Name and Roll No.: ________________________

Answer the questions in the spaces provided on the question paper. You can use the additional sheets for rough work.

Question No.:	1	2	3	4	5	**Total**
Marks:	3	3	4	5	5	20
Score:						

1. A binary operation $*$ on a finite set S can be represented by a square grid where rows and columns are indexed by elements of S; and the entry in the row corresponding to a and the column corresponding to b is $a * b$. For example, $(\mathbb{Z}/5\mathbb{Z}, \times)$ can be represented by the following grid: [3]

$$\begin{array}{c|cccc} \times & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \hline \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{2} & \overline{2} & \overline{4} & \overline{1} & \overline{3} \\ \overline{3} & \overline{3} & \overline{1} & \overline{4} & \overline{2} \\ \overline{4} & \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{array}$$

If $(G, *)$ is a group and G is a finite set, prove that every row and every column of its grid is a permutation of the elements of G.

Solution: We first show that no row has duplicate elements. For the sake of contradiction, suppose there is a row (say row indexed by a) with duplicate elements. Let the columns corresponding to these elements be indexed by b and c respectively where $b \neq c$. So, $a * b = a * c$. This implies $a^{-1} * a * b = a^{-1} * a * c$. So, $b = c$. This contradicts the fact that $b \neq c$. So, our assumption that there is a row with with duplicate elements is false.

The proof for columns is similar.

Since every row and every column contains n elements and there are no duplicates, every row and every column is a permutation of the elements of the group.

2. What is wrong with the following proof: [3]

Theorem. *All horses are of the same colour.*

Proof. We prove the theorem by induction on the number of horses.
Base case: If there is only one horse, the theorem is trivial.
Inductive step: Suppose the theorem is true for $n-1$ horses i.e. every horse in a group of $n-1$ horses is of the same colour. Now consider a group of n horses. By induction hypothesis, horses $1, 2, \ldots, n-1$ are of the same colour. Similarly, by induction hypothesis, horses $2, 3, \ldots, n$ are of the same colour. Therefore horses 1 and n are also of the same colour. So horses $1, 2, \ldots n$ are of the same colour. This completes the proof. □

Solution: If $n = 2$, the sets $\{1, \ldots, n-1\}$ and $\{2, \ldots, n\}$ do not intersect; and so it cannot be inferred that horses 1 and n have the same colour. So, the *Inductive Step* fails for $n = 2$.

3. Suppose $(G, *)$ is a group and H is a non-empty subset of G. Suppose for all a, b in H, $a * b^{-1}$ is also in H. Prove that $(H, *)$ is a group. $\boxed{4}$

Solution:

- *Identity element:* Since $H \neq \varnothing$, there exists an element in H. Let this element be called a. Since $a \in H$, $a * a^{-1} = e \in H$. Therefore H contains the identity element.
- *Inverse:* Let $a \in H$. We have to show that $a^{-1} \in H$. Since $e, a \in H$, so $e * a^{-1} = a^{-1} \in H$.
- *Closure:* Let $a, b \in H$. We have to show that $a * b \in H$. Since $b \in H$, $b^{-1} \in H$. Since $a, b^{-1} \in H$, $a * (b^{-1})^{-1} = a * b \in H$.
- *Associativity:* Since $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$, and since H is a subset of G, $(a * b) * c = a * (b * c)$ for all $a, b, c \in H$.

4. Recall $\mathbb{R}[x]$ is the set of polynomials with Real coefficients and non-negative degree. We can define congruence relation on $\mathbb{R}[x]$. We say two polynomials f and g are congruent modulo a polynomial h if h divides $f - g$. Given $h \in \mathbb{R}[x]$, we can define $\mathbb{R}[x]/h\mathbb{R}[x]$ analogous to $\mathbb{Z}/m\mathbb{Z}$.

(a) What are the elements of the set $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$? $\boxed{1}$

Solution: Given $f \in \mathbb{R}[x]$, let $\overline{f} = \{g \in \mathbb{R}[x] \mid f \equiv g \pmod{x^2+1}\}$, Then $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is defined as follows: $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x] = \{\overline{f} \mid f \text{ is a polynomial of degree less than } 2\}$.

Notice that all zero degree polynomials (i.e. Real numbers) lie in different congruence classes. If $a \neq b$, polynomials $x + a$ and $x + b$ lie in different congruence classes. If a, α and β are Real numbers, then polynomials $x + a$ and $\alpha(x^2+1) + \beta(x + a)$ lie in the same congruence class.

(b) How are operations $+$ and $\times$ defined on $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$? $\boxed{1}$

Solution: $\overline{f} + \overline{g} \overset{def}{=} \overline{f+g}$ and $\overline{f} \times \overline{g} \overset{def}{=} \overline{f \times g}$

If we have to add two congruence classes $\overline{f}$ and $\overline{g}$, we add polynomials f and g and return the corresponding congruence class $\overline{f+g}$. Since the degree of $f + g$ is less than 2 if the degree of both f and g is less than 2, so $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is closed under $+$.

If we have to multiply two congruence classes $\overline{f}$ and $\overline{g}$, we multiply polynomials f and g and return the corresponding congruence class $\overline{f \times g}$. If the degree of $f \times g$ is greater than or equal to 2, then there is another polynomial h of degree less than 2 such that $\overline{f \times g} = \overline{h}$. Therefore, $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is closed under $\times$.

(c) Is $\Big(\big(\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]\big) - \{0\}, \times\Big)$ a group? Why / Why not? $\boxed{3}$

Solution: Yes, it is a group.

- *Closure:* Proved in the previous part.
- *Associativity:* Proof similar to $\mathbb{Z}/m\mathbb{Z}$.
- *Identity:* Identity element is $\overline{1}$.
- *Inverse:* Given $f \in \mathbb{R}[x]/h\mathbb{R}[x]$, it can be shown that equation $\overline{f} \times \overline{X} = \overline{1}$ has a solution in $\mathbb{R}[x]/h\mathbb{R}[x]$ if $\gcd(f, h)$ is a unit. Since $x^2 + 1$ is a irreducible, every polynomial f of degree less than $x^2 + 1$ satisfies $\gcd(f, x^2+1)$ is a unit. Therefore every element of $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ has an inverse.

5. Let $+$ denote the usual addition operation on integers. Let $a, b \in \mathbb{Z}$.

   (a) Is there a proper subset S of $\mathbb{Z}$ containing a and b such that $(S, +)$ is a group. If yes, give the subset; otherwise prove that such a subset doesn't exist. $\boxed{2}$

   > **Solution:** $S = \{ax + by \mid x, y \in \mathbb{Z}\}$ is the smallest subset of $\mathbb{Z}$ containing a and b which is a group. This is a proper subset of $\mathbb{Z}$ if $\gcd(a, b) \neq 1$.

   (b) Given a group $(G, +)$. An element $g \in G$ is called a generator of the group if $G = \{ig \mid i \in \mathbb{Z}\}$. [Note: Here na is a shorthand for $\underbrace{a + a + \cdots + a}_{n \text{ times}}$]. Does $(S, +)$ (defined in the previous part of the question) have a generator? If yes, give the generator; otherwise prove it doesn't exist. $\boxed{3}$

   > **Solution:** If $\gcd(a, b) \neq 1$, then $(S, +)$ is a group and $\gcd(a, b)$ is a generator.