Exercise 30

Let $\pi : G \to G/N$ be a canonical group homomorphism. whree N is a normal subgroup of G

1. prove that $\pi(K)$ is a subgroup of G/N if K is a subgroup of G
2. prove that $\pi^{-1}(H)$ is a subgroup of G containing N if H is a subgroup of G/N
3. prove that $\pi(\pi^{-1}(H)) = H$ and $\pi^{-1}(\pi(K)) = K$ where H is a subgroup of G/N and K is a subgroup of G containing N
4. Let G be a cyclic group and $f : G \to K$ a surjective group homomorphism. Prove that K is cyclic.
5. let $n \in \ltimes$ prove using the canonical group homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ that subgroup of H of $\mathbb{Z}/N\mathbb{Z}$ is cyclic

Proof.

1. Let K be a subgroup of G. We need to show that $\pi(K)$ is a subgroup of G/N. Since K is a subgroup of G, it is non-empty. Let $x, y \in \pi(K)$. Then, there exist $a, b \in K$ such that $\pi(a) = x$ and $\pi(b) = y$. Since K is a subgroup of G, $ab \in K$. Therefore, $\pi(ab) = \pi(a)\pi(b) = xy \in \pi(K)$. Also, since K is a subgroup of G, $a^{-1} \in K$. Therefore, $\pi(a^{-1}) = \pi(a)^{-1} = x^{-1} \in \pi(K)$. Hence, $\pi(K)$ is a subgroup of G/N.
2. Let H be a subgroup of G/N. We need to show that $\pi^{-1}(H)$ is a subgroup of G containing N. Since H is a subgroup of G/N, it is non-empty. Let $x, y \in \pi^{-1}(H)$. Then, there exist $a, b \in G$ such that $\pi(a) = x$ and $\pi(b) = y$. Since H is a subgroup of G/N, $xy \in H$. Therefore, $\pi(ab) = \pi(a)\pi(b) = xy \in H$. Also, since H is a subgroup of G/N, $x^{-1} \in H$. Therefore, $\pi(a^{-1}) = \pi(a)^{-1} = x^{-1} \in H$. Hence, $\pi^{-1}(H)$ is a subgroup of G containing N.
3. Let H be a subgroup of G/N and K be a subgroup of G containing N. We need to show that $\pi(\pi^{-1}(H)) = H$ and $\pi^{-1}(\pi(K)) = K$. Let $x \in \pi(\pi^{-1}(H))$. Then, there exists $a \in G$ such that $\pi(a) = x$. Since $a \in \pi^{-1}(H)$, $\pi(a) \in H$. Therefore, $x \in H$. Hence, $\pi(\pi^{-1}(H)) = H$. Let $y \in \pi^{-1}(\pi(K))$. Then, there exists $b \in G$ such that $\pi(b) = y$. Since $b \in \pi(K)$, $\pi(b) \in \pi(K)$. Therefore, $y \in K$. Hence, $\pi^{-1}(\pi(K)) = K$.
4. Let G be a cyclic group and $f : G \to K$ be a surjective group homomorphism. We need to show that K is cyclic. Since G is cyclic, there exists $a \in G$ such that $G = \langle a \rangle$. Since f is surjective, $K = f(G) = f(\langle a \rangle) = \langle f(a) \rangle$. Hence, K is cyclic.
5. Let $n \in \mathbb{N}$. We need to prove using the canonical group homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ that every subgroup H of $\mathbb{Z}/N\mathbb{Z}$ is cyclic. Since $\mathbb{Z}$ is cyclic, there exists $a \in \mathbb{Z}$ such that $\mathbb{Z} = \langle a \rangle$. Since π is surjective, $\mathbb{Z}/N\mathbb{Z} = \pi(\mathbb{Z}) = \pi(\langle a \rangle) = \langle \pi(a) \rangle$. Hence, $\mathbb{Z}/N\mathbb{Z}$ is cyclic.

□

Exercise 33

Consider $Z \subset \mathbb{Q}$ as abelian groups with $+$ as composition. Let $[q] = q + Z \in \mathbb{Q}/Z$, where $q \in \mathbb{Q}$.

1. show that $[\frac{9}{4}]$ has order 4 in $\mathbb{Q}/Z$

Proof.
The order of $[\frac{9}{4}]$ in $\mathbb{Q}/Z$ is the smallest positive integer n such that $n \cdot [\frac{9}{4}] = [0]$ in $\mathbb{Q}/Z$. This means:

$$n \cdot \left(\frac{9}{4} + Z\right) = 0 + Z \implies \frac{9n}{4} \in Z.$$

Since Z consists of rational numbers of the form $\frac{k}{1}$ for $k \in \mathbb{Z}$, $\frac{9n}{4}$ must be an integer. The smallest n for which $\frac{9n}{4}$ is an integer is 4. Therefore, the order of $[\frac{9}{4}]$ in $\mathbb{Q}/Z$ is 4. $\square$

(ii) Determine the order of ab in $\mathbb{Q}/Z$, where $a \in Z$, $b \in \mathbb{N} \setminus \{0\}$, and $\gcd(a, b) = 1$.

Proof.
To determine the order of $[ab]$ in $\mathbb{Q}/Z$, we have $a \in Z$ and $b \in \mathbb{N}\setminus\{0\}$ with $\gcd(a, b) = 1$. The element $[ab]$ is defined as $ab + Z$.

The order of $[ab]$ is the smallest positive integer n such that:

$$n \cdot [ab] = [0] \quad \text{in } \mathbb{Q}/Z.$$

This means:

$$n \cdot (ab + Z) = 0 + Z \implies nab \in Z.$$

Since Z consists of rational numbers of the form $\frac{k}{1}$ for $k \in \mathbb{Z}$, nab must be an integer.

Given $\gcd(a, b) = 1$, the smallest n for which nab is an integer is b. Therefore, the order of $[ab]$ in $\mathbb{Q}/Z$ is b.

Thus, every element in $\mathbb{Q}/Z$ has finite order, and there are elements in $\mathbb{Q}/Z$ of arbitrary large order.

$\square$

(iii) Show that $\mathbb{Q}/Z$ is an infinite group that is not cyclic.

Proof. To show that $\mathbb{Q}/Z$ is infinite, consider the elements of the form $\left[\frac{1}{n}\right]$ for $n \in \mathbb{N}$. Each $\left[\frac{1}{n}\right]$ is distinct in $\mathbb{Q}/Z$ because:

$$\left[\frac{1}{n}\right] = \left[\frac{1}{m}\right] \implies \frac{1}{n} - \frac{1}{m} \in Z \implies \frac{m-n}{mn} \in \mathbb{Z},$$

which is not possible unless $n = m$. Thus, there are infinitely many distinct elements in $\mathbb{Q}/Z$.

To show that $\mathbb{Q}/Z$ is not cyclic, assume for contradiction that $\mathbb{Q}/Z$ is cyclic. Then there exists some $[q]$ such that every element can be expressed as $n \cdot [q]$ for some integer n.

However, for $q = \frac{1}{p}$ (where p is a prime), the elements $\left[\frac{1}{p}\right]$ generate $\mathbb{Z}/Z$, which does not include elements like $\left[\frac{1}{2}\right]$ if $p \neq 2$. Hence, there are elements in $\mathbb{Q}/Z$ that cannot be generated by any single element, proving that $\mathbb{Q}/Z$ is not cyclic. $\square$

Exercise 34

Prove that $(\mathbb{Q}/\{0\}, \cdot)$ is not cyclic a group.

Proof. Assume for contradiction that $(\mathbb{Q} \setminus \{0\}, \cdot)$ is cyclic and let $g \in \mathbb{Q} \setminus \{0\}$ be a generator.

We can express g in its lowest terms:

$$g = \frac{a}{b},$$

where $a, b \in \mathbb{Z} \setminus \{0\}$ and $\gcd(a, b) = 1$.

Now, consider g^n:

$$g^n = \left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}.$$

This shows that all powers of g will also be rational numbers of the form $\frac{m}{n}$ where $m = a^n$ and $n = b^n$.

For $(\mathbb{Q} \setminus \{0\}, \cdot)$ to be cyclic, it must be able to generate all non-zero rational numbers, which can be represented in the form $\frac{p}{q}$, where $p, q \in \mathbb{Z} \setminus \{0\}$.

1. Choose p such that p is not divisible by a or b. 2. For g^n to equal $\frac{p}{q}$, we need:

$$\frac{a^n}{b^n} = \frac{p}{q},$$

implying $a^n q = pb^n$.

This requires the ability to represent every p and q using the integer powers of a and b.

However, it is clear that for any fixed $g = \frac{a}{b}$, the set of numbers g^n will produce only those rational numbers whose numerators and denominators are powers of a and b, respectively.

Since there are infinitely many rational numbers that cannot be expressed in the form g^n for any integer n we conclude that $(\mathbb{Q} \setminus \{0\}, \cdot)$ cannot be generated by a single element.

Thus, $(\mathbb{Q} \setminus \{0\}, \cdot)$ is not a cyclic group.

□

Exercise 35

35. Give an example of a non-cyclic group of order 8.

Proof. an example of a non-cyclic group of order 8 is the dihedral group D_4. The dihedral group D_4 is the group of symmetries of a square. It consists of 8 elements: 4 rotations and 4 reflections. The group operation is composition of symmetries. The group is non-cyclic because it does not have an element of order 8.

□

Exercise 36

Let G be a finite group of order N. Let $\psi(d)$ be the number of elements in G of order d.

(i) Prove that $\psi(d) = 0$ if $d \nmid N$ and that G is cyclic if and only if $\psi(N) > 0$.

(ii) Prove that

$$\sum_{d|N} \psi(d) = N.$$

(iii) Suppose that for every divisor d of N, there is a unique subgroup H in G of order d. Prove that $\psi(d) \leq \varphi(d)$ and that G is a cyclic group.

Proof. 1. If $d \nmid N$, by Lagrange's theorem, the order of any element in G must divide the order of the group N. Therefore, there cannot be any elements of order d, which implies:

$$\psi(d) = 0.$$

For the second part, G is cyclic if and only if there exists an element $g \in G$ such that the order of g is equal to N. This means that there is at least one element of order N. Thus, if G is cyclic, $\psi(N) > 0$. Conversely, if $\psi(N) > 0$, then there exists at least one element of order N, which generates G, making G cyclic.

2. Each element of G has a well-defined order d, and by the class equation, each element of order d contributes to $\psi(d)$ for each divisor d of N. The elements of order d can be grouped according to their orders. Since the order of each element divides N, the total number of elements, summed over all divisors of N, must equal N:

$$\sum_{d|N} \psi(d) = N.$$

3. If there is a unique subgroup H of order d, then by the properties of groups, all elements in H must have the same order d (or orders that divide d). Specifically, if g is a generator of H, then all elements of H can be expressed as g^k for $k = 0, 1, \ldots, d-1$.

   Since H has $\varphi(d)$ elements of order d (where φ is the Euler's totient function), it follows that:

$$\psi(d) \leq \varphi(d).$$

   Furthermore, since there is a unique subgroup for each divisor d of N, the presence of an element of order N guarantees that G is cyclic. Thus, if $\psi(N) > 0$, it implies G is cyclic because it can be generated by a single element of order N.

□