Integral Domain and Field

Definition. Let R be a ring and $0 \neq a \in R$, then a is said to be ***zero divisor*** if there is $0 \neq b \in R$ such that a.b. = 0.

Example. In a ring of integers modulo $6(\mathbb{Z}_6, +_6, ._6)$, $\bar{2}.\bar{3} = \bar{0}$ and $\bar{3}.\bar{4} = \bar{0}$, then $\bar{2}, \bar{3}, \bar{4}$ are zero divisors.

Remarks. In a ring R,

1. $0 \neq a \in R$, then a is said to be ***nonzero divisor*** if $\nexists$ $0 \neq b \in R$ such that a.b = 0.
2. 0, 1 are nonzero divisor.
3. Any invertible element in any ring R is nonzero divisor (any element in $\mathbb{Z}_5$ is invertible).

Proof 2. Let 1 be the identity element of (R, .) and suppose that 1 is zero divisor element in R $\rightarrow \exists\ 0 \neq b \in R$ such that 1.b = 0. But 1.b = 0 $\rightarrow$ b = 0 C!

$\therefore$1 is nonzero divisor.

(in the same way 0 is nonzero divisor)

Proof 3. Let a be invertible element in R $\rightarrow \exists\ a^{-1} \in R$ such that $a.a^{-1} = a^{-1}.a = 1$. Suppose that a is zero divisor element in R $\rightarrow \exists\ 0 \neq b \in R$ such that a.b = 0 $\rightarrow a^{-1}.a.b = a^{-1}.0$

$\rightarrow$ 1.b = 0 and by (1), 1 is nonzero divisor $\rightarrow$ b = 0 C!

$\therefore$ a is nonzero divisor.

Theorem. A ring R has no zero divisors iff R satisfies the cancellation laws for multiplication (i.e for all a, b, $c \in R$ if ab = ac with $a \neq 0$, then b = c).

Proof. ⟹) Suppose that R has no zero divisors and ab = ac with a≠0 → ab – ac =0 → a(b - c) = 0. Since R has no zero divisor, then b - c = 0 → b = c.

⟸) Suppose that R satisfies the cancellation laws and 0≠a∈R such that a.b = 0 = a.0 → b = 0.

Examples.

1. $(\mathbb{Z}_n, +_n, \cdot_n)$ has no zero divisor iff n is prime.

Proof. **⟹)** suppose that $\mathbb{Z}_n$ has no zero divisors

i.e. for all 0≠a,b ∈ $\mathbb{Z}_n$ if a.b ≠ 0→ a.b ≠ n → n is prime.

⟸) suppose that $\mathbb{Z}_n$ has zero divisors

i.e. ∃ 0≠a,b ∈ $\mathbb{Z}_n$ such that a.b = 0→ a.b = kn.

But n is prime →n\a.b→ either n\a or n\b→ either a=0 or b=0 C! (n cannot be decomposable with n>a and n>b) → $\mathbb{Z}_n$ has no zero divisors.

2. (ℤ, +, .) has nonzero divisors (since for all a, b ∈ ℤ, if a.b=0 , then either a = 0 or b = 0).

Definition. A ring R is said to be ***integral domain*** if R is commutative ring with identity and has no zero divisors.

H.W. Every integral domain satisfies the cancellation laws.

Examples.

1. Each of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2})$ is an integral domain.
2. The ring $\mathbb{Z}_p$(p is prime) is an integral domain.

Proof. ⟸) let p be a prime number. Then the ring $\mathbb{Z}_p$ has no zero divisors and commutative ring with identity.

$\therefore (\mathbb{Z}_p, +_p, \cdot_p)$ is an integral domain.

Suppose that $\mathbb{Z}_p$ is an integral domain and p is not prime.

i.e. $p = p_1.p_2$ and $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ with $p = 0 \rightarrow p = p_1.p_2 = 0$. Since $\mathbb{Z}_p$ is integral domain, then either $p_1=0$ and so $p=p_1$ or $p_2=0$ and so $p=p_2 \rightarrow$ p is prime.

3. $\mathbb{Z}_e$ is no integral domain since it has no identity.
4. The commutative ring $\mathbb{Z}(i)$ with identity 1+0i is an integral domain.

Proof. Let x = a + bi and y = c + di with $x \neq y \in \mathbb{Z}(i)$ such that xy = 0 $\rightarrow$ (a + bi)(c + di) = (ac - bd) + (ad + bc)i

= 0

= 0 + 0i

$\rightarrow$ ac - bd = 0 $\rightarrow$ ac = bd

and

ad + bc = 0 $\rightarrow$ ad = bc $\rightarrow$ $d = \frac{-bc}{a}$ $\rightarrow$ $ac = b(\frac{-bc}{a}) \rightarrow a^2c = -b^2c \rightarrow (a^2 + b^2)c = 0 \rightarrow$ either $a^2 + b^2 = 0$ or c = 0.

If c = 0$\rightarrow$ d = 0 $\rightarrow$ y = c + di =0 $\rightarrow$ $\mathbb{Z}(i)$ is an integral domain

or $a^2 + b^2 = 0 \rightarrow a = b = 0 \rightarrow x = a + bi = 0 \rightarrow \mathbb{Z}(i)$ is an integral domain.

5. The ring $M_2(\mathbb{Z})$ is not integral domain.

Proof. since $M_2(\mathbb{Z})$ is not commutative ring(why?) and one can find A, B $\in M_2(\mathbb{Z})$ such that AB = 0 with $A \neq 0$ and B≠0 ($\exists\, A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is zero divisor in the ring $M_2(\mathbb{Z})$ (prove that).

H.W. The subring of integral domain needed not integral domain.

Remarks.

1. Every nonzero nilpotent element is zero divisors.
   Proof. Let $0 \neq a \in R$ be a nilpotent element and n be the smallest positive integer such that $a^n = 0 \rightarrow a^k = 0, \ \forall\, k > n$.
   Now, $a^n = 0 \rightarrow a^n = a \,.\, a^{n-1} = 0$. But $a^{n-1} \neq 0$ (since $n-1 < n$ and n is the smallest integer with $a^n = 0$)
   $\therefore \forall\, a \neq 0, \exists\, b = a^{n-1} \neq 0$ such that $a \,.\, b = a \,.\, a^{n-1} = 0$.

   $\therefore$ a is zero divisor

2. The converse of (1) is not true in general; for example: in $\mathbb{Z}_6$, the element $\bar{2}$ is zero divisor but $\bar{2}$ is not nilpotent element in $\mathbb{Z}_6$ (since $\nexists\, n \in \mathbb{Z}^+$ such that $(\bar{2})^n = 0$).
3. The nilpotent element in an integral domain is zero.
   Proof. Suppose that $a \neq 0$ is a nilpotent element in an integral domain R. $\therefore$ a is zero divisors (by (1)). But R has no nonzero divisors $\rightarrow a = 0$.
4. Let R be a ring with identity and a nilpotent in R, then 1+a has an inverse.
   Proof. Let $0 \neq a$ be a nilpotent element in $R \rightarrow \exists$ a smallest positive integer n such that $a^n = 0$. Now to prove $1 + a$ has inverse, must be find an element $b \in R$ such that $(1 + a)b = 1$.
   Claim that $b = 1-a+a^2 - \ldots + (-1)^{n-1} a^{n-1}$ satisfy $(1 + a)b = 1$.
   $\therefore (1+a)b = (1 + a)(1-a+a^2 - \ldots + (-1)^{n-1} a^{n-1})$
   $= 1-a+a^2 - \ldots + (-1)^{n-1} a^{n-1} + a-a^2 - \ldots + (-1)^{n-2} a^{n-1} + (-1)^{n-1} a^n$
   $= 1$ (since $a^n = 0 \rightarrow (-1)^{n-1} a^n = 0$)
   $\therefore$ b is the inverse element of $1 + a$

Problems. Prove the following:

1. The only idempotent element in an integral domain is 0, 1.
2. Let R be a ring and a an idempotent element in R, then $a^n = a$ for all n ∈ R.
3. A nonzero idempotent element cannot be nilpotent element.
4. The set of all nilpotent elements of a commutative ring is a subring in R.

Every nonzero element in $\mathbb{Z}_n$ is either zero divisor or has inverse.

Definition. A commutative ring with identity (R, +, .) is said to be ***field*** if every nonzero element has inverse.

Remark. If (F, +, .) field, then :

1. (F, +, .) is an abelian group.
2. (F^*, +, .) is an abelian group.
3. for all a, b, c ∈ F
   a. (b + c) = ab + ac and (a + c) .a = ba + ca

Theorem. Every field is an integral domain.

Proof. Let F be a field and 0 ≠ a ∈ F such that ab=0 with b ≠ 0.

∵ F field → a has inverse element say a^{-1} → $a^{-1}(ab) = 0$ → 1.b = 0 → b = 0 C! (b ≠ 0) → F has no zero divisor. Farther more, F is commutative ring with identity → F is integral domain

Remark. The converse of the previous theorem is not true in general as the following example.

Example. The ring (ℤ, +, .) is an integral domain which is not field since there is a = 2 ∈ ℤ has no inverse in ℤ.

The following theorem gives the necessary condition for the converse:

Theorem. Every finite integral domain is field.

Proof. Let (R, +, .) be a finite integral domain

Suppose that $R = \{a_1, a_2, \ldots, a_n\}$. Let $0 \neq a \in R$ be a fixed element, then consider the n product $aa_1, aa_2, \ldots, aa_n$: these product are distance. If not: $aa_i=aa_j$, by the cancellation law $a_i=a_j \rightarrow R = \{aa_1, aa_2, \ldots, aa_n\} \rightarrow \exists\ 1 \leq i \leq n$ such that $aa_i = 1$ and $a_ia = 1$ (R is commutative) $\rightarrow a^{-1} = a_i \rightarrow$ every nonzero element has inverse in R $\rightarrow$ (R, +, .) field.

Example. Each of $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{p})$ (p is prime) is a field.

Definition. In a field (F, +, .) the nonempty subset A of F is said to be ***subfield*** if (E, +, .) is field.

Examples.

1. $\mathbb{Q}$ is subfield of $\mathbb{R}$ and $\mathbb{C}$.
2. $\mathbb{R}$ is subfield of $\mathbb{C}$.
3. $\mathbb{Q}(\sqrt{p})$ is subfield of $\mathbb{R}$ for all prime p.
4. $\mathbb{Q}(\sqrt{3})$ is not subfield of $\mathbb{Q}$.
5. $\mathbb{Z}_3$ is not subfield of $\mathbb{Z}_5$(since $\mathbb{Z}_5$ has no proper subring).

Remark. If F_1 and F_2 are subfields of F, then $F_1 \cap F_2$ is subfield of F with $F_1, F_2 \neq F$.

Characteristic of the ring

Definition. let R be a ring. If there exist a positive integer n such that na=0 for all a ∈ R, then the smallest positive integers with this property is called ***Characteristic of the ring R***. If no such positive integers exists, then is said to be ***characteristic of zero*** (i.e charR = 0).

Examples.

1. char($\mathbb{R}$) = char($\mathbb{Q}$) = char($\mathbb{Z}$) = 0
2. char($\mathbb{Z}_n$) = n
3. char($\mathbb{Z}_6$) = 6
4. char(P(X), Δ, ∩) = 2 (because 2A = AΔA = (A-A)∪(A-A) = ∅.

Remarks.

1. If char R = 0, then R is an infinite (for examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$).
2. If char R = n, then the characteristic for any subring of R is equal or less than n.
3. Characteristic for finite ring R divisible order R(i.e: char R\ o(R)).

Theorem. Let R be a ring with identity then char R= n > 0 if and only if n is n the smallest positive integer such that n.1 = 0.

Proof. ⟹) suppose that, char R = n, then na = 0, ∀ a ∈ R.

Since 1 ∈ R → n.1 = 0. Suppose that ∃ m ∈ $\mathbb{Z}$ such that 0 < m < n with m.1 = 0.

∴ m.a = m(1. a) = (m.1). a = 0. A , ∀ a∈ R.

∴ m.a = 0

$\because$ $0 < m < n$ and $m.a = 0 \rightarrow$ char R = m C! (char R = n)

$\therefore$ n is the smallest positive integer.

$\Leftarrow$) Let $0 \neq a \in R$. Since $na = n(1.a) = (n.1) \,.\, a = 0 \,.\, a = 0$.

$\therefore$ char R = n

Theorem. If R is an integral domain, then char R is either 0 or prime number.

Proof. Suppose that char R = n > 0 and to prove char R = prime number.

Suppose n is not prime $\rightarrow$ char R = n_1n_2 such that $1 < n_1 < n_2 < n$.

$\because$ R is ring with identity $\rightarrow$ n_1n_2 is the smallest positive integer such that $(n_1n_2) \,.\, 1 = 0 \rightarrow n \,.\, 1 = (n_1n_2)(1 \,.\, 1) = (n_1 \,.\, 1)(n_2 \,.\, 1) = 0$

$\because$ $(n_1 \,.\, 1)(n_2 \,.\, 1) \in R$

$\because$ R is an integral domain $\rightarrow$ R has no zero divisors.

$\therefore$ either $n_1 \,.\, 1 = 0$ or $n_2 \,.\, 1 = 0$.

$\therefore$ either char R = n_1 or char R = n_2.

But $n_1 < n$ and $n_2 < n$ C! $\rightarrow n \neq n_1n_2$.

$\therefore$ n is prime number

Corollary. If R is a finite integral domain, then char R = p (p is prime number).

Example. char $\mathbb{Z}_p$ = p (p is prime number).