Recall: Let R and S be rings. The mapping $\phi : R \to S$ is a ring homomorphism if for all $a, b \in R$

$$\phi(a +_R b) = \phi(a) +_S \phi(b) \quad \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$$

On the assignment:

$$\boxed{\boxed{\text{Q8a: } \phi(0_R) = 0_S}}$$

(How can we use the idea of ring homomorphisms to prove Q8a?)

Definition 1. Let $\phi : R \to S$ be a ring homomorphism. The *kernel of* ϕ is the set

$$\ker(\phi) = \{r \in R : \phi(r) = 0_S\}$$

Observations:

- $0_R \in \ker(\phi)$
- If ϕ is one-to-one, then $\ker(\phi) = \{0_R\}$

★ It can be shown that $\ker(\phi) \leq R$.

Proof of ★. We want to show that $\ker(\phi)$ satisfies the three conditions of a subring.

- Indeed, since $0_R \in \ker(\phi)$, $\ker(\phi) \neq \emptyset$.
- ~~Let $x, y \in \ker(\phi)$ be arbitrary. We want to show that $x - y \in \ker(\phi)$.~~ If $\phi(a) = 0_S$ and $\phi(b) = 0_S$, then we want to show that $\phi(a - b) = 0_S$, i.e. $\phi(a + (-b)) = \phi(a) + \phi(-b)$. From here, we want to show that $\phi(-b) = -\phi(b)$. Indeed, since $0_R = b + (-b)$, then $\phi(0_R) = \phi(b + (-b)) = \phi(b) + \phi(-b)$, and thus, $\phi(-b) = -\phi(b)$. Finally, $\phi(a + (-b)) = \phi(a) - \phi(b) = 0 - 0 = 0$, so $a - b \in \ker(\phi)$.
- If $a, b \in \ker(\phi)$, then $\phi(a) = \phi(b) = 0$, and so

$$\phi(ab) = \phi(a)\phi(b) = 0_S \cdot 0_S = 0$$

  Therefore, $ab \in \ker(\phi)$

We have shown that $\ker(\phi) \leq R$. □

Observation:

- For every $a \in \ker(\phi)$ and $r \in R$, then $\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0_S = 0$ which implies that $ra \in \ker(\phi)$. On the other hand, $\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0$, and so $ar \in \ker(\phi)$.

The above observation is very important when we are talking about ideals.

Definition 2. An ideal (two-sided ideal) in a ring R is a subring $I \leq R$ such that for all $a \in I$ and $r \in R$, $ar, ra \in R/I$. We denote that I is an ideal of R by $I \lhd R$.

Recall in group theory, G/H denotes the factor group. In ring theory, we denote R/S to be the factor rings.

Example 1. $\ker(\phi)$ is an ideal of R.

Example 2. The evaluation function $\phi_a : \mathbb{Z}[x] \to \mathbb{Z}$ given by $\phi_a(f(x)) = f(a)$, the kernel of ϕ_a is the set

$$\ker(\phi_a) = \{g(x)x : g(x) \in \mathbb{Z}[x]\}$$

Question 1. Let R be a ring with identity and $I \lhd R$. What can we say about I if it contains a unit b?

Because R is a ring with an identity, then $b^{-1} \in R$, and so $b^{-1}b = 1 \in I$, and so $r1 = r \in I$ for all $r \in R$, so $I = R$.

Proposition 1. *Let F be a field. An ideal $I \lhd F$ is either $\{0\}$ or F.*

Proposition 2. *Let R be a ring. Then $I \lhd R$ if and only if*

1. *$I \neq \emptyset$,*
2. *For all $x, y \in I$, $a - b \in I$.*
3. *For all $x \in I$ and $y \in R$, $ar = ra \in I$*

Definition 3. Let R be a commutative ring with identity. If $x \in R$, then the set

$$\langle x \rangle = \{rx : r \in R\}$$

is called the principal ideal generated by a. More generally, if $x_1, ..., x_n \in R$, then

$$\langle x_1, ..., x_n \rangle = \{r_1x_1 + \cdots + r_nx_n : r_1, ..., r_n \in R\}$$

is called the ideal generated by a.

Exercise 1. *Show that $\langle x \rangle$ and $\langle x_1, ..., x_n \rangle$ are ideals.*

Example 3. In $\mathbb{Z}[x]$, consider the then the set

$$\begin{aligned}\langle 2, x \rangle &= \{\text{polynomials in } \mathbb{Z}[x] \text{ with even constant terms}\}\\ &= \{2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\}\end{aligned}$$

is not a principal ideal, because $x \notin \langle 2 \rangle$.

Example 4. We define on $\mathbb{Q}[x]$,

$$\langle 2, x\rangle = \{2f(x) + xg(x) : f(x), g(x) \in \mathbb{Q}[x]\} = \mathbb{Q}[x]$$

because 2 has a unit in $\mathbb{Q}[x]$.

Theorem 1. *Every ideal in $\mathbb{Z}$ is a principal ideal.*

Proof. The zero ideal $\{0\}$ is a principal ideal since $\langle 0\rangle = \{0\}$. If $I \neq \{0\} \lhd \mathbb{Z}$, then I must contain some positive integer m. Then by the Well-Ordering Principle, there exists a least positive integer n in I. Let $a \in I$ be arbitrary. Then by the division algorithm, we know that there exist integer q and r such that

$$a = nq + r$$

where $0 \leq r < n$. This equation tells us that $r = a - nq \in I$, but $r = 0$ because n is the least positive element in I. Hence, $a = nq$ implies that $I = \langle n\rangle$. $\square$