MA4J8 Commutative algebra II

Week 3 – Completion and the Artin–Rees lemma

The material here mostly comes from [A&M, Chapter 10] or [Matsumura, Section 8].

3.1 Introductory discussion

The idea of *completion* is to work with formal power series in place of polynomials. For example, $k[\![x_1, \dots, x_n]\!]$ as a substitute for $k[x_1, \dots, x_n]$ or p-adics $\mathbb{Z}_p$ in place of the subring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$. The word "formal" reflects that we allow all infinite power series, ignoring convergence – this is the same idea as replacing a differentiable function by its Taylor series to all orders. These formal rings are bigger (usually uncountably so), but much simpler in structure. Any nonsingular point $P \in X$ of any algebraic variety or complex analytic space (independently of X, or $P \in X$) has a small neighbourhood isomorphic to a ball around $0 \in \mathbb{C}^n$, and formal functions on it make up the completed ring $\mathbb{C}[\![x_1, \dots, x_n]\!]$. The same idea applies to the formal neighbourhood of a point on a singular variety. Completion is thus a drastic form of localisation.

As an algebraic process, completion passes from a filtration such as the I-adic filtration (that is, the descending chain of submodules $M \supset IM \supset \dots \supset I^n M \supset \dots$) to the *inverse limit*

$$\varprojlim M/I^n M \quad \text{also written} \quad \operatorname{proj\,lim} M/I^n M. \tag{3.1}$$

(In LaTeX, the first is `\varprojlim`, the second is `\projlim`, for *projective limit*.) I run through the construction below. For now, I want to discuss the finished product and the advantages of working with it.

Definition 3.1 (first attempt) Let A be a ring and I an ideal. We say that A is *I-adically complete* to mean that

$$A = \varprojlim_n A/I^n. \tag{3.2}$$

This means

(I) an element $f \in A$ is uniquely determined by its class in A/I^n for every n; in other words, $\bigcap_n I^n = 0$.

(II) If $\{f_n \in A/I^n\}_{n\in\mathbb{N}}$ is a *compatible sequence* of elements mod I^n then there is $f \in A$ that maps to f_n for every n.

Here compatible means that for $m > n$, the element $f_m \in A/I^m$ reduces modulo I^n to $f_n \in A/I^n$. An equivalent statement of (II) is as a sequence $\{f_n\}$ of elements of A with the formal Cauchy sequence property:

> for every $N > 0$, there exists n_0 such that
> for all $n, m \geq n_0$ the difference $f_n - f_m \in I^N$.

In overall logic, this puts I-adic completion on a similar footing to completion in a metric space.

The real motivation for completion is to solve problems in $A[\![t]\!]$ using term-by-term calculations. Thus for example, if a_0 is invertible in A, you can find the inverse of $a_0 + a_1 t + \cdots$ by calculating successive coefficients. Or if a_0 is a perfect square in A (and the $n!$ are invertible), then you can take the square root of $a_0 + a_1 t + \cdots$ using the binomial theorem and term-by-term approximation.

3.2 Application: Hensel's Lemma

The highpoint is Hensel's Lemma: under appropriate conditions, if you can solve a polynomial equations modulo m (so over the residue field $k = A/m$), you can solve it over A.

Theorem 3.2 (Hensel's lemma) *Let (A, m, k) be a local ring, and suppose that A is m-adically complete.*

Let $F(x) \in A[x]$ be a monic polynomial, and set $\overline{F} = f \in k[x]$. (That is, reduce the coefficients of $F \in A[x]$ modulo m.) Suppose f factors as $f = gh$ with $g, h \in k[x]$ monic and coprime.

Then F has a factorisation $F = GH$ where $G, H \in A[x]$ are still monic, and satisfy

$$\overline{G} = g \quad \text{and} \quad \overline{H} = h. \tag{3.3}$$

Applying this with a linear factor $g(x) = x - r$ of $\overline{F}$ gives the corollary that if the reduction $f(x) \in k[x]$ of $\overline{F}(x) \in A[x]$ has a simple root $r \in k$, then $F(x) \in A[x]$ has a root in A that reduces to r mod m. Here *simple root* means a root of $f(x) \in k[x]$ such that $x - r$ is coprime to $f(x)/(x - r)$, or equivalently, the derivative $f'(x) \neq 0$.

For example, if a polynomial $f \in \mathbb{Z}[x]$ has a simple root r when viewed as a congruence modulo p, this r lifts to a root in the ring $\mathbb{Z}_p$ of p-adic integers.[1] This version of Hensel's lemma is popular with number theorists.

[1] Do a few of the exercises, which are quite fun.

Preliminary step in proof Write $\deg g = n$ and $\deg h = m$. Then g, h coprime in $k[x]$ means I can choose polynomials a, b with

$$\deg a \le m-1 \text{ and } \deg b \le n-1 \quad \text{such that} \quad ag + bh = 1. \tag{3.4}$$

You know how to prove this by repeated division with remainder (the Euclidean algorithm). A direct alternative argument: polynomials of degree $\le n+m-1$ form a vector space of dimension $n+m$ over k, and

$$(1, x, \dots, x^{m-1})g, \quad (1, x, \dots, x^{n-1})h \tag{3.5}$$

are $n+m$ linearly independent elements in it: in fact, since $k[x]$ is a UFD, a relation $\alpha g + \beta h = 0$ would give a common factor $c = \frac{g}{\beta} = -\frac{j}{\alpha}$ between them. Hence they form a basis, and 1 is a linear combination of g, h.

The induction step Starting from $f = gh$, choose $G_1, H_1 \in A[x]$ that are monic of the same degree as $g, h \in k[x]$ and reduce to them modulo m. Reducing mod m gives

$$F - G_1H_1 \in mA[x], \quad \text{that is,} \quad F - G_1H_1 = \sum m_i U_i \tag{3.6}$$

with $m_i \in m$, and $U_i \in k[x]$ polynomials with $\deg U_i < \deg F$.

I show how to cancel each U_i mod m, modifying G_1, H_1 to G_2, H_2 by adding corrections in m, to achieve

$$F - G_2H_2 \in m^2A[x]. \tag{3.7}$$

This is elementary algebra in $k[x]$: for each i, write $u_i \in k[x]$ for the reduction of U_i mod m, and use the a, b with $ag + bh = 1$ provided by (3.4) to obtain

$$gau_i + hbu_i = u_i. \tag{3.8}$$

Division with remainder gives $au_i = hq + v_i$, with quotient q and remainder v_i of degree $< \deg h$. I then rewrite (3.8) as

$$\begin{gathered} g(v_i + hq) + h(w_i - gq) = u_i \quad \text{where } w_i = bu_i - gq. \\ \text{so that } gv_i + hw_i = u_i. \end{gathered} \tag{3.9}$$

Here u_i and gv_i both have degree $< \deg f$, so that also $\deg hw_i < \deg f$.

Now choose lifts $V_i, W_i \in A[x]$ of the v_i, w_i of (3.9), of the same degrees, and modify G_1, H_1 by setting:

$$G_2 = G_1 + \sum m_i W_i \quad \text{and} \quad H_2 = H_1 + \sum m_i V_i \tag{3.10}$$

using the same coefficients m_i as in (3.6). Comparing with (3.6) gives

$$F - G_2H_2 = F - G_1H_1 - \sum m_i(G_1V_1 + H_1W_1) - m_i^2V_1W_1 \in m^2A[x]. \quad (3.11)$$

Each term of the sum subtracts off a term that cancels the m_iU_i of (3.6) modulo m^2 by (3.9), and the final term m_i^2 is in $m^2A[x]$.

The inductive step from G_n, H_n satisfying $F - G_nF_n \in m^nA[x]$ to G_{n+1}, H_{n+1} repeats the above argument verbatim.

Each step only modifies G_n and H_n by terms in $m^nA[x]$, so that both sequences are Cauchy sequences for the m-adic topology. Q.E.D.

3.3 General theory of completion

I introduced completion in simple-minded terms above, and described Hensel's lemma as a major consequence. Now I treat it more formally.

A *directed set* Λ is a partially ordered set so that any two $\lambda, \mu \in \Lambda$ have a bound $\nu \in \Lambda$, that is, $\lambda, \mu \leq \nu$.

Let A be a ring and M an A-module. The starting point is a set $\{M_\lambda\}_{\lambda\in\Lambda}$ of submodules of M indexed by a directed set Λ, with $M_\mu < M_\lambda$ for every $\mu > \lambda$. (Finer and finer as μ gets bigger, so that $M/M_\mu \twoheadrightarrow M/M_\lambda$.)

The case $\Lambda = \mathbb{N}$ would be perfectly adequate for most of our needs in this chapter:[2] the main case in practice is $\{I^nM\}$ for $n \in \mathbb{N}$ and $I^m \subset I^n$ or $I^mM \subset I^nM$ if $m > n$, so that $M/I^mM \twoheadrightarrow M/I^nM$.

Lemma 3.3 *(1) There is a topology on M (the* linear topology *corresponding to $\{M_\lambda\}$) determined by*

- *(a) the $\{M_\lambda\}$ form a basis for the neighbourhoods of 0, and*
- *(b) the module operations are continuous.*

(2) If we give the quotients M/M_λ the discrete topology, the quotient maps $M \to M/M_\lambda$ are continuous.

(3) The topology is separated (Hausdorff) if and only if the intersection of the M_λ is zero: $\bigcap_{\lambda\in\Lambda} M_\lambda = 0$.

[2] The more general idea of directed set comes into play for example in the filtration of $\mathbb{Z}$ by ideals (n), with the integers $n = \prod p_i^{a_i}$ ordered alphanumerically by the exponents a_i. The inverse limit $\varprojlim Z/n$ taken over $\mathbb{Z}/m \twoheadrightarrow \mathbb{Z}/n$ for $n \mid m$ is the profinite completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$. This is the direct product $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ of the p-adic integers $\mathbb{Z}_p$ taken over all p. Compare the general philosophical discussion of 3.4.

Proof (1) The "directed" property of Λ gives that the intersection $M_\lambda \cap M_\mu$ contains M_ν, so is still a neighbourhood of 0. Requiring addition by $x \in M$ to be continuous ensures that every $x \in M$ has a basis of neighbourhoods given by the cosets $\{x + M_\lambda\}$.

(2) For any of the quotient maps $M \to M/M_\lambda$, the inverse image of any subset of the quotient is a union of cosets $x + M_\lambda$, so open.

(3) The topology separates $x, y \in M$ if and only if there exists M_λ not containing $x - y$. $\square$

Construction of completion The $\{M_\lambda\}$ correspond to the inverse system

$$M/M_\mu \to M/M_\lambda \quad \text{that takes} \quad x \bmod M_\mu \text{ to } x \bmod M_\lambda \text{ for } \mu > \lambda. \tag{3.12}$$

The *completion* of M w.r.t. the topology $\{M_\lambda\}$ is defined as the inverse limit $\widehat{M} = \varprojlim M/M_\lambda$. This consists of compatible sequences of elements

$$\{x_\lambda \in M/M_\lambda\}_{\lambda\in\Lambda} \quad \text{such that } x_\mu \mapsto x_\lambda \text{ for every } \mu > \lambda. \tag{3.13}$$

There is a homomorphism $M \to \widehat{M}$ that takes $x \in M$ to the constant sequence $x \bmod M_\lambda$ for all λ. This has kernel the intersection $\bigcap_{\lambda\in\Lambda} M_\lambda$. In any argument, if we assume $\bigcap M_\lambda = 0$, we can work with M as a submodule $M \subset \widehat{M}$. Otherwise, we have to divide M by the kernel $\bigcap M_\lambda$ to get its image in $\widehat{M}$.

By construction, $\widehat{M}$ has a surjective homomorphism to each M/M_λ. The kernel of $\widehat{M} \to M/M_\lambda$ is the completion $(M_\lambda)\widehat{\ }$ of the submodule $M_\lambda \subset M$ w.r.t. to the subspace topology. These kernels in turn induces a topology on $\widehat{M}$ with $\widehat{M}/(M_\lambda)\widehat{\ } = M/M_\lambda$. The inverse limit of this sequence of quotients is of course $\widehat{M}$ itself, which shows that $\widehat{M}$ is complete w.r.t. its induced topology.

The particular case $M = A$ starts from a filtration of A by ideals I_λ and leads to the completion $\widehat{A} = \varprojlim A/I_\lambda$, which is a ring having a surjective map $\widehat{A} \to A/I_\lambda$ to each of the quotient rings A/I_λ.

3.4 Rambling philosophy

This type of completion in terms of inverse limit appears in all areas of math. For example, consider all the rational roots of unity in $\mathbb{C}^\times$. This is the union (= direct limit $\operatorname{inj\,lim}$ or $\varinjlim$) of the $\boldsymbol{\mu}_n$ (the cyclic group of nth roots of 1, generated by $\exp\frac{2\pi i}{n}$) with inclusions $\boldsymbol{\mu}_n \hookrightarrow \boldsymbol{\mu}_{mn}$: the roots of

$z^{mn} = 1$ include the roots of $z^n = 1$ as a subgroup. Since the $\boldsymbol{\mu}_n$ form a direct system, their character groups

$$\mathbb{Z}/n = \mathrm{Hom}(\boldsymbol{\mu}_n, \mathbb{C}^\times) \tag{3.14}$$

form an inverse system $\mathbb{Z}/nm \to \mathbb{Z}/n$ (the homomorphisms take an integer x mod nm to mx mod n), whose inverse limit $\varprojlim \mathbb{Z}/n = \widehat{Z}$ is the *profinite completion* of $\mathbb{Z}$. This is an uncountable group, equal to the direct product over all p of the p-adic integers $\mathbb{Z}_p$.

You know that the real line $\mathbb{R}$ is the universal cover of the unit circle, with $\mathbb{R} \to S^1 \subset \mathbb{C}^\times$ given by $\exp(2\pi i\theta)$, having the kernel $\mathbb{Z}^+ = \pi_1 S^1$. The exponential function is not algebraic. But in algebra I can define the usual n-fold cover $z \mapsto z^n$ as a map $\mathbb{C}^\times \to \mathbb{C}^\times$ or $S^1 \to S^1$, with the advantage that these are algebraic varieties and morphisms, and correspond to the inverse system $\mathbb{C}^\times/\boldsymbol{\mu}_{mn} \to \mathbb{C}^\times/\boldsymbol{\mu}_n$ for all n.

This idea replaces the exponential cover $\mathbb{C}^+ \to \mathbb{C}^\times$ or $\mathbb{R}^+ \to S^1 \subset \mathbb{C}^\times$ familiar in analysis or topology by the algebraic inverse limit $\varprojlim \mathbb{C}^\times/\mu_n$ which is "much bigger". For example, the inverse image of the identity $1 \in \mathbb{C}$ (corresponding to $0 \in \mathbb{R}$) is uncountable: it contains the profinite completion of the $\boldsymbol{\mu}_n$, a group that is isomorphic to $\widehat{Z}$ (the argument depend on the axiom of choice), but with a nontrivial structure of Galois module ("Tate module").

As you know, a finite Galois field extension $K \subset L$ has a finite Galois group $\mathrm{Gal}(L/K)$. Now an infinite Galois extension $K \subset L$ is the union (= direct limit) of normal finite subfields L_i: in fact each individual element $x \in L$ is algebraic, so belongs to a finite extension, and to the corresponding normal subfield (the splitting field of the minimal polynomial of x). The Galois group $\mathrm{Gal}(L/K)$ takes each finite normal subfields L_i to itself, so has a surjective map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L_i/K)$ to the finite Galois group of the extension L_i, and this makes $\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(L_i/K)$, which is therefore a profinite group: Everything to do with the group is determined by its finite quotients, but these get bigger and bigger, and there are infinitely many of them – the inverse limit is uncountable, because an element of it make a choice of element of each of the infinitely many finite groups $\mathrm{Gal}(L_i/K)$.

The group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a central object of study in algebraic number theory. For example, Wiles' 1994 proof of Fermat's Last Theorem depends on work on the representation theory of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in particular Serre's conjecture that its algebraic representations are "modular". (The progress since Wiles' work has only solved a small fraction of this conjecture.)

3.5 Exactness properties of completion

The next issue is the following question on exactness: suppose

$$0 \to N \hookrightarrow M \twoheadrightarrow M/N \to 0 \tag{3.15}$$

is a short exact sequence (s.e.s.) of A-modules. This means $N \subset M$ with quotient module M/N. Suppose we take the completion of $N, M, M/N$ (with respect to some topology specified later). Under what circumstances can we prove that

$$0 \to \widehat{N} \hookrightarrow \widehat{M} \twoheadrightarrow (M/N)\widehat{\ } \to 0 \tag{3.16}$$

is again a short exact sequence?

Let me give a formal argument first, and understand what exactly it proves later. We know the Snake Lemma: for a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & P & \to & Q & \to & R & \to & 0 \\ & & c_P\downarrow & & c_Q\downarrow & & c_R\downarrow & & \\ 0 & \to & P' & \to & Q' & \to & R' & \to & 0 \end{array} \tag{3.17}$$

with the two horizontal rows short exact sequence, the kernels and cokernels of the down maps give a long exact sequence

$$\begin{aligned} 0 \to \ker c_P \to \ker c_Q \to \ker c_R \xrightarrow{\delta} \\ \to \operatorname{coker} c_P \to \operatorname{coker} c_Q \to \operatorname{coker} c_R \to 0. \end{aligned} \tag{3.18}$$

For this you have to think through how the boundary map

$$\delta\colon \ker c_R \to \operatorname{coker} c_P \tag{3.19}$$

is defined: lift an element of $\ker c_R \subset R$ to Q anyhow, map it down by c_Q to an element of Q' that goes to $0 \in R'$, so belongs to P', then check the result is independent of the choice, and that the resulting sequence is exact.

The argument of [A&M] applies this to an exact sequence of inverse systems. Define an inverse system to be a system of A-modules P_i with homomorphisms $\pi_{i+1}\colon P_{i+1} \to P_i$, initially with no further assumptions. Its inverse limit $\widehat{P} = \varprojlim P_i$ is defined as the set of compatible sequences

$$\{x_i \in P_i\} \quad \text{with} \quad \pi_{i+1}(x_{i+1}) = x_i \quad \text{for every } i. \tag{3.20}$$

Fact By definition, the inverse limit $\widehat{P} = \varprojlim P_i$ is the set of compatible sequences of elements of P_i, which is the same thing as the kernel of the homomorphism

$$c_P \colon \prod_i P_i \to \prod_i P_i \tag{3.21}$$

of direct products, where c_P takes

$$\text{a sequence } \{x_i\} \ \mapsto \ \text{new sequence } \{\pi_{i+1}(x_{i+1}) - x_i\}. \tag{3.22}$$

To unwrap this, at the end of the sequence,

$$\text{the image of } \{\dots, x_2, x_1\} \text{ is } \{\dots, \pi(x_3) - x_2, \pi(x_2) - x_1\}. \tag{3.23}$$

Taking $\ker c_P$ imposes on the sequence $\{x_i\}$ the conditions that $\pi(x_2) = x_1$, then $\pi(x_{i+1}) = x_i$ for each i, which means exactly that the sequence is compatible.

Note this refers specifically to the *direct product* of the P_i: any elements x_i are allowed at each i (including infinitely many different choices), as opposed to the usual *direct sum* of algebra, that assumes only finitely many x_i are nonzero.

A homomorphism $P \to Q$ between inverse systems P and Q is a system of homomorphisms $f_i \colon P_i \to Q_i$ for each i that form commutative squares

$$\begin{array}{ccc} P_{i+1} & \to & Q_{i+i} \\ \downarrow & & \downarrow \\ P_i & \to & Q_i \end{array} \tag{3.24}$$

with the down maps π_i. It is clear that this induces a homomorphism $\widehat{P} \to \widehat{Q}$ of the respective inverse limits.

A short exact sequence of inverse systems $0 \to P \to Q \to R \to 0$ is given by a pair of homomorphisms $f \colon P \hookrightarrow Q$ and $g \colon Q \twoheadrightarrow R$ of inverse systems such that for each i the homomorphisms f_i and g_i give short exact sequences

$$0 \to P_i \to Q_i \to R_i \to 0. \tag{3.25}$$

This means of course simply that $f_i \colon P_i \hookrightarrow Q_i$ is injective, and g_i is the corresponding quotient homomorphism $g_i \colon Q_i \twoheadrightarrow R_i = Q_i / f_i(P_i)$. The fact just discussed, together with the snake lemma implies the following result:

Proposition 3.4 (Exactness I) *(1) A s.e.s. of inverse systems*

$$0 \to P \to Q \to R \to 0 \tag{3.26}$$

induces an exact sequence

$$0 \to \widehat{P} \to \widehat{Q} \to \widehat{R} \tag{3.27}$$

between their completions.

(2) If moreover the morphisms $\pi_{i+1}\colon P_{i+1} \to P_i$ in the inverse system P are all surjective, then

$$0 \to \widehat{P} \to \widehat{Q} \to \widehat{R} \to 0 \tag{3.28}$$

is again a short exact sequence.

If you haven't seen this kind of thing before, you should note the counter-intuitive feature that establishing something about the end of the sequence $\widehat{Q} \to \widehat{R}$ requires a surjectivity assumption on the P at the start. This offers a glimpse of the world of homological algebra.

Proof (1) comes directly from the snake lemma. For (2), we just need to deduce that c_P is surjective from the assumption that all $\pi_{i+1}\colon P_{i+1} \to P_i$ are surjective. That is, given a sequence $\{a_i \in P_i\}$, we require to find a sequence of elements $\{x_i \in P_i\}$ with $c_P(x_i) = a_i$.

This is straightforward given the surjectivity of all the π_i. In fact, choose $x_1 = 0$, then $x_2 \in P_2$ with $\pi_2(x_2) = a_1$. At each successive step, we have the target $a_i \in P_i$, and the current choice of $x_i \in P_i$ (that covers a_{i-1}). So choose

$$x_{i+1} \in P_{i+1} \quad \text{such that} \quad \pi_{i+1}(x_{i+1}) = a_i + x_i. \tag{3.29}$$

Then, of course, c_P applied to the sequence $\ldots, x_{i+1}, x_i, \ldots, x_1$ has the ith entry $\pi_{i+1}(x_{i+1}) - x_i = a_i$. This constructs by induction a sequence $\{x_i \in P_i\}$ such that $c_p(x_i) = a_i$. Q.E.D.

3.6 The Artin–Rees lemma

Compare [Matsumura, p. 59].

There is still a gap in applying the Exactness Proposition 3.4 to I-adic completions: the assumptions of the Proposition is that we have three inverse systems P, Q, R with short exact sequences $0 \to P_i \to Q_i \to R_i \to 0$ for each i. Unfortunately however, what we have in applications is not quite this. We start from a submodule,

$$N \subset M \quad \text{and the quotient} \quad M/N, \tag{3.30}$$

take the I-adic filtrations of the three modulse

$$I^n N, \quad I^n M \quad \text{and} \quad I^n(M/N), \tag{3.31}$$

and the inverse systems corresponding to the quotients. It is not true that these filtrations form short exact sequences for each n.

The Artin–Rees lemma bridges this gap: under the standard finiteness assumptions of commutative algebra, it gives a compatibility between the I-adic filtration $\{I^n N\}$ of the submodule N and the restriction to N of the I-adic filtration $\{I^n M\}$ of the module M.

Theorem 3.5 (Artin–Rees lemma) *Assume A is Noetherian and I an ideal of A. Let M be a finite module and $N \subset M$ a submodule.*

Then there exists $c > 0$ such that

$$I^n M \cap N = I^{n-c}(I^c M \cap N) \quad \textit{for every } n > c. \tag{3.32}$$

Discussion The left-hand side defines the subspace topology of the I-adic topology of M restricted to N. The right-hand side is the I-adic topology on a submodule of N. In particular the subspace topology is itself the I-adic topology on some module.

Set-up for the proof Write $I = (a_1, \dots, a_r)$ for generators. Then I^n is of course generated as A-module by the monomials

$$S^n(a_1, \dots, a_r) = \{a_1^n, a_1^{n-1}a_2, \dots, a_r^n\}. \tag{3.33}$$

Exercise: It will be useful for you to know that there are $\binom{n-1+r}{n}$ of these.

We distinguish the monomials in I^n and their coefficients by introducing the bigger A-algebra $B = A[x_1, \dots, x_r]$ with the A-algebra homomorphism $B \to A$ taking $x_i \mapsto a_i$.

Write $m_1, \dots, m_s \in M$ for generators, giving a surjective A-module homomorphism $A^s \twoheadrightarrow M$. Extend this to $\pi\colon B^s \to M$ that does

$$\{f_j(x_1, \dots, x_r)\} \in B^s \mapsto \sum_{j=1}^{s} f_j(a_1, \dots, a_r) m_j \in M. \tag{3.34}$$

Now we are ready to start on the proof.

Proof of Theorem 3.5 The inclusion $\supset$ is clear.

The image of an s-tuple $\{f_j\} \in B^s$ is in M, and it is in $I^n M$ if all the f_j belong to $(x_1, \ldots, x_r)^n$, that is, have all terms of degree $\geq n$ in the x_i.

Imposing in addition the condition that $\pi(\{f_j\}) \in N$, we define the following B-submodule of B^s:

$$J_n = \left\{ \{f_1, \ldots, f_s\} \in B^s \;\middle|\; \begin{array}{l} \text{each } f_j \in B \text{ is homogeneous of} \\ \text{degree } = n, \text{ and } \sum f_j(a) m_j \in N \end{array} \right\}. \tag{3.35}$$

Set $C = \sum_{n \geq 0} J_n$ for the B-submodule of B^s generated by all the J_n. Since B is Noetherian, this is generated by finitely many s-tuples

$$C = \sum B u_j, \quad \text{with each } u_j = (u_{j_1}, \ldots, u_{j_s}) \in J_{d_j}. \tag{3.36}$$

We set $c = \max\{d_j\}$.

An element $y \in I^n M \cap N$ is a sum $y = \sum f_i(a) m_i$ with s-tuple of coefficients in J_n, so that

$$(f_1, \ldots, f_s) = \sum p_j(x_1, \ldots, x_r) u_j \quad \text{for some } p_j \in B. \tag{3.37}$$

By definition of J_n, each term on the left is homogeneous of degree n in $(x_1, \ldots, x_r)$. Therefore all terms on the r-hs. of homogeneous degree $\neq n$ must all cancel out. Since the u_j consist of terms of degree d_j, only polynomials p_j that are homogeneous of degree $n - d_j$ contribute to the sum.

Thus when $n \geq c = \max\{d_j\}$ we get y as a sum of terms each of which has s-tuple of coefficients that are homogeneous of degree

$$n - d_j = (n - c) + (c - d_j). \tag{3.38}$$

Now $I^{n-c} I^{c-d_j}$, and hence $y \in I^{n-c}(I^c M \cap N)$ as required. Q.E.D.

Corollary 3.6 *The I-adic topology on M and induces a subspace topology on $N \subset M$. Under the current assumptions that A is Noetherian and M finite over A, the induced topology on N coincides with the I-adic topology on N.*

3.7 Exactness of I-adic completion

The point of the Artin–Rees lemma is that it allows us to use the argument of Proposition 3.4 under a slightly weaker assumption: rather than insisting that all $P_{i+1} \to P_i$ are surjective, we only require the weaker "surjective in the limit" given by the Artin–Rees lemma, that P_i is in I^c times the image of P_{i+c} for some fixed c.

Addendum

I should have treated tensor product and flatness in the earlier prerequisite sections. Under Noetherian and finite assumptions (so that Artin–Rees is applicable), the completion $\widehat{M}$ coincides with $\widehat{A} \otimes M$, and $M \to \widehat{M}$ is an exact functor on modules, so that $\widehat{A}$ is a flat A-module.

Exactness of completion I-adic completion is an exact functor. Equivalently, the I-adic completion $\widehat{A}$ of A is a flat A-algebra.

In particular, working with I-adic completions, we know that if $L \subset M$ is a submodule then $\widehat{L} \subset \widehat{M}$ is a submodule, and $\widehat{L}/\widehat{M} = (L/M)\widehat{\ }$.

Let A be a ring and I an ideal of A. We have just seen that I-adic completion gives an exact functor on A-modules. At the same time, it is clear that the I-adic completion $\widehat{M}$ is a module over $\widehat{A}$, and is the same thing as $M \otimes_A \widehat{A}$.

The exactness result just proved for I-adic localisations means exactly that $\widehat{A}$ is a flat A-algebra.

Comparison with exactness of localisation We saw before the exactness statements for S^{-1} and flatness of $S^{-1}A$ (these are much more straightforward to prove).

For A a ring and S a multiplicative sequence in A, we know how to construct the partial ring of fractions $S^{-1}A$. We can make essentially the same construction for an A-module M, obtaining an A-module $S^{-1}M$. It consists of expressions $\{m/s\}$ modulo the same kind of equivalence relation, and the construction gives that $S^{-1}M$ is an A-module on which every $s \in S$ acts bijectively. This means that $S^{-1}M$ is also an $S^{-1}A$-module, and in fact one sees that $S^{-1}M = S^{-1}A \otimes_A M$.

Proposition 3.7 *Let S be a multiplicative set in A and suppose that morphisms $\alpha\colon L \to M$ and $\beta\colon M \to N$ of A-modules give an exact sequence $L \to M \to N$ that is exact (only in the middle, $\operatorname{im}\alpha = \ker\beta$.*

Then α, β induce an exact sequence $S^{-1}L \to S^{-1}M \to S^{-1}N$ of localised modules (with morphisms α' and β').

In particular, working with localisation, we know that if $L \subset M$ is a submodule then $S^{-1}L \subset S^{-1}M$ is a submodule, and $(S^{-1}L)/(S^{-1}M) = S^{-1}(L/M)$.

Proof from [UCA, 6.6] Suppose $m/s \in S^{-1}M$. Then

$$\begin{aligned} \beta'(m/s) = 0 &\iff \exists u \in S \text{ such that } u\beta(m) = 0 \\ &\iff \exists u \in S \text{ such that } \beta(um) = 0. \end{aligned} \tag{3.39}$$

Now since $\mathrm{im}(al) = \ker(\beta)$ in the sequence $L \to M \to N$, this happens

$$\begin{aligned} &\iff \text{there exists } u \in S \text{ and there exists } n \in L \text{ s.t. } u * m = \alpha(n) \\ &\iff m/s = \alpha'(n/us). \square \end{aligned} \tag{3.40}$$

Localisation S^{-1} applied to M can be thought of as $S^{-1}M = S^{-1}A \otimes M$, and the exactness statement just proved can be stated as $S^{-1}A$ is a flat A-algebra.

Informal discussion – why modules?

To study a ring A, we may need to do linear algebra inside A, but also in all kinds of structures related to A: its ideals I, how the I are generated, the quotients A/I, the relations between the generators of I, eventually tensor products $A \otimes A$, derivations and differentials, and much more. We might as well go the whole hog and do linear algebra systematically in modules over A.

Why completions? Let A be a ring and M an A-module. Suppose we are told $M = IM$ for an ideal I of A. Can we deduce that $M = 0$?

Take $m \in M$. Then $m = \sum a_i m_i$ with $a_i \in I$ and $m_i \in M$. On the other hand, the same argument applies to each m_i: if $m_i = \sum b_{ij} m_j$ then $m = \sum_{i,j} a_i b_{ij} m_j$, so that $M = I^2 M$, then $M = I^3 M$. This is getting ridiculous! Surely continuing the argument gives $M = 0$? Not so. For example, it may happen that I contains invertible elements, in which case $M = IM$ tells us nothing.

That's not the right way to go. I remind you of a basic result.

Lemma 3.8 (Nakayama's lemma) *Suppose M is finite (finitely generated as A-module), and $M = IM$. Then there exists $a \in A$ with $a - 1 \in I$ such that $aM = 0$*

Proof This is called the *determinant trick* or the Cayley–Hamilton theorem.

Choose generators $m_1, \ldots, m_n$ such that

$$M = \sum Am_i. \tag{3.41}$$

Then each $m_i \in M$, so $m_i \in IM$. Hence there exists elements $a_{ij} \in I$ with $m_i = \sum a_{ij} m_j$. Rewrite this as

$$\sum (\delta_{ij} - a_{ij}) m_j = 0 \quad \text{where } \delta \text{ is the Kronecker delta.} \tag{3.42}$$

Write N for the $n \times n$ matrix $N = \{\delta_{ij} - a_{ij}\}$. Recall the standard linear algebra formula $N^\dagger \cdot N = (\det N)\,\mathrm{Id}_n$, where $N^\dagger$ is the adjugate matrix of N (made up of $(n-1) \times (n-1)$ cofactors).

Multiply (3.42) by $N^\dagger_{jk}$ and sum over j to get $(\det N) m_j = 0$ for all j, hence $(\det N) \cdot M = 0$. This is what we wanted:

$$a = \det N \quad \text{has} \quad aM = 0 \text{ and } a \equiv 1 \bmod I. \tag{3.43}$$

Corollary 3.9 *If $A \subset B$ be a finite extension ring, every $b \in B$ is integral over A.*

This looks like the easy result from Galois theory that a finite extension of fields is algebraic: since B is finite over A there is a linear dependence relation between the powers $\{1, b, b^2, \ldots, b^n\}$, and you can divide through by the leading coefficient to make it monic.

That doesn't work if A is only assumed to be a field, because you may not be able to divide through. Instead, consider the multiplication map $B \to B$ by b and apply the determinant trick in a straightforward way.