Lecture XXXVI: Ring Homomorphisms, Ideals

Recall: $(R, +, \cdot, 0, 1)$ is a ring if

(I) $(R, +, 0)$ is an abelian group

(II) $\cdot : R \times R \longrightarrow R$ is an associative binary operation with 1_R = Neutral element.

(III) Distributivity $\quad a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$

$\qquad (b+c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$

Definition: A subring A of R is a subset $(A \subseteq R)$ containing 0_R & 1_R (= 0 & 1 of A) such that
$$\left.\begin{array}{ll} a+b \in A & , -a \in A \\ a \cdot b \in A & \end{array}\right\} \forall a, b \in A.$$

Definition: A field is a commutative ring R where $R^\times = \{a \in R : \exists b \in R : a \cdot b = 1_R\}$ equals $R \smallsetminus \{0\}$.

§ 36.1 Ring homomorphisms:

Let R and S be two rings:

Definition: A ring homomorphism $f: R \longrightarrow S$ is a function of sets which preserves the ring structure on R and S

More precisely: $\quad f(0_R) = 0_S \;;\; f(1_R) = 1_S \quad$ [Neutral Elements of R & S, resp.]
$$\left.\begin{array}{l} f(a +_R b) = f(a) +_S f(b) \\ f(a \cdot_R b) = f(a) \cdot_S f(b) \end{array}\right\} \forall a, b \in R$$

As with group homomorphisms, we have the usual notions of Kernel and Image

- $\mathrm{Ker}(f) = \{a \in R : f(a) = 0_S\} \subseteq R \qquad$ (Kernel of f)
- $\mathrm{Im}(f) = \{s \in S : \exists a \in R \text{ st } f(a) = s\} \subseteq S \qquad$ (Image of f)

Note: $\mathrm{Im}(f)$ is a subring of S

$\mathrm{Ker}(f)$ is not a subring of R because $1_R \notin \mathrm{Ker}(f)$ $(f(1_R) = 1_S \neq 0_S)$

$\mathrm{Ker}(f)$ will be a different algebraic substructure, namely, a two-sided ideal.

Definition: A ring isomorphism is a ring homomorphism $f: R \longrightarrow S$ with an inverse that is also a ring homomorphism.

Lemma: $f: R \longrightarrow S$ ring iso $\iff$ f is a ring homomorphism & a bijection.

§36.2 Ideals:

Let R be a ring and $I \subseteq R$

Definition: We say I is a <u>left ideal</u> of R if I satisfies

(i) I is an abelian subgroup of $(R,+,0)$

(ii) $\forall r \in R \ \forall x \in I \ : r \cdot x \in I$

I is a <u>right-ideal</u> of R if I satisfies (i) and

(ii') $\forall r \in R \ \forall x \in I \quad x \cdot r \in I$

I is a <u>two-sided ideal</u> of R if I is both a left- and a right-ideal.

Remark: For a commutative ring R, all these notions are the same, so we just say $I \subseteq R$ is an ideal (ie I is a subgroup of $(R,+,0)$ & $\underset{\forall x \in I}{\forall r \in R} : r \cdot x \in I$.)

Examples: $I = \{0_R\}$ & $I = R$ are two-sided ideals of any ring R.
We call R the <u>unit ideal</u>.

Lemma: Let $f: R \longrightarrow S$ be a ring homomorphism. Then, $\mathrm{Ker}(f)$ is a two-sided ideal.

Proof: $\mathrm{Ker}(f)$ is clearly a subgroup of $(R,+,0)$ because a ring homomorphism is a group homomorphism.

Now, if $r \in R$ & $x \in \mathrm{Ker}(f)$ we have

$f(r \cdot x) = f(r) f(x) = f(r) \cdot 0_S = 0_S$ (by Lemma §35.3) $\Rightarrow r \cdot x \in \mathrm{Ker} f$

$f(x \cdot r) = f(x) f(r) = 0_S \cdot f(r) = 0_S$ (———) $\Rightarrow x \cdot r \in \mathrm{Ker} f$

Thus $\mathrm{Ker}(f)$ is a two-sided ideal. $\square$

§36.3 Examples:

① $R = K$ a field

Let $I \subseteq K$ be an ideal. Either $I = \{0\}$, or there is some $\lambda \neq 0$, $\lambda \in I$. In the latter case, $\underset{K}{\lambda^{-1}} \cdot \underset{I}{\lambda} \in I$ because I is an ideal. Thus, $1 \in I$

If $x \in K$, then $x = \underset{K}{x} \cdot \underset{I}{1} \in I$

Hence, set of ideals of a field $= \{\{0\}, K\}$

Same argument proves:

Proposition 1: R ring, $I \subseteq R$ ideal. If $R^\times \cap I \neq \emptyset$, then $I = R$ (unit ideal)

② $R = \mathbb{Z}$ commutative ring

Proposition 2: Set of ideals of $\mathbb{Z}$ $= \{ I_n := n\mathbb{Z} \quad n \in \mathbb{Z}_{\geq 0} \}$

Proof: Let $I \subseteq \mathbb{Z}$ be an ideal. Assume $I \neq \{0\}$. Let

k = smallest positive element of I ($I \cap \mathbb{Z}_{\geq 0} \neq \emptyset$ because $x \in I \cap \mathbb{Z}_{<0} \Rightarrow -x \in I \cap \mathbb{Z}_{\geq 0}$)

Claim: $I = k\mathbb{Z}$

Pf/ . $k\mathbb{Z} \subset I$ as $I \subseteq \mathbb{Z}$.

. Conversely, if $l \in I$, then $l = qk + r$ for $k, r \in \mathbb{Z}$ $0 \leq r \leq k-1$. By the minimality of k we have $\left.\begin{matrix} r = l - qk \in I \\ 0 \leq r \leq k-1 \end{matrix}\right\} \Rightarrow r = 0$. Thus, $l \in k\mathbb{Z}$. Hence $I \subseteq k\mathbb{Z}$. □

Proposition 3: Operations on $\mathbb{Z}$ important for number theory can be translated to ideals

In $\mathbb{Z}_{\geq 0}$		In Set of Ideals of $\mathbb{Z}$
n	$\longleftrightarrow$	I_n
(1) $d = \gcd(n, m)$	$\longleftrightarrow$	$I_d = I_m + I_n$ (smallest ideal containing both I_m & I_n)
(2) $l = \operatorname{lcm}(n, m)$	$\longleftrightarrow$	$I_l = I_m \cap I_n$ (largest ideal contained in both I_m and I_n)
(3) n divides m (m is divisible by n)	$\longleftrightarrow$	$I_m \subseteq I_n$

Proof: (3) $I_m \subseteq I_n$ means $m\mathbb{Z} \subseteq n\mathbb{Z}$ ie $m \in n\mathbb{Z}$ which is the same as saying $m = nq$ for some $q \in \mathbb{Z}$, i.e, m is divisible by n.

(2) $I_m \cap I_n \ni x \iff x$ is divisible by both m & n

ie $x = \operatorname{lcm}(n, m)\, q$ for some $q \in \mathbb{Z}$

ie $x \in l\mathbb{Z} = I_l \qquad l = \operatorname{lcm}(n, m)$.

(1) Let I be an ideal containing I_n and I_m. So $m, n \in I$ and hence

$am + bn \in I \quad \forall a, b \in \mathbb{Z} \underset{\text{Euclidean Algorithm}}{\Longrightarrow} \gcd(m, n) \in I \Rightarrow I_d \subseteq I$

$d = \gcd(m, n)$. □