Imperial College London

PROBLEM SHEETS AND SOLUTIONS FOR COMMUTATIVE ALGEBRA

JEAN-STEFAN KOSKIVIRTA

1. Problem sheet 1

Exercise 1: Let A be an integral domain. Show that $A[X]$ is an integral domain.

Solution: Let $f, g \in A[X]$ be nonzero polynomials. Write $f = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$ and $g = b_m X^m + b_{m-1} X^{m-1} + ... + b_0$ with $a_n, b_m \neq 0$. Then the coefficient of degree $n + m$ of fg is $a_n b_m$, hence is nonzero, so $fg \neq 0$.

Exercise 2: Let A be a ring and $\mathcal{J}(A)$ its Jacobson radical. Show that

$$x \in \mathcal{J}(A) \Longleftrightarrow 1 - ax \text{ is a unit for all } a \in A.$$

In particular, show that if x is nilpotent, then $1 - x$ is a unit.

Solution: ($\Longrightarrow$) Let $x \in \mathcal{J}(A)$ and let $\mathfrak{m} \subset A$ be a maximal ideal. Then for all $a \in A$, one has $1 - ax \notin \mathfrak{m}$, because otherwise $1 = (1 - ax) + ax \in \mathfrak{m}$ which is impossible. Hence $1 - ax$ is not contained in any maximal ideal of A, so it is a unit.

($\Longleftarrow$) Assume $x \notin \mathcal{J}(A)$. Then there exists a maximal ideal $\mathfrak{m} \subset A$ such that $x \notin \mathfrak{m}$. Then the ideal $\mathfrak{m} + Ax$ must be all of A, so we can write $1 = y + ax$ with $a \in A$ and $y \in \mathfrak{m}$. It follows that $1 - ax = y \in \mathfrak{m}$ is not a unit.

In particular, if x is nilpotent, $1 + x$ is a unit because $\mathcal{N}(A) \subset \mathcal{J}(A)$.

Exercise 3: Let A be a ring and $\mathcal{N}(A)$ its nilradical. Show that the following assertions are equivalent:

(1) A has exactly one prime ideal.
(2) Every element of A is either a unit or nilpotent.
(3) $A/\mathcal{N}(A)$ is a field.

Solution: (1) $\Rightarrow$ (2) Let $\mathfrak{p} \subset A$ be the unique prime ideal of A. Then $\mathcal{N}(A) = \mathfrak{p}$ because $\mathcal{N}(A)$ is the intersection of all prime ideals. If $x \notin \mathfrak{p} = \mathcal{N}(A)$, then x is not contained in any maximal ideal (the only maximal ideal being $\mathfrak{p}$), so it is a unit.

(2) $\Rightarrow$ (3) Let $x \in A$ not nilpotent. Then x is a unit in A with inverse y. Hence the class $x + \mathcal{N}(A)$ is a unit in $A/\mathcal{N}(A)$ with inverse $y + \mathcal{N}(A)$. It follows that any nonzero element of $A/\mathcal{N}(A)$ is a unit.

(3) $\Rightarrow$ (1) By assumption, the ideal $\mathcal{N}(A)$ is maximal. It is the intersection of all prime ideals. Thus if $\mathfrak{p} \subset A$ is prime, we must have $\mathfrak{p} = \mathcal{N}(A)$ by maximality of $\mathcal{N}(A)$. Hence $\mathcal{N}(A)$ is the only prime ideal in A.

Exercise 4 : Let A be a ring. An element $x \in A$ is called *idempotent* if $x^2 = x$. Show that if A is a local ring, its only idempotent elements are 0 and 1.

Solution: Let $\mathfrak{m} \subset A$ denote the unique maximal ideal of the local ring A. Recall that the units of A are $A \setminus \mathfrak{m}$. Clearly $0, 1$ are idempotent. Let $x \in A$, $x \neq 0, 1$ be idempotent. From $x^2 = x$, we deduce $x(x-1) = 0$. In particular, x and $x-1$ are zero-divisors, so are not units. Hence $x, x-1 \in \mathfrak{m}$, and then $1 = x - (x-1) \in \mathfrak{m}$ which is a contradiction. It follows that $0, 1$ are the only idempotent elements of A.

Exercise 5 : Let $\mathbf{Z}[i]$ denote the set of complex numbers of the form $a + bi$ with $a, b \in \mathbf{Z}$.

(i) Show that $\mathbf{Z}[i]$ is a subring of $\mathbf{C}$.

(ii) If p is a prime number, show that
$$\mathbf{Z}[i]/(p) \simeq \mathbf{F}_p[X]/(X^2 + 1)$$
where $\mathbf{F}_p$ denotes the finite field with p elements.

(iii) Deduce that the ideal (p) is a prime ideal of $\mathbf{Z}[i]$ if and only if there exists no element $x \in \mathbf{F}_p$ such that $x^2 + 1 = 0$.

(iv) Show that this is the case if and only if $p \equiv 3 \mod 4$.

Solution: (i) One has $0, 1 \in \mathbf{Z}[i]$. If $a, b, c, d \in \mathbf{Z}$, then $(a + bi) + (c + di) = (a+c)+(b+d)i \in \mathbf{Z}[i]$ and $-(a+bi) = (-a)+(-b)i \in \mathbf{Z}[i]$. Finally $(a+bi)(c+di) = (ac - bd) + (ad + bc)i \in \mathbf{Z}[i]$. Hence $\mathbf{Z}[i]$ is a subring of $\mathbf{C}$.

(ii) Let $\mathrm{ev}_i : \mathbf{Z}[X] \to \mathbf{Z}[i]$ be the unique $\mathbf{Z}$-algebra homomorphism mapping X to i. It is clearly surjective. If $P \in \mathrm{Ker}(\mathrm{ev}_i)$, then $P(i) = 0$. Write down the polynomial division of P by $X^2 + 1$ in $\mathbf{Z}[X]$ (this is possible because $X^2 + 1$ is monic) : There exists $Q, R \in \mathbf{Z}[X]$ such that $P = (X^2 + 1)Q + R$ and $\deg(R) < 2$. Hence we can write $R = a+bX$ with $a, b \in \mathbf{Z}$. By evaluating at i, we find $a+bi = 0$, hence $a = b = 0$. It follows that $\mathrm{Ker}(\mathrm{ev}_i) = (X^2 + 1)$. From this we obtain an isomorphism $\mathbf{Z}[X]/(X^2 + 1) \simeq \mathbf{Z}[i]$. It induces an isomorphism:
$$\mathbf{Z}[X]/(p, X^2 + 1) \simeq \mathbf{Z}[i]/(p).$$
Now consider the map $\mathbf{Z}[X] \to \mathbf{F}_p[X]$ given by reducing coefficients modulo p. This map is surjective with kernel $(p) = p\mathbf{Z}[X]$. Hence there is an isomorphism $\mathbf{Z}[X]/(p) \simeq \mathbf{F}_p[X]$, and it induces an isomorphism:
$$\mathbf{Z}[X]/(p, X^2 + 1) \simeq \mathbf{F}_p[X]/(X^2 + 1).$$
Combining these two isomorphisms, we find $\mathbf{Z}[i]/(p) \simeq \mathbf{F}_p[X]/(X^2 + 1)$.

(iii) We have equivalences
$$\begin{aligned}(p) \text{ prime in } \mathbf{Z}[i] &\iff \mathbf{Z}[i]/(p) \text{ is an integral domain} \\ &\iff \mathbf{F}_p[X]/(X^2+1) \text{ is an integral domain} \\ &\iff X^2+1 \text{ is irreducible in } \mathbf{F}_p[X] \\ &\iff X^2+1 \text{ has no root in } \mathbf{F}_p.\end{aligned}$$
The last equivalence holds because $X^2 + 1$ has degree 2.

(iv) If $p = 2$, then $1^2 + 1 = 0$, so there is a solution. Now assume p is an odd prime number. For all $x \in \mathbf{F}_p^\times$, we have
$$\begin{aligned}x^2 + 1 = 0 &\iff x^2 = -1 \\ &\iff x \text{ has order 4 in the group } \mathbf{F}_p^\times.\end{aligned}$$

Since $\mathbf{F}_p^\times$ is cyclic of order $p-1$, the existence of an element of order 4 is equivalent to $4|p-1$, which is the same as $p \equiv 1 \pmod 4$.

2. Problem sheet 2

Exercise 1: Let A be a nonzero ring. An A-module M is *free* if M is isomorphic to a direct sum $\bigoplus_{i\in I} M_i$ where $M_i = A$ for all $i \in I$.

(1) Show that M is free and finitely generated if and only if M is isomorphic to A^n for some $n \geq 0$.
(2) Show that if $A^n \simeq A^m$ for $n, m \geq 0$, then $n = m$. Hence if M is free and finitely generated, we can define its *rank* $\mathrm{rk}(M)$ as the unique integer $n \geq 0$ such that $M \simeq A^n$.
(3) Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of finitely generated free modules. Show that $\mathrm{rk}(M) = \mathrm{rk}(M') + \mathrm{rk}(M'')$.

Solution:

(1) clearly A^n is free, finitely generated. Conversely, assume $M = \bigoplus_I A$ is finitely generated. Then we will show that I is finite. Assume the contrary and let $x_1, ..., x_n \in M$ be a generating system. For $j \in I$, denote by $p_j : M \to A$ the natural projection map $(a_i)_{i\in I} \mapsto a_j$. It is a surjective A-module homomorphism. Since I is infinite, we can find $j \in I$ such that $p_j(x_1) = ... = p_j(x_n) = 0$. But $x_1, ..., x_n$ generate M so their images $p_j(x_1), ..., p_j(x_n)$ generate A because p_j is surjective. This is a contradiction.

(2) Let $f : M \to N$ be an isomorphism of A-modules. Since A is nonzero, there exists a maximal ideal $\mathfrak{m} \subset A$. Clearly, one has $f(\mathfrak{m}M) = \mathfrak{m}N$. Hence it follows that f induces an isomorphism of A-modules

$$M/\mathfrak{m}M \longrightarrow N/\mathfrak{m}N.$$

In particular, this is an isomorphism of $A/\mathfrak{m}$-vector spaces (note that $M/\mathfrak{m}M$ has a natural structure of $A/\mathfrak{m}$-vector space).

Now assume that $M = A^n$ for some $n \geq 0$. Then $M/\mathfrak{m}M = A^n/\mathfrak{m}A^n \simeq (A/\mathfrak{m})^n$ is an n-dimensional $A/\mathfrak{m}$-vector space. It follows that if $A^n \simeq A^m$ as A-modules, we must have $n = m$.

(3) Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be an exact sequence of finitely generated free modules.

<u>Claim</u>: There exists an A-linear map $\beta : M'' \to M$ such that $g \circ \beta = \mathrm{id}_{M''}$.

To show this, we may assume for simplicity $M'' = A^r$ for some $r \geq 1$. Denote by $e_1, ..., e_r \in A^r$ the usual basis vectors of A^r. Since g is surjective, we may choose $x_i \in M$ such that $g(x_i) = e_i$ for all $i = 1, ..., r$. Define β by

$$\beta(a_1, ..., a_r) := \sum_{i=1}^r a_i x_i.$$

It is clear that β satisfies the condition $g \circ \beta = \mathrm{id}_{M''}$, which proves the claim.

<u>Claim</u>: M is the direct sum of $f(M') = \mathrm{Ker}(g)$ and $\beta(M'')$.

Let $x \in M$. We have $g(x) \in M''$ so $g(\beta(g(x))) = g(x)$, hence $g(x - \beta(g(x))) = 0$ and thus $x - \beta(g(x)) \in \mathrm{Ker}(g)$. Hence any element of M is the sum of an element of $\mathrm{Ker}(g)$ and an element of $\beta(M'')$. To show $M = \mathrm{Ker}(g) \oplus \beta(M'')$, it remains to prove $\mathrm{Ker}(g) \cap \beta(M'') = 0$. For this, let $x \in \mathrm{Ker}(g) \cap \beta(M'')$. We can write $x = \beta(y)$ with $y \in M''$. Then $0 = g(x) = g(\beta(y)) = y$ and then $x = 0$.

Now we finish the proof. We have $f(M') \simeq M' \simeq A^d$ where $d = \mathrm{rk}(M')$ and $\beta(M'') \simeq M'' \simeq A^r$. We deduce $M \simeq A^d \oplus A^r \simeq A^{r+d}$.

Exercise 2 : Let A be a subring of $\mathbf{Q}$. Show that there exists a multiplicative subset $S \subset \mathbf{Z}$ such that $A = S^{-1}\mathbf{Z}$.

Solution:

For a multiplicative subset $S \subset \mathbf{Z}$, there is a ring homomorphism $S^{-1}\mathbf{Z} \to \mathbf{Q}$, $\frac{a}{s} \mapsto \frac{a}{s}$ (where the second fraction is to be understood as a fraction of two integers). This map is well-defined and injective. It induces an identification of $S^{-1}\mathbf{Z}$ with a subring of $\mathbf{Q}$. More precisely,

$$S^{-1}\mathbf{Z} = \left\{ \frac{a}{s} \in \mathbf{Q},\ s \in S,\ a \in \mathbf{Z} \right\}.$$

Let $A \subset \mathbf{Q}$ be a subring. Clearly, A contains $\mathbf{Z}$ because $1 \in A$ and A is an additive group. We want to find a multiplicative subset $S \subset \mathbf{Z}$ such that $A = S^{-1}\mathbf{Z}$. Using the previous considerations, it is natural to define

$$S := \left\{ s \in \mathbf{Z},\ \frac{1}{s} \in A \right\}.$$

In other words, $S = \mathbf{Z} \cap A^{\times}$, and this shows clearly that S is a multiplicative subset of $\mathbf{Z}$.

Claim: $A = S^{-1}\mathbf{Z}$.

If $a \in \mathbf{Z}$ and $s \in S$, then $\frac{a}{s} = a\frac{1}{s} \in A$. Hence $S^{-1}\mathbf{Z} \subset A$. Conversely, let $x \in A$ and write $x = \frac{a}{b}$ with $a, b \in \mathbf{Z}$, $b \neq 0$ and a, b coprime. We can find $r, s \in \mathbf{Z}$ such that $ar + bs = 1$. It follows

$$\frac{1}{b} = s + rx \in A$$

and we deduce $b \in S$, and hence $x \in S^{-1}\mathbf{Z}$. This proves the claim.

Exercise 3 : Let S be a multiplicative subset of a ring A and let M be a finitely generated A-module. Show that $S^{-1}M = 0$ if and only if there exists $s \in S$ such that $sM = 0$.

Solution:

For any A-module M, the equation $S^{-1}M = 0$ means exactly that for each $m \in M$, there exists $s \in S$ such that $sm = 0$. Of course, the element s that satisfies $sm = 0$ may depend on m. The point of the exercise is to show, provided M is finitely generated, that we can find s independent of m. This is achieved as follows: Take a finite generating system $x_1, ..., x_n \in M$. As we explained above, for each $i = 1, ..., n$ we can find $s_i \in S$ such that $s_i x_i = 0$. Then define

$$s := s_1 ... s_n.$$

It is clear that $sx_i = 0$ for all $i = 1, ..., n$. Since every element of M is a linear combination of $x_1, ..., x_n$, it follows that $sm = 0$ for all $m \in M$. In other words, $sM = 0$.

Exercise 4 : Let A be a ring, and let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be a sequence of A-modules. Show that the following conditions are equivalent:

(1) The sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact.

(2) The sequence $0 \to M'_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} M_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} M''_{\mathfrak{p}} \to 0$ is exact for all prime ideals $\mathfrak{p} \subset A$.

(3) The sequence $0 \to M'_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} M_{\mathfrak{m}} \xrightarrow{g_{\mathfrak{m}}} M''_{\mathfrak{m}} \to 0$ is exact for all maximal ideals $\mathfrak{m} \subset A$.

Solution:

(1) $\Rightarrow$ (2) follows from the lectures. (2) $\Rightarrow$ (3) is clear. It remains to show the implication (3) $\Rightarrow$ (1).

(a) f is injective.

Consider the exact sequence $0 \to \operatorname{Ker}(f) \to M' \xrightarrow{f} M$. For any maximal ideal $\mathfrak{m} \subset A$, the sequence $0 \to \operatorname{Ker}(f)_{\mathfrak{m}} \to M'_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} M_{\mathfrak{m}}$ is thus exact. By assumption (3), the map $f_{\mathfrak{m}}$ is injective, which implies $\operatorname{Ker}(f)_{\mathfrak{m}} = 0$ for all maximal ideal $\mathfrak{m} \subset A$. It follows by the lectures that $\operatorname{Ker}(f) = 0$.

(b) g is surjective.

Definition 2.0.1. *The cokernel of a A-module homomorphism $f : M \to N$ is defined as $N/\operatorname{ima}(f)$.*

Note that $\operatorname{Coker}(f) = 0 \Leftrightarrow f$ is surjective. Hence, it is equivalent to show $\operatorname{Coker}(g) = 0$. As above, it suffices to show that $\operatorname{Coker}(g)_{\mathfrak{m}} = 0$ for all maximal ideal $\mathfrak{m} \subset A$. Look at the exact sequence $M \xrightarrow{g} M'' \to \operatorname{Coker}(g) \to 0$. Localizing at $\mathfrak{m}$, we obtain an exact sequence $M_{\mathfrak{m}} \xrightarrow{g_{\mathfrak{m}}} M''_{\mathfrak{m}} \to \operatorname{Coker}(g)_{\mathfrak{m}} \to 0$. By assumption, $g_{\mathfrak{m}}$ is surjective, and so $\operatorname{Coker}(g)_{\mathfrak{m}} = 0$.

(c) One has $g \circ f = 0$ (in other words $\operatorname{ima}(f) \subset \operatorname{Ker}(g)$).

We know that the localization $g_{\mathfrak{m}} \circ f_{\mathfrak{m}}$ of the map $g \circ f$ is zero at all maximal ideals $\mathfrak{m} \subset A$, by assumption. Hence it suffices to prove the following general lemma:

Lemma 2.0.2. *Let $f : M \to N$ be an A-module homomorphism. If $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is the zero map for all maximal ideal $\mathfrak{m} \subset A$, then $f = 0$.*

To prove the Lemma, let $x \in M$ be an element. There is a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \downarrow \\ M_{\mathfrak{m}} & \xrightarrow{f_{\mathfrak{m}}} & N_{\mathfrak{m}} \end{array}$$

It follows that the image of $f(x) \in N$ in $N_{\mathfrak{m}}$ is zero for all maximal ideal $\mathfrak{m} \subset A$. Hence it follows from the lecture that $f(x) = 0$.

(d) One has $\operatorname{ima}(f) = \operatorname{Ker}(g)$.

The inclusion map $\operatorname{ima}(f) \to \operatorname{Ker}(g)$ is surjective (i.e an equality) when localized at each maximal ideal $\mathfrak{m} \subset A$. As in step (b), we deduce that it must be surjective, hence $\operatorname{ima}(f) = \operatorname{Ker}(g)$, which terminates the proof.

Exercise 5 : Let A be a ring and $I \subset A$ a decomposable ideal. If $r(I) = I$, show that I has no embedded prime ideals (recall that $r(I)$ denotes the radical of I).

Solution:

Let $I = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n$ be a minimal primary decomposition of I. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$, $i = 1, ..., n$ denote the prime ideals belonging to I. Recall that a non-minimal element of the set $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$ (with respect to inclusion) is called an embedded prime. Taking radicals, we deduce

$$I = r(I) = r(\mathfrak{q}_1 \cap ... \cap \mathfrak{q}_n) = \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_n.$$

Since I has exactly n prime ideals belonging to it, the decomposition $I = \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_n$ must be a minimal decomposition of I (otherwise I would have a minimal decomposition with strictly less than n primary ideals). Hence we deduce that $\mathfrak{p}_i$ is not contained in $\mathfrak{p}_j$ for all $i \neq j$. The result follows.

3. Problem sheet 3

Exercise 1 : Let A be a nonzero ring.

(1) Let M be a Noetherian A-module and $f : M \to M$ a surjective A-module homomorphism. Show that f is an isomorphism.
(2) Assume that M is Artinian, and let $f : M \to M$ be an injective A-module homomorphism. Show that f is an isomorphism.

Solution:

(1) We have an ascending chain of submodules of M:

$$\mathrm{Ker}(f) \subset \mathrm{Ker}(f^2) \subset ...$$

Since M is Noetherian, this chain is stationary: There exists $n \geq 1$ such that $\mathrm{Ker}(f^n) = \mathrm{Ker}(f^{n+1}) = ...$ Let $x \in \mathrm{Ker}(f)$. Since f is surjective, we can find $y \in M$ such that $x = f^n(y)$. Hence $f^{n+1}(y) = f(x) = 0$, so $y \in \mathrm{Ker}(f^{n+1}) = \mathrm{Ker}(f^n)$. Hence we conclude $x = 0$, so f is injective.

(2) We have a descending chain of submodules of M:

$$\mathrm{ima}(f) \supset \mathrm{ima}(f^2) \supset ...$$

Since M is Artinian, this chain is stationary: There exists $n \geq 1$ such that $\mathrm{ima}(f^n) = \mathrm{ima}(f^{n+1}) = ...$ Now let $y \in M$ be an element. Applying f^n we have $f^n(y) \in \mathrm{ima}(f^n) = \mathrm{ima}(f^{n+1})$. Hence there exists $x \in M$ such that $f^n(y) = f^{n+1}(x)$. Since f is injective, we deduce $y = f(x)$ and hence f is surjective.

Exercise 2 :

(1) Let A be a nonzero ring and $S \subset A$ a multiplicative subset. Let M be a Noetherian (resp. Artinian) A-module. Show that $S^{-1}M$ is a Noetherian (resp. Artinian) $S^{-1}A$-module. In particular, show that if A is a Noetherian (resp. Artinian) ring, then $S^{-1}A$ is a Noetherian (resp. Artinian) ring.
(2) Let A be a ring such that $A_{\mathfrak{p}}$ is Noetherian for all prime ideals $\mathfrak{p} \subset A$. Does it imply that A is Noetherian?

Solution:

(1) If N is a submodule of M, then $S^{-1}N$ is a submodule of $S^{-1}M$. We claim

that for every submodule $N' \subset S^{-1}M$, there exists a submodule $N \subset M$ such that $N' = S^{-1}N$. Indeed, put

$$N := \{x \in M,\ \frac{x}{1} \in N'\}.$$

In other words, $N = f^{-1}(N')$ where $f : M \to S^{-1}M$, $x \mapsto \frac{x}{1}$. Then N is clearly a submodule of M.

Claim : One has $S^{-1}N = N'$.

Indeed, if $x \in N$ and $s \in S$, then $\frac{x}{s} = \frac{1}{s} \cdot \frac{x}{1} \in N'$, so $S^{-1}N \subset N'$. Conversely, if $\frac{x}{s} \in N'$ where $x \in M$ and $s \in S$, then one has $\frac{x}{1} = \frac{s}{1} \cdot \frac{x}{s} \in N'$ which implies $x \in N$ and thus $\frac{x}{s} \in S^{-1}N$.

Hence we showed that for all submodule $N' \subset S^{-1}M$, one has the formula $S^{-1}(f^{-1}(N')) = N'$. Now assume that M is a Noetherian (resp. Artinian) A-module. Take an ascending (resp. descending) chain $\mathcal{C}$ of $S^{-1}A$-submodules in $S^{-1}M$. The chain $f^{-1}\mathcal{C}$ obtained by taking preimages in M by f is again ascending (resp. descending), hence is stationary by assumption. But then applying S^{-1} shows that the chain $\mathcal{C} = S^{-1}(f^{-1}(\mathcal{C}))$ is also stationary. Hence $S^{-1}M$ is a Noetherian (resp. Artinian) S^{-1}-module.

(2) If $A_\mathfrak{p}$ is Noetherian for all prime ideal $\mathfrak{p}$, it does not imply that A is Noetherian. For example, let k be a field and A the ring

$$A := k^{\mathbf{N}}$$

where addition and multiplication are defined componentwise. We claim that A has Krull dimension 0 (in other words, every prime ideal is a maximal ideal). This follows from the following lemma:

Lemma 3.0.1. *Let A be a nonzero ring such that for all $x \in A$, there exists $y \in A$ such that $x = x^2y$. Then*

(a) Every prime ideal of A is maximal.
(b) If $\mathfrak{m} \subset A$ is maximal ideal, the local ring $A_\mathfrak{m}$ is a field.

Proof.

(a) Let $\mathfrak{p}$ be a prime ideal and $x \in A$ such that $x \notin \mathfrak{p}$. There exists $y \in A$ such that $x = x^2y$, hence $x(1 - xy) = 0$. Since $x \notin \mathfrak{p}$, we deduce that $1 - xy \in \mathfrak{p}$. This shows that the class $x + \mathfrak{p}$ is a unit in the ring $A/\mathfrak{p}$. Hence every nonzero element of $A/\mathfrak{p}$ is a unit, so $A/\mathfrak{p}$ is a field and $\mathfrak{p}$ is maximal.

(b) First we claim that if $x \in \mathfrak{m}$, then $\frac{x}{1} = 0$ in $A_\mathfrak{m}$. Indeed, let $y \in A$ such that $x(1 - xy) = 0$. Since $x \in \mathfrak{m}$, we have $1 - xy \notin \mathfrak{m}$ (otherwise $1 = 1 - xy + xy \in \mathfrak{m}$ is a contradiction). Hence $\frac{x}{1} = \frac{x(1-xy)}{1-xy} = 0$. Next, we claim that the natural map $f : A \to A_\mathfrak{m}$, $z \mapsto \frac{z}{1}$ is surjective. It suffices to show that any element of the form $\frac{1}{x}$ for $x \in A - \mathfrak{m}$ is in the image of f. Choose $y \in A$ such that $x(1 - xy) = 0$. Since $x \notin \mathfrak{m}$, we have $1 - xy \in \mathfrak{m}$ since $\mathfrak{m}$ is prime. Hence $y \notin \mathfrak{m}$ because otherwise $1 = 1 - xy + xy \in \mathfrak{m}$ leads to a contradiction. We deduce:

$$\frac{1}{x} = \frac{xy}{x} = \frac{y}{1}.$$

Hence f is surjective. Note that $A_\mathfrak{m}$ is not the zero ring, because the multiplicative subset $A - \mathfrak{m}$ does not contain 0. Since $\mathfrak{m} \subset \mathrm{Ker}(f)$, we deduce that $\mathrm{Ker}(f) = \mathfrak{m}$ and $A_\mathfrak{m} \simeq A/\mathfrak{m}$, thus $A_\mathfrak{m}$ is a field.

□

Let us show that $A = k^{\mathbf{N}}$ satisfies the condition of Lemma 3.0.1. If $x = (x_n) \in k^{\mathbf{N}}$, then define $y := (y_n)$ by

$$y_n := \begin{cases} \frac{1}{x_n} & \text{if } x_n \neq 0 \\ 0 & \text{if } x_n = 0. \end{cases}$$

It is clear that $x = x^2 y$.

Since a field is a Noetherian ring, the localization $A_{\mathfrak{m}}$ is Noetherian for all maximal ideal $\mathfrak{m} \subset A$. Finally, we claim that A is not Noetherian. For a subset $m \in \mathbf{N}$, define an ideal

$$I_m := \{x = (x_n) \in k^{\mathbf{N}},\ x_j = 0 \text{ for all } j \geq m\}.$$

It is clear that we have a strictly ascending chain of ideals

$$I_0 \subset I_1 \subset I_2 \subset \cdots$$

which shows that A is not Noetherian.

Exercise 3 :

(1) Let A be a ring where every prime ideal is finitely generated. Show that A is Noetherian.
(2) Let A be an integral domain where every prime ideal is principal. Show that A is a PID.

Solution:

(1) Assume that A is not Noetherian. Let Σ denote the set of all ideals which are not finitely generated. Since A is Noetherian, Σ is nonempty. Assume that $\Delta \subset \Sigma$ is a nonempty, totally ordered subset. We claim that the set

$$J := \bigcup_{I \in \Delta} I$$

is an upper bound of Δ in Σ. It is easy to see that J is an ideal (because Δ is totally ordered). If J was finitely generated, then there would exist $x_1, ..., x_n \in J$ generating J. There exists $I \in \Delta$ such that $x_1, ..., x_n \in I$, but then $J = I$ is in Δ, so it is not finitely generated, which is a contradiction. Hence we have showed that Σ satisfies the condition of Zorn's Lemma. Therefore there exists a maximal element in Σ, denote by J such a maximal element.

We claim that J is a prime ideal. Let $x, y \in A$ such that $xy \in J$. Assume for a contradiction that $x \notin J$ and $y \notin J$. The ideal $J+(x)$ and $J+(y)$ contain J properly, hence by maximality these ideals are not in Σ, so they are finitely generated. Let $z_1, ..., z_n$ be a generating system of $J + (x)$. We can write $z_i = y_i + a_i x$, where $y_i \in J$ and $a_i \in A$ for each $i = 1, ..., n$. Let $I \subset J$ denote the ideal $I = (y_1, ..., y_n)$. It is clear that we have the relation

$$I + (x) = J + (x).$$

The ideal quotient $(J : x)$ contains J and $y \in (J : x)$, so the inclusion $J \subset (J : x)$ is strict. Hence by maximality of J, the ideal $(J : x)$ is finitely generated. One has the relation

$$J = I + (x)(J : x).$$

Indeed, one clearly has $I + (x)(J : x) \subset J$. Conversely, let $z \in J$. We can write

$$z = w + ax$$

for some $a \in A$ and $w \in I$. Since $ax \in J$, we have $a \in (J : x)$, so $z \in I + (x)(J : x)$. Finally, I and $(J : x)$ are finitely generated, so $J = I + (x)(J : x)$ is finitely generated, which is a contradiction. We have showed that J is a prime ideal.

Now by assumption, every prime ideal is finitely generated, so J is finitely generated. This is a contradiction. It follows that A is Noetherian.

(2) By (1), we know that A is Noetherian. Assume that A is not a PID and let Σ be the set of ideals which are not principal. Since A is Noetherian, there exists a maximal element $J \in \Sigma$. We claim that J is a prime ideal. For a contradiction, assume there is $x, y \in A$ such that $x \notin J$, $y \notin J$ and $xy \in J$. The ideals $J + (x)$ and $J + (y)$ contain J properly, so they are principal by maximality of J. Hence $J + (x) = (a)$ and $J + (y) = (b)$ for some $a, b \in A$. Note that we have

$$(J : a)a = J.$$

Indeed, for all $z \in J$, we have $z = az'$ for $z' \in A$ thus $z' \in (J : a)$ and hence $z \in (J : a)a$. The inclusion $J \subset (J : a)$ is strict because $b \in (J : a)$ and $b \notin J$. It follows by maximality of J that $(J : a)$ is principal, and hence so is $J = (J : a)a$. This is a contradiction. We have proved the claim that J is a prime ideal. Now by assumption every prime ideal is principal, so J is principal, and this is a contradiction. In conclusion, A is a PID.

Exercise 4 : Let p be a prime number, and $U \subset \mathbf{C}^\times$ defined by

$$U := \left\{ x \in \mathbf{C}^\times,\ \exists n \geq 1,\ x^{p^n} = 1 \right\}.$$

Since U is an abelian group, it is endowed with a natural structure of $\mathbf{Z}$-module. Show that U is an Artinian $\mathbf{Z}$-module which is not Noetherian.

Solution:

For each $n \geq 1$, let $U_n \subset U$ denote the subgroup of $z \in U$ such that $z^{p^n} = 1$. We have an infinite strictly ascending sequence

$$U_0 \subset U_1 \subset U_2 \subset \dots$$

which shows that U is not a Noetherian $\mathbf{Z}$-module.

Claim : The U_n are exactly the proper subgroups of U.

First of all, it is clear that U_n is cyclic of order p^n and that $U_0, ..., U_{n-1}$ are exactly the proper subgroups of U_n. Now, let $H \subset U$ be a proper subgroup. Let m be the supremum of all integers k such that $U_k \subset H$. Since the union of all U_n is all of U, it must be a finite integer. Let $x \in H$. It generates a cyclic subgroup of order p^r for some $r \geq 0$ and we must have $\langle x \rangle = U_r$. Hence $r \leq m$ because otherwise $U_{m+1} \subset U_r \subset H$ contradicts the definition of m. Finally, we obtain $H \subset U_m$, and then clearly $H = U_m$. This proves the claim.

It follows easily that any descending chain of subgroups must be stationary, so U is an Artinian $\mathbf{Z}$-module.

Exercise 5 : What is the length of $\mathbf{Z}/n\mathbf{Z}$ as a $\mathbf{Z}$-module?

Solution:

If $n = p$ is a prime number, then it is clear that $\ell(\mathbf{Z}/p\mathbf{Z}) = 1$. We claim that if

$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with $\alpha_i \in \mathbf{N}$ and $p_1, ..., p_r$ pairwise distinct prime numbers, then

$$\ell(\mathbf{Z}/n\mathbf{Z}) = \sum_{i=1}^{r} \alpha_i.$$

Let $\delta(n)$ denote this function. One has clearly $\delta(nm) = \delta(n)+\delta(m)$ for all $n, m \geq 1$. We prove by induction on $\delta(n)$ that $\ell(\mathbf{Z}/n\mathbf{Z}) = \delta(n)$ for all $n \geq 1$. If $\delta(n) = 1$ then n is prime and $\ell(\mathbf{Z}/n\mathbf{Z}) = \delta(n) = 1$. Now let $n \geq 1$ not prime. We can write $n = dm$ with $1 < d, m < n$. Let $H \subset \mathbf{Z}/n\mathbf{Z}$ denote the unique (cyclic) subgroup of order d. The quotient $H' := (\mathbf{Z}/n\mathbf{Z})/H$ is cyclic of order m. We have an exact sequence:

$$0 \to H \to \mathbf{Z}/n\mathbf{Z} \to H' \to 0.$$

Hence by additivity of the length we deduce $\ell(\mathbf{Z}/n\mathbf{Z}) = \ell(H) + \ell(H')$. Since $\delta(d)$ and $\delta(m)$ are $< \delta(n)$, we deduce by induction that $\ell(H) = \delta(d)$ and $\ell(H') = \delta(m)$. Hence

$$\ell(\mathbf{Z}/n\mathbf{Z}) = \delta(d) + \delta(m) = \delta(n)$$

which terminates the proof.

4. Problem sheet 4

Exercise 1 : Let k be a field and V, W finite-dimensional k-vector spaces. Let $\mathcal{B} := (e_1, ..., e_n)$ and $\mathcal{B}' := (u_1, ..., u_m)$ be basis of V and W, respectively. For k-linear endomorphisms $f : V \to V$ and $g : W \to W$, denote by A and B the matrices of f and g in the basis $\mathcal{B}$ and $\mathcal{B}'$, respectively. Determine the matrix of $f \otimes g$ in the basis $(e_i \otimes u_j)_{i,j}$ of $V \otimes W$.

Solution:
The map

$$V \times W \to V \otimes W$$

defined by $(x, y) \mapsto f(x) \otimes g(y)$ is k-bilinear and hence induces a k-linear map $f \otimes g : V \otimes W \to V \otimes W$ mapping $x \otimes y$ to $f(x) \otimes g(y)$.

We know by the lectures that $(e_i \otimes u_j)_{i,j}$ is a k-basis of $V \otimes W$. Let $A = (a_{r,s})_{1 \leq r,s \leq n}$ and $B = (b_{r,s})_{1 \leq r,s \leq m}$ denote the matrices of f and g in the basis $(e_1, ..., e_n)$ and $(u_1, ..., u_m)$ respectively. In other words

$$f(e_i) = \sum_{r=1}^{n} a_{r,i} e_r$$

$$g(u_j) = \sum_{s=1}^{m} b_{s,j} u_s$$

for all $1 \leq i \leq n$ and $1 \leq j \leq m$. It follows:

$$\begin{aligned} (f \otimes g)(e_i \otimes f_j) &= f(e_i) \otimes g(e_j) \\ &= \left(\sum_{r=1}^{n} a_{r,i} e_r \right) \otimes \left(\sum_{s=1}^{m} b_{s,j} u_s \right) \\ &= \sum_{r=1}^{n} \sum_{s=1}^{m} a_{r,i} b_{s,j} (e_r \otimes u_s). \end{aligned}$$

We order the set $\{1,...,n\}\times\{1,...,m\}$ by lexicographic order, i.e

$$(a,b)\leq(c,d)\Longleftrightarrow(a<c)\text{ or }(a=c\text{ and }b\leq d).$$

This gives an ordering of the vectors $e_i\otimes u_j$ and the matrix of $f\otimes g$ in this basis is:

$$\begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & & \vdots \\ a_{n,1}B & \cdots & a_{n,n}B \end{pmatrix}\in M_{nm}(k).$$

Exercise 2 : Let A be a nonzero ring and B an A-algebra. Let M be an A-module and N a B-module. Show that

$$\mathrm{Hom}_A(M,N)\simeq\mathrm{Hom}_B(M\otimes_A B,N).$$

Solution:
If $f:M\to N$ is an A-linear map, we define an A-bilinear map

$$M\times B\to N,\ (x,b)\mapsto bf(x).$$

It follows that there is a unique A-linear map $\phi(f):M\otimes_A B\to N$ mapping $x\otimes b$ to $bf(x)$. Recall that $M\otimes_A B$ is naturally endowed with a structure of B-module such that $b'(x\otimes b)=x\otimes bb'$ for all $b,b'\in B$ and $x\in M$.

Claim : The map $\phi(f)$ is B-linear.

Indeed, for all $x\in M$, $b,b'\in B$, one has

$$\phi(f)(b'(x\otimes b))=\phi(f)(x\otimes bb')=bb'f(x)=b'(\phi(f)(x\otimes b)).$$

We have defined a map $f\mapsto\phi(f)$, $\mathrm{Hom}_A(M,N)\to\mathrm{Hom}_B(M\otimes_A B,N)$. The set $\mathrm{Hom}_B(M\otimes_A B,N)$ has a natural structure of B-module by the lectures. One can also define a B-module structure on $\mathrm{Hom}_A(M,N)$ as follows: If $f\in\mathrm{Hom}_A(M,N)$ and $b\in B$, then we define bf by

$$bf:M\to N,\ x\mapsto bf(x).$$

It is easy to see that $\mathrm{Hom}_A(M,N)$ becomes a B-module in this way.

Claim : The map $f\mapsto\phi(f)$ defined above is B-linear.

Let $f\in\mathrm{Hom}_A(M,N)$ and $b'\in B$. One has for all $x\in M$ and $b\in B$,

$$\phi(b'f)(x\otimes b)=b((b'f)(x))=b(b'(f(x)))=bb'f(x)=b'(\phi(f)(x\otimes b))=(b'\phi(f))(x\otimes b)$$

which shows that $\phi(b'f)=b'\phi(f)$ as claimed.

Claim : ϕ is injective.

Indeed, assume that $f\in\mathrm{Hom}_A(M,N)$ and $\phi(f)=0$. In particular, one has for all $x\in M$:

$$0=(\phi(f))(x\otimes 1)=f(x)$$

hence $f=0$.

Claim : ϕ is surjective.

Let $g\in\mathrm{Hom}_B(M\otimes_A B,N)$ be an element. Define a map $f:M\to N$ by

$$f(x)=g(x\otimes 1)$$

for all $x\in M$. It is clear that f is A-linear. We show that $\phi(f)=g$. Indeed, for all $x\in M$ and $b\in B$, one has

$$\phi(f)(x\otimes b)=bf(x)=bg(x\otimes 1)=g(x\otimes b)$$

which proves the claim.

We have shown that ϕ defines an isomorphism of B-modules $\mathrm{Hom}_A(M, N) \simeq \mathrm{Hom}_B(M \otimes_A B, N)$.

Exercise 3 : A ring A is called *absolutely flat* if every A-module is flat. Show that the following assertions are equivalent:

(1) A is absolutely flat.
(2) Every principal ideal I satisfies $I^2 = I$.
(3) For every finitely generated ideal $I \subset A$, there exists an ideal J such that $A = I \oplus J$.

Solution:
(1) $\Rightarrow$ (2) : Let $x \in A$. By assumption, $A/(x)$ is a flat A-module. Consider the injection $(x) \to A$. Then after tensoring with $A/(x)$, we obtain an injective map

$$f : (x) \otimes_A (A/(x)) \to A/(x).$$

Recall that $M \otimes_A A/I \simeq M/IM$ for all A-module M. Hence $(x) \otimes_A (A/(x)) \simeq (x)/(x^2)$. Since f maps x to 0, we deduce that $f = 0$, and so we must have $(x) \otimes_A (A/(x)) = 0$, hence $(x) = (x^2)$.

(2) $\Rightarrow$ (3) : Let $x \in A$. Then $x = ax^2$ for some element $a \in A$. Hence $ax = a^2x^2 = (ax)^2$, so $e := ax$ is idempotent. Clearly $e \in (x)$ so $(e) \subset (x)$. Conversely, $x = ex \in (e)$ so we deduce $(e) = (x)$. Hence every principal ideal is generated by an idempotent.

Claim : If $e, f \in A$ are idempotents, then the ideal (e, f) is generated by $e+f-ef$.

Indeed, one has clearly $(e+f-ef) \subset (e, f)$. Conversely, one has $e(e+f-ef) = e^2 + ef - e^2f = e$ and similarly $f(e+f-ef) = f$. This proves the claim.

By induction, we deduce that any finitely generated ideal of A is principal, generated by an idempotent element. If e is an idempotent, then one has

$$A = (e) \oplus (1-e).$$

Indeed, if $x \in A$ then $x = xe + x(1-e)$ so $A = (e) + (1-e)$. Furthermore, the intersection $(e) \cap (1-e)$ is 0 because if $x = ae = b(1-e)$ for some $a, b \in A$, then $x = ae = ae^2 = b(1-e)e = 0$. This shows (3).

(3) $\Rightarrow$ (1) :

We will need the following proposition:

Proposition 4.0.1. *Let M be an A-module. The following are equivalent:*

(i) M is flat A-module.
(ii) For every finitely generated ideal $I \subset A$, the induced map $I \otimes M \to A \otimes M \simeq M$ is injective.

Before proving the Proposition, we need some lemmas:

Lemma 4.0.2. *Let M, N be A-modules. Let $x_1, ..., x_n \in M$ and $y_1, ..., y_n \in N$.*

(i) Assume that $\sum_{i=1}^n x_i \otimes y_i \neq 0$ in $M \otimes N$. If $M' \subset M$ and $N' \subset N$ are submodules such that $x_1, ..., x_n \in M'$ and $y_1, ..., y_n \in N'$, then one has $\sum_{i=1}^n x_i \otimes y_i \neq 0$ in $M' \otimes N'$.
(ii) Assume that $\sum_{i=1}^n x_i \otimes y_i = 0$ in $M \otimes N$. Then there exists finitely generated submodules $M' \subset M$ and $N' \subset N$ such that $x_1, ..., x_n \in M'$ and $y_1, ..., y_n \in N'$ and $\sum_{i=1}^n x_i \otimes y_i = 0$ in $M' \otimes N'$.

Proof. (i) : One has the following equivalence:

$$\sum_{i=1}^{n} x_i \otimes y_i = 0 \text{ in } M \otimes N \iff \forall \text{ bilinear map } B : M \times N \to P, \text{ one has } \sum_{i=1}^{n} B(x_i, y_i) = 0$$

Indeed, this follows simply from the fact that for each bilinear map $B : M \times N \to P$, there exists an A-linear map $f : M \otimes N \to P$ such that $B(x, y) = f(x \otimes y)$.

Hence, we also have an equivalence :

$$\sum_{i=1}^{n} x_i \otimes y_i \neq 0 \text{ in } M \otimes N \iff \exists \text{ a bilinear map } B : M \times N \to P, \text{ such that } \sum_{i=1}^{n} B(x_i, y_i) \neq 0$$

Hence if $M' \subset M$ and $N' \subset N$ are as in the assumption, there exists a bilinear map $M \times N \to P$ such that $\sum_{i=1}^{n} B(x_i, y_i) \neq 0$ in P. Hence by restriction of B, we obtain a bilinear map $B : M' \times N' \to P$ such that $\sum_{i=1}^{n} B(x_i, y_i) \neq 0$ in P. Hence using again the above equivalence for M' and N', we deduce that $\sum_{i=1}^{n} x_i \otimes y_i \neq 0$ in $M' \otimes N'$. This proves (1).

(ii) : We use the construction of the tensor product $M \otimes N$. Recall by lectures that

$$M \otimes N = A^{(M \times N)}/D$$

where $A^{(M \times N)}$ is the direct sum of copies of A indexed by $M \times N$, and $D \subset A^{(M \times N)}$ is the submodule generated by the elements of the form

$$\begin{aligned}
&[x + x', y] - [x, y] - [x', y] \\
&[x, y + y'] - [x, y] - [x, y'] \\
&[ax, y] - a[x, y] \\
&[x, ay] - a[x, y].
\end{aligned}$$

for $x, x' \in M,\ y, y' \in N,\ a \in A$. Here $[x, y]$ denotes the basis vector of $A^{(M \times N)}$ corresponding to $(x, y) \in M \times N$.

We now prove the assertion. Assume that $\sum_{i=1}^{n} x_i \otimes y_i = 0$ in $M \otimes N$. This means that

$$\sum_{i=1}^{n} [x_i, y_i] \in D.$$

Hence $\sum_{i=1}^{n} [x_i, y_i]$ can be written as a finite sum of elements of $A^{(M \times N)}$ of the 4 types listed above. This finite sums involves a finite number of elements $x'_1, ..., x'_r \in M$ and $y'_1, ..., y'_s \in N$. Let $M' \subset M$ (respectively $N' \subset N$) denote the submodule generated by $x_1, ..., x_n, x'_1, ..., x'_r$ (respectively $y_1, ..., y_n, y'_1, ..., y'_s$).

Then it is clear that a similar relation is true in the module $A^{(M' \times N')}$, and this shows that $\sum_{i=1}^{n} x_i \otimes y_i = 0$ in $M' \otimes N'$. This terminates the proof of the lemma. □

Using the above lemma, we deduce the following result, which is weaker that Proposition 4.0.1:

Lemma 4.0.3. *Let M be an A-module. The following are equivalent:*

(i) M is flat A-module.

(ii) For all injective map $f : N_1 \to N_2$ of finitely generated A-modules, the map $id_M \otimes f : M \otimes N_1 \to M \otimes N_2$ is injective.

Proof. $(i) \Rightarrow (ii)$ is obvious.
$(ii) \Rightarrow (i)$: Let $f : N_1 \to N_2$ be an injective map of A-modules (we don't assume N_1, N_2 are finitely generated). Assume by way of contradiction that the map

$$id \otimes f : M \otimes N_1 \to M \otimes N_2$$

is not injective. Let $\sum_{i=1}^n x_i \otimes y_i \in M \otimes N_1$ be a <u>nonzero</u> element in the kernel of f. Hence we have

$$\sum_{i=1}^{n} x_i \otimes f(y_i) = 0$$

in $M \otimes N_2$. By part (ii) of the previous lemma, there exists a finitely generated submodule $N_2' \subset N_2$ such that $f(y_1), ..., f(y_n) \in N_2'$ and $\sum_{i=1}^n x_i \otimes f(y_i) = 0$ in $M \otimes N_2'$. Let $N_1' \subset N_1$ denote the submodule generated by $y_1, ..., y_n$. It is clear that f restricts to an injective map

$$f' : N_1' \longrightarrow N_2'$$

and hence we get a map $id_M \otimes f' : M \otimes N_1' \to M \otimes N_2'$. We have again $\sum_{i=1}^n x_i \otimes y_i \in \mathrm{Ker}(id_M \otimes f')$. By part (i) of the previous lemma, we have $\sum_{i=1}^n x_i \otimes y_i \neq 0$ in $M \otimes N_1'$. This shows that $id_M \otimes f'$ is not injective, which contradicts the assumption. This terminates the proof of the lemma. □

We now prove another weaker version of Proposition 4.0.1:

Lemma 4.0.4. *Let M be an A-module. The following are equivalent:*

(i) M is flat A-module.
(ii) For every ideal $I \subset A$, the induced map $I \otimes M \to A \otimes M$ is injective.

Proof. $(i) \Rightarrow (ii)$ is obvious.

$(ii) \Rightarrow (i)$: By Lemma 4.0.3, it suffices to show that for all injective maps $f : N' \to N$ of finitely generated A-modules, $id_M \otimes f : M \otimes N' \to M \otimes N$ is injective. We may assume that $N = A^n/D$ and $N' = D'/D$ where $D \subset D' \subset A^n$ are submodules. Write $\iota : D \to A^n$ and $\iota' : D' \to A^n$ and $f : N' \to N$ for the inclusion maps. We have a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
M \otimes D & \longrightarrow & M \otimes D' & \longrightarrow & M \otimes N' & \longrightarrow & 0 \\
\big\downarrow = & & \big\downarrow id_M \otimes \iota' & & \big\downarrow id_M \otimes f & & \\
M \otimes D & \xrightarrow{id_M \otimes \iota} & M \otimes A^n & \longrightarrow & M \otimes N & \longrightarrow & 0
\end{array}$$

Assume that both maps $id_M \otimes \iota'$ and $id_M \otimes \iota'$ are injective. Then we show that $id_M \otimes f$ is also injective. Indeed, if $x \in \mathrm{Ker}(id_M \otimes f)$, choose a preimage $y \in M \otimes D'$. Then by commutativity, $(id_M \otimes \iota')(y)$ is mapped to 0 in $M \otimes N$, so there exists $z \in M \otimes D$ such that

$$(id_M \otimes \iota')(y) = (id_M \otimes \iota)(z)$$

But then the image of z by the map $M \otimes D \to M \otimes D'$ must be y because of commutativity and injectivity of the map $id_M \otimes \iota'$ (by assumption). It follows that $x = 0$ and so $id_M \otimes f$ is injective.

Hence it suffices to show that if $D \subset A^n$ is a submodule, then $M \otimes D \to M \otimes A^n \simeq M^n$ is injective. This holds for $n = 1$ by assumption. Assume this is true for some $n \geq 1$. We then show that it holds for $n+1$. Let $D \subset A^{n+1}$ be a submodule. Let $D' \subset D$ be the set of elements of the form $(x, 0, ..., 0)$ (some $x \in A$) in D. Then D'

is the kernel of the restriction to D of the map $A^{n+1} \to A^n$, $p : (x_0, x_1, ..., x_n) \mapsto (x_1, ..., x_n)$. In particular, p yields an injective map $\iota'' : D'' := D/D' \to A^n$. We get a commutative diagram:

$$\begin{array}{ccccccccc} & & M \otimes D' & \longrightarrow & M \otimes D & \longrightarrow & M \otimes D'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_M \otimes \iota'} & & \downarrow{\scriptstyle id_M \otimes \iota} & & \downarrow{\scriptstyle id_M \otimes \iota''} & & \\ o & \longrightarrow & M & \longrightarrow & M^{n+1} & \longrightarrow & M^n & \longrightarrow & 0 \end{array}$$

The injectivity of the maps $id_M \otimes \iota'$ and $id_M \otimes \iota''$ implies the injectivity of $id_M \otimes \iota$. This terminates the proof of the lemma. □

Finally, we finish the proof of Proposition 4.0.1. Again, note that $(i) \Rightarrow (ii)$ is obvious. The proof of $(ii) \Rightarrow (i)$ is basically a combination of Lemmas 4.0.3 and 4.0.4. Indeed, let M be an A-module satisfying (ii). To show that M is flat, it suffices to show by Lemma 4.0.4 that for all ideal $I \subset A$ (not necessarily finitely generated), the induced map $I \otimes M \to A \otimes M$ is injective. Assuming this is not the case, then we can find (using the proof of Lemma 4.0.3) a finitely generated ideal $I' \subset I$ such that $I' \otimes M \to A \otimes M$ is not injective. This contradicts the assumption (ii), and proves the Proposition.

We finally can prove the implication (3) $\Rightarrow$ (1) of Exercise 3. Assume that for every finitely generated ideal $I \subset A$, there exists an ideal $J \subset A$ such that $A = I \oplus J$. Let M be any A-module. We need to show that M is flat. By Proposition 4.0.1, it suffices to show that for each finitely generated ideal $I \subset A$, the map $I \otimes M \to A \otimes M$ is injective.

Let $J \subset A$ an ideal such that $I \oplus J = A$ and let $p : A \to I$ denote the projection map with respect to this decomposition. If $\iota : I \to A$ is the natural inclusion map, we have $p \circ \iota = id_I$. Hence we deduce that the composition

$$I \otimes M \xrightarrow{\iota \otimes id_M} A \otimes M \xrightarrow{p \otimes id_M} I \otimes M$$

is again the identity map of $I \otimes M$. It follows that $\iota \otimes id_M$ is injective. This shows (3).

Exercise 4 : Let A be a ring such that for every $x \in A$, there exists $n > 1$ such that $x^n = x$. Show that:

(1) Every prime ideal of A is maximal.
(2) A is absolutely flat.

Solution:
(1) : Let $\mathfrak{p} \subset A$ be a prime ideal and $x \in A \setminus \mathfrak{p}$. There exists $n > 1$ such that $x^n = x$, thus $x(x^{n-1} - 1) = 0$. Since $x \notin \mathfrak{p}$, we deduce $x^{n-1} - 1 \in \mathfrak{p}$, which shows that $x + \mathfrak{p}$ is a unit in $A/\mathfrak{m}$ with inverse $x^{n-2} + \mathfrak{p}$. Hence $A/\mathfrak{p}$ is a field, so $\mathfrak{p}$ is maximal.

(2) : By Exercise 3, it suffices to show $I^2 = I$ for each principal ideal $I \subset A$. Let $x \in A$ and $I = (x)$. Then $I^2 = (x^2) \subset (x)$. Conversely, $x = x^n = x^2(x^{n-2}) \in (x^2)$ which shows $I^2 = I$. We deduce that A is absolutely flat.

Exercise 5 : Let A be a nonzero ring and M an A-module. Show that the following assertions are equivalent:

(1) M is a flat A-module.
(2) $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module for all prime ideal $\mathfrak{p}$.
(3) $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module for all maximal ideal $\mathfrak{m}$.

Solution:
(1) $\implies$ (2): We know by the lectures that if M is a flat A-module, then $B \otimes_A M$ is a flat B-module for any A-algebra B. In particular, $M_{\mathfrak{p}} \simeq A_{\mathfrak{p}} \otimes_A M$ is a flat $A_{\mathfrak{p}}$-algebra for all prime ideal $\mathfrak{p} \subset A$.
(2) $\implies$ (3) is obvious.
(3) $\implies$ (1): Let $f : N' \to N$ be an injective map of A-modules. We have to show that $id_M \otimes f : M \otimes_A N' \to M \otimes_A N$ is injective. For all maximal ideal $\mathfrak{m} \subset A$, there is an isomorphism

$$(M \otimes_A N)_{\mathfrak{m}} \simeq M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} N_{\mathfrak{m}}$$

Hence, by the assumption that $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module, we know that the localization at $\mathfrak{m}$ of the map $id_M \otimes f : M \otimes_A N' \to M \otimes_A N$ is injective, for all $\mathfrak{m}$. One then deduces that $id_M \otimes f : M \otimes_A N' \to M \otimes_A N$ is injective as in Ex.4 of Problem sheet 2.

5. Problem sheet 5

Exercise 1 : If $A = (A_n, \alpha_n)_n$ and $B = (B_n, \beta_n)_n$ are two inverse systems, a morphism of inverse systems $f : A \to B$ is a family of maps $f_n : A_n \to B_n$ such that the following diagram commutes for all $n \geq 0$:

$$\begin{array}{ccc} A_n & \xrightarrow{f_n} & B_n \\ \uparrow{\scriptstyle \alpha_{n+1}} & & \uparrow{\scriptstyle \beta_{n+1}} \\ A_{n+1} & \xrightarrow{f_{n+1}} & B_{n+1} \end{array}$$

(1) Show that f induces a group homomorphism $\tilde{f} : \varprojlim A_n \to \varprojlim B_n$
(2) Let $A = (A_n, \alpha_n)_n$, $B = (B_n, \beta_n)_n$ and $C = (C_n, \gamma_n)_n$ be three inverse systems and
$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$
an exact sequence (i.e the sequence for each n is exact). Then show that the sequence
$$0 \to \varprojlim A_n \xrightarrow{\tilde{f}} \varprojlim B_n \xrightarrow{\tilde{g}} \varprojlim C_n$$
is exact.
(3) Assume further that for each $n \geq 1$, the map α_n is surjective. Show that $\tilde{g}$ is surjective.
(4) Deduce the following result: Let $0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$ be an exact sequence of abelian groups, and $(G_n)_n$ a descending chain of subgroups of G. Endow G with the attached topology, and G' (resp. G'') with the topology attached to the chain $(f^{-1}(G_n))_n$ (resp. $(g(G_n))_n$). Then one has an exact sequence of completions
$$0 \to \hat{G}' \xrightarrow{\hat{f}} \hat{G} \xrightarrow{\hat{g}} \hat{G}'' \to 0$$

Solution:
(1) : Let $(x_n)_{n\geq 0} \in \varprojlim A_n$. Then the commutativity of the above diagram shows that the sequence $(f(x_n))_{n\geq 0}$ is an element of $\varprojlim B_n$. This induces a map

$$\tilde{f} : \varprojlim A_n \to \varprojlim B_n$$

which is clearly a group homomorphism.

(2) : Since $f_n : A_n \to B_n$ is injective for each $n \geq 0$, it is clear that $\tilde{f}$ is injective. We also have $\tilde{g} \circ \tilde{f} = 0$ because $g_n \circ f_n = 0$ for each $n \geq 0$. Finally, let $(y_n)_{n\geq 0} \in \varprojlim B_n$ be in the kernel of $\tilde{g}$. Hence $g_n(y_n) = 0$ for each $n \geq 0$, so we can write $y_n = f(x_n)$ for some $x_n \in A_n$. It remains to show that $(x_n)_{n\geq 0}$ is an element of $\varprojlim A_n$. We have for each $n \geq 0$:

$$f_n(x_n) = y_n = \beta_{n+1}(y_{n+1}) = \beta_{n+1}(f_{n+1}(x_{n+1})) = f_n(\alpha_{n+1}(x_{n+1}))$$

Since f_n is injective, we deduce $x_n = \alpha_{n+1}(x_{n+1})$ which shows that $(x_n)_{n\geq 0}$, hence $\mathrm{Ker}(\tilde{g}) = \mathrm{ima}(\tilde{f})$.

(3) : Let $z := (z_n)_{n\geq 0} \in \varprojlim C_n$ be an element. We construct a preimage in $\varprojlim B_n$. For each $n \geq 0$, let $y_n \in B_n$ such that $g_n(y_n) = z_n$. It is not true in general that $(y_n)_{n\geq 0} \in \varprojlim B_n$, so we need to modify y_n. We will construct a sequence (y'_n) by induction satisfying $g_n(y'_n) = z_n$ and $y'_n = \beta_{n+1}(y'_{n+1})$ for all $n \geq 0$.

Put $y'_0 := y_0$. Assume we have constructed $y'_0, ..., y'_n$. We define $y'_{n+1} \in B_{n+1}$ as follows. Note that

$$\begin{aligned} g_n(y'_n - \beta_{n+1}(y_{n+1})) &= z_n - g_n(\beta_{n+1}(y_{n+1})) \\ &= z_n - \gamma_{n+1}(g_{n+1}(y_{n+1})) \\ &= z_n - \gamma_{n+1}(z_{n+1}) \\ &= 0. \end{aligned}$$

It follows that $y'_n - \beta_{n+1}(y_{n+1}) \in \mathrm{Ker}(g_n) = \mathrm{ima}(f_n)$, so we can write

$$y'_n - \beta_{n+1}(y_{n+1}) = f_n(x_n)$$

for some $x_n \in A_n$. Since α_{n+1} is surjective, we can find $x_{n+1} \in A_{n+1}$ such that $\alpha_{n+1}(x_{n+1}) = x_n$. Then define

$$y'_{n+1} = y_{n+1} + f_{n+1}(x_{n+1}).$$

We have the relation:

$$\begin{aligned} \beta_{n+1}(y'_{n+1}) &= \beta_{n+1}(y_{n+1}) + \beta_{n+1}(f_{n+1}(x_{n+1})) \\ &= \beta_{n+1}(y_{n+1}) + f_n(\alpha_{n+1}(x_{n+1})) \\ &= \beta_{n+1}(y_{n+1}) + f_n(x_n) \\ &= y'_n. \end{aligned}$$

Hence this construction gives a sequence $y' := (y'_n)_{n\geq 0}$ which lies in $\varprojlim B_n$ and such that $\tilde{g}(y') = z$. This shows that $\tilde{g}$ is surjective.

(4) : Consider the inverse systems $(G/G_n)_n$, $(G'/f^{-1}(G'_n))_n$ and $(G''/g(G_n))_n$ where the maps are the obvious ones. We have an exact sequence of inverse systems

$$\begin{array}{ccccccccc} & & \vdots & & \vdots & & \vdots & & \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & G'/f^{-1}(G'_n) & \longrightarrow & G/G_n & \longrightarrow & G''/g(G_n) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & G'/f^{-1}(G'_{n+1}) & \longrightarrow & G/G_{n+1} & \longrightarrow & G''/g(G_{n+1}) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ & & \vdots & & \vdots & & \vdots & & \end{array}$$

The assumptions of Question (3) are satisfied in this situation, so we deduce an exact sequence:

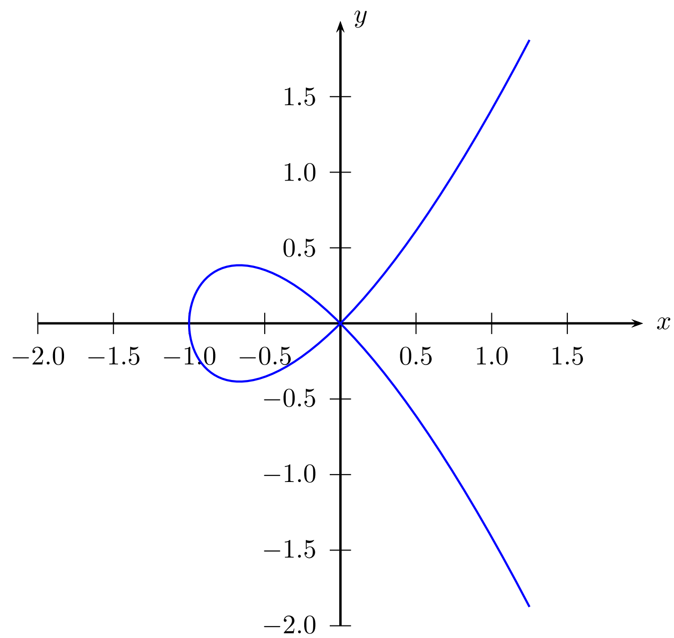
$$0 \to \varprojlim G'/f^{-1}(G'_n) \xrightarrow{\tilde{f}} \varprojlim G/G_n \xrightarrow{\tilde{g}} \varprojlim G''/g(G_n).$$

These inverse limits identify with the completions of G', G, G'' with respect to the chains of subgroups $(f^{-1}(G'_n))_n$, $(G_n)_n$, $(g(G_n))_n$. Hence we have an exact sequence:

$$0 \to \hat{G}' \xrightarrow{\hat{f}} \hat{G} \xrightarrow{\hat{g}} \hat{G}'' \to 0.$$

Exercise 2 : Let A be an integral domain and $I \subset A$ an ideal. If A is an integral domain, is the I-adic completion $\hat{A}$ an integral domain?

Solution:
Consider the polynomial $P(X,Y) = Y^2 - X^2 - X^3 \in \mathbf{C}[X,Y]$ and let $I \subset \mathbf{C}[X,Y]$ denote the ideal generated by I. If we plot the vanishing locus of P in $\mathbf{R}^2$, we get the following picture:



In a neighborhood of the $(0,0)$, the term x^3 becomes negligible in comparison to the lower order terms x^2 and y^2, hence when $(x,y) \in \mathbf{R}^2$ is close to 0, the equation $P(x,y) = 0$ is close to the equation $y^2 - x^2 = 0$, which is equivalent to $y = \pm x$. This explains the two branches of the curve around the point $(0,0)$.

Let A be the quotient ring:

$$A := \frac{\mathbf{C}[X,Y]}{(Y^2 - X^2 - X^3)}$$

It is clear that A is an integral domain. This amounts to showing that I is a prime ideal. This follows easily from the fact that the polynomial $Y^2 - X^2 - X^3$ is irreducible in the UFD $\mathbf{C}[X,Y]$.

The maximal ideals of A correspond to maximal ideals of $\mathbf{C}[X,Y]$ containing I. It is shown in Algebraic Geometry that the maximal ideals of $\mathbf{C}[X,Y]$ are all of the form $(X-a, Y-b)$ for all $(a,b) \in \mathbf{C}^2$. Hence maximal ideals of A correspond bijectively to those pairs $(a,b) \in \mathbf{C}^2$ satisfying $P(a,b) = 0$. Given the behavior of the above curve locally around $(0,0)$, we consider the ideal corresponding to the point $a = 0$, $b = 0$. Hence, let $x, y \in A$ denote the classes of X and Y respectively and consider the maximal ideal $\mathfrak{m}$ defined by

$$\mathfrak{m} := (x,y).$$

Note that the quotient $A/\mathfrak{m}$ is isomorphic to $\mathbf{C}$ by the map $Q(x,y) + \mathfrak{m} \mapsto Q(0,0)$ (where $Q \in \mathbf{C}[X,Y]$). Let $\hat{A}$ denote the $\mathfrak{m}$-adic completion of A. Consider the exact sequence of abelian groups

$$0 \to I \to \mathbf{C}[X,Y] \xrightarrow{\pi} A \to 0$$

Let $\mathfrak{m}_0 \subset \mathbf{C}[X,Y]$ be the maximal ideal $\mathfrak{m}_0 := (X,Y)$. Then we have the chain of ideals of $\mathbf{C}[X,Y]$:

$$\mathbf{C}[X,Y] \supset \mathfrak{m}_0 \supset \mathfrak{m}_0^2 \supset ...$$

which defines the $\mathfrak{m}_0$-adic topology on $\mathbf{C}[X,Y]$. The image of this chain by π is the chain of powers of $\mathfrak{m}$. Since I is a finitely generated $\mathbf{C}[X,Y]$-module, we obtain an exact sequence

$$0 \to \hat{I} \to \widehat{\mathbf{C}[X,Y]} \to \hat{A} \to 0.$$

Furthermore, since I is generated by P, multiplication by P is a surjective map of $\mathbf{C}[X,Y]$-modules $\mathbf{C}[X,Y] \to I$, hence after completion, multiplication by P induces a surjective map $\widehat{\mathbf{C}[X,Y]} \to \hat{I}$. In other words, $\hat{I}$ is generated by P as an $\widehat{\mathbf{C}[X,Y]}$-module. We have proved:

$$\hat{A} \simeq \frac{\widehat{\mathbf{C}[X,Y]}}{(P)}.$$

In Exercise 5, it is shown that the (X)-adic completion of $\mathbf{C}[X]$ is the ring of power series $\mathbf{C}[[X]]$. By following precisely the same arguments, one can show that the completion of $\mathbf{C}[X,Y]$ for the (X,Y)-adic topology is the ring

$$\widehat{\mathbf{C}[X,Y]} \simeq \mathbf{C}[[X,Y]]$$

of formal series in the variables X,Y. An element of $\mathbf{C}[[X,Y]]$ is a formal sum

$$f = \sum_{n,m\geq 0} a_{n,m} X^n Y^m$$

Multiplication is defined similarly to Exercise 5: If $f = \sum_{n,m\geq 0} a_{n,m} X^n Y^m$ and $g = \sum_{n,m\geq 0} b_{n,m} X^n Y^m$, then let fg be the power series $\sum_{n,m\geq 0} c_{n,m} X^n Y^m$ where $c_{n,m}$ is defined by

$$c_{n,m} = \sum_{(i,j)+(r,s)=(n,m)} a_{i,j} b_{r,s}$$

The sum is over the set of pairs of pairs $((i,j),(r,s))$ of non-negative integers such that $(i,j)+(r,s)=(n,m)$ (hence this is a finite sum). Similarly to Ex 5. Question (3), the units of $\mathbf{C}[X,Y]$ are the power series $f = \sum_{n,m\geq 0} a_{n,m} X^n Y^m$ such that $a_{0,0} \neq 0$.

Therefore, we conclude:

Lemma 5.0.1. *The completion of A for the $\mathfrak{m}$-adic topology is isomorphic to the ring*

$$B := \frac{\mathbf{C}[[X,Y]]}{(Y^2 - X^2 - X^3)}$$

The element $1+X$ is a unit of $\mathbf{C}[X,Y]$ because its constant term is nonzero in $\mathbf{C}$. We claim:

Lemma 5.0.2. *Let A be a ring such that $2 \in A^\times$. Let $g = \sum_{n\geq 0} b_n X^n \in A[[X]]$. Assume that $b_0 \in A^\times$ and is a square in A. Then there exists $f \in A[[X]]$ such that $f^2 = g$.*

Proof. we construct $f = \sum_{n\geq 0} a_n X^n$ inductively. Since b_0 is a square, let $a_0 \in A^\times$ be an element such that $a_0^2 = b_0$. Assume that we have defined $a_0, ..., a_n$. Then define:

$$a_{n+1} = \frac{1}{2a_0}\left(b_{n+1} - \sum_{k=1}^{n} a_k a_{n+1-k}\right)$$

Note that a_{n+1} is well-defined because $2a_0$ is a unit of A. Then it is clear that $f^2 = g$. □

For example, the element $1 + X \in \mathbf{C}[[X]]$ is a unit and its constant term is a square in $\mathbf{C}$. Therefore, there exists $F \in \mathbf{C}[[X]]$ such that $F^2 = 1 + X$.

Denote by $x, y \in B$ the classes modulo (P) of X, Y respectively. Denote also by $f \in B$ the class of F. We have the relation

$$y^2 = x^2(1 + x) = x^2 f^2 = (xf)^2$$

In other words, we have the relation $(y - xf)(y + xf) = 0$ in the ring B. It is clear that none of the elements $y \pm xf$ is zero, because otherwise, the element $Y \pm FX$ would be divisible by $Y^2 - X^2 - X^3$ in the ring $\mathbf{C}[[X, Y]]$. This is a contradiction because if $Y \pm FX = (Y^2 - X^2 - X^3)Q(X, Y)$ for some $Q \in \mathbf{C}[[X, Y]]$, then by replacing X by 0 we get that $Y = Y^2 Q(0, Y)$, which is clearly impossible. Hence we have seen that the completion $\hat{A}$ is not an integral domain even though A is an integral domain.

Actually, one can simplify further the expression of the ring $\hat{A}$ as follows. Note that $(Y - XF)(Y + XF) = Y^2 - X^2F^2 = Y^2 - X^2 - X^3$. One can show that there is an isomorphism

$$\frac{\mathbf{C}[[X, Y]]}{(XY)} \simeq \frac{\mathbf{C}[[X, Y]]}{(Y - XF)(Y + XF)} = \frac{\mathbf{C}[[X, Y]]}{(Y^2 - X^2 - X^3)}$$

defined by mapping $h(X, Y)$ to $h(Y - FX, Y + FX)$.

By repeating all previous arguments, one recognizes that $\frac{\mathbf{C}[[X,Y]]}{(XY)}$ is the completion of the ring $C := \frac{\mathbf{C}[X,Y]}{(XY)}$ with respect to the $\mathfrak{m}_1$-adic topology, where $\mathfrak{m}_1 = (x, y)$ (again, x, y denote the classes of X, Y). The representation in $\mathbf{R}^2$ of the equation $xy = 0$ is simply a cross : Two line intersecting perpendicularly at $(0, 0)$. The above isomorphism says that the above curve has a singularity at the point $(0, 0)$ which "looks like" a cross.

Exercise 3 : Let A be a Noetherian ring and $I \subset A$ an ideal. Show that $I \subset J(A)$ if and only if every maximal ideal of A is closed with respect to the I-adic topology of A.

Solution:
$(\Rightarrow)$: Assume $I \subset J(A)$ and let $\mathfrak{m} \subset A$ be a maximal ideal. We must show that $A \setminus \mathfrak{m}$ is open with respect to the I-adic topology. Let $x \in A \setminus \mathfrak{m}$. Then the set $x + I$ is an open neighborhood of x and is contained in $A \setminus \mathfrak{m}$. Indeed, if $x + I$ would intersect $\mathfrak{m}$, it would imply a relation $x + y = z$ with $y \in I$ and $z \in \mathfrak{m}$, thus $x = z - y \in \mathfrak{m}$, which is a contradiction.

$(\Leftarrow)$: Assume that every maximal ideal is closed for the I-adic topolgy and assume for a contradiction that there exists $x \in I$ which is not contained in a maximal ideal $\mathfrak{m}$. Since $A\setminus$ is open, there exists $n \geq 1$ such that $x + I^n \subset A \setminus \mathfrak{m}$. Since $x^n \notin \mathfrak{m}$

(because $\mathfrak{m}$ is a prime ideal), the ideal $\mathfrak{m} + (x^{n-1})$ is strictly larger than $\mathfrak{m}$ hence $\mathfrak{m} + (x^{n-1}) = A$ by maximality. We deduce that we can write $1 = ax^{n-1} + y$ with $y \in \mathfrak{m}$. But then

$$x - ax^n = xy$$

is an element of $x + I^n$ which lies in $\mathfrak{m}$, which is a contradiction. This proves the assertion.

Exercise 4 : Let A be a ring and $I \subset A$ an ideal. Show that the completion $\hat{A}$ is a flat A-algebra.

Solution:

Using Lemma 0.0.3 of the Solutions to Problem sheet 4, Exercise 3, it suffices to show that for each injective map $M' \to M$ of finitely generated A-modules, the induced map

$$\hat{A} \otimes_A M' \to \hat{A} \otimes_A M$$

is injective. Let $\hat{M}$ and $\hat{M}'$ be the I-adic completions of M and M'. By the Artin-Rees lemma, the topology induced on M' from the I-adic topology on M coincides with the I-adic topology of M'. Hence we may apply Exercise 1 (4) to show that

$$\hat{M}' \to \hat{M}$$

is again injective. Since M, M' are finitely generated, we have $\hat{A} \otimes_A M \simeq \hat{M}$. Hence it follows that $\hat{A} \otimes_A M' \to \hat{A} \otimes_A M$ is injective, which proves that $\hat{A}$ is a flat A-algebra.

Exercise 5 : Let A be a ring. Denote by $A[[X]]$ the ring of power series with coefficients in A. An element $f \in A[[X]]$ is a formal sum $f = \sum_{n\geq 0} a_n X^n$. Addition and multiplication are defined as follows:

$$\sum_{n\geq 0} a_n X^n + \sum_{n\geq 0} b_n X^n = \sum_{n\geq 0} (a_n + b_n) X^n$$

$$\sum_{n\geq 0} a_n X^n \cdot \sum_{n\geq 0} b_n X^n = \sum_{n\geq 0} c_n X^n \quad \text{with } c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

(1) Show that $A[[X]]$ is a ring.
(2) Determine the group of units of $A[[X]]$.
(3) Show that $A[[X]]$ is isomorphic to the (X)-adic completion of $A[X]$.

Solution:
(1) : It is clear that $(A[[X]], +)$ is an abelian group. We show that multiplication is associative: Let $f = \sum_{n\geq 0} a_n X^n$, $g = \sum_{n\geq 0} b_n X^n$ and $h = \sum_{n\geq 0} c_n X^n$ three elements of $A[[X]]$. Write $(f \cdot g) \cdot h = \sum_{n\geq 0} d_n X^n$. We have:

$$\begin{aligned} d_n &= \sum_{k=0}^{n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) c_{n-k} \\ &= \sum_{r+s+t=n} a_r b_s c_t \end{aligned}$$

where the sum is over all nonnegative $r, s, t \geq 0$ such that $r + s + t = n$. This expression is clearly symmetric, so we deduce that $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

Finally, it is easy to see that multiplication is distributive with respect to addition and that the element

$$1 + 0X + 0X^2 + ...$$

(denoted simply by 1) the an identity element for multiplication.

(2) : We claim that one has the following description:

$$A[[X]]^\times = \left\{ \sum_{n\geq 0} a_n X^n,\ a_0 \in A^\times \right\}.$$

It is clear that $\sum_{n\geq 0} a_n X^n \mapsto a_0$ defines a ring homomorphism $A[[X]] \to A$, hence sends a unit to a unit. This proves the inclusion "$\subset$". Now, let $f = \sum_{n\geq 0} a_n X^n$ be an element of $A[[X]]$ such that $a_0 \in A^\times$. We construct an inverse to f. Define $b_0 := a_0^{-1}$ and by induction:

$$b_n := -\frac{1}{a_0} \sum_{i=1}^{n} a_i b_{n-i}$$

It is clear by definition that $fg = 1$. Thus f is a unit in $A[[X]]$.

(3) : Let $\widehat{A[X]}$ denote the completion of $A[X]$ with respect to the (X)-adic topology. We know that

$$\widehat{A[X]} \simeq \varprojlim A[X]/(X^n)$$

Define a map $\phi : A[[X]] \to \widehat{A[X]}$ by mapping $f = \sum_{n\geq 0} a_n X^n$ to the sequence $(P_n + (X^n))_{n\geq 1}$ where

$$P_n = \sum_{k=0}^{n-1} a_k X^k$$

It is clear that $(P_n)_n \in \widehat{A[X]}$. The map ϕ is clearly a ring homomorphism. It is injective because if $P_n \in (X^n)$ for each $n \geq 1$, then we deduce that $a_0 = ... = a_n = 0$ for all $n \geq 0$, so $f = 0$. Finally, we prove surjectivity: Let $x := (Q_n + (X^n))_{n\geq 1}$ be a sequence in $\varprojlim A[X]/(X^n)$. By definition, the difference $Q_{n+1} - Q_n$ must be divisible by X^n. This shows that for each $n \geq 0$, the n-th coefficient of Q_m is the same for all $m \geq n$. Denote by $a_n \in A$ this coefficient. Then it is clear that $f = \sum_{n\geq 0} a_n X^n$ satisfies $\phi(f) = x$. This shows that ϕ is an isomorphism.