Definition Let A be a proper ideal of a commutative ring R.

It is a **prime ideal** $a, b \in R$ satisfying $ab \in A$ imply that $a \in A$ or $b \in A$.

It is a **maximal ideal** if there is no other ideal lying strictly between A and R.

R/A Integral domain

Example $n\mathbb{Z}$ is prime if and only if n is prime; $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideal in $\mathbb{Z}_{36}$; $\langle x^2+1 \rangle$ is a maximal ideal in $\mathbb{R}[x]$.

$A \subsetneq B \subsetneq R$

Ideal

(1)

$n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal.

It is a prime ideal $\Leftrightarrow$ n is prime

If n is not a prime, i.e., $n = ab$, $1 < a, b < n$

then $ab \in n\mathbb{Z}$

but $a, b \notin n\mathbb{Z}$.

If n is prime,

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

i.e. $ab = nk$ for some $k \in \mathbb{Z}$

$\therefore$ $n \mid (ab)$

$\therefore$ $n \mid a$ or $n \mid b$.

So $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$

(2)

$\mathbb{Z}_{36}$

$\langle 2 \rangle = \{\bar{2}, \bar{4}, \bar{6}, \cdots\}$

If $\langle 2 \rangle \subsetneq B \subseteq \mathbb{Z}_{36}$

then B contains an "odd" element, say $2k+1$.

Then $(2k+1)-(2k) \in B$

$\therefore$ $1 \in B \Rightarrow B = R = \mathbb{Z}_{36}$

$\langle 3 \rangle = \{\bar{3}, \cdots, \overline{36} = \bar{0}\}$

If $\langle 3 \rangle \subsetneq B \subseteq R = \mathbb{Z}_{36}$

Then $\exists\ b = 3k \pm 1$.

$\therefore$ $1 \in B \Rightarrow B = R$.

(3) $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$.

$\{ax+b + A : a, b \in \mathbb{R}\}$

$\mathbb{Z}_{36}/\langle 2 \rangle \cong \mathbb{Z}_2$

$\mathbb{Z}_{36}/\langle 3 \rangle \cong \mathbb{Z}_3$

Theorem 14.3-4 Let A be an ideal of a commutative ring R with unity.

(a) The factor ring R/A is an integral domain if and only if A is prime.

(b) The factor ring R/A is a field if and only if A is maximal.

Remark If A is maximal, then A is prime. The ideal $\langle x \rangle$ is prime in $\mathbb{Z}[x]$, but not maximal.

(a) $a+A, b+A \in R/A$ (R/A is a commutative integral domain) $(a+A)(b+A) = A \Leftrightarrow a+A = A$ or $b+A \in A$.
(Prime ideal) i.e., $ab \in A \Leftrightarrow a \in A$ or $b \in A$.

(b) ($\Leftarrow$) Assume that A is max. Let $b+A \neq A$

Consider $B = \{ br+a : r \in R, a \in A \} \supsetneq A$ $\because \{ b\cdot 0 + a \in B \ \forall a$, $b\cdot 1 + 0 \in B$

B is an ideal because $0 \in B \neq \emptyset$. $br_1+a_1, br_2+a_2 \in B \Rightarrow b(r_1-r_2)+(a_1-a_2) \in B$

$x \in B, y \in R \Rightarrow x = br+a$ so that $xy = bry + ay \in B$. $\therefore B = R$.

($\Leftarrow$) Assume that A is not max. $A \subsetneq B \neq R$, $A \neq \{0\}$ ideal

Assume that R/A is a field

Let $b+A \neq A$, $b \in B - A$ so that $b \notin B$

$\exists \ (b+A)(a+A) = 1+A$

Then $ab+A = 1+A$

$\Leftrightarrow ab + \hat{a} = 1$.

$\therefore ab - 1 \in A$

$\therefore ab - 1 = \hat{a}$ for some $\hat{a} \in A$

$\therefore 1 = ab - \hat{a}$ $ab - \hat{a} \in B$ as $ab \in B$, $\hat{a} \in A \subseteq B$

$\therefore 1 \in B$

$\Rightarrow 1 \cdot r \in B \ \forall r \in R$

$\Rightarrow B = R$. !!!

So $1 \in R$ can be written as $1 = br+a$.

$\therefore (b+A)(r+A) = br+A = br+a+A = 1+A$

Chapter 15 Ring Homomorphisms

Definitions Let R_1, R_2 be rings. A function $\phi : R_1 \to R_2$ is a ring homomorphism if $\phi(a+b) = \phi(a)+\phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R_1$. If in addition that ϕ is bijective, then ϕ is a ring isomorphism.

Theorem 15.1-2 let $\phi : R_1 \to R_2$ be a ring homomoprhism.

(1) For any $r \in R$ and positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = \phi(r)^n$.

(2) If A is a subring of R_1, then $\phi(A)$ is a subring of R_2.

(3) If A is an ideal of R_1, then $\phi(A)$ is an ideal of $\phi(R_1)$.

(4) If B is a subring/ideal of R_2, then $\phi^{-1}(B)$ is a subring/ideal of R_1. In particular, $Ker(\phi)$ is an ideal.

(5) If A is a commutative subring of R, then $\phi(A)$ is commutative.

(6) If R_1 has a unity, then $\phi(1)$ is a unity of $\phi(R_1)$.

(7) The map ϕ is injective if and only if $Ker(\phi) = \{0\}$.