N$  and so we get

$$(h_1n_1)(h_2n_2) = h_1(n_1h_2)n_2 = h_1(h_2n_3)n_2 = (h_1h_2)(n_3n_2) \in HN.$$

## Step 4

4 of

**Step 2:** Clearly, the identity element  $e \in G$  is in  $HN$ , as  $e \in H$  and  $e \in N$ . Let  $h \in H$  and  $n \in N$ . We have to show  $(hn)^{-1} \in H$ .

Notice that  $hN = Nh$ , for all  $h \in H$ , as  $N \triangleleft G$ . Thus we get

$$(hn)^{-1} = n^{-1}h^{-1} \in Nh^{-1} = h^{-1}N \subset HN.$$

Therefore, the inverse of every element in  $HN$  is also in  $HN$ .

Hence  $HN$  is a subgroup of  $G$ .

**Answer for (c):** First notice that  $N \subset HN$ , as for  $n \in N$  we have  $n = en \in HN$ , where  $e \in H \subset G$ .

Now we have to show  $N \triangleleft HN$ . Let  $h \in H$  and  $n \in N$ . Notice that  $h^{-1}Nh \subset N$ , as  $N$  is normal subgroup in  $G$ . Then we have

$$(hn)^{-1}N(hn) = n^{-1}(h^{-1}Nh)n \subset n^{-1}Nn = N$$

Hence  $N$  is normal subgroup of  $HN$ .

### Step 6

**Answer for (d):** From earlier part we know that  $H \cap N \triangleleft H$  and  $N \triangleleft HN$ .

Now let us define a map from  $\Psi : H/(H \cap N) \rightarrow (HN)/N$  as

$$\Psi(h(H \cap N)) = hN, \quad \text{for all } h \in H.$$

Now we have to verify  $\Psi$  well-defined.

To do this, let  $h \in H$  then  $h = he \in HN$  and so  $\Psi$  sends cosets of  $H \cap N$  to cosets of  $N$ . Again let  $h_1, h_2 \in H$  such that  $h_1(H \cap N) = h_2(H \cap N)$ . This gives us

$$h_1h_2^{-1} \in H \cap N \implies h_1h_2^{-1} \in N \implies h_1N = h_2N \implies \Psi(h_1(H \cap N)) = \Psi(h_2(H \cap N)).$$

Hence  $\Psi$  is well defined.

Now we show  $\Psi$  is injective. Let  $h_1, h_2 \in H$  and  $\Psi(h_1(H \cap N)) = \Psi(h_2(H \cap N))$ . Thus we get  $h_1N = h_2N \implies h_1h_2^{-1} \in N$ . But  $h_1, h_2 \in H$ , give us  $h_1h_2^{-1} \in H \cap N$ , so we get  $h_1$  and  $h_2$  are in the same coset of  $H \cap N$ . Thus,  $h_1(H \cap N) = h_2(H \cap N)$  and so  $\Psi$  is injective.

Now we show  $\Psi$  is surjective. Let  $g = hn \in HN$ , where  $h \in H$  and  $n \in N$ . Then we have

$$gN = (hn)N = h(nN) = hN.$$

Therefore we get  $\Psi(h(H \cap N)) = hN = gN$  and so  $\Psi$  is surjective.

### Step 8

8 of 9

Finally we show  $\Psi$  is homomorphism. Let  $h_1, h_2 \in H$ .

$$\begin{aligned} \Psi(h_1(H \cap N)h_2(H \cap N)) &= \Psi(h_1h_2(H \cap N)) \\ &= (h_1h_2)N \\ &= (h_1N)(h_2N) \\ &= \Psi(h_1(H \cap N))\Psi(h_2(H \cap N)) \end{aligned}$$

Thus  $\Psi$  is a homomorphism.

### Result

Therefore,  $\Psi$  is an isomorphism and so  $(HN)/N \cong H/(H \cap N)$ .

6. a

**Question:** If  $G$  is a group and  $N \triangleleft G$ , show that if  $a \in G$  has finite order  $o(a)$ , then  $Na$  in  $G/N$  has finite order  $m$ , where  $m|o(a)$ . (Prove this by using the homomorphism of  $G$  onto  $G/N$ .)

## Step 2

2 of 5

Let us define a map  $\varphi : G \rightarrow G/N$  by  $\varphi(g) = Ng$ , for all  $g \in G$ . Clearly,  $\varphi$  is an homomorphism, as for  $g, h \in G$  we have

$$\varphi(gh) = N(gh) = (Ng)(Nh) = \varphi(g)\varphi(h).$$

Also note that  $\varphi$  is onto, as for given  $gN \in G/N$ , we have  $\varphi(g) = gN$ . Therefore  $\varphi(G) = G/N$ .

## Step 3

3 of 5

Suppose  $a \in G$ . Assume that  $o(a) = n$ . (Note  $N$  is the identity element in  $G/N$ ) Now using the fact  $\varphi$  is an homomorphism we get

$$(\varphi(a))^n = \varphi(a^n) = \varphi(e) = N.$$

Therefore order of the element  $\varphi(a)$  is less than  $n$  and so finite.

Let  $o(\varphi(a)) = m$  and  $d = \gcd(m, n)$ . Then there exist two integers  $u$  and  $v$  such that  $d = mu + nv$ . Then we get

$$(\varphi(a))^d = (\varphi(a))^{mu}(\varphi(a))^{nv} = ((\varphi(a))^m)^u((\varphi(a))^n)^v = N^uN^v = N$$

Now  $d = \gcd(m, n)$  so  $d \leq m$ . But  $o(\varphi(a)) = m$  so  $d = m$ . Again  $d = \gcd(m, n)$  give us  $d|n$  and so  $m|n$ , that means  $m|o(a)$ .

## Result

5 of 5

Click here to see the solution.

## 7. a

**Given:** Let  $\phi$  be an onto homomorphism between two groups  $G$  and  $G'$ , and  $N$  be a normal subgroup of  $G$ .

**To Prove:**  $\phi(N)$  is a normal subgroup of  $G'$ .

## Step 2

2 of 4

**Proof:** We first assert that  $\phi(N)$  is a subgroup of  $G'$ .

Since  $N$  is a subgroup of  $G$ ,  $e_G \in N$ , where  $e_G$  is the identity element of  $G$ .

As  $\phi(e_G) \in \phi(N)$ ,  $\phi(N)$  is a non-empty subset of  $G'$ .

Let  $a', b' \in \phi(N)$ .

Then there exist elements  $a, b$  in  $N$  such that  $\phi(a) = a'$ ,  $\phi(b) = b'$ .

Since  $N$  is a subgroup,  $a \in N, b \in N \implies ab^{-1} \in N$ .

Therefore  $\phi(ab^{-1}) \in \phi(N)$ .

Now,  $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\{\phi(b)\}^{-1} = a'(b')^{-1} \in \phi(N)$ .

Therefore  $a' \in \phi(N), b' \in \phi(N) \implies a'(b')^{-1} \in \phi(N)$ .

**This proves that  $\phi(N)$  is a subgroup of  $G'$ .**

Now, we need to show that  $\phi(N)$  is a normal subgroup of  $G'$ .

Let  $\phi(N) = N'$ , subgroup of  $G'$ .

Let  $x' \in G'$ ,  $h' \in N'$ . Since  $\phi$  is onto, there exist elements  $x \in G$  and  $h \in N$  such that  $\phi(x) = x'$ ,  $\phi(h) = h'$ .

$$x'h'(x')^{-1} = \phi(x)\phi(h)\{\phi(x)\}^{-1}$$

$$= \phi(x)\phi(h)\phi(x^{-1}), \text{ since } \phi \text{ is a homomorphism}$$

$$= \phi(xhx^{-1}). i$$

Since  $N$  is a normal subgroup of  $G$ ,  $x \in G$ ,  $h \in N \implies xhx^{-1} \in N$  and therefore  $\phi(xhx^{-1}) \in \phi(N)$ .

Thus  $x' \in G'$ ,  $h' \in \phi(N)$  implies  $x'h'(x')^{-1} \in \phi(N)$  and this proves that  $\phi(N)$  is a normal subgroup of  $G'$ .

## Result

4 of 4

Click for proof.

# Section 2–8

## 1. a

Assume that  $f(a_1, \dots, a_p) = (a_1, \dots, a_p)$ , then the definition of  $f$  gives us that

$$(a_1, \dots, a_p) = (a_p, a_1, \dots, a_{p-1})$$

i.e.

$$a_1 = a_p, a_2 = a_1, \dots, a_{p-1} = a_{p-2} \text{ and } a_p = a_{p-1}$$

Therefore, from the result above we obtain that

$$a_1 = a_2 = \dots = a_p$$

if  $f(s) = s$ . Hence, must be  $f(s) \neq s$  if some two entries in  $(a_1, \dots, a_p)$  are different.

Order of  $f$  is equal  $p$ , then the orbit of  $f$  has less or equal  $p$  elements. If the orbit has less than  $p$  elements, then there is  $j$  and  $k$  such that  $1 \leq k < j \leq p$  and  $f^j(a_1, \dots, a_p) = f^k(a_1, \dots, a_p)$ .

This result gives us that

$$f^{j-k}(f^k(a_1, \dots, a_p)) = f^k(a_1, \dots, a_p)$$

i.e.

$$f^{j-k}(a_{p-k+1}, \dots, a_p - k) = (a_{p-k+1}, \dots, a_p - k)$$

then using the result above it is not hard to conclude that  $a_1 = a_2 = \dots = a_p$ , but this is not possible.

Therefore, the orbit has  $p$  elements.

## Result

Note that  $f(s) = s$  implies that  $a_1 = a_2 = \dots = a_p$ .

## 2. a

$G$  be a group of order  $35 = 5 \cdot 7$ . Now, by Cauchy's theorem there exists a subgroup of order 7. Now, let there be two distinct subgroups  $A$  and  $B$  of order 7. Now consider the subset of  $G$ ,  $AB$ . We know that  $|AB| = \frac{|A||B|}{|A \cap B|}$ . But  $A \cap B = \{e\}$ . So  $|AB| = 49$ , which is contradiction. So, there is a unique subgroup of order 7, hence normal. Let  $B$  be the unique subgroup of order 7. So,  $B = \langle b \rangle$ , where  $b$  has order 7. also, there exists a subgroup of order 5 generated by  $a$ (say). Now since  $B$  is normal,  $aba^{-1} = b^i$  for some  $i$ . This implies  $b = a^5ba^{-5} = b^{i^5} \implies b^{i^5-1} = e$ . So 7 divides  $i^5 - 1$ . By Fermat's little theorem 7 divides  $i^6 - 1$ . which implies 7 divides  $i - 1$ . So  $i = 1$  and hence  $ab = ba$ . so order of  $ab = 35$ , and hence  $G$  is cyclic

## Result

See the proof

3. a

Group  $\mathbb{G}$  is of finite order  $pq$  and  $A$  is the subgroup of index  $\frac{|G|}{|A|} = \frac{pq}{p} = q$ .

Assume that  $pq$  divides  $q!$ , we obtain that  $p$  divides  $(q-1)!$ . From the fact that  $p$  is prime and  $p > q$  we have that  $p$  can not divide  $(q-1)!$

Therefore, using the result of Problem 40 of Section 5 and the preceding results we obtain that there is a non trivial normal subgroup of  $G$  contained in  $A$ . From the fact that  $A$  is an only non trivial subgroup of  $A$ , we have that  $A$  is normal subgroup of  $G$ .

THE PROOF!

## Result

2 of 2

(HINT:) Group  $\mathbb{G}$  is of finite order  $pq$  and  $A$  is the subgroup of index

$$\frac{|G|}{|A|} = \frac{pq}{p} = q$$

4. a

**To Construct:** A non-abelian group of order 21.

**Construction:**

Let  $G$  be a group of order 21.

Let  $P$  be a

**Sylow-3-subgroup of  $G$ ,  $P \in Syl_3(G)$ , and let  $Q \in Syl_7(G)$ .**

If  $(7 - 1) = 6$  were not divisible by 3, it is easy.

Now,

**$P$  and  $Q$  are unique Sylow subgroups of  $G$  and  $G = P \times Q$ .**

However,  $(7 - 1) = 6$  is divisible by 3.

In this case, we use a **semidirect product**

and

$$G = Q \rtimes_{\phi} P \cong C_7 \rtimes_{\phi} C_3,$$

$$\text{for some } \phi : C_3 \rightarrow Aut(C_7)$$

(We know that

**$Q$  is a unique Sylow-7-subgroup in  $G$ , thus it is normal in  $G$ . However,  $P$  is not a unique Sylow-3-subgroup in  $G$**

).

Since

$$Aut(C_7) \cong \mathbb{Z}_6$$

and  $|Aut(C_7)|$  is divisible by  $|\phi(x)|$ , where  $x$  in  $C_3$ , we see that  $\phi$  is not trivial.

Let  $C_3 = \langle x \rangle$ ,  $C_7 = \langle y \rangle$ ; and let  $a = (y, 1)$ ,  $b = (1, x)$ .

Then  $G = \langle a, b \rangle$  with some relationships, where  $a^7 = 1$  and  $b^3 = 1$ .

Now, consider

$$ba = (1, x)(y, 1) = (1\phi(x)(y), x) = (y^2, x) = a^2b$$

We see that

$$\phi : C_3 \rightarrow Aut(C_7)$$

is defined by

$$x \rightarrow (y \rightarrow y^2)$$

here since  $Aut(C_7)$  is

**cyclic, containing a unique subgroup of order 3 by Cauchy's theorem;**

the latter parenthesis is used to denote the automorphism of order 3.

Thus we have  $G = \langle a, b | a^7 = 1, b^3 = 1, bab^{-1} = a^2 \rangle$ , where  $|G| = 21$ .

## Result

Solution.

5. a

We have  $G$ , a group such that  $|G| = p^n \cdot m$ , and  $(p, m) = 1$ .  $P$  is a normal subgroup of order  $p^n$ . We need to prove that if  $\theta$  is an automorphism then  $\theta(P) = P$ . Now since  $\theta$  is an automorphism,  $\theta(P) = Q$ , where  $Q$  is a normal subgroup of order  $p^n$ . Now If  $P \neq Q$ , then  $|P \cap Q| = p^r$ , where  $r < n$ . Also  $PQ$  is a subgroup, and  $|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{p^{2n}}{p^r} = p^{2n-r}$ . Clearly  $2n - r > n$ . But  $|PQ|$  must divide the order of the group, but the highest power of  $p$  that divides the order of the group is  $n$ , thus giving a contradiction to the fact that  $P \neq Q$ . Hence,  $P = Q$ .

### Result

2 of 2

[See the proof](#)

## 6. a

We use the following formula: If  $G$  be a group and  $A, B$  be subgroups, define  $AB = \{ ab | a \in A, b \in B \}$ , then  $|AB| = \frac{|A||B|}{|A \cap B|}$ . Now we have  $AB \subseteq G$ , so that  $|AB| \leq G$ . Given that  $|A| > \sqrt{G}, |B| > \sqrt{G}$ . Let us suppose that  $A \cap B = \{ e \}$ . So  $|A \cap B| = 1$ . So by the above formula, we have  $|AB| = |A||B| > G$ , which is a contradiction, thus proving the result, that is,  $A \cap B \neq \{ e \}$ .

### Result

[See the proof](#)

## 7. a

We use the following formula: If  $G$  be a group and  $A, B$  be subgroups, define  $AB = \{ ab | a \in A, b \in B \}$ , then  $|AB| = \frac{|A||B|}{|A \cap B|}$ . Now  $|A| = m, |B| = n$  such that  $(m, n) = 1$ . Clearly by lagrange's theorem  $A \cap B = \{ e \}$ . So  $|AB| = |A||B| = mn$ .

### Result

[See the proof](#)

## 8. a

To prove that a group of order 99 has a non-trivial normal subgroup. Now  $|G| = 99 = 9 \cdot 11 = 3^2 \cdot 11$ . Cauchy theorem guarantees that there exists a subgroup of order 11. Now the claim is that There is a unique subgroup of order 11. Let  $A, B$  be distinct subgroups of order 11. Consider the set  $AB$ . Now  $|AB| = \frac{|A||B|}{|A \cap B|}$ . But  $|A \cap B| = \{e\}$ . So  $|AB| = 121 > 99$ , a contradiction. So, there is a unique subgroup of order 11. hence that subgroup is normal, because a well known result asserts that if  $G$  is a group with a unique subgroup  $H$  of order  $n$ , then  $H$  is normal.

### Result

[See the proof](#)

9. a

To prove that a group of order 42 has a non-trivial normal subgroup. Now  $|G| = 42 = 6 \cdot 7 = 2 \cdot 3 \cdot 7$ . Cauchy theorem guarantees that there exists a subgroup of order 7. Now the claim is that There is a unique subgroup of order 7. Let  $A, B$ , be distinct subgroups of order 7. Consider the set  $AB$ . Now  $|AB| = \frac{|A||B|}{|A \cap B|}$ . But  $|A \cap B| = \{e\}$ . So  $|AB| = 49 > 42$ , a contradiction. So, there is a unique subgroup of order 7. hence that subgroup is normal, because a well known result asserts that if  $G$  is a group with a unique subgroup  $H$  of order  $n$ , then  $H$  is normal.

### Result

[See the proof](#)

10. a

In the previous problem with  $|G| = 42$ , we found out that there exists a non-trivial normal subgroup of order 7, call it  $H$ . Consider  $G/H$ . This factor group has order  $6 = 2 \cdot 3$ . Now this group has a normal subgroup of order 3 by the same reason as the previous problem, call that normal subgroup  $K_1$ . so  $K_1 = K/H$  for some normal subgroup  $K$  of  $G$ . and  $|K_1||H| = 21$ .

### Result

2 of 2

[See the proof](#)

11. a

We will prove this result in two case.

**Case-1:** Suppose  $A \cap B = \{e\}$ . We need to show  $AB$  has  $|A||B|$  distinct elements.

## Step 2

2 of 10

Suppose  $AB$  has  $k$  many distinct element. Now by the definition of  $AB$  give us  $k \leq |A||B|$ .

## Step 3

3 of 10

We will show  $k = |A||B|$  by contradiction. If possible let  $k < |A||B|$ . Then there exist  $a \neq a_1 \in A$  such that

$$ab = a_1b_1 \implies a_1^{-1}a = b_1b^{-1}.$$

Clearly  $a_1^{-1}$  and  $a_1^{-1}a$  both are in  $A$  as  $A$  is a subgroup. Similarly  $b^{-1}$  and  $b_1b^{-1}$  both are in  $B$  as  $B$  is a subgroup.

Therefore we have

$$a_1^{-1}a \in A \cap B \implies a_1^{-1}a = e \implies a_1 = a, \text{ a contradiction.}$$

Hence  $k = |A||B|$ .

## Step 5

5 of 10

**Case-2:** Suppose  $A \cap B \neq \{e\}$ . We need to show  $AB$  has  $\frac{|A||B|}{|A \cap B|}$  distinct elements.

## Step 6

6 of 10

Let  $a \in A$  and  $b \in B$ . Then for each  $h \in A \cap B$ .

$$ab = (ah)(h^{-1}b) = a_1b_1$$

Clearly,  $a_1 = ah \in A$ , since  $a \in A$ ,  $h \in A \cap B \subseteq A$  and  $b_1 = h^{-1}b \in K$ , since  $b \in B$ ,  $h^{-1} \in A \cap B \subseteq B$ .

Conversely, assume  $ab = a_1b_1$ , for some  $a_1 \in A, b_1 \in B$ . Then  $a_1^{-1}a = b_1b_1^{-1} = h$ , say. Clearly,  $h \in A$  as  $a, a_1 \in A$  and  $h \in B$  as  $b, b_1 \in B$ . Therefore  $h \in A \cap B$ .

### Step 8

8 of 10

Thus for each element in  $A \cap B$  gives us a duplicate element for  $ab$ . Therefore the element  $ab$  appear in the list of  $AB$  exactly  $|A \cap B|$  times.

### Step 9

9 of 10

Thus number of distinct element in  $AB$  is the total number in the listing of  $AB$ , that is  $|H||K|$  divided by the number of time given element appears, that is  $|A \cap B|$ .

### Result

10 of 10

Hence we get  $AB$  has  $\frac{|A||B|}{|A \cap B|}$  distinct elements.

## 12. a

By Cauchy's theorem (**theorem 2.8.2**) we have that if  $G$  is a group of order 21 then it has an element  $a$  of order 3 and an element  $b$  of order 7. By **exercise 2.5.41** we have that the subgroup generated by  $b$  is normal, so there is some  $i = 0, 1, 2, 3, 4, 5, 6$  such that  $aba^{-1} = b^i$ . We know  $i \neq 0$  since that implies  $ab = a$  and so that  $b = e$ , a contradiction, and we know  $i \neq 1$  since then  $ab = ba$  and this would imply  $G$  is abelian, which we are assuming is not the case.

Now,  $a$  has order 3 so we must have  $b = a^3ba^{-3} = b^{i^3 \pmod{7}}$ , and so  $i$  is restricted by the modular equation  $i^3 \equiv 1 \pmod{7}$ .

$x$	$x^3 \pmod{7}$
2	1
3	6
4	1
5	6
6	6

Therefore the only options are  $i = 2$  and  $i = 4$ . Now suppose  $G$  is such that  $aba^{-1} = b^2$  and let  $G'$  be another group of order 21 with an element  $c$  of order 3 and an element  $d$  of order 7 such that  $cdc^{-1} = d^4$ . We now prove that  $G$  and  $G'$  are isomorphic. Define

$$\begin{aligned}\phi : G &\rightarrow G' \\ a &\mapsto c^{-1} \\ b &\mapsto d\end{aligned}$$

since  $a$  and  $c^{-1}$  have the same order and  $b$  and  $d$  have the same order this is a well defined function. Since

$$\begin{aligned}\phi(a)\phi(b)\phi(a)^{-1} &= c^{-1}dc \\ &= (cd^{-1}c^{-1})^{-1} \\ &= (d^{-4})^{-1} \\ &= d^4 \\ &= (d^2)^2 \\ &= \phi(b)^2\end{aligned}$$

$\phi$  is actually a homomorphism. For any  $c^i d^j \in G'$  we have  $\phi(a^{-i} b^j) = c^i d^j$  so  $\phi$  is onto and  $\phi(a^i b^j) = c^{-i} d^j = e$  only if  $i = j = 0$ , so  $\phi$  is 1-to-1. Therefore  $G$  and  $G'$  are isomorphic and so up to isomorphism there is only one nonabelian group of order 21.

## Result

2 of 2

For a group of order 21 there are elements  $a$  of order 3 and  $b$  of order 7. If  $G$  is not abelian the only possible results for  $aba^{-1}$  are either  $b^2$  and  $b^4$ , and a choice fixes the rest of the structure of  $G$ . We can show that the resulting groups for either choices are isomorphic, so actually up to isomorphism there is a unique nonabelian group of order 21.

13. a

**To Prove:** Any group of order 99 is abelian.

### Proof:

Let  $G$  be a group of order 99.

Now,  $99 = 11 \cdot 3^2$ .

Let

$n_3$  be the number of Sylow-3-subgroups of  $G$ .

Then  $n_3 = 3k + 1$  for some integer  $k \geq 0$  and  $n_3$  divides 99.

It follows that

$G$  has unique Sylow-3-subgroup, say  $H$  which is normal in  $G$  and  $|H| = 9$ .

Similarly let  $n_{11}$  be the number of Sylow-11-subgroups of  $G$ .

Then  $n_{11} = 11k' + 1$  for some integer  $k' \geq 0$  and  $n_{11}$  divides 99.

It yield's that

$G$  has unique Sylow-11-subgroup, say  $K$  which is normal in  $G$  and  $|K| = 11$ .

Then  $H \cap K = \{e\}$  and  $|HK| = |H||K| = 99$

implies that

$$G = HK.$$

Thus  $G$  is an **internal direct product** of  $H$  and  $K$ .

Hence,

$$G \cong H \times K.$$

Since  $|H| = 3^2$ , so  $H$  is **abelian** and  $|K| = 11$  implies that  $K$  is **abelian**.

Therefore  $G$  is abelian.

This completes the proof.

## Result

Click for proof.

14. a

Suppose  $G$  is a group of order  $pq$ . By Cauchy's theorem (**theorem 2.8.2**) in  $G$  there is an element  $a$  of order  $q$  and an element  $b$  of order  $p$ . Since  $i_G(\langle b \rangle) = q$  and  $pq \nmid q!$  (since  $q < p$ ) we have by **exercise 2.5.40** that the subgroup generated by  $b$  is normal. Therefore there is some  $i \in \mathbb{Z}_p$  such that  $aba^{-1} = b^i$ . The whole group structure of  $G$  is determined by this choice of  $i$ , and it will be nonabelian if  $i \neq 1$ . We can't choose arbitrarily since the choice must be consistent with the relations  $a^q = b^p = e$ .

Now, we know  $U_p$  has  $p - 1$  elements and is cyclic. Suppose  $k$  generates  $U_p$ . Since  $q \mid p - 1$  we may set  $i = k^{\frac{p-1}{q}}$ . We then have that  $b = a^pba^{-p} = (b^{(k^{\frac{p-1}{q}})^q}) = b^{k^{p-1}} = b$ , which shows us that indeed this choice of  $i$  is consistent with the other relations and gives us a nonabelian group of order  $pq$ .

## Result

2 of 2

For  $a$  an element of order  $q$ ,  $b$  an element of order  $p$  and  $k$  a generator of  $U_p$  we may define a nonabelian group of order  $pq$  by setting the relation  $aba^{-1} = b^{k^{\frac{p-1}{q}}}$ .

15. a

Consider the construction of the nonabelian group of order  $pq$  in exercise 14. There the structure of the group  $G$  is set by determining the relation  $aba^{-1} = b^{k^{\frac{p-1}{q}}}$  for some generator  $k$  of the cyclic group. Here we are using the fact that  $k^{\frac{p-1}{q}}$  is a generator for the unique subgroup of order  $q$  in  $U_p$  (a cyclic group of order  $m$  has a unique subgroup of order  $d$  for each divisor  $d$  of  $m$ ). The other possible generators of this subgroup are  $k^{\frac{l(p-1)}{q}}$  for each  $1 \leq l \leq q - 1$ , so these give potentially new group structures. Let  $G'$  be a group with an element  $c$  of order  $q$ , an element  $d$  of order  $p$  with structure defined by the relation  $cdc^{-1} = d^{k^{\frac{l(p-1)}{q}}}$ . We may then define

$$\begin{aligned}\phi : G' &\rightarrow G \\ c &\mapsto a^l \\ d &\mapsto b\end{aligned}$$

since  $c$  and  $a^l$  have the same order and  $b$  and  $d$  have the same order this is a well defined function. Since

$$\begin{aligned}\phi(c)\phi(d)\phi(c)^{-1} &= a^lba^{-l} \\ &= b^{(k^{\frac{p-1}{q}})^l} \\ &= b^{k^{\frac{l(p-1)}{q}}} \\ &= \phi(d)^{k^{\frac{l(p-1)}{q}}}\end{aligned}$$

$\phi$  is actually a homomorphism. For any  $a^i b^j \in G$  we have  $\phi(a^i b^j) = a^i b^j$  so  $\phi$  is onto and  $\phi(c^i d^j) = a^{il} b^j = e$  only if  $i = j = 0$ , so  $\phi$  is 1-to-1. Therefore  $G$  and  $G'$  are isomorphic and so up to isomorphism there is only one nonabelian group of order  $pq$ .

## Result

The argument is similar to the one in [exercise 12](#).

# Section 2–9

1. a

**Given :**  $G_1$  and  $G_2$  are two groups.

**To Prove :**  $G_1 \times G_2 \cong G_2 \times G_1$

Let us define a map  $\phi : G_1 \times G_2 \rightarrow G_2 \times G_1$  by

$$\phi(g_1, g_2) = (g_2, g_1) \quad \forall g_1 \in G_1, g_2 \in G_2$$

### Step 2

**Claim :**  $\phi$  is a **group Isomorphism**.

**Proof :** We first show that  $\phi$  is an **Injection**.

Let  $\phi(g_1, g_2) = \phi(g'_1, g'_2)$  for some  $g_1, g'_1 \in G_1$  and  $g_2, g'_2 \in G_2$ .

This implies that  $(g_2, g_1) = (g'_2, g'_1) \implies g_2 = g'_2$  and  $g_1 = g'_1$ .

It follows that  $\phi$  is injective.

Now we show that  $\phi$  is a **surjection**.

Let  $(g_2, g_1) \in G_2 \times G_1$ . Then we observe that for  $(g_1, g_2) \in G_1 \times G_2$ ,

$\phi(g_1, g_2) = (g_2, g_1)$ . This shows that  $\phi$  is onto.

Finally, it suffices to show that  $\phi$  is a **group homomorphism**.

Let  $(g_1, g_2), (g'_1, g'_2) \in G_1 \times G_2$ . Now,

$$\phi((g_1, g_2)(g'_1, g'_2)) = \phi(g_1g'_1, g_2g'_2) = (g_2g'_2, g_1g'_1) = (g_2, g_1)(g'_2, g'_1) = \phi(g_1, g_2)\phi(g'_1, g'_2)$$

**Therefore, being a bijective group homomorphism,  $\phi$  is a group Isomorphism**

## Result

Click for proof.

2. a

It is given that  $G_1$  and  $G_2$  are cyclic groups of orders  $m$  and  $n$ . Let  $a \in G_1$  and  $b \in G_2$  be generator of  $G_1$  and  $G_2$ , respectively. Then we know that  $o(a) = m$  and  $o(b) = n$ . Let us first prove the following lemma.

## Step 2

2 of 6

**Lemma.** Show that order of the element  $(a, b) \in G_1 \times G_2$  is the least common multiple of  $m$  and  $n$ , that means,  $o(a, b) = \text{lcm}(m, n)$ .

## Step 3

3 of 6

### Proof of the Lemma:

To verify this, note the following  $(a, b)^k = (a^k, b^k)$ , for all positive integer  $k$ . Now let  $p$  is the order of the element  $(a, b)$ . Then we have  $(a, b)^p = (e_1, e_2)$ , where  $e_i$  is the identity element in  $G_i$ , for  $i = 1, 2$ . This gives us

$$a^p = e_1 \quad \text{and} \quad b^p = e_2 \implies m|p \quad \text{and} \quad n|p \implies \text{lcm}(m, n)|p.$$

Again notice that

$$(a, b)^{\text{lcm}(m, n)} = (a^{\text{lcm}(m, n)}, b^{\text{lcm}(m, n)}) = (e_1, e_2)$$

Therefore we have  $p = \text{lcm}(m, n)$ . Hence its proved the Lemma.

Note that the lemma is true for any two graphs  $G_1$  and  $G_2$ , irrespective of cyclic.

Now suppose  $m$  and  $n$  are relatively prime. Then the order of the element  $(a, b) \in G_1 \times G_2$  is

$$o(a, b) = \text{lcm}(m, n) = mn$$

Notice that  $|G_1 \times G_2| = mn$  and there exist an element  $(a, b) \in G_1 \times G_2$  such that  $o(a, b) = mn$ . Therefore,  $G_1 \times G_2$  is cyclic

## Step 5

5 of 6

Conversely, assume that  $G_1 \times G_2$  is cyclic. We have to show  $m$  and  $n$  are relatively prime.

Suppose that  $\gcd(m, n) = d$  and  $(g_1, g_2)$  is a generator of  $G_1 \times G_2$ . Clearly,  $o(g_1, g_2) = mn$ , as  $|G_1 \times G_2| = mn$

Let  $k = m/d$  and  $\ell = n/d$ . Then  $k, \ell$  are positive integer and so we have

$$(g_1, g_2)^{mn/d} = ((g_1^m)^\ell, (g_2^n)^k) = (e_1^\ell, e_2^k) = (e_1, e_2).$$

Therefore,  $mn = o(g_1, g_2) \leq \frac{mn}{d}$ .

## Result

6 of 6

Hence  $d = 1$  and so  $m$  and  $n$  are relatively prime.

3. a

**(a)** We claim that  $\tau : T \rightarrow G$  defined by  $\tau((g, g)) = g$  is an **Isomorphism**. Let  $(g_1, g_1)$  and  $(g_2, g_2)$  be two elements of  $T$ , then we have

$$\begin{aligned}\tau((g_1, g_1)(g_2, g_2)) &= \tau((g_1g_2, g_1g_2)) \\ &= g_1g_2 \\ &= \tau((g_1, g_1))\tau((g_2, g_2))\end{aligned}$$

from where we see that  $\tau$  is a homomorphism. Furthermore it is one-to-one because if  $\tau((g_1, g_1)) = \tau((g_2, g_2))$ , then  $g_1 = g_2$  from which it follows directly that  $(g_1, g_1) = (g_2, g_2)$ . It is onto because we have  $(g, g) \in T$  for any  $g \in G$ , and thus  $\tau((g, g)) = g$ , i.e.  $g$  is in the image of  $\tau$ .

**(b)** Before proving this, let us note that  $T$  is a subgroup of  $A$  regardless of whether  $G$  is abelian. For let  $(g_1, g_1), (g_2, g_2) \in T$ , then

$$(g_1, g_1)(g_2^{-1}, g_2^{-1}) = (g_1g_2^{-1}, g_1g_2^{-1}) \in T,$$

which implies that  $T$  is a subgroup of  $A$  by criterion proved in exercise 15 in the Subgroups section.

Now suppose  $G$  is abelian, we want to show that  $T$  is a normal subgroup of  $A$ . This is immediate from noting that if  $G$  is abelian then so is  $A$ , and using the fact that **every subgroup of an abelian group is normal**.

To prove the converse, suppose that  $T$  is a normal subgroup of  $A$ . Then, for every  $(g_1, g_2) \in A$  and every  $(g, g) \in T$ , we have  $(g_1, g_2)(g, g)(g_1, g_2)^{-1} \in T$ . In particular let  $g_1, g_2 \in G$  be arbitrary, then  $(g_1, g_2)$  is an element of  $A$  and  $(g_1, g_1) \in T$ , and so

$$\begin{aligned}(g_1, g_2)(g_1, g_1)(g_1, g_2)^{-1} &= (g_1g_1g_1^{-1}, g_2g_1g_2^{-1}) \\ &= (g_1, g_2g_1g_2^{-1}) \in T,\end{aligned}$$

where by the definition of  $T$  we get that  $g_1 = g_2g_1g_2^{-1}$ , i.e.  $g_1g_2 = g_2g_1$ , which means that  $G$  is commutative.

## Result

3 of 3

- a. We define  $\tau : T \rightarrow G$  by  $\tau((g, g)) = g$  and show that it is an isomorphism.
- b. One direction follows from the fact that every subgroup of an abelian group is normal, while for the other we use that fact that  $N$  is a normal subgroup of  $G$  if and only if for every  $g \in G$  and every  $n \in N$  we have  $gng^{-1} \in N$ .

Click for the detailed proof.

4. a

Note, the fact that order of element divide the order of group implies  $\mathbb{P}_i \cap \mathbb{P}_j = \{e\}$  for  $1 \leq i < j \leq k$ . We can prove that  $\mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k < \mathbb{G}$ :

1. Identity element  $e$  is in  $\mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k$ , because each of  $\mathbb{P}_i$   $i = 1, \dots, k$  is subgroup of  $\mathbb{G}$
2. For an arbitrary elements  $p_1 p_2 \dots p_k, q_1 q_2 \dots q_k \in \mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k$  the fact that  $\mathbb{G}$  is abelian group gives that

$$p_1 p_2 \dots p_k q_1 q_2 \dots q_k = \underbrace{p_1}_{\in \mathbb{P}_1} \underbrace{q_1}_{\in \mathbb{P}_2} \underbrace{p_2}_{\in \mathbb{P}_2} \dots \underbrace{p_k}_{\in \mathbb{P}_k} \underbrace{q_2}_{\in \mathbb{P}_k} \dots \underbrace{q_k}_{\in \mathbb{P}_k} \in \mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k$$

3. For an arbitrary element  $p_1 p_2 \dots p_k \in \mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k$ , we have that  $p_1^{-1} p_2^{-1} \dots p_k^{-1} \in \mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k$ , each of  $\mathbb{P}_i$   $i = 1, \dots, k$  is subgroup of  $\mathbb{G}$ . Therefore, the fact that  $\mathbb{G}$  is abelian group gives that

$$p_1^{-1} p_2^{-1} \dots p_k^{-1} = (p_1 p_2 \dots p_k)^{-1}$$

Results from (1), (2) and (3) implies that  $\mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k < \mathbb{G}$

Note that each element  $p \in \mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k$  has unique representation, i.e. there are unique element  $p_i \in \mathbb{P}_i$   $i = 1, \dots, k$  such that  $p = p_1 p_2 \dots p_k$  (This follows from  $p_1 \dots p_k = q_1 \dots q_k \Leftrightarrow p_i q_i^{-1} = p_1 q_1 \dots p_{i-1} q_{i-1}^{-1} p_{i+1} q_{i+1}^{-1} \dots p_k q_k^{-1}$  and the fact  $\mathbb{P}_i \cap \mathbb{P}_j = \{e\}$  for  $1 \leq i < j \leq k$ )

Further, using the results above we obtain that

$$|\mathbb{P}_1 \mathbb{P}_2 \dots \mathbb{P}_k| = |\mathbb{P}_1| \cdot |\mathbb{P}_2| \cdot \dots \cdot |\mathbb{P}_k| = |G|$$

then this and the fact  $\mathbb{P}_i$   $i = 1, \dots, k$  is normal subgroup of  $\mathbb{G}$  ( $\mathbb{G}$  is abelian and for each subgroup we have that it is normal) implies that  $\mathbb{G}$  is the internal direct product of  $\mathbb{P}_i$   $i = 1, \dots, k$ .

Finally, using the [Theorem 2.9.4.](#) we have the proof!

## Result

Use the [Theorem 2.9.4.](#)

### 5. a

Let us define a map  $\Psi : N_1 \times N_2 \times \dots \times N_k \rightarrow G$  by

$$\Psi(n_1, n_2, \dots, n_k) = n_1 n_2 \dots n_k, \quad \text{for all } n_i \in N_i, i = 1, 2, \dots, k.$$

It is given that  $G = N_1 N_2 \dots N_k$  and so  $\Psi$  is a surjective map.

Now notice that

$$|N_1 \times N_2 \times \dots \times N_k| = |N_1| |N_2| \dots |N_k| = |G|.$$

Since  $G$  and  $N_1 \times N_2 \times \dots \times N_k$  both are finite set with same number of elements and  $\Psi$  is surjective and so  $\Psi$  is injective.

## Step 2

2 of 3

Therefore  $\Psi$  is a bijective map and so for every element  $g \in G$  there exist an unique element in  $N_1 \times N_2 \times \dots \times N_k$ , say  $(n_1, n_2, \dots, n_k) \in \prod_{i=1}^k N_i$  such that  $\Psi(n_1, n_2, \dots, n_k) = g$ . That means, for every element  $g \in G$  can be uniquely represented in the form  $g = n_1 n_2 \dots n_k$  with  $n_i \in N_i$  for all  $i = 1, 2, \dots, k$ .

## Result

Therefore,  $G$  is the direct product of  $N_1, N_2, \dots, N_k$ .

## 6. a

We have to show that every element  $g \in G$  can uniquely represent of the form  $g = n_1 n_2 \cdots n_k$  with  $n_i \in N_i$  for all  $i = 1, 2, \dots, k$ .

### Step 2

2 of 10

Let  $g \in G$  such that

$$g = n_1 n_2 \cdots n_k = m_1 m_2 \cdots m_k, \quad \text{for all } n_i, m_i \in N_i, i = 1, 2, \dots, k.$$

We need to show that  $n_i = m_i$ , for all  $i$ .

### Step 3

3 of 10

Notice that, for  $i \neq j$ ,  $N_j \subseteq (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_k)$  and therefore

$$N_i \cap N_j \subseteq N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_k) = (e).$$

As  $N_i$  are normal subgroup of  $G$  with  $N_i \cap N_j = (e)$ , for all  $i \neq j$ , so from Lemma 2.9.2 of Page 94, we get if  $a \in N_i$  and  $b \in N_j$  then  $ab = ba$ , for all  $i \neq j$ . In particular  $n_i n_j = n_j n_i$  and  $n_i m_j = m_j n_i$ , for all  $i \neq j$ .

### Step 5

5 of 10

Now for a fixed  $i$ , let  $p = n_1 \cdots n_{i-1}$ ,  $q = n_{i+1} \cdots n_k$  and  $r = m_1 \cdots m_{i-1}$ ,  $s = m_{i+1} \cdots m_k$ . Then from  $n_1 n_2 \cdots n_k = m_1 m_2 \cdots m_k$  we have

$$pn_i q = rm_i s \implies r^{-1}pn_i = m_i s q^{-1} \implies n_i m_i^{-1} = p^{-1}rsq^{-1}$$

### Step 6

6 of 10

Therefore, we get

$$n_i m_i^{-1} = (n_{i-1}^{-1} \cdots n_1^{-1})(m_1 \cdots m_{i-1} m_{i+1} \cdots m_k)(n_k^{-1} \cdots n_{i+1}^{-1})$$

Now after repeatedly applying the fact that any two element from distinct  $N_i$ 's are commutative we get

$$n_i m_i^{-1} = (n_1^{-1} m_1) \cdots (n_{i-1}^{-1} m_{i-1}) (n_{i+1}^{-1} m_{i+1}) \cdots (n_k^{-1} m_k)$$

### Step 8

8 of 10

Clearly  $(n_1^{-1} m_1) \cdots (n_{i-1}^{-1} m_{i-1}) (n_{i+1}^{-1} m_{i+1}) \cdots (n_k^{-1} m_k) \in N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_k$  and so we get

$$n_i m_i^{-1} = N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_k) \implies n_i m_i^{-1} = (e) \implies n_i = m_i$$

### Step 9

9 of 10

Thus  $n_i = m_i$ , for all  $i = 1, 2, \dots, k$ . Hence every element  $g \in G$  can uniquely represent of the form  $g = n_1 n_2 \cdots n_k$  with  $n_i \in N_i$  for all  $i = 1, 2, \dots, k$ .

### Result

10 of 10

Therefore,  
 $G$  is the direct  
product of  $N_1, N_2, \dots, N_k$ .

## Section 2–10

### 1. a

**Given:**  $A$  is a normal subgroup of a group  $G$  and there is an element  $b \in G$  such that  $o(b) = p$ , where  $p$  is a prime and  $b \notin A$ .

**To prove:**  $A \cap (b) = (e)$

### Step 2

2 of 3

**Proof:** Now  $b$  is an element of order  $p$  in  $G$  implies that  $(b)$  is a cyclic group of order  $p$ .

Since  $A$  is a subgroup of  $G$ ,  $A \cap (b)$  is a subgroup of  $G$ . Also  $A \cap (b) \subseteq (b)$ .

So  $A \cap (b)$  is a subgroup of  $(b)$ . Since  $(b)$  is a cyclic group of order  $p$ , the only subgroups of  $(b)$  are  $(e)$  and  $(b)$  itself.

Therefore, either  $A \cap (b) = (e)$  or  $A \cap (b) = (b)$ .

If  $A \cap (b) = (e)$  then we are done.

Otherwise, if  $A \cap (b) = (b)$  then  $A \subseteq (b)$ . Since  $A$  is a subgroup of  $G$  and  $A \subseteq (b)$ , it follows that  $A$  is a subgroup of  $(b)$ .

Since the only subgroups of  $(b)$  are  $(e)$  and  $(b)$  itself we have either  $A = (e)$  or  $A = (b)$ .

If  $A = (e)$ , then  $A \cap (b) = (e)$  and we are done.

But if  $A = (b)$ , then  $b \in A$  as  $b \in (b)$ , which contradicts our hypothesis that  $b \notin A$ . So  $A \neq (b)$ .

Hence  $A \cap (b) \neq (b)$ .

Therefore,  $A \cap (b) = (e)$ .

This completes our proof.

## Result

Click for proof.

### 2. a

From the fact that order of each element  $x \in \mathbb{G}$  must divide the order of  $\mathbb{G}$ , we obtain  $o(x)$  must be of the form  $p^j$  for some  $j \in \{1, \dots, n\}$  and  $p^j \leq o(a)$ .

For element  $a$  of maximal order, there exist  $\ell \in \{1, \dots, n\}$  such that  $o(a) = p^\ell$ .

Let consider an arbitrary element  $x \in \mathbb{G}$ . We noted that its order is of the form of the form  $p^j$  for some  $j \in \{1, \dots, n\}$  and  $p^j \leq o(a)$ , so that

$$x^{o(a)} = x^{p^\ell} = x^{p^{\ell-j} \cdot p^j} = (x^{p^j})^{p^{\ell-j}} = e^{p^{\ell-j}} = e$$

Hence, the proof!

## Result

Use the fact that order of each element  $x \in \mathbb{G}$  must divide the order of  $\mathbb{G}$

### 3. a

a)

It is not hard to conclude that

$$(aN)^{o(a)} = a^{o(a)}N = eN = N$$

and this gives us  $o(aN)$  divides  $o(a)$ . Also,  $o(aN) \leq o(a)$ .

b)

Further, from the fact that

$$N = (aN)^{o(aN)} = a^{o(aN)}N$$

we obtain  $a^{o(aN)} \in N$ . Further, the facts that  $a^{o(aN)} \in (a)$  and  $(a) \cap N = \{e\}$  give us that  $a^{o(aN)} = e$ . Therefore,  $o(a)$  divides  $o(aN)$  and  $o(a) \leq o(aN)$ .

Finally, the inequalities  $o(a) \leq o(aN)$  and  $o(aN) \leq o(a)$  implies that

$$o(a) = o(aN)$$

## Result

(HINT:) Use the fact if  $a^m = e$ , then  $o(a) \mid m$ .

## Section 2–11

1. a

The group  $S_3$  has only 6 elements, so it is easy to verify by direct inspection that there are 3 conjugacy classes:

$$\{\{()\}, \{(12), (13), (23)\}, \{(123), (132)\}\}$$

The class equation then holds since, using **theorem 2.11.2**, we have

$$\begin{aligned} i_{S_3}(C(())) + i_{S_3}(C((12))) + i_{S_3}(C((123))) &= |\text{cl}(())| + |\text{cl}((12))| + |\text{cl}((123))| \\ &= 1 + 3 + 2 = 6 \\ &= |S_3|. \end{aligned}$$

### Result

2 of 2

The conjugacy classes are

$$\{\{()\}, \{(12), (13), (23)\}, \{(123), (132)\}\}$$

The class equation can then be easily verified using **theorem 2.11.2**.

2. a

Let  $r$  be the  $90^\circ$  counterclockwise rotation and  $s$  the vertical reflection in  $G$ . The dihedral group  $G$  has only 8 elements, so it is easy to verify by direct inspection that there are 5 conjugacy classes:

$$\{\{id\}, \{r^2\}, \{r, r^3\}, \{s, r^2s\}, \{rs, r^3s\}\}$$

The class equation then holds since, using **theorem 2.11.2**, we have

$$\begin{aligned} i_G(C(id)) + i_G(C(r^2)) + i_G(C(r)) + i_G(C(s)) + i_G(C(rs)) \\ = \text{cl}(id) + \text{cl}(r^2) + \text{cl}(r) + \text{cl}(s) + \text{cl}(rs) \\ = 1 + 1 + 2 + 2 + 2 \\ = |G|. \end{aligned}$$

### Result

2 of 2

The conjugacy classes are

$$\{\{id\}, \{r^2\}, \{r, r^3\}, \{s, r^2s\}, \{rs, r^3s\}\}$$

The class equation then can be easily verified using **theorem 2.11.2**.

3. a

Let  $G$  be a group and  $a \in G$ . To prove  $C(x^{-1}ax) = x^{-1}C(a)x$ . Let  $z \in x^{-1}C(a)x$ . That implies  $z = x^{-1}yx$  for some  $y \in C(a)$  which in turn implies  $y^{-1}ay = a$ . Now  $z^{-1}x^{-1}axz = x^{-1}y^{-1}xx^{-1}axx^{-1}yx = x^{-1}(y^{-1}ay)x = x^{-1}ax$ . So  $z \in C(x^{-1}ax)$ . We get  $x^{-1}C(a)x \subseteq C(x^{-1}ax)$ . In the other direction, Let  $y \in C(x^{-1}ax) \implies y^{-1}x^{-1}axy = x^{-1}ax$ . To show that  $y \in x^{-1}C(a)x$ . Now we have  $(xy^{-1}x^{-1})a(xy^{-1}x^{-1}) = a$ . Let  $z = xyx^{-1} \implies y = x^{-1}zx$ . Now  $z \in C(a)$  because by definition of  $z$ , we have  $z^{-1}az = a$ . so  $y \in x^{-1}C(a)x$ . So,  $C(x^{-1}ax) \subseteq x^{-1}C(a)x$ . So  $C(x^{-1}ax) = x^{-1}C(a)x$ .

### Result

2 of 2

[See the proof](#)

### 4. a

Let  $G$  be a group and  $\phi$  an automorphism of  $G$ . To prove:  $C(\phi(a)) = \phi(C(a))$ . Let  $y \in C(\phi(a)) \implies y^{-1}\phi(a)y = \phi(a)$ . Now we need to prove that  $y \in \phi(C(a))$ . There exists  $z \in G$  such that  $\phi(z) = y$ . Now,  $\phi(z)^{-1}\phi(a)\phi(z) = \phi(a) \implies \phi(z^{-1}az) = \phi(a) \implies z^{-1}az = a$ , as  $\phi$  is a automorphism. So  $z \in C(a)$ . So  $y \in \phi(C(a))$  as needed. This gives  $C(\phi(a)) \subseteq \phi(C(a))$ . In the reverse direction, Let  $y \in \phi(C(a)) \implies y = \phi(z)$  with  $z \in C(a) \implies z^{-1}az = a$ . We need to prove that  $y \in C(\phi(a))$ . We have  $z^{-1}az = a \implies \phi(z^{-1}az) = \phi(a) \implies y^{-1}\phi(a)y = \phi(a)$ . So  $y \in C(\phi(a))$ . So,  $\phi(C(a)) \subseteq C(\phi(a))$ . So, the equality is proved

### Result

2 of 2

[See the proof](#)

### 5. a

**Given:**  $G$  be a finite group of order  $p^3$ , and  $|Z(G)| \geq p^2$ , where  $p$  is a prime.

**To Prove:**  $G$  is an abelian group.

**Proof:** We first start with a lemma.

**Lemma:** If  $G/Z(G)$  is cyclic, then  $G$  is abelian.

**Proof of the Lemma:** Since  $G/Z(G)$  is cyclic, there is an element  $x \in G$  such that

$$G/Z(G) = \langle xZ(G) \rangle,$$

where  $xZ(G)$  is the coset with representative  $x$ .

Now let  $g \in G$ .

We know that

$$gZ(G) = (xZ(G))^m$$

for some  $m$ .

Then by definition we have

$$(xZ(G))^m = x^m Z(G).$$

Now, in general, if  $H$  is a subgroup of  $G$ , then by definition we can conclude that

$$aH = bH \text{ if and only if } b^{-1}a \in H.$$

Now we have that  $gZ(G) = x^m Z(G)$ , and this happens if and only if  $(x^m)^{-1}g \in Z(G)$ .

Theretofore, there exists a  $z \in Z(G)$  such that

$$(x^m)^{-1}g = z,$$

and so  $g = x^m z$ .

Now let us take  $g_1, g_2 \in G$ . Then there exist  $x_1, x_2 \in G$  and  $z_1, z_2 \in Z(G)$  such that

$$g_1 = x_1^{a_1} z_1 \text{ and } g_2 = x_2^{a_2} z_2.$$

Now,

$$\begin{aligned} g_1 g_2 &= (x_1^{a_1} z_1)(x_2^{a_2} z_2) \\ &= x_1^{a_1} x_2^{a_2} z_1 z_2 \\ &= x^{a_1+a_2} z_2 z_1 \\ &= x^{a_2} x^{a_1} z_2 z_1 \\ &= (x^{a_2} z_2)(x^{a_1} z_1) = g_2 g_1. \end{aligned}$$

Hence we have proved that for any elements  $g_1, g_2 \in G$ ,  $g_1 g_2 = g_2 g_1$ .

So,  $G$  is abelian.

This proves the Lemma.

Now back to our question.

Note that,  $|Z(G)| \geq p^2$ . Then either  $|Z(G)| = p^3$  or  $|Z(G)| = p^2$ .

**Case-1:**  $|Z(G)| = p^3$ .

In this case

$$Z(G) = G.$$

Since  $Z(G)$  is an **abelian subgroup** of  $G$ ,  $G$  is trivially abelian in this case.

#### Step 4

4 of 5

**Case-2:**  $|Z(G)| = p^2$ .

Let us now consider the **quotient group**  $G/Z(G)$ . Since,  $|G| = p^3$  and  $|Z(G)| = p^2$ , then  $G/Z(G)$  is a group of order  $p$ .

Hence  $G/Z(G)$  is a **cyclic group** of order  $p$ .

Now by our Lemma, it follows that  $G$  is abelian.

Consequently,

**In either case we conclude that  $G$  is abelian.**

This completes our proof.

#### Result

5 of 5

Being  $|Z(G)| \geq p^2$ , we made two cases according as  $|Z(G)| = p^3$  or  $|Z(G)| = p^2$ . Then by using above Lemma, we have proved in each case that  $G$  is an abelian group.

Click for the detailed proof.

#### 6. a

let  $G$  be a group and  $P$  a sylow-p subgroup. Given  $P$  is normal. By sylow second theorem the sylow-p subgroups are conjugate. Let  $K$  be any other sylow-p subgroup. Then there exists  $g \in G$  such that  $K = gPg^{-1}$ . But since  $P$  is normal  $K = gPg^{-1} = P$ . Hence the sylow-p subgroup is unique.

#### Result

2 of 2

See the proof

#### 7. a

Let  $\phi$  be an automorphism of  $G$ . Let  $P$  be a normal sylow p-subgroup.  $\phi(P)$  is also a sylow-p subgroup. But since  $P$  is normal, it is unique. Hence  $\phi(P) = P$ .

#### 8. a

Cauchy's Theorem: Let a prime  $p$  divides the order of group  $G$  then there is an element whose order is prime.

Proof: If  $|G| = p$ , then the group is cyclic whose generator is of order  $p$  therefore we suppose  $|G| > p$ .

Case 1: Suppose  $G$  is abelian. We prove the result using induction. Let this be true for all groups whose order is less than that of  $G$ . If  $G$  is cyclic then  $|G| = np$  for some  $n$  hence there is an element  $g^n$  whose order is prime. If  $G$  is not cyclic, then there is non-trivial subgroup  $H = \langle h \rangle$ . Since  $G$  is abelian,  $H$  is normal in  $G$ . Therefore  $p$  divides either  $|H|$  or  $|G/H|$ . If  $p$  divides  $|H|$  then by induction hypothesis, the result is true. Suppose  $p \mid |G/H|$  then since  $|G/H| < |G|$  there is element  $gH \in G/H$  such that  $(gH)^p = H$ . This gives

$$(gH)^p = g^pH = H$$

therefore  $g^p = e$  which shows the existence of element whose order is  $p$ .

Case 2. Suppose  $G$  is not abelian, if  $p \mid |Z(G)|$  then  $|Z(G)| < |G|$  hence by induction hypothesis there is  $g \in Z(G)$  such that  $g^p = e$ . If  $p \nmid |Z(G)|$  then consider the class equation

$$|G| = |Z(G)| + \sum_{i=1, g_i \notin Z(G)}^r |[G : C_G(g_i)]|$$

Since  $p \nmid |Z(G)|$ , then  $p \nmid |[G : C_G(g_i)]|$  for at least one  $i$ , therefore  $p \mid |C_G(g_i)|$  since  $p \mid |G|$ . Since centralizer of  $g_i$  is a group whose order is less than that of  $G$ , by induction there must be element of order  $p$ . This completes the proof.

## 9. a

Given  $H$  is subgroup of  $G$  and  $N(H) = \{x \in G \mid x^{-1}Hx = H\}$ . Then  $N(H) \leq G$ .

Clearly  $e \in N(H)$  since  $e^{-1}He = H$ . For  $x, y \in N(H)$ ,  $(xy)^{-1}H(xy) = y^{-1}(x^{-1}Hx)y = y^{-1}Hy = H$  so  $xy \in N(H)$ .  $x^{-1}Hx = H \implies xHx^{-1} = H$  therefore  $x^{-1} \in H$ . Therefore  $N(H)$  is subgroup of  $G$ .

For all  $x \in H$ ,  $x^{-1}Hx = H$  since  $H$  is subgroup and remains closed therefore  $x \in N(H)$ . This shows  $H \triangleleft N(H)$ .

## 10. a

To prove :  $N(x^{-1}Hx) = x^{-1}N(H)x$ . By definition,  $N(H) = \{x \in G \mid x^{-1}Hx = H\}$ . Let  $y \in N(x^{-1}Hx) \implies y^{-1}x^{-1}Hxy = x^{-1}Hx$ . To prove that  $y \in x^{-1}N(H)x$ . We have  $(xy^{-1}x^{-1})H(xy^{-1}x^{-1}) = H$ . Let  $z = xy^{-1}x^{-1} \implies y = x^{-1}zx$ . Now, by definition of  $z$ , we have  $z^{-1}Hz = H$ . Hence,  $z \in N(H)$ . So  $y \in x^{-1}N(H)x$ . Therefore,  $N(x^{-1}Hx) \subseteq x^{-1}N(H)x$ . Now, Let  $y \in x^{-1}N(H)x \implies y = x^{-1}zx$ . So,  $z \in N(H) \implies z^{-1}Hz = H$ . To show that  $y \in N(x^{-1}Hx)$ . Now  $y^{-1}(x^{-1}Hx)xy = (x^{-1}zx)^{-1}(x^{-1}Hx)x^{-1}zx = (x^{-1}z^{-1}x)(x^{-1}Hx)(x^{-1}zx) = x^{-1}z^{-1}Hzx = x^{-1}Hx$ . so  $y \in N(x^{-1}Hx)$ . Hence  $x^{-1}N(H)x = N(x^{-1}Hx)$ .

### Result

See the proof

## 11. a

Let  $H$  be a sylow-p subgroup of  $G$ . Since  $|N(H)|$  divides  $|G|$ , so the power of the prime  $p$  occurring in  $|N(H)|$  is same as that occurring in  $|G|$ , hence  $H$  is a p-sylow subgroup of  $N(H)$ . We have to prove that  $H$  is the only sylow-p subgroup inside  $N(H)$ . Now suppose on the contrary that  $K$  is another p-sylow subgroup distinct from  $H$  inside  $N(H)$ . Now we have  $H$  is normal in  $N(H)$ . Also observe that  $H$  is a p-sylow subgroup of  $N(H)$ . But then Sylow second theorem asserts that since  $H$  is normal then  $H$  is the only p-sylow subgroup of  $N(H)$ . But then  $K$  is also a p-sylow subgroup of  $N(H)$  for same reason. Hence,  $H = K$ .

### Result

2 of 2

[See the proof](#)

## 12. a

Given that  $G$  is a group and  $P$  be a sylow-p subgroup. Now we have  $a \in G$  of order  $p^m$  such that  $aPa^{-1} = P$ . Hence  $a \in N(P)$ . But since order of  $a$  is  $p^m$ , the subgroup generated by  $a, < a >$  is of order  $p^m$ . Now, this implies that  $< a >$  is contained in sylow-p subgroup of  $G$ , and also contained in  $N(P)$ . But by problem 11 of this same chapter  $P$  is the unique sylow-p subgroup contained in  $N(P)$ , and hence  $< a > \subseteq P$ . In particular  $a \in P$ .

### Result

2 of 2

[See the proof](#)

## 13. a

Let us denote  $i_G(N(H)) = \{ gHg^{-1} | g \in G \}$ . Hence  $C(H)$  is the number of conjugates of  $H$  in  $G$ . Let  $P$  be the set of all distinct subgroups of  $G$ . Now, We know that  $G$  acts on  $P$  by conjugation, that is, if  $H \in P$ , then  $g.P = gPg^{-1}$ . This is clearly a group action. Now let us clearly observe what is  $C(H)$ . It is very clear that  $C(H)$  is nothing but the orbit of  $H$  under this group action. Now we use the orbit stabilizer theorem which states that if a group  $G$  acts on a set  $A$  then  $|o(a)| = \frac{|G|}{|Stab_G(a)|}$ , where  $o(a)$  denotes orbit of  $a \in A$  and  $Stab_G(a) = \{ g \in G : g.a = a \}$ . Now since  $|o(H)| = |N(H)|$  we need to determine what is  $Stab_G(H)$  which is by definition  $\{ g \in G : gHg^{-1} = H \}$ . But then,  $Stab_G(H)$  is basically  $N(H)$ , i.e, the normalizer of  $H$ . Hence we have  $|C(H)| = \frac{|G|}{|N(H)|} = [G : N(H)] = i_G(N(H))$ , by the orbit-stabilizer theorem.

### Result

[See the proof](#)

## 14. a

Let  $G$  be a group and  $P$  be a sylow-p subgroup. We need to prove that the number of conjugates of  $P$ , that is the cardinality of the set  $\{x^{-1}Px | x \in G\}$  is not a multiple of  $p$ . Now we already have proved that given a subgroup  $H$ , the number of distinct conjugates is  $i_G(H)$  (see problem 13 of this chapter). So, in this case we have that the number of distinct conjugates is  $i_G(N(P))$ . Now if  $|G| = p^n \cdot m$  such that  $(m, p) = 1$ . So,  $|P| = p^n$ . We know that  $P \subset N(P)$ , hence  $|N(P)| = p^n \cdot k$  such that  $p^n \cdot k \mid p^n \cdot m$ , by lagrange' theorem, so  $k \mid m$ , or in other words  $m/k$  is an positive integer, and  $p \nmid \frac{m}{k}$ . But observe that  $i_G(N(P)) = \frac{m}{k}$ . So we have  $p \nmid i_G(N(P))$  and hence we have the required result.

### Result

See the proof

## 15. a

If  $N \triangleleft G$  and  $B(N) = \{x \in G \mid xa = ax \quad \forall a \in N\}$  then  $B(N) \triangleleft G$ .

Proof: Let  $g \in G$ , then  $gNg^{-1} = N$  since  $N$  is normal in  $G$ . Then

$gB(N)g^{-1} = \{gxg^{-1} \mid xa = ax \quad \forall a \in N\}$ . If we let  $gxg^{-1} = y$  then  $x = g^{-1}yg \implies xa = g^{-1}yga = ag^{-1}yg = ax$ . i.e.

$$B(N) = \{y \in G \mid g^{-1}yga = ag^{-1}yg \quad \forall a \in N\}$$

Then we need to show that  $g^{-1}yg \in B(N)$ . Since  $N$  is normal,  $ga = bg$  for some  $b \in N$ . This also gives  $ag^{-1} = g^{-1}b$  thus

$$g^{-1}yga = g^{-1}ybg = g^{-1}byg = ag^{-1}yg$$

Therefore  $g^{-1}yg \in B(N)$  so we get

$$gB(N)g^{-1} = \{x \in G \mid xa = ax \quad \forall a \in N\}$$

This shows  $B(N)$  is normal in  $G$ .

## 16. a

We use the result from problem 40 of section 2.5 which is as follows: Suppose  $G$  is a group,  $H$  is a subgroup and  $|G| = n$  and  $n \nmid (i_G(H))!$ . Then there exists a normal subgroup  $K \neq \{e\}$  and  $K \subseteq H$ .

So, we have now a group  $G$  of order  $36 = 2^2 \cdot 3^2$ , so there exists a 3-sylow subgroup of order 9, call it  $A$ . Now  $i_G(A) = 4$ , so  $36 \nmid 4!$ , hence by the above result there is a normal subgroup  $K$ , non-trivial and  $K \subseteq A$ . But  $|A| = 9$ . So either  $A$  itself is normal or contains a normal subgroup of order 3. Hence  $G$  has a subgroup of order 9 or 3.

### Result

See the proof

## 17. a

We use the result from problem 40 of section 2.5 which is as follows: Suppose  $G$  is a group ,  $H$  is a subgroup and  $|G| = n$  and  $n \nmid (i_G(H))!$ . Then there exists a normal subgroup  $K \neq \{e\}$  and  $K \subseteq H$ .

So, we have now a group  $G$  of order  $108 = 2^2 \cdot 3^3$ , and so there exists a 3-sylow subgroup of order 27, call it  $A$ . Now  $i_G(A) = 4$ , so  $108 \nmid 4!$ , hence by the above result there is a normal subgroup  $K$ , non-trivial and  $K \subseteq A$ . But  $|A| = 27$ . So either  $A$  itself is normal or contains a normal subgroup of order 9 or of order 3. Now if it is itself normal or contains a normal subgroup of order 9, we are done as for then the group  $G$  has normal subgroup of order 9 or 27. Now suppose that we have a normal subgroup of order 3 , call it  $K \subset A$ . Now consider  $G/K$ .  $|G/K| = 36$ . And also  $A/K$  is a order 9 subgroup of  $G/K$ . By previous problem . There exists normal subgroup of order 3 or 9 contained in  $A/K$ . so either  $A/K$  is normal or there exists  $R \subset A$  such that  $R/K$  is normal and  $|R/K| = 3$ . Hence either  $A$  itself is normal, or  $R$  is normal and  $|R| = 9$ . so again we have proved that there exists subgroup of order 27 or 9.

---

### Result

[See the proof](#)

18. a

Let  $P$  be a sylow-p subgroup. We want to prove  $N(N(P)) = N(P)$ . By definition  $N(P) = \{ g \in G | gPg^{-1} = P \}$  . Also this is a standard fact that  $P \subseteq N(P)$ . So, clearly  $N(P) \subseteq N(N(P))$ . For the other inclusion, Let  $x \in N(N(P)) \implies xN(P)x^{-1} = N(P)$ . In particular as  $P \subseteq N(P)$ , we have  $xPx^{-1} \subseteq N(P)$ . But, observe that  $xPx^{-1}$  is also a sylow-p subgroup of  $G$  which is contained in  $N(P)$ . By problem number 11 of this same chapter we have that  $P$  is the unique p-sylow subgroup which is contained in its normalizer. So,  $xPx^{-1} = P$ . Hence  $N(N(P)) \subseteq N(P)$ . Hence  $N(N(P)) = N(P)$ .

---

### Result

[See the proof](#)

19. a

Given  $|G| = p^n$  then  $G$  has a subgroup of order  $p^m$  for all  $1 \leq m \leq n$ .

**Proof:** We use induction to prove it. For  $n = 0$ , the result is trivially true as for  $n = 1$ . Let this be true for groups whose order is less than  $p^n$ .

Consider the class equation

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} |G : C_G(a)|$$

Since  $p^n \mid |G|$  then  $|G : C_G(a)| |C_G(a)| = |G| = p^n$  therefore  $p \mid |C_G(a)|$  since  $a \notin Z(G)$  is not identity element. This shows that  $p \mid |Z(G)|$  from class equation.

By Cauchy theorem, there is element  $x \in Z(G)$  whose order is  $p$ . Consider the subgroup generated by  $\langle x \rangle$ . Since it lies in center of group, it has to be normal group and its order is  $p$ . Consider quotient group  $\bar{G} = G/\langle x \rangle$  whose order is  $p^{n-1}$ . By induction this group has subgroup of order  $p^k$  where  $1 \leq k < n$ . Let this subgroup be  $\bar{H}$ . The subgroup  $\bar{H}$  of quotient group  $\bar{G}$  should have following structure.

$$\bar{H} = \{h\langle x \rangle : h \in H\} = H/\langle x \rangle$$

where  $H$  is subgroup of  $G$ . Then we get

$$|H| = |\bar{H}| |\langle x \rangle| = p^{k+1}$$

Thus we found subgroup  $H$  of  $G$  whose order is  $p^k$  where  $2 \leq k+1 \leq n$ . This completes the proof.

## 20. a

**Given:**  $p^m$  divides the order of a group  $G$ , where  $p$  is a prime.

**To Prove:**  $G$  has a subgroup of order  $p^m$ .

**Proof:**

Let us assume that  $n$  be the order of  $G$ , i.e.  $|G| = n$ .

Then by the given condition  $p^m$  divides  $n$ , where  $p$  is a prime.

We will show that

**$G$  has a subgroup  $H$  of order  $p^m$  by induction on  $n$**

If  $|G| = 1$ , then this is trivial.

Let us now consider that the statement is true for

**all groups of order less than  $n$**

If  $G$  has a proper subgroup  $H$  such that  $p^m$  divides the order of  $H$ , then, by our inductive hypothesis,  $H$  has a subgroup of order  $p^m$  and we are done.

Thus, we may assume that

**$p^m$  does not divide the order of any proper subgroup of  $G$**

Let us now consider the **class equation** for  $G$  in the form

$$|G| = |Z(G)| + \sum |G : C(a)|,$$

where we sum over a representative of each **conjugacy class**  $cl(a)$ , where  $a \notin Z(G)$ .

Since  $p^m$  divides  $|G| = |G : C(a)||C(a)|$  and  $p^m$  **does not divide**  $|C(a)|$ , we know that  $p$  must divide  $|G : C(a)|$  for all  $a \notin Z(G)$ . Therefore, it follows from the class equation that  $p$  divides  $|Z(G)|$ .

Then by the **Fundamental Theorem of Finite Abelian Groups**, we conclude that  $Z(G)$  contains an element of order  $p$ , say  $x$ .

Since  $x$  is in the center of  $G$ ,  $\langle x \rangle$  is a **normal subgroup** of  $G$ , and hence the **quotient group**  $G/\langle x \rangle$  exists.

Now note that  $p$  divides  $|G/\langle x \rangle|$ , that is  $p$  divides the order of the quotient group  $G/\langle x \rangle$ .

Thus, by the induction hypothesis,  $G/\langle x \rangle$  has a subgroup of order  $p^{m-1}$ , say  $H/\langle x \rangle$ , where  $H$  is a subgroup of  $G$ .

So,  $|H/\langle x \rangle| = p^{m-1}$  and  $|\langle x \rangle| = p$  implies that order of the subgroup  $H$  is  $p^m$ .

Then, by induction on  $n$  we proved that  $G$  has a subgroup  $H$  of order  $p^m$ .

This completes the proof.

## Result

3 of 3

$G$  being a finite abelian group with order  $n$  and  $p^m$  divides  $n$ , where  $p$  is a prime, we have proved by the induction method on  $|G|$  that  $G$  has a subgroup  $H$  of order  $p^m$ .

[Click for the detailed proof.](#)

## 21. a

We can prove this by induction on  $n$ . If  $n = 1$  then  $G$  must be isomorphic to  $Z_p$  whose only proper subgroup is  $\{0\}$ , whose normalizer is the whole group  $Z_p$ , so the condition holds.

Suppose  $n > 1$  and the condition holds for all groups of order  $p^k$  for  $k < n$ . Let  $H < G$  be a proper subgroup. Recall that  $Z(G)$  is a normal subgroup of  $G$  which is nontrivial by **theorem 2.11.4**. Note also that by the definition of  $Z(G)$  and  $N(H)$  we have that  $Z(G) < N(H)$ . If  $Z(G)$  is not contained in  $H$  we are done, otherwise we have that  $H/Z(G)$  is a subgroup of  $G/Z(G)$  which is a group of order  $p^k$  for some  $k < n$ . By the inductive hypothesis the normalizer of  $H/Z(G)$  in  $G/Z(G)$  contains some element  $gZ(G)$  not contained in  $H/Z(G)$ . Note in particular that this means that  $g \notin H$ . Then for all  $h \in H$  there is some  $h'$  such that  $ghZ(G) = h'gZ(G)$ , so there is some  $c \in Z(G)$  such that  $gh = ch'g$ . Since by assumption  $c \in H$  we have that  $ch' \in H$  which means  $g \in N(H)$ .

## Result

2 of 2

This can be proved by induction using **theorem 2.11.4**.

## 22. a

**Given:** Let  $G$  be a group of order  $p^n$ ,  $p$  is a prime.

**To Prove:** Any subgroup of  $G$  of order  $p^{n-1}$  is normal in  $G$ .

## Step 2

2 of 4

**Proof:** First we prove the following **lemma**.

**Lemma:** If  $G$  is a finite  $p$ -group with  $|G| > 1$ , then  $Z(G)$ , the center of  $G$ , has more than one element, i.e., if  $|G| = p^k$  with  $k \geq 1$ , then  $|Z(G)| > 1$ .

**Proof of the lemma:** Consider the class equation

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)].$$

If  $G = Z(G)$ , then the lemma is immediate.

Suppose  $Z(G) \subset G$  and consider  $a \in G$  such that  $a \notin Z(G)$ .

Then  $C(a)$  is a proper subgroup of  $G$ . Then by the fact that  $C(a)$  is a subgroup of a  $p$ -group,  $p \mid [G : C(a)]$  for all  $a \notin Z(G)$ .

This implies that  $p$  divides  $|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)]$ .

Since  $p$  also divides  $|G|$ ,  $p$  divides  $|Z(G)|$ .

Hence,  $|Z(G)| > 1$ .

This proves our **lemma**.

{lemma}.

We will prove the result by induction on  $n$ .

If  $n = 1$ , the  $G$  is a cyclic group of prime order and hence every subgroup of  $G$  is normal in  $G$ . Thus, the result is true for  $n = 1$ .

Suppose the result is true for all groups of order  $p^m$ , where  $1 \leq m < n$ .

Let  $H$  be a subgroup of order  $p^{n-1}$ .

Consider  $N(H) = \{g \in H : gH = Hg\}$ .

If  $H \neq N(H)$ , then  $|N(H)| > p^{n-1}$ . Thus,  $|N(H)| = p^n$  and  $N(H) = G$ .

In this case  $H$  is normal in  $G$ .

Let  $H = N(H)$ . Then  $Z(G)$ , the center of  $G$ , is a subset of  $H$  and  $Z(G) \neq \{e\}$ .

By **Cauchy's theorem** and the above **Claim**, there exists  $a \in Z(G)$  such that  $o(a) = p$ .

Let  $K = \langle a \rangle$ , a cyclic group generated by  $a$ .

Then  $K$  is a normal subgroup of  $G$  of order  $p$ . Now,  $|H/K| = p^{n-2}$  and  $|G/K| = p^{n-1}$ .

Thus, by induction hypothesis,

$H/K$  is a normal subgroup of  $G/K$

23. a

a)

- [(reflexivity)]  $\mathbb{H}$  is a subgroup of  $\mathbb{G}$ , then it contains identity element  $e$ . Hence, for an arbitrary element  $a \in \mathbb{G}$  we obtain that

$$a = e^{-1}ae \Leftrightarrow a \sim a$$

- [(symmetry)] Assume that  $a, b \in \mathbb{G}$  are the arbitrary elements such that  $a \sim b$ , then there is an element  $h \in H$  that

$$a \sim b \Leftrightarrow b = h^{-1}ah \Leftrightarrow (h^{-1})^{-1}bh^{-1} = a \Leftrightarrow b \sim a$$

- [(transitivity)] Assume that  $a, b, c \in \mathbb{G}$  are the arbitrary elements such that  $a \sim b$  and  $b \sim c$ , then there is an element  $h, \ell \in H$  that

$$a \sim b \wedge b \sim c \Rightarrow b = h^{-1}ah \wedge c = \ell^{-1}b\ell \Rightarrow c = (\ell h^{-1})^{-1}a\ell h^{-1} \Rightarrow a \sim c$$

Remark: Last implication is obtained from the fact that  $\mathbb{H}$  contains  $\ell h^{-1}$ , because it is a subgroup of  $\mathbb{G}$ .

Therefore, the given relation is equivalence relation on  $\mathbb{G}$  and the equivalence class of  $a$  is given by

$$[a] = \{h^{-1}ah | h \in H\}$$

b)

It is not hard to conclude that  $\mathbb{H} \cap C(a)$  defines a subgroup of  $H$  as intersection of two subgroups of  $\mathbb{G}$  which is contained in  $H$ . It is well-known that  $i_H(H \cap C(a))$  is equal to the number of distinct right cosets, that is an inspiration to define the mapping

$$\psi : [a] \rightarrow \{(H \cap C(a))s | s \in H\}$$

as

$$\psi(s^{-1}as) = (H \cap C(a))s$$

Assume that  $s, h \in H$  are the arbitrary such that  $s^{-1}as = h^{-1}ah$  than

$$\begin{aligned} s^{-1}as = h^{-1}ah &\Leftrightarrow hs^{-1}ash^{-1} = a \Leftrightarrow hs^{-1} \in C(a) \cap H \Leftrightarrow h \in (C(a) \cap H)s \\ &\Leftrightarrow (C(a) \cap H)h \in (C(a) \cap H)s \Leftrightarrow \psi(s^{-1}as) = \psi(h^{-1}ah) \end{aligned}$$

Hence, this mapping is well-defined and injective. Also, this is surjective mapping and that conclusion it is not hard to make.

Finally, from the fact that  $G$  is a finite group we have that  $i_H(H \cap C(a))$  is finite, then result above gives us that the number of elements in  $[a]$  is equal to  $i_H(H \cap C(a))$ .

## Result

3 of 3

Use that  $i_H(H \cap C(a))$  is equal to the number of distinct right cosets.

24. a

a)

- [(reflexivity)]  $\mathbb{H}$  is a subgroup of  $\mathbb{G}$ , then it contains identity element  $e$ . Hence, for an arbitrary subgroup  $A$  of  $\mathbb{G}$  we obtain that

$$a = e^{-1}ae \Leftrightarrow A \sim A$$

- [(symmetry)] Assume that  $A, B < \mathbb{G}$  are the arbitrary subgroups of  $\mathbb{G}$  such that  $A \sim B$ , then there is an element  $h \in H$  that

$$A \sim B \Leftrightarrow B = h^{-1}Ah \Leftrightarrow (h^{-1})^{-1}Bh^{-1} = A \Leftrightarrow B \sim A$$

- [(transitivity)] Assume that  $A, B, C < \mathbb{G}$  are the arbitrary subgroups such that  $A \sim B$  and  $B \sim C$ , then there is an element  $h, \ell \in H$  that

$$A \sim B \wedge B \sim C \Rightarrow B = h^{-1}Ah \wedge C = \ell^{-1}B\ell \Rightarrow C = (h\ell)^{-1}Ah\ell \Rightarrow A \sim C$$

Remark: Last implication is obtained from the fact that  $\mathbb{H}$  contains  $h\ell$ , because it is a subgroup of  $\mathbb{G}$ .

Therefore, the given relation is equivalence relation on  $\mathbb{G}$  and the equivalence class of  $a$  is given by

$$[A] = \{h^{-1}Ah | h \in H\}$$

b)

It is not hard to conclude that  $\mathbb{H} \cap N(A)$  defines a subgroup of  $H$  as intersection of two subgroups of  $\mathbb{G}$  which is contained in  $H$ . It is well-known that  $i_H(H \cap N(A))$  is equal to the number of distinct right cosets, that is an inspiration to define the mapping

$$\lambda : [A] \rightarrow \{(H \cap N(A))s | s \in H\}$$

as

$$\lambda(s^{-1}As) = (H \cap N(A))s$$

Assume that  $s, h \in H$  are the arbitrary such that  $s^{-1}As = h^{-1}Ah$  than

$$\begin{aligned}s^{-1}As = h^{-1}Ah &\Leftrightarrow hs^{-1}Ash^{-1} = A \Leftrightarrow hs^{-1} \in H \cap N(A) \Leftrightarrow h \in (H \cap N(A))s \\ &\Leftrightarrow (H \cap N(A))h = (H \cap N(A))s \Leftrightarrow \lambda(s^{-1}As) = \lambda(h^{-1}Ah)\end{aligned}$$

Hence, this mapping is well-defined and injective. Also, this is surjective mapping and that conclusion it is not hard to make.

Finally, from the fact that  $G$  is a finite group we have that  $i_H(H \cap N(A))$  is finite, then result above gives us that the number of elements in  $[A]$  is equal to  $i_H(H \cap N(A))$ .

## Result

3 of 3

Use that  $i_H(H \cap N(A))$  is equal to the number of distinct right cosets.

25. a

From the fact that  $\mathbb{Q}, \mathbb{P}$  are the  $p$ -Sylow subgroups of  $\mathbb{G}$ , we have that each  $a \in \mathbb{P}$  such that  $a^{-1}\mathbb{P}a = \mathbb{P}$  is contained in  $\mathbb{Q}$ . Therefore, it is not hard to conclude that  $N(\mathbb{Q}) \cap \mathbb{P} \neq \mathbb{P}$ , because  $\mathbb{P} \neq \mathbb{Q}$ .

Result of preceding problem gives us that the number of distinct  $a^{-1}\mathbb{Q}a$  equals the index of  $N(\mathbb{Q}) \cap \mathbb{P}$  in  $\mathbb{P}$ . We are already proved that  $N(\mathbb{Q}) \cap \mathbb{P} \neq \mathbb{P}$  and this gives  $i_{\mathbb{P}}(N(\mathbb{Q}) \cap \mathbb{P}) = p^k$  for some positive integer  $k$ .

Hence, THE PROOF!

## Result

2 of 2

(HINT:) Use Problem 24.

## 26. a

It is not hard to conclude that equivalence class of  $\mathbb{P}$  has only one element and from the preceding problem we have that order of each class of  $p$ -Sylow subgroup distinct than  $\mathbb{P}$  is multiple of  $p$ .

Now, from fact that the set of all equivalence classes form a partition of  $S$ , we obtain that number of elements in  $S$  must be of the form

$$1 + kp$$

## Result

2 of 2

(HINT:) The set of all equivalence classes form a partition of  $S$ .

## 27. a

- (a) By assumption all elements of  $S$  are different from  $P$ . Consider the equivalence relation  $Q_1 \sim Q_2$  if  $Q_1 = a^{-1}Q_2a$  for some  $a \in P$ . We can then partition  $S$  into equivalence classes of this relation, and by **exercise 25** we have that the number of elements in each such equivalence class is a multiple of  $p$ . Therefore  $|S|$  is a sum of multiples of  $p$  and is therefore a multiple of  $p$ .
- (b) The conclusion of item (a) directly contradicts the conclusion of **exercise 14**, therefore the conclusion of item (a) cannot hold.
- (c) By the basic principle of a proof by contradiction, we must discard some assumption that led to the contradictory conclusion in item (a). The only assumption we made was that there was no  $x \in G$  such that  $Q = x^{-1}Px$ . Therefore by contradiction we may conclude the existence of at least one  $x \in G$  such that  $Q = x^{-1}Px$ .

## Result

2 of 2

The conclusion in item (a) follows from **exercise 25**. This conclusion directly contradicts **exercise 14**, so we must conclude that the assumption that there are non-conjugate Sylow  $p$ -subgroups is false.

## 28. a

**Given:** Let  $G$  be a finite group of order  $p^m$ , for some integer  $m$  and  $H$  be a subgroup of  $G$ .

**To Prove:**  $H$  is contained in some Sylow-p-subgroup of  $G$ .

**Proof:**

Let  $K$  be a Sylow-p-subgroup of  $G$  and let  $C = \{K_1, K_2, \dots, K_n\}$  with  $K = K_1$  be

**the set of all conjugates of  $K$  in  $G$ .**

Since

**conjugation is an automorphism, each element of  $C$  is a Sylow-p-subgroup of  $G$**

Let  $S_C$  denotes the group of all permutations of  $C$ .

For each  $g \in G$ , define

$$\phi_g : C \rightarrow C$$

by the assignment

$$\phi_g(K_i) = gK_ig^{-1}.$$

It is easy to show that each  $\phi_g \in S_C$ .

Now define a mapping  $T : G \rightarrow S_C$  by

$$T(g) = \phi_g.$$

Since

$$\phi_{gh}(K_i) = (gh)K_i(gh)^{-1} = g(hK_ih^{-1})g^{-1} = g\phi_h(K_i)g^{-1} = \phi_g(\phi_h(K_i)) = (\phi_g\phi_h)(K_i),$$

we conclude that

$$\phi_{gh} = \phi_g\phi_h,$$

and therefore  $T$  is a

**homomorphism from  $G$  to  $S_C$ .**

Next consider  $T(H)$ , the image of  $H$  under  $T$ .

Since

$$|H| \text{ is a power of } p, \text{ so is } |T(H)|.$$

Thus, by

**Orbit-Stabilizer theorem, for each  $i$ ,  $|orb_{T(H)}(K_i)|$  divides  $|T(H)|$ , so that  $|orb_{T(H)}(K_i)|$  is a power of  $p$ .**

Now,  $|orb_{T(H)}(K_i)| = 1$  means that

$$\phi_g(K_i) = gK_ig^{-1} = K_i \quad \forall g \in H;$$

that is,  $|orb_{T(H)}(K_i)| = 1$  if and only if  $H$  is a subgroup of  $N(K_i)$ .

But the

**only elements of  $N(K_i)$  that have orders that are powers of  $p$  are those of  $K_i$ .**

Thus,  $|orb_{T(H)}(K_i)| = 1$  if and only if  $H$  is a **subgroup** of  $K_i$ .

So, to complete the proof, all we need to do is to show that for some  $i$ ,

$$|orb_{T(H)}(K_i)| = 1.$$

Now we have

$$|C| = |G : N(K)|.$$

And since

$$|G : K| = |G : N(K)||N(K) : K|$$

**is not divisible by  $p$ , neither is  $|C|$ .**

Because the orbits partition  $C$ ,  $|C|$  is the sum of powers of  $p$ .

**If no orbit has size 1, then  $p$  divides each summand and, therefore,  $p$  divides  $|C|$ ,**

which is a contradiction.

Thus,

**there is an orbit of size 1,**

and the proof is complete.

## 29. a

Suppose  $g \in G$  is such that  $a = g^{-1}bg$ . Consider the centralizer  $C_G(a) = \{c \in G \mid ac = ca\}$ . Since  $a \in Z(P)$  we have that  $P \subset C_G(a)$ . Also since  $b \in Z(P)$  we have that  $g^{-1}Pg \subset C_G(a)$ , as we can directly verify:

$$\begin{aligned} g^{-1}pga &= g^{-1}pgg^{-1}bg \\ &= g^{-1}pb \\ &= g^{-1}bg \\ &= g^{-1}bgg^{-1}pg \\ &= ag^{-1}pg \end{aligned}$$

Therefore  $P$  and  $g^{-1}Pg$  are Sylow  $p$ -subgroups of  $C_G(a)$  and so by the second Sylow theorem there is some  $h \in C_G(a)$  such that  $P = h^{-1}g^{-1}Pgh$ . Therefore  $gh \in N(P)$  and  $a = h^{-1}ah = h^{-1}g^{-1}bgh$ .

### Result

2 of 2

Apply the second Sylow theorem to the centralizer of  $a$ .

# Chapter 3

## Section 3–1

1. a

We use the notation  $\sigma : x \rightarrow y$  to denote that  $\sigma$  maps  $x$  to  $y$ . Recall that we multiply permutations from right to left.

### Step 2

2 of 5

(a)

Denote the first element in the product by  $\sigma$  and the second one by  $\tau$ . We have that

- $\tau : 1 \rightarrow 2$  and  $\sigma : 2 \rightarrow 4$ , so  $\sigma\tau : 1 \rightarrow 4$ ,
- $\tau : 2 \rightarrow 3$  and  $\sigma : 3 \rightarrow 5$ , so  $\sigma\tau : 2 \rightarrow 5$ ,
- $\tau : 3 \rightarrow 4$  and  $\sigma : 4 \rightarrow 2$ , so  $\sigma\tau : 3 \rightarrow 2$ ,
- $\tau : 4 \rightarrow 5$  and  $\sigma : 5 \rightarrow 1$ , so  $\sigma\tau : 4 \rightarrow 1$ ,
- $\tau : 5 \rightarrow 6$  and  $\sigma : 6 \rightarrow 3$ , so  $\sigma\tau : 5 \rightarrow 3$ ,
- $\tau : 6 \rightarrow 1$  and  $\sigma : 1 \rightarrow 6$ , so  $\sigma\tau : 6 \rightarrow 6$ ,

so that

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}.$$

(b)

We again denote the first element in the product by  $\sigma$  and the second one by  $\tau$ . We have that

- $\tau : 1 \rightarrow 3$  and  $\sigma : 3 \rightarrow 3$ , so  $\sigma\tau : 1 \rightarrow 3$ ,
- $\tau : 2 \rightarrow 2$  and  $\sigma : 2 \rightarrow 1$ , so  $\sigma\tau : 2 \rightarrow 1$ ,
- $\tau : 3 \rightarrow 1$  and  $\sigma : 1 \rightarrow 2$ , so  $\sigma\tau : 3 \rightarrow 2$ ,
- $\tau : 4 \rightarrow 4$  and  $\sigma : 4 \rightarrow 4$ , so  $\sigma\tau : 4 \rightarrow 4$ ,
- $\tau : 5 \rightarrow 5$  and  $\sigma : 5 \rightarrow 5$ , so  $\sigma\tau : 5 \rightarrow 5$ ,

so that

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}.$$

**(c)**

We denote the first element in the product as  $\sigma$ , the second one as  $\tau$  and the third one as  $\rho$ . Note that an inverse of a permutation, written in this chapter's notation, is given by interchanging the top and bottom rows, i.e.

$$\begin{aligned}\sigma &= \begin{pmatrix} 4 & 1 & 3 & 2 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}.\end{aligned}$$

Since multiplication of permutations is associative, our product can be found either by computing  $(\sigma\tau)\rho$  or  $\sigma(\tau\rho)$ . Let us do the former; then analogously with **(a)** and **(b)** parts of the problem we have that

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix},$$

so that then

$$(\sigma\tau)\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}.$$

## Result

**(a)**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$$

**(b)**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

**(c)**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

## 2. a

We're going to use the following fact to characterise  $\sigma^k$  for all  $k$ : if  $g$  is an element of group  $G$  with order  $n \in \mathbb{N}$ , then  $g^a = g^{a \bmod n}$  for all  $a \in \mathbb{Z}$ ; i.e.  $g^a$  is determined by the residue class of  $a$  modulo  $n$ . This means that it is sufficient, in order to find  $\sigma^k$  for all  $k$ , to find the order of the element  $\sigma$ , say it is  $n$ , and the values  $\sigma^0, \sigma^1, \dots, \sigma^{n-1}$ .

**(a)**

We have that

$$\begin{aligned}\sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}, \\ \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}, \\ \sigma^4 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}, \\ \sigma^5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix},\end{aligned}$$

and  $\sigma^6$  is the identity permutation. Now we see that  $\sigma^k = \sigma^{k \bmod 6}$ , and we have determined  $\sigma^k$  for  $k = 0, 1, \dots, 5$ , giving us the complete classification.

**Step 3**

3

**(b)**

We see that  $\sigma^2$  is the identity permutation. Thus  $\sigma^k = \sigma$  if  $k$  is odd, and  $\sigma^k = \text{id}$  if  $k$  is even.

**(c)**

We have that

$$\begin{aligned}\sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 6 & 5 \end{pmatrix}, \\ \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 3 & 1 \end{pmatrix},\end{aligned}$$

and  $\sigma^4$  is the identity permutation. Thus by the aforementioned fact we have classified all the powers of  $\sigma$ .

## Result

(a)

$$\sigma^k = \begin{cases} \text{id} & \text{if } k \equiv 0 \pmod{6} \\ \sigma & \text{if } k \equiv 1 \pmod{6} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} & \text{if } k \equiv 2 \pmod{6} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} & \text{if } k \equiv 3 \pmod{6} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} & \text{if } k \equiv 4 \pmod{6} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} & \text{if } k \equiv 5 \pmod{6} \end{cases}$$

(b)  $\sigma^k = \sigma$  if  $k$  is odd,  $\sigma^k$  is the identity permutation if  $k$  is even.

(c)

$$\sigma^k = \begin{cases} \text{id} & \text{if } k \equiv 0 \pmod{4} \\ \sigma & \text{if } k \equiv 1 \pmod{4} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 6 & 5 \end{pmatrix} & \text{if } k \equiv 2 \pmod{4} \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 3 & 1 \end{pmatrix} & \text{if } k \equiv 3 \pmod{4} \end{cases}$$

### 3. a

Due to uniqueness of inverses in groups, it is sufficient to prove that

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

is the identity permutation. However, that is immediate from that fact that the  $\sigma$  is a product of two permutations such that the right one -- and recall that we multiply permutations from right to left -- maps  $j$  to  $i_j$ , for all  $j \in \{1, \dots, n\}$ , while the left one maps  $i_k$  to  $k$  for all  $k \in \{1, \dots, n\}$ . Thus for every  $m \in \{1, \dots, n\}$ ,  $m$  is mapped to  $i_m$  by the right permutation, and then  $i_m$  is mapped to  $m$  by the left permutation, so that  $\sigma(m) = m$ .

## Result

2 of 2

We show that

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

is the identity permutation; the result then follows by the uniqueness of inverses in groups. Click for more details.

### 4. a

We use the fact that if  $g$  is an element of group  $G$  with order  $n$ , then if  $\gcd(m, n) = 1$ , we have that  $g^m$  also has order  $n$ . This follows from noting that  $(g^m)^n = g^{mn} = (g^n)^m = 1_G$ , where  $1_G$  is the identity in  $G$ , and that  $m, 2m, \dots, nm$  is a complete residue system modulo  $n$ .

## Step 2

2 of 5

### (a)

We see that order of  $\sigma$  is 6 because  $\sigma^6 = \text{id}$  and  $\sigma^j$  isn't the identity permutation for any positive integer less than 6.

For  $\sigma^2$  we have that  $(\sigma^2)^2 \neq \text{id}$  but  $(\sigma^2)^3 = \sigma^6 = \text{id}$  so that  $\sigma^2$  has order 3.

Analogously we see that  $\sigma^3$  has order 2,  $\sigma^4$  has order 3 because  $(\sigma^4)^2 = \sigma^8 = \sigma^2 \neq \text{id}$ , while  $(\sigma^4)^3 = \sigma^{12} = \text{id}$ , and  $\sigma^5$  has order 6 because  $\gcd(5, 6) = 1$ .

## Step 3

3 of 5

### (b)

$\sigma$  has order 2.

### (c)

$\sigma$  has order 4,  $\sigma^2$  has order 2 (because  $\sigma^2 \neq \text{id}$  and  $(\sigma^2)^2 = \sigma^4 = \text{id}$ ) and  $\sigma^3$  has order 4.

## Result

5 of 5

- [(a)] We have that  $\sigma$  has order 6,  $\sigma^2$  has order 3,  $\sigma^3$  has order 2,  $\sigma^4$  has order 3, and  $\sigma^5$  has order 6.
- [(b)]  $\sigma$  has order 2.
- [(c)]  $\sigma$  has order 4,  $\sigma^2$  has order 2, and  $\sigma^3$  has order 4.

Click for more details.

## 5. a

In the (a) part we obtained the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}.$$

We calculate

$$\begin{aligned} \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix}, \\ \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 1 & 5 & 6 \end{pmatrix}, \\ \sigma^4 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix}, \\ \sigma^5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}, \end{aligned}$$

and we further calculate that  $\sigma^6$  is the identity permutation. Thus, order of  $\sigma$  is 6.

In the **(b)** part we obtained the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}.$$

We calculate

$$\begin{aligned}\sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}, \\ \sigma^3 &= \text{id},\end{aligned}$$

where  $\text{id}$  is the identity permutation. Thus, the order of  $\sigma$  is 2.

### Step 3

In the **(c)** part we obtained the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}.$$

We immediately compute that  $\sigma^2 = \text{id}$ , so the order of  $\sigma$  is 2.

### Result

4 of

Orders for the resulting permutations in the **(a)**, **(b)**, and **c** sections are 6, 3, and 2, respectively. Click for more details.

## Section 3–2

### 1. a

Let  $\tau$  and  $\sigma$  be two disjoint cycles in  $S_n$ . If  $i \in \{1, \dots, n\}$ , then either  $\tau(i) = \sigma(i) = i$  or at most one of them doesn't map  $i$  to  $i$ ; this is given by their disjointness. In the first case, we have that

$$\sigma(\tau(i)) = \sigma(i) = i$$

and

$$\tau(\sigma(i)) = \tau(i) = i.$$

Now let us suppose, without a loss of generality, that we have  $\tau(i) = i$  and  $\sigma(i) \neq i$ . Then we have

$$\sigma(\tau(i)) = \sigma(i)$$

and

$$\tau(\sigma(i)) = \sigma(i)$$

where last the equality follows from their disjointness, i.e.  $\sigma(i)$  occurs in  $\sigma$  and so it doesn't occur in  $\tau$ .

### Result

2 of 2

If  $\tau$  and  $\sigma$  are two disjoint cycles in  $S_n$ , and  $i \in \{1, \dots, n\}$ , at most for one of them we have that  $\sigma(i) \neq i$ . Click here for the detailed proof.

## 2. a

We use the notation  $\sigma : x \rightarrow y$  to denote that  $\sigma(x) = y$ .

### Step 2

2 of 5

#### (a)

Let the given permutation be denoted by  $\sigma$ , then

$$\begin{aligned}\sigma &: 1 \rightarrow 3, \\ \sigma &: 3 \rightarrow 4, \\ \sigma &: 4 \rightarrow 2, \\ \sigma &: 2 \rightarrow 1,\end{aligned}$$

and as we've reached an element we started from, this determines one cycle. To find the other, we note that

$$\begin{aligned}\sigma &: 5 \rightarrow 7, \\ \sigma &: 7 \rightarrow 9, \\ \sigma &: 9 \rightarrow 5.\end{aligned}$$

As we've enumerated all the elements of  $\{1, \dots, 9\}$  except 6 and 8 for which we have  $\sigma(8) = 8$  and  $\sigma(6) = 6$ , we've obtained our cycle decomposition as

$$(1 \ 3 \ 4 \ 2)(5 \ 7 \ 9).$$

By **Theorem 3.2.4** the order of this permutation is equal to  $\text{lcm}(3, 4) = 12$ .

#### (b)

Again we denote the given permutation with  $\sigma$ . We have

$$\begin{aligned}\sigma &: 1 \rightarrow 7, \\ \sigma &: 7 \rightarrow 1\end{aligned}$$

also

$$\begin{aligned}\sigma &: 2 \rightarrow 6, \\ \sigma &: 6 \rightarrow 2,\end{aligned}$$

and

$$\begin{aligned}\sigma &: 3 \rightarrow 5, \\ \sigma &: 5 \rightarrow 3.\end{aligned}$$

So then by noting that  $\sigma(4) = 4$ , we get the cycle decomposition

$$\sigma = (1 \ 7)(2 \ 6)(3 \ 5).$$

By **Theorem 3.2.4** the order of this permutation is equal to  $\text{lcm}(2, 2, 2) = 2$ .

(c)

We first multiply the product to get

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 4 & 2 & 1 & 3 \end{pmatrix}.$$

Note that we have  $\sigma(4) = 4$  and that every other element belongs to a 2-cycle, so

$$\sigma = (1\ 6)(2\ 5)(3\ 7).$$

Again by **Theorem 3.2.4** the order of this permutation is  $\text{lcm}(2, 2, 2) = 2$ .

## Result

(a)  $(1\ 3\ 4\ 2)(5\ 7\ 9)$  which has order 12.

(b)  $(1\ 7)(2\ 6)(3\ 5)$  which has order 2.

(c)  $(1\ 6)(2\ 5)(3\ 7)$  which has order 2.

[Click for more details.](#)

## 3. a

For each of these problems we will first write out the resulting permutation, and then convert that into a product of disjoint cycles. In each problem we use **Theorem 3.2.4** to compute the order of the permutation.

### Step 2

2 of 8

(a)

Let  $\sigma = (1\ 2\ 3\ 5\ 7)$  and  $\tau = (2\ 4\ 7\ 6)$ . Then we have that

$$\begin{aligned}\tau(1) &= 1 \text{ and } \sigma(1) = 2, \\ \tau(2) &= 4 \text{ and } \sigma(4) = 4, \\ \tau(3) &= 3 \text{ and } \sigma(3) = 5, \\ \tau(4) &= 7 \text{ and } \sigma(7) = 1, \\ \tau(5) &= 5 \text{ and } \sigma(5) = 7, \\ \tau(6) &= 2 \text{ and } \sigma(3) = 3, \\ \tau(7) &= 6 \text{ and } \sigma(6) = 6,\end{aligned}$$

so that

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 1 & 7 & 3 & 6 \end{pmatrix} = (1\ 2\ 4)(3\ 5\ 7\ 6).$$

See the previous exercise for a detailed writeup of how to get the cycle decomposition of a permutation. The order of this permutation is  $\text{lcm}(3, 4) = 12$ .

**(b)**

We have that the product is equal to

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 3\ 2).$$

The order of this permutation is 4.

**Step 4****(c)**

We obtain that the product is equal to

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 7\ 3\ 6\ 2\ 5).$$

The order of this permutation is 7.

**(d)**

We evaluate the product as

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

which is the identity permutation, and has order 1.

**Step 6**

6 of 8

**(e)**

Let  $\sigma = (1\ 2\ 3)$ . Then as  $\sigma(1) = 2$ , we have  $\sigma^{-1}(2) = 1$  -- we can do this because  $\sigma$  is a bijection -- similarly  $\sigma^{-1}(1) = 3$  and  $\sigma^{-1}(3) = 2$  so that

$$(1\ 2\ 3)^{-1} = (1\ 3\ 2).$$

(Note that this is also given by the (d) part via the uniqueness of inverses in groups.) Now we evaluate the product as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 3 & 4 & 7 & 6 & 9 & 8 & 1 \end{pmatrix} = (1\ 5\ 7\ 9).$$

This permutation has order 4.

(f)

We find that the product is equal to

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} = (1\ 4\ 2\ 5\ 3).$$

This permutation has order 5.

## Result

(a)  $(1\ 2\ 4)(3\ 5\ 7\ 6)$  with order 12,

(b)  $(1\ 4\ 3\ 2)$  with order 4,

(c)  $(1\ 4\ 7\ 3\ 6\ 2\ 5)$  with order 7,

(d) product is the identity permutation, which has order 1,

(e)  $(1\ 5\ 7\ 9)$  with order 4,

(f)  $(1\ 4\ 2\ 5\ 3)$  with order 5.

[Click for more details.](#)

4. a

**To Prove:** Every permutation in  $S_n$  is the product of disjoint cycles.

**Proof:** First we prove the following lemma.

**Lemma:** Every permutation of a finite set can be written as a product of disjoint cycles.

**Proof of the Lemma:** Let  $\alpha$  be a permutation on a finite set

$$A = \{1, 2, \dots, n\}.$$

Pick any element of  $A$ , say  $a_1$ .

Compute  $a_2 = \alpha(a_1)$ ,  $a_3 = \alpha(a_2) = \alpha^2(a_1)$  and so on.

**Because  $A$  is finite, the sequence  $a_1, \alpha(a_1), \alpha^2(a_1), \dots$  must also be finite, thus there is a repetition,**

**that is there exists  $i < j$  for which  $\alpha^i(a_1) = \alpha^j(a_1)$  and hence  $a_1 = \alpha^m(a_1)$  with  $m = j - i$**

So we can write  $\alpha = (a_1, a_2, \dots, a_m) \dots$  where the dots indicate

**we may not have exhausted all the elements of  $A$ .**

If we did not, we pick  $b_1$  among the elements of  $A$  which do not appear in  $(a_1, a_2, \dots, a_m)$  and repeat the same process to get a cycle  $(b_1, b_2, \dots, b_k)$ .

First we note that

**the two cycles  $(a_1, a_2, \dots, a_m)$  and  $(b_1, b_2, \dots, b_k)$  are disjoint.**

If they had elements in common, then for some  $i$  and  $j$  we would have  $\alpha^i(a_1) = \alpha^j(b_1)$  that is  $b_1 = \alpha^{i-j}(a_1)$  but this would imply  $b_1$  is an element of the cycle  $(a_1, a_2, \dots, a_m)$  which contradicts the way  $b_1$  was chosen.

We now have  $\alpha = (a_1, a_2, \dots, a_m)(b_1, b_2, \dots, b_k) \dots$  where the cycles appearing so far are disjoint and the dots indicate we may have not exhausted all the elements of  $A$ .

If there are elements of  $A$  left we repeat the procedure.

We know this must end since

**$A$  has a finite number of elements.**

This completes our **Lemma**.

Therefore, we conclude that "**Every permutation of a finite set can be written as a product of disjoint cycles.**"

Since

**$S_n$  is a finite set,**

then every permutation of  $S_n$  is a product of disjoint cycles.

This completes our proof.

## 5. a

**To Prove:** The order of an  $k$ -cycle is  $k$ .

**Proof:**

Let  $p = (a_1, a_2, \dots, a_k)$  be an  $k$ -cycle on the set  $S = \{a_1, a_2, \dots, a_n\}$ .

Then

$$p(a_1) = a_2, p^2(a_1) = p(a_2) = a_3, \dots, p^k(a_1) = p(a_k) = a_1$$

Similarly,

$$p^k(a_2) = a_3, p^k(a_3) = a_4, \dots, p^k(a_k) = a_1.$$

Also

$$p(a_s) = a_s \text{ for } s = k+1, \dots, n,$$

and so,

$$p^k(a_s) = a_s \text{ for } s = k+1, \dots, n.$$

It follows that

$$p^k(a_m) = a_m \text{ for } m = 1, 2, \dots, n$$

and

**therefore  $p^k$  is the identity permutation.  
 $k$  is the least positive integer such that  $p^k = i$**

Because if  $p^l = i$  for some positive integer  $l < k$  then  $p^l(a_1)$  must be  $a_1$ , which is not so.

**Therefore the order of  $p$  is  $k$ .**

Since,  $p$  is an arbitrary  $k$ -cycle, order of any  $k$ -cycle is  $k$ .

This completes the proof.

## 6. a

It was shown in the text that this problem is equivalent to finding an element of  $S_{13}$  with order 42. Further, by using

**Theorem 3.2.4.** we have that it is sufficient to find a  $\sigma \in S_{13}$  which is product of two disjoint cycles of length  $k_1, \dots, k_n$  such that  $\text{lcm}(k_1, \dots, k_n) = 42$ . Note that  $42 = 7 \cdot 6$  and  $\text{lcm}(7, 6) = 42$ , so that

$$\sigma = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7)(8 \ 9 \ 10 \ 11 \ 12 \ 13)$$

fits our desiderata.

### Result

2 of 2

Since this problem is equivalent to finding an element of  $S_{13}$  with order 42, a solution is given by

$$\sigma = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7)(8 \ 9 \ 10 \ 11 \ 12 \ 13).$$

## 7. a

Following the same line of reasoning as in **Problem 6**, we have that  $\text{lcm}(5, 4) = 20$ , so that an example of a permutation which fits our requirements is

$$\sigma = (1 \ 2 \ 3 \ 4 \ 5)(6 \ 7 \ 8 \ 9)$$

### Result

2 of 2

$\sigma = (1 \ 2 \ 3 \ 4 \ 5)(6 \ 7 \ 8 \ 9)$  fits our requirements. Click for more details.

8. a

Note from the text that the  $k$ -cycle  $(i_1 \ i_2 \ \dots \ i_k)$  is equal to  $(i_1 \ i_k)(i_1 \ i_{k-1}) \dots (i_1 \ i_2)$ . We use this to write our permutations as products of transpositions.

### Step 2

2 of 8

(a)

$$(1 \ 2 \ 4)(3 \ 5 \ 7 \ 6) = (1 \ 4)(1 \ 2)(3 \ 6)(3 \ 7)(3 \ 5),$$

### Step 3

3 of 8

(b)

$$(1 \ 4 \ 3 \ 2) = (1 \ 2)(1 \ 3)(1 \ 4),$$

(c)

$$(1 \ 4 \ 7 \ 3 \ 6 \ 2 \ 5) = (1 \ 5)(1 \ 2)(1 \ 6)(1 \ 3)(1 \ 7)(1 \ 4),$$

### Step 5

(d)

$$\text{id} = (1 \ 1)(2 \ 2)(3 \ 3),$$

### Step 6

(e)

$$(1 \ 5 \ 7 \ 9) = (1 \ 9)(1 \ 7)(1 \ 5),$$

(f)

$$(1\ 4\ 2\ 5\ 3) = (1\ 3)(1\ 5)(1\ 2)(1\ 4).$$

### Result

(a)  $(1\ 4)(1\ 2)(3\ 6)(3\ 7)(3\ 5),$

(b)  $(1\ 2)(1\ 3)(1\ 4),$

(c)  $(1\ 5)(1\ 2)(1\ 6)(1\ 3)(1\ 7)(1\ 4),$

(d)  $(1\ 1)(2\ 2)(3\ 3),$

(e)  $(1\ 9)(1\ 7)(1\ 5),$

(f)  $(1\ 3)(1\ 5)(1\ 2)(1\ 4).$

Click for more details.

9. a

Here we use a lemma which states that if  $\tau$  is  $k$ -cycle  $(i_1\ i_2\ \dots\ i_k)$  then  $\sigma\tau\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_k))$  for any  $\sigma \in S_n$ . A more general form of this lemma is proved in **Problem 22**.

### Step 2

2 of 3

We need to find a permutation  $\sigma$  such that

$$(\sigma(1)\ \sigma(2)) = (1\ 3).$$

Thus we must have either  $\sigma(1) = 1$  and  $\sigma(2) = 3$  or  $\sigma(1) = 3$  and  $\sigma(2) = 1$ . Two permutations which these relations describe are  $(2\ 3)$  and  $(1\ 3\ 2)$ , which we can easily check to satisfy our equality.

### Result

3 of 3

$$\sigma = (1\ 3\ 2) \text{ or } \sigma = (2\ 3). \text{ Click for more details.}$$

10. a

We use a lemma which states that if  $\tau$  is  $k$ -cycle  $(i_1 \ i_2 \ \cdots \ i_k)$  then  $\sigma\tau\sigma^{-1} = (\sigma(i_1) \ \sigma(i_2) \ \cdots \ \sigma(i_k))$  for any  $\sigma \in S_n$ . A more general form of this lemma is proved in **Problem 22**.

## Step 2

2 of 3

By this lemma we have that  $\sigma(1 \ 2)\sigma^{-1} = (\sigma(1) \ \sigma(2))$ . However, this is a 2-cycle and cannot be equal to a 3-cycle, which finishes our proof.

## Result

3 of 3

The left hand side is going to remain a 2-cycle regardless of the choice of  $\sigma$ , so it cannot be equal to a 3-cycle.  
[Click for more details.](#)

## 11. a

We use a lemma which states that if  $\tau$  is  $k$ -cycle  $(i_1 \ i_2 \ \cdots \ i_k)$  then  $\sigma\tau\sigma^{-1} = (\sigma(i_1) \ \sigma(i_2) \ \cdots \ \sigma(i_k))$  for any  $\sigma \in S_n$ . A more general form of this lemma is proved in **Problem 22**.

## Step 2

2 of 3

Using this lemma we find that we're looking for a  $\sigma$  such that  $(\sigma(1) \ \sigma(2) \ \sigma(3)) = (4 \ 5 \ 6)$ . Obviously  $\sigma = (1 \ 4)(2 \ 5)(3 \ 6)$  fits the bill. Indeed

$$(1 \ 4)(2 \ 5)(3 \ 6)(1 \ 2 \ 3)(1 \ 4)(2 \ 5)(3 \ 6) = (4 \ 5 \ 6),$$

where we have used the fact that the inverse of a transposition, and then also a product of disjoint transpositions, is its own inverse.

## Result

3 of 3

A  $\sigma = (1 \ 4)(2 \ 5)(3 \ 6)$  satisfies the required equality.

## 12. a

We use a lemma which states that if  $\tau$  is  $k$ -cycle  $(i_1 \ i_2 \ \cdots \ i_k)$  then  $\sigma\tau\sigma^{-1} = (\sigma(i_1) \ \sigma(i_2) \ \cdots \ \sigma(i_k))$  for any  $\sigma \in S_n$ . A more general form of this lemma is proved in **Problem 22**.

## Step 2

2 of 3

Using our lemma, we see that the question is equivalent to proving there is no  $\sigma$  such that

$$(\sigma(1) \ \sigma(2) \ \sigma(3)) = (1 \ 2 \ 4)(5 \ 6 \ 7).$$

However, this is immediate from the fact that the left hand side is a 3-cycle, and the right hand side is a product of two disjoint 3-cycles.

## Result

3 of 3

We show that the left hand side is, regardless of the choice of  $\sigma$ , a 3-cycle, while the right hand side is a product of two disjoint 3-cycles, and thus they cannot be equal. Click for more details.

13. a

**To Prove:** The transposition  $(1 \ 2)$  cannot be written as the product of any number of disjoint 3 – cycles.

## Step 2

2 of 3

**Proof:**

We know that

a  $k$ -cycle has order  $k$

Then a 3-cycle must have order 3.

Now,

**the product of any number of disjoint 3-cycles will have order 3**

, but the given transposition  $(1 \ 2)$  has order 2.

Thus the transposition  $(1 \ 2)$  cannot be written as the product of any number of disjoint 3-cycles.  
This completes the proof.

14. a

This is a special case of **Problem 15** with  $k = 2$ , while Problem 15 is in turn a special case of **Problem 22**.

## Step 2

2 of 3

In particular this follows from noting that if  $\tau = (i_1 \ i_2)$ , then for any permutation  $\sigma$  we have that

$$\sigma\tau\sigma^{-1} = (\sigma(i_1) \ \sigma(i_2)),$$

i.e.  $\sigma\tau\sigma^{-1}$  is transposition.

## Result

3 of 3

See the solution of **Problem 22** for a proof of a more general statement. Click for more details.

## 15. a

This is a special case of **Problem 22**.

## Step 2

2

In particular if  $\tau = (i_1 \ \cdots \ i_k)$ , then for any  $\sigma$  we have that

$$\sigma\tau\sigma^{-1} = (\sigma(i_1) \ \cdots \ \sigma(i_k)),$$

i.e.  $\sigma\tau\sigma^{-1}$  is a  $k$ -cycle.

## Result

3

See the solution of **Problem 22** for a proof of a more general statement. Click for more details.

## 16. a

We use the result of **Problem 17** which states that  $S_3$  is generated by  $(1\ 2)$  and  $(1\ 2\ 3)$ . This implies that any automorphism  $\Phi : S_3 \rightarrow S_3$  is determined by its value on  $(1\ 2)$  and  $(1\ 2\ 3)$ .

## Step 2

2 of 5

Note that the elements of  $S_3$  are given by  $\text{id}$ ,  $(1\ 2)$ ,  $(1\ 3)$ ,  $(2\ 3)$ ,  $(1\ 2\ 3)$ ,  $(1\ 3\ 2)$ , with orders 1, 2, 2, 2, 3, 3, respectively.

Now since order of  $(1\ 2)$  is 2 and order of  $(1\ 2\ 3)$  is 3, and since an automorphism preserves orders, we have that it can only map  $(1\ 2)$  to  $(1\ 2)$ ,  $(1\ 3)$  or  $(2\ 3)$ , and that it can only map  $(1\ 2\ 3)$  to itself or  $(1\ 3\ 2)$ .

## Step 3

3 of 5

Let us inspect the automorphisms induced by those choices. Note that for a given  $\sigma$ ,  $\phi$  defined by  $\phi(\tau) = \sigma^{-1}\tau\sigma$  is an automorphism -- this is shown in **example 9** in the section **Homomorphisms and normal subgroups**. This means that if we find a  $\sigma$  which yields our given choice for values of  $\phi$  on  $(1\ 2)$  and  $(1\ 2\ 3)$ , then this immediately extends to an automorphism of  $S_3$ .

First, let

$$\phi_1((1\ 2)) = (1\ 2) \text{ and } \phi_1((1\ 2\ 3)) = (1\ 2\ 3),$$

this is obtained by setting  $\sigma = \text{id}$ .

Now let

$$\phi_2((1\ 2)) = (1\ 2) \text{ and } \phi_2((1\ 2\ 3)) = (1\ 3\ 2),$$

this is obtained by setting  $\sigma = (1\ 2)$ .

Let

$$\phi_3((1\ 2)) = (1\ 3) \text{ and } \phi_3((1\ 2\ 3)) = (1\ 2\ 3),$$

this is obtained by setting  $\sigma = (1\ 2\ 3)$ .

Let

$$\phi_4((1\ 2)) = (1\ 3) \text{ and } \phi_4((1\ 2\ 3)) = (1\ 3\ 2),$$

this obtained by setting  $\sigma = (2\ 3)$ .

Now let

$$\phi_5((1\ 2)) = (2\ 3) \text{ and } \phi_5((1\ 2\ 3)) = (1\ 2\ 3),$$

this is obtained by setting  $\sigma = (1\ 3\ 2)$ .

Lastly, let

$$\phi_6((1\ 2)) = (2\ 3) \text{ and } \phi_6((1\ 2\ 3)) = (1\ 2\ 3),$$

this is obtained by setting  $\sigma = (1\ 3)$ .

## Result

5 of 5

We have used the result of **Problem 15** to enumerate all the possible automorphisms. Click for the detailed proof.

## 17. a

Since, as it has been shown in the text, every element of  $S_n$  can be written as a product of transpositions, it is sufficient to prove that  $\tau = (1\ 2)$  and  $\sigma = (1\ 2\ \dots\ n)$  generate all the transpositions.

### Step 2

2 of 5

First note that

$$(1\ 2\ \dots\ n)(1\ 2)(1\ 2\ \dots\ n)^{-1} = (\sigma(1)\ \sigma(2)) = (2\ 3), \quad (1)$$

where the first equality follows from **Problem 22**. Likewise we see that if  $i, j < n$ , then

$$(1\ 2\ \dots\ n)(i\ j)(1\ 2\ \dots\ n)^{-1} = (\sigma(1)\ \sigma(2)) = (i+1\ j+1), \quad (2)$$

with a similar statement holding if one of them is equal to  $n$ . Now from (1) and (2) it inductively follows that  $\tau$  and  $\sigma$  generate all the transpositions  $(i\ i+1)$  where  $i < n$ , as well as  $(n\ 1)$ .

Now we note that

$$(2\ 3)(1\ 2)(2\ 3) = (1\ 3), \quad (3)$$

and similarly

$$(i\ i+1)(1\ i)(i\ i+1) = (1\ i+1). \quad (4)$$

Now by application of (3) and (4) and the result of the previous paragraph, we get that  $\tau$  and  $\sigma$  generate  $(1\ i)$  for all  $i \in \{2, \dots, n\}$ .

### Step 4

4 of 5

Let  $(a\ b)$  be an arbitrary transposition, then we have that

$$(1\ a)(1\ b)(1\ a) = (a\ b),$$

i.e.  $(a\ b)$  is generated by  $\tau$  and  $\sigma$ , which is what we needed to prove.

### Result

5 of 5

We note that it is sufficient to prove that they generate all the transpositions of  $S_n$  and then use that facts that  $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$ ,  $(i\ i+1)(1\ i)(i\ i+1) = (1\ i+1)$ , and  $(1\ a)(1\ b)(1\ a) = (a\ b)$  to prove that they do. Click for the detailed proof.

## 18. a

Let  $\tau_1 = (t_1 \ t_2)$  and  $\tau_2 = (t_3 \ t_4)$ . Let us first try to express this as a product of two 3-cycles. Suppose that we want to find out if there exist  $x_1, x_2, x_3$  such that

$$\tau_1\tau_2 = (x_1 \ x_2 \ x_3)(t_1 \ t_2 \ t_3).$$

Denote  $\pi = (x_1 \ x_2 \ x_3)$  and  $\rho = (t_1 \ t_2 \ t_3)$ . As we require  $\pi\rho(t_1) = t_2$ , since this is necessary for the equality to hold, this implies that  $\pi(t_2) = t_2$ . Furthermore, we also get that  $\pi\rho(t_2) = \pi(t_3) = t_1$ . Likewise,  $\pi\rho(t_3) = \pi(t_1) = t_4$  and  $\pi\rho(t_4) = \pi(t_4) = t_3$ .

Collecting these results we see that it's necessary that we have

$$\pi(t_1) = t_4, \ \pi(t_2) = t_2, \ \pi(t_3) = t_1, \ \pi(t_4) = t_3;$$

this is the permutation  $(t_1 \ t_4 \ t_3)$ . It is straightforward to check that this really satisfies our requirement, i.e. that

$$\tau_1\tau_2 = (t_1 \ t_4 \ t_3)(t_1 \ t_2 \ t_3).$$

## Result

2 of 2

If  $\tau_1 = (t_1 \ t_2)$  and  $\tau_2 = (t_3 \ t_4)$  then  $\tau_1\tau_2 = (t_1 \ t_4 \ t_3)(t_1 \ t_2 \ t_3)$ . Click for more details.

## 19. a

Let us break down this in possible cases.

First suppose they are all disjoint, then their product cannot be the identity since  $\tau_1(i) \neq i$  for some  $i$ , and by their disjointness so do we have  $\tau_1\tau_2\tau_3(i) \neq i$ .

## Step 2

2 of 4

Suppose they are not disjoint. If at least two of them are the same, say  $\tau_1 = \tau_2$ , then  $\tau_1\tau_2\tau_3 = \tau_3 \neq e$ . If no two are the same, but at least two of them share a common element, say (without the loss of generality)  $\tau_1 = (t_1 \ t_2)$  and  $\tau_2 = (t_2 \ t_3)$ , then

$$\tau_1\tau_2\tau_3 = (t_1 \ t_2 \ t_3)\tau_3,$$

and now since  $\tau_3$  is a transposition and can act at most two of the  $t_1, t_2$ , and  $t_3$ , it follows that the product maps at least one of them to something other than itself.

## Step 3

3 of 4

Since this explores all the possible cases: either they are disjoint, or at least two are the same, or at least two of them share one common element; then this finishes our proof.

## Result

4 of 4

We break down the proof in three cases, depending on whether they're disjoint, or at least two are the same, or at least two of them share one common element. Click for more details.

## 20. a

Suppose they are disjoint. Then by **Problem 1** we have that they commute, and their product cannot be the identity permutation, so then

$$(\tau_1 \tau_2)^2 = \tau_1 \tau_2 \tau_1 \tau_2 = (\tau_1)^2 (\tau_2)^2 = \text{id},$$

where  $\text{id}$  is the identity permutation.

## Step 2

2 of 3

Suppose now that they are not disjoint, then because they are distinct they share at most one element. Without the loss of generality we write  $\tau_1 = (t_1 \ t_2)$  and  $\tau_2 = (t_2 \ t_3)$ , then

$$\tau_1 \tau_2 = (t_1 \ t_2 \ t_3),$$

which has order 3 as it is a 3-cycle.

## Result

3 of 3

They are either disjoint, in which case their product has order 2, or they share one element, in which case their product has order 3. Click for more details.

## 21. a

Note that  $\sigma\tau = e$  can equivalently be phrased as  $\tau$  being the inverse of  $\sigma$ . Our statement is then equivalent to the statement that an inverse of a nonidentity permutation disturbs at least one same element as that permutation. To prove this, let  $\sigma$  be a nonidentity permutation, then let  $(i_1 \cdots i_n)$  be a cycle in  $\sigma$ . Then we have that

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{n-1}) = i_n, \sigma(i_n) = i_1,$$

but then also

$$i_1 = \tau(i_2), i_2 = \tau(i_3), \dots, i_{n-1} = \tau(i_n), i_n = \tau(i_1),$$

i.e. its inverse disturbs  $i_1, \dots, i_n$ .

## Result

2 of 2

Note that the statement is equivalent to the statement that an inverse of a nonidentity permutation disturbs at least one same element as that permutation. Click for the detailed proof.

## 22. a

We prove the following statement, which is the crux of the algorithm: suppose  $\sigma$  is any permutation in  $S_n$  and  $\tau$  a permutation in  $S_n$  which we write as a product of disjoint cycles, i.e.  $\tau = (x_1 \dots x_m)(y_1 \dots y_k) \dots$  (where the dots denote an arbitrary but finite number of disjoint cycles). Then

$$\sigma\tau\sigma^{-1} = (\sigma(x_1) \dots \sigma(x_m))(\sigma(y_1) \dots \sigma(y_k)) \dots$$

## Step 2

2 of 5

To prove this, let us investigate the image of an integer  $i \in \{1, \dots, n\}$  under both left-and right-hand sides. There are two cases we want to consider: the first one is when  $i = \sigma(t_j)$  for some  $t_j$  in cycle decomposition of  $\tau$ . Suppose, without loss of generality, that  $i = \sigma(x_1)$ , then we have

$$\sigma\tau\sigma^{-1}(i) = \sigma\tau(x_1) = \sigma(x_2),$$

but this is exactly the image of  $i$  under the right hand side as well.

## Step 3

3 of 5

Second case occurs when  $i \neq \sigma(t_j)$  for any  $t_j$  in the cycle decomposition of  $\tau$ . Then the right hand side obviously fixes  $i$ . Note that the fact that  $i \neq \sigma(t_j)$  implies that  $\sigma^{-1}(i) \neq t_j$  for any  $t_j$  in the cycle decomposition of  $\tau$ , i.e.  $\tau$  leaves  $\sigma^{-1}(i)$  fixed. This implies that

$$\sigma\tau(\sigma^{-1}(i)) = \sigma\sigma^{-1}(i),$$

which is what we wanted to obtain.

Thus we have shown that

$$\sigma\tau\sigma^{-1} = (\sigma(x_1) \dots \sigma(x_m))(\sigma(y_1) \dots \sigma(y_k)) \dots$$

since image of any  $i \in \{1, \dots, n\}$  is the same under both sides.

## Result

Steps for the algorithm:

1. Write  $\tau$  as a product of disjoint cycles.
2. For each number  $i$  in the cycle decomposition of  $\tau$ , replace it with  $\sigma(i)$ .
3. The resulting permutation is equal to  $\sigma\tau\sigma^{-1}$ .

23. a

Let  $\tau, \sigma \in S_n$  such that

$$\tau = (t_1 \cdots t_{m_1})(t_{m_1+1} \cdots t_{m_1+m_2}) \cdots (t_{m_1+\cdots+m_{k-1}+1} \cdots t_{m_1+\cdots+m_k})$$

and

$$\sigma = (s_1 \cdots s_{m_1})(s_{m_1+1} \cdots s_{m_1+m_2}) \cdots (s_{m_1+\cdots+m_{k-1}+1} \cdots s_{m_1+\cdots+m_k}).$$

Note that since all  $t_i$ , for  $i = 1, \dots, m_1 + \cdots + m_k$ , are distinct numbers in  $\{1, \dots, n\}$ , and as are all  $s_j$  for  $j = 1, \dots, m_1 + \cdots + m_k$ , then the following is a well-defined permutation:

$$\rho(l) = \begin{cases} t_r & \text{if } l = s_r \text{ for some } r \in \{1, \dots, n\} \\ l & \text{else.} \end{cases}$$

## Step 2

2 of 3

Now by the result of **Problem 22** we get that

$$\rho\sigma\rho^{-1} = (\rho(s_1) \cdots \rho(s_{m_1}))(\rho(s_{m_1+1}) \cdots \rho(s_{m_1+m_2})) \cdots (\rho(s_{m_1+\cdots+m_{k-1}+1}) \cdots \rho(s_{m_1+\cdots+m_k})) = \tau.$$

## Result

We use the **Problem 22** and define a suitable  $\rho$ . Click for more details.

## 24. a

Recall that the conjugacy class of an element  $g$  in group  $G$  is the set

$$\text{cl}(g) = \{a \in G : \text{there exists } b \in G \text{ such that } a = bgb^{-1}\}.$$

## Step 2

2 of 5

From **Problem 22** we have that for any  $\sigma \in S_n$ ,  $\sigma(1 2 \cdots n)\sigma^{-1} = (\sigma(1) \sigma(2) \cdots \sigma(n))$ ; thus a conjugate of  $(1 2 \cdots n)$  is an  $n$ -cycle. Furthermore, by **Problem 23** we have that each  $n$ -cycle is obtainable this way. Thus  $\text{cl}(a)$  is comprised of all the  $n$ -cycles in  $S_n$ .

## Step 3

3 of 5

To answer the question about the order of the centralizer, recall **Theorem 2.11.2** which states that the index of the centralizer of an element  $g$  in a finite group  $G$  is equal to the number of distinct conjugates of  $g$ . In symbols this turns into the equation

$$|G|/|C(g)| = |\text{cl}(g)|, \quad (1)$$

where  $|A|$  denotes the cardinality of  $A$  and  $C(g)$  denotes the centralizer of  $g$ . From (1) it follows that  $|C(g)| = |G|/|\text{cl}(g)|$ .

To find  $|\text{cl}((1 2 \cdots n))|$  we need to count all the  $n$ -cycles in  $S_n$ . Suppose  $(i_1 \cdots i_n)$  is an  $n$ -cycle in  $S_n$ , then there are  $n$  choices for  $i_1$ ,  $n - 1$  choices for  $i_2$ , etc., so in total  $n(n - 1)(n - 2) \cdots 2 \cdot 1 = n!$  choices for the numbers that appear in it. But note that we have overcounted, since we have

$$(i_1 i_2 i_3 \cdots i_{n-2} i_{n-1} i_n) = (i_2 i_3 \cdots i_n i_1) = (i_3 \cdots i_n i_1 i_2) = \dots,$$

i.e. there are  $n$  ways of writing an  $n$ -cycle. Thus

$$|\text{cl}((1 2 \cdots n))| = n!/n = (n - 1)!.$$

Now using  $|S_n| = n!$  we have that

$$|C((1 2 \cdots n))| = n!/(n - 1)! = n.$$

## Result

5 of 5

We find that the conjugacy class of  $(1 2 \cdots n)$  in  $S_n$  is the set of all  $n$ -cycles, and that order of its centralizer is  $n$ .

## 25. a

Recall that the conjugacy class of an element  $g$  in group  $G$  is the set

$$\text{cl}(g) = \{a \in G : \text{there exists } b \in G \text{ such that } a = bgb^{-1}\}.$$

### Step 2

2 of 4

From **Problem 22** we have that for any  $\sigma \in S_n$ ,  $\sigma(1 2)(3 4)\sigma^{-1} = (\sigma(1) \sigma(2))(\sigma(3) \sigma(4))$ . Thus we see that any permutation in the conjugacy class of  $(1 2)(3 4)$  is a product of two disjoint transpositions (because  $\sigma$  is one-to-one). Also from **Problem 23** we get that any product of two disjoint transposition can be obtained by conjugating  $(1 2)(3 4)$ ; this completely describes the conjugacy class of  $(1 2)(3 4)$  in  $S_n$ .

To find the order of the centralizer we again use **Theorem 2.11.2** (see the previous exercise for the statement), so that

$$|C((1 2)(3 4))| = |S_n| / |\text{cl}((1 2)(3 4))|. \quad (1)$$

Now in order to find  $|\text{cl}((1 2)(3 4))|$ , we have to count the number of products of two disjoint transpositions in  $S_n$ . Note that there are  $\binom{n}{2}$  ways to pick the first transposition and  $\binom{n-2}{2}$  ways to pick the second one. Since disjoint transpositions commute and so the order in which we pick them is irrelevant, we divide the result of this multiplication by 2 to arrive at

$$\begin{aligned} |\text{cl}((1 2)(3 4))| &= \frac{1}{2} \binom{n}{2} \binom{n-2}{2} \\ &= \frac{1}{2} \frac{n!}{2!(n-2)!} \frac{(n-2)!}{2!(n-4)!} \\ &= \frac{n!}{8(n-4)!} = \frac{1}{8} n(n-1)(n-2)(n-3). \end{aligned}$$

We substitute the known values into (1) to obtain

$$|C((1 2)(3 4))| = \frac{n!}{\frac{1}{8} n(n-1)(n-2)(n-3)} = 8(n-4)!.$$

The conjugacy class of  $(1\ 2)(3\ 4)$  in  $S_n$  is the set of all permutations which can be written as a product of two disjoint cycles, and the order of the centralizer of  $(1\ 2)(3\ 4)$  in  $S_n$  is equal to  $8(n - 4)!$ .

## Section 3–3

1. a

**To find:** Parity of the permutations given below.

(a)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix}$$

(b)  $(1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9)$

(c)  $(1\ 2\ 3\ 4\ 5\ 6)(1\ 2\ 3\ 4\ 5\ 7)$

(d)  $(1\ 2)(1\ 2\ 3)(4\ 5)(5\ 6\ 8)(1\ 7\ 9)$

**Solution:**

(a) Now the given permutation can be written as

$$\begin{aligned} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix} \\ &= (1\ 2\ 4)(3\ 5)(6\ 7\ 8\ 9) \\ &= (1\ 4)(1\ 2)(3\ 5)(6\ 9)(6\ 8)(6\ 7) \end{aligned}$$

The given permutation is written as **product of 6 transpositions, and 6 being even the parity of**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix}$$

**is even permutation.**

(b) Now the given permutation can be written as

$$\begin{aligned} & (1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9) \\ &= (1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)(7\ 9)(7\ 8) \end{aligned}$$

The given permutation is written as

**product of 7 transpositions, and 7 being odd the parity of  $(1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9)$  is odd permutation.**

(c) Now the given permutation can be written as

$$\begin{aligned} & (1 \ 2 \ 3 \ 4 \ 5 \ 6)(1 \ 2 \ 3 \ 4 \ 5 \ 7) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 \end{pmatrix} \\ &= (1 \ 3 \ 5 \ 7 \ 2 \ 4 \ 6) \\ &= (1 \ 6)(1 \ 4)(1 \ 2)(1 \ 7)(1 \ 5)(1 \ 3) \end{aligned}$$

The given permutation is written as

**product of 6 transpositions, and 6 being even the parity of  $(1 \ 2 \ 3 \ 4 \ 5 \ 6)(1 \ 2 \ 3 \ 4 \ 5 \ 7)$  is even permutation.**

(d) Now the given permutation can be written as

$$\begin{aligned} & (1 \ 2)(1 \ 2 \ 3)(4 \ 5)(5 \ 6 \ 8)(1 \ 7 \ 9) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 2 & 5 & 6 & 8 & 9 & 4 & 1 \end{pmatrix} \\ &= (1 \ 7 \ 9)(2 \ 3)(4 \ 5 \ 6 \ 8) \\ &= (1 \ 9)(1 \ 7)(2 \ 3)(4 \ 8)(4 \ 6)(4 \ 5) \end{aligned}$$

The given permutation is written as

**product of 6 transpositions, and 6 being even the parity of  $(1 \ 2)(1 \ 2 \ 3)(4 \ 5)(5 \ 6 \ 8)(1 \ 7 \ 9)$  is even permutation.**

## Result

(a),(c) and (d) are even permutation whereas (b) is an odd permutation.

[Click for the detailed solution.](#)

2. a

**Given:**  $\sigma$  is a  $k$ -cycle.

**To Prove:**  $\sigma$  is an odd permutation if  $k$  is even, and is an even permutation if  $k$  is odd.

**Proof:**

Let us consider

$$\sigma = (\alpha_1, \alpha_2, \dots, \alpha_k).$$

Then  $\sigma$  is a  $k$ -cycle.

**We endeavour to prove that we can write  $\sigma$  as a product of  $k - 1$  transpositions**

. We will do it by **Induction** on  $k$ .

If  $k = 2$  then

$$\sigma = (\alpha_1, \alpha_2),$$

which is 1 transposition, so we are done for  $k = 2$ .

Let our statement is true for any natural number less than  $k$ .

That is,

**any  $(k - 1)$  - cycle can be written as a product of  $k - 2$  transpositions**

**Inductive step:** Let

$$\sigma = (\alpha_1, \alpha_2, \dots, \alpha_k)$$

be a  $k$ -cycle, then

$$(\alpha_1, \alpha_2, \dots, \alpha_k) = (\alpha_1, \alpha_2, \dots, \alpha_{k-1})(\alpha_{k-1}, \alpha_k).$$

By the inductive assumption we know that  $(\alpha_1, \alpha_2, \dots, \alpha_{k-1})$  can be written as a product of  $k - 2$  transpositions (because it is a  $k - 1$  cycle, the inductive assumption applies here).

Moreover  $(\alpha_{k-1}, \alpha_k)$  is a **transposition**, so altogether this implies that  $(\alpha_1, \alpha_2, \dots, \alpha_k)$  can be written as a product of  $k - 1$  transpositions.

Hence our induction is done.

Therefore we have proved that,  $\sigma$  being a  $k$ -cycle can be written as a product of  $k - 1$  transpositions

Now two cases arise.

**Case-1:**  $k$  is even.

In this case  $k - 1$  is odd.

Then  $\sigma$  being a  $k$ -cycle, **It can be written as a product of odd number of transposition.**

Hence  $\sigma$  is an **odd permutation**.

**Case -2:**  $k$  is odd.

In this case  $k - 1$  is even.

Then  $\sigma$  being a  $k$ -cycle, **It can be written as a product of even number of transposition.**

Hence  $\sigma$  is an **even permutation**.

Consequently,  $\sigma$  is an odd permutation if  $k$  is even, and is an even permutation if  $k$  is odd.

This completes the proof.

## Result

4 of 4

$\sigma$  being a  $k$  cycle, we first proved that we can write  $\sigma$  as a product of  $k - 1$  transpositions, then from here we proposed that  $\sigma$  is an odd permutation if  $k$  is even, and is an even permutation if  $k$  is odd.

Click for the detailed proof.

### 3. a

Recall that we have a homomorphism  $\nu : S_n \rightarrow \{1, -1\}$ , where the latter is understood to be a group under ordinary integer multiplication,

**such that  $\nu$  maps all the even permutations to 1 and all the odd permutations to -1**

. Now we have

$$\nu(\tau^{-1}\sigma\tau) = \nu(\tau^{-1})\nu(\sigma)\nu(\tau) = (\nu(\tau))^2\nu(\sigma) = \nu(\sigma),$$

where we have used the facts that the parity of  $\tau$  and  $\tau^{-1}$  is the same and that  $x^2 = 1$  for any  $x \in \{1, -1\}$ .

Noting the aforementioned property of  $\nu$  this completes the proof.

#### Result

2 of

We use the homomorphism  $\nu : S_n \rightarrow \{1, -1\}$  which maps all the even permutations to 1 and all the odd permutations to -1. Click for more details.

### 4. a

Let  $n > m$ , then  $\sigma$  can be seen as an element of  $S_n$  via the procedure described in the problem statement. However, our previous decomposition of  $\sigma$  as a product of an even number of transpositions still holds in  $S_n$ , since the extension to  $S_n$  neither changed any of the previous mappings nor add any nonfixed points, so that no new transpositions are needed; this completes the proof.

#### Result

2 of 2

This is a consequence of the fact that the cycle decomposition remains essentially the same when passing from  $S_m$  to  $S_n$ . Click for more details.

### 5. a

**Given:**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & & & 7 & 8 & 9 & 6 \end{pmatrix}$$

is an even permutation in  $S_9$ .

**To Find:** The images of 4 and 5.

**Solution:** There are two cases arise.

**Case-1:** Image of 4 is 4 and image of 5 is 5 itself.

Then the given permutation becomes

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 4 & 5 & 7 & 8 & 9 & 6 \end{pmatrix}.$$

If we split the permutation, we get

$$\begin{aligned} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 4 & 5 & 7 & 8 & 9 & 6 \end{pmatrix} \\ &= (1 \ 3 \ 2)(6 \ 7 \ 8 \ 9) \\ &= (1 \ 2)(1 \ 3)(6 \ 9)(6 \ 8)(6 \ 7) \end{aligned}$$

It follows that the given permutation is odd in this case, which contradict the even parity. So, this case closed.

**Case-2:** Image of 4 is 5 and image of 5 is 4.

Then the given permutation becomes

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 5 & 4 & 7 & 8 & 9 & 6 \end{pmatrix}.$$

If we split the permutation, we get

$$\begin{aligned} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 5 & 4 & 7 & 8 & 9 & 6 \end{pmatrix} \\ &= (1 \ 3 \ 2)(4 \ 5)(6 \ 7 \ 8 \ 9) \\ &= (1 \ 2)(1 \ 3)(4 \ 5)(6 \ 9)(6 \ 8)(6 \ 7). \end{aligned}$$

It follows that the given permutation is even in this case, which coincides to our given condition.

So, the images of 4 is 5 and 5 is 4.

## Result

Result: Image of 4 is 5 and that of 5 is 4.

[Click for the detailed solution.](#)

## 6. a

**To Prove:** Every element in  $A_n$  is a product of 3-cycles.

**Proof:**

Let  $\sigma \in A_n$ .

Then

$$\sigma = \alpha_1 \alpha_2 \dots \alpha_{2t-1} \alpha_{2t}$$

where  $\alpha'_i$ s are **transpositions**.

Group these in pairs as follows:

$$\sigma = (\alpha_1 \alpha_2) (\alpha_3 \alpha_4) \dots (\alpha_{2t-1} \alpha_{2t})$$

Now consider the first pair  $(\alpha_1 \alpha_2)$  and without loss of generality call

$\alpha_1 = (i, j)$  and  $\alpha_2 = (k, l)$ .

If  $j = k$  then

$$\alpha_1 \alpha_2 = (i, j)(k, l) = (i, j)(j, l) = (i, l, j).$$

In this case  $\alpha_1 \alpha_2$  is a 3-cycle.

Otherwise,

$$\alpha_1 \alpha_2 = (i, j)(k, l) = (i, j)(j, k)(j, k)(k, l) = (i, k, j)(j, l, k).$$

In this case  $\alpha_1 \alpha_2$  is a **product of two 3-cycles**.

Continuing with the remaining pairs,

**we express the even permutation  $\sigma$  as a product of 3-cycles.**

Since  $\sigma$  is arbitrary, every element in  $A_n$  is a product of 3-cycles.

This completes the proof.

## Result

Click for proof.

### 7. a

By the **Problem 6** it is sufficient to prove that any 3-cycles can be written as a product of  $n$ -cycles. Let  $a, b, c$  be arbitrary distinct numbers from 1 to  $n$ , and let

$$\tau = (a \ b \ c \ \dots),$$

and

$$\sigma = (b \ a \ c \ \dots),$$

where the dots signify all the remaining numbers from 1 to  $n$ , written in the same order in both  $\tau$  and  $\sigma$ .

## Step 2

2 of 3

We compute

$$\tau \sigma^{-1} = (a \ c \ b).$$

Since an inverse of a  $k$ -cycle is again a  $k$ -cycle, and since  $a, b, c$  were arbitrary, we have obtained that any 3-cycle can be obtained as a product of two  $n$ -cycles, which is what we wanted.

We use **Problem 6** to reduce the question to showing that every 3-cycle is a product of  $n$ -cycles. Click for more details.

## 8. a

**To Find:** A normal subgroup of order 4 of the alternating group  $A_4$ .

**Construction:**

$A_4$  is the

group of even permutations of the set {1, 2, 3, 4}.

Precisely  $A_4$  is the set

$$A_4 := \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 2, 3), (1, 3, 2), (1, 2, 4), (1, 3, 4), (2, 3, 4), (2, 4, 3), (1, 4, 2), (1, 4, 3)\}$$

Now let us consider the subgroup  $H$  of  $A_4$  as

$$H := \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

Then  $H$  is a **subgroup of order 4** in  $A_4$ .

**Conjugation in  $S_n$  does not change the cycle structure, so that in particular it does not do that in  $A_n$**

Any element of  $A_4$  is of the form  $(i, j)(k, l)$ , call it as  $f$ .

Now for any element  $g$  in  $A_4$  the elements  $f$  and  $gfg^{-1}$

**have the same parity i.e. both have same order 2.**

But all the order 2 elements in  $A_4$  belongs to  $H$ , it follows that  $gfg^{-1}$  belongs to  $H$ .

This means that this subgroup is normal, because  $gHg^{-1} \subseteq H$ , which is an **equivalent condition for normality of a subgroup**.

Hence,  $H$  is a **normal subgroup** of  $A_4$  of order 4.

## Result

Solution.

## 9. a

See **Theorem 6.1.9.** for the case  $n \geq 6$ , we prove the case when  $n = 5$ . Note that all the elements of  $A_n$  are of one of these forms: a 5-cycle, a product of two transpositions, and a 3-cycle. If we prove that if  $N$  contains a 5-cycle then it contains a 3-cycle, and that if  $N$  contains a product of two transpositions then it contains a 3-cycle, we are done.

First suppose that  $N$  contains a 5-cycle  $\tau = (n_1 \dots n_5)$ . We want to conjugate  $\tau$  by an element of  $A_5$  such that the product of  $\tau$  and that conjugate is a 3-cycle.

To that end note that  $\sigma = (n_1 n_2)(n_3 n_4)$  is in  $A_5$  since it is a product of an even number of transpositions. Now we compute the conjugate of  $\tau$  by  $\sigma$ :

$$\sigma\tau\sigma^{-1} = (n_1 n_4 n_3 n_5 n_2).$$

Since  $N$  is normal, we have that  $\sigma\tau\sigma^{-1} \in N$ , but then as  $N$  is a group also  $\tau(\sigma\tau\sigma^{-1}) \in N$ , which we compute:

$$\tau(\sigma\tau\sigma^{-1}) = (n_1 \dots n_5)(n_1 n_4 n_3 n_5 n_2) = (n_1 n_5 n_3),$$

i.e.  $N$  contains a 3-cycle, which is what we wanted to prove.

### Step 3

3 of 4

Suppose now that  $N$  contains a product of two disjoint transpositions which we denote  $\tau$ . We follow the same basic strategy as in the first case; let  $\tau = (n_1 n_2)(n_3 n_4)$  and let  $\sigma = (n_1 n_2 k)$  where  $k \neq n_i$  for  $i = 1, \dots, 4$ . We have that

$$\sigma\tau\sigma^{-1} = (n_2 k)(n_3 n_4),$$

which is again in  $N$ . Now once more  $\tau(\sigma\tau\sigma^{-1}) \in N$  where we compute

$$\tau(\sigma\tau\sigma^{-1}) = (n_1 n_2 k),$$

which completes our proof.

### Result

A slightly less general form, when  $n \geq 6$ , is proved in **Chapter 6**, section

#### The Simplicity of $A_n$

. We prove the case for  $n = 5$ . Click for more details.

### 10. a

This is proved in **Theorem 6.1.8** and **Theorem 6.1.9**. However, those proofs use a different strategy to deal with the  $n = 5$  case. Now that we solved the **Problem 9** for  $n = 5$  we can use to prove the simplicity of  $A_5$  (though this would generalize, word-for-word, to the case  $n \geq 6$ , if we had proved the analogue of **Problem 9** for  $n \geq 6$ ; but this in any case proved in **Theorem 6.1.9**).

### Step 2

2 of 3

Suppose  $A_5$  has a nontrivial normal subgroup  $N$ . Then by **Problem 9**  $N$  contains a 3-cycle. By **Lemma 6.1.6**, all the 3-cycles are conjugate in  $A_5$ , so that by normalcy of  $N$  it contains all the 3-cycles. However, by **Problem 6** every element in  $A_5$  is a product of 3-cycles, and therefore  $N = A_5$ , which is what we wanted to prove.

### Result

3 of 3

This is proved in general in **chapter 6**, section

#### The Simplicity of $A_n$

. We use our solution of **Problem 9**, **Problem 6**, and **Lemma 6.1.6** to give a proof for  $A_5$ .



# 4

---

## Chapter 4

### Section 4–1

1. a

We consider  $\mathbb{Z}_{24} = \{[0], [1], \dots, [23]\}$ . Note that neither a zero nor a zero divisor can be invertible. Let  $[n] \in \mathbb{Z}_{24}$  be such that  $\gcd(n, 24) > 1$ , where  $\gcd(a, b)$  denotes the greatest common divisor of  $a$  and  $b$ , then there exists  $[k] \in \mathbb{Z}_{24}$ ,  $k \neq 0$ , such that 24 divides  $nk$ , and thus  $[n][k] = [0]$ , so that  $[n]$  is a zero divisor.

#### Step 2

2 of 4

Suppose now that  $[n] \in \mathbb{Z}_{24}$  such that  $\gcd(n, 24) = 1$ . Then by **Theorem 1.5.3** there exist integers  $m_0$  and  $n_0$  such that  $1 = n_0n + 24m_0$ , from which we get

$$n_0n \equiv 1 \pmod{24},$$

so that  $[n_0]$  is the inverse of  $n$  in  $\mathbb{Z}_{24}$ .

#### Step 3

3 of 4

As we have determined that elements  $[n]$  of  $\mathbb{Z}_{24}$  which are invertible are exactly those with  $\gcd(n, 24) = 1$ , and those are

$$[1], [5], [7], [11], [13], [17], [19], [23].$$

#### Result

4 of 4

The invertible elements are given by the residue classes  $[1], [5], [7], [11], [13], [17], [19], [23]$ . Click for more details.

2. a

Let  $F$  be a field. Since this, by the definition, means that  $F$  is a commutative ring, in order to show that  $F$  is an integral domain we just need to show it has no zero-divisors.

Suppose we have  $ab = 0$  for some  $a \neq 0, b$  in  $F$ . As  $F$  is a field then there exist an inverse of  $a$  in  $F$ , thus

$$\begin{aligned}a^{-1}(ab) &= a^{-1}0, \\(a^{-1}a)b &= 0, \\b &= 0.\end{aligned}$$

Since  $a$  was arbitrary nonzero element of  $F$ , it follows that there exist no zero-divisors in  $F$ , which completes our proof.

## Result

2 of 2

If  $a \neq 0$ , write  $ab = 0$ , multiply by the inverse of  $a$  to see that  $b = 0$  and thus there are no zero-divisors in  $F$ .

[Click for the detailed proof.](#)

## Method 2.

② Let  $F$  be a field. (1+0)  
Then  $F$  is a ring with unity and it is also commutative.  
Let  $a \in F \setminus \{0\}$  then  
 $a \cdot b = 1$  for some  $b \in F$ .  
Let  $a \cdot c = 0$  for some  $c \in F \setminus \{0\}$ .  
 $\Rightarrow c \cdot 1 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 0$   
but  $c \neq 0$  i.e. it is in contradiction  
Hence,  $F$  has no zero divisors  
 $\Rightarrow F$  is an integral domain.

3. a

Suppose that  $n$  isn't a prime and consider the ring  $\mathbb{Z}_n$ , then there exist positive integers  $1 < k, m < n$  such that  $n = km$ . But then

$$[k][m] = [n] = [0],$$

i.e. there are zero-divisors in  $\mathbb{Z}_n$ , which coupled with **Problem 2** means that  $\mathbb{Z}_n$  cannot be a field, thus proving that if  $\mathbb{Z}_n$  is a field then  $n$  must be prime.

## Step 2

2 of 3

Suppose now that  $n$  is a prime. We know that  $\mathbb{Z}_n$  is a commutative ring and thus to prove that it is a field it suffice to show that every nonzero element has an inverse. Since for every  $[k] \in \{[1], [2], \dots, [n-1]\}$  we have that  $\gcd(k, n) = 1$  then by **Theorem 1.5.3.**, there exist integers  $n_0$  and  $k_0$  such that  $1 = n_0n + k_0k$ ; this implies that

$$1 \equiv k_0k \pmod{n},$$

i.e. we have found an inveres of an arbitrary nonzero element in  $\mathbb{Z}_n$  so it follows that it is a field.

## Result

3 of 3

We prove and use the fact that  $\mathbb{Z}_n$  has no zero-divisors if and only if  $n$  is a prime.

4. a

(4). Let  $\mathbb{Q}_{\text{odd}} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \text{ & } \begin{array}{l} \gcd(p, q) = 1 \\ q \neq 0, q \text{ is odd} \end{array} \right\}.$

$\frac{0}{1} \in \mathbb{Q}_{\text{odd}}$  &  $\frac{1}{1} \in \mathbb{Q}_{\text{odd}}$

$\Rightarrow \mathbb{Q}_{\text{odd}} \neq \emptyset.$

further let  $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in \mathbb{Q}_{\text{odd}}$

then  $\frac{p_1}{q_1} - \frac{p_2}{q_2} = \frac{p_1q_2 - p_2q_1}{q_1q_2} \in \mathbb{Q}_{\text{odd}}$

(since  $q_1q_2$  is odd)

also  $\frac{p_1}{q_1} \cdot \frac{p_2}{q_2} \in \mathbb{Q}_{\text{odd}}$  (since  $q_1q_2$  is odd)

$\frac{p}{q}$  is invertible in  $\mathbb{Q}_{\text{odd}}$  if  $p$  is odd

Since  $\frac{q}{p} \in \mathbb{Q}_{\text{odd}}$  iff  $p$  is odd.

Method 2.

This is a special case of **Problem 5**, in case when  $p = 2$ . See it for a proof.

## Result

This is the  $p = 2$  case of **Problem 5**. See it for a proof.

### 5. a

Recall that  $R_p$ , for a prime  $p$ , is given by all the  $a \in \mathbb{Q}$  such that  $a = \frac{n}{k}$  where  $\gcd(n, k) = 1$  and  $k$  isn't divisible by  $p$ . Note that addition and multiplication on  $R_p$  are restrictions of multiplication on  $\mathbb{Q}$  so this implies their associativity and commutativity of addition, as well as distributivity of multiplication over addition, i.e. axioms (from the definition of a ring) **(b)**, **(c)**, **(g)**, **(h)** hold for  $R_p$ . We prove that the remaining axioms also hold.

#### Step 2

2 of 7

##### Axiom (a)

Let  $a, b \in R_p$  with  $a = c/d, b = e/f$  with  $\gcd(c, d) = \gcd(e, f) = 1$ . Now

$$a + b = \frac{cf + ed}{df}.$$

Since  $p$  doesn't divide  $d$  nor does it divide  $f$ , we have that it doesn't divide  $df$  (by the uniqueness of prime factorization of integers). Note that  $\frac{cf+ed}{df}$  isn't necessarily a reduced fraction, but any further reduction can only remove factors from  $df$ , so it cannot make it divisible by  $p$ .

##### Axiom (d)

We have  $0 = \frac{0}{1} \in R_p$ , i.e. the additive identity is in  $R$ .

#### Step 4

##### Axiom (e)

If  $n/k \in R_p$ , then  $-n/k \in R_p$  since  $1 = \gcd(n, k) = \gcd(-n, k)$  and  $p$  doesn't divide  $k$ .

#### Step 5

##### Axiom (f)

Let  $a, b \in R_p$  with  $a = c/d, b = e/f$  with  $\gcd(c, d) = \gcd(e, f) = 1$ . Then

$$ab = \frac{ce}{df},$$

where the identical consideration as in the **(a)** part hold.

Note that for any rational  $a/b$ ,  $ab \neq 0$  its multiplicative inverse is  $b/a$ ; thus  $a/b \in R_p$  has a multiplicative inverse in  $R_p$  if and only if  $b/a \in R_p$ . A necessary and sufficient condition for this is that  $p$  doesn't divide  $a$ , i.e. nonzero  $a/b$  is invertible in  $R_p$  iff  $p \nmid a$ .

## Result

7 of 7

We directly verify all the ring axioms. Click for the proof.

## Method 2.

**a (5)** Let  $\mathbb{Q}_p = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0, \gcd(p, q) = 1 \text{ & for fixed prime } p, p \nmid q \right\}$ .

$0, 1 \in \mathbb{Q}_p \Rightarrow \mathbb{Q}_p \neq \emptyset$ .

Let  $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in \mathbb{Q}_p \Rightarrow \frac{p_1}{q_1} - \frac{p_2}{q_2} = \frac{p_1 q_2 - p_2 q_1}{q_1 q_2} \in \mathbb{Q}_p$ .  
 (since  $p \nmid q_1, p \nmid q_2 \Rightarrow p \nmid q_1 q_2$ )

further  $\frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2} \in \mathbb{Q}_p$ .

$\frac{p_1}{q_1}$  is invertible in  $\mathbb{Q}_p$  iff  $p \nmid p_1$ .  
 (since  $\frac{q_1}{p_1} \in \mathbb{Q}_p$  iff  $p \nmid p_1$ ).

## 6. a

This is proved (and \LaTeX ified), in slightly more generality, in solution of **Problem 10**.

## Result

See **Problem 10** for a proof of a more general fact.

## Method 2.

$$\begin{aligned}
 ⑥ \quad & \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left( \begin{array}{cc} r & s \\ t & u \end{array} \right) = \left( \begin{array}{cc} ar+bt & as+bu \\ cr+dt & cs+du \end{array} \right) \\
 & \left\{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left( \begin{array}{cc} r & s \\ t & u \end{array} \right) \right\} \left( \begin{array}{cc} x & y \\ z & w \end{array} \right) = \left( \begin{array}{cc} axr+bxt+azs & ayx+byt \\ crx+dtx+czw & cyx+dty+cuw \end{array} \right) \\
 & \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left\{ \left( \begin{array}{cc} r & s \\ t & u \end{array} \right) \left( \begin{array}{cc} x & y \\ z & w \end{array} \right) \right\} = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left( \begin{array}{cc} rx+sz & ry+sw \\ tx+uz & ty+uw \end{array} \right) \\
 & = \left( \begin{array}{cc} arx+bsz+ & ayx+asw \\ btx+buw & +bty+buw \\ crx+csz+ & cxy+csw \\ dtx+duw & +dty+duw \end{array} \right)
 \end{aligned}$$

Hence, the multiplication is associative.

7. a

(a)

By the definition of matrix multiplication we have that it is equal to

$$\left( \begin{array}{cc} 1 \cdot \frac{1}{5} + 2 \cdot 0 & 1 \cdot \frac{2}{3} + 2 \cdot 1 \\ 4 \cdot \frac{1}{5} + (-7) \cdot 0 & 4 \cdot \frac{2}{3} + (-7) \cdot 1 \end{array} \right) = \left( \begin{array}{cc} \frac{1}{5} & \frac{8}{3} \\ \frac{4}{5} & -\frac{13}{3} \end{array} \right).$$

### Step 2

(b)

We have

$$\left( \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \right) \left( \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \right) = \left( \begin{array}{cc} 1 \cdot 1 + 1 \cdot 1 & 1 \cdot 1 + 1 \cdot 1 \\ 1 \cdot 1 + 1 \cdot 1 & 1 \cdot 1 + 1 \cdot 1 \end{array} \right) = \left( \begin{array}{cc} 2 & 2 \\ 2 & 2 \end{array} \right).$$

**(c)**

First we compute

$$\begin{pmatrix} 1/2 & 1/2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1/4 & 1/4 \\ 0 & 0 \end{pmatrix},$$

and then

$$\begin{pmatrix} 1/4 & 1/4 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1/8 & 1/8 \\ 0 & 0 \end{pmatrix}.$$

#### Step 4

**(d)**

Multiplying those two pairs of matrices we get

$$\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} - \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -b \\ c & 0 \end{pmatrix}.$$

#### Result

**(a)**

$$\begin{pmatrix} \frac{1}{2} & \frac{8}{3} \\ 0 & \frac{-3}{3} \end{pmatrix},$$

**(b)**

$$\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix},$$

**(c)**

$$\begin{pmatrix} 1/8 & 1/8 \\ 0 & 0 \end{pmatrix},$$

**(d)**

$$\begin{pmatrix} 0 & -b \\ c & 0 \end{pmatrix}.$$

Click for more details.

8. a

We have that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix},$$

and

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

From this we get that they commute if and only if

$$\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

which is equivalent to  $b = c = 0$ . Thus the set of all such matrices is given by all the matrices of form

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix},$$

where  $a, d$  are arbitrary real numbers.

## Result

The set of matrices which commute with

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

is given by all the matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

where  $a$  and  $d$  are arbitrary real numbers.

## Method 2.

$$\begin{aligned} \textcircled{\$} \quad & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Rightarrow \quad & \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \\ \Rightarrow \quad & c = 0, \quad b = 0. \\ \text{hence} \quad & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \quad & b = 0 = c, \quad a \text{ and } d \text{ are arbitrary}. \end{aligned}$$

9. a

From problem no (8) we see that if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

were to commute with

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

, we must have  $b = c = 0$ . Thus,

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

gives

$$\begin{pmatrix} ap & aq \\ dr & ds \end{pmatrix} = \begin{pmatrix} ap & dq \\ ar & ds \end{pmatrix}$$

This gives  $aq = dq \implies a = d$ . Thus all matrix of the forms

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

commutes with every  $2 \times 2$  matrices because

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

where  $a$  is some scalar and identity matrix commutes with every other matrix.

## 10. a

(a) Let

$$A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$$

$$B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

and

$$C = \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$$

We get

$$BC = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} = \begin{pmatrix} a_2a_3 + b_2c_3 & a_2b_3 + b_2d_3 \\ a_3c_2 + c_3d_2 & b_3c_2 + d_2d_3 \end{pmatrix}$$

and

$$\begin{aligned} A(BC) &= \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2a_3 + b_2c_3 & a_2b_3 + b_2d_3 \\ a_3c_2 + c_3d_2 & b_3c_2 + d_2d_3 \end{pmatrix} \\ &= \begin{pmatrix} a_3(a_1a_2 + b_1c_2) + c_3(a_1b_2 + b_1d_2) & b_3(a_1a_2 + b_1c_2) + (a_1b_2 + b_1d_2)d_3 \\ a_3(a_2c_1 + c_2d_1) + c_3(b_2c_1 + d_1d_2) & b_3(a_2c_1 + c_2d_1) + (b_2c_1 + d_1d_2)d_3 \end{pmatrix} \end{aligned}$$

And we have

$$AB = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ a_2c_1 + c_2d_1 & b_2c_1 + d_1d_2 \end{pmatrix}$$

and

$$(AB)C = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ a_2c_1 + c_2d_1 & b_2c_1 + d_1d_2 \end{pmatrix} \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_3(a_1a_2 + b_1c_2) + c_3(a_1b_2 + b_1d_2) & b_3(a_1a_2 + b_1c_2) + (a_1b_2 + b_1d_2)d_3 \\ a_3(a_2c_1 + c_2d_1) + c_3(b_2c_1 + d_1d_2) & b_3(a_2c_1 + c_2d_1) + (b_2c_1 + d_1d_2)d_3 \end{pmatrix}$$

This shows

$$(AB)C = A(BC)$$

(b) It is clear that

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in R \right\}$$

forms the additive abelian group as the addition occurs index wise. From problem no 9, we know that matrix multiplication is associative. Being subset of  $2 \times 2$  matrix, distributive laws hold as it holds in  $S$ . It remains to show that the multiplication is closed.

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$$

as  $a_1a_2, a_1b_2 + b_1c_2, c_1c_2 \in R$ , it remains closed under multiplication therefore given set is subring of  $S$ .

(c) Let

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

This gives

$$\begin{pmatrix} ap + br & aq + bs \\ cr & cs \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

With  $c \neq 0$  gives  $r = 0$  and we get

$$ap + br = ap = 1$$

and  $cs = 1$ . This shows if  $a$  and  $c$  have inverses in  $R$ , the given matrix is invertible. The inverse is

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix}$$

11. a

Given  $F : \mathbb{C} \rightarrow \mathbb{C}$  defined by  $F(a + bi) = a - bi$ .

(a) Let  $x = a_1 + ib_1$  and  $y = a_2 + ib_2$

$$\begin{aligned} F(xy) &= F((a_1 + ib_1)(a_2 + ib_2)) \\ &= F(a_1a_2 - b_1b_2 + i(a_2b_1 + a_1b_2)) \\ &= a_1a_2 - b_1b_2 - i(a_2b_1 + a_1b_2) \\ &= a_1(a_2 - ib_2) - ib_1(a_2 - ib_2) \\ &= (a_1 - ib_1)(a_2 - ib_2) \\ &= F(x)F(y) \end{aligned}$$

(b)

$$\begin{aligned} F(x\bar{x}) &= F((a + bi)(a - bi)) \\ &= F((a^2 + b^2) + 0i) \\ &= a^2 + b^2 - 0i \\ &= |x|^2 \end{aligned}$$

(c) Take  $x = a + ib$  and  $y = c + id$ . Then

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= F(x\bar{x})F(y\bar{y}) \\ &= F(x\bar{x}y\bar{y}) \\ &= F(xy\bar{x}\bar{y}) \\ &= F(xy)F(\bar{x}\bar{y}) \\ &= F((ac - bd) + i(ad + bc))F((ac - bd) - i(ad + bc)) \\ &= ((ac - bd) + i(ad + bc))((ac - bd) - i(ad + bc)) \\ &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

## 12. a

We have

$$\begin{aligned} (ac - bd)^2 + (ad + bc)^2 &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &= (a^2 + b^2)(c^2 + d^2) \end{aligned}$$

## 13. a

(a)

$$\begin{aligned}(i+j)(i-j) &= i \times i - i \times j + j \times i - j \times j \\&= -1 - k - k - (-1) \\&= -2k\end{aligned}$$

(b)

$$(1-i+2j-2k)(1+2i-4j+6k) = 23 + 5i + 4k$$

(c)

$$\begin{aligned}(2i-3j+4k)^2 &= -2^2 - 3^2 - 4^2 \\&= -29\end{aligned}$$

(d)

$$\begin{aligned}i(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) - (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)i \\= \alpha_2(i \times j) + \alpha_3(i \times k) - \alpha_2(j \times i) - \alpha_3(k \times i) \\= -2\alpha_3 j + 2\alpha_2 k\end{aligned}$$

## 14. a

It is clear that  $\alpha + \beta i$  commutes with  $i$  as

$$i(\alpha + \beta i) = i\alpha - \beta = \alpha i + \beta(i \times i) = (\alpha + i\beta)i$$

No quaternion of the form  $\gamma j + \zeta k$  commutes with  $i$ .

$$i(\gamma j + \zeta k) = \gamma k - \zeta j$$

and

$$(\gamma j + \zeta k)i = -\gamma k + \zeta j$$

Thus,  $i(\gamma j + \zeta k) = (\gamma j + \zeta k)i$  implies  $\gamma = \zeta = 0$ .

## 15. a

From problem no (14), we see that quaternions that commute with  $i$  is of the form  $\alpha + \beta i$ . If it were to commute with  $j$ , we have

$$j\alpha - \beta k = j(\alpha + \beta i) = (\alpha + \beta i)j = \alpha j + \beta k$$

This implies  $\beta = 0$ . Therefore the quaternions that commute with both  $i$  and  $j$  are of the form  $\alpha + 0i + 0j + 0k$ .

## 16. a

We have

$$\alpha_0(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = \alpha_0^2 - \alpha_0 \alpha_1 i - \alpha_0 \alpha_2 j - \alpha_0 \alpha_3 k \quad (1)$$

$$\alpha_1 i(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = \alpha_1^2 + \alpha_0 \alpha_1 i + \alpha_1 \alpha_3 j - \alpha_1 \alpha_2 k \quad (2)$$

$$\alpha_2 j(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = \alpha_2^2 - \alpha_2 \alpha_3 i + \alpha_0 \alpha_2 j + \alpha_1 \alpha_2 k \quad (3)$$

$$\alpha_3 k(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = \alpha_3^2 + \alpha_2 \alpha_3 i - \alpha_1 \alpha_3 j + \alpha_0 \alpha_3 k \quad (4)$$

Adding all those four, we get

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$$

## 17. a

Let  $\gamma_0, \gamma_1, \gamma_2, \gamma_3$  be defined as in (I) on page 132; we write  $a$  for  $\alpha$  and  $b$  for  $\beta$ . Then we have that  $\gamma_0^2 + \gamma_1^2 + \gamma_2^2 + \gamma_3^2$  is equal to

$$\begin{aligned} & (a_0 b_0)^2 + (a_1 b_1)^2 + (a_2 b_2)^2 + (a_3 b_3)^2 \\ & \quad - 2a_0 b_0 a_1 b_1 - 2a_0 b_0 a_2 b_2 - 2a_0 b_0 a_3 b_3 + 2a_1 b_1 a_2 b_2 + 2a_1 b_1 a_3 b_3 + 2a_2 b_2 a_3 b_3 \\ & + (a_0 b_1)^2 + (a_1 b_0)^2 + (a_2 b_3)^2 + (a_3 b_2)^2 \\ & \quad + 2a_0 b_1 a_1 b_0 + 2a_0 b_1 a_2 b_3 - 2a_0 b_1 a_3 b_2 + 2a_1 b_0 a_2 b_3 - 2a_1 b_0 a_3 b_2 - 2a_2 b_3 a_3 b_2 \\ & + (a_0 b_2)^2 + (a_1 b_3)^2 + (a_2 b_0)^2 + (a_3 b_1)^2 \\ & \quad - 2a_0 b_2 a_1 b_3 + 2a_0 b_2 a_2 b_0 + 2a_0 b_2 a_3 b_1 - 2a_1 b_3 a_2 b_0 - 2a_1 b_3 a_3 b_1 + 2a_2 b_0 a_3 b_1 \\ & + (a_0 b_3)^2 + (a_1 b_2)^2 + (a_2 b_1)^2 + (a_3 b_0)^2 \\ & \quad + 2a_0 b_3 a_1 b_2 - 2a_0 b_3 a_2 b_1 + 2a_0 b_3 a_3 b_0 - 2a_1 b_2 a_2 b_1 + 2a_1 b_2 a_3 b_0 - 2a_2 b_1 a_3 b_0 \end{aligned}$$

where the same-colored terms cancel out, and we get

$$\begin{aligned} & (a_0 b_0)^2 + (a_1 b_1)^2 + (a_2 b_2)^2 + (a_3 b_3)^2 + (a_0 b_1)^2 + (a_1 b_0)^2 + (a_2 b_3)^2 + (a_3 b_2)^2 \\ & + (a_0 b_2)^2 + (a_1 b_3)^2 + (a_2 b_0)^2 + (a_3 b_1)^2 + (a_0 b_3)^2 + (a_1 b_2)^2 + (a_2 b_1)^2 + (a_3 b_0)^2 \\ & = (a_0^2 + a_1^2 + a_2^2 + a_3^2)(b_0^2 + b_1^2 + b_2^2 + b_3^2), \quad (1) \end{aligned}$$

which is what we needed.

## 18. a

Given

$$|\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k| = \sqrt{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2}$$

Let  $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$  and  $y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$ . Then

$$|xy| = |\gamma_0 + i\gamma_1 + j\gamma_2 + k\gamma_3| = \sqrt{\gamma_0^2 + \gamma_1^2 + \gamma_2^2 + \gamma_3^2}$$

Where  $\gamma$ 's are defined as

$$\begin{aligned}\gamma_0 &= \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 \\ \gamma_1 &= \alpha_1\beta_0 + \alpha_0\beta_1 - \alpha_3\beta_2 + \alpha_2\beta_3 \\ \gamma_2 &= \alpha_2\beta_0 + \alpha_3\beta_1 + \alpha_0\beta_2 - \alpha_1\beta_3 \\ \gamma_3 &= \alpha_3\beta_0 - \alpha_2\beta_1 + \alpha_1\beta_2 + \alpha_0\beta_3\end{aligned}$$

By Lagrange identity, we get

$$(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2) = \gamma_0^2 + \gamma_1^2 + \gamma_2^2 + \gamma_3^2$$

Taking square root gives

$$\sqrt{(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2)} = \sqrt{\gamma_0^2 + \gamma_1^2 + \gamma_2^2 + \gamma_3^2}$$

Or,

$$|x||y| = |xy|$$

## 19. a

Let  $x = ai + bj + ck$  then

$$x^2 = (ai + bj + ck)(ai + bj + ck) = -a^2 - b^2 - c^2 = -1$$

This gives  $a^2 + b^2 + c^2 = 1$  which has infinitely many solutions for  $-1 < a, b, c < 1$ .

## 20. a

**(a)**

We first note that  $1 = 1 + 0i + 0j + 0k$  is the identity directly by the definition of multiplication of quaternions; furthermore it was proved in the chapter (see the discussion following (II)) that any nonzero quaternion has a multiplicative inverse, and by inspecting the form of that inverse we conclude that each element of  $Q$  has an inverse in  $Q$ .

Since  $Q$  is obviously closed under multiplication, it remains to show that the multiplication is associative. To that end, we define the following matrices in  $\mathbb{C}$

$$i' = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad j' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \text{and} \quad k' = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

We want to prove that these matrices have the same multiplicative relations as  $i, j$ , and  $k$ , which, when noted that matrix multiplication is associative, implies the associativity of  $Q$ . Of course,  $1$  is represented by the identity matrix  $I$  and  $-1$  by  $-I$ .

We have

$$i'^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I, \quad j'^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I, \quad k'^2 = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} = -I.$$

Also

$$i'j' = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} = k', \quad j'k' = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} = i', \quad k'i' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = j',$$

and

$$j'i' = \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix} = -k', \quad k'j' = \begin{pmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} = -i', \quad i'k' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -j'.$$

**(b)**

Denote by  $\langle s_1, s_2, \dots, s_n \rangle$  the subgroup generated by the elements  $s_1, \dots, s_n$ . We have the following nontrivial (cyclic) subgroups generated by each of the elements of  $Q$ :  $\langle -1 \rangle = \{1, -1\}$ ,  $\langle i \rangle = \{1, -1, i, -i\}$ ,  $\langle j \rangle = \{1, -1, j, -j\}$ ,  $\langle k \rangle = \{1, -1, k, -k\}$ . Furthermore, it is easy to see that these are all the subgroups, for if a subgroup of  $Q$  contained two elements from  $\{i, j, k\}$ , say  $i$  and  $j$ , then as  $ij = k$  and  $i^2 = -1$ , we easily see that it would equal the whole  $Q$ .

**Step 3**

3 of 5

**(c)**

Recall that the center of a group is the set (which can be shown to be a subgroup) of its elements which commute with all its other elements. Thus,  $1$  is in the center because the identity commutes with every element, and  $-1$  is also in it since multiplication by scalar commutes with every quaternion (this can be seen from the definition of the multiplication). Obviously  $i, j, k$  cannot be in the center of  $Q$  as neither them commutes with each other. Thus the center is equal to  $\{1, -1\}$ .

**(d)**

Its nonabelianness follows from the multiplication rules, e.g.  $ij = k$  but  $ji = -k$ . Now note that since  $\langle -1 \rangle$  is the center, by the **example 4** of page 73 it follows that it is a normal subgroup of  $Q$ . Recall also **Theorem 2.5.6.** which says that a subgroup  $N$  of  $G$  is normal if every left coset in  $G$  is a right coset in  $G$ .

Now note that  $|Q| = 8$  and  $|\langle i \rangle| = |\langle j \rangle| = |\langle k \rangle| = 4$ ,

These are all subgroups of order  $|Q|/2$ , so suppose that  $H$  is any of them and that  $g \notin H$ , then since  $|gH| = |H|$  and  $H \neq gH$ , we also have that  $gH = H^c$ , where  $H^c$  denotes the complement of  $H$  in  $G$ , and likewise  $Hg = H^c$ ; so that each left coset is a right coset.

**Result**

5 of 5

For **(a)**, we deal with the tricky part (associativity) by defining matrices which have the same multiplicative properties as members of  $Q$ .

In the **(b)** part we find that nontrivial groups of  $Q$  are given by  $\langle -1 \rangle, \langle i \rangle, \langle j \rangle, \langle k \rangle$ .

As for the **(c)** part, we find that the center of  $Q$  is equal to  $\{1, -1\}$ , and the **(d)** part proceeds by noting that all the subgroups of  $Q$  are either the center (which is always normal) or of cardinality  $|Q|/2$ .

[Click for more details.](#)

**21. a**

Let  $R$  be a division ring and  $a, b \in R$  such that  $ab = 0$ . If  $a \neq 0$  then  $a^{-1} \in R$  such that  $a^{-1}a = 1$ . This gives

$$a^{-1}(ab) = a^{-1} \cdot 0 \implies (a^{-1}a)b = 0 \implies 1 \cdot b = 0 \implies b = 0$$

Similarly if  $b \neq 0$ , the operating by  $b^{-1}$  from left side gives  $a = 0$ . Therefore the division is a domain.

**22. a**

We know that quaternion group  $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$  is not commutative since  $ij = k \neq -k = ji$ .

Take ring

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}$$

defined with usual addition and quaternion multiplication. This is ring with unity. This is not division ring because the only elements with inverses are members of  $Q_8$ . However it is a domain because no product of two non zero elements of  $\mathbb{H}$  is zero.

**23. a**

Let  $x = a_0 + a_1i + a_2j + a_3k$  and  $y = b_0 + b_1i + b_2j + b_3k$ .

### Step 2

#### (a)

We have that  $x^* = a_0 - a_1i - a_2j - a_3k$  and therefore

$$(x^*)^* = a_0 - (-a_1i) - (-a_2j) - (-a_3k) = a_0 + a_1i + a_2j + a_3k = x.$$

### Step 3

#### (b)

We have  $x + y = (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k$  and therefore

$$\begin{aligned} (x + y)^* &= (a_0 + b_0) - (a_1 + b_1)i - (a_2 + b_2)j - (a_3 + b_3)k \\ &= a_0 - a_1i - a_2j - a_3k + b_0 - b_1i - b_2j - b_3k \\ &= x^* + y^*. \end{aligned}$$

#### (c)

We have, by the definition of quaternion multiplication,

$$\begin{aligned} xx^* &= (a_0 + a_1i + a_2j + a_3k)(a_0 - a_1i - a_2j - a_3k) \\ &= (a_0^2 + a_1^2 + a_2^2 + a_3^2) + (-a_0a_1 + a_1a_0 - a_2a_3 + a_3a_2)i \\ &\quad + (-a_0a_2 + a_1a_3 + a_2a_0 - a_3a_1)j + (-a_0a_3 - a_1a_2 + a_2a_1 + a_3a_0)k \\ &= (a_0^2 + a_1^2 + a_2^2 + a_3^2) + 0i + 0j + 0k = (a_0^2 + a_1^2 + a_2^2 + a_3^2). \end{aligned}$$

This is a sum of squares of real numbers, so it is a positive real number. By inspecting the definition of quaternion multiplication and the forms of  $x$  and  $x^*$  we note that the product  $x^*x$  would be the same except that all the terms  $a_i a_j$  where  $i \neq j$  would change their sign; but since they sum to 0 anyway, we get that  $xx^* = x^*x$ .

**(d)**

We have that, by the definition of quaternion multiplication

$$\begin{aligned}(xy)^* &= ((a_0b_0 - a_1b_0 - a_2b_2 - a_3b_3) + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)i \\ &\quad + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)j + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0)k)^* \\ &= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + (-a_0b_1 - a_1b_0 - a_2b_3 + a_3b_2)i \\ &\quad + (-a_0b_2 + a_1b_3 - a_2b_0 - a_3b_1)j + (-a_0b_3 - a_1b_2 + a_2b_1 - a_3b_0)k.\end{aligned}$$

We also have

$$\begin{aligned}y^*x^* &= (b_0 - b_1i - b_2j - b_3k)(a_0 - a_1i - a_2j - a_3) = \\ &= (b_0a_0 - b_1a_1 - b_2a_2 - b_3a_3) + (-b_0a_1 - b_1a_0 - b_2a_3 + b_3a_2)i \\ &\quad + (-b_0a_2 + b_1a_3 - b_2a_0 - b_3a_1)j + (-b_0a_3 - b_1a_2 + b_2a_1 - b_3a_0)k \\ &= (xy)^*.\end{aligned}$$

**Result**

6 of 6

We use the definition of  $x^*$  to write out the terms and show equality straightforwardly in each part. Click for the detailed proof.

**24. a**

We have that

$$\begin{aligned}|xy| &= \sqrt{(xy)(xy)^*} \\ &= \sqrt{xyy^*x^*} \\ &= \sqrt{x(yy^*)x^*} \\ &= \sqrt{xx^*(yy^*)} \\ &= \sqrt{xx^*}\sqrt{yy^*} = |x||y|,\end{aligned}$$

where we used the definition of  $|\cdot|$ , properties (c) and (d) from the previous problem; in the fourth equality we used the fact that  $yy^*$  is a real number and thus it commutes with quaternions, in particular with  $x^*$ .

**Result**

2 of 2

We write out  $|xy|$  and use the properties (c) and (d) from the previous problem to transform that into  $|x||y|$ . Click to see more details.

**25. a**

Let  $x = a_0 + a_1i + a_2j + a_3k$ ,  $y = b_0 + b_1i + b_2j + b_3k$ . Note that by the (c) part of **Problem 23** we have that

$$|x| = \sqrt{a_0^2 + a_1^2 + a_2^2 + a_3^2},$$

and likewise for  $y$ . Now if  $xy = \gamma_0 + \gamma_1i + \gamma_2j + \gamma_3k$  (for the forms of  $\gamma_i$  see (l) on page 132) then by

**Problem 24** we have that

$$\gamma_0^2 + \gamma_1^2 + \gamma_2^2 + \gamma_3^2 = (|xy|)^2 = |x|^2|y|^2 = (a_0^2 + a_1^2 + a_2^2 + a_3^2)(b_0^2 + b_1^2 + b_2^2 + b_3^2),$$

which is what we needed to prove.

## Result

2 of 2

We note that  $|x| = \sqrt{a_0^2 + a_1^2 + a_2^2 + a_3^2}$  for  $x = a_0 + a_1i + a_2j + a_3k$ , from where Lagrange's Identity follows from a simple application of **Problem 24**. Click for more details.

## 26. a

The matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$$

has (a right, but everything is analogues for the left) inverse if and only if there exist a matrix

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \in R$$

such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

That is, if the system

$$\begin{aligned} ae + bg &= 1 \\ af + bh &= 0 \\ ce + dg &= 0 \\ cf + dh &= 1, \end{aligned}$$

has a solution. Note that if either  $a = 0$  and  $b = 0$  or  $c = 0$  and  $d = 0$  then the system has no solutions because either the first or the last equations is of the form  $0 = 1$ . Assume, without loss of generality, that  $a \neq 0$  and  $d \neq 0$ . Let us multiply the second equation by  $c$ , the last equation by  $a$ , and subtract them:

$$\begin{aligned} (acf + adh) - (caf + bhc) &= a - 0, \\ adh - bhc &= a, \\ h(ad - bc) &= a \end{aligned}$$

where we see that for the system to be solvable it is necessary that  $ad - bc \neq 0$ , since  $a \neq 0$ . However, this procedure gives us the converse as well, for following via this procedure we get that

$$e = \frac{d}{ad - bc}, \quad f = \frac{-b}{ad - bc}$$

$$g = \frac{-c}{ad - bc}, \quad h = \frac{a}{ad - bc}$$

yielding our inverse

$$\frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Thus, as we can arrive at the inverse supposing that  $ad - bc \neq 0$ , we proved our statement.

## Result

2 of 2

We write out

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and solve the equations for  $e, f, g, h$ . Click for more details.

27. a

Let

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$y = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

. We compute

$$\begin{aligned} \det xy &= \det \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} \\ &= (ae + bg)(cf + dh) - (af + bh)(ce + dg) \\ &= \cancel{aecf} + \cancel{aedh} + \cancel{bgcf} + \cancel{bgdh} - \cancel{afce} - \cancel{afdg} - \cancel{bhce} - \cancel{bhdg} \\ &= aedh + bgcf - afdg - bhce \\ &= ad(eh - fg) + bc(gf - he) \\ &= (ad - bc)(eh - fg) = \det x \det y, \end{aligned}$$

which is what we needed to prove.

## Result

2 of 2

We write out  $\det xy$  by the definition of the  $\det$  and show that it is equal to  $\det x \det y$ . Click for more details.

28. a

To show that  $G$  is closed under matrix multiplication, recall **Problem 27** where it was shown that  $\det xy = \det x \det y$ . So suppose that  $x \in G$  and  $y \in G$ , then  $\det xy = \det x \det y \neq 0$  because  $\det x \neq 0$  and  $\det y \neq 0$ , so that  $xy \in G$ .

### Associativity

In **Problem 10** it was shown that matrix multiplication is associative.

### Identity

We have that for any matrix  $A$  and for

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

we have

$$AI = IA = A,$$

and also  $\det(I) = 1 \cdot 1 - 0 \cdot 0 = 1$  so that  $I \in G$ .

### Inverses

It was proven in **Problem 26** that  $\det x \neq 0$  is a necessary and a sufficient condition for  $x$  to be invertible, therefore every element of  $G$  is invertible and its inverse again in  $G$  because  $\det x^{-1} = 1/\det x$ , which follows from **Problem 27** because we have

$$1 = \det(I) = \det xx^{-1} = \det x \det x^{-1}.$$

To show that  $N$  is a subgroup of  $G$ , note that if  $x, y \in N$  then  $\det xy^{-1} = \det x \det y^{-1} = 1 \cdot 1 = 1$ , so that  $xy^{-1} \in N$ . By the **Problem 15** in Subgroups section (page 55) this suffices to show that  $N$  is a subgroup.

Now recall that  $N$  is a normal subgroup of  $G$  if for every  $g \in G$  and for every  $n \in N$ , we have that  $gng^{-1} \in N$ . So now let  $g \in G$  and  $n \in N$ , then

$$\det gng^{-1} = \det g \det n \det g^{-1} = (\det g) \left( \frac{1}{\det g} \right) = 1,$$

which means that  $gng^{-1} \in N$ , so  $N$  is a normal subgroup of  $G$ .

### Result

3 of 3

We use the previous problems where we have proved various properties of matrices and determinants to give these two proofs. Click for more details.

### Method 2.

28 We use the property  $\det(xy) = \det(x)\det(y)$ .

To show  $\{x \in R : \det(x) = 1\} = G$  is a group.

We show following

①  $\det I = 1 \neq 0$ , there  $I \in G$ .

② Let  $x \in G$ ,  $\det(x^{-1}) = \frac{1}{\det(x)} \neq 0$  therefore  $x^{-1} \in G$

③ Let  $x, y \in G$ ,  $\det(xy) = \det(x)\det(y) \neq 0$  therefore  
 $xy \in G$

④ Matrix multiplication is associative.

Therefore  $G$  is a group.

Let  $N = \{x \in R \mid \det(x) = 1\}$ . We first show  $N$  is subgroup

① for  $x \in N$ ,  $\det(x^{-1}) = \frac{1}{\det(x)} = 1 \Rightarrow x^{-1} \in N$

② for  $x, y \in N$ ,  $\det(xy) = \det(x)\det(y) = 1 \Rightarrow xy \in N$

③  $I \in N$  because  $\det I = 1$

This shows  $N$  is subgroup of  $G$ .

To show it is normal, let  $n \in N$ ,  $g \in G$ ,

$$\begin{aligned}\det(gng^{-1}) &= \det(g) \cdot \det(n) \cdot \det(g^{-1}) \\ &= \det(g) \cdot 1 \cdot \frac{1}{\det(g^{-1})} = 1\end{aligned}$$

$\therefore gng^{-1} \in N \Rightarrow N$  is normal in  $G$ .

29. a

Let us first suppose that  $\det x \neq 0$  but that  $x$  is a zero-divisor. Then there exist the inverse  $x^{-1} \in R$  and a  $y \in R$ ,  $y \neq 0$ , such that

$$xy = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

but then

$$\begin{aligned}x^{-1}xy &= x^{-1} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \\ y &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\end{aligned}$$

which contradicts assumption that  $y \neq 0$ , so that we have arrived at contradiction: thus we must have that that  $\det x = 0$ .

Now suppose that  $x \in R$  such that

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$$

but  $\det x = ad - bc = 0$ . Then at least one of  $a, b, c, d$  isn't zero, since  $x \neq 0$ ; without loss of generality assume that  $a \neq 0$ , then the matrix

$$\begin{pmatrix} b & b \\ -a & -a \end{pmatrix} \neq 0$$

but we have that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} b & b \\ -a & -a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

i.e.  $x$  is a zero divisor.

## Result

3 of 3

For the first statement we use the fact that if  $\det x$  then  $x$  has an inverse, while for the second one we pick a suitable matrix to show that  $x$  is a zero-divisor. Click for the detailed proof.

## 30. a

Let

$$F = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \text{ real} \right\}.$$

In order to show that  $(F, +, \cdot)$  is a field we have to show  $(F, +)$  is an abelian group, that  $(F \setminus \{0\}, \cdot)$  is an abelian group and that  $\cdot$  distributes over  $+$ .

Firstly, associativity in  $(F, +)$  follows from associativity of more general matrices, which just follows from addition of real numbers being associative; commutativity also follows from the commutativity of addition of real numbers, since addition is performed ``coordinatewise''. Now, in order to show that  $F$  is closed under  $+$ , we compute

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in F.$$

We also have that

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in F$$

for  $a = 0$  and  $b = 0$ , so that  $F$  contains the additive identity. Lastly, to show the existence of inverses in  $F$ , note that if

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in F$$

then

$$-A = \begin{pmatrix} -a & -b \\ -(-b) & -a \end{pmatrix} \in F.$$

Now, note that associativity of  $(F \setminus \{0\}, \cdot)$  follows from associativity of general matrices, proven in **Problem 10**.

We have to show that  $F \setminus \{0\}$  is closed under multiplication:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} \in F \quad (1)$$

And that

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

and

$$\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

commute:

$$\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ca - db & cb + da \\ -da - cb & -db + ca \end{pmatrix} = (1).$$

Furthermore, we see that the identity is in  $F$  for  $a = 1$  and  $b = 0$ . To show that an element of  $F$  has an inverse in  $F$ , note that

$$\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2,$$

so that

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \begin{pmatrix} a/(a^2 + b^2) & -b/(a^2 + b^2) \\ -(-b/(a^2 + b^2)) & a/(a^2 + b^2) \end{pmatrix} \in F.$$

#### Step 4

4 of 5

Lastly, we want to show distributivity; this is true for general matrices so it is true in particular for matrices in  $F$ . For we have that

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left( \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e+i & f+j \\ g+k & h+l \end{pmatrix} \\ &= \begin{pmatrix} a(e+i) + b(g+k) & a(f+j) + b(h+l) \\ c(e+i) + d(g+k) & c(f+j) + d(h+l) \end{pmatrix} \\ &= \begin{pmatrix} ae + ai + bg + bk & af + aj + bh + bl \\ ce + ci + dg + dk & cf + cj + dh + dl \end{pmatrix} \\ &= \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} + \begin{pmatrix} ai + bk & aj + bl \\ ci + dk & cj + dl \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} i & j \\ k & l \end{pmatrix}, \end{aligned}$$

which is what we needed to get. Note that  $F$  is isomorphic to  $\mathbb{C}$ .

#### Result

We check that all field axioms hold for those matrices. Click for the detailed proof.

31. a

We claim that if  $ad - bc \neq 0$  --and note that  $ad - bc$  here refers to an element of the field of  $\mathbb{Z}_p$  -- then

$$\begin{pmatrix} d/(ad - bc) & -b/(ad - bc) \\ -c/(ad - bc) & a/(ad - bc) \end{pmatrix} \in R$$

, then the result follows by matrix multiplication.

Recall that  $\mathbb{Z}_p$  is a field, so that any  $ad - bc \neq 0$  is invertible. Thus for any  $k \in \mathbb{Z}_p$ ,  $k/(ad - bc) \in \mathbb{Z}_p$ , and then so is that matrix in  $R$ .

## Result

2 of 2

We note that  $\mathbb{Z}_p$  is a field, so we can use the classical formula for the inverse of a matrix. Click for more details.

## 32. a

By the virtue of  $\mathbb{Z}_p$  being a field, the same calculation as in **Problem 27** holds.

## Result

2 of 2

See **Problem 27** for the calculation which shows this equality. The calculation holds for any  $2 \times 2$  with entries in a field, and so in particular it holds matrices with entries from  $\mathbb{Z}_p$ .

## 33. a

### (a)

Note that the proof from **Problem 28** generalizes  $2 \times 2$  matrices with entries in any field, so in particular for  $\mathbb{Z}_p$ .

## Step 2

2 of 5

### (b)

We want to find out the number of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$$

such that  $ad - bc \neq 0$ ; in other words, we want to count the number of  $a, b, c, d \in \mathbb{Z}_p$  such that  $ad \neq bc$ . Note, however, that as we know the total number of matrices in  $R$  ( $p^4$ ,  $p$  choices for each of  $a, b, c, d$ ) then we can just as well count all the  $a, b, c, d$  such that  $ad = bc$  and then subtract that from  $p^4$ .

Suppose first  $a = 0$ . Then we must have  $b = 0$  or  $c = 0$ , or both, while  $d$  is arbitrary. Thus there are  $p$  ways to choose  $d$ , while for  $(b, c)$  we have all the  $(0, y)$ ,  $y \in \mathbb{Z}_p \setminus \{0\}$  ( $p - 1$  choices), all the  $(x, 0)$ ,  $x \in \mathbb{Z}_p \setminus \{0\}$  ( $p - 1$  choices), and  $(0, 0)$ , so a total of  $p((p - 1) + (p - 1) + 1) = p(2p - 1)$  choices.

Now suppose that  $a \neq 0$ , then we have  $d = bc/a$ . Since the only restriction on  $a$  that we have is that it's nonzero, we have  $p - 1$  choices for  $a$ , and since we have no restriction on  $b, c, d$ , but  $d$  is determined completely by our choices of  $a, b, c$ , then we are left with  $p$  choices for  $b$  and  $p$  choices for  $c$ .

Now we can compute the order of  $G$  as

$$p^4 - p(2p - 1) - (p - 1)pp = p^4 - 2p^2 + p - p^3 + p^2 = p^4 - p^3 - p^2 + p.$$

(c)

Recall that **Problem 8** and **Problem 9** did not use any special properties of  $\mathbb{R}$ , but rather that the calculation made there hold for  $2 \times 2$  matrices over any field. Thus the matrices in the center are given by

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

for any  $a \in \mathbb{Z}_p$ .

(d)

Recall that a  $p$ -Sylow subgroup of  $G$  is a subgroup of order  $p^n$  such that  $n$  is the highest number such that  $p^n$  divides  $|G|$ . First note that

$$|G| = p^4 - p^3 - p^2 + p = p(p^3 - p^2 - p + 1),$$

where we have that  $p^3 - p^2 - p + 1 \equiv 1 \pmod{p}$ , i.e.  $p$  doesn't divide  $p^3 - p^2 - p + 1$  so that we have that  $n = 1$  is the highest number such that  $p^n \mid |G|$ . Also recall that a group of prime order is cyclic; so we have to find a matrix  $A \in G$  such that  $|\langle A \rangle| = p$ , or equivalently a matrix  $A$  such that its order is  $p$ . Note that if

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

then

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

$$A^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix},$$

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

so that

$$A^p = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$A^n \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

for  $n = 1, \dots, p-1$ , which is what we needed.

## Result

(a) **Problem 28** generalizes straightforwardly to this case.

(b) We employ some simple combinatorics in order to count the order of  $G$ .

(c) Follows from considerations in **Problem 8** and **Problem 9**.

(d) We note that it is sufficient to find an element of order  $p$  in  $G$ , then we note that

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

fits the bill.

[Click for more details.](#)

By the **Problem 33** we have that the order of  $T$  is  $2^4 - 2^3 - 2^2 + 2 = 6$ ; we now find those six matrices:

$$\begin{aligned} A_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & A_2 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ A_3 &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, & A_4 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \\ A_5 &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, & A_6 &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

with orders 1, 2, 2, 2, 3, 3 respectively.

Note that  $S_3$  is composed of elements

$$\text{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2),$$

with orders 1, 2, 2, 2, 3, 3 respectively. Also note that, by **Problem 17** of **Cycle Decomposition** section of the third chapter we have that  $(1\ 2)$  and  $(1\ 2\ 3)$  generate  $S_3$ . We also have that  $(1\ 3\ 2) = (1\ 2\ 3)(1\ 2\ 3)$ , that  $(1\ 3) = (1\ 2\ 3)(1\ 2)$ ,  $(1\ 2)(1\ 2\ 3) = (2\ 3)$  and  $(1\ 2)(1\ 2) = \text{id}$ .

Now we can check that  $\tau(A_2) = (1\ 2)$ ,  $\tau(A_5) = (1\ 2\ 3)$  induces an isomorphism. We compute

$$\begin{aligned} \tau(A_1) &= \tau(A_2 A_2) = \tau(A_2) \tau(A_2) = \text{id} \\ \tau(A_3) &= \tau(A_5 A_2) = \tau(A_5) \tau(A_2) = (1\ 2\ 3)(1\ 2) = (1\ 3) \\ \tau(A_4) &= \tau(A_2 A_5) = \tau(A_2) \tau(A_5) = (1\ 2)(1\ 2\ 3) = (2\ 3) \\ \tau(A_6) &= \tau(A_5 A_5) = \tau(A_5) \tau(A_5) = (1\ 3\ 2). \end{aligned}$$

Thus we see that  $\tau$  extended to an isomorphism, since  $A_2$  and  $A_5$  generate  $T$ , so that  $\tau(A_i A_j) = \tau(A_i) \tau(A_j)$  follows from writing  $A_i$  and  $A_j$  in terms of  $A_2$  and  $A_5$  and using the equalities and relations shown above.

## Result

We use generators of  $T$  and  $S_3$  to find an isomorphism between them. Click for more details.

### 35. a

Let us find zero-divisors in  $S$ .

Let

$$f(x) = \begin{cases} (x - 1/2)^2 & \text{if } x \leq 1/2 \\ 0 & \text{if } x > 1/2 \end{cases}$$

and

$$g(x) = \begin{cases} 0 & \text{if } x \leq 1/2 \\ (x - 1/2)^2 & \text{if } x > 1/2. \end{cases}$$

Then we immediately see that  $fg(x) = 0$  for all  $x \in (0, 1)$ . We prove that  $f$  is differentiable on  $(0, 1)$ , since the proof for  $g$  is completely analogous.

Note that differentiability of  $f$  on all points except  $1/2$  is obvious, since polynomials are always differentiable.

To show differentiability, consider the limit

$$\lim_{h \rightarrow 0} \frac{f(1/2 + h) - f(1/2)}{h} = \lim_{h \rightarrow 0} \frac{f(1/2 + h)}{h},$$

this limit exists if the limits as  $h$  approaches 0 from the right and approaches 0 to the right exist and are equal, i.e. if limits

$$\lim_{h \rightarrow 0^+} \frac{f(1/2 + h)}{h} \text{ and } \lim_{h \rightarrow 0^-} \frac{f(1/2 + h)}{h}$$

exist and are equal. The first limit is obviously equal to 0 as  $f(1/2 + h) = 0$  for  $h > 0$ . Second limit evaluates to

$$\lim_{h \rightarrow 0^-} \frac{f(1/2 + h)}{h} = \lim_{h \rightarrow 0^-} \frac{(1/2 + h - 1/2)^2}{h} = \lim_{h \rightarrow 0^-} \frac{h^2}{h} = 0.$$

As  $fg(x) = 0$  for all  $x \in (0, 1)$  this completes our proof.

### Result

3 of 3

We find zero-divisors in  $S$ . Click for the complete proof.

### 36. a

To show that  $H(\mathbb{C})$  is not a division ring, it suffices to find a zero divisor in it, for zero-divisor cannot have an inverse. Due to possible of confusion we write  $\mathcal{I}$  for the imaginary unit in  $\mathbb{C}$  and  $i$  for the quaternion  $i$ . Now we have that

$$(1 - i\mathcal{I})(1 + i\mathcal{I}) = 1 + i^2 = 0,$$

which completes our proof.

### Result

2 of

We find a zero-divisor in  $H(\mathbb{C})$ . Click for more details.

### 37. a

We want to find  $a_0, a_1, a_2, a_3 \in \mathbb{C}$  such that

$$(a_0 + a_1i + a_2j + a_3k)(a_0 + a_1i + a_2j + a_3k) = 0 + 0i + 0j + 0k. \quad (1)$$

Now using the definition of quaternion multiplication we see that (1) is equivalent to

$$\begin{aligned} a_0^2 - a_1^2 - a_2^2 - a_3^2 &= 0, \\ a_0a_1 + a_1a_0 + a_2a_3 - a_3a_2 &= 0, \\ a_0a_2 - a_1a_3 + a_2a_0 + a_3a_1 &= 0, \\ a_0a_3 + a_1a_2 - a_2a_1 + a_3a_0 &= 0. \end{aligned}$$

From the first equation we have that  $2a_0a_1 = 0$ , from the second that  $2a_0a_2 = 0$  and from the third that  $2a_0a_3 = 0$ . Thus if we put  $a_0 = 0$  then from the first equation we need to find  $a_1, a_2, a_3 \in \mathbb{C}$  such that  $a_1^2 + a_2^2 + a_3^2 = 0$ ; this is satisfied for  $a_1 = 1$  and  $a_2 = i$  (by  $i$  we denote the imaginary unit in  $\mathbb{C}$ ) and  $a_3 = 0$ . Indeed we see that  $a_0 = 0, a_1 = 1, a_2 = i, a_3 = 0$  satisfies all the above equations, so our example is given by  $x = i + Ij$ .

## Result

2 of 2

Such  $x$  is given by  $i + Ij$  where  $i$  is the quaternion  $i$  and  $I$  is the imaginary unit in  $\mathbb{C}$ . Click for more details.

## 38. a

Both directions are essentially consequences of (II), and the discussion that follows it, on page 132 and 133.

### Step 2

2 of 4

For suppose first that  $H(F)$  is a division ring but that we have  $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 0$  for some  $a_1, a_2, a_3, a_4 \in F$  with some  $a_n \neq 0$  for some  $n \in \{1, 2, 3, 4\}$ . Then by (II) we get that

$$(a_0 + a_1i + a_2j + a_3k)(a_0 - a_1i - a_2j - a_3k) = a_1^2 + a_2^2 + a_3^2 + a_4^2 = 0,$$

but note that since  $a_n \neq 0$  we have that both factors in our product are nonzero, and thus we obtain that  $H(F)$  has zero-divisors, which contradicts the assumption that it's a division ring.

### Step 3

3 of 4

For the converse note that the results follows directly from the discussion following (II), on page 133, for the only assumption made there in order to show that  $H(\mathbb{R})$  is a division ring is that it's a field and that for squares of four real numbers, of which at least one is not zero, is not zero, which is given as the hypotheses here, and thus  $H(F)$  is a division ring.

## Result

4 of 4

Both directions are more-or-less direct consequences of (II), and the discussion that follows it, on page 132 and 133. Click for more details.

## 39. a

By **Problem 38** it suffices to show if we have  $a_1, a_2, a_3, a_4 \in \mathbb{Q}$  such that  $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 0$  then  $a_1 = a_2 = a_3 = a_4 = 0$ .

Suppose we had

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = 0, \quad (1)$$

but that one of the  $a_i \neq 0$ , say  $a_1$ . Then as squares are always nonnegative and square of a nonzero number is nonzero we have that  $a_1^2 > 0$  and  $a_2^2 \geq 0, a_3^2 \geq 0, a_4^2 \geq 0$ , combining these we get that  $a_1^2 + a_2^2 + a_3^2 + a_4^2 > 0$ , contradicting (1).

## Result

2 of 2

We use **Problem 38** to reduce the question to showing that if we have  $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 0$  for rational  $a_i, i = 1, 2, 3, 4$ , then  $a_1 = a_2 = a_3 = a_4$ . Click for more details.

40. a

**To Prove:** A finite domain is a division ring.

**Proof:** Let  $R$  be a finite non-zero domain (Division ring cannot be trivial).

**Then  $R$  contains no divisor of zero.**

Let  $x \in R$  be an arbitrary non-zero element.

Since  $R$  is

**finite, there are only a finitely many distinct powers of  $x$**

Suppose that  $x^m = x^n$  for some  $m > n$ .

Then,  $0 = x^m - x^n = x^n(x^{m-n} - 1)$ . Since

**$R$  has no zero divisors, one of  $x^n$  and  $x^{m-n} - 1$  must be zero.**

If  $x^n = 0$ , then  $x$  is a zero divisor, which is a contradiction.

Therefore  $x^{m-n} - 1 = 0$  i.e.  $x^{m-n} = x \cdot x^{m-n-1} = 1$ . Therefore

**$x$  has an inverse,**

and since  $x$  is arbitrary, this holds for all non-zero  $x$  in  $R$ .

Thus, we conclude that

**$R$  is a non-zero finite domain such that every element of  $R$  has inverse.**

It follows that,  $R$  is a **division ring**.

This completes the proof.

41. a

**To Proof:**  $\mathbb{Z}_p$  is a field when  $p$  is a prime.

**Prove:**

The ring  $(\mathbb{Z}_p, +, \cdot)$  is clearly a

**commutative ring with unity, 1 being the unity.**

We now show that  $(\mathbb{Z}_p, +, \cdot)$  is a domain, where  $p$  is a prime.

Let  $\bar{m}$  be a non-zero element  $\mathbb{Z}_p$ .

Then  $0 < m < p$ .

Since  $p$  is a prime,  $\gcd(m, p) = 1$ .

Therefore

**there exist integers  $u$  and  $v$  such that  $um + vp = 1$ .**

Consequently,  $um \equiv 1 \pmod{p}$ . Clearly,  $u \not\equiv 0 \pmod{p}$ .

Let  $u \equiv r \pmod{p}$ , where  $0 < r < p$ .

Then we have,  $u \equiv r \pmod{p} \implies um \equiv rm \pmod{p} \implies 1 \equiv rm \pmod{p} \implies \bar{r}\bar{m} = 1$ .

**Since the ring is commutative,  $\bar{r}\bar{m} = \bar{m}\bar{r} = 1$**

This proves that  $\bar{m}$  is a **unit** and therefore

**$\bar{m}$  is not a divisor of zero.**

**Hence the ring contains no divisor of zero and therefore it is a domain.**

Now  $\mathbb{Z}_p$  is a finite commutative domain with unity  $\bar{1}$ .

We know that **a finite commutative domain is a field**, it follows that  $\mathbb{Z}_p$  is a field.

This completes the proof.

## Result

Click for proof.

# Section 4–2

1. a

Note that we have

$$na = \underbrace{a + \cdots + a}_{n \text{ times}},$$

and therefore

$$\begin{aligned}(na)(mb) &= (\underbrace{a + \cdots + a}_{n \text{ times}})(\underbrace{b + \cdots + b}_{m \text{ times}}) \\ &= \underbrace{ab + \cdots + ab}_{mn \text{ times}} = (mn)(ab),\end{aligned}$$

where the second equality follows from the distributive property.

## Result

We write out  $(a + \cdots + a)(b + \cdots + b)$  and use the distributive property. Click for more details.

## Method 2.

① Let  $R$  be a ring  
 $na = \underbrace{a + a + \cdots + a}_{n\text{-times}}$  for  $n \in \mathbb{Z}, a \in R$

claim:  $(na)(mb) = (nm)ab$ .

Proof:  
$$\begin{aligned}&(\underbrace{a + a + \cdots + a}_{n \text{ times}})(\underbrace{b + b + \cdots + b}_{m \text{ times}}) \\ &= \underbrace{ab + ab + \cdots + ab}_{nm \text{ -times}} \quad (\text{using distributive property}) \\ &= (nm)(ab).\end{aligned}$$

## 2. a

We have that if  $ab = ac$  then  $ab - ac = 0$ , and so

$$a(b - c) = 0.$$

As  $R$  is an integral domain then we must have that either  $a = 0$  or  $b - c = 0$ , but as our hypothesis is that  $a \neq 0$  we have that  $b - c = 0$ , i.e.  $b = c$ .

## Result

2 of 2

We transform the equality into (the equivalent)  $a(b - c) = 0$  and use the fact that  $R$  is an integral domain. Click for more details.

## Method 2.

② R is an integral domain.  
 Let  $ab = ac$  for  $a \neq 0$  &  $b, c \in R$ .  
 $\Rightarrow ab - ac = 0$   
 $\Rightarrow a(b - c) = 0$   
 Since  $a \neq 0$  & R does not have a zero divisor  
 $b - c = 0$   
 $\Rightarrow b = c$ .

### 3. a

If R is an integral domain, all that we have to show to demonstrate that it is a field is that every of its nonzero elements is invertible.

So let  $a \in R$ ,  $a \neq 0$ , and define the map  $\phi : R \rightarrow R$  by  $\phi(r) = ar$ . It follows directly from **Problem 2** that this map is injective. However, since  $\phi$  is an injective map from a finite set to itself, it follows that it must also be surjective, i.e. a bijection. This means that  $\phi^{-1}(1)$  exists, and this is exactly the inverse of  $a$ .

#### Result

2 of 2

We define a map  $\phi : R \rightarrow R$  by  $\phi(r) = ar$  for  $a \neq 0$  in R, and use the previous problem to show that it is a bijection, from where it directly follows that  $a$  is invertible.

### Method 2.

③ Let R be an integral domain. Let  $|R| = n$ .  
 Assume  $a \in R \setminus \{0\}$ , then a is not a zero divisor.  
 Since R is finite  $a^m = a^k$  for  $m > n$  & for some  $k < n$   
 $\Rightarrow a^k(a^{m-k} - 1) = 0$   
 $\Rightarrow a^{m-k} = 1$  since  $a^k \neq 0$ .  
 Hence  $a$  is a unit.  
 $\Rightarrow$  every non-zero element is a unit  $\Rightarrow R$  is a field.

### 4. a

**Given:**  $R$  is a ring with  $e \in R$  such that  $e^2 = e$ .

**To Prove:**  $(xe - exe)^2 = (ex - exe)^2 = 0$

### Step 2

**Proof:** We have  $e^2 = e$ .

Then,  $(xe - exe)^2$

$$= (xe - exe)(xe - exe)$$

$$= xexe - xeexe - exexe + exeeexe$$

$$= xexe - xeexe - exexe + exexe$$

$$= 0$$

Again,

$$(ex - exe)^2$$

$$= (ex - exe)(ex - exe)$$

$$= exex - exexe - exexex = exeeexe$$

$$= exex - exexe - exex + exexe$$

$$= 0$$

Consequently,

$$(xe - exe)^2 = (ex - exe)^2 = 0$$

### 5. a

It is given that  $x^3 = x$  for all  $x \in R$ . We have to show  $xy = yx$ , for all  $x, y \in R$ .

### Step 2

**Step-1:** Show that  $6x = 0$ , for all  $x \in R$ .

### Step 3

Let  $x$  be any two element in  $R$ . Then from given hypothesis we have

$$2x = (2x)^3 \implies 2x = 8x^3 \implies 2x = 8x \implies 6x = 0.$$

### Step 4

**Step-2:** Show that  $3(x + x^2) = 0$ , for all  $x \in R$ .

Notice that as  $x + x^2 \in R$ , thus by using hypothesis

$$x + x^2 = (x + x^2)^3 = x^3 + 3x^4 + 3x^5 + x^6 = x + 3x^2 + 3x + x^2 = 4(x + x^2)$$

Therefore, we get  $3(x + x^2) = 0$

### Step 6

**Step-3:** Show that  $3xy = 3yx$ , for all  $x, y \in R$ .

### Step 7

Let  $x, y \in R$ , then  $x + y \in R$ . Now from step-2, we have

$$\begin{aligned} & 3((x + y) + (x + y)^2) = 0 \\ \implies & 3(x + x^2 + x + xy + yx + y^2) = 0 \\ \implies & 3((x + x^2) + (y + y^2) + (xy + yx)) = 0 \\ \implies & 3(xy + yx) = 0 \quad [\text{Using step-2}] \\ \implies & 3xy + 3yx = 0 \end{aligned}$$

Now we know that  $xy \in R$ , therefore from step-1 we get  $6xy = 0$ . Thus we get

$$6xy - (3xy + 3yx) = 0 - 0 \implies 3xy = 3yx.$$

**Step-4:** Show that  $2xy = 2yx$ , for all  $x, y \in R$ .

Let  $x, y \in R$ . Then  $x + y \in R$  and so the given hypothesis yields that

$$0 = (x+y)^3 - (x+y) = (x^3 + x^2y + xyx + yx^2 + xy^2 + yxy + y^2x + y^3) - (x+y)$$

Therefore, using  $x^3 = x$  and  $y^3 = y$  we have

$$x^2y + yxy + yx^2 + xy^2 + yxy + y^2x = 0 \quad (4.2.1.1)$$

Similarly, we have  $x - y \in R$  and so the given hypothesis yields that

$$0 = (x-y)^3 - (x-y) = (x^3 - x^2y - xyx - yx^2 + xy^2 + yxy + y^2x - y^3) - (x-y)$$

Therefore, using  $x^3 = x$  and  $y^3 = y$  we have

$$-x^2y - yxy - yx^2 + xy^2 + yxy + y^2x = 0 \quad (4.2.1.2)$$

Now subtract equation (4.2.1.2) from equation (4.2.1.1) we have

$$2(x^2y + yxy + yx^2) = 0 \quad (4.2.1.3)$$

Multiply the equation (4.2.1.3) by  $x$  from left side we get

$$2(xy + x^2yx + yxy^2) = 0 \quad (4.2.1.4)$$

Multiply the equation (4.2.1.3) by  $x$  from right side we get

$$2(x^2yx + yxy^2 + yx) = 0 \quad (4.2.1.5)$$

Now subtract equation (4.2.1.5) from equation (4.2.1.4) we get

$$2xy - 2yx = 0 \implies 2xy = 2yx$$

**Step-5:** Show that  $xy = yx$ , for all  $x, y \in R$ .

### Step 11

Let  $x, y \in R$ . Then notice that  $xy = 3xy - 2xy$ . Thus using step-3 and step-4 we get

$$xy = 3xy - 2xy = 3yx - 2yx = yx$$

6. a

**Given:**  $R$  is a ring such that

$$a^2 = 0, \text{ for } a \in R.$$

**To Prove:** The element  $ax + xa$  commutes with  $a$  in  $R$ .

**Proof:** We need to show that

$$a(ax + xa) = (ax + xa)a \text{ for } a, x \in R.$$

Now,

$$\begin{aligned} a(ax + xa) &= a(ax) + a(xa) \\ &= a^2x + axa \\ &= 0 + axa = axa. \end{aligned}$$

Again,

$$\begin{aligned} (ax + xa)a &= (ax)a + (xa)a \\ &= axa + xa^2 \\ &= axa + 0 = axa. \end{aligned}$$

It follows that,

$$a(ax + xa) = (ax + xa)a, \text{ for } x, a \in R.$$

This shows that  $ax + xa$  commutes with  $a$ .

This completes the proof.

### Result

Being  $a^2 = 0$ , we have proved that  $a(ax + xa) = axa = (ax + xa)a$  for  $a, x \in R$ .

[Click for the complete proof.](#)

7. a

We can quickly see that  $R$  must be of characteristic 2, i.e. that  $2x = 0$ , because we have

$$-x = (-x)^4 = x^4 = x.$$

## Step 2

2 of 5

We also have  $(x^2 + x)^2 = x^4 + 2x^3 + x^2 = x^2 + x$ , so that  $x^2 + x$  has the property that it is equal to its square, i.e. it is idempotent. We now prove that an idempotent element commutes with all the elements of  $R$ .

First let us prove that if for  $x, y \in R$  we have  $xy = 0$ , then  $yx = 0$ . Note that

$$yx = (yx)^4 = y(xy)xyxyx = 0,$$

where we have used the associativity of the ring multiplication in the third equality.

Now if  $z$  is idempotent, i.e.  $z^2 = z$ , we have that  $zy - z^2y = 0$  or  $z(y - zy) = 0$ , so that by the previous paragraph  $(y - zy)z = 0$ , or

$$yz = zyz. \quad (1)$$

Likewise we have that  $yz^2 - yz = (yz - y)z = 0$ , so that  $z(yz - y) = 0$  or

$$zyz = zy. \quad (2)$$

Now combining (1) and (2) we have that  $yz = zy$ . As  $y$  was arbitrary, it follows that  $z$  commutes with every element of  $R$ .

Now we write  $x = x_1 + x_2$  for  $x_1$  and  $x_2$  arbitrary. Using what we just proved, we have that for any  $y \in R$ ,

$$y(x^2 + x) = (x^2 + x)y,$$

where substituting  $x = x_1 + x_2$  yields

$$\begin{aligned} y(x_1^2 + x_2^2 + x_1x_2 + x_2x_1 + x_1 + x_2) &= (x_1^2 + x_2^2 + x_1x_2 + x_2x_1 + x_1 + x_2)y \\ yx_1^2 + yx_2^2 + yx_1x_2 + yx_2x_1 + yx_1 + yx_2 &= x_1^2y + x_2^2y + x_1x_2y + x_2x_1y + x_1y + x_2y \\ y(x_1^2 + x_1) + y(x_2^2 + x_2) + yx_1x_2 + yx_2x_1 &= (x_1^2 + x_1)y + (x_2^2 + x_2)y + x_1x_2y + x_2x_1y \\ y(x_1x_2 + x_2x_1) &= (x_1x_2 + x_2x_1)y \end{aligned} \quad (3)$$

where the blue and red terms cancel out by the result from the previous section.

Now take  $y = x_1$  in (3), where we get

$$\begin{aligned} x_1(x_1x_2 + x_2x_1) &= (x_1x_2 + x_2x_1)x_1 \\ x_1^2x_2 + x_1x_2x_1 &= x_1x_2x_1 + x_2x_1^2 \\ x_1^2x_2 &= x_2x_1^2, \end{aligned}$$

so that  $x_1^2$  commutes with any  $x_2 \in R$ , where  $x_1$  was arbitrary as well.

Now note that we have obtained that both  $(x^2 + x)$  and  $x^2$  for any  $x \in R$  commute with all the elements of  $R$ , but then so do we have that for any  $y \in R$ ,

$$\begin{aligned} xy &= ((x^2 + x) - x^2)y \\ &= (x^2 + x)y - x^2y \\ &= y(x^2 + x) - yx^2 \\ &= y((x^2 + x) - x^2) = yx, \end{aligned}$$

which is what we needed to get.

We first prove that  $R$  must be of characteristic 2, then we prove and use the fact that idempotent elements commute with all the elements of  $R$ ; then it suffices to find two well-chosen forms of idempotents such that their difference is an arbitrary element of  $R$ . Click for the detailed proof.

## 8. a

**Given:**  $F$  is a finite field.

**To Prove:**

- a) There exists a prime element  $p$  such that  $pa = 0$  for all  $a \in F$ .
- b) If  $F$  has  $q$  elements, then  $q = p^n$  for some integer  $n$ .

**Proof:**

- a) Let us assume  $|F| = n$ , since  $F$  is finite.

Then by

Lagrange's theorem, we know that  $na = 0$  for all  $a \in F$ .

Let  $p$  be the

smallest positive integer such that  $p \cdot 1 = 0$ ,

where 1 is the multiplicative identity of  $F$ .

We will propose to prove that  $p$  is a prime.

If possible, let us assume that  $p$  is composite.

Then  $p = mn$  for some  $n, m > 1$ .

Then,

$$0 = p \cdot 1 = (nm) \cdot 1 = (n \cdot 1)(m \cdot 1)$$

Since every field is a domain, we thus know that either  $n \cdot 1 = 0$  or  $m \cdot 1 = 0$ .

But either leads to a contradiction since  $p$  is the smallest integer such that  $p \cdot 1 = 0$ .

Thus  $p$  is a prime.

Now notice that if  $p \cdot 1 = 0$ , then

$$\begin{aligned} pa &= p(a \cdot 1) = (p \cdot 1)a = 0 \cdot a = 0 \\ &\quad \text{for any } a \in F \end{aligned}$$

Therefore,

$$pa = 0 \text{ for all } a \in F$$

This completes the proof.

b) Let us assume that  $|F| = q$ .

Now, from the part (a) we know that

**$p$  divides  $q$  by Lagranges theorem.**

On the other hand, if any prime  $p' \neq p$  divides  $q$ , then

**by Cauchy's theorem for the additive group of  $F$ ,  $F$  contains an element  $x$  of order  $p'$ .**

Then

$$p'x = 0$$

But we also know that  $pa = 0$  for all  $a \in F$ , so  $px = 0$  and it follows that

**$p$  divides the order of  $x$**

i.e.  $p$  divides  $p'$ .

Which leads to a contradiction to the fact that  $p$  and  $p'$  are **distinct**.

This concludes that

**$p$  is the only prime that divides  $q$ .**

Then it's obvious that  $q = p^n$  for some  $n$ .

This completes the proof.

## 9. a

**Given:**  $\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{(p-1)} = \frac{a}{b}$ , where  $p$  is an odd prime and  $a, b$  are integers.

**To Prove:**  $p \mid a$  if  $p$  is an odd prime.

### Step 2

**Proof:**

First we proof for prime  $p = 3$  and then for all prime  $p > 3$ .

Let us take  $p = 3$ .

**Then the sum**

$$\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{(p-1)}$$

becomes

$$1 + \frac{1}{3-1} = 1 + \frac{1}{2} = \frac{3}{2}.$$

Therefore in this case  $\frac{a}{b} = \frac{3}{2}$  implies  $3 \mid a$  i.e.  $p \mid a$ .

Now for odd prime  $p > 3$ .

Let us consider  $f(x) = (x - 1)(x - 2) \dots (x - (p - 1))$ .

Now,

**by Fermat, we know that the coefficients of  $f(x)$  other than the  $x^{p-1}$  and  $x^0$  are divisible by  $p$ .**

So if,

$$f(x) = x^{p-1} + \sum_{i=0}^{p-2} a_i x^i$$

and  $p > 3$ .

Then  $p \mid a_2$ , and

$$f(p) \equiv a_1 p + a_0 \pmod{p^3}$$

But we see that

$$f(x) = (-1)^{p-1} f(p-x) \text{ for any } x,$$

so

**If  $p$  is odd**

$$f(p) = f(0) = a_0,$$

So it follows that:

$$0 = f(p) - a_0 \equiv a_1 p \pmod{p^3}$$

Therefore,

$$0 \equiv a_1 \pmod{p^2}.$$

Hence,

$$0 \equiv a_1 \pmod{p}.$$

Now **our sum is just**  $\frac{a_1}{(p-1)!} = \frac{a}{b}$ .

It follows that  $p$

**divides  $a$ .**

This completes the proof.

## 10. a

**Given:**  $\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{(p-1)} = \frac{a}{b}$ , where  $p$  is an odd prime and  $a, b$  are integers.

**To Prove:**  $p^2 \mid a$  if  $p > 3$ .

Let us consider  $f(x) = (x - 1)(x - 2) \dots (x - (p - 1))$ .

Now,

by Fermat, we know that the coefficients of  $f(x)$  other than the  $x^{p-1}$  and  $x^0$  are divisible by  $p$ .

So if,

$$f(x) = x^{p-1} + \sum_{i=0}^{p-2} a_i x^i$$

and  $p > 3$ .

Then  $p \mid a_2$ , and

$$f(p) \equiv a_1 p + a_0 \pmod{p^3}$$

But we see that

$$f(x) = (-1)^{p-1} f(p-x) \text{ for any } x,$$

so

If  $p$  is odd

$$f(p) = f(0) = a_0,$$

So it follows that:

$$0 = f(p) - a_0 \equiv a_1 p \pmod{p^3}$$

Therefore,

$$0 \equiv a_1 \pmod{p^2}.$$

Now our sum is just  $\frac{a_1}{(p-1)!} = \frac{a}{b}$ .

It follows that  $p^2$

divides  $a$ .

This completes the proof.

## Section 4–3

1. a

We need to prove

1. that  $L(a)$  is an additive subgroup of  $R$ ,
2. that given  $r \in R$  and  $b \in L(a)$ , then  $rb \in I$  and  $br \in I$ .

## Step 2

2 of 4

First, in order to prove (1), note that if  $x \in L(a)$  and  $y \in L(a)$  then  $xa = 0$  and  $ya = 0$ , so that

$$\begin{aligned}xa - ya &= 0 \\(x - y)a &= 0,\end{aligned}$$

i.e.  $L(a)$  is an additive subgroup of  $R$ . (We have used the criterion that  $H$  is a subgroup of  $G$  if for any  $h_1, h_2 \in H$  we have that  $h_1 h_2^{-1} \in H$ ; this is the result of **Problem 15** from **Subgroups** section of chapter 2.)

Now we prove (2). Let  $r \in R$  and  $b \in L(a)$ , then  $ba = 0$ , and so  $xba = 0$  which by associativity of multiplication in  $R$  is equivalent to

$$(xb)a = 0, \quad (1)$$

so that  $xb \in L(a)$ . Since  $R$  is commutative, (1) implies that  $(bx)a = 0$ , so that  $bx \in L(a)$ , which concludes the proof that  $L(a)$  is an ideal.

## Result

4 of 4

We check that  $L(a)$  satisfies the definition of an ideal. Click for the detailed proof.

## 2. a

Note that since  $R$  is a commutative ring with 1, then in order to prove that is a field it is sufficient to prove that every of its nonzero elements is invertible.

## Step 2

2 of 3

Let  $a \neq 0$  be an element of  $R$ , then we have that the ideal generated by  $a$ ,  $(a) = \{xa : x \in R\}$  (see **Example 9** for a proof that this is an ideal), is equal to  $R$ . But then  $1 \in (a)$ , so that there exists  $x \in R$  such that  $xa = 1$ ; this means that  $a$  is invertible, which finishes our proof.

## Result

3 of 3

We use the fact that for a nonzero  $a$ ,  $(a) = R$ , from which it follows that  $a$  is invertible. Click for the detailed proof.

## 3. a

Since  $\varphi$  is onto, let  $r' \in R'$  be arbitrary, then there exists  $r \in R$  such that  $\varphi(r) = r'$ .

Then we have that

$$\begin{aligned} r' &= \varphi(r) \\ &= \varphi(1 \cdot r) \\ &= \varphi(1)\varphi(r) \\ &= \varphi(1)r' \end{aligned}$$

and similarly  $r' = r'\varphi(1)$ , proving that  $\varphi(1)$  is the multiplicative identity in  $R'$ .

## Result

2 of 4

We use the fact that  $\varphi$  is onto to write  $\varphi(r) = r'$  for an arbitrary  $r' \in R'$ , and then use the fact that  $\varphi$  is homomorphism and that  $r \cdot 1 = 1 \cdot r$  to finish the proof. Click for more details.

## Method 2.

②-  $\varphi: R \rightarrow R'$  is a homomorphism of  $R$  onto  $R'$ .  
 $1 \in R$ . then claim:  $\varphi(1)$  is unit element in  $R'$ .  
let  $r' \in R'$  then  $\exists r \in R$  st  
 $\varphi(r) = r'$ .  
 $r' \cdot \varphi(1) = \varphi(r) \cdot \varphi(1) = \varphi(r \cdot 1)$   
 $= \varphi(r) = r'$ .  
similarly,  $r' \cdot \varphi(1) = \varphi(1) \cdot r' = r'$ .  
hence  $\varphi(1)$  is unit element in  $R'$ .

## 4. a

We have to prove

1. that  $I + J$  is an additive subgroup of  $R$ , and
2. that for any  $r \in R$  and  $k \in I + J$  we have that  $rk \in I + J$  and  $kr \in I + J$ .

## Step 2

2 of 4

First, in order to prove (1), note that since  $I$  and  $J$  are nonempty, then so is  $I + J$ . Now let  $k_1, k_2 \in I + J$  where  $k_1 = i_1 + j_1$  and  $k_2 = i_2 + j_2$  for  $i_1, i_2 \in I$  and  $j_1, j_2 \in J$ . Now note that since  $I$  is an ideal, so that if  $i \in I$  then  $(-1)i = -i \in I$ , and similarly for  $J$ .

Then we have that

$$k_1 - k_2 = (i_1 + j_1) - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J$$

where we have used the criterion that  $H$  is a subgroup of  $G$  is for any  $h_1, h_2 \in H$  we have that  $h_1 h_2^{-1} \in H$ ; this is the result of **Problem 15** from **Subgroups** section of chapter 2.

To prove the (2), let  $k = i + j \in I + J$ . Then  $rk = ri + rj$  where since  $I, J$  are ideals we have that  $ri \in I$  and  $rj \in J$ , so that  $rk \in I + J$ , and similarly  $kr \in I + J$ , finishing our proof.

### Result

4 of 4

We prove that  $I + J$  satisfies the definition of an ideal. Click for the detailed proof.

### Method 2.

(4) since  $I, J$  are ideals.  
 $0 \in I \text{ & } 0 \in J \Rightarrow 0 \in I + J \Rightarrow I + J \neq \emptyset$

let  $i_1 + j_1, i_2 + j_2 \in I + J$ .  
 $\Rightarrow (i_1 + j_1) - (i_2 + j_2) = (i_1 - i_2) + (j_1 - j_2) \in I + J$ .

further let  $r \in R$ ,  
 $r(i_1 + j_1) = (r \cdot i_1) + (r \cdot j_1) \in I + J$ .

hence  $I + J$  is an ideal in  $R$ .

5. a

Since  $A$  is a subring of  $R$  it contains 0, and since  $I$  contains 0 too, we have that  $0 \in I \cap A$ , i.e.  $I \cap A$  is nonempty.

### Step 2

2 of 4

Let  $x \in I \cap A$  and  $y \in I \cap A$ , then  $-y \in I \cap A$  since  $I$  is an ideal and  $A$  is a subring, and so

$$x - y \in I \cap A$$

because both  $I$  and  $A$  are additive subgroups of  $R$ .

### Step 3

3 of 4

Let  $x \in I \cap A$  and  $y \in I \cap A$ , then  $-y \in I \cap A$  since  $I$  is an ideal and  $A$  is a subring, and so

$$x - y \in I \cap A$$

because both  $I$  and  $A$  are additive subgroups of  $R$ .

### Result

4 of 4

We use the fact that both  $I$  and  $A$  are closed under addition and that both are also closed under multiplication by elements of  $A$ . Click for the detailed proof.

### Method 2.

⑤ let  $I$  is an ideal of  $R$ ,  $A$  subring in  $R$ .  
 $0 \in I \cap A \Rightarrow I \cap A \neq \emptyset$ .

let  $x, y \in I \cap A$ .  
 $\Rightarrow x, y \in I \text{ & } x, y \in A \Rightarrow x-y \in I \cap A$   
 $\Rightarrow x-y \in I \text{ & } x-y \in A \Rightarrow x-y \in I \cap A$

let  $a \in A$ ,  $x \in I \cap A$  (since  $I$  is an ideal)  
 $\Rightarrow ax \in I \text{ & } ax \in A$  (&  $A$  is subring)  
 $\Rightarrow ax \in I \cap A$   
 $\Rightarrow I \cap A$  is an ideal in  $A$ .

## 6. a

**Given:**  $R$  is a ring and  $I, J$  are two ideals of  $R$ .

**To Prove:**  $I \cap J$  is an ideal of  $R$ .

**Proof:** Since  $I$  and  $J$  are ideal, then  $0 \in I$  and  $0 \in J$ .

Therefore,  $0 \in I \cap J$ . This shows that the set  $I \cap J$  is non-empty.

Let  $a, b \in I \cap J$ .

Then

$$a, b \in I \text{ and } a, b \in J.$$

Since  $I$  is an ideal of  $R$ ,

$$a, b \in I \implies a - b \in I$$

and

$$a \in I, r \in R \implies ra \in I \text{ and also } ar \in I.$$

Since  $J$  is an ideal of  $R$ ,

$$a, b \in J \implies a - b \in J$$

and

$$a \in J, r \in R \implies ra \in J \text{ and also } ar \in J.$$

It follows that

$$a, b \in I \cap J \implies a - b \in I \cap J$$

and

$$a \in I \cap J, r \in R \implies ar \in I \cap J \text{ and also } ra \in I \cap J.$$

Therefore,  $I \cap J$  is an ideal of  $R$ .

This completes the proof.

Considering  $a, b$  in  $I \cap J$  and  $r \in R$  we have shown that  $a - b \in I \cap J$  and  $ra$  and  $ar$  both belongs to  $I \cap J$ , follows that  $I \cap J$  is an ideal of  $R$ .  
Click for the complete proof.

## Method 2.

⑥.  $I, J$  are ideals in  $R$ .

$o \in I \cap J \Rightarrow I \cap J \neq \emptyset$ .

let  $x, y \in I \cap J \Rightarrow x, y \in I \text{ & } x, y \in J$   
 $\Rightarrow x-y \in I \text{ & } x-y \in J$   
 $\Rightarrow x-y \in I \cap J$ .

let  $r \in R$  and  $x \in I \cap J$ .  
 $\Rightarrow rx \in I \text{ & } rx \in J$ .  
 $\Rightarrow rx \in I \cap J$ .

Hence,  $I \cap J$  is an ideal in  $R$ .

7. a

Let  $R$  be a ring and  $K$  an ideal of  $R$ .

### Step 2

2 of 5

First we prove that the quotient group  $R/K$ , where  $R$  and  $K$  are seen as their additive groups, is a ring with the multiplication defined by  $(a+K)(b+K) = ab+K$ . It was already shown in the text that this multiplication is well-defined. But note that since the product is well-defined, associativity of multiplication follows from the associativity in  $R$ ; and so does the distributivity if we note that  $(a+K)+(b+K) = (a+b)+K$ . Thus  $R/K$  is a ring.

### Step 3

3 of 5

Now let us show that  $\varphi : R \rightarrow R/K$ , defined by  $\varphi(a) = a+K$ , is a homomorphism, and that it is onto with also having  $K$  as its kernel.

The fact that it is onto follows from the fact that -- by the definition of a quotient group -- any  $l \in R/K$  can be written as  $l' + K$  for some  $l' \in R$ , so that  $\varphi(l') = l$ . The homomorphicity of  $\varphi$  follows quickly the facts that  $(a+K)+(b+K) = (a+b)+K$  and that  $(a+K)(b+K) = ab+K$ , since these imply  $\varphi(a+b) = \varphi(a) + \varphi(b)$  and  $\varphi(ab) = \varphi(a)\varphi(b)$ .

In order to show that  $K$  is its kernel, let  $k \in K$ , then  $\varphi(k) = k + K = K = 0 + K$ , so that  $k \in \ker \varphi$ . If  $r \notin K$ , then we have that  $r + K \neq K$ , so that  $\varphi(r) \neq 0 + K$ , showing that  $r$  is not in  $\ker \varphi$ , proving that  $\ker \varphi = K$ .

## Result

5 of 5

We put finishing touches on the proof outlined in the text. Click for more details.

### 8. a

First we prove that  $I$  is an ideal of  $R$ . Since  $\varphi$  is onto we have that  $I$  is nonempty. Let  $i_1 \in I$  and  $i_2 \in I$ , then by the definition of  $I$  this means that  $\varphi(i_1) \in I'$  and  $\varphi(i_2) \in I'$ . Now as  $I'$  is an ideal we have that  $\varphi(i_1) - \varphi(i_2) \in I'$ , but since  $\varphi$  is a homomorphism then  $\varphi(i_1) - \varphi(i_2) = \varphi(i_1 - i_2)$  from which it follows that  $i_1 - i_2 \in I$ .

Similarly, let  $i \in I$ , so that  $\varphi(i) \in I'$ , and let  $r \in R$ , then we have that  $\varphi(r)i = r\varphi(i) = \varphi(r)\varphi(i)$ , which is again in  $I'$  because  $I'$  is an ideal, and so  $ri \in I$ . Analogously we get that for  $ir \in I$ , so that  $I$  is an ideal.

## Step 2

2 of 5

Let  $k \in K$ , then  $\varphi(k) = 0$ . But  $\varphi(k) = 0 \in I'$ , because 0 is always in an ideal, so that  $k \in I$ , i.e.  $K \subset I$ .

## Step 3

3 of 5

Now let  $\tau : I \rightarrow I'$  be defined as  $\tau(i) = \varphi(i)$ . By the definition of  $I'$  this is well-defined, i.e. the image of  $\tau$  is indeed in  $I'$ , and it is obviously onto. To show the desired isomorphism,  $I/K \cong I'$ , we have to check that  $\ker \tau = K$ , and then the isomorphism follows from the first homomorphism theorem (whether we think of ideals as additive groups or as rings without a unit). If  $k \in K = \ker \varphi$ , then  $\tau(k) = \varphi(k) = 0$ , so that  $k \in \ker \tau$ , i.e.  $K \subseteq \ker \tau$ . Now if  $t \in \ker \tau$  then  $\tau(t) = 0$  so that  $\varphi(t) = 0$  which means that  $t \in \ker \varphi = K$ , i.e.  $\ker \tau \subseteq K$ , which proves that  $\ker \tau = K$ .

To explain the last sentence, note that the correspondence is given by  $I' \mapsto I$ . To prove that it is  $1 - 1$  we have to show that distinct ideals of  $R'$  map to distinct ideals of  $R$ , so let  $I'$  and  $J'$  be distinct ideals of  $R'$  which map to  $I, J$  respectively, and let  $\ell$  be an element which is in one of  $I'$  or  $J'$  and not in the other, say it is in  $I'$ , then there exists  $r \in R$  such that  $\varphi(r) = \ell$ , i.e.  $r \in I$ , but since  $\ell \notin J'$  then  $r \notin J'$ , i.e.  $I$  and  $J$  are distinct.

## Result

5 of 5

We first proceed straightforwardly from the definition of  $I$  to prove that it is ideal, and that  $K \subseteq I$ . We prove that isomorphism  $I/K \cong I'$  by showing that a particular homomorphism between  $I$  and  $I'$  has kernel  $K$ , and lastly we note that the  $1 - 1$  correspondence, which we prove to be such, is given by  $I' \mapsto I$ . Click for more details.

### 9. a

**(a)**

In order to show that  $A$  is a ring we have to show that it is nonempty and that given  $a, b \in A$  we have that  $ab \in A$  and  $a \pm b \in A$ . First, nonemptiness of  $A$  follows from  $\varphi$  being onto.

Now let  $a, b \in A$ , then by the definition of  $A$  this means that  $\varphi(a) \in A'$  and  $\varphi(b) \in A'$ . But now since  $\varphi$  is a homomorphism, and so it preserves addition and multiplication, and  $A'$  is by the hypothesis ring, then it quickly follows that  $ab \in A$  and  $a \pm b \in A$ , e.g.  $ab \in A$  because

$$\begin{aligned}\varphi(a)\varphi(b) &\in A', \text{ (because } A' \text{ is a ring)} \\ \varphi(ab) &\in A' \text{ (because } \varphi \text{ is a homomorphism).}\end{aligned}$$

Furthermore if  $k \in K$  then  $\varphi(k) = 0 \in A'$ , where  $0' \in A'$  because  $A'$  is a ring, so that  $k \in A$ , i.e.  $K \subset A$ .

**Step 2**

2 of 4

**(b)**

We define a homomorphism  $\tau : A \rightarrow A'$  by  $\tau(a) = \varphi(a)$ . By the definition of  $A$  we have that  $\tau(a) = \varphi(a) \in A'$  for all  $a \in A$  and that  $\tau$  is onto. If we prove that  $K = \ker \tau$  then our desired result follows from the first homomorphism theorem for rings. If  $k \in K$ , then  $\tau(k) = \varphi(k) = 0$ , so that  $K \in \ker \tau$ , while if  $t \in \ker \tau$  then  $\tau(t) = 0 = \varphi(t)$  so that  $t \in \ker \varphi = K$ , showing that  $K = \ker \tau$ .

**(c)**

Suppose  $A'$  is a left ideal of  $R'$ , we have to prove that given  $a, b \in A$  and  $r \in R$  we have that  $a - b \in A$  and  $ra \in A$ . Note that  $a - b \in A$  follows from the **(a)** part, so let us prove that  $ra \in A$ . We have that  $\varphi(r) \in R'$ , so that  $\varphi(r)\varphi(a) \in A'$  because  $A'$  is a left ideal, but then since  $\varphi$  is a homomorphism  $\varphi(ra) \in A'$ , i.e.  $ra \in A$ .

**Result**

4 of 4

We use the definition of  $A$  and the other hypotheses to show that  $A$  is a ring. We then use the first homomorphism theorem for rings to do the **(b)** part, and **(c)** part again follows easily from using the hypotheses that  $A'$  is a ring/left ideal and  $\varphi$  a homomorphism. Click for more details.

10. a

First note that the equivalence between the two statements is given by the first homomorphism theorem (**Problem 4.3.3**) and correspondence theorem (**Theorem 4.3.4**, proven in **Problem 8**), for they show that  $R/K \cong R'$  and  $I/K \cong I'$ .

## Step 2

2 of 4

We shall now prove the latter statement. We define a function  $\varphi : R/K \rightarrow R/I$  by  $\varphi(r+K) = r+I$ . We have that  $\varphi$  is well defined because if  $r+K = r'+K$ , then  $r-r' \in K$ , and since by hypotheses  $K \subseteq I$ , then also  $r-r' \in I$ , so that  $\varphi(r+K) = \varphi(r'+K)$ .

Furthermore, note that  $\varphi$  is onto because for any  $r \in R$ ,  $r+I$  is mapped to by  $r+K$ , i.e.  $\varphi(r+K) = (r+I)$ .

## Step 3

3 of 4

Now by the first homomorphism theorem for rings we have that

$$(R/K)/\ker \varphi \cong R/I,$$

so we are done if  $\ker \varphi = I/K$ . Note that  $r+K \in \ker \varphi$  iff  $r+I = 0+I$ , i.e. iff  $r \in I$ , so that the  $\ker \varphi = I/K$ , which is what we needed.

## Result

4 of 4

We prove the equivalence between two statements and then show the latter using the first homomorphism theorem for rings. Click for more details.

## 11. a

Note that  $R/I$  is composed of equivalence classes  $\frac{a}{b} + I = I$  where  $\gcd(a, b) = 1$  and  $a$  is even, and  $\frac{c}{d} + I$  where  $\gcd(c, d) = 1$  and  $c$  is odd.

Thus by the considerations in the discussion of **Example 3**, an explicit isomorphism is given by

$$\tau\left(\frac{a}{b} + I\right) = \begin{cases} 0 & \text{if } a \text{ is even,} \\ 1 & \text{if } a \text{ is odd.} \end{cases}$$

## Result

2 of 2

We adapt the homomorphism given in the **Example 3** into an isomorphism. Click for more details.

## 12. a

Let  $\frac{a}{b} \in R$  with  $\gcd(b, p) = 1$ , then we define a function  $\varphi : R \rightarrow \mathbb{Z}_p$  by

$$\varphi\left(\frac{a}{b}\right) = (a \bmod p) \cdot (b \bmod p)^{-1}$$

where  $a \bmod p$  denote the remainder of  $a$  divided by  $p$  and  $(b \bmod p)^{-1}$  denotes the inverse of  $b \bmod p$ , so that the right-hand side product is in  $\mathbb{Z}_p$ ; note also that this product is well defined since if  $\frac{a}{b}$  is not reduced the common factor must still be relatively prime with  $p$  so it 'cancels out'.

We want to show that  $\varphi$  is a homomorphism; for simplicity we denote  $x \bmod p$  as  $\bar{x}$ .

Now let  $\frac{a}{b} \in R$  and  $\frac{c}{d} \in R$ , then

$$\begin{aligned}\varphi\left(\frac{a}{b} + \frac{c}{d}\right) &= \varphi\left(\frac{ad + cb}{bd}\right) \\ &= (\overline{ad + bc})(\overline{bd})^{-1} \\ &= (\overline{ad} + \overline{bc})(\overline{b}^{-1}\overline{d}^{-1}) \\ &= \overline{ab}^{-1} + \overline{cd}^{-1} \\ &= \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right),\end{aligned}$$

where we freely used various properties of arithmetic in  $\mathbb{Z}_p$ .

$$\begin{aligned}\varphi\left(\frac{a}{b} \frac{c}{d}\right) &= \varphi\left(\frac{ac}{bd}\right) \\ &= (\overline{ac})(\overline{bd})^{-1} \\ &= (\overline{ab}^{-1})(\overline{cd}^{-1}) \\ &= \varphi\left(\frac{a}{b}\right)\varphi\left(\frac{c}{d}\right).\end{aligned}$$

Since the mapping is obviously onto, our desired result would now follow from the first homomorphism theorem for rings if  $\ker \varphi = I$ . Note that this is equivalent with  $(a \bmod p) \cdot (b \bmod p)^{-1} = 0 \bmod p$ , but since  $(b \bmod p)^{-1}$  is invertible this is again equivalent with  $a \bmod p = 0 \bmod p$ , which is exactly what we needed to get.

## Result

4 of 4

We define a mapping from  $R$  to  $\mathbb{Z}_p$  by  $\varphi\left(\frac{a}{b}\right) = (a \bmod p) \cdot (b \bmod p)^{-1}$  and show that it is homomorphism with kernel  $I$ . The result then follows from the first homomorphism theorem. Click for the detailed proof.

13. a

We define a map  $\varphi$  from  $R$  to  $H(\mathbb{Z}_p)$  by

$$\varphi(a_0 + a_1i + a_2j + a_3k) = (a_0 \bmod p) + (a_1 \bmod p)i + (a_2 \bmod p)j + (a_3 \bmod p)k.$$

This map is obviously onto and its kernel is  $I_p$ , since  $\varphi(a_0 + a_1i + a_2j + a_3k) = 0 = 0 + 0i + 0j + 0k$  is equivalent with  $a_i \bmod p = 0$ , for all  $i = 0, 1, 2, 3$ .

2 of 3

## Step 2

Now, by the first homomorphism theorem for rings, if we prove that  $\varphi$  is a homomorphism we are done. But note that as, if we have

$$(a_0 + a_1i + a_2j + a_3k) + (b_0 + b_1i + b_2j + b_3k) = (c_0 + c_1i + c_2j + c_3k)$$

or

$$(a_0 + a_1i + a_2j + a_3k)(b_0 + b_1i + b_2j + b_3k) = (d_0 + d_1i + d_2j + d_3k)$$

then  $c_i$  and  $d_i$ , for  $i = 0, 1, 2, 3$ , are by the definition of addition and multiplication just formed by multiplying and adding  $a_i$ s and  $b_i$ s for  $i = 0, 1, 2, 3$ , but then the homomorphicity of  $\varphi$  follows from the fact that

$$(x + y) \bmod p = (x \bmod p) + (y \bmod p)$$

and

$$(xy) \bmod p = (x \bmod p)(y \bmod p),$$

where the right-hand expressions are again taken to be elements of  $\mathbb{Z}_p$  (i.e. a remainder  $\bmod p$  is again computed).

3 of 3

## Result

We note that

$$\varphi(a_0 + a_1i + a_2j + a_3k) = (a_0 \bmod p) + (a_1 \bmod p)i + (a_2 \bmod p)j + (a_3 \bmod p)k$$

defines an onto homomorphism from  $R$  to  $H(\mathbb{Z}_p)$  and use this to prove the isomorphism. Click for more details.

## 14. a

Note that it was proven in the **Problem 30** of the first section of this chapter that  $R$  is a field. We need to prove that  $\psi$  is 1-1 and onto, as well as that we have

$$\psi(x + y) = \psi(x) + \psi(y) \text{ and } \psi(xy) = \psi(x) + \psi(y).$$

2 of 4

## Step 2

The fact that  $\psi$  is 1-1 and onto follows directly from the definition, for it is obvious that for any choice of  $a + bi$ , i.e. a choice of real  $a$  and  $b$ ,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

is in  $R$ , so that

$$\psi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + bi$$

and  $\psi$  is onto. To show that it is 1 – 1 note that if if two matrices in  $R$  map to the same complex number then they must be the same, for we have that, for real  $a, b, c, d$ ,  $a + bi = c + di$  if and only if  $a = c$  and  $b = d$ .

Next we prove additive and multiplicative property of the homomorphism:

$$\begin{aligned}\psi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) &= \psi \left( \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \right) \\ &= a+c+(b+d)i = (a+bi)+(c+di) \\ &= \psi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) + \psi \left( \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right),\end{aligned}$$

and

$$\begin{aligned}\psi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) &= \psi \left( \begin{pmatrix} ac-bd & (ad+bc)i \\ -(ad+bc) & ac-bd \end{pmatrix} \right) \\ &= (ac-bd)+(ad+bc)i = (a+bi)(c+di) \\ &= \psi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) + \psi \left( \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right).\end{aligned}$$

## Result

4 of 4

We show that  $\psi$  is 1-1 and onto, as well that the additive and multiplicative property of the homomorphism hold.

[Click for more details.](#)

Method 2.

(14)  $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$

define  $\psi: R \rightarrow \mathbb{C}$ .

$$\begin{aligned}\psi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) &= a+bi. \\ \psi \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right\} &= (a+c)+(b+d)i \\ &= \psi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) + \psi \left( \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right). \\ \psi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) &= \psi \left( \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{pmatrix} \right) \\ &= ac-bd+i(ad+bc) \\ &= (a+bi)(c+di) \\ &= \psi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) \psi \left( \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right).\end{aligned}$$

$\psi$  is bijective by definition

Hence,  $\psi$  is an isomorphism  $\Rightarrow R \cong \mathbb{C}$ .

15. a

We can write  $IJ$  as

$$IJ = \left\{ \sum_{k=1}^n i_k j_k : n \text{ is a natural number and } i_k \text{ and } j_k \text{ are in } I \text{ and } J, \text{ respectively, for all } k \right\}. \quad (1)$$

First, we have that  $IJ$  is nonempty since  $0 \in I$  and  $0 \in J$ , so that  $0 \in IJ$ .

## Step 2

2 of 4

Let us now show that  $IJ$  is an additive subgroup, then let  $x, y \in IJ$ ,  $x = \sum_{k=1}^n i_k j_k$  and  $y = \sum_{t=1}^m \bar{i}_t \bar{j}_t$ , both written in the form given in (1).

It is sufficient to show that  $x - y \in IJ$ , but this is immediate as  $-y \in IJ$  because

$$-y = -\sum_{t=1}^m \bar{i}_t \bar{j}_t = \sum_{t=1}^m (-\bar{i}_t) \bar{j}_t$$

and  $-\bar{i}_t \in I$  because  $I$  is an ideal, so that  $x - y$  is indeed a sum of products of elements from  $I$  and  $J$ , since a sum of two sums is again a sum.

Now let  $r \in R$  and  $x = \sum_{k=1}^n i_k j_k$ , then

$$rx = \sum_{k=1}^n (ri_k) j_k$$

which is again a sum of products of elements of  $I$  and  $J$  because  $ri_k \in I$  since  $I$  is an ideal, showing that  $IJ$  is a left ideal. Completely analogous computations can be used to show that  $IJ$  is a right ideal, which finishes our proof.

## Result

4 of 4

In order to show that  $IJ$  is a subgroup we use the fact that sum of two sums is again a sum, while in order to show that it is ideal we use the fact that multiplication distributes over sums in rings. Click for the detailed proof.

## Method 2.

$$(15) . \quad IJ = \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}, a_i \in I \text{ & } b_i \in J \right\}.$$

$$o \in IJ \Rightarrow IJ \neq \emptyset.$$

$$\text{let } \sum_{i=1}^n a_i b_i, \sum_{j=1}^m a'_j b'_j \in IJ.$$

$$\text{then } \sum_{i=1}^n a_i b_i - \sum_{j=1}^m a'_j b'_j = \sum_{k=1}^{m+n} a_k b_k \\ \text{where } a_k = -a'_j, b_k = b'_j, \\ k = n+j, 1 \leq j \leq m$$

$$\text{so, } \sum_{k=1}^{m+n} a_k b_k \in IJ$$

also, if  $r \in R$ .

$$r \cdot \sum a_i b_i = \sum (r \cdot a_i) b_i \in IJ \quad \text{since } r \cdot a_i \in I \\ \text{for } a_i \in I.$$

Similarly  $(\sum a_i b_i) \cdot r \in IJ$ .

Hence,  $IJ$  is an ideal in  $R$ .

## 16. a

Let

$$I = \left\{ \begin{pmatrix} n & 0 \\ m & 0 \end{pmatrix} : n, m \text{ real numbers} \right\}$$

Then  $I$  is obviously an additive subgroup of the ring of  $2 \times 2$  matrices. To show that it is indeed a left ideal, we compute

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} n & 0 \\ m & 0 \end{pmatrix} = \begin{pmatrix} an + bm & 0 \\ cn + dm & 0 \end{pmatrix} \in I.$$

Similarly we see that

$$I' = \left\{ \begin{pmatrix} 0 & n \\ 0 & m \end{pmatrix} : n, m \text{ real numbers} \right\}$$

is also a left ideal.

Likewise it is completely analogous to verify that

$$J = \left\{ \begin{pmatrix} n & m \\ 0 & 0 \end{pmatrix} : n, m \text{ real numbers} \right\}$$

and

$$J' = \left\{ \begin{pmatrix} 0 & 0 \\ n & m \end{pmatrix} : n, m \text{ real numbers} \right\}$$

are right ideals in our ring.

## Result

Two left ideals are given by

$$I = \left\{ \begin{pmatrix} n & 0 \\ m & 0 \end{pmatrix} : n, m \text{ real numbers} \right\}$$

and

$$I' = \left\{ \begin{pmatrix} 0 & n \\ 0 & m \end{pmatrix} : n, m \text{ real numbers} \right\}.$$

[Click for more details.](#)

## 17. a

First we show that  $A + I$  is a subring of  $R$ . Let  $x, y \in A + I$  where  $x = a_1 + i_1$  and  $y = a_2 + i_2$  for  $a_1, a_2 \in A$  and  $i_1, i_2 \in I$ .

Now we have that

$$x \pm y = (a_1 \pm a_2) + (i_1 \pm i_2),$$

where  $a_1 \pm a_2 \in A$  because  $A$  is a ring and  $i_1 \pm i_2 \in I$  because  $I$  is an ideal. Also

$$xy = a_1a_2 + a_1i_2 + i_1a_2 + i_1i_2,$$

where  $a_1a_2 \in A$  because  $A$  is a ring and  $a_1i_2, i_1a_2, i_1i_2 \in I$  because  $I$  is an ideal; finishing our proof that  $A + I$  is a subring.

## Step 2

2 of 4

Next, in order to show that  $I$  is an ideal of  $A + I$ , note that  $I$  is nonempty because it is already an ideal of  $R$ , and that  $I \subset A + I$  since  $0 \in A$ . But now the fact we're trying to prove is immediate, since we can use the hypothesis that  $I$  is an ideal of  $R$  to conclude that it is an additive group, and that it is closed under multiplication by elements of  $A + I$  because it is closed under multiplication by elements of  $R$  and  $A + I \subset R$ .

Finally, we show the required isomorphism by defining a map  $\varphi : A \rightarrow (A + I)/I$  by

$$\varphi(a) = a + I.$$

As  $A \subset A + I$  we have that this is a well-defined mapping which can easily be shown to be a homomorphism. We also have that it is onto for if  $(a + i) + I$  is an arbitrary element of  $(A + I)/I$ , then

$$\varphi(a) = a + I = a + (i + I) = (a + i) + I.$$

If we now show that  $\ker \varphi = A \cap I$  we are done by the first homomorphism theorem for rings.

Suppose now that  $p \in \ker \varphi$ , then  $\varphi(p) = 0$ , i.e.  $p + I = 0 + I = I$ , so that  $p \in I$ , and thus  $p \in A \cap I$ .

Conversely, let  $q \in A \cap I$ , then  $q \in I$ , and so  $\varphi(q) = q + I = I = 0 + I$ , so that  $q \in \ker \varphi$ , finishing our proof.

## Result

4 of 4

$A + I$  being a subring of  $R$  follows straightforwardly from  $A$  being a ring and  $I$  being an ideal, as does the fact that  $I$  is an ideal of  $A + I$ . We prove the final claim by exhibiting an onto homomorphism from  $A$  to  $(A + I)/I$  with kernel  $A \cap I$ . Click for the detailed proof.

## 18. a

We verify all the ring axioms from the definition of a ring from page 126.

### Step 2

2 of 10

(a)

Immediate from the definition, since  $R$  and  $S$  are rings so a sum of two of their elements is again in them, ergo a sum of two elements of  $R \oplus S$  is again in  $R \oplus S$ .

### Step 3

3 of 10

(b)

Immediate from the commutativity of addition in  $R$  and  $S$ , since addition is performed coordinatewise -- so that the computations in the first element of the ordered pair always happen" in  $R$  and computations in the second element of the ordered pair always happen" in  $S$ . We will implicitly use this often throughout the proof.

(c)

Immediate from the associativity of addition in  $R$  and  $S$ ; again, just look at the first coordinate and the second coordinate separately.

### Step 5

5 of 10

(d)

We have that  $(0_R, 0_S) \in R \oplus S$ , where  $0_R$  is the additive identity in  $R$  and  $0_S$  is the additive identity in  $S$ . From this it follows that for any  $(r, s) \in R \oplus S$  we have that

$$(r, s) + (0_R, 0_S) = (r + 0_R, s + 0_S) = (r, s).$$

### Step 6

6 of 10

(e)

Let  $(r, s) \in R \oplus S$ , then  $-r \in R$  and  $-s \in S$ , so that  $(-r, -s) \in R \oplus S$ , where we have that

$$(r, s) + (-r, -s) = (r + (-r), s + (-s)) = (0_R, 0_S).$$

(f)

Immediate from the fact that  $R$  and  $S$  are closed under multiplication.

### Step 8

(g)

Immediate from the associativity of multiplication in  $R$  and  $S$ .

### Step 9

(g)

Immediate from the distributivity of multiplication over addition in both  $R$  and  $S$ .

### Result

We verify that all the ring axioms hold for  $R \oplus S$ . Click for more details.

19. a

**(a)**

$R$  is obviously closed under addition, its addition is commutative and associative because addition in  $R$  is commutative and associative, and the additive identity is in  $R$  for  $a = b = c = 0$ .

Furthermore,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix} \in R,$$

and multiplication in  $R$  is associative because multiplication of matrices is in general associative; the same holds for distributivity of multiplication over addition, finishing our proof that  $R$  is a ring.

**Step 2**

2 of 4

**(b)**

We see that  $I$  is an additive subgroup of  $R$  because

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b - c \\ 0 & 0 \end{pmatrix} \in R,$$

and that  $I$  is closed under left and right multiplication because

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & ad \\ 0 & 0 \end{pmatrix} \in I, \\ \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} &= \begin{pmatrix} 0 & cd \\ 0 & 0 \end{pmatrix} \in I. \end{aligned}$$

**(c)**

We define a map  $\varphi : R \rightarrow F \oplus F$  by

$$\varphi \left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) = (a, c)$$

and claim that it is a homomorphism. For we have that

$$\begin{aligned} \varphi \left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \right) &= \varphi \left( \begin{pmatrix} a+d & b+e \\ 0 & c+f \end{pmatrix} \right) \\ &= (a+d, c+f) \\ &= (a, c) + (d, f) \\ &= \varphi \left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) + \varphi \left( \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \right). \end{aligned}$$

Likewise

$$\begin{aligned} \varphi \left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \right) &= \varphi \left( \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix} \right) \\ &= (ad, cf) \\ &= (a, c)(d, f) \\ &= \varphi \left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) \varphi \left( \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \right). \end{aligned}$$

Since  $\varphi$  is also obviously onto, by the first homomorphism theorem our result follows if we prove that  $\ker \varphi = I$ .

Note that we have that

$$\varphi \left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) = (a, d) = (0, 0)$$

is equivalent with  $a = b = 0$ , and puts no restrictions on  $b$ . Thus, the kernel is exactly equal to  $I$ .

## Result

4 of 4

For **(a)** and **(b)** parts we directly check the definition of a ring/ideal, while for the **(c)** part we define a (what we show to be) homomorphism  $\varphi$  by

$$\varphi \left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) = (a, c)$$

and then use the first homomorphism theorem. Click for more details.

## 20. a

$\varphi$  is obviously a map from  $R$  to  $R_1 \oplus R_2$  since  $r + I \in R_1$  and  $i + J \in R_2$  by the definition of a quotient ring.

Now let  $r_1, r_2 \in R$ , then

$$\begin{aligned} \varphi(r_1 + r_2) &= ((r_1 + r_2) + I, (r_1 + r_2) + J) \\ &= ((r_1 + I) + (r_2 + I), (r_1 + J) + (r_2 + J)) \\ &= (r_1 + I, r_1 + J) + (r_2 + I, r_2 + J) \\ &= \varphi(r_1) + \varphi(r_2), \end{aligned}$$

and also

$$\begin{aligned} \varphi(r_1 r_2) &= (r_1 r_2 + I, r_1 r_2 + J) \\ &= ((r_1 + I)(r_2 + I), (r_1 + J)(r_2 + J)) \\ &= (r_1 + I, r_1 + J)(r_2 + I, r_2 + J) \\ &= \varphi(r_1) + \varphi(r_2), \end{aligned}$$

where the second equality follows from the definition of the coset multiplication in quotient rings (see discussion on page 141).

To compute the kernel of this homomorphism, note that  $\varphi(r) = (r + I, r + J) = (0 + I, 0 + J) = (0, 0)$  if and only if  $r + I = 0 + I$  and  $r + J = 0 + J$ , so that  $r - 0 = r \in I$  and  $r - 0 = r \in J$ , which is equivalent with  $r \in I \cap J$ .

## Result

3 of 3

We use the properties of addition and multiplication in quotient rings to show that  $\varphi$  is a homomorphism, and then find the kernel by considering the conditions on  $r$  which yield that  $\varphi(r) = (0 + I, 0 + J)$ . Click for more details.

## 21. a

Using the notation of **Problem 20** let  $R = \mathbb{Z}_{15}$ , and let  $I$  be the ideal generated by 5 (i.e. by  $[5]$ , but we drop the equivalence class notation for simplicity), and  $J$  the ideal generated by 3.

Then  $I = \{0, 5, 10\}$  and  $J = \{0, 3, 6, 9, 12\}$ . It is easy to see that  $I$  and  $J$  are indeed subrings of  $R$ , and that they are isomorphic to  $\mathbb{Z}_3$  and  $\mathbb{Z}_5$  respectively.

Now note that the homomorphism outlined in **Problem 20** is onto and that  $I \cap J = \emptyset$ , and so by application of **Problem 20** and the first homomorphism theorem for rings we get the isomorphism

$$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5.$$

## Result

2 of 2

We use **Problem 20** to get the isomorphism. Click for more details.

## Method 2.

② claim:  $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$ .

$(1, 1) \in \mathbb{Z}_3 \oplus \mathbb{Z}_5$  and  $|(1, 1)| = \gcd(3, 5) = 15$

i.e.  $\mathbb{Z}_{15} = \langle 1 \rangle$  and  $\mathbb{Z}_3 \oplus \mathbb{Z}_5 = \langle (1, 1) \rangle$ .

$\Rightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_5$  and  $\mathbb{Z}_{15}$  both are cyclic groups of order 15.

$\Rightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15}$  (isomorphism is given by map  $\phi$  s.t.  $\phi(1, 1) = 1$ )

22. a

(a)

We solve this in slightly greater generality, when  $m, n$  are arbitrary integers, and then specialize it to the case where  $m, n$  are relatively prime.

Since  $x \in I_m$  is equivalent with  $x$  being a multiple of  $m$ , then  $x \in I_m \cap I_n$  is equivalent with  $x$  being a multiple of  $m$  and  $x$  being a multiple of  $n$ , but note that this is equivalent with  $x$  being a multiple of the least common multiple of  $m$  and  $n$ . This can be seen by noting that the least common multiple of  $m = (-1)^{k_0} \prod p_i^{k_i}$  and  $n = (-1)^{l_0} \prod p_i^{l_i}$  (where we can think of the product as ranging over all primes, with only finitely many  $k_i$  and  $l_i$  nonzero), denoted by  $\text{lcm}(m, n)$ , is given by

$$\text{lcm}(m, n) = \prod p_i^{\max(k_i, l_i)}.$$

Now, any number divisible by both  $m$  and  $n$  (i.e. any multiple of both  $m$  and  $n$ ) is surely going to also be divisible by the  $p_i^{\max(k_i, l_i)}$  for all primes  $p_i$ , for this is just a consequence of the uniqueness of prime factorization. Likewise, if a number is divisible by  $p_i^{\max(k_i, l_i)}$  for all primes  $p_i$ , then it is divisible by both  $m$  and  $n$  and thus is a multiple of both of them. Thus,  $I_m \cap I_n = I_{\text{lcm}(m, n)}$ .

If  $m, n$  are relatively prime then  $\text{lcm}(m, n) = mn$  and  $I_m \cap I_n = I_{mn}$ .

**(b)**

Using the notation of **Problem 20** take  $R = \mathbb{Z}$ ,  $I = I_m$  and  $J = I_n$ . Then **Problem 20** yields a homomorphism  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$  with  $\ker \varphi = I_{mn}$ ; this induces a homomorphism  $\bar{\varphi} : \mathbb{Z}/I_{mn} \rightarrow \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$  by setting  $\bar{\varphi}(x + I_{mn}) = \varphi(x)$ . To show that this homomorphism is one-to-one, suppose that  $\bar{\varphi}(x + I_{mn}) = \bar{\varphi}(y + I_{mn})$ , but then  $\bar{\varphi}((x - y) + I_{mn}) = \varphi(x - y) = (0, 0)$ , but this implies that  $x - y \in I_m$  and  $x - y \in I_n$ , so that  $x - y \in I_{mn}$ , or equivalently  $(x - y) + I_{mn} = 0$ , i.e.  $x + I_{mn} = y + I_{mn}$ , proving that this homomorphism is one-to-one.

**Result**

3 of 3

In the **(a)** part we show that  $I_m \cap I_n = I_{mn}$ , while in **(b)** part we use the **Problem 20** with  $R = \mathbb{Z}$ ,  $I = I_m$  and  $J = I_n$  and together with the **(a)** part in order to produce the desired proof. Click for more details.

23. a

**To Prove:**  $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$ , where  $m$  and  $n$  are relatively prime

**Proof:**

Let us consider the map

$$f : \mathbb{Z} \rightarrow \mathbb{Z}_m \bigoplus \mathbb{Z}_n$$

by the assignment

$$f(a) = (a \bmod m, a \bmod n).$$

First

**we show that  $f$  is a homomorphism**

Let us consider the elements  $a, b \in \mathbb{Z}$ .

Then

$$f(a) = (a \bmod m, a \bmod n) \text{ and } f(b) = (b \bmod m, b \bmod n).$$

Now,

$$\begin{aligned} f(a+b) &= ((a+b) \bmod m, (a+b) \bmod n) \\ &= (a \bmod m, a \bmod n) + (b \bmod m, b \bmod n) \\ &= f(a) + f(b). \end{aligned}$$

Now,

$$f(ab) = (ab \bmod m, ab \bmod n)$$

We know that

$$ab \bmod m = (a \bmod m)(b \bmod m)$$

it follows that

$$f(ab) = (ab \bmod m, ab \bmod n) = (a \bmod m, a \bmod n)(b \bmod m, b \bmod n) = f(a)f(b).$$

**Consequently**, for all  $a, b \in \mathbb{Z}$  we have

$$f(a+b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b).$$

This shows that  $f$  is a **ring homomorphism**.

We now

**show that  $f$  is surjective**

Since  $m$  and  $n$  are **relatively prime, then there exist integers**  $u$  and  $v$  such that

$$mu + nv = 1.$$

Then we have

$$mu \equiv 1 \pmod{n} \text{ and } nv \equiv 1 \pmod{m}.$$

Let us consider the element  $(x, y) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$  and take  $xnv + ymu = a$ .

Then

$$\begin{aligned} f(a) &= f(xnv + ymu) \\ &= ((xnv + ymu) \bmod m, (xnv + ymu) \bmod n) \\ &= (x \bmod m, y \bmod n) \end{aligned}$$

since,

$$ymu \equiv y \pmod{n} \text{ and } xnv \equiv x \pmod{m}.$$

Therefore,  $f(a) = (x \bmod m, y \bmod n)$ .

Therefore,  $f$  is **surjective**

**Claim:**  $\text{Ker}(f) = mn\mathbb{Z}$

**Proof of the Claim:** Let  $a \in \text{Ker}(f)$ .

Then

$$f(a) = (0, 0), \text{ zero element in } \mathbb{Z}_m \bigoplus \mathbb{Z}_n.$$

This implies

$$(a \bmod m, a \bmod n) = (0, 0).$$

That is,

$$a \bmod m = 0 \text{ and } a \bmod n = 0.$$

This gives

$$a \equiv 0 \pmod{m} \text{ and } a \equiv 0 \pmod{n}$$

$$\implies a \equiv 0 \pmod{\text{lcm}(m, n)}.$$

Since,  $m$  and  $n$  are **relatively prime**,  $\text{lcm}(m, n) = mn$ .

This implies,

$$a \equiv 0 \pmod{mn}.$$

Thus,  $a \in mn\mathbb{Z}$ . Hence,  $\text{Ker}(f) \subset mn\mathbb{Z}$ .

**Conversely**, let  $x \in mn\mathbb{Z}$ .

Then

$$x \equiv 0 \pmod{mn} \implies x \equiv 0 \pmod{m} \text{ and } x \equiv 0 \pmod{n}$$

$$\implies x \in \text{Ker}(f).$$

Hence,

$$mn\mathbb{Z} \subset \text{Ker}(f).$$

Consequently,  $\text{Ker}(f) = mn\mathbb{Z}$ .

Hence, the Claim is done.

Now, we **observe that**

$$f : \mathbb{Z} \rightarrow \mathbb{Z}_m \bigoplus \mathbb{Z}_n$$

is a **surjective ring homomorphism with kernel  $mn\mathbb{Z}$** .

Then by **First Isomorphism Theorem** we have,

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}_m \bigoplus \mathbb{Z}_n$$

That is

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \bigoplus \mathbb{Z}_n.$$

This completes the proof.

## Result

6 of 6

Being the function  $f : \mathbb{Z} \rightarrow \mathbb{Z}_m \bigoplus \mathbb{Z}_n$  is a surjective homomorphism with Kernel  $mn\mathbb{Z}$ , by First Isomorphism Theorem we have proved that

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \bigoplus \mathbb{Z}_n.$$

Click for the detailed proof.

## 24. a

Note that the statement that  $x \equiv a \pmod{m}$  and  $x \equiv b \pmod{n}$  is equivalent with there being integers  $x$  such that  $(x \bmod m, x \bmod n) = (a, b) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$ . Now define a map  $f : \mathbb{Z} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$  by  $f(t) = (t \bmod m, t \bmod n)$ , which was shown in the proof **Problem 23** to be a surjective homomorphism. But note that this means that for any  $(a, b) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$ ,  $f^{-1}(a, b)$  is nonempty, and any  $x \in f^{-1}(a, b)$  satisfies our requirements.

### Result

2 of 2

In the course of proving **Problem 23** it was proven that the function  $f : \mathbb{Z} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$  defined by  $f(t) = (t \bmod m, t \bmod n)$  is a surjective homomorphism, which quickly provides us with the required  $x$ . Click for more details.

## 25. a

Suppose that  $I$  is a nontrivial ideal of  $R$ , and let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where not all of  $a, b, cd$  are zero. Suppose, without loss of generality -- our steps would be completely analogous, modulo some different placement of 1s in our matrices, if we assumed some other element to be nonzero -- that  $a \neq 0$ . Then we have that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in I$$

and so

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I$$

so that

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in I$$

for any real  $x$ . Now, also for any real  $x$ ,

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \in I.$$

Likewise

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} \in I$$

and

$$\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}.$$

Thus, as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}$$

and since all the terms on the right side are in  $I$  and  $I$  is an additive group, it follows that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for arbitrary  $a, b, c, d$  is in  $I$ , i.e.  $I = R$ .

Note that the intuition for picking these matrices is that, if we denote by  $E_{ij}$  the matrix with 1 at position  $(i, j)$  and 0 elsewhere, then

$$E_{ij} \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} E_{nm} = a_{j,n} E_{im}.$$

## Result

2 of 2

We suppose  $I$  contains some nonzero matrix and show that it contains all the  $2 \times 2$  matrices, i.e. the whole  $R$ .

### 26. a

Let  $I$  be an ideal of  $S$  and  $J'$  be the set of all  $R$  which appear as entries in matrices in  $I$ . We need to prove that  $J'$  is an ideal of  $R$ .

#### Step 2

2 of 5

Note, however, that it is sufficient to show that set  $J''$  of all entries in the first row and the first column (i.e. in position  $(1, 1)$ ) of matrices in  $I$  forms an ideal, for using the transformations analogous to those **Problem 25** we can show that this is equal to the whole  $J'$ ; this is possible because  $1 \in R$ .

For illustration, let  $d$  be an element of  $J'$  such that it appears in the second row and second column for some matrix in  $I$ , i.e.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S$$

for some  $a, b, c$ . But then

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix}$$

which is again in  $I$  because it is an ideal and thus closed under left and right multiplication -- see the end of the solution of **Problem 25** to see how we chose our matrices.

Now let  $a \in J''$  and let  $r \in R$ . Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in I$$

for some  $b, c, d$ , and then

$$\begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ra & rb \\ 0 & 0 \end{pmatrix},$$

so that  $ra \in J''$ , and similarly we get  $ar \in J''$  by commuting the elements in (1).

From this we get that since  $1 \in R$ , and thus  $-1 \in R$ ,  $-a \in J''$  for any  $a \in J'$ , so in order to show that  $J'$  is an additive subgroup of  $R$  and it is sufficient to show that if  $a_1 \in J'$  and  $a_2 \in J'$  then  $a_1 + a_2 \in J'$ . But note that  $a_1 \in J'$  and  $a_2 \in J'$  implies there exist  $b_1, b_2, c_1, c_2, d_1, d_2 \in J'$  such that

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in I$$

and

$$\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in I$$

. But since  $I$  is an ideal we have that

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} \in I,$$

so that  $a_1 + a_2 \in J''$ , finishing our proof.

## Result

5 of 5

We note that it is sufficient to show that all the entries in the first row and the first column forms an ideal in  $R$ , and then we show that. Click for more details.

## 27. a

Note that we can, via mathematical induction, extend the result of **Problem 23** to get

$$\mathbb{Z}_{p_1 \dots p_n} \cong \mathbb{Z}_{p_1} \oplus \dots \oplus \mathbb{Z}_{p_n}, \quad (1)$$

where arbitrary finite direct sums are defined analogously with direct sums. Now note that if we have that  $x^2 = x$  for  $x \in \mathbb{Z}_{p_1 \dots p_n}$  then we have, because the mapping given by  $k \mapsto (k \bmod p_1, \dots, k \bmod p_n)$  (where  $k$  is seen as an integer giving rise to equivalence class in  $\mathbb{Z}_{p_1 \dots p_n}$ ) gives the isomorphism in (1), corresponds to an element  $y \in \mathbb{Z}_{p_1} \oplus \dots \oplus \mathbb{Z}_{p_n}$  such that  $y^2 = y$ , and conversely, if  $y^2 = y$  for a  $y \in \mathbb{Z}_{p_1} \oplus \dots \oplus \mathbb{Z}_{p_n}$  then this gives us an element  $x \in \mathbb{Z}_{p_1 \dots p_n}$  with  $x^2 = x$ .

## Step 2

2 of 3

Now we count the number of solutions of  $y^2 = y$  in  $\mathbb{Z}_{p_1} \oplus \dots \oplus \mathbb{Z}_{p_n}$ . We have to have  $y^2 \equiv y \pmod{p_l}$  for all  $l = 1, \dots, n$ . Now note that for a fixed odd prime  $p$ , since  $y^2 \equiv y \pmod{p_l}$  is equivalent with  $y(y-1) \equiv 0 \pmod{p}$ , and there are no zero divisors in  $\mathbb{Z}_p$ , we infer that the two solutions are given by  $y = 0$  and  $y = 1$ . So we have two solutions for each of the primes  $p_l$ , and since we can choose these independently (by the definition of the direct sum), it follows that there are a total of  $2^n$  solutions.

We note that **Problem 23** can be generalized to  $\mathbb{Z}_{p_1 \dots p_n} \cong \mathbb{Z}_{p_1} \oplus \dots \oplus \mathbb{Z}_{p_n}$  and use this isomorphism to count the solutions. Click for more details.

## 28. a

**Given:** Let  $R$  be a ring such that the only left ideals of  $R$  are  $(0)$  and  $R$ .

**To Prove:** Either  $R$  is a division ring or  $R$  is a ring with a prime number of elements in which  $ab = 0$  for every  $a, b \in R$ .

### Proof:

We define

$$U = \{x \in R \mid rx = 0 \forall r \in R\}$$

and

we claim  $U$  is a left-ideal of  $R$

Clearly  $0 \in U$  as  $r.0 = 0 \forall r \in R$ .

Suppose

$$u_1, u_2 \in U,$$

therefore

$$ru_1 = 0 \quad \forall r \in R$$

and

$$ru_2 = 0 \quad \forall r \in R.$$

But

$$r(u_1 - u_2) = ru_1 - ru_2 = 0 - 0 = 0 \quad \forall r \in R,$$

therefore  $u_1 - u_2 \in U$ .

So

$$U$$

forms a subgroup of  $R$  under addition.

Also for  $u \in U$  and  $r \in R$ , we have

$$ru = 0 \in U.$$

So

$$ru \in U \quad \forall u \in U, r \in R.$$

Thus  $U$  is a right-ideal of  $R$ .

But

the only left-ideals of  $R$  are  $(0)$  and  $R$ , therefore, either  $U = (0)$  or  $U = R$ .

**Case 1:** When  $U = R$ ,

it means

$$ru = 0 \quad \forall u \in U, r \in R$$

that is,

$$ru = 0 \quad \forall u, r \in R.$$

Also

**multiplicative identity, 1 does not exist**

t as if it had existed  
would mean

$$1 \in U \implies 1R = \{0\} \implies R = \{0\} \implies 1 \notin R \text{ as } 1 \neq 0.$$

Also

**any subgroup of  $R$  under addition is a right-ideal as 0 belongs to all subgroup of  $R$  under addition**

Therefore  $\{0\}$  and  $R$  are the **only subgroup** of  $R$  under addition.

But that mean either  $R = \{0\}$  or

**order of  $R$  is a prime**

Thus in this case

either  $R = \{0\}$  or a ring with prime order, with **no multiplicative identity** and satisfying

$$r_1r_2 = 0 \quad \forall r_1, r_2 \in R.$$

Note when  $R = \{0\}$ , then it is trivially a division ring.

**Case 2 :** When  $U = (0)$ ,

it means

$$rx = 0 \quad \forall r \in R$$

only for  $x = 0$ .

In other

words, for  $a \neq 0$  we have  $ra \neq 0$  at least for some  $r \in R$ .

Now either  $R = (0)$   
or  $R \neq (0)$ .

Suppose  $R \neq (0)$ , **there exist some**  $a \in R$  with  $a \neq 0$ .

But

then  $Ra \neq (0)$ .

Also  $Ra$  is a **left-ideal**; and  $(0)$  and  $R$  are the **only possible left-ideals**, therefore,  $Ra = R$ .

We claim  $R$  to be a **division ring**.

To establish  
our claim, we need to show the

**existence of multiplicative right-Identity 1 and right-inverse of any any non-zero element**

, say  $a$ .

Suppose some  $x, y \in R$  such  
that  $xy = 0$  with  $x \neq 0$  and  $y \neq 0$ .  
We have  $Rx = R$  and  $Ry = R$  as  $x \neq 0$  and  
 $y \neq 0$ .  
But then

$$R(xy) = (Rx)y = (R)y = R.$$

So

$$xy = 0 \implies R0 = R \text{ or } > \{0\} = R,$$

which is not the case.

Therefore in  $R$ ,

$$x \neq 0 \text{ and } y \neq 0 \implies xy \neq 0.$$

Reading the  
**contrapositive of the statement**, we have  
 $xy = 0 \implies x = 0 \text{ or } y = 0$ , or  $R$  has no zero-divisors.

Now  $Ra = R$  implies there exist some element  $u_0 \in R$  such that

$$u_0 a = a.$$

Clearly  $u_0 \neq 0$  otherwise that would mean  $a = 0$ .

Also

$$u_0(u_0 a) = u_0 a, \text{ or } (u_0 u_0 - u_0)a = 0.$$

But  $R$  has **no zero-divisors** and  $a \neq 0$ ,

so

$$u_0 u_0 - u_0 = 0.$$

Therefore  $u_0 u_0 = u_0$ .

We claim  $u_0$  to the required **multiplicative left-identity**.

Suppose if not, then there must exist some  $r \in R$  such that  $u_0r \neq r$ .

But then

$$u_0(u_0r - r) = u_0u_0r - u_0r = u_0r - u_0r = 0,$$

that is,

$$u_0(u_0r - r) = 0.$$

Again  $R$  has **no zero-divisors**,

so

$$u_0r - r = 0 \text{ as } u_0 \neq 0.$$

Thus  $u_0r = r$  which is a **contradiction**.

Hence  $u_0r = r$  for all  $r \in R$ , or  $u_0$  is the multiplicative left-identity of  $R$ .

Again  $Ra = R$  implies that there exist some  $a'$  such that

$$a'a = u_0.$$

So the left-inverse  $a'$  of an arbitrarily chosen element  $a \neq 0$  exists in  $R$ .

This establishes  $R$  to be a **division ring**.

So we have either  $R = (0)$  or is a division ring.

But  $\{0\}$  itself is a division ring.

So  $R$  is a **division ring**.

This completes the case 2.

Combining both Cases, we have either  $R$  is a division ring or  $R$  is a ring of prime order with  $r_1r_2 = 0$  for all  $r_1, r_2 \in R$ .

Hence the result.

## Result

7 of 7

So for a given ring  $R$  with two ideals only,  $(0)$  and  $R$  itself, we have proved that  $R$  is either a Division ring or  $R$  is a ring with a prime number of elements in which  $ab = 0$  for every  $a, b \in R$ .  
Click for the detailed proof.

29. a

**Given:**  $R$  is a ring with unity 1. Let  $a \in R$  such that the left inverse  $b$  of  $a$  is unique i.e. there exists only one element  $b$  in  $R$  such that  $ba = 1$ .

**To Prove:**  $ab = 1$

### Step 2

2 of

**Proof:** If  $a$  has only one left inverse  $b$ , then  $ba = 1$ .

Now we have,

$$(1 - ab)a = a - (ab)a = a - a(ba) = 0.$$

Now,

$$(1 - ab + b)a = (1 - ab)a + ba = 1.$$

Hence,

$$(1 - ab + b)a = 1.$$

But by the uniqueness of left inverse of  $a$  we have,

$1 - ab + b = b$ , so  $1 = ab$  and  $b$  is a right inverse.

This completes the proof.

## Section 4–4

### 1. a

If  $a$  and  $b$  aren't divisible by 3 then we know that  $(a, b)$  are congruent to either  $(1, 1)$ ,  $(1, 2)$ ,  $(2, 1)$  or  $(2, 2)$  modulo 3, where we can identify the middle two options due to addition of commutativity.

If  $a \equiv 1 \pmod{3}$  and  $b \equiv 1 \pmod{3}$  then  $a^2 + b^2 \equiv 2 \pmod{3}$ , so 3 doesn't divide  $a^2 + b^2$ .

If  $a \equiv 1 \pmod{3}$  and  $b \equiv 2 \pmod{3}$  then  $a^2 + b^2 \equiv 2 \pmod{3}$ , so 3 doesn't divide  $a^2 + b^2$ .

If  $a \equiv 2 \pmod{3}$  and  $b \equiv 2 \pmod{3}$  then  $a^2 + b^2 \equiv 2 \pmod{3}$ , so 3 doesn't divide  $a^2 + b^2$ .

### Result

2 of 2

We check the values of  $a^2 + b^2$  modulo 3. Click for more details.

### 2. a

It was shown in **Example 2** that it is a field, we prove that it has nine elements.

## Step 2

2 of 3

We investigate the cosets of  $M$  in  $R$ . Note that  $a + bi + M = c + di + M$  if and only if  $(a - c) + (b - d)i \in M$  which is equivalent with  $3 \mid a - c$  and  $3 \mid b - d$ , i.e. iff  $a \equiv c \pmod{3}$  and  $b \equiv d \pmod{3}$ . But this implies that cosets of  $M$ , given by  $a + bi + M$  with  $a, b \in \mathbb{Z}$  are determined exclusively and completely by congruence classes of  $a$  and  $b$  modulo 3. As there 3 choices for the congruence class of  $a$  and 3 choices for the congruence class of  $b$ , and we can make these choices independently, it follows there are 9 cosets of  $M$  in  $R$ , i.e. that  $R/M$  has 9 elements.

## Result

3 of 3

We investigate and enumerate all the cosets of  $M$  in  $R$ . Click for more details.

### 3. a

Problem: Show that

$M = \{x(2+i) \mid x \in R\}$  is a maximal ideal of  $R = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

## Step 2

### Method 1

Let  $I$  be an ideal of  $R$  such that  $M \subsetneq I \subsetneq R$ . We need to show that  $I = R$  or  $I = M$ .  
Let  $a = (x+yi) \in I - M$ .

Hence 5 doesn't divide  $x^2 + y^2$  as  $a$  cannot be written as a multiple of  $(2+i)$ . (Check)  
Consider the set

$$\begin{aligned} S &= \{(A.\bar{a}).a + (B.\overline{(2+i)}).(2+i) \mid A, B \in \mathbb{Z}\} \\ &= \{A.(x^2 + y^2) + B.5 \mid A, B \in \mathbb{Z}\} \\ &= \{z.\gcd((x^2 + y^2), 5) \mid z \in \mathbb{Z}\} \text{ (By Bezout's Lemma)} \\ &= \mathbb{Z} \text{ as 5 is a prime and 5 doesn't divide } x^2 + y^2. \end{aligned}$$

Therefore  $S = \mathbb{Z}$ .

Observe that  $a, (2+i) \in I$  implies that  $S = \mathbb{Z} \subsetneq I$  as  $I$  is an ideal of  $R$ .

Thus  $1 \in I$ . So  $\forall r \in R, r.1 = r \in I$  as  $I$  is an ideal. Hence  $I = R$ .

**Method 2:**

\$\textbf{Note}\$: This proof uses basic theorems and results all of which aren't stated in the book before this exercise.

Theorem:  $\mathbb{Z}[i]$  is an Euclidean Domain. [This is given as problem 29 on page 166].

Theorem: Every Euclidean Domain is a Principal Ideal Domain.

Theorem: Every maximal ideal of a Principal Ideal Domain is generated by an irreducible element.

Result:  $(2+i)$  is an irreducible element of  $\mathbb{Z}[i]$ .

Proof: Observe that  $N(2+i)=5$  and if  $(2+i) = x \cdot y$  where  $x, y \in \mathbb{Z}[i]$ , then  $N(y)=1$  or  $N(x)=1$  as 5 is a prime, which implies that  $x$  or  $y$  must be an unit. Hence  $(2+i)$  is irreducible in  $\mathbb{Z}[i]$ .

Note:  $N(x+iy) = x^2+y^2$

In this problem  $I$  is the ideal generated by  $2+i$ . Hence the proof follows.

**4. a**

We are going to construct an onto homomorphism  $\varphi : \mathbb{Z} \rightarrow R/M$  with  $\ker \varphi = (5)$ , which is going to prove our assertion by the first homomorphism theorem for rings.

**Step 2**

2 of 4

We define  $\varphi : \mathbb{Z} \rightarrow R/M$  by

$$\varphi(n) = n + M,$$

where recall that  $M = (2+i)$ , i.e.  $\varphi(n)$  maps  $n$  to the coset of  $M$  to which  $n$  belongs. Let  $a, b$  be arbitrary integers, then  $(2+i)b \in M$ , so that

$$a + bi + M = a + bi - (2+i)b + M = a - 2b + M,$$

but this implies that

$$\varphi(a - 2b) = a + bi + M$$

where  $a - 2b \in \mathbb{Z}$  and  $a$  and  $b$  were arbitrary, so that  $\varphi$  is onto.

Now  $x \in \ker \varphi$  iff  $x \in M = (2+i)$ , which means that  $(2+i) | x$ . This means that there exists a  $y \in R$  such that  $(2+i)y = x$ , but taking complex conjugates we get that

$$(2-i)\bar{y} = \bar{x},$$

where  $\bar{x} = x$  because  $x$  is an integer, so that  $(2-i) | x$ . It can easily be shown that  $2+i$  and  $2-i$  are relatively prime in  $R$ , so that  $(2+i)(2-i) = 5$  divides  $x$ , i.e.  $\ker \varphi \subset (5)$ ; in order to show equality we have to show that  $5 \in \ker \varphi$ , but this follows directly from  $(2+i) | 5$ , finishing our proof.

**Result**

4 of 4

We construct an onto homomorphism  $\varphi : \mathbb{Z} \rightarrow R/M$  with  $\ker \varphi = (5)$ . Click for more details.

**5. a**

Recall from **Problem 4** that if  $M = (2 + i)$  then  $R/M \cong \mathbb{Z}_5$ . Furthermore, the exact same line of reasoning used in **Problem 3** to show that  $M$  is maximal can be adapted to show that  $K = (2 - i)$  is also a maximal ideal and that  $R/K \cong \mathbb{Z}_5$ .

## Step 2

2 of 5

We define a map  $\varphi : R \rightarrow R/M \oplus R/K$  by

$$\varphi(r) = (r + M, r + K)$$

then **Problem 20** of the last section (page 147) shows that this is a homomorphism and that its kernel is  $M \cap K$ . Therefore, we are finished (by the first homomorphism theorem) if we prove that  $M \cap K = I$  and that  $\varphi$  is onto.

Let us first prove that  $M \cap K \subseteq I$ . Suppose that  $x \in M \cap K$ , then we can write  $x$  as  $x = (m_0 + m_0i)(2 + i)$  and  $x = (k_0 + k_1i)$  for some integers  $m_0, m_1, k_0, k_1$ , so that

$$x^2 = (2 + i)(2 - i)(m_0 + m_0i)(k_0 + k_1i) = 5(m_0 + m_0i)(k_0 + k_1i),$$

i.e.  $x^2 \in I$ , where if  $x = x_0 + x_1i$  we have that  $x^2 = (x_0^2 - x_1^2) + 2x_0x_1i$ , i.e.  $5 \mid x_0^2 - x_1^2$  and  $5 \mid 2x_0x_1i$ . The latter of these implies that 5 divides at least one of  $x_0$  or  $x_1$ , but then the first one implies that it divides the other one as well. Thus  $x \in I$ .

To prove the opposite inclusion, note that  $5 = (2 + i)(2 - i)$  i.e.  $5 \in M \cap K$ , from which it follows that  $I \subseteq M \cap K$ , finishing our proof of  $M \cap K \subseteq I$ .

## Step 4

4 of 5

Finally, in order to prove that  $\varphi$  is onto, note that the ideal  $(2 + i, 2 - i)$  generated by  $2 + i$  and  $2 - i$  is equal to the whole  $R$ , since  $5 \in (2 + i, 2 - i)$  and since  $i(2 + i)^2 - (2 - i)^2 = -8 \in (2 + i, 2 - i)$ , then also  $5 \cdot (-11) + (-8) \cdot (-7) = 1 \in (2 + i, 2 - i)$ , so that any  $r \in R/M$  can be written as  $k + M$  for some  $k \in K$  and any  $r \in R/K$  can be written as  $m + K$  for  $m \in M$ .

Now let  $(r_1 + M, r_2 + K) \in R/M \oplus R/K$ , then  $r_1 = k_1 + m_1$  and  $r_2 = m_2 + k_2$  for some  $k_1, k_2 \in K$  and  $m_1, m_2 \in M$ , so that

$$\varphi(k_1 + m_2) = (k_1 + m_2 + M, k_1 + m_2 + K) = (r_1 + M, r_2 + K),$$

proving that it is onto.

## Result

5 of 5

For  $M = (2 + i)$  and  $K = (2 - i)$  we define a function  $\varphi : R \rightarrow R/M \oplus R/K$  by

$$\varphi(r) = (r + M, r + K)$$

for which the **Problem 20** of the last section shows that it is a homomorphism and that its kernel is  $M \cap K$ , where we show that  $M \cap K = I$  and that  $\varphi$  is onto, whereby we're finished by the first homomorphism theorem. Click for more details.

## 6. a

Let suppose that  $I$  was an ideal with  $M \subset I \subseteq R$ , and let  $a + b\sqrt{2}$  be an element in  $I$  which is not in  $M$ , then 5 doesn't divide either  $a$  or  $b$ .

Suppose that it doesn't divide  $a$  but it does divide  $b$ , then  $b\sqrt{2} \in M$ , so that since  $I$  is also an ideal  $a \in I$ , but since  $\gcd(a, 5) = 1$ , there exist, by **Theorem 1.5.3.**,  $n_0, n_1$  such that  $an_0 + 5n_1 = 1 \in I$ , proving that  $I = R$ .

Now suppose that it does divide  $a$  but it doesn't divide  $b$ , then following similar reasoning as in the last paragraph  $b\sqrt{2} \in I$ , and so since  $I$  is an ideal  $\sqrt{2}(b\sqrt{2}) = 2b \in I$ . But  $\gcd(5, 2b) = 1$ , so that analogous reasoning as in the last paragraph shows that  $I = R$ .

Finally, suppose 5 divides neither  $a$  nor  $b$ . Then  $(a - b\sqrt{2})(a + b\sqrt{2}) = a^2 - 2b^2$  is also in  $I$ . Looking at  $a^2 - 2b^2$  modulo 5 we see that

for  $a = 1$  and  $b = 1$  we have  $a^2 - 2b^2 \equiv 4 \pmod{5}$ ,  
 for  $a = 1$  and  $b = 2$  we have  $a^2 - 2b^2 \equiv 3 \pmod{5}$ ,  
 for  $a = 1$  and  $b = 3$  we have  $a^2 - 2b^2 \equiv 3 \pmod{5}$ ,  
 for  $a = 1$  and  $b = 4$  we have  $a^2 - 2b^2 \equiv 4 \pmod{5}$ ,  
 for  $a = 2$  and  $b = 2$  we have  $a^2 - 2b^2 \equiv 1 \pmod{5}$ ,  
 for  $a = 2$  and  $b = 3$  we have  $a^2 - 2b^2 \equiv 1 \pmod{5}$ ,  
 for  $a = 2$  and  $b = 4$  we have  $a^2 - 2b^2 \equiv 2 \pmod{5}$ ,  
 for  $a = 3$  and  $b = 3$  we have  $a^2 - 2b^2 \equiv 1 \pmod{5}$ ,  
 for  $a = 3$  and  $b = 4$  we have  $a^2 - 2b^2 \equiv 2 \pmod{5}$ ,  
 for  $a = 4$  and  $b = 4$  we have  $a^2 - 2b^2 \equiv 4 \pmod{5}$ ,

so that  $\gcd(a^2 - 2b^2, 5) = 1$  and thus by the similar considerations as before  $I = R$ .

## Result

3 of 3

We suppose there is an ideal  $I$  with  $M \subset I \subseteq R$  and prove that if  $I$  contains some element not in  $M$ , then  $I = R$ . Click for the detailed proof.

## 7. a

In the last exercise it was proved that  $M$  is a maximal ideal, so that  $R/M$  is a field.

Now, by analogous considerations as in **Problem 2**, as we have that if  $a, b, c, d$  are integers, then  $a + b\sqrt{2} = c + d\sqrt{2}$  if and only if  $a = c$  and  $b = d$ , so that we have that cosets  $(a + b\sqrt{2} + M)$  of  $M$  depend only on values of  $a$  and  $b$  modulo 5. Thus, as we can choose them independently, and there are 5 choices for each, we have a total of 25 cosets, i.e. 25 elements of  $R/M$ .

## Result

2 of 2

We use the last exercise to show that it is field, while the counting proceeds analogously as in **Problem 2**. Click for more details.

## 8. a

**To Construct:** A field having 49 elements.

**Construction:**

Since  $49 = 7^2$ ,  
we start with

**a field  $\mathbb{Z}_7$  of characteristic 7**

and look for an **irreducible polynomial** of degree 2 in  $\mathbb{Z}_7[x]$ .

Let us consider the polynomial  $p(x) = x^2 + 1$  in  $\mathbb{Z}_7[x]$ .

Clearly

$p(x)$  is irreducible in  $\mathbb{Z}_7[x]$

, since it is a polynomial in degree 2 and there exist no element  $a$  in  $\mathbb{Z}_7$  such that  $p(a) = 0$  holds, 0 being the additive identity of  $\mathbb{Z}_7$ .

Hence

$$\mathbb{Z}_7[x]/\langle x^2 + 1 \rangle$$

is a

**field of order 49**

The elements of this field are:

$$\begin{aligned}\mathbb{Z}_7[x]/\langle x^2 + 1 \rangle &:= \{ax + b + \langle x^2 + 1 \rangle \mid a, b \in \mathbb{Z}_7\} \\ &= \{a\alpha + b \mid a, b \in \mathbb{Z}_7\},\end{aligned}$$

where  $\alpha = x + \langle x^2 + 1 \rangle$ .

**Result**

3 of 3

Being  $\mathbb{Z}_7$  is a field of char 7, we have constructed a field with 49 elements by considering an irreducible polynomial in  $\mathbb{Z}_7[x]$ .

Click for the detailed proof.

9. a

**To Prove:**

If  $p$  is an odd prime, then there are exactly  $\frac{(p-1)}{2}$  quadratic residues mod  $p$  and  $\frac{(p-1)}{2}$  quadratic non-residues mod  $p$  among the integers  $1, 2, \dots, p - 1$ .

**Step 2****Proof:**

To find all the quadratic residues mod  $p$  among the integers  $1, 2, \dots, p - 1$ , we compute the least positive residues modulo  $p$  of the squares of the integers  $1, 2, \dots, p - 1$ .

Since there are  $p - 1$  squares to consider, and since each congruence

$$x^2 \equiv a \pmod{p}$$

has either zero or two solutions, there must be exactly  $\frac{(p-1)}{2}$  quadratic residues mod  $p$  among the integers  $1, 2, \dots, p - 1$ .

The remaining

$$(p-1) - \frac{(p-1)}{2} = \frac{(p-1)}{2}$$

positive integers less than  $p - 1$  are quadratic non-residues of mod  $p$ .

**Result**

If  $p$  is an odd prime, then we prove that there are exactly  $\frac{(p-1)}{2}$  quadratic residues and  $\frac{(p-1)}{2}$  quadratic non-residues mod  $p$  among the integers  $1, 2, \dots, p - 1$ .

[Click for the detailed solution.](#)

**10. a**

Note that  $R$  is a subset of  $\mathbb{R}$ , so that associativity of usual addition and multiplication of real numbers implies that addition and multiplication on  $R$  are associative, and the same holds for distributivity of multiplication over addition.

**Step 2**

2 of 3

We are left to prove that  $0, 1 \in R$  which is obtained by choosing  $a = 0, b = 0$  and  $a = 1, b = 0$ , respectively, as well as that  $R$  is closed under addition and multiplication.

To show those two, let  $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ , then

$$(a_1 + \sqrt{m}b_1) + (a_2 + \sqrt{m}b_2) = (a_1 + a_2) + \sqrt{m}(b_1 + b_2),$$

which is in  $R$  because  $a_1 + b_1, a_2 + b_2 \in \mathbb{Z}$ . Also

$$\begin{aligned} (a_1 + \sqrt{m}b_1)(a_2 + \sqrt{m}b_2) &= a_1a_2 + \sqrt{m}a_1b_2 + \sqrt{m}b_1a_2 + ma_2b_2 \\ &= (a_1 + a_2 + ma_2n_2) + \sqrt{m}(a_1b_2 + b_1a_2), \end{aligned}$$

which is in  $R$  because  $a_1 + a_2 + ma_2n_2, a_1b_2 + b_1a_2 \in \mathbb{Z}$ .

## Result

3 of 3

We use the fact that addition and multiplications on  $R$  are restrictions of the usual addition and multiplication on  $\mathbb{R}$ , as well as show directly that sum and product of two elements in  $R$  are again in  $R$ . Click for more details.

## 11. a

$I_p$  is obviously not empty, so let us prove it is an additive subgroup of  $R$  and that it is closed under multiplication by elements of  $R$ .

### Step 2

2 of 4

#### $I_p$ is an additive subgroup of $R$

If  $a_0 + b_0\sqrt{m} \in I_p$  and  $a_1 + b_1\sqrt{m} \in I_p$ , this means that  $p$  divides  $a_0, a_1, b_0, b_1$ , but then it also divides  $a_0 + a_1$  and  $b_0 + b_1$ , so that

$$(a_0 + b_0\sqrt{m}) + (a_1 + b_1\sqrt{m}) = (a_0 + a_1) + (b_0 + b_1)\sqrt{m} \in I_p.$$

#### $I_p$ is closed under multiplication by elements of $R$

Suppose that  $a_0 + b_0\sqrt{m} \in I_p$  and  $a + b\sqrt{m} \in R$ . Then we have that

$$(a + b\sqrt{m})(a_0 + b_0\sqrt{m}) = (aa_0 + mbb_0) + (ab_0 + ba_0)\sqrt{m}.$$

Now as  $p \mid a_0$  and  $p \mid b_0$  we have that  $p \mid aa_0 + mbb_0$  and  $p \mid ab_0 + ba_0$ , so that the product is again in  $I_p$ , which finishes our proof.

## Result

4 of 4

We verify that  $I_p$  is an additive subgroup of  $R$  and that it is closed under multiplication by elements of  $R$ . Click for more details.

## 12. a

Suppose that we have an ideal  $I$  with  $I_p \subset I \subseteq R$ , where  $I$  contains an element  $a + b\sqrt{m}$  not in  $I_p$ , we want to prove that  $I = R$ . First note that  $p = I_p$  for  $b = 0$  and  $a = p$ . Next, note that  $(a - b\sqrt{m})(a + b\sqrt{m}) = a^2 - mb^2 \in I$ . If we prove that, for any  $a, b$  such that they're not both divisible by  $p$ , we have that  $a^2 - mb^2$  is not divisible by  $p$ , then  $\gcd(a^2 - mb^2, p) = 1$  and by an application of **Theorem 1.5.3.** we have that  $1 \in I$ , hence  $I = R$ .

## Step 2

2 of 3

Suppose there were  $a, b$ , not both divisible by  $p$ , such that  $a^2 - mb^2 \equiv 0 \pmod{p}$ , which is equivalent to

$$a^2 \equiv mb^2 \pmod{p}.$$

If  $b^2 \equiv 0 \pmod{p}$ , then  $b \equiv 0 \pmod{p}$ , so that  $b$  is divisible by  $p$ , but then  $a \equiv 0 \pmod{p}$ , i.e.  $a$  is also divisible. The same line of reasoning, if we note that  $\gcd(m, p) = 1$  because  $m$  is a quadratic nonresidue mod  $p$ , holds to show that if  $a^2 \equiv 0 \pmod{p}$  then  $b$  is also divisible by  $p$ .

The last remaining case is if both  $a$  and  $b$  are not divisible by  $p$ ; then  $b$  is invertible mod  $p$ , and so is  $b^2$ . Thus we have

$$m \equiv a^2(b^2)^{-1} \equiv (ab^{-1})^2 \pmod{p},$$

contradicting the assumption that  $m$  is a quadratic nonresidue modulo  $p$ . As we have arrived at a contradiction, we conclude there are no such  $a, b$ , so that the procedure outlined in the first paragraph demonstrates that  $I = R$ , so that  $I_p$  is maximal.

## Result

3 of 3

Key insight that we use is that if  $m$  is a quadratic nonresidue modulo  $p$ , then  $(a - b\sqrt{m})(a + b\sqrt{m}) = a^2 - mb^2$  is never divisible by  $p$  unless both  $a$  and  $b$  are divisible by  $p$ . Click for the detailed proof.

## 13. a

By **Problem 12**  $I_p$  is maximal, so that  $R/I_p$  is a field. Note that  $a + b\sqrt{m}$  and  $c + d\sqrt{m}$  are in the same coset of  $I_p$  if

$$\begin{aligned}(a + b\sqrt{m}) - (c + d\sqrt{m}) &\in I_p \\ (a - c) + (b - d)\sqrt{m} &\in I_p\end{aligned}$$

which is equivalent with  $a \equiv c \pmod{p}$  and  $b \equiv d \pmod{p}$ . Thus, cosets  $(a + b\sqrt{m} + I)$  of  $I_p$  are completely determined by values of  $a, b$  modulo  $p$ . Since this choice is independent, and there are  $p$  choices for both  $a$  and  $b$ , it follows that there are  $p^2$  distinct cosets of  $I_p$ , or in other words that  $R/I_p$  has  $p^2$  elements.

## Result

2 of 2

We show that a coset  $a + b\sqrt{m} + I_p$  is completely determined by values of  $a$  and  $b$  modulo  $p$ , from which it easily follows that  $R/I_p$  has  $p^2$  elements. Click for the detailed proof.

# Section 4–5

## 1. a

Suppose  $f$  is an invertible element with the inverse  $f^{-1}$ , so that  $ff^{-1} = 1$ .

Then

$$\begin{aligned}\deg(ffff^{-1}) &= \deg(1) \\ \deg(f) + \deg(f^{-1}) &= 0\end{aligned}$$

where we used the fact that for any polynomials  $f$  and  $g$ ,  $\deg(fg) = \deg(g) + \deg(f)$ .

## Step 2

2 of 3

Since  $\deg(f)$  and  $\deg(f^{-1})$  must be nonnegative integers, then  $\deg(f) = \deg(f^{-1}) = 0$ , i.e.  $f$  is a nonzero constant, or in other words  $f$  is a nonzero element of  $F$ .

## Result

3 of 3

We use that fact that  $\deg(fg) = \deg(g) + \deg(f)$ . Click for the detailed proof.

## Method 2.

① Let  $F$  be a field. Let  $f(x) \in F[x]$  s.t  
 $\exists g(x) \in F[x]$ . and  
 $f(x) \cdot g(x) = 1$   
 $\Rightarrow \deg f(x) + \deg g(x) = 0$   
 $\Rightarrow \deg f(x) = \deg g(x) = 0$   
 $\Rightarrow$  only invertible elements in  $F[x]$  are  
in  $F \setminus \{0\}$ .

2. a

**(a)**

Analogously with **Lemma 4.5.2**, if the degree of  $f(x)$  is  $m \geq 0$  and the degree of  $g(x)$  is  $n \geq 0$ , then by the definition of the multiplication of polynomials the highest power of  $x$  which can occur in the product  $f(x)g(x)$  is  $x^{m+n}$ . But this is all we need for a proof, since  $\deg f(x) + \deg g(x) = m + n$ .

**Step 2**

2 of 3

**(b)**

Let  $R = \mathbb{Z}_{10}$ , and let  $f(x) = 5x + 1$  and  $g(x) = 2x + 1$ , then

$$f(x)g(x) = (5x + 1)(2x + 1) = 10x^2 + 5x + 2x + 1 = 7x + 1,$$

i.e.  $\deg f(x)g(x) = 1$ , while  $\deg f(x) + \deg g(x) = 2$ .

**Result**

3 of 3

Proof in (a) is analogous with that of **Lemma 4.5.2**. For (b), take  $R = \mathbb{Z}_{10}$ ,  $f(x) = 5x + 1$  and  $g(x) = 2x + 1$ .

[Click for more details.](#)

**3. a****(a)**

Since  $x + 4$  has degree 1, only possible common divisor of these polynomials with degree greater than 0 is  $x + 4$ . Note that  $x + 4$  dividing  $x^3 - 6x + 7$  is equivalent with  $-4$  being a root of  $x^3 - 6x + 7$ , which we directly check:  $(-4)^3 - 6(-4) + 7 = -64 + 24 + 7 \neq 0$ , so that

$$\gcd(x^3 - 6x + 7, x + 4) = 1.$$

**Step 2**

2 of 5

**(b)**

Note that  $x^2 - 1 = (x + 1)(x - 1)$ . By the uniqueness of factorization we have to check whether 1 and/or  $-1$  are roots of  $2x^7 - 4x^5 + 2$ : for  $x = 1$  we get  $2 - 4 + 2 = 0$ , while for  $x = -1$  we get  $-2 + 4 + 2 = 4$ , so that  $x - 1 \mid 2x^7 - 4x^5 + 2$  and then

$$\gcd(x^2 - 1, 2x^7 - 4x^5 + 2) = x - 1.$$

**(c)**

We get that  $3x^2 + 1$  is irreducible over  $\mathbb{Q}$ , because it is of degree 2 and all its roots are  $\pm\frac{1}{\sqrt{3}}i \notin \mathbb{Q}$ , so that only polynomials that divide it are constant ones. However, we need to investigate whether  $3x^2 + 1$  divides  $x^6 + x^4 + x + 1$ . By an application of long division we get

$$x^6 + x^4 + x + 1 = (x^4/3 + 2x^2/9 - 2/27)(3x^2 + 1) + x + 29/27$$

from which we see that  $3x^2 + 1$  doesn't divide  $x^6 + x^4 + x + 1$ , so that

$$\gcd(3x^2 + 1, x^6 + x^4 + x + 1) = 1.$$

**Step 4**

4 of 5

**(d)**

Note that  $x^7 - x^4 + x^3 - 1 = x^4(x^3 - 1) + x^3 - 1 = (x^3 - 1)(x^4 + 1)$ , so that

$$\gcd(x^3 - 1, x^7 - x^4 + x^3 - 1) = x^3 - 1.$$

**Result**

We have the following results:

**(a)**  $\gcd(x^3 - 6x + 7, x + 4) = 1,$

**(b)**  $\gcd(x^2 - 1, 2x^7 - 4x^5 + 2) = x - 1,$

**(c)**  $\gcd(3x^2 + 1, x^6 + x^4 + x + 1) = 1,$

**(d)**  $\gcd(x^3 - 1, x^7 - x^4 + x^3 - 1) = x^3 - 1.$

[Click for more details.](#)

**4. a**

Let  $p(x) = \sum_{i=0}^n a_i x^i$  and  $q(x) = \sum_{i=0}^m b_i x^i$  with  $a_n \neq 0$  and  $b_m \neq 0$ , so that  $\deg p(x) = n$  and  $\deg q(x) = m$ . We also define  $a_i = 0$  for all  $i > n$  and  $b_i = 0$  for all  $i > m$ . Then the sums can be taken over all nonnegative integers.

**Step 2**

2 of 3

Now we have

$$p(x) + q(x) = \sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i = \sum_{i=0}^{\max(n, m)} (a_i + b_i) x^i$$

where we're looking for the largest  $j$  such that  $a_j + b_j \neq 0$ . To prove the lemma it is sufficient to prove that  $j \leq \max(m, n)$ , but this is just a consequence of the fact that for any  $i > m$  and  $i > n$ , which is equivalent with  $i > \max(m, n)$ ,  $a_i = 0$  and  $b_i = 0$ , so that  $a_i + b_i = 0$  for  $i > \max(m, n)$ , proving our inequality.

**Result**

3 of 3

We look at the sum of two polynomials and investigate what is the greatest exponent which can be nonzero. Click [for the detailed proof.](#)

## Method 2.

④  $p(x), q(x) \in F[x]$ ,  $p(x) + q(x) \neq 0$

TST:  $\deg(p(x) + q(x)) \leq \max(\deg(p(x)), \deg(q(x)))$ .

**Proof:** Let  $\deg(p(x)) = n$ ,  $\deg(q(x)) = m$

$$p(x) = \sum_{i=0}^n a_i x^i, \quad q(x) = \sum_{i=0}^m b_i x^i$$

$$p(x) + q(x) = \sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i$$

case (i)  $n \geq m$

$$p + q = \sum_{i=0}^m (b_i + a_i) x^i + a_{m+1} x^{m+1} + \dots + a_n x^n$$

$$\Rightarrow \deg(p+q) \leq n$$

case (ii)  $m > n$

$$p + q = \sum_{i=0}^n (b_i + a_i) x^i + b_{n+1} x^{n+1} + \dots + b_m x^m$$

$$\Rightarrow \deg(p+q) \leq m$$

∴ Either case gives  $\boxed{\deg(p+q) \leq \max(n, m)}$ .

## 5. a

Recall that the results of **Problem 3** are:

- (a)  $\gcd(x^3 - 6x + 7, x + 4) = 1$ ,
- (b)  $\gcd(x^2 - 1, 2x^7 - 4x^5 + 2) = x - 1$ ,
- (c)  $\gcd(3x^2 + 1, x^6 + x^4 + x + 1) = 1$ ,
- (d)  $\gcd(x^3 - 1, x^7 - x^4 + x^3 - 1) = x^3 - 1$ .

### Step 2

2 of 3

By **Theorem 4.5.7**, we have that  $\gcd(f(x), g(x)) = \{f(x)a(x) + g(x)b(x)\}$ , so that in parts (a) and (c) we get that  $I = (1) = R$ .

In the (b) part we have  $x - 1 \in I$ , but since  $x - 1 \mid x^2 - 1$  and  $x - 1 \mid 2x^7 - 4x^5 + 2$ , then  $x - 1 \mid i$  for any  $i \in I$ , so that  $I = (x - 1)$ .

Analogous reasoning shows that in the (d) part we have that  $I = (x^3 - 1)$ .

## Result

We use **Theorem 4.5.7.** to show that

(a)  $I = (1)$ ,

(b)  $I = (x - 1)$ ,

(c)  $I = (1)$ ,

(d)  $I = (x^3 - 1)$ .

Click for more details.

## 6. a

Since  $g(x) | f(x)$ , then there exist  $k(x) \in F[x]$  such that  $g(x)k(x) = f(x)$ .

Now let  $p(x) \in (f(x))$ , then

$$p(x) = q(x)f(x)$$

for some  $q(x) \in F[x]$ , but then also

$$p(x) = (q(x)k(x))g(x),$$

where  $q(x)k(x) \in F[x]$ , so that  $p(x) \in (g(x))$ , proving the  $(f(x)) \subset (g(x))$ .

## Result

2 of 2

If  $g(x) | f(x)$  then  $g(x)k(x) = f(x)$  for some  $k(x) \in F[x]$ , and we use to prove the desired fact. Click for more details.

## Method 2.

⑥ let  $f(x), g(x) \in F[x]$ .  
and  $g(x) | f(x)$   
 $\Rightarrow f(x) = q(x)h(x)$  for some  $h(x) \in F[x]$ .  
 $\Rightarrow f(x) \in (g(x))$ .  
hence  $f(x) \cdot k(x) \in (g(x)) \quad \forall k(x) \in F[x]$ .  
 $\Rightarrow (f(x)) \subset (g(x))$ .

## 7. a

Suppose  $k_1(x)$  and  $k_2(x)$  are both greatest common divisors of two polynomials. Then since by definition of greatest common divisors they are divided by every other divisors, we have that  $k_1(x) \mid k_2(x)$ , and also  $k_2(x) \mid k_1(x)$ . Now by **Lemma 4.5.8** we have  $k_1(x) = ak_2(x)$ , but again by definition  $k_1(x)$  and  $k_2(x)$  are monic, so that  $a = 1$  and

$$k_1(x) = k_2(x).$$

## Result

2 of 2

We use **Lemma 4.5.8** to show that any two greatest common divisors are equal. Click for the detailed proof.

## Method 2.

(7) Let  $\gcd(p(x), q(x)) = h_1(x)$   
and  $\gcd(p(x), q(x)) = h_2(x)$ .  
then by def of gcd  $h_2(x) \mid h_1(x)$   
and  $h_1(x) \mid h_2(x)$ .  
by Lemma 4.5.8 we have  $h_1(x) = h_2(x)$ .  
Hence, gcd of two polynomials is unique  
in  $F[x]$ .

## 8. a

Since  $f(x) \mid h(x)$ , then there exists  $k_1(x) \in F[x]$  such that  $f(x)k_1(x) = h(x)$ , and likewise there exists a  $k_2(x) \in F[x]$  such that  $g(x)k_2(x) = h(x)$ . Now, since  $\gcd(f(x), g(x)) = 1$ , by **Theorem 4.5.7** we have that there exist polynomials  $a(x), b(x) \in F[x]$  such that

$$\begin{aligned} f(x)a(x) + g(x)b(x) &= 1, \\ f(x)a(x)h(x) + g(x)b(x)h(x) &= h(x), \\ f(x)a(x)k_2(x)g(x) + g(x)b(x)k_1(x)f(x) &= h(x), \\ f(x)g(x)(a(x)k_2(x) + b(x)k_1(x)) &= h(x) \end{aligned}$$

i.e.  $f(x)g(x) \mid h(x)$ , which is what we wanted to prove.

## Result

2 of 2

We use **Theorem 4.5.7** to give our proof. Click for more details.

## 9. a

If  $p(x) \mid a_1(x)$  then we are done. If not, then since  $p(x)$  is irreducible,  $p(x)$  and  $a_1(x)$  are relatively prime, and thus by **Theorem 4.5.10**.

$$p(x) \mid a_2(x) \cdots a_k(x).$$

Now again if  $p(x) \mid a_2(x)$  we are done, if not then by an application of **Theorem 4.5.10**. we get that

$$p(x) \mid a_3(x) \cdots a_k(x).$$

Either we will be done at  $i$ th,  $i < k$ , step, so that  $p(x) \mid a_i(x)$ , or on the  $k$ th step we will get that  $p(x) \mid a_k(x)$ , finishing our proof.

## Result

2 of 2

We use use the associativity of multiplication, i.e. the fact that  $a_1(x)a_2(x) \cdots a_k(x) = a_1(x)(a_2(x) \cdots a_k(x))$ , and **Theorem 4.5.10**. to give our proof. Click for more details.

10. a

### (a)

As this is a polynomial of degree 2 to show that it is irreducible it is sufficient to show that it has no roots in  $F = \mathbb{R}$ ; this due to the equivalence of  $\ell$  being a root of  $f$  and  $x - \ell$  dividing  $f$ . But it is immediate that it has no roots in  $\mathbb{R}$  since we see that its roots are  $\pm i\sqrt{7} \notin \mathbb{R}$ .

### Step 2

2 of 7

### (b)

As this is a polynomial of degree 3 then the same thing (by the **Problem 11**) holds as in the case of degree 2, so it is sufficient to show that it has no rational roots. Suppose  $\frac{a}{b}$  with  $\gcd(a, b) = 1$  was a rational root, then  $x^3 - 3x + 3 = 0$  implies

$$a^3 - 3ab^2 + 3 = 0.$$

From this we see that  $3 \mid a$ , so that  $a = 3k$  for some integer  $k$ , so that

$$27k^3 - 9kb^2 + 3 = 0$$

where by dividing with 3 we get

$$9k^3 - 3kb^2 + 1 = 0,$$

but this doesn't have any solutions in integers  $b, k$  because the left-hand side is always congruent to 1 modulo 3, thus proving that  $x^3 - 3x + 3$  has no rational roots.

**(c)**

It is again sufficient to check whether there are any roots of  $x^2 + x + 1$  in  $\mathbb{Z}_2$ . We see that both  $x = 1$  and  $x = 0$  give values of 1, so that that's that.

4 of 7

**Step 4****(d)**

We need to verify that there is no element in  $\mathbb{Z}_{19}$  such that its square is  $-1 \equiv 18 \pmod{19}$ . To that end we compute all the squares in  $\mathbb{Z}_{19}$ , for numbers  $1, 2, \dots, 18$ :

$$1, 4, 9, 16, 6, 17, 11, 7, 5, 5, 7, 11, 17, 6, 16, 9, 4, 1.$$

As 18 is not in this list, we are done.

**(e)**

Again by the next problem (**Problem 11**) we are left investigating whether  $x^3 - 9$  has a root over  $\mathbb{Z}_{13}$ , i.e. whether 9 is a cube of some element in  $\mathbb{Z}_{13}$ . Again we compute all the cubes, for numbers  $1, 2, \dots, 12$ :

$$1, 8, 1, 12, 8, 8, 5, 5, 1, 12, 5, 12.$$

As 9 is not in this list, we are done.

**(f)**

Note that if we substitute  $y = x^2$  then by a simple application of quadratic formula we get that

$$x^4 + 2x^2 + 2 = (x^2 + (1-i))(x^2 + (1+i))$$

so that all its roots are complex and it has no roots in  $\mathbb{Q}$ . It remains to prove that there are no quadratic factors over  $\mathbb{Q}[x]$ , so suppose that

$$\begin{aligned} x^4 + 2x^2 + 2 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (c+a)x^3 + (d+b+ac)x^2 + (ad+bc)x + bd \end{aligned}$$

So that we get equations

$$\begin{aligned} c + a &= 0 \\ d + b + ac &= 2 \\ ad + bc &= 0 \\ bd &= 2. \end{aligned}$$

From the first equation we can immediately substitute  $a = -c$  into the rest to get

$$\begin{aligned} d + b - a^2 &= 2 \\ ad - ab &= 0 \\ bd &= 2, \end{aligned}$$

where from the second equation it follows that either  $a = 0$  or  $b = d$ . First, if  $a = 0$  then  $b = 2 - d$  into the third equation we get  $b^2 - 2b + 2 = 0$ , which can be seen by quadratic formula not to have any rational solutions. If  $b = d$ , then  $b^2 = 2$ , i.e.  $b = \sqrt{2}$ , which again contradicts the rationality of  $b$ , proving that there are no such  $a, b, c, d$ .

As a 4 degree polynomial must have either a first degree or a second degree divisor if it has any, we have proved that our polynomial is irreducible over  $\mathbb{Q}$ .

## Result

7 of 7

We obtain all the results except the last ((f)) by showing that the polynomial has no roots in that field, while in (f) we also investigate quadratic factors. Click for more details.

### 11. a

Equivalently we can show the contrapositive, which is that if  $p(x)$  is reducible, then there is an element  $r \in F$  such that  $p(r) = 0$ .

If  $p(x)$  is reducible, then by degree considerations it must factor as  $p(x) = a_0 q(x)l(x)$  where  $q(x), l(x)$  are monic and  $\deg q(x) = 2, \deg l(x) = 1$ ,  $q(x)$  not necessarily being irreducible. But since  $\deg l(x) = 1$  we have that  $l(x) = x - r_0$  for some  $r_0 \in F$ , so that

$$p(r_0) = a_0 q(r_0)(r_0 - r_0) = 0,$$

which is what we wanted to prove.

## Result

2 of 2

We show the contrapositive, that if  $p(x)$  is reducible then there is an element  $r \in F$  such that  $p(r) = 0$ , by considering the possible factorization of  $p(x)$ . Click for the proof.

### 12. a

**Given:**  $F \subseteq K$  are two fields and  $f(x), g(x) \in F[x]$  are relatively prime in  $F[x]$ .

**To Prove:**  $f(x)$  and  $g(x)$  are relatively prime in  $K[x]$ .

**Proof:** There are two cases.

**Case-1:** If the degree of either  $f(x)$  or  $g(x)$  is less than or equal to zero, then the proof is obvious.

**Case-2:** Suppose that Case-1 is not happen.

We prove first that

**for any polynomials**  $f(x), g(x) \in F[x]$  **where**  $F$  **is any field, the elements**  $f(x)$  **and**  $g(x)$  **are relatively prime if and only if there are**

$s(x), t(x) \in F(x)$  **such that**

$$f(x)s(x) + g(x)t(x) = 1.$$

Actually, necessity is easy to show because

If there are  $s(x), t(x) \in F[x]$  such that  $f(x)s(x) + g(x)t(x) = 1$ , then any divisor of  $f(x)$  and  $g(x)$  must also divide 1,

and hence cannot have positive degree

(so  $f(x)$  and  $g(x)$  must be relatively prime in that case).

Suppose then that  $f(x)$  and  $g(x)$  are **relatively prime**, let  $S$  be the set

$$S := \{f(x)s(x) + g(x)t(x) \mid s(x), t(x) \in F[x], \deg(f(x)s(x) + g(x)t(x)) > 0\}$$

and let

$$S' = \{\deg(h(x)) \mid h(x) \in S\}.$$

Since  $f(x) \in S$ , it is clear that  $S$  is **non-empty**.

Therefore  $S'$  is non-empty and by the **Well Ordering Axiom there is a smallest element**  $a \in S'$ .

Let  $s(x), t(x) \in F[x]$  such that

$$h(x) = f(x)s(x) + g(x)t(x)$$

has degree  $a$ .

Now we can divide both  $f(x)$  and  $g(x)$  by  $h(x)$ .

So there are  $q_1(x), r_1(x), q_2(x), r_2(x) \in F[x]$  such that

$$f(x) = h(x)q_1(x) + r_1(x), g(x) = q_2(x)h(x) + r_2(x)$$

and

$$\deg(r_1(x)), \deg(r_2(x)) < \deg(h(x)) = a.$$

**Because the degrees of the  $r_i(x)$  are strictly smaller than  $a$**

, it must be that  $\deg(r_i(x)) \notin S'$ , and hence  $r_i(x) \notin S$  (for  $i = 1, 2$ ).

But

$$\begin{aligned} r_i(x) &= f(x) - h(x)q_i(x) \\ &= f(x) - f(x)s(x)q_i(x) - g(x)t(x)q_i(x) \\ &= f(x)(1 - s(x)q_i(x)) + g(x)(-t(x)q_i(x)), \end{aligned}$$

so  $r_i(x) \in S$  unless  $\deg(r_i(x)) \leq 0$  (again for  $i = 1, 2$ ).

Suppose that  $\deg(r_i(x)) = 0$  for either  $i = 1$  or  $i = 2$  (without loss of generality we may assume that  $\deg(f_1(x)) = 0$ ),

**then  $r_1(x)$  is a non-zero constant**

and thus

$$f(x)(1 - s(x)q_1(x))(r_1(x))^{-1} + g(x)t(x)q_1(x)(r_1(x))^{0-1} = 1$$

proving the assertion.

If

$$\deg(r_i(x)) = -1$$

for both  $i$ , that is, if

$$r_i(x) = 0$$

for  $i = 1$  and  $i = 2$ , then

$$f(x) = q_1(x)(f(x)s(x) + g(x)t(x))$$

and

$$g(x) = q_2(x)(f(x)s(x) + g(x)t(x)).$$

Note that according to these equations  $\deg(f(x)) = \deg(q_1(x)) + a$  and  $\deg(g(x)) = \deg(q_2(x)) + a$ .

**Because  $a$  is smallest in  $S'$ , it must therefore be that  $q_1(x)$  and  $q_2(x)$  have degree zero**

This implies, however, that  $f(x)$  and  $g(x)$  are associates, and **can not be relatively prime**, a contradiction.

Having established this fact, the proof becomes very easy.

If  $f(x)$  and  $g(x)$  are **relatively prime**

over  $F$ , then there are  $s(x), t(x) \in F[x]$  such that

$$f(x)s(x) + g(x)t(x) = 1.$$

Since this equation also holds over  $K[x]$ , that is,  $f(x), g(x), s(x)$ , and  $t(x)$  are also polynomials in  $K[x]$  such that

$$f(x)s(x) + g(x)t(x) = 1,$$

**we conclude that  $f(x)$  and  $g(x)$  are relatively prime over  $K$  as required.**

This completes the proof.

## Result

6 of 6

Since we get polynomials  $s(x)$  and  $t(x)$  are in  $K[x]$  such that

$$f(x)s(x) + g(x)t(x) = 1,$$

holds we proved that  $f(x)$  and  $g(x)$  are relatively prime over  $K[x]$ .

13. a

We first show that any element of  $\mathbb{R}[x]/(x^2 + 1)$  can be written as  $a + bu$ , where  $u$  is the image of  $x$  in  $\mathbb{R}[x]/(x^2 + 1)$ . Let  $p(x) \in \mathbb{R}[x]$ , then we want to show that  $p(x) + (x^2 + 1) = a + bx + (x^2 + 1)$  for some  $a, b \in \mathbb{R}$ , where  $(x^2 + 1)$  denotes the ideal generated by  $x^2 + 1$  in  $\mathbb{R}[x]$ .

But this is a quick consequence of division algorithm for polynomials in  $\mathbb{R}[x]$  (**Theorem 4.5.5.**) by which we have that  $p(x) = q(x)(x^2 + 1) + r(x)$  for some  $q(x), r(x) \in \mathbb{R}[x]$  where  $\deg r(x) < \deg(x^2 + 1) = 2$ , i.e.  $r(x)$  can be written as  $r(x) = ax + b$  because it's of degree 1 or lower. Now we have that

$$p(x) + (x^2 + 1) = q(x)(x^2 + 1) + r(x) + (x^2 + 1) = r(x) + (x^2 + 1)$$

finishing our proof.

We also want to show that  $x^2 + (x^2 + 1) = -1 + (x^2 + 1)$  but this is immediate since  $x^2 - (-1) = x^2 + 1 \in (x^2 + 1)$ .

## Step 2

2 of 4

Note now that since  $x^2 + 1$  is irreducible then  $(x^2 + 1)$  is a maximal ideal (**Theorem 4.5.11.**), so that  $\mathbb{R}[x]/(x^2 + 1)$  is a field (by **Theorem 4.4.2.**) such that each of its elements can be written as  $a + bu$  where  $u^2 = -1$ .

Only thing left to show is that addition and multiplication in  $\mathbb{R}[x]/(x^2 + 1)$  behaves as it does in  $\mathbb{C}$  (for this would allow us to straightforwardly formally verify that intuitive map  $a + bu \mapsto a + bi$  is an isomorphism). We have that

$$(a + bx) + (x^2 + 1) + (c + dx) + (x^2 + 1) = (a + c) + (b + d)x + (x^2 + 1)$$

whereas in  $\mathbb{C}$  we have that  $(a + bi) + (c + di) = (a + c) + (b + d)i$ . We also have that

$$\begin{aligned} ((a + bx) + (x^2 + 1))((c + dx) + (x^2 + 1)) &= (a + bx)(c + dx) + (x^2 + 1) \\ &= ac + adx + bcx + bdx^2 + (x^2 + 1) \\ &= ac + adx + bcx - bd + (x^2 + 1) \\ &= (ac - bd) + (ad + bc)x + (x^2 + 1), \end{aligned}$$

where we use the fact that  $x^2 + (x^2 + 1) = -1 + (x^2 + 1)$ , whereas in  $\mathbb{C}$  we have that  $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ , completing our proof.

## Result

4 of 4

We use division algorithm for polynomials to prove that every element of  $\mathbb{R}[x]/(x^2 + 1)$  can be written in form  $ax + b + (x^2 + 1)$ , and then note that  $\mathbb{R}[x]/(x^2 + 1)$  is a field and that the only thing left to verify is that addition and multiplication in it behave like they do in  $\mathbb{C}$ , which we then proceed to do. Click for the detailed proof.

14. a

**(a)**

Note that since  $p(x)$  is of degree 2 its irreducibility is equivalent with it not having any roots in  $\mathbb{Z}_{11}$ ; and note that  $p(x) = 0$  iff  $x^2 \equiv -1 \equiv 10 \pmod{11}$  for some  $x$ . Now irreducibility can easily be seen as images of elements  $0, 1, 2, \dots, 11$  under the map  $x \mapsto x^2$  in  $\mathbb{Z}_{11}$ , are:

$$1, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1.$$

Now since  $p(x)$  is irreducible then by  $(p(x))$  is a maximal ideal (by **Theorem 4.5.11**) and  $\mathbb{Z}_{11}[x]/(p(x))$  is a field, by **Theorem 4.4.2**.

By division algorithm we can see (see the beginning of my solution of **Problem 13** for details how to do this) that every element of  $\mathbb{Z}_{11}[x]/(p(x))$  is of the form  $a + bx + (p(x))$  where  $a, b \in \mathbb{Z}_{11}$ . Furthermore, each of these cosets is distinct, since if

$$a + bx + (p(x)) = c + dx + (p(x)) \quad (1)$$

then  $(a - c) + (b - d)x \in (p(x))$ , so that  $p(x)q(x) = (a - c) + (b - d)x$  for some  $q(x) \in \mathbb{Z}_{11}[x]$ , but by

**Lemma 4.5.2.** (which states that the degree of the product of polynomials is a sum of their degrees), the degree of the left-hand side is 2 or greater unless  $q(x) = 0$ , in which case it is  $-\infty$ , and the degree of the left-hand side is 1 or 0 unless  $a - c = 0$  and  $b - d = 0$ , in which case it is also  $-\infty$ , from which we see that the only way for (1) to hold is that  $a = c$  and  $b = d$ .

Thus we have 11 choices for  $a$  and 11 choices for  $b$ , we can make those choices independently and each gives rise to a different element of  $\mathbb{Z}_{11}[x]/(p(x))$ , from which it follows that

$$|\mathbb{Z}_{11}[x]/(p(x))| = 11 \cdot 11 = 121.$$

**(b)**

All of the reasoning employed in the (a) part is completely analogous here, for again using division algorithm we get that the elements of  $\mathbb{Z}_{11}[x]/(p(x))$  can be written as  $a + bx + cx^2$  for  $a, b, c \in \mathbb{Z}_{11}$  and that each of these choices gives rise to a distinct element of  $\mathbb{Z}_{11}[x]/(p(x))$ , so that we have  $11 \cdot 11 \cdot 11 = 11^3$  distinct choices and these enumerate all the elements of  $\mathbb{Z}_{11}[x]/(p(x))$ .

Thus the only thing we have to check is that  $p(x) = x^3 + x + 4$  is irreducible. By **Problem 11** it is sufficient to show that  $p(x)$  has no roots in  $\mathbb{Z}_{11}$ , which we do by computing the images of all the elements of  $\mathbb{Z}_{11}$  under  $p(x)$ :

$$\begin{aligned} p(0) &= 4, p(1) = 6, p(2) = 3, p(3) = 1, p(4) = 6, p(5) = 2, \\ p(6) &= 6, p(7) = 2, p(8) = 7, p(9) = 5, p(10) = 2. \end{aligned}$$

**Result**

3 of 3

In (a) part we show that elements of  $\mathbb{Z}_{11}[x]/(p(x))$  can be written in the form of  $ax + b$  for  $a, b \in \mathbb{Z}_{11}$  and that all distinct choices of  $a$  and  $b$  give rise to different elements of  $\mathbb{Z}_{11}[x]/(p(x))$ , which gives our desired proof. We proceed along the same lines in the (b) part as well. Click for the details.

15. a

We immediately get that  $F[x]/(q(x))$  is a field because  $q(x)$  is irreducible, we just have to show that it has at most  $p^n$  elements. To do this, we prove that each element of  $F[x]/(q(x))$  can be written in the form

$$a_{n-1}x^{n-1} + \cdots + a_1x + a_0 + (q(x)).$$

2 of 3

## Step 2

Let  $p(x) \in F[x]$ , then by division algorithm for polynomial (**Theorem 4.5.5**) we have that we can write  $p(x) = q(x)w(x) + r(x)$  where  $w(x), r(x) \in F[x]$  and  $\deg r(x) < \deg q(x) = n$ . Now we have that

$$p(x) + (q(x)) = q(x)w(x) + r(x) + (q(x)) = r(x) + (q(x))$$

because  $q(x)w(x) \in (q(x))$ . This proves our theorem, as there are  $p^n$  polynomials of degree  $n - 1$  or lower in  $\mathbb{Z}_p[x]$ , as there  $p^n$  ways to choose elements

$$a_{n-1}, a_{n-2}, \dots, a_1, a_0$$

of  $\mathbb{Z}_p$ , and polynomials are equal if and only if all their coefficients are equal.

3 of 3

## Result

This follows from division algorithm showing that for any  $p(x) \in F[x]$  we have that  $p(x) + (q(x)) = a_{n-1}x^{n-1} + \cdots + a_1x + a_0 + (q(x))$  for some  $a_{n-1}, \dots, a_0 \in \mathbb{Z}_p$ , from which our desired result follows by counting the number of polynomials of degree  $n - 1$  or lower in  $\mathbb{Z}_p[x]$ . Click for more details.

## 16. a

In the previous problem we have shown that any for any  $p(x) \in F[x]$ , we have that

$$p(x) + (q(x)) = a_{n-1}x^{n-1} + \cdots + a_1x + a_0 + (q(x))$$

for some  $a_{n-1}, \dots, a_0 \in F$ , and that there are  $p^n$  choices for these numbers, so that  $F[x]/(q(x)) \leq p^n$ . In order to show that equality holds, we have to show that each of these choices induces a different element of  $F[x]/(q(x))$ ; in other words, that each different polynomial of degree  $n - 1$  or lower belongs to a different coset of  $(q(x))$  in  $F[x]$ .

Suppose now, then, that

$$a_{n-1}x^{n-1} + \cdots + a_1x + a_0 + (q(x)) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0 + (q(x))$$

which is equivalent with  $(a_{n-1} - b_{n-1})^{n-1} + \cdots + (a_1 - b_1)x + (a_0 - b_0) \in (q(x))$ , which is in turn equivalent with there being a  $w(x) \in F[x]$  such that

$$q(x)w(x) = (a_{n-1} - b_{n-1})^{n-1} + \cdots + (a_1 - b_1)x + (a_0 - b_0).$$

Degree of the right hand side is strictly smaller than  $n$ , while the degree of the left hand side is greater or equal to  $n$  except if  $w(x) = 0$ , so that if equality is hold we must have that  $w(x) = 0$ , but then since polynomials are equal iff all of their coefficient are equal we get that  $a_{n-1} - b_{n-1} = 0, \dots, a_1 - b_1 = 0, a_0 - b_0 = 0$ , i.e.

$$a_{n-1} = b_{n-1}, \dots, a_1 = b_1, a_0 = b_0$$

which is what we needed to prove.

## Result

3 of 3

We use the result of the previous problem and then show that each polynomial of degree  $n - 1$  or lower belongs to a different coset of  $(q(x))$  in  $F[x]$ , proving that  $|F[x]/(q(x))| = p^n$ . Click for the detailed proof.

## 17. a

For simplicity we prove the case when  $k = 2$ ; the general case follows from this by some easy induction and noting that if we have, for rings  $R, R', P, P'$ , that  $R \cong R'$  and  $P \cong P'$ , then  $R \oplus P \cong R' \oplus P'$ ; for if  $\varphi$  is an isomorphism between  $R$  and  $R'$  and  $\tau$  is an isomorphism between  $P$  and  $P'$ , it is not hard to check that the map given by  $(r, p) \mapsto (\varphi(r), \tau(p))$  is an isomorphism between  $R \oplus P$  and  $R' \oplus P'$ .

### Step 2

2 of 4

Now, let

$$\psi : F[x] \rightarrow \frac{F[x]}{(p_1(x))} \oplus \frac{F[x]}{(p_2(x))}$$

be defined by  $\psi(f(x)) = (f(x) + (p_1(x)), f(x) + (p_2(x)))$ . This map is onto by the definition of quotient rings and it is a homomorphism with kernel equal to  $(p_1(x)) \cap (p_2(x))$  by **Problem 20** of section 3 of this chapter,

**Ideals, Homomorphisms, and Quotient Rings**.

Thus, by the first homomorphism theorem  $\psi$  is an isomorphism between

$$F[x]/((p_1(x)) \cap (p_2(x)))$$

and

$$\frac{F[x]}{(p_1(x))} \oplus \frac{F[x]}{(p_2(x))},$$

where our result follows if we prove that  $(p_1(x)) \cap (p_2(x)) = (q(x)) = (p_1(x)p_2(x))$ .

If  $p(x) \in (p_1(x)p_2(x))$  then

$$p(x) = p_1(x)p_2(x)w(x)$$

for some  $w(x) \in F[x]$ , so that  $p(x) \in (p_1(x))$  and  $p(x) \in (p_2(x))$ , proving the inclusion

$$(p_1(x)p_2(x)) \subseteq (p_1(x)) \cap (p_2(x)).$$

Now let  $t(x) \in (p_1(x)) \cap (p_2(x))$ , then there exist  $w_1(x), w_2(x) \in F[x]$  such that  $t(x) = w_1(x)p_1(x)$  and  $t(x) = w_2(x)p_2(x)$ . Note also that since  $p_1(x)$  and  $p_2(x)$  are distinct and irreducible, then

$$\gcd(p_1(x), p_2(x)) = 1$$

and thus by **Theorem 4.5.7.** there exist polynomials  $a(x), b(x) \in F[x]$  such that

$$p_1(x)a(x) + p_2(x)b(x) = 1.$$

But now

$$\begin{aligned} p_1(x)a(x)t(x) + p_2(x)b(x)t(x) &= t(x) \\ p_1(x)a(x)w_2(x)p_2(x) + p_2(x)b(x)tw_1(x)p_1(x) &= t(x) \\ p_1(x)p_2(x)(a(x)w_2(x) + b(x)w_1(x)) &= t(x) \end{aligned}$$

so that  $t(x) \in (p_1(x)p_2(x))$ , proving the inclusion

$$(p_1(x)) \cap (p_2(x)) \subseteq (p_1(x)p_2(x))$$

and finishing our proof.

## Result

4 of 4

We prove the case when  $k = 2$  and outline how the general case proceeds from it. The case  $k = 2$  proceeds by constructing a homomorphism

$$F[x] \rightarrow \frac{F[x]}{(p_1(x))} \oplus \frac{F[x]}{(p_2(x))}$$

via the **Problem 20** of section 3, and then concluding that this is an isomorphism after proving that  $(p_1(x)) \cap (p_2(x)) = (p_1(x)p_2(x))$  and using the first homomorphism theorem for rings. Click for the detailed proof.

18. a

Note that the given assertion is

**equivalent to the assertion that there are infinitely many irreducible polynomials in  $F[x]$**

, since there are only finitely many polynomials of degree  $< n$ , where  $n \in \mathbb{N}$ , as there is only finitely many choices for each coefficient.

Let us then suppose there are finitely many irreducible polynomials in  $F[x]$ , enumerate them as  $F_1(x), F_2(x), \dots, F_m(x)$ . Consider the polynomial

$$G(x) = F_1(x) \cdot F_2(x) \cdots F_m(x) + 1,$$

then by the uniqueness of factorization in  $F[x]$  we have that  $G(x)$  is either irreducible or a product of irreducible polynomials in  $F[x]$ . But none of  $F_i(x)$ ,  $i = 1, \dots, m$  can divide  $G$  because then we would obtain that an irreducible polynomial divides 1, which is impossible, since multiplication of a polynomial by a positive degree polynomial can never lower its degree. Thus  $F_i(x)$ ,  $i = 1, \dots, m$ , cannot be all the irreducible polynomials in  $F[x]$ . We have reached a contradiction, so our starting assumption that there are finitely many irreducible polynomials in  $F[x]$  is false.

## Result

2 of 2

We consider an assumption that there are finitely many irreducible polynomials, say  $F_1(x), \dots, F_m(x)$ , in  $F[x]$ , and use this to arrive at contradiction by considering divisors of  $G(x) = F_1(x) \cdots F_m(x) + 1$ . Click for more details.

## 19. a

By **Problem 16** it is sufficient to find an irreducible polynomial of degree 2 in  $\mathbb{Z}_p$ , i.e. to prove one such exists. To this end, we prove that the map  $\tau : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  given by

$$\tau(x) = x^2$$

is not surjective. Once we have proven this, then let  $t$  an element of  $\mathbb{Z}_p$  such that it is not in the image of  $\tau$ , then  $x^2 - t$  has no roots over  $\mathbb{Z}_p$  and thus is irreducible.

## Step 2

2 of 3

Note that a mapping from a finite set to itself is injective if and only if it is surjective (this is proven in **problems 28** and **29** of section 3, **Mappings**, of the first chapter), so that we can equivalently show  $\tau$  is not injective. But this is immediate since  $\tau(1) = 1$  and  $\tau(p-1) = \tau(-1) = 1$ , where we used the fact that  $p-1 \equiv -1 \pmod{p}$ . Following the procedure outlined in the first paragraph and the construction outlined in **Problems 15** and **16**, this gives our construction.

## Result

3 of 3

Following up on **Problem 16** the only missing gap for the construction is the proof that there exist an irreducible polynomial of degree 2 in  $\mathbb{Z}_p$  for any odd prime  $p$ . We prove this by considering the image of the map  $\tau : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  given by  $\tau(x) = x^2$ . Click for the detailed proof.

## 20. a

Let  $R$  be a Euclidean ring,  $I$  an ideal of  $R$ , and  $d$  be the function described in the definition of a Euclidean ring. Then as  $d(I \setminus \{0\})$ , the image of set  $I \setminus \{0\}$  under  $d$ , is a subset of natural numbers, so there is a least element in it, and then let  $a \in I \setminus \{0\}$  be such that it maps to that least element.

## Step 2

2 of 3

We claim that  $I = (a)$ . For let  $b \in I$ ,  $b \neq 0$ , then since  $R$  is Euclidean we have that

$$b = ac + r$$

for some  $c, r \in R$  such that either  $r = 0$  or  $r \neq 0$  and  $d(r) < d(a)$ . If the latter is true, then note that

$$r = b - ac,$$

where  $b \in I$  and  $ac \in I$ , so that  $r \in I$ , which contradicts the minimality of  $d(a)$ . So it follows that we must have  $r = 0$ , but then  $b = ac$  so that  $b \in (a)$ , proving that  $I \subseteq (a)$ . As the reverse inclusion is obvious, we arrive at

$$I = (a).$$

## Result

3 of 3

We consider an element of  $I \setminus \{0\}$  whose image under  $d$  is the smallest and prove that it generates  $I$ . Click for the detailed proof.

21. a

**Given:**  $R$  is an Euclidean ring.

**To Prove:**  $R$  has a unit element.

**Proof:** First of all we start with a Lemma.

**Lemma:** The elements of  $R$  of second smallest size are the units of  $R$ .

**Proof of the Lemma:** Suppose  $a \in R$  is of **second smallest size**.

Then write

$$1 = qa + r$$

for some  $q, r \in R$  with  $N(r) < N(a)$ .

**Since  $A$  has second smallest size,  $r$  must have smallest size**

so

$$r = 0.$$

Thus,

$$1 = qa, \text{ and } a \text{ is a unit.}$$

Now suppose that  $a$  is a unit, with  $ab = 1$ .

Then

$$N(a) \leq N(ab) = N(1) \leq N(a).$$

Thus

$$N(a) = N(1).$$

But we know that

**the size of 1 is second smallest**

, since

$$N(1) \leq N(1.x) = N(x)$$

for all  $x \in R$ .

Thus, the size of  $a$  is smallest second.

This completes the lemma.

Now by the given condition,  $R$  is an Euclidean ring ( $\neq 0$ ).

Then

**there must exists an element  $x \in R$  such that the size of  $x$  is smallest second**

. Then by above lemma  $x$  must be a unit.

This completes the proof.

## Result

3 of 3

By the aforesaid argument, the elements of  $R$  of second smallest size are the units of  $R$  and there must exists an element  $x \in R$  such that the size of  $x$  is smallest second, hence there exists a unit element in  $R$ .

[Click for the detailed proof.](#)

## 22. a

Let the two even numbers be 12 and 8. Then Euclid's algorithm not holding means that there do not exist even integers  $q$  and  $r$ , with  $0 \leq r < 8$ , such that

$$12 = 8q + r.$$

This is immediate upon noting that  $q$  must be greater than 0 (or else  $r > 8$ ), and also  $q$  must be smaller than 2 or else the right-hand side is greater than 12. So the only possible choice for  $q$  is 1, which is not an even number.

## Result

2 of 2

Take numbers 12 and 8. [Click for more details.](#)

## 23. a

By **Problem 11** we have that  $p(x)$  and  $q(x)$  are irreducible if they have no roots in  $\mathbb{Z}_7$ , which can easily be checked. E.g. for  $p(x)$  we have that  $p(0) = 5, p(1) = 6, p(2) = 6, p(3) = 4, p(4) = 6, p(5) = 4, p(6) = 4$ , and similarly for  $q(x)$ .

Again by consideration of **Problems 15** and **16** we have that every element of  $F[x]/(p(x))$  is equal to  $ax^2 + bx + c + (p(x))$ , and likewise for  $F[x]/(q(x))$ . We consider a map  $\tau : F[x]/(p(x)) \rightarrow F[x]/(q(x))$  given by

$$\tau(ax^2 + bx + c + (p(x))) = ax^2 - bx + c + (q(x)).$$

This map is obviously onto, and since  $|F[x]/(p(x))| = |F[x]/(q(x))| = 7^3$  by **Problem 16**, it is also one-to-one. We claim that it is a homomorphism. Additivity of  $\tau$  is immediate by the linearity of addition of polynomial coefficient, so we just have to check the multiplicativity; if  $n = ax^2 + bx + c + (p(x))$  and  $m = dx^2 + ex + f + (p(x))$  then

$$\begin{aligned}\tau(nm) &= \tau(adx^4 + (ae + bd)x^3 + (af + be + cd)x^2 + (bf + ce)x + cf + (p(x))) \\ &= \tau(2adx + 2(ae + bd) + (af + be + cd)x^2 + (bf + ce)x + cf + (p(x))) \\ &= \tau((af + be + cd)x^2 + (bf + ce + 2ad)x + (cf + 2ae + 2bd) + (p(x))) \\ &= (af + be + cd)x^2 - (bf + ce + 2ad)x + cf + 2ae + 2bd + (q(x)) \\ &= adx^4 - (ae + bd)x^3 + (af + be + cd)x^2 - (bf + ce)x + cf + (q(x)) \\ &= (ax^2 - bx + c + (q(x)))(dx^2 - ex + f + (q(x))) \\ &= \tau(n)\tau(m).\end{aligned}$$

where in the second equality we used that  $x^3 + p(x) = 2 + p(x)$  and in the fifth we used that  $x^3 + q(x) = -2 + q(x)$ .

## Result

3 of 3

We prove that  $\tau : F[x]/(p(x)) \rightarrow F[x]/(q(x))$  given by  $\tau(ax^2 + bx + c + (p(x))) = ax^2 - bx + c + (q(x))$  is an isomorphism. Click for more details.

## 24. a

First we show that  $\{a + b\alpha : a, b \in \mathbb{Q}\}$  is a field by showing that it is isomorphic to  $\mathbb{Q}[x]/(q(x))$ ; in particular, the isomorphism is given by  $\alpha \mapsto x + (q(x))$ .

Note that we know that  $\mathbb{Q}[x]/(q(x))$  is a field because  $q(x)$  has no roots in  $\mathbb{Q}$  and therefore it's irreducible over  $\mathbb{Q}$ . By reasoning analogous to that in previous **problems**, **15** and **16**, we know that each element of  $\mathbb{Q}[x]/(q(x))$  is given by  $a + bx + (q(x))$  for  $a, b \in \mathbb{Q}$ , so that our map described in the first paragraph extends linearly to  $\tau(a + b\alpha) = a + bx + (q(x))$ . Only nonobvious property to show that  $\tau$  is an isomorphism is multiplicativity, for additivity follows by linearity and surjectivity and injectivity quickly follow by noting that different choices of  $a, b$  correspond to different elements in both  $\mathbb{Q}[x]/(q(x))$  and  $\{a + b\alpha : a, b \in \mathbb{Q}\}$ .

So then

$$\begin{aligned}\tau((a + b\alpha)(c + d\alpha)) &= \tau(ac + ada\alpha + bca\alpha + bda\alpha^2) \\ &= \tau(ac + (ad + bc)\alpha + bd(-1 - \alpha)) \\ &= \tau(ac - bd + (ad + bc - bd)\alpha) \\ &= ac - bd + (ad + bc - bd)x + (q(x)) \\ &= ac - bd + (ad + bc)x - bdx + (q(x)) \\ &= ac - bd + (ad + bc)x - bd(-1 - x^2) + (q(x)) \\ &= ac + (ad + bc)x + bdx^2 + (q(x)) \\ &= (a + bx + q(x))(c + dx + q(x)) \\ &= \tau(a + b\alpha)\tau(c + d\alpha).\end{aligned}$$

In order to show it in the second way, note that  $\{a + b\alpha : a, b \in \mathbb{Q}\}$  is a subring of  $\mathbb{C}$  which obviously contains 0, 1, additive inverses, and inherits associativity/commutativity of addition and multiplicativity from  $\mathbb{C}$ . Thus this is why it is sufficient for us to prove that it's closed under multiplicative inverses. To find this, we investigate when, for which  $a, b \in \mathbb{Q}$ , there exist  $c, d$  such that

$$\begin{aligned}(a + b\alpha)(c + d\alpha) &= 1 \\ ac + ada\alpha + bca\alpha + bd\alpha^2 &= 1 \\ ac + ada\alpha + bca\alpha + bd(-1 - \alpha) &= 1 \\ ac - bd + (ad + bc - bd)\alpha &= 1\end{aligned}$$

where, since  $\alpha \notin \mathbb{Q}$ , we have that we must have  $ac - bd = 1$  and  $ad + bc - bd = 0$ . If  $a = b = 0$ , then obviously our system has no solutions, so assume at least one of them is distinct from 0, say  $b$ . Then the second equation implies

$$c = \frac{bd - ad}{b},$$

and substituting this into the first equation we get

$$\begin{aligned}a \left( \frac{bd - ad}{b} \right) - bd &= 1 \\ abd - a^2d - b^2d &= b \\ d(ab - a^2 - b^2) &= b.\end{aligned}$$

Since we can take inverses of nonzero elements in  $\mathbb{Q}$ , this implies that the system is solvable (in the  $b \neq 0$  case, but it is completely analogous in the  $a \neq 0$  case) if and only if  $ab - a^2 - b^2 \neq 0$ , which is in turn equivalent to  $2(a^2 - ab + b^2) \neq 0$ . We have that

$$2a^2 - 2ab + 2b^2 = a^2 + b^2 + a^2 - 2ab + b^2 = a^2 + b^2 + (a - b)^2,$$

where all terms are nonnegative so that it is equal to zero if and only if  $a = b = 0$ , finishing our proof.

## Result

3 of 3

For the first method we check that map given by  $\tau(a + b\alpha) = a + bx + (q(x))$  is an isomorphism, while for the second one we investigate the solvability of  $(a + b\alpha)(c + d\alpha) = 1$ . Click for more details.

25. a

**To Prove:**  $f(x) = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1$  is irreducible over  $\mathbb{Q}[x]$ , if  $p$  is a prime.

## Step 2

2 of 4

**Proof:**

**Lemma:** Let  $F$  be a field and  $f(x) \in F[x]$ . If  $c \in F$  and  $f(x+c)$  is irreducible in  $F[x]$ , then  $f(x)$  is irreducible in  $F[x]$ .

**Proof of the Lemma:** Suppose that  $f(x)$  is reducible, i.e., there exist **non-constant**  $g(x), h(x) \in F[x]$  so that

$$f(x) = g(x)h(x).$$

In particular, then we have

$$f(x+c) = g(x+c)h(x+c).$$

Note that  $g(x+c)$  and  $h(x+c)$

**have the same degree at  $g(x)$  and  $h(x)$  respectively; in particular, they are non-constant polynomials**

So our assumption is wrong.

Hence,  $f(x)$  is irreducible in  $F[x]$ .

This proves our Lemma.

Now recall the identity

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1.$$

We prove that  $f(x+1)$  is

**irreducible in  $\mathbb{Q}[x]$  and then apply the Lemma to conclude that  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .**

Note that

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{x^p + px^{p-1} + \dots + px}{x} \\ &= x^{p-1} + px^{p-2} + \dots + p. \end{aligned}$$

Using that the

**binomial coefficients occurring above are all divisible by  $p$ , we have that  $f(x+1)$  is irreducible in  $\mathbb{Q}[x]$  by Eisenstein's criterion applied with prime  $p$ .**

Then by Lemma  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .

This completes the proof.

## Result

Being  $f(x+1)$  is irreducible in  $\mathbb{Q}[x]$ , we have proved that the given  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .

Click for the complete proof.

26. a

Let  $q(x) \in R[x]$  be a zero divisor,

$$q(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m$$

where  $a_0 \neq 0$ , and let  $p(x) \in R[x]$  such that  $q(x)p(x) = 0$ ,

$$p(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m,$$

where  $b_0 \neq 0$ .

## Step 2

2 of 4

Since polynomials are equal iff their coefficient are equal, we have that all the coefficient of  $q(x)p(x)$  are equal to 0, so by the definition of the matrix multiplication

$$c_{m+n-i} = \sum_{j=0}^i a_j b_{i-j} = 0$$

for all  $i \leq m+n$ , where we define  $a_j = 0$  for  $j > n$  and  $b_j = 0$  for  $j > m$ .

If  $i = 0$  we get that

$$c_{m+n} = a_0 b_0 = 0,$$

from which it is naturally to consider  $b_0$  as our candidate for  $b$ . Indeed we have that for  $i = 1$ ,  $c_{m+n-1} = a_0 b_1 + a_1 b_0 = 0$ , where multiplying by  $b_0$  we get that

$$\begin{aligned} a_0 b_1 b_0 + a_1 b_0 b_0 &= 0 \\ a_1 b_0^2 &= 0, \end{aligned}$$

But if  $a_1 b_0^2 = 0$ , then, as  $R$  is commutative,

$$(a_1 b_0)^2 = a_1 b_0 a_1 b_0 = a_1 (a_1 b_0^2) = 0, \quad (1)$$

so that  $a_1 b_0 = 0$ . Similarly, if  $i = 2$ ,  $c_{m+n-2} = a_0 b_2 + a_1 b_1 + a_2 b_0 = 0$ , where multiplying by  $b_0$  and using  $a_0 b_0 = a_1 b_0 = 0$ , we get

$$\begin{aligned} a_0 b_2 b_0 + a_1 b_1 b_0 + a_2 b_0 b_0 &= 0 \\ a_2 b_0^2 &= 0 \end{aligned}$$

where we can repeat the reasoning of (1) to arrive at  $a_2 b_0 = 0$ .

In general, if we have obtained that  $a_0 b_0 = 0, a_1 b_0 = 0, \dots, a_{k-1} b_0 = 0$ , then

$$c_{m+n-k} = \sum_{j=0}^k a_j b_{i-j} = 0$$

from which by multiplying by  $b_0$  we get

$$\sum_{j=0}^k a_j b_{i-j} b_0 = 0$$
$$a_k b_0^2 = 0,$$

from where we get  $a_k b_0 = 0$ , which (by commutativity of multiplication in  $R$ , i.e.  $a_k b_0 = b_0 a_k$ ) finishes our proof.

## Result

4 of 4

If  $q(x)$  is a zero divisor with  $p(x) \in R[x]$  such that  $q(x)p(x)$ , where  $p(x) = b_0 x^m + b_1 x^{m-1} + \cdots + b_{m-1} x + b_m$ , we show  $b_0$  is an element of  $R$  which satisfies our requirements. Click for the detailed proof.

27. a

### (a)

It is immediate that  $I[x]$  is an additive subgroup of  $R[x]$  since  $I$  is an additive subgroup of  $R$  and coefficient addition of polynomials is done by adding their corresponding coefficients, so at any point we're only dealing with addition in  $I$ .

To show that it is closed under multiplication by elements of  $R[x]$ , note that if  $q(x) \in I[x]$  and  $p(x) \in R[x]$ , then each coefficient of  $q(x)p(x)$  is a sum of the elements of the form  $a_i b_j$ , where  $a_j$  is a coefficient of  $q(x)$ , and thus  $a_i \in I$ , and  $b_j$  is a coefficient of  $p(x)$ , so that since  $I$  is an ideal  $a_i b_j \in I$ . Since  $I$  is an additive subgroup and thus closed under finite summations, we are finished.

### (b)

We define a mapping  $\tau : R[x] \rightarrow (R/I)[x]$  by

$$\tau(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = (a_n + I)x^n + (a_{n-1} + I)x^{n-1} + \cdots + (a_1 + I)x + (a_0 + I).$$

This is obviously onto by the definition of the quotient  $R/I$ , and it is immediate from the definition of addition and multiplication in quotient rings that  $\tau$  is a homomorphism, since  $(a_i + I) + (a_j + I) = (a_i + a_j) + I$  and  $(a_i + I)(a_j + I) = (a_i a_j) + I$ .

Now, if we prove that  $\ker \tau = I[x]$  then we are done by the first homomorphism theorem for rings.

If  $p(x) \in \ker \tau$ ,  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ , then  $a_n + I = 0 + I$ ,  $a_{n-1} + I = 0 + I$ ,  $\vdots$ ,  $a_0 + I = 0 + I$ , so that  $a_i \in I$  for  $i = 0, 1, \dots, n$ , but then  $p(x) \in I[x]$ . Equivalently, if  $p(x) \in I[x]$ , then all its coefficients are in  $I$ , so that  $\tau(p(x)) = 0$ , proving that  $\ker \tau = I[x]$  and finishing our proof.

## Result

3 of 3

The (a) part is an easy consequence of definition of polynomial addition and multiplication, why for the (b) part we construct an onto homomorphism  $\tau : R[x] \rightarrow (R/I)[x]$  with  $\ker \tau = I[x]$ , where we are finishes by the first homomorphism theorem for rings. Click for the detailed proof.

28. a

If  $q(x) \in R[x]$ ,

$$q(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

is a zero divisor, then there exists  $p(x)$ ,

$$p(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m$$

of the lowest degree  $m$  such that  $q(x)p(x) = 0$ . Furthermore,  $b_m \neq 0$ , for if  $b_m = 0$  then

$$\begin{aligned} q(x)(b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x) &= 0 \\ q(x)(b_0x^{m-1} + b_1x^{m-2} + \cdots + b_{m-1})x &= 0. \end{aligned}$$

Now, as it is easy to show  $x$  is not a zero divisor in  $R[x]$ , for multiplication by  $x$  cannot turn any nonzero coefficients into zero coefficients, it follows that

$$q(x)(b_0x^{m-1} + b_1x^{m-2} + \cdots + b_{m-1}) = 0,$$

contradicting the minimality of  $m$ .

Now from  $q(x)p(x) = 0$  we get that  $a_n b_m = 0$ . We claim that  $b_m$  satisfies our requirements. Let  $k < n$  be the smallest  $k$  such that  $a_k b_m = 0$  and  $a_j b_m = 0$  for all  $j$  such that  $n \geq j > k$ . If  $k = 0$  then we are done, so suppose  $k > 0$ , so that  $a_{k-1} b_m \neq 0$  and that for any  $j \geq k$  we have

$$\begin{aligned} p(x)a_j &= b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m \\ &= b_0a_jx^m + b_1a_jx^{m-1} + \cdots + b_{m-1}a_jx \\ &= (b_0a_jx^{m-1} + b_1a_jx^{m-2} + \cdots + b_{m-1}a_j)x. \end{aligned}$$

But also since  $q(x)p(x) = 0$  then  $q(x)p(x)a_j = 0$ , and thus since  $x$  is again not a zero-divisor in  $R[x]$ , then

$$q(x)(b_0a_jx^{m-1} + b_1a_jx^{m-2} + \cdots + b_{m-1}a_j) = 0,$$

where by the minimality of  $m$  we have that  $b_0a_j = 0, b_1a_j = 0, \dots, b_{m-1}a_j = 0$ . Since for every  $j \geq k$  we have that  $b_i a_j = 0$  for  $i = 0, 1, \dots, m$ , then also  $p(x)a_j = 0$ , or  $a_j p(x) = 0$  by commutativity of  $R$ . Therefore

$$\begin{aligned} 0 &= q(x)p(x) \\ &= (a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n)p(x) \\ &= a_0p(x)x^n + a_1p(x)x^{n-1} + \cdots + a_{n-1}p(x)x + a_np(x) \\ &= a_0p(x)x^n + \cdots a_{k-1}p(x)x^{n-k+1} \\ &= (a_0x^n + \cdots a_{k-1}x^{n-k+1})p(x) \\ &= (a_0x^n + \cdots a_{k-1}x^{n-k+1})(b_0x^m + b_1x^{m-1} + \cdots + b_m). \end{aligned}$$

But since the coefficient of  $x^{n-k+1}$  is  $a_{k-1}b_m$  this implies that  $a_{k-1}b_m = 0$ , contradicting our assumption. Thus  $k = 0$  and our proof is finished.

## Result

3 of 3

We take  $p(x)$  such that  $q(x)p(x)$  and  $p(x)$  is in the lowest degree and prove that the constant coefficient of  $p(x)$  satisfies our requirements. Click for the proof.

29. a

First we prove the easy part, the part **(a)**, which follows from simply writing everything out. If  $a = x + iy$  and  $b = w + iz$  then

$$d(a) = x^2 + y^2$$

and

$$\begin{aligned} d(ab) &= d((xw - yz) + (xz + wy)i) \\ &= (xw - yz)^2 + (xz + wy)^2 \\ &= (xw)^2 - 2(xwyz) + (yz)^2 + (xz)^2 + 2(xzwy) + (wy)^2 \\ &= (xw)^2 + (yz)^2 + (xz)^2 + (wy)^2 \\ &= (x^2 + y^2)(w^2 + z^2). \end{aligned}$$

Now since  $w$  and  $z$  are integers out of which at least one is nonzero, we have that  $w^2 + z^2 \geq 1$ , which implies

$$d(a) \leq d(ab).$$

Note that our calculations actually prove that  $d(ab) = d(a)d(b)$  for any complex numbers  $a, b$ . In particular this also proves that for nonzero complex number  $a$ ,  $d(a^{-1}) = d(a)^{-1}$  where the inverse on the left-hand side is in the complex numbers and the inverse on the right side is in the real numbers.

We give a geometric proof of **(b)**. First note that the Gaussian integers form a lattice in the complex plane  $\mathbb{C}$ , where a complex number  $a + bi$  is thought of as a point  $(a, b)$  in the plane  $\mathbb{R}^2$ . Thus Gaussian integers partition the complex plan, identifying it for a second with the real plane  $\mathbb{R}^2$ , into  $1 \times 1$  squares with their vertices at points  $(a, b)$ ,  $a, b$  integers.

We need to prove that for  $a \neq 0, b \neq 0, a, b \in R$ , there exist  $q$  and  $r \in R$  such that

$$b = qa + r \tag{1}$$

where  $r = 0$  or

$$d(r) < d(a). \tag{2}$$

Dividing by  $a$  through (1) we get

$$\frac{b}{a} - q = \frac{r}{a}.$$

But also dividing by  $d(a)$  through (2) and using the result of the first paragraph we get that (2) is equivalent to  $d\left(\frac{r}{a}\right) < 1$ . This it is sufficient to find  $q \in R$  such that

$$d\left(\frac{b}{a} - q\right) < 1.$$

This is where geometry comes into play. Note that  $\sqrt{d(a - b)}$  gives the Euclidean distance of complex numbers  $a = x + iy$ ,  $b = w + iz$  thought of as points  $(x, y)$  and  $(w, z)$ , and also note that  $d\left(\frac{b}{a} - q\right) < 1$  is equivalent to

$$\sqrt{d\left(\frac{b}{a} - q\right)} < \sqrt{1} = 1$$

Now inspecting the location of the complex number  $a/b$ , and noting the kind of lattices that Gaussian integers make (see the second paragraph), we note that there is some Gaussian integer  $q$  such that the distance between  $\frac{b}{a}$  is not greater than half the length of the diagonal of a  $1 \times 1$  square, i.e. not greater than  $\frac{1}{2}\sqrt{2}$ . But now our results follows simply by noting that  $\frac{1}{2}\sqrt{2} < 1$ .

## Result

3 of 3

The part (a) follows from writing everything out, while we give a geometric proof of the part (b), thinking of Gaussian integers as forming a lattice in the complex plane.

# Section 4–6

## 1. a

Suppose that  $g(x) = f(x + 1)$  is irreducible but that  $f(x)$  isn't. Then there are polynomials  $f_1(x)$ ,  $f_2(x)$ ,  $\deg f_1(x) > 0$  and  $\deg f_2(x) > 0$  such that  $f(x) = f_1(x)f_2(x)$ . But then also

$$g(x) = f(x + 1) = f_1(x + 1)f_2(x + 1).$$

Now, if we prove that for a  $p(x) \in \mathbb{Q}[x]$  we have that  $\deg p(x) = \deg p(x + 1)$ , this would imply that  $g(x)$  is reducible, which is a contradiction.

## Step 2

2 of 3

So let

$$p(x) = a_n x^n + \dots + a_0,$$

$a_n \neq 0$ , so that  $\deg p(x) = n$ , then

$$\begin{aligned} p(x + 1) &= a_n(x + 1)^n + \dots + a_0 \\ &= a_n x^n + (\text{terms of the form } kx^j \text{ with } j < n) \end{aligned}$$

so that  $\deg p(x + 1) = n$ , which finishes our proof.

## Result

We suppose that  $f(x)$  is reducible and reach a contradiction. Click for the proof.

## Method 2.

(1). Let  $g(x)$  is irreducible in  $\mathbb{Q}[x]$ .  
 $g(x) = f(x+1)$ .  
let if possible  $f(x)$  is reducible  
 $\Rightarrow f(x) = f_1(x) f_2(x)$  for  $\deg f_1(x)$ ,  
 $\deg f_2(x) < 4$ .  
 $\Rightarrow g(x) = f_1(x+1) f_2(x+1)$   
s.t.  $\deg f_1(x+1), \deg f_2(x+1) < 4$   
 $\Rightarrow g(x)$  is reducible.  
which is in contradiction  
 $\Rightarrow$   $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .

## 2. a

Given:  $f(x) = x^3 + 3x + 2$  is a polynomial in  $\mathbb{Q}[x]$ .

To Prove:  $f(x)$  is **Irreducible** in  $\mathbb{Q}[x]$ .

### Step 2

2 of

**Proof:** Let us assume that  $f(x)$  is **reducible** over  $\mathbb{Q}[x]$ .

Then there exists a rational root of  $f(x)$ .

Let  $p/q$  be a **rational root** of  $f(x)$ , where  $\gcd(p, q) = 1$ .

Then  $f(p/q) = 0$ .

Now,

$$f(p/q) = (p/q)^3 + 3(p/q) + 2 \implies (p/q)^3 + 3(p/q) + 2 = 0 \implies p^3 + 3pq^2 = -2q^3 \implies p(p^2 + 3q^2) = -q^3$$

It follows that,

$p$  divides  $q$  which is a contradiction to the fact that  $\gcd(p, q) = 1$

This implies that  $f(x)$  has **no rational root**.

Now we know that,

**a polynomial of degree two or three over a field  $F$  is reducible if and only if it has a root in  $F$ .**

Now  $f(x)$  is a 3 degree polynomial having no root in  $\mathbb{Q}$ .

So,  $f(x)$  is **Irreducible** in  $\mathbb{Q}[x]$ .

This completes the proof.

## 3. a

Via **Eisenstein's criterion** and observation that 5 divides 15 and  $-30$ , it is sufficient to find infinitely many  $a$  such that 5 divides  $a$ , but  $5^2 = 25$  doesn't divide  $a$ . For example  $5 \cdot 2^k$  for  $k = 0, 1, \dots$  is one such infinite sequence.

### Result

2 of 2

We use Eisenstein's criterion to suggest  $a = 5 \cdot 2^k$  for  $k = 0, 1, \dots$  Click for more details.

#### 4. a

Let  $g(x) = a_0^{n-1}f(x)$ , then

$$\begin{aligned} g(x) &= a_0^n x^n + a_0^{n-1} a_1 x^{n-1} + a_0^{n-1} x^{n-2} + \cdots + a_0^{n-1} a_{n-1} x + a_0^{n-1} a_n \\ &= (a_0 x)^n + a_1 (x a_0)^{n-1} + a_0 a_2 (a_0 x)^{n-2} + \cdots + a_0^{n-2} a_{n-1} (a_0 x) + a_0^{n-1} a_n, \end{aligned}$$

so that with substitution  $y = a_0 x$  we get

$$g(x) = h(y) = y^n + a_1 y^{n-1} + a_0 a_2 y^{n-2} + \cdots + a_0^{n-2} a_{n-1} y + a_0^{n-1} a_n.$$

Now, by hypothesis  $p \mid a_1, p \mid a_2, \dots, p \mid a_n$ , and so  $p \mid a_1, p \mid a_0 a_2, \dots, p \mid a_0^{n-1} a_n$ . Moreover, because  $p \nmid a_0$ , then also  $p \nmid a_0^{n-1}$  and so  $p^2 \nmid a_0^{n-1} a_n$ . Now the hypotheses of Eisenstein Criterion are satisfied, so that  $h(y)$  is irreducible and then so are  $g(x)$  and  $f(x)$ .

#### Result

2 of 2

We perform a transformation of  $f$  so that we can apply the ordinary Eisenstein Criterion to it. Click for more details.

#### 5. a

**To Prove:**  $f(x) = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1$  is irreducible over  $\mathbb{Q}[x]$ , if  $p$  is a prime.

##### Proof:

**Lemma:** Let  $F$  be a field and  $f(x) \in F[x]$ . If  $c \in F$  and  $f(x+c)$  is irreducible in  $F[x]$ , then  $f(x)$  is irreducible in  $F[x]$ .

**Proof of the Lemma:** Suppose that  $f(x)$  is reducible, i.e., there exist **non-constant**  $g(x), h(x) \in F[x]$  so that

$$f(x) = g(x)h(x).$$

In particular, then we have

$$f(x+c) = g(x+c)h(x+c).$$

Note that  $g(x+c)$  and  $h(x+c)$

**have the same degree at  $g(x)$  and  $h(x)$  respectively; In particular, they are non-constant polynomials**

So our assumption is wrong.

Hence,  $f(x)$  is irreducible in  $F[x]$ .

This proves our Lemma.

Now recall the identity

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1.$$

We prove that  $f(x+1)$  is

**Irreducible in  $\mathbb{Q}[x]$  and then apply the Lemma to conclude that  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .**

Note that

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{x^p + px^{p-1} + \dots + px}{x} \\ &= x^{p-1} + px^{p-2} + \dots + p. \end{aligned}$$

Using that the

**binomial coefficients occurring above are all divisible by  $p$ , we have that  $f(x+1)$  is irreducible in  $\mathbb{Q}[x]$  by Eisenstein's criterion applied with prime  $p$ .**

Then by Lemma  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .

This completes the proof.

Being  $f(x+1)$  is irreducible in  $\mathbb{Q}[x]$  we prove that  $f(x) = x^{p-1} + x^{p-2} + \dots + x^2 + x + 1$  is irreducible over  $\mathbb{Q}[x]$ , if  $p$  is a prime.

Click for the detailed proof.

## 6. a

Note that if

$$f(x) = f_1(x)f_2(x)$$

is a factorization of  $f(x)$  then by the multiplicative property of homomorphisms

$$g(x) = \varphi(f(x)) = \varphi(f_1(x))\varphi(f_2(x))$$

is a factorization of  $g(x)$ . Now we are done if we show that  $\varphi$  sends constants to constants (and it does, by the hypothesis) and that  $\varphi$  sends positive degree polynomials to positive degree polynomials.

### Step 2

2 of 3

Suppose that  $\varphi$  sent a polynomial  $p(x)$  to a constant  $c$ , i.e.  $\varphi(p(x)) = c$ ; but note that we also have  $\varphi(c) = c$ , and as  $\varphi$  is an automorphism and therefore one-to-one, we have that  $p(x) = c$ . So as  $\varphi$  cannot send a positive degree polynomial to a constant, it has to send it to a positive degree polynomial, finishing our proof.

### Result

3 of 3

We note that if we have a factorization of  $f(x)$  in  $F[x]$  then  $\varphi$  gives a factorization of  $g(x)$  in  $F[x]$ , and we finish off the proof by proving that  $\varphi$  sends constants to constants and positive degree polynomials to positive degree polynomials.

## 7. a

If  $f(x)$  is a constant polynomial, i.e.  $f(x) = a$  for  $a \in F$ , then  $f(x+1) = a$ , which shows that  $\varphi(a) = a$ .

2 of 4

## Step 2

Now we prove that  $\varphi$  is one-to-one and onto. Firstly, if  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  is in  $F[x]$ , then  $g(x) = a_n(x-1)^n + a_{n-1}(x-1)^{n-1} + \dots + a_1(x-1) + a_0$  is also in  $F[x]$  and we have that  $\varphi(g(x)) = f(x)$ , proving that  $f$  is onto.

If  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  and  $g(x) = b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$  are polynomials in  $F[x]$  such that  $\varphi(f(x)) = \varphi(g(x))$ , then note that we can write

$$f(x) = a'_n(x-1)^n + a'_{n-1}(x-1)^{n-1} + \dots + a'_1(x-1) + a'_0$$

and

$$g(x) = b'_n(x-1)^n + b'_{n-1}(x-1)^{n-1} + \dots + b'_1(x-1) + b'_0$$

for some  $a'_n, \dots, a'_0, b'_n, \dots, b'_0$  in  $F$ . This essentially follows from writing  $\varphi(f(x)) = f(x+1) = c_nx^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$ , and making a substitution  $y = x+1$ .

But then  $\varphi(f(x)) = \varphi(g(x))$  implies that  $a'_n = b'_n, \dots, a'_0 = b'_0$ , so that  $f(x) = g(x)$ .

Finally we show that it is a homomorphism by proving that it's additive and multiplicative. Let  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  and  $g(x) = b_mx^m + b_{m-1}x^{m-1} + \dots + b_1x + b_0$  be polynomials in  $F[x]$ . We also define  $a_i = 0$  for every  $i > n$  and  $b_j = 0$  for every  $j > m$ . Then

$$\begin{aligned} \varphi(f(x) + g(x)) &= \varphi((a_{n+m} + b_{n+m})x^{n+m} + (a_{n+m-1} + b_{n+m-1})x^{n+m-1} \\ &\quad + \dots + (a_1 + b_1)x + (a_0 + b_0)) \\ &= (a_{n+m} + b_{n+m})(x+1)^n + (a_{n+m-1} + b_{n+m-1})(x+1)^{n+m-1} \\ &\quad + \dots + (a_1 + b_1)(x+1) + (a_0 + b_0) \\ &= a_n(x+1)^n + a_{n-1}(x+1)^{n-1} + \dots + a_1(x+1) + a_0 \\ &\quad + b_m(x+1)^m + b_{m-1}(x+1)^{m-1} + \dots + b_1(x+1) + b_0 \\ &= \varphi(f(x)) + \varphi(g(x)). \end{aligned}$$

Also

$$\begin{aligned} \varphi(f(x)g(x)) &= \varphi\left(\sum_{i=0}^{n+m} \sum_{j=0}^i a_{i-j}b_j x^i\right) \\ &= \sum_{i=0}^{n+m} \sum_{j=0}^i a_{i-j}b_j (x+1)^i \\ &= \sum_{i=0}^n a_i(x+1)^i \sum_{j=0}^m b_j(x+1)^j \\ &= \varphi(f(x))\varphi(g(x)), \end{aligned}$$

where the third equality can be justified by substituting  $x+1 = y$  and using the definition of polynomial multiplication.

## Result

4 of 4

We straightforwardly check that  $\varphi(a) = a$  for every  $a \in F$ , then prove that  $\varphi$  is one-to-one and onto, and lastly check that it has additive and multiplicative properties to confirm it is a homomorphism. Click for the detailed proof.

## 8. a

This is the  $c = 0$  case of **Problem 9**. See it for a proof.

## Result

This is a special case of **Problem 9**, when  $c = 0$ . See the solution of **Problem 9**.

### 9. a

If  $f(x) = a$ ,  $a \in F$ , then  $f(bx + c) = a$ , so that  $\varphi(a) = a$ .

Now we prove that  $\varphi$  is one-to-one and onto. If  $f(x) \in F[x]$ ,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

then the polynomial  $g(x)$  given by

$$g(x) = a_n \left( \frac{x-c}{b} \right)^n + a_{n-1} \left( \frac{x-c}{b} \right)^{n-1} + \cdots + a_1 \left( \frac{x-c}{b} \right) + a_0$$

is also in  $F[x]$  and  $\varphi(g(x)) = f(x)$ , so that  $\varphi$  is onto.

Now suppose  $\varphi(f(x)) = \varphi(g(x))$ , where

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0.$$

Note that we can write

$$f(x) = a'_n \left( \frac{x-c}{b} \right)^n + a'_{n-1} \left( \frac{x-c}{b} \right)^{n-1} + \cdots + a'_1 \left( \frac{x-c}{b} \right) + a'_0$$

and

$$g(x) = b'_n \left( \frac{x-c}{b} \right)^n + b'_{n-1} \left( \frac{x-c}{b} \right)^{n-1} + \cdots + b'_1 \left( \frac{x-c}{b} \right) + b'_0$$

for some  $a'_n, \dots, a_0, b'_n, \dots, b'_0 \in F$ . This is essentially a consequence of going in reverse direction from that which we went when we were proving that it is onto, for  $\varphi(f(x)) = f(bx + c) = c_n x^n + \cdots + c_1 x + c_0$ , and then our rewrite of  $f(x)$  follows from making a substitution  $bx + c = y$  and solving for  $x$ . Now  $\varphi(f(x)) = \varphi(g(x))$  implies that  $a'_n = b'_n, \dots, a'_0 = b'_0$ , but then  $f(x) = g(x)$ .

Now we show that  $\varphi$  is homomorphism by showing that it's additive and multiplicative. Additivity just follows straightforwardly by linearity of coefficient addition in polynomials. See solution of **Problem 7** to see how it goes. Multiplicativity also goes smoothly, for if  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  and  $g = b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$  then

$$\begin{aligned}\varphi(f(x)g(x)) &= \varphi\left(\sum_{i=0}^{n+m} \sum_{j=0}^i a_{i-j}b_j x^i\right) \\ &= \sum_{i=0}^{n+m} \sum_{j=0}^i a_{i-j}b_j \left(\frac{x-c}{b}\right)^i \\ &= \sum_{i=0}^n a_i \left(\frac{x-c}{b}\right)^i \sum_{j=0}^m b_j \left(\frac{x-c}{b}\right)^j \\ &= \varphi(f(x))\varphi(g(x)),\end{aligned}$$

where the third equality is a result of making a substitution  $y = \frac{x-c}{b}$ , using the definition of polynomial multiplication, and then resubstituting  $y = \frac{x-c}{b}$ .

## Result

3 of 3

We directly prove that  $\varphi$  is an one-to-one and onto homomorphism for which  $\varphi(a) = a$  for  $a \in F$ . Click for the detailed proof.

## 10. a

It is obviously sufficient to prove that  $\varphi(x)$  is a polynomial of degree 1, for then

$$\varphi(a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0) = a_n\varphi(x)^n + a_{n-1}\varphi(x)^{n-1} + \dots + a_1\varphi(x) + a_0$$

is a polynomial of degree  $n$ .

### Step 2

2 of 3

Suppose now that  $\deg \varphi(x) = m > 1$ , then for any polynomial  $b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$ ,  $b_n \neq 0$  and  $n \geq 1$ , then

$$\varphi(b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0) = b_n\varphi(x)^n + b_{n-1}\varphi(x)^{n-1} + \dots + b_1\varphi(x) + b_0,$$

but this is a polynomial of degree  $mn > 1$ . Thus, if  $\deg \varphi(x) > 1$  then the image of any nonconstant polynomial has degree  $> 1$ , and every constant polynomial just gets mapped to itself, which contradicts the fact that  $\varphi$  is an automorphism and thus onto.

## Result

3 of 3

We show it's sufficient to show that  $\varphi(x)$  has degree 1, and then prove it by assuming to contrary and showing that would force an image of any nonconstant polynomial to be of degree  $> 1$ . Click for the detailed proof.

## 11. a

In **Problem 10** we proved that  $\varphi(x)$  must be of degree 1, thus that there exist  $b, c \in F$ ,  $b \neq 0$ , such that  $\varphi(x) = bx + c$ . But then if  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$  we have that

$$\begin{aligned}\varphi(f(x)) &= a_n \varphi(x)^n + a_{n-1} \varphi(x)^{n-1} + \cdots + a_1 \varphi(x) + a_0 \\ &= a_n(bx + c)^n + a_{n-1}(bx + c)^{n-1} + \cdots + a_1(bx + c) + a_0 \\ &= f(bx + c),\end{aligned}$$

which is what we needed to prove.

## Result

2 of 2

We use the result of **Problem 10** in which we showed that  $\varphi(x)$  must be of degree 1. Click for more details.

## 12. a

From previous exercises we have that the mapping  $\varphi : \mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$  given by  $\varphi(f(x)) = f(bx + c)$ , where  $b \neq 0$ , **is an automorphism**.

We investigate whether any automorphism of that form satisfies our requirement; from  $\varphi^2$  being identity we infer that we need

$$b(bx + c) = x, \text{ i.e. } b^2x + bc = x.$$

Since polynomials are equal if and only if all their coefficients are equal, this necessitates  $b^2 = 1$  and  $bc = 0$ .

There are two solutions of this system:  $b = 1$  and  $c = 0$ , which yields the identity automorphism, and

$$b = -1 \text{ and } c = 0$$

, which doesn't yield the identity automorphism, so it satisfies our requirements.

## Result

2 of 2

Such an automorphism is given by  $\varphi(f(x)) = f(-x)$ . Click for more details.

## 13. a

Let  $\varphi$  an arbitrary automorphism of  $\mathbb{Q}[x]$ . Since

$$\varphi(0) + \varphi(0) = \varphi(0 + 0) = \varphi(0)$$

we know that  $\varphi(0) = 0$ , and since

$$1 = \varphi(a)\varphi(a)^{-1} = \varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1)$$

we know that  $\varphi(1) = 1$ .

Furthermore, if  $n$  is a natural number then we can write as a sum of  $n$  1s, i.e.  $n = 1 + \dots + 1$ , so that

$$\varphi(n) = \varphi(1 + \dots + 1) = \varphi(1) + \dots + \varphi(1) = n.$$

We also have that

$$1 = \varphi(1) = \varphi((-1)(-1)) = \varphi(-1)\varphi(-1) = \varphi(-1)^2,$$

so that  $\varphi(-1)$  is either 1 or  $-1$ , but it cannot be 1 due to  $\varphi$  being an automorphism and therefore one-to-one.

From this it now also follows that  $\varphi(k) = k$  for any integer  $k$ . Finally, if  $q \in \mathbb{Q}$ , then  $q = a/b$  for integers  $a, b$ , so that

$$\varphi(q) = \varphi(a)/\varphi(b) = a/b = q.$$

## Result

2 of 2

We use properties of an automorphism  $\mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$  to first prove that it first fixed all the natural numbers, then the integers and finally all the rational numbers. Click for more details.

## 14. a

If  $n = 1$  then just take the identity mapping, and for an integer  $n > 1$ , let

$$\zeta_n = e^{2\pi i/n} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n},$$

then basics of arithmetic with complex numbers show that  $\zeta_n^n = 1$  and that  $\zeta_n^k \neq 1$  for  $k = 1, \dots, n-1$ .

## Step 2

2 of 3

Define a map  $\varphi : \mathbb{C}[x] \rightarrow \mathbb{C}[x]$  given by

$$\varphi(f(x)) = f(\zeta_n x).$$

Then by reasoning completely analogously as we did in **Problem 9** we have that  $\varphi$  is an automorphism of  $\mathbb{C}[x]$ ; furthermore, since we have that

$$\varphi^k(f(x)) = f(\zeta_n^k x)$$

for a positive integer  $k$ , where  $\varphi^k$  denotes  $\varphi$  applied  $k$  times, then by the properties of  $\zeta_n$  mentioned in the first paragraph we have that  $\varphi$  has order  $n$ .

## Result

3 of 3

Let  $\zeta_n = e^{2\pi i/n} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ , then such an automorphism is given by the map  $f(x) \mapsto f(\zeta_n x)$ . Click for more details.

## Section 4–7

### 1. a

Let  $F$  be a field of fractions of  $D$ . Recall that addition in  $F$ , for  $[a, b], [c, d] \in F$ , is defined as

$$[a, b] + [c, d] = [ad + bc, bd].$$

Now we have that

$$\begin{aligned} ([a, b] + [c, d]) + [e, f] &= [ad + bc, bd] + [e, f] \\ &= [(ad + bc)f + bde, bdf] \\ &= [adf + bcf + bde, bdf] \\ &= [adf + b(cf + de), b(df)] \\ &= [a, b] + [cf + de, df] \\ &= [a, b] + ([c, d] + [e, f]), \end{aligned}$$

where we used the facts that addition and multiplication commutative and associative in  $D$ , as well as that multiplication distributes over addition in  $D$ .

#### Result

2 of 2

We directly write out  $([a, b] + [c, d]) + [e, f]$  and then use properties of  $D$  to show that it is equal to  $[a, b] + ([c, d] + [e, f])$ .

### 2. a

Let  $F$  be a field of fractions of an integral domain  $D$ , and let  $[a, b], [c, d] \in F$ , then

$$\begin{aligned} [a, b] + [c, d] &= [ad + bc, bd] \\ &= [cb + da, db] \\ &= [c, d] + [a, b] \end{aligned}$$

where we used the commutativity and associativity of addition and multiplication in  $D$ .

#### Result

2 of 2

We write out  $[a, b] + [c, d]$  and use properties of  $D$  to show that it is equal to  $[c, d] + [a, b]$ . Click for the proof.

### 3. a

Let  $F$  be a field of fractions of an integral domain  $D$  and let  $[a, b], [c, d], [e, f] \in F$ . Then

$$\begin{aligned}[a, b][c, d] &= [ac, bd] \\ &= [ca, db] \\ &= [c, d][a, b]\end{aligned}$$

because multiplication in  $D$  is commutative, so that multiplication in  $F$  is also commutative.

## Step 2

2 of 3

Also

$$\begin{aligned}([a, b][c, d])[e, f] &= [ac, bd][e, f] \\ &= [ace, bdf] \\ &= [a(ce), b(df)] \\ &= [a, b][ce, df] \\ &= [a, b]([c, d][e, f])\end{aligned}$$

because multiplication in  $D$  is associative, so that multiplication in  $F$  is also associative.

## Result

3 c

We use commutativity and associativity of multiplication in  $D$  to show commutativity and associativity of multiplication in  $F$ . Click for the proof.

## 4. a

We define a map  $\tau : F \rightarrow K$  by

$$\tau([a, b]) = ab^{-1}.$$

In order to show that this map is well-defined, note that  $b^{-1}$  exists in  $K$  because it is a field and  $b \neq 0$ , and let  $[a, b] = [a', b']$ , then  $ab' = ba'$ , so that  $ab^{-1} = a'b'^{-1}$ .

## Step 2

2 of 4

We now prove that  $\tau$  is a one-to-one homomorphism, in which case  $F \cong \tau(F)$ , so that we may identify  $F$  with the image of  $F$  under  $\tau$ , which is a subset of  $K$ .

First, in order to prove that it is one-to-one, note that if

$$\tau([a, b]) = \tau([c, d])$$

then

$$ab^{-1} = cd^{-1},$$

which is equivalent to  $ad = bc$ , so by definition of  $F$  we have  $[a, b] = [c, d]$ .

Next, in order to prove it is a homomorphism we verify addition and multiplicative properties. We have

$$\begin{aligned}\tau([a,b] + [c,d]) &= \tau([ad+bc, bd]) \\&= (ad+bc)(bd)^{-1} \\&= ab^{-1} + cd^{-1} \\&= \tau([a,b]) + \tau([c,d]).\end{aligned}$$

And also

$$\begin{aligned}\tau([a,b][c,d]) &= \tau([ac, bd]) \\&= (ac)(bd)^{-1} \\&= (ab^{-1})(cd^{-1}) \\&= \tau([a,b])\tau([c,d]).\end{aligned}$$

## Result

4 of 4

We verify that a map from  $F$  to  $K$  defined by  $[a,b] \mapsto ab^{-1}$  is a one-to-one homomorphism, so that we may identify  $F$  with its isomorphic image  $\tau(F)$  in  $K$ . Click for more details.

# 5

---

## Chapter 5

### Section 5–1

1. a

**To Prove:** A field is an integral domain.

**Proof:** Let  $F$  be a field. Then  $F$  is a

**non-trivial commutative ring with unity and each non-zero element of  $F$  is a unit.**

Let us consider  $a$  be a non-zero element of  $F$ .

Then

$$a^{-1} \in F \text{ and } a^{-1} \cdot a = 1.$$

Let us assume that  $a \cdot b = 0$ .

Then

$$\begin{aligned} a \cdot b = 0 &\implies a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \\ &\implies (a^{-1} \cdot a) \cdot b = 0 \\ &\implies 1 \cdot b = 0 \\ &\implies b = 0. \end{aligned}$$

This proves that  $a$  is not a left divisor of zero.

**Since  $F$  is a field, multiplication is commutative on  $F$ . So,  $a$  is not a right divisor of zero. And consequently,  $a$  is not a divisor of zero.**

Therefore  $F$  contains no divisor of zero.

Therefore,  $F$  is a non-trivial commutative ring with unity and  $F$  contains no divisor of zero. Hence  $F$  is an integral domain.

This completes our proof.

#### Result

2 of 2

Considering any element  $a \neq 0$  in  $F$  we have shown that  $a \cdot b = 0 \implies b = 0$ , that is,  $F$  contains no divisor of zero. Hence  $F$  is an integral domain. Click for the complete proof.

2. a

Suppose,  $D$  is integral domain which has no unit element. Suppose,  $0$  is not characteristic of  $D$ .

**To show:** its characteristic is a prime number.

Suppose, if possible  $m$  is characteristic of  $D$ ,

where  $m = m_1 m_2$  with  $m_1, m_2 > 1$ . By minimality of  $m$ ,  $m_1 x$  can not be  $0$  for all  $x \in D$ . Therefore, there exists  $a \in D$  such that  $m_1 a \neq 0$ . similarly, there exists  $b \in D$  such that  $m_2 b \neq 0$ . Now  $mab = 0$ ,

$$\begin{aligned} &\implies m_1 m_2 ab = 0 \\ &\implies (m_1 a)(m_2 b) = 0 \end{aligned}$$

But  $m_1 a \neq 0$  and  $m_2 b \neq 0$ , which contradicts that  $D$  is integral domain. So,  $m$  has to be prime.

## Result

2 of 2

[Click Here To See Explanation.](#)

3. a

### Part a.

We already know that any element from ring  $S = R[x]$  has the form  $\sum a_i x^i$ , where each  $a_i \in R$ .

By analogy, elements from ring  $T = S[y]$  have the form

$$\sum b_j y^j, \quad (*)$$

where each  $b_j \in S$ . Now for each  $j$  we can write

$$b_j = \sum a_{ij} x^i,$$

where each  $a_{ij} \in R$ . Plugging this in to equation  $(*)$ , we obtain that elements from ring  $T$  have the desired form:

$$\sum b_j y^j = \sum \left( \sum a_{ij} x^i \right) y^j = \sum \sum a_{ij} x^i y^j.$$

**Part b.**

The condition is completely analogous to standard condition of equality of polynomials. It says that two polynomials  $f(x, y) = \sum \sum a_{ij} x^i y^j$  and  $g(x, y) = \sum \sum a'_{ij} x^i y^j$  from  $T$  are equal if and only if  $a_{ij} = a'_{ij}$ , for all  $i, j$ , where all  $a_{ij}$  and  $a'_{ij}$  are from  $R$ .

One direction of this claim is immediately apparent, while second can be proven using the following simple argument. If we consider  $f$  and  $g$  as elements of ring  $S[y]$  (see **part a**), then we know from theory of polynomials in one variable that  $f = g$  only if  $b_j = b'_j$  for all  $j$ . But since these are polynomials from  $R[x]$ , we obtain  $a_{ij} = a'_{ij}$  for all  $i, j$ .

**Part c.**

This is the well-known first-grade pre-algebra rule: "Thou shalt add coefficients besides equal expressions". In other words:

$$f(x, y) + g(x, y) = \sum \sum a_{ij} x^i y^j + \sum \sum a'_{ij} x^i y^j = \sum \sum (a_{ij} + a'_{ij}) x^i y^j.$$

**Part d.**

This is also a well-known rule, but more complicated to write. We denote first

$$b_{k\ell} = \sum_{\substack{i+i'=k \\ j+j'=\ell}} a_{ij} a'_{i'j'}.$$

Finally we write the product of  $f$  and  $g$  as

$$f(x, y)g(x, y) = \sum \sum b_{k\ell} x^k y^\ell.$$

**Result**

Never enough indices to play with ...

**4. a**

**Given:**  $D$  is an integral domain.

**To Prove:**  $D[x, y]$  is an integral domain.

**Proof:** Since  $D$  is an integral domain then  $D$  is a non-trivial commutative ring with unity contains no divisor of zero.

**Then the ring  $D[x, y]$  is a commutative ring with unity (same as  $D$ ). The zero element in the ring  $D[x, y]$  is the constant polynomial 0.**

Let  $f(x, y)$  and  $g(x, y)$  be non zero polynomials in  $D[x, y]$ .

Let us assume

$$f(x, y) = \sum_i \sum_j a_{ij} x^i y^j$$

$$g(x, y) = \sum_i \sum_j b_{ij} x^i y^j$$

where  $a_{ij}$  and  $b_{ij}$  belongs to  $D$ .

Now consider  $f(x, y)g(x, y) = 0$ .

Then

$$f(x, y)g(x, y) = 0$$

$$\Rightarrow (\sum_i \sum_j a_{ij} x^i y^j)(\sum_i \sum_j b_{ij} x^i y^j) = 0.$$

Then

**comparing above two sides of the equation we have got each coefficient of  $x^i y^j$  in  $f(x, y)g(x, y)$  are zero at some context.**

This follows that either

$$a_{ij} = 0 \text{ or } b_{ij} = 0 \text{ for all } i, j.$$

Therefore,

$$\text{either } f = 0 \text{ or } g = 0.$$

Hence for any two elements  $f, g$  in  $D[x, y]$  with  $fg = 0$  we have concluded that either  $f = 0$  or  $g = 0$ .

So,  $D[x, y]$  contains no divisor of zero.

Therefore  $D[x, y]$  is an integral domain.

This completes the proof.

## Result

2 of 2

Considering any two elements  $f, g$  from the ring  $D[x, y]$  with  $fg = 0$  we have shown that either  $f = 0$  or  $g = 0$ .

This follows that  $D[x, y]$  is a commutative ring with unity contains no divisor of zero, so an integral domain. Click for the complete proof.

5. a

By the given condition  $F$  is a field and  $D = F[x, y]$ .

Now the **Field of Quotients** of  $D$  is denoted by  $F(x, y)$ , it is also called the

### Field of rational functions in two variables over $F$

Let us now consider two elements  $f(x, y)$  and  $g(x, y)$  from  $F[x, y]$  such that

$$f(x, y) \neq 0 \text{ and } \text{Gcd}(f(x, y), g(x, y)) = 1.$$

Let us now assume the element

$$\frac{g(x, y)}{f(x, y)}.$$

Say

$$h(x, y) = \frac{g(x, y)}{f(x, y)}.$$

Then  $\frac{g(x, y)}{f(x, y)}$  is the typical element of  $F(x, y)$  where

$$f(x, y) \neq 0 \text{ and } \text{Gcd}(f(x, y), g(x, y)) = 1.$$

### Result

2 of 2

The typical element of  $F(x, y)$  is of the form  $\frac{g(x, y)}{f(x, y)}$ , where  $f(x, y) \neq 0$  and  $\text{Gcd}(f(x, y), g(x, y)) = 1$ . Click for the complete solution.

### 6. a

**To Prove:**  $F(x, y)$  is isomorphic to  $F(y, x)$ .

**Proof:**  $F(x, y)$  is the field of rational functions in two variable over  $F$ . Let us consider the domains  $F[x, y]$  and  $F[y, x]$ .

Let us define a map  $\phi : F[x, y] \rightarrow F[y, x]$  by the assignment

$$\phi\left(\sum_i \sum_j a_{ij}x^i y^j\right) = \sum_i \sum_j a_{ij}y^i x^j.$$

Trivially  $\phi$  is well-defined on  $F[x, y]$ , since it only exchange the indeterminate  $x$  and  $y$  (replacing the indeterminate).

Now we will show that  $\phi$  is a Ring Homomorphism.

Let us consider two elements  $f(x, y)$  and  $g(x, y)$  from  $F[x, y]$ .

Let us assume

$$\begin{aligned} f(x, y) &= \sum_i \sum_j a_{ij}x^i y^j \\ g(x, y) &= \sum_i \sum_j b_{ij}x^i y^j, \text{ where } a_{ij}, b_{ij} \in F. \end{aligned}$$

Then clearly we have

$$\begin{aligned} \phi(f + g) &= \phi\left(\sum_i \sum_j a_{ij}x^i y^j + \sum_i \sum_j b_{ij}x^i y^j\right) \\ &= \sum_i \sum_j a_{ij}y^i x^j + \sum_i \sum_j b_{ij}y^i x^j \\ &= \phi\left(\sum_i \sum_j a_{ij}x^i y^j\right) + \phi\left(\sum_i \sum_j b_{ij}x^i y^j\right) \\ &= \phi(f) + \phi(g). \end{aligned}$$

Now we show that

$$\phi(fg) = \phi(f)\phi(g).$$

So,

$$\begin{aligned}\phi(fg) &= \phi\left(\left(\sum_i \sum_j a_{ij}x^i y^j\right)\left(\sum_i \sum_j b_{ij}x^i y^j\right)\right) \\ &= \phi\left(\sum_{i,j} \sum_{k,l} a_{ij}b_{kl}x^{i+k}y^{j+l}\right) \\ &= \sum_{i,j} \sum_{k,l} a_{ij}b_{kl}y^{i+k}x^{j+l} \\ &= \left(\sum_i \sum_j a_{ij}y^i x^j\right)\left(\sum_i \sum_j b_{ij}y^i x^j\right) \\ &= \phi\left(\sum_i \sum_j a_{ij}x^i y^j\right)\phi\left(\sum_i \sum_j b_{ij}x^i y^j\right) \\ &= \phi(f)\phi(g).\end{aligned}$$

This proves that  $\phi$  is a ring homomorphism.

**Claim:**  $\phi$  is bijective.

**Proof of the Claim:** Let us consider an element  $f$  in  $F[x, y]$ .

Let us assume

$$f(x, y) = \sum_i \sum_j a_{ij}x^i y^j, \text{ where } a_{ij} \in F.$$

Now

$$\begin{aligned}\phi(f) = 0 &\implies \sum_i \sum_j a_{ij}x^i y^j = 0 \\ &\implies a_{ij} = 0, \text{ for all } i, j \\ &\implies f(x, y) = 0.\end{aligned}$$

So,  $\phi$  is injective.

In order to show that  $\phi$  is surjective let us assume an element  $g$  from  $F[y, x]$  such that

$$g(y, x) = \sum_i \sum_j a_{ij}y^i x^j, \text{ where } a_{ij} \in F.$$

Look at the element  $f(x, y)$  in  $F[x, y]$  given by

$$f(x, y) = \sum_i \sum_j a_{ij} x^i y^j.$$

Clearly

$$\phi(f(x, y)) = g(x, y).$$

This follows that

**for every element  $g$  in  $F[y, x]$  there exists an element  $f$  in  $F[x, y]$  which is a preimage of  $g$  under  $\phi$ .**

Hence  $\phi$  is surjective. Consequently,  $\phi$  is bijective.

Therefore,  $\phi$  is a bijective ring homomorphism, hence  $\phi$  is a ring isomorphism.

Therefore

$$F[x, y] \cong F[y, x].$$

Trivially, our result achieved that

$$F(x, y) \cong F(y, x).$$

This completes our proof.

## Result

4 of 4

Considering the domains  $F[x, y]$ ,  $F[y, x]$  and assign an mapping  $\phi$  between them we have shown that  $\phi$  introduce a bijection between them, hence  $F[x, y] \cong F[y, x]$  and consequently,  $F(x, y) \cong F(y, x)$ . Click for the complete proof.

## 7. a

**Given:**  $F$  be a field of Char  $p \neq 0$ .

Then for any element  $x$  in  $F$

$$px = 0.$$

**To Prove:** For all  $a, b$  in  $F$

$$(a + b)^p = a^p + b^p.$$

**Proof:** Since  $F$  is of characteristic  $p$  and we have considered arbitrary two elements  $a, b$  in  $F$  we have

$$pa = pb = 0.$$

Now we know from Binomial Theorem that

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i}.$$

Here

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Now we know that for any integer  $n$  and any integer  $k$  satisfying  $1 \leq k < n$ ,  $n$  always divides  $\binom{n}{k}$ . So in our case for  $i$  in the range  $1 \leq i < p$ ,  $p$  divides  $\binom{p}{i}$ . Therefore other than the terms  $a^p$  and  $b^p$  in the expansion  $\sum_{i=0}^p \binom{p}{i} a^i b^{p-i}$  will vanish due to char  $p$  nature of  $F$ .

Hence we have

$$\sum_{i=0}^p \binom{p}{i} a^i b^{p-i} = a^p + b^p.$$

This follows that, for all  $a, b \in F$

$$(a + b)^p = a^p + b^p.$$

This completes the proof.

## Result

2 of 2

Being  $F$  is a characteristic  $p$  field,  $pa = pb = 0$  for every  $a, b \in F$  and then expanding  $(a + b)^p$  by using Binomial theorem we conclude that except  $a^p$  and  $b^p$  all other terms get vanished. Hence we get our result. Click for the detailed proof.

## 8. a

**Given:**  $F$  be a field of Char  $p \neq 0$ .

Then for any element  $x$  in  $F$

$$px = 0.$$

**To Prove:** For all  $a, b$  in  $F$

$$(a + b)^m = a^m + b^m, \text{ where } m = p^n.$$

**Proof:** Since  $F$  is of characteristic  $p$  and we have considered arbitrary two elements  $a, b$  in  $F$  we have

$$\begin{aligned} pa &= pb = 0 \\ \implies p^n a &= p^n b = 0 \\ \implies ma &= mb = 0. \end{aligned}$$

Now we know from Binomial Theorem that

$$(a + b)^m = \sum_{i=0}^m \binom{m}{i} a^i b^{m-i}.$$

Here

$$\binom{m}{i} = \frac{m!}{i! (m - i)!}.$$

Now we know that for any integer  $n$  and any integer  $k$  satisfying  $1 \leq k < n$ ,  $n$  always divides  $\binom{n}{k}$ . So in our case for  $i$  in the range  $1 \leq i < m$ ,  $m$  divides  $\binom{m}{i}$ . It follows that  $p$  divides  $\binom{m}{i}$ , for  $i$  satisfying  $1 \leq i < m$ , since  $m = p^n$  for any integer  $n$ . Therefore other than the terms  $a^m$  and  $b^m$  in the expansion  $\sum_{i=0}^m \binom{m}{i} a^i b^{m-i}$  will vanish due to char  $p$  nature of  $F$ .

Hence we have

$$\sum_{i=0}^m \binom{m}{i} a^i b^{m-i} = a^m + b^m.$$

This follows that, for all  $a, b \in F$

$$(a + b)^m = a^m + b^m.$$

This completes the proof.

## Result

2 of 2

Being  $F$  is a field of Characteristic  $p$  and  $m = p^n$ , then  $mx = 0$  for all  $x \in F$ . Hence by using binomial theorem we have proved that  $(a + b)^m = a^m + b^m$ , for all  $a, b \in F$ . Click for the complete solution.

## 9. a

**a) Given:**  $F$  is a field of **characteristics**  $p \neq 0$  and  
 $\phi : F \rightarrow F$  is defined by the assignment:  $\phi(a) = a^p$  for all  $a \in F$ .  
**To Prove:**  $\phi$  is a **monomorphism** of  $F$  into itself.

### Step 2

**Proof:** Given that  $\phi(a) = a^p$  for all  $a \in F$ .

First we show that  $\phi$  is a **ring homomorphism**.

Let  $a, b \in F$ .

$$\begin{aligned} \text{Now, } \phi(a+b) &= (a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p, \\ &\quad \text{by using Binomial expansion} \\ &= a^p + b^p, \quad \text{as } F \text{ is a field of characteristics } p \neq 0 \text{ and } p \text{ divides } \binom{p}{k}. \end{aligned}$$

Now,  $\phi(ab) = (ab)^p = a^p b^p$ , since  $F$  is **commutative**.

Therefore we have,  $\phi(a+b) = a^p + b^p$        $\phi(ab) = a^p b^p$ , for all  $a, b \in F$ .

So,  $\phi$  is a **Field homomorphism**.

Now, we assert that  $\phi$  is an **Injection**.

It suffices to show that  $\phi(a) = 0 \implies a = 0$  for  $a \in F$ .

Let  $\phi(a) = 0$  for some  $a \in F$ .

**Since  $F$  is a field,  $F$  does not contain divisor of zero.**

So we have,  $a^p = 0 \implies a = 0$

It follows that  $\phi(a) = 0 \implies a = 0$  for  $a \in F$ .

So,  $\phi$  is **Injective**.

Consequently,  $\phi$  is an

**Injective homomorphism i.e. a monomorphism into itself.**

(b) Give an example of a field where  $\phi$  is **not onto**.

**Ans:** Let us consider the field  $\mathbb{F}_2[t]$ .

Then  $\mathbb{F}_2[t]$  is a

**field of char 2.**

Now define  $\phi$  as  $\phi : \mathbb{F}_2[t] \rightarrow \mathbb{F}_2[t]$  by  $\phi(a) = a^2$  for all  $a \in \mathbb{F}_2[t]$ .

**We now show that  $\phi : \mathbb{F}_2[t] \rightarrow \mathbb{F}_2[t]$  is not onto.**

Let us now consider the element  $t$  in  $\mathbb{F}_2[t]$ . It is clear that  $t$  is

**not a square in  $\mathbb{F}_2[t]$ .**

Therefore there

**does not exist any element  $f$  in  $\mathbb{F}_2[t]$  such that  $\phi(f) = t$ .**

**Thus  $t$  has no pre-image in  $\mathbb{F}_2[t]$  under  $\phi$ .**

So,  $\phi$  is **not onto**.

## 10. a

and this shows that  $f$  is onto. Since  $f$  is 1 – 1 as well as onto,  $f$  is a bijection.

This completes our Claim.

According to the question  $F$  is a finite field (set), and  $\phi$  is an injective map from  $F$  to itself. Hence  $\phi$  is surjective as well by the above Claim. Therefore,  $\phi$  is a bijection.

So,  $\phi$  is a bijective homomorphism from  $F$  to itself, hence an Automorphism of  $F$ .

This completes the proof.

### Result

3 of 3

Being  $F$  is finite field, every injective map from  $F$  to itself gives a bijection, since by our given condition  $\phi$  is an injective homomorphism from  $F$  to itself and  $F$  is finite,  $\phi$  is an Automorphism. Click for the complete proof.

By the given condition  $F$  is finite field of characteristic  $p \neq 0$ . A mapping  $\phi : F \rightarrow F$  is defined by the assignment

$$\phi(a) = a^p, \quad \forall a \in F.$$

Now  $\phi$  defines an injective field homomorphism (monomorphism) into itself.

**Claim:** Let  $A, B$  be both finite sets of  $n$  elements and a mapping  $f : A \rightarrow B$  is injective. Then  $f$  is a bijection.

**Proof of the Claim:** Let us assume that  $A = \{a_1, a_2, \dots, a_n\}$ .

Then  $f(a_1), f(a_2), \dots, f(a_n)$  all belong to  $B$ . Since  $f$  is injective,  $f(a_1), f(a_2), \dots, f(a_n)$  are all distinct elements of  $B$ .

As they are  $n$  in number, they are all the elements of  $B$ .

Let  $b \in B$ . Then

$$b = f(a_i), \text{ for some } a_i \in A,$$

## Section 5–2

1. a

**1(a).** Suppose  $x_1, x_2$  and  $x_3 \in \mathbb{R}$  such that

$$x_1(1, 2, 3) + x_2(4, 5, 6) + x_3(7, 8, 9) = (0, 0, 0)$$

implies that

$$x_1 + 4x_2 + 7x_3 = 0 \quad (1)$$

$$2x_1 + 5x_2 + 8x_3 = 0 \quad (2)$$

$$3x_1 + 6x_2 + 9x_3 = 0. \quad (3)$$

Multiplying (1) with 2 and subtract it from (2) and multiplying (1) with 3 and subtract it from (3), we get

$$-(3x_2 + 6x_3) = 0 \quad (4)$$

$$-(6x_2 + 12x_3) = 0. \quad (5)$$

Simplifying, we get

$$x_2 + 2x_3 = 0.$$

So  $x_2 = 2$  and  $x_3 = -1$  is one solution of above equation and putting it in (1) we get  $x_1 = -1$ .

Now  $(x_1, x_2, x_3) = (-1, 2, -1)$  is one non-trivial solution for above linear system. Hence  $(1, 2, 3), (4, 5, 6)$  and  $(7, 8, 9)$  are linearly dependent.

**1(b).** Suppose  $x_1, x_2$  and  $x_3 \in \mathbb{R}$  such that

$$x_1(1, 0, 1) + x_2(0, 1, 2) + x_3(0, 0, 1) = (0, 0, 0)$$

implies that

$$x_1 + 0x_2 + 0x_3 = 0 \quad (6)$$

$$0x_1 + x_2 + 0x_3 = 0 \quad (7)$$

$$x_1 + 2x_2 + x_3 = 0. \quad (8)$$

So, from (1) and (2) we get  $x_1 = x_2 = 0$  and then from (3)  $x_3 = 0$ . Now  $(x_1, x_2, x_3) = (0, 0, 0)$  is only solution for above linear system.

Hence  $(1, 0, 1), (0, 1, 2)$  and  $(0, 0, 1)$  are linearly independent.

**1(c).** Suppose  $x_1, x_2$  and  $x_3 \in \mathbb{R}$  such that

$$x_1(1, 2, 3) + x_2(0, 4, 5) + x_3\left(\frac{1}{2}, 3, \frac{21}{4}\right) = (0, 0, 0)$$

implies that

$$x_1 + 0x_2 + \frac{1}{2}x_3 = 0 \quad (9)$$

$$2x_1 + 4x_2 + 3x_3 = 0 \quad (10)$$

$$3x_1 + 5x_2 + \frac{21}{4}x_3 = 0. \quad (11)$$

From (1) we get

$$2x_1 + x_3 = 0 \implies x_3 = -2x_1.$$

Putting  $x_3 = -2x_1$  in (2), we get  $x_3 = -2x_2$ . So,  $x_1 = x_2 = -\frac{1}{2}x_3$ .

Now from (3) we get

$$\begin{aligned}3x_1 + 5x_2 + \frac{21}{4}x_3 &= 0 \\ \implies 3x_1 + 5x_1 + \frac{21}{4}(-\frac{1}{2}x_1) &= 0 \\ \implies \frac{43}{8}x_1 &= 0 \\ \implies x_1 &= 0.\end{aligned}$$

Now  $(x_1, x_2, x_3) = (0, 0, 0)$  is only solution for above linear system.

Hence  $(1, 2, 3), (0, 4, 5)$  and  $(\frac{1}{2}, 3, \frac{21}{4})$  are linearly independent.

## 2. a

In  $\mathbb{Z}_5$  given that

$$x_1 + x_2 + x_3 = 0 \quad (1)$$

$$x_1 + 2x_2 + 3x_3 = 0 \quad (2)$$

$$3x_1 + 4x_2 + 2x_3 = 0. \quad (3)$$

Multiplying (1) with 1 and subtract it from (2) and multiplying (1) with 3 and subtract it from (3), we get

$$x_2 + 2x_3 = 0 \quad (4)$$

$$x_2 - x_3 = 0. \quad (5)$$

### Step 2

2 of 3

From above two equation we get that  $3x_3 = 0$ , Now 3 is non-zero element of  $\mathbb{Z}_5$ . So  $x_3 \equiv 0 \pmod{5}$ . Therefore,  $x_2 \equiv 0 \pmod{5}$  and from above equation we will get that  $x_1 \equiv 0 \pmod{5}$ .

### Result

3 of 3

Hence the given system has no non-trivial solution in  $\mathbb{Z}_5$ .

## 3. a

**Given:**  $V$  is a vector space of dimension  $n$  over the field  $\mathbb{Z}_p$ , where  $p$  is a prime.

**To Prove:**  $V$  has  $p^n$  elements.

**Proof:** In order to prove our content, first we start with a Lemma.

**Lemma:** Let  $V$  be a vector space of dimension  $n$  over a field  $F$ . Then  $V$  is isomorphic to  $F^n$ .

**Proof of the Lemma:** An isomorphism between  $V$  and  $F^n$  can be established in many ways.

Let  $(b_1, b_2, \dots, b_n)$  be an ordered basis of  $V$ . Then any vector  $v$  of  $V$  can be expressed as

$$v = c_1 b_1 + c_2 b_2 + \dots + c_n b_n,$$

where  $c_1, c_2, \dots, c_n$  are unique scalars in  $F$ .

Let us define a mapping  $\phi : V \rightarrow F^n$  by the assignment

$$\phi(v) = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}, \text{ where } v = (c_1 b_1 + c_2 b_2 + \dots + c_n b_n) \in V.$$

Let us now consider

$$x = \sum_{k=1}^n x_k b_k \in V$$

$$y = \sum_{k=1}^n y_k b_k \in V.$$

Then

$$x + y = (x_1 + y_1)b_1 + (x_2 + y_2)b_2 + \dots + (x_n + y_n)b_n \in V.$$

Now

$$\phi(x) = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad \phi(y) = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \text{ and}$$

$$\phi(x + y) = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \phi(x) + \phi(y) \dots \dots (1)$$

Let us assume  $p \in F$ . Then  $px \in V$  and

$$px = (px_1)b_1 + (px_2)b_2 + \dots + (px_n)b_n.$$

Then

$$\phi(px) = \begin{pmatrix} px_1 \\ px_2 \\ \vdots \\ px_n \end{pmatrix} = p \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = p\phi(x) \dots \dots (2)$$

From (1) and (2) we have concluded that  $\phi$  is a homomorphism.

To prove that  $\phi$  is one-to-one, let  $x, y \in V$  be such that

$$\begin{aligned}\phi(x) = \phi(y), \text{ where } x &= \sum_{k=1}^n x_k b_k \in V \\ y &= \sum_{k=1}^n y_k b_k \in V.\end{aligned}$$

Now

$$\begin{aligned}\phi(x) = \phi(y) &\implies \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ &\implies x_1 = y_1, x_2 = y_2, \dots, x_n = y_n \\ &\implies x = y.\end{aligned}$$

So,  $\phi$  is one-to-one.

To prove that  $\phi$  is onto, let

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$$

be an element in  $F^n$ .

Then

$$r_1 b_1 + r_2 b_2 + \dots + r_n b_n \in V.$$

And we have

$$\phi(r_1 b_1 + r_2 b_2 + \dots + r_n b_n) = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}.$$

So  $\phi$  is onto.

**Since  $\phi$  is a homomorphism which is both one-to-one and onto,  $\phi$  is an isomorphism.**

**Since  $\phi$  is an isomorphism,  $V$  is isomorphic to  $F^n$ .**

This completes our Lemma.

According to the question,  $V$  is a vector space of finite dimension  $n$  over the field  $\mathbb{Z}_p$ , where  $p$  is a prime. Then by the above Lemma, we have

$$V \cong \mathbb{Z}_p^n.$$

Since  $\mathbb{Z}_p^n$  contains  $p^n$  elements,  $V$  has  $p^n$  elements.

This completes our proof.

## Result

4 of 4

First we prove that for a vector space  $V$  of dimension  $n$  over a field  $F$ ,  $V$  is isomorphic to  $F^n$ . By the given condition,  $V$  is isomorphic to  $\mathbb{Z}_p^n$ , which implies  $V$  contains  $p^n$  elements. Click for the complete solution.

#### 4. a

**Problem:** If  $V$  is a vector space of dimension  $n$  over  $\mathbb{Z}_p$ ,  $p$  is a prime, show that  $V$  has  $p^n$  elements.

##### Step 2

2 of 4

Since  $V$  is a vector space of dimension  $n$ , thus by the Theorem 5.2.7, every linearly independent set with  $n$  elements form a basis of  $V$ . Suppose  $\{v_1, v_2, \dots, v_n\}$  be a basis of the vector space  $V$ . Then by Lemma 5.2.3. we know that

$$V = \{a_1v_1 + a_2v_2 + \dots + a_nv_n \mid a_i \in \mathbb{Z}_p, i = 1, 2, \dots, n\}$$

##### Step 3

3 of 4

Thus every element of  $V$  can be written in the form  $a_1v_1 + a_2v_2 + \dots + a_nv_n$  for some unique scalars  $a_1, a_2, \dots, a_n \in \mathbb{Z}_p$ . Now we know that  $\mathbb{Z}_p$  has  $p$  distinct elements. Thus for each  $a_i, i = 1, 2, \dots, p$  we have exactly  $p$  choices, that means,  $a_1$  has  $p$  choices,  $a_2$  has  $p$  choices and so on.

##### Result

4 of 4

Therefore  $V$  has  $\underbrace{p \times p \times \dots \times p}_{n\text{-times}} = p^n$  elements.

#### 5. a

**Given:**  $F$  is a field and  $V = F[x]$ , the polynomial ring in  $x$  over  $F$ . Trivially  $V$  is a vector space over  $F$ .

**To Prove:** Dimension of  $V$  over  $F$  is infinite, that is,

$$\dim_F V = \infty.$$

**Proof:** In order to show that  $V$  is not a finite dimensional vector space over the field  $F$ ,

**we will propose to prove that there exists an infinite subset of  $V$  which is linearly independent.**

Let us consider the infinite subset given by

$$S := \{1, x, x^2, \dots, x^n, x^{n+1}, \dots\}.$$

In order to show that  $S$  is a linearly independent subset of  $V$ , it suffices to show that

**any finite dimensional subset of  $S$  is linearly independent.**

Without loss of generality let us consider the set

$$T = \{1, x, x^2, \dots, x^n\} \subset S.$$

To show that  $T$  is linearly independent let us assume

$$\sum_{i=0}^n c_i x^i = 0, \quad \text{where } c_i \in F, \quad \forall i.$$

Therefore,

$$c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} + c_nx^n = 0$$
$$\implies c_0 = c_1 = c_2 = \dots = c_{n-1} = c_n = 0, \text{ since the equation satisfies for all values of } x.$$

This shows that the set  $T$  is linearly independent in  $S$ , which yields that any finite subset of  $S$  is linearly independent.

Hence,  $S$  itself is a linearly independent subset of  $V$ .

This completes the proof that

$$\dim_F V = \infty.$$

## Result

2 of 2

Considering the infinite subset  $\{1, x, x^2, \dots, x^n, \dots\}$  of  $V$  we have shown that  $\{1, x, x^2, \dots, x^n, \dots\}$  is an infinite linearly independent subset of  $V$ , follows the result that dimension of  $V$  over the field  $F$  cannot be finite. Click for the complete proof.

## 6. a

**Given:** Let  $V$  be a finite dimensional vector space over  $F$  and  $W$  be a subspace of  $V$ .

**To Prove:**

- (a)  $W$  is a finite dimensional over  $F$  and  $\dim_F(W) \leq \dim_F(V)$ .
- (b) If  $\dim_F(W) = \dim_F(V)$ , then  $V = W$ .

**Solution:**

- (a) Without loss of generality let us assume that  $\dim_F(V) = n < \infty$ .

In order to show that  $W$  is a finite dimensional over  $F$  and

$\dim_F(W) \leq \dim_F(V)$ , it suffices to show that  $\dim_F(W) \leq n$ .

Let us now consider two cases.

**Case-1:**  $W = \{\theta\}$ , where  $\theta$  is the null vector.

Then

$$\dim_F(W) = 0 < n.$$

**Case-2:**  $W \neq \{\theta\}$ .

Then there exists a non-zero vector, say  $\alpha$ , in  $W$ .

If  $\{\alpha\}$  spans  $W$  then we have a finite basis  $\{\alpha\}$  for  $W$ . If not, there is a non-zero vector  $\beta$  in  $W$  such that the set  $\{\alpha, \beta\}$  is linearly independent.

If  $\{\alpha, \beta\}$  spans  $W$  then we have a finite basis  $\{\alpha, \beta\}$  for  $W$ . If not, the process can be continued and after a finite number of steps we get a linearly independent set  $S$  forming a basis of  $W$ .  $S$  being a linearly independent set in  $V$  also,  $S$  contains at most  $n$  vectors.

Therefore

$$\dim_F(W) \leq n.$$

This completes (a).

(b) Without loss of generality let us assume that  $\dim_F(V) = n < \infty$ .

Then according to the hypothesis we have

$$\dim_F(W) = \dim_F(V) = n.$$

We will propose to show that  $V = W$ .

By the **Fundamental Theorem of Linear Algebra** we know that,

If  $V$  is a vector space of finite dimension  $n$  over a field  $F$  then  $V \cong F^n$ .

By our given condition, dimension of both  $V$  and  $W$  over the field  $F$  is  $n$ .

Hence

$$V \cong W \cong F^n.$$

So  $W$  is isomorphic to  $V$ . Since  $W$  is a subspace of  $F$ ,  $W$  must be equal to  $V$ .

Therefore

$$V = W.$$

This completes the proof.

## Result

3 of 3

For (a) we have used the continued process to show that,  $S$  contains at most  $n$  vectors and follows that  $W$  is a finite dimensional over  $F$  and  $\dim_F(W) \leq \dim_F(V)$ . And for (b) we have used the Fundamental Theorem of Linear Algebra to show that  $V$  equals  $W$ . Click for the detailed solution.

## 7. a

**Given:**  $V$  and  $W$  be two vector spaces over a field  $F$ .

**Construction:** We will now define what we feel about a Vector space homomorphism.

Let us consider a map  $\psi : V \rightarrow W$  defined by the assignment

$$\psi(v + v') = \psi(v) + \psi(v') \quad \text{where } v \in V, v' \in V \quad (1)$$

$$\psi(cv) = c.\psi(v), \text{ where } c \in F, v \in V. \quad (2)$$

So, if a map  $\psi$  between  $V$  to  $W$  satisfies the above two properties (1) and (2), we say that  $\psi$  is a Vector space homomorphism from  $V$  to  $W$ .

**Kernel of a Vector space Homomorphism:** By the aforesaid argument let us consider a Vector space Homomorphism  $\psi : V \rightarrow W$ .

Then the set of all vectors  $\alpha \in V$  such that

$$\psi(\alpha) = 0, 0 \text{ being the null vector in } W,$$

is said to be the kernel of  $\psi$  and is denoted by  $\text{Ker } T (= K)$ .

That is, we can write

$$K = \{\alpha \in V \mid \psi(\alpha) = 0\}.$$

We now claim that,  $K$  is a subspace of  $V$ .

**Proof of the Claim:** We have

$$K = \{\alpha \in V \mid \psi(\alpha) = 0\}.$$

Since  $\psi(0) = 0$ , it follows that  $0 \in K$ . Therefore  $K$  is non-empty.

If  $K = \{0\}$ , then clearly  $K$  is a subspace of  $V$ .

Let us assume  $K \neq \{0\}$ . Then consider an element  $\alpha$  in  $K$ .

By the definition of kernel we have

$$\psi(\alpha) = 0 \text{ in } W.$$

Let  $c \in F$ . Then we have

$$\begin{aligned}\psi(c\alpha) &= c.\psi(\alpha), \text{ since } \psi \text{ is a homomorphism} \\ &= c.0 \\ &= 0.\end{aligned}$$

this yields that  $c\alpha \in K$ .

Now let us consider  $\alpha, \beta \in K$ .

Then we have

$$\psi(\alpha) = \psi(\beta) = 0 \text{ in } W.$$

Now

$$\begin{aligned}\psi(\alpha + \beta) &= \psi(\alpha) + \psi(\beta), \text{ since } \psi \text{ is a homomorphism} \\ &= 0 + 0 = 0.\end{aligned}$$

Therefore,  $\alpha + \beta \in K$ . Thus

$$\alpha, \beta \in K \implies \alpha + \beta \in K \tag{3}$$

$$\alpha \in K \implies c\alpha \in K \text{ for all } c \in F. \tag{4}$$

This proves that  $K$  is a subspace of  $V$ .

**Vector space Isomorphism:** Given  $V$  and  $W$  are vector space over a field  $F$ . A vector space homomorphism  $\psi : V \rightarrow W$  is said to be an isomorphism if  $\psi$  is both injective and surjective.

**Claim:**  $\psi$  is injective if and only if  $K = \{0\}$ .

**Proof of the Claim:** Let  $\psi$  is injective.

Since

$$\psi(0) = 0 \text{ in } W,$$

$0$  in  $V$  is a pre-image of  $0$  in  $W$  and since  $\psi$  is injective,  $0$  is the only pre-image of  $0$  in  $W$ .

Hence we have

$$K = \{0\}.$$

Conversely, let us assume  $K = \{0\}$ .

Let  $\alpha$  and  $\beta$  be two elements in  $V$  such that

$$\psi(\alpha) = \psi(\beta) \text{ in } W.$$

Now we have

$$\begin{aligned}0 &= \psi(\alpha) - \psi(\beta) \\ &= \psi(\alpha - \beta), \text{ since } \psi \text{ is a homomorphism.}\end{aligned}$$

This gives  $\alpha - \beta \in K$  and since  $K = \{0\}$ , we have  $\alpha = \beta$ . Thus

$$\psi(\alpha) = \psi(\beta) \implies \alpha = \beta.$$

Therefore  $\psi$  is injective.

This proves the claim.

Thus if we reformed the definition of Isomorphism we have the following:

Given  $V$  and  $W$  are vector space over a field  $F$ . A vector space homomorphism  $\psi : V \rightarrow W$  is said to be an isomorphism if  $\psi$  is surjective and  $\text{Ker } \psi = \{0\}$ .

## Result

4 of 4

First we define vector space homomorphism and then gives a brief idea of kernel of a vector space homomorphism from the vector spaces  $V$  to  $W$  and lastly we define vector space isomorphism connection with the kernel. Click for the complete solution.

## 8. a

### Quotient Vector Space

Let  $V$  be a vector space over a field  $F$ . Let  $W$  be a subspace of  $V$ .

Let us consider an element  $\alpha$  in  $V$ .

Then look at the set

$$\{\alpha + w \mid w \in W\}$$

is a subset of  $V$ .

It is called a **coset** of  $W$  in  $V$  and is denoted by  $\alpha + W$ .

Now let us look at the below Lemma:

**Lemma:** Let  $\alpha, \beta \in V$ . Then the cosets  $\alpha + W = \beta + W$  if and only if  $\alpha - \beta \in W$ .

Now the set of all distinct cosets of  $W$  is denoted by  $V/W$ . Since  $(V, +)$  is an additive group,  $(W, +)$  is an additive subgroup of  $V$ .

Then  $V/W$  is an additive group under the composition  $+$  defined by

$$(\alpha + W) + (\beta + W) = (\alpha + \beta) + W, \text{ for all } \alpha, \beta \in V.$$

We like to equip the set with a structure of a vector space over  $F$ . For this purpose we define scalar multiplication in  $V/W$  by

$$c(\alpha + W) = c\alpha + W \text{ for all } \alpha \in V, \text{ all } c \in F.$$

First we prove that the scalar multiplication is well defined in the sense that

$$\text{if } \alpha + W = \beta + W \text{ then } c\alpha + W = c\beta + W.$$

Now

$$\alpha + W = \beta + W \implies \alpha - \beta \in W.$$

Therefore

$$c\beta - c\alpha = c(\beta - \alpha) = cw_1 \in W.$$

Consequently,

$$c\alpha + W = c\beta + W.$$

Hence the scalar multiplication is well defined on the set  $V/W$ .

Hence these two operations defines  $V/W$  a vector space over the field  $F$ .

The null element in the vector space is the coset  $W$  itself.

## Result

3 of 3

Firstly we define addition by the assignment  $(\alpha + W) + (\beta + W) = (\alpha + \beta) + W$ , for all  $\alpha, \beta \in V$  and then the operation called multiplication by

$$c(\alpha + W) = c\alpha + W \text{ for all } \alpha \in V, \text{ all } c \in F.$$

And these two operations defined  $V/W$  as a vector space over the field  $F$ . Click for the complete solution.

## 9. a

**Problem:** If  $V$  is a finite-dimensional vector space over  $F$  and  $v_1, \dots, V_n$  in  $V$  are linearly independent over  $F$ , show we can find  $w_1, \dots, w_r$  in  $V$ , where  $m + r = \dim_F(V)$ , such that  $v_1, \dots, V_n, w_1, \dots, w_r$  form a basis of  $V$ .

### Step 2

2 of 5

Let  $S = \{v_1, \dots, V_n\}$ . Then  $S$  is a linearly independent set. If  $\text{span}(S) = V$ , then  $S$  is a basis of  $V$ .

Now suppose  $\text{span}(S) \neq V$ . Then there exist  $v \in V$  such that  $w_1 \notin \text{span}(S)$ . Clearly  $w_1 \neq 0$ , as  $0 \in \text{span}(S)$ . Consider  $S_1 = S \cup \{w_1\}$ .

**Claim:**  $S_1$  is linearly independent set of  $V$ .

To justify our claim let us consider

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n + b_1w_1 = 0$$

If possible let  $b_1 \neq 0$ , then we get

$$w_1 = -\frac{1}{b_1}(a_1v_1 + a_2v_2 + \cdots + a_nv_n) \in \text{span}(S),$$

which is a contradiction. Thus  $b_1 = 0$ . Again  $v_1, \dots, V_n$  are linearly independent and so  $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$  yields that  $a_1 = a_2 = \cdots = a_n = 0$ . Therefore  $S_1$  is a linearly independent set of  $V$ . Hence our claim verified.

#### Step 4

4 of 5

Again if  $\text{span}(S_1) = V$  then we are done. Otherwise we can repeat the process and expand it into larger independent set. But we know that no linearly independent set in  $V$  can contain more than  $\dim_F(V)$  vectors.

Therefore, after  $r$ -th step the process will stop, where  $r = \dim_F(V) - n$ . In that case  $S_r = \{v_1, \dots, V_n, w_1, \dots, w_r\}$  is a linearly independent set in  $V$  such that  $\text{span}(S_r) = V$ . Hence  $S_r$  is a basis of  $V$

## 10. a

**Given:**  $V$  and  $V'$  are two vector spaces over a field  $F$  and  $\psi : V \rightarrow V'$  is an onto homomorphism with kernel  $K$ .

**To Prove:**  $V/K$  is isomorphic to  $V'$ .

**Proof:** By the given condition

$$\psi : V \rightarrow V'$$

is a vector space isomorphism with  $\text{Ker } \psi = K$ .

Let us now define a map  $\phi : V/K \rightarrow V'$  by the assignment

$$\phi(v+K) = \psi(v) \text{ where } v \in V.$$

First we show that  $\phi$  is well defined in the sense that

$$\text{if } v_1 + K = v_2 + K \text{ then } \phi(v_1 + K) = \phi(v_2 + K).$$

Now we have

$$\begin{aligned} v_1 + K = v_2 + K &\implies v_1 - v_2 \in K \\ &\implies \psi(v_1 - v_2) = 0, \text{ since } \text{ker } \psi = K \\ &\implies \psi(v_1) = \psi(v_2) \\ &\implies \phi(v_1 + K) = \phi(v_2 + K). \end{aligned}$$

This shows that  $\phi$  is well defined.

Now we show that  $\phi$  is a homomorphism.

Let us consider two elements  $a + K$  and  $b + K$  from  $V/K$ , where  $a, b \in V$ .

Then we have

$$\begin{aligned} \phi[(a + K) + (b + K)] &= \phi[(a + b) + K] \\ &= \psi(a + b), \text{ by definition} \\ &= \psi(a) + \psi(b), \text{ since } \psi \text{ is a homomorphism} \\ &= \phi(a + K) + \phi(b + K). \end{aligned}$$

Also

$$\begin{aligned}\phi[(a+K)(b+K)] &= \phi[(ab)+K] \\ &= \psi(ab), \text{ by definition} \\ &= \psi(a)\psi(b), \text{ since } \psi \text{ is a homomorphism} \\ &= \phi(a+K)\phi(b+K).\end{aligned}$$

Therefore  $\phi$  is a homomorphism from  $V/K$  to  $V'$ .

Let us consider two elements  $a+K, b+K \in V/K$ . We now prove that  $\phi$  is one-one.

We have

$$\begin{aligned}\phi(a+K) = \phi(b+K) &\implies \psi(a) = \psi(b) \\ &\implies \psi(a) - \psi(b) = 0 \\ &\implies \psi(a-b) = 0 \\ &\implies a-b \in K \\ &\implies (a+K) = (b+K).\end{aligned}$$

Thus for any two elements  $a+K, b+K \in V/K$  we have

$$\phi(a+K) = \phi(b+K) \implies (a+K) = (b+K).$$

This proves that  $\phi$  is one-one.

Finally  $\phi$  is onto, because

**each element of  $V'$  is of the form  $\psi(a)$  for some  $a \in V$  and since the pre-image of**

$\psi(a)$  is  $a+K$  in  $V/K$ .

Thus  $\phi$  is an isomorphism and  $V/K$  is isomorphic to  $V'$ .

This completes the proof.

## Result

3 of 3

Considering a well defined map  $\phi : V/K \rightarrow V'$  we have shown that  $\phi$  is one-to-one and onto homomorphism by using the help of  $\psi$  which is onto hmomorphism from  $V$  to  $V'$ . Click for the complete solution.

11. a

**Given:**  $V$  is a vector space of dimension  $n$  over a field  $F$  and  $W$  is a subspace of  $V$  such that  $\dim_F W = m$ .

**To Prove:**  $\dim_F(V/W) = n - m$

## Step 2

2 of 4

**Proof:**

**Extension Theorem-** A linearly independent set of vectors in a finite dimensional vector space  $V$  over a field  $F$  is either a basis of  $V$ , or it can be extended to a basis of  $V$ .

Now return to the main question.

Since  $\dim_F W = m$ , let  $\{x_1, x_2, \dots, x_m\}$  be a basis of  $W$ .

Then by **Extension Theorem**, let  $\{x_1, x_2, \dots, x_m, x_{m+1}, \dots, x_n\}$  be a basis of  $V$ .

Let  $x + W \in V/W$ .

Then  $x \in V$ .

Then  $x$  can be expressed as  $x = c_1x_1 + c_2x_2 + \dots + c_mx_m + c_{m+1}x_{m+1} + \dots + c_nx_n$ , where  $c_i \in F$ .

$$\implies x - (c_{m+1}x_{m+1} + \dots + c_nx_n) = c_1x_1 + c_2x_2 + \dots + c_mx_m \in W.$$

$$\begin{aligned} \text{Therefore, } x + W &= (c_{m+1}x_{m+1} + \dots + c_nx_n) + W \\ &= (c_{m+1}x_{m+1} + W) + (c_{m+2}x_{m+2} + W) + \dots + (c_nx_n + W) \\ &= c_{m+1}(x_{m+1} + W) + c_{m+2}(x_{m+2} + W) + \dots + c_n(x_n + W). \end{aligned}$$

This shows that  $x + W$  belongs to the **linear span** of the vectors

$$\{x_{m+1} + W, x_{m+2} + W, \dots, x_n + W\}.$$

We now show that the set  $\{x_{m+1} + W, x_{m+2} + W, \dots, x_n + W\}$  is **linearly independent**.

Let us consider the relation

$$p_{m+1}(x_{m+1} + W) + p_{m+2}(x_{m+2} + W) + \dots + p_n(x_n + W) = \theta + W, \text{ where } p_i \in F \text{ and } \theta \text{ is the zero element of } V.$$

$$\text{Then } (p_{m+1}x_{m+1} + W) + (p_{m+2}x_{m+2} + W) + \dots + (p_nx_n + W) = W$$

$$\implies (p_{m+1}(x_{m+1} + p_{m+2}x_{m+2} + \dots + p_nx_n) + W = W$$

$$\implies p_{m+1}(x_{m+1} + p_{m+2}x_{m+2} + \dots + p_nx_n) \in W.$$

Since  $\{x_1, x_2, \dots, x_m\}$  is a basis of  $W$ ,

$$(p_{m+1}(x_{m+1} + p_{m+2}x_{m+2} + \dots + p_nx_n) = q_1x_1 + q_2x_2 + \dots + q_mx_m, \text{ for some } q_i \in F.$$

This gives

$$(p_{m+1}(x_{m+1} + p_{m+2}x_{m+2} + \dots + p_nx_n) - (q_1x_1 + q_2x_2 + \dots + q_mx_m) = \theta$$

Since  $\{x_1, x_2, \dots, x_m, x_{m+1}, \dots, x_n\}$  is a linearly independent set in  $V$ , we have

$$q_1 = q_2 = \dots = q_m = 0 \text{ and } p_{m+1} = p_{m+2} = \dots = p_n = 0.$$

This proves that the set  $\{x_{m+1} + W, x_{m+2} + W, \dots, x_n + W\}$  is linearly independent.

So it is a basis of  $V/W$ .

The dimension of  $V/W = (n - (m + 1)) + 1 = n - m = \dim_F V - \dim_F W$ .

This completes the proof.

12. a

**To Prove:** Let  $V$  be a vector space of dimension  $n$  over a field  $F$ . Then  $V$  is isomorphic to  $F^n$ .

**Proof:** Let  $(b_1, b_2, \dots, b_n)$  be an ordered basis of  $V$ . Then any vector  $v$  of  $V$  can be expressed as

$$v = c_1b_1 + c_2b_2 + \dots + c_nb_n,$$

where  $c_1, c_2, \dots, c_n$  are unique scalars in  $F$ .

Let us define a mapping  $\phi : V \rightarrow F^n$  by the assignment

$$\phi(v) = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}, \text{ where } v = (c_1b_1 + c_2b_2 + \dots + c_nb_n) \in V.$$

Let us now consider

$$\begin{aligned} x &= \sum_{k=1}^n x_k b_k \in V \\ y &= \sum_{k=1}^n y_k b_k \in V. \end{aligned}$$

Then

$$x + y = (x_1 + y_1)b_1 + (x_2 + y_2)b_2 + \dots + (x_n + y_n)b_n \in V.$$

Now

$$\begin{aligned} \phi(x) &= \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad \phi(y) = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \text{ and} \\ \phi(x + y) &= \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \phi(x) + \phi(y) \dots\dots\dots(1) \end{aligned}$$

Let us assume  $p \in F$ . Then  $px \in V$  and

$$px = (px_1)b_1 + (px_2)b_2 + \dots + (px_n)b_n.$$

Then

$$\phi(px) = \begin{pmatrix} px_1 \\ px_2 \\ \vdots \\ px_n \end{pmatrix} = p \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = p\phi(x) \dots\dots\dots(2)$$

From (1) and (2) we have concluded that  $\phi$  is a homomorphism.

To prove that  $\phi$  is one-to-one, let  $x, y \in V$  be such that

$$\begin{aligned}\phi(x) &= \phi(y), \text{ where } x = \sum_{k=1}^n x_k b_k \in V \\ y &= \sum_{k=1}^n y_k b_k \in V.\end{aligned}$$

Now

$$\begin{aligned}\phi(x) = \phi(y) &\implies \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ &\implies x_1 = y_1, x_2 = y_2, \dots, x_n = y_n \\ &\implies x = y.\end{aligned}$$

So,  $\phi$  is one-to-one.

To prove that  $\phi$  is onto, let

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$$

be an element in  $F^n$ .

Then

$$r_1 b_1 + r_2 b_2 + \dots + r_n b_n \in V.$$

And we have

$$\phi(r_1 b_1 + r_2 b_2 + \dots + r_n b_n) = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}.$$

So  $\phi$  is onto.

**Since  $\phi$  is a homomorphism which is both one-to-one and onto,  $\phi$  is an isomorphism.**

**Since  $\phi$  is an isomorphism,  $V$  is isomorphic to  $F^n$ .**

This completes our proof.

## Result

4 of 4

Considering an ordered basis of  $V$  and a map  $\phi : V \rightarrow F^n$ , we have shown that the map  $\phi$  is both one-to-one and onto together with  $\phi$  is a homomorphism, hence an isomorphism between  $V$  and  $F^n$ . Click for the detailed proof.

13. a

(13) Let  $F \subset K$  be two fields.

Assume  $K$  as a vector space over  $F$ .

$$\dim_F K = n$$

$\Rightarrow$  cardinality of maximal linearly independent set is  $n$ .

Hence for  $a \in K$ ,  $\{1, a, a^2, \dots, a^n\}$  is linearly dependent since  $|\{1, a, a^2, \dots, a^n\}| = n+1$ .  
there exist  $d_0, \dots, d_n \in F$  s.t.

$$d_0 \cdot 1 + d_1 \cdot a + \dots + d_n \cdot a^n = 0.$$

14. a

(14)  $F[x] =$  the polynomial ring in  $x$  over  $F$ ,  
 $0 \neq f(x) \in F[x]$   $\deg f(x) = n$ .

by remainder theorem, for any  $g(x) \in F[x]$

$$g(x) = h(x) f(x) + r(x)$$

for some  $h(x), r(x)$  in  $F[x]$

s.t  $\deg(r(x)) < \deg f(x)$ .

or  $r(x) = 0$ .

$$J = \langle f(x) \rangle \text{ in } F[x].$$

$$V = F[x]/J.$$

Consider the set  $\{1+J, x+J, \dots, x^{n-1}+J\} = B$ .

since any  $g(x) \in F[x]$  can be written as

linear combination of elements of above set

(since  $r(x)$  (corresponding to  $g(x)$ ) can  
be written in terms of  $\{1, x, \dots, x^{n-1}\}$ )

$\Rightarrow$  set  $B$  spans  $F[x]/J$ .

$$\text{further } c_1(1+J) + \dots + c_n(x^{n-1}+J) = 0, c_i \in F.$$

$$\Rightarrow c_i = 0 \text{ since } J = \langle f(x) \rangle.$$

Hence  $B$  is a basis

$$\& \dim V = \deg f(x) = n.$$

15. a

15) Let  $V$  and  $W$  be vector spaces over  $F$ .

also  $\dim_F V = n$ ,  $\dim_F W = m$

then claim:  $\dim_F(V \oplus W) = m+n$

Proof: Let  $\{v_1, \dots, v_n\}$  be a  $F$ -basis of  $V$ .  
 &  $\{w_1, \dots, w_m\}$  be a  $F$ -basis of  $W$ .

then  $\{(v_1, 0), \dots, (v_n, 0), (0, w_1), \dots, (0, w_m)\}$  is  
 a basis of  $V \oplus W$  over  $F$ .

since

$$(i) \sum_{i=1}^n c_i(v_i, 0) + \sum_{k=1}^m d_k(0, w_k) = 0.$$

$$c_i, d_k \in F.$$

$$\Rightarrow \sum_{i=1}^n c_i v_i = 0 \quad \& \quad \sum_{k=1}^m d_k w_k = 0$$

$$\Rightarrow c_i = 0 \quad \& \quad d_k = 0 \quad \forall 1 \leq i \leq n \\ \& \quad 1 \leq k \leq m$$

i.e. the set  $\{(v_1, 0), \dots, (v_n, 0), (0, w_1), \dots, (0, w_m)\}$  is L.I.

(ii) Let  $(v, w) \in V \oplus W$ .

$$\text{then } v = \sum_{i=1}^n c_i v_i \quad \& \quad w = \sum_{k=1}^m d_k w_k$$

$$\Rightarrow (v, w) = \sum_{i=1}^n c_i(v_i, 0) + \sum_{k=1}^m d_k(0, w_k)$$

$$\text{Hence } V \oplus W = \text{span}\{(v_1, 0), \dots, (v_n, 0), (0, w_1), \dots, (0, w_m)\}$$

Therefore by (i) & (ii)

$$\dim_F(V \oplus W) = \dim_F V + \dim_F W.$$

16. a

**Given:**  $V$  is a vector space over a field  $F$  and  $U, W$  are two subspaces of  $V$ .

**To Prove:**

- (a)  $U + W$  is a subspace of  $V$ .
- (b)  $U + W$  is finite dimensional over  $F$  if both  $U$  and  $W$  are.
- (c)  $U \cap W$  is a subspace of  $V$ .
- (d)  $U + W$  is a homomorphic image of  $U \oplus W$ .
- (e) If  $U$  and  $W$  are finite dimensional over  $F$ , then

$$\dim_F(U + W) = \dim_F(U) + \dim_F(W) - \dim_F(U \cap W).$$

**Proof:** By the given condition,  $U$  and  $V$  are subspaces of the vector space  $V$  over the field  $F$ . Then the linear sum of  $U$  and  $V$  is defined as

$$U + V := \{u + w \mid u \in U, w \in V\}.$$

(a) We show that  $U + V$  is a subspace of  $V$ .

Let us consider

$$S = U + V = \{u + w \mid u \in U, w \in V\}.$$

Then

$$0 \in U, 0 \in V \implies 0 \in U + V \text{ and therefore } S \text{ is non-empty.}$$

Let us consider  $a_1, a_2 \in S$ .

Then

$$\begin{aligned} a_1 &= u_1 + w_1 \text{ for some } u_1 \in U, w_1 \in V; \\ a_2 &= u_2 + w_2 \text{ for some } u_2 \in U, w_2 \in V. \end{aligned}$$

Since  $u_1 + u_2 \in U$  and  $w_1 + w_2 \in V$  we have

$$a_1 + a_2 = (u_1 + u_2) + (w_1 + w_2) \in S.$$

Let  $c$  be a scalar in  $F$ .

Then

$$\begin{aligned} ca_1 &= c(u_1 + w_1) \\ &= cu_1 + cw_1 \in S, \text{ since } cu_1 \in U, cw_1 \in V. \end{aligned}$$

Therefore,

$$\begin{aligned} a_1 \in S, a_2 \in S &\implies a_1 + a_2 \in S; \\ c \in F, a_1 \in S &\implies ca_1 \in S. \end{aligned}$$

This proves that  $S$  is a subspace of  $V$ , that is,  $U + V$  is a subspace of  $V$ .

This completes the proof of (a).

(c) We will prove that  $U \cap W$  is a subspace of  $V$ .

Now  $U \cap W$  is non-empty, since

$$0 \in U, 0 \in W \implies 0 \in U \cap W.$$

**Case-1:** Let  $U \cap W = \{0\}$ .

Then trivially  $U \cap W$  is a subspace of  $V$ .

**Case-2:** Let  $U \cap W \neq \{0\}$ .

Let us consider

$$a_1 \in U \cap W \text{ and } a_2 \in U \cap W.$$

Then we have

$$a_1, a_2 \in U \text{ and } a_1, a_2 \in W.$$

Since  $U$  and  $W$  are subspaces of  $V$ ,

$$a_1 + a_2 \in U \text{ and } ca_1 \in U, c \text{ being a scalar in } F; \quad (1)$$

$$a_1 + a_2 \in W \text{ and } ca_1 \in W, c \text{ being a scalar in } F. \quad (2)$$

Therefore from (1) and (2) it follows that

$$a_1 + a_2 \in U \cap W \text{ and } ca_1 \in U \cap W.$$

This proves that  $U \cap W$  is a subspace of  $V$ .

(d) We know that  $U \oplus W$  is a subspace of  $V$  such that every vector  $\alpha$  in  $U \oplus W$  has a unique representation of the form

$$\alpha = u + w, \text{ where } u \in U, w \in W.$$

Let us consider a homomorphism  $f : U \oplus W \rightarrow V$  by the assignment

$$f(\alpha) = u + w, \text{ where } \alpha \in U \oplus W.$$

In the above defined homomorphism  $u$  and  $w$  are the components of  $\alpha$  along  $U$  and  $W$  respectively. Then it is clear that,  $f$  is well defined. Also  $f$  is a homomorphism (given).

Clearly it follows that, for any  $\alpha$  in  $U \oplus W$ , there exist unique  $u \in U$  and  $w \in W$  such that  $\alpha = u + w$ . Hence, the image of  $U \oplus W$  under  $f$  is  $U + W$ . Thus  $U + W$  is a homomorphic image of  $U \oplus W$ .

Before proving the last one, we will start with a Lemma.

**Lemma:** If  $U$  be a subspace of a finite dimensional vector space  $V$  and  $\dim V = n$ , then  $U$  is finite dimensional and  $\dim U \leq n$ .

**Proof of the Lemma:** If  $U = \{0\}$ . Then trivially  $\dim(U) = 0 < n$ .

So let us assume that  $U \neq \{0\}$ . Then there exists a non-zero vector, say  $a$ , in  $U$ .

If  $\langle a \rangle = U$  then we have a finite basis  $\{a\}$  for  $U$ . If not, there is a non-zero vector  $b$  in  $U$  such that the set  $\{a, b\}$  is linearly independent.

If  $\langle a, b \rangle = U$  then we have a finite basis  $\{a, b\}$  for  $U$ . If not, the process can be continued and after a finite number of steps we get a linearly independent set  $S$  forming a basis of  $U$ .  $S$  being linearly independent set in  $V$  also,  $S$  contains at most  $n$  vectors.

Therefore, we have

$$\dim(U) \leq n.$$

This completes the Lemma.

(e) Since  $U$  and  $W$  are finite dimensional, then by the above lemma  $U \cap W$  is finite dimensional.

Let us assume

$$\dim(U \cap W) = r, \quad \dim(U) = r + s, \quad \dim(W) = r + t.$$

Let  $S = \{a_1, a_2, \dots, a_r\}$  be a basis for  $U \cap W$  and let  $S'$  be supplemented by additional vectors  $b_1, b_2, \dots, b_s$  to make up a basis for  $U$ .

Similarly, let  $S$  be supplemented by additional vectors  $x_1, x_2, \dots, x_t$  to make up a basis for  $W$ .

We propose to prove that

$$B = \{a_1, a_2, \dots, a_r, b_1, b_2, \dots, b_s, x_1, x_2, \dots, x_t\}$$

is a basis for  $U + W$ .

Clearly it follows that

$$B \subset U + W.$$

Therefore linear span of the set  $B$  is a subset of  $U + W$ , that is,

$$\langle B \rangle \subset U + W.$$

Any vector  $\phi$  in  $U + W$  is of the form  $u + w$  where

$$u \in \langle a_1, \dots, a_r, b_1, \dots, b_s \rangle \text{ and } w \in \langle a_1, \dots, a_r, x_1, \dots, x_t \rangle.$$

Therefore we have

$$U + W \subset \langle B \rangle.$$

Consequently

$$U + W = \langle B \rangle.$$

In order to establish linearly independence of the set  $B$ , let

$$j_1a_1 + j_2a_2 + \dots + j_ra_r + k_1b_1 + k_2b_2 + \dots + k_sb_s + l_1x_1 + l_2x_2 + \dots + l_tx_t = 0,$$

for some scalars  $j_i, k_i, l_i \in F$ .

Then we have

$$j_1a_1 + j_2a_2 + \dots + j_ra_r + k_1b_1 + k_2b_2 + \dots + k_sb_s = -(l_1x_1 + l_2x_2 + \dots + l_tx_t).$$

We observe that the left hand vector belongs to  $U$ . Hence the right hand vector belongs to both  $U$  and  $W$  and so is in  $U \cap W$ .

Therefore we have

$$-(l_1x_1 + l_2x_2 + \dots + l_tx_t) = d_1a_1 + d_2a_2 + \dots + d_ra_r \text{ for some } d_i \in F.$$

$$\implies l_1x_1 + l_2x_2 + \dots + l_tx_t + d_1a_1 + d_2a_2 + \dots + d_ra_r = 0.$$

But since the vectors  $a_1, a_2, \dots, a_r, x_1, x_2, \dots, x_t$  constitute a basis for  $W$ , the above relation implies

$$l_1 = l_2 = \dots = l_t = d_1 = d_2 = \dots = d_r = 0.$$

Therefore we have

$$j_1a_1 + j_2a_2 + \dots + j_ra_r + k_1b_1 + k_2b_2 + \dots + k_sb_s = 0.$$

Since the vectors  $a_1, a_2, \dots, a_r, b_1, b_2, \dots, b_s$  constitute a basis for  $U$ , we have

$$j_1 = j_2 = \dots = j_r = k_1 = k_2 = \dots = k_s = 0.$$

Since all scalars  $j_i, k_i, l_i$  are shown to be zero, we conclude that the set  $B$  is linearly independent and we have already shown that  $B$  generates  $U + W$ . Thus  $B$  is a basis for  $U + W$ .

Hence we have

$$\dim_F(U + W) = r + s + t = \dim_F(U) + \dim_F(W) - \dim_F(U \cap W).$$

This completes the proof of (e).

Now left to show (b).

(b) Since  $U$  and  $V$  are finite dimensional, then by the aforeproved lemma we have  $U \cap W$  is finite dimensional.

And by the above formula we have  $\dim_F(U + W)$  is finite dimensional.

This completes the proof.

## Result

7 of 7

Using vector subspace criterion of linearity, we have shown that  $U + W$  and  $U \cap W$  are subspace of  $V$  and using basis of  $U, W$  we have proved the last formula and the others derived from these above. Click for the complete proof.

17. a

### Part a.

Properties 1 - 3 from definition of vector space on page 180 are trivially satisfied, since  $V$  is vector space over  $K$  and  $F \subset K$ . Fourth condition is valid as well, because unity from  $F$  is the same as unity from  $K$ .

### Part b.

From  $\dim_F(K) = m$  we know that there are elements  $k_1, k_2, \dots, k_m \in K$  such that  $\{k_1, k_2, \dots, k_m\}$  is linearly independent and spans  $K$  over  $F$ .

Since  $V$  is finite dimensional over  $K$ , there are elements  $v_1, v_2, \dots, v_n \in V$  such that  $\langle v_1, v_2, \dots, v_n \rangle_K = V$ .

Now take any element  $v \in V$ . First there are elements  $\alpha_1, \alpha_2, \dots, \alpha_n \in K$  such that

$$v = \sum_{i=1}^n \alpha_i v_i. \quad (*)$$

Now for each  $\alpha_i \in K$ , there are elements  $\beta_{i1}, \beta_{i2}, \dots, \beta_{im} \in F$  such that

$$\alpha_i = \sum_{j=1}^m \beta_{ij} k_j.$$

Plugging this into equation (\*), we get

$$v = \sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^n \left( \sum_{j=1}^m \beta_{ij} k_j \right) v_i = \sum_{i=1}^n \sum_{j=1}^m \beta_{ij} (k_j v_i).$$

By property of vector space  $V$  over field  $K$ , we have that  $k_j v_i \in V$  for all  $i, j$ . But this means that we have succeeded in showing any element of  $V$  as a **linear combination of finite number of its elements with coefficients from field  $F$** . This directly implies that  $V$  is finite dimensional over  $F$  as well.

**Part c.**

We expand on the proof of **part b** to solve this part. This time say that set  $\{v_1, v_2, \dots, v_n\}$  is linearly independent and spans  $V$  over  $K$ .

We immediately conclude that set  $\{k_j v_i; j = 1, 2, \dots, m, i = 1, 2, \dots, n\}$  spans  $V$  over  $F$ . Now we have to prove that this set is linearly independent over  $F$ .

Therefore, for  $i = 1, 2, \dots, n$  and  $j = 1, 2, \dots, m$ , take any  $\gamma_{ij} \in F$  such that

$$0 = \sum_{i=1}^n \sum_{j=1}^m \gamma_{ij} (k_j v_i) = \sum_{i=1}^n \left( \sum_{j=1}^m \gamma_{ij} k_j \right) v_i.$$

We need to prove that  $\gamma_{ij} = 0$ , for all  $i = 1, 2, \dots, n$  and  $j = 1, 2, \dots, m$ .

From this second formulation, where the coefficients in brackets are from the field  $K$ , and the fact that set  $\{v_1, v_2, \dots, v_n\}$  is linearly independent over  $K$ , we conclude that for each  $i = 1, 2, \dots, n$  we must have

$$\sum_{j=1}^m \gamma_{ij} k_j = 0.$$

Now we use the linear independence of set  $\{k_1, k_2, \dots, k_m\}$  over  $F$  to conclude that for all  $j = 1, 2, \dots, m$  it must be  $\gamma_{ij} = 0$ .

## Result

Remember the definition of finite dimensionality of vector space and use it carefully.

### 18. a

Say that  $\dim_F(V) = n$ ; then there is linearly independent set  $\{v_1, v_2, \dots, v_n\}$  which spans  $V$  over  $F$ . Analogously, if we let  $\dim_F(K) = m$ , then there is linearly independent set  $\{k_1, k_2, \dots, k_m\}$  which spans  $K$  over  $F$ .

Now, since  $F$  is a subset of  $K$ , it is obvious that same set  $\{v_1, v_2, \dots, v_n\}$  spans  $V$  over  $K$  as well, which means that  $\dim_K(V)$  is finite. Let us now determine its exact size. So far we are convinced it is less or equal to  $n$ .

Take any set  $\{u_1, u_2, \dots, u_\ell\}$  of vectors from  $V$  over field  $K$ . We need to determine what is the greatest possible of  $\ell$  for which this set can be linearly independent. That number is precisely the desired dimension, by **Theorem 5.2.6**.

Take  $\alpha_1, \alpha_2, \dots, \alpha_\ell \in K$  such that

$$\sum_{i=1}^{\ell} \alpha_i u_i = 0. \quad (*)$$

Then for each  $\alpha_i$  find scalars  $\beta_{i1}, \beta_{i2}, \dots, \beta_{im} \in F$  such that

$$\alpha_i = \sum_{j=1}^m \beta_{ij} k_j.$$

Plugging the last expression into equation  $(*)$ , we obtain

$$\sum_{i=1}^{\ell} \sum_{j=1}^m \beta_{ij} (k_j u_i) = 0.$$

Now, we know that  $\dim_F(V)$  is equal to  $n$ . This means that if there is more than  $n$  vectors  $k_j v_i \in V$ , then the set of vectors

$$\{k_j v_i : j = 1, 2, \dots, m, i = 1, 2, \dots, \ell\}$$

is surely not linearly independent. Then some of  $\beta$ 's would not be zero, and consequently some of  $\alpha$ 's would not be zero, hence making the original set  $\{u_1, u_2, \dots, u_\ell\}$  linearly dependent. Therefore, we conclude that there are at most  $n$  vectors in this set, i.e. since their number is exactly  $m \cdot \ell$ , we obtain  $\boxed{m \cdot \ell \leq n}$ .

Remember that we were looking for greatest value of  $\ell$ , which equals  $\dim_K(V)$ .

So finally, we have that  $\boxed{\dim_K(V) = \frac{n}{m} = \frac{\dim_F(V)}{\dim_F(K)}}$ .

*Note that we could obtain the same value more elegantly by calling upon the result of previous Exercise.*

## Result

Use the result of previous Exercise, or follow the more complicated proof presented here.

### 19. a

**Given:**  $D$  be an integral domain with 1, and  $F$  be a field.

Let,  $D$  be a finite dimensional vector space over  $F$ .

**To Prove:**  $D$  is a field.

#### Proof:

We need to show that

**any nonzero  $r \in D$  has an inverse.**

Since  $D$  is

**finite dimensional over  $F$ , we have  $\{1, r, r^2, \dots, r^n\}$  is a linear dependent set for some finite  $n$  over  $F$**

In particular, if  $r \neq 0$  and  $r \in D$ , then

$$a_n r^n + a_{n-1} r^{n-1} + \dots + a_0 = 0$$

has a **nontrivial solution** where each  $a_i \in F$ .

If  $a_0 = 0$  then

$$\begin{aligned} a_n r^n + a_{n-1} r^{n-1} + \dots + a_1 r &= 0 \\ \implies r(a_n r^{n-1} + a_{n-1} r^{n-2} + \dots + a_1) &= 0 \\ \implies a_n r^{n-1} + a_{n-1} r^{n-2} + \dots + a_1 &= 0 \end{aligned}$$

since  $D$  is an integral domain.

If  $a_1 = 0$  repeat the previous step.

Clearly this

**process will terminate once we get to some nonzero  $a_i$**

Therefore we may assume without loss of generality that  $a_0 \neq 0$ . But then

$$\begin{aligned} a_n r^n + a_{n-1} r^{n-1} + \cdots + a_0 &= 0 \\ \implies a_n r^n + a_{n-1} r^{n-1} + \cdots + a_1 r &= -a_0 \\ \implies b_n r^n + b_{n-1} r^{n-1} + \cdots + b_1 r &= 1 \\ \implies r(b_n r^{n-1} + b_{n-1} r^{n-2} + \cdots + b_1) &= 1 \end{aligned}$$

where  $b_i = -a_0^{-1} a_i$ , showing that

**$r$  has an Inverse in  $D$**

Therefore

**every non-zero elements in  $D$  has inverse.**

**$D$  being an integral domain, it is a field.**

This completes the proof.

## Result

3 of 3

Being a finite dimensional vector space and an integral domain, we prove that every non-zero element of  $D$  has a multiplicative inverse and hence it is a field. Click for the detailed proof.

## 20. a

**Given:** Let  $F$  be an infinite field and  $V$  be a vector space over  $F$ .

**To Prove:**  $V$  cannot be written as set-theoretic union of a finite number of proper subspaces.

**Proof:**

If possible, let  $V$  is the set-theoretic union of  $n$  proper subspaces

$U_i$  ( $1 \leq i \leq n$ ), that is,  $V = \cup_{i=1}^n U_i$ .

Without loss of generality we may assume that

no  $U_i$  is contained in the union of other subspaces.

Let us consider

$u \in U_i$  but  $u \notin \cup_{j \neq i} U_j$  and  $v \notin U_i$ .

Then we have,

$$(v + Fu) \cap U_i = \emptyset$$

and  $(v + Fu) \cap U_j$  ( $j \neq i$ ) contains at most one vector since otherwise  $U_j$  would contain  $u$ .

Hence

$$|v + Fu| = |F| \leq n - 1.$$

Since  $n$  if a finite natural number, it contradicts the fact that the given field  $F$  is finite.

|| Therefore our assumption that

" $V$  can be written as set-theoretic union of proper subspaces  $U_i$  ( $1 \leq i \leq n$ )"

is wrong.

Hence,

$V$  cannot be written as set-theoretic union of a finite number of proper subspaces.

This completes the proof.

## Section 5–3

1. a

**Answer for (a).** Suppose  $\alpha = \sqrt{2} + \sqrt{3}$ , then

$$\begin{aligned}\alpha^2 &= 2 + 2\sqrt{2}\sqrt{3} + 3 \\ \implies \alpha^2 &= 5 + 2\sqrt{6} \\ \implies \alpha^2 - 5 &= 2\sqrt{6} \\ \implies (\alpha^2 - 5)^2 &= (2\sqrt{6})^2 \\ \implies \alpha^4 - 10\alpha^2 + 25 &= 24 \\ \implies \alpha^4 - 10\alpha^2 + 1 &= 0\end{aligned}$$

So  $\alpha$  is a root of  $f(x) = 0$  where  $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$ . Hence  $\sqrt{2} + \sqrt{3}$  is an algebraic number.

**Answer for (b).** Suppose  $\beta = \sqrt{7} + \sqrt[3]{12}$  then,

$$\begin{aligned}\beta - \sqrt{7} &= \sqrt[3]{12} \\ \implies (\beta - \sqrt{7})^3 &= (\sqrt[3]{12})^3 \\ \implies \beta^3 - 3\beta^2\sqrt{7} + 3\beta(\sqrt{7})^2 - (\sqrt{7})^3 &= 12 \\ \implies \beta^3 + 21\beta - 12 - \sqrt{7}(3\beta^2 + 7) &= 0 \\ \implies (\beta^3 + 21\beta - 12)^2 &= (\sqrt{7})^2(3\beta^2 + 7)^2 \\ \implies \beta^6 + 441\beta^2 + 144 + 42\beta^4 - 24\beta^3 - 504\beta &= 7(9\beta^4 + 42\beta^2 + 49) \\ \implies \beta^6 - 21\beta^4 - 24\beta^3 + 420\beta^2 - 504\beta - 199 &= 0\end{aligned}$$

So  $\beta$  satisfies  $g(x) = 0$ , where

$$g(x) = x^6 - 21x^4 - 24x^3 + 420x^2 - 504x - 199 \in \mathbb{Z}[x].$$

Hence  $\sqrt{7} + \sqrt[3]{12}$  is an algebraic number.

**Answer for (c).** Suppose  $\gamma = 2 + i\sqrt{3}$ , where  $i^2 = -1$ , then

$$\begin{aligned}\gamma - 2 &= i\sqrt{3} \\ \implies (\gamma - 2)^2 &= (i\sqrt{3})^2 \\ \implies \gamma^2 - 4\gamma + 4 &= -3 \\ \implies \gamma^2 - 4\gamma + 7 &= 0.\end{aligned}$$

So  $\gamma$  is a root of  $h(x) = 0$ , where

$$h(x) = x^2 - 4x + 7 \in \mathbb{Z}[x].$$

Hence  $2 + i\sqrt{3}$  is an algebraic integer.

**Answer for (d).** Suppose  $\delta = \cos\left(\frac{2\pi}{k}\right) + i \sin\left(\frac{2\pi}{k}\right)$ , where  $k$  is a positive integer.

Now we know that

$$\begin{aligned}\delta^k &= \left(\cos\left(\frac{2\pi}{k}\right) + i \sin\left(\frac{2\pi}{k}\right)\right)^k \\ &= \cos\left(\frac{2k\pi}{k}\right) + i \sin\left(\frac{2k\pi}{k}\right) \\ &= (\cos 2\pi + i \sin 2\pi) \\ &= 1 + i \cdot 0 \\ &= 1\end{aligned}$$

So,  $\delta$  satisfies  $x^k - 1 = 0$  and  $x^k - 1 \in \mathbb{Z}[x]$ . Hence  $\delta$  is an algebraic number.

## 2. a

### Part 1:

Here  $\alpha = \sqrt{2} + \sqrt{3}$ . Now  $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 4$ , since  $\alpha$  satisfies a polynomial in  $\mathbb{Z}[x]$  of degree 4. We will show that  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ . It is enough to show that  $f(x) = x^4 - 10x^2 + 1$  is irreducible in  $\mathbb{Q}[x]$ . Suppose, if possible  $x^4 - 10x^2 + 1$  is not irreducible.

$$x^4 - 10x^2 + 1 = h_1(x)h_2(x),$$

where  $\deg(h_1(x)), \deg(h_2(x)) \geq 1$ . As  $x^4 - 10x^2 + 1$  is in  $\mathbb{Z}[x]$  and a monic polynomial so by Gauss lemma

$h_1(x)$  and  $h_2(x)$  are in  $\mathbb{Z}[x]$  and monic. Now roots of

$x^4 - 10x^2 + 1 = 0$  are  $\pm\sqrt{2} \pm \sqrt{3}$  i.e. no roots of  $f(x)$  is in  $\mathbb{Q}$ . So  $f(x)$  does not have any linear factor in  $\mathbb{Z}[x]$ .

So  $h_1(x)$  and  $h_2(x)$  both are monic quadratic polynomials.

Let  $h_1(x) = x^2 + ax + b$  and  $h_2(x) = x^2 + cx + d$ , where  $a, b, c, d \in \mathbb{Z}$ . Now We have

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d).$$

Comparing the coefficients of  $x$  in both side we get

$$a + c = 0 \quad (1)$$

$$ac + b + d = -10 \quad (2)$$

$$ad + bc = 0 \quad (3)$$

$$bd = 1 \quad (4)$$

Now if  $a = c = 0$ , then

$$\begin{aligned} b + d &= -10 \\ bd &= 1 \end{aligned}$$

which does not have solution in  $\mathbb{Z}$ . So suppose  $a, c \neq 0$ , then  $a = -c$

$$\begin{aligned} b - d &= 0 \\ bd &= 1 \end{aligned}$$

So from equation (2) we get that

$$-a^2 + 2b = -10, \text{ where } b = \pm 1.$$

It is easily verified that above equation does have solutions in  $\mathbb{Z}$ . So, our assumption is wrong. Therefore,  $f(x)$  is irreducible polynomial. We are done.

#### Part 2:

$\gamma = 2 + i\sqrt{3}$ , where  $i^2 = -1$ , and  $\gamma$  satisfies  $h(x) = x^2 - 4x + 7 = 0$ . Now  $h(x)$  is irreducible in  $\mathbb{Z}[x]$  because its roots are  $2 \pm i\sqrt{3}$  which are not  $\mathbb{Q}$ . Therefore,  
 $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2$ .

#### Result

[Click Here To See The Explanation.](#)

3. a

$$\begin{aligned}
& \text{Let } \alpha = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) \\
& \implies \alpha = \frac{1}{2} + i \frac{\sqrt{3}}{2} \\
& \implies \alpha - \frac{1}{2} = i \frac{\sqrt{3}}{2} \\
& \implies (\alpha - \frac{1}{2})^2 = (i \frac{\sqrt{3}}{2})^2 \\
& \implies \alpha^2 - \alpha + \frac{1}{4} = \frac{-3}{4} \\
& \implies \alpha^2 - \alpha + 1 = 0.
\end{aligned}$$

So,  $\alpha$  satisfies  $x^2 - x + 1 = 0$  where  $x^2 - x + 1 \in \mathbb{Q}[x]$  is irreducible. Since, it is a quadratic and roots are  $\frac{1}{2} \pm i \frac{\sqrt{3}}{2}$ , which are not elements of  $\mathbb{Q}$ .

Therefore, degree of  $\cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$  over  $\mathbb{Q}$  is 2.

## Result

2 of 2

Final Answer: 2

## 4. a

Let  $\beta = \cos\left(\frac{2\pi}{8}\right) + i \sin\left(\frac{2\pi}{8}\right)$ , then

$$\begin{aligned}
\beta^4 &= \left(\cos\left(\frac{2\pi}{8}\right) + i \sin\left(\frac{2\pi}{8}\right)\right)^4 \\
&= \left(\cos\left(\frac{2.4\pi}{8}\right) + i \sin\left(\frac{2.4\pi}{8}\right)\right) \quad (\text{by De Moivre's theorem}) \\
&= (\cos \pi + i \sin \pi) \\
&= -1
\end{aligned}$$

So,  $\beta$  satisfies  $x^4 + 1 = 0$ . Now  $[\mathbb{Q}(\beta) : \mathbb{Q}] \leq 4$ , since  $\beta$  satisfies a polynomial in  $\mathbb{Z}[x]$  of degree 4. We will show that

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = 4.$$

It is enough to show that  $f(x) = x^4 + 1$  is irreducible in  $\mathbb{Q}[x]$ . Suppose, if possible  $x^4 + 1$  is not irreducible.

$$x^4 + 1 = f_1(x)f_2(x),$$

where  $\deg(f_1(x)), \deg(f_2(x)) \geq 1$ . As  $x^4 + 1$  is in  $\mathbb{Z}[x]$  and a monic polynomial so by **Gauss lemma**  $f_1(x)$  and  $f_2(x)$  are in  $\mathbb{Z}[x]$  and monic. Now roots of

$$x^4 + 1 = 0 \text{ are } \pm \frac{1}{\sqrt{2}}(1 \pm i) \text{ i.e. no roots of } f(x) \text{ is in } \mathbb{Q}. \text{ So } f(x) \text{ does not have any linear factor in } \mathbb{Z}[x].$$

So  $f_1(x)$  and  $f_2(x)$  both are monic quadratic polynomials.

Let  $f_1(x) = x^2 + ax + b$  and  $f_2(x) = x^2 + cx + d$ , where  $a, b, c, d \in \mathbb{Z}$ . Now We have

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d).$$

Comparing the coefficients of  $x$  in both side we get

$$a + c = 0 \quad (1)$$

$$ac + b + d = 0 \quad (2)$$

$$ad + bc = 0 \quad (3)$$

$$bd = 1 \quad (4)$$

Now if  $a = c = 0$ , then

$$b + d = 0$$

$$bd = 1$$

which does not have solution in  $\mathbb{Z}$ . So suppose  $a, c \neq 0$ , then  $a = -c$

$$b - d = 0$$

$$bd = 1$$

So from equation (2) we get that

$$-a^2 + 2b = 0, \text{ where } b = \pm 1.$$

It is easily verified that above equation does have solutions in  $\mathbb{Z}$ . So, our assumption is wrong. Therefore,  $f(x)$  is irreducible polynomial. We are done.

## Result

Final Answer: 4

### 5. a

Let  $\alpha = \cos\left(\frac{2\pi}{p}\right) + i \sin\left(\frac{2\pi}{p}\right)$ , then

$$\begin{aligned} \alpha^p &= \left(\cos\left(\frac{2\pi}{p}\right) + i \sin\left(\frac{2\pi}{p}\right)\right)^p \\ &= \left(\cos\left(\frac{2p\pi}{p}\right) + i \sin\left(\frac{2p\pi}{p}\right)\right) \quad (\text{by De Moivre's theorem}) \\ &= \left(\cos(2\pi) + i \sin(2\pi)\right) \\ &= 1 \end{aligned}$$

So,  $\alpha$  is root of  $x^p - 1 = 0$ . Now

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

Now,  $\alpha \neq 1$  which imply  $\alpha$  is a root of  $x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$ .

Let  $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ . If we can show that  $f(x)$  is irreducible then we can conclude that  $f(x)$  is minimal polynomial of  $\alpha$  and degree of  $\alpha$  over  $\mathbb{Q}$  is  $p - 1$ .

Now if  $f(x)$  is reducible then  $f(x+1)$  is also reducible.  $f(x)$  can be written as follows

$$f(x) = \frac{x^p - 1}{x - 1}.$$

Therefore, we have

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{(x+1)^p - 1}{x} \end{aligned}$$

Now  $(x+1)^p - 1 = \sum_{r=0}^p \binom{p}{r} x^r$ . So, we have

$$f(x+1) = \sum_{r=1}^p \binom{p}{r} x^{r-1}.$$

Now the binomial coefficient  $\binom{p}{r}$  is divisible by  $p$  if  $1 \leq r \leq p-1$ , and  $\binom{p}{1} = p$  is not divisible by  $p^2$ .

Hence by **Eisenstein's criterion**  $f(x+1)$  is irreducible, where Eisenstein's criterion states that Suppose we have the following polynomial with integer coefficients.

$$q(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

If there exists a prime number  $p$  such that the following three conditions all apply:

1.  $p$  divides each  $a_i$  for  $i \neq n$ ,
2.  $p$  does not divide  $a_n$ , and
3.  $p^2$  does not divide  $a_0$ .

Then  $q(x)$  is irreducible.

Hence  $f(x)$  is irreducible. We are done.

## 6. a

We know that  $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \cdots$ .

Suppose, if possible,  $e$  is rational then  $e = \frac{p}{q}$ , where  $p \in \mathbb{Z}$  and  $q \in \mathbb{N}$ . Let

$$x_q = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{q!}.$$

Then

$$e - x_q = \frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \frac{1}{(q+3)!} + \cdots.$$

So

$$\frac{1}{(q+1)!} < e - x_q < \frac{1}{q!} \left( \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \cdots \right) = \frac{1}{q \cdot q!}.$$

Therefore

$$\frac{1}{q+1} < q! \cdot e - x_q \cdot q! < \frac{1}{q}.$$

This is a contradiction, since  $(q! \cdot e - x_q \cdot q!)$  is an integer.

## Result

Hence  $e$  is irrational.

## 7. a

Given that  $a^2$  is algebraic over the subfield  $F$  of  $K$ , we need to show that  $a$  is algebraic over  $F$ .

### Step 2

2 of 3

Since  $a^2$  is algebraic over  $F$ , there exist a non-zero polynomial  $f(x)$  in  $F[x]$  such that  $f(a^2) = 0$ . Consider a new polynomial  $g(x)$  defined as  $g(x) = f(x^2)$ . Clearly  $g(x) \in F[x]$  and  $g(a) = f(a^2) = 0$ .

### Result

3 of 3

Therefore,  $a$  is algebraic over  $F$ .

## 8. a

Given that  $F \subset K$ , let  $f(x) =$  where  $n \geq 1$  and, since degree of  $f$  is positive and  $a_i \in F$  for all  $i$ . Now

$$f(a) = a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0.$$

It is given that  $f(a)$  is algebraic, so there exists a polynomial

$$h(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \in F[x]$$

such that  $f(a)$  satisfies  $h(x) = 0$  i.e.  $h(f(a)) = 0$ .

$$\begin{aligned} h(f(a)) &= b_m f(a)^m + b_{m-1} f(a)^{m-1} + \cdots + b_1 f(a) + b_0 \\ &= b_m (a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0)^m + \cdots \\ &\quad + b_1 (a_n a^n + a_{n-1} a^{n-1} + \cdots + a_1 a + a_0) + b_0 \\ &= c_{mn} a^{mn} + c_{mn-1} a^{mn-1} + \cdots + c_1 a + c_0. \end{aligned}$$

Where  $c_j = \sum b_{k_1} a_{k_2}^r$ , so  $c_j \in F$  for all  $j$ . Now  $h(f(a)) = 0$  imply that

$$c_{mn} a^{mn} + c_{mn-1} a^{mn-1} + \cdots + c_1 a + c_0 = 0.$$

So,  $a$  satisfies  $c_{mn} x^{mn} + c_{mn-1} x^{mn-1} + \cdots + c_1 x + c_0 = 0$ .

### Result

Therefore,  $a$  is algebraic over  $F$ .

## 9. a

Here  $F(a) \cong F[x]/M$ , where  $M = (p(x))$ , where  $p(x) \in F[x]$  is irreducible polynomial such that  $p(a) = 0$ ,  $a \in K$ .

**To show:**  $F[x]/M$  is of degree  $n = \deg p(x)$ .

## Step 2

2 of 4

Let  $\theta \equiv x \pmod{p(x)} \in F[x]/M$ . Then our claim is the elements

$$1, \theta, \theta^2, \dots, \theta^{n-1}$$

are a basis for  $F[x]/M$ , so the degree of the extension is  $n$ .

Let  $a(x) \in F[x]$  be any polynomial be any polynomial. Since  $F$  is field, so  $F(x)$  is a Euclidean domain, we may divide  $a(x)$  by  $p(x)$ :

$$a(x) = q(x)p(x) + r(x)$$

$q(x), r(x) \in F[x]$  with  $\deg r(x) < n$ . Since  $q(x)p(x)$  is zero element in  $(p(x))$ , it follows that  $a(x) \equiv r(x) \pmod{p(x)}$ , which shows that every residue class in  $F(x)/(p(x))$  is represented by a polynomial of degree less than  $n$ . Hence the images

$1, \theta, \theta^2, \dots, \theta^{n-1}$  of  $1, x, x^2, \dots, x^{n-1}$  in the quotient span the quotient as a vector space over  $F$ .

It remains to see that these elements are linearly independent, so form a basis for the quotient over  $F$ .

If possible,  $1, \theta, \theta^2, \dots, \theta^{n-1}$  are linearly dependent in  $F(x)/(p(x))$  then there would be a linear combination

$$b_0 + b_1\theta + b_2\theta^2 + \dots + b_{n-1}\theta^{n-1} = 0$$

in  $F(x)/(p(x))$ , with  $b_0, b_1, b_2, \dots, b_{n-1} \in F$ , not all 0. Equivalently saying

$$b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1} \equiv 0 \pmod{p(x)}$$

i.e,

$$p(x) \text{ divides } b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1}$$

in  $F[x]$ . But it is not possible, since  $p(x)$  is of degree  $n$  and degree of the nonzero polynomial on the right is less than  $n$ . This proves that  $1, \theta, \theta^2, \dots, \theta^{n-1}$  are a

basis for  $F(x)/(p(x))$  over  $F$ . Therefore  $F[x]/M$  is of degree  $n$ .

And since  $F(a) \cong F[x]/M$ , so  $[F(a) : F] = n$ .

## Result

4 of 4

Therefore  $F[x]/M$  is of degree  $n$

10. a

This is another approach to solve this problem different from Sourav Panja's Solution.

## Step 2

**To Show:**  $\cos 1^\circ$  is algebraic over  $\mathbb{Q}$ .

Let  $\alpha = \cos 1^\circ + i \sin 1^\circ$ , then

$$\begin{aligned}\alpha^{180} &= (\cos 1^\circ + i \sin 1^\circ)^{180} \\ &= (\cos 180^\circ + i \sin 180^\circ) \quad (\text{by De Moivre's theorem}) \\ &= -1\end{aligned}$$

Now

$$(\cos 1^\circ + i \sin 1^\circ)^{180} = \sum_{r=0}^{180} \binom{180}{r} (\cos 1^\circ)^{180-r} (i \sin 1^\circ)^r.$$

Now

$$\sum_{r=0}^{180} \binom{180}{r} (\cos 1^\circ)^{180-r} (i \sin 1^\circ)^r = -1.$$

Consider the real part of left hand side, we get

$$\sum_{r=0}^{180} \binom{180}{r} (\cos 1^\circ)^{180-r} (i \sin 1^\circ)^r = -1, \quad \text{where } r \text{ runs over all even integers.} \quad (1)$$

Now

$$\begin{aligned}(i \sin 1^\circ)^{2n} &= (i)^{2n} (\sin 1^\circ)^{2n} \\ &= \pm (\sin^2 1^\circ)^n \\ &= \pm (1 - \cos^2 1^\circ)^n.\end{aligned}$$

Putting these in (1), we get

$$\begin{aligned}\sum_{n=0}^{90} \binom{180}{2n} (\cos 1^\circ)^{180-2n} (i \sin 1^\circ)^{2n} &= -1 \\ \implies \sum_{n=0}^{90} \binom{180}{2n} (\cos 1^\circ)^{180-2n} (\pm (1 - \cos^2 1^\circ)^n) &= -1\end{aligned}$$

So,  $\cos 1^\circ$  satisfies

$$\sum_{n=0}^{90} \binom{180}{2n} (x)^{180-2n} (\pm (1 - x^2)^n) + 1 = 0$$

and

$$\sum_{n=0}^{90} \binom{180}{2n} (x)^{180-2n} (\pm (1 - x^2)^n) + 1 \in \mathbb{Q}[x].$$

## Result

Therefore,  $\cos 1^\circ$  is algebraic over  $\mathbb{Q}$ .

## Method 2.

**To Prove:**  $\cos 1^\circ$  is algebraic over  $\mathbb{Q}$ .

### Step 2

2 of 3

**Proof:**

To see this, note that  $e^{2\pi i/360} = e^{\pi i/180}$  is

**algebraic over  $\mathbb{Q}$  because it is a root of the polynomial  $x^{360} - 1 \in \mathbb{Q}[x]$**

Therefore  $\mathbb{Q}(e^{\pi i/180})$  is an algebraic extension of  $\mathbb{Q}$ .

As such, any element of  $\mathbb{Q}(e^{\pi i/180})$  is algebraic over  $\mathbb{Q}$ .

Finally,

$$\frac{e^{\pi i/180} + e^{-\pi i/180}}{2} = \frac{\cos(\pi/180) + i \sin(\pi/180) + \cos(\pi/180) - i \sin(\pi/180)}{2} = \cos(\pi/180) = \cos(1^\circ)$$

Now,

$\mathbb{Q}(e^{\pi i/180})$  is closed under multiplication, so the fact that

$$e^{-\pi i/180} = \frac{1}{e^{\pi i/180}}$$
 implies  $\cos(1^\circ) \in \mathbb{Q}(e^{\pi i/180})$

, completing the proof.

## 11. a

It is a good thing that  $a \in K$  is transcendental, because this means that there is no polynomial  $g(x) \in F[x]$  such that  $g(a) = 0$ , so we don't have to worry about zero in denominator. Hence, set

$$F(a) = \{ f(a)/g(a) \mid f(x), g(x) \neq 0 \in F[x] \}$$

is at least well-defined.

Let's prove first that  $F(a)$  is indeed a field. Since  $f(a), g(a) \in K$  for any  $f(x), g(x) \in F[x]$ , it follows  $f(a)/g(a) = f(a)g(a)^{-1} \in K$ , which implies that  $F(a) \subset K$ . Thus we have to show that  $F$  is subfield of  $K$ . Therefore, prove we take any  $f, f', g, g' \in F[x]$  and compute

$$(f(a)/g(a)) \cdot (f'(a)/g'(a))^{-1} = (f(a)g'(a)) / (g(a)f'(a)) \in F(a).$$

This is enough to prove that  $F$  is subfield of  $K$ .

Finally, we prove the last assertion, i.e. that  $F(a)$  is the smallest subfield of  $K$  containing both  $F$  and  $a$ . It is apparent that  $F(a)$  contains both  $a$  (take  $f(x) = x$  and  $g(x) = 1$ ) and whole set  $F$  (for any  $u \in F$ , take  $f(x) = u$  and again  $g(x) = 1$ ). Now take any subfield  $M$  of  $K$  which contains both  $F$  and  $a$ . We must prove that  $F(a) \subseteq M$ . But then  $M$  must contain all expressions  $f(a)/g(a)$ , because they are obtained by means of multiplication and addition of elements in  $F$  and  $a$ .

## Result

Follow proof of **Theorem 5.3.5**.

## 12. a

Given that  $a$  is transcendental over  $F$ , that means  $g(a) \neq 0$ , for any non-zero polynomial  $g(x) \in F[x]$ . We need to show that  $F(a) \cong F(x)$ .

### Step 2

2 of 9

Let us consider the function  $\phi : F(x) \rightarrow F(a)$  defined as  $\phi(f(x)/g(x)) = f(a)/g(a)$ . Clearly,  $\phi$  is well-defined, as  $g(a) \neq 0$  for any non-zero  $g(x)$ .

### Step 3

3 of 9

Let  $f(x)/g(x)$  and  $f'(x)/g'(x)$  are in  $F(x)$ . Then we have

$$\begin{aligned}\phi\left(\frac{f(x)}{g(x)} + \frac{f'(x)}{g'(x)}\right) &= \phi\left(\frac{f(x)g'(x) + f'(x)g(x)}{g(x)g'(x)}\right) \\ &= \frac{f(a)g'(a) + f'(a)g(a)}{g(a)g'(a)} \\ &= \frac{f(a)}{g(a)} + \frac{f'(a)}{g'(a)} \\ &= \phi\left(\frac{f(x)}{g(x)}\right) + \phi\left(\frac{f'(x)}{g'(x)}\right)\end{aligned}$$

Again we have,

$$\begin{aligned}\phi\left(\left(\frac{f(x)}{g(x)}\right)\left(\frac{f'(x)}{g'(x)}\right)\right) &= \phi\left(\frac{f(x)f'(x)}{g(x)g'(x)}\right) \\ &= \frac{f(a)f'(a)}{g(a)g'(a)} \\ &= \left(\frac{f(a)}{g(a)}\right)\left(\frac{f'(a)}{g'(a)}\right) \\ &= \phi\left(\frac{f(x)}{g(x)}\right)\phi\left(\frac{f'(x)}{g'(x)}\right)\end{aligned}$$

### Step 5

Therefore,  $\phi$  is a ring homomorphism. Now we will show  $\phi$  is bijective.

Let  $\frac{f(x)}{g(x)} \in \text{Ker}(\phi)$ . Then we have

$$\phi\left(\frac{f(x)}{g(x)}\right) = 0 \implies \frac{f(a)}{g(a)} = 0 \implies f(a) = 0.$$

### Step 7

7 of 9

But it is given that  $a$  is transcendental over  $F$ , so  $f(x)$  must be the zero polynomial, that is,  $f(x) = 0$ . Thus we get

$$\frac{f(x)}{g(x)} = 0 \implies \text{Ker}(\phi) = \{0\}.$$

Therefore  $\phi$  is injective.

### Step 8

8 of 9

Clearly  $\phi$  is surjective because for any  $f(a)/g(a) \in K(a)$  we have polynomial  $f(x)$  and  $g(x)$  such that  $\phi(f(x)/g(x)) = f(a)/g(a)$ .

### Result

Hence  $\phi$  is ring isomorphism and so  $F(a) \cong F(x)$ .

13. a

**Given:**  $K$  is a finite field and  $F$  is a subfield of  $K$  such that  $[K : F] = n$  and  $F$  has  $q$  elements.

**To Prove:**  $K$  has  $q^n$  elements.

**Proof:** Since  $K/F$  is a field extension of the field  $F$ , we can always assume  $K$  is a vector space over the field  $F$ . Since we have  $[K : F] = n$ ,  $K$  is a finite dimensional vector space over  $F$  of dimension  $n$ . Then by the vector space theory, since dimension of  $K$  is  $n$  over the field  $F$ , there exists a basis of  $K$  over  $F$  consisting of  $n$  elements.

Let  $\{x_1, x_2, \dots, x_n\}$  be a basis of  $K$  over  $F$ .

Then

**every element of  $K$  can be uniquely represented in the form**

$$\sum_{i=1}^n c_i x_i, \text{ where } c_i \in F \text{ for all } i = 1, 2, \dots, n.$$

That is, for any elements  $k \in K$ , there exist scalars  $c_1, c_2, \dots, c_n$  such that

$$k = c_1 x_1 + c_2 x_2 + \dots + c_n x_n.$$

Since each  $c_i \in F$  can take  $q$  values, as  $F$  has  $q$  elements,  $K$  must have exactly  $q^n$  elements.

This completes the proof.

### Result

2 of 2

Considering  $K$  as a vector space over the field  $F$  of dimension  $n$ , we have proved that  $K$  must have exactly  $q^n$  elements. Click for the complete solution.

14. a

**Problem:** Using the result of Problem 13, show that a finite field has  $p^n$  elements for some prime  $p$  and some positive integer  $n$ .

### Step 2

2 of 4

Let  $K$  be the finite field with characteristic  $p$ . Then from Theorem 5.1.1,  $p$  is a prime number. Clearly

$\underbrace{1 + 1 + \cdots + 1}_{p\text{-times}} = 0$  Consider the set  $F$ , where

$$F = \left\{ \underbrace{1 + 1 + \cdots + 1}_{m\text{-times}} : 0 \leq m \leq p - 1 \right\}$$

Clearly  $F$  is closed under addition and multiplication. Therefore  $F$  is a subring of the field  $K$  and so  $F$  is an integral domain. Clearly  $F$  is also a finite integral domain and so  $F$  is a field.

### Step 3

3 of 4

Let us calculate  $[K : F]$ . Since  $K$  is a field and  $F$  is a subfield of  $K$ . Therefore  $[K : F]$  is finite, say  $[K : F] = n$ , for some positive integer  $n$ . Also note that  $|F| = p$ . Therefore from problem 13, we have  $|K| = p^n$ .

### Result

Therefore, every finite field has  $p^n$  elements for some prime  $p$  and some positive integer  $n$ .

15. a

**To Construct:** Fields  $F$  and  $K$  such that  $K$  is an algebraic extension of  $F$  but is not a finite extension of  $F$ .

### Step 2

2 of 3

#### Construction:

Let us choose  $F = \mathbb{Q}$ .

Let

$K$  be the algebraic closure in

$\mathbb{R}$ .

Clearly,  $F$  is algebraic over  $K$ .

Suppose that  $[K : F] = n < \infty$ , and let us choose  $a = \frac{1}{2^{n+1}} \in \mathbb{R}$ .

Notice that  $\frac{1}{2^n}$  is a root of the polynomial  $f(x) = x^{n+1} + 2$ , which is irreducible in  $\mathbb{Q}[x]$  by Eisenstein.

Thus  $a$  is algebraic and so  $a \in K$ .

Therefore we have the chain  $F \subseteq F(a) \subseteq K$  of extension fields and so:  $[K : F] = [K : F[a]].[F[a] : F]$  But  $[F[a] : F] = n + 1$  and so  $n + 1$  divides  $[K : F] = n$ , which is a contradiction.

## Section 5–4

1. a

Let  $\alpha = \sqrt{2} - \sqrt{3}$ . Squaring gives

$$\alpha^2 = 2 - 2\sqrt{3}\sqrt{2} + 3 = 5 - 2\sqrt{6}$$

Rearranging and squaring gives

$$(\alpha^2 - 5)^2 = (2\sqrt{6})^2$$

Or,

$$\alpha^4 - 10\alpha^2 + 25 = 24$$

Or,

$$\alpha^2 - 10\alpha^2 + 1 = 0$$

If we let  $f(x) = x^4 - 10x^2 + 1$ , we get  $f(\alpha) = 0$ . Therefore  $\alpha = \sqrt{2} - \sqrt{3}$  is algebraic over  $\mathbb{Q}$  of at most degree 4.

2. a

Let  $f(x), g(x) \in K[x]$  be irreducible polynomials of degree  $m$  and  $n$  respectively such that  $f(a) = 0$  and  $g(a) = 0$ . Then we have  $[F(a, b) : F] = [F(a, b) : F(b)] \cdot [F(b) : F]$ . We know  $[F(b) : F] = n$ . This shows  $n \mid [F(a, b) : F]$ . Similarly,  $[F(a, b) : F] = [F(a, b) : F(a)] \cdot [F(a) : F]$  implies  $m \mid [F(a, b) : F]$ . Since  $(m, n) = 1$ , we must have  $[F(a, b) : F] = mnk$  where  $k$  is positive integer.

On the other hand, we have  $F[x] \in F[a][x]$  therefore  $f(x) \in F[a][x]$ . Let  $h(x) \in F(a)[x]$  be the minimal polynomial of  $b$  over  $F(a)$ . It follows that  $h(x) \mid g(x)$  therefore  $\deg(h(x)) \leq n$ . We get the inequality  $[F(a, b) : F] \leq mn$ . From these two relations, we get  $k = 1$  hence  $[F(a, b) : F] = mn$ .

3. a

Given  $a \in \mathbb{C}$  such that  $p(a) = 0$ , where

$$p(x) = x^5 + \sqrt{2}x^3 + \sqrt{5}x^2 + \sqrt{7}x + \sqrt{11}$$

Here, we note that  $p(x) \in \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})$  and

$$\begin{aligned} [Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}) : \mathbb{Q}] &= [Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}) : Q(\sqrt{2}, \sqrt{5}, \sqrt{7})] \cdot [Q(\sqrt{2}, \sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{2}, \sqrt{5})] \\ &\quad \cdot [\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= 2 \cdot 2 \cdot 2 \cdot 2 \\ &= 16 \end{aligned}$$

Here, we note that  $p(x)$  is of degree 5 over  $\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})$ . If  $a$  is root of  $p(x)$ , then

$$[Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}, a) : \mathbb{Q}] = [Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}) : Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})] \cdot 15$$

and  $[Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}) : Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})] \leq 5$ . We get equality if  $p(x)$  is irreducible over  $Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})$ . This gives

$$[Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}, a) : \mathbb{Q}] \leq 16 \cdot 5 = 80$$

4. a

Given  $F \subset K$  and  $[K : F] = p$ . Suppose  $a_1, a_2, \dots, a_n \in K$  such that

$$K = F(a_1, \dots, a_n)$$

Then this gives

$$[K : F] = [F(a_1, \dots, a_n) : F(a_2, \dots, a_n)] \cdots [F(a_n) : F]$$

But  $p$  is prime so one of extension  $[F(a_k, \dots, a_n) : F(a_{k+1}, \dots, a_n)] = p$  and rest extensions are of degree 1. It shows that  $F = F(a_{k+1}, \dots, a_n)$  and  $K = F(a_k)$  and  $a_i \in F$  if  $i \neq k$ .

## 5. a

Given  $[K : F] = 2^n$  and  $T$  is subfield of  $K$  containing  $F$ . Then we have

$$[K : F] = [K : T] \cdot [T : F] = 2^n$$

since 2 is prime, we must have  $[K : T] = 2^{n-m}$  and  $[T : F] = 2^m$  for some  $0 \leq m \leq n$ .

## 6. a

Take  $a = \sqrt[3]{4}$  and  $b = \frac{1}{2}(1 - \sqrt{-3})$  which is root of  $x^2 + x + 1$ . The product is

$$ab = \frac{1}{\sqrt[3]{2}}(1 - \sqrt{-3})$$

Cubing gives

$$(ab)^3 = \frac{1}{\sqrt[3]{2}}(1 - \sqrt{-3})^3 = \frac{1}{2}(1 - 3(-3) + 3\sqrt{-3} - 3\sqrt{-3}) = -4$$

Thus  $ab$  is of degree 3 which is less than 6 over  $\mathbb{Q}$ .

## 7. a

We only need to prove that for any two  $a, b \in K$ ,  $F(a, b)$  equals  $F(b, a)$ . Then the claim follows easily using mathematical induction, as the field extension  $F(a_1, a_2, \dots, a_n)$  is defined in inductive manner. That said, our work only begins.

We will be playing with definitions a bit. We are going to prove that both  $F(a, b)$  and  $F(b, a)$  are the smallest subfields of  $K$  containing  $F$ ,  $a$  and  $b$ . Then it is obvious that they are equal. Furthermore, it will be enough to prove this fact only for subfield  $F(a, b)$ , since the argument translates symmetrically to the subfield  $F(b, a)$ . Let us start.  $F(a)$  is the smallest subfield of  $K$  containing  $F$  and  $a$ . Also,  $F(a, b) = (F(a))(b)$  is the smallest subfield containing  $F(a)$  and  $b$ . Thus, we conclude that  $F(a, b)$  definitely contains  $F$  and  $a$  and  $b$ .

To prove that it is the smallest subfield of  $K$  having this property, take any subfield  $M \subseteq K$  containing  $F$  and  $a$  and  $b$ . Then since  $M$  contains  $F$  and  $a$ , it must contain field  $F(a)$ , as it is the smallest subfield of  $K$  containing  $F$  and  $a$ . Now we have that  $M$  contains both  $F(a)$  and  $b$ , which means it must contain field  $F(a, b)$ . Thus  $F(a, b) \subseteq M$ , as desired. And that's it, we have proved the crucial claim!

## Result

Playing with definition of extension fields yields the proof.

## Section 5–5

1. a

As suggested in the sketch of proof for **Theorem 5.5.1**, we only need to prove that property 1 remains valid. This is because multiplication and division behave well with respect to absolute value.

For this purpose, let  $a$  and  $b$  be constructible numbers. This means that  $\sqrt{a}$  and  $\sqrt{b}$  are constructible lengths. By original property 1, we know that  $\sqrt{a} + \sqrt{b}$  and  $\sqrt{a} - \sqrt{b}$  are also constructible lengths (assuming that  $\sqrt{a} \geq \sqrt{b}$ , obviously). Now there are few cases, depending on signs of  $a$  and  $b$ . We illustrate the proof by choosing the case where  $a \geq 0$  and  $b \geq 0$ . Then  $a + b$  is also negative, and  $\sqrt{a} + \sqrt{b} = \sqrt{a} + \sqrt{b}$ . This length is constructible, which by definition means that  $a + b$  is constructible number. Analogously for  $a - b$ .

**Result**

2 of 2

Playing with the absolute values of sum and difference.

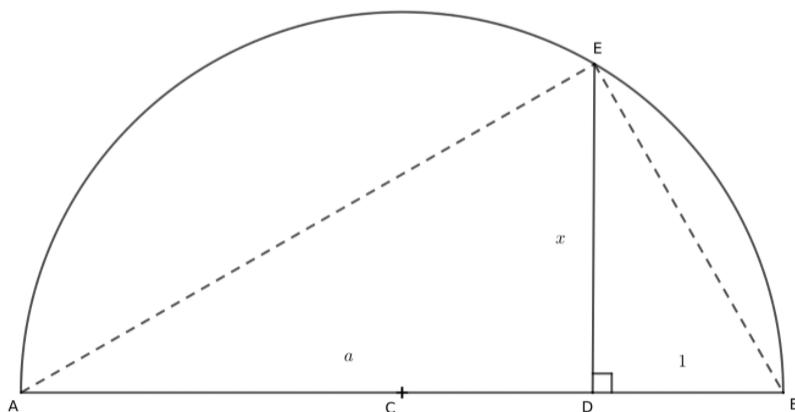
2. a

Let  $p(x) = x^3 - 3x - 1$ . Then

$$p(x+1) = (x+1)^3 - 3(x+1) - 1 = x^3 + 3x^2 - 3$$

We have  $3 \mid 3, 3 \mid 0$  but  $3 \nmid 1$  and  $3^2 \nmid 3$ . Thus the polynomial is irreducible over  $\mathbb{Q}$  by 3-Eisenstein criterion.

3. a



Look at image above. By Tales theorem, we know that angle  $\angle AEB$  is the right angle. Then by theorem about angles having perpendicular rays, we conclude that angle  $\angle AED$  is the same as angle  $\angle DBE$ . The same applies for angles  $\angle EAD$  and  $\angle BED$ . This implies that triangles  $\triangle ADE$  and  $\triangle DBE$  are **similar**, because they have two pairs of congruent angles.

Now similarity proportions yield  $\frac{x}{\sqrt{a}} = \frac{\sqrt{a}}{x}$ . This leads to expected result

$$x = |DE| = \sqrt{a}$$

## Result

Sweet dose of geometry among so much algebra.

4. a

**To Prove:** The regular heptagon is not constructible with straight-edge and compass.

**Proof:** First of all, we prove the following lemma.

**Lemma-1:**  $\cos(\frac{2\pi}{7})$  is not rational.

**Proof:** Let us consider the polynomial  $f(x) = x^3 + x^2 - 2x - 1$ .

We will show that  $f(x)$  has no rational root.

If possible, let  $\frac{a}{b}$  is a

rational root in lowest terms (i.e.  $a, b \in \mathbb{Z}$  with  $a, b$  coprime).

Then we have

$$\frac{a^3}{b^3} + \frac{a^2}{b^2} - 2\frac{a}{b} - 1 = 0,$$

or

$$a^3 + a^2b - 2ab^2 - b^3 = 0.$$

Taking  $b^3$  to the right hand side we find that  $a$  divides  $b^3$ .

But since  $a$  and  $b$  are coprime this implies that  $a = \pm 1$ .

Similarly, taking  $a^3$  to the right hand side shows that  $b$  divides  $a^3$ , and hence  $b = \pm 1$ .

We can easily check that **neither of these is a root, and hence there are no rational roots.**

Since  $2\cos(\frac{2\pi}{7})$  is a root of the polynomial, we conclude that it is not rational.

This implies that  $\cos(\frac{2\pi}{7})$  is **not rational**.

This proves **Lemma-1**.

**Lemma-2:**  $\cos\left(\frac{2\pi}{7}\right)$  is not constructible.

**Proof:** Now consider above  $f(x)$  and let  $F \subseteq F[\sqrt{c}]$  be any

**quadratic field extension such that  $\mathbb{Q} \subseteq F$**

We know that

**If  $f(x)$  has a root in  $F[\sqrt{c}]$  then it is also a root in  $F$ .**

Now suppose for contradiction that  $\cos\left(\frac{2\pi}{7}\right)$  is constructible.

**Then there exists a chain of quadratic extensions**

$$\mathbb{Q} \subseteq F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_k$$

such that  $\cos\left(\frac{2\pi}{7}\right) \in F_k$ .

That is,  $f(x)$  has a root in  $F_k$ .

But by the above remark, this implies that  $f(x)$  also has a root in  $F_{k-1}$ .

**Repeating this argument  $k$  times shows that  $f(x)$  has a root in  $\mathbb{Q}$**

which has shown in **Lemma-1**, a contradiction.

So,  $\cos\left(\frac{2\pi}{7}\right)$  is **not constructible**.

Now back to the proof.

If possible, let the regular heptagon is constructible with straightedge and compass.

**Consider the fan of rays from the center of the heptagon through its vertices and intersect this with a unit circle to get a heptagon of unit radius.**

We can assume that one of the vertices has coordinates  $(1, 0)$  and hence the next vertex counterclockwise has coordinates  $(\cos\left(\frac{2\pi}{7}\right), \sin\left(\frac{2\pi}{7}\right))$ .

This implies that the number  $\cos\left(\frac{2\pi}{7}\right)$  is constructible, which is a contradiction from **Lemma-2**.

Hence the

regular heptagon is not constructible with straight-edge and compass.

This completes the proof.

## Result

5 of 5

Since  $\cos\left(\frac{2\pi}{7}\right)$  is not constructible, we prove that the regular heptagon is not constructible with straight-edge and compass.

Click for the detailed proof.

# Section 5–6

1. a

**Answer for (a):**

Given that  $\delta : F[x] \rightarrow F[x]$  is a mapping such that

$$\delta(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_1 + 2a_2x + \cdots + ia_ix^{i-1} + \cdots + na_nx^{n-1}.$$

**To show:**  $\delta((f(x) + g(x))) = \delta(f(x)) + \delta(g(x)).$

Let  $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$  and  $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ .

Without loss of generality consider  $n \geq m$ .

Then we have

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_m + b_m)x^m \\ &\quad + a_{m+1}x^{m+1} + \cdots + a_nx^n. \end{aligned}$$

Therefore

$$\begin{aligned} \delta(f(x) + g(x)) &= \delta((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_m + b_m)x^m \\ &\quad + a_{m+1}x^{m+1} + \cdots + a_nx^n). \\ &= (a_1 + b_1) + 2(a_2 + b_2)x + \cdots + i(a_i + b_i)x^{i-1} + \cdots + m(a_m + b_m)x^{m-1} \\ &\quad + (m+1)a_{m+1}x^m + \cdots + na_n^{n-1}. \\ &= (a_1 + 2a_2x + \cdots + ma_mx^{m-1} + \cdots + na_n^{n-1}) + (b_1 + 2b_2x + \cdots + mb_mx^{m-1}). \\ &= \delta(f(x)) + \delta(g(x)) \text{ (Proved).} \end{aligned}$$

**Answer for (b):**

Let  $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$  and  $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ .

Then we have

$$f(x)g(x) = \sum_{k=0}^{m+n} (a_0b_k + a_1b_{k-1} + \cdots + a_kb_0)x^k.$$

Let fix  $k$ ,  $0 \leq k \leq m+n$ .

The coefficient of  $x^{k+1}$  in  $f(x)g(x)$  is  $(a_0b_{k+1} + a_1b_k + \cdots + a_{k+1}b_0)$

Thus the coefficient of  $x^k$  in  $\delta(f(x)g(x)) = (k+1)(a_0b_{k+1} + a_1b_k + \cdots + a_{k+1}b_0)$ .

Now

$$\delta(f(x)) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

and

$$\delta(g(x)) = b_1 + 2b_2x + \cdots + mb_mx^{m-1}.$$

Coefficient of  $x^k$  in  $\delta(f(x))g(x) = a_1b_k + 2a_2b_{k-1} + \cdots + (k+1)a_{k+1}b_0$  and Coefficient of  $x^k$  in  $f(x)\delta(g(x)) = (k+1)a_0b_{k+1} + ka_1b_k + \cdots + a_kb_1$ .

Therefore,

Coefficients of  $x^k$  in  $\delta(f(x))g(x) + f(x)\delta(g(x))$

$$\begin{aligned} &= (a_1b_k + 2a_2b_{k-1} + \cdots + (k+1)a_{k+1}b_0) + ((k+1)a_0b_{k+1} + ka_1b_k + \cdots + a_kb_1) \\ &= (k+1)(a_0b_{k+1} + a_1b_k + \cdots + a_{k+1}b_0). \end{aligned}$$

Hence coefficient of  $x^k$  in  $\delta(f(x))g(x) + f(x)\delta(g(x))$  = the coefficient of  $x^k$  in  $\delta(f(x)g(x))$ .

Now we know that  $k$  is arbitrary integer from  $\{0, 1, \dots, m+n\}$ , therefore it is true for all integers  $0, 1, \dots, m+n$ . Hence

$$\delta(f(x))g(x) + f(x)\delta(g(x)) = \delta(f(x)g(x)).$$

### Result

Final Answer: [Click here for details answer.](#)

$$\boxed{\delta(f(x))g(x) + f(x)\delta(g(x)) = \delta(f(x)g(x)).}$$

### 2. a

If  $q = 2$ , we have  $-1 = 1$ . If  $q \neq 2$ , the non unit elements of field form a group with respect to multiplication operation and each element is paired with its inverse if its inverse is not equal to itself. If  $F$ ,  $x^2 = 1$ , has two solutions,  $x = \pm 1$ . This gives

$$q_1 \dots q_n = -1 \cdot 1 \cdot (\text{product of rest of elements with inverse}) = -1$$

### 3. a

Take  $p(x)(x-1) = x^5 - 1$ . Let  $\zeta$  be the primitive 5-th root of unity, i.e.  $\zeta^n = 1 \implies n = 5$  or  $5 \mid n$ . Then  $\zeta$  is not root of  $x-1$  hence must be root of  $p(x)$ . As  $p(x+1)$  is irreducible by 5-Eisenstein criterion,  $p(x)$  is also reducible. Thus, define

$$K = \mathbb{Q}(\zeta) = \mathbb{Q}[x]/(x^4 + x^3 + x^2 + x + 1)$$

and we get  $[K : \mathbb{Q}] = 4$ . Furthermore, each  $\zeta^i$ ,  $i = 2, 3, 4$ , is root of  $p(x)(x-1)$  which is not equal to 1. Therefore  $p(x)$  splits in  $K$ .

### 4. a

Let  $r$  be a rational number with is root of  $q(x) = x^n + a_1x^{n-1} + \dots + a_n$ , where  $a_i$  are integers. Then, by definition of root, we have

$$q(r) = r^n + a_1r^{n-1} + \dots + a_n = 0$$

As  $r$  is root of  $q(x)$ , we have

$$q(x) = (x - r)(x^{n-1} + b_1x^{n-2} + \dots + b_{n-1})$$

Let  $r = s/t$  such that  $(s, t) = 1$ , this gives

$$tq(x) = (tx - s)(x^{n-1} + b_1x^{n-2} + \dots + b_{n-1})$$

Here, since  $t$  is an integer and it must divide one of the polynomials  $(tx - s)$  or  $x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}$ . Since  $(s, t) = 1$ , it must divide  $x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}$ . But dividing it means it divides all coefficients. i.e. it divides 1, coefficient of  $x^{n-1}$ . Thus  $t = 1$ . Therefore  $r \in \mathbb{Z}$ .

[Comment: this proof is similar to Gauss lemma proof]

To show  $r \mid a_n$ , we have

$$q(r) = r^n + a_1r^{n-1} + \dots + a_{n-1}r + a_n = 0$$

Or,

$$r(r^{n-1} + a_1r^{n-2} + \dots + a_{n-1}) = -a_n$$

This shows  $r \mid a_n$  because  $r^{n-1} + a_1r^{n-2} + \dots + a_{n-1}$  is an integer which equals  $-a_n/r$ .

[Comment: this is essentially rational root theorem]

## 5. a

Let  $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}_2[x]$  be a function defined by

$$\varphi(a_nx^n + \dots + a_0) = \bar{a}_nx^n + \dots + \bar{a}_0$$

where  $\bar{a}_0, \dots, \bar{a}_n$ . This is a surjective homomorphism with kernel  $2\mathbb{Z}_2[x]$ .

$$\varphi(x^3 - 7x + 11) = x^3 + x + 1$$

If it is reducible in  $\mathbb{Z}_2[x]$ , then it must have a root (a reducible cubic has a linear factor). Put  $x = \bar{0}$ , we get  $0^3 + 0 + 1 = 1 \neq 0$ . Put  $x = 1$ , we get  $1^3 + 1 + 1 = 3 \equiv 1 \neq 0$ . Therefore it is irreducible in  $\mathbb{Z}_2[x]$ .

We note that if  $f(x) \in \mathbb{Z}[x]$  is reducible then  $\varphi(f(x))$  is reducible in  $\mathbb{Z}_2[x]$  ( $\varphi$  being homomorphism). Using contraposition, we get if  $\varphi(f(x))$  is not reducible in  $\mathbb{Z}_2[x]$  then  $f(x)$  is not reducible in  $\mathbb{Z}[x]$  either.

This shows  $q(x)$  is irreducible in  $\mathbb{Z}[x]$  thus by Gauss lemma, irreducible in  $\mathbb{Q}$  too.

## 6. a

Let  $F$  be a field of characteristic  $p \neq 0$ , then  $p \cdot a = 0$  for all  $a \in F$ . Using Binomial expansion, we get

$$(a + b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p$$

Now,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

which corresponds to number of  $k$  combination from  $p$  choices. It is clearly an integer. But neither  $k \nmid p$  and  $(p - k) \nmid p$ . Therefore  $\binom{p}{k} = p \cdot m_k$  for some integer  $m_k$ . Therefore

$$(a + b)^p = a^p + b^p + p \left( \sum_{k=1}^{p-1} m_k a^{p-k} b^k \right) = a^p + b^p$$

## 7. a

Finite fields have characteristic prime. The characteristic of field  $F$  is  $p$ . Suppose there are  $m = p^n$  elements in it. Using Binomial expansion, we get

$$(a + b)^m = a^m + \sum_{k=1}^{m-1} \binom{m}{k} a^{m-k} b^k + b^m$$

Now,

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} = \frac{m \cdots (m-k+1)}{k!}$$

Suppose if  $p \nmid k!$  then  $\binom{m}{k} = p \cdot c_k$  for some integer  $c_k$ . If  $p \mid k!$ , then  $k \geq p^l$ , then  $p^{l(l+1)/2} \mid k!$ . Between  $p^n - k + 1$  and  $p^n$ , there are  $k - 1$  numbers which will have at least multiplicity of  $p^{l+1} \cdots p^{l+(n-l)} = p^{n(n+1)/2 - l(l+1)/2}$ . Since  $n(n+1)/2 - l(l+1)/2 > l(l+1)/2$  for  $l < n$ , we have  $p \mid \binom{p^n}{k}$  for  $0 < k < p$ . This gives

$$(a + b)^m = a^m + p \left( \sum_{k=1}^{m-1} c_k a^{m-k} b^k \right) + b^m = a^m + b^m$$

where  $c_k$  is some positive integer.

## 8. a

To solve this exercise, we must carefully examine the proof of **Theorem 5.6.5**. More precisely, we will use two important facts about extension field  $K$  which are implicitly contained there. First is that field  $K$  is **commutative** if  $F$  is commutative, which can be seen directly from  $K = F[x]/M$ . Secondly, field  $K$  has **characteristic  $p$**  if  $F$  does, since, I cite: ``\dots every element in  $K$  is of the form  $r(a)$ , where  $r(x)$  is in  $F[x]$  \dots''.

Now we can proceed to solve the exercise. Take any two  $a, b \in K_0$ . This means that  $a$  and  $b$  are roots of polynomial  $x^m - x \in F[x]$ . This polynomial is also member of  $K[x]$ , since  $F \subset K$ . Thus, we have

$$\begin{aligned} a^m - a &= 0 \text{ and} \\ b^m - b &= 0, \end{aligned}$$

i.e.  $a^m = a$  and  $b^m = b$  in field  $K$ . We first use commutativity of field  $F$  to prove that  $\frac{a}{b}$  is a root of  $x^m - x$  as well, i.e. a member of  $K_0$ .  $\left( \frac{a}{b} \right)^m - \frac{a^m}{b^m} = \left( \frac{a}{b} \right)^m - \frac{a^m}{b^m} = \left( \frac{a}{b} \right)^m - \left( \frac{a}{b} \right)^m = 0$ . Next we use the result of previous exercise (we can, since  $K$  is of characteristic  $p$ ) to prove that  $a - b$  is a root as well.  $(a - b)^m - (a - b)^m = a^m - b^m - a + b = (a^m - a) - (b^m - b) = 0 - 0 = 0$ . This proves that  $K$  is a field. It obviously has at most  $p^n$  elements, since polynomial  $x^m - x$  is of degree  $p^n$  and hence can have at most that many linear factors.

## Result

We examine the proof of **Theorem 5.6.5** to collect valuable facts about extension field  $K$ .

### 9. a

In the last exercise we have argued that every polynomial of degree  $m$  has at most  $m$  linear factors. In fact, it has **exactly** (how convenient, ha) that many linear factors, counting the multiplicities of course.

Now, Problem 14 suggests that all roots of  $x^m - x$ , where  $m = p^n$ , are distinct. This then implies that multiplicity of each root is 1. Hence there are exactly  $p^n$  elements in  $K_0$ .

## Result

2 of 2

Direct implication of Problem 14.

### 10. a

$x^n - 2$  is an irreducible polynomial over  $\mathbb{Q}$ . This is true because it clearly has no integer roots, and then we use Gauss lemma.

Thus the extension field  $K_n$  of  $\mathbb{Q}$  containing at least one root of polynomial  $x^n - 2$  satisfies  $[K_n : \mathbb{Q}] = n$ , for each  $n \in \mathbb{N}$ .

## Result

2 of 2

Irreducibility of  $x^n - 2$  over  $\mathbb{Q}$  comes in handy.

## 11. a

Ok, derivation, now it's enough. Come out, we see you.

I obviously will not be re-telling you the good old story of additivity of derivation ( $\text{part a}$ ), and let alone Leibniz formula ( $\text{part b}$ ). I guess your analysis professors bored you quite enough with that.

## Result

2 of 2

Good old hide-and-seek with derivation.

## 12. a

$F$  is a field of characteristic  $p \neq 0$ . Suppose  $f(x) \in F[x]$  is given by,

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

Then, we have

$$\delta(f(x)) = a_1 + 2a_2x + \cdots + ia_ix^{i-1} + \cdots + na_nx^{n-1}.$$

Now  $\delta f(x) = 0$  implies that all the coefficients of  $\delta f(x)$  is divisible by  $p$ .

So, if the degree of all monomials of  $f(x)$  is multiple of  $p$  then after applying  $\delta$  on  $f(x)$ , we will get all the coefficients of  $\delta(f(x))$  is multiple of  $p$  i.e.  $\delta(f(x)) = 0$ . So if

$$f(x) = a_0 + a_1x^{pm_1} + a_2x^{pm_2} + \cdots + a_rx^{pm_r},$$

where  $m_1, m_2, \dots, m_r$  are non-negative integers then

$$\delta(f(x)) = pm_1a_1x^{pm_1-1} + pm_2a_2x^{pm_2-1} + \cdots + pm_ra_rx^{pm_r-1} = 0.$$

## Result

2 of 2

**Final Answer** ([Click here to see complete answer.](#))

$$\boxed{\delta(f(x)) = pm_1a_1x^{pm_1-1} + pm_2a_2x^{pm_2-1} + \cdots + pm_ra_rx^{pm_r-1} = 0.}$$

## 13. a

Suppose  $c$  is a root of  $f(x) \in F[x]$  of multiplicity at least 2.

Then  $f(x)$  can be written as

$$f(x) = (x - c)^2g(x),$$

where  $g(x) \in F[x]$ . now

$$\begin{aligned} f(x) = (x - c)^2g(x) \implies \delta(f(x)) &= \delta((x - c)^2g(x)), \\ &= g(x)\delta((x - c)^2) + (x - c)^2\delta(g(x)), \\ &= 2g(x)(x - c)^2 + (x - c)^2\delta(g(x)), \\ &= (x - c)(2g(x) + (x - c)\delta(g(x))), \\ &= (x - c)h(x). \end{aligned}$$

Where  $h(x) = 2g(x) + (x - c)\delta(g(x)) \in F[x]$ , since  $g(x), (x - c)$  and  $\delta(g(x)) \in F[x]$ .  $(x - c)$  divides both  $f(x)$  and  $\delta(f(x))$ , so  $f(x)$  and  $\delta(f(x))$  are not relatively prime.

## Result

2 of 2

**Final Answer:** [Click here for details answer.](#)

$$\boxed{f(x) \text{ and } \delta(f(x)) \text{ are not relatively prime}}$$

## 14. a

**Given:**  $F$  is a field of characteristic  $p \neq 0$ .

**To Prove:** All roots of the polynomial  $x^m - x$  are distinct where  $m = p^n$ , for some  $n \in \mathbb{N}$ .

**Proof:** Let us consider  $f(x) = x^m - x$ .

Then  $f \in F[x]$ .

**Claim:**  $f(x)$  has a multiple root in some extension of  $F$  if and only if  $f(x)$  is not relatively prime to its derivative,  $f'(x)$ .

**Proof of the Claim:** Let us assume that  $f(x)$  has a multiple root in some extension of  $F$ . Let  $y$  be a multiple root of  $f(x)$ .

Then over a splitting field, we have

$$f(x) = (x - y)^n g(x), \text{ for some integer } n \geq 2.$$

Here  $g(x)$  is a polynomial such that  $g(y) \neq 0$ .

Now taking derivative of  $f$  we get

$$f'(x) = n.(x - y)^{n-1}g(x) + (x - y)^n g'(x) \quad \dots\dots\dots(1)$$

here  $g'(x)$  implies derivative of  $g$  with respect to  $x$ .

Since we have  $n \geq 2$ , this implies  $(n - 1) \geq 1$ . Hence, (1) shows that  $f'(x)$  has  $y$  as a root.

Therefore,  $f(x)$  is not relatively prime to  $f'(x)$ .

We now prove the other direction.

Conversely, let us assume that  $f(x)$  is not relatively prime to  $f'(x)$ . Let  $y$  is a root of both  $f(x)$  and  $f'(x)$ .

Since  $y$  is a root of  $f(x)$ , we can write

$$f(x) = (x - y).g(x) \quad \dots\dots\dots(2)$$

for some polynomial  $g(x)$ . then taking derivative of  $f(x)$  we have

$$f'(x) = g(x) + (x - y).g'(x) \quad \dots\dots\dots(3)$$

where  $g'(x)$  is the derivative of  $g(x)$  with respect to  $x$ .

Since  $y$  is a root of  $f'(x)$  also we have

$$f'(y) = 0.$$

Then from (3) we have

$$\begin{aligned} f'(y) &= g(y) + (y - y).g'(y) \\ \implies f'(y) &= g(y) \\ \implies g(y) &= 0. \end{aligned}$$

This implies  $y$  is a root of  $g(x)$  also.

Therefore we have

$$g(x) = (x - y).h(x)$$

for some polynomial  $h(x)$ .

Now form (2) we have

$$f(x) = (x - y)^2.h(x).$$

This follows that  $y$  is a multiple root of  $f(x)$ .

Therefore,  $f(x)$  has a multiple root in some extension of the field  $F$ .

This completes the proof of the Claim.

In our case,  $f(x) = x^m - x$ , where  $m = p^n$ .

Now we calculate the derivative of  $f$ . That is

$$f'(x) = mx^{m-1} - 1 \equiv -1 \pmod{p}.$$

By the above condition it follows that,  $f'$  has no root same as  $f$ , that is,  $f(x)$  and  $f'(x)$  are relatively prime.

Hence,  $f(x)$  has no multiple root in  $F$ . Since  $f(x) = x^m - x$  is a polynomial of degree  $m$ , it follows that  $f(x)$  has  $m$  distinct roots in  $F$ , where  $m = p^n$ .

This completes the proof.

## Result

4 of 4

Using the lemma that " $f(x)$  has a multiple root in some extension of  $F$  if and only if  $f(x)$  is not relatively prime to its derivative,  $f'(x)$ ", we have shown that the polynomial  $x^m - x$  has no multiple root, hence have  $m$  distinct roots in  $F$ . Click for the detailed solution.

15. a

### Part a.

Assume the contrary, i.e. that characteristic of  $F$  is 0. Polynomial  $f$  is of degree  $n \geq 2$  and hence its derivation is the polynomial of degree  $n - 1$  (because field is of characteristic 0). Because  $f$  has a multiple root  $\alpha$ , by Problem 13 we conclude that  $f(x)$  and  $f'(x)$  are not relatively prime in field  $F[x]$ . But this means that  $f(x)$  has a divisor in  $F[x]$ , which is a contradiction with its irreducibility.

### Part b.

By the same reasoning as above, we conclude that  $f'(x) = 0$ . But this can happen when only exponents of  $f(x)$  are multiples of field's characteristic  $p$ , since then all coefficients get canceled out.

## Result

Using Problem 13 and definition of characteristic.

# 6

---

## Chapter 6

### Section 6–1

1. a

We have

$$Z(S_n) = \{\sigma \in S_n \mid \sigma\phi\sigma^{-1} = \phi \quad \forall \phi \in S_n\}$$

For  $n > 2$ , let  $\sigma \in S_n$  s.t.  $\sigma \neq e$ . We will show that there always exists  $\phi$  for which  $\sigma$  does not commute.

Let  $\sigma(i) = j$  and for  $n \geq 3$ , we can always find element  $\phi \neq e$  such that  $\phi(i) = i$  i.e. fixes  $i$ . Let  $\phi(j) = k$ . We get

$$\begin{aligned}\phi\sigma\phi^{-1}(i) &= \phi\sigma(i) \\ &= \phi(j) \\ &= k \\ &\neq i\end{aligned}$$

Therefore  $\sigma$  does not commute with  $\phi$  therefore  $\sigma \notin Z(S_n)$ . Hence  $Z(S_n)$  must be a trivial group.

2. a

We have  $A_n \subset S_n$  and for  $n > 2$  the center of  $S_n$  is trivial group. For  $n > 3$ , the center of  $A_n$  is also trivial group.

Let  $\sigma \in A_n$  such that  $\sigma(i) = j$ . For  $n \geq 4$  we can always find  $\tau \in A_n$  such that  $\tau(i) = i, \tau(j) = k, \tau(k) = l$ . Then we get

$$\begin{aligned}\tau\sigma\tau^{-1}(i) &= \tau\sigma(i) \\ &= \tau(j) \\ &= k \\ &\neq i\end{aligned}$$

This shows that  $Z(A_n) = \{e\}$  for  $n > 3$ .

3. a

Suppose we have two 3-cycles with no elements in common  $(abc)$  and  $(ijk)$ , then  $(abc)(ijk)$  is associated with the partition  $6 = 3 + 3$ .

Suppose we have two 3-cycles with one element in common  $(abc)$  and  $(ajk)$ , then  $(abc)(ajk) = (ajkbc)$  is a 5-cycle, ie is associated with the trivial partition  $5 = 5$ .

Suppose we have two 3-cycles with two element in common  $(abc)$  and  $(abk)$ , then  $(abc)(abk) = (ac)(nk)$  is a product of 2-cycle associated with the partition  $4 = 2 + 2$ . We could also have considered 3-cycles  $(abc)$  and  $(akb)$ , then  $(abc)(akb) = (akc)$  is a 3-cycle associated with the trivial partition  $3 = 3$ .

Suppose we have two 3-cycles with three element in common  $(abc)$  and  $(abc)$ , then  $(abc)(abc) = (acb)$  is a 3-cycle associated with the trivial partition  $3 = 3$ . We could also have considered 3-cycles  $(abc)$  and  $(acb)$ , then  $(abc)(acb) = ()$  is the identity.

## Result

2 of 2

The product of 3-cycles could be disjoint, a 5-cycle, a product of disjoint 2-cycles, a 3-cycle or the identity.

### 4. a

If  $m < n$ , then  $S_n \subseteq S_m$ . Let  $\sigma \in S_m$ , then  $\sigma$  is permutation of  $m$  elements. Since  $m < n$ ,  $\sigma$  is also permutation of  $n$  items that fixes at least  $n - m$  items therefore  $\sigma \in S_n$  which shows that  $S_m \subseteq S_n$ . Clearly  $S_m$  is isomorphic to itself that is subset of  $S_n$ .

### 5. a

**Given:** Let  $G$  be an abelian group having no proper subgroups.

**To Prove:**  $G$  is a cyclic group of prime order.

**Proof:**

Without loss of generality, let us assume that  $G$  is **non-trivial abelian group**.

Since  $G$  is nontrivial,

**there exists an element  $g \neq e$  in  $G$ ,  $e$  being the identity element in  $G$ .**

Then, consider  $\langle g \rangle$ , the

**subgroup generated by  $g$**

This is a nontrivial subgroup, hence, by hypothesis,  $\langle g \rangle = G$ .

Hence,

**$G$  is a cyclic group.**

Now there are two cases.

**Case-1:**  $g$  has infinite order, that is

**no positive power of  $g$  is trivial.**

In this case, the group  $G$  is **isomorphic** to (i.e., can be identified with) the group  $\mathbb{Z}$ , under the identification  $n \mapsto g^n$ .

In particular, the subgroup generated by  $g^2$ , which **corresponds to the even integers, is a proper nontrivial subgroup**, leading to a contradiction. Therefore,  $g$  can be of infinite order.

**Case-2:**  $g$  cannot have infinite order.

Let  $n$  be the order of  $g$ .

Then,

$$g^n = e.$$

**Suppose that  $n$  is composite.**

Then,  $G$  is

**isomorphic to the cyclic group of order  $n$ ,**

under the identification  $a \mapsto g^a$ .

Pick a positive integer  $d \neq 1, n$  such that  $d|n$ .

Then the subgroup generated by  $g^d$  is a

**proper nontrivial subgroup of  $G$**

(corresponds to the multiples of  $d \pmod{n}$ ).

More precisely, it is a subgroup of order  $n/d$ , because the order of  $g^d$  is  $n/d$ .

This is again a contradiction.

So,

**$n$  is prime**

Consequently,  $G$

is a cyclic group of prime order  $p$ .

This completes the proof.

## Result

4 of 4

Therefore in either case, if  $G$  is an abelian group having no proper subgroups then we prove that  $G$  is a cyclic group of prime order.  
Click for the detailed proof.

## 6. a

By **lemma 6.1.5** the number of conjugacy classes of  $S_6$  equals the number of partitions of 6. These are:

- $6 = 6;$
- $6 = 1 + 5;$
- $6 = 2 + 4;$
- $6 = 3 + 3;$
- $6 = 1 + 1 + 4;$
- $6 = 1 + 2 + 3;$
- $6 = 2 + 2 + 2;$
- $6 = 1 + 1 + 1 + 3;$
- $6 = 1 + 1 + 2 + 2;$
- $6 = 1 + 1 + 1 + 1 + 2;$
- $6 = 1 + 1 + 1 + 1 + 1 + 1.$

Therefore there are 11 conjugacy classes of  $S_6$ .

## Result

There are 11 conjugacy classes of  $S_6$ .

## 7. a

Well, if  $b$  would commute with every generator of  $G$ , then there would be no reason why it would not commute with absolutely every element of  $G$ . But of course, then it would not be noncentral element.

Formally, every  $x \in G$  can be written as product  $x = \prod_i a_i$ . Then, if we can commute  $b$  with each  $a_i$ , then it can also commute with  $x$ .

## Result

2 of 2

If  $b$  commutes with all generators, then it would commute with any element from  $G$ .

## 8. a

**Given:**  $M$  and  $N$  are two subgroups of a group  $G$  such that  $M$  is normal in  $N$  and  $N$  is normal in  $G$ .

**To Prove:**  $aMa^{-1}$  is a normal subgroup of  $N$ , for all  $a \in G$ .

**Proof:** Since  $M$  and  $N$  are normal subgroup of  $G$  we have

$$\begin{aligned} gmg^{-1} &\in M \text{ for all } m \in M \text{ and } g \in G, \\ gng^{-1} &\in N \text{ for all } n \in N \text{ and } g \in G, \end{aligned}$$

**Claim:** A subgroup  $H$  of a group  $G$  is normal if  $aHa^{-1} = H$

for every  $a$  in  $G$ .

**Proof of the Claim:** Since  $H$  is a normal subgroup of  $G$  then we have

$$aH = Ha, \text{ for every } a \in G.$$

Let us now assume  $p \in aHa^{-1}$ .

Then

$$\begin{aligned} p &= ah_1a^{-1} \text{ for some } h_1 \in H \\ &= (h_2a)a^{-1} \text{ since } aH = Ha, \text{ for some } h_2 \in H \\ &= h_2 \in H. \end{aligned}$$

Thus

$$p \in aHa^{-1} \implies p \in H$$

and therefore we have

$$aHa^{-1} \subset H.$$

Now let us consider  $q \in H$ .

Then we have

$$qa \in Ha = aH.$$

Hence,

$$qa = ah_3, \text{ for some } h_3 \in H$$

and therefore we have

$$q = ah_3a^{-1} \in aHa^{-1}.$$

Thus we have conclude that

$$q \in H \implies q \in aHa^{-1}$$

and therefore

$$H \subset aHa^{-1}.$$

Consequently we have

$$aHa^{-1} = H \text{ for every } a \in G.$$

This proves our Claim.

Now back to our problem.

Since  $M$  is normal in  $N$ , we have

$$nMn^{-1} = M \text{ for every } n \in N.$$

In order to show that  $aMa^{-1}$  is normal in  $N$  for every  $a \in G$ , we will show that

$$n \in N \text{ and } x \in aMa^{-1} \implies nxn^{-1} \in aMa^{-1}.$$

For  $x \in aMa^{-1}$ , we have an element  $m$  in  $M$  such that  $x = ama^{-1}$ .

Now

$$\begin{aligned} nxn^{-1} &= n(ama^{-1})n^{-1} \\ &= (a.a^{-1})n(ama^{-1})n^{-1}(a.a^{-1}) \\ &= a(a^{-1}na)m(a^{-1}n^{-1}a)a^{-1} \\ &= a.n_1mn_1^{-1}a^{-1}, \text{ since } N \text{ is normal in } G, a^{-1}na = n_1 \in N \\ &= am_1a^{-1}, \text{ since } M \text{ is normal in } N, n_1[mn_1]^{-1} = m_1 \in M. \end{aligned}$$

This follows that

$$nxn^{-1} = am_1a^{-1}, \text{ for some } m_1 \in M.$$

Hence

$$nxn^{-1} \in aMa^{-1}.$$

Therefore we have conclude that  $aMa^{-1}$  is normal in  $N$ , for every  $a$  in  $G$ .

This completes the proof.

## Result

4 of 4

Being  $M$  is normal in  $N$  we write  $M = nMn^{-1}$  for any  $n \in N$ , then use this to show that  $nxn^{-1} \in aMa^{-1}$  for any  $x \in aMa^{-1}$ . And follows the result. Click for the detailed solution.

## 9. a

**Given:**  $M$  and  $N$  are two **normal subgroups** of a group  $G$ .

$$MN = \{mn : m \in M \text{ and } n \in N\}.$$

**To Prove:**  $MN$  is a **normal subgroup** of  $G$ .

### Step 2

2 of 4

**Proof:** We first show that  $MN$  is a **subgroup** of  $G$ .

Let  $m_1, m_2 \in M$  and  $n_1, n_2 \in N$ .

Then  $m_1n_1 \in MN$  and  $m_2n_2 \in MN$ .

$$\text{Now we have, } (m_1n_1)^{-1}(m_2n_2) = (n_1^{-1}m_1^{-1})(m_2n_2) = n_1^{-1}m_1^{-1}m_2n_1n_1^{-1}n_2$$

Since  $M$  is **normal** in  $G$ ,  $m_1^{-1}m_2 \in M$  and  $n_1 \in G \implies n_1^{-1}m_1^{-1}m_2n_1 \in M$  and since  $N$  is a **subgroup** of  $G$ ,  $n_1, n_2 \in N \implies n_1^{-1}n_2 \in N$

This implies  $n_1^{-1}m_1^{-1}m_2n_1n_1^{-1}n_2 \in MN$ .

Therefore,  $(m_1n_1)^{-1}(m_2n_2) \in MN$ .

It follows that  $m_1n_1 \in MN$  and  $m_2n_2 \in MN \implies (m_1n_1)^{-1}(m_2n_2) \in MN$ .

Hence,  $MN$  is a **subgroup** of  $G$ .

Now we assert that  $MN$  is **normal** in  $G$ .

Let  $g \in G$  and  $mn \in MN$ .

$$\text{Now we have, } gmng^{-1} = (gmg^{-1})(gng^{-1}),$$

Since  $M$  and  $N$  are **normal** in  $G$ ,  $m \in M$  and  $g \in G \implies gmg^{-1} \in M$   $n \in N$  and  $g \in G \implies gng^{-1} \in N$

Therefore,  $gmng^{-1} \in MN$ .

So, for  $g \in G$  and  $mn \in MN$  we have  $gmng^{-1} \in MN$ .

This implies  $MN$  is **normal** in  $G$ .

This completes our proof.

## 10. a

Let  $H < A_6$  be the subgroup generated by the  $n$ -cycles. Let  $\prod_{i=1}^k \sigma_i \in H$ , with each  $\sigma_i$  an  $n$ -cycle, and let  $\tau \in A_n$ . Then

$$\tau \left( \prod_{i=1}^k \sigma_i \right) \tau^{-1} = \prod_{i=1}^k \tau \sigma_i \tau^{-1}$$

which by **lemma 6.1.3** is an element of  $H$ . Therefore  $H$  is a normal subgroup of  $A_n$ . Since  $H$  is nonempty (all  $n$ -cycles for  $n$  odd are in  $A_n$ ) and  $n \geq 5$  we have by **theorem 6.1.9** that  $H = A_n$ .

### Result

2 of 2

This follows by **lemma 6.1.3** and **theorem 6.1.9**.

## 11. a

First note that one way to define the centralizer of an element  $a$  is a group  $G$  is  $C(a) = \{g \in G \mid gag^{-1} = a\}$ . Therefore by **lemma 6.1.3** we have that  $\tau \in \tau \in C((123 \cdots k))$  if and only if it is a disjoint product  $\tau = \sigma(123 \cdots k)^i$  for some  $0 \leq i < k$ , where disjointness means  $\sigma(j) = j$  for  $1 \leq j \leq k$ . Therefore  $\tau \in C((123 \cdots k))$  if it is the product of some permutation of the  $n - k$  elements  $k + 1, \dots, n$ , of which there are  $(n - k)!$ , with some power of  $(123 \cdots k)$ , of which there are  $k$ , giving us a total of  $k(n - k)!$  elements in the centralizer of  $(123 \cdots k)$ .

By **lemma 6.1.4** an element of  $S_n$  is conjugate to  $(123 \cdots k)$  if and only if it is a  $k$ -cycle, of which there are  $\frac{n!}{k(n-k)!}$ . This can be computed by considering that there are  $\frac{n!}{(n-k)!}$  strings of  $k$  distinct elements of  $\{1, 2, 3, \dots, n\}$ , and two such strings represent the same element of  $S_n$  if we can get one from the other by cycling the elements, so there are  $k$  such representatives of the  $k$ -cycles in  $S_n$ .

### Result

2 of 2

The first part follows by **lemma 6.1.3**, and the second by **lemma 6.1.4**.

## 12. a

Remember that  $MN = \{mn : m \in M, n \in N\}$ ,  $M \cap N = \{e\}$  and  $|M| = |N|$ . Obviously, in order to prove that  $|MN| = |M||N| = |N|^2$ , we must show that all elements  $mn$  are distinct.

Assume that for  $m_1, m_2 \in M$  and  $n_1, n_2 \in N$  we have  $m_1n_1 = m_2n_2$ . Then we obtain

$$a = \underbrace{m_2^{-1}m_1}_{\in M} = \underbrace{n_2n_1^{-1}}_{\in N}.$$

Hence the element  $a$  is an element of  $M \cap N$ . This implies that  $a = e$ , which in turn means  $m_1 = m_2$  and  $n_1 = n_2$ . This proves the claim.

### Result

This amounts to proving that elements in  $MN$  are distinct.

## Section 6–2

1. a

**Given:**  $G$  is a group and  $a$  is an element of  $G$  of order  $d$ .

**To Prove:** Order of  $a^r$  is  $d$  if and only if  $r$  and  $d$  are relatively prime.

**Proof:** Let us assume order of  $a^r$  is  $d$ . We need to show that  $d$  and  $r$  are relatively prime to each other.

Let us now consider the cyclic subgroup  $H$  of the group  $G$ , such that  $H$  is generated by  $a$ .

Since order of  $a$  is  $d$ , order of the subgroup  $H$  is  $d$ .

From now we will denote the order of  $a$  and  $H$  as

$$o(a) \text{ and } o(H).$$

Since  $H = \langle a \rangle$ ,

$$a^d = e \text{ and } H := \{a, a^2, \dots, a^{d-1}, a^d (= e)\}.$$

**Since  $a^r$  has order  $d$  and  $a^r \in H$ , since  $H$  is cyclic group generated by  $a$ , then  $a^r$  is a generator of the group  $H$ .**

Then,

$$1 \leq r < d.$$

Since  $a^r$  is a generator and  $a \in H$ ,

$$a = (a^r)^k \text{ for some integer } k.$$

Hence,

$$a^{rk-1} = e.$$

Since order of  $a$  is  $d$ ,  $d$  is a divisor of  $rk - 1$ .

So,

$$rk - 1 = sd \text{ for some integer } s.$$

That is

$$kr + s'd = 1 \text{ where } k \text{ and } s' \text{ are integers}$$

and this implies

$$\gcd(r, n) = 1.$$

It follows that  $r$  is prime to  $d$ .

Before start the converse part let us go through a Lemma.

**Lemma:** Let  $a$  be an element of a group  $G$  and if  $o(a) = n$ , then for a positive integer  $m$ ,

$$o(a^m) = \frac{n}{\gcd(m, n)}.$$

**Proof of the Lemma:** Let us assume  $o(a^m) = k$ .

Then

$$a^{mk} = e, \text{ } e \text{ being the identity element of } G.$$

Now order of  $a$  is  $n \implies n$  divides  $mk$ .

Let  $\gcd(m, n) = d$ . Then

$$m = du, \quad n = dv, \text{ where } \gcd(u, v) = 1.$$

Now,

$$\begin{aligned} n|mk &\implies dv|duk \\ &\implies v|uk \\ &\implies v|k, \text{ since } \gcd(u, v) = 1. \end{aligned}$$

Again we have

$$\begin{aligned} (a^m)^v &= (a^{du})^v \\ &= a^{dsv} \\ &= (a^u)^n = e. \end{aligned}$$

So,  $o(a^m) = k$  and  $(a^m)^v = e \implies k$  divides  $v$ .

Therefore from above two arguments it follows that

$$k = v, \text{ i.e. } k = \frac{n}{d}.$$

Therefore

$$o(a^m) = \frac{n}{\gcd(m, n)}.$$

This completes the proof of the Lemma.

Now back to our problem.

Let us assume that  $d$  and  $r$  are relatively prime.

Then

$$\gcd(d, r) = 1.$$

By the above Lemma we have

$$o(a^r) = \frac{d}{\gcd(r, d)} = d.$$

Hence we proved that order of  $a^r$  is  $d$ .

This completes our proof.

## Result

4 of 4

Being  $o(a^r) = d$  we have considered the cyclic subgroup  $H$  of  $G$  generated by  $a$  and shown that  $a^r$  is a generator of  $H$  if and only if  $r$  is relatively prime to  $d$ . And the required solution follows. Click for the complete solution.

2. a

Candidates for a primitive root of  $\mathbb{Z}_{11}^*$  are given by (residue classes of) 2, 3, 4, ..., 10. We are going to start from the smallest and stop when we find a primitive root.

We have  $2^2 \equiv 4 \pmod{11}$ ,  $2^3 \equiv 8 \pmod{11}$ ,  $2^4 \equiv 5 \pmod{11}$ ,  $2^5 \equiv 10 \pmod{11}$ ,  $2^6 \equiv 9 \pmod{11}$ ,  $2^7 \equiv 7 \pmod{11}$ ,  $2^8 \equiv 3 \pmod{11}$ ,  $2^9 \equiv 6 \pmod{11}$ ,  $2^{10} \equiv 1 \pmod{11}$ ; we see that

2 is a primitive root for  $\mathbb{Z}_{11}^*$

### Result

2 of 1

2 is one cyclic generator for  $\mathbb{Z}_{11}^*$ . Click for more details.

### 3. a

We need to find an element of  $\mathbb{Z}_p^*$  of order 16. After short verification, using any online modulo calculator, we verify that 3 is the one.

### Result

2 of 2

3 is the man.

### 4. a

Look at field  $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$ . It is really a field, since  $\mathbb{Z}_3[x]$  is an integral domain and  $x^2 + 1$  is an irreducible polynomial in it, which means that ideal  $\langle x^2 + 1 \rangle$  is maximal.

Elements of this field are: \$0, 1, 2, x, 2x, x + 1, x + 2, 2x + 1, 2x + 2\$. It is easy to verify that  $(x + 1)$  is generator for cyclic group of non-zero elements.

### Result

2 of

We introduce the classic example.

### 5. a

Problem 7 solves the question of number of elements in  $\{a \in \mathbb{Z}_m \mid (a, p) = 1\}$ . To prove that this is cyclic group, we just have to observe that set  $\{a \in \mathbb{Z}_m \mid (a, p) = 1\} \cup \{0\}$  is a finite field. Then the claim follows immediately from **Theorem 6.2.4**.

### Result

Use **Theorem 6.2.4**.

## 6. a

The important thing to note is that non-zero elements of this finite field have absolute value 1. Otherwise we could obtain infinitely many elements from one element, by exponentiation.

On the other hand, each element has to have finite order, which means it has to have finite order. Therefore, it must be  $n$ -th complex root of 1. It is easy to see that for each  $n$  we obtain one field of complex  $n$ -th roots of 1.

### Result

2 of 2

First look at absolute value, then at degree.

## 7. a

Recall the definition of Euler  $\varphi$ -function. The Euler  $\phi$ -function is defined by:  $\varphi(1) = 1$  and, for  $n > 1$ ,  $\varphi(n)$  is the number of positive integers less than  $n$  and relatively prime to  $n$ .

### Step 2

2 of 3

Now notice that the positive integer less than equal to  $p^n$  which are not relatively prime to  $p^n$  are  $p, 2p, 3p, \dots, p^{n-1}p$ . Therefore the number of positive integers less than  $p^n$  and prime to  $p^n$  are  $p^n - p^{n-1}$ .

### Result

3 of 3

Therefore,  $\varphi(p^n) = p^{n-1}(p - 1)$ .

## 8. a

Let us first recall problem 2.4.37, If  $G$  be a cyclic group of order  $n$ , then for each positive divisor  $m$  of  $n$  there are exactly  $\phi(m)$  elements of order  $m$  in  $G$ .

## Step 2

2 of 11

Let us consider a finite cyclic group  $G$  of order  $mn$ . Suppose  $A, B$  and  $C$  be the set of all elements in  $G$  that have orders  $m, n, mn$  respectively, that means,

$$\begin{aligned}A &= \{x \in G \mid x^m = e \text{ and } x^k \neq e, \text{ for all } k < m\} \\B &= \{x \in G \mid x^n = e \text{ and } x^k \neq e, \text{ for all } k < n\} \\C &= \{x \in G \mid x^{mn} = e \text{ and } x^k \neq e, \text{ for all } k < mn\}\end{aligned}$$

## Step 3

3 of 11

Our aim is to show that  $|C| = |A||B|$ .

Let us define a map  $f : A \times B \rightarrow C$  by  $f((a, b)) = ab$ , for all  $a \in A, b \in B$ .

## Step 5

5 of 11

We will first check that  $f$  is well defined, that means  $f(a, b) \in C$  for  $a \in A$  and  $b \in B$ . Notice that the order of elements  $a$  and  $b$  in  $G$  are coprime, and  $G$  is abelian, so the order of the element  $ab$  is  $mn$ , so  $f$  is well-defined.

## Step 6

6 of 11

Notice that  $f$  is an injective map. To show this let  $f((a_1, b_1)) = f((a_2, b_2))$  then  $a_1b_1 = a_2b_2 \implies a_2^{-1}a_1 = b_2b_1^{-1}$ . Clearly  $a_2^{-1}a_1 \in A$  and  $b_2b_1^{-1} \in B$ . Also the possible order of the element  $a_2^{-1}a_1$  is 1 or  $m$  and possible order for the element  $b_2b_1^{-1}$  is 1 or  $n$ .

Since  $a_2^{-1}a_1 = b_2b_1^{-1}$  and  $m$  and  $n$  are co prime. Therefore  $a_2^{-1}a_1 = b_2b_1^{-1} = e$  and so,  $a_1 = a_2$  and  $b_1 = b_2$ , the map is injective. Thus,  $|A \times B| \leq |C|$ .

### Step 8

8 of 11

To show the reverse inequality let us define map  $g : C \rightarrow A \times B$  defined by

$$g(k) = (k^n, k^m).$$

### Step 9

9 of 11

Clearly  $g$  is injective. To show this Let  $g(k) = g(\ell)$  then  $k^n = \ell^n$  and  $k^m = \ell^m$ . Suppose  $k = u\ell$ . Then  $k^m = u^m\ell^m = u^mk^m$ . Therefore  $u^m = e$ . Similarly,  $u^n = e$ . Therefore,  $m$  and  $n$  must have a common divisor which is the order of  $u$ . Thus,  $u = e$ . Hence  $g$  is injective, so  $|C| \leq |A \times B|$ . Therefore,  $|C| = |A \times B| = |A||B|$ , as desired.

### Step 10

10 of 11

Now we know that from problem 2.4.37.  $|A| = \varphi(m)$ ,  $|B| = \varphi(n)$  and  $|C| = \varphi(mn)$ .

### Result

Therefore we get

$$\varphi(mn) = \varphi(m)\varphi(n).$$

### 9. a

Suppose  $n$  is a positive integer, then by **the uniqueness of factorization of positive integers** we have that  $n = \prod_{j=1}^m p_j^{k_j}$  where  $m$  and  $k_j$  are positive integers, and  $p_j$  are distinct prime numbers. Using the previous exercises we now directly obtain

$$\begin{aligned}\varphi(n) &= \varphi\left(\prod_{j=1}^m p_j^{k_j}\right) \\ &= \prod_{j=1}^m \varphi(p_j^{k_j}) \\ &= \prod_{j=1}^m p_j^{k_j-1}(p_j - 1),\end{aligned}$$

which is what we wanted.

### Result

2 of 2

$$\varphi(n) = \prod_{j=1}^m p_j^{k_j-1}(p_j - 1) \text{ where } n = \prod_{j=1}^m p_j^{k_j}. \text{ Click for more details.}$$

### 10. a

In last Problem we have found out that  $\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$ . Now we want to find a simple lower bound on this value, which is growing to infinity as  $n$  does.

We use notation  $\omega(n)$  for the number of prime divisors of number  $n$ . Since the smallest prime number is 2, we have  $\omega(n) \geq \log_2 n$ . Now we compute:

$$\begin{aligned}\varphi(n) &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \cdot \left(1 - \frac{1}{2}\right) \cdot \prod_{p|n, p \geq 3} \left(1 - \frac{1}{p}\right) \\ &\geq \frac{n}{2} \cdot \left(1 - \frac{1}{3}\right)^{\omega(n)-1} \geq \frac{n}{2} \cdot \left(\frac{2}{3}\right)^{\log_2 n - 1} = \frac{3}{4} n^{2 - \log_2 3}.\end{aligned}$$

The last expression obviously has grows to infinity as  $n$  does, which proves the claim.

## Result

2 of 1

Follows immediately from result of previous Problem.

## Section 6–3

### 1. a

Let  $f(x)$  and  $g(x)$  not be relatively prime in  $K[x]$ . This means there is polynomial  $h(x) \in K[x]$  which is a common divisor of  $f(x)$  and  $g(x)$ . But then  $f(x)$  and  $g(x)$  have a common root  $a$ , which is the root of  $h(x)$  in some extension of  $K$ , i.e. of  $F$ .

Now assume, on the contrary, that  $f(x)$  and  $g(x)$  are relatively prime in  $F[x]$ . Then there are polynomials  $u(x)$  and  $v(x)$  from  $F[x]$  such that  $u(x)f(x) + v(x)g(x) = 1$  holds. Plugging in  $x = a$  yields the obvious contradiction  $0 = 1$ .

## Result

2 of 2

Analogous proof is valid.

### 2. a

**Given:**  $F$  is a field and  $f(x)$  is a polynomial with coefficients in  $F$ , that is,  $f \in F[x]$ .

**To Prove:**  $f(x)$  has a multiple root in some extension of  $F$  if and only if  $f(x)$  is not relatively prime to its derivative,  $f'(x)$ .

**Proof:** Let us assume that  $f(x)$  has a multiple root in some extension of  $F$ . Let  $y$  be a multiple root of  $f(x)$ . Then over a splitting field, we have

$$f(x) = (x - y)^n g(x), \text{ for some integer } n \geq 2.$$

Here  $g(x)$  is a polynomial such that  $g(y) \neq 0$ .

Now taking derivative of  $f$  we get

$$f'(x) = n.(x - y)^{n-1}g(x) + (x - y)^n g'(x) \quad \dots\dots\dots(1)$$

here  $g'(x)$  implies derivative of  $g$  with respect to  $x$ .

Since we have  $n \geq 2$ , this implies  $(n - 1) \geq 1$ . Hence, (1) shows that  $f'(x)$  has  $y$  as a root.

Therefore,  $f(x)$  is not relatively prime to  $f'(x)$ .

We now prove the other direction.

Conversely, let us assume that  $f(x)$  is not relatively prime to  $f'(x)$ . Let  $y$  is a root of both  $f(x)$  and  $f'(x)$ .

Since  $y$  is a root of  $f(x)$ , we can write

$$f(x) = (x - y).g(x) \quad \dots\dots\dots(2)$$

for some polynomial  $g(x)$ . then taking derivative of  $f(x)$  we have

$$f'(x) = g(x) + (x - y).g'(x) \quad \dots\dots\dots(3)$$

where  $g'(x)$  is the derivative of  $g(x)$  with respect to  $x$ .

Since  $y$  is a root of  $f'(x)$  also we have

$$f'(y) = 0.$$

Then from (3) we have

$$\begin{aligned} f'(y) &= g(y) + (y - y).g'(y) \\ \implies f'(y) &= g(y) \\ \implies g(y) &= 0. \end{aligned}$$

This implies  $y$  is a root of  $g(x)$  also.

Therefore we have

$$g(x) = (x - y).h(x)$$

for some polynomial  $h(x)$ .

Now form (2) we have

$$f(x) = (x - y)^2.h(x).$$

This follows that  $y$  is a multiple root of  $f(x)$ .

Therefore,  $f(x)$  has a multiple root in some extension of the field  $F$ .

This completes the proof.

## Result

3 of 3

Considering that  $f$  has multiple root in some extension of the field  $F$ , we have proved that there exist a root if  $f$  which is also a root of  $f'$ , follows that  $f$  and  $f'$  are not relatively prime, and vice versa. Click for the complete proof.

### 3. a

**Given:**  $F$  is a field and  $f(x)$  is a polynomial with coefficients in  $F$ , that is,  $f \in F[x]$ .

**To Prove:**  $f(x)$  has a multiple root in some extension of  $F$  if and only if  $f(x)$  is not relatively prime to its derivative,  $f'(x)$ .

**Proof:** Let us assume that  $f(x)$  has a multiple root in some extension of  $F$ . Let  $y$  be a multiple root of  $f(x)$ . Then over a splitting field, we have

$$f(x) = (x - y)^n g(x), \text{ for some integer } n \geq 2.$$

Here  $g(x)$  is a polynomial such that  $g(y) \neq 0$ .

Now taking derivative of  $f$  we get

$$f'(x) = n.(x - y)^{n-1}g(x) + (x - y)^ng'(x) \quad \dots\dots(1)$$

here  $g'(x)$  implies derivative of  $g$  with respect to  $x$ .

Since we have  $n \geq 2$ , this implies  $(n - 1) \geq 1$ . Hence, (1) shows that  $f'(x)$  has  $y$  as a root.

Therefore,  $f(x)$  is not relatively prime to  $f'(x)$ .

We now prove the other direction.

Conversely, let us assume that  $f(x)$  is not relatively prime to  $f'(x)$ . Let  $y$  is a root of both  $f(x)$  and  $f'(x)$ .

Since  $y$  is a root of  $f(x)$ , we can write

$$f(x) = (x - y).g(x) \quad \dots\dots\dots\dots(2)$$

for some polynomial  $g(x)$ . then taking derivative of  $f(x)$  we have

$$f'(x) = g(x) + (x - y).g'(x) \quad \dots\dots\dots\dots(3)$$

where  $g'(x)$  is the derivative of  $g(x)$  with respect to  $x$ .

Since  $y$  is a root of  $f'(x)$  also we have

$$f'(y) = 0.$$

Then from (3) we have

$$\begin{aligned} f'(y) &= g(y) + (y - y).g'(y) \\ \implies f'(y) &= g(y) \\ \implies g(y) &= 0. \end{aligned}$$

This implies  $y$  is a root of  $g(x)$  also.

Therefore we have

$$g(x) = (x - y).h(x)$$

for some polynomial  $h(x)$ .

Now from (2) we have

$$f(x) = (x - y)^2 \cdot h(x).$$

This follows that  $y$  is a multiple root of  $f(x)$ .

Therefore,  $f(x)$  has a multiple root in some extension of the field  $F$ .

This completes the proof.

## Result

3 of 3

Considering that  $f$  has multiple root in some extension of the field  $F$ , we have proved that there exist a root if  $f$  which is also a root of  $f'$ , follows that  $f$  and  $f'$  are not relatively prime, and vice versa. Click for the complete proof.

## 4. a

We use derivative, since every multiple root of a polynomial must be a root of its derivative. So, polynomial is  $f(x) = x^n - x$  and derivative is  $f'(x) = nx^{n-1} - 1$ .

Now assume that  $f(a) = 0$ . We need to prove that  $f'(a) = 0$  is impossible. From  $f(a) = 0$  we obtain  $a = a^n$ . If  $a \neq 0$  this implies  $a^{n-1} = 1$ . Then for derivative we have  $f'(a) = n a^{n-1} - 1 = n-1 \neq 0$  since  $(n-1)$  is not a multiple of field characteristic. Case  $a = 0$  is trivial. Hence, polynomials  $f(x)$  and  $f'(x)$  can not have a common root, which means that  $f(x)$  can not have a multiple root.

## Result

2 of

Use derivative.

## 5. a

Just note that  $m - 1 = p^n - 1$  can not be a multiple of characteristic  $p$ . Now apply the result of previous Problem.

## Result

2 of

Just note that  $m - 1 = p^n - 1$  can not be a multiple of characteristic  $p$ .

## 6. a

I'll leave you to verify that 4 is a multiple root of polynomial  $x^6 - x$  over field  $\mathbb{Z}_5$ . I suggest you use derivative.

## Result

2 of

4 is a multiple root of polynomial  $x^6 - x$  over field  $\mathbb{Z}_5$ .

## 7. a

**Given:**  $K$  is a finite field having  $p^n$  elements and  $m$  is a divisor of  $n$ .

**To Prove:** There exists a subfield of  $K$  with  $p^m$  elements.

**Proof:**

First of all, if  $m$  divides  $n$ , consider the set  $S_m(F)$  of all  $a \in F$  such that  $a^{p^m} = a$ .  
This

subset is clearly closed under multiplication,

and it is also closed under addition because of the binomial theorem and the fact that  $pa = 0$  for every  $a \in F$ .

It contains 0 and 1, and hence it is a subring of  $F$  and hence a

**subfield**  
(since  $F$  is finite).

The set  $S_m$  is in fact the

**set of roots of the polynomial  $x^{p^m} - x$ , and hence  $S_m$  has at most  $p^m$  elements**

Note that  $0 \in S_m(F)$  and so  $S'_m(F) := S_m(F) - \{0\}$  has at most  $p^m - 1$  elements; furthermore

**$S'_m(F)$  is the set of roots of the polynomial  $x^{p^{m-1}} - 1$  in  $F$ .**

Since  $n$  is divisible by  $m$ , we can write  $n = md$  for some integer  $d$ .

Then

$$p^n - 1 = p^{md} - 1 = (p^m - 1)(1 + p^m + p^{2m} + \dots + p^{md-d}).$$

In particular,

$$p^m - 1 \text{ divides } p^n - 1.$$

We know that

**the group  $F^*$  is cyclic of order  $p^{n-1}$ , and since  $p^m - 1$  divides  $p^n - 1$ ,  $F^*$  contains a unique subgroup of order  $p^{m-1}$ ,**

**namely, the set of elements  $x$  such that  $x^{p^{m-1}} - 1 = 0$**

This shows that  $S'_m(F)$  has exactly  $p^{m-1}$  elements and hence that  $S_m(F)$  has exactly  $p^m$  elements, hence is a subfield of order  $p^m$ .

Therefore, we conclude

**the existence of a subfield of  $K$  with  $p^m$  elements.**

**Done.**

### Result

3 of 3

Therefore, for a finite field  $K$  with  $p^n$  elements we get a sub-field of  $K$  with  $p^m$  elements, where  $m$  divides  $n$ .

Click for the detailed Solution.

## Section 6–5

1. a

$\phi_2(x)$  has no choice but to be irreducible. For the rest of the polynomial guys, we only need to verify that they do not have integer roots, because of Gauss lemma. This is straightforward since polynomials are simple.

**Result**

2 of 2

Use Gauss lemma.

2. a

Using the inductive formula for cyclotomic polynomials, we compute:

- $\phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$
- $\phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
- $\phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$

**Result**

Use the formula.

3. a

**Given:**  $(x^m - 1)$  divides  $(x^n - 1)$ , for some integers  $m, n$ .

**To Prove:**  $m$  divides  $n$ .

**Proof:** First we start with a claim.

**Claim:** If  $m$  divides  $n$ , then  $x^m - 1$  divides  $x^n - 1$ .

**Proof of the Claim:** If  $m$  divides  $n$ , then there exists a positive integer  $k$  such that

$$n = km.$$

Therefore we have,

$$\begin{aligned} x^n - 1 &= x^{km} - 1 \\ &= (x^m)^k - 1 \\ &= (x^m - 1)(1 + x^m + \dots + (x^m)^{k-1}). \end{aligned}$$

Since  $x, m$  and  $k$  are positive integers, then all the terms in the above parenthesis on the right hand side are integers, so that their sum is an integer.

Hence,  $x^m - 1$  divides  $x^n - 1$ .

This completes our Claim.

We now proceed with contrapositive.

If possible, let us assume that  $m$  does not divide  $n$ . Then there exist integers  $k \geq 0$  and  $r$  satisfying  $0 < r < n$ , such that  $n = km + r$ .

Then we have

$$\begin{aligned}x^n - 1 &= x^{(km+r)} - 1 \\&= x^r x^{(km)} - 1 \\&= x^r x^{(km)} - x^r + x^r - 1 \\&= x^r(x^{(km)} - 1) + x^r - 1\end{aligned}$$

Since  $m$  divides  $km$ , it follows from the above Claim that  $x^m - 1$  divides  $x^{km} - 1$ .

Hence, there is an integer  $p$  such that

$$x^{km} - 1 = p(x^m - 1).$$

Therefore, it yields from the above result that

$$x^n - 1 = px^r(x^m - 1) + x^r - 1.$$

Now  $p \cdot x^r$  is a positive integer. And since we have  $0 < r < n$ , then we can conclude that

$$0 < x^r - 1 < x^m - 1.$$

Hence, it follows from aforesaid argument that the division of  $x^n - 1$  by  $x^m - 1$  leaves a positive remainder, that is,  $x^m - 1$  does not divide  $x^n - 1$ .

Therefore,

$$m \text{ does not divide } n \implies x^m - 1 \text{ does not divide } x^n - 1.$$

Hence it follows that

$$x^m - 1 \text{ divides } x^n - 1 \implies m \text{ divides } n.$$

This completes the proof.

## Result

3 of 3

First we show that if  $m$  divides  $n$  then  $x^m - 1 | (x^n - 1)$  and then by contrapositive we have proved that

$$m \text{ does not divide } n \implies x^m - 1 \text{ does not divide } x^n - 1.$$

Click for the detailed solution.

4. a

**Given:**  $a$  is an integer such that  $a > 1$  and  $(a^m - 1)$  divides  $(a^n - 1)$ , for some integers  $m, n$ .

**To Prove:**  $m$  divides  $n$ .

**Proof:** First we start with a claim.

**Claim:** If  $m$  divides  $n$ , then  $a^m - 1$  divides  $a^n - 1$ .

**Proof of the Claim:** If  $m$  divides  $n$ , then there exists a positive integer  $k$  such that

$$n = km.$$

Therefore we have,

$$\begin{aligned} a^n - 1 &= a^{km} - 1 \\ &= (a^m)^k - 1 \\ &= (a^m - 1)(1 + a^m + \dots + (a^m)^{k-1}). \end{aligned}$$

Since  $a > 1$ ,  $m$  and  $k$  are positive integers, then all the terms in the above parenthesis on the right hand side are integers, so that their sum is an integer.

Hence,  $a^m - 1$  divides  $a^n - 1$ .

This completes our Claim.

We now proceed with contrapositive.

If possible, let us assume that  $m$  does not divide  $n$ . Then there exist integers  $k \geq 0$  and  $r$  satisfying  $0 < r < n$ , such that  $n = km + r$ .

Then we have

$$\begin{aligned} a^n - 1 &= a^{(km+r)} - 1 \\ &= a^r a^{(km)} - 1 \\ &= a^r a^{(km)} - a^r + a^r - 1 \\ &= a^r (a^{(km)} - 1) + a^r - 1 \end{aligned}$$

Since  $m$  divides  $km$ , it follows from the above Claim that  $a^m - 1$  divides  $a^{km} - 1$ .

Hence, there is an integer  $p$  such that

$$a^{km} - 1 = p(a^m - 1).$$

Therefore, it yields from the above result that

$$a^n - 1 = pa^r(a^m - 1) + a^r - 1.$$

Now  $p \cdot a^r$  is a positive integer. And since we have  $a > 1$  and  $0 < r < n$ , then we can conclude that

$$0 < a^r - 1 < a^m - 1.$$

Hence, it follows from aforesaid argument that the division of  $a^n - 1$  by  $a^m - 1$  leaves a positive remainder, that is,  $a^m - 1$  does not divide  $a^n - 1$ .

Therefore,

$$m \text{ does not divide } n \implies a^m - 1 \text{ does not divide } a^n - 1.$$

Hence it follows that

$$a^m - 1 \text{ divides } a^n - 1 \implies m \text{ divides } n.$$

This completes the proof.

## Result

3 of 3

First we show that if  $m$  divides  $n$  then  $a^m - 1 | (a^n - 1)$  and then by contrapositive we have proved that

$$m \text{ does not divide } n \implies a^m - 1 \text{ does not divide } a^n - 1.$$

Click for the detailed solution.

## 5. a

**Given:**  $K$  be a finite field extension of  $\mathbb{Q}$ , the field of rationals.

**To Prove:** There is only a finite number of roots of unity in  $K$ .

**Proof:**

Let  $S$  be

**the set of roots of unity in  $K$ .**

Now

**every root of unity is a primitive  $n$ -th root of unity for some  $n \in \mathbb{N}$  and this integer  $n$  is uniquely determined by the root**

Let  $S_n$  be the set of primitive  $n - th$  roots of unity in  $K$ .

Clearly,

$$S_n \cap S_m = \emptyset \text{ for } n \neq m$$

Hence we can write

$$S = S_1 \cup S_2 \cup S_3 \cup \dots$$

i.e.  $S$  is the **disjoint union** of  $S_n$ 's.

We should note that

**some of the sets  $S_n$  may be empty**

Now if possible let us assume that the set  $S$  has infinitely many elements.

As each of the sets  $S_n$  has at most  $n$  many elements

(because it is the solution set of the polynomial  $x^n - 1$  in  $K$ ),  
we must have an increasing sequence of integers  $n_1 < n_2 < \dots$ , which is unbounded,

such that

$$S_{n_i} \neq \emptyset.$$

But for  $\alpha \in S_{n_i}$  we have  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(n_i)$  where  $\phi$  is the **Euler's phi function** (~over  $\mathbb{Q}$  the  $n - th$

**cyclotomic polynomial is irreducible of degree  $\phi(n)$  for any  $n \in \mathbb{N}$**

).

From the **definition** of  $\phi$  it is clear that

$$\phi(n_i) \rightarrow \infty \text{ as } n \rightarrow \infty$$

Now we have

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)]\phi(n_i),$$

hence it follows that

$$\phi(n_i) | [K : \mathbb{Q}].$$

But given that

**$[K : \mathbb{Q}]$  is finite and  $\phi(n_i) \rightarrow \infty$  by our assumption, we have arrived at a contradiction.**

So,

$$|S| < \infty.$$

This completes the proof.