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 $J \subseteq R$, the following are equivalent:

(i) $J \subseteq \mathfrak{J}(R)$;

(ii) $1 - j \in R^*$ for all $j \in J$;

(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. (i) $\Rightarrow$ (ii): Suppose $1 - j \not\in R^*$ for some $j \in J$. Then $1 - j$ belongs to some maximal ideal $m$, and obviously $j \in m$. So $1 \in m$, which is ridiculous.

(ii) $\Rightarrow$ (iii): Assume $M \neq \{0\}$, $n$ is the minimal length of a generating set, and write $M = R(\mu_1, \ldots, \mu_n)$; in particular, $\mu_1 \neq 0$. Then $JM = M$ $\Rightarrow$ $\mu_1 = \sum i \cdot j_i \mu_i \Rightarrow (1 - j_1) \mu_1 = \sum_{i \geq 2} j_i \mu_i$ $\overset{(ii)}{\Rightarrow}$

$$\mu_1 = (1 - j_1)^{-1} \sum_{i \geq 2} j_i \mu_i = \sum_{i \geq 2} \frac{\mu_i}{1 - j_i}.$$

But then $\mu_2, \ldots, \mu_n$ generate $M$, a contradiction.\footnote{If $n = 1$, the displayed equation says that $\mu_1 = 0$, which is just as much a contradiction.}
(iii) $\implies$ (iv): $M = JM + N \implies \frac{M}{N} = J \frac{M}{N}$; clearly $\frac{M}{N} = \{0\}$ hence $M = N$.

(iv) $\implies$ (i): Let $N := m \subset R =: M$ be a maximal ideal. Clearly $m \subset JR + m$, and if $JR + m = R$ then (iv) gives $R = m$, a contradiction. So $JR + m = m$, and $J \subset m$. □

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

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

$$M = mM \implies M = \{0\}.$$ 

IV.E.4. REMARK. Of course, $M = mM$ is the same as $M/mM = \{0\}$: so this is saying that if the fiber of the module over $m$ 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 $m$. Recall from IV.A.20 that if all these stalks $M_m$ vanish, so does $M$; but now by IV.E.3, if all the fibers $M/mM$ 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 $\theta : N' \to N$ 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 $m$ at each maximal ideal: is $M/mM$ zero, i.e. is the $k_m$-linear map $N'/mN' \to N/mN$ 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. $(\implies)$: 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) $\implies$ (iii)).

$(\impliedby)$: Given a maximal ideal $m \subset R$, set $M := R/m$ (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 $J \subset m$. □

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

Proof. For the local case: set $J = m$ and $M = R$, so that $J^n M = m^n$, and apply IV.E.5.

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

IV.E.7. Example. Let $R$ be the ring of germs of smooth functions at $0 \in \mathbb{R}$. (Take the $C^\infty$ 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 $m$ consisting of the functions vanishing at $0$. The intersection $\cap m^n$ 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 $m$-adic) topology on a Noetherian local ring $(R, m)$ is generated by the basis of open neighborhoods $r + m^n$ 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 $r_1 - r_2 \notin m^k$. It follows that $(r_1 + m^k) \cap (r_2 + m^k) = \emptyset$; 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 $m$, the $m$-adic completion $\hat{R}_m$ is the inverse limit of

$$
\cdots \to R/m^n \to \cdots \to R/m^2 \to R/m.
$$
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 \(R \to \hat{R}_m\) (sending \(r\) to its reductions modulo each power of \(m\)) is injective provided \(\cap m^k = \{0\}\), which happens when \(R\) is Noetherian and either local or a domain (by IV.E.6). Evidently \(S := R \setminus m\) is sent to units (why?), and so we have embeddings \(R \hookrightarrow R_m \hookrightarrow \hat{R}_m\).

If \(m = (\mu)\) is principal, then we can think of the sequences as “power series” \(\sum_{k \geq 0} b_k \mu^k\), with \(b_k \in k_m := R/m\). So \(\hat{Z}_{(p)}\) recovers what are known as the \(p\)-adic integers, and we have \(Z \hookrightarrow \mathbb{Z}_{(p)} \hookrightarrow \hat{Z}_{(p)}\). Note that \(\hat{Z}_{(p)}\) 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 \(m\) is not principal is \(m = (x_1, \ldots, x_n)\) in \(R = \mathbb{C}[x_1, \ldots, x_n]\). The completion \(\hat{R}_m\) 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

\[
\begin{array}{ccc}
A & \xrightarrow{g} & B \\
\downarrow{h} & & \downarrow{f} \\
M & & \\
\end{array}
\]

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

**IV.E.10. Lemma.** If \(M\) is projective, then any short-exact sequence

\[0 \to A \to B \xrightarrow{g} M \to 0\]

is split, i.e. \(B \cong A \oplus M\).
PROOF. From the diagram

\[
\begin{array}{c}
\text{M} \\
\downarrow \text{id}_M \\
\text{B} \xrightarrow{g} \text{M}
\end{array}
\]

and IV.E.9, we get \( h \) with \( g \circ h = \text{id} \). 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 \( \pi : F \to M \), where \( F := R^\oplus n \) is free, defined by sending \( e_i \mapsto m_i \). Denote \( R \)'s unique maximal ideal by \( m \).

Suppose \( K := \ker(\pi) \not\subset mF \). Then there exists \( k \in K \setminus (mF \cap K) \), which we can write uniquely as \( k = \sum_{i=1}^n r_i e_i \), assuming (wolog) \( r_1 \not\in m \). Since \( R \) is local, this puts \( r_1 \in R^* \), allowing us to write \( e_1 - r_1^{-1}k = -r_1^{-1}r_2 e_2 - \cdots - r_1^{-1}r_n e_n \) hence

\[
m_1 = \pi(e_1) = \pi(e_1 - r_1^{-1}k) = \pi(-\sum_{i=2} r_1^{-1}r_i e_i) = -\sum_{i=2} r_1^{-1}r_i m_i
\]

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

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