11/12/2018
M0

29.1

Last time (1) Products of ideals: if $I, J \subseteq R$ are ideals,

$I \cdot J$ = smallest ideal containing $\{ab \mid a \in I, b \in J\}$

$= \{a_1 b_1 + \cdots + a_n b_n \mid n \geq 1, a_i \in I, b_j \in J\}$.

(2) direct sum $R_1 \oplus R_2$ of rings

(3) Quotient rings R/I ($I \subseteq R$ ideal)

Example $\varphi : \mathbb{R}^2 \longrightarrow \mathbb{R}[x]/\langle x^2+1 \rangle$ where $\langle x^2+1 \rangle := (x^2+1)\mathbb{R}[x]$

$\varphi(a,b) = a + bx + (x^2+1)$

is an isomorphism of abelian groups.

We check that φ is a homomomorphism:

$\varphi((a,b)+(c,d)) = \varphi(a+c, b+d) = (a+c) + (b+d)x + \langle x^2+1 \rangle$

$= \big((a+bx) + (c+dx)\big) + \langle x^2+1 \rangle = \big(a+bx+\langle x^2+1 \rangle\big) + (c+dx+\langle x^2+1 \rangle)$

$\ker \varphi = \{(a,b) \mid a+bx+\langle x^2+1 \rangle = 0 + \langle x^2+1 \rangle\}$

$= \{(a,b) \mid a+bx \in \langle x^2+1 \rangle\} = \{(a,b) \mid a+bx = q(x)\cdot(x^2+1)$ for some $q(x) \in \mathbb{R}[x]\}$.

Since $1 \geq \deg(a+bx) = \deg(q(x)\cdot(x^2+1)) = \deg(x^2+1) + \deg q$

$= 2 + \deg q$

we must have $\deg q = -\infty$, i.e. $q = 0$

$\Rightarrow \ker \varphi = \{(0,0)\}$. $\Rightarrow \varphi$ is injective.

$\forall\ p(x) \in \mathbb{R}[x]$ $\exists\ q(x), r(x) \in \mathbb{R}[x]$ s.t.

$p(x) = (x^2+1)q(x) + r(x)$ and $\deg r < \deg(x^2+1) = 2$.

$\Rightarrow r(x) = a+bx$ for some $a, b \in \mathbb{R}$.

$\Rightarrow p(x) + \langle x^2+1 \rangle = a+bx + q(x)(x^2+1) + \langle x^2+1 \rangle = a+bx + \langle x^2+1 \rangle$

$= \varphi(a,b)$.

$\Rightarrow \varphi$ is onto.

Now, $\forall\ (a,b), (c,d) \in \mathbb{R}^2$

$\varphi(a,b)\varphi(c,d) = (a+bx+\langle x^2+1 \rangle)(c+dx+\langle x^2+1 \rangle)$

$= (ac + (ad+bc)x + bdx^2) + \langle x^2+1 \rangle$

$= (ac + (ad+bc)x + bd(x^2+1) - bd) + \langle x^2+1 \rangle =$

$= ac - bd + (ad+bc)x + \langle x^2+1\rangle$

$= \varphi(ac-bd,\ ad+bc)$

$\Rightarrow$ If we define $(a,b)\cdot(c,d) := (ac-bd,\ ad+bc)$

Then φ is an isomorphism of rings.

In other words: $\varphi : \mathbb{C} \to \mathbb{R}[x]/\langle x^2+1\rangle$

$\varphi(z) = \mathrm{Re}\,z + (\mathrm{Im}\,z)x + \langle x^2+1\rangle$

is an isomorphism of rings.

Note: $\varphi(1) = x + \langle x^2+1\rangle$ and

$(x+\langle x^2+1\rangle)(x+\langle x^2+1\rangle) = x^2 + \langle x^2+1\rangle = (x^2+1-1) + \langle x^2+1\rangle$

$= -1 + \langle x^2+1\rangle = \varphi(-1)$.

Theorem 29.1 (homomorphism theorem for rings; a version of 1st isomorphism theorem for rings)

Let $\varphi : R \to R'$ be a unital ring homomorphism (i.e. $\varphi(1_R) = 1_{R'}$), $I = \ker\varphi$.

(1) There is a unique injective ring homomorphism $\overline{\varphi} : R/I \to R'$ with $\overline{\varphi}(r+I) = \varphi(r)$ $\forall\, r \in R$

(2) $\overline{\varphi} : R/I \to \varphi(R)$ is an isomorphism.

Proof We know that $\varphi(R) = \{\varphi(r) \mid r \in R\}$ is a subring of R' and $\overline{\varphi} : R/I \to \varphi(R)$ is a well-defined isomorphism of abelian groups. Moreover $\overline{\varphi}$ is unique.

It remains to check that $\forall\ a+I,\ b+I \in R/I$

$\overline{\varphi}((a+I)(b+I)) = \overline{\varphi}(a+I)\,\overline{\varphi}(b+I)$.

Now $\overline{\varphi}((a+I)(b+I)) = \overline{\varphi}(ab+I) = \varphi(ab)$ by def of $\overline{\varphi}$

$= \varphi(a)\varphi(b)$ since φ is a ring homomorph

$= \overline{\varphi}(a+I)\,\overline{\varphi}(b+I)$ $\square$

Ex Recall the substitution principle: given commutative rings R, S, $\varphi: R \to S$ a unital ring homomorphism and $\alpha \in S$, $\exists!$ ring homomorphism $\varphi_\alpha: R[x] \to S$ with $\varphi_\alpha\left(\sum_{j=0}^{n} a_j x^j\right) = \sum_{j=0}^{n} \varphi(a_j)\alpha^j$.

Now consider $\varphi: \mathbb{R} \to \mathbb{C}$, $\varphi(a) = a$, $\alpha = \sqrt{-1}$

We get $\varphi_\alpha: \mathbb{R}[x] \to \mathbb{C}$, $\varphi_\alpha\left(\sum a_j x^j\right) = \sum_{j=0}^{n} a_j (\sqrt{-1})^j$

Then φ_α is unital: $\varphi_\alpha(1) = 1$.

φ_α is onto: given $a + bi \in \mathbb{C}$, $a + bi = \varphi_\alpha(a + bx)$

Claim $\ker \varphi_\alpha = \langle x^2+1 \rangle = (x^2+1)\mathbb{R}[x]$.

Proof $\varphi_\alpha(x^2+1) = (\sqrt{-1})^2 + 1 = -1 + 1 = 0$.

$\Rightarrow$ $x^2+1 \in \ker \varphi_\alpha$. $\Rightarrow$ $(x^2+1)\mathbb{R}[x] \subseteq \ker \varphi_\alpha$.

Conversely, suppose $g(x) \in \ker \varphi_\alpha$

By the division algorithm $\exists!\ q(x), r(x) \in \mathbb{R}[x]$ s.t.

$$g(x) = (x^2+1)q(x) + r(x) \quad \text{and} \quad \deg r < \deg(x^2+1) = 2.$$

Note! $r(x) = a + bx$ for some $a, b \in \mathbb{R}$

Now, since $\varphi_\alpha(g) = 0$,

$$0 = ((\sqrt{-1})^2 + 1)q(\sqrt{-1}) + a + b\sqrt{-1} = a + b\sqrt{-1}$$

$\Rightarrow a = b = 0$.

$\Rightarrow g(x) = (x^2+1)q(x) \in \langle x^2+1 \rangle$.

$\therefore \ker \varphi_\alpha = \langle x^2+1 \rangle$.

Homomorphism Theorem $\Rightarrow$

$$\overline{\varphi}_\alpha : \mathbb{R}[x]/\langle x^2+1 \rangle \longrightarrow \mathbb{C}$$

$$p(x) + \langle x^2+1 \rangle \longmapsto p(\sqrt{-1})$$

is a well-defined isomorphism of rings.

Ex For any commutative ring R, $R[x]/\langle x \rangle \cong R$

Consider $\varphi: R[x] \to R$, $\varphi(p) = p(0)$.

φ is a ring homomorphism by the substitution principle.

φ is onto since $\forall a \in R$, $\varphi(a) = a$.

$\ker \varphi = \{ a_0 + a_1 x + \cdots + a_n x^n \mid a_0 + a_1 \cdot 0 + \cdots + a_n 0^n = 0 \}$

$= \{ a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \geq 1, a_1, \ldots, a_n \in R \}$

$= x R[x] = \langle x \rangle$.

Homomorphism thm $\Rightarrow$

$$\overline{\varphi}: R[x]/\langle x \rangle \longrightarrow R$$
$$\overline{\varphi}(p(x) + \langle x \rangle) = p(0)$$

is a well-defined isomorphism of rings

Remark The ring $\mathbb{R} \oplus \mathbb{R}$ cannot be isomorphic to any field F.

Reasons (1) $\mathbb{R} \oplus \mathbb{R}$ has zero divisors: $\forall a, b \in R$, $a, b \neq 0$

$(a, 0) \cdot (0, b) = (a \cdot 0, 0 \cdot b) = (0, 0)$.

No field has zero divisors: if F is a field, $a, b \in F$, $a \neq 0$ and $ab = 0$, then $0 = a^{-1} \cdot 0 = a^{-1} ab = b$.

(2) $I = \mathbb{R} \oplus 0 := \{ (a, b) \in \mathbb{R} \oplus \mathbb{R} \mid b = 0 \}$ is an ideal and $\mathbb{R} \oplus 0 \neq \{0\}$, $\mathbb{R} \oplus 0 \neq \mathbb{R} \oplus \mathbb{R}$

ie I is a proper ideal in $\mathbb{R} \oplus \mathbb{R}$.

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

Note $\mathbb{R} \oplus \mathbb{R} / I \simeq \mathbb{R}$.

Reason $f: \mathbb{R} \oplus \mathbb{R} \to \mathbb{R}$ $f(a, b) = b$ is a surjective ring homomorphism and $\ker f = \{ (a, b) \mid b = 0 \}$.

Homomorphism Thm $\Rightarrow$

$$\overline{f}: \mathbb{R} \oplus \mathbb{R}/I \to \mathbb{R} \quad \overline{f}((a, b) + I) = b$$

is an isomorphism.