Homework 5

Due: June 1st (Monday), 11:59 pm

- Please submit your work on Blackboard.
- You are required to submit your work as a single pdf.
- Please make sure your handwriting is clear enough to read. Thanks.
- No late work will be accepted.
- There are five randomly picked questions (2 pts for each) that will be graded.
  (1), (5), (8), (9), (10)

---

(1) Show that the multiplicative group $\mathbf{Z}_7^\times$ is isomorphic to the additive group $\mathbf{Z}_6$.

Define a function $\phi : \mathbf{Z}_6 \to \mathbf{Z}_7^\times$ by letting $\phi([n]_6) = [3]_7^n$ since $\mathbf{Z}_7^\times = \langle [3]_7 \rangle$.

- If $[n_1] = [n_2]$, i.e., $n_1 \equiv n_2 \pmod 6$, then $[3]_7^{n_1} = [3]_7^{n_2}$ since $o([3]_7) = 6$. This implies that $\phi([n_1]_6) = \phi([n_2]_6)$.Thus, ϕ is well-defined.
- For any two elements $[m]_6, [n]_6 \in \mathbf{Z}_6$, we have
  $\phi([m]_6 + [n]_6) = \phi([m+n]_6) = [3]_7^{m+n} = [3]_7^m \cdot [3]_7^n = \phi([m]_6) \cdot \phi([n]_6)$.
  Thus, ϕ respects the two operations.
- If $\phi([n]_6) = [3]_7^n = [1]_7$, then $6|n$ since $o([3]_7) = 6$. So $[n]_6 = [0]_6$. By Proposition 5, ϕ is one-to-one.
- Since $|\mathbf{Z}_6| = |\mathbf{Z}_7^\times| = 6$, any any one-to-one mapping must be onto.

Thus, ϕ is an isomorphism.

(2) Show that the multiplicative group $\mathbf{Z}_8^\times$ is isomorphic to the group $\mathbf{Z}_2 \times \mathbf{Z}_2$.

$\mathbf{Z}_8^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ and $\mathbf{Z}_2 \times \mathbf{Z}_2 = \{([0]_2, [0]_2), ([1]_2, [0]_2), ([0]_2, [1]_2), ([1]_2, [1]_2)\}$
Define a function $\phi : \mathbf{Z}_8 \to \mathbf{Z}_2 \times \mathbf{Z}_2$ by letting

$\phi([1]_8) = ([0]_2, [0]_2), \phi([3]_8) = ([1]_2, [0]_2), \phi([5]_8) = ([0]_2, [1]_2), \phi([7]_8) = ([1]_2, [1]_2)$.

- It is easy to see that ϕ is one-to-one and onto from the definition of ϕ.
- It follows that from the straightforward calculation that ϕ respects the two operations. For any $[a]_8, [b]_8 \in \mathbf{Z}_8^\times$, we have $\phi([a]_8[b]_8) = \phi([a]_8)\phi([b]_8)$.

Thus, ϕ is an isomorphism.

You can also write the function ϕ in a compact version. In particular,

$$\phi([3]_8^m[5]_8^n) = ([m]_2, [n]_2) \text{ for } m = 0, 1 \text{ and } n = 0, 1.$$

(3) Show that $\mathbf{Z}_5^\times$ is not isomorphic to $\mathbf{Z}_8^\times$ by showing that the first group has an element of order 4 but the second group does not.

In $\mathbf{Z}_5^\times$, the element $[3]_5$ has order 4. And $\mathbf{Z}_5^\times = \langle [3]_5 \rangle$ implies that $\mathbf{Z}_5^\times$ is cyclic.

In $\mathbf{Z}_8^\times$, every non-identity element has order 2. Moreover, $\mathbf{Z}_8^\times$ is not cyclic.

Thus there cannot be an isomorphism between them by Proposition 3 (a)/(b).

(4) Let $(G, \cdot)$ be a group. Define a new binary operation $*$ on G by the formula

$$a * b = b \cdot a, \text{ for all } a, b \in G.$$

Show that the group $(G, *)$[1] is isomorphic to the group $(G, \cdot)$.

Let $G_1 = (G, \cdot)$ and let $G_2 = (G, *)$. Define a function $\phi : G_1 \to G_2$ by

$$\phi(a) = a^{-1} \text{ for all } a \in G_1.$$

- well-defined: $\phi(a) = a^{-1} \in G_2$ since G is a group.
- respects the two operations: For any two elements $a, b \in G_1$, we have
$$\phi(a \cdot b) = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = a^{-1} * b^{-1} = \phi(a) * \phi(b).$$
- one-to-one: If $\phi(x) = e$ for $x \in G_1$, then $x^{-1} = e$ and so $x = e$.
- onto: For any $a \in G_2$, we have $\phi(a^{-1}) = (a^{-1})^{-1} = a$.

Thus, ϕ is an isomorphism.

(5) Find two abelian groups of order 8 that are not isomorphic.

$\mathbf{Z}_8 \ncong \mathbf{Z}_2 \times \mathbf{Z}_4$. The first one is cyclic, but the second one is not cyclic;

$\mathbf{Z}_8 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$. Same reason as above;

$\mathbf{Z}_2 \times \mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$. The first group has an element of order 4, eg. $([1], [1])$. However, in the second group, every non-identity element has order 2.

(6) Let G be any group, and let a be a fixed element of G. Define a function

$$\phi_a : G \to G \text{ by } \phi_a(x) = axa^{-1}, \text{ for all } x \in G.$$

Show that ϕ_a is an isomorphism.

- well-defined: Trivial.
- respects the two operations: For any $x, y \in G$, we have
$$\phi_a(xy) = axya^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y).$$
- one-to-one: If $\phi_a(x) = e$, then $axa^{-1} = e$, and so $x = a^{-1}ea = e$.
- onto: For any $y \in G$, we have $\phi_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = y$.

Thus, ϕ is an isomorphism.

(7) Let G be any group. Define $\phi : G \to G$ by $\phi(x) = x^{-1}$, for all $x \in G$.

(a) Prove that ϕ is one-to-one and onto.

To show ϕ is one-to-one and onto, we are trying to find its inverse function. Define $\phi^{-1} : G \to G$ by letting $\phi^{-1}(x) = x^{-1}$ for all $x \in G$. Then we have $\phi(\phi^{-1}(x)) = \phi(x^{-1}) = (x^{-1})^{-1} = x; \phi^{-1}(\phi(x)) = \phi^{-1}(x^{-1}) = (x^{-1})^{-1} = x$ for all $x \in G$. This shows that ϕ^{-1} is the inverse function of ϕ. $\square$

(b) Prove that ϕ is an isomorphism if and only if G is abelian.

By part (a), to show ϕ is an isomorphism, it suffices to show that ϕ preserves products. For any two elements $x, y \in G$, we have

$$\phi(xy) = (xy)^{-1} = y^{-1}x^{-1}.$$

- If G is abelian, $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$. ✓
- If ϕ preserves products, then we have $\phi(xy) = \phi(x)\phi(y)$. That is, $y^{-1}x^{-1} = x^{-1}y^{-1} \Rightarrow (xy)y^{-1}x^{-1}(yx) = (xy)x^{-1}y^{-1}(yx) \Rightarrow yx = xy$ This shows that G is abelian since x, y are arbitrary elements in G.

[1] In Homework 2 (3), we have shown that $(G, *)$ is a group.

In conclusion, ϕ is an isomorphism if and only if G is abelian.

(8) Define $*$ on $\mathbf{R}$ by $a * b = a + b - 1$, for all $a, b \in \mathbf{R}$. Show that the group $(\mathbf{R}, *)$[2] is isomorphic to the group $(\mathbf{R}, +)$.

Let $G_1 = (\mathbf{R}, *)$ and let $G_2 = (\mathbf{R}, +)$. Define a function $\phi : G_1 \to G_2$ by

$$\phi(a) = a - 1 \text{ for all } a \in G_1.$$

- well-defined: Trivial.
- ϕ respects the two operations: For any two elements $a, b \in G_1$, we have $\phi(a * b) = \phi(a + b - 1) = a + b - 1 - 1 = (a - 1) + (b - 1) = \phi(a) + \phi(b)$.
- one-to-one: If $\phi(a) = e_2 = 0$, then $a - 1 = 0$, and so $a = 1 = e_1$. ✓
- onto: For any $x \in G_2$, we have $\phi(x + 1) = x + 1 - 1 = x$. ✓

Thus, ϕ is an isomorphism.

(9) Let $G = \mathbf{R} - \{-1\}$. Define $*$ on G by $a * b = a + b + ab$. Show that the group $(G, *)$[3] is isomorphic to the multiplicative group $\mathbf{R}^\times$.

Define a function $\phi : G \to \mathbf{R}^\times$ by letting $\phi(a) = \dfrac{1}{a+1}$ for all $a \in G$.

- Since $a \in G$, i.e., $a \neq -1$, so $\phi(a) = \dfrac{1}{a+1} \in \mathbf{R}^\times$ is well-defined.
- ϕ preserves the two operations. For any two elements $a, b \in G$, we have $\phi(a * b) = \phi(a + b + ab) = \dfrac{1}{a + b + ab + 1} = \dfrac{1}{(a+1)(b+1)} = \phi(a) \cdot \phi(b)$.
- one-to-one: If $\phi(a) = e_2 = 1$, then $\dfrac{1}{a+1} = 1$ implies that $a = 0 = e_1$. ✓
- onto: For any element $x \in \mathbf{R}^\times$, we have $\phi\left(\dfrac{1}{a} - 1\right) = \dfrac{1}{\frac{1}{a} - 1 + 1} = a$.✓

Thus, ϕ is an isomorphism.

Define a function $\phi : G \to \mathbf{R}^\times$ by letting $\phi(a) = a + 1$ for all $a \in G$. ✓(easier)

(10) Let $G = \{x \in \mathbf{R} \mid x > 1\}$. Define $*$ on G by $a * b = ab - a - b + 2$, for all $a, b \in G$. Define $\phi : G \to \mathbf{R}^+$ by $\phi(x) = x - 1$, for all $x \in G$.

(a) Show that $(G, *)$ is a group.

(i) Closure: For any two elements $a, b \in G$, we have $a * b = ab - a - b + 2 = ab - a - b + 1 + 1 = (a - 1)(b - 1) + 1 > 1$ since $a > 1$ and $b > 1$. This shows that $a * b \in G$.

[2] In Homework 2 (7), we have shown that $(\mathbf{R}, *)$ is a group.

[3] In Homework 2 (8), we have shown that $(G, *)$ is a group.

(ii) Associativity: For any $a, b, c \in G$, we have

$$\begin{aligned}(a*b)*c = (ab-a-b+2)*c =& (ab-a-b+2)c-(ab-a-b+2)-c+2\\ =& abc-ac-bc+2c-ab+a+b-c\\ =& abc-ac-bc-ab+a+b+c\\ a*(b*c) = a*(bc-b-c+2) =& a(bc-b-c+2)-a-(bc-b-c+2)+2\\ =& abc-ab-ac+2a-a-ba+b+c\\ =& abc-ab-ac-ba+a+b+c\end{aligned}$$

commutativity: $a*b = ab-a-b+2 = ba-b-a+2 = b*a$.

(iii) Identity: The identity element is 2. In particular, we have

$$a*2 = 2a-a-2+2 = a.$$

The other equation holds because of the commutativity.

(iv) Inverses: For any element $a \in G$, its inverse is $\dfrac{a}{a-1}$. In particular,

$$a*\frac{a}{a-1} = a\frac{a}{a-1}-a-\frac{a}{a-1}+2 = \frac{a^2-a^2+a-a}{a-1}+2 = 2.$$

The other equation holds because of the commutativity.

(b) Show that ϕ is an isomorphism.

- well-defined: For any $a \in G$, we have $\phi(a) = a-1 > 0$ since $a > 1$.
- ϕ respects the two operations: For any $a, b \in G$, we have $\phi(a*b) = \phi(ab-a-b+2) = ab-a-b+1 = (a-1)(b-1) = \phi(a)\cdot\phi(b)$.
- one-to-one: If $\phi(a) = e_2 = 1$, then $a-1 = 1$ implies that $a = 2 = e_1$.
- onto: For any element $x \in R^+$, we have $\phi(x+1) = x+1-1 = x$.✓

Thus, ϕ is an isomorphism.