Lecture 35  Homomorphisms of rings

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 $x, y \in R$,
\begin{align*}
  \varphi(x+y) &= \varphi(x) + \varphi(y) \quad \text{(so $\varphi : (R,+) \to (S,+)$ is a homomorphism of groups)} \\
  \varphi(xy) &= \varphi(x) \cdot \varphi(y)
\end{align*}

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

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

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 \( \varphi_a(x) = \varphi(x) \),

\[
\begin{align*}
\varphi_a \left( \sum_{i=0}^{N} r_i x^i \right) &= \sum_{i=0}^{N} \varphi_a(r_i x^i) = \sum_{i=0}^{N} \varphi_a(r_i) \varphi_a(x^i) \\
&= \sum_{i=0}^{N} \varphi_a(r_i) \varphi_a(x)^i = \sum_{i=0}^{N} \varphi(r_i) a^i
\end{align*}
\]

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,

\[
\begin{align*}
\varphi_a(p+q) &= \varphi_a \left( \sum_{i=0}^{\max(N,M)} cr_i + r'_i x^i \right) \\
&= \sum_{i=0}^{\max(N,M)} \varphi(c r_i + r'_i) a^i = \sum_{i=0}^{\max(N,M)} (\varphi(c r_i) + \varphi(r'_i)) a^i \\
&= \sum_{i=0}^{N} \varphi(r_i) a^i + \sum_{j=0}^{M} \varphi(r'_j) a^j = \varphi_a(p) + \varphi_a(q)
\end{align*}
\]

\[
\begin{align*}
\varphi_a(pq) &= \varphi_a \left( \sum_{k=0}^{N+M} \left( \sum_{i=0}^{k} r_i r'_{k-i} \right) x^k \right) = \sum_{k=0}^{N+M} \varphi(\sum_{i=0}^{k} r_i r'_{k-i}) a^k \\
&= \sum_{k=0}^{N+M} \left( \sum_{i=0}^{k} \varphi(r_i) \varphi(r'_{k-i}) \right) a^k = \left( \sum_{i=0}^{N} \varphi(r_i) a^i \right) \left( \sum_{j=0}^{M} \varphi(r'_j) a^j \right) \\
&= \varphi_a(p) \varphi_a(q) \quad \text{by distributive law in } S.
\end{align*}
\]