Definition.(The ideal)

Let R be a ring and $\emptyset \neq I \subseteq R$. then I is said to be an ***ideal*** of R if for all a, b $\in$I and r $\in$ R:

1. $a - b \in I$
2. $a . r \in I$ and $r . a \in I$

Remarks.

1. Every ideal is a subring.
   Proof. Let $\emptyset \neq I \subseteq R$ be an ideal of R and a, b $\in$ I, then
   i. $a - b \in I$ (I ideal)
   ii. Since $b \in I \subseteq R \rightarrow b \in R \rightarrow ab \in I$ and $ba \in I$ (I ideal).
2. The converse of (1) is not true in general. **For example**: the ring of integers $(\mathbb{Z}, +, .)$ is a subring of $(\mathbb{Q}, +, .)$ which is not ideal, for that: if a = 2 and r = 1/3, then a.r = 2/3 $\notin \mathbb{Z}$.
3. Let R be a ring, then $\{0\}$ and R are the trivial ideals in R.
4. Every ideals of the form $n\,\mathbb{Z}$ is an ideal in $\mathbb{Z}$.
5. $\{0\}$ and $\mathbb{Q}$ are the only ideals in $\mathbb{Q}$.
6. Let R be a ring with identity 1 and I be an ideal of R. If $1 \in I$, then I = R.
   Proof. Suppose that $1 \in I \rightarrow$ for all $r \in R$, $1.r \in I \rightarrow R \subseteq I$. But $I \subseteq R \rightarrow I = R$
7. Let R be a ring and I be an ideal of R. If I contain an invertible element, then R = I.
   Proof. Let $a \in I$ has inverse say $b \rightarrow 1 = a . b \in I \rightarrow 1 \in I \rightarrow I = R$.
8. If F is field, then the trivial ideals in R are only ideals in R.
   Proof. H . W.

Definition. Let I be an ideal in a ring R. Then $\frac{R}{I}$ is a ring and is said to be ***quotient ring*** of R by I, where $\frac{R}{I} = \{r + I \mid r \in R\}$

Define

$(r_1 + I)\oplus(r_2 + I) = (r_1 + r_2) + I$

$(r_1 + I)\odot(r_2 + I) = r_1 . r_2 + I$

Note that $\oplus$ is well defined where I is a subring of R.

To prove $\odot$ is well defined: let $r_1, a_1, r_2, a_2 \in R$ such that

$r_1 + I = a_1 + I \rightarrow r_1 - a_1 \in I$

$r_2 + I = a_2 + I \rightarrow r_2 - a_2 \in I$

$\because$ I is an ideal of R $\rightarrow r_1 (r_2 - a_2) \in I$ and $(r_1 - a_1) a_2 \in I$

$\therefore r_1 (r_2 - a_2) + (r_1 - a_1) a_2 \in I$

$\therefore r_1r_2 - a_1a_2 \in I \rightarrow r_1r_2 + I = a_1a_2 + I$

$\therefore$ $\odot$ is well defined.

We can prove that $(\frac{R}{I}, \oplus,\odot)$ is a quotient ring of R by I (H.W.)

Remarks.

1. Let R be a ring with identity, then $\frac{R}{I}$ is a ring with identity.
2. If R is a commutative ring, then so is $\frac{R}{I}$.
3. If R is an integral domain, then that not necessary $\frac{R}{I}$ is an integral domain. For example: the ring of integers $\mathbb{Z}$ is an

integral domain while $\frac{\mathbb{Z}}{4\mathbb{Z}} \cong \mathbb{Z}_4$ is not integral domain since $\overline{2} . \overline{2} = \overline{0}$ in $\mathbb{Z}_4$ but $\overline{2} \neq \overline{0}$ in $\mathbb{Z}_4$.

Definition. Let R be a ring and S be a nonempty subset of R. A set (S) (or <S>):

$(S) = \cap$ { I| I is an ideal of R containing S}

is called set ***generated by the set S***.

Remarks. Let R be a ring, then:

1. $(S) \neq \emptyset$ $(S \leq (S))$
2. (S) is an ideal of R (since the intersection of ideals is an ideals)
3. (S) is the smallest ideal contain S.
4. (S) = S if S is an ideal.
5. If $S = \{a_1, a_2, \ldots, a_n\}$ is a finite set, then (S) is called ***finitely generated ideal***. ((S) is f.g.)
6. If S = {a}, then (S) = (a) is said to be ***principal ideal***.
7. If R is commutative ring with identity, then
   $(a) = \{ar | r \in R\}$
8. If (S) is finitely generated, then (S) may be not in general finite set. For example: let $R = \mathbb{Z}$ and S = {1}, then $(S) = \mathbb{Z}$ is finitely generated which is not finite set.

Definition. A ring R is called ***principal ideal ring*** (PIR) if every ideal of R is principal.

Definition. A PIR is said to be ***principal ideal domain*** (PID), if R is domain.

Remark. $$\text{PID} \underset{\nleftarrow example\ \mathbb{Z}_6}{\overset{by\ definition}{\longrightarrow}} \text{PIR}$$

Examples.

1. Every ideal in $\mathbb{Z}$ is principal.
   Proof. To prove that $\mathbb{Z} = (n)$, let I be an ideal in $\mathbb{Z}$. If $I = \{0\}$, then $I = (0)$ is principal. Suppose that $I \neq \{0\} \rightarrow \exists\ (0 \neq)\ m \in I$. Let n be the smallest positive integers in $I \rightarrow rn \in I$ (I is an ideal and $n \in I$, $r \in R$). Thus $(n) \subseteq I$.
   Let $k \in I$ and $n \neq 0 \rightarrow$ By division algorithm, $k = qn + r$ for $0 \leq r < n \rightarrow r = k - qn \in I \rightarrow r \in I \rightarrow r = 0$ (since $r < n$ and n is the smallest positive integers) $\rightarrow k = qn \in (n) \rightarrow I \subseteq (n)$. By that $I = (n)$.
2. The ring $\mathbb{Z}$ is PID.
   Proof. since $\mathbb{Z}$ is an integral domain and every ideal of $\mathbb{Z}$ principal of the form $(n) = n\mathbb{Z}$ for $n = 1,2,3,\ldots$
3. The ring $\mathbb{Z}_6$ is not PID.
   Proof. The ring $\mathbb{Z}_6$ is commutative ring with identity and has nonzero divisor (**why?**) and so it's not integral domain. Therefore $\mathbb{Z}_6$ is not PID. But every ideal in $\mathbb{Z}_6$ is principal, so $\mathbb{Z}_6$ is PIR.
4. The ring $\mathbb{Q}$ is PID.
   Proof. The ring $\mathbb{Q}$ is commutative ring with identity and has no nonzero divisor (**why?**) so $\mathbb{Q}$ is integral domain. Now, $\mathbb{Q}$ have only the trivial two ideals $\{0\}$ and $\mathbb{Q}$. Since $\{0\} = (0)$ and $\mathbb{Q} = (1) = \{r.1 \mid r \in \mathbb{Q}\}$. Hence $\mathbb{Q}$ is PID.

Theorem Let R be a commutative ring with identity, then R is field if and only if R has no nontrivial ideals.

Proof. $\Longrightarrow$) Suppose that R is field and we want to prove that R contains only two ideals $\{0\}$ and R. Suppose that I be a nonzero ideal of R.

∵ $I \neq 0 \to \exists 0 \neq a \in I$

∵ R field → a has inverse element say a^{-1}

∴ $a^{-1} . a \in I \to 1 \in R \to I = R$.

⟸) Suppose that R contains only two ideals {0} and R.

If $0 \neq a \in R$, then the ideal generated by a, $(a) \neq 0 \to (a) = R$.

∴ $1 \in R \to 1 \in (a) \to 1 = r_0 . a$ for some $r_0 \in R$

$= a . r_0$ (R is commutative)

∴ $r_0 . a = a . r_0 = 1 \to r_0$ is the inverse element of a → R is field.

Remarks.

1. Let I and J be two ideals of a ring R. Then

$I + J = \{x + y \mid x \in I \text{ and } y \in J\}$

(is said to be ***sum of two ideals***) is an ideal of R.

Proof. H.W.

2. Let I be a left ideal and J be a right ideal of a ring R. Then

$IJ = \{\sum_{i=1}^{n} x_i y_i \mid x_i \in I \text{ and } y_i \in J\}$

(is said to be ***product of* I and J**) is an ideal in R.

Proof. H.W.

Remarks.

1. The sum of n-ideals $I_1, I_2, \ldots, I_n = \{\sum_{i=1}^{n} a_i \mid a_i \in I, i = 1, 2, \ldots, n\}$ is an ideal of R.

2. The product of n-ideals $I_1, I_2, \ldots, I_n = \{\sum_{i=1}^{n} a_{1i}\, a_{2i} \ldots a_{ni} \mid a_{ji} \in I_j, j = 1, 2, \ldots, n\}$ is an ideal of R.
3. The intersection of two ideals of R is an ideal of R.
   Proof. H.W.
4. The union of two ideals of R is not necessary ideal of R in general.
   Example. Let I = (2) and J = (3) are two principal ideals of $\mathbb{Z}$. Each of 3,2∈ I ∪ J but 3 – 2 = 1 ∉ I ∪ J. Hence I ∪ J is not ideal of $\mathbb{Z}$.
5. IJ ⊆ I ∩ J
6. If $I^2 = I$, then I is said to be ***idempotent ideal***.
7. If $I^n = 0$ for some $n \in \mathbb{Z}_+$, then I is said to be ***nilpotent ideal***.
8. If I and J are both idempotents ideals of a ring R. Then I + J is an idempotent.
9. An ideal I of R is said to be ***nil ideal*** if every element in I is nilpotent.
10. Every nilpotent ideal is nil ideal.
11. R = I + J iff every element in R can be written in **one way** as x + y for x ∈ I and y ∈ J

Definition. A ring R is said to be ***direct sum of two ideals*** I_1, I_2 if:

1. $R = I_1 + I_2$
2. $I_1 \cap I_2 = \{0\}$

and write $R = I_1 \oplus I_2$. In this case R is said to be ***decomposable ring***.

Remark.

1. Let $I_1, I_2, \ldots, I_n$ be ideals of a ring R. If
   i. $R = I_1 + \ldots + I_n$
   ii. $I_J \cap (I_1 + \ldots + I_{J-1} + I_{J+1} + \ldots + I_n) = \{0\}$

Then $R = I_1 \oplus \dots \oplus I_n$

2. If R cannot be written as $I_1 \oplus I_2$, then R is said to be ***indecomposable ring***.

Example.

1. $\mathbb{Z}$ is an indecomposable ring.
2. $\mathbb{Z}_6 = I_1 \oplus I_2$ where $I_1 = \{\bar{0}, \bar{3}\}$ and $I_2 = \{\bar{0}, \bar{2}, \bar{4}\}$.

Ring Homomorphism

Definition.(Ring Homomorphism)

Let f: R →R' be function from a ring R into a ring R', then f is said to be ***ring homomorphism*** if : for all a, b ∈ R,

1. f(a + b) = f(a) + f(b)
2. f(a . b) = f(a) . f(b)

Example. let $f: \mathbb{Z} \to \mathbb{Q}$ defined by f(n) = n, $\forall\, n \in \mathbb{Z}$, then:

1. f(n + m) = n + m = f(n) + f(m)
2. f(n . m) = n . m = f(n) . f(m)
   $\forall\, n, m \in \mathbb{Z}$
   ∴ f is a ring homomorphism

Definition. (kernel of f)

Let f : R → R' be a ring homomorphism. Then

1. The set

$$\ker f = \{x \in R \mid f(x) = 0\}$$

is said to be ***kernel*** of the homomorphism f

2. The set

$$\text{Im } f = \{f(x) \mid x \in R\} = f(R)$$

is said to be ***Image*** of the homomorphism f and f is said to be onto if f(R) = R'.

Proposition. Let $f : R \to R'$ be a ring homomorphism, then:

1. ker f is an ideal in R.
2. Im f is a subring of R.
3. If f is 1-1, then f is said to be ***monomorphism***
4. ker f = {0} iff f is monomorphism.
5. If f is onto, then f is said to be ***epimorphism***
6. If f is 1-1 and onto, then f is said to be ***isomorphism***
7. If $f : R \to R$ and f is an isomorphism, then f is said to be ***automorphism***

Proof 1.

i. Let $a, b \in \ker f \to f(a) = 0$ and $f(b) = 0$.
   $\because$ R is a ring , then $a - b \in R$
   $\because$ f is a ring homomorphism, then $f(a - b) = f(a) - f(b) = 0 - 0 = 0$
   $\therefore a - b \in \ker f$

ii. Let $r \in R$ and $a \in \ker f$, then $f(a) = 0$.
   $\because ar \in R$ (R is ring) $\to f(ar) = f(a) . r = 0 . r = 0 \to f(ar) = 0$
   $\therefore ar \in \ker f$
   $\therefore$ ker f is an ideal of R.

Proof 2. H.W.

Proof 4. H.W.

Examples.

1. Let f: $\mathbb{Z}_5 \rightarrow \mathbb{Z}_{10}$ defined by f(x) = 5x for x$\in \mathbb{Z}_5$. Then f is not ring homomorphism.
   Proof. If x = $\bar{2}$ and y = $\bar{4} \in \mathbb{Z}_5$, then f(x + y) = f($\bar{1}$) = $\bar{5}$
   While f(x) + f(y) = f($\bar{2}$) + f($\bar{4}$) = 5($\bar{2}$) + 5($\bar{4}$) = $\bar{0}$ + $\bar{0}$ = $\bar{0}$
   ∴f(x + y) ≠ f(x) + f(y) → f is not ring homomorphism.
2. Let R be a ring with identity and g: $\mathbb{Z}$ → R defined by g(n) = n.1 for all n ∈ $\mathbb{Z}$. Then g is ring homomorphism(why?).

Remark. Let f : R → S be a ring homomorphism, then $f(1_R) = f(1_S)$ is **not necessary true**.

Example.Define $f: M_2(\mathbb{Q}) \longrightarrow M_3(\mathbb{Q})$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Then $f\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and f is a ring homomorphism.

But $f\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq I_3$ (where $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$)

Note that here $f(A)f(I_2) = f(a.I_2) = f(A)$. So $f(I_2)$ seems to work like the multiplicative identity **on the range of *f***.

Remarks. Let f : R → R' be a ring homomorphism, then:

1. f(0) = 0'

2. $f(-r) = -f(r)$
3. If R and R' rings with identity 1 and 1' respectively, with $f(R) = R'$ then:

i. $f(1) = 1'$ (i.e $f(1)$ is an identity of R')

ii. If a is invertible, then $f(a^{-1}) = (f(a))^{-1}$.

iii. If I is an ideal of R, then f(I) is an ideal of R'.

iv. If I' is an ideal of R', then $f^{-1}(I') = \{r \in R \mid f(r) \in I'\}$ is an ideal of R

Proof 3:

(i) Let $f: R \to R'$ be an epimorphism and 1 is the identity element of R. Let $x \in R'$, then $\exists\ a \in R$ such that $f(a) = x$ (f is an epimorphism).

Now,

$x.\ f(1) = f(a)\ .\ f(1) = f(a\ .\ 1) = f(a) = x$ and $f(1).\ x = f(1)\ .\ f(a) = f(1.a) = f(a) = x$.

$\therefore\ x\ .\ f(1) = f(1)\ .\ x = x \to f(1)$ is the identity element of R'.

(ii) Let $a \in R$, then $f(a^{-1}).\ f(a) = f(a^{-1}.a) = f(1) = 1'$ and $f(a).\ f(a^{-1}) = f(a.a^{-1}) = f(1) = 1'$. $\to f(a^{-1})$ is the inverse element of $f(a) \to f(a^{-1}) = (f(a))^{-1}$.

(iii). Let $f: R \to R'$ be a ring homomorphism and I be an ideal of R. To prove that f(I) is an ideal in R':

Firstly, let $x, y \in f(I) \to \exists\ a, b \in I$ such that $f(a) = x$ and $f(b) = y$. Since I is an ideal of R, then $a - b \in I \to f(a - b) \in f(I) \to f(a) - f(b) \in f(I) \to x - y \in f(I)$.

Secondly, let $x \in f(I)$ and $r' \in R'$, then $\exists\ a \in I, \exists\ r \in R$ such that $f(a) = x$ and $f(r)=r'$. Since I an ideal in $R \to f(ar) = f(a)\ f(r) = x\ .\ r' \in f(I)$.

∴ f(I) is an ideal of R'.

(iv) $f^{-1}(I') = \{r \in R | f(r) \in I'\}$.

Let a, b ∈ $f^{-1}(I')$ → a ∈ R and f(a) ∈ I' and b ∈ R and f(b) ∈ I'.

∵ R ring→ a – b ∈R → f(a - b) = f(a) – f(b) → f(a) – f(b) ∈ I' (I' is an ideal of R') → f(a - b) ∈ I' → a – b ∈ $f^{-1}(I')$.

Now, let a, b ∈ $f^{-1}(I') \leq R$ → a . b ∈ R → f(a . b) = f(a) . f(b) ∈ I' (I' is an ideal of R') → f(a . b) ∈ I' → a . b ∈ $f^{-1}(I')$

∴ $f^{-1}(I')$ is a subring of R.

Now, to prove $f^{-1}(I')$ is an ideal, let c ∈ R, a ∈ $f^{-1}(I') \leq R$→ f(a) ∈ I' and ca ∈R (R is ring) → f(ca) = f(c) . f(a) ∈ I'(I' is an ideal) → f(ca) ∈ I' → ca ∈$f^{-1}(I')$.

By the same way, ac ∈ $f^{-1}(I')$.

∴ $f^{-1}(I')$ is an ideal of R.

Definition. A ring homomorphism which is 1-1 and onto is said to be ***isomorphism*** (R ≅ R')

The Isomorphism Theorems

First Isomorphism Theorem. (F.I.Th.)

Let R and R' be two rings and f: R → R' be an epimorphism, then $\frac{R}{ker f} \cong R'$.

Proof. H.W.

Remark. If f is not epimorphism in F.I.Th., then $\frac{R}{ker f} \cong f(R)$

Second Isomorphism Theorem. (S.I.Th.)

Let I and J be two ideals of a ring R, then $\frac{I+J}{J} \cong \frac{I}{I\cap J}$

Proof. H.W.

Third Isomorphism Theorem. (T.I.Th.)

Let I and J be two ideals of a ring R, with $I \subseteq J$, then $\frac{\frac{R}{I}}{\frac{J}{I}} \cong \frac{R}{J}$.

Proof. H.W.

Theorem. Let f: K → K' be a ring homomorphism, with K, K' are fields. Then either f is one – to – one or f is zero function.

Proof. Since K is field and kerf is an ideal in K. Then either kerf = 0, so f is one – to – one or kerf = K hence f ≡ 0.

Remark. Let f: R → R' be a ring homomorphism, then $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$.

Proof. Define g: $\frac{\mathbb{Z}}{n\mathbb{Z}} \rightarrow \mathbb{Z}_n$ by g(x + n ℤ) = [x]. Then g is an isomorphism.

(if x + nℤ ∈ ker g → [0] = g(x + nℤ) = [x] → x∈ [0] → x + nℤ = nℤ. Since nℤ is the zero of $\frac{\mathbb{Z}}{n\mathbb{Z}}$ → g is monomorism)