Rings of Polynomials :

- R commutative ring with identity

Def: The *polynomial ring* $R[x]$ with coefficients in R is the set whose elements are

$$R[x] = \left\{ \sum_{k=0}^{n} r_k x^k \;\middle|\; \begin{array}{l} r_0, r_1, \dots, r_n \in R \\ n \geq 0 \text{ integer} \end{array} \right\}$$

- $$\left(\sum_{k=0}^{n} r_k x^k\right) + \left(\sum_{k=0}^{n} s_k x^k\right) = \sum_{k=0}^{n} (r_k + s_k)\, x^k$$

- $$\left(\sum_{j=0}^{m} r_j x^j\right) \cdot \left(\sum_{k=0}^{n} s_k x^k\right) = \sum_{j=0}^{m} \sum_{k=0}^{n} r_j s_k\, x^{j+k}$$

Operations $\cdot$ and $+$ make $R[x]$ a ring.

Ex: $\mathbb{Q}[x]$ elements include $x+1$, $x^2 + 3x + \frac{5}{9}$, $\frac{1}{2}x + 4$

Ex: $R[x]$ where $R = \mathbb{Q}[y]$

elements include

$$\underbrace{(y^2+2)}_{\text{coeffs}} \underline{x^2} + \underbrace{\left(\tfrac{3}{2}y + 1\right)}_{\text{coeffs}} \underline{x} + \underline{4}$$

$R[x] = \mathbb{Q}[x,y]$ multi-variate poly's in variables x and y.

Ex: $\mathbb{Z}_2[x]$ elements include x, $x+1$, x^2+1, x^2+x+1, x^3+x

$$(x+1)(x+1) = x^2 + x + x + 1 = x^2 + \underbrace{(1+1)}_{=0}x + 1 = x^2 + 1$$

$$(x+1)^2 = x^2 + 1^2 = x^2+1.$$

Freshman's Dream:

Let p be prime

Consider $x+a \in \mathbb{Z}_p[x]$.

Then

$$(x+a)^p = x^p + a^p$$

Let R be a subring of a ring S.

Def: Take $s \in S$.

The **evaluation homomorphism** is

$$\phi_s : R[x] \longrightarrow S$$

$$\sum_{k=0}^{n} r_k x^k \longmapsto \sum_{k=0}^{n} r_k s^k$$

NOTATION: we write $R[s]$ to mean the image of ϕ_s.

Ex: $R = \mathbb{Z} \subseteq \mathbb{R} = S$ Choose $\sqrt{2} \in S$

$$\underline{\phi_{\sqrt{2}}\left(\sum_{k=0}^{n} r_k x^k\right)} = \sum_{k=0}^{n} r_k (\sqrt{2})^k \quad \text{where } r_0, r_1, \dots, r_n \in \mathbb{Z}$$

$\operatorname{img} \phi_{\sqrt{2}} = \mathbb{Z}[\sqrt{2}] \leftarrow$ question: what is this?

$$\sum_{k=0}^{n} r_k (\sqrt{2})^k = \sum_{k=0}^{\lfloor n/2 \rfloor} r_{2k} (\sqrt{2})^{2k} + \sum_{k=0}^{\lfloor n/2 \rfloor} r_{2k+1} (\sqrt{2})^{2k+1}$$

$$= \underbrace{\sum_{k=0}^{\lfloor n/2 \rfloor} r_{2k} 2^k}_{\in \mathbb{Z}} + \underbrace{\sum_{k=0}^{\lfloor n/2 \rfloor} r_{2k+1} 2^k}_{\in \mathbb{Z}} \underbrace{\sqrt{2}}_{\sqrt{2}}$$

$$\boxed{\mathbb{Z}[\sqrt{2}] = \{ a + \sqrt{2}\, b \mid a, b \in \mathbb{Z} \}}$$

David's Idea

$R = \mathbb{R}$ $\quad S = \mathbb{C}$ $\quad i \in S$

$$\phi_i : \mathbb{R}[x] \to \mathbb{C}$$
$$p(x) \mapsto p(i) \qquad \sum_{k=0}^{n} r_k x^k \mapsto \sum_{k=0}^{n} r_k i^k$$

$$\operatorname{rng} \phi_i = \mathbb{R}[i] = \left\{ \sum_{k=0}^{n} r_k i^k \,\middle|\, n \geq 0 \text{ integer}, r_0, \dots, r_n \in \mathbb{R} \right\}$$
$$= \{ a + ib \mid a, b \in \mathbb{R} \} = \mathbb{C}$$

$\mathbb{C} = \mathbb{R}[i]$

Ex: $R = \mathbb{Q}$, $S = \mathbb{R}$
$\pi \in \mathbb{R}$

$$\phi_\pi : \sum_{k=0}^{n} r_k x^k \mapsto \sum_{k=0}^{n} r_k \pi^k$$

Since π is not a root of any polynomial

$$\mathbb{Q}[\pi] = \{ r_0 + r_1 \pi + r_2 \pi^2 + \dots + r_n \pi^n \mid n \geq 0 \text{ integer}, r_0, \dots, r_n \in \mathbb{Q} \}$$

Def: If $R \subseteq S$ are rings and $\alpha \in S$ we call $R[\alpha]$ the extension of R by α.

Ex: $\mathbb{Z}[i]$ is called the Gaussian integers

$$\mathbb{Z}[i] = \{ a + ib \mid a, b \in \mathbb{Z} \}.$$

Ex: $\mathbb{Z}[\frac{1}{2}]$ contains $\mathbb{Z}$ and $\frac{1}{2}\mathbb{Z}$ and $\frac{1}{4}\mathbb{Z}$.

$$\mathbb{Z}[\tfrac{1}{2}] = \left\{ \frac{m}{2^k} \;\middle|\; m, k \text{ integers}, \; k \geq 0 \right\}.$$

Localization.

~~Locolization~~

Ex: $R = \mathbb{Q}[x]$, $\quad S = \mathbb{Q}(x)$

$$R[\tfrac{1}{x}] = \mathbb{Q}[x][\tfrac{1}{x}] = \left\{ \frac{p(x)}{x^k} \;\middle|\; p(x) \in \mathbb{Q}[x], \; k \geq 0 \text{ integer} \right\}$$

"Laurent polynomials"

Back to ring homomorphisms

Ideals and Quotients

Recall: A ring homomorphism $\phi : R \to R'$ is a function which satisfies

- $\phi(a+b) = \phi(a) + \phi(b)$
- $\phi(ab) = \phi(a)\phi(b)$

The kernel of ϕ is $\ker \phi = \{ r \in R \mid \phi(r) = \phi \}$

NOTE! $\ker \phi$ is not a subring.

Def: Let R be a commutative ring. An ideal $I \subseteq R$ satisfying

- ✓ $a + b \in I$ for all $a, b \in I$
- ✓ $ar \in I$ for all $a \in I$ and $r \in R$.

Proposition: Let $\phi: R \to R'$ be a ring homomorphism. Then $\ker\phi$ is an ideal!

Proof:

$a, b \in \ker\phi \Rightarrow \phi(a)=0, \phi(b)=0$

$\phi(a+b) = \phi(a)+\phi(b) = 0+0 = 0$

$a+b \in \ker\phi$

$a \in \ker\phi, r \in R$ $\quad \phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$

$ar \in \ker\phi$

Ex: Consider the ring homomorphism

$$\phi_{\sqrt{2}} : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\sqrt{2}]$$

$$\ker(\phi_{\sqrt{2}}) = \{p(x) \in \mathbb{Q}[x] \mid \phi_{\sqrt{2}}(p(x)) = 0\}$$

$$= \{p(x) \in \mathbb{Q}[x] \mid p(\sqrt{2}) = 0\}$$

$$= \{p(x) \in \mathbb{Q}[x] \mid p(x) \text{ has } \sqrt{2} \text{ as a root}\}$$

$$= \{x^2-2, kx^2-2k, 0, x^3-2x, p(x)(x^2-2), \ldots\}$$

$$= \{(x^2-2)p(x) \mid p(x) \in \mathbb{Q}[x]\}.$$

ideal generated by x^2-2

Def: The ideal generated by $a \in R$ is

$\langle a \rangle = \{ra \mid r \in R\}$.

Prop: $\langle a \rangle$ is an ideal.

Proof:

Take $\alpha, \beta \in \langle a \rangle$. Then $\alpha = ra$ with $r \in R$

$\beta = sa$ with $s \in R$

$$\alpha + \beta = ra + sa = \underbrace{(r+s)}_{\in R}a \in \langle a \rangle$$

Take $t \in R$ NTS $\alpha t \in \langle a \rangle$

$$\alpha t = rat = (rt)a \in \langle a \rangle$$

$\square$

<u>Quotient Ring</u>

<u>Def</u>: Let R be a commutative ring, $I \subseteq R$ ideal.
The <u>quotient ring</u> R/I is the set

$$R/I = \{ r + I \mid r \in R \}$$

with binary operations:

- $(r+I) + (s+I) = (r+s) + I$
- $(r+I)(s+I) = rs + I$