Maximal Ideal.

Def: An ideal $S \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $S \subseteq U \subseteq R$, then either $S = U$ or $U = R$.

Example: 1. A field F has only two ideals F and $\{0\}$. So there doesnot exist an ideal U s.t. $\{0\} \subset U \subset R$. Hence $\{0\}$ is a maximal ideal of F.

—x—

Ex 2: Let $\langle E, +, \cdot \rangle$ be the ring of even integers. Let $H_4 = \{4n, n \in \mathbb{Z}\}$. Then H_4 is a maximal ideal of the ring E.

Ex 3. The ideal S of the ring of integers I is maximal iff S is generated by some prime integers.

Proof: We know that every ideal of the ring of integers $\mathbb{Z}$ is a principal ideal. Suppose S is an ideal generated by p so that $S = \langle p \rangle$. Since p and $-p$ generate the same ideal, we can assume p as positive.

First we show that: S is maximal if p is prime.

Suppose p is prime and $S = \langle p \rangle$.
Suppose T be an ideal of $\mathbb{Z}$ such that $S \subseteq T \subseteq \mathbb{Z}$.
Since T is also a principal ideal of $\mathbb{Z}$,
Let $T = \langle q \rangle$, where q is some +ve integer.

Now, $S \subseteq T \Rightarrow \langle p \rangle \subseteq T$

$\Rightarrow p \in T$

$\Rightarrow p \in \{xq : x \in I\}$ (1)

$\Rightarrow p = rq$ for some +ve int r.

$\because p$ is prime, so either $q = 1$ or $q = p$.

If $q = 1$, we have $T = \langle 2 \rangle = \langle 1 \rangle = I$

and $q = p$, we have $T = \langle q \rangle = \langle p \rangle = S$,

Thus either $T = I$ or $T = S$.

Hence $\langle p \rangle$ is maximal.

conversely, let prove that

p is prime if S is maximal.

Let $\langle p \rangle = S$ be a maximal ideal, we are to show that p is prime

If possible let p is composite (or $\neq 1$). $(\mathbb{Z} \equiv I)$

Let $p = mn$, $1 < m, n < p$.

Obviously $\langle p \rangle \subseteq \langle m \rangle \subseteq I$.

But $\langle p \rangle$ is maximal ideal, therefore either $\langle m \rangle = \langle p \rangle$ or $\langle m \rangle = I$.

If $\langle m \rangle = I$, then $m = 1$ which is a contradiction.

If $\langle m \rangle = \langle p \rangle$, then $m = kp$ for some $k \in \mathbb{Z}$,

(∵ each element of $\langle p \rangle$ is a multiple of p)

~~$p = mn = kpn = p(kn)$~~

$p = mn = kpn = p(kn)$

$\Rightarrow kn = 1 \Rightarrow n = 1$. which is a contradiction.

Hence p is a prime number.

Prime ideal :- Let R be a ring and S an ideal in R. Then S is said to be a prime ideal if $ab \in S$, $a, b \in R \Rightarrow a \in S$ or $b \in S$.

ex. Consider the ring of integers I and the principal ideal

$$(7) = \{7r \mid r \in I\}$$

$$= \{\ldots, -14, -7, 0, 7, 14, \ldots\}$$

Obviously if $ab \in \langle 7 \rangle$, then a or b must be a multiple of 7. Hence (7) is a prime ideal.

Next, consider $(6) = \{6r \mid r \in I\}$

$$= \{\ldots, -12, -6, 0, 6, 12, \ldots\}$$

We observe that $12 \in (6)$, $12 = 3 \times 4$ but $3 \notin (6), 4 \notin (6)$

∴ (6) is not a prime ideal.

—x—

Quotient Ring :-

Introduction :- Let $\langle R, +, \cdot \rangle$ be a ring and N be an ideal of R. Then $\langle R, + \rangle$ is an additive Abelian group. Consequently $\langle N, + \rangle$ is an additive subgroup of $(R, +)$ which is normal in $\langle R, + \rangle$. Therefore, we can talk of the additive quotient group R/N.

In group theory, we see that each $r+N$ is an equivalence class for the relation of congruence modulo N. Thus $\frac{R}{N}$ can be considered as the set of all equivalence classes for the relation of congruence modulo N.

The cosets of N in R are called residue classes of N in R. Thus we can construct a ring structure on the set R/N by defining addition and multiplication of residue classes.

Theorem: Let R be a ring and N be an ideal of R; then $\frac{R}{N}$ is a ring under the addition and multiplication as under :

For $r+N, s+N \in R/N$, $(r+N)+(s+N) = (r+s)+N$

$(r+N)\cdot(s+N) = rs+N$

First we show that the operations are well defined

(1) Let $r+N = r_1+N$ and $s+N = s_1+N$ for $r, r_1, s, s_1 \in R$

$\Rightarrow r - r_1 \in N$ and $s - s_1 \in N$ (Law of cosets)

$\Rightarrow r - r_1 = n_1$, $s - s_1 = n_2$ for some $n_1, n_2 \in N$

$\Rightarrow r = n_1 + r_1$ and $s = s_1 + n_2$

$\Rightarrow rs = (n_1 + r_1)(s_1 + n_2)$

$= n_1 n_2 + n_1 s_1 + r_1 n_2 + r_1 s_1$

As $n_1, n_2 \in N$ and N is an ideal, so $n_1 n_2, n_1 s_1, r_1 n_2 \in N$ and consequently $n_1 n_2 + n_1 s_1 + r_1 n_2 \in N$.

$\Rightarrow rs - r_1 s_1 \in N$ $\Leftrightarrow$

$\Rightarrow rs + N = r_1 s_1 + N$

$\Rightarrow (r+N)(s+N) = (r_1+N)(s_1+N)$

Hence multiplication in R/N is well defined.

Again $r+N = r_1+N$ and $s+N = s_1+N$

$\Rightarrow r_1 \in r+N$ and $s_1 \in s+N$

$\Rightarrow \exists\ n_1, n_2 \in N$ such that

$r_1 = r+n_1$ and $s_1 = s+n_2$

Now, $r_1 + s_1 = r+n_1+s+n_2$

$\Rightarrow r_1+s_1 = (r+s)+(n_1+n_2)$

$\Rightarrow (r_1+s_1)-(r+s) = n_1+n_2 \in N$.

$\Rightarrow (r_1+s_1)-(r+s) \in N$

$\Rightarrow (r_1+s_1)+N = (r+s)+N$

$\Rightarrow (r_1+N)+(s_1+N) = (r+N)+(s+N)$

Hence addition is well defined in R/N.

19

Thus $\frac{R}{N}$ is closed with respect to addition and multiplication.

Let $r, s, t \in R$.

Now (i) Obviously $\langle R/N, + \rangle$ is an Abelian group.

(ii) Multiplication is associative:

$(r+N)[(s+N)\cdot(t+N)] = (r+N)[st+N]$

$= r(st)+N$

$= (rs)t+N$ $(\because r,s,t \in R$

$= (rs+N)(t+N)$

$= [(r+N)\cdot(s+N)](t+N)$

(iii) Distributive Laws:

$(r+N)[(s+N)+(t+N)] = (r+N)[(s+t)+N]$

$= r(s+t)+N$

$= rs+rt+N$ $(\because r,s,t \in R)$

$= (rs+N)+(rt+N)$

$= (r+N)(s+N)+(r+N)(t+N)$

Hy, we get- right-distributive law as

$$[(s+N)+(t+N)](r+N)$$
$$= (s+N)(r+N)+(t+N)(r+N),$$

Hence $\frac{R}{N}$ is a ring. (Quotient Ring)

Defⁿ. Let R be a ring and N be an ideal of R. Then the system $\langle \frac{R}{N}, +, \cdot \rangle$ where

$\frac{R}{N} = \{r+N \mid r \in R\}$ is set of all cosets of N in R

$+, \cdot$ are binary compositions defined by

$(r+N)+(s+N) = r+s+N$ and $(r+N)\cdot(s+N) = rs+N \;\forall\; r, s \in R$

is a ring. This ring is called a Quotient ring or Factor ring of R with respect to ideal N.

Ex. $\frac{Z}{4Z} = \{0+4Z, 1+4Z, 2+4Z, 3+4Z\}$ is a Q. ring.

Here $(2+4Z)+(3+4Z) = 5+4Z = 1+4+4Z = 1+4Z$

$(2+4Z)\cdot(3+4Z) = 6+4Z = 2+4+4Z = 2+4Z.$

Note:- the two operations are comparable to modulo 4 arithmetic

Ex- $\frac{2Z}{6Z}$ is $\{0+6Z, 2+6Z, 4+6Z\}$