Name ____ Quiz 8

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.

Theorem T1: Let a, b, and c be elements of a ring R. If $a + b = a + c$, then $b = c$.

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. $a \in S \Rightarrow -a \in S$

Definition D2: Let R be a ring. A multiplicative identity of R is an element $s \in R$ such that $sr = rs = r$ for all $r \in R$. (Do NOT call it "1" until you justify that notation by proving that it is unique.)

Theorem T8: Let R be a ring. If R has a multiplicative identity, then it is unique.

Definition D3: Let R and S be rings. A function $\varphi: R \to S$ is called a ring homomorphism if is satisfies:

1. $\varphi(r+s) = \varphi(r) + \varphi(s)$ for all $r, s \in R$.
2. $\varphi(rs) = \varphi(r)\varphi(s)$ for all $r, s \in R$.

Definition D4: Let R and S be rings. A ring homomorphism $\varphi: R \to S$ is called a ring isomorphism if is also one-to-one and onto. In this case R and S have an identical structure as rings.

Definition D5: Let R be a ring. An element $b \neq 0$ in R is called a zero divisor if there is another nonzero element $a \in R$ such that $ab = 0$.

Definition D6: A ring that is commutative with unity and no zero divisors is called an integral domain.

Theorem T9: Let R be an integral domain and suppose $a \neq 0$. If $ab = ac$, then $b = c$.

Definition D7: Let R be a ring with unity and $x \in R$. If there is some element $y \in R$ such that $xy = 1$, we say that x is invertible, or a unit. The set of all units of R is denoted either $U(R)$ or R^*.

Definition D8: Let R be a commutative ring and $a, b \in R$. We say that a and b are associates of each other if there is some $u \in R^*$ such that $a = ub$.

Definition D9: An integral domain in which every nonzero element is invertible is called a field.

Theorem T10: $x \in \mathbb{Z}_m$ is a unit if and only if $\gcd(x, m) = 1$.

Theorem T11: Let n be an integer at least 2. $\mathbb{Z}_n$ is a field if and only if p is prime.

Theorem T12: Let p be a prime number and $0 \neq x \in \mathbb{Z}_p$. Then $x^{p-1} = 1$ in $\mathbb{Z}_p$.

Theorem T13: Let R be a finite integral domain. Then R is a field.

Problem 1) Prove Theorem T12.

Problem 2) Suppose R_1 and R_2 are rings with 15 and 18 elements, respectively. Is it possible that R_1 is isomorphic to R_2? Justify your answer.