Lecture 25 Homomorphisms of rings

Let R and S be rings.

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

- $\varphi(x+y) = \varphi(x) + \varphi(y)$
- $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

(so $\varphi : (R,+) \to (S,+)$ is a homomorphism of groups)

If R and S both have 1, and $\varphi(1_R) = 1_S$, then φ is called <u>unital</u>.

An <u>isomorphism of rings</u> is a homomorphism of rings that is bijective.

<u>Examples</u>: (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 $\varphi(k) = \underbrace{1_R + 1_R + \cdots + 1_R}_{k \text{ times}}$. Check that this is a ring homomorphism. (uses distributive law in R)

<u>Proposition</u> (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 φ_a is unique if it exists:

If φ_a is a homomorphism such that $\varphi_a(r)=\varphi(r)$ and $\varphi_a(x)=a$, 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 φ_a <u>must</u> 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

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

$$= \sum_{i=0}^{\mathrm{Max}(M,N)} \varphi(r_i + r_i')a^i = \sum_{i=0}^{\mathrm{Max}(M,N)} (\varphi(r_i)+\varphi(r_i'))\, a^i$$

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

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

$$= \sum_{k=0}^{N+M}\left(\sum_{i=0}^{k} \varphi(r_i)\,\varphi(r_{k-i}')\right)a^k = \left(\sum_{i=0}^{N} \varphi(r_i)a^i\right)\left(\sum_{j=0}^{M} \varphi(r_j')a^j\right)$$

$$= \varphi_a(p)\,\varphi_a(q)$$

by distributive law in S.

Ideals

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

<u>Def</u> The <u>kernel</u> of φ is
$$\ker\varphi = \varphi^{-1}(0) = \{r \in R \mid \varphi(r) = 0\}$$

<u>Lemma</u> φ 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 subring called an ideal:

<u>Def</u>: An <u>ideal</u> in a ring R is a subset $I \subseteq R$ such that
- I is a subgroup of R with respect to addition:
  $a, b \in I \Rightarrow a+b \in I$ and $-a \in I$.
- I is closed under multiplication by elements of R.
  $a \in I, r \in R \Rightarrow ra \in I$ and $ar \in I$

In the case where R is non-commutative, we say that
I is a <u>left ideal</u> if $a, r \in I \Rightarrow ra \in I$
(but not necessarily $ar \in I$)
I is a <u>right ideal</u> if $a, r \in I \Rightarrow ar \in I$
(but not necessarily $ra \in I$)
In this context, we say I is a <u>two sided ideal</u> (or simply <u>Ideal</u>) if it is both a left and right ideal.

<u>Proposition</u> (6.2.15) If $\varphi : R \to S$ is a ring homomorphism, then $\ker(\varphi)$ is an ideal in R.

<u>Proof</u>: Since $\varphi : (R,+) \to (S,+)$ is a homomorphism of groups, its kernel is a subgroup.
Let $r \in R$ and $a \in \ker(\varphi)$ then
$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)\cdot 0 = 0 \Rightarrow ra \in \ker(\varphi)$$
$$\varphi(ar) = \varphi(a)\varphi(r) = 0\cdot\varphi(r) = 0 \Rightarrow ar \in \ker(\varphi) \quad \blacksquare$$

<u>Example</u> (i) $\varphi : \mathbb{Z} \to \mathbb{Z}_n \quad \varphi(k) = [k]_n$
$\ker(\varphi) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ all multiples of n.

(ii) Let K be a field, $a \in K$ define $\varphi_a : K[x] \to K$ to be the unique homomorphism such that $\varphi_a(r) = r$ for $r \in K$ and $\varphi_a(x) = a$. If $f(x)$ is a polynomial, we have
$$\varphi_a(f) = f(a).$$

So $\ker \varphi_a = \{f \mid f(a) = 0\}$ 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.

<u>Proposition</u> (a) The intersection of ideals is an ideal:
If $\{I_\alpha\}_{\alpha \in A}$ are ideals in R, then $\bigcap_{\alpha \in A} I_\alpha$ is an ideal in R

(b) If I and J are ideals in R, then
$$I\cdot J := \{a_1 b_1 + \cdots + a_s b_s \mid s \geq 1 \ \ a_i \in I \ \ b_j \in J\}$$
is an ideal in R and $I\cdot J \subseteq I \cap J$

(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.