Lecture 16: Algebra of ideals ; modules

Recall : Last time we defined rings, left/right/two-sided ideals, subrings & homomorphisms of rings.

$R^\times = \mathcal{U}(R)$ = multiplicative group of invertible elements (or units of R)

Fix a ring R & $\mathfrak{a} \subset R$ an ideal (ie $\mathfrak{a} \subset R$ subgroup (w/+) so that $\forall r \in R, a \in \mathfrak{a}$: $r \cdot a$ & $a \cdot r \in \mathfrak{a}$).

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

§1. Algebra of ideals:

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

- Given $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}(R)$, define:

① $\mathfrak{a} + \mathfrak{b} := \{ a+b : a \in \mathfrak{a}, b \in \mathfrak{b} \}$

② $\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{N} a_i b_i \text{ where } N \geq 0 \text{ is arbitrary}, \begin{array}{l} a_1, \dots, a_N \in \mathfrak{a} \\ b_1, \dots, b_N \in \mathfrak{b} \end{array} \right\}$

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

- $(\mathcal{I}(R), +, (0))$ is an additive monoid.
- $(\mathcal{I}(R), \cdot, (1))$ is a multiplicative monoid.

§2. Ideals generated by sets:

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

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

The right-ideal ———— is $a_1R + \dots + a_nR =: (a_1, \dots, a_n)_R$.

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

• More generally, for any subset $X \subset R$, the ideal generated by X is:

$$\boxed{(X) = \bigcap_{\substack{\mathfrak{a} \in \mathcal{I}(R) \\ X \subset \mathfrak{a}}} \mathfrak{a}}$$

Similarly, we have $(X)_R = \bigcap_{\substack{\mathfrak{a} \subset R \\ \text{right-ideal} \\ X \subseteq \mathfrak{a}}} \mathfrak{a}$ & ${}_R(X) = \bigcap_{\substack{\mathfrak{a} \subset R \\ \text{left-ideal} \\ X \subseteq \mathfrak{a}}} \mathfrak{a}$

[Lecture 15: These intersections always give left/right/two-sided ideals.]

<u>Definition</u>: 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 $\mathfrak{a} = (a_1, \dots, a_m)$

. An ideal $\mathfrak{a}$ is <u>principal</u> if $\mathfrak{a} = (a) = RaR$ for some $a \in R$

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

<u>Main examples</u>: $\mathbb{Z}$ is a principal ideal ring (actually domain)
PID
$\mathbb{C}[x]$ is also a principal ideal domain. (PID)

<u>Non-example</u>: $\mathbb{Z}[x]$ $\quad \mathfrak{a} = (2, x)$ is not principal.

<u>Example</u> Ideals in $\mathbb{Z}/N\mathbb{Z}$ $\quad$ By 2^{nd} Iso Theorem.

Ideals in $\mathbb{Z}/N\mathbb{Z}$ $\longleftrightarrow$ ideals in $\mathbb{Z}$ containing N
$= \{(d) : d \text{ divides } N\}$

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

§3 <u>Characteristic of a ring</u>:

<u>Remark</u>: Let $f: R_1 \to R_2$ be a homomorphism of rings & $\mathfrak{a}_2 \in \mathcal{I}(R_2)$

$$f: \begin{tikzcd} R_1 \arrow[r] \arrow[rr, bend right, "g"'] & R_2 \arrow[r] & R_2/\mathfrak{a}_2 \end{tikzcd}$$

$\ker(g) = f^{-1}(\mathfrak{a}_2) =: \mathfrak{a}_1$

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

Let R be a ring. We have a natural ring homomorphism:

$$\varphi : \mathbb{Z} \longrightarrow R$$

$$m \longmapsto m \cdot 1_R = \underbrace{1_R + \cdots + 1_R}_{m \text{ times}} \qquad \text{for } m \geq 0$$

and $\varphi(-n) = -\varphi(n)$ for $n \geq 0$.

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

Thus $\mathrm{Ker}(\varphi) = (N)$ for some $N \geq 0$, $N \neq 1$.

- If $N = 0$: we say the characteristic of R is zero [$\mathbb{Z}$ is the characteristic subring of R]
- If $N > 0$: $\mathbb{Z}/N\mathbb{Z} \hookrightarrow R$ is the characteristic subring

Obs: If R is a domain, then $\mathrm{char}(R) = 0$ or a prime number.
(because $\mathbb{Z}/N\mathbb{Z}$ cannot have zero divisors since R has none)

§4. Modules: Definitions & examples

In what follows, we set R = an arbitrary ring
A = a commutative ring

Def: Left and right modules over R

- A left (resp right) module M (resp. N) over R is an abelian group M (resp. N) together with a bilinear map

$$R \times M \xrightarrow{\ \cdot\ } M \qquad (\text{resp } N \times R \xrightarrow{\ \cdot\ } N)$$

such that
$$1 \cdot m = m \qquad (\text{resp } n \cdot 1 = n) \quad \forall a, b \in R$$
$$(a \cdot b) \cdot m = a \cdot (b \cdot m) \qquad n(a \cdot b) = (n \cdot a) \cdot b \quad m \in M,\ n \in N$$

Bilinear means linear in each component:

$$(a+b, m) \longmapsto (a+b) \cdot m = (a \cdot m) + (b \cdot m)$$

$(a, m+m') \longmapsto a\cdot(m+m') = a\cdot m + a\cdot m'$.

Note: $(-a)\cdot m = -(a\cdot m) = a\cdot(-m)$ from bilinearity

$0_R \cdot m = 0_M$ for all $m \in M$.

Remark: A more economical way of defining left/right modules over R would be to have an abelian group M (resp. N) and a ring hom

$\lambda : R \longrightarrow \mathrm{End}_{gp}(M)$ (resp: $R^{op} \longrightarrow \mathrm{End}_{gp}(N)$)

same as R as an abelian gp
$a\cdot b$ in R^{op} $= ba$ in R

where $\lambda(r) : M \longrightarrow M$ (resp $\rho(\lambda) : N \longrightarrow N$)
$m \longmapsto r\cdot m$ $\quad$ $n \longmapsto n\cdot r$

Obs: When the ring is commutative, left = right, so we simply use the term module.

Examples: ① $\mathfrak{a} \subset R$ left ideal is a left module $/R$
right ——— right ———

② Every abelian group is a module over $\mathbb{Z}$

$(n\cdot m = \underbrace{m + \cdots + m}_{n \text{ times}}$ for $n \geq 0$ or $n\cdot m = (-n)\cdot(-m)$) for $n \leq 0$.

③ $\forall n \geq 1$: $M = R^n$ (resp $N = R^n$) is a left (resp. right) module over R.

§5 Homomorphisms of modules:

Let M_1 & M_2 be two left R-modules. An R-linear map (or left R-module homomorphism) is a homomorphism of abelian groups $f : M_1 \longrightarrow M_2$ such that $f(r\cdot m_1) = r\, f(m_1)$ $\forall r \in R, m_1 \in M_1$

Write $f \in \mathrm{Hom}_R(M_1, M_2)$ = set of all R-linear maps $M_1 \longrightarrow M_2$.

Obs: $\mathrm{Hom}_R(M_1, M_2)$ has a structure of an abelian gp

$f, g \in \mathrm{Hom}_R(M_1, M_2)$, then $f+g \in \mathrm{Hom}_R(M_1, M_2)$

via $(f+g)(m_1) = f(m_1) + g(m_1) \underset{M_2 \text{ ab}}{=} g(m_1) + f(m_1) =: (g+f)(m_1)$

- We have the usual notions of submodules, submodules generated by sets, quotient modules, kernels & images. In particular, we have the 3 isomorphism Thms (HW6)

Eg: $f: M_1 \longrightarrow M_2 \rightsquigarrow$

$$\begin{tikzcd} M_1 \arrow[r, "f"] \arrow[d, "\pi"'] & M_2 \\ M_1/\ker f \arrow[r, "\cong", "\bar{f}"'] & \mathrm{Im} f \arrow[u, hook] \end{tikzcd}$$

§6. Direct Sum of modules:

Def Let I be a set and $(M_i)_{i\in I}$ a set of (left) R-modules.

$$\bigoplus_{i\in I} M_i = \{ (x_i)_{i\in I} : \begin{array}{l} x_i \in M_i \ \forall i \\ x_i = 0 \text{ for all but } \underline{\text{finitely many}}\ i \in I \end{array} \}$$

is again a (left) R-module (with componentwise operations:

$$\begin{cases} (x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \\ r\cdot(x_i)_{i\in I} = (r x_i)_{i\in I} \end{cases}$$

Universal Property:

Given a left R-module N and $\{f_i \in \mathrm{Hom}_R(M_i, N)\}_{i\in I}$, there exists a unique R-linear map

$$f: \bigoplus_{i\in I} M_i \longrightarrow N$$
$$(x_i)_{i\in I} \longmapsto \sum_{i\in I} f(x_i) \quad \text{(finite sum by definition of } \bigoplus_{i\in I} M_i\text{)}$$

Obs: $M_j \overset{\varphi_j}{\hookrightarrow} \bigoplus_{i\in I} M_i$ gives $f \circ \varphi_j = f_j$

$$\begin{tikzcd} \bigoplus M_i \arrow[dr, dashed, "f"] & \\ M_j \arrow[u, hook] \arrow[r, "f_j"'] & N \end{tikzcd}$$

Special case: M a left R-module, $M_1, M_2 \subset M$ submodules

Prop: $M \xleftarrow{\sim} M_1 \oplus M_2$ if & only if
- $M_1 + M_2 = M$
- $M_1 \cap M_2 = \{0\}$

Proof: As $M_1 \hookrightarrow M$, $M_2 \hookrightarrow M$ are R-linear, we get by the universal property

$$M_1 \oplus M_2 \xrightarrow{f} M$$
$$(m_1, m_2) \longmapsto m_1 + m_2$$

- Image of f = submodule of M generated by M_1 & M_2
- Kernel of $f = \{(x, -x) : x \in M_1 \cap M_2\}$

Thus, f is an isomorphism iff $M = M_1 + M_2$ & $M_1 \cap M_2 = \{0\}$.

Exercise: Generalize to $\{M_i \hookrightarrow M\}_{i \in I}$ that is:

$\bigoplus_{i \in I} M_i \longrightarrow M$ is an isomorphism iff

(1) $M = \sum_{i \in I} M_i$ (submodule generated by $\{M_i\}_{i \in I}$)

(2) $M_i \cap \sum_{\substack{j \in I \\ j \neq i}} M_j = 0 \quad \forall i \in I$

§7. Short exact sequences:

Def: If M_1, M_2, M_3 are three left R-modules, and $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ are R-linear maps, we say this sequence is exact (at M_2) if

Image of f = Kernel of g

Def 2: $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ s.e.s

means
- f injective, g surjective
- $\mathrm{Im}(f) = \mathrm{Ker}(g)$

Def 3: A short exact sequence $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is **Trivial** if we have an R-linear isomorphism $M_1 \oplus M_3 \xrightarrow{\eta} M_2$ st:

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "f"] \arrow[d, equal] \arrow[dr, phantom, "\circlearrowleft"] & M_2 \arrow[r, "g"] \arrow[dr, phantom, "\circlearrowleft"] & M_3 \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & M_1 \arrow[r, hook, "i"] & M_1 \oplus M_3 \arrow[r, "\pi_2"] \arrow[u, "\eta"] & M_3 \arrow[r] & 0 \end{tikzcd}$$

Proposition: A short exact sequence $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is Trivial if and only if $\exists$ R-linear $s: M_3 \to M_2$ st $g \circ s = id_{M_3}$ ($\exists$ section)

Proof: ($\Rightarrow$) Take $j: M_3 \hookrightarrow M_1 \oplus M_3$ as the usual inclusion and define $s: M_3 \to M_2$ as $\eta \circ j$.

($\Leftarrow$) $\eta: M_1 \oplus M_3 \longrightarrow M_2$ is R-linear

$(x, y) \longmapsto f(x) + s(y)$

and it makes the diagram commute

Exercise: Verify that η is an isomorphism.

§8. Direct Product:

Again, if I is a set and $\{M_i\}_{i \in I}$ is a collection of left R-modules, the **direct product** $\prod_{i \in I} M_i$ is defined as

$$\prod_{i \in I} M_i = \{ (x_i)_{i \in I} \text{ where } x_i \in M_i \ \forall i \}$$

(NOTE: No finiteness condition!)

Remark: For I finite $\bigoplus_{i \in I} M_i \xrightarrow{\sim} \prod_{i \in I} M_i$ as left R-modules. For general I, they are different.

Universal Property: Given a left R-module N and R-linear maps $f_i : N \longrightarrow M_i$, there exists a unique map

$$\begin{aligned} N &\xrightarrow{\ f\ } \prod_{i \in I} M_i \\ n &\longmapsto (f_i(n))_{i \in I} \end{aligned}$$

This will not be allowed for direct sums unless I is finite

Furthermore $\pi_i : \prod_{i \in I} M_i \longrightarrow M_i$ is the projection to the i^{th} term, we have

$$\begin{tikzcd} N \arrow[d, "f_i"'] & \prod_{i \in I} M_i \arrow[l, "f"'] \arrow[dl, "\pi_i"] \\ M_i & \end{tikzcd}$$