Homework 6 Solution

Chapter 6.

1. Find an isomorphism from the group of integers under addition to the group of even integers under addition.

   Let $2\mathbb{Z}$ be the set of all even integers. Define a map $\phi : \mathbb{Z} \to 2\mathbb{Z}$ as $\phi(n) = 2n$. We claim that ϕ is an isomorphism. $\phi(n) = \phi(m) \Rightarrow 2n = 2m \Rightarrow n = m$ so it is one-to-one. For any even integer $2k$, $\phi(k) = 2k$ thus it is onto. Also

   $$\phi(n+m) = 2(n+m) = 2n + 2m = \phi(n) + \phi(m),$$

   so it has the operation preserving property.

2. Find $\mathrm{Aut}(\mathbb{Z})$.

   Note that $\mathbb{Z} = \langle 1 \rangle$, a cyclic group generated by 1. There are two generators, 1 and -1. Because an automorphism ϕ of a cyclic group sends a generator to a generator, $\phi(1) = 1$ or $\phi(1) = -1$. Because $\phi(m \cdot 1) = m\phi(1)$, for the former case we have the identity map, and for the latter case, we have $\phi(x) = -x$. Therefore $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}, \phi\}$ where $\phi(x) = -x$.

4. Show that $U(8)$ is not isomorphic to $U(10)$.

   $U(10) = \{1, 3, 7, 9\}$ is a cyclic group generated by 3. So 3 is an element of order 4. But all non-identity elements of $U(8) = \{1, 3, 5, 7\}$ have order 2, so there is no element of order 4. Therefore they are not isomorphic to each other.

5. Show that $U(8)$ is isomorphic to $U(12)$.

   $U(8) = \{1, 3, 5, 7\}$ and $U(12) = \{1, 5, 7, 11\}$. Take a bijective map $\phi : U(8) \to U(12)$ defined by $\phi(1) = 1, \phi(3) = 11, \phi(5) = 5$, and $\phi(7) = 7$. We claim that it has the operation preserving property. Because $U(8)$ is an Abelian group, it suffices to check followings:

   $$\phi(3^2) = \phi(1) = 1 = 11^2 = \phi(3)^2,$$
   $$\phi(5^2) = \phi(1) = 1 = 5^2 = \phi(5)^2,$$
   $$\phi(7^2) = \phi(1) = 1 = 7^2 = \phi(7)^2,$$
   $$\phi(3 \cdot 5) = \phi(7) = 7 = 11 \cdot 5 = \phi(3) \cdot \phi(5),$$
   $$\phi(3 \cdot 7) = \phi(5) = 5 = 11 \cdot 7 = \phi(3) \cdot \phi(7),$$
   $$\phi(5 \cdot 7) = \phi(3) = 11 = 5 \cdot 7 = \phi(5) \cdot \phi(7).$$

   In general, you may show that *any* bijective map $\psi : U(8) \to U(12)$ with $\psi(1) = 1$ is an isomorphism.

10. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.

    If α is an isomorphism, for any two elements $x, y \in G$,

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

    So $xy = (x^{-1})^{-1}(y^{-1})^{-1} = (y^{-1}x^{-1})^{-1} = (x^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx$, and G is Abelian.

    Suppose that G is Abelian. $\alpha : G \to G$ is a bijective function, because α itself is the inverse function of α. Moreover, because

    $$\alpha(xy) = \alpha(yx) = (yx)^{-1} = x^{-1}y^{-1} = \alpha(x)\alpha(y),$$

    it has the operation preserving property. So α is an isomorphism.

14. Find $\mathrm{Aut}(\mathbb{Z}_6)$.

    $\mathbb{Z}_6$ is a cyclic group generated by 1. There are two generators, $1, 5$. So for an isomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_6$, $\phi(1) = 1$ or $\phi(1) = 5 = -1$. We have two such isomorphisms: the identity map and $\phi(x) = -x$. Therefore $\mathrm{Aut}(\mathbb{Z}_6) = \{\mathrm{id}, \phi\}$ where $\phi(x) = -x$.

15. If G is a group, prove that $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups.

    Both sets are subsets of S_G, the permutation group of the set G. Because $\mathrm{id} \in \mathrm{Aut}(G)$ and $\mathrm{id} = \phi_e \in \mathrm{Inn}(G)$, we may apply a subgroup test.

    Step 1. $\mathrm{Aut}(G)$. Suppose that $\alpha, \beta \in \mathrm{Aut}(G)$. Then $\alpha\beta : G \to G$ and α^{-1} are elements of S_G, so they are bijective. Therefore it is sufficient to show the operation preserving property. For any $x, y \in G$, $\alpha\beta(xy) = \alpha(\beta(xy)) = \alpha(\beta(x)\beta(y)) = \alpha(\beta(x))\alpha(\beta(y)) = \alpha\beta(x)\alpha\beta(y)$. Therefore $\alpha\beta \in \mathrm{Aut}(G)$.

    Suppose that $\alpha(a) = x, \alpha(b) = y$. Then $\alpha(ab) = \alpha(a)\alpha(b) = xy$. Thus $\alpha^{-1}(xy) = ab = \alpha^{-1}(x)\alpha^{-1}(y)$ and α^{-1} has the operation preserving property as well. Therefore $\alpha^{-1} \in \mathrm{Aut}(G)$. By the subgroup test 1, $\mathrm{Aut}(G) \le S_G$.

    Step 2. $\mathrm{Inn}(G)$. Let $\phi_a, \phi_b \in \mathrm{Inn}(G)$. Then $\phi_a\phi_b(x) = \phi_a(\phi_b(x)) = \phi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x)$. So $\phi_a\phi_b = \phi_{ab} \in \mathrm{Inn}(G)$.

    Note that $\phi_{a^{-1}}\phi_a(x) = \phi_{a^{-1}}(\phi_a(x)) = \phi_{a^{-1}}(axa^{-1}) = a^{-1}axa^{-1}(a^{-1})^{-1} = a^{-1}axa^{-1}a = x$ and $\phi_a\phi_{a^{-1}}x = \phi_a(\phi_{a^{-1}}(x)) = \phi_a(a^{-1}xa) = aa^{-1}xaa^{-1} = x$. So $\phi_a^{-1} = \phi_{a^{-1}} \in \mathrm{Inn}(G)$. By the subgroup test 1, $\mathrm{Inn}(G) \le S_G$.

24. Suppose that $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{20}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$?

    Because an automorphism ϕ maps a generator to a generator, $\phi(1)$ is one of $1, 3, 7, 9, 11, 13, 17, 19$. Because $\phi(5) = \phi(5 \cdot 1) = 5\phi(1) = 5$ in $\mathbb{Z}_{20}$, the only possible $\phi(1)$ are $1, 9, 13, 17$. Therefore $\phi(x) = x, 9x, 13x$, or $17x$.

28. The group $\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \,\Big|\, a \in \mathbb{Z} \right\}$ is isomorphic to what familiar group? What if $\mathbb{Z}$ is replaced by $\mathbb{R}$?

    Let $G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \,\Big|\, a \in \mathbb{Z} \right\}$. We claim that G is isomorphic to an additive group $\mathbb{Z}$. Define $\phi : G \to \mathbb{Z}$ as $\phi(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}) = a$. Obviously it is a bijection map.

    $$\phi(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}) = \phi(\begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}) = a + b = \phi(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}) + \phi(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}).$$

    Therefore ϕ has the operation preserving property, so it is an isomorphism.

    If we replace $\mathbb{Z}$ by $\mathbb{R}$, then the group is isomorphic to the additive group $\mathbb{R}$. We can use the same isomorphism.

31. Suppose that $\phi : G \to \overline{G}$ is an isomorphism. Show that $\phi^{-1} : \overline{G} \to G$ is an isomorphism.

    Because ϕ^{-1} is also a bijective map, it suffices to show the operation preserving property. For $x, y \in \overline{G}$, there are a, b such that $\phi(a) = x, \phi(b) = y$. Then $\phi(ab) = \phi(a)\phi(b) = xy$. So
    $$\phi^{-1}(xy) = ab = \phi^{-1}(x)\phi^{-1}(y)$$
    and ϕ^{-1} is an isomorphism.

32. Suppose that $\phi : G \to \overline{G}$ is an isomorphism. Show that if K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

    Because $\phi(e) \in \phi(K)$, $\phi(K) \neq \emptyset$. Let $x, y \in \phi(K)$. Then $x = \phi(a)$, $y = \phi(b)$ for some $a, b \in K$. Then $xy = \phi(a)\phi(b) = \phi(ab) \in \phi(K)$ because $ab \in K$. Also because $a^{-1} \in K$, $x^{-1} = (\phi(a))^{-1} = \phi(a^{-1}) \in \phi(K)$. By subgroup test 1, $\phi(K) \leq \overline{G}$.

34. Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.

    In $U(20)$, $3^2 = 9, 3^3 = 27 = 7, 3^4 = 81 = 1$. So $|3| = 4$. On the other hand, in $U(24)$, all non-identity elements have order two. Therefore they are not isomorphic to each other.

39. Let $\mathbb{C}$ be the complex numbers and
    $$M = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \,\Big|\, a, b \in \mathbb{R} \right\}.$$
    Prove that $\mathbb{C}$ and M are isomorphic under addition and that $\mathbb{C}^*$ and M^*, the nonzero elements of M, are isomorphic under multiplication.

Define a map $\phi : \mathbb{C} \to M$ as $\phi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. It is bijective.

$$\phi(\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix}) = \phi(\begin{bmatrix} a+c & -(b+d) \\ (b+d) & (a+c) \end{bmatrix})$$

$$= (a+c) + (b+d)i = (a+bi) + (c+di) = \phi(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}) + \phi(\begin{bmatrix} c & -d \\ d & c \end{bmatrix})$$

So ϕ is an isomorphism.

On the other hand, if we restrict ϕ to $\mathbb{C}^*$, then ϕ is a bijective map between $\mathbb{C}^*$ and M^*, and

$$\phi(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} c & -d \\ d & c \end{bmatrix}) = \phi(\begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix})$$

$$= ac - bd + (ad+bc)i = (a+bi)(c+di) = \phi(\begin{bmatrix} a & -b \\ b & a \end{bmatrix})\phi(\begin{bmatrix} c & -d \\ c & d \end{bmatrix}).$$

Therefore ϕ restricted to $\mathbb{C}^*$ is an isomorphism between $\mathbb{C}^*$ and M^*.

48. Let ϕ be an isomorphism from a group G to a group $\overline{G}$ and let a belong to G. Prove that $\phi(C(a)) = C(\phi(a))$.

Let $x \in \phi(C(a))$. Then there is $y \in C(a)$ such that $\phi(y) = x$. $x\phi(a) = \phi(y)\phi(a) = \phi(ya) = \phi(ay) = \phi(a)\phi(y) = \phi(a)x$. So $x \in C(\phi(a))$. Therefore $\phi(C(a)) \subset C(\phi(a))$.

Conversely, suppose that $x \in C(\phi(a))$. There is $y \in G$ such that $\phi(y) = x$. $\phi(ya) = \phi(y)\phi(a) = x\phi(a) = \phi(a)x = \phi(a)\phi(y) = \phi(ay)$. Because ϕ is one-to-one, $ya = ay$ and $y \in C(a)$. Therefore $x = \phi(a) \in \phi(C(a))$. So $C(\phi(a)) \subset \phi(C(a))$ and $C(\phi(a)) = \phi(C(a))$.