Day 21 — July 3, 2024

Isomorphism theorems for rings

Let I be an ideal of a ring R and consider

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

This is the canonical homomorphism for I.

Thm. [First isomorphism thm for rings]
Let $\psi: R \to S$ be a ring homom. and let $I = \ker\psi$. Then I is an ideal of R and $\exists$ a unique isomorphism $\eta: R/I \to \psi(R)$ s.t.

$$\begin{tikzcd} R \arrow[r, "\psi"] \arrow[dr, "\phi"'] & \psi(R) \subseteq S \arrow[d, phantom, "\circlearrowright"] \\ & R/I \arrow[u, dotted, "\exists!\eta"'] \end{tikzcd}$$

commutes.

Thm. [Second isomorphism thm for rings]
Let S be a subring of R, I an ideal of R. Then $S \cap I$ is an ideal of S and

$$S/(S\cap I) \cong (S+I)/I$$

Thm. [Correspondence thm for rings]
Let I be an ideal of a ring R. Then $S \mapsto S/I$ gives a bijective correspondence btwn the subrings of R which contain I and the subrings of R/I. Moreover, the ideals of R/I correspond to ideals of R which contain I.

Thm. [Third isomorphism thm for rings]
Let R be a ring and let $J \subseteq I \subseteq R$ be ideals of R. Then

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

Maximal & prime ideals

Throughout, R is a commutative ring with unity.

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

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

(Proof.) First, $\supseteq$ M is maximal and choose $a+M \neq 0+M$.
We NTS that $a+M$ has an inverse in R/M.
Set $\quad I_a := \{ar + m \mid r \in R, m \in M\} \subseteq R$.
Check: I_a is an ideal in R.
Note that $M \subseteq I_a$ (set $r=0$).
Since M is maximal, $I_a = M$ or $I_a = R$.
But $a \in I_a$ (set $r=1$ and $m=0$).

Since $a+M \neq 0+M$, $a \notin M$. So $I_a \neq M$.
So $I_a = R$. In particular, $1 \in I_a$.
$\therefore$ we can choose $b \in R$ and $m \in M$ s.t.

$$ab + m = 1 \Rightarrow 1 + M = ab + M$$
$$= (a+M)(b+M).$$

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

Next, suppose R/M is a field.
Then $0 + M \neq 1 + M \in R/M$.
So $1 \notin M$, and thus $M \neq R$.
Suppose $I \subseteq R$ is an ideal with $M \subsetneq I$.
Pick $a \in I - M$. Then $a + M \neq 0 + M$,
so $\exists$ $b + M = (a+M)^{-1}$, i.e.,
$(a+M)(b+M) = ab + M = 1 + M$.
$\therefore$ $1 = ab + m$, for some $m \in M$.

$$\left.\begin{array}{l} \text{Now } a \in I \Rightarrow ab \in I \\ m \in M \Rightarrow m \in I \end{array}\right\} \rightarrow ab + m \in I.$$

So $1 \in I \Rightarrow I = R$. $\leftarrow$ $\left(\begin{array}{l} rI \subseteq I, \forall r \in R \\ 1 \in I \Rightarrow r \cdot 1 \in I \end{array} \right)$
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** if, for any $a, b \in R$ with $ab \in P$, we have $a \in P$ or $b \in P$.

<u>Thm</u> Let P be an ideal of a commutative ring with unity R. Then P is prime iff R/P is an integral domain.

(Proof.) ($\Rightarrow$) P is prime. Choose $a+P, b+P \in R/P$ s.t.

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

Then $ab \in P$, so $a \in P$ or $b \in P$

$$a \in P \downarrow \quad a+P = 0+P \qquad b \in P \downarrow \quad b+P = 0+P.$$

So R/P is an I.D.

($\Leftarrow$) R/P is an I.D. and pick $a, b \in R$ s.t. $ab \in P$. Then

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

So $a+P = 0+P$ or $b+P = 0+P$, since R/P is an I.D.

$$a+P = 0+P \downarrow \quad a \in P \qquad b+P = 0+P \downarrow \quad b \in P$$

So P is a prime ideal. ∎

Cor. Every maximal ideal in a commutative ring is a prime ideal.

Ex

① We know that every ideal of $\mathbb{Z}$ has the form $n\mathbb{Z}$ and that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Since $\mathbb{Z}_n$ is an I.D. iff n is prime, $n\mathbb{Z} \subseteq \mathbb{Z}$ is a prime ideal iff n is prime.

In fact, $\mathbb{Z}_p$ is a field, for any prime p.

So all prime ideals of $\mathbb{Z}$ are maximal.

(2) Consider the principal ideal $\langle x \rangle$ in the polynomial ring $\mathbb{Z}[x]$.

Indeed $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$.

$$\left(\text{Proof: } \begin{array}{ccc} \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}. \\ x & \longmapsto & 0 \end{array} \text{ Apply F.I.T.} \right)$$

Since $\mathbb{Z}$ is an I.D. but not a field, $\langle x \rangle$ is prime but not maximal.