Lecture 24

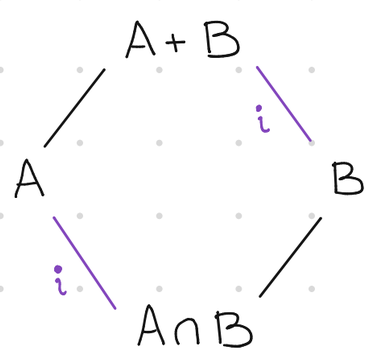
Isomorphism Theorems for Rings

First Isomorphism Theorem: Let $\varphi : R \longrightarrow S$ be a ring homomorphism. Then

(1) $\operatorname{Ker}\varphi$ is an ideal of R

(2) $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$

Second Isomorphism Theorem: Let A, B be subrings of a ring R s.t. B is an ideal. Then



(1) $A+B$ is a subring of R.

(2) B is an ideal of $A+B$.

(3) $A \cap B$ is an ideal of A

(4) $A/_{A\cap B} \cong (A+B)/_B$

Third Isomorphism Theorem: Let I, J be ideals of R s.t. $I \subseteq J$. Then

(1) J/I is an ideal of R/I.

(2) $\left(R/I\right)\Big/_{(J/I)} \cong R/J$

Fourth Isomorphism Theorem: Let I be an ideal of a ring R and let $\pi : R \longrightarrow R/I$ be the natural projection, $\pi(r) = r + I$. There is a bijection

$$\left\{\begin{array}{l}\text{subrings of } R \text{ that}\\ \text{contain } I\end{array}\right\} \xrightarrow{\Pi} \left\{\begin{array}{l}\text{subrings}\\ \text{of } R/I\end{array}\right\}$$

$$S \longmapsto \pi(S) = S/I$$

Π has the following properties: Let A, B be subrings of R s.t. $I \subseteq A, B$.

(1) $A \subseteq B \iff A/I \subseteq B/I$

(2) $A \subseteq B \implies [B : A] = [B/I : A/I]$

(3) $(A \cap B)/I = (A/I) \cap (B/I)$

(4) A is an ideal of $R \iff A/I$ is an ideal of R/I

Important Ideals

- $I + J$ and IJ where I and J are ideals.
- (a) and $(a_1, \dots, a_n)$ where $a, a_1, \dots, a_n \in R$
- Maximal ideals
- Prime ideals

Def: Let R be a ring. An ideal M of R is called a maximal ideal if

(1) $M \subsetneq R$ ← M is a proper ideal

(2) If I is an ideal of R and $M \subseteq I \subseteq R$, then $I = M$ or $I = R$. ← only ideals containing M are M and R

Remarks:

1. How to prove $M \subseteq R$ is a maximal ideal?

   By def

   Prove (1).
   Prove: If I is an ideal and $M \subsetneq I$, then $I = R$

   Prove (1).
   Prove: If I is an ideal and $I \subsetneq R$, then $I = M$.

2. A general ring need not have maximal ideals, e.g. $(\mathbb{Q}, +,$ trivial multiplication$)$
   $ab = 0 \ \forall a, b \in \mathbb{Q}$

   Ideals of this ring are all its subgroups. $(\mathbb{Q}, +)$ has no maximal subgroups.

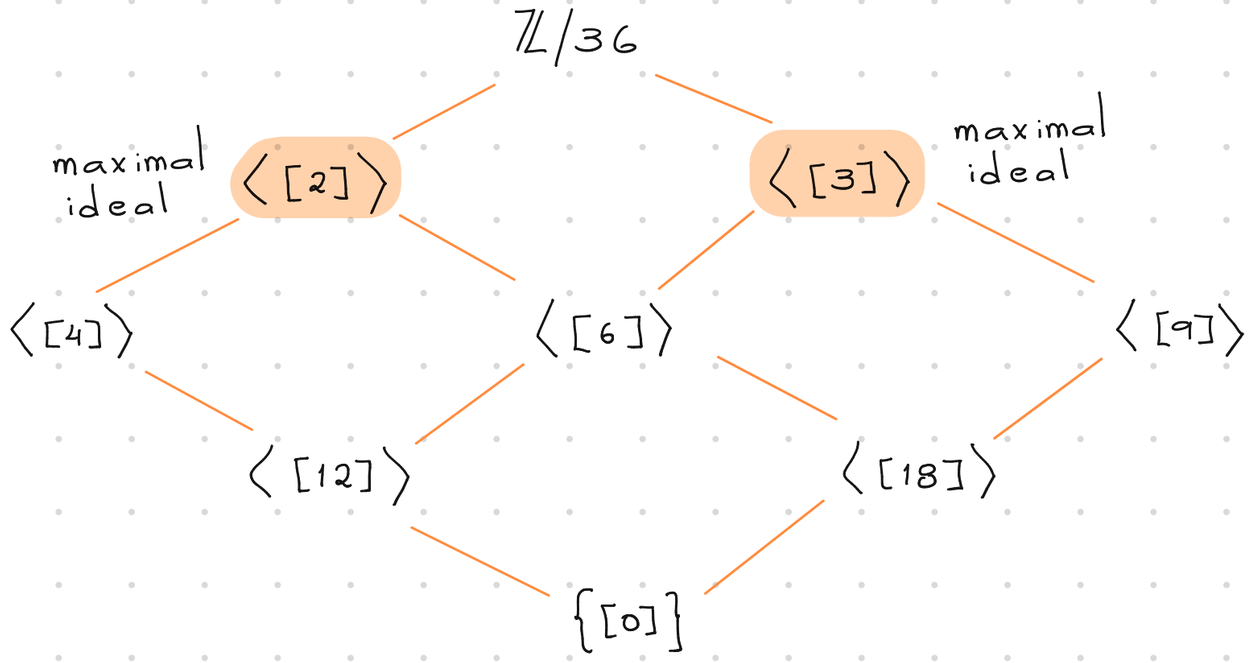
   We won't prove this, we need advanced concepts

3. Prop: Let R be a ring with identity. Every proper ideal is contained in a maximal ideal.

   We won't prove this, it uses Zorn's lemma.

Ex:

1. $\mathbb{Z}/36$. Consider its lattice of ideals:



2. $\mathbb{R}[x]$. The ideal (x^2+1) is maximal in $\mathbb{R}[x]$.

Suppose I is an ideal of $\mathbb{R}[x]$ such that $(x^2+1) \subsetneq I$. WTS: $I = \mathbb{R}[x]$.

Claim: $\exists\, c \in \mathbb{R}\setminus\{0\}$ s.t. $c \in I$ (i.e. I contains a unit)

Let $f(x) \in I \setminus (x^2+1)$, then $f(x) \notin (x^2+1)$ By the Division Algorithm for poly with real coefficients $f(x) = q(x)(x^2+1) + r(x)$ where $r(x) \neq 0$ and $0 < \deg r(x) < \deg (x^2+1) = 2$. Then $r(x) = ax + b$ with $a \neq 0$ or $b \neq 0$.

Notice that $ax+b = \underbrace{q(x)(x^2+1)}_{\in (x^2+1)} - \underbrace{f(x)}_{\in I} \in I$.

Hence, $a^2x^2 - b^2 = (ax+b)(ax-b) \in I$ (it absorbs on the right).

We also have that $a^2(x^2+1) \in I$ (it absorbs on the left).

Consequently, $0 \neq a^2 + b^2 = (a^2x^2 - b^2) + (a^2x^2 + a^2) \in I$

By Prop 14 (1), $I = \mathbb{R}[x]$. The result follows.

Theorem 16: Let R be a commutative ring with identity. Let M be an ideal of R.

$$M \text{ is a maximal ideal} \iff R/M \text{ is a field}$$

Proof:

($\Rightarrow$) From hypothesis, $(R/M, +, \cdot)$ is a commutative ring with identity.

WTS: If $a+M \neq M$, then $a+M$ has a multiplicative inverse.

Let $I := \{ ar + m \mid r \in R \text{ and } m \in M \}$.

Claim: I is an ideal of R and $M \subsetneq I \subseteq R$.

- $I \neq \phi$ because $a0 + 0 \in I$
- $(ar_1 + m_1) - (ar_2 + m_2) = a(r_1 - r_2) + (m_1 - m_2) \in I \quad \forall r_1, r_2 \in R \quad \forall m_1, m_2 \in M$
- $r_1(ar + m) = r_1(ar) + r_1 m = a(r_1 r) + (r_1 m) \in I \quad \forall r_1, r \in R \quad \forall m \in M$

  (R comm; M ideal)

  $(ar + m)r_1 \in I$

Now, notice that for all $m \in M$, $m = a0 + m \in I$, i.e. $M \subseteq I$. Furthermore, $a = a1 + 0 \in I$ but $a \notin M$ (because $a+M \neq M$). It follows that I is an ideal of R that contains M properly. Since M is maximal, then $I = R$. Thus $1 \in R$, i.e. $\exists\, r \in R$ and $m \in M$ s.t. $1 = ar + m$. Hence

$$1 + M = (ar + m) + M = ar + (m + M) = ar + M = (a+M)(r+M).$$

($\Leftarrow$) Let I be an ideal of R s.t. $M \subsetneq I$. WTS: $I = R$

Let $a \in I$ s.t. $a \notin M$. Then $a + M \neq M$. Given that R/M is a field, $\exists\, b+M$ s.t. $1 + M = (a+M)(b+M) = (ab) + M$, i.e. $1 - ab \in M$. Moreover, $ab \in I$ because $a \in I$ and I is an ideal. From this $1 = (1-ab) + ab \in I$. By Prop 14 (1) $I = R$.

■

Def: Let R be a commutative ring. An ideal P of R is called a prime ideal if

(1) $P \subsetneq R$ ⇐ P is a proper ideal

(2) The following property is satisfied for all $a, b \in R$:

If $ab \in P$, then $a \in P$ or $b \in P$.

Remarks: This definition is a generalization of the notion of a "prime" in $\mathbb{Z}$.

$p \in \mathbb{Z}$ is prime if (1) $p \neq 1$ $\iff$ $(p) \neq \mathbb{Z}$

(2) $p|ab \Rightarrow p|a$ or $p|b$ $\iff$ $ab \in (p) \Rightarrow a \in (p)$ or $b \in (p)$

where (p) is the ppal ideal generated by p.

Ex:

1. D an integral domain. Then $\{0\}$ is a prime ideal ✓ $\{0\} \subsetneq D$
   ✓ $ab = 0 \Rightarrow a = 0$ or $b = 0$ (no zero divisors)
2. $\mathbb{Z}$. @ $\{0\}$ is a prime ideal.
   @ $n \neq 1$. (n) is a prime ideal $\Leftrightarrow$ p is prime. Prove it!
3. $\mathbb{F}_2[x]$. The ideal (x^2+1) is not prime in $\mathbb{F}_2[x]$.

Observe that $(x+1)(x+1) = x^2 + 2x + 1 = x^2 + 1 \in (x^2+1)$,

but $x+1 \notin (x^2+1)$.

Theorem 17: Let R be a commutative ring with identity. Let P be an ideal of R.

$$P \text{ is a prime ideal} \iff R/P \text{ is an integral domain}$$

Proof: It follows by definition of prime ideals and integral domains.

Let a class $r+P \in R/P$ be denoted by $\overline{r}$ for all $r \in R$.

$$P \text{ is a prime ideal} \iff P \subsetneq R \text{ and } (\forall a,b \in R)(ab \in P \Rightarrow a \in P \text{ or } b \in P)$$

$$\iff R/P \text{ is not trivial and } (\forall a,b \in R)(\overline{ab} = \overline{0} \Rightarrow \overline{a} = \overline{0} \text{ or } \overline{b} = \overline{0})$$

$$\iff R/P \text{ is not trivial and } (\forall a,b \in R)(\overline{a}\,\overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0} \text{ or } \overline{b} = \overline{0})$$

■

!!! **Corollary 18:** Let R be a commutative ring with identity.

$$R \text{ is an integral domain} \iff \{0\} \text{ is a prime ideal}$$

Proof: $\{0\}$ is a prime ideal $\iff R/\{0\} \cong R$ is an integral domain.

!!! **Corollary 19:** Let R be a commutative ring with identity. Every maximal ideal is a prime ideal.

Proof:

I is maximal	$\iff$	R/I is a field	(By Prop 16)
	$\Rightarrow$	R/I is an ID	(By def)
	$\iff$	I is prime	(By Prop 17)

The converse of this corollary is not true as an ID is not necessarily a field.

Ex: $\mathbb{Z}[x]$

$(2,x)$ $(2,x)$ is maximal because $\mathbb{Z}[x]/(2,x) \cong \mathbb{F}_2$ a field.

(x) (x) is prime but not maximal because $\mathbb{Z}[x]/(x) \overset{①}{\cong} \mathbb{Z}$ an ID.

$\{0\}$ $\{0\}$ is prime not maximal because $\mathbb{Z}[x]/\{0\} \overset{②}{\cong} \mathbb{Z}[x]$ an ID.

You may prove isomorphisms ① and ② using evaluation at 0 and the 1st IT for rings.

$e: \mathbb{Z}[x] \longrightarrow \mathbb{F}_2$

$p(x) \longmapsto [p(0)]$

$\operatorname{Ker} e = \{ p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z} \} = (2,x)$

$e: \mathbb{Z}[x] \longrightarrow \mathbb{Z}$

$p(x) \longmapsto p(0)$

$\operatorname{Ker} e = \{ p(x) \in \mathbb{Z}[x] \mid p(0) = 0 \} = (x)$