Lecture 2.2

Last time:

- A ring homomorphism is a map $\varphi : A \to B$ that preserves ring structure. On your own, recall what that means.

- For any element $a \in A$ in a commutative ring, the polynomial evaluation map

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

is a ring homomorphism.

Lemma For any ring A, there exists a unique ring homomorphism $\varphi : \mathbb{Z} \to A$.

Pf : We must have $\varphi(1) = 1$, and this determines $\varphi(n)$ for any $n \in \mathbb{Z}$:

$$\varphi(n) := \underbrace{\varphi(1) + \dots + \varphi(1)}_{n \text{ times}} .$$

It follows that $\varphi(n+m) = \varphi(n) + \varphi(m)$ and $\varphi(nm) = \varphi(n)\varphi(m)$ for any $n, m \in \mathbb{Z}$. $\square$

Remark : This says that $\mathbb{Z}$ is the initial

Remark: This says that $\mathbb{Z}$ is the initial ring: it "comes first" and has arrows pointing at every other ring.

Since $\varphi : \mathbb{Z} \longrightarrow A$ is an abelian group homomorphism, it has a kernel

$$\ker(\varphi) \leq \mathbb{Z}.$$

In particular, $\ker(\varphi) = n\mathbb{Z}$ for some $n \geq 0$. This number n is called the **characteristic** of A, written $\operatorname{char} A$.

Ex: For $A = \mathbb{Z}$ itself, φ is

Ex 1 For $A = \mathbb{Z}$ itself, φ is

the identity $n \longmapsto n$ and this

has kernel $0\mathbb{Z}$, so $\operatorname{char} \mathbb{Z} = 0$.

2 For any $n \geq 1$ and $A = \mathbb{Z}/n\mathbb{Z}$,

φ is the quotient map

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

which has kernel $n\mathbb{Z}$. So $\mathbb{Z}/n\mathbb{Z}$

has characteristic n.

We will see shortly that any field has

either characteristic 0 or p for a prime p.

If $\mathbb{F}$ has characteristic p, we call $\mathbb{F}_p$ its prime subfield.

Let $\varphi : A \longrightarrow B$ be a ring homomorphism. From group theory, we know:

- $\ker(\varphi)$ is a subgroup of the abelian group $(A, +)$;
- $\operatorname{im}(\varphi)$ is a subgroup of the abelian group $(B, +)$.

$\boxed{\text{Prop}}$ For any ring homomorphism

(φ) is a subring

$\varphi: A \longrightarrow B$, $\mathrm{im}(\varphi)$ is a subring

of B.

Exercise 1: prove it!

On the other hand, $\ker(\varphi)$ is not always a subring — in fact, since subrings must contain 1 and $\varphi(1) = 1$, the only way for $\ker(\varphi)$ to be a subring of A is if $B = 0$.

So what is $\ker(\varphi)$?

Notice that for any $x \in \ker(\varphi)$

and <u>any</u> $a \in A$,

$$\left.\begin{aligned}\varphi(ax) &= \varphi(a)\varphi(x) = \varphi(a)\cdot 0 \\ &= 0.\end{aligned}\right\} \text{HW}$$

$$\Rightarrow ax \in \ker(\varphi)$$

$$\varphi(xa) = \varphi(x)\varphi(a) = \underbrace{0 \cdot \varphi(a) = 0}_{\text{same}}$$

$$\Rightarrow xa \in \ker(\varphi).$$

$\boxed{\text{Def}}$ An **ideal** in a ring A is a subgroup $I \leq (A, +)$ such that the "absorption property" holds: for every $x \in I$ and $a \in A$,

$$ax, \ xa \in I.$$

Remarks: (i) By the above, if $\varphi : A \longrightarrow B$ is a ring homomorphism then $\ker(\varphi) \subseteq A$ is an ideal.

(ii) An analogy with groups:

<u>rings</u>		<u>groups</u>
subrings	$\longleftrightarrow$	subgroups

e.g. $\mathrm{im}(\varphi)$ e.g. $\mathrm{im}(\varphi)$

ideals $\longleftrightarrow$ normal subgroups

e.g. $\ker(\varphi)$ e.g. $\ker(\varphi)$

(iii) If we only ask for $ax \in I$, I is called a left ideal of A. Likewise, right ideals only satisfy $xa \in I$. If A is commutative, then ideals = left ideals = right ideals, but these are all distinct in general!

$\boxed{\text{Def}}$ For any element $x \in A$, the set

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

is called the principal ideal generated by x.

$\boxed{\text{Lemma}}$ For any $x \in A$, (x) is an ideal.

Pf: Easy. $\square$

Remark: when A is commutative,

$$(x) = \{ ax \mid a \in A \}.$$

$\boxed{\text{Ex}}$ 3 $(0) = \{0\}$ is an ideal in any ring. Same for $(1) = A$.

4 In $\mathbb{Z}$, every ideal is an additive subgroup of $(\mathbb{Z}, +)$, hence of the form $n\mathbb{Z}$ for some $n \geq 0$. Each of these is in fact a principal ideal:

$$n\mathbb{Z} = (n).$$

Hence every ideal in $\mathbb{Z}$ is principal, making $\mathbb{Z}$ a principal ideal domain (PID).

Def An integral domain is a principal ideal domain (PID) if every ideal is principal.

5. In $A[x]$, the kernel of each evaluation map

$$ev_a : A[x] \longrightarrow A$$
$$p(x) \longmapsto p(a)$$

is a principal ideal, namely

$$\ker(ev_a) = \{ p(x) \mid p(a) = 0 \}$$
$$= \{ p(x) \mid p(x) = (x-a)\,q(x) \text{ for some } q \in A[x] \}$$
$$= (x-a).$$

However, depending on what ring A is, not all ideals in $A[x]$ need to be principal.

$\boxed{\text{Theorem}}$ A commutative ring $\mathbb{F}$ is a field if and only if the only ideals in $\mathbb{F}$ are (0) and $(1) = \mathbb{F}$.

Pf: ($\Longrightarrow$) If $\mathbb{F}$ is a field, take some ideal $I \subseteq \mathbb{F}$, $I \neq (0)$.

Then there is some $x \in I$, $x \neq 0$.

By hypothesis, $x \in \mathbb{F}^\times$, so $xy = 1$ for some $y \in \mathbb{F}^\times$.

But by the absorption property,

$$1 = xy \in I.$$

Hence $A = (1) \subseteq I$, so $I = A$.

$(\Leftarrow)$ Now suppose $\mathbb{F}$ is any commutative ring with only two ideals (0) and (1).

Take $x \in \mathbb{F} \setminus \{0\}$; want $x \in \mathbb{F}^\times$.

We have $(x) = (1)$, so in particular $1 \in (x)$, i.e. $1 = ax$ for some $a \in A$.

Thus $a = x^{-1}$ and $x \in \mathbb{F}^\times$, so $\mathbb{F}$ is a field. $\square$

Remark: there are noncommutative rings (and therefore non-fields) that only have two ideals, so the commutative hypothesis is required.

Next time: isomorphism theorems.