

H/wk 7, Solutions to selected problems

Problem 6.

Show that there are exactly two homomorphisms from C_6 to C_4 .

Solution.

Let $C_6 = \langle a \rangle = \{1, a, a^2, a^3, a^4, a^5\}$ and $C_4 = \langle b \rangle = \{1, b, b^2, b^3\}$ where $|a| = 6$ and $|b| = 4$.

Suppose $\alpha : C_6 \rightarrow C_4$ is a homomorphism. By Theorem 2 in Ch 2.5, since $C_6 = \langle a \rangle$, any homomorphism $C_6 \rightarrow C_4$ is uniquely determined by its value on the generator a of C_6 . Indeed, if $x = \alpha(a) \in C_4$ is known then $\alpha(a^i) = \alpha(a)^i = x^i$ for $i = 0, 1, 2, 3, 4, 5$.

There are at most 4 possibilities for $\alpha(a) \in C_4$ and we have to decide which ones of them correspond to homomorphisms from C_6 to C_4 and which ones do not.

Since $a^6 = 1$ in C_6 , for any homomorphism $\alpha : C_6 \rightarrow C_4$ we have $\alpha(a)^6 = 1$ in C_4 .

In C_4 we have $1^6 = 1$, $b^6 = b^2 \neq 1$, $(b^2)^6 = b^{12} = 1$, $(b^3)^6 = b^{18} = b^2 \neq 1$. Since $b^6 \neq 1$ and $(b^3)^6 \neq 1$ in C_4 , it follows that $\alpha(a) \neq b$ and $\alpha(a) \neq b^3$.

The other two possibilities, namely $\alpha(a) = 1$ and $\alpha(a) = b^2$ do give rise to homomorphisms $C_6 \rightarrow C_4$.

Namely, $\alpha_1 : C_6 \rightarrow C_4$, $\alpha_1(g) = 1$ for every $g \in C_6$ is obviously a homomorphism.

Also, $\alpha_2 : C_6 \rightarrow C_4$ given by $\alpha_2(a) = \alpha_2(a^3) = \alpha_2(a^5) = b^2$, $\alpha_2(1) = \alpha_2(a^2) = \alpha_2(a^4) = 1$, can be seen to be a homomorphism by a direct check.

Thus there are exactly two homomorphisms from C_6 to C_4 , namely α_1 and α_2 .

Problem 12. In each case determine whether $\alpha : G \rightarrow G_1$ is an isomorphism.

(a) $G = G_1 = \mathbb{R}$, $\alpha(x) = 2x$ for $x \in \mathbb{R}$.

Answer: Yes, this is an isomorphism. The map α is obviously bijective and it is a homomorphism since $\alpha(x_1 + x_2) = 2(x_1 + x_2) = 2x_1 + 2x_2 = \alpha(x_1) + \alpha(x_2)$.

(b) $G = G_1 = \mathbb{Z}$ and $\alpha(b) = 2n$.

Answer: No, this is not an isomorphism. The map α is not onto. Indeed, $\alpha(\mathbb{Z}) = 2\mathbb{Z}$ is the set of all even integers, and, for example, $1 \notin \alpha(\mathbb{Z})$.

(c) $G = G_1 = \mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ and $\alpha(g) = g^2$ for $g \in G$.

Answer: No, this is not an isomorphism since α is not injective. Indeed, $\alpha(\bar{1}) = \bar{1}^2 = \bar{1}$ and $\alpha(\bar{4}) = \bar{4}^2 = \bar{3}\bar{6} = \bar{1}$.

(d) $G = G_1 = \mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ and $\alpha(g) = g^3$ for $g \in G$.

Answer: Yes, this is an isomorphism. Indeed, G is abelian and hence $\alpha(gh) = (gh)^3 = g^3h^3 = \alpha(g)\alpha(h)$ for any $g, h \in G$. Thus α is a homomorphism. By a direct computation we can check that α is a bijection:

$$\alpha(\bar{1}) = \bar{1}, \alpha(\bar{2}) = \bar{8} = \bar{3}, \alpha(\bar{3}) = \bar{27} = \bar{2}, \alpha(\bar{4}) = \bar{64} = \bar{4}.$$

Thus α is a bijective homomorphism, so that it is an isomorphism.

(e) $G = G_1 = \mathbb{Z}_7$, $\alpha(g) = 2g$.

Answer: Yes, this is an isomorphism. It is easy to see that this is a homomorphism (again because G is abelian). One can verify that α is bijective either by a direct check, as in part (d) or indirectly, as follows. Since $\alpha(\bar{1}) = \bar{2}$, it follows that the cyclic subgroup generated by $\bar{2}$ is a subset of the image of α . Since $\gcd(2, 7) = 1$,

we know that $\langle \bar{2} \rangle = \mathbb{Z}_7$. Therefore α is onto. Since α is a function from a finite set to itself, the fact that it is onto implies that α is a bijection.

Thus α is a bijective homomorphism, so that it is an isomorphism.

(f) $G = G_1 = \mathbb{Z}_8$ and $\alpha(g) = 2g$.

Answer: No, this is not a homomorphism since α is not injective. In particular $\alpha(\bar{0}) = \alpha(\bar{4}) = \bar{0}$.

(g) $G = G_1 = \mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ and $\alpha(g) = g^2$.

Answer: Yes, this is an isomorphism. The map $\alpha(g) = g^2$ is a homomorphism since G is abelian. It is also clear that $\alpha : (0, \infty) \rightarrow (0, \infty)$, $\alpha(x) = x^2$, is both injective and onto.

(h) $G = \mathbb{R}$, $G_1 = \mathbb{R}^+$ and $\alpha(g) = |g|$.

Answer: No, this is not an isomorphism. In fact, α is not even a function from \mathbb{R} to $\mathbb{R}^+ = (0, \infty)$. Indeed, $0 \in \mathbb{R}$ but $|0| = 0 \notin \mathbb{R}^+$.

(i) $G = 2\mathbb{Z}$, $G_1 = 3\mathbb{Z}$, $\alpha(2k) = 3k$.

Answer: Yes, this is an isomorphism. It is easy to see that α is a homomorphism and that it is injective and onto.

(j) $G = G_1 = \mathbb{R}$, $\alpha(g) = ag$, where $a \neq 0$ is a fixed number.

Answer: Yes, this is an isomorphism.

Indeed, $\alpha(x_1 + x_2) = a(x_1 + x_2) = ax_1 + ax_2 = \alpha(x_1) + \alpha(x_2)$, so that α is a homomorphism. It is obvious that α is a bijection.

Problem 22.

Show that the groups \mathbb{R} and \mathbb{R}^* are not isomorphic.

Solution.

Recall that \mathbb{R} is a group with respect to addition of real numbers and that $\mathbb{R}^* = \mathbb{R} - \{0\}$ is a group with respect to multiplication of real numbers. The identity element in \mathbb{R} is $0 \in \mathbb{R}$ and the identity element in \mathbb{R}^* is $1 \in \mathbb{R}$.

First, notice that every nontrivial (that is, nonzero) element in \mathbb{R} has infinite order. Indeed, if $a \in \mathbb{R}$, $a \neq 0$ then for $n \geq 1$ the n -th additive power of a is na and $na \neq 0$ for every integer $n \geq 1$; hence $|a| = \infty$ in \mathbb{R} for any $a \neq 0$. Of course, the order of 0 in \mathbb{R} is equal to 1 . In particular, this shows that the group \mathbb{R} has no elements of order 2 .

On the other hand, in \mathbb{R}^* we do have an element of order 2 , namely -1 . Indeed, $-1 = (-1)^1 \neq 1$ but $(-1)^2 = 1$, so that indeed -1 has order 2 in \mathbb{R}^* .

Since \mathbb{R}^* has an element of order 2 but \mathbb{R} has no elements of order 2 , these groups are not isomorphic.

Problem 25.

Are the additive groups \mathbb{Z} and \mathbb{Q} isomorphic?

Solution.

No, they are not isomorphic, because \mathbb{Z} is cyclic while \mathbb{Q} is not cyclic.

Indeed, $\mathbb{Z} = \langle 1 \rangle$ (as an additive group). The group $(\mathbb{Q}, +)$ is not cyclic. Indeed, $\langle 0 \rangle = \{0\} \neq \mathbb{Q}$. Also, if $a \in \mathbb{Q}$, $a \neq 0$ then $\langle a \rangle = \{na | n \in \mathbb{Z}\} \neq \mathbb{Q}$ since $\frac{a}{2} \notin \langle a \rangle$. Thus for every element $r \in \mathbb{Q}$ we have $\langle r \rangle \neq \mathbb{Q}$, and hence \mathbb{Q} is not cyclic, as claimed.

Problem 26.

Show that $\mathbb{Z}_{14}^* \cong \mathbb{Z}_{18}^*$.

Solution.

We have

$$\mathbb{Z}_{14}^* = \{[k]_{14} \mid \gcd(k, 14) = 1\} = \{[1]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\}$$

and

$$\mathbb{Z}_{18}^* = \{[k]_{18} \mid \gcd(k, 18) = 1\} = \{[1]_{18}, [5]_{18}, [7]_{18}, [11]_{18}, [13]_{18}, [17]_{18}\}$$

where both groups are considered with respect to multiplication.

We claim that both \mathbb{Z}_{14}^* and \mathbb{Z}_{18}^* are cyclic groups of order 6. Note that each of \mathbb{Z}_{14}^* and \mathbb{Z}_{18}^* has order 6.

Note also that in order to show that a group G of order 6 is a cyclic group of order 6, it is enough to find an element g of order 6 in such a group. Then we would have $|\langle g \rangle| = |g| = 6 = |G|$ and hence $G = \langle g \rangle$.

For \mathbb{Z}_{14}^* we have

$$\begin{aligned} [3]_{14}^1 &= [3]_{14}, & [3]_{14}^2 &= [9]_{14}, & [3]_{14}^3 &= [27]_{14} = [-1]_{14} = [13]_{14} \\ [3]_{14}^4 &= [-3]_{14} = [11]_{14}, & [3]_{14}^5 &= [-9]_{14} = [5]_{14}, & [3]_{14}^6 &= [15]_{14} = [1]_{14}. \end{aligned}$$

Thus we see that $|[3]_{14}| = 6$ and $\mathbb{Z}_{14}^* = \langle [3]_{14} \rangle$ is cyclic of order 6.

Similarly, for \mathbb{Z}_{18}^* we have

$$\begin{aligned} [5]_{18}^1 &= [5]_{18}, & [5]_{18}^2 &= [7]_{18}, & [5]_{18}^3 &= [35]_{18} = [-1]_{18} = [17]_{18} \\ [5]_{18}^4 &= [-5]_{18} = [13]_{18}, & [5]_{18}^5 &= [-25]_{18} = [11]_{18}, & [5]_{18}^6 &= [55]_{18} = [1]_{18}. \end{aligned}$$

Hence $|[5]_{18}| = 6$ and $\mathbb{Z}_{18}^* = \langle [5]_{18} \rangle$ is cyclic of order 6.

Thus \mathbb{Z}_{14}^* and \mathbb{Z}_{18}^* are both cyclic of order 6. Therefore by Example 13 in Ch. 2.5 they are both isomorphic to $(\mathbb{Z}_6, +)$ and therefore to each other.