Lecture 32

(32.0) Recall: we defined <u>a ring R</u> as follows:

- R is an abelian group $(R, +, 0_R)$ together with another binary <u>associative</u> operation $\cdot : R \times R \to R$, $(a,b) \mapsto a \cdot b$, for which we have another $(1_R \neq 0_R)$ neutral element:

$$1_R \cdot a = a \cdot 1_R = a \quad \forall a \in R.$$

Moreover $\cdot$ distributes over $+$.

- $R^\times$ = (multiplicative) group of invertible elements of R (also called units)

$$= \{ a \in R \text{ such that there exists } b \in R \text{ so that } a \cdot b = b \cdot a = 1_R \}$$

For <u>commutative rings</u> (i.e., R such that $a \cdot b = b \cdot a \ \forall a, b \in R$).

we introduced the notion of a <u>zero-divisor</u>, $x \in R$ is a zero-divisor if there exists $y \in R \setminus \{0_R\}$ such that

$$xy = 0_R.$$

(32.1) Lemma. If R is a commutative ring and $a \in R^\times$, then a is <u>not</u> a zero divisor.

Proof. As $a \in R^\times$, we have $b \in R^\times$ such that

$$ab = 1_R.$$

Now, if a is a zero divisor, we must have some $y \in R$, $y \neq 0$, such that $ay = 0$. But then

$$\left.\begin{array}{l} bay = b \cdot 0 = 0 \\ \quad \parallel \\ aby = 1_R y = y \end{array}\right\} \text{ contradicting } y \neq 0.$$

$\square$

(32.2) <u>Integral domain</u> is a <u>commutative ring</u> with no non-zero, zero-divisors.

<u>Field</u> is a commutative ring R, where $R^\times = R \setminus \{0\}$.

The lemma (32.1) $\Rightarrow$ $\boxed{\text{every field is an integral domain.}}$

(32.3) Situation in non-commutative setting - an example

Let H be the following abelian group. (We will consider $R = \mathrm{End}_{gp}(H)$).

$$H = \{(a_1, a_2, \ldots, a_n, \ldots) \text{ where } a_1, a_2, \ldots \in \mathbb{Z}\}$$

Component-wise addition.

$$R = \mathrm{End}_{gp}(H) = \text{set of all group hom-s } H \xrightarrow{f} H$$

R as a ring $\longrightarrow$
$$\left[\begin{array}{l} (f_1 + f_2)(h) = f_1(h) + f_2(h) \\ (f_1 \cdot f_2)(h) = f_1(f_2(h)) \\ 0_R(h) = (0,0,\dots) \quad \forall\, h \in H \\ 1_R(h) = h \quad \forall\, h \in H \end{array}\right.$$

Take $\varphi : H \longrightarrow H$, $(a_1, a_2, \dots) \longmapsto (0, a_1, a_2, \dots)$. Injective but not surjective.

- If we take $\psi : H \longrightarrow H$, $(a_1, a_2, \dots) \longmapsto (a_2, a_3, \dots)$, then $\psi \circ \varphi = 1_R$
- If we take $\pi_1 : H \longrightarrow H$, $(a_1, a_2, \dots) \longmapsto (a_1, 0, \dots 0,)$ then $\pi_1 \circ \varphi = 0_R$ $(\pi_1 \neq 0_R)$.

Thus in absolute generality, we must be careful - left-invertible, has a left-zero divisor and so on...

We will <u>not</u> dwell into this for our course, and hence treat the notion of <u>zero-divisor, in particular, for comm. rings only.</u>

(32.4) Ring homomorphisms.

Let R and S be two rings. A <u>ring homomorphism</u>

$f : R \longrightarrow S$ is a function of sets which preserves

the ring structures on R and S.

<u>Precisely</u> : $f(0_R) = 0_S$; $f(1_R) = 1_S$. [Neutral elements of R & S resp.]

$$\left.\begin{aligned} f(\underset{\text{in } R}{a + b}) &= f(a) \underset{\text{in } S}{+} f(b) \\ f(\underset{\text{in } R}{a \cdot b}) &= f(a) \underset{\text{in } S}{\cdot} f(b) \end{aligned}\right\} \forall\, a, b \in R.$$

A <u>subring</u> A of R is <u>a subset</u> $(A \subseteq R)$ containing 0_R & 1_R $(0, 1 \in A)$

such that

$$\left.\begin{aligned} a + b &\in A \\ a \cdot b &\in A \end{aligned}\right\} \forall\, a, b \in A.$$

Given a ring homomorphism $f : R \longrightarrow S$ we have the usual notions of <u>kernel</u> and <u>image</u> of f

$$\mathrm{Ker}(f) = \{ a \in R : f(a) = 0_S \} \subseteq R$$

(read: kernel of f)

$\mathrm{Im}(f) = \{ b \in S : b = f(a) \text{ for some } a \in R \} \subseteq S$

(image of f)

<u>Note</u>: $\mathrm{Im}(f)$ is a subring of S.

$\mathrm{Ker}(f)$ is <u>NOT</u> a subring of R. Simply because $1_R \notin \mathrm{Ker}(f)$.

(32.5) Ideals.- Let R be a ring and $I \subset R$.

We say I is a <u>left</u> (resp. <u>right</u>; resp. <u>two-sided</u>) <u>ideal</u> of R, if

(i) I is an abelian subgroup of R.

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

[For right ideal : $x \cdot r \in I \quad \forall\, x \in I,\ r \in R$.
Two-sided : both left and right]

Remark. For a commutative ring R, all these are the same thing, so we just say $I \subset R$ is an ideal if $I \subset R$ is an abelian subgroups and $r \cdot x \in I \ \forall\, r \in R,\ x \in I$.

(32.6) Let $f : R \longrightarrow S$ be a ring hom.

Lemma. $\mathrm{Ker}(f) \subset R$ is a two-sided ideal

Proof. $\mathrm{Ker}(f)$ is clearly a subgroup of $(R, +, 0)$
"R as an ab. group"

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

$$f(r \cdot x) = f(r) \cdot f(x) = f(r) \cdot 0_S = 0_S$$
$$f(x \cdot r) = f(x) \cdot f(r) = 0_S \cdot f(r) = 0_S .$$

$\Rightarrow$ $r \cdot x$ and $x \cdot r$ are in $\mathrm{Ker}(f)$.

Hence it is a 2-sided ideal. $\square$

(32.7) Examples. $R = \mathbb{Z}$.

Prove that every ideal of R is of the form $(n = 0, 1, 2, \dots)$
$$I_n = n \cdot \mathbb{Z} \subset \mathbb{Z}$$
all #'s divisible by n.

~~Solution. Let $I \subset \mathbb{Z}$ be an ideal.~~

See lecture 33.