Lecture 23: Artinian rings II

Last time: We defined Artinian rings R as rings with DCC

Proposition 1: Let R be an Artinian commutative ring. Then:

(i) Every prime ideal in R is maximal.

(ii) There are only finitely many maximal ideals in R

Property: R Artinian & integral domain $\Rightarrow$ R is a field.

Corollary: Nilradical = Jacobson radical for Artinian rings

Proposition 2: The nilradical ideal $\mathcal{N} \subset R$ (Artinian) is nilpotent, ie $\exists\, n \geq 0$ such that $\mathcal{N}^n = (0)$.

Examples: 1 $\mathbb{K}$ $(\mathcal{N} = (0))$; 2 $\mathbb{K}[x]/(x^n)$. $(\mathcal{N} = (x))$

§1. Geometric interpretation of Artinian Rings.

We let $\boxed{\mathfrak{m}_1, \ldots, \mathfrak{m}_\ell}$ be the maximal ideals (= prime ideals) of R

Note that maximal ideals are always coprime

In the sequel, we will need the following general result:

Lemma 1: Fix A a commutative ring and $\mathfrak{a}, \mathfrak{b} \subset A$ be two coprime ideals. Then $\mathfrak{a}^i$ & $\mathfrak{b}^i$ are coprime $\forall i \geq 1$.

Moreover $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$ (same is true for finite intersections of coprime ideals)

Proof: Since $\mathfrak{a} + \mathfrak{b} = 1$ $\exists\, a \in \mathfrak{a}$ & $b \in \mathfrak{b}$ with $1 = a + b$

$$1 = (a+b)^{2i} = \sum_{j=0}^{2i} \binom{2i}{j} a^{2i-j} b^j$$

So $1 = \underbrace{\left(\sum_{j=0}^{i} \binom{2i}{j} b^j a^{i-j}\right) a^i}_{\in \mathfrak{a}^i} + \underbrace{\left(\sum_{j=1}^{i} \binom{2i}{j+i} a^{i-j} b^j\right) b^i}_{\in \mathfrak{b}^i}$

- $\mathfrak{a}\cdot\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ is always true
- Pick $x \in \mathfrak{a} \cap \mathfrak{b}$ $\quad 1 = a+b \quad$ so $\quad x = \underbrace{a\overset{\in\mathfrak{b}}{x}}_{\in\mathfrak{a}\mathfrak{b}} + \underbrace{\overset{\in\mathfrak{a}}{x}b}_{\in\mathfrak{a}\mathfrak{b}} \in \mathfrak{a}\mathfrak{b}$ $\square$

By Proposition 2, pick n with $\mathcal{N}^n = (0)$. Since $\{m_1^n, \dots, m_\ell^n\}$ are pairwise coprime, we use the Chinese Remainder Theorem to get a surjective map of rings:

$$\varphi : R \longrightarrow R/_{m_1^n} \times \cdots \times R/_{m_\ell^n}$$

$$\mathrm{Ker}\,\varphi = m_1^n \cap \cdots \cap m_\ell^n \underset{\text{Lemma 1}}{=} m_1^n \cdots m_\ell^n \underset{(*)}{\subseteq} \mathcal{N}^n = (0)$$

$(*)$ since $\mathcal{N} = m_1 \cap \cdots \cap m_\ell \underset{\text{Lemma 1}}{=} m_1 \cdots m_\ell$

This implies the following Structure Theorem for Artinian rings:

Theorem: $\quad R \simeq R/_{m_1^n} \times R/_{m_2^n} \times \cdots \times R/_{m_\ell^n}$

R Artinian & Max ideals $= \{m_1, \dots, m_\ell\}$ with n s.t. $\mathcal{N}^n = (0)$.

Here, $R/_{m_j^n}$ is a local ring with unique maximal ideal $\overline{m}_j = \pi(m_j)$ where $\pi : R \twoheadrightarrow R/_{m_j^n}$ is the natural projection.

Proof The isomorphism follows from the discussion above

It remains to show that R/m_j^n is local $\forall 1 \le j \le l$.

Let $q \subsetneq R/m_j^n$ be a maximal ideal, so it's prime

Then q is the image of $\mathfrak{p} = \pi^{-1}(q) \subseteq R$ & $\mathfrak{p}$ is a prime ideal containing m_j^n.

Problem 12 HW7: $m^n \subseteq \mathfrak{p}$, m maximal & $\mathfrak{p}$ prime $\Rightarrow m = \mathfrak{p}$.

We conclude $m_j = \mathfrak{p}$ & so $q = \pi(m_j)$ $\square$

§2 The local case:

Proposition: If R is Artinian and local, then R is Noetherian

Pf/ Let m be the unique maximal ideal of R & write $k = R/m$ for the quotient. We know k is a field.

For each $j \ge 0$: the set m^j/m^{j+1} is a module over k, i.e. a k-vector space. By Lemma 2 below, $\boxed{\dim_k m^j/m^{j+1} < \infty}$.

Pick $\mathfrak{a} \subsetneq R$ & consider $\mathfrak{a}_j = \mathfrak{a} \cap m^j$.

$$\begin{tikzcd} \mathfrak{a}_j \arrow[r, hook] \arrow[rr, bend right, "f"'] & m^j \arrow[r, "\pi"] & m^j/m^{j+1} \end{tikzcd}$$

$$\ker(f) = \mathfrak{a}_j \cap m^{j+1} = \mathfrak{a} \cap m^j \cap m^{j+1} = \mathfrak{a} \cap m^{j+1} = \mathfrak{a}_{j+1}.$$

So $\mathfrak{a}_j/\mathfrak{a}_{j+1}$ is a k-subspace of m^j/m^{j+1}, so finite dimensional

Let $\{\bar{a}_1^{(j)}, \ldots, \bar{a}_{\alpha_j}^{(j)}\}$ be a k-basis for $\mathfrak{a}_j/\mathfrak{a}_{j+1}$, with $a_1^{(j)}, \ldots, a_{\alpha_j}^{(j)} \in \mathfrak{a}_j$.

For each $m \geq 1$, let $\tilde{\mathfrak{a}} \subseteq \mathfrak{a}$ be the ideal of R generated by

$$B := \bigcup_{j \geq 1} \{ a_1^{(j)}, \dots, a_{\alpha_j}^{(j)} \}$$

Since $\mathfrak{m}^n = (0)$ $\therefore$ $\tilde{\mathfrak{a}}$ is finitely generated ($\mathfrak{a}_m = (0)$ $\forall m \geq n$)

Set $\tilde{\mathfrak{a}}_j = \tilde{\mathfrak{a}} \cap \mathfrak{m}^j$ $\forall j = 1, \dots, n$.

<u>Claim</u>: $\tilde{\mathfrak{a}}_j = \mathfrak{a}_j$ $\forall$ $1 \leq j \leq n$

Pf/ By reverse induction of j

- <u>Base case</u>: $j = n$ $\tilde{\mathfrak{a}}_n = \mathfrak{a}_n = (0)$ since $\mathfrak{m}^n = (0)$
- <u>Inductive step</u>: We know $\tilde{\mathfrak{a}}_{j+1} = \mathfrak{a}_{j+1}$ by inductive hyp.

So $\tilde{\mathfrak{a}}_j / \tilde{\mathfrak{a}}_{j+1} \subseteq \mathfrak{a}_j / \mathfrak{a}_{j+1} = k \langle \bar{a}_1^{(j)}, \dots, \bar{a}_{\alpha_j}^{(j)} \rangle = \tilde{\mathfrak{a}}_j / \tilde{\mathfrak{a}}_{j+1}$.

but $a_1^{(j)}, \dots, a_{\alpha_j}^{(j)} \in \mathfrak{a}_j \cap \tilde{\mathfrak{a}} = \tilde{\mathfrak{a}}_j$

So $\dfrac{\tilde{\mathfrak{a}}_j}{\tilde{\mathfrak{a}}_{j+1}} = \mathfrak{a}_j / \mathfrak{a}_{j+1}$ is k-v.s of dim $< \infty$ & $\mathfrak{a}_{j+1} \subseteq \tilde{\mathfrak{a}}_j \subseteq \mathfrak{a}_j$

So given $a \in \mathfrak{a}_j$ $\exists$ $b \in \tilde{\mathfrak{a}}_j$ with $a - b \in \tilde{\mathfrak{a}}_{j+1} \subseteq \tilde{\mathfrak{a}}_j$

$\Rightarrow$ $a \in \tilde{\mathfrak{a}}_j$. We conclude $\tilde{\mathfrak{a}}_j = \mathfrak{a}_j$. $\square$

The claim gives $\underset{\mathfrak{a} \subsetneq R}{\mathfrak{a} = \mathfrak{a} \cap \mathfrak{m}} = \mathfrak{a}_1 = \underset{\tilde{\mathfrak{a}} \subseteq \mathfrak{a} \subsetneq R}{\tilde{\mathfrak{a}}_1 = \tilde{\mathfrak{a}} \cap \mathfrak{m}} = \tilde{\mathfrak{a}}$. So $\mathfrak{a}$ is f.g

So R is Noetherian by construction. $\square$

As a natural consequence of this proposition & the Structure Thm we get

<u>Corollary</u> Artinian $\Rightarrow$ Noetherian

Lemma 2: If (R,m) is Artinian, then $\dim_{R/m} m^j/m^{j+1} < \infty$. $\forall j$.

Pf/ We view $k = R/m = (R/m^{j+1}) / (m/m^{j+1})$ (By 2nd Iso Thm for rings)

Then, subspaces (over k) in m^j/m^{j+1} correspond bijectively to ideals I in R/m^{j+1} with $I \subseteq m^j/m^{j+1}$.

Why? $R \xrightarrow{\pi} R/m^{j+1}$ $I \subset \frac{m^j}{m^{j+1}}$ k-vs is also a R-mod (ideal) So

$$\underbrace{m^{j+1} \subseteq \pi^{-1}(I)}_{=:J} \subset \pi^{-1}(m^j/m^{j+1}) \underset{(*)}{=} m^j + m^{j+1} = m^j \Rightarrow Jm \subseteq m^{j+1}$$

$\hookrightarrow m^{j+1} \subseteq m^j$

meaning $\frac{m}{m^{j+1}}$ annihilates I.

Conversely if $J \subseteq m^j/m^{j+1}$ & $\frac{m}{m^{j+1}} J = (0)$, then J is a k-module.

If $\dim_k m^j/m^{j+1} = \infty$, we can find an infinite strictly descending chain of subspaces, starting with a countable infinite, linear independent set & removing one such vector at a time. This sequence gives an infinite strictly descending chain of ideals in R/m^{j+1} annihilated by m/m^{j+1}.

This cannot happen because R/m^{j+1} is Artinian.

§3. Hensel's Lemma:

The next result, known as Hensel's Lemma, is used to factor any polynomial by working modulo $m, m^2, \ldots\ldots$

The main instance of this is when we work with diophantine equations: we aim to factor over $\mathbb{Z}_{(p)} = \{\frac{a}{b} : p \nmid b\}$ (computing the p-adic expansion of factors) Other applications include solving equations by p-adic approximation.

Hensel's Lemma: Let (R, m) be an Artinian local ring.

Let $f(x) \in R[X]$ and assume we have $g(x), h(x)$ in $R[X]$ s.t.

- $f(x) - g(x)h(x) \in m[x] = mR[x]$
- $g(x)$ & $h(x)$ are coprime modulo m, i.e. $\exists\, a(x), b(x) \in R[x]$ s.t. $ag + bh = 1$ in $(R/m)[x]$

Then, $\exists\, \tilde{g}, \tilde{h} \in R[X]$ st $f(x) = g(x)h(x)$ and $g(x) \equiv \tilde{g}(x)$ & $h(x) \equiv \tilde{h}(x)$ modulo $m[x]$.

Proof: We will build approximations of g & h working modulo m^{ℓ} for each $\ell \geq 1$.

Claim $\exists\, g_\ell, h_\ell \in R[x]$ st $f - g_\ell h_\ell \in m^{\ell}[x]$, $g_\ell - g \in m[x]$ & $h_\ell - h \in m[x]$

Pf/ By induction on ℓ

Base case: $\ell = 1$ Take $g_1 = g$ & $h_1 = h$ (statement's hypothesis)

Inductive Step: Assume we've constructed $\{g_\ell, h_\ell\}$. Let

$$\boxed{c_\ell(x) = f(x) - g_\ell(x)h(x)} \in m^{\ell}[x].$$

Set $\begin{cases} g_{\ell+1} = g_\ell + c_\ell b & \leadsto g_\ell - g_{\ell+1} \in m^{\ell}[x] \subseteq m[x] \\ h_{\ell+1} = h_\ell + c_\ell a & \leadsto h_\ell - h_{\ell+1} \in m^{\ell}[x] \subseteq m[x] \end{cases}$

Then $f(x) - g_{\ell+1}h_{\ell+1} = \underbrace{f(x) - g_\ell h_\ell}_{= c_\ell} - c_\ell(ag_\ell + bh_\ell) + c_\ell^2 ab$

$$= \underbrace{c_\ell\,(1-(\underbrace{ag+bh}_{\in 1+m[x]}))}_{\in m^\ell m[x] = m^{\ell+1}[x]} + \underbrace{c_\ell a\,(\underbrace{g-g_\ell}_{\in m[x]})}_{\in m^{\ell+1}[x]} + \underbrace{c_\ell b\,(\underbrace{h-h_\ell}_{\in m[x]})}_{\in m^{\ell+1}[x]} + c_\ell^2 ab$$

$c_\ell \in m^\ell[x]$, $c_\ell \in m^\ell[x]$, $c_\ell^2 ab \in m^{2\ell}(x) \subseteq m^{\ell+1}(x)$

So $f(x) - g_{\ell+1} h_{\ell+1} \in m^{\ell+1}[x]$ ✓

- $g_{\ell+1} - g = (g_{\ell+1} - g_\ell) + (\underbrace{g_\ell - g}_{\in m(x) \text{ by IH}}) \in m[x]$ ✓

- $h_{\ell+1} - h = (h_{\ell+1} - h_\ell) + (h_\ell - h) \in m[x]$ ✓ $\square$

Using the claim for $\ell = n$ with $m^n = (0)$ we get

- $f - g_n h_n \in m^0[x] \rightsquigarrow f = g_n h_n$
- $g_n - g \in m[x]$ & $h_n - h \in m[x]$

Thus $\tilde{g} = g_n$ & $\tilde{h} = h_n$ satisfy the desired properties. $\square$