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.

2. What is wrong with the following proof: $\boxed{3}$

   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. $\square$

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. $\boxed{4}$

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 $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$? $\boxed{1}$

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

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

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. $\boxed{2}$

   (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. $\boxed{3}$