Non zero divisor of a ring $(R,+,\cdot)$ (Commutative)

$$NZ(R) = \{x \in R \mid x \text{ is a non-zero divisor} \\ \text{i.e. } x \neq 0, \text{ \& if } xy = 0 \Rightarrow y = 0\}$$

~~If~~ Generally, $NZ(R) \supseteq R^{\times}$.

Example: Consider $(\mathbb{Z}, +, \cdot)$, $\mathbb{Z}^{\times} = \{\pm 1\}$

$$NZ(\mathbb{Z}) = \mathbb{Z}^{*}, \quad \mathbb{Z}^{*} \neq \mathbb{Z}^{\times}$$

If $NZ(R) = R^{*}$, then R is called a integral domain.

It can be shown that if $NZ(R) = R^{*}$, then R^{*} is a monoid.

R is an field $\Rightarrow$ R is an integral domain, but the converse is not true. eg:- $(\mathbb{Z}, +, \cdot)$

Example: Consider the ring $R = (\mathbb{Z}_n, +_n, \cdot_n)$

$$\mathbb{Z}_n^{\times} = \{m \mid \gcd(m,n) = 1\}$$

$$|\mathbb{Z}_n^{\times}| = \phi(n)$$

$$NZ(\mathbb{Z}_n) = \mathbb{Z}_n^{\times}, \quad Z(\mathbb{Z}_n) = \{m \mid 0 \leq m < n, \gcd(m,n) \neq 1\}$$

For $\mathbb{Z}_n$ to be a ~~field~~ integral domain, then $\mathbb{Z}_n^{\times} = \mathbb{Z}_n^{*}$. This is possible only if $n = p$ (Prime).

Also, $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow n = p$ (Prime) $\Leftrightarrow \mathbb{Z}_n$ is a field.

Show that: R is a finite integral domain $\Rightarrow$ R is a field

Ring homomorphism: f is a ring homomorphism from $R \to S$ if (i) $f : (R,+) \longrightarrow (S,+)$ is a group homomorphism

(ii) $f : (R,\cdot) \longrightarrow (S,\cdot)$ is a monoid homomorphism

Example:

$$\begin{aligned} \mathbb{Z} &\xrightarrow{\ \gamma_{\mathbb{Z}}\ } R \\ 1 &\longrightarrow 1_R \\ n &\longrightarrow n 1_R \end{aligned}$$

Quotient field: Given an integral domain R, $\exists$ a ~~field~~ smallest field $Q(R)$ (called the quotient field), which contains R. There exists an injective ring homomorphism from $R \to Q(R)$.

What is meant by the smallest field? If there is any field K such that there exists a ~~no~~ injective map from R to K, then there always exist an injective map from $Q(R)$ to K.

$$\begin{tikzcd} R \arrow[r] \arrow[d, "\text{injective}"'] & Q(R) \arrow[dl, "\text{injective}"] \\ K & \end{tikzcd}$$

Construction of $Q(R)$: Define a relation on $R \times R^*$:

$(a,b) \sim (c,d) \iff ad = bc$.

Show that the above relation is an equivalence relation. The quotient set $Q(R)$ is the ~~set of~~ equivalence class on $R \times R^*$ under the relation $\sim$.

A element of this equivalence class is denoted as $\frac{a}{b} = [(a,b)]$. Note if $\frac{a}{b} = \frac{c}{d} \iff ad = bc$

On this set $Q(R)$ we define the '+' and '$\cdot$' operations

$+$: $\frac{a}{b}, \frac{c}{d} \in Q(R)$ $\qquad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

Show that '+' is well defined and $Q(R)$ is a Abelian group under this operation.

$\cdot$: $\frac{a}{b}, \frac{c}{d} \in Q(R)$ $\qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{bd}$

Show that '$\cdot$' is well defined and $(Q(R)^*, \cdot)$ is a Abelian group.

We define the ring homomorphism f

$$\begin{aligned} R &\xrightarrow{f} Q(R) \\ a &\longrightarrow a/_1 \end{aligned}$$

Verify that f is a ring homomorphism.

Also, show that f is injective.

Now, we will check if $Q(R)$ is the smallest field. This is done by showing the existence of a injective homomorphism from $Q(R)$ to K field.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "g"'] & Q(R) \arrow[dl, "\bar{f}"] \\ K \text{ field} & \end{tikzcd}$$

Let g be a injective ring homomorphism from $R \to K$.

We define a map $\bar{f} : Q(R) \longrightarrow K$ by

$$\bar{f}\left(\frac{a}{b}\right) = g(a)\, g(b)^{-1}$$

Note $b \in R^*$, therefore $g(b) \neq 0 \Rightarrow g(b)^{-1}$ exists in K.

Show that $\bar{f}$ is a ring homomorphism.

To show that $\bar{f}$ is injective,

let $\bar{f}\left(\frac{a}{b}\right) = \bar{f}\left(\frac{c}{d}\right) \Rightarrow g(a)\, g(b)^{-1} = g(c)\, g(d)^{-1}$

Since $g(b)^{-1}$, $g(d)^{-1}$ are elements of the field K,

$$g(a)\, g(d) = g(c)\, g(b) \Rightarrow g(ad) = g(cb)$$

($\because g$ is a monoid homomorphism)

Since g is injective $ad = bc \Rightarrow \frac{a}{b} = \frac{c}{d}$.

$$\Rightarrow \bar{f}\left(\frac{a}{b}\right) = \bar{f}\left(\frac{c}{d}\right) \Rightarrow \frac{a}{b} = \frac{c}{d}.$$

$Q(R)$ is the smallest field containing R.

The rational numbers is the smallest field containing ~~$\mathbb{R}$~~ $\mathbb{Z}$.

Subring: A subset of R ($A \subseteq R$) is a subring if
(i) $(A,+)$ is a subgroup abelian, (ii) $(A,\cdot)$ is a sub monoid
(iii) $1_A = 1_R$.

Note $2\mathbb{Z}$ is not a subring of $\mathbb{Z}$ because $1 \notin 2\mathbb{Z}$.

Ideal: A is a ideal of R; (i) $A \subseteq R$, (ii) $(A,+)$ is a subgroup of $(R,+)$, (iii) if $a \in R$, $x \in A \Rightarrow ax \in A$.
(Scalar multiplication of R on A).

$R \times R \longrightarrow R$ Under this multiplication
$(a,b) \longmapsto (ab)$

$$\begin{array}{ccc} R \times A & \longrightarrow & A \\ \cap\mid & & \cap\mid \\ R \times R & & A \end{array}$$

Example: $2\mathbb{Z}$ is a ideal. For any ring R, $x \in R$
$Rx = \{ax \mid a \in R\}$ is a ideal in R which is called
~~13.1 Lemma: Every ideal in $\mathbb{Z}$~~ principal ideal generated by x. Note $\{0\}$ is always an ideal.

13.1 Lemma: Every ideal in $\mathbb{Z}$ is a principal ideal generated by some $n \in \mathbb{N}$, i.e. $A = n\mathbb{Z}$

Proof: If $A = \{0\}$ Nothing to prove. Assume $A \neq \{0\}$.
Consider $A^+ = \{m \in \mathbb{N}^* \mid m \in A\}$. obviously $A^+ \subseteq \mathbb{N}$.

Therefore A^+ must have a minimal element. Call it n.
Consider any element $m \in \mathbb{N}$, $m \in A$. Using the Euclid algorithm $m = qn + r$ $0 \leq r < n$
$\Rightarrow$ $m - qn = r$. Since $m \in A$, $n \in A$, $m - qn = r \in A$.
If $r \neq 0$, then it contradicts the minimality of n.
$\therefore r = 0$. Every element of A is divisible by n.
Every ideal of $\mathbb{Z}$ is a principal element generated by some $n \in \mathbb{N}$.