# Assignment 1 solutions

Vedantam Srivatsav

May 2025

1. Prove that in any group $G$, the identity element is unique.

**Solution:** consider elements $e_1, e_2$ to be the identity elements of G.
we have,

$$e_1 = e_1 \cdot e_2 = e_2$$

Therefore we have $e_1 = e_2$
$\Rightarrow$ idenitity of a group is unique.

2. Let $G$ be a group. Prove that for any $a \in G$, the inverse of $a$ is unique.

**Solution:** consider $a \in G$, and $b, c \in G$ such that b,c are inverse of a. we have,

$$\begin{gathered} b = b \cdot e = b \cdot (a \cdot c) \\ b \cdot (a \cdot c) = (b \cdot a) \cdot c \quad \text{(by associativity)} \\ \Rightarrow b = c \quad (\text{because } b \cdot a = e) \end{gathered}$$

Hence we have unique inverse for all elements in G.

3. Let $a \in G$, where $G$ is a group. Prove that $(a^{-1})^{-1} = a$.

**Solution:** Consider $a \in G$. We have an inverse $a^{-1}$ such that

$$a \cdot a^{-1} = e$$

Let $b \in G$ be such that $b = (a^{-1})^{-1}$. Then:

$$b \cdot a = e$$

But from Question 2, we know that inverses in a group are unique. Since both $b$ and $a$ are left inverses of $a^{-1}$, we conclude:

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

4. Let $G$ be a group and $a \in G$. Prove that the set $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of $G$.

**Solution:** Let $n, m \in \mathbb{Z}$

1. **Closure:** let $a^n, a^m \in \langle a \rangle$,
$$a^n \cdot a^m = a^{n+m} \in \langle a \rangle$$
hence the set follows closure property.
2. **Identity:** $a^0 = e \in \langle a \rangle$, so we can say $\langle a \rangle$ has identity element.
3. **Associativity:** since all the elements in $\langle a \rangle$ are in G, they also satisfy associativity
4. **Inverse:** for every $a^n \in \langle a \rangle$, we also have $a^{-n} \in \langle a \rangle$, such that
$$a^n \cdot a^{-n} = e$$
Hence $\langle a \rangle$ satisfies inverse property.

Hence we can say that $\langle a \rangle$ is a subgroup of G.

5. Prove that every subgroup of a cyclic group is cyclic.

**Solution:**

- consider a **cyclic group G** $= \langle g \rangle$, where g is the generator of the cyclic group.
- let **H** be a non-trivial subgroup of G and choose an element a such that $a \in H$,
since a also belongs to G, we have
$$a = g^k \quad \text{for some } k \in \mathbb{Z}^+ (\text{if k is supposed to be negative, just choose } a^{-1})$$
- if $a \in H$, then every power of a also belongs to H $\Rightarrow$ every power of $g^k$ also belongs to H.
- by the **Well-ordering-principle,** we have an element $h \in H$ such that
$$h = g^m, m \in \mathbb{Z}^+$$
where m is the smallest such power of g.
- consider another element $b \in H$, such that $b = g^n$ for some $n \in \mathbb{Z}^+$, use the **Eulclid's division lemma** to write down,
$$n = mq + r \quad \text{where } 0 \leq r < m$$
- from the above equation we get,
$$g^n = g^{mq+r} = g^{mq} \cdot g^r \Rightarrow g^r = (g^{mq})^{-1} \cdot g^n$$
which implies $g^r \in$ H.
- but we considered m to be the smallest non-zero element, so r has to be equal to 0, therefore m divides every n which satisfies the above property for b, giving us $g^m$ as the generator for the subgroup H, making it cyclic.

Hence, every subgroup of a cyclic group is cyclic.

6. Let $G$ be a finite group and $a \in G$. Prove that the order of $a$ divides the order of $G$.

**Solution:**

- **Lagrange's theorem** states that if H is a subgroup of G, then the **order** of H divides the order of G. we derive it from:

  $$|G| = [G:H] * |H| \quad \text{where [G:H] is the } \textbf{index} \text{ of the subgroup H.}$$

- From question 2. we know that $\langle a \rangle$, where a $\in G$ is a subgroup of G.
- **Claim:** order of a is equal to order of the subgroup $\langle a \rangle$.
  proof: consider n = order of a, for any value $m > n$, and $m = nq + r$, where $r < n$, we have

  $$a^m = a^{nq+r} = e \cdot a^r = a^r$$

  $\Rightarrow$ every element after $a^n$ repeats the elements that appear before, which means the subgroup $\langle a \rangle$ has n unique elements.
- since $\langle a \rangle$ has n unique elements, it means order of $\langle a \rangle$ is n.
- we have

  $$|\langle a \rangle| = |a| = n, \quad \text{and}$$

  $$|\langle a \rangle| \text{ divides } |G| \Rightarrow n \text{ divides } |G| \quad \text{(by lagrange's theorem)}$$

Hence proved that the order of a divides the order of G.

7. Let $a$ be an element of order $n$ in a group. Prove that $a^k = e$ if and only if $n \mid k$.

**Solution:**

- We apply **Euclid's division lemma** on k and n, to get

  $$k = nq + r \quad \text{for some q} \in \mathbb{Z} \text{ and } 0 \leq r < n$$

- **Note:** since n is the order of a, we have

  $$(a^n)^q = e^q = a^{nq}$$

  Therefore every multiple of n gives e when taken as power of a.
- from the above equation, we get:

  $$a^k = a^{nq+r} = a^{nq} \cdot a^r = e \cdot a^r = e$$

  which implies $a^r = e$, but r is less than n and since n is the order of a, n is the smallest non-zero power of a which satisfies $a^n = e$, hence r has to be equal to 0.
- Therefore we have,

  $$k = nq + 0 = nq$$

  $\Rightarrow$ n divides q.

Hence $a^k = e$ iff $n \mid k$ (the reverse implication is a direct result from the Note).

8. Let $H \subseteq G$ and suppose that for all $a, b \in H$, we have $ab^{-1} \in H$. Prove that $H$ is a subgroup of $G$.

**Solution:**

1. **Identity:**let a $\in H$, then we have $e = a \cdot a^{-1} \in H$.
2. **Inverse:** let e,a $\in H$, then we have $a^{-1} = e \cdot a^{-1} \in H$
3. **Associativity:** since every element in H is from G, they all satisfy associativity.
4. **Closure:** sicne we proved inverses exist, if $a, b, b^{-1} \in H$, then $a \cdot b \in H$, hence the elements of this set follow closure.

from the above properties, we have shown that H is a subgroup of G.

9. Let $G = \mathbb{Z}$ under addition. Prove that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{N} \cup \{0\}$.

**Solution:**

- consider a non-trivial subgroup G, which contains non-zero elements, since it is a group, if n exists in G, -n also exists(by inverse property of groups).
- Hence we can say every non trivial subgroup has positive as well as negative elements.
- By **Well ordering principle** we have a smallest positive integer p in the subgroup.
- if p exists in the group, all the multiples of p also exist in the group by closure property of addition.
- consider another element a in G which is not a multiple of p, by **Euclid's division lemma**, we have:

$$a = pq + r \quad \text{where } r \in \mathbb{Z} \text{ and } r < p$$
$$r = a - pq \Rightarrow r \in G \quad \text{by closure property of G}$$

  but our initial assumption was n to be the smallest positive integer in G, therefore there is a contradiction and r is supposed to be 0
- Hence every element of G will be a multiple of the smallest positive integer in G.
- This can be represented as $n\mathbb{Z}$ for some $n \in \mathbb{N} \cup \{0\}$

10. Let $R$ be a ring. Prove that $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.

**Solution:** By the **Distributive property** of rings, we get
(**Note:** here we use $\cdot$ for multiplication, which is different from the arbitrary binary operation considered in the above questions).

$$a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \tag{1}$$
$$a \cdot 0 = 2(a \cdot 0) \tag{2}$$
$$\Rightarrow (a \cdot 0) = 0 \tag{3}$$

11. Let $R$ be a commutative ring with unity. Prove that the set of units in $R$ forms a group under multiplication.

**Solution:**

1. **Identity:** 1 will be the identity element of all the elements.
2. **Inverse:** since the set of units is the set of all elements with inverse, if $a \in U$, then $a^{-1} \in U$ where U is the set of all units in R.
3. **Associativity:** all elements of a Ring satisfy associativity under multiplication, hence elements of U also satisfy associativity.
4. **Closure:** for any two elements a,b in U, we have,

$$a(b+0) = ab + 0 \cdot a = ab \in U$$

Hence the set of units U forms a group under multiplication.

12. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $\varphi(a) = \bar{a}$. Prove that $\varphi$ is a ring homomorphism.

**Solution:**

1. let $\bar{a} = n_1$ and $\bar{b} = n_2$, we have

$$\begin{aligned} \varphi(a+b) &= \overline{(a+b)} \\ \overline{(a+b)} &= \bar{a} + \bar{b} \quad \text{(by the rules of modulo)} \\ \bar{a} + \bar{b} &= \varphi(a) + \varphi(b) \\ \Rightarrow \varphi(a+b) &= \varphi(a) + \varphi(b) \end{aligned}$$

2. we have

$$\begin{aligned} \varphi(ab) &= \overline{ab} \\ \overline{ab} = \bar{a} \cdot \bar{b} &= \varphi(a) \cdot \varphi(b) \\ \Rightarrow \varphi(ab) &= \varphi(a) \cdot \varphi(b) \end{aligned}$$

Hence the given relation is a ring homomorphism.

13. Let $\varphi : R \to S$ be a ring homomorphism. Prove that $\varphi(0_R) = 0_S$ and $\varphi(-a) = -\varphi(a)$ for all $a \in R$.

**Solution:**

1.

$$\begin{aligned} \varphi(0_R + 0_R) &= \varphi(0_R) + \varphi(0_R) \\ \varphi(0_R) &= 2 \cdot \varphi(0_R) \\ \Rightarrow \varphi(0_R) &= 0_S \end{aligned}$$

hence we have $\varphi(0_R) = 0_S$

2.

$$\begin{aligned} \varphi(-1+1) = \varphi(0) &= \varphi(-1) + \varphi(1) \\ \Rightarrow \varphi(-1) &= -\varphi(1) \\ \text{using the above relation we get} \\ \varphi(-1 \cdot a) = \varphi(-a) &= \varphi(-1) \cdot \varphi(a) \\ \varphi(-a) = -\varphi(1) \cdot \varphi(a) &= -\varphi(1 \cdot a) \\ \Rightarrow \varphi(-a) &= -\varphi(a) \end{aligned}$$

Hence we have $-\varphi(-a) = \varphi(a)$

14. Let $R$ be a ring with unity. Prove that the characteristic of $R$ is the smallest positive integer $n$ such that $n \cdot 1 = 0$, or 0 if no such $n$ exists.

**Solution:**

- **Definition:** The characteristic of a ring $R$ is $n$ precisely if the statement $ka = 0$ for all $a \in R$ implies that $k$ is a multiple of $n$.
- assume n is the charecteristic of R, let r be a positive integer and assume $r < n$, if r satisfies the above property, we have:
$$ra = 0 \quad \forall a \in R$$
$\Rightarrow$ n divides r.
- But r is less than n, which means r doesn't exist (as we assumed r is a positive integer)
- Therefore we have n to be the **Smallest** positive integer which satisfies $n \cdot 1 = 0$, and if no such positive n exists, the smallest integer which satisfies the property will be 0.

15. Prove that the number of integers less than $n$ and coprime to $n$ is given by

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product is over all distinct prime divisors $p$ of $n$.

**Solution:**

1.