Prime Ideal

Def. $(R,+,\cdot)$ Ring. R is a intergral Ring $\Leftrightarrow$

$R \neq \{0\}$

R is commutative

$\forall a,b \in R, (ab=0 \Rightarrow a=0 \text{ or } b=0)$

if $a \neq 0$, $\exists b \neq 0$, $ab=0 \Rightarrow a$ is a zero divisor

Def. $(R,+,\cdot)$ commutative $p \lhd R$, p is a prime ideal $\Leftrightarrow$

$\forall a,b \in \mathbb{Z}$ $(ab \in p \Leftrightarrow a \in p$ or $b \in p)$

$p \neq R$

Prop. $p \lhd R$ p is a prime ideal $\Leftrightarrow \mathbb{R}/p$ is a integral Ring

Proof. sufficieney:

$(a+p)(b+p) = ab+p = ba+p = (b+p)(a+p)$

thus R/p is commutative

suppose $(a+p)(b+p) = 0+p$

then $ab \in p$

suppose $a \in p$

then $a+p = 0+p$

necessity:

suppose $a,b \in R$, $ab \in p$

$ab+p = (a+p)(b+p) = 0+p$

suppose $a+p = 0+p$

then $a \in p$

Def. $(R,+,\cdot)$ commutative $m \triangleleft R$, m is a maximal ideal $\Leftrightarrow$

$m \neq R$

$\forall I \triangleleft R$, $(I \supsetneq m \Rightarrow I = R)$

Prop. $m \triangleleft R$, m is a maximal ideal $\Leftrightarrow$ R/m is a field

Proof. sufficiency:

m is a maximal ideal $\Rightarrow$ R/m is a commutative Ring

suppose $a+m \in R/m$ $(a+m \neq 0+m)$ $a \notin m$

$m + R\cdot a = (m, a)$

since m is maximum Ideal, so $m + Ra = R$

where $1 \in R$

thus $1 \in m + Ra$

thus there exist $b \in R$ s.t $ab + m = 1$

necessity:

for an Ideal $I \supsetneq m$, for $a \in I \setminus m$

so $a+m \neq 0+m$

thus $\exists\ b \in R$, $ab + m = 1 + m$

thus $\exists\ m \in m$: $1 = ab + m$

thus for $r \in R$

$r = r(ab+m) = rab + rm \in Ib + m \subset I + I = I$

$I = R$

Lemma. $(R,+,\cdot)$ is a field, R is an integral Ring

Prop. $(R,+,\cdot)$ commutative $\Rightarrow$ every maximum Ideal is prime

Def. $(R,+,\cdot)$ commutative, $I \trianglelefteq R$, $a,b \in R$
call a,b module I congruence, denoted as $a \equiv b \mod I$
if $a-b \in I$

Prop $a \equiv b \mod I$, $c \equiv d \mod I \Rightarrow$
$a+c \equiv b+d \mod I$
$ac \equiv bd \mod I$
$a^n \equiv b^n \mod I$

Prop. (Chinese Reminder Theorem)
$(R,+,\cdot)$ commutative $(I_i)_{1 \le i \le n}$ is a family of coprime ideal
for all $a_1, \dots, a_n \in R$ $\exists$ $x \in R$ s.t.

$x \equiv a_1 \mod I_1$
$\vdots$
$x \equiv a_n \mod I_n$

Proof. I_1 and I_j $(j \neq 1)$ are coprime
thus $\exists$ $b_j \in I_1$ $c_j \in I_j$ s.t. $b_2 + c_2 = 1$ $\dots$ $b_n + c_n = 1$
suppose $x_1 = c_2 \cdots c_n \in R$
then for $j \neq 1$. $c_2 \cdots c_j \cdots c_n \equiv 0 \mod I_j$
& $1 - \prod c_i = \prod (b_i + c_i) - \prod c_i$ ①
every term of ① contains at least one b_i
thus, $1 - \prod c_i \in I_1$
thus $x_1 = c_2 \cdots c_n \equiv 1 \mod I_1$
similarly for $x_2 \dots x_n$
suppose $x = a_1 x_1 + \dots + a_n x_n$ where $x_i \equiv 1 \mod I_i$
$x_i \equiv 0 \mod I_j$ if $j \neq i$

such x satisfies $x \equiv a_i \mod I_i$

Prop. (equivalent to Chinese Remindor Theorem)

$(R,+,\cdot)$ commutative $(I_i)_{1\le i\le n}$ coprime

(I) $\pi : R \to \prod^{n} (R/I_i)$

$\pi(a) = (a+I_1, \cdots, a+I_n)$

is a epimorphism.

particularly. $R/\bigcap I_i \cong \prod (R/I_i)$

(II) π is a isomorphism $\Leftrightarrow$ $\bigcap I_i = \{0\}$

Proof: (II) $\pi(a) = 0 \iff \forall i, a+I_i = 0+I_i$

$\iff \forall i,\ a \in I_i$

$\iff a \in \bigcap I_i$

according to the first theorem of homomorphism

$R/\bigcap I_i \cong \prod (R/I_i)$

thus π is a isomorphism $\iff$ π is injective

$\iff \ker(\pi) = \{0\}$

$\iff \bigcap I_i = \{0\}$