IV.E. Nakayama's lemma

This is a basic result in commutative algebra, which exists in many different versions and with many interesting corollaries. We continue to denote by R a commutative ring.

IV.E.1. DEFINITION. The **Jacobson radical** $\mathfrak{J}(R)$ of R is the intersection of all maximal ideals in R.

This is of course zero in rings like $\mathbb{Z}$ and $\mathbb{C}[x,y]$, but that misses the point. In a local ring it is the unique maximal ideal, and we get local rings by localizing rings like $\mathbb{Z}$ and $\mathbb{C}[x,y]$; furthermore, there are "in between" cases with (say) finitely many maximal ideals.

The form in which the next result is most often found is that (iii) holds for $J = \mathfrak{J}(R)$. This following version from **[Hungerford]** includes several common variants.

IV.E.2. NAKAYAMA'S LEMMA. *For an ideal $J \subset R$, the following are equivalent:*
(i) $J \subset \mathfrak{J}(R)$;
(ii) $1 - \jmath \in R^*$ *for all* $\jmath \in J$;
(iii) *if M is a f.g. R-module and $JM = M$, then $M = \{0\}$; and*
(iv) *if M is a f.g. R-module, and N a submodule with $M = JM + N$, then $M = N$.*

PROOF. <u>(i) $\implies$ (ii)</u>: Suppose $1 - \jmath \notin R^*$ for some $\jmath \in J$. Then $1 - \jmath$ belongs to some maximal ideal $\mathfrak{m}$, and obviously $\jmath \in \mathfrak{m}$. So $1 \in \mathfrak{m}$, which is ridiculous.

<u>(ii) $\implies$ (iii)</u>: Assume $M \neq \{0\}$, n is the minimal length of a generating set, and write $M = R\langle \mu_1, \ldots, \mu_n \rangle$; in particular, $\mu_1 \neq 0$. Then $JM = M \implies \mu_1 = \sum_i \jmath_i \mu_i \implies (1 - \jmath_1)\mu_1 = \sum_{i \geq 2} \jmath_i \mu_i \stackrel{\text{(ii)}}{\implies}$

$$\mu_1 = (1 - \jmath_1)^{-1} \textstyle\sum_{i \geq 2} \jmath_i \mu_i = \sum_{i \geq 2} \frac{\jmath_i}{1 - \jmath_i} \mu_i.$$

But then $\mu_2, \ldots, \mu_n$ generate M, a contradiction.[4]

[4]If $n = 1$, the displayed equation says that $\mu_1 = 0$, which is just as much a contradiction.

<u>(iii) $\Longrightarrow$ (iv)</u>: $M = JM + N \implies \frac{M}{N} = J\frac{M}{N}$; clearly $\frac{M}{N}$ is f.g. By (iii), $\frac{M}{N} = \{0\}$ hence $M = N$.

<u>(iv) $\Longrightarrow$ (i)</u>: Let $N := \mathfrak{m} \subset R =: M$ be a maximal ideal. Clearly $\mathfrak{m} \subset JR + \mathfrak{m}$, and if $JR + \mathfrak{m} = R$ then (iv) gives $R = \mathfrak{m}$, a contradiction. So $JR + \mathfrak{m} = \mathfrak{m}$, and $J \subset \mathfrak{m}$. □

It is easiest to get a sense of what this is saying in the local case:

IV.E.3. COROLLARY. *If $\mathcal{R}$ is a local ring with maximal ideal $\mathfrak{m}$, and $\mathcal{M}$ is a finitely generated $\mathcal{R}$-module, then*

$$\mathcal{M} = \mathfrak{m}\mathcal{M} \implies \mathcal{M} = \{0\}.$$

IV.E.4. REMARK. Of course, $\mathcal{M} = \mathfrak{m}\mathcal{M}$ is the same as $\mathcal{M}/\mathfrak{m}\mathcal{M} = \{0\}$: so this is saying that if the *fiber* of the module over $\mathfrak{m}$ is zero, then the whole module is zero. More generally, we can take M to be an R-module, and apply IV.E.3 to the localizations of these at each maximal ideal $\mathfrak{m}$. Recall from IV.A.20 that if all these stalks $M_{\mathfrak{m}}$ vanish, so does M; but now by IV.E.3, if all the *fibers* $M/\mathfrak{m}M$ vanish, then so do the *stalks*, and thus M! *Provided*, of course, that M is finitely generated.

To see how this might be useful, consider now a homomorphism $\theta \colon N' \to N$ of f.g. R-modules. We want to know whether it is surjective, i.e. whether $M := N/\theta(N')$ is zero. We can now reduce this question mod $\mathfrak{m}$ at each maximal ideal: is $M/\mathfrak{m}M$ zero, i.e. is the $k_{\mathfrak{m}}$-linear map $N'/\mathfrak{m}N' \to N/\mathfrak{m}N$ surjective? This replaces the original question by a linear algebra one.

We now revisit Krull's theorem IV.D.21 in the light of Nakayama.

IV.E.5. COROLLARY. *Let $J \subset R$ be an ideal. Then*

$$J \subset \mathfrak{J}(R) \iff \cap_{n\geq 1} J^n M = \{0\} \text{ for all Noetherian } R\text{-modules } M.$$

PROOF. <u>($\Longrightarrow$)</u>: Set $N = \cap J^n M$. By IV.D.21, $JN = N$. Now M Noetherian $\implies N$ f.g. $\implies N = \{0\}$ by IV.E.2((i) $\Longrightarrow$ (iii)).

<u>($\Longleftarrow$)</u>: Given a maximal ideal $\mathfrak{m} \subset R$, set $M := R/\mathfrak{m}$ (i.e. the residue field). As an R module, this is simple, hence Noetherian,

and so by hypothesis $\cap J^n M = \{0\}$. But since it is simple, either $JM = M$ (a contradiction) or $JM = \{0\}$, whence $J \subset \mathfrak{m}$. $\square$

IV.E.6. KRULL INTERSECTION THEOREM (v. 2). *Let R be Noetherian and either local or a domain. Let $\mathfrak{m} \subset R$ be a maximal ideal. Then $\cap_{n\geq 1}\mathfrak{m}^n = \{0\}$.*

PROOF. For the local case: set $J = \mathfrak{m}$ and $M = R$, so that $J^n M = \mathfrak{m}^n$, and apply IV.E.5.

If R is a Noetherian domain, then its localization $R_\mathfrak{m}$ is also Noetherian (use IV.A.8(i)). By the local case, we have $\cap_{n\geq 1}(\mathfrak{m}R_\mathfrak{m})^n = \{0\}$ in $R_\mathfrak{m}$. The map $\phi \colon R \to R_\mathfrak{m}$ from (IV.A.6) sends $\mathfrak{m} \mapsto \mathfrak{m}R_\mathfrak{m}$, hence $\cap_{n\geq 1}\mathfrak{m}^n \mapsto \{0\}$. Since R is a domain, ϕ is injective. $\square$

IV.E.7. EXAMPLE. Let R be the ring of germs of smooth functions at $0 \in \mathbb{R}$. (Take the C^∞ functions on neighborhoods of 0, modulo the equivalence relation: $f \sim g \iff f = g$ on some $(-\epsilon, \epsilon)$.) This is a local ring with unique maximal ideal $\mathfrak{m}$ consisting of the functions vanshing at 0. The intersection $\cap\mathfrak{m}^n$ comprises functions all of whose derivatives vanish at 0. This is not zero, containing for example the germ of the function given by 0 at 0 and e^{-1/x^2} away from 0. In view of IV.E.6, you may regard this both as a proof that this R is non-Noetherian and that the Krull theorem need not hold for non-Noetherian rings.

IV.E.8. REMARK. (i) The *Krull* (or $\mathfrak{m}$-*adic*) *topology* on a Noetherian local ring $(R, \mathfrak{m})$ is generated by the basis of open neighborhoods $r + \mathfrak{m}^n$ with $r \in R$ and $n \in \mathbb{N}$. Given distinct $r_1, r_2 \in R$, by IV.E.6 there exists $k \in \mathbb{N}$ sufficiently large that $r_1 - r_2 \notin \mathfrak{m}^k$. It follows that $(r_1 + \mathfrak{m}^k) \cap (r_2 + \mathfrak{m}^k) = \emptyset$; that is, r_1 and r_2 have non-intersecting open neighborhoods. So Krull's theorem implies that this topology is Hausdorff!

(ii) If R is any commutative ring with maximal ideal $\mathfrak{m}$, the **$\mathfrak{m}$-adic completion** $\hat{R}_\mathfrak{m}$ is the *inverse limit* of

$$\cdots \to R/\mathfrak{m}^n \to \cdots \to R/\mathfrak{m}^2 \to R/\mathfrak{m}.$$

That is, its elements are sequences $(\ldots, a_n, \ldots, a_2, a_1)$ with $a_k \mapsto a_{k-1}$ for each k. This is a local ring (with maximal ideal given by elements with $a_1 = 0$), and the natural map $R \to \hat{R}_{\mathfrak{m}}$ (sending r to its reductions modulo each power of $\mathfrak{m}$) is injective provided $\cap \mathfrak{m}^k = \{0\}$, which happens when R is Noetherian and either local or a domain (by IV.E.6). Evidently $\mathcal{S} := R \backslash \mathfrak{m}$ is sent to units (why?), and so we have embeddings $R \hookrightarrow R_{\mathfrak{m}} \hookrightarrow \hat{R}_{\mathfrak{m}}$.

If $\mathfrak{m} = (\mu)$ is principal, then we can think of the sequences as "power series" $\sum_{k \geq 0} b_k \mu^k$, with $b_k \in k_{\mathfrak{m}} := R/\mathfrak{m}$. So $\hat{\mathbb{Z}}_{(p)}$ recovers what are known as the *p-adic integers*, and we have $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)} \hookrightarrow \hat{\mathbb{Z}}_{(p)}$. Note that $\hat{\mathbb{Z}}_{(p)}$ is much larger than $\mathbb{Z}_{(p)}$: indeed, the former is uncountable, by applying Cantor's diagonal argument to the "power series" in p.

An example where $\mathfrak{m}$ is not principal is $\mathfrak{m} = (x_1, \ldots, x_n)$ in $R = \mathbb{C}[x_1, \ldots, x_n]$. The completion $\hat{R}_{\mathfrak{m}}$ is exactly the power-series ring $\mathbb{C}[[x_1, \ldots, x_n]]$.

Our last application of Nakayama's lemma will be to projective modules over local rings.

IV.E.9. DEFINITION. A module M over a ring R is **projective** if for any diagram of R-module homomorphisms

$$\begin{tikzcd} & M \arrow[dl, dashed, "h"'] \arrow[d, "f"] \\ A \arrow[r, two heads, "g"'] & B \end{tikzcd}$$

there exists an h such that $g \circ h = f$.

IV.E.10. LEMMA. *If M is projective, then any short-exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} M \to 0$ is split, i.e. $B \cong A \oplus M$.*

PROOF. From the diagram

$$\begin{tikzcd} & M \arrow[dl, dashed, "h"'] \arrow[d, "\mathrm{id}_M"] \\ B \arrow[r, two heads, "g"'] & M \end{tikzcd}$$

and IV.E.9, we get h with $g \circ h = \mathrm{id}$. So h is injective, and gives a copy $h(M)$ of M in B. For $b \in B$, write $b = b - h(g(b)) + h(g(b))$, and note that $g\{b - h(g(b))\} = g(b) - g(b) = 0 \implies b - h(g(b)) = f(a)$ for some $a \in A$. If $b = h(m)$ is an element of $f(A) \cap h(M)$, then $g(b) = 0 \implies m = g(h(m)) = 0 \implies b = 0$. So $B = f(A) \oplus h(M)$. $\square$

We will prove the following result only for *finitely generated* projective modules. When R is the coordinate ring of a variety X, these modules correspond to (sections of) vector bundles over X. What the result is saying is that locally, at the stalk level, these bundles are trivial (i.e. constant, not zero).

IV.E.11. THEOREM (Kaplansky, 1958). *If R is a local ring, then every projective R-module is free.*

PROOF IN F.G. CASE. Let M be a f.g. projective R-module, with $\{m_1, \ldots, m_n\} \subset M$ a minimal generating set. Then we have $\pi\colon F \twoheadrightarrow M$, where $F := R^{\oplus n}$ is free, defined by sending $\mathbf{e}_i \mapsto m_i$. Denote R's unique maximal ideal by $\mathfrak{m}$.

Suppose $K := \ker(\pi) \not\subset \mathfrak{m}F$. Then there exists $k \in K \backslash (\mathfrak{m}F \cap K)$, which we can write uniquely as $k = \sum_{i=1}^{n} r_i \mathbf{e}_i$, assuming (wolog) $r_1 \notin \mathfrak{m}$. Since R is local, this puts $r_1 \in R^*$, allowing us to write $\mathbf{e}_1 - r_1^{-1}k = -r_1^{-1}r_2\mathbf{e}_2 - \cdots - r_1^{-1}r_n\mathbf{e}_n$ hence

$$m_1 = \pi(\mathbf{e}_1) = \pi(\mathbf{e}_1 - r_1^{-1}k) = \pi(-\textstyle\sum_{i\geq 2} r_1^{-1}r_i\mathbf{e}_i) = -\textstyle\sum_{i\geq 2} r_1^{-1}r_i m_i$$

(where we used that $\pi(k) = 0$ and π is an R-module homomorphism). But then $m_2, \ldots, m_n$ generate M, contradicting the minimality of n.

So we have $K \subset \mathfrak{m}F$. Applying IV.E.10 to the s.e.s. $K \to F \to M$ yields $F = \tilde{M} \oplus K \subset \tilde{M} \oplus \mathfrak{m}F$, where $\tilde{M} \cong M$. So given $f \in F$, we have $f = \tilde{m} + \sum \mu_i \mathbf{e}_i$ for some $\mu_i \in \mathfrak{m}$ and $\tilde{m} \in \tilde{M}$; and in $F/\tilde{M}$ this becomes $\bar{f} = \sum \mu_i \bar{\mathbf{e}}_i \in \mathfrak{m}(F/\tilde{M})$. Now $F/\tilde{M}$ is f.g. since F is, and $F/\tilde{M} = \mathfrak{m}(F/\tilde{M}) \implies F/\tilde{M} = \{0\}$ by IV.E.3. So $F = \tilde{M} \cong M$, $K = 0$, and M is free. $\square$