Recall: If I is an ideal of a ring R, then R/I is a ring with mult. defined by $(r+I)(s+I) := rs+I$, and

$$\begin{aligned} R &\longrightarrow R/I \\ r &\longmapsto r+I \end{aligned}$$

is a homom. of rings called the canonical homomorphism.

Thm (First isomorphism theorem) Let $\psi: R \to S$ be a homom. of rings, and let $I = \ker\psi \subseteq R$. Then I is an ideal of R, and there is a unique isomorphism $\eta: R/I \to \psi(R)$

s.t.

$$\begin{tikzcd} R \arrow[rr, "\psi"] \arrow[dr, "\phi_I"'] & & S \\ & R/I \arrow[ur, dotted, "\exists!\,\eta"'] & \end{tikzcd}$$

commutes.

Canonical homom.

Thm (Second isomorphism theorem) Let S be a subring of R, I an ideal of R. Then

1. $S \cap I$ is an ideal of S;
2. I is an ideal of $S+I$;
3. $S/(S\cap I) \cong (S+I)/I$.

Thm. (Correspondence theorem) Let I be an ideal of R. Then

$$S \longmapsto S/I$$

gives a bijective correspondence btwn subrings S of R which contain I and subrings of R/I. Moreover, the ideals of R/I correspond to ideals of R which contain I.

Thm (Third isomorphism theorem) Let R be a ring, with $I \subseteq J$ ideals of R. Then

$$R/J \cong \frac{R/I}{J/I}.$$

Maximal and prime ideals

Throughout this section R is a commutative ring with unity.

$$\{\text{rings}\} \supsetneq \{\text{integral domains}\} \supsetneq \{\text{fields}\}$$

Q: Under what circumstances is R/I an I.D.?
A field?

Def. Let R be a ring, $M \subsetneq R$ a proper ideal. We call M a maximal ideal if the only ideals of R containing M are M & R.

Thm. Let R be a commutative ring with unity. Then M is a maximal ideal of R iff R/M is a field.

(Proof.) First, suppose that M is a maximal ideal in R.

Then R/M is a commutative ring with unity $1+M$, Exercise.

and we NTS $a+M \neq 0+M$ has a mult. inverse.

$$a+M \neq 0+M \longleftrightarrow a \notin M.$$

Define $I_a := \{ar+m \mid r\in R, m\in M\} \subseteq R$.

Check: I_a is an ideal.

Note: $r=0 \Rightarrow M \subseteq I_a$

$r=1$ & $m=0 \Rightarrow a \in I_a \Rightarrow M \neq I_a$.

So I_a is an ideal which properly contains M.

i.e., $I_a = R$.

In particular, $1 \in I_a$. So $\exists\, b\in R$ & $m \in M$ s.t.

$$1 = ab + m.$$

$$\therefore\ 1+M = (ab+m)+M = ab+M$$

$$= (a+M)(b+M).$$

So $(a+M)^{-1} = b+M$. R/M is a field.

OTOH, $\mathcal{S}$ R/M is a field. Then R/M contains at least two elements — $0+M$ & $1+M$ — and thus $M \neq R$. (Namely, $1 \notin M$.)

Now let $I \subseteq R$ be an ideal which properly contains M. We NTS $I = R$.

Since $I \supsetneq M$, pick $a \in I \setminus M$.

Then $a + M \neq 0 + M$ in R/M,

so $\exists\ b + M \in R/M$ s.t.

$$1 + M = (a+M)(b+M) = ab + M.$$

So $1 = ab + m$, for some $m \in M$.

$\therefore$ $m \in M \subsetneq I$ and $a \in I \Rightarrow ab \in I$.

$\therefore$ $1 = ab + m \in I$.

$\therefore$ $I = R$.

So M is maximal. $\blacksquare$

<u>Def</u>. Let R be a commutative ring, and let $P \subsetneq R$ be a proper ideal. We call P a **prime ideal** of R if, for any $a, b \in R$, $ab \in P$ implies $a \in P$ or $b \in P$.

Thm. Let R be a commutative ring with unity. Then ~~M~~ P is a ~~maximal~~ prime ideal of R iff $R/$~~M~~P is ~~a field.~~ an integral domain.

(Proof.) § P is a prime ideal in R. If $a+P,\ b+P \in R/P$ satisfy $0+P = (a+P)(b+P) = ab+P$, then $ab \in P$. So $a \in P$ or $b \in P$.

That is, $a+P = 0+P$ or $b+P = 0+P$.

So R/P admits no zero divisors, and thus is an I.D.

OTOH, § R/P is an I.D. Take $a, b \in R$ s.t. $ab \in P$. Then

b/c $ab \in P$.

$$(a+P)(b+P) = ab+P = 0+P.$$

R/P an I.D. $\Rightarrow a+P = P$ or $b+P = P$

i.e., $a \in P$ or $b \in P$.

So P is prime. $\blacksquare$

Cor. All maximal ideals in commutative rings are prime ideals.

Ex. (1) Ideals of $\mathbb{Z}$ are $n\mathbb{Z}$, $n \in \mathbb{Z}$.

n composite $\Rightarrow \mathbb{Z}/n\mathbb{Z}$ is not an I.D.

$\Rightarrow n\mathbb{Z}$ is not prime

n prime $\Rightarrow \mathbb{Z}/n\mathbb{Z}$ is a field

$\Rightarrow n\mathbb{Z}$ is maximal.

(x)

(2) Consider $R = \mathbb{Z}[x]$ and the ideal $I = \langle x \rangle$.

Then $R/I = \mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ is an I.D., not a field.

$\therefore \langle x \rangle$ is prime, but not maximal.