Problem Set 3 solutions

Problem 1. Show that for every integer $n \geqslant 2$, there is no nontrivial group homomorphism $\mathbb{Z}/n \longrightarrow \mathbb{Z}$.

Proof. Suppose that $f : \mathbb{Z}/n \longrightarrow \mathbb{Z}$ is a group homomorphism. Denote the class of $i \in \mathbb{Z}$ by $[i]$. Then

$$\begin{aligned} 0 &= f([0]) && \text{since } f \text{ is a group homomorphism} \\ &= f([n]) && \text{since } [n] = [0] \\ &= f(n[1]) && \text{since } n[1] = [n] \\ &= nf([1]) && \text{since } f \text{ is a homomorphism} \end{aligned}$$

Thus $nf([1]) = 0$, which implies that $f([1]) = 0$. But $[1]$ generates $\mathbb{Z}/n$, and we conclude that f must be the trivial map, since for any $[a] \in \mathbb{Z}/n$, we have

$$f([a]) = af([1]) = 0. \quad \square$$

For groups G and H, the group $G \times H$, known as the **product of G and H**, refers to the set

$$G \times H := \{(g, h) \mid g \in G, h \in H\}$$

equipped with the multiplication rule

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 \cdot_G g_2, h_1 \cdot_H h_2).$$

You may take it as a known fact that the product of two groups is also a group.

Problem 2. Let G and H be groups, and consider elements $g \in G$ and $h \in H$.

2.1. Show that if $g^n = e$ for some integer $n \geqslant 1$, then $|g|$ divides n.

Proof. First note that the fact that $g^n = e$ implies that g has finite order, so let $|g| = d$. By the Division Algorithm, we can find integers q, r with $0 \leqslant r < d$ such that $n = qd + r$. Moreover,

$$e = g^n = g^{qd+r} = (g^d)^q g^r = e^q g^r = g^r.$$

Thus $g^r = e$, but by minimality of d, we conclude that $r = 0$. Thus $d = |g|$ divides n. $\square$

2.2. Show that $|g|$ and $|h|$ are both finite, then $|(g, h)| = \operatorname{lcm}(|g|, |h|)$.

Proof. Let $|g| = a$ and $|h| = b$, and let $\ell = \operatorname{lcm}(|g|, |h|)$. Since ℓ is a multiple of both a and b, we can write $\ell = ac$ and $\ell = bd$. Then

$$(g, h)^\ell = (g^{ac}, h^{bd}) = ((g^a)^c, (h^b)^d) = (e_G, e_H) = e_{G \times H}.$$

Thus $|(g, h)| \leqslant \ell$. Moreover, let $n := |(g, h)|$. Then $(g^n, h^n) = (g, h)^n = e$, so in particular $g^n = e$ and $h^b = e$. By 2.1., we conclude that $|g|$ and $|h|$ both divide n, and thus n must be a multiple of $\operatorname{lcm}(|g|, |h|)$. In particular, $n \geqslant \operatorname{lcm}(|g|, |h|)$. We showed that $|(g, h)| \leqslant \operatorname{lcm}(|g|, |h|)$ and $\operatorname{lcm}(|g|, |h|) \geqslant |(g, h)|$, so we must have $\operatorname{lcm}(|g|, |h|) = |(g, h)|$. $\square$

2.3. Show that if at least one of g or h has infinite order, then (g, h) also has infinite order.

Proof. By contrapositive. Suppose that $(g, h) \in G \times H$ has finite order n. Then

$$(g^n, h^n) = (g, h)^n = (e_G, e_H),$$

so in particular $g^n = e$ and $h^n = e$. We conclude that g and h both have finite order. $\square$

Problem 3. For each of the following pairs of groups, show that the two groups are not isomorphic.

3.1. $(\mathbb{C}, +)$ and $(\mathbb{Q}, +)$.

Proof. These groups are not isomorphic since $\mathbb{C}$ and $\mathbb{Q}$ have different cardinalities, and any isomorphism is in particular a bijection of sets. $\square$

3.2. $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{R}, +)$.

Proof. They are not isomorphic since $(\mathbb{R} \setminus \{0\}, \cdot)$ has ono element of order 2, namely -1, while every element of $(\mathbb{R}, +)$ has infinite order. $\square$

3.3. $\mathbb{Z}/2 \times \mathbb{Z}/2$ and $\mathbb{Z}/4$.

Proof. They are not isomorphic since $\mathbb{Z}/4$ has an element of order 4 and $\mathbb{Z}/2 \times \mathbb{Z}/2$ has no such elements. To be more precise:

- In $\mathbb{Z}/4$, $[1]$ has order 4.
- Every element of $\mathbb{Z}/2$ has order 1 or 2; in fact, there are only 2 elements in $\mathbb{Z}/2$, the identity and $[1]$, which has order 2.

By 2.2., the order of any element in $\mathbb{Z}/2 \times \mathbb{Z}/2$ must be 1 or 2, since it is the lcm of two integers in the set $\{1, 2\}$. $\square$

3.4. $Q_8 \times \mathbb{Z}/3$ and S_4.

Proof. Since $|-1| = 2$ and $|[1]_3| = 3$, the element $(-1, [1])$ in $Q_8 \times \mathbb{Z}/3$ has order $\operatorname{lcm}(2, 3) = 6$. We claim that S_4 has no elements of order 6.

To prove that, consider any element $\sigma \in S_4$. We can write σ as a product of disjoint cycles $\sigma = \sigma_1 \cdots \sigma_k$. By Problem Set 1, the order of σ is $\operatorname{lcm}(\sigma_1, \ldots, \sigma_k)$. Any cycle in S_4 that is not the identity has order 2, 3, or 4, so the only way to get an element of order 6 would be to take the product of a 3-cycle with a 2-cycle. But if $\sigma_1 = (i_1 i_2 i_3)$ and $\sigma_2 = (j_1, j_2)$ with $i_k, j_k \in [4]$, we must have

$$\{i_1, i_2, i_3\} \cap \{j_1, j_2\} = \emptyset.$$

Thus this is impossible, and S_4 has no elements of order 6. $\square$

Problem 4. Let

$$G = \prod_{i \in \mathbb{N}} \mathbb{Z} = \{(n_i)_{i \geqslant 0} \mid n_i \in \mathbb{Z}\}$$

be the group whose elements are sequences of integers, equipped with the operation given by componentwise addition. Let $H = (\mathbb{Z}, +)$. Show that $G \times H \cong G$.

Note: this gives us an example of groups G, H such that there is an isomorphism $G \times H \cong G$ but H is nontrivial. Since $G \times H \cong G$ can be rewritten as $G \times H \cong G \times \{e\}$, this shows that in general one cannot cancel groups in isomorphisms between direct products.

Proof. Consider the map that prepends an integer to a sequence of integers, more formally

$$f \colon G \times H \longrightarrow G$$

$$f((z_i)_{i \in \mathbb{N}}, h) = (h, z_0, z_1, z_2, \ldots).$$

We clam that this a group homomorphism. Indeed:

$$\begin{aligned} f((z_i)_{i\in\mathbb{N}}, a) + f((w_i)_{i\in\mathbb{N}}, b) &= (a, z_0, z_1, \ldots) + (b, w_0, w_1, \ldots) && \text{by definition of } f \\ &= (a + b, z_0 + w_0, z_1 + w_1, \ldots) && \text{by definition of } G \times H \\ &= f((z_i + w_i)_i, a + b) && \text{by definition of } f \\ &= f(((z_i)_i, a) + ((w_i), b)) && \text{by definition of } G \times H \end{aligned}$$

Moreover, this map surjective, since given any $(z_i)_{i \in \mathbb{N}}$,

$$f((z_1, z_2, z_3, \ldots), z_0) = (z_i)_i.$$

The map f is also injective: if we denote the constant sequence equal to 0 by $\mathbf{0}$, then

$$f((z_i)_i, h) = \mathbf{0} \iff (h, z_0, z_1, \ldots) = \mathbf{0} \iff h = 0 \text{ and } z_i = 0 \text{ for all } i \geqslant 0 \iff ((z_i)_i, h) = 0_{G \times H}.$$

We have established the desired isomorphism. □