Lecture 23

Important Ideals

Def: Let R be a ring. Let I and J be ideals of R.

(1) The sum of I and J is $I + J := \{ a+b \mid a \in I, b \in J \}$

(2) The product of I and J is $IJ := \{ a_1 b_1 + \cdots + a_n b_n \mid n \in \mathbb{N}, a_i \in I, b_i \in J \}$

(3) $I^n := \underbrace{I \cdot I \cdot \dots \cdot I}_{n\text{-times}}$ $n \in \mathbb{Z}^+$.

Remarks: @ IJ is the set of all finite sums of elements of the form ab, $a \in I$ and $b \in J$.

@ IJ is different to HK in group theory.

Example: Let R be a finite ring, $I = \{0, a_1, a_2, a_3\}$ and $J = \{0, b_1, b_2\}$.

$$I + J = \{0, a_1, a_2, a_3, b_1, b_2, a_1 + b_1, a_1 + b_2, \dots, a_3 + b_2\}$$

$$\begin{array}{cccc} \text{length } 1 & \text{length } 2 & \text{length } 3 & \cdots \end{array}$$

$$IJ = \left\{ \begin{array}{llll} 0 & & & \\ a_1 b_1 & 2a_1 b_1 & 3a_1 b_1 & \\ a_1 b_2 & 2a_1 b_2 & 3a_1 b_2 & \\ a_2 b_1 & \vdots & \vdots & \\ a_2 b_2 & a_1 b_1 + a_1 b_2 & a_1 b_1 + a_1 b_2 + a_2 b_1 & \\ a_3 b_1 & a_1 b_1 + a_2 b_1 & \vdots & \\ a_3 b_2 & a_1 b_1 + a_2 b_2 & & \\ & \vdots & & \\ & a_3 b_2 + a_3 b_1 & & \end{array} \right\}$$

Proposition 12: Let R be a ring. Let I and J be ideals of R.

(1) $I+J$ is an ideal of R. Moreover, $I+J$ is the smallest ideal of R containing both I and J.

(2) IJ is an ideal of R. Moreover, IJ contained in $I \cap J$.

Proof:

(1) We know $I+J$ is a normal subgroup of R. Thus it suffices to prove that $I+J$ "absorbs" R. Let $a \in I$, $b \in J$ and $r \in R$, then

$$r(a+b) = \underset{\substack{\cap \\ I}}{ra} + \underset{\substack{\cap \\ J}}{rb} \in I+J \quad \text{and} \quad (a+b)r = \underset{\substack{\cap \\ I}}{ar} + \underset{\substack{\cap \\ J}}{br} \in I+J.$$

Hence, $I+J$ is an ideal of R.

Since $0 \in I \cap J$, then $I \subseteq I+J$ and $J \subseteq I+J$. Suppose there exists an ideal K of R such that $K \supseteq I, J$. It follows that $a+b \in K$ for all $a \in I$ and $b \in J$, i.e. $I+J \subseteq K$.

(2) Let $x := a_1 b_1 + \cdots + a_n b_n \in IJ$. Since I and J are ideals, $x \in I$ and $x \in J$.

This is $IJ \subseteq I \cap J$.

- $IJ \neq \phi$ because $0 = 0 \cdot 0 \in IJ$.

- Let $a_1 b_1 + \cdots + a_m b_m$ and $c_1 d_1 + \cdots + c_n d_n$ in IJ where $a_i, c_j \in I$ and $b_i, d_j \in J$.

  Then $a_1 b_1 + \cdots + a_m b_m - (c_1 d_1 + \cdots + c_n d_n) \underset{\text{Prop 1}}{=} a_1 b_1 + \cdots + a_m b_m + (-c_1) d_1 + \cdots + (-c_n) d_n \in IJ$

  because $-c_i \in I$ for all i.

Let $a_1b_1 + \cdots + a_nb_n \in IJ$ and $r \in R$, then

$$r(a_1b_1 + \cdots + a_nb_n) = (ra_1)b_1 + \cdots + (ra_n)b_n \in IJ \quad \text{because } ra_i \in I \ \forall i$$

$$(a_1b_1 + \cdots + a_nb_n)r = a_1(b_1r) + \cdots + a_n(b_nr) \in IJ \quad \text{because } b_ir \in J \ \forall i$$

Examples:

1) $\mathbb{Z}$: Consider $6\mathbb{Z}$ and $10\mathbb{Z}$.

$$6\mathbb{Z} + 10\mathbb{Z} = \{ 6x + 10y \mid x, y \in \mathbb{Z} \}$$

Claim: $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$

($\subseteq$) $\forall x, y \in \mathbb{Z}$, $6x + 10y = 2(3x + 5y) \in 2\mathbb{Z}$

($\supseteq$) Observe that $2 = 6(2) + 10(-1)$. Then

$$2x = 6(2)x + 10(-1)x \in 6\mathbb{Z} + 10\mathbb{Z} \text{ for all } x \in \mathbb{Z}.$$

In general, $m\mathbb{Z} + n\mathbb{Z} = \gcd(m,n)\mathbb{Z}$ for all $m, n \in \mathbb{Z}$. Prove it!

◎ $(6\mathbb{Z})(10\mathbb{Z}) = \{ (6x_1)(10y_1) + \cdots + (6x_n)(10y_n) \mid n \in \mathbb{N} \text{ and } x_i, y_i \in \mathbb{Z} \} = 60\mathbb{Z}$

In general, $(m\mathbb{Z})(n\mathbb{Z}) = (mn)\mathbb{Z}$ for all $m, n \in \mathbb{Z}$.

2) $\mathbb{Z}[x]$: Consider $I = \{ p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z} \}$

◎ $I + I = \{ p(x) + q(x) \in \mathbb{Z}[x] \mid p(0), q(0) \in 2\mathbb{Z} \} = I$

◎ $I \cdot I = \{ p_1(x)q_1(x) + \cdots + p_n(x)q_n(x) \mid n \in \mathbb{N} \text{ and } p_i(x), q_i(x) \in \mathbb{Z}[x] \} \subsetneq I$

For example $x^2 + 2 \in I$ but $x^2 + 2 \notin I^2$.

$$x^2 + 2 = x \cdot x + 2 \cdot 1 \quad \text{where } 1 \notin I$$

$$x^2 + 2 = \underbrace{(x - \sqrt{2})}_{\notin I} \underbrace{(x + \sqrt{2})}_{\notin I}$$

Def: Let R be a commutative ring with identity.

(1) Let $a \in R$, then $(a) := \{ar \mid r \in R\}$ is called the principal ideal generated by a.

(2) Let $a_1, a_2, \ldots, a_n \in R$, then $(a_1, a_2, \ldots, a_n) := \{a_1 r_1 + \cdots + a_n r_n \mid r_i \in R\}$ is called the ideal generated by $a_1, \ldots, a_n$.

Generators are not unique.

Proposition 13: Let R be a commutative ring with identity. Let $a_1, a_2, \ldots, a_n \in R$. Then $(a_1, a_2, \ldots, a_n)$ is an ideal of R.

Proof: Exercise.

Examples:

1) R commutative with identity. $\{0\} = (0)$ and $R = (1)$

2) $\mathbb{Z}$: $n\mathbb{Z} = (n) = (-n)$ principal ideal generated by n or $-n$.

Claim: $(m, n) = (\gcd(m,n))$. Prove it!

Claim: Every ideal of $\mathbb{Z}$ is principal. Prove it!

3) $\mathbb{Z}[x]$: $(2, x) = \{ 2p(x) + x\,q(x) \mid p(x), q(x) \in \mathbb{Z}[x] \}$

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

Claim: $(2, x)$ is not a principal ideal.

Assume by contradiction that $(2, x) = (a(x))$ for some $a(x) \in \mathbb{Z}[x]$.

Since $2 \in (a(x))$, $\exists\, p(x) \in \mathbb{Z}[x]$ s.t. $2 = a(x)p(x)$. Then $a(x)$ and $p(x)$ must be constant polynomials; $a(x) = a$, $p(x) = p \in \mathbb{Z}$. Given that 2 is prime, we have $a \in \{\pm 1, \pm 2\}$.

If $a = \pm 1$, then $(a) = \mathbb{Z}[x]$. Contradiction!!! (a) is a proper ideal.

If $a = \pm 2$, then $x \in (2) = (-2)$, i.e. $x = 2q(x)$ for some $q(x) \in \mathbb{Z}[x]$. Contradiction!!! $x \neq 2x$.

Thus, $(2, x)$ is not a principal ideal.

4) $\mathbb{R}[x]$: $\quad (x) = \{\, x p(x) \mid p(x) \in \mathbb{R}[x] \,\}$

$$= \{\, p(x) \in \mathbb{R}[x] \mid p(0) = 0 \,\}$$

Proposition 14: Let R be a ring with identity. Let I be an ideal of R.

(1) $I = R \iff \exists u \in R$ such that u is a unit and $u \in I$

(2) Assume R is commutative.

R is a field $\iff$ The only ideal of R are $\{0\}$ and R

Proof:

(1) ($\Rightarrow$) If $I = R$, then $1 \in I$.

($\Leftarrow$) Suppose $\exists u \in R$ such that u is a unit and $u \in I$. Then for all $r \in R$,

$r = r \cdot 1 = r(u^{-1}u) = (ru^{-1})u \in I$ because I is an ideal.

(2) ($\Rightarrow$) Let I be a nonzero ideal of R. Then $\exists\ a \neq 0$ s.t. $a \in I$ Since R is a field, a is a unit. By (1), $I = R$.

($\Leftarrow$) Let $u \in R \setminus \{0\}$. By hypothesis $(u) = R$ and so $1 \in (u)$. Thus $\exists v \in R$ s.t. $uv = 1 = vu$. So R is a field.

Corollary 15: If F is a field then any nonzero ring homomorphism from F to another ring is injective.

Proof: Let $\phi : F \longrightarrow R$ be a nonzero ring homomorphism. Then $\operatorname{Ker} \phi \subsetneq F$. Since $\operatorname{Ker} \phi$ is an ideal, then $\operatorname{Ker} \phi = \{0\}$ by Prop 14 (b). So, ϕ is injective.