Isomorphisms

Q1 prove or disprove the following

(i) $\boxed{U(9) \cong U(7)}$

SOL: $U(9) = \{1,2,4,5,7,8\}$

is cyclic since
$2^1 \equiv 2$
$2^2 \equiv 4$
$2^3 \equiv 8$
$2^4 \equiv 16 \equiv 7$
$2^5 \equiv 14 \equiv 5$
$2^6 \equiv 10 \equiv 1$

Hence, $\langle 2 \rangle = U(9)$

since $|U(9)| = 6$, and $U(9)$ is cyclic, we know

$U(9) \cong \mathbb{Z}_6$

by our classification of cyclic groups.

Similarly $U(7) = \{1,2,3,4,5,6,7\}$

is cyclic.
$2^1 \equiv 2$
$2^2 \equiv 4$
$2^3 \equiv 8 \equiv 1$

o.k. this does not generate $U(7)$ but maybe 3:

$3^1 \equiv 3$
$3^2 \equiv 9 \equiv 2$
$3^3 \equiv 6$
$3^4 \equiv 18 \equiv 4$
$3^5 \equiv 12 \equiv 5$
$3^6 \equiv 15 \equiv 1$.

Hence, $U(7) = \langle 3 \rangle$ and also $|U(7)| = 6$ →

Thus, $U(7) \cong \mathbb{Z}_6$.

Hence $U(9) \cong \mathbb{Z}_6 \cong U(7)$, which means indeed

$$U(9) \cong U(7).$$

$\square$.

(ii) $\boxed{U(9) \cong D_3}$

D_3 is a nonabelian group AND $U(9)$ is abelian. This means they cannot be isomorphic (even though $|U(9)| = 6 = |D_3|$.).

Thus, $U(9) \ncong D_3$. $\square$.

(iii) $\boxed{U(9) \cong U(5)}$

$U(9) = \langle 2 \rangle$ ← cyclic and order $|U(9)| = 6$.

$U(5) = \{1,2,3,4\} = \langle 2 \rangle$ ← cyclic and order $|U(5)| = 4$.

Since the orders of these groups are not the same, they cannot be isomorphic.

Thus, $U(9) \ncong U(5)$ $\square$

(iv) $\boxed{U(9) \cong \mathbb{Z}_3 \times \mathbb{Z}_2}$

Recall, $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} \longleftrightarrow \gcd(n,m) = 1$

Thus, $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$

from (i) we see $U(9) \cong \mathbb{Z}_6$ so indeed.

$$U(9) \cong \mathbb{Z}_3 \times \mathbb{Z}_2$$

$\square$.

(v) $\boxed{\mathbb{Z} \cong 5\mathbb{Z}}$

SOL 1:

$5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\} = \langle 5 \rangle$

so this is cyclic and infinite. By our classification of cyclic groups. $\mathbb{Z} \cong 5\mathbb{Z}$.

$\square$

SOL 2: you can verify $\varphi(n) = 5n$ is indeed an isomorphism for a $\varphi: \mathbb{Z} \to 5\mathbb{Z}$. $\square$.

(vi) $\boxed{\mathbb{Z} \cong n\mathbb{Z}}$

Similarly $n\mathbb{Z} = \langle n \rangle$

so this is cyclic and finite. Hence

$n\mathbb{Z} \cong \mathbb{Z}$. $\square$.

(v) $\boxed{\mathbb{Q} \cong \mathbb{Z}}$

Recall, $\mathbb{Q}$ is not cyclic. Hence,

$\mathbb{Q} \ncong \mathbb{Z}$.

(vi) $\boxed{\mathbb{R} \cong \mathbb{Z}}$

Many reasons why this is false but two quick ones: $\mathbb{R}$ is uncountably infinite while $\mathbb{Z}$ is countably infinite hence

$\mathbb{R} \ncong \mathbb{Z}$.

also $\mathbb{R}$ is not cyclic. hence

$\mathbb{R} \ncong \mathbb{Z}$.

(2) Define $\varphi : (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}^+, \cdot)$ by

$$\forall x \in \mathbb{R}^+, \quad \varphi(x) = \sqrt{x}.$$

Prove that φ is an automorphism.

$\boxed{\text{SOL}}$.

(i) φ is well defined since $\sqrt{x} \geq 0$, so $\sqrt{x} \in \mathbb{R}^+$ if $x \in \mathbb{R}^+$.

(ii) φ is one-to-one:

Let $x, y \in \mathbb{R}^+$. (the domain here)

Suppose $\varphi(x) = \varphi(y)$ (Show: $x = y$)

$\sqrt{x} = \sqrt{y}$

$(\sqrt{x})^2 = (\sqrt{y})^2$

$x = y$. ✓ so φ is one-to-one ✓

(iii) φ is ONTO:

Let $y \in \mathbb{R}^+$ (the codomain here).

(Show: $\exists x \in \mathbb{R}^+$ (the domain) such that $\varphi(x) = y$).

Let $x = y^2$.

Then $\varphi(x) = \sqrt{x} = \sqrt{y^2} = |y| = y$. since $y \in \mathbb{R}^+$.

so φ is onto. ✓

(iv) φ is operation preserving.

Let $x, y \in \mathbb{R}^+$ (the domain here.).

(Show: $\underset{\substack{\uparrow \\ \text{operation in domain is } \cdot}}{\varphi(xy)} = \varphi(x) \underset{\substack{\uparrow \\ \text{operation in codomain is } \cdot}}{\,} \varphi(y)$)

$$\varphi(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = \varphi(x)\varphi(y) \quad ✓$$

by (i)-(iv) φ is an automorphism □.

(Q3) Let G be a group. ~~[illegible]~~ Let $\varphi: G \to G$ be defined by:

$$\forall g \in G, \ \varphi(g) = g^{-1}$$

Prove: that φ is an automorphism iff G is abelian.

$\boxed{\text{proof}}$

($\longrightarrow$) Suppose φ is an automorphism

(Show: G is abelian).

Let $a, b \in G$. (Show: $ab = ba$).

SOL 1: Since φ is an automorphism $\exists x, y \in G$ s.t. $a = \varphi(x)$, $b = \varphi(y)$.

$$ab = \varphi(x)\varphi(y) = \varphi(xy) \quad \text{since } \varphi \text{ is operation preserving.}$$
$$= (xy)^{-1}$$
$$= y^{-1}x^{-1}$$
$$= \varphi(y)\varphi(x)$$
$$= ba.$$

✓

SOL 2: $ab = \varphi((ab)^{-1})$ by definition of φ

$= \varphi(b^{-1}a^{-1})$ by socks-and-shoes.

$= \varphi(b^{-1})\varphi(a^{-1})$ since φ is an automorphism.

$= (b^{-1})^{-1}(a^{-1})^{-1}$ by definition of φ

$= ba.$

✓

($\longleftarrow$) Suppose G is abelian. (Show φ is an automorphism.)

Check properties (i) – (iii) (quick).

(iv) Let $a, b \in G$.

$$\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} \overset{\text{since } G \text{ is abelian}}{=} a^{-1}b^{-1} = \varphi(a)\varphi(b).$$

✓

Q4 Let φ be an automorphism of G.
Prove that $H = \{ x \in G \mid \varphi(x) = x \} \leq G$.

$\boxed{\text{proof}}$ 3-step subgroup test.

(i) (Show that the identity $e \in G$ is also in H.)

Since φ is an automorphism and $\varphi: G \to G$.

$\varphi(e) = e$

Thus, $e \in H$ (by definition.)

(ii) Let $a, b \in H$. (<u>show</u> $ab \in H$).

<u>Closure</u>

Since $a \in H \to \varphi(a) = a$

Since $b \in H \to \varphi(b) = b$.

(If we want $ab \in H$ we need to show $\varphi(ab) = ab$)

$\varphi(ab) = \varphi(a)\varphi(b)$ since φ is an automorphism.

$= ab$ since $a, b \in H$.

Hence, $ab \in H$.

(iii) Let $a \in H$ (<u>show</u> $a^{-1} \in H$).

<u>inverses</u>

Since $a \in H \to \varphi(a) = a$.

(If we want $a^{-1} \in H$ we need to show $\varphi(a^{-1}) = a^{-1}$)

$\varphi(a^{-1}) = (\varphi(a))^{-1}$ (property of isomorphism/automorphism.)

$= (a)^{-1}$ since $a \in H$.

$= a^{-1}$

Thus, $a^{-1} \in H$.

Hence, $H \leq G$. $\square$