Name ____ Quiz 4

Using only the definition and facts about rings below, prove the theorems below.

Definition D1: A ring is a set of elements with two binary operations, called addition and multiplication, such that:

- Addition is closed
- Addition is commutative
- Addition is associative
- There exists an additive identity. (Do NOT call it 0 unless we have the uniqueness theorem)
- There exist additive inverses (Do NOT call them $-a$ unless we have the uniqueness theorem)
- Multiplication is closed
- Multiplication is associative
- Multiplication distributes over addition

Definition D2: Let R be a ring and $S \subseteq R$. S is said to be a subring of R if S is itself a ring with the same operations as R.

1) Let a, b, and c be elements of a ring R. Assume $a + b = a + c$, and prove that $b = c$.
(This is theorem T1. You cannot use theorems T2+ on this problem)

Proof: Because $a \in R$, we know that it has an addititve inverse, $d \in R$, such that $a + d = d + a = I$, where I is an additive identity.

$$a + b = a + c$$
$$\therefore d + a + b = d + a + c$$
$$\therefore I + b = I + c$$
$$\therefore b = c$$

Theorem T2: Let a and b be elements of a ring R. Then $a + x = b$ always has a unique solution.

Theorem T3: Let R be a ring. If $a + 0_1 = a$ and $a + 0_2 = a$ for all elements $a \in R$, then $0_1 = 0_2$.

Theorem T4: For each element a in a ring R, it's additive inverse is unique.

Theorem T5: Let a be an element of a ring R and denote the additive identity as 0. Then $a \cdot 0 = 0 \cdot a = 0$.

Theorem T6: Let R be a ring and let $a, b \in R$. Denote the additive inverse of each element $c \in R$ as $-c$, no matter what c is. Then $a(-b) = (-a)b = -(ab)$.

Theorem T7: Let R be a ring, and S a subset of R. S is a subring if and only if all of the following are satisfied for all elements $a, b \in S$:

1. $S \neq \emptyset$
2. $a, b \in S \Rightarrow a + b \in S$
3. $a, b \in S \Rightarrow a \cdot b \in S$
4. $a \in S \Rightarrow -a \in S$

2) Prove that $2\mathbb{Z}$ is a ring.

Proof: Note that $2\mathbb{Z} \subseteq \mathbb{Z}$, which is a ring. Hence we can use the subring theorem, T7, above.

1) $2 = 2 \cdot 1 \in 2\mathbb{Z}$, and so $2\mathbb{Z} \neq \emptyset$

Let $a, b \in 2\mathbb{Z}$, that means that we can write $a = 2k$ and $b = 2l$ for some $k, l \in \mathbb{Z}$.

2) $a + b = 2k + 2l = 2(k + l) \in 2\mathbb{Z}$.

3) $ab = (2k)(2l) = 4kl = 2(2kl) \in 2\mathbb{Z}$.

4) $-a = -2k = 2(-k) \in 2\mathbb{Z}$.