

# Lecture 35

①

(35.0) Examples of rings; ideals; and their interpretation.

(1)  $R = K[X]$  polynomial ring in 1-variable with coefficients from a field  $K$  (say  $\mathbb{C}$  or  $\mathbb{R}$  or  $\mathbb{Q}$ ).

Idea: Euclidean algorithm works in  $K[X]$ .

Meaning: given  $g(x) \neq 0$  and  $f(x)$ , we have  
(assume monic, i.e.  $g(x) = 1 \cdot x^d + \dots$   $d = \deg(g)$ ).

$$d = \deg(g)$$

$$n = \deg(f)$$

$$f(x) = q(x)g(x) + r(x) \quad \text{where} \\ \text{degree of } r(x) < \deg(g(x))$$

Proof. - Induction on degree of  $f(x)$ .

$$\text{If } 0 \leq \deg(f) < \deg(g), \text{ then } \begin{aligned} q(x) &= 0 \\ r(x) &= f(x) \end{aligned}$$

If  $\deg(f) \geq \deg(g)$ ; if leading coeff. of  $f(x) = a \in K^x$   
( $n \geq d$ ) (i.e.  $f(x) = x^n \cdot a + \boxed{x^{n-1} \dots}$  lower deg. terms)

replace  $f(x)$  by  $\tilde{f}(x) = f(x) - ax^{n-d}g(x)$ .

$\deg(\tilde{f}) < \deg(f) \Rightarrow$  (by induction)

$$\tilde{f}(x) = \tilde{q}(x)g(x) + r(x) \quad (\deg(r) < \deg(\tilde{f}))$$

(unless  $\tilde{f} = 0$ , in which case  $f(x) = ax^{n-d}g(x) + 0$ )

$$\Rightarrow f(x) = (\tilde{q}(x) + ax^{n-d})g(x) + r(x) \quad \square$$

Conclusion. - Every ideal in  $K[X]$  is principal. (2)

Proof. - Let  $I \subset K[X]$  be an ideal. Assume

$I \neq (0)$ . Choose  $g(x) \in I \setminus \{0\}$  of smallest degree

Clearly  $(g(x)) \subset I$ . Now if  $f(x) \in I$ , by

Euclidean algorithm,  $f(x) = q(x)g(x) + r(x)$

and  $\deg(r) < \deg(g)$ . By minimality of degree of  $g$ , we conclude that  $r = 0$ . Hence  $f(x) \in (g(x))$

$\Rightarrow I = (g(x))$  □

Set of ideals of  $K[X]$   $\leftrightarrow$   $\{ (g(x)) \text{ where } g(x) \in K[X] \text{ is monic} \}$

Over  $\mathbb{C}$ , by fundamental theorem of algebra,

$g(x) \in \mathbb{C}[X]$  monic of degree  $d \leftrightarrow g(x) = (x-z_1) \cdots (x-z_d)$   
 $z_1, \dots, z_d \in \mathbb{C}$ .

(i.e.  $g(x) = x^d + \dots$   
leading coeff. = 1)

(2)  $R = \mathbb{Z}[i] = \{ a+bi \text{ where } a, b \in \mathbb{Z} \}$ .

Addition:  $(a_1+b_1i) + (a_2+b_2i) = (a_1+a_2) + (b_1+b_2)i$   
(component-wise)

Mult:  $(a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i$   
( $i^2 = -1$ )

$\forall I \subset R$  is an ideal. Assume  $I \neq \{0\}$ .

$R = \mathbb{Z}[i]$  consist of complex numbers  $z \in \mathbb{C}$  s.t.  
RealPart( $z$ ), ImaginaryPart( $z$ )  $\in \mathbb{Z}$ .

$\leadsto$  we get Norm :  $\mathbb{Z}[i] \longrightarrow \mathbb{Z}_{\geq 0}$   
 $z = a+bi \longmapsto a^2+b^2 = |z|^2$

(1)  $R^{\times} = \{\pm 1, \pm i\}$ .

Proof.  $z \in R^{\times} \Rightarrow zw = 1$  for some  $w \in R^{\times}$ .

$\Rightarrow$  Norm( $zw$ ) = 1. But Norm( $zw$ ) = Norm( $z$ ) \* Norm( $w$ )  
(all in  $\mathbb{Z}_{\geq 0}$ )

$\Rightarrow$  Norm( $z$ ) = 1

$\Rightarrow z = \pm 1$  or  $\pm i$  □

(2) Euclidean algorithm works.

Let  $z \in R \setminus \{0\}$  and  $w \in R$ . Then  $\frac{w}{z} \in \mathbb{C}$   
 $\parallel$   
 $s+it$

Up to shifts by integers, we can make sure  $-\frac{1}{2} \leq s, t \leq \frac{1}{2}$

i.e.  $\exists a, b \in \mathbb{Z}$  s.t.  $-\frac{1}{2} \leq s-a, t-b \leq \frac{1}{2}$

$\Rightarrow$  Norm  $\left( \frac{w}{z} - (a+bi) \right) \leq \frac{1}{2}$

so  $w = (a+bi)z + \overset{\textcircled{r}}{r}$   $\longleftarrow$  has Norm  $\leq \frac{1}{2}|z| < |z|$ .

Hence we have proved: given  $w \in R, z \in R \setminus \{0\}$   
we can find  $q, r \in R$  s.t.

$w = qz + r$	and $ r ^2 <  z ^2$ <small>↑                    ↑</small> Norm(r)        Norm(z)
--------------	--

Cor. Every ideal in  $\mathbb{Z}[i]$  is principal.

(35.1) Some more general properties of an ideal.

Let  $R_1, R_2$  be two rings. Let  $f: R_1 \rightarrow R_2$  be a ring homomorphism.

Lemma. If  $I_2 \subset R_2$  is an ideal (say, left)  
then so is  $I_1 = \{ a \in R_1 \mid f(a) \in I_2 \} \subset R_1$ .

Proof.  $I_1$  is clearly a subgroup of  $R_1$ .

$(0_{R_1} \in I_1$  because  $f(0_{R_1}) = 0_{R_2} \in I_2$ .)

$a, b \in I_1 \Rightarrow f(a), f(b) \in I_2$

$\Rightarrow f(a \pm b) \in I_2 \Rightarrow a \pm b \in I_1$ .)

Now if  $x \in I_1$  and  $r \in R_1$  then

$$f(r \cdot x) = f(r) \cdot \underbrace{f(x)}_{\in I_2} \Rightarrow f(r \cdot x) \in I_2$$

$$\Rightarrow r \cdot x \in I_1 \quad \square$$

(35.2) Note: image of an ideal need not be an ideal. (5)

e.g.  $f: \mathbb{Z} \longrightarrow \mathbb{Q}$  .  $2\mathbb{Z} \subset \mathbb{Z}$  ideal

$$n \longmapsto \frac{n}{1}$$

$$\text{But } \left\{ \frac{2n}{1} : n \in \mathbb{Z} \right\} \subset \mathbb{Q}$$

is not an ideal [only subgp.]

(remember: Ideals in  $\mathbb{Q}$   
=  $\{ \{0\}; \mathbb{Q} \}$ )

Lemma. If  $f: R_1 \longrightarrow R_2$  is surjective, then

$f(I_1) \subset R_2$  is an ideal, if  $I_1 \subset R_1$  is an ideal (left).

Proof. Let  $I_2 = f(I_1) \subset R_2$ . As image of a subgroup is a subgroup, we need to check  $r_2 \cdot x_2 \in I_2 \quad \forall r_2 \in R_2; x_2 \in I_2$

But  $f$  is surjective, so we can find  $r_1 \in R_1$  s.t.  $f(r_1) = r_2$ .

Also  $x_2 = f(x_1)$  for some  $x_1 \in I_1$ . (by defn. of  $I_2$ ).

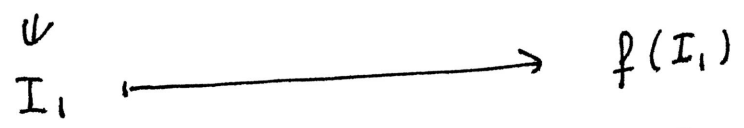
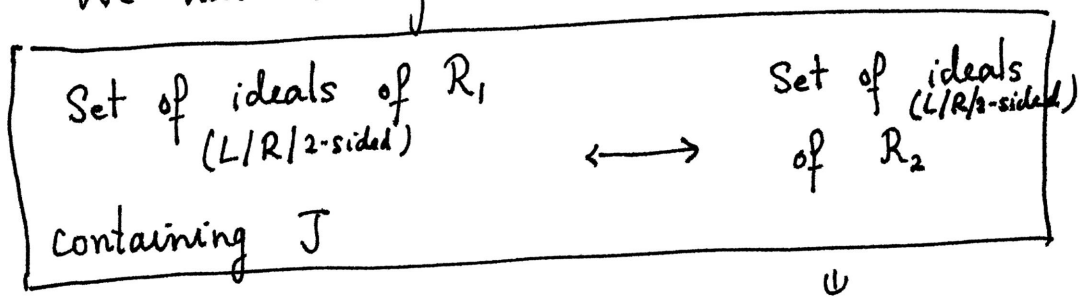
$$\Rightarrow f(r_1 \cdot x_1) = r_2 \cdot x_2 \in I_2 \text{ as we wanted. } \square$$

(35.3) Similar to the case of groups, we have the following:

Let  $f: R_1 \longrightarrow R_2$  be a surjective ring hom and let

$$J = \text{Ker}(f) \subset R_1 \quad (2\text{-sided ideal})$$

Theorem. We have a bijection

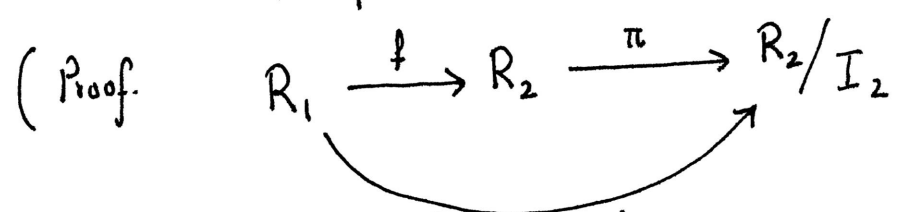


$f^{-1}(I_2) = \{a \mid f(a) \in I_2\} \longleftarrow I_2$

This bijection preserves our usual operations on ideals. For instance,

if  $I_2 \subset R_2$  is a 2-sided ideal,  $I_1 = f^{-1}(I_2) \subset R_1$  corresponding 2-sided ideal of  $R_1$

Then  $R_1/I_1 \cong R_2/I_2$



define this ring hom. to be  $g$

$g$  is surjective, because both  $\pi$  &  $f$  are.

$\text{Ker}(g) = \{a \in R_1 \mid f(a) \in I_2\} = I_1 \subset R_1$

1<sup>st</sup> iso thm  $\Rightarrow R_1/I_1 \cong R_2/I_2$

$\psi$   
 $a \pmod{I_1} \mapsto f(a) \pmod{I_2}$

□