Solutions Sheet 10

Completions of rings and modules

Let R be a commutative ring, k an algebraically closed field.

1. (a) Fix a prime $p \geqslant 2$. For every integer $n \geqslant 1$, define a injective morphism of groups $\alpha_n \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ by setting $\alpha_n(1) = p^{n-1} \bmod p^n\mathbb{Z}$. Let M denote the direct sum of countably many copies of $\mathbb{Z}/p\mathbb{Z}$, and $N = \bigoplus_{n\geqslant 1} \mathbb{Z}/p^n\mathbb{Z}$. Both M and N are considered naturally as $\mathbb{Z}$-modules in what follows.

   Prove that the p-adic completion of M (i.e. the completion with respect to the descending filtration of submodules $(p^nM)_n$) is M itself, but the completion of M with respect to the topology induced by the p-adic topology on N is the direct *product* $\prod_{n\geqslant 1} \mathbb{Z}/p\mathbb{Z}$ (here M clearly injects into N by means of the direct sum of all maps α_n, hence the induced topology on M is the subspace topology).

   (b) Deduce from the previous point that p-adic completion is *not* a right-exact functor on the category of all $\mathbb{Z}$-modules.

Solution.

(a) We obviously have $pM = 0$, hence the inverse system defining the p-adic completion of M is just $\cdots \to M \xrightarrow{\text{id}} M \xrightarrow{\text{id}} M$; the associated inverse limit is clearly isomorphic to M itself.

On the other hand, for every integer $n \geqslant 1$, we have $p^nN = \bigoplus_{j>n} p^n\mathbb{Z}/p^j\mathbb{Z}$. As $\mathrm{Im}(\alpha_j) = p^{j-1}\mathbb{Z}/p^j\mathbb{Z} \subset p^n\mathbb{Z}/p^j\mathbb{Z}$ as long as $j > n$, we deduce that $\alpha_j^{-1}(p^n\mathbb{Z}/p^j\mathbb{Z})$ is $\mathbb{Z}/p\mathbb{Z}$ if $j > n$, and 0 otherwise. Thus the filtration on M induced by the p-adic topology on N is given by

$$(M_n)_{n\in\mathbb{N}} = \left(\bigoplus_{j>n} (\mathbb{Z}/p\mathbb{Z})_j\right)_{n\in\mathbb{N}},$$

where $(\mathbb{Z}/p\mathbb{Z})_j$ denotes the j-th factor in the direct sum defining M. Therefore $M/M_n \simeq \bigoplus_{j=1}^n (\mathbb{Z}/p\mathbb{Z})_j$. Associating to each (equivalence class of) coherent sequence $[(\xi_n)_n] \in \varprojlim M/M_n$ the sequence of its components $\pi_n(\xi_n)$ (where $\pi_n \colon M/M_n \to \mathbb{Z}/\mathbb{Z}$ is the projection map) defines an isomorphism $\varprojlim M/M_n \simeq \prod_{n\geqslant 1} \mathbb{Z}/p\mathbb{Z}$.

(b) Consider the short exact sequence $0 \to M \xrightarrow{\alpha} N \to N/\alpha(M) \to 0$. Taking p-adic completions, we obtain a sequence $0 \to \hat{M} = M \to \hat{N} \to \widehat{N/\alpha(M)} \to 0$; since $M \neq \prod_n \mathbb{Z}/p\mathbb{Z}$, this sequence is not exact at $\hat{N}$, hence p-adic completion is not a right-exact functor.

2. Let R be a noetherian ring, $\mathfrak{a} \subset R$ an ideal, $\hat{R}$ the $\mathfrak{a}$-adic completion of R. For any $x \in R$, denote by $\hat{x}$ its image in $\hat{R}$.

   (a) Prove that $\hat{x}$ is not a zero-divisor in $\hat{R}$ whenever x is not a zero-divisor in R.

   (b) Does the previous point imply that $\hat{R}$ is an integral domain provided that R is an integral domain? *(Hint: prove that the completion of R with respect to the product of two coprime ideals is isomorphic to the direct product of the completions with respect to each ideal separately.)*

   Solution.

   (a) Let $x \in R$ be a nonzerodivisor. Thus multiplication by x in R is injective, i.e. the sequence $0 \to R \xrightarrow{x} R$ is exact. Applying (10.3) in [1], we get that the corresponding sequence $0 \to \hat{R} \to \hat{R}$ is exact, where the induced map on the right-hand side is multiplication by $\hat{x}$, so that $\hat{x}$ is a nonzerodivisor in $\hat{R}$.

   (b) Let $\mathfrak{a}, \mathfrak{b} \subset R$ be two coprime ideals; since all powers $\mathfrak{a}^n, \mathfrak{b}^n$ remain coprime (being coprime is equivalent to say that there is no prime ideal containing the sum of the two ideals, then use the fact that if $\mathfrak{a}^n \subset \mathfrak{p}$ for some prime ideal $\mathfrak{p}$, then $\mathfrak{a} \subset \mathfrak{p}$), by the Chinese remainder theorem we get that the map $R/(\mathfrak{a}\mathfrak{b})^n \to R/\mathfrak{a}^n \times R/\mathfrak{b}^n$ is an isomorphism, for all $n \geqslant 1$. This isomorphism carries over to the inverse limit (taken on both sides), so that the completion $\hat{R}_{\mathfrak{a}\mathfrak{b}}$ is isomorphic to the direct product $\hat{R}_{\mathfrak{a}} \times \hat{R}_{\mathfrak{b}}$ which is not an integral domain. If we take R to be an integral domain, such as $\mathbb{Z}$, we deduce that the completion of an integral domain is not necessarily integral.

3. Let R be a noetherian ring, $\mathfrak{a} \subset R$ an ideal. Prove that $\mathfrak{a}$ is contained in the Jacobson radical of R if and only if every maximal ideal of R is closed for the $\mathfrak{a}$-adic topology on R (a noetherian topological ring in which the topology is defined by an ideal contained in the Jacobson radical is called a *Zariski ring*).

   Solution. It suffices to show that a maximal ideal $\mathfrak{m} \subset R$ is closed in the $\mathfrak{a}$-adic topology if and only if $\mathfrak{a} \subset \mathfrak{m}$.

   Assume first that $\mathfrak{a} \subset \mathfrak{m}$, and let $x \notin \mathfrak{m}$; then, for every integer $n \geqslant 1$, the open neighborhood $x + \mathfrak{a}^n \subset x + \mathfrak{m}$ of x is disjoint from $\mathfrak{m}$. Hence the complement of $\mathfrak{m}$ is $\mathfrak{a}$-adically open, which implies that $\mathfrak{m}$ is closed.

   Conversely, if $\mathfrak{a} \not\subseteq \mathfrak{m}$, any element of $\mathfrak{a} \smallsetminus \mathfrak{m}$ projects onto a unit in the field $R/\mathfrak{m}$; therefore, there exists an element $x \in \mathfrak{a}$ such that $x \equiv 1$ modulo $\mathfrak{m}$. Then $x^n \in \mathfrak{a}^n$ and $x^n \equiv 1$ modulo $\mathfrak{m}$, so that $1 - x^n \in (1 + \mathfrak{a}^n) \cap \mathfrak{m}$ for all $n \geqslant 1$, despite the fact that $1 \notin \mathfrak{m}$. This concludes the proof that $\mathfrak{m}$ is not closed.

4. Let R be a noetherian ring, $\mathfrak{a} \subset R$ an ideal. Denote by $\hat{R}$ the $\mathfrak{a}$-adic completion of R. Prove that the following two conditions are equivalent:

   (a) R is a Zariski ring (see previous exercise for the terminology);

   (b) for any finitely generated R-module M, the canonical map $M \to \hat{M}$ is injective (where $\hat{M}$ denotes the completion of M with respect to the $\mathfrak{a}$-stable filtration $(\mathfrak{a}^n M)_n$).

   (Hint: use the Krull intersection theorem, more precisely its corollary given in Corollary 10.19 *in [1], and the previous exercise.)*

   Solution. [(*a*) $\Longrightarrow$ (*b*)] Assume that R is a Zariski ring, whose topology is defined by the ideal $\mathfrak{a}$ contained in the Jacobson radical of R, and let M be a finitely generated R-module. By Corollary 10.19 in [1], we have that $\bigcap_n \mathfrak{a}^n M = 0$. Sinc the latter is precisely the kernel of the canonical map $M \to \hat{M}$, this shows that this map is injective.

   [(*b*) $\Longrightarrow$ (*a*)] If $\mathfrak{a}$ is not contained in the Jacobson radical of R, there exists a maximal ideal $\mathfrak{m} \notin V(\mathfrak{a})$. By the previous exercise, $\mathfrak{m}$ is not closed for the $\mathfrak{a}$-adic topology on R, which implies that $\{0\}$ is not closed in the finitely generated R-module $M = R/\mathfrak{m}$. Thus $\{0\}$ cannot be the kernel of the continuous homomorphism $M \to \hat{M}$, which achieves the proof.

5. The aim of this exercise is to prove another version of *Hensel's lemma*: let R be a local ring with maximal ideal $\mathfrak{m} \subset R$, and assume that R is complete with respect to its $\mathfrak{m}$-adic filtration. For any polynomial $f(X) \in R[X]$, denote by $\bar{f}(X)$ its reduction modulo $\mathfrak{m}$, so that $\bar{f}(X) \in (R/\mathfrak{m})[X]$. Assume that $f(X)$ is monic of degree n and there exist coprime monic polynomials $\bar{g}(X), \bar{h}(X) \in (R/\mathfrak{m})[X]$ of degrees $r, n-r$ respectively with $\bar{f} = \bar{g}\bar{h}$. Then there are monic polynomials $g, h \in R[X]$ such that $\bar{g}, \bar{h}$ are their respective reductions modulo $\mathfrak{m}$ and $f = gh$.

   (a) Assume inductively that we have constructed $g_k, h_k \in R[X]$ with $g_k h_k - f \in \mathfrak{m}^k R[X]$. Use the fact that $\bar{g}$ and $\bar{h}$ are coprime to find $\bar{a}_p, \bar{b}_p \in (R/\mathfrak{m})[X]$ of degree $\leqslant n-r, r$ respectively, such that $X^p = \bar{a}_p \bar{g}_k + \bar{b}_p \bar{h}_k$ in $(R/\mathfrak{m})[X]$, where p is an integer between 1 and n.

   (b) Use completeness of R to show that the sequences $(g_k)_k$ and $(h_k)_k$ converge to some polynomials $g, h \in R[X]$. Prove that g, h thus defined verify the conclusion of Hensel's lemma.

   Solution.

   (a) Given $\bar{g}, \bar{h} \in (R/\mathfrak{m})[X]$ satisfying the assumption, choose representatives for all the non-vanishing coefficients of both (pick 1 as representative of $1 + \mathfrak{m}$). This defines two monic polynomials $g_1, h_1 \in R[X]$ of degree r, $n - r$

respectively with $\bar{g_1} = \bar{g}$ and $\bar{h_1} = \bar{h}$. Since by hypothesis $\bar{f} = \bar{g}\bar{h} = \overline{g_1 h_1}$, we have that $f \equiv g_1 h_1$ modulo $\mathfrak{m}R[X]$.

Now assume inductively that g_k amd h_k have been constructed with the requested properties. We shall show how to construct g_{k+1}, h_{k+1}. Since $\bar{g}, \bar{h}$ are coprime, Bezout's theorem ensures the existence of polynomials $\alpha, \beta \in R[X]$ such that

$$1 \equiv \alpha g_k + \beta h_k \bmod \mathfrak{m}R[X] \tag{1}$$

. The inductive hypothesis is that $f - g_k h_k \in \mathfrak{m}^k R[X]$; multiplying (1) by $f - g_k h_k$ we find that

$$f - g_k h_k \equiv (f - g_k h_k)\alpha g_k + (f - g_k h_k)\beta h_k \bmod \mathfrak{m}^{k+1} R[X] \ .$$

We now aim to replace the polynomials $(f - g_k h_k)\alpha$ and $(f - g_k h_k)\beta$ with polynomials of degree strictly less than $r, n - r$ (respectively). Since h_k is monic, the division algorithm in $R[X]$ produces $\gamma, \varepsilon \in R[X]$ such that $\deg \varepsilon < n - r$ and $(f - g_k h_k)\alpha = \gamma h_k + \varepsilon$. Since $(f - g_k h_k)\alpha \in \mathfrak{m}^k R[X]$, we have $0 \equiv \gamma h_k + \varepsilon$ modulo $\mathfrak{m}^k R[X]$; as h_k is monic, it has degree $n - r$ also in the ring $(R/\mathfrak{m}^k)[X]$, so that uniqueness of the division algorithm in $(R/\mathfrak{m}^k)[X]$ forces $\gamma, \varepsilon \in \mathfrak{m}^k R[X]$. Therefore,

$$f - g_k h_k \equiv \varepsilon g_k + \delta h_k \bmod \mathfrak{m}^{k+1} R[X]$$

where $\delta = \gamma g_k + (f - g_k h_k)\beta \in \mathfrak{m}^k R[X]$. Since both $f - g_k h_k$ and εg_k have degree $< n$, so does δh_k, which implies that $\deg \delta < r$. We thus see that the polynomials $g_{k+1} = g_k + \delta$ and $h_{k+1} = h_k + \varepsilon$ are monic of degree $r, n - r$ and satisfy $f \equiv g_{k+1} h_{k+1}$ modulo $\mathfrak{m}^{k+1} R[X]$, $\overline{f_{k+1}} = \bar{f}$, $\overline{g_{k+1}} = \bar{g}$.

For the purpose of the following point, let us also remark that g_{k+1} and h_{k+1} are the unique polynomials satisfying the previous properties (this can be proved by induction on k).

(b) If $1 \leqslant i < j$, then $f - g_j h_j \in \mathfrak{m}^j R[X] \subset \mathfrak{m}^i R[X]$, so that $f \equiv g_j h_j$ modulo $\mathfrak{m}^i R[X]$. By the uniqueness claim in the previous point, this forces $g_i \equiv g_j$ and $f_i \equiv f_j$ modulo $\mathfrak{m}^i R[X]$. This shows that the sequence of coefficients are Cauchy in R (for the $\mathfrak{m}$-adic topology), hence by completeness they converge, defining two polynomials g, h of degree r and $n - r$ respectively. Using convergence of the coefficients and the fact that $\bar{g_k} = \bar{g}$, $\bar{h_k} = \bar{h}$ for all $k \geqslant 1$, we deduce that $\bar{g}$ and $\bar{h}$ are the reductions modulo $\mathfrak{m}$ of g and h.

It remains to prove that $f = gh$. First, an easy computation shows that the coefficients of $g_k h_k$ converge (in R) towards the corresponding coeffcients of gh. Since every coefficient of $f - g_k h_k$ belongs to $\mathfrak{m}^k$ by construction, this shows that every coefficient of $f - gh$ is in $\mathfrak{m}^k$. As k is arbitrary, all the coefficients of $f - gh$ are in $\bigcap_k \mathfrak{m}^k = 0$, where the last equality follows from the assumption on R together with Corollary 10.19 in [1]. The proof is concluded.

6. Prove the following corollary of Hensel's lemma: let k be a field, $f(T, X)$ a polynomial in two variables with coefficients in k, and assume that $a \in k$ is a simple root of the polynomial $f(0, X) \in k[X]$. Then there exists a unique power series $X(T) \in k[[T]]$ such that $X(0) = a$ and $f(T, X(T)) = 0$ identically in $k[[T]]$.

   (Hint: apply Hensel's lemma as stated in [2], Theorem 7.3, to $R = k[[T]]$ and $\mathfrak{m} = (T)$.)

   Solution. Let $R = k[[T]]$, which is complete with respect to the maximal ideal $\mathfrak{m} = (T)$. We can see the polynomial $f(T, X)$ as a polynomial $\tilde{f}(X)$ in the variable X with coefficients in R. The assumption that $a \in k$ is a simple root of $f(0, X) \in k[X]$ means precisely that $\tilde{f}(a) \equiv 0$ modulo $\mathfrak{m}$. Hensel's lemma (as stated in Theorem 7.3, [2]) gives that there exists a unique element $X(T) \in R$ such that $\tilde{f}(X(T)) = 0$ and $X(T) \equiv a$ modulo $\mathfrak{m}$. Spelling out this two conditions, this means that $f(T, X(T)) = 0$ identically in $k[[T]]$ and $X(0) = a$.

References

[1] M.Atiyah, Y.McDonald (1994), *Introduction to commutative algebra*, Addison-Wesley Publishing Company.

[2] D.Eisenbud (2004), *Commutative Algebra with a View towards Algebraic Geometry*, Springer.