Warm-Up: Define

$$\varphi : \mathbb{R}[x] \to \mathbb{R}$$
$$p(x) \mapsto p(5)$$

- Show φ is a ring hom.
- Find the image and kernel of φ.

Thm: Let $\varphi : R \to S$ be a ring homomorphism. Then

① $\varphi(R)$ is a subring of S.

② $\ker \varphi$ is a subring of R.

③ For all $a \in \ker \varphi$ and $r \in R$, we have $ra \in \ker \varphi$ and $ar \in \ker \varphi$.

Proof: We already know $\varphi(R)$ is a subgroup of S and $\ker\varphi$ is a subgroup of R.

To show they are subrings, we just need closure under multiplication.

① Let $s_1, s_2 \in \varphi(R)$. Then

$$s_1 = \varphi(r_1) \quad \text{and} \quad s_2 = \varphi(r_2)$$

for some $r_1, r_2 \in R$.

Now,

$$s_1 s_2 = \varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) \in \varphi(R).$$

② Let $a_1, a_2 \in \ker\varphi$. Then

$$\varphi(a_1 a_2) = \varphi(a_1)\cdot\varphi(a_2) = 0\cdot 0 = 0,$$

so $a_1 a_2 \in \ker\varphi$.

③ Now, let $a \in \ker \varphi$ and $r \in R$. Similar to ②, we have

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)\cdot 0 = 0$$

and

$$\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0.$$

So $ra, ar \in \ker \varphi$. $\blacksquare$

<u>Cor</u>: The kernel of a ring homomorphism $\varphi: R \to S$ is an <u>ideal</u> in R.

<u>Note</u>: No special notation for ideals.

Ex: In any ring R, the sets $\{0\}$ and R are ideals.

Ex: In a field F, $\{0\}$ and F are the only ideals.

Proof: Suppose I is an ideal, $I \neq \{0\}$.
Then there is some nonzero $x \in I$.
Since F is a field, x is a unit.
Hence $\underset{\text{in } F}{x^{-1}} \cdot \underset{\text{in } I}{x} = 1 \in I$.

But now $a = a \cdot 1 \in I$ for all $a \in F$.
Thus, $I = F$. ∎

Ex: Let R be a commutative ring with 1.
For any $a \in R$, define

$$(a) = \{ ra \mid r \in R \}.$$

Then (a) is an ideal, called the principal ideal generated by a.

Proof: We show (a) is an additive subgroup:

Identity: $0 = 0 \cdot a \in (a)$. ✓

Closure: $r_1 a + r_2 a = (r_1 + r_2) a \in (a)$ ✓

Inverses: $-(r_1 a) = (-r_1) a \in (a)$ ✓

Now, for any $ra \in (a)$ and $s \in R$, we have

$$s(ra) = (sr)a \in (a),$$

so (a) is an ideal $\blacksquare$

Thm: Every ideal in $\mathbb{Z}$ is principal.

Proof: Certainly $\{0\} = (0)$ is principal.

Let $I \neq \{0\}$ be an ideal. Then I contains some positive integer (why?) so by Well-Ordering it contains a least positive integer $n \in I$.

For any $a \in I$, the division algorithm yields

$$a = nq + r,$$

where $0 \leq r < n$. But $r = a - nq \in I$, so $r = 0$ by minimality of n.

$\in I$

Thus, $a = nq$, so $I = (n) = n\mathbb{Z}$. $\blacksquare$

Ex: Similarly, every ideal in $\mathbb{R}[x]$ is principal.

Why? Polynomial long division!

Ex: The set

$$I = \{ p(x,y) \mid p(0,0) = 0 \} \subseteq \mathbb{R}[x,y]$$

is an ideal which is not principal.

Why? Both $x \in I$ and $y \in I$, but there is no polynomial $q(x,y)$ such that both x and y are multiples of q.

Def: Let R be a ring with 1. The **characteristic** of R is the smallest positive integer such that

$$n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

If there is no such positive integer, then we say R has **characteristic 0**.

Ex: $\mathbb{Z}_n$ has characteristic n

Ex: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}[x], \ldots$ have characteristic 0.

Alternative perspective:

There is a ring homomorphism

$$\varphi : \mathbb{Z} \to R$$

defined by

$$\varphi(k) = k \cdot 1 = \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} & k > 0 \\ 0 & k = 0 \\ \underbrace{(-1) + (-1) + \cdots + (-1)}_{k \text{ times}} & k < 0 \end{cases}$$

Then $\ker \varphi = n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, and n is the characteristic of R.