Definition (Maximal Ideal) Let R be a ring such that $R \neq \{0\}$. A proper ideal M of R is said to be a maximal ideal in R if M is not contained in any other proper ideal of R, i.e., for any ideal U of R satisfying $M \subseteq U \subseteq R$ either $M = U$ or $U = R$.

Examples: 1. The null is a maximal ideal in a field F, since there is no proper ideal of F strictly containing the ideal $\{0\}$.

2. The null ideal is a maximal ideal in a simple ring.

3. In the ring $R = \mathbb{Z}$, the ideal $2\mathbb{Z}$ is a maximal ideal. Let U be an ideal of the ring $\mathbb{Z}$ such that $2\mathbb{Z} \subseteq U \subseteq R$. Since $\mathbb{Z}$ is a principal ideal ring, U is a principal ideal of $\mathbb{Z}$. Let $U = \langle m \rangle$ for some positive integer m. Then $U = m\mathbb{Z}$

$2 \in 2\mathbb{Z} \subseteq m\mathbb{Z} \Rightarrow m$ divides 2. This implies $m = 1$ or 2

If $m = 1$ then $U = \langle 1 \rangle = \mathbb{Z}$. If $m = 2$, then $U = \langle 2 \rangle = 2\mathbb{Z}$

So, $2\mathbb{Z} \subseteq U \subseteq R$ implies $U = R = \mathbb{Z}$ or $U = 2\mathbb{Z}$

This proves that $2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$

4. $6\mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$ as

$$6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$$

5. In the ring R of all real valued continuous functions defined on $[0,1]$, let $S = \{f \in R : f(\tfrac{1}{2}) = 0\}$. Then we prove that S is an ideal of R. For the zero function $0(\tfrac{1}{2}) = 0$, so $0 \in S$. So, S is non-empty. Let $f, g \in S$, Then $f(\tfrac{1}{2}) = 0$ and $g(\tfrac{1}{2}) = 0$. So, $(f-g)(\tfrac{1}{2}) = f(\tfrac{1}{2}) - g(\tfrac{1}{2}) = 0 - 0 = 0$. So, $f - g \in S$. Let $f \in S$ and $g \in R$. Then $(f \cdot g)(\tfrac{1}{2}) = f(\tfrac{1}{2})\, g(\tfrac{1}{2})$ $= 0 \cdot g(\tfrac{1}{2}) = 0$. So, $f \cdot g \in R$. Similarly if $f \in S$ and $g \in R$

then $g \cdot f \in S$. So, S is an ideal of R.

We prove that S is a maximal ideal of R. Let U be an ideal properly containing S. Then there is a function g in R such that $g \in U$ but $g \notin S$. So, g is continuous on $[0,1]$ and $g(\frac{1}{2}) = a \neq 0$. Let $h(x) = g(x) - a$. Then h is continuous on $[0,1]$ and $h(\frac{1}{2}) = 0$. So, $h \in U$.

Since U is an ideal of R, $g \in U$, $h \in U \Rightarrow g - h \in U$. So, $a \in U$. Since a is a non-zero real number, $a^{-1} \in R$ (as a non-zero constant function and therefore a continuous function). Since U is an ideal of R, $a \in U$, $a^{-1} \in R \Rightarrow aa^{-1} = 1 \in U$. So, $U = R$. This proves that S is a maximal ideal of R.

Maximal ideal in the ring $\mathbb{Z}$

The ideal $p\mathbb{Z}$ in the ring $\mathbb{Z}$ is maximal if and only if p is a prime.

Proof: Let U be an ideal of $\mathbb{Z}$ such that $p\mathbb{Z} \subseteq U \subseteq \mathbb{Z}$. Let $p\mathbb{Z} \neq U$. Then $\exists$ an element q in U such that $q \notin p\mathbb{Z}$. Clearly q is not a multiple of p.

Since p is prime (it is assumed), $\gcd(p, q) = 1$. So, $pu + qv = 1$ for some integers u, v. $pu \in p\mathbb{Z} \subseteq U$ $\Rightarrow pu \in U$ and $q \in U \Rightarrow qv \in U$. So $pu + qv = 1 \in U$. This implies $U = \mathbb{Z}$. So no proper ideal of $\mathbb{Z}$ properly contains the ideal $p\mathbb{Z}$ and this proves that $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$.

Conversely, suppose U be a maximal ideal of $\mathbb{Z}$

Since every ideal of $\mathbb{Z}$ is a principal ideal, $U = p\mathbb{Z}$ for positive integer p. Since U is maximal, $U \neq \mathbb{Z}$. So, $p \neq 1$. Let p be not a prime. Then $p = ab$ for some integers a, b each greater than 1. So, a is a proper divisor of p, i.e., $a \neq p$

a is a proper divisor p implies the ideal $p\mathbb{Z}$ is properly contained in the ideal $a\mathbb{Z}$. $a \neq 1$ implies $a\mathbb{Z}$ is a proper ideal of $\mathbb{Z}$. Thus the ideal $a\mathbb{Z}$ properly contains $p\mathbb{Z}$ and it is not equal to $\mathbb{Z}$ and this contradicts that $p\mathbb{Z}$ is maximal. So, p is a prime. This completes the proof.

3.2 <u>Quotient ring or Factor ring</u> : Let R be a ring and U be an ideal in R. Since R is an additive commutative group and U is a subgroup of R, U is a normal subgroup of R. The set all distinct cosets of U in the additive group R forms an additive group R/U, where addition is defined by $(a+U)+(b+U) = (a+b)+U$ for $a, b \in R$. We like to equip the set R/U with a multiplication. Let us define a multiplication on the set by

$$(a+U).(b+U) = ab + U \quad \text{for } a, b \in R$$

We first that this operation is well defined in the sense that if $a'+U = a+U$, $b'+U = b+U$ then

$$(a'+U).(b'+U) = ab + U$$

Now $a'+U = a+U \Rightarrow a'-a \in U \Rightarrow a' = a+u_1$ for some $u_1 \in U$

$b'+U = b+U \Rightarrow b'-b \in U \Rightarrow b' = b+u_2$ for some $u_2 \in U$

Now $a'b' - ab = (a+u_1)(b+u_2) - ab = u_1 b + a u_2 + u_1 u_2$

Since U is an ideal of R, $u_1 b \in U$, $au_2 \in U$, $u_1 u_2 \in U$. So, $a'b' - ab \in U$. Consequently $a'b' + U = ab + U$. So, $(a'+U).(b'+U) = ab + U$. This proven that $.$ is well defined. We can verify that $.$ is associative on the set R/U and both the distributive laws hold in the set (verify it). So, R/U is a ring. It is called the quotient ring or factor ring.

Note: If $U = \{0\}$ then $R/U = R$. If $U = R$ then $R/U = \{0\}$. The zero element in the quotient ring R/U is U.

If R be a commutative ring then the quotient ring R/U is also a commutative ring. (Verify it)

If R be a ring with unity 1 and U be a proper ideal of R then the quotient ring R/U is a ring with unity, $1+U$ being the unity (Verify it).

Examples 1. Let $R = (\mathbb{Z}, +, \cdot)$, $U = (3\mathbb{Z}, +, \cdot)$. Then U is an ideal of R. The quotient ring R/U is a commutative ring of three elements, U, $1+U$, $2+U$. $1+U$ is the identity elements in the ring R/U.

2. Let $R = (2\mathbb{Z}, +, \cdot)$, $U = (6\mathbb{Z}, +, \cdot)$. Then U is an ideal of R. The quotient ring R/U is a commutative ring of three elements U, $2+U$, $4+U$. $4+U$ is a non-zero element and it is ~~a ring~~ The identity element in the ring R/U. R is a ring without unity, but the quotient ring is with unity.

3. Let $R = (\mathbb{Z}_6, +, \cdot)$, $U = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$. Then U is an ideal of R. The quotient ring R/U is a ring of three elements U, $\bar{1}+U$, $\bar{2}+U$. Here R is not an integral domain but the quotient ring R/U is an integral domain