Let $R$ and $S$ be rings.

**Def.** A **homomorphism of rings** from $R$ to $S$ is a function $\varphi: R \to S$ such that for all $x, y \in R$,

- $\varphi(x+y) = \varphi(x) + \varphi(y)$ (so $\varphi: (R,+) \to (S, +)$ is a homomorphism of groups)
- $\varphi(xy) = \varphi(x) \cdot \varphi(y)$

If $R$ and $S$ both have 1, and $\varphi(1_R) = 1_S$, then $\varphi$ is called **unital**.

An **isomorphism of rings** is a homomorphism of rings that is bijective.

**Examples:**

1. $\varphi: \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(k) = [k]$ is a unital homomorphism

   $\varphi(k+l) = [k+l] = [k] + [l] = \varphi(k) + \varphi(l)$

   $\varphi(k \cdot l) = [kl] = [k][l] = \varphi(k) \cdot \varphi(l)$

2. Let $R$ be any ring with 1 and define $\varphi: \mathbb{Z} \to R$ by $\varphi(k) = \underbrace{1_R + 1_R + \ldots + 1_R}_{k \text{ times}}$. Check that this is a ring homomorphism.

**Proposition (6.2.5) Substitution principle.** Let $R$ and $S$ be commutative rings with 1, and let $\varphi: R \to S$ be a unital ring homomorphism. Pick some $a \in S$.

Then there is a unique ring homomorphism $\varphi_a: R[x] \to S$ such that, for all $r \in R$, $\varphi_a(r) = \varphi(r)$ and $\varphi_a(x) = a$.

It is given by

$$\varphi_a \left( \sum_{i=0}^{N} r_i x^i \right) = \sum_{i=0}^{N} \varphi(r_i) a^i$$
Proof. First we see that $\varphi_a$ is unique if it exists.

If $\varphi_a$ is a homomorphism such that $\varphi_a(r) = \varphi(r)$ and $\varphi_a(x) = 0$, then

$$\varphi_a \left( \sum_{i=0}^{N} r_i x^i \right) = \sum_{i=0}^{N} \varphi_a(r_i) x^i = \sum_{i=0}^{N} \varphi_a(r_i) \varphi_a(x^i)$$

$$= \sum_{i=0}^{N} \varphi_a(r_i) \varphi_a(x)^i = \sum_{i=0}^{N} \varphi(r_i) a^i$$

So $\varphi_a$ must be given by this formula if it exists.

We just need to check that this formula defines a homomorphism.

Let $p = \sum_{i=0}^{N} r_i x^i$ and $q = \sum_{j=0}^{M} r'_j x^j$ be two polynomials.

Then

$$\varphi_a(p+q) = \varphi_a \left( \sum_{i=0}^{\max(N,M)} (r_i + r'_i) x^i \right)$$

$$= \sum_{i=0}^{\max(N,M)} \varphi(r_i + r'_i) a^i = \sum_{i=0}^{\max(N,M)} (\varphi(r_i) + \varphi(r'_i)) a^i$$

$$= \sum_{i=0}^{N} \varphi(r_i) a^i + \sum_{j=0}^{M} \varphi(r'_j) a^j = \varphi_a(p) + \varphi_a(q)$$

$$\varphi_a(pq) = \varphi_a \left( \sum_{k=0}^{N+M} \left( \sum_{i=0}^{k} r_i r'_{k-i} \right) x^k \right) = \sum_{k=0}^{N+M} \varphi \left( \sum_{i=0}^{k} r_i r'_{k-i} \right) a^k$$

$$= \sum_{k=0}^{N+M} \left( \sum_{i=0}^{k} \varphi(r_i) \varphi(r'_{k-i}) \right) a^k = \left( \sum_{i=0}^{N} \varphi(r_i) a^i \right) \left( \sum_{j=0}^{M} \varphi(r'_j) a^j \right)$$

$$= \varphi_a(p) \varphi_a(q) \quad \text{by distributive law in } S.$$
Ideals

Let \((R, +, \cdot)\) and \((S, +, \cdot)\) be rings.
Let \(\varphi : R \to S\) be a ring homomorphism.

**Def.** The kernel of \(\varphi\) is
\[
\ker \varphi = \varphi^{-1}(0) = \{ r \in R \mid \varphi(r) = 0 \}.
\]

**Lemma.** \(\varphi\) is injective if and only if \(\ker \varphi = \{0\}\).

This is true because a ring homomorphism is always a homomorphism of groups \(\varphi : (R, +) \to (S, +)\).

Now for groups, the kernel is always a normal subgroup.
For rings, the kernel is a special kind of subgroup, called an ideal:

**Def.** An ideal in a ring \(R\) is a subset \(I \subseteq R\) such that
- \(I\) is a subgroup of \(R\) with respect to addition;
  \[ a, b \in I \implies a + b \in I \text{ and } -a \in I. \]
- \(I\) is closed under multiplication by elements of \(R\);
  \[ a \in I, r \in R \implies ra \in I \text{ and } ar \in I. \]

In the case where \(R\) is non-commutative, we say that
- \(I\) is a left ideal if \(a, r \in I \implies ra \in I\)
  (but not necessarily \(ar \in I\))
- \(I\) is a right ideal if \(a, r \in I \implies ar \in I\)
  (but not necessarily \(ra \in I\))

In this context, we say \(I\) is a two-sided ideal
(or simply \(I\) -ideal) if it is both a left and right ideal.
Proposition (6.2.15) If \( \phi : R \to S \) is a ring homomorphism, then \( \ker(\phi) \) is an ideal in \( R \).

Proof: Since \( \phi : (R,+) \to (S,+) \) is a homomorphism of groups, its kernel is a subgroup.

Let \( r \in R \) and \( a \in \ker(\phi) \), then

\[
\phi(ra) = \phi(r) \phi(a) = \phi(r) \cdot O = O = \phi(ra) = O \cdot \phi(r) = O \Rightarrow ra \in \ker(\phi)
\]

\[
\phi(ar) = \phi(a) \phi(r) = O \cdot \phi(r) = O \Rightarrow ar \in \ker(\phi)
\]

Example (i) \( \phi : \mathbb{Z} \to \mathbb{Z}_n \)

\[
\ker(\phi) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z} \} \text{ all multiples of } n.
\]

Example (ii) Let \( K \) be a field, \( a \in K \) define \( \phi_a : K[x] \to K \)

to be the unique homomorphism such that \( \phi_a(r) = r \) for \( r \in K \)

and \( \phi_a(x) = a \). If \( f(x) \) is a polynomial, we have

\[
\phi_a(f(x)) = f(a).
\]

So \( \ker(\phi_a) = \{f \mid f(a) = 0\} \) This is the set of polynomials that become 0 under the substitution \( x \to a \). This is the set of polynomials that have \( a \) as a root.

Proposition (a) The intersection of ideals is an ideal:

If \( \exists I_x \in \{I_i \in R \mid a \in A \} \) are ideals in \( R \), then \( \bigcap I_x \) is an ideal in \( R \).

(b) If \( I \) and \( J \) are ideals in \( R \), then

\[
I : J = \{a_i b_1 + \cdots + a_j b_j \mid s \geq 1, a_i \in I, b_j \in J\}
\]

is an ideal in \( R \) and \( I : J \subseteq I \cap J \)

(c) If \( I \) and \( J \) are ideals in \( R \) then

\[
I + J = \{a + b \mid a \in I, b \in J\}
\]
is an ideal in \( R \).