Definition 13.1 (Zero Divisor). *Let R a commutative ring, a non-zero element $a \in R$ is a zero-divisor, if there is a non-zero element $b \in R$ such that $ab = 0$.*

Definition 13.2 (Integral Domain). *Let R a commutative ring with unity, R is integral domain if there is no zero-divisor.*

It is equivalent to define integral domain by $ab = 0$ implies $a = 0$ or $b = 0$ instead of zero-divisor.

Lemma 13.1. *Let R a integral domain, then for any $a\ b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.*

Proof. Newline please!!

- If $a = 0$, then trivial.
- If $a \neq 0$ and $b = 0$, then trivial.
- If $a \neq 0$ and $b \neq 0$, then a is a zero-divisor, which contradict the definition of integral domain.

$\square$

Theorem 13.1 (Cancellation). *Let R a integral domain, for any $a\ b\ c \in R$, if $a \neq 0$ and $ab = ac$, then $b = c$.*

Proof. $ab = ac \to ab - ac = 0 \to a(b - c) = 0$, since $a \neq 0$, we know $b - c = 0$ and then $b = c$. $\square$

Definition 13.3 (Field). *Let R a commutative ring with unity, R is field if every non-zero element in R are unit.*

Lemma 13.2 (Fields are Integral domains). *Let R a field, then R is also a integral domain.*

Proof. Let $a \in R$ and $a \neq 0$, then for any $b \in R$, $ab = 0 \to a^{-1}ab = a^{-1}0 \to b = 0$. $\square$

Theorem 13.2 (Finite Integral domains are Fields). *Let R a finite integral domain, then R is field.*

Proof. For any non-zero element $a \in R$, the mapping $f(b) = ab : R \to R$ is one-to-one by Theorem 13.1. Since R is finite, then f is also onto, therefore $aR = R$. By Exercise 12.60, we know R has a unity and every non-zero element are unit. Therefore R is a field.

The following solution comes from textbook.

For any non-zero element $a \in R$, consider the sequence a^1 a^2 a^2 $\ldots$, since R is finite, there must be $a^i = a^j$ where $i = j + k$ where $k > 0$. Then $a^i = a^{j+k} = a^j a^k = a^j 1$ implies $a^k = 1$ by cancellation, therefore $a^{k-1}a = a^k = 1$ and a^{k-1} is the inverse of a. □

Corollary 13.1. *Z_p is field.*

Proof. For any non-zero element $a \in Z_p$, and $b \in Z_p$, if $ab = 0$, then

- If $b = 0$, everything is good.
- If $b \neq 0$, then a $b \in U(p)$, however, $0 \notin U(p)$, so $ab \neq 0$.

Therefore, Z_p has no zero-divisor, then Z_p is integral domain. By Theorem 13.2, Z_p is field. □

Definition 13.4 (Characteristic)**.** *The* ***characteristic*** *of a ring R is the least positive integer n such that $n \cdot x = 0$ for all $x \in R$. If no such n exists, we say R has characteristic 0. The characteristic of R is denoted by* $\operatorname{char} R$

Theorem 13.3. *Let R be a ring with unity. If the order under addition of 1 is infinite, then $\operatorname{char} R = 0$. If the order under addition of 1 is n, then $\operatorname{char} R = n$.*

Proof. If $|1| = \infty$, so there is no positive integer n such that $n \cdot 1 = 0$, so $\operatorname{char} R = 0$. If $|1| = n$, then for any $a \in R$, $n \cdot 1 = 0 \to (n \cdot 1)a = 0a \to n \cdot (1a) = 0 \to n \cdot a = 0$. Therefore $\operatorname{char} R = n$. □

Theorem 13.4 (Characteristic of Integral domain)**.** *The characteristic of a integral domain is 0 or prime.*

Proof. Let R a integral domain, if $|i| = \infty$ or $|i| = n$ and n is prime, then trivial. We focus on $|i| = n$ but n is not prime. Note that $n \neq 1$ which implies $1 = 0$.

Since n is not prime, then $n = ij$ where i and j are positive integers but not 1. $(ij) \cdot 1 = 0 \to (ij) \cdot 11 = 0 \to (i \cdot 1)(j \cdot 1) = 0$ where $i \cdot 1$ and $j \cdot 1$ are not 0, since $|1| = ij$ and $i < |1|$ and $j < |1|$. This contradict the definition of integral domain.

The following solution comes from textbook, I think it is better than mine.

We need to show if $|1| = n$ then n is prime. Let s be a divisor of n, then $n = st$ where $1 \leq s, t \leq n$. Then $n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1) = 0$, which implies $s \cdot 1 = 0$ or $t \cdot 1 = 0$. But n is the least integer such that $n \cdot 1 = 0$, therefore $s = n$ or $t = n$ (then $s = 1$). From this, we conclude that any divisor of n is either 1 or n, therefore n is prime. $\square$