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

Algebra of ideals set $\boxed{\mathcal{J}(R) = \text{set of all ideals of } R.}$

$\mathfrak{a}, \mathfrak{b} \in \mathcal{J}(R)$, define $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}\cdot\mathfrak{b} \in \mathcal{J}(R)$ via

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

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

- $(\mathcal{J}(R), +, (0))$ is an additive monoid.

$\Rightarrow$

- $(\mathcal{J}(R), \cdot, (1))$ is a multiplicative monoid

Ideals generated by sets

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

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

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

The <u>ideal</u> generated by $a_1, \dots, a_n$ is $(a_1, \dots, a_n) := Ra_1R + \dots + Ra_nR$

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

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

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 $\mathcal{A} \subset R$ is said to be **finitely generated** if $\exists\, a_1, \ldots, a_m \in \mathcal{A}$ such that $\mathcal{A} = (a_1, \ldots, a_m)$

. An ideal $\mathcal{A}$ is **principal** if $\mathcal{A} = (a) = RaR$ for some $a \in R$

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

Main examples: ($\mathbb{Z}$ is a principal ideal ring (actually domain)) — PID

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

Non-example: $\mathbb{Z}[x]$ $\quad \mathcal{A} = (2, x)$ is not principal.

Example: Ideals in $\mathbb{Z}/N\mathbb{Z} = ?$ By 2nd Iso Theorem.

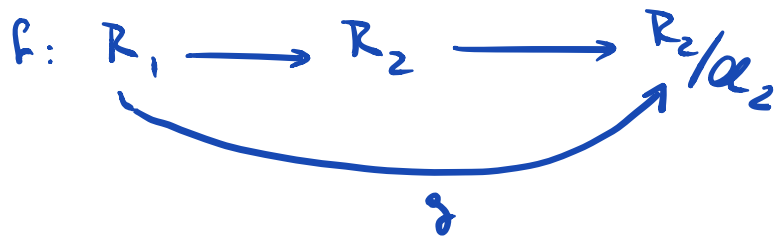
Ideals in $\mathbb{Z}/N\mathbb{Z}$ $\longleftrightarrow$ ideals in $\mathbb{Z}$ containing N

$= (d\mathbb{Z}/N\mathbb{Z})$ $\quad = \{(d) : d \text{ divides } N\}$

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

Characteristic of a ring

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



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

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 $n \geq 0$.

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

Thus $\ker(\varphi) = (N)$ 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 $\operatorname{char}(R) = 0$ 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

$$R \times M \xrightarrow{\cdot} M \quad \left(\text{resp } N \times R \xrightarrow{\cdot} N \right)$$

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

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

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

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

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

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

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

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

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

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

Homomorphisms of modules

Fix M_1, M_2 left R-modules.

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

Notation: $\mathrm{Hom}_R(M_1, M_2)$ = 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

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

via $(f+g)(m_1) = f(m_1) + g(m_1) = g(m_1) + f(m_1) =: (g+f)(m_1)$

(M_2 ab)

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

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

$$\begin{array}{ccc} M_1 & \xrightarrow{f} & M_2 \\ \pi \downarrow & & \uparrow \\ M_1/\ker f & \xrightarrow[\cong]{\bar{f}} & \mathrm{Im}\, f \end{array}$$

Direct Sums

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

$$\bigoplus_{i\in I} M_i = \{ (x_i)_{i\in I} : x_i \in M_i \ \forall i, \ x_i = 0 \text{ for all but finitely many } i \in I \}$$

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

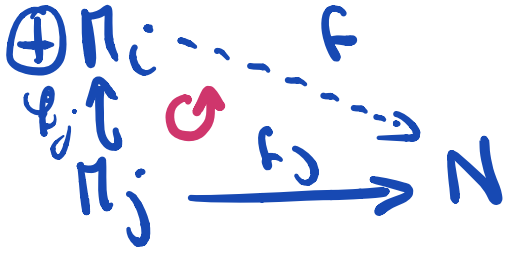
$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \qquad r\cdot(x_i)_{i\in I} = (rx_i)_{i\in I}$$

Universal Property: Given a left R-module N and $M_i \xrightarrow{f_i} N \ \forall i$ there exists a unique R-linear map

$$f : \bigoplus_{i\in I} M_i \longrightarrow N$$
$$(x_i)_{i\in I} \longmapsto \sum_{i\in I} f(x_i)$$

(finite sum by definition of $\bigoplus_{i\in I} M_i$)

Satisfying



where $\varphi_j : M_j \hookrightarrow \bigoplus_{i\in I} M$ inclusion in i^{th} spot.

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

$$\begin{array}{ccc} M_1 \oplus M_2 & \xrightarrow{f} & M \\ (m_1, m_2) & \longmapsto & m_1 + m_2 \end{array}$$

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

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

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 $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is **Trivial** if we have an R-linear isomorphism

$M_1 \oplus M_3 \xrightarrow{\cong} M_2$ st :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f} & M_2 & \xrightarrow{g} & M_3 & \longrightarrow & 0 \\ & & \| & & \circlearrowleft \cong \uparrow & & \circlearrowleft \| & & \\ 0 & \longrightarrow & M_1 & \xrightarrow{i} & M_1 \oplus M_3 & \xrightarrow{\pi_2} & M_3 & \longrightarrow & 0 \end{array}$$

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

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

Direct Product

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

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

(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

$$N \xrightarrow{f} \prod_{i\in I} M_i$$

$$n \longmapsto (f_i(n))_{i\in I}$$

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

Furthermore for $\pi_i: \prod_{i\in I} M_i \longrightarrow M_i$, then

(projection to i^{th} spot)