Practice Exam 1

1. Let $f : A \to B$ and $g : B \to C$ be maps.

   (a) If f and g are both one-to-one functions, show that $g \circ f$ is one-to-one.

   (b) If $g \circ f$ is onto, show that g is onto.

   (c) If $g \circ f$ is one-to-one, show that f is one-to-one.

   (d) If $g \circ f$ is one-to-one and f is onto, show that g is one-to-one.

   (e) If $g \circ f$ is onto and g is one-to-one, show that f is onto.

   Proof.

   (a) Suppose $g \circ f(x) = g \circ f(y)$, i.e., $g(f(x)) = g(f(y))$. Since g is one-to-one, then $f(x) = f(y)$. Since f is one-to-one, then $x = y$. Therefore $g \circ f$ is one-to-one.

   (b) Let $c \in C$. Since $g \circ f$ is onto, there exists an $a \in A$ such that $g \circ f(a) = c$. Let $b = f(a) \in B$. Then $g(b) = g(f(a)) = c$. So $g(b) = c$. Therefore g is onto.

   (c) Suppose $f(x) = f(y)$, then $g(f(x)) = g(f(y))$. Since $g \circ f$ is one-to-one and $g \circ f(x) = g \circ f(y)$, then $x = y$. Therefore f is one-to-one.
   An **alternative proof** would be to assume for the sake of contradiction that f is not one-to-one, i.e., there exist distinct x and y such that $f(x) = f(y)$. But then $g(f(x)) = g(f(y)$, which implies that $x = y$, contradicting the fact that x and y are distinct.
   The two proofs are very similar but I wrote both of them to illustrate that you don't have to think about it a certain way.

   (d) Let $x, y \in B$ and suppose $g(x) = g(y)$. Since $x \in B$ and $y \in B$ and f is onto, there exist $a_1, a_2 \in A$ such that $f(a_1) = x$ and $f(a_2) = y$. Therefore $g(f(a_1)) = g(f(a_2))$, so $g \circ f(a_1) = g \circ f(a_2)$. Since $g \circ f$ is one-to-one, then $a_1 = a_2$. But then $f(a_1) = f(a_2)$, so $x = y$. Therefore g is one-to-one.

   (e) Let $b \in B$. Now consider $c = g(b) \in C$. Since $g \circ f$ is onto, then there exists an $a \in A$ such that $g \circ f(a) = c$. Therefore $g(f(a)) = c = g(b)$. Since g is one-to-one, $f(a) = b$. So we've shown that there exists an $a \in A$ such that $f(a) = b$, which shows that f is onto.

   □

2. Determine whether or not the following relations are equivalence relations on the given set. If the relation is an equivalence relation, describe the partition given by it. If the relation is not an equivalence relation, state why it fails to be one.

   (a) $x \sim y$ in $\mathbb{R}$ if $x \geq y$

   (b) $m \sim n$ in $\mathbb{Z}$ if $mn > 0$

   (c) $x \sim y$ in $\mathbb{R}$ if $|x - y| \leq 4$

   (d) $m \sim n$ in $\mathbb{Z}$ if $m \equiv n \pmod 6$

   Proof.

(a) It's not an equivalence relation because it is not symmetric. For example $3 \sim 2$ because $3 \geq 2$, but $2 \not\sim 3$ since $2 \ngeq 3$.

(b) It's not an equivalence relation because it is not reflexive since $0 \not\sim 0$.

(c) It's not an equivalence relation because it is not transitive. Indeed, $4 \sim 0$ since $|4-0| \leq 4$ and $0 \sim -4$ since $|0-(-4)| \leq 4$. Yet $4 \not\sim -4$ because $|4-(-4)| = 8 > 4$.

(d) It is an equivalence relation. The equivalence relation partitions the set $\mathbb{Z}$ into the following six equivalence classes:

- $[0]$ is the set of multiples of 6.
- $[1]$ is the set of numbers of the form $6k+1$ for some integer k.
- $[2]$ is the set of numbers of the form $6k+2$ for some integer k.
- $[3]$ is the set of numbers of the form $6k+3$ for some integer k.
- $[4]$ is the set of numbers of the form $6k+4$ for some integer k.
- $[5]$ is the set of numbers of the form $6k+5$ for some integer k.

□

3. For each of the following pairs of numbers a and b, calculate $\gcd(a,b)$ and find integers r and s such that $\gcd(a,b) = ra + sb$.

(a) 14 and 39

(b) 234 and 165

Proof.

(a)

$$\begin{aligned} 39 &= 14 \times 2 + 11 \\ 14 &= 11 \times 1 + 3 \\ 11 &= 3 \times 3 + 2 \\ 3 &= 2 \times 1 + 1. \end{aligned}$$

Therefore the gcd is 1. Now,

$$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (11 - 3 \times 3) \times 1 \\ &= 3 \times 4 - 11 \times 1 \\ &= (14 - 11) \times 4 - 11 \times 1 \\ &= 14 \times 4 - 11 \times 5 \\ &= 14 \times 4 - (39 - 14 \times 2) \times 5 \\ &= 14 \times 14 - 39 \times 5. \end{aligned}$$

Therefore if $r = 14$ and $s = -5$ we have $14a + 39b = 1$.

(b)

$$\begin{aligned} 265 &= 165 \times 1 + 69 \\ 165 &= 69 \times 2 + 27 \\ 69 &= 27 \times 2 + 15 \\ 27 &= 15 \times 1 + 12 \\ 15 &= 12 \times 1 + 3 \\ 12 &= 3 \times 4 + 0. \end{aligned}$$

Therefore the gcd is 3.
Now,

$$\begin{aligned} 3 &= 15 - 12 \times 1 \\ &= 15 - (27 - 15 \times 1) \times 1 \\ &= 15 \times 2 - 27 \times 1 \\ &= (69 - 27 \times 2) \times 2 - 27 \times 1 \\ &= 69 \times 2 - 27 \times 5 \\ &= 69 \times 2 - (165 - 69 \times 2) \times 5 \\ &= 69 \times 12 - 165 \times 5 \\ &= (234 - 165 \times 1) \times 12 - 165 \times 5 \\ &= 234 \times 12 - 165 \times 17. \end{aligned}$$

Therefore if $r = 12$ and $s = -17$ we have $234r + 165s = 3$.

□

4. Which of the following associative multiplication tables defined on the set $G = \{a, b, c, d\}$ form a group? Support your answer in each case.

(a)

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(c)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

Proof. (a) It's not a group since it doesn't have an identity. The easy way to see that it does not have an identity is that no row of the Cayley table matches the top row.

(b) The identity is a. All elements have inverses (the inverse of a is a, the inverse of b is b, the inverse of c is c and the inverse of d is d). The operation is closed by definition. Since the operation is also associative by assumption, $\{a, b, c, d\}$ is a group.

(c) The identity is a. All elements have inverses (the inverse of a is a, the inverse of b is b, the inverse of c is c and the inverse of d is d). The operation is closed by definition. Since the operation is associative by assumption, it is a group!

(d) The identity is a. However, d does not have an inverse, so it is not a group.

□

5. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Proof. First let's show that $*$ is closed, i.e., that if $a, b \in S$, then $a * b \in S$. Since S is every real except -1 then we want to show that if $a \neq -1$ and $b \neq -1$, then $a * b \neq -1$. For the sake of contradiction, suppose $a * b = -1$. Then

$$\begin{aligned} a + b + ab &= -1 \\ a(b+1) + b &= -1 \\ a(b+1) &= -(b+1). \end{aligned}$$

Since $b \neq -1$, then we can divide both sides by $b + 1$. But then we have that $a = -1$, which contradicts that $a \neq -1$. Therefore $a * b \neq -1$, so $a * b \in S$, so $*$ is a binary operation on S.

Now let's show that $*$ is associative. Suppose $a, b, c \in S$.

$$\begin{aligned} (a * b) * c = (ab + a + b) * c &= (ab + a + b)(c) + (ab + a + b) + c \\ &= abc + ac + bc + ab + a + b + c \\ &= a(bc + c + b) + a + (bc + b + c) \\ &= a(b * c) + a + (b * c) \\ &= a * (b * c). \end{aligned}$$

Therefore $*$ is associative.

Let's show that 0 is the identity for S. Let $a \in S$. Then $a * 0 = a + 0 + 0 = a$ and $0 * a = 0 + 0 + a = a$. Therefore $0 * a = a * 0 = a$, so 0 is the identity of S.

To finish our proof that S is a group, we need to show every element has an inverse. Let $a \in S$. We want to find an inverse for a, so we want to find a $b \neq -1$ such that $a * b = 0$.

$$\begin{aligned} a * b &= 0 \\ ab + a + b &= 0 \\ b(a+1) &= -a \\ b &= -\frac{a}{a+1}. \end{aligned}$$

Since $a \neq -1$, b exists and $a * b = 0$, so $b = -\dfrac{a}{a+1}$ is the inverse of a. Note that $b = -1 + \dfrac{1}{a+1} \neq -1$, so $b \in S$.

We've shown that S is a group together with the operation $*$. To show that it is an abelian group we must prove that $*$ is commutative. Let $a, b \in S$. Then

$$a * b = ab + a + b = ba + b + a = b * a,$$

therefore it is an abelian group.

□

6. Find all the subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$. Use this information to show that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not the same group as $\mathbb{Z}_9$.

Proof. The subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ are

(a) $\{(0,0)\}$,
(b) $\{(0,0),(1,0),(2,0)\}$,
(c) $\{(0,0),(0,1),(0,2)\}$,
(d) $\{(0,0),(1,1),(2,2)\}$,
(e) $\{(0,0),(1,2),(2,1)\}$,
(f) $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Meanwhile, the subgroups of $\mathbb{Z}_9$ are:

(a) $\{0\}$,
(b) $\{0,3,6\}$,
(c) $\mathbb{Z}_9$.

Since there are a different number of subgroups in each group $\mathbb{Z}_3 \times \mathbb{Z}_3 \neq \mathbb{Z}_9$.

□

7. Let $n = 0, 1, 2, \ldots$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Prove that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Show that these subgroups are the only subgroups of $\mathbb{Z}$.

Proof. First let's show $n\mathbb{Z}$ is a subgroup for any $n \in \mathbb{N} \cup \{0\}$:

(a) First let's show addition is closed on $n\mathbb{Z}$. If $a, b \in n\mathbb{Z}$, then there exist $k_1, k_2 \in \mathbb{Z}$ such that $a = k_1 n$ and $b = k_2 n$. Then

$$a + b = k_1 n + k_2 n = (k_1 + k_2)n \in n\mathbb{Z}.$$

(b) The identity of $\mathbb{Z}$, 0, is an element of $n\mathbb{Z}$, since $0 = n \times 0$, so $0 \in n\mathbb{Z}$.

(c) Finally, let's show that any element of $n\mathbb{Z}$ has an inverse. Indeed if $a \in n\mathbb{Z}$, then $a = k_1 n$ for some integer k_1. Then $-a = -k_1 n = (-k_1)n \in n\mathbb{Z}$. Therefore the inverse of a is also an element of $n\mathbb{Z}$.

By (a), (b) and (c), $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ with the addition operation.

Now, we want to show that all subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ with $n \in \mathbb{N} \cup \{0\}$. Suppose $H \subseteq \mathbb{Z}$ is a subgroup. If $H = \{0\}$, then $H = 0\mathbb{Z}$. Suppose $H \neq \}0\}$. By the Well-Ordering principle, there exists a nonzero element $n \in H$ such that $|n|$ is minimal. Since H is a subgroup of $\mathbb{Z}$, then the inverse of n is also in H, i.e., $-n \in H$. Since n and $-n$, then we can assume without loss of generality that n is positive. Since H is a subgroup, then all multiples of n must be in H. This means that $n\mathbb{Z} \subseteq H$. Now suppose that there is an element $m \in H$ such that $m \notin n\mathbb{Z}$. By the division algorithm, there exist integers q and r such that:

$$m = qn + r,$$

where $0 \leq r < n$. Since $m \notin n\mathbb{Z}$, then $r \neq 0$. Since $m \in H$ and $qn \in H$, then $-qn \in H$, so $m - qn \in H$. Therefore $r \in H$. But $0 < r < n$ which implies that $|r| < |N|$, which contradicts the minimality of $|n|$. This means no element m exists. That proves that $H = n\mathbb{Z}$.

Alternative Solution: An alternative solution to prove that if H is a subgroup of $\mathbb{Z}$, then $H = n\mathbb{Z}$ is the following:

Since $\mathbb{Z}$ is cyclic, H is cyclic. Therefore $H =< m >$ for some $m \in \mathbb{Z}$. Since $-m$ is the inverse of m, then $< m >=< -m >=< |m| >$. So if $n = |m|$, then $H =< n >$ for some nonnegative integer n. But $< n >= \{kn : k \in \mathbb{Z}\}$, so $< n >= n\mathbb{Z}$, which is what we wanted to prove.

□

8. Prove or disprove each of the following statements.

(a) $\mathbb{Z}_8^\times$ is cyclic.

(b) All of the generators of $\mathbb{Z}_{60}$ are prime.

(c) $\mathbb{Q}$ is cyclic.

(d) If every proper subgroup of a group G is cyclic, then G is a cyclic group.

(e) A group with a finite number of subgroups is finite.

Proof.

(a) It is not cyclic because none of the cyclic subgroups is the whole group. Indeed the cyclic subgroups are:

- $< 1 >= \{1\}$,
- $< 3 >= \{1, 3\}$,
- $< 5 >= \{1, 5\}$,
- $< 7 >= \{1, 7\}$.

(b) It's not true because $< 49 >= \mathbb{Z}_{60}$ and 49 is not prime. Also $< 1 >= \mathbb{Z}_{60}$ and 1 is not prime either.

(c) Suppose that $\mathbb{Q}$ is cyclic. Suppose that it has a as its generator. Since $a \in \mathbb{Q}$, then there exist p and q relatively prime integers such that $a = \frac{p}{q}$. Since a is a generator, then any rational number x can be written in the form ka for some integer k. Therefore $x = kp/q$. Therefore qx is an integer, for any rational number x. The rational number $r = \frac{1}{q+1}$ doesn't satisfy that $qr \in \mathbb{Z}$. This contradicts our assumption that $\mathbb{Q}$ is cyclic, so it is not cyclic.

(d) False. The group of symmetries of the equilateral triangle (D_3) is a non-cyclic group with proper subgroups all cyclic.

(e) True. This one is hard to prove. Let G be a group with finitely many subgroups. Then in particular, there are finitely many cyclic subgroups of the form $< g >$. Now define the following equivalence relation on the set G: $g \sim h$ if $< g >=< h >$. The set of equivalence classes partitions G. Since each equivalence class creates a subgroup of G and G has finitely many subgroups, the set of equivalence classes is finite.

For the sake of contradiction assume that G is infinite. Then, by the Pigeonhole principle, at least one of the equivalence classes has infinitely many elements. Suppose the equivalence class with infinitely many elements is $[g]$. Let $g, h \in [g]$ such that $g \neq h$, and $h \neq g^{-1}$. Since $< g >=< h >$, then there exist $k, j \in \mathbb{Z}$ such that $g = h^k$ and $h = g^j$. Therefore $g = h^k = (g^j)^k = g^{jk}$. Therefore $g^{jk-1} = e$ (the identity). Now, note that since g and h are not the identity, inverses of each other or equal to each other, then $jk \neq 1$, so $jk - 1 \neq 0$. So then $| < g > | \leq |jk - 1|$. But if $r \in [g]$, then $r \in < g >$ because $< r >=< g >$ implies $r \in < g >$. Since $[g]$ is infinite, $< g >$ should have infinitely many elements, yet $< g >$ has finitely many. This contradicts our assumption that G is infinite, proving that G is finite.

□

9. Find the order of each of the following elements.

(a) $5 \in \mathbb{Z}_{12}$

(b) $\sqrt{3} \in \mathbb{R}$

(c) $\sqrt{3} \in \mathbb{R}^*$

(d) $-i \in \mathbb{C}^*$

Proof.

(a) $gcd(5, 12) = 1$, therefore $| < 5 > | = 12$.

(b) $|\sqrt{3}| = \infty$.

(c) $< \sqrt{3} >= \{\ldots, -3, -\sqrt{3}, 1, \sqrt{3}, 3, 3\sqrt{3}, \ldots\}$, so $|\sqrt{3}| = \infty$.

(d) $< -i >= \{1, -i, -1, i\}$, so $| < -i > | = 4$.

□

10. Prove that $\mathbb{Z}_p$ has no nontrivial proper subgroups if p is prime.

Proof. $\mathbb{Z}_p =< 1 >$. Suppose H is a nontrivial subgroup of $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is cyclic, H must be cyclic. Suppose $H =< b >$. But $b = b \cdot 1$. Therefore the order of b is $\frac{p}{gcd(b,p)} = \frac{p}{1} = p$. But then H is $\mathbb{Z}_p$. So the only subgroups of $\mathbb{Z}_p$ are $\{0\}$ and $\mathbb{Z}_p$.

□