Lecture 33

(33.0) Recall the definitions - (i) A ring R is an abelian group equipped with a "bilinear, associative, unital" multiplication

$$\begin{array}{ccc} R\times R & \longrightarrow & R \\ (a,b) & \longmapsto & a\cdot b \end{array}$$

(bilinear: ②)

$(a+b)\cdot c = a\cdot c + b\cdot c$, $a\cdot(b+c) = a\cdot b + a\cdot c$

(associative: $(ab)c = a(bc)$)

(unital: $\exists\, 1_R \in R$ s.t. $a\cdot 1_R = a = 1_R\cdot a$)

(ii) R is a commutative ring if its multiplication operation is commutative: $ab = ba$ $\forall a,b\in R$.

(iii) $R^\times = \{a\in R$ such that a admits both a left and a right inverse$\}$

(Sometimes called "group of units of R".)

(these end up being equal, by associativity: if $b_1 a = 1_R = a b_2$, then

$$\begin{array}{ccc} (b_1 a)b_2 & = & b_1(ab_2) \\ \| & & \| \\ 1_R\cdot b_2 & & b_1\cdot 1_R \\ \| & & \| \\ b_2 & \text{hence} & b_1 \end{array}$$

)

(iv) (R: commutative)

$a\in R$ is a zero divisor, if there exists $b\in R\setminus\{0\}$ such that $ab = 0$.

(v) A ring homomorphism $f: R\to S$ is a homomorphism of underlying abelian group such that (in addition)

$$f(1_R) = 1_S\,, \qquad f(a\cdot b) = f(a)\cdot f(b)\ \ \forall a,b\in R$$

(vi) $A \subset R$ is a <u>subring</u> if $A \leq R$ (as abelian groups), $1_R \in A$

and $a.b \in A$, $\forall a, b \in A$.

(vii) $I \subset R$ is a <u>(left) ideal</u>, if $I \leq R$ (as abelian groups) and

$r.x \in I$, $\forall r \in R, x \in I$.

(<u>right ideal</u> $\rightsquigarrow$ $x.r \in I$ $(\forall r \in R, x \in I)$.)

<u>2-sided ideal</u> = both left and right ideal.)

(viii) $f : R \to S$ ring hom. $\rightsquigarrow$ $\mathrm{Ker}(f) \subset R$ is a <u>2-sided ideal</u>.

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

(33.1) Some examples.– (i) $R = K$: a field (recall: a field K is a commutative ring where $K^\times = K \setminus \{0\}$.)

Let $I \subset K$ be an ideal. Either $I = \{0\}$, or there is some $\lambda \neq 0$, $\lambda \in I$. In the latter case, $\lambda^{-1} \cdot \lambda \in I$ ($\lambda^{-1} \in K$, $\lambda \in I$, by defn. of an ideal)

$\Rightarrow 1 \in I \Rightarrow x = x \cdot 1 \in I$, $\forall x \in K$

Hence, Set of ideals of a field $= \{\{0\}, K\}$ (K: usually the whole ring is called <u>unit ideal</u>.)

Same argument proves:

$$R^\times \cap I \neq \phi \Rightarrow I = R \quad (\text{unit ideal.})$$

$I \subset R$ ideal

(ii) $R = \mathbb{Z}$.

Proposition.– Set of ideals of $\mathbb{Z}$ $= \{ I_n = n\cdot\mathbb{Z} : n = 0, 1, 2, \ldots \}$

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

k = smallest positive element of I ($k \in \mathbb{Z}_{\geq 1}$.)

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

Clearly $k\cdot\mathbb{Z}$ = subgroup generated by k $\subset I$; as $I \leq \mathbb{Z}$. Conversely, let $l \in I$. Write $l = q\cdot k + r$, (assume $l \geq 0$ for simplicity)

where $0 \leq r \leq k-1$. Then $r = l - q\cdot k \in I$ and by minimality of k, r must be zero. This means $l \in k\cdot\mathbb{Z}$

Hence $I = k\cdot\mathbb{Z}$. □

Operations, important for number theory, on $\mathbb{Z}$, and how they look in the set of ideals:

In $\mathbb{Z}_{\geq 0}$		In Set of ideals of $\mathbb{Z}$
n	$\longleftrightarrow$	I_n
(1) $d = \gcd(m,n)$	$\longleftrightarrow$	$I_d = I_m + I_n$ ↑ smallest ideal containing both I_m & I_n
(2) $l = \text{l.c.m.}(m,n)$	$\longleftrightarrow$	$I_l = I_m \cap I_n$ ↑ largest ideal contained in both I_m and I_n
(3) n divides m (m is div. by n)	$\longleftrightarrow$	$I_m \subset I_n$

Proofs: (3): $I_m \subset I_n$ means $m\cdot\mathbb{Z} \subset n\cdot\mathbb{Z}$; i.e.

$m \in n\mathbb{Z}$, which is same as saying $m = n\cdot q$ for some $q \in \mathbb{Z}$; i.e., m is div. by n.

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

i.e. $x = l.c.m(m,n)\cdot q$ for some $q \in \mathbb{Z}$

i.e. $x \in l\cdot\mathbb{Z} = I_l$. $(l = lcm(m,n))$.

(1). Let $I \subset \mathbb{Z}$ be an ideal containing I_m and I_n.

So $m, n \in I$ and hence $am + bn \in I \quad \forall a, b \in \mathbb{Z}$

$\Rightarrow \gcd(m,n) \in I$

$\Rightarrow I_d \subset I \quad (d = \gcd(m,n))$.

(33.2) Some terminology is borrowed from this "dictionary".

(R: commutative). $I, J \subset R$ two ideals are said to be

coprime if $I + J = R$.

Lemma. $I + J \overset{defn}{:=} \{a+b : a \in I, b \in J\}$ is an ideal;

and smallest one containing both I & J.

Pf. - $I + J$ is clearly a subgroup of R; and $I, J \subset I+J$.

For $r \in R$; $x = a+b \in I+J$

$r\cdot x = r\cdot a + r\cdot b \in I+J$

$\Rightarrow I+J$ is an ideal.

If $K \subset R$ is an ideal s.t. $I, J \subset K$; then

$\forall\, a \in I,\ b \in J$; $a+b \in K$; hence $I+J \subset K$.

$\Downarrow$ $\quad \Uparrow$

$a, b \in K$

□

(33.3) Quotient rings. Let R be a ring and $I \subsetneq R$ be a 2-sided ideal.

$a \pmod I \quad (= \bar{a})$

$\overline{R} = R/I$ = To be defined as a ring. $=$ $\begin{cases} \bullet\ (R/I\ ;\ +\pmod I\ ;\ 0 \pmod I) \\ \qquad \text{as abelian group.} \\ \bullet\ a \pmod I \overset{\text{mult in } R/I}{\cdot}\ b \pmod I \\ \qquad \overset{\text{defn.}}{=} ab \pmod I \\ \qquad (a, b \in R). \end{cases}$

Need to check: mult in R/I as written above is well-defined: meaning:

$a_1 \equiv a_2 \mod I \quad \Rightarrow \quad a_1 b_1 \equiv a_2 b_2 \pmod I$

$b_1 \equiv b_2 \mod I$

pf: $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2$

$= a_1 \underbrace{(b_1 - b_2)}_{\in I} + \underbrace{(a_1 - a_2)}_{\in I} b_2$

$\Rightarrow a_1 b_1 = a_2 b_2 \pmod I$

$b_1 - b_2 \in I$ because it is a left ideal

$a_1 - a_2 \in I$ because I is a right ideal.

□

$0_R \not\equiv 1_R \pmod I$ since we assumed $I \subsetneq R$.

We denote the ring just defined as R/I (quotient ring).

It is naturally equipped with a ring homomorphism

$$\begin{array}{ccc} \pi : R & \longrightarrow & R/I \\ \cup & & \cup \\ a & \longmapsto & a \pmod I \end{array}$$

$$(a = b \pmod I \leftrightarrow a - b \in I)$$

(33.4) Analogue of 1st iso. thm.

First Isomorphism theorem for rings: Let $f : R \to S$ be a ring hom. $I = \ker(f) \subsetneq R$ (2-sided ideal).

Then f factors through π: $f = \overline{f} \circ \pi$:

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ & \searrow^{\pi} \quad \nearrow_{\overline{f}} & \\ & R/I & \end{array}$$

$\overline{f}$ can be viewed as an <u>isomorphism</u> of rings

$$R/I \xrightarrow{\sim} \mathrm{Im}(f) \text{ (subring of } S).$$

Proof - $\overline{f} : R/I \to S$ is defined as

$$a \pmod I \longmapsto f(a).$$

It is unambiguous because if $a \equiv b \pmod I$

then $a - b \in I \implies f(a-b) = 0$ (remember $I = \ker f$)

Hence $f(a) = f(b)$ in S.

It is <u>almost by definition of R/I</u> that $\bar{f}$ is a ring hom

and $f = \bar{f} \circ \pi$.

Now $\bar{f}$ restricted to $\mathrm{Im}(f) \subset S$ is injective,

because $\ker(\bar{f}) \ni a \pmod I$; It is also surjective,

$\Updownarrow$

$f(a) = 0$ i.e. $a = 0 \pmod I$

by defn of the image. Hence we get an iso. $R/\ker(f) \xrightarrow{\sim} \mathrm{Im} f$

$\bar{a} \longmapsto f(a)$

$a \pmod{\ker f}$.

□