Lecture 26

(26.0) Recall: we defined rings, left/right/two-sided ideals, subrings and homomorphisms of rings.

Let R be a ring. $\mathfrak{a} \subset R$ an ideal (i.e. $\mathfrak{a} \subset R$ is a subgroup such that $\forall\, r \in R,\ a \in \mathfrak{a}$, $r.a$ and $a.r$ are in $\mathfrak{a}$).

Recall $R^\times$ = the multiplicative group of invertible elements in R

Note: $\mathfrak{a} \cap R^\times \neq \phi \implies \mathfrak{a} = R$ (called the unit ideal).
$= (1)$

(26.1) Algebra of ideals.

Let $\mathcal{I}(R)$ = set of all ideals of R.

$\forall\, \mathfrak{a}, \mathfrak{b} \in \mathcal{I}(R)$, define $\mathfrak{a} + \mathfrak{b} := \{ a+b : a \in \mathfrak{a},\ b \in \mathfrak{b} \}$

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{N} a_i b_i \text{ where } N \geq 0 \text{ is arbitrary},\ a_1, \dots, a_N \in \mathfrak{a},\ b_1, \dots, b_N \in \mathfrak{b} \right\}$$

Easy check: $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a} \cdot \mathfrak{b}$ are again ideals of R.

$(\mathcal{I}(R), +, (0))$ ← additive monoid

$(\mathcal{I}(R), \cdot, (1))$ ← multiplicative monoid

(26.2) Let R be a ring and $a_1, \dots, a_n \in R$.

The left-ideal generated by $a_1, \dots, a_n = Ra_1 + \dots + Ra_n$
$=: {}_R(a_1, \dots, a_n)$

The right ideal generated by $a_1, \dots, a_n = a_1R + \dots + a_nR$
$=: (a_1, \dots, a_n)_R$

The ideal generated by $a_1, \dots, a_n = Ra_1R + \dots + Ra_nR$
$=: (a_1, \dots, a_n)$

More generally for any subset $X \subset R$, the ideal generated by X: $(X) = \bigcap_{\mathfrak{a} \subset R \text{ ideal}, X \subset \mathfrak{a}} \mathfrak{a}$ (similarly ${}_R(X)$ & $(X)_R$)

Definition: An ideal $\mathfrak{a} \subset R$ is said to be <u>finitely generated</u> if $\exists\, a_1, \dots, a_m \in \mathfrak{a}$ such that

$$\mathfrak{a} = (a_1, \dots, a_m)$$

$\mathfrak{a}$ is called <u>a principal ideal</u> if $\exists\, a \in R$ such that

$$\mathfrak{a} = (a) = RaR$$

We say that R is a principal ideal ring if every ideal $\mathfrak{a} \subset R$ is principal.

e.g. $\mathbb{Z}$ is a principal ideal ring (actually domain).

$\mathbb{C}[x]$ is also a principal ideal domain.

(26.3) Ideals in $\mathbb{Z}/N\mathbb{Z}$.

By the analogue of first isomorphism theorem,

$$\text{Ideals in } \mathbb{Z}/N\mathbb{Z} \longleftrightarrow \text{Ideals in } \mathbb{Z} \text{ containing } N$$

$$= \{(d) : d \text{ divides } N\}$$

The analogue of 'divisibility of N by d' is the containment '$(N) \subset (d)$'.

(26.4) Remark: let $f : R_1 \to R_2$ be a hom of rings, $\mathfrak{a}_2 \subset R_2$ be an ideal.

$$f : R_1 \longrightarrow R_2 \longrightarrow R_2/\mathfrak{a}_2$$

$$\bar{g}$$

$\ker(g) = \bar{f}^{-1}(\mathfrak{a}_2) =: \mathfrak{a}_1$ and hence we get

$$R_1/\mathfrak{a}_1 \hookrightarrow R_2/\mathfrak{a}_2$$

(26.5) Characteristic of a ring.

Let R be a ring. We have a natural ring hom

$$\varphi : \mathbb{Z} \longrightarrow R$$
$$m \longmapsto m \cdot 1_R = \underbrace{1_R + \dots + 1_R}_{m \text{ times}} \quad (m \geq 0)$$

and $\varphi(-n) = -\varphi(n)$

$\mathrm{Ker}(\varphi) \subset \mathbb{Z}$ is an ideal. Since $1_R \neq 0_R$, $\mathrm{Ker}(\varphi) \neq \mathbb{Z}$.

Thus $\mathrm{Ker}(\varphi) = (N)$ for some $N \in \mathbb{Z}_{\geq 0}$; $N \neq 1$. (N: characteristic of R)

$N = 0$: characteristic of R is zero [$\mathbb{Z}$ is the characteristic subring of R]

$N > 0$: $\mathbb{Z}/N\mathbb{Z} \hookrightarrow R$ is the characteristic subring.

If R is a domain, $\mathrm{Char}(R)$ must be 0 or a prime number.

(26.6) Ideals in a commutative ring.

Let R be a commutative ring. The arithmetic of natural numbers has its analogue in the set of ideals of R.

Divisibility $\leftrightarrow$ Inclusion (for $\mathbb{Z}$, $n \mid m \iff (m) \subset (n)$)

Greatest Common divisor $\leftrightarrow$ Sum ($(n) + (m) = (\gcd(m,n))$)

Least common multiple $\leftrightarrow$ Intersection ($(n) \cap (m) = (\operatorname{lcm}(m,n))$)

Multiplication $\leftrightarrow$ Product ($(n) \cdot (m) = (nm)$)

With this dictionary in mind, we say two ideals $\mathfrak{a}, \mathfrak{b} \subset R$ are <u>coprime</u> if $\mathfrak{a} + \mathfrak{b} = R = (1)$.

Similarly we write $r_1 \equiv r_2 \pmod{\mathfrak{a}}$ if $r_1 - r_2 \in \mathfrak{a}$

(i.e. $\pi(r_1) = \pi(r_2)$ for $\pi : R \longrightarrow R/\mathfrak{a}$)

<u>Sun Tzu's theorem</u> Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals in R which are pairwise coprime (i.e. $\forall\, i \neq j$, $\mathfrak{a}_i + \mathfrak{a}_j = R$).

Then for any $x_1, \dots, x_n \in R$, $\exists\, x \in R$ such that

$$x \equiv x_i \pmod{\mathfrak{a}_i} \quad (1 \leq i \leq n).$$

Proof. The proof uses the following fact (easy to demonstrate)

$$\underset{\text{ideals}}{\mathfrak{b}_1, \ldots, \mathfrak{b}_r} \subset R \quad \Rightarrow \quad \prod_{i=1}^{r} \mathfrak{b}_i \subset \bigcap_{i=1}^{r} \mathfrak{b}_i \qquad - (*)$$

Idea: find $y_1, \ldots, y_n \in R$ such that $\forall\ 1 \leq i \leq n$

$$y_i \equiv 1 \mod \mathfrak{o}_i \quad , \quad y_i \equiv 0 \mod \mathfrak{o}_j \quad (\forall j \neq i)$$

If we succeed, we will set $x = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$

and get that $x \equiv x_i \mod \mathfrak{o}_i$ for each $1 \leq i \leq n$.

<u>$n = 2$ case.</u> $R = \mathfrak{o}_1 + \mathfrak{o}_2 \Rightarrow 1 = a_1 + a_2$ for some $a_1 \in \mathfrak{o}_1$, $a_2 \in \mathfrak{o}_2$

Take $y_1 = a_2$ and $y_2 = a_1$

[Check: $y_1 = a_2 \in \mathfrak{o}_2 \Rightarrow y_1 \equiv 0 \mod \mathfrak{o}_2$

$1 = a_1 + y_1 \Rightarrow 1 - y_1 \in \mathfrak{o}_1$ i.e. $y_1 \equiv 1 \mod \mathfrak{o}_1$]

<u>General case.</u> Since $R = \mathfrak{o}_1 + \mathfrak{o}_j \quad (2 \leq j \leq n)$

$$1 = a_1^{(j)} + a_j \qquad \left(a_1^{(j)} \in \mathfrak{o}_1,\ a_j \in \mathfrak{o}_j \right)$$

$$\Rightarrow 1 = \prod_{j=2}^{n} \left(a_1^{(j)} + a_j \right) \in \mathfrak{o}_1 + \prod_{j=2}^{n} \mathfrak{o}_j$$

By $n=2$ case, we can find $y_1 \in R$ s.t.

$$y_1 \equiv 1 \bmod \mathfrak{a}_1 \qquad y_1 \in \prod_{j=2}^{n} \mathfrak{a}_j \subset \bigcap_{j=2}^{n} \mathfrak{a}_j$$

i.e. $y_1 \equiv 1 \bmod \mathfrak{a}_1$ and $y_1 \equiv 0 \bmod \mathfrak{a}_j$ $(2 \le j \le n)$

Repeat this argument for each i to find $y_i \in R$ such that $y_i \equiv 1 \pmod{\mathfrak{a}_i}$ and $y_i \equiv 0 \pmod{\mathfrak{a}_j}$ $(j \neq i)$.

□

Cor. $$R/\bigcap_{i=1}^{n} \mathfrak{a}_i \xrightarrow{\sim} \prod_{i=1}^{n} R/\mathfrak{a}_i$$

[under the assumptions imposed by Theorem above].

Pf. $$R \xrightarrow{f} R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times \cdots \times R/\mathfrak{a}_n$$

is surjective by the theorem. $\operatorname{Ker}(f) = \bigcap_{i=1}^{n} \mathfrak{a}_i$

and we are done by the 1st iso. thm. □