Past Paper: Group Theory (2022)

Rashid M. Talha

Question 1 (a).

Definition: A group G is called cyclic if there exists $g \in G$ such that every element of G can be written in the form g^n for some $n \in \mathbb{Z}$.

Infinite cyclic: The group $\mathbb{Z}$ of integers with the usual addition is an infinite cyclic group generated by 1.

Finite cyclic: The group $(\mathbb{Z}_3, +_3)$ of integers with addition modulo 3 is a finite cyclic group generated by [1]. The group $(\mathbb{Z}_5, +_5)$ of integers with addition modulo 5 is a finite cyclic group generated by [1].

Question 1 (b).

Consider the group $\mathbb{Z}$ with the usual addition. Both $2\mathbb{Z}$ and $3\mathbb{Z}$ are subgroups of $\mathbb{Z}$.

Let, $F = 2\mathbb{Z} \cup 3\mathbb{Z}$. Then, $2, 3 \in F$ but $2 + 3 = 5 \notin F$. So, F is not closed under the group operation. Therefore, $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $\mathbb{Z}$.

Question 2 (a).

Firstly, the set H is non-empty because $a^0 = e \in H$.

Next, take any $x, y \in H$. Then, we can write $x = a^p$ and $y = a^q$ for some $p, q \in \mathbb{Z}$. So,

$$xy^{-1} = a^p a^{-q} = a^{p-q} \in H$$

because $p - q \in \mathbb{Z}$. Therefore, by the subgroup criteria, $H \leq G$.

Question 2 (b).

Let $G = (\mathbb{C}, +)$ and $H = \{a + bi \mid a, b \in \mathbb{R}, ab \geq 0\}$.

Take $z_1 = -2 + 0i$ and $z_2 = 1 + 1i$. We note that $z_1 \in H$ because $-2, 0 \in R$ and $(-2)(0) = 0 \geq 0$. Also, $z_2 \in H$ because $1 \in R$ and $(1)(1) = 1 \geq 0$.

However, $z_1 + z_2 = -1 + 1i \notin H$ because $(-1)(1) = -1 \ngeq 0$.

So, H is not closed under the group operation. Therefore, H is not a subgroup of G.

Question 3.

Let H be a non-empty subset of G.

Suppose $H \leq G$. Take any $a, b \in H$. Then, $b^{-1} \in H$ by the existence of inverses, and $ab^{-1} \in H$ by the closure property.

Conversely, suppose $ab^{-1} \in H$ for all $a, b \in H$.

- (Associativity.) H has the same binary operator as G, so it inherits associativity.
- (Identity.) As $H \neq \emptyset$, we have some $a \in H$. Therefore, $aa^{-1} \in H \implies e \in H$.
- (Inverses.) Take any $a \in H$, so $e, a \in H$ and $ea^{-1} \in H \implies a^{-1} \in H$.
- (Closure.) Take any $a, b \in H$. Then, $b^{-1} \in H$. So, $a(b^{-1})^{-1} = ab \in H$.

Therefore, H is a subgroup of G.

Question 4.

Definition: Let G be a group and $g \in G$. The order of g is the smallest positive integer n such that $g^n = e$, the identity element of G.

The order of each element in $\mathbb{Z}_{12}$ is

$$\begin{array}{llll} O(0) = 1 & O(1) = 12 & O(2) = 6 & O(3) = 4 \\ O(4) = 3 & O(5) = 12 & O(6) = 2 & O(7) = 12 \\ O(8) = 3 & O(9) = 4 & O(10) = 6 & O(11) = 12 \end{array}$$

Question 5 (a).

Let G be a group and $a \in G$. By the existence of inverses, $a^{-1} \in G$ such that $aa^{-1} = e$. Again, by the existence of inverses, $(a^{-1})^{-1} \in H$ such that $(a^{-1})(a^{-1})^{-1} = e$. So,

$$(a^{-1})^{-1} = e(a^{-1})^{-1} = (aa^{-1})(a^{-1})^{-1} = a(a^{-1}(a^{-1})^{-1}) = ae = a.$$

We used the properties of e and associativity in the last step.

Question 5 (a).

Let G be a group and $a, b \in G$. Then, $ab \in G$ by closure. By the existence of inverses $(ab)^{-1} \in G$ such that $(ab)(ab)^{-1} = (ab)^{-1}(ab) = e$.

Now, $(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$.

And, $(b^{-1}a^{-1})(ab) = (b^{-1}(a^{-1}a))b = (b^{-1}e)b = b^{-1}b = e$.

So, $(b^{-1}a^{-1})$ is also an inverse of ab. By the uniqueness of inverses $(b^{-1}a^{-1}) = (ab)^{-1}$.

Question 5 (c).

Firstly, by definition, $(a^{-1}ba)^5 = (a^{-1}ba)(a^{-1}ba)(a^{-1}ba)(a^{-1}ba)(a^{-1}ba)$.

So, by associativity, we can write

$$\begin{aligned} (a^{-1}ba)^5 &= (a^{-1}ba)(a^{-1}ba)(a^{-1}ba)(a^{-1}ba)(a^{-1}ba) \\ &= a^{-1}baa^{-1}baa^{-1}baa^{-1}baa^{-1}ba \\ &= a^{-1}(b(aa^{-1}))(b(aa^{-1}))(b(aa^{-1}))(b(aa^{-1}))ba \\ &= a^{-1}(be)(be)(be)(be)ba \\ &= a^{-1}bbbbba \\ &= a^{-1}b^5a \end{aligned}$$