Lecture 2:

02 September 2020 18:10

* Let R be a (comm) ring with unity.

Recall an <u>ideal</u> I of R is subset s.t. $\forall a,b\in I$ $a+b\in I$ and $\forall r\in R$ & $a\in I$, $ra\in I$.

A <u>subring</u> R_1 of R is a subset s.t. $\forall a,b\in R_1$, $a-b$ & ab are in R_1.

<u>Examples</u>: 1) $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\}$ is a subring of $\mathbb{R}$

$(a+b\sqrt{2})(c+d\sqrt{2}) = ac+2bd+(ad+bc)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$.

2) $\mathbb{Z}[\frac{1}{2}]\subseteq\mathbb{Q}$ smallest subring of $\mathbb{Q}$ containing $\mathbb{Z}$ & $\frac{1}{2}$.

$\mathbb{Z}[\frac{1}{2}]=\{\frac{a}{2^n} \mid a\in\mathbb{Z},\ n\geq 0, n\in\mathbb{Z}\}=: R$

Pf: $R\supseteq\mathbb{Z}[\frac{1}{2}]$ ✓

Let $\alpha\in R$ then $\alpha=\frac{a}{2^n}$ for some $a\in\mathbb{Z}$ & $n\geq 0$.

$\Rightarrow \alpha = a\cdot(\frac{1}{2})^n\in\mathbb{Z}[\frac{1}{2}] \Rightarrow R\subseteq\mathbb{Z}[1/2]$.

3) $\mathbb{Z}[\pi]\subseteq\mathbb{R}$; $\mathbb{Z}[\pi]=\{a_0+a_1\pi+a_2\pi^2+\dots+a_n\pi^n \mid n\geq 0,\ a_0,\dots,a_n\in\mathbb{Z}\}$

* $\mathbb{Z}[i]\subseteq\mathbb{C}$ is similar to $\mathbb{Z}[\sqrt{2}]$, i.e. $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$. Are they isomorphic?

* A map $\phi:(R_1,+,\cdot)\longrightarrow(R_2,\oplus,\odot)$ is said to be a ring homo. if

$$\phi(a+b)=\phi(a)\oplus\phi(b)$$
$$\phi(a\cdot b)=\phi(a)\odot\phi(b)$$

$\phi:\mathbb{Z}[\sqrt{2}]\to\mathbb{Z}[\ \subseteq\mathbb{C}$

$\phi(\sqrt{2})=?$

$\phi(\sqrt{2})\phi(\sqrt{2}) = \phi(2) = 2\phi(1) =$

$\Rightarrow \phi(\sqrt{2}) = \sqrt{2}$ or $-\sqrt{2}$

* Intersection of subrings of a ring is a subring.

<u>Pf:</u> Let R be ring & $\{R_\alpha \mid \alpha\in\Omega\}$ be a collection of subrings of R. Ω an indexing set.

Let $R_0=\bigcap_{\alpha\in\Omega}R_\alpha$. Then R_0 is a subring

R_0 is an additive subgroup of R.

$a,b\in R_0 \Rightarrow a,b\in R_\alpha\ \forall\alpha\in\Omega \Rightarrow a\cdot b\in R_0$

$\Rightarrow a\cdot b\in R_\alpha$ "

∎

Polynomial ring

Let $(R,+,\cdot)$ be a (commutative) ring with unity.

The polynomial ring $R[x]$ over R consists of polynomials with coefficients in R with polynomial addition and multiplication as the binary operators.

A typical element of $R[x]$ is

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0$$

where a_i's are in R.

Formally $R[x] := \{ a : \mathbb{Z}_{\geq 0} \to R \mid$ for some $n \geq 0$, $a(i) = 0 \ \forall\, i > n \}$. For $a, b \in R[x]$

$$(a \oplus b)(n) = a(n) + b(n) \quad \text{for } n \in \mathbb{Z}_{\geq 0}$$

$$(a \odot b)(n) = \sum_{i=0}^{n} a(i)\cdot b(n-i) \quad \text{for } n \in \mathbb{Z}_{\geq 0}$$

<u>Prop:</u> $(R[x], \oplus, \odot)$ is a ring with unity. If R is commutative then so is $R[x]$.

(*) $a \in R[x]$ is denoted as

$$a(n)\, x^n + a(n-1)\, x^{n-1} + \dots + a(0)$$

where $n = \max\{ i \mid a(i) \neq 0 \}$ is called the degree of a.

Pf: $(R[x], \oplus)$ is an abelian group.

- $a \in R[x]$ then $b(n) := -a(n)$ $\forall n \in \mathbb{Z}_{\geq 0}$
  $b \in R[x]$ & $a \oplus b = 0$ ← the zero function.
  where $0(i) = 0_R$. check 0 function is the additive identity
- $\oplus$ is assoc.
- $\odot$ is assoc
- Distributive laws
- $1_{R[x]}(0) = 1$, $1_{R[x]}(n) = 0$ $\forall n \geq 1$.
  then $1_{R[x]}$ is the unity of $R[x]$
- R is comm $\Rightarrow$ $R[x]$ is comm

$a, b, c \in R[x]$, $n \geq 0$

$$((a \odot b) \odot c)(n) = \sum_{i=0}^{n} (a \odot b)(i) \cdot c(n-i)$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{i} a(j) \cdot b(i-j) \cdot c(n-i)$$

$$a \odot (b \odot c)(n) = \sum_{i=0}^{n} a(i) \cdot (b \odot c)(n-i)$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{n-i} a(i) \cdot b(j) \cdot c(n-i-j)$$

set $k = i+j \Rightarrow j = k-i$

$$= \sum_{i=0}^{n} \sum_{k=i}^{n} a(i) b(k-i) c(n-k)$$

$$= \sum_{0 \leq i \leq k \leq n} a(i) b(k-i) c(n-k)$$

$$\shortparallel$$

$$= \sum_{0 \leq j \leq i \leq n} a(j) b(i-j) c(n-i)$$

(*) The map $R \xrightarrow{i} R[\cancel{x}]$ which sends

$a \longmapsto f_a$ where $f_a \begin{cases} n \longmapsto 0 & n \geq 1 \\ 0 \longmapsto a \end{cases}$

is an injective ring homo.

Pf: i is an injective function is clear.

Since $f_a = f_b \Rightarrow \underset{a}{f_a(0)} = \underset{b}{f_b(0)}$

$i(a+b) = f_{a+b}$

$f_{a+b}(n) = \begin{cases} 0 = f_a(n) + f_b(n) & \text{if } n > 0 \\ a+b = f_a(0) + f_b(0) & \text{if } n = 0 \end{cases}$

$f_{a+b}(n) = f_a(n) + f_b(n) \quad \forall\, n \in \mathbb{Z}_{\geq 0}$

$\Rightarrow f_{a+b} = f_a \oplus f_b$

$i(ab) = f_{ab}$

$i(a)\, i(b) = f_a \odot f_b$

$f_a \odot f_b\,(n) = \sum_{i=0}^{n} f_a(i) f_b(n-i)$

$= \begin{cases} 0 & n > 0 \\ ab & n = 0 \end{cases}$

$= f_{ab}$

Hence i is ring homo.