Practice Problem Solutions

1. Let $f : A \to C$ and $g : B \to D$ be functions and let $h : A \times B \to C \times D$ be defined by $h(a, b) = (f(a), g(b))$.

   (a) Prove that if f and g are injective then h is injective.
   Suppose f and g are injective and that $h(a, b) = h(c, d)$. Then $(f(a), g(b)) = (f(c), g(d))$ so $f(a) = f(c)$ and $g(b) = g(d)$. Since f and g are injective, this implies $a = c$ and $b = d$. Therefore $(a, b) = (c, d)$, so h is injective.

   (b) Prove that if f and g are surjective then h is surjective.
   Suppose f and g are surjective and that $(c, d) \in C \times D$. Since f and g are sujective, there exists $a \in A$ such that $f(a) = c$ and $b \in B$ such that $g(b) = d$. Therefore $h(a, b) = (c, d)$, so h is surjective.

2. Determine if each function is injective and if it is surjective.

   (a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$.
   Injective and surjective.

   (b) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = |x|$.
   Neither.

   (c) $f : \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x, y) = x - y$.
   Surjective.

   (d) $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ defined by $f(\overline{x}) = \overline{2x + 1}$.
   Neither.

3. Find a right-inverse for the quotient map $q : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ defined by $q(x) = \overline{x}$.
   Let $g : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}$ be defined by $g(\overline{0}) = 0$, $g(\overline{1}) = 1$, and $g(\overline{2}) = 2$.

4. Prove that there exists a bijective function $f : \mathbb{R} \to \mathbb{R}^2$.
   On Problem Set 7 we proved that $|\mathcal{P}(\mathbb{N}_1) \times \mathcal{P}(\mathbb{N}_1)| = \mathfrak{c}$. Since $|\mathcal{P}(\mathbb{N}_1)| = |\mathbb{R}| = \mathfrak{c}$, this implies that
   $$|\mathbb{R} \times \mathbb{R}| = |\mathcal{P}(\mathbb{N}_1) \times \mathcal{P}(\mathbb{N}_1)| = \mathfrak{c} = |\mathbb{R}|.$$
   Since $\mathbb{R}$ and $\mathbb{R}^2$ have the same cardinality, there exists a bijection between them.

5. Find the cardinality of each set and prove your answer.

   (a) $\mathcal{P}(\mathbb{Z} \times \{1, 2, 3\})$.
   The cardinality is $\mathfrak{c}$. $\mathbb{Z} \times \{1, 2, 3\}$ is countable because it is the product of two countable sets. Since it's infinite, the cardinality must be $\aleph_0$. Therefore $|\mathbb{Z} \times \{1, 2, 3\}| = |\mathbb{N}_1|$. Then $|\mathcal{P}(\mathbb{Z} \times \{1, 2, 3\})| = |\mathcal{P}(\mathbb{N}_1)| = \mathfrak{c}$.

   (b) $\mathbb{Q} \cap [0, 1]$.
   The cardinality is $\aleph_0$. This set is a subset of $\mathbb{Q}$, so $|\mathbb{Q} \cap [0, 1]| \leq |\mathbb{Q}| = \aleph_0$. On the other hand there is injective function $f : \mathbb{N}_1 \to \mathbb{Q} \cap [0, 1]$ defined by $f(n) = 1/n$. Therefore $|\mathbb{Q} \cap [0, 1]| \geq \aleph_0$. Then apply the Cantor-Schröder-Bernstein Theorem.

(c) The symmetric group on four elements, $\mathfrak{S}_4$.

The cardinality is 24. The elements of the symmetric group on four elements are the bijections from $\{1,2,3,4\}$ to itself. On Problem Set 6 we proved that the set of such functions has cardinality $4! = 24$.

6. Let A be the set of functions from $\mathbb{R}$ to $\mathbb{Z}$. Prove that A is uncountable.

Let $f : \mathbb{R} \to A$ be defined by $f(x) = \chi_{\{x\}}$, where $\chi_{\{x\}}$ is the function that maps x to 1 and all other real numbers to 0. If $x \neq y$ then $\chi_{\{x\}}(x) = 1$ but $\chi_{\{y\}}(x) = 0$ so $\chi_{\{x\}} \neq \chi_{\{y\}}$. Therefore f is injective. So $|A| \geq |\mathbb{R}| > \aleph_0$.

7. Prove that if A is an infinite set and B is a countably infinite set, then $|A \cup B| = |A|$.

Because B is countable, $B \setminus A$ is also countable. As we proved on Problem Set 7, A has a countably infinite subset C. The union of countable sets is countable so $C \cup (B \setminus A)$ is countably infinite. Since $|C| = |C \cup (B \setminus A)|$, there exists a bijection $f : C \to C \cup (B \setminus A)$. Define $g : A \to A \cup B$ by

$$g(x) = \begin{cases} f(x) & \text{if } x \in C \\ x & \text{if } x \notin C \end{cases}.$$

g bijectively maps $A \setminus C$ to itself since it is the identity function here, and bijectively maps C to $C \cup (B \setminus A)$ using f. Since A is the disjoint union of $A \setminus C$ and C, and $A \cup B$ is the disjoint union of $A \setminus C$ and $C \cup (B \setminus A)$, g is a bijection.

8. Prove for each pair of groups that they are not isomorphic.

(a) $(\mathbb{Z}/5\mathbb{Z}, +)$ and $(\mathbb{Z}/6\mathbb{Z}, +)$

$(\mathbb{Z}/5\mathbb{Z}, +)$ has order 5 but $(\mathbb{Z}/6\mathbb{Z}, +)$ has order 6 so they are not isomorphic.

(b) The symmetry group of a square and $(\mathbb{Z}/8\mathbb{Z}, +)$.

The symmetry group of a square is not abelian but $(\mathbb{Z}/8\mathbb{Z}, +)$ is abelian so they are not isomorphic. Alternatively, since $(\mathbb{Z}/8\mathbb{Z}, +)$ is cyclic, it has at least one element of order 8 (actually four of them), but the symmetry group of the square has no elements of order 8.

(c) $(\mathbb{Z}, +)$ and $(\mathbb{Q} \setminus \{0\}, \cdot)$.

$(\mathbb{Z}, +)$ is cyclic, because it is generated by 1. Suppose $(\mathbb{Q} \setminus \{0\}, \cdot)$ is cyclic, so it has a generator a/b where a and b are nonzero integers. Then

$$\langle a/b \rangle = \{\ldots, (a/b)^{-2}, (a/b)^{-1}, 1, (a/b)^1, (a/b)^2, \ldots\} = \mathbb{Q} \setminus \{0\}.$$

Let p be a prime that appears neither in the prime factorizations of a nor b. Since $p \in \mathbb{Q} \setminus \{0\}$, $p = (a/b)^n$ for some $n \in \mathbb{Z}$. If $n > 0$ then $a^n = pb^n$ implies that p divides b. If $n < 0$ then $b^{-n} = pa^{-n}$ implies that p divides a. If $n = 0$ then $p = 1$. None of these conclusions are true, which is a contradiction. Therefore $(\mathbb{Q} \setminus \{0\}, \cdot)$ is not cyclic.

9. Prove that $(\mathcal{P}(\mathbb{Z}), \Delta)$ is a group where Δ denotes the symmetric difference operation defined as $A \,\Delta\, B = (A \setminus B) \cup (B \setminus A)$.

Associativity: For $A, B, C \in \mathcal{P}(\mathbb{Z})$, we can show that $(A \,\Delta\, B) \,\Delta\, C$ is the set of integers that appear in exactly one of A, B, C or in all three,

$$(A \,\Delta\, B) \,\Delta\, C = (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus (A \cup B)) \cup (A \cap B \cap C).$$

This is symmetric in all three sets, so it's equal to $A \,\Delta\, (B \,\Delta\, C)$.

Identity: The identity element is $\emptyset$ because

$$A \,\Delta\, \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A,$$

and similarly for $\emptyset \,\Delta\, A$.

Inverses: The inverse of A is A because

$$A \,\Delta\, A = (A \setminus A) \cup (A \setminus A) = \emptyset \cup \emptyset = \emptyset.$$

10. Write the Cayley table for $(\mathbb{Z}/5\mathbb{Z}, +)$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

11. Find the order of each element of $(\mathbb{Z}/8\mathbb{Z}, +)$.

- $\overline{0}$ has order 1,
- $\overline{1}$ has order 8,
- $\overline{2}$ has order 4,
- $\overline{3}$ has order 8,
- $\overline{4}$ has order 2,
- $\overline{5}$ has order 8,
- $\overline{6}$ has order 4,
- $\overline{7}$ has order 8.

12. Prove that the set $\{(x, x) \mid x \in \mathbb{R}\}$ is a subgroup of $(\mathbb{R}^2, +)$.

Suppose $a, b \in H = \{(x, x) \mid x \in \mathbb{R}\}$. Then $a = (x, x)$ and $b = (y, y)$ for some $x, y \in \mathbb{R}$. Then $a - b = (x - y, x - y)$, which is in H. Therefore H is a subgroup.

13. Let $f : G \to H$ be a group homomorphism and let K be a subgroup of G. Prove that $\{f(k) \mid k \in K\}$ is a sugroup of H.

Let $L = \{f(k) \mid k \in K\}$. Suppose $a, b \in L$ so $a = f(x)$ and $b = f(y)$ for some $x, y \in K$. Since K is a subgroup, $y^{-1} \in K$, and then $xy^{-1} \in K$, so $f(xy^{-1}) \in L$. Using the fact that f is a homomorphism,

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = ab^{-1}.$$

Since $ab^{-1} \in L$, L is a subgroup.

14. Let R be a ring with multiplicative indentity 1. For any $a \in R$ prove that $(-1) \cdot a = -a$.

We want to show that $(-1) \cdot a$ is the additive inverse of a. Since 1 is the multiplicative identity, we have $1 \cdot a = a \cdot 1 = a$. Then

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0,$$

which proves that $(-1) \cdot a = -a$.