

Worksheet

1. What is the definition of a homomorphism, using additive notation for both operations?

2. Let $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ be a homomorphism. Suppose $f([1]_m) = [b]_n$.
 - a. For any element $[a]_m \in \mathbb{Z}_m$, what is $f([a]_m)$?
 Since $[a]_m = a[1]_m$, we have $f([a]_m) = f(a[1]_m) = af([1]_m) = a[b]_n$.
 - b. Let $f(\mathbb{Z}_m)$ denote the image of \mathbb{Z}_m under f . Prove $f(\mathbb{Z}_m) \subseteq \langle [b]_n \rangle$.
 Since $\langle [b]_n \rangle = \{k[b]_n : k \in \mathbb{Z}\}$ and $f([a]_m) = a[b]_n$ for all $[a]_m \in \mathbb{Z}_m$, we have $f(\mathbb{Z}_m) \subseteq \langle [b]_n \rangle$.

3. Let $f : 2\mathbb{Z} \rightarrow \mathbb{Z}_n$ be a homomorphism. Suppose $f(2) = [b]_n$.
 - a. For any $a \in 2\mathbb{Z}$, what is $f(a)$?
 Since $a \in 2\mathbb{Z}$ implies that there exists an $x \in \mathbb{Z}$ such that $a = 2x$, we have $f(a) = f(2x) = xf(2) = x[b]_n$.
 - b. Prove $f(2\mathbb{Z}) \subseteq \langle [b]_n \rangle$.
 Since $\langle [b]_n \rangle = \{k[b]_n : k \in \mathbb{Z}\}$, and $f(2x) = x[b]_n$ for all $2x \in 2\mathbb{Z}$, we have $f(2\mathbb{Z}) \subseteq \langle [b]_n \rangle$.

4. Let G be a cyclic group with $G = \langle g \rangle$, and H be any group. Let $f : G \rightarrow H$, with $f(g) = b$, where $b \in H$.
 - a. For any $x \in G$, what is $f(x)$?
 $x \in G = \langle g \rangle$ implies that there exists an $n \in \mathbb{Z}$ such that $x = g^n$. Then $f(x) = f(g^n) = f(g)^n = b^n$.
 - b. Prove $f(G) \subseteq \langle b \rangle$ and $\langle b \rangle \subseteq f(G)$ (i.e. $\langle b \rangle = f(G)$).
 Since $b = f(g) \in f(G)$, we have $\langle b \rangle \subseteq f(G)$. From the above, for each $x \in G$, $f(x) = b^n$ for some $n \in \mathbb{Z}$. Thus $f(G) \subseteq \langle b \rangle$.
 - c. Prove that $f(G)$ is a subgroup of H .
 Note $f(G) = \{f(g) : g \in G\}$. Let $a, b \in f(G)$. Then there are $x, y \in G$ such that $a = f(x)$ and $b = f(y)$. Then $ab^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$ so $ab^{-1} \in f(G)$, since $xy^{-1} \in G$. Thus $f(G)$ is a subgroup.

5. Does $(\mathbb{Z}_{15}, +)$ contain any elements of order 7? order 6? order 5? If you answer yes, name them.
 Since the order of an element must divide the order of the group, there are no elements of orders 6 and 7 (neither 6 nor 7 divide 15). There are elements of order 5. $[a]_{15}$ has order 5 iff 5 is the smallest positive integer such that $15|5a$. For this to be true, $[a]_{15}$ must be

- $[3]_{15}, [6]_{15}, [9]_{15}$ or $[12]_{15}$ (note that 0 has order 1 so though $15|5 \cdot 0$, 5 is not the smallest positive integer with that property).
6. Let G and H be groups. Prove that if $g \in G$ has finite order and $f : G \rightarrow H$ is a homomorphism, then $o(f(g))|o(g)$.
If $n = o(g)$, then $g^n = e$ so $e = f(g^n) = f(g)^n$, which implies that $o(f(g))|n$. Thus $o(f(g))|o(g)$.
 7. a. What is the order of $[1]_6$ in \mathbb{Z}_6 ?
 $[1]_6$ has order 6.
 - b. What elements of \mathbb{Z}_{18} have order dividing 6?
Elements of order 1: $[0]_{18}$; elements of order 2: $[9]_{18}$; elements of order 3: $[6]_{18}, [12]_{18}$; elements of order 6: $[3]_{18}, [15]_{18}$
 - c. List all possible homomorphisms from \mathbb{Z}_6 into \mathbb{Z}_{18} (you should get one for each element you listed in 7b).
 $f_0([x]_6) = [0x]_{18}, f_3([x]_6) = [3x]_{18}, f_6([x]_6) = [6x]_{18}, f_9([x]_6) = [9x]_{18}, f_{12}([x]_6) = [12x]_{18}, f_{15}([x]_6) = [15x]_{18}$.
 - d. How many elements are there in the image of \mathbb{Z}_6 under each of the homomorphisms you listed in 7c? (Remember that $o(g) = |\langle g \rangle|$.)
 $f_0(\mathbb{Z}_6)$ has 1 element. $f_3(\mathbb{Z}_6)$ has 6 elements. $f_6(\mathbb{Z}_6)$ has 3 elements. $f_9(\mathbb{Z}_6)$ has 2 elements. $f_{12}(\mathbb{Z}_6)$ has 3 elements. $f_{15}(\mathbb{Z}_6)$ has 6 elements.
 8. If G and H are finite sets and $f : G \rightarrow H$, prove f is onto if and only if $|f(G)| = |H|$ (where if S is a set, then $|S|$ denotes the number of elements in S), and f is one-to-one if and only if $|G| = |f(G)|$.
 9. For each of the following, if the answer is yes, give an example of a function with the desired properties; if the answer is no, say why not.
 - a. Let $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_4$ be a function. Could f be one-to-one? (Note that it could be onto.)
 f cannot be one-to-one since there are more elements in \mathbb{Z}_8 than in \mathbb{Z}_4 .
 - b. Let $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_8$ be a function. Could f be onto? (Note that it could be one-to-one.)
 f cannot be onto since there are less elements in \mathbb{Z}_4 than in \mathbb{Z}_8 .
 - c. Let $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_{10}$ be a homomorphism. Could f be one-to-one? Since f is a homomorphism, $f(\mathbb{Z}_8) = \langle f([1]_8) \rangle$ is a subgroup of \mathbb{Z}_{10} , so by Lagrange's Theorem, $|f(\mathbb{Z}_8)|$ must divide $|\mathbb{Z}_{10}| = 10$. But $|f(\mathbb{Z}_8)| = o(f([1]_8))$ must divide $o([1]_8) = 8$ as well. So $|f(\mathbb{Z}_8)| = 1$ or 2 , and cannot equal 8 , as required for f to be one-to-one.
 - d. Let $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_{24}$ be a homomorphism. Could f be one-to-one?

- f could be one to one. For example, the map $f([x]_8) = [3x]_{24}$ is a one-to-one homomorphism.
- e. Let $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_5$ be a homomorphism. Could f be onto?
 f cannot be onto since $|f(\mathbb{Z}_8)|$ must divide both 5 and 8, and hence must be 1.
- f. Let $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_4$ be a homomorphism. Could f be onto?
 f could be onto. For example $f([x]_8) = [x]_4$ is an onto homomorphism.
10. Let $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ be a homomorphism, with $f([1]_m) = [b]_n$. What condition on $[b]_n$ will guarantee that f is one-to-one? onto?
 f is onto if and only if $[b]_n$ generates \mathbb{Z}_n , i.e. if and only if $(b, n) = 1$.
 f is one-to-one if and only if $[b]_n$ has order m .
11. What is the order of $[1]_n$ in \mathbb{Z}_n ? Is \mathbb{Z}_n cyclic?
 $[1]_n$ has order n , so $\langle [1]_n \rangle$ has n elements and must be all of \mathbb{Z}_n . Thus \mathbb{Z}_n is cyclic.
12. a. What is the order of $([1]_2, [1]_5)$ in $\mathbb{Z}_2 \times \mathbb{Z}_5$? Is $\mathbb{Z}_2 \times \mathbb{Z}_5$ cyclic?
 $([1]_2, [1]_5)$ has order $10 = lcm(o([1]_2), o([1]_5)) = lcm(2, 5)$. Since $\mathbb{Z}_2 \times \mathbb{Z}_5$ has 10 elements, $\langle ([1]_2, [1]_5) \rangle$ must be the whole group, and $\mathbb{Z}_2 \times \mathbb{Z}_5$ is cyclic.
- b. Is $\mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10}$? If so, find the isometry.
Let $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_5$ be given by $f([x]_{10}) = ([x]_2, [x]_5)$. Check that this is an isomorphism.
13. a. Does $\mathbb{Z}_2 \times \mathbb{Z}_6$ contain an element of order 12? Is $\mathbb{Z}_2 \times \mathbb{Z}_6$ cyclic?
The order of an element of $\mathbb{Z}_2 \times \mathbb{Z}_6$ is at most $lcm(2, 6) = 6$, so there are no elements of order 12. Thus $\mathbb{Z}_2 \times \mathbb{Z}_6$ is not cyclic.
- b. Is $\mathbb{Z}_2 \times \mathbb{Z}_6$ isomorphic to \mathbb{Z}_{12} ?
No, since \mathbb{Z}_{12} is cyclic and $\mathbb{Z}_2 \times \mathbb{Z}_6$ is not cyclic.
14. What is $o([1]_m, [1]_n)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$?
 $o([1]_m, [1]_n) = lcm(m, n)$.
15. Using 14, prove that if $(m, n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.
If $(m, n) = 1$ then $mn = lcm(m, n)$, and $o([1]_m, [1]_n) = mn$. Since $\mathbb{Z}_m \times \mathbb{Z}_n$ has mn elements, it is cyclic.
16. Prove that if $(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
Check that the function $f : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, given by $f([x]_{mn}) = ([x]_m, [x]_n)$ is an isometry.