Ring Homomorphisms

A Homomorphism is a function $\varphi : R \to R'$ such that

(1) $\varphi(a +_R b) = \varphi(a) +_{R'} \varphi(b)$

or simply $\varphi(a+b) = \varphi(a) + \varphi(b)$.

(2) $\varphi(ab) = \varphi(a)\varphi(b)$.

(3) $\varphi(1_R) = 1_{R'}$

For any ring R, there exists only 1 homomorphism from $\mathbb{Z}$ to R.

Proof

For any $\varphi : \mathbb{Z} \to R$,

$\varphi(1) = 1_R = 1$

$\varphi(n) = \varphi(1 + \cdots + n \text{ times})$

$= \varphi(1) + \cdots + n \text{ times}$

$\varphi(1) + \cdots n$ times

$= \underline{1} + \cdots + n$ times.

$$\varphi(0) = \varphi\big(\underline{1} + (-\underline{1})\big) = \varphi(\underline{1}) + \varphi(-1) = \underline{1} + \varphi(-1)$$

Also $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$

$$\Rightarrow \varphi(0) = 0$$

Using the value of $\varphi(0)$,

$$0 = \underline{1} + \varphi(-1)$$

$$\Rightarrow \varphi(-1) = 0 - \underline{1} = -\underline{1}.$$

$\Rightarrow \varphi(-1) + \cdots n$ times $= -\underline{1} + \cdots n$ times

$\Rightarrow \varphi(-1 + \cdots n$ times$) = -\underline{1} + \cdots n$ times

$\Rightarrow \varphi(-n) = -1 + \cdots n$ times

Thus we will always have only 1 homomorphism $\varphi : \mathbb{Z} \to R$

Kernel

$$\boxed{\ker(\varphi) = \{a \in R \mid \varphi(a) = 0\}}$$

→ $Ker(\varphi)$ is a subgroup of $(R, +)$.

→ Let $a \in Ker(\varphi)$ and $r \in R$.

$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0$

$\Rightarrow ra \in Ker(\varphi)$.

An ideal I of R is a subset of R if $(I, +)$ is a subgroup of R and if $a \in I$, $r \in R \Rightarrow ra \in I$.

$Ker(\varphi)$ is thus an ideal of R.

Any ideal of $\mathbb{Z}$ has the form

$n\mathbb{Z} = \{an \mid n \in \mathbb{Z}\}$ where $n \geq 0$.

Proof Let I be the ideal of $\mathbb{Z}$.

If $I = \{0\}$

$\Rightarrow I = 0\mathbb{Z}$.

When $I \neq \{0\}$, since $(I, +)$ is a subgroup of $(\mathbb{Z}, +)$, for any $a \in I$

$\Rightarrow -a \in I$

and vice versa. Let n be the smallest positive integer in I. Also, lets choose any other positive integer $m \in I$.

$m \geq n$.

$m = qn + r$ where $0 \leq r < n$

Notice that $n \in I \Rightarrow nq \in I$.

$\Rightarrow (m - nq) \in I$

$\Rightarrow r \in I$.

$\Rightarrow r = 0$

since n is the smallest positive integer in I.

$m = nq$.

We can similarly show that all negative integers in I are multiples of n.

Thus $I = n\mathbb{Z}$ where $n > 0$.

Prime Ideals

$\boxed{\text{Let } a, b \in R \text{ and } ab \in I. \ I \text{ is called a prime ideal if } a \in I \text{ or } b \in I \text{ and } I \neq R}$

Remember, if p is a prime which divides $ab \in \mathbb{Z}$ then p must divide a or b. So

if $ab \in p\mathbb{Z}$

$\Rightarrow a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

$p\mathbb{Z}$ is thus a prime ideal.

Now, consider a prime ideal $n\mathbb{Z}$ where n is not a prime number. Then

$n = ab$ where $0 < a < n$ and $0 < b < n$.

$n = ab \in n\mathbb{Z}$.

$\Rightarrow a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$.

$\Rightarrow a$ or b must be n. Thus n must be a prime number.

Integral Domains

R is called an integral domain if, when $a, b \in R$ and $ab = 0$

$\Rightarrow a = 0$ or $b = 0$.

If I is an ideal of R, then it is prime if R/I is an integral domain.

Proof: Let I be a prime ideal of R.

We will choose $(a+I)$ and $(b+I) \in R/I$ such that $(a+I)(b+I) = I$.

$\Rightarrow ab + I = I$. Since the 2 cosets are equal $\Rightarrow ab \in I$

$\Rightarrow a \in I$ or $b \in I$

Consider $R = \mathbb{Q}[x]$.

$I = \{0\}$ is a prime ideal. Because if $ab = 0$ then one of the polynomials (a or b) must be 0.

Any ideal generated by x $((x))$ is also prime.

$(x) = \{ f(x) \cdot x \mid f(x) \in \mathbb{Q}[x] \}$

$= \{$ All polynomials in $\mathbb{Q}[x]$ which have the constant term $= 0\}$

Suppose $f(x), g(x) \in \mathbb{Q}[x]$ such that $f(x)g(x) \in (x)$. One of the polynomials $f(x)$ or $g(x)$ must have the constant term $= 0$.

$\Rightarrow$ either $f(x)$ or $g(x) \in (x)$.

$\Rightarrow (x)$ is a prime ideal.

All ideals are not prime ideals. For example, consider $I = (6)$.

Here $6 = 2.3$ where $2 \notin I$ and $3 \notin I$.

$\Rightarrow a + I = I$ or $b + I = I$.

$\Rightarrow R/I$ is thus an integral domain. I here is the 0th element of R/I.

If R is an integral domain, then $R[x]$ is also an integral domain.

Proof/ Let $f(x)$ and $g(x) \in R[x]$ and both of them are nonzero. We need to prove that $f(x)\,g(x) \neq 0$.

$$f(x) = \sum_{r=0}^{m} a_r x^r$$ where atleast one coefficient $a_i \neq 0$. Similarly, for $g(x)$, atleast one coefficient $b_j \neq 0$. In $f(x)\,g(x)$ we will have a term with $a_i b_j \neq 0$ since R is an integral domain. So, $f(x)\,g(x) \neq 0$.

We can easily prove that, if R is an integral domain, then any subring R' of it is also an integral domain.

Maximal Ideals

I is a maximal ideal if

[illegible] $(I \neq R)$

① it is proper ($I \neq R$)

② if J is an ideal such that $I \subseteq J \subseteq R$, then $J = I$ or R.

For any ring R, every maximal ideal is a prime ideal.

Proof/ Let $a, b \in R$ and I be a maximal ideal of R, such that $ab \in I$.

Suppose $a \notin I$. We need to show $b \in I$.

Consider ideal $J = I + (a)$

$$= \{x + ar \mid x \in I \text{ and } r \in R\}$$

Since J is generated by I and the principal ideal generated by a, J contains I. $\Rightarrow I \subset J$. Here $J \neq I$ since $a \in J$ but not I. Now since I is maximal, $J = R$.

$\Rightarrow 1 \in J = R$

$\Rightarrow \exists\, x \in I$ and $r \in R$ such that
$1 = x + ar$

$$\Rightarrow b = (x + ar) \cdot b$$

$$\Rightarrow b = xb + arb$$

$$= xb + (ab) \cdot r$$

Now $ab \in I$. $\Rightarrow (ab) \cdot r \in I$. Similarly, since $x \in I \Rightarrow x . b \in I$.

$$\Rightarrow x . b + (ab) \cdot r \in I$$

$$\Rightarrow b \in I.$$

Thus I is a prime ideal.