

Definition

A local ring: Exactly one maximal ideal

A semilocal ring: At least one, and at most finitely many max ideals

Non-ent criterion:

$$A \cong \underbrace{\underbrace{n}_{\text{non units}}}_{\text{non units}} \iff A \text{ local} \iff \underbrace{n}_{\text{ideal}} \text{ (maximal ideal)}$$

$$\text{Pf. } n \subseteq \mathcal{O} \text{ all proper ideal} \Rightarrow n \text{ ideal} \Rightarrow \text{only max ideal} \Rightarrow \text{local}$$

(Prime avoidance)

$$1) \mathcal{O} \subseteq R \cong \underbrace{\mathcal{O}}_{\text{ring}} \supseteq \underbrace{\mathcal{O}}_{\text{prime ideals}} \text{ s.t. } \mathcal{O} \subseteq \bigcup_{i=1}^n \mathcal{O}_i \Rightarrow \exists i \text{ s.t. } \mathcal{O} \subseteq \mathcal{O}_i$$

$$2) \mathcal{O}_1, \dots, \mathcal{O}_n \subseteq R \cong \underbrace{\mathcal{O}_i}_{\text{ideals}} \text{ s.t. } \bigcap_{i=1}^n \mathcal{O}_i \subseteq \mathcal{O} \Rightarrow \exists i \text{ s.t. } \mathcal{O}_i \subseteq \mathcal{O}$$

Pf. 1) By induction on n . For $n=1$ obvious. Suppose true for $n-1$. Then for each $i \exists x_i \in \mathcal{O}$ s.t. $x_i \notin \mathcal{O}_j$ for $j \neq i$. If for some i , $x_i \notin \mathcal{O}_i$, then \mathcal{O} . If not, $x_i \in \mathcal{O}_i \forall i$.

Put

$$y = \sum_{i=1}^n x_i \prod_{j \neq i} x_j$$

We have $y \in \mathcal{O}$, and $y \notin \mathcal{O}_i$.

2) Suppose $\mathcal{O}_i \not\subseteq \mathcal{O} \forall i$. Then $\exists x_i \in \mathcal{O}_i$ s.t. $x_i \notin \mathcal{O}$.

$$\Rightarrow x_1 \dots x_n \in \prod \mathcal{O}_i \subseteq \prod \mathcal{O}_i \subseteq \bigcap \mathcal{O}_i$$

$$\bullet x_1 \dots x_n \notin \mathcal{O} \text{ (prime)}$$

$$\Rightarrow \bigcap \mathcal{O}_i \not\subseteq \mathcal{O}$$

If $\mathcal{O} = \bigcap \mathcal{O}_i$, then $\mathcal{O} \subseteq \mathcal{O}_i$, combined with 2) $\mathcal{O}_i \subseteq \mathcal{O}$

$$\text{gives } \mathcal{O} = \mathcal{O}_i$$

$\sigma \subseteq R$
ideal ring

$$r(\sigma) = \bigcap_{\mathfrak{p} \supseteq \sigma} \mathfrak{p} = \sqrt{\sigma} = \{x \in R \mid x^n \in \sigma \text{ for some } n > 0\}$$

Pf. \subseteq : Let $x \in \sqrt{\sigma}$, i.e. $x^n \in \sigma$. Suppose $\sigma \subseteq \mathfrak{p}$, then $x^n \in \mathfrak{p}$

$$\Rightarrow x \in \mathfrak{p} \Rightarrow x \in \bigcap_{\mathfrak{p} \supseteq \sigma} \mathfrak{p} = r(\sigma)$$

\supseteq : Suppose $x \notin \sqrt{\sigma}$. Then $x^n \notin \sigma \forall n$, i.e. $S = \{1, x, x^2, \dots\}$ multiplicative and $S \cap \sigma = \emptyset$.

$$\Rightarrow \exists \mathfrak{p} \supseteq \sigma \text{ s.t. } x \notin \mathfrak{p}.$$

prime

($S = \{b \in R \mid b \supseteq \sigma, b \cap \sigma = \emptyset\} \neq \emptyset$ (since $1 \in S$), poset.

and any sequence $b_1 \subset b_2 \subset \dots$ of nested ideals is majorized by their union $\Rightarrow \exists$ maximal element $\mathfrak{p} \in S$ (by Zorn's lemma). Let $x, y \in \mathfrak{p}$ and $x, y \notin \mathfrak{p}$. Then

$(x) + \mathfrak{p}, (y) + \mathfrak{p} \notin S$. But $\sigma \subseteq (x) + \mathfrak{p}, (y) + \mathfrak{p}$, so we must have $(x) + \mathfrak{p} \cap S \neq \emptyset$ (and $(y) + \mathfrak{p} \cap S \neq \emptyset$) i.e. $ax + \mathfrak{p} \in S$

and $by + \mathfrak{p} \in S, p, q \in \mathfrak{p}$. But then $(ax + \mathfrak{p})(by + \mathfrak{p}) \in S$

$$S \ni (ax + \mathfrak{p})(by + \mathfrak{p}) = abxy + aqy + bpq + pq \in \mathfrak{p}$$

$$\Rightarrow S \cap \mathfrak{p} \neq \emptyset \text{ Contradiction.}$$

$$\Rightarrow \text{No } \sigma \Rightarrow x \notin \bigcap_{\mathfrak{p} \supseteq \sigma} \mathfrak{p} \text{ and } \bigcap_{\mathfrak{p} \supseteq \sigma} \mathfrak{p} \subseteq \sqrt{\sigma}$$

Definition of module.

- M
 R -module
- Additive abelian group
 - scalar multiplication $R \times M \rightarrow M \quad (r, m) \mapsto rm$
 - distributive, associative, unitary

Alternative:

$R \rightarrow \text{End}_Z(M)$ (as abelian group)
 ring homomorphism

$$r \mapsto \varphi_r, \quad \varphi_r(m) = rm$$

Faithful module

$$R \rightarrow \text{End}_Z(M)$$

injective

$$(0 : M) = \text{Ann}(M) \subset R.$$

0

Ex. \mathbb{R} ; Module = Vector space
 field

\mathbb{Z} ; Module = Abelian group

$M \subset R$; Module = Ideal

R -Module homomorphism : $\varphi(rm) = r \cdot \varphi(m)$

$\text{Hom}_R(M, N)$ is itself a R -module

$$(f+g)(m) = f(m) + g(m)$$

$$(r \cdot f)(m) = r \cdot f(m).$$

Quotient module

$$M' \subset M \rightarrow M/M' \text{ as abelian groups}$$

$$r \cdot (m+M') = rm+M'$$

UMP for modules

If $\mathcal{K}(M') = 0$ and given $\alpha : M \rightarrow N$ s.t. $\alpha(M') = 0$

$\Rightarrow \exists!$ homomorphism $M/M' \rightarrow N$

$$\begin{array}{ccc}
 M/M' & \xrightarrow{\exists! \bar{\alpha}} & N \\
 \uparrow \alpha & \searrow \alpha & \\
 M & &
 \end{array}$$

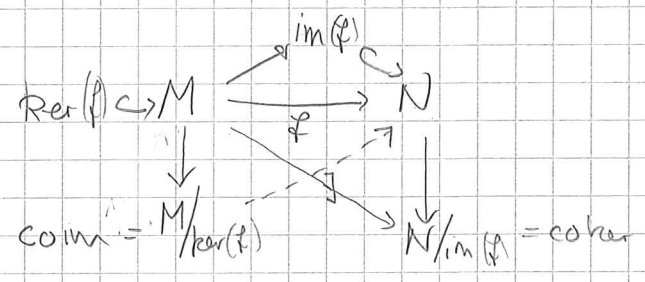
$\alpha(M') = 0$

Cyclic module $M = R \cdot m$ for some $m \in M$
 $\Rightarrow R/\text{Ann}(m) \cong M$

Finitely generated: $M = Rm_1 + Rm_2 + \dots + Rm_n, m_1, \dots, m_n \in M$

$f: M \rightarrow N$ Cokernel (f): $\text{coker}(f) := N/\text{im}(f)$

Coimage (f): $\text{coim}(f) := M/\text{ker}(f)$



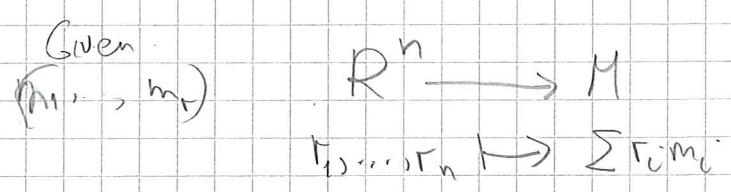
Free modules:

$$M = \sum_{\{i\}} R \cdot m_i$$

↑
generators.

$\{m_i\}$
 minimal generating set
 if strictly smaller generator set gives proper submodule.

Free generating set: $\sum m_i r_i = 0$ iff $r_i = 0 \forall i$



Ex. $R = \mathbb{Z}$
 $M = \mathbb{Q}$

\mathbb{Q} is not free $\nexists \mathbb{Z}$
 $\frac{a}{b} \neq \frac{c}{d} \in \mathbb{Q}$, then $bc \frac{a}{b} + (-ad) \frac{c}{d} = 0$, but $bc, ad \neq 0$

Direct product

Λ set
 R ring
 M_λ module for each $\lambda \in \Lambda$

$$M = \prod_{\lambda \in \Lambda} M_\lambda = \text{Mor}(\Lambda, M)$$

$$\bigoplus_{\lambda \in \Lambda} M_\lambda = \{(x, m_\lambda, \dots) \mid \text{only finitely many } m_\lambda \neq 0\}$$

$$\text{Hom}(N, \prod_{\lambda \in \Lambda} M_\lambda) = \prod_{\lambda \in \Lambda} \text{Hom}(N, M_\lambda)$$

$$\text{Hom}(\bigoplus_{\lambda \in \Lambda} M_\lambda, N) = \prod_{\lambda \in \Lambda} \text{Hom}(M_\lambda, N)$$

More about finitely generated modules.

Cayley-Hamilton Theorem.

R ring
 $A = (a_{ij}), a_{ij} \in R$. $n \times n$ -matrix
 I_n identity element
 T variable

$$p_A(A) = \det(T \cdot I_n - A) \\ = T^n + a_1 T^{n-1} + \dots + a_n I_n$$

characteristic polynomial

C-H-Thm: $p_M(A) = 0$

Determinant Trick Thm.

$M = \langle m_1, \dots, m_n \rangle$
 R -module

$\varphi: M \rightarrow M$ endomorphism

$$\varphi(m_i) = \sum_{j=1}^n a_{ij} m_j$$

$$A = (a_{ij})$$

$$\Rightarrow p_A(\varphi) = 0 \text{ in } \text{End}(M)$$

Δ char. pol.

$$\text{cofa}(\Delta) (\Delta X) = 0$$

$$0 = (\text{cofa} \Delta \cdot \Delta) X = \det \Delta \cdot I_n \cdot X$$

$$\Rightarrow \det(\Delta) \cdot X = 0$$

$$\Rightarrow \det(\Delta) \cdot m_j = 0 \quad \forall j$$

$$\Rightarrow p_A(\varphi) = 0$$

Notation: $\delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$

μ_a : multiplication

$$\Delta = (\delta_{ij} \varphi - M a_{ij})$$

$X = (m_j)$ column vector

Proposition

M fin. gen. R
 $\sigma \in R$
 Then $M = \sigma \cdot M \iff \exists a \in R$ s.t. $(1+a)M = 0$

Pf. Assume $\sigma M = M$, $M = \langle m_1, \dots, m_n \rangle$. For $m_i \in M = \sigma \cdot M$

we have $m_i = \sum a_{ij} \cdot m_j$. Let $A = (a_{ij})$, and

$$P_A(T) = T^n + a_1 T^{n-1} + \dots + a_n.$$

Let $a = a_1 + a_2 + \dots + a_n$. Put $\varphi = 1_M$ in

Determinant Trick Thm.

$$\begin{aligned} \Rightarrow P_A(1_M) &= 1_M + a_1 1_M + \dots + a_n 1_M = 1 + a \\ &= (1 + a_1 + \dots + a_n) \cdot 1_M = 0. \end{aligned}$$

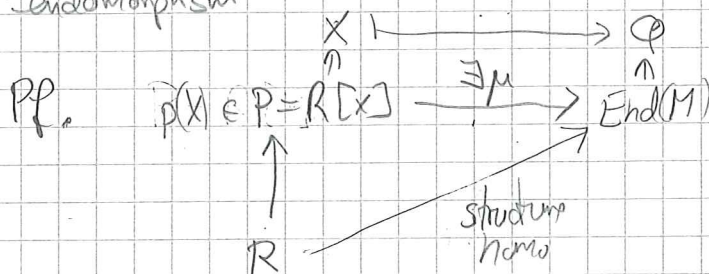
$$\Rightarrow (1+a)M = 0.$$

Conversely, if $\exists a \in R$ s.t. $(1+a)M = 0$,
 then $m = -am \forall m \in M \Rightarrow M \subseteq \sigma \cdot M \subseteq M \Rightarrow M = \sigma \cdot M$.

Corollary.

R ring M fin. gen. R
 Then φ surjective $\Rightarrow \varphi$ isomorphism

$\varphi: M \rightarrow M$
 endomorphism



We have $p(X) \cdot M = p(\varphi) \cdot M$. Let $\alpha = (X)$

φ surjective $\Rightarrow M = \alpha M$

Then $\exists a \in \alpha$ s.t. $(1+a)M = 0$, $a = X \cdot \varphi$

$$\Rightarrow 1 + \varphi \cdot \varphi(\varphi) = 0$$

Consequence: Any n generators v_1, \dots, v_n of the free module R^n form a free basis

Pf $\alpha: R^n \rightarrow R^n \Rightarrow \alpha$ isomorphism
 $e_i \mapsto v_i$
 Surjective

$$\left(\Rightarrow R^m \cong R^n \Rightarrow m = n. \right)$$

Nakayamas Lemma

$\alpha \in R$ ring M fin. gen R $M = \alpha M \Rightarrow M = 0$.

$\mathfrak{m} \subseteq R$

Pf. We have $\exists a \in \mathfrak{m}$ s.t. $(1+a)M = 0$

$$R \xrightarrow{\text{local}} 1+a \xrightarrow{\text{unit}} M = (1+a)^{-1} (1+a)M = 0.$$

Proposition

R ring $N \subseteq M$ R -modules \uparrow M/N fin. gen and $N + \mathfrak{m}M = M \Rightarrow N = M$

$\mathfrak{m} \subseteq R$

2) M fin. gen R . Then $M = \langle m_1, \dots, m_n \rangle$
 $M/\mathfrak{m}M = \langle m_i \dots m_i \rangle$

Pf. 1) $\mathfrak{m} \cdot M/N = M/N$ means $\mathfrak{m}M + N = M + N$ ok

2) Put $N = \langle m_1, \dots, m_n \rangle$. $M \Rightarrow M/N$ fin. gen. Apply (1) to M/N
 then $\langle m_i, m_i \rangle + \mathfrak{m}M = \langle m_i, m_i \rangle$, where $m_i = m_i + \mathfrak{m}$.

Ex $R \supseteq R \supseteq \mathfrak{m}$
 ring

$\gamma = \alpha + \beta$ is an isomorphism.

$\alpha, \beta: M \rightarrow N$
 fin. gen.

Pf. $\forall y \in N \exists x \in M$ s.t. $\alpha(x) = y$ γ iso

α surjective, $\beta(M) \subseteq \mathfrak{m}N$

$$\Rightarrow y = \alpha(x) + \beta(x) - \beta(x) = \gamma(x) - \beta(x) \in \gamma(M) + \mathfrak{m}N \Rightarrow \gamma(M) = N$$