TUESDAY, AUGUST 29, 2017

Definition

A local ring: Exactly one maximal ideal

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

Non-unit criterion:

$$\underset{\text{non-units}}{A \supseteq \mathfrak{n}} \quad \underset{\text{local}}{A} \iff \underset{\text{ideal}}{\mathfrak{n}} \quad \text{(maximal ideal)}$$

Pf. $\underset{\text{all proper ideal}}{\mathfrak{n} \supseteq \mathfrak{a}} \Rightarrow \underset{\text{ideal}}{\mathfrak{n}} \Rightarrow$ only max ideal $\Rightarrow$ local

(Prime avoidance)

1) $\mathfrak{a} \subseteq \underset{\text{ring}}{R} \supseteq \underset{\text{prime ideals}}{\mathfrak{p}_1, \dots, \mathfrak{p}_n}$ s.t. $\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i \Rightarrow \exists i$ s.t. $\mathfrak{a} \subseteq \mathfrak{p}_i$

2) $\underset{\text{ideals}}{\mathfrak{a}_1, \dots, \mathfrak{a}_n} \subseteq R \supseteq \underset{\text{prime}}{\mathfrak{p}}$ s.t. $\bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p} \Rightarrow \exists i$ s.t. $\mathfrak{a}_i \subseteq \mathfrak{p}$

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

$$y = \sum_{i=1}^{n} x_1 \cdots \hat{x}_i \cdots x_n$$

We have $y \in \mathfrak{a}$, and $y \notin \mathfrak{p}_i$

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

$\Rightarrow$ • $x_1 \cdots x_n \in \prod \mathfrak{a}_i \subseteq \prod \mathfrak{a}_i \subseteq \bigcap \mathfrak{a}_i$

• $x_1 \cdots x_n \notin \mathfrak{p}$ (prime)

$\Rightarrow \bigcap \mathfrak{a}_i \not\subseteq \mathfrak{p}$

If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} \subseteq \mathfrak{a}_i$, combined with 2) $\mathfrak{a}_i \subseteq \mathfrak{p}$ gives $\mathfrak{p} = \mathfrak{a}_i$

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

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

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

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

$$\Rightarrow \exists \underset{\text{prime}}{\mathfrak{p}} \supseteq \mathfrak{a} \text{ s.t. } x \notin \mathfrak{p}.$$

($S' = \{\mathfrak{b} \subseteq R \mid \mathfrak{b} \supseteq \mathfrak{a}, \mathfrak{b} \cap S = \emptyset\} \neq \emptyset$ (since $\mathfrak{a} \in S'$), poset and any sequence $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \dots \subseteq$ of nested ideals is majorized by their union $\Rightarrow \exists$ maximal element $\mathfrak{p}$ in S' (by Zorns lemma). Let $xy \in \mathfrak{p}$ and $x, y \notin \mathfrak{p}$. Then $(x)+\mathfrak{p}, (y)+\mathfrak{p} \notin S'$. But $\mathfrak{a} \subset (x)+\mathfrak{p}, (y)+\mathfrak{p}$, so we must have $(x)+\mathfrak{p} \cap S \neq \emptyset$ (and $(y)+\mathfrak{p} \cap S \neq \emptyset$) i.e. $ax+p \in S$ and $by+q \in S$, $p, q \in \mathfrak{p}$. But then

$$S \ni (ax+p)(by+q) = abxy + aqx + bpy + pq \in \mathfrak{p}$$

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

$\Rightarrow$ ~~Now~~ $\Rightarrow x \notin \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p}$ and $\bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p} \subseteq \sqrt{\mathfrak{a}}$

Definition of module

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

Alternative :

$R \longrightarrow End_{\mathbb{Z}}(M)$ (as abelian group)
ring homomorphism

$r \longmapsto \varphi_r$, $\varphi_r(m) = rm$

Faithfull module

$R \to End_R(M)$ injective
$\Updownarrow$
$(0:M) = Ann(M) \subset R$.
$= 0$

Ex. R field ; Module = Vector space

$\mathbb{Z}$: Module = Abelian group

$M \subset R$: Module = Ideal

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

$Hom_R(M,N)$ is itself a R-module

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

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

Quotient module

$M' \hookrightarrow M \longrightarrow M/M'$ as abelian groups

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

UMP for modules

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

$\Rightarrow \exists !$ homomorph. $M/M' \to N$

$$\begin{tikzcd} M/M' \arrow[r, dashed, "\alpha(M')=0 \Rightarrow \exists \bar{\alpha}"] & N \\ M \arrow[u, "\mathcal{H}"] \arrow[ur, "\alpha"'] \arrow[r, phantom, "\circ"] & \end{tikzcd}$$

Cyclic module $\quad M = R\cdot m \quad$ for some $m \in M$

$$\Rightarrow \quad R/_{\mathrm{Ann}(m)} \simeq M$$

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

$f: M \to N \qquad$ Cokernel (f): $\quad \mathrm{coker}(f) := N/_{\mathrm{im}(f)}$

Coimage (f): $\quad \mathrm{coim}(f) := M/_{\mathrm{Ker}(f)}$

$$\begin{tikzcd}
 & & \mathrm{im}(f) \arrow[dr, hook] & \\
\mathrm{Ker}(f) \arrow[r, hook] & M \arrow[ur] \arrow[rr, "f"] \arrow[d] \arrow[rrd] & & N \arrow[d] \\
 & \mathrm{coim} := M/_{\mathrm{ker}(f)} \arrow[rru, dashed] & & N/_{\mathrm{im}(f)} = \mathrm{coker}
\end{tikzcd}$$

Free modules:

$$M = \sum_{(i)} R\cdot m_i \qquad \{m_\lambda\}$$

generators.

minimal generating set if strictly smaller generator set gives proper submodule.

Free generating set: $\sum m_\lambda r_\lambda = 0$ gives $r_\lambda = 0 \; \forall$.

Given $(m_1, \dots, m_r)$

$$R^n \longrightarrow M$$
$$r_1, \dots, r_n \longmapsto \sum r_i m_i$$

Ex. $\quad R = \mathbb{Z} \qquad \mathbb{Q}$ is not free $/\mathbb{Z}$.

$\quad\;\; M = \mathbb{Q}$

$\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, then $bc\frac{a}{b} + (-ad)\cdot\frac{c}{d} = 0$, but $bc, ad \neq 0$

Direct product

Λ set, R ring, M_λ module for each $\lambda \in \Lambda$; $M = \prod_{\lambda\in\Lambda} M_\lambda = Mor(\Lambda, M)$.

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

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

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

More about finitely generated modules.

Cayley-Hamilton Theorem.

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

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

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

Determinant Trick Thm.

$M = \langle m_1, \dots, m_n\rangle$ R-module $\Rightarrow$ $p_A(\varphi) = 0$ in $End(M)$.

$\varphi: M \to M$ endomorphism

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

$A = (a_{ij})$

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

μ_a: multiplication.

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

$X = (m_j)$ column vector

Pf. $\Delta X = 0$ char. pol.

$cofa(\Delta)(\Delta X) = 0$

$0 = (cofa\,\Delta \cdot \Delta) X = det\,\Delta \cdot I_n X$

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

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

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

Proposition

M fin.gen/R, $\mathfrak{a} \subseteq R$. Then $M = \mathfrak{a} \cdot M \iff \exists a \in \mathfrak{a}$ s.t. $(1+a)M = 0$

Pf. Assume $\mathfrak{a}M = M$, $M = \langle m_1, \dots, m_n \rangle$. For $m_i \in M = \mathfrak{a} \cdot M$ we have $m_i = \sum a_{ij} m_j$. 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.

$$\Rightarrow P_A(1_M) = 1_M + a_1 1_M + \dots + a_n 1_M$$

$$= (1 + a_1 + \dots + a_n) \cdot 1_M = 0.$$

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

Conversley, if $\exists a \in \mathfrak{a}$ s.t. $(1+a) M = 0$, then $m = -am$ $\forall m \in M \Rightarrow M \subseteq \mathfrak{a}M \subseteq M \Rightarrow M = \mathfrak{a}M$.

Corollary.

R ring, M fin.gen/R, $\varphi : M \to M$ endomorphism. Then φ surjective $\Rightarrow$ φ isomorphism

Pf.

$$\begin{tikzcd} X \arrow[r, mapsto] & \varphi \\ p(X) \in P = R[X] \arrow[r, "\exists \mu"] & \mathrm{End}(M) \\ R \arrow[u] \arrow[ur, "\text{structure homo}"'] & \end{tikzcd}$$

We have $p(X) \cdot M = p(\varphi) \cdot M$. Let $\mathfrak{a} = (X)$

φ surjective $\Rightarrow M = \mathfrak{a} M$

Then $\exists a \in \mathfrak{a}$ s.t. $(1+a) M = 0$, $a = X \cdot f$

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

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

Pf. $\alpha : R^n \twoheadrightarrow R^n$, $e_i \mapsto v_i$ surjective $\Rightarrow$ α isomorphism

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

Nakayamas Lemma

$\mathfrak{a} \subseteq R$ ring, M fin.gen/R, $\underline{m} \subseteq r(R)$

$M = \underline{m} M \Rightarrow M = 0.$

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

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

Proposition

$\underset{\text{ring.}}{R}$ $\underset{\text{R-modules}}{N \subseteq M.}$

$\underline{m} \subseteq r(R)$

1) $\underset{\text{fin. gen}}{M/N}$ and $N + \underline{m}M = M \Rightarrow N = M$

2) $\underset{\text{fin.gen/R}}{M}$. Then $M = \langle m_1 \dots m_n \rangle$
$\Updownarrow$
$M/_{\underline{m}M} = \langle \bar{m}_1 \dots \bar{m}_n \rangle.$

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

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

Ex $\underset{\text{ring}}{R} \supseteq r(R) \supseteq \underline{m}$

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

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

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

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

$\Rightarrow y = \alpha(x) + \beta(x) - \beta(x)$ $\qquad \Uparrow$

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