Last time: Defined rings, subrings, ring homomorphisms.

Recall: A subset I of a ring R is an ideal if

1) I is a subgroup of $(R,+,0)$ (so $\forall x,y \in I$, $x-y \in I$)
2) $\forall r \in R$, $\forall x \in I$, $r \cdot x$, $x \cdot r \in I$

A ring R is a field if R is commutative and $\forall x \in R, x \neq 0$ $\exists y \in R$ s.t. $x \cdot y = 1$. That is, any $x \in R$, $x \neq 0$ is a unit.

Remarks
- For any ring R, $\{0\}$ and R are ideals in R.
- $\mathbb{Z} \subseteq \mathbb{Q}$ is a subring. It's not an ideal: $\frac{1}{2} \in \mathbb{Q}$, $1 \in \mathbb{Z}$ but $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$.

We saw:
- if $f: R \to R'$ is a ring homomorphism then $\ker f := \{r \in R \mid f(r) = 0\}$ is an ideal in R.
- if $I \subseteq R$ is an ideal and $1 \in I$ then $I = R$.

Lemma 26.1 Suppose R is a ring, $I \subseteq R$ an ideal and suppose I contains a unit. Then $I = R$.

Proof Suppose $u \in I$ is a unit. Then $\exists v \in R$ s.t. $v \cdot u = 1$
$\Rightarrow 1 = v \cdot u \in I$. $\Rightarrow I = R$.

Corollary 26.2 The only ideals in a field F are $\{0\}$ and F.

Proof Suppose $I \subseteq F$ is an ideal and $I \neq \{0\}$. Then $\exists x \in I$ s.t. $x \neq 0$. Since F is a field, x is a unit. By 26.1, $I = F$.

Corollary 26.3 Suppose $f: F \to R$ is a ring homomorphism and F is a field. Then either f is 1-1 or

$f(x) = 0$ for all $x \in F$.

__Proof__ $\ker f$ is an ideal in F. By 26.2 either $\ker f = \{0\}$ (and then f is 1–1) or $\ker f = F$ (and then $F(x) = 0 \; \forall x \in F$).

__Polynomial rings.__

Let R be a commutative ring (with 1)

$R[x] = \{ a_0 + a_1 x + \dots + a_n x^n \mid n \geq 0, \; a_0, \dots a_n \in R \}$

We've seen polynomial rings when $R = \mathbb{Q}$ or $\mathbb{R}$. But they make sense for __any__ commutative ring

__Lemma 26.4__ Let $f: R \to S$ be a ring homomorphism. Then $f(R) = \{ f(r) \mid r \in R \}$ is a subring of S.

__Proof__ Since f is a group homomorphism, $f(R)$ is a subgroup of $(S, +, 0_S)$.

Remain to check that $f(R)$ is closed under multiplication.

$s_1, s_2 \in f(R) \Rightarrow s_1 = f(x_1), \; s_2 = f(x_2)$ for some $x_1, x_2 \in R$

$\Rightarrow s_1 \cdot s_2 = f(x_1) f(x_2) = f(x_1 x_2) \in f(R)$ $\square$

__Proposition 6.2.5__ Suppose R, S are two commutative rings (with $\varphi(1_R) = 1_S$), $\varphi: R \to S$ a ring homomorphism, $a \in S$. Then there is a unique ring homomorphism $\varphi_a : R[x] \to S$ with

$\varphi_a(x) = a$ and $\varphi_a(r) = \varphi(r)$ for all $r \in R$.

__Proof__ (uniqueness) Suppose ψ_1, ψ_2 are two such homomorphisms, $p(x) = r_0 + r_1 x + \dots + r_n x^n \in R[x]$ a polynomial.

Then $\psi_1(p(x)) = \psi_1(r_0 + r_1 x + \dots + r_n x^n) = \psi_1(r_0) + \psi_1(r_1)\psi_1(x) + \dots + \psi_1(r_n)(\psi_1(x))^n = \varphi(r_0) + \varphi(r_1) a + \dots + \varphi(r_n) a^n$

Similarly $\psi_2(p(x)) = \varphi(r_0) + \varphi(r_1) a + \dots + \varphi(r_n) a^n$.

So $\Rightarrow \psi_1(p(x)) = \psi_2(p(x)) \quad \forall\, p(x) \in R[x]. \Rightarrow \psi_1 = \psi_2.$

(Existence) Define $\varphi_a : R[x] \to S$ by

$$\varphi_a\left(\sum_{i=0}^{n} r_i x^i\right) = \sum_{i=1}^{n} \varphi(r_i) a^i. \quad [\text{if } n=0, \text{ we set } \varphi_a(r) = \varphi(r)]$$

Then $\varphi_a(r) = \varphi(r) \quad \forall\, r \in R$

and $\varphi_a(x) = \varphi_a(1_R x) = \varphi(1_R) a = 1_S \cdot a = a.$

Also φ_a is a homomorphism:

$$\varphi_a\left(\left(\sum_{i=0}^{n} r_i x^i\right) \cdot \left(\sum_{j=0}^{k} t_j x^j\right)\right) = \varphi_a\left(\sum_{i,j} r_i t_j x^{i+j}\right)$$

$$= \sum_{i+j} \varphi(r_i t_j) a^{i+j} = \sum_{i+j} \varphi(r_i)\varphi(t_j) a^i a^j = \left(\sum \varphi(r_i) a^i\right)\left(\sum \varphi(t_j) a^j\right)$$

$$= \varphi_a\left(\sum r_i x^i\right) \varphi_a\left(\sum t_j x^j\right)$$

Similarly φ_a preserves $+$, Hence φ_a is a homomorphism.

"Applications"

Corollary 6.2.8 A homomorphism $\psi : R \to S$ of commutative rings (with $\varphi(1_R) = 1_S$) defines a unique homomorphism $\tilde{\psi} : R[x] \to S[y]$ of polynomial rings with $\tilde{\psi}\left(\sum r_i x^i\right) = \sum \psi(r_i) y^i$.

Proof Consider $\varphi : R \to S[y]$, $\varphi(r) = \psi(r)$ ← thought of as a degree 0 polynomial in $S[x]$.

φ is a homomorphism, and $\varphi(1_R) = \psi(1_R) = 1_S$.

Take $a = y$. Then $\varphi_a\left(\sum r_i x^i\right) = \sum \varphi(r_i) y^i = \sum \psi(r_i) y^i$.

Ex $R = \mathbb{Z}$, $S = \mathbb{Z}_n$ $\pi : \mathbb{Z} \to \mathbb{Z}_n$ $\pi(k) = [k]$.

$\tilde{\pi} : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$, $\tilde{\pi}\left(\sum k_i x^i\right) = \sum [k_i] x^i$

"reduction of coefficients modulo n."

Ex (Evaluation map) For any commutative ring R and any $a \in R$ we have

$$ev_a : R[x] \to R, \quad ev_a\left(\sum r_i x^i\right) = \sum r_i a^i$$

In terms of 6.25 $\quad ev_a = \varphi_a$ where $\varphi(r) = r \ \forall r \in R$

<u>Remark</u> We have seen that for any ring homomorphism $f : R \to S$, $\ker f$ is an ideal in R.

<u>Q.</u> What ideal is $\ker(ev_a : R[x] \to R)$?

<u>A.</u> $\ker(ev_a) = \{p(x) \mid ev_a(p) = 0\}$

$ev_a(\Sigma r_i x^i) = \Sigma r_i a^i = p(a)$!

So $\ker(ev_a) = \{p(x) \in R[x] \mid p(a) = 0\}$

$= \{p(x) \in R[x] \mid a \text{ is a root of } p\}$.

<u>WARNING</u> Given $p(x) \in R[x]$ we can evaluate it at <u>any</u> $a \in R$.

This gives us a function $R \to R$, $a \mapsto p(a)$.

<u>Note</u> <u>Different</u> polynomials can define the <u>same</u> function

<u>Ex</u> $R = \mathbb{Z}_p$ (p prime) $\quad \forall a \in \mathbb{Z}_p \quad a^p = a$

(if $a \neq 0$, $a^{p-1} = 1$, so $a^p = a$. if $a = 0$, $a^p = 0 = a$.)

$\Rightarrow p(x) = x^p$ and $q(x) = x$ define the <u>same</u> function

<u>Ex</u> $R = \mathbb{Z}_n$, $n > 0$. The set of polynomials $\mathbb{Z}_n[x]$ is infinite:

$\forall k \in \mathbb{N}, \quad x^k \in \mathbb{Z}_n[x]$.

The # of functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ is n^n, which is <u>finite</u>.

<u>Moral</u> For general rings R elements of $R[x]$ are <u>not</u> functions. There is a map

$$\psi : R[x] \to \mathrm{Map}(R, R) := \{f : R \to R \mid f \text{ a function}\}$$

$$p \mapsto (a \mapsto p(a))$$

But ψ need not be 1-1 or onto.

(If $R = \mathbb{Z}_n$ it's not 1-1, if $R = \mathbb{R}$, it's not onto