Lecture 4.2

Last time:

- $M \subsetneq A$ is a maximal ideal if and only if A/M is a field.

- If $\mathbb{F}$ is a field, then for any $\alpha \in \mathbb{F}$,

$$M_\alpha = (x - \alpha)$$

is a maximal ideal, but depending on $\mathbb{F}$, the converse may not be true.

- (x^2+1) is a maximal ideal in $\mathbb{R}[x]$ with $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Ex ① Let's try the same trick over $\mathbb{Z}$.

Define $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{C}$

$p(x) \longmapsto p(i)$.

This is again a ring homomorphism,

but $\operatorname{im}(\varphi) = \{a+bi \mid a,b \in \mathbb{Z}\} \subsetneq \mathbb{C}$.

In fact, this subring has a special

name and notation:

$$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$$

the ring of Gaussian integers.

Again we have $\ker(\varphi) = (x^2+i)$, so

$$\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i].$$

But $\mathbb{Z}[i]$ is not a field — for example, for any $a = a + 0i \in \mathbb{Z}[i]$, $a^{-1} = \frac{1}{a} \in \mathbb{C}$ but $a \notin \mathbb{Z}[i]$.

Therefore (x^2+1) is <u>not</u> a maximal ideal in $\mathbb{Z}[x]$ — what is it??

Let's dig deeper into this example.

Consider the ideal $(2+i) \subseteq \mathbb{Z}[i]$.

By the Correspondence Theorem,

$$\left\{ \text{ideals } I \text{ in } \mathbb{Z}[x], \right\} \longleftrightarrow \left\{ \text{ideals} \right\}$$

$(x^2+1) \subseteq I \subseteq \mathbb{Z}[x]$ $\qquad$ $J \subseteq \mathbb{Z}[i]$

$$I = \varphi^{-1}((2+i)) \quad \longleftrightarrow \quad (2+i) = J.$$

Notice $\varphi(x+2) = 2+i$ so $x+2 \in I$.

Also, $(x^2+1) \subseteq I$ and one can use the Polynomial Division Algorithm to show that

$$I = (x^2+1, x+2)$$
$$= \{a(x)(x^2+1) + b(x)(x+2) \mid a, b \in \mathbb{Z}[x]\}.$$

This shows

$$\mathbb{Z}[x]/I \cong \mathbb{Z}[i]/(2+i).$$

Observe that

$$x^2+1 = (x+2)(x-2) + 5$$

so in $\mathbb{Z}[x]/I = \mathbb{Z}[x]/(x^2+1, x+2)$

we have $I = (x^2+1) + I = 5 + I$

i.e. $0 = 5$.

Claim: $\mathbb{Z}[i]/(2+i) \cong \mathbb{F}_5$.

Since $5 = (x^2+1) - (x+2)(x-2) \in I$,

$$(5, x+2) \subseteq I = (x^2+1, x+2).$$

$$\Rightarrow (5, x+2) = I$$

$$\Rightarrow \mathbb{Z}[i]/(2+i) \cong \mathbb{Z}[x]/(5, x+2).$$

Now consider

$$ev_{-2} : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$$
$$p(x) \longmapsto p(-2).$$

By previous work, ev_{-2} is surjective with kernel $(x+2)$, so by the Correspondence Theorem,

$$\mathbb{Z}[x]/I \cong \mathbb{Z}/(I/(x+2))$$

but $$I/(x+2) = (5, x+2)/(x+2) = (5),$$

so $$\mathbb{Z}[x]/I \cong \mathbb{Z}/(5) = \mathbb{F}_5.$$

Putting everything together,

$$\mathbb{Z}[x]/(x^2+1, x+2) = \mathbb{Z}[x]/(5, x+2)$$

$\cong$ $\qquad\qquad$ $\cong$

$\mathbb{Z}[i]/(2+i) \qquad\qquad \mathbb{F}_5$

So $(2+i)$ is a maximal ideal in $\mathbb{Z}[i]$ and $(x^2+1, x+2)$ is maximal in $\mathbb{Z}[x]$.

Q: What kind of ideal is (x^2+1) in $\mathbb{Z}[x]$?

Recall that $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$.

Lemma $\mathbb{Z}[i]$ is an integral domain.

Pf: Take $a+bi, c+di \in \mathbb{Z}[i]$, with

$a, b, c, d \in \mathbb{Z}$ and suppose $a + bi \neq 0$

and $(a+bi)(c+di) = 0.$

Then $0 = (ac - bd) + i(ad + bc)$

$\Rightarrow \quad ac - bd = 0 \Rightarrow ac = bd$

and $\quad ad + bc = 0 \Rightarrow ad = -bc.$

If $a \neq 0$, then

$$ac = bd$$

$$\Rightarrow ac^2 = bcd = -ad^2$$

$$\Rightarrow c^2 = -d^2$$ b/c $a \neq 0$ and

$\mathbb{Z}$ is an int. domain

$\Rightarrow \quad c = d = 0.$

If $b \neq 0$,

$$ac = bd$$

$$\Rightarrow \quad adc = bd^2$$

$$\Rightarrow \quad -bc^2 = bd^2$$

$$\Rightarrow -c^2 = d^2 \quad \text{(same reason)}$$

$$\Rightarrow \quad c = d = 0.$$

Therefore if $a+bi \neq 0$, $c+di = 0$, so

$\mathbb{Z}[i]$ is an integral domain. $\square$

Def A **prime ideal** of a commutative ring A is an ideal $P \subsetneq A$ such that for all ideals $I, J \subseteq A$ such that $IJ \subseteq P$, we have $I \subseteq P$ or $J \subseteq P$.

Ex ② The name comes from:

$(n) \subseteq \mathbb{Z}$ is prime $\Leftrightarrow$ n is prime.

This is because for any $I = (a)$ and $J = (b)$ ideals in $\mathbb{Z}$,

$(a)(b) = (ab) \subseteq (n) \iff n \mid ab$

and when $n = p$ is prime,

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$

$$\iff (a) \subseteq (p) \text{ or } (b) \subseteq (p).$$

For any composite n, this fails, e.g.

$$(2^2) \subseteq (4) \text{ but } (2) \not\subseteq (4).$$

Prop An ideal $P \subseteq A$ is prime if and only if A/P is an integral domain.

Pf: ($\Rightarrow$) Suppose $a, b \in A$ such that

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

in A/P. Then $ab + P = P$, so

$ab \in P$ and hence $(a)(b) = (ab) \subseteq P$.

Since P is prime, $(a) \subseteq P$ or $(b) \subseteq P$,

showing $a + P = P$ or $b + P = P$

in A/P.

($\Leftarrow$) Suppose A/P is an integral domain.

To show P is prime, let $I, J \subseteq A$

be ideals such that $IJ \subseteq P$ but

$I \not\subseteq P$.

Take $a \in I$, $a \notin P$; in particular,

$a \neq 0$.

Then for all $b \in J$,

$$ab \in IJ \subseteq P$$

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

Since A/P is an integral domain and

$a+P \neq P$, we have $b+P = P$.

So $b \in P$. This is true for all

$b \in J$, so $J \subseteq P$.

Hence P is prime. $\square$

Corollary Every maximal ideal is also a prime ideal.

Pf: Every field is also an integral domain. $\square$

Corollary A commutative ring $A \neq 0$ is an integral domain if and only if (0) is a prime ideal.

Exercise 1: prove it!

How do we decide if an ideal is maximal or prime or neither?

Def Let A be a commutative ring.

- An element $m \in A$ is **irreducible** if whenever we can write $m = ab$ for some $a, b \in A$, then a or b is a unit $(a \in A^\times$ or $b \in A^\times)$.

- An element $p \in A$ is **prime** if for any $a, b \in A$ such that $ab \in (p)$, we have $a \in (p)$ or $b \in (p)$.

Prop Let A be an integral domain. Then

(1) $p \in A$ is prime if and only if (p) is a prime ideal.

(2) $m \in A$ is irreducible if and only if (m) is maximal among all principals.

(3) If A is a PID, then $m \in A$

(3) If A is a PID, then $m \in A$ is irreducible if and only if (m) is a maximal ideal.

(4) If A is a PID, then $p \in A$ is prime if and only if it's also irreducible.

Exercise 2: try to prove some parts yourself, and look it up in a textbook if you get stuck.

Next time: wrapping up polynomial rings.