Lecture 4.1

Last time:

- The Isomorphism Theorems hold for rings!:

  (1) $A/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

  (2) $(I+J)/J \cong I/(I+J)$.

  (3) $(A/I)/(J/I) \cong A/J$.

  (4) There is a 1-to-1 correspondence

$$\left\{\begin{array}{c}\text{ideals} \\ I \subseteq J \subseteq A\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ideals of} \\ A/I\end{array}\right\}.$$

- A maximal ideal in a commutative ring A is an ideal $M \subsetneq A$ such that for any ideal $M \subseteq I \subseteq A$, either $I = M$ or $I = A$.

Ex ① In $A = \mathbb{C}[x]$, the maximal ideals are exactly the principal ideals generated by linear polynomials:

$$M_\alpha = (x-\alpha) = \{p(x) \mid p(\alpha)=0\} = \ker(\mathrm{ev}_\alpha)$$

for $\alpha \in \mathbb{C}$. (By dividing out by the leading term, we can always replace $ax-b$ by $x-\alpha$ for $\alpha = \frac{b}{a}$.)

We will prove that the ideals M_α are maximal in a moment, but to see that these are the only maximal

ideals in $\mathbb{C}[x]$, suppose $I \subseteq \mathbb{C}[x]$ is any ideal. Choose $p(x) \in I$.

By the Fundamental Theorem of Algebra, $p(\alpha) = 0$ for some $\alpha \in \mathbb{C}$, so $x - \alpha \mid p(x)$, i.e. $p(x) \in (x-\alpha)$. If $I = (p(x))$, this shows $I \subseteq (x-\alpha)$.

Moreover, we will show later that every ideal in $\mathbb{C}[x]$ is principal (i.e. $\mathbb{C}[x]$ is a PID) so the only maximal ideals are $(x-\alpha)$, $\alpha \in \mathbb{C}$.

Let $M \subset A$ be a maximal ideal. By the

Correspondence Theorem,

$$\left\{ \begin{array}{c} \text{ideals} \\ M \subseteq I \subseteq A \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{ideals of} \\ A/M \end{array} \right\}$$

but there are only two things on the left:

M and A.

This proves:

Prop An ideal $M \subseteq A$ is maximal if and only if A/M is a field.

Corollary For any field $\mathbb{F}$ and every $a \in \mathbb{F}$,

the ideal $M_\alpha = (x-\alpha) \subseteq \mathbb{F}[x]$ is maximal.

Pf: Consider the evaluation map

$$ev_\alpha : \mathbb{F}[x] \longrightarrow \mathbb{F}$$
$$p(x) \longmapsto p(\alpha).$$

We already showed that ev_α is a surjective ring homomorphism with

$$\ker(ev_\alpha) = M_\alpha.$$

So by the First Isomorphism Theorem,

$$\mathbb{F}[x]/M_\alpha \cong \mathbb{F}$$

which implies M_α is maximal by the

Prop. □

Ex (1, cont'd.) This (almost) finishes our proof that $\{\text{maximal ideals } M \subseteq \mathbb{C}[x]\} \longleftrightarrow \{\text{complex numbers } \alpha \in \mathbb{C}\}$.

This correspondence, called **Hilbert's Nullstellensatz**, is the jumping off point for an area of math called algebraic geometry:

Algebra	Geometry
max'l. ideals in $\mathbb{C}[x]$	points in $\mathbb{C}$
ideals in $\mathbb{C}[x,y]$	points and curves in $\mathbb{C}$
max'l. ideals in A	points in ??
ideals in A	???

(2) This gives an alternate proof that $(n) \subseteq \mathbb{Z}$ is maximal if and only if n is prime:

(n) is maximal $\iff$ $\mathbb{Z}/n\mathbb{Z}$ is a field

$\iff$ n is prime.

(3) In $\mathbb{R}[x]$, the ideals $M_a = (x-a)$ for $a \in \mathbb{R}$ are maximal, but not all maximal ideals are of this form.

Claim: $(x^2+1) \subseteq \mathbb{R}[x]$ is maximal.

Recall the "evaluation map"

$$\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$$
$$p(x) \longmapsto p(i).$$

Exercise 1: φ is a ring homomorphism.

φ is surjective: $a+bi = \varphi(a+bx)$ ✓

($a+bi$ ✓ real numbers)

$\ker(\varphi) = (x^2+1)$:

$x^2+1 \in \ker(\varphi)$:

$$\varphi(x^2+1) = i^2+1 = -1+1 = 0.$$

$$\Rightarrow (x^2+1) \subseteq \ker(\varphi). \quad ✓$$

For the other containment, we need to show that for any $p(x) \in \ker(\varphi)$, $p(x)$ is divisible by x^2+1. This motivates our next big theorem.

Theorem (Polynomial Division Algorithm)

Let A be a commutative ring. Then for any $p(x), f(x) \in A[x]$, with $f(0) \in A^\times$,

$$p(x) = f(x)\,q(x) + r(x)$$

for unique $q(x), r(x) \in A[x]$ where

$$\deg r(x) < \deg f(x).$$

Pf: Fix $f(x)$ (think: try to divide stuff by f, with remainders)

and let $n = \deg f(x) \geq 0$,
$m = \deg p(x) \geq 0$.

If $m < n$ then

$$p(x) = f(x) \cdot 0 + p(x)$$

works. Otherwise, $m \geq n$ and we can

induct on m.

First, if $m = n = 0$ then $f(x) = a_0 \in A^\times$

and $p(x) = b_0 \in A$, and

$$p(x) = a_0 q(x) + 0$$

where $q(x) = a_0^{-1} b_0$

To induct, suppose $m = \deg p(x) \geq 1$ and suppose the division algorithm holds for all polynomials of degree $< m$.

For $f(x) = a_0 + a_1 x + \ldots + a_n x^n$

and $p(x) = b_0 + b_1 x + \ldots + b_m x^m$,

set $q_0(x) = a_n^{-1} b_m x^{m-n}$ and

$$p_1(x) = p(x) - q_0(x) f(x)$$

$$= (b_0 + \ldots + b_m x^m) - (\ldots + b_m x^m)$$

$$= b_0 + \ldots + (b_{m-1} - a_n^{-1} b_{m-1} a_{m-1}) x^{m-1}$$

so that $\deg p_1(x) < m$.

By induction, $p_1(x) = f(x)q_1(x) + r_1(x)$

for some $q_1(x), r_1(x) \in A[x]$ with

$\deg r_1(x) < \deg f(x)$.

Now $p(x) = f(x)q_0(x) + p_1(x)$

$= f(x)q_0(x) + \left(f(x)q_1(x) + r_1(x)\right)$

$= f(x)q(x) + r(x)$

where $q(x) = q_0(x) + q_1(x)$, $r(x) = r_1(x)$

and $\deg r(x) = \deg r_1(x) < \deg f(x)$.

Uniqueness is similar to the original proof for $\mathbb{Z}$, which you can prove for exercise. $\square$

Remarks: (i) If we don't specify that the leading coefficient of $f(x)$ is a unit, the algorithm <u>fails</u>.

For example, in $A = \mathbb{Z}/4\mathbb{Z}$, there is no way to divide $p(x) = x^2$ by $f(x) = 2x$ with remainder:

$x \neq 2x\,q(x) + r(x)$ for any

$q(x), r(x) \in \mathbb{Z}/4\mathbb{Z}[x]$.

(ii) When $\mathbb{F}$ is a field, every nonzero polynomial has leading coefficient which is a unit, so the division algorithm is slightly easier to state.

Ex (3, cont'd.) Let's prove that for

$$\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$$
$$x \longmapsto i$$

we have $\ker(\varphi) \subseteq (x^2+1)$.

For any $p(x) \in \ker(\varphi)$, write

$$p(x) = (x^2+1)q(x) + r(x)$$

for $q(x), r(x) \in \mathbb{C}[x]$ with $\deg r < 2$.

Then $r(x) = r_0 + r_1 x$, $r_0, r_1 \in \mathbb{R}$.

Since $p(x) \in \ker(\varphi)$ and $x^2+1 \in \ker(\varphi)$,

notice that

$$r(x) = p(x) - (x^2+1)q(x) \in \ker(\varphi).$$

So $0 = r(i) = r_0 + r_1 i$

$$\Rightarrow r_0 = 0 \quad \text{and} \quad r_1 = 0.$$

So $r(x) = r_0 + r_1 x = 0$, so

$$p(x) = (x^2+1)q(x)$$

Hence $\ker(\varphi) = (x^2+1)$.

To summarize, $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ is a surjective ring homomorphism with $\ker(\varphi) = (x^2+1)$, so

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

But $\mathbb{C}$ is a field, so (x^2+1) is automatically maximal.

Next time: more on maximal ideals.