Lecture 35

(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 algorthism works in $K[X]$.

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

$d = \text{degree}(g)$

$n = \text{degree}(f)$

$$f(X) = q(X)\, g(X) + r(X)$$ where degree of $r(X) < \deg(g(X))$

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

If. $0 \leq \deg(f) < \deg(g)$, then $q(X) = 0$, $r(X) = f(X)$

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

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

$\text{degree}(\tilde{f}) < \text{degree}(f) \Rightarrow$ (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 $f(x) = ax^{n-d} g(x) + 0$)

$$\Rightarrow f(X) = \left(\tilde{q}(x) + aX^{n-d}\right) g(X) + r(X)$$ $\square$

Conclusion. – Every ideal in $K[X]$ is principal.

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 ~~deg~~ $r = 0$. Hence $f(x) \in (g(x))$

$\Rightarrow \quad I = (g(x))$ $\square$

Set of ideals of $K[X]$ $\longleftrightarrow$ $\{ (g(x))$ where $g(x) \in K[X]$ is <u>monic</u> $\}$

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

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

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

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

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

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

~~Let $I \subset R$ be an ideal. Assume $I \neq \{0\}$.~~

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

$\rightsquigarrow$ we get

$$\begin{aligned} \text{Norm} : \mathbb{Z}[i] &\longrightarrow \mathbb{Z}_{\geq 0} \\ z = a+bi &\longmapsto a^2+b^2 = |z|^2 \end{aligned}$$

(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 $\pm i$ $\square$

(2) Euclidean algorithm works.

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

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. $-\frac{1}{2} \leq s-a,\ t-b \leq \frac{1}{2}$

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

so $w = (a+bi)z + r$

r 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.

$$\boxed{w = qz + r \quad \text{and} \quad \underset{\text{Norm}(r)}{|r|^2} < \underset{\text{Norm}(z)}{|z|^2}}$$

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 $f: R_1 \longrightarrow R_2$ be a ring homomorphism.

Lemma. If $I_2 \subset R_2$ is an ideal (say, left) then so is $I_1 = \{ \cancel{a} \ a_1 \in R_1 \mid f(a_1) \in I_2 \} \subset R_1$.

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

$$f(r.x) = f(r) \cdot \underset{I_2}{\underset{\cap}{f(x)}} \Rightarrow f(r.x) \in I_2$$

$$\Rightarrow r.x \in I_1 \qquad \square$$

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

e.g. $f : \mathbb{Z} \longrightarrow \mathbb{Q}$, $\quad n \longmapsto \frac{n}{1}$.

$2\mathbb{Z} \subset \mathbb{Z}$ ideal

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 (left), 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 $r_2 \cdot x_2 \in I_2 \ \forall r_2 \in R_2 ; x_2 \in I_2$

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).

$\Rightarrow f(r_1 \cdot x_1) = r_2 \cdot x_2 \in I_2$ 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

$J = Ker(f) \subset R_1$ (2-sided ideal)

Theorem. We have a bijection

$$\boxed{\begin{array}{lcl} \text{Set of ideals of } R_1 & & \text{Set of ideals } (L/R/2\text{-sided}) \\ (L/R/2\text{-sided}) & \longleftrightarrow & \text{of } R_2 \\ \text{containing } J & & \end{array}}$$

$$\begin{array}{ccc} \Psi & & \Psi \\ I_1 & \longmapsto & f(I_1) \\ \text{"}f^{-1}(I_2)\text{"} = \{a \mid f(a) \in I_2\} & \longleftarrow & I_2 \end{array}$$

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 $R_1/I_1 \cong R_2/I_2$

(Proof.

$$\begin{tikzcd} R_1 \arrow[r, "f"] \arrow[rr, bend right, "g"'] & R_2 \arrow[r, "\pi"] & R_2/I_2 \end{tikzcd}$$

define this ring hom. to be g

g is surjective, because both π & f are.

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

1st iso thm $\Rightarrow$ $R_1/I_1 \cong R_2/I_2$ $\square$

$$\begin{array}{ccc} \Psi & & \\ a \pmod{I_1} & \longmapsto & f(a) \pmod{I_2} \end{array}$$