3.4 Lecture 12: The Fundamental Homomophism Theorem

If $\phi : R \longrightarrow S$ is a ring homomorphism, then the image of ϕ is basically a copy of the factor ring $R/\ker\phi$. To give a precise meaning to "basically a copy of", we need a few concepts and words.

Definition 43. *Let $\phi : R \longrightarrow S$ be a ring homomorphism. Then ϕ is called an isomorphism if*

1. *ϕ is surjective (onto); i.e.* $\mathrm{Im}\phi = S$*, and*
2. *ϕ is injective (one-to-one) i.e. $\phi(r_1) \neq \phi(r_2)$ whenever $r_1 \neq r_2$ in* R.

NOTE: ϕ is injective if and only if $\ker\phi$ is the zero ideal of R.
To see this, first suppose ϕ is injective. Then $\ker\phi = \{0_R\}$, otherwise if $r \in \ker\phi$ for some $r \neq 0$ we would have $\phi(r) = \phi(0_R)$, contrary to the injectivity of ϕ.

On the other hand suppose $\ker\phi = \{0_R\}$. Then if there exist elements r_1 and r_2 of R with $\phi(r_1) = \phi(r_2)$ we must have $\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0_S$. This means $r_1 - r_2 \in \ker\phi$, so $r_1 - r_2 = 0_R$ and ϕ is injective.

The characterisation of injectivity in the above note can be very useful.

If $\phi : R \longrightarrow S$ is an isomorphism, then S is an "exact copy" of R. This means that S and R are structurally identical, and only differ in the way their elements are labelled. We say that R and S are *isomorphic* and write $R \cong S$.

Theorem 44. *(The Fundamental Homomorphism Theorem) Let $\phi : R \longrightarrow S$ be a homomorphism of rings. Then the image of ϕ is isomorphic to the factor ring $R/\ker\phi$.*

Proof: Let I be the kernel of ϕ, so I is a two-sided ideal of R. Define a function $\bar{\phi} : R/I \longrightarrow \mathrm{Im}\phi$ by

$$\bar{\phi}(a + I) = \phi(a) \text{ for } a \in R.$$

1. $\bar{\phi}$ is well-defined (i.e. the image of $a+I$ does not depend on a choice of coset representative).
   Suppose that $a + I = a_1 + I$ for some $a, a_1 \in R$. Then $a - a_1 \in I$ by Lemma 42. Hence $\phi(a - a_1) = 0_S = \phi(a) - \phi(a_1)$. Thus $\phi(a) = \phi(a_1)$ as required.
2. $\bar{\phi}$ is a ring homomorphism.
   Suppose $a + I, b + I$ are elements of R/I. Then

   $$\begin{aligned} \bar{\phi}\left((a + I) + (b + I)\right) &= \bar{\phi}\left((a + b) + I\right) \\ &= \phi(a + b) \\ &= \phi(a) + \phi(b) \\ &= \bar{\phi}(a + I) + \bar{\phi}(b + I). \end{aligned}$$

   So ϕ is additive.

   Also

   $$\begin{aligned} \bar{\phi}\left((a + I)(b + I)\right) &= \bar{\phi}(ab + I) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= \bar{\phi}(a + I)\bar{\phi}(b + I). \end{aligned}$$

   So $\bar{\phi}$ is multiplicative - $\bar{\phi}$ is a ring homomorphism.
3. $\bar{\phi}$ is injective.
   Suppose $a + I \in \ker\bar{\phi}$. Then $\bar{\phi}(a + I) = 0_S$ so $\phi(a) = 0_S$. This means $a \in \ker\phi$, so $a \in I$. Then $a + I = I = 0_R + I$, $a + I$ is the zero element of R/I. Thus $\ker\bar{\phi}$ contains only the zero element of R/I.

4. $\bar{\phi}$ is surjective.
   Let $s \in \text{Im}\phi$. Then $s = \phi(r)$ for some $r \in R$. Thus $s = \bar{\phi}(r + I)$ and every element of $\text{Im}\phi$ is the image under $\bar{\phi}$ of some coset of I in R.

Thus $\bar{\phi} : R/\ker\phi \longrightarrow \text{Im}\phi$ is a ring isomorphism, and $\text{Im}\phi$ is isomorphic to the factor ring $R/\ker\phi$. $\square$