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 $\forall r \in R, a \in \mathfrak{a}$: $r \cdot a$ & $a \cdot r \in \mathfrak{a}$).

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 ${}_R(a_1, \dots, a_n)$

The right-ideal ________________________ is $(a_1, \dots, a_n)_R$

The ideal generated by $a_1, \dots, a_n$ is $(a_1, \dots, a_n)$

- 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.]

Finitely Generated Ideals - Principal Ideals

Definition: An ideal $\mathfrak{a} \subset R$ is said to be finitely generated if $\exists\, a_1, \ldots, a_m \in \mathfrak{a}$ such that $\mathfrak{a} = (a_1, \ldots, a_m)$

- An ideal $\mathfrak{a}$ is principal if $\mathfrak{a} = (a) = RaR$ for some $a \in R$
- We say that R is a principal ideal ring if every ideal $\mathfrak{a} \subset R$ is principal.

Characteristic of a ring

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

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

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

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

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

$$\varphi: \mathbb{Z} \longrightarrow R \qquad m \longmapsto m \cdot 1_R = \underbrace{1_R + \cdots + 1_R}_{m \text{ times}} \qquad \text{for } m \geq 0$$

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)

Modules: Definitions & examples

Def 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 $1 \cdot m = m$ (resp $n \cdot 1 = n$) $\forall a, b \in R$

$(a \cdot b) \cdot m = a \cdot (b \cdot m)$ $\qquad n(a \cdot b) = (n \cdot a) \cdot b$ $\quad m \in M \ n \in N$

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 $m \in M$.

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

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

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

where

$$\lambda(r) : M \longrightarrow M \qquad (\text{resp } \rho(r) : N \longrightarrow N \quad)$$
$$m \longmapsto r \cdot m \qquad\qquad n \longmapsto n \cdot r$$

Homomorphisms of modules

Fix M_1, M_2 left R-modules.

<u>Def</u>: An R-linear map (or left R-module homomorphism) is a homomorphism of abelian groups $f: M_1 \longrightarrow M_2$ such that $f(r \cdot m_1) = r f(m_1)$ $\forall r \in R, m_1 \in M_1$

<u>Notation</u>. $\mathrm{Hom}_R(M_1, M_2)$ = set of all R-linear maps $M_1 \longrightarrow M_2$

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

Direct Sums

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

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

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

$$\boxed{(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \qquad r\cdot (x_i)_{i\in I} = (r x_i)_{i\in I}}$$

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 $M_1 + M_2 = M$ & $M_1 \cap M_2 = \{0\}$

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

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

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

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

Proposition: A short exact sequence $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ is trivial if and only if $\exists$ R-linear $s : M_3 \longrightarrow M_2$ st

$$g \circ s = id_{M_3} \quad (\exists \text{ section})$$

Direct Product

Def: Again, if I is a set and $\{M_i\}_{i\in I}$ is a collection of left R-modules, the <u>direct product</u>

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

(<u>NOTE</u>: No finiteness condition!)

<u>Remark</u>: 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