Question 1

Prove that $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ is cyclic if and only if p, q, r are pairwise relatively prime.

Solution: Denote $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ as G.
($\Longrightarrow$):

If G is cyclic, then there is an element g that generates G, or $\langle g \rangle = G$. Let $g = ([g_1]_p, [g_2]_q, [g_3]_r)$. Assume that p, q, r are not pairwise relatively prime. Let say that $\gcd(p, q) = d > 1$ without loss of generality. Then there is $a, b \in \mathbb{Z}$ such that $ap + bq = d$ Then consider all value $k \in \mathbb{N}$ such that $(dk)g_1 \equiv 0 \mod p$, and $(dk)g_2 \equiv 1 \mod q$. Then

$$\begin{aligned} dk(g_1 + g_2) - 1 &= \alpha p + \beta q \\ (ap + bq)k(g_1 + g_2) - \alpha p - \beta q &= 1 \\ (a(g_1 + g_2) - \alpha)kp + (b(g_1 + g_2) - \beta)kq &= 1 \end{aligned}$$

So, $d = 1$ contradicts that p and q are not relatively prime.

Hence, G is cyclic implies p, q, r are pairwise relatively prime.

($\Longleftarrow$):

If p, q, r is pairwise relatively prime, then consider any $g = (g_1, g_2, g_3) \in G$. Notice that $g^n = (g_1^n, g_2^n, g_3^n)$, and

$$g_1^{kp+k'} = g_1^{k'}, g_2^{kq+k'} = g_2^{k'}, g_3^{kr+k'} = g_3^{k'}$$

But a $k \in \mathbb{N}$ satisfying the following exists by the chinese remainder theorem.

$$\begin{aligned} k &\equiv k_1 \mod p \\ k &\equiv k_2 \mod q \\ k &\equiv k_3 \mod r \end{aligned}$$

Hence, $\forall h \in G, \exists n \in \mathbb{N} \quad g^n = h$, proving that G is cyclic.

Question 2

Prove that a group G is abelian if and only if the map $f : G \to G$ given by $f(g) = g^{-1}$ for all $g \in G$ is a homomorphism.

Solution:
($\Longrightarrow$):

If the group is abelian, then for all $g, h \in G$, $gh = hg$. So

$$g^{-1}h^{-1} = h^{-1}g^{-1} = (gh)^{-1}$$

Hence, a function $f(g) = g^{-1}$ preserves the binary operator, as $f(g)f(h) = f(gh)$, and thus, is a homomorphism.

($\Longleftarrow$):

If f is a homomorphism, then $\forall g, h \in G \quad f(g)f(h) = f(gh)$. Which means that

$$g^{-1}h^{-1} = (gh)^{-1} = h^{-1}g^{-1}$$

But since $g^{-1} \in G$ for any g, then the above relation shows that every element is commutative. Hence, the group is abelian.

Question 3

Show that the map $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $f(a) = [a]_n$ is an epimorphism with $\ker f = \{ mn \mid m \in \mathbb{Z} \}$

Solution: The map f is well-defined since for $a = b$, $f(a) = [a]_n = [b]_n = f(b)$ as $b = a + nk$ for some $n \in \mathbb{N}$. Consider that $\mathbb{Z}/n\mathbb{Z} = \{ [0]_n, \ldots, [n-1]_n \}$, then we know that $f(a) = [a]_n$ for all integer $0 \leq a < n$. Therefore, f is surjective, hence, an epimorphism.

Moreover, for $f(x) = [0]_n$, we get that $n|x$, so $\ker f = \{ x \mid n|x \} = \{ mn \mid m \in \mathbb{Z} \}$

Question 4

Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. Exhibit a proper subgroup of the additive group $\mathbb{Q}$ that is not cyclic.

Solution: Note that I use the convention notation g^n instead of ng despite the group being additive.

Let S be a subgroup of the additive group $\mathbb{Q}$ that is generated by $g_1, \dots, g_n$. Then we can choose g_0 such that

$$g_1 = g_0^{k_1}, g_2 = g_0^{k_2}, \dots, g_n = g_0^{k_n} \quad \exists k_1, \dots, k_n$$

(for example, by taking $g_0 = \frac{1}{g_1' \times \cdots \times g_n'}$ where g_i' denotes the denominator of g_i

Since $\forall h \in S, \quad h = g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}$, then

$$h = g_0^{k_1 m_1} \cdots g_0^{k_n m_n} = g_0^{k_1 m_1 + \cdots + k_n m_n}$$

Hence, the group is generated by g_0. Thus the group is cyclic.

For a proper subgroup of the additive group $\mathbb{Q}$ that is not cyclic, consider the group

$$C = \left\{ \frac{a}{2^b} \mid a, b \in \mathbb{Z} \right\}$$

Firstly, note that C is a subgroup, since for all $\frac{a}{2^b}, \frac{c}{2^d} \in C$, the element $\frac{a2^d + b2^c}{2^{b+d}} \in C$. Moreover, for every $a \in C$, $-a \in C$.

However, $\frac{1}{3} \notin C$ as $3 = 2^x$ has no integer solution.

Lastly, C is not generated by a single element. To show this, assume otherwise that $C = \langle g \rangle$. Then $g \neq 0$, as if $g = 0$, $g^n = 0$. Moreover, $\frac{g}{2} \in C$ but is not in $\langle g \rangle$. This shows that C is not cyclic.

Question 5

Let G be a cyclic group of order n and let d be a divisor of n. Show that G has exactly one subgroup order d.

Solution:

> **Claim 1**
>
> All finite subgroups of a cyclic group is cylic.
>
> ***Proof:*** Since a cyclic group G is generated by a single element, g, then each element in the subgroup $S \leq G$ is in G, which means that it must be some power of g. Then, let $S = \{ g^{a_1}, \dots, g^{a_n} \}$, then it is possible to choose the smallest positive a_i, so let b be that element. With the division algorithm, we know that for some a, $g^a = g^{mb+c}$ for some integer m and $0 \leq c < b$. The closure of the group asserts that g^c must be an element of S, but $0 \leq c < b$, so $c = 0$.
>
> Hence, g^b generates S. □

From claim 1, a subgroup of order d must be cyclic. And since every finite cyclic group of order n is isomorphic to the group $\mathbb{Z}/n\mathbb{Z}$, then we will show that the subgroup of order d of $\mathbb{Z}/n\mathbb{Z}$ is unique. This generalize naturally to every cyclic groups.

Let $\frac{n}{d} = k \in \mathbb{N}$, and consider $[1]_n$ is an element of order n in G. Then, there is an element $k[1]_n$ denoted by $[k]_n$ such that $\langle [k]_n \rangle$ is a subgroup of order d.

Now, any subgroup S of order d must be generated by one element, that is of order d, as an element of order p will always generate a group with p distinct elements.

Therefore, $\langle [k]_n \rangle = \langle [m]_n \rangle$ for some element m with order d. But since $[m]_n = m[1]_n$, then $dm[1]_n = [0]_n$. So, $n|dm$. Hence, $k(\frac{dm}{n}) = m$, so $(\frac{dm}{n})[k]_n = [m]_n$.

Lastly, $[m]_n \in \langle [k]_n \rangle$ implies that S must be unique.

Question 6

Find the center of the group $SL_2(\mathbb{R})$

Solution: Consider 2 matrices $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, and $B = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$, then

$$AB = \begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix} \text{ and } BA = \begin{bmatrix} ax+cy & bx+dy \\ az+cw & bz+dw \end{bmatrix}$$

So, $AB = BA$ when

$$\begin{aligned} bz &= cy \\ ay+bw &= bx+dy \\ cx+dz &= az+cw \end{aligned}$$

Since $bz = cy$ must holds for any value of b and c, then $y = z = 0$ is the only possible option. Then it follows that $x = w$. Therefore, $B = \begin{bmatrix} w & 0 \\ 0 & w \end{bmatrix}$ commutes with any matrix $A \in SL_2(\mathbb{R})$. But since $B \in SL_2(\mathbb{R})$, Then $\det B = 1$, which means that $w = \pm 1$. Therefore, the center of $SL_2(\mathbb{R})$ is $\{ I_2, -I_2 \}$.

Question 7

Let $f : G \to H$ be a homomorphism and $g \in G$. Assume that $|g|$ and $|f(g)|$ are finite. Show that $|f(g)|$ divides $|g|$

Solution: Let the order of g be n. Since a homomorphism must preserve the binary operator, then

$$f(1) = f(g^n) = f(g)^n = 1$$

Therefore, if the order of $f(g)$ be d, then there exist integer k such that $f(g)^{dk} = f(g)^n = 1$. So, d divides n.

Question 8

Let p be a prime and let n be a positive integer. Find the order of $[p]$ in the multiplicative group $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ and deduce that $n|\varphi(p^n-1)$, where φ denotes Euler's function.

Solution: let the order of $[p]$ be d, then $p^d \equiv 1 \mod p^n - 1$, but since for $d < n$, $p^d < p^n$, then $d = n$ is the smallest solution, and thus is the order of $[p]$.

Moreover, $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times = \{ m < p^n - 1 \mid \gcd(m, p^n-1) = 1 \}$. So $|(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times| = \varphi(p^n-1)$ by definition. Lastly, by lagrange theorem, the order of subgroup divides the order of the group, and $\langle [p] \rangle$ is a cyclic subgroup of $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$, therefore, $n|\varphi(p^n-1)$

Question 9

Show that the quaternion group Q_8 and the dihedral group D_8 are not isomorphic. Show also that Q_8 is not isomorphic to a subgroup of S_n for any $n \leq 7$

Solution: Consider that there is an element r in D_8 such that $r \neq 1$, $r^2 \neq 1$, $r^3 \neq 1$ and $r^4 = 1$. But in $Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \}$, if $q \in Q_8$, $q^2 = 1$. Hence, there cannot be an isomorphism between D_8 and Q_8.

Note that S_n is a subgroup of S_{n+1}. Hence, we will only show that Q_8 is not a subgroup of S_7, as if it is not a subgroup of S_7, then it is not a subgroup of a subgroup of S_7.

Now, assume that there is a isomorphism between Q_8 and a subgroup of S_7. The assumption is equivalent to having an injective homomorphism from Q_8 to S_7. Which means that there must be a group action between Q_8 and A where A is a set with 7 elements, such that $|setg \mid g \cdot x = x| = 1$, followed from the fact that the homomorphism must be injective.

This follows from the derivation of the equivalence of homomorphism and group action. The construction of the equivalence of φ to a group action asserts the the kernel of φ consists of all the element $g \in G$ such that $g \cdot x = x$.

From the assumption, we construct the operator $(\cdot)$. Firstly $1 \cdot x = x$ and for $g \neq 1$, $g \cdot x \neq x$. Let there be an element $a \in A$. Then we know that

$$-1 \cdot a = b \quad \exists b \neq a$$

. Moreover

$$i \cdot a = -i \cdot i \cdot i \cdot a = -i \cdot -1 \cdot a = -i \cdot b = c$$

for an element c that is pairwise distinct from a and b. Next,

$$j \cdot c = j \cdot i \cdot a = j \cdot -i \cdot b = d$$

for an element d that is pairwise distinct from a, b, c, since $ji \neq 1$ and $j(-i) \neq 1$. Next,

$$-1 \cdot d = -j \cdot c = -k \cdot b = k \cdot a = e$$

for some element e that is distinct from a, b, c, d. Then we can have,

$$i \cdot e = -i \cdot d = k \cdot c = j \cdot b = -j \cdot a = f$$

for some element f that is distinct from a, b, c, d, e Then

$$-k \cdot f = -j \cdot e = j \cdot d = -1 \cdot c = i \cdot b = -i \cdot a = g$$

for some g that is distinct from a, b, c, d, e, f. Making the set A contain exactly 7 elements.

However, since

$$-k \cdot g = -1 \cdot f = -i \cdot e = i \cdot d = k \cdot c = -j \cdot b = j \cdot a = h$$

such that h is pairwise distinct from the prior 7 elements, this means that A contains more than 7 elements.

Thus, it can be concluded that there is no isomorphism from Q_8 to a subgroup of S_7, by contradiction. And lastly, there must be no isomorphism from Q_8 to a subgroup of S_n for any $n < 8$.

Question 10

Find all homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Q}$.

Solution: Consider a homomorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}$, then

$$\varphi([0]_n) = \varphi(n[1]_n) = n\varphi([1]_n) = 0$$

but for $q \in \mathbb{Q}$, $nq = 0$ if and only if $q = 0$. Therefore, there is only one homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Q}$ which is $\forall x\ \varphi(x) = 0$.