Lecture 3.1

Last time:

- An ideal in a ring A is an additive subgroup $I \subseteq A$ with the property that for all $x \in I$ and $a \in A$, $ax, xa \in I$.

- The kernel of a ring map $\varphi: A \to B$ is always an ideal of A.

- For any $x \in A$, the principal ideal generated by x is

$$(x) = \{axb \mid a, b \in A\}.$$

$$= \{ax \mid a \in A\} \text{ if } A \text{ is commutative}$$

- A commutative ring $\mathbb{F}$ is a field exactly when (0) and (1) are its only ideals.

(0) and (1) are its only ideals.

$\boxed{\text{Corollary}}$ Suppose $\varphi : \mathbb{F} \longrightarrow B$ is a ring homomorphism, where $\mathbb{F}$ is a field. Then either $B = 0$ or φ is injective.

Pf: By last time, either

$$\ker(\varphi) = (0) \quad \text{or} \quad \ker(\varphi) = \mathbb{F}.$$

Case 1: $\ker(\varphi) = (0)$. Then φ is injective because φ is an (additive group homomorphism $(\mathbb{F},+) \to (B,+)$).

Case 2: $\ker(\varphi) = \mathbb{F} \implies \varphi = 0$.

But $1 = \varphi(1) = 0 \implies B = 0$. $\square$

Corollary Any homomorphism $\varphi : \mathbb{F}' \to \mathbb{F}$ between fields is injective.

Ring Isomorphism Theorems

Recall that for a group homomorphism $\varphi : G \to G'$, we have $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

To write down a version for rings, we first need to prove:

Prop Let A be a ring and $I \subseteq A$ an ideal. Then the abelian group

$$A/I = \{x + I \mid x \in A\}$$

is also a ring under coset multiplication:

$$(x+I)(y+I) = xy + I.$$

Pf: This is basically the same as our proof that $\mathbb{Z}/n\mathbb{Z}$ is a ring, but let's be thorough.

Well-defined: suppose $x + I = x' + I$

and $y + I = y' + I$.

Then $x' = x + i$ for some $i \in I$

$y' = y + j$ for some $j \in I$.

Want: $\underline{x'y' \in xy + I}$. $\Longrightarrow$ $xy + I = x'y' + I$

We have: $x'y' = (x+i)(y+j)$

$= xy + \underset{I}{xj} + \underset{I}{iy} + \underset{I}{ij}$

$= xy + (\text{something in } I)$

$\in xy + I$.

<u>Associative</u>: take $x, y, z \in A$. Then

$$\big((x+I)(y+I)\big)(z+I) = (xy+I)(z+I)$$

$$= (xy)z + I$$

$$= x(yz) + I$$

$$= (x+I)(yz+I)$$

$$= (x+I)\big((y+I)(z+I)\big).$$

<u>Distributive</u> :

$$(x+I)\big((y+I)+(z+I)\big) = (x+I)\big((y+z)+I\big)$$

$$= x(y+z) + I$$

$$= (xy + xz) + I$$

$$= (xy+I) + (xz+I)$$

$$= (x+I)(y+I) + (x+I)(y+I).$$

Similarly, $\big((x+I)+(y+I)\big)(z+I) =$

$$(x+I)(z+I) + (y+I)(z+I)$$

$\ldots (y+I)(z+I).$

<u>Multiplicative identity</u>:

$$(1+I)(x+I) = 1x + I$$
$$= x + I$$

Similarly, $(x+I)(1+I) = x + I$. $\square$

$\boxed{\text{Corollary}}$ For any ring A and any ideal $I \subseteq A$, the group homomorphism

$$\pi : A \longrightarrow A/I$$
$$x \longmapsto x + I$$

is a surjective ring homomorphism with

$\ker(\pi) = I$.

$\boxed{\textbf{Theorem (First Isomorphism Theorem)}}$ For any ring homomorphism $\varphi : A \to A'$, there is an isomorphism of rings

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

Pf: Set $K = \ker(\varphi)$. We already have an isomorphism of abelian groups

$$\begin{aligned} \overline{\varphi} : A/\ker(\varphi) &\xrightarrow{\sim} \mathrm{im}(\varphi) \\ x + K &\longmapsto \varphi(x). \end{aligned}$$

We just need to check it's actually a ring homomorphism:

$$\bar{\varphi}((x+K)(y+K)) = \bar{\varphi}(xy+I)$$
$$= \varphi(xy)$$
$$= \varphi(x)\varphi(y)$$
$$= \bar{\varphi}(x+I)\bar{\varphi}(y+I).$$

$$\bar{\varphi}(1+I) = \varphi(1) = 1. \qquad \square$$

Theorem (Second Isomorphism Theorem) For any ideals $I, J \subseteq A$,

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

Theorem (Third Isomorphism Theorem) F

Theorem (Third Isomorphism Theorem) For any ideals $I, J \subseteq A$ with $I \subseteq J$, J/I is an ideal of A/I and

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

Theorem (Correspondence Theorem) For any surjective ring homomorphism $\varphi : A \twoheadrightarrow A'$, there is a bijective correspondence

$$\left\{ \begin{array}{c} \text{ideals } I \text{ of } A, \\ \ker(\varphi) \subseteq I \subseteq A \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{ideals } J \\ \text{of } A' \end{array} \right\}$$

$$I \longmapsto \varphi(I) =: I/\ker(\varphi)$$

$$\varphi^{-1}(J) \longleftarrow\!\shortmid\; J.$$

Exercise 1: Prove them!

Ex 1 Let A be a commutative ring and pick any $a \in A$. Then

$$\begin{aligned} ev_a : A[x] &\longrightarrow A \\ p(x) &\longmapsto p(a) \end{aligned}$$

is a surjective (why?) ring homomorphism with $\ker(ev_a) = (x-a)$, so by the First Isomorphism Theorem,

$$A[x]/(x-a) \cong A.$$

In particular, if $\mathbb{F}$ is a field, then $\mathbb{F}[x]/(x-a) \cong \mathbb{F}$ for any $a \in \mathbb{F}$.

By the Correspondence Theorem,

$$\left\{\begin{array}{c}\text{ideals } I \text{ with} \\ (x-a) \subseteq I \subseteq \mathbb{F}[x]\end{array}\right\} \longleftrightarrow \{\text{ideals of } \mathbb{F}\}$$

$$\longleftrightarrow \quad (0)$$

$$\longleftrightarrow \quad (1) = \mathbb{F}$$

That is, there are no ideals of $\mathbb{F}[x]$ such that $(x-a) \subsetneq I \subsetneq \mathbb{F}[x]$.

This means $(x-a)$ is what we call

a maximal ideal.

Maximal Ideals

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

Ex ② In $A = \mathbb{Z}$, all ideals are of the form (n) for $n \geq 0$. Which of these are maximal?

Observation: $(a) \subseteq (b) \iff b \mid a$.

$a \in (b)$ implies $(a) \subseteq (b)$ b/c (b) has absorption

Are there $n \in \mathbb{Z}$ s.t.

$$(n) \subsetneq (m) \subsetneq \mathbb{Z}$$

$$\Updownarrow$$

$1 \nmid m \mid n$ never holds?

Yes! (p) is maximal for p prime!

Takeaway: maximal ideals in $\mathbb{F}[x]$ and in $\mathbb{Z}$ gives us quotients that are <u>fields</u>.

Next time: more on maximal ideals, fields and polynomial rings.