Quiz 3
Sample Solutions

Name: ______________________________

Student Number: ______________________________

In the space provided, please write your solutions to the following exercises. *Fully explain your reasoning.* Remember to use good notation and full sentences.

Good Luck!

1. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

   Solution: Since $\gcd(a, b) = 1$, there exist integers x and y such that
   $$ax + by = 1.$$
   Thus,
   $$acx + bcy = c.$$
   Now $a|bc$ and so there exists $k \in \mathbb{Z}$ such that $bc = ak$. Hence,
   $$acx + aky = a(cx + ky) = c.$$
   We conclude that $a|c$.

 Turn over for Exercise (2)...

2. Let G be a set.

(i) Complete the following definition: A *binary operation* on G is

Solution: a function $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$ in G.

(ii) Let $G = \mathbb{R}^* \times \mathbb{Z}$ where $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Define a binary operation $\circ$ on G by

$$(a, m) \circ (b, n) = (ab, m + n).$$

Show that G is a group under this operation. *You may assume without verification that $\circ$ is indeed a binary operation.*

Solution: We are given that the operation $\circ$ is a binary operation. We now check the three remaining axioms of a group.

- <u>Associativity:</u> Let $(a, m), (b, n)$ and (c, l) be elements of G. Then

$$(a, m) \circ ((b, n) \circ (c, l)) = (a, m) \circ (bc, n + l) = (abc, m + n + l)$$

and

$$((a, m) \circ (b, n)) \circ (c, l) = (ab, m + n) \circ (c, l) = (abc, m + n + l).$$

Since the two above quantities are equal, the binary operation is associative.

- <u>Identity Element:</u> Consider $(1, 0) \in G$. For all $(a, m) \in G$, we have

$$(a, m) \circ (1, 0) = (a \cdot 1, m + 0) = (a, m)$$

and

$$(1, 0) \circ (a, m) = (1 \cdot a, 0 + m) = (a, m).$$

Hence, by definition, $(1, 0)$ is the identity element of G.

- <u>Inverse Elements:</u> Let $(a, m) \in G$. Consider $(1/a, -m) \in G$. Observe that

$$(a, m) \circ (1/a, -m) = (a \cdot 1/a, m - m) = (1, 0)$$

and

$$(1/a, -m) \circ (a, m) = (1/a \cdot a, -m + m) = (1, 0).$$

Thus, (a, m) has the inverse element $(1/a, -m)$.