Supplement and solutions on Matsumura's Commutative Ring Theory

Byeongsu Yu

July 4, 2021

Abstract

This solution heavily depends on the textbook itself and [2]. I verified all the writings in this document, however, I do not claim (and should not claim) any originality on these solutions. Please use it at your own risk.

Contents

Disclaimer: Ex 14.6 is missed since it is nothing but just a proof from an article [5]. Also, Ex. 18.2, Ex. 23.3 were missed since I don't know. Also, I admit that I did not carefully go over the section 30.

1 Ideals

1. Let $b \in A$ such that $ab \cong 1$ in A/I. Then, $ab = 1 + c$ for some $c \in I$. Since c is nilpotent, $ab = 1 + c$ is unit; thus there exists $d \in A$ such that $abd = 1$. So a is unit, whose inverse is bd. (If $c^n = 0$, then $d = 1 + (-c) + (-c)^2 + \cdots (-c)^{n-1}$.)

2. Ideals of product ring is product of ideals in each ring. Let $I = I_1 \times \cdots \times I_n$ be an ideal of $A = \prod_{i=1}^n A_i$. Then, $A/I = \prod_{i=1}^n A_i/I_i$. Suppose that two of $\{I_i\}_{i=1}^n$ are proper, for example, $I_1 \neq A_1$ and $I_2 \neq A_2$. Then, A/I contains $aa = (0, a, \cdots)$ and $bb = (b, 0, \cdots)$ for some nonzero a and b, hence $aa \cdot bb = 0$. This implies that A/I is not integral domain. Thus, if I is prime, then only one summand is proper. So we may assume that $I = (\prod_{j\neq i}^n A_j) \times I_i$. Then $A/I \cong A_i/I_i$, so I is prime if and only if I_i is prime.

3. (a) Let $I = \ker f$. Then $B \cong A/I$. Thus, $V(I) \cong \mathrm{Spec}B$, which implies all maximal ideals of B has its preimage in A. Thus, if $x \in \mathrm{rad}A$, then x in all maximal ideals containing I. Thus, $f(x)$ is all maximal ideals of B, which implies $f(\mathrm{rad}A) \subseteq \mathrm{rad}B$.

   Counter example: $A = \mathbb{Z}, B = \mathbb{Z}/4\mathbb{Z}$. Then, $\mathrm{rad}A = 0, \mathrm{rad}B = (2)$.

   (b) If A is semilocal, let $m_1, \cdots, m_n$ are maximal ideals. Suppose that if $1 \le i \le s$ for some $s \le n$, then $m_i \supseteq I$. Otherwise, $m_i \not\supseteq I$. Then, let $y \in \mathrm{rad}B$. By surjectivity, $\exists x \in A$ such that $f(x) = y$. Thus, $x \in \bigcap_{i=1}^s m_i$. Then, x is a sum of products of form $x_1 \cdots x_s$ such that $x_i \in m_i$ for each i.

   Now, $I + m_j = A$ if $j > s$, thus let $1 = a_i + b_i$ where $a_i \in m_i$ and $b_i \in I$ for each $s + 1 \le j \le n$. Then, $x_1 \cdots x_s = x_1 \cdots x_s a_{s+1} \cdots a_n + b$ for some $b \in I$. Thus, $x \in \prod_{i=1}^n m_i + I$. Let $x = x' + b$ where $x' \in \prod_{i=1}^n m_i$ and $b \in I$. Then $f(x) = f(x')$. Thus, $f(\mathrm{rad}A) \supseteq \mathrm{rad}B$.

4. Let A be UFD. Take x be an irreducible element. Then by definition, $ab \in (x)$ implies $ab = cx$ for some c. Now take unique factorization $a = a_1 \cdots a_n, b = b_1 \cdots b_m, c = c_1 \cdots c_r$, where each a_i, b_i, c_i are prime element. By uniqueness of factorization, $a_1 \cdots a_n b_1 \cdots b_m = c_1 \cdots c_r x$, thus by definition of UFD, $x = a_i$ or b_i for some i. Thus, $a \in (x)$ or $b \in (x)$. This implies (x) is prime. Moreover, let $(a_1) \subseteq (a_2) \subseteq \cdots$ be an ascending chain of principal ideals. Let $a_1 = p_1^{i_1} \cdots p_n^{i_n}$. Then, $a_1 \in a_i$ implies $a_i = p_1^{i'_1} \cdots p_n^{i'_n}$ for $i_j < i'_j$. Thus, this sequence stabilizes after finitely many steps.

   Conversely, the ascending chain condition implies that every nonzero nonunit can be expressible as product of irreducibles; to see this, suppose x cannot have such product. Then $x = ab$ for a, b neither irreducible nor unit. Then either y and z also cannot have such product. By applying the same argument, we have infinite ascending chain of principal ideals, contradiction. Then, since irreducibles are prime, using the argument in the book p.5, it has a unique factorization.

5. The fact that $\bigcap_\lambda P_\lambda$ is an ideal is clear. To see it is prime, let $xy \in \bigcap_\lambda P_\lambda$ but both x and y are not in the intersection. Then, $x \in P_{\lambda_1}$ and $y \in P_{\lambda_2}$. Since it is totally ordered, we may assume that $P_{\lambda_1} \supseteq P_{\lambda_2}$ without loss of generality. Then, there exists P_{λ_1} which does not have x and P_{λ_2} which does not have y. By the total order, without loss of generality we may assume $P_{\lambda_1} \supseteq P_{\lambda_2}$, thus, P_{λ_2} does not have x too. Hence it does not have xy by prime property. This implies $xy \notin \bigcap_\lambda P_\lambda$, contradiction. Thus at least one of x or y is in the intersection. Hence it is prime.

   For the second statement, let $P := \bigcap_{I \subseteq P_\lambda} P_\lambda$. We claim that it is also a prime ideal containing I and it is the minimal element. Ideal is clear. Since the set of all prime ideals containing I is still totally ordered, P is prime by the first statement. Now, if there is a prime ideal contained in P, then it should included in the definition of P. Thus it is minimal.

6. Do induction. If $n = 1$, done. Suppose $n \geq 2$. By inductive hypothsis, we can choose $x_i \in I \setminus \bigcup_{j \neq i}^n P_i$. If one of x_i is not in P_i, done. Otherwise, let $x = x_1 \cdots x_{n-1} + x_n$. We claim it is not in any P_i. First of all, if $x \in P_i$ for $i < n$, then since $x_i \in P_i$, $x_n \in P_i$, contradicting the construction of x_n. If $x \in P_n$, then $x_1 \cdots x_{n-1} \in P_n$. If $n = 2$, $x = x_1 + x_2$, thus $x_1 \in P_2$, contradiction. If $n \geq 2$, since P_n is prime, one of x_i with $1 \leq i \leq n-1$ should be in P_n, contradiction.

2 Modules

In the proof of Theorem 2.5, by tensoring $A/\mathfrak{m}$, we get

$$F \otimes A/\mathfrak{m} \cong (A/\mathfrak{m})^n$$

and

$$\psi(M) \otimes A/\mathfrak{m} \oplus K \otimes A/\mathfrak{m} \cong \psi(M) \otimes A/\mathfrak{m} \oplus K \otimes A/\mathfrak{m} \cong M/\mathfrak{m}M \oplus K/\mathfrak{m}M$$

Lastly, since F and M has the same cardinality of minimal bases, by tensoring $A/\mathfrak{m}$, $F/\mathfrak{m}F \cong M/\mathfrak{m}$ as a k-vector spaces. Thus,

$$M/\mathfrak{m} \cong F \otimes A/\mathfrak{m} \cong M/\mathfrak{m}M \oplus K/\mathfrak{m}M$$

which implies $K = \mathfrak{m}K$.

In the proof of Lemma 2, p.11, the meaning of "in view of what we have seen above" is came from the condition $a_i \notin \sum_{j \neq i} Aa_j$. This shows $1 - c_{ii}$ and c_{ij} are not units.

1. Let $M = I$. Then, by NAK with $M = IM$, we have $a \in A$ such that $a \equiv 1 \mod I$ and $aI = 0$. Thus let $a = 1 - e$ for some $e \in I$. Then, $(1-e)I = 0$ implies $eI = I$. Also, since $e \in I$, $Ae \subseteq I$. Conversely, if $f \in I$, then $(1-e)f = 0$ implies $f = ef \in Ae$. Hence, $Ae = I$. Thus I is generated by e. Moreover, $e(1-e) = 0$ implies $e^2 = e$.

2. If $x \in \operatorname{ann}(M/IM)$, then $xM \subseteq IM$. Thus as a map $x : M \to M$, theorem 2.1 gives $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ as a map $M \to M$. Hence, $(x^n + y)M$ where $y = a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in I$. Thus, $(x^n + y) - y \in \operatorname{ann}(M) + I$, therefore $x \in \sqrt{\operatorname{ann}(M) + I}$. Conversely, if $x \in \operatorname{ann}(M) + I$, then $x - y \in \operatorname{ann} M$, hence $(x-y)M = 0$ implies $xM = yM \subseteq IM$. Thus, $x \in \operatorname{ann}(M/IM)$.

3. Second isomorphism theorem of module gives $(M+N)/N \cong M/(M \cap N)$. Since $M + N$ is finite, $(M+N)/N$ is finite, therefore $M/(M \cap N)$ is finite, and since $M \cap N$ is finite, M is finite. Thus, N is finite.

4. (a) For the first question, let $\mathfrak{m}$ be a maximal ideal of A, and let $\phi : A^m \to A^n$ be an isomorphism as A-module. Then, $1 \otimes \phi : (A/\mathfrak{m}) \bigotimes_A A^m \to (A/\mathfrak{m}) \bigotimes_A A^n$ is also an isomorphism as A-module. If we let $k = A/\mathfrak{m}$, a residue field, then $(A/\mathfrak{m}) \bigotimes_A A^m \cong (A/\mathfrak{m})^m = \bigoplus_{i=1}^m k \cong k^m$ and by the same argument $(A/\mathfrak{m}) \bigotimes_A A^n \cong k^n$. And we already know that $k^n \cong k^m$ as a vector space if and only if $n = m$, using argument on the basis.

(b) Assume $m = r+1$. Then, from the given condition that $(r+1)\times(r+1)$ minor exists, $n \geq m$. Suppose m column vectors are linearly independent. Then, we may find m rows of C whose minor is nonvanishing, from the definition of the rank as the largest k such that there is a nonzero $k\times k$ minor. This contradicts to the fact that all $m \times m$ minor vanishes. So m columns should be linearly dependent.

Now, suppose $\phi : A^m \to A^n$ be the isomorphism. Then we can represent ϕ as a $n\times m$ matrix. If $n > m$, at most m rows are linearly independent since other minors do not exists; thus n rows of ϕ are linearly dependent. Hence, we have a nonzero element b in A^m such that $\phi(b) = 0$. This implies ϕ has a nonzero kernel, contradiction. Thus, $n \leq m$. Do the same argument on $A^n \to A^m$ we have the desired answer.

(c) Suppose $B = \{v_1, \cdots, v_n\}$ be a minimal generator of $A^n = \bigoplus_{i=1}^n Ae_i$. (From the standard basis $\{e_i\}_{i=1}^n$, we knows that B has cardinality n.) Then, each $v_i = \sum_{j=1}^n a_{ij}e_i$ for some a_{ij}, by construction of A^n. Thus, by theorem 2.3.(iii), $A = (a_{ij})$ is an invertible matrix. And observes that each column matrix is nothing but v_i.

5. (a) Let $\alpha : F \to L$ and $\beta : F' \to N$ be a surjection from free modules F and F'. Then,

$$\begin{tikzcd} 0 \arrow[r] \arrow[d] & F \arrow[r] \arrow[d] & F\oplus F' \arrow[r] \arrow[d] & F' \arrow[r] \arrow[d] & 0 \arrow[d] \\ 0 \arrow[r] & L \arrow[r] & M \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

and all four maps except $F \otimes F' \to M$ are surjection. (The map $F\otimes F' \to M$ determined by Horseshoe lemma in Homological algebra, since we may regard α and β be a map inside of a projective resolution of each L and N.) Then, five lemma gives $F\oplus F' \to M$ is surjective. Hence, M has finite presentation.

(b) Again, let $\alpha : F \to L$ and $\beta : F' \to M$ be surjective maps with canonical embedding, i.e., sending canonical basis to set of generators. Then, we can induce $\phi : F \to F'$ as follow; since $g : L \to M$ is injective, for each generator ξ_j of L, if $g(\xi_j) = \sum_{i=1}^q a_i\omega_i$ for some $a_i \in A$ and generating set $\{\omega_i\}_{i=1}^q$ of M, we let $\phi(e_j) = (a_1, \cdots, a_q)$. So we may have

$$\begin{tikzcd} 0 \arrow[r] \arrow[d] & F \arrow[r] \arrow[d] & F' \arrow[d] \\ 0 \arrow[r] & L \arrow[r] & M \end{tikzcd}$$

which is a commuting diagram. Now, take cokernel of ϕ, then we have a commuting diagram of an exact sequence

$$\begin{tikzcd} 0 \arrow[r] \arrow[d] & F \arrow[r, "\phi"] \arrow[d] & F' \arrow[r] \arrow[d] & \mathrm{coker}\phi \arrow[r] \arrow[d] & 0 \arrow[d] \\ 0 \arrow[r] & L \arrow[r] & M \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

where coker$\phi \to N$ is defined by $(a_1, \cdots, a_q)+\phi(F) \mapsto \sum_{i=1}^q a_i f(\omega_i)$ where f is the map $M \to N$. This is well-defined, since if $(a_1, \cdots, a_q) + \phi(F) = (a_1', \cdots, a_q') + \phi(F)$, then $(a_1, \cdots, a_q) + b = (a_1', \cdots, a_q')$ for some $b \in \phi(F)$, thus sending b through $F' \to M \to N$ is zero, therefore both $(a_1, \cdots, a_q)$ and $(a_1', \cdots, a_q')$ are sent to $\sum_{i=1}^q a_i f(\omega_i)$.

Now apply five lemma again to conclude that coker$\phi \to N$ is surjection, therefore $F' \to$ coker$\phi \to N$ is composition of surjection, thus surjection. Thus N is finitely presented.

3 Chain Conditions

3.1.(i): if $n_2 \in N_2$, then $n_2 + N_2 \cap M' = n_1 + N_1 \cap M'$ from $\phi(N_1) = \phi(N_2$, thus $n := n_2 - n_1 \in N_2 \cap M' = N_1 \cap M'$ implies $n_2 = n + n_1 \in N_1$. Hence, $N_2 \subset N_1$, which implies $N_2 = N_1$.

(ii): Given ascending (or descending) chain M_i, take n_1 such that $M_i \cap M'$ stabilizes from Noetherian (or Artinian) of M', and take n_2 such that $M_i/M_i \cap M'$ stabilizes from Noetherian (or Artinian) of $M'' \cong M/M'$. Then for $n > \max_{i=1,2} n_i$, the assumption of (i) holds.

(iii) Use induction on $0 \to A \to A^n \to A^{n-1} \to 0$.

In the proof of theorem 3.2, NAK can be applied as a contrapositive of the corollary in this textbook. Also, $M/\mathfrak{p}_i$ is finite dimensional, since M and $M\mathfrak{p}_i$ are Artinian module, and every vector space with infinite dimension does not have Artinian property.

For theorem 3.7, (ii), IB where I is an ideal of A is actually a right ideal of B. Also, for (iii), IB has two sided ideal structure since for any $ab \in IB$ and $c \in B$, $cab = acb = a(cb)$ since $I \subset A \subset Z(B)$, the center of B.

1. Let $\phi : A \to \oplus_{i=1}^n A/I_i$ as $a \mapsto (\overline{a}, \cdots, \overline{a})$. Then, $\ker \phi = 0$, since $\ker \phi = \bigcap_i I_i$. Thus, $A \cong \phi(A)$ as an A-module. Since direct sum of Noetherian modules are also Noetherian, A is a Noetherian A-module, which implies A is Noetherian ring since all submodules of A are just all ideals.

2. Let $\pi_A : A \times_C B \to A$, $\pi_B : A \times_C B \to B$ be a natural projection. First of all, these are surjective; to see this, let $a \in A$. Then, for $f(a) \in C$, $\exists b \in B$ such that $f(a) = g(b)$ by surjectivity of g. Thus, $(a, b) \in A \times_C B$, which implies $\pi_A(a, b) = a$. Likewise, π_B is surjective by surjectivity of f. Then, think $\ker \pi_A$ and $\ker \pi_B$. We claim that $\ker \pi_A \cap \ker \pi_B = (0)$. To see this, if $(a, b) \in \ker \pi_A \cap \ker \pi_B$, then $\pi_A(a, b) = a = 0$ and $\pi_B(a, b) = b = 0$, thus $(a, b) = (0, 0)$. Moreover, $A \times_C B/\ker \pi_A \cong A$ and $A \times_C B/\ker \pi_B \cong B$ are Noetherian. Thus, by 3.1, $A \times_C B$ is Noetherian.

3. Let I be a nonzero ideal. Then, $I \subset \mathfrak{m} = (m)$. Since I is nonzero, there exist $n \in \mathbb{N}$ such that $\mathfrak{m}^n \supseteq I$ but $\mathfrak{m}^{n+1} \not\supseteq I$. To see this, first of all, when $n = 1$, $I \subset \mathfrak{m}$, done. For $n = 2$, there are two possible cases, whether $I \subset \mathfrak{m}^2$ or not. If I is inside of $\mathfrak{m}^2$, increase n. Otherwise, set $n = 2$. By this procedure, if this procedure does not stop at finitely many time, it means that I is contained in all powers of $\mathfrak{m}$, which implies $I = 0$, contradiction.

   Now, from $\mathfrak{m}^{n+1} \not\supseteq I$, let $a \in I \setminus \mathfrak{m}^{n+1}$. If such a does not exists, then $I \setminus \mathfrak{m}^{n+1} = \emptyset$ which implies $I \cap \mathfrak{m}^{n+1} = I$, thus $I \subset \mathfrak{m}^{n+1}$,contradicting the assumption that $\mathfrak{m}^{n+1} \not\supseteq I$. Then, $a \in \mathfrak{m}^n$, thus $a = rm^n$. Now $r \in A \setminus \mathfrak{m}$, otherwise $a \in \mathfrak{m}^{n+1}$, contradiction. Since A is local, r is unit, thus $(a) = (m^n)$. This implies $(m^n) \supseteq I$. Thus, by assumption, $(m^n) = I$.

   Hence, every ideal I is finitely generated since it is power of the maximal ideal, thus it is Noetherian.

4. Since $II^{-1} = A$, thus $\exists$ finitely many $x_i \in I$ and $y_i \in I^{-1}$ such that $1 = \sum_{i=1}^n x_i y_i$. Now we claim that $I = \sum x_i A$. To see this, since I is A-submodule, $I \supseteq \sum x_i A$ is clear. Conversely, for any $x \in I$, $x = x \cdot 1 = \sum_{i=1}^n x \cdot x_i y_i$. Thus, x is sum of $x x_i y_i = (x y_i) x_i$. Since $x \in I$, $y_i \in I^{-1}$, $x y_i \in A$ for any i, thus $(x y_i) x_i \in \sum x_i A$ therefore $x \in \sum x_i A$.

5. Let I be an ideal of A. Since $A \subset K$, definitely I is a A-submodule of K, and I is definitely fractional ideal since for any $a \in A \subset K$, $aI \subset A$. Now suppose I is invertible. Then, by 3.4, I is finitely generated, say $I = (a_1, \cdots, a_n) \subset A$. Now we claim that $I^{-1} := (1/a)A$, where $a = \text{h.c.f}\{a_1, \cdots, a_n\}$. To see this, first of all, definitely $a_i/a \in A$, thus $1/a \in I^{-1}$. Conversely, if $b/c \in I^{-1}$, where b and c are coprime, then $a_i b/c \in A$ for all i implies $a_i/c \in A$ for all i, thus c divides a, hence $a = cr$ for some $r \in A$, thus $b/c = br/cr = br/a \in (1/a)A$. Now,

   $$II^{-1} = (a_1/a, \cdots, a_n/a) = A.$$

   by invertibility of I. Thus, there exists $b_i \in A$ such that $1 = \sum_{i=1}^n (b_i a_i)/a$. Thus, $a \in I$. Since $a_i/a \in A$, this implies $(a) \supseteq I$. Thus, $I = (a)$, which implies that I is principal.

6. Suppose $\ker \phi \neq 0$. Let $I_n = \{a \in A : \phi^n(a) = 0\}$ and $I_0 = 0$. Then, $I_1 = \ker \phi$. We claim that for each $i \geq 0$, $I_{i+1} \supsetneq I_i$. For $i = 0$, it holds by the given assumption. For $i > 0$, suppose it holds for all $0 \leq j < i$. Then, $I_i \neq 0$. We claim that for any $a \in I_i \setminus I_{i-1}$, $\phi^{-1}(a) \notin I_i$. Suppose there is $b \in I_i$ such that $\phi(b) = a$. Then, $0 \neq \phi^{i-1}(a) = \phi^i(b) = 0$, contradiction. Thus, $I_{i+1} \supsetneq I_i$ since $b \in I_{i+1}$, done.

   Thus, $\{I_i\}_{i=0}^{\infty}$ form an infinite ascending chain of ideals, contradicting the fact that A is Noetherian. Hence, ϕ is injective. Thus, ϕ is bijective, meaning that it is automorphism of A.

7. Let M be a finite A-module. Then we may assume that $M = \sum_{i=1}^{n} A\omega_i$ for some $\omega_i \in M, n \in \mathbb{N}$. Then, we have a map $A^n \to M$ by $(a_1, \cdots, a_n) \mapsto \sum_{i=1}^{n} a_i\omega_i$. This is surjective by construction, thus

$$0 \to \ker\phi \to A^n \to M \to 0$$

is a short exact sequence. Since $\ker\phi$ is a submodule of A^n, which is still Noetherian since it is a submodule of a direct sum of Noetherian module A, $\ker\phi$ is finitely generated, say $\ker\phi = \sum_{i=1}^{m} A\zeta_i$ for some $\zeta_i \in A^n$. Then, we can have a map $\varphi : A^m \to \ker\phi$ by sending $(a_1, \cdots, a_m)$ into $\sum_{i=1}^{m} a_i\zeta_i$. This is surjective. By identifying $\ker\phi$ as a submodule of A^n, this induces a sequence

$$A^m \xrightarrow{\varphi} A^n \xrightarrow{\phi} M \to 0.$$

We claim that it is exact. Notes that $\operatorname{Im}\varphi = \ker\phi$, and $\operatorname{Im}\phi = M$, which is a kernel of the zero map $M \to 0$. Thus, it is exact. Hence, M is finitely presented.

Conversely, if A is not Noetherian, then there is an ideal I which is not finitely generated. Let $M = A/I$. Then, we have a natural exact sequence

$$0 \to I \to A \to A/I = M \to 0.$$

And A is finitely generated. Thus, contrapositive of theorem 2.6 says that since I is not finitely generated, M is not finitely presented.

4 Localisation and Spec of a ring

For Corollary 3 in p.24, take $B = A_S$. Corollary 4 is special case of corollary 3. If $f : A \to B$, then ${}^a f : \operatorname{Spec} B \to \operatorname{Spec} A$.

In the proof of theorem 4.10 (ii), you can choose suitable $D(a)$ by (i). Also, the meaning of "applying (i) with $r = 0$" implies that take U_0 for K, then $\mathfrak{p} \in U_0$, thus $V = U_0$ is an open neighborhood of $\mathfrak{p}$ such that $K_{\mathfrak{q}} = 0$ for all $\mathfrak{q} \in V$.

1. Let I be primary. Then, suppose $xy \in \sqrt{I}$. This implies $x^n y^n \in I$ for some $n \in \mathbb{N}$. Since I is primary, $x^n \in I$ or $y^{nm} \in I$ for some $m > 0$. Thus, $x \in \sqrt{I}$ or $y \in \sqrt{I}$ by definition of radical. Thus, $\sqrt{I}$ is prime.

   Now suppose $A \supsetneq I \supseteq \mathfrak{m}^v$. Then, $\sqrt{I} \supseteq \sqrt{\mathfrak{m}^v} = \mathfrak{m}$ implies $\sqrt{I} = \mathfrak{m}$. This implies $\mathfrak{m} \supseteq I \supseteq \mathfrak{m}^v$. Now suppose $xy \in I$ but $x \notin I$. Since $I \subseteq \mathfrak{m}$, there are two cases.

   Case 1: If $x \notin \mathfrak{m}$, then $y \in \mathfrak{m}$, thus $y^v \in I$.

   Case 2: If $x \in \mathfrak{m} \setminus I$, then there are two cases; if $y \notin \mathfrak{m}$, then $x^v \in I$ implies that xy satisfies primary condition. If $y \in \mathfrak{m}$, then still $y^v \in I$, thus xy satisfies primary condition.

   Hence, in any case, I satisfies the condition (2) of the definition of primary ideal.

2. Let $a \in P^n A_P \cap A$. Then, by letting $f : A \to A_P$, $f(a) = a/1 \in P^n$. Thus, $a/1 = p^n/s$ for some $p \in P^n$ and $s \in A \setminus P$. Thus, $ta \in P^n \subset P$ for some $t \in A \setminus P$. Since $t \notin P$, this implies $a \in P$. Hence, $P^n A_P \cap A \subset P$. Moreover, if $a^n \in P^n A_P \cap A$, then $a^n \in P$ by the same argument, thus $a \in P$ since P is prime. Hence, $\sqrt{P^n A_P \cap A} \subseteq P$. Conversely, $a \in P$ implies $a^n \in P^n$, thus $f(a^n) \in P^n A_P$, therefore $a^n \in P^n A_P \cap A$, thus $P \subseteq \sqrt{P^n A_P \cap A}$. Hence, $\sqrt{P^n A_P \cap A} = P$.

   Now notes that $I = P^n A_P$ is an ideal containing power of maximal ideals of A_P, thus it is PA_P primary by Exercise 4.1. By the correspondence (Theorem 4.1), thus $PA_P \cap A$ is primary.

3. By Theorem 4.1, we have a one-to-one correspondence between $\operatorname{Spec}(S^{-1}A)$ and $S^{-1}X := \{\mathfrak{p} \in \operatorname{Spec}(A) : \mathfrak{p} \cap S = \emptyset\}$ given by ${}^a\phi$ (contraction) and extension of prime ideal, where let $\phi : A \to A_S$.

   To show homeomorphism, since we already knows that ${}^a\phi$ is continuous, we want to show that ${}^a\phi$ is also closed map. Let $V(\mathfrak{a})$ be closed set in $\operatorname{Spec}(S^{-1}A)$ for some ideal $\mathfrak{a}$ of $S^{-1}A$. Then,

   $${}^a\phi(V(\mathfrak{a})) = \{\mathfrak{p}^c : \mathfrak{p} \in V(\mathfrak{a})\} = \{\mathfrak{q} \in S^{-1}X : \mathfrak{q} \supseteq \phi^{-1}(\mathfrak{a})\} = V(\phi^{-1}(\mathfrak{a})) \cap S^{-1}X.$$

   Thus, if $\mathfrak{a}$ is proper, then $\phi^{-1}(\mathfrak{a})$ is also a proper ideal, thus $V(\phi^{-1}(\mathfrak{a})) \cap S^{-1}X$ is closed in $S^{-1}X$ as subspace topology. This shows that ϕ is closed map, thus homeomorphism.

4. From the section 1, we already knows that $V(I)$ and $\mathrm{Spec}(A/I)$ has one-to-one correspondence. Moreover, this correspondence is from ${}^a\phi$ where $\phi : A \to A/I$ canonical ring morphism. Thus, ${}^a\phi$ is bijective continuous, thus it suffices to show that ${}^a\phi$ is closed. To see this, for given ideal $\bar{\mathfrak{a}}$ of A/I from $\mathfrak{a} \in \mathrm{Spec}(A)$,
$$ {}^a\phi(V(\bar{\mathfrak{a}})) = \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supseteq \mathfrak{a}\} = V(\mathfrak{a}) $$
thus done.

5. Given an open covering $\{U_\lambda\}_{\lambda\in\Lambda}$, let $V(I_\lambda) = \mathrm{Spec}A \setminus U_\lambda$ for some ideal I_λ. (This is possible since all closed sets in $\mathrm{Spec}A$ are of form $V(I)$ for some ideal I.) Then,
$$ \mathrm{Spec}A = \bigcup_{\lambda\in\Lambda} U_\lambda = \bigcup_{\lambda\in\Lambda} V(I_\lambda)^c = \left(\bigcap_{\lambda\in\Lambda} V(I_\lambda)\right)^c \implies \bigcap_{\lambda\in\Lambda} V(I_\lambda) = 0 $$
by De Morgan's law. Thus, from p.24, $\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V(\sum_{\lambda\in\Lambda} I_\lambda) = 0$. So $\sum_{\lambda\in\Lambda} I_\lambda = (1)$. Hence, $1 = \sum_{j=1}^n a_j i_{\lambda_j}$ for some $n \in \mathbb{N}$, $a_j \in A$, $i_{\lambda_j} \in I_{\lambda_j}$ and $\lambda_j \in \Lambda$. Hence,
$$ 0 = V(\sum_{j=1}^n I_{\lambda_j}) = \bigcap_{j=1}^n V(I_{\lambda_j}) \implies \mathrm{Spec}A = \left(\bigcap_{j=1}^n V(I_{\lambda_j})\right)^c = \bigcup_{j=1}^n U_{\lambda_j}. $$
Hence, the given cover has a finite subcover $\{U_{\lambda_j}\}_{j=1}^n$, done.

6. If $X = \mathrm{Spec}(A)$ is disconnected, then there is two disjoint clopen sets whose union is $X = \mathrm{Spec}(A)$. Thus $X = V(I) \cup V(J)$ for some ideal I and J with $V(I) \cap V(J) = \emptyset$. Thus, $V(I+J) \subseteq V(I) \cap V(J) = \emptyset$. Hence $I + J$ does not lie in any prime ideal, thus it cannot be a proper ideal; otherwise it has a maximal ideal containing itself. Thus $I + J = A$. Also, $X = V(I) \cup V(J) = V(IJ)$. This implies IJ is contained in any prime ideal, hence $IJ \subseteq \mathrm{nil}(A)$. Also, from the coprime condition of I and J, $IJ = I \cap J$ (see [2][p.7].)

   Now let $a \in I, b \in J$ such that $a + b = 1$. (Notes that a, b are nonzero and not 1.) Then, ab is nilpotent, thus $\exists n \in \mathbb{N}$ such that $a^n b^n = 0$. Now think about $(a + b)^{2n}$. Then, we can let
$$ e_1 = a^{2n} + \binom{2n}{1} a^{2n-1} b + \cdots + \binom{2n}{n-1} a^{n+1} b^{n-1}, e_2 = \binom{2n}{n+1} a^{n-1} b^{n+1} + \cdots + \cdots \binom{2n}{2n-1} a b^{2n-1} + b^{2n}. $$
   Then, $e_1 + e_2 + \binom{2n}{n} a^n b^n = e_1 + e_2 = 1$ and $e_1 e_2 = 0$ since every term in $e_1 e_2$ contains $a^n b^n$. Hence, $e_1(1 - e_1) = 0$ implies $e_1(e_1 - 1) = 0$ thus $e_1^2 = e_1$. Similarly, $e_2^2 = e_2$. Also we know that $e_1 \in I, e_2 \in J$ thus they are nontrivial idempotent.

7. Notes that any ideal of $A \times B$ can be identified as $I \times J$, since for given ideal Q of $A \times B$, $\pi_A(Q)$ form an ideal of A, since for any $(a, b) \in Q$ and $(a', b') \in A \times B$, $(a, b) \cdot (a', b') = (aa', bb') \in Q$ implies for any $a \in \pi_A(Q)$, $a' \in A$, $aa' \in \pi_A(Q)$.

   Now given a prime ideal $I \times J$, let I is proper. Then, we claim I is prime of A and $J = B$. To see this, if $aa' \in I$, then $(aa', b) \in I \times J$, thus $(a.1) \cdot (a', b) \in I \times J$ implies $(a, 1) \in I \times J$ or $(a', b) \in I \times J$. In any case, $a \in I$ or $a' \in I$, thus I is prime.

   Moreover, $A \times B/I \times J \cong A/I \times B/J$. However, direct product of integral domain is not integral domain, since $(0, s) \times (t, 0) = (0, 0)$. Hence, $J = B$ since I is proper.

8. $\supseteq$ is clear. To see the other side, let $a \in N_S \cap N'_S$. Then, $a = n/s = n'/s'$ where $n \in N, s \in S$ and $n' \in N, s' \in S$. Thus, $n(ts') = n'(st)$ for some $t \in S$. Thus, $n(ts') \in N \cap N'$. This implies $a \in (N \cap N')_S$, since $a = n(ts')/s(ts')$.

9. Before proving this, we claim
$$ V(I) \supseteq V(J) \iff \sqrt{I} \subseteq \sqrt{J}. $$
   This came from the fact that $\sqrt{I} = \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p}$. (p.3 of the textbook.)

Now, given a descending chain of closed sets in Spec$A$ can be denoted as

$$V(I_1) \supseteq V(I_2) \supseteq \cdots.$$

This induces $\sqrt{I_1} \subseteq \sqrt{I_2} \subseteq \cdots$, which is an ascending chain of ideals in A, which is Noetherian, thus stabilizes at some points. Hence, the chain $V(I_1) \supseteq V(I_2) \supseteq \cdots$ also stabilizes at some point.

10. Suppose $V(\mathfrak{p}) = V_1 \cup V_2$ for some closed set V_1 and V_2. By definition of Zariski topology, we may assume $V_1 = V(\mathfrak{a})$ and $V_2 = V(\mathfrak{b})$ for some ideal $\mathfrak{a}$ and $\mathfrak{b}$. Now, let $\mathfrak{q} \in V(\mathfrak{p})$. Then, $\mathfrak{q} \supseteq \mathfrak{p}$ and $\mathfrak{q} \supseteq \mathfrak{a}$ or $\mathfrak{q} \supseteq \mathfrak{b}$. Thus, $\mathfrak{q} \supseteq \mathfrak{a} \cap \mathfrak{b}$. When $\mathfrak{q} = \mathfrak{p}$, then $\mathfrak{p} \supseteq \mathfrak{a} \cap \mathfrak{b}$. Since $\mathfrak{p}$ is prime, this implies one of $\mathfrak{a}$ and $\mathfrak{b}$ is contained in $\mathfrak{p}$. WLOG, assume $\mathfrak{p} \supseteq \mathfrak{a}$. Then, $V(\mathfrak{a}) \supseteq V(\mathfrak{p})$, thus $V(\mathfrak{a}) = V(\mathfrak{p})$. This shows that $V(\mathfrak{p})$ is irreducible.

    Conversely, suppose V be an irreducible closed set. Again, by definition, $V = V(\mathfrak{a})$. We may assume $\mathfrak{a}$ is radical. Suppose that $\mathfrak{a}$ is not prime. Then, $\exists a, b \in A$ such that $ab \in \mathfrak{a}$ but $a, b \notin \mathfrak{a}$. Now, we claim $V(\mathfrak{a}) = V(\langle \mathfrak{a}, a\rangle) \cup V(\langle \mathfrak{a}, b\rangle)$. To see this,

    $$V(\langle \mathfrak{a}, a\rangle) \cup V(\langle \mathfrak{a}, b\rangle) = V(\langle \mathfrak{a}, a\rangle \cap \langle \mathfrak{a}, b\rangle) = V(\langle \mathfrak{a}, a\rangle\langle \mathfrak{a}, b\rangle) = V(\mathfrak{a}).$$

    Moreover, $\langle \mathfrak{a}, a\rangle \neq \mathfrak{a}$, $\langle \mathfrak{a}, b\rangle \neq \mathfrak{a}$, which shows that $V(\mathfrak{a})$ is not irreducible, contradiction.

11. See Hartshorne, Proposition 1.5.

12. By 4.10 and 4.11, since $V(I)$ is a closed set in Spec$A$, $V(I)$ can be written as a finite union $\bigcup_{i=1}^n V(\mathfrak{p}_i)$ for some prime ideals $\mathfrak{p}_i$. Now we may assume that any two of prime ideals $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are not contained in each other. (If it was, then get rid of the smaller one.) Now we claim $\{\mathfrak{p}_i\}_{i=1}^n$ is a set containing all minimal elements in $V(I)$. Suppose a prime ideal $P \in V(I)$ is minimal. Then, from $V(I) = \bigcup_{i=1}^n V(\mathfrak{p}_i)$, $P \in V(\mathfrak{p}_i)$ for some i, thus $P \supseteq \mathfrak{p}_i$. By minimality of P, $P = \mathfrak{p}_i$. Thus all minimal elements are in $\{\mathfrak{p}_i\}_{i=1}^n$. Hence $V(I)$ has only finitely many minimal elements.

5 The Hilhert Nullstellensatz and first steps in dimension theory

In Example 1, to see that every PID A which is not a field is 1-dimensional, suppose that; then since it is not a field, definitely it has nonunits, thus one may form a nonzero maximal ideal. Moreover, since PID is integral domain, (0) is prime. Thus, $\dim A \geq 1$. Now let $\mathfrak{p}$ be a nonzero prime ideal. Then $\mathfrak{p} = \langle a\rangle$. Now take maximal ideal $\mathfrak{m} = \langle m\rangle$ containing $\mathfrak{p}$. This implies $a = mb$ for some $b \in A$. Since $\mathfrak{p}$ is prime, whether m or b should be in $\mathfrak{p}$. If $m \in \mathfrak{p}$, then $\mathfrak{a} = \mathfrak{m}$, done. If $b \in \mathfrak{p}$, then $b = ac$ for some $c \in A$, thus $a = mac$. Thus, $a(1 - mc) = 0$. Since A is domain, this implies $1 = mc$, so m is unit, contradiction.

In the proof of theorem 5.5, one may identify that $\{\mathfrak{m} : \mathfrak{m} \supseteq I\}$ as a set of all algebraic zeros of I. Thus, if f is in the righthandside, then f vanishes on all algebraig zeros of I, thus Nullstellensatz implies that $f \in \sqrt{I}$.

In the proof of theorem 5.6, the residue class of X_1 is not algebraic over k, otherwise there exists $f(X)_1) \in P_{r-1}$, which implies that $P_{r-1} \cap S \neq \emptyset$, contradiction.

In the proof of theorem 5.8, X_n is complement of U_{n-1}, since $U_r \supseteq U_{r-1}$ for any r.

1. Let k be a field, $R = k[X_1, \cdots, X_n]$ and let $P \in \text{Spec}R$. Then ht$P$ + coht$P = n$.
    The proof follows the argument in the hint.

    Proof. Let x_i be the image of X_i in R/P. Then $R/P = k[x_1, \cdots, x_n]$ is an integral domain. Then theorem 5.6 says that coht$P = \text{tr.deg}_k k(x_1, \cdots, x_n)$ where $k(x_1, \cdots, x_n)$ is the field of fraction of R/P. By following hints, let $r = \text{tr.deg}_k k(x_1, \cdots, x_n)$. Then, we may assume that $\{x_1, \cdots, x_r\}$ is a transcendence basis of $k(x)$ over k. Notes that by the assumption $X_1, \cdots, X_r \notin P$. Moreover, $S = k[X_1, \cdots, X_r] - \{0\}$ is disjoint with P as subsets of R since $x_1, \cdots, x_r$ form a transcendence basis. Thus, $R_P \cong S^{-1}R_{S^{-1}P}$ since $R \setminus P \supseteq S$. This implies

    $$k[X_1, \cdots, X_n]_P \cong k(X_1, \cdots, X_r)[X_{r+1}, \cdots, X_n]_{S^{-1}P}.$$

By the 1-1 correspondence of prime ideals, $S^{-1}P$ is still a prime ideal and $\mathrm{ht}P = \mathrm{ht}S^{-1}P$.

If $r = 0$, then $x_1, \cdots, x_n$ are algebraic over k. Thus, the kernel $\mathfrak{p}_i$ of the map $k[X_1, \cdots, X_n] \to k[x_1, \cdots, x_i, X_{i+1}, \cdots, X_n]$ gives the strictly increasing chain of prime ideals $0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = P$. This shows $\mathrm{ht}P \geq n$. Also, by the corollary of theorem 6, $\mathrm{ht}P \leq n$. In case of $r > 1$, just do the same argument on the $x_{r+1}, \cdots, x_n$ to get the same conclusion. □

2. A zero dimensional Noetherian ring is Artinian.
The proof follows the argument in the Atiyah-Macdonald.

Proof. Let A be a zero dimensional Noetherian ring. By theorem 6.5, $Ass(A/0) = Ass(A)$ is finite. Hence, (0) has finitely many minimal prime ideals. Since $\dim A = 0$, these are all maximal ideals. Thus, $Supp(A) = Ass(A) = \{\mathfrak{m}_i\}_{i=1}^k$ for some $k < \infty$. Therefore A has only finitely many prime ideals. By p.3 of the textbook, $nil(A) = \bigcap_{i=1}^k \mathfrak{m}_i$ is the intersection of all prime ideals which are finitely many. Let $(x_1, \cdots, x_n) = nil(A)$. Then, there exists $N > 0$ such that $x_i^N = 0$ for all $i = 1, \cdots, n$ by taking N be the maximal t such that $x_i^t = 0$ for some $t > 0$. Thus, $nil(A)^{nN+1} = 0$ since for any element $x \in nil(A)$, $y = \sum_{i=1}^n a_i x_i$ for some $a_i \in A$, thus $y^{nN} = \sum_{j_1+\cdots+j_n=nN+1} c_{j_1,\cdots,j_n} x_1^{j_1} \cdots x_n^{j_n} = 0$ since one of $j_i > N$ by the pigeonhole principle. Hence, $nil(A)$ are nilpotent. By abuse of notation, let $N = nN+1$ such that $nil(A)^N = (0)$. Then,

$$\prod_{i=1}^k \mathfrak{m}_i^N \subseteq (\bigcap_{i=1}^k \mathfrak{m}_i)^N = nil(A)^N = (0).$$

Then consider a chain

$$A \supseteq \mathfrak{m}_1 \subseteq \mathfrak{m}_1\mathfrak{m}_2 \subseteq \cdots \subseteq \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k \subseteq \mathfrak{m}_1^2\mathfrak{m}_2\cdots\mathfrak{m}_k \subseteq \cdots \subseteq \mathfrak{m}_1^N\mathfrak{m}_1^N\cdots\mathfrak{m}_k^N = 0$$

Then, each fraction of incident two elements forms a vector space over $A/\mathfrak{m}_i$ for some i. Since each $\mathfrak{m}_i$ is finitely generated (from the Noetherian condition) all vector spaces arised in the fraction are finite dimensional. Hence, we can add a submodule between them which lift such vector spaces. This gives a composition series with a finite chain. Hence, $l(A) < \infty$. This implies A has a descending chain condition, since for any chain of ideal, we can make another chain by intersecting with the finite composition which stabilizes. □

6 Associated primes and primary decomposition

In proof of Theorem 6.2., Noetherian assumption is needed; if $\mathfrak{p}$ is infinitely generated by $\{a_i\}$, then this implies that $t_i a_i x = 0$ since P is $\mathrm{Ass}_{A_S}(M)$. So, without Noetherian assumption, $\prod t_i$ may not exists since it is infinite product.

In proof of Theorem 6.3, for $P \in \mathrm{Ass}(M)$, let $P = \mathrm{ann}(x)$. Then $N = Ax$ gives desired N. Moreover, we need one more claim;

Claim 1. *If $N \subset M$ be a submodule, then suppose $P \in \mathrm{Ass}(M)$ and $P = \mathrm{ann}(x)$ for some $x \in N \subset M$. Then, $P \in \mathrm{Ass}(N)$.*

Proof. Suppose not. Then $P' \in \mathrm{Ass}(N)$ such that $P' \supsetneq P$. Then, let $P' = \mathrm{ann}(y)$ for some $y \in N \subset M$. Then, $P \notin \mathrm{Ass}(M)$ since P is not maximal element anymore, contradiction. □

For Theorem 6.6,

Claim 2. *If M is finitely generated module, $\sqrt{\mathrm{ann}(M)} = \bigcap_{P \in \mathrm{Ass}(M)} P$.*

This is needed for $V(P) \implies P = \sqrt{\mathrm{ann}(M/N)}$

Proof. One inclusion is clear. For the other inclusion, suppose $x \in \bigcap_{P\in \mathrm{Ass}(M)} P$. Then, we claim $M_x = 0$. Suppose not; then by Theorem 6.1(i), $P \in \mathrm{Ass}(M_x)$ for some prime ideal P. Then, from Theorem 6.2, $P \in \mathrm{Ass}(M_x) = \mathrm{Ass}(M) \cap \mathrm{Spec}(A_x)$. Thus, there is an associate prime of M do not containing x, contradiction; hence for any $m \in M$, $exists n_m \in \mathbb{N}$ such that $x^{n_m} m = 0$. Since M is finitely generated, suppose $\{m_i\}$ are generator. Then $x^{\sum_i n_{m_i}} \in \mathrm{ann}(M)$, done. ☐

For Theorem 6.7, $M \to M/N \oplus M/N'$ induces the injective map $M/N \cap N' \hookrightarrow M/N \oplus M/N'$.

For Theorem 6.8, proof of (ii), we use below claim

Claim 3. *If Q is P_1-primary then $Q : M$ is primary of P_1.*

Proof. Let $xy \in (Q : M) = \mathrm{ann}(M/Q)$. Suppose $y \notin (Q : M)$. Then, $xy(M/Q) = 0$ but $y(M/Q) \neq 0$, thus if we let $\bar{\phi}_x : M/Q \to M/Q$ by $\overline{m} \mapsto x \cdot \overline{m}$, then

$$\bar{\phi}_x \circ \bar{\phi}_y = \bar{\phi}_{xy} = 0.$$

Since $\bar{\phi}_y$ is nonzero, $\ker \bar{\phi}_x \supseteq \mathrm{Im}(\bar{\phi}_y) \neq 0$. Hence $\bar{\phi}_x$ has nonzero kernel, thus x is zero divisor of Q. Since Q is primary, $\exists n \in \mathbb{N}$ such that $\bar{\phi}_{x^n} = 0$. Thus, $x^n M \subseteq Q$, which implies $x^n \in (Q : M)$. Thus $(Q : M)$ is primary. ☐

Moreover, $P_1^v M \subset N_1$ for some v are came from the proof of Exercise 3.3, or, you can use Proposition 7.14 of [2]. For the last sentence, $y \notin N_1$, thus for any $a \in A$, if $ay \in N_1$, then $a^v M \subseteq N_1$ for some v. However, in this case, $ay \in N_1$ means that $ay = 0$ since $\bigcap_{i=1}^r N_i = 0$. Thus, it implies that $ann(y) \subseteq \sqrt{ann(M/N_1)} \subseteq P_1$.

1. Find Ass (M) for the $\mathbb{Z}$ -module $M = \mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})$.

   Proof. $\mathrm{ann}((x, y)) = (0), \mathrm{ann}((0, z)) = (3)$ for any nonzero $x \in \mathbb{Z}, z \in \mathbb{Z}/3\mathbb{Z}$ and any $y \in \mathbb{Z}/3\mathbb{Z}$. Hence, $\mathrm{Ass}_M = \{(0), (3)\}$. Or use $0 \to \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \to 0$ with Theorem 6.3. ☐

2. If M is a finite module over a Noetherian ring A, and M_1, M_2 are submodules of M with $M = M_1 + M_2$ then can we say that $\mathrm{Ass}(M) = \mathrm{Ass}\,(M_1) \cup \mathrm{Ass}\,(M_2)$?

   Proof. No. For example, given M in above exercise, set $M_1 = M, M_2 = \mathbb{Z} \oplus 0$. Then, $M_1 + M_2 = M$ but $\mathrm{Ass}(M_i) = \{(0)\}$ for both i. ☐

3. Let A be a Noetherian ring and let $x \in A$ be an element which is neither a unit nor a zero-divisor; prove that the ideals xA and $x^n A$ for $n = 1, 2 \ldots$ have the same prime divisors:

   $$\mathrm{Ass}_A(A/xA) = \mathrm{Ass}_A\,(A/x^n A)$$

   Proof. First of all, if $P \in \mathrm{Ass}(A/x^n A)$, then $P = ann(y/x^n A)$ for some $y \in A$. Thus, $Py \subseteq x^n A \subseteq xA$, thus $P = ann(y/xA)$. This implies $\mathrm{Ass}(A/x^n A) \subseteq \mathrm{Ass}(A/xA)$ for any n. Thus it suffices to show the other inclusion.

   Next, $0 \to \ker \phi \to A/x^n A \xrightarrow{\phi} A/xA \to 0$ is exact. We knows that $\ker \phi$ is the ideal $x(A/x^n A)$ of $A/x^n A$. We claim $\ker \phi \cong A/x^{n-1}A$; to see this, think the map $A \to xA \to x(A/x^n A)$ where the first morphism is just multiplication by x and the second one is canonical morphism. Then, if a is in the kernel of the composition of maps, then $xa = x^n b$ for some $a, b \in A$. Since x is not zero divisor, $x(a - x^{n-1}b)$ implies $a = x^{n-1}b$. Hence, the kernel is $x^{n-1}A$. Then apply the first isomorphism theorem.

   Hence, $0 \to A/x^{n-1}A \to A/x^n A \xrightarrow{\phi} A/xA \to 0$, is an exact sequence. Theorem 6.3 implies $\mathrm{Ass}(A/x^n A) \subseteq \mathrm{Ass}(A/x^{n-1}A) \cup \mathrm{Ass}(A/xA)$. Apply induction; if $n = 2$, done. Suppose it holds for less than n. Then, again, this implies $\mathrm{Ass}(A/x^n A) \supseteq \mathrm{Ass}(A/xA)$. ☐

4. Let I and J be ideals of a Noetherian ring A. Prove that if $JA_P \subset IA_P$ for every $P \in \mathrm{Ass}_A(A/I)$ then $J \subset I$

Proof. Suppose not; then $(I+J)/I \neq 0$, hence there exists $P \in \mathrm{Ass}((I+J)/I) \subseteq \mathrm{Ass}(A/I)$. Thus, $PA_P \in \mathrm{Ass}_{A_P}((I+J)/I)_P = \emptyset$ since $((I+J)/I)_P \cong (IA_P + JA_P)/IA_P = 0$, contradiction. □

5. Prove that the total ring of fractions of a reduced Noetherian ring A is a direct product of fields.

   Proof. First of all, prime divisors of the zero ideal is are associated primes of $A/(0)$. Thus, all minimal prime ideals associated to $A/(0)$ is of form $ann(x)$. Thus, the set of all zero divisors D are union of all minimal associated primes of $A/(0)$. Let $S = A \setminus D$. Then, the total ring of fraction is $S^{-1}A$, and $\mathrm{Spec}(S^{-1}A)$ consists of the extensions of all minimal associated primes of $A/(0)$. Thus, they are coprime in $S^{-1}A$ because a minimal associate prime ideal do not contain the other. Moreover, all prime ideals are maximal. Denotes them as $P_iS^{-1}A_i$ for some $i = 1, 2, \cdots n$. Thus, by Chinese Remainder theorem, we have an isomorphism.

$$S^{-1}A/I \to \otimes_{i=1}^n S^{-1}A/(P_iS^{-1}A_i)$$

   where $I = \bigcap_{i=1}^n P_iS^{-1}A_i = 0$. Here, $S^{-1}A/(P_iS^{-1}A_i)$ is a field since $P_iS^{-1}A_i$ is maximal. □

6. (Taken from [Nor 1], p. 30.) Let k be a field. Show that in $k[X,Y]$ we have

$$\left(X^2, XY\right) = (X) \cap \left(X^2, Y\right) = (X) \cap \left(X^2, XY, Y^2\right)$$

   Proof. $\left(X^2, XY\right) \supseteq (X) \cap \left(X^2, Y\right) \supseteq (X) \cap \left(X^2, XY, Y^2\right) \supseteq \left(X^2, XY\right)$ by comparing their generators. □

7. Let $f : A \longrightarrow B$ be a homomorphism of Noetherian rings, and M a finite B module. Write ${}^af$: $\mathrm{Spec}\, B \longrightarrow \mathrm{Spec}\, A$ as in \$4. Prove that ${}^af\,(\mathrm{Ass}_B(M)) = \mathrm{Ass}_A(M)$. (Consequently , $\mathrm{Ass}_A(M)$ is a finite set for such M)

   Proof. ${}^af\,(\mathrm{Ass}_B(M)) \subseteq \mathrm{Ass}_A(M)$ is clear since A acts on M via f and the contraction of the prime ideal is prime. Now, suppose $P \in \mathrm{Ass}_A(M)$. Then, $P = \mathrm{ann}_A(m)$ for some $m \in M$, in other words, for any $a \in P$, $f(a)m = 0$. Now let $Q = \mathrm{ann}_B(m)$. We claim $Q = P^e$; $Q \supseteq f(P)$ is clear. For any $c \in P^e$, $c = \sum_i^n b_i f(p_i)$ for some $p_i \in P$, $b_i \in B$, thus $cm = 0$, which implies $c \in Q$. Lastly, suppose that $Q' \in \mathrm{Ass}_B(M)$ such that $Q' \supseteq Q$. Then, ${}^af(Q') \supseteq P$. Since P is maximal, $P =^a f(Q')$. This shows $P \in^a f\,(\mathrm{Ass}_B(M))$, done. □

8. An A -module M is coprimary if $\mathrm{Ass}(M)$ has just one element. Show that a finite module $M \neq 0$ over a Noetherian ring A is coprimary if and only if the following condition is satisfied: for every $a \in A$, the endomorphism $a : M \to M$ is either injective or nilpotent. In this case $\mathrm{Ass}\, M = \{P\}$ where $P = \sqrt{\mathrm{ann}\, M}$.

   Proof. Suppose M is coprimary. From claim 2, $P = \sqrt{\mathrm{ann}(M)}$. Hence, for any $a \in P$, a is nilpotent. For any $a \notin P$, a is injective.

   Conversely, if $a : M \to M$ is either injective or nilpotent for all $a \in A$, we knows that $\sqrt{\mathrm{ann}(M)}$ can classify elements of A. Now we claim M is coprimary. It suffices to show that $\sqrt{\mathrm{ann}(M)}$ is prime; if $ab \in \sqrt{\mathrm{ann}(M)}$ but $a, b \notin \sqrt{\mathrm{ann}(M)}$, then both a and b are injective, contradiction. □

9. Show that if M is an A -module of finite length then M is coprimary if and only if it is secondary. Show also that such a module M is a direct sum of secondary modules belonging to maximal ideals, and $\mathrm{Ass}(M) = \mathrm{Att}(M)$.

Proof. Since M is of finite length, M is both Noetherian and Artinian by Theorem 6.8 of [2]. Thus, we claim that $a : M \to M$ is injective iff surjective. If $a : M \to M$ injective but not surjective, $(a^i M)$ form a descending chain, thus there exists $n \in \mathbb{N}$ such that $a^n M = a^{n+1}M$. Now pick $m \in M \setminus aM$. Then, $a^n m = a^{n+1}m'$ for some $m' \in M$, thus $a^n(m - am') = 0$. By injectivity of a, $m = am' \in aM$, contradiction. Conversely, suppose $a : M \to M$ is surjective but not injective. Thus, $\ker(a^i)$ form an ascending chain, thus there exists $n \in \mathbb{N}$ such that $\ker(a^n) = \ker(a^{n+1})$. Now pick $m \in \ker(a^n)$, then $m = am'$ for some $m' \in M$ by the surjectivity of a. Thus, $m' \in \ker(a^{n+1}) = \ker(a^n)$, hence $a^{n-1}m = 0$. This implies $m \in \ker(a^{n-1})$. Since m was arbitrarily chosen, $\ker(a^{n-1}) = \ker(a^n)$. By the same argument, one can see $\ker(a) = \ker(a^2) = \cdots = \ker(a^n)$. Lastly, if $m \in \ker(a)$, then $m = am'$, which implies $m' \in \ker(a^2) = \ker(a)$, thus $m = 0$, this shows $\ker(a) = 0$. The first statement comes from this claim.

For the second statement, replace A with $A/\operatorname{ann}(M)$, then $\operatorname{ann}(M) = 0$. Since $\operatorname{ann}(M)$ lies inside of any associate prime ideal, thus $\operatorname{Ass}(M)$ is not changed. Moreover, M is a faithful Artinian module over A with finite length. Thus, by claim 4, A is Artinian. Hence, A has finitely many prime ideals, which are all maximal. Thus, if $M = N_1 + \cdots + N_n$ is a minimal secondary representation of M, then the attached prime ideals are $\operatorname{att}(M) = \{P_1, \cdots, P_n\}$ where $P_i = \sqrt{\operatorname{ann}(N_i)}$ by Theorem 6.9. These are all maximal ideals. Now we claim $M = N_1 + \cdots + N_n$ is direct sum by induction. If $n = 2$, then $P_1 \cap P_2 \subseteq \sqrt{\operatorname{ann}(M)} = \sqrt{0}$, and $\sqrt{0}$ is the maximal ideal since A is Artinian. Thus, one of P_i, say P_1 wlog, should be $\sqrt{0}$. However, in that case, $P_2 \supsetneq \sqrt{0}$ since annihilator of M is also annihilator of N_2. Therefore $P_2 = \sqrt{0}$, contradicting the fact that $n \neq 2$. Now suppose the direct sum holds for all cases when $|\operatorname{att}(M)| < n - 1$. Now suppose M is of the such module with $\operatorname{att}(M) = \{P_1, \cdots, P_n\}$. Then, from its minimal representation $M = N_1 + \cdots + N_n$, the inductive hypothesis shows that $N_1 + \cdots N_{n-1}$ is the direct sum. Also, $N_i + N_n$ is direct sum by the inductive hypothesis for any $i \in \{1, 2, \cdots, n-1\}$. Hence, M is the direct sum. And these are all belong to the maximal ideals, since A is Artinian.

Now it suffices to show that $\operatorname{Att}(M) = \operatorname{Ass}(M)$. Before doing this, we claim that for M of finite length with coprimary property, $\operatorname{Att}(M) = \operatorname{Ass}(M) = \{\sqrt{\operatorname{ann}(M)}\}$ first. Let P be an attached prime ideal of M. Then there exists a proper submodule $N \subset M$ such that M/N is P-secondary, i.e., $P = \sqrt{\operatorname{ann}(M/N)}$. Now, if $x \in P$, then $x^n \in \operatorname{ann}(M/N)$ for some $n > 0$, thus $x^n M \subseteq N$. Hence $x^n : M \to M$ is not surjective, therefore it is nilpotent by the assumption that M is secondary. Hence, $x \in \operatorname{ann}(M)$. Thus, $P \subseteq \sqrt{\operatorname{ann}(M)}$. Conversely, $P = \sqrt{\operatorname{ann}(M/N)} \supseteq \sqrt{\operatorname{ann}(M)}$ clear from the definition. Thus, $\operatorname{Att}(M) = \operatorname{Ass}(M)$.

Therefore, for general M of finite length with the minimal representation $M = N_1 + \cdots + N_n$, $\operatorname{Att}(N_i) = \operatorname{Ass}(N_i)$ for all i. This shows $\operatorname{Att}(M) = \operatorname{Ass}(M)$, since claim 5 shows that the associate prime of direct sums are union of those of summands. $\square$

Claim 4. *If there exists M a faithful A-module of finite length, then A is Artinian.*

Proof. Since M is of finite length, M has finitely generated, say $m_1, \cdots, m_n$. Then, $\phi : A \to M^n$ by $r \mapsto (rm_1, \cdots, rm_n)$ is an injective map since $\ker(\phi) \subseteq \operatorname{ann}(M) = 0$. Hence, A is a submodule of Artinian module, hence Artinian. $\square$

Claim 5. *For the commutative ring A with modules M_1 and M_2,* $\operatorname{Ass}(M_1 \oplus M_2) = \operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_2)$.

Proof. Let $P \in \operatorname{Ass}(M_1 \oplus M_2)$. We may assume $P = \operatorname{ann}(m_1 + m_2)$ by Theorem 6.1. Thus, $P \subseteq \operatorname{ann}(m_1) \cap \operatorname{ann}(m_2)$. Conversely, if $a \in \operatorname{ann}(m_1) \cap \operatorname{ann}(m_2)$, then $a(m_1 + m_2) = 0$, thus $P = \operatorname{ann}(m_1) \cap \operatorname{ann}(m_2)$. By Proposition 1.11 ii) of [2], either $P = ann(m_1)$ or $P = \operatorname{ann}(m_2)$. Thus, $P \in \operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_2)$. This shows $\operatorname{Ass}(M_1) \cup \operatorname{Ass}(M_2) \supseteq \operatorname{Ass}(M_1 \oplus M_2)$. The other inclusion came from Theorem 6.3 with the exact sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$. $\square$

7 Flatness

For (3),(4) of the Transitivity, the faithfully flatness is crucial. For example, *proof of (3) and (4).* (3): To show B is flat over A, let a sequence of A-module $\mathcal{S}$ is exact. Then, $\mathcal{S} \otimes_A M$ is exact by flatness of M over A, thus $(\mathcal{S} \otimes_A B) \otimes_B M$ is exact, therefore faithfully flatness of M over B shows $\mathcal{S} \otimes_A B$ is exact.

(4): To show B is faithfully flat over A, let a sequence of A-module $\mathcal{S}$ is exact. Then, $\mathcal{S} \otimes_A M$ is exact by flatness of M over A. Hence, $(\mathcal{S} \otimes_A B) \otimes_B M$ is exact. Faithfully flatness of M over B shows $(\mathcal{S} \otimes_A B)$ is exact. Conversely, if $(\mathcal{S} \otimes_A B)$ is exact, then $(\mathcal{S} \otimes_A B) \otimes_B M$ is exact by flatness of M over B, thus $(\mathcal{S} \otimes_A M)$ is exact, and faithfully flatness of M over A implies $\mathcal{S}$ is exact. $\square$

For the proof of Theorem 7.2 (3) $\implies$ (2), we want to show $Ax \otimes M \neq 0$ if $M \neq \mathfrak{m}M$. The contravariant of this statement is that if $Ax \otimes M = 0$ then $M = \mathfrak{m}M$. To see this, notes that $Ax \otimes M = A/\operatorname{ann}(x) \otimes M \cong M/\operatorname{ann}(x)$. Since $\subseteq M/\mathfrak{m}M \neq 0$ and a canonical surjective map $M/\operatorname{ann}(x) \to M/\mathfrak{m}M$ implies $M/\operatorname{ann}(x) \neq 0$.

(2) $\implies$ (1), $\operatorname{Im}(g \circ f) \to N''$ is an injective map, thus "by flatness" of M, $\operatorname{Im}(g \circ f) \otimes M \to N'' \otimes M$ is injective. Hence, $\operatorname{Im}(g \circ f) \otimes M$ is submodule of $N'' \otimes N$, and by the comparison with $\operatorname{Im}(g_M \circ f_M)$ we can conclude that $\operatorname{Im}(g \circ f) \otimes M = \operatorname{Im}(g_M \circ f_M)$. Also, $H \otimes M = \ker(g_M)/\operatorname{Im}(f_M)$ can be shown by taking the tensor on exact sequence $0 \to \operatorname{Im}(f) \to \ker(g) \to H \to 0$.

In p.47, to show

$$\{P \in \operatorname{Spec}(B) : P \supseteq \mathfrak{p}B \text{ and } P \cap f(S) = \emptyset\} = \{P \in \operatorname{Spec}(B) : P \cap A = \mathfrak{p}\},$$

$P \supseteq \mathfrak{p}B \implies P \cap A \supseteq \mathfrak{p}$, and for any $x \in P \cap A$, $f(x) \notin f(S) \implies f(x) \in f(\mathfrak{p})$, thus $x \in \mathfrak{p}$, which implies $P \cap A \subseteq \mathfrak{p}$.

For the proof of Theorem 7.3, PB_P is the Jacobson Radical, and that's why $PM_P = PB_PM_P \neq M_P$ from $M_P \neq 0$.

In p. 48, in the quote "If this happens then by Theorem 2, or Theorem 3, (ii)," Theorem 2 means Theorem 2 (3) by replacing M with B as A-module. Also, "we see that it is equivalent to say that f is flat or faithfully flat" means that "f is flat" $\implies$ "f is faithfully flat and vice versa. f may not be flat, though.

For Theorem 7.6, "if the above conclusion holds for the case of a single equation (that is for Y= l), then M is flat." actually means that "if the above conclusion holds for any cases of a single equation, then M is flat"

To see $\operatorname{Tor}_1^A(M, A) = 0$, think about the projective resolution $\cdots \to P_2 \to P_1 \to P_0 \to M$; then $\operatorname{Tor}_1^A(M, A) = H_1(\cdots \to P_2 \to P_1 \to P_0 \to 0) = 0$.

In Theorem 7.11, both are left exact since $\otimes_A B$ is exact due to flatness of B.

In Theorem 7.12, C_m is zero since $\operatorname{Hom}_{A_m}(M_m, -)$ is exact because M_m is free (thus projective.)

1. Suppose $B \otimes_A M$ is B-flat. Let $\mathcal{S}$ be an exact sequence of A-modules. Then, since B is flat A-module, $B \otimes_A \mathcal{S}$ is exact, thus

$$(B \otimes_A M) \otimes_A \mathcal{S} = ((B \otimes_A M) \otimes_B B) \otimes_A \mathcal{S} = (B \otimes_A M)_B (B \otimes_A \mathcal{S})$$

implies $(B \otimes_A M) \otimes_A \mathcal{S}$ is exact. Conversely, if M is A-flat, let $\mathcal{S}$ be an exact sequence of B-modules. Then,

$$(B \otimes_A M) \otimes_B \mathcal{S} = M \otimes_A B \otimes_B \mathcal{S} = M \otimes_A \mathcal{S}$$

thus $M \otimes_A \mathcal{S}$ is exact as sequences of A-module because of the flatness of M. Also, it is exact as sequences of B-module, by tensoring B, which does not change the sequences but still exact because B is faithfully flat over A. Hence, $(B \otimes_A M)$ is B-flat.

For faithfully cases, suppose $B \otimes_A M$ is faithfully B-flat. Then, suppose $M \otimes_A \mathcal{S}$ is exact for some exact sequence of A-modules. Then, $B \otimes_A M \otimes_A \mathcal{S} = (B \otimes_A M) \otimes_B B \otimes_A \mathcal{S}$ is exact since B is faithfully flat over A, and by faithfully flatness of $B \otimes_A M$, $B \otimes \mathcal{S}$ is exact, which implies $\mathcal{S}$ is exact since B is faithfully flat over A. Conversely, if M is faithfully flat, take $(B \otimes_A M)_B \mathcal{S}$ is an exact sequence of B-modules. Then, $M \otimes_A \mathcal{S}$ is exact, thus $\mathcal{S}$ is exact as sequences of A-modules. Thus, $B \otimes \mathcal{S} = \mathcal{S}$ is exact as sequences of B-module since B is faithfully flat over A.

2. For $b \in B$, b is element of the field of fraction of A, thus $b = y/x$ for some $y, x \in A$. Then, $bx = y \in xB \cap A$. By Theorem 7.5 (ii), $\langle x \rangle B \cap A = \langle x \rangle$. Thus, $y \in \langle x \rangle$, therefore $y = ax$ for some $a \in A$. This implies $a = b$ in the field of fractions, thus $b \in A$.

3. Let $M' = \oplus_\lambda A m_\lambda$ be an A-submodule of M. Then, $0 \to M' \to M \to M/M' \to 0$ is exact. By tensoring with B, which gives an exact, $0 \to B \otimes_A M' \to B \otimes_A M \to B \otimes_A (M/M') \to 0$ is exact, thus $B \otimes_A (M/M') = 0$. By Theorem 7.2 (2), $M/M' = 0$.

4. Let $M = \prod_\lambda M_\lambda$. We use Theorem 7.7; we try to show $I \otimes M \to IM$ is injective for every finitely generated ideal I. (Since A is Noetherian in this exercise, all ideals are finitely generated.) Let $I = \langle a_i \rangle_{i=1}^n$. Then, define $f : A^n \to A$ such that $f(x_1, \cdots x_n) = \sum a_i x_i$. Then, $0 \to \ker f \to A^n \to A$ is exact, thus $0 \to \ker f \otimes M_\lambda \to (M_\lambda)^n \to M_\lambda$ is exact for all λ.

   Now, pick an element $\sum_{i=1}^n a_i \otimes \xi_i \in I \otimes M$ such that $a_i \xi_i = 0$. Then, since each ξ_i can be represented as coordinate in the direct product, $\xi_i = (\cdots, \xi_{i\lambda}, \cdots)$. Thus, $a_i \xi_i = 0$ implies that $a_i \xi_{i\lambda} = 0$ for all λ. Thus, $(\xi_{1\lambda}, \cdots, \xi_{n\lambda}) \in \ker f \otimes M_\lambda$ for any λ.

   Since A is Noetherian, $\ker f = \sum_{j=1}^r A\beta_j$ for some $\beta_j = (\beta_{1j}, \cdots, \beta_{nj}) \in \ker f \subset A^n$ for some r. Therefore, choosing suitable $a'_j \in A$,

$$(\xi_{1\lambda}, \cdots, \xi_{n\lambda}) = \underbrace{\sum_{j=1}^r a'_j \beta_j \otimes \eta_{j\lambda}}_{\text{as element of } \ker f \otimes M_\lambda} = \underbrace{\sum_{j=1}^r (a'_j \beta_{1j} \eta_{j\lambda}, \cdots, a'_i \beta_{nj} \eta_{j\lambda})}_{\text{as element of } M_\lambda^n} = (\sum_{j=1}^r a'_j \beta_{1j} \eta_{j\lambda}, \cdots, \sum_{j=1}^r a'_j \beta_{nj} \eta_{i\lambda})$$

   since $\beta_j \otimes \eta_{j\lambda} = (\beta_{1j} \eta_{j\lambda}, \cdots, \beta_{nj} \eta_{i\lambda})$ in $(M_\lambda)^n$. (Notes that this is not true in $\ker f \otimes M_\lambda$ since you do not have 1 in $\ker f$.) Hence,

$$\xi_{i\lambda} = \sum_{j=1}^r a'_j \beta_{ij} \eta_{j\lambda}$$

   Now, for the economy of notation, let $b_{ij} = a'_j \beta_{ij}$. Then,

$$\xi_{i\lambda} = \sum_{j=1}^r b_{ij} \eta_{j\lambda}.$$

   Moreover, since $a'_j \beta_j \in \ker f$, $\sum_{i=1}^n a_i b_{ij} = 0$ for any $1 \le j \le r$. Thus,

$$\xi_i = (\cdots, \sum_{j=1}^r b_{ij} \eta_{j\lambda}, \cdots) = \sum_{j=1}^r b_{ij} \eta_j$$

   where $\eta_j = (\cdots, \eta_{j\lambda}, \cdots) \in M$. Thus,

$$\sum_{i=1}^n a_i \otimes \xi_i = \sum_{i=1}^n a_i \otimes \sum_{j=1}^r b_{ij} \eta_j = \sum_{j=1}^r \left((\sum_{i=1}^n a_i b_{ij}) \otimes \eta_j \right) = 0.$$

   Since formal power series $A[[x_1, \cdots, x_n]]$ is an infinite direct product of A as A-module, it is flat A-algebra.

5. Since a is A-regular, $0 \to A \xrightarrow{a} A$ is exact, therefore $0 \to N \xrightarrow{a} N$ is exact by the flatness of N, thus $ax \neq 0$ for any $x \in N$. This shows a is N-regular.

6. Let $\cdots \to C_{i+1} \xrightarrow{d_i}\to C_i \to \cdots$ be $C_\bullet$. Then,

$$0 \to \operatorname{Im} d_i \to \ker d_{i-1} \to H_i(C_\bullet) \to 0$$

   is exact, Now, since N is flat, $- \otimes N$ is exact functor, thus

$$(1) \quad 0 \to \operatorname{Im} d_i \otimes N \to \ker d_{i-1} \otimes N \to H_i(C_\bullet) \otimes N \to 0.$$

However, $\operatorname{Im} d_i \otimes N = \operatorname{Im}(d_i \otimes 1_N)$ since both $0 \to \operatorname{Im} d_i \otimes N \to C_i \otimes N$ and $0 \to \operatorname{Im}(d_i \otimes 1_N) \to C_i \otimes N$ are injective, and for any $a \otimes b \in \operatorname{Im}(d_i \otimes 1_N)$, $a \otimes b \in \operatorname{Im}(d_i) \otimes N$ and vice versa. Do the same thing on the kernel, we have

$$(2) \quad 0 \to \operatorname{Im}(d_i \otimes 1_N) \to \ker(d_{i-1} \otimes 1_N) \to H_i(C_\bullet \otimes N) \to 0$$

with four isomorphisms between components in (1) and (2). Apply the five lemma to get the desired result.

7. Take projective resolution $P^\bullet \to M$. Then, since B is flat over A, $P^\bullet \otimes B \to M \otimes B$ is also the projective resolution.

$$\begin{aligned} Tor_i^A(M,N) \otimes_A B &= H_\bullet(P_{i+1} \otimes_A N \to P_i \otimes_A N \to P_{i-1} \otimes_A N) \otimes_A B \\ &\underbrace{=}_{\text{Exercise 7.6}} H_\bullet(P_{i+1} \otimes_A N \otimes_A B \to P_i \otimes_A N \otimes_A B \to P_{i-1} \otimes_A N \otimes_A B) \end{aligned}$$

and

$$Tor_i^B(M \otimes B, N \otimes B) = H_\bullet((P_{i+1} \otimes_A B) \otimes_B (B \otimes_A N) \to (P_i \otimes_A B) \otimes_B (B \otimes_A N) \to (P_{i-1} \otimes_A B) \otimes_B (B \otimes_A N)).$$

Now observes that $P_i \otimes_A N \otimes_A B = (P_i \otimes_A B) \otimes_B (B \otimes_A N)$ by property of tensor product.

For Ext, apply Theorem 7.11 on the injective resolution of M for each side.

8. Tensor product does not commute with infinite direct products. To construct the counter example, let $\{p_i\}$ be the set of all prime numbers. Then, $\bigcap_i p_i\mathbb{Z} = 0$ However, $\bigcap_i (p_i\mathbb{Z} \otimes \mathbb{Q}) = \bigcap_i \mathbb{Q} = \mathbb{Q}$. To see the last equality, notes that for any $p_i a \otimes b/c$ for some $a,b,c \in \mathbb{Z}$ with $\gcd(b,c) = 0$, $p_i a \otimes b/c = 1 \otimes p_i ab/c = p_j \otimes p_i ab/cp_j$ as an element of $\mathbb{Z} \otimes \mathbb{Q}$ for any j, thus any $p_i\mathbb{Z} \otimes \mathbb{Q} = p_j\mathbb{Z} \otimes \mathbb{Q} \cong \mathbb{Q}$ for any i, j.

9. Suppose I is an ideal of A. Then, $IB \cap A = I$ by Theorem 7.5. Thus, for any ascending chain $I_1 \subset I_2 \subset \cdots$ of ideals of A, the ascending chain $I_1B \subset I_2B \subset \cdots$ eventually terminates. Say, $I_nB = I_{n+1}B$. If $a \in I_{n+1}$, then $f(a) \in I_{n+1}B = I_nB$, thus $a \in I_nB \cap A = I_n$, which implies $I_n = I_{n+1}$.

For example 2 of pure submodules, if $M = P \oplus Q$ then $0 \to P \otimes E \to M \otimes E = (P \otimes E) \oplus (Q \otimes E)$ shows the statement.

For example 3, suppose $N \cap mM = mN$ for all $m > 0$. Then, for any $0 \neq n \otimes a \in N \otimes \mathbb{Z}/m\mathbb{Z}$, $n \notin mN = N \cap mM$, thus $n \notin mM$, which implies $n \otimes a \neq 0$ in $M \otimes \mathbb{Z}/m\mathbb{Z}$. Conversely, if $0 \to N \otimes \mathbb{Z}/m\mathbb{Z} \to M \otimes \mathbb{Z}/m\mathbb{Z}$ is exact, then for any $0 \neq n \otimes a \in N \otimes \mathbb{Z}/m\mathbb{Z}$, $n \notin mM \cap N$ nor $n \notin mN$. Hence, $(N \setminus mN) \subseteq (N \setminus (mM \cap N))$. Conversely, if $n \in (N \setminus (mM \cap N))$, then $n \otimes a \neq 0$ in $M \otimes \mathbb{Z}/m\mathbb{Z}$, thus it is nonzero in its submodule $N \otimes \mathbb{Z}/m\mathbb{Z}$, thus $n \notin mN$. This shows the equality.

In the proof of Theorem 7.13,

$$\sum_i x_i \otimes \overline{e}_i = \sum_i \sum_j a_{ij} m_j \otimes \overline{e}_i = \sum_i \sum_j (m_j \otimes a_{ij}\overline{e}_i) = \sum_j \sum_i (m_j \otimes a_{ij}\overline{e}_i) = \sum_j (m_j \otimes \sum_i (a_{ij}\overline{e}_i))$$

For the reversing preceding argument means that, if you pick an arbitrary element of $N \otimes E$, then it forms $x = \sum_i x_i \otimes \overline{e}_i \in N \otimes E$ with $x_i \neq 0$ in $N \subseteq M$. If x is zero in $M \otimes E$, then, from $x_i \neq 0$, $x = \sum_j y_j \otimes \sum_i a_{ij} e_i$ for some $y_j \in N$. Then, by the above equation, $x_i = \sum_{j=1}^s a_{ij} m_j$, hence by the assumption $x_i = \sum_j^s a_{ij} y_j$. Thus, $x = \sum_i \sum_{j=1}^s a_{ij} m_j \otimes \overline{e}_i = 0$ by the above equation, again.

8 Completion and the Artin-Rees lemma

To see addition and subtractions are continuous, notes that $(-+b)^{-1}(x + M_\lambda) = \{a \in M : a + b \in x + M_\lambda\}$, thus $a = x - b + m$ for some $m \in M_\lambda$, therefore we claim $(-+b)^{-1}(x + M_\lambda) = (x - b) + M_\lambda$. To see this,

$(-+b)^{-1}(x+M_\lambda) \subseteq (x-b)+M_\lambda$ is clear by construction, and for any $a \in (x-b)+M_\lambda$, $a = x-b+m$ for some $m \in M$, thus $a+b \in x+M_\lambda$. This shows the equality. Hence, $(+): M^2 \to M$ is separately continuous. Now, to see $+$ is continuous, it suffices to show that for all subbasis of M^2, the preimage is continuous. Take $x+M_\lambda$ in the subbase of the linear topology. Then, $(+)^{-1}(x+M_\lambda) = \{(a,b) : a+b = x+m \text{ for } m \in M_\lambda\}$. This preimage contains the arbitrary union of $((x-b)+M_\lambda) \times (b+M_\lambda))$ for all b s.t. there exists a s.t. $a+b = x+m$. Conversely, for any $(a,b) \in (+)^{-1}(x+M_\lambda)$, (a,b) is contained in the cover, thus the preimage is open. Hence $+$ is continuous. By the similar reasoning one can show $-$ is continuous. Moreover, the scalar multiplication $a : M \to M$ is open, since $(a\cdot -)^{-1}(x+M_\lambda) = \{b \in M : ab \in x+M_\lambda\}$, thus it is arbitrary union of $(b+M_\lambda)$ over $\{b \in M : ab = x\}$, which shows the continuity. Multiplication is similar.

For the Hausdorff condition, refer [2][Lemma 10.1]. Also, ϕ is continuous by thinking the inverse limit in the category of topological space, which is complete and cocomplete. To see $\phi(M)$ is dense, pick an open neighborhood U of $\tilde{x} \in M$ as $U = \tilde{M} \cap \prod_{\lambda_i \notin \Lambda}(\tilde{x}_\lambda + M)\prod_{i=1}^{n}(\tilde{x}_\lambda + M_{\lambda_i})$ for some finitely many n. Now, we may decompose U as union of open sets $\{U_\mu \cap U\}_{\mu\in\Lambda}$ such that $U_\mu = \tilde{M} \cap (\prod_{\lambda\neq\mu}(\tilde{x}_\lambda + M)) \times (\tilde{x}_\mu + M_\mu)$ for fixed μ. Then, we can take a preimage $x \in M$ such that $\overline{x} = \tilde{x}_\phi$ for all $\phi \in \{\lambda_i\}_{i=1}^{n} \cup \{\mu\}$. Then, $x \in U_\mu \cap U$. Since μ was arbitrarily chosen, $\tilde{x}$ is a limit point of $\phi(M)$. This shows $\phi(M)$ is dense.

And, to see the linear topology of $\{M_\lambda^*\}$ coincide with the topology of M^λ, just recall that $\pi^{-1}(M_\lambda^*)$ is the basic open sets of the product topology.

In the proof of Hensel's lemma, $\deg hw_i < \deg F$ implies $\deg w_i < \deg g$ since $\deg F = \deg hg$. And, limit exist because A is m-adically complete.

For the proof of Theorem 8.3, the separatedness property of M was used for the last line, $\bigcap M_\lambda = 0$.

For the Artin-Rees lemma, $\subset$ is not clear since $a^n m \in I^n M \cap N$ does not implies $a^c m \in I^c M \cap N$. Also, $\sum_i u_{ji}(a)\omega_i \in I^{d_j} M \cap N$ by construction of J_n.

For the Theorem 8.7, the author did not prove that the completion commutes with direct sum. To see this as below form, for M and N are A-module,

$$\left(\varprojlim M/\left(I^n M\right)\right) \oplus \left(\varprojlim N/\left(I^n N\right)\right) \simeq \varprojlim (M\oplus N)/\left(I^n(M\oplus N)\right),$$

take a map $\left(\varprojlim M/\left(I^n M\right)\right) \oplus \left(\varprojlim N/\left(I^n N\right)\right) \to (M\oplus N)/(I^n(M\oplus N))$ by $\pi_n((x_1,\cdots)\oplus(y_1,\cdots)) = \overline{x_n}\oplus\overline{y_n}$, check it is well-defined, and use the universal property to get the isomorphism, since the kernel is $(\bigcap_n I^n M) \oplus (\bigcap_n I^n N) = 0$ in the lefthandside.

In proof of Theorem 8.10 (i), M/M' should be changed as M'/M.

Theorem 8.14 (1) is just the Krull's intersection theorem (i).

Theorem 8.14 (2) $\Longrightarrow$ (3) uses Theorem 7.3. (ii).

Notes that for $\{a_i : a_i \in I^n\}$, $\{\sum_{j=1}^{i} a_j\}$ is Cauchy sequence for I-adic linear topology.

1. Notes that $(I+J)^{2n} \subset I^n + J^n$ since all multiple from $(I+J)^{2n}$ has exponent greater than n for I or J. Thus, if we have a sequence $x_1,\cdots$, such that $x_{n+1}-x_n \in (I+J)^{2n}$, then $x_{n+1}-x_n = u_n + v_n$ for some $u_n \in I^n, v_n \in J^n$. Thus, $\{x_n\}$ converges to $x_1 + \sum_i^\infty u_i + \sum_i^\infty v_i$, which is unique since A is I and J-complete. Moreover, this can be shown for arbitrary sequence by regarding elements of $(I+J)^{2n+1}$ as those of $I^n + J^n$. Hence, A is $(I+J)$-complete.

2. If $\{x_n\}$ is a Cauchy sequence of J-adic topology, then $x_{n+1}-x_n \in J^n$. Since $I \supseteq J$, $\{x_n\}$ converges to x in I-adic topology. To see that x is also a J-adic limit, for an arbitrary i, take m large enough to get $x - x_m \in I^i$. Thus, $x_n - x = x_n - x_m + x_m - x \in J^n + I^i$. Since i was arbitrarily chosen, $x_n - x \in \bigcap_i (J^n + I^i) = J^n$, where the equality came from Theorem 8.10 (i). Thus, x is also the unique J-adic limit.

3. Let α be the generator of $\mathfrak{a}\tilde{A}$ such that $\alpha = \sum a_i\xi_i$ for $a_i \in \mathfrak{a}$ and $\xi_i \in \tilde{A}$. Let I be an ideal of definition of A. Then, we may take $x_i \in A$ such that $\xi_i - x_i \in I\tilde{A}$. Let $a = \sum a_i x_i$. Then, $a \in \mathfrak{a}$, and $\mathfrak{a}\tilde{A} \subseteq a\tilde{A} + I\mathfrak{a}\tilde{A}$ since $\alpha = \sum_i a_i x_i + (\sum_i a_i(\xi_i - x_i)$. This implies $\mathfrak{a}\tilde{A} = a\tilde{A} + I\mathfrak{a}\tilde{A}$ since the right hand side belongs to the left hand side by construction. By the Nakayama lemma, with the assumption that $I \subset \mathrm{rad}(A)$ by definition of Zariski ring, and $\mathfrak{a}\tilde{A}/a\tilde{A}$ is a finite module (because of Notherianity), we get $\mathfrak{a}\tilde{A} = a\tilde{A}$. Hence, $\mathfrak{a} = a\tilde{A} \cap A = aA$.

4. In this case, notes that $\bigcap_\nu I^\nu = I = eA$. Thus, it suffices to show that $y \in (X-e)A[[X]]$ for any $y \in I$. We may write $y = ey'$ for some $y' \in I$. Now we claim $y = y'(e-X)(e+eX+eX^2+\cdots)$ since $(e-X)(e+eX+eX^2+\cdots) = e$.

5. Notes that for any proper prime ideal $\mathfrak{p}A_S$, its maximal ideal $\mathfrak{m}$ in A contains I; otherwise, $\mathfrak{m}+I = A$ implies that $\mathfrak{m}A_S$ is not proper; contradiction. Hence, $I \subseteq rad(A_S)$. Thus, by Theorem 8.14, A_S with IA_S-adic topology is the Zariski ring.

   Now, using Theorem 8.12, if we let $I = (a_1, \cdots, a_n)$, then IA_S is also generated by $a_1/1, \cdots, a_S/1$, thus

$$\tilde{A_S} \cong A_S[[X_1, \cdots, X_n]]/(X_1 - a_1, \cdots, X_n - a_n), \quad \tilde{A} \cong A[[X_1, \cdots, X_n]]/(X_1 - a_1, \cdots, X_n - a_n)$$

   Thus, definitely, there is a canonical embedding $\tilde{A} \to \tilde{A_S}$. Moreover, for any $(1+a_i) \in A_S[[X]]/(X_i - a_i)_{i=1}^n$, which is unit in $\tilde{A_S}$, its notes that $(1+a_i)\cdot(\sum_{j=0}^\infty (-1)^j X_i^j) = 1$ in $\tilde{A_S}$ where $\sum_{j=0}^\infty (-1)^j X_i^j \in \tilde{A}$, which implies that $(1+a_i) \in \tilde{A}$ is also unit in $\tilde{A}$. Hence $\tilde{A} \cong \tilde{A_S}$.

6. Let $\{f_n\}$ be a Cauchy sequence of $(IB+XB)$-adic topology, i.e., $f_{n+1} - f_n \in (IB+XB)^n$. We may write it as $f_{n+1} - f_n = (\sum_{i=0}^{n-1} a_{i,n}X^i) + \sum_{i=n}^\infty b_{i,n}X^i$, where $a_{i,n} \in I^n, b_{i,n} \in A$. Thus, $\{f_n\}$ converges to $f = f_1 + \sum_i (\sum_n a_{i,n})X^i$, since $\sum_n a_{i,n}$ converges in A for each i, from the fact that A is I-adic complete. Moreover, this f is unique since each $\sum_n a_{i,n}$ is unique by the I-adic completeness of A. Hence, $A[[X]]$ is $(IB+XB)$-complete.

7. By Theorem 8.6(b) in [2], $A/\mathfrak{m}^n$ is Artinian local ring. Thus, by d.c.c., there exists $t(n) > 0$ such that $\mathfrak{a}_{t(n)} + \mathfrak{m}^n = \mathfrak{a}_j + \mathfrak{m}^n$ for all $j > t(n)$. Moreover, by renumbering if needed, we may assume $t(n) < t(n+1) < \cdots$.

   To get the contradiction, suppose $\mathfrak{a}_{t(r)} \not\subseteq \mathfrak{m}^r$ for some r. Then, take $a_r \in \mathfrak{a}_{t(r)} \setminus \mathfrak{m}^r$. Now pick $a_{r+1} \in \mathfrak{a}_{t(r+1)}$ s.t. $a_{r+1} - a_r \in \mathfrak{m}^r$, and proceed in the same way that taking $a_i \in \mathfrak{a}_{t(i)}$ s.t. $a_i - a_{i-1} \in \mathfrak{m}^{i-1}$ for $i \geq r$. Then, $a = \lim_i a_i$ exists since A is complete. Moreover,

$$a = a + a_r + (-a_r + a_{r+1}) + (-a_{r+1} + a_{r+2}) + \cdots + (-a_{i-1} + a_i) + \cdots \equiv a + a_r \mod \mathfrak{m}^r,$$

   which implies $-a_i \equiv a_r \mod \mathfrak{m}^r$, thus each $a_i \notin \mathfrak{m}^r$. Therefore, $a \notin \mathfrak{m}^r$, since by Theorem 8.14, $\mathfrak{m}^r$. However, this implies $0 \equiv a_r \mod \mathfrak{m}^r$, contradiction.

8. Just replicate the proof of the Artin-Rees lemma (Theorem 8.5) with multi-homogeneous polynomials.

9. First of all, A_P is a Noetherian local ring with the maximal ideal PA_P. Then, by Theorem 8.9, by letting $N = \bigcap_{n>0}(PA_P)^n$, there exists $a \in A_P$ such that $a \equiv 1 \mod PA_P$, and $aN = 0$. Since PA_P is the Jacobson radical, so a is unit, by Proposition 1.9 in [2]. Hence, $aN = 0$ implies $N = (0)$. Now, by the given condition, there exists a nonzero $x \in A_P$ such that $xPA_P = 0$. Hence, $x \in PA_P$. And since x is nonzero, $x \notin (PA_P)^c$ for some integer $c > 0$. Thus, for any ideal $I_P \subseteq P^c$, $\overline{x} \neq 0$ in A_P/I_P, and $\overline{x}(P+I)/I = 0$, which implies $P \in \mathrm{Ass}(A_P/I_P) \subseteq \mathrm{Ass}(A/I)$ by Theorem 6.2.

10. Let $\mathfrak{m} = (X,Y) \subset k[X,Y]$ and $A = k[X,Y]_\mathfrak{m}$. Then, let $\varphi(X) := \sum_i^\infty a_iX^i \in k[[X]]$ be transcendental over $k(X)$. (One can take such element, i.e., $\sum_i x^i$; no $f(x)/g(x) \in K(X)$ can be solution of $\sum_i x^i = 0$.) Set $\mathfrak{a}_v = (X^{v+1}, Y - \sum_{i=1}^v a_iX^i)$. Clearly, $\mathfrak{a}_{v+1} = X\mathfrak{a}_v$, thus $\{\mathfrak{a}_v\}$is d.c.c. Moreover, none of a_v is not contained in $\mathfrak{m}^2$.

    Now we claim $\bigcap_n \mathfrak{a}_n = 0$. To see this, notes that $\mathfrak{a}_v = j^{-1}((y-\varphi(X))k[[x,y]] + (x,y)^nk[[x,y]])$ where $j : k[x,y]_\mathfrak{m} \to k[[x,y]]$ the canonical inclusion. Thus, $\bigcap_n \mathfrak{a}_n = j^{-1}(\bigcap_n((y-\varphi)k[[x,y]] + (x,y)^nk[[x,y]])) = j^{-1}((y-\varphi)k[[x,y]])$. Thus, it suffices to show that there is no preimage of $(y-\varphi)k[[x,y]]$; to see this, let $h \in k[[x,y]]$ such that $h(y-\varphi(X))h$ is equal to a rational function $R(x,y)$. If such a function exists, then its numerator should be in preimage. Now, we choose $\varphi(X)$ as transcendental over $k(X)$, and $R(x,\varphi(x)) = h(\varphi(X) - \varphi(X)) = 0$. Therefore, the equation $R(x,y)$ should be equal to 0, since by definition, no nonzero polynomial in $k(X)[Y]$ has transcendental element as its solution. Thus, only 0 is in the preimage.

9 Integral extensions

In the first remark, to see $A/\mathfrak{p}_1$ is integrally closed domain, localize it by some prime ideal P pick x be an element of its ring of fraction s.t $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Then, $(x, 0, \cdots, 0)$ is in the ring of fraction of $A_{P\times A/\mathfrak{p}_2\times\cdots\times A/\mathfrak{p}_n}$ and $(x, 0, \cdots, 0)^n + (a_1, 0, \cdots, 0)(x, 0, \cdots, 0)^{n-1} + \cdots + (a_n, 0, \cdots, 0) = 0$. Hence, by the normality of A, $(x, 0, \cdots, 0) \in A_{P\times A/\mathfrak{p}_2\times\cdots\times A/\mathfrak{p}_n}$, which implies $x \in A_P$. Hence $A/\mathfrak{p}_1$ is integrally closed domain. Conversely, the direct product of finite number of integrally closed domain is normal, since its spec is just disjoint union of sets homeomorphic to spec of each component, (See Exercise 1.22 in [2]) therefore, any localization is of form a localization times the original component.

For example, 1, Let α be a root of a monic polynomial $f(x)$ over a UFD. We can express α as $\frac{a}{b}$ with $a, b \in A$, and using unique factorization we may assume that no irreducible of A divides both a and b.If $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$, then plugging in α and multiplying through by b^n we obtain $a^n + c_{n-1}ba^{n-1} + \cdots + c_0b^n = 0$. Now, $c_{n-1}ba^{n-1} + \cdots + c_0b^n$ is divisible by b, hence a^n is divisible by b. Since no irreducible of A divides both a and b, it follows that b must be a unit by unique factorization. Hence $\alpha \in A$.

For example 2, t is solution of $f(x) = X^2 - t^2$. For example 3, see Proposition 5.12 of [2] for details. For Example 4, since $\alpha^2 = f$, $\alpha = \frac{f}{\alpha}$ and $\frac{\alpha}{f} = \frac{1}{\alpha}$ in $K(\alpha)$, thus we may change every rational in $K(\alpha)$ as of form $x + y\alpha$.

For proof of Theorem 9.5, $B_{P'}$ is faithfully flat over $A_{\mathfrak{p}'}$ by Theorem 7.3. (iii).

1. By localizing with $\mathfrak{p}$, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. Hence, by Theorem 9.3, there exists a prime ideal of $B_\mathfrak{p}$ which lies over $\mathfrak{p}$. Definitely, this includes $\mathfrak{p}B_\mathfrak{p} \subseteq PB_\mathfrak{p}$. However, by the given assumption, $PB_\mathfrak{p}$ is the only prime ideal lying over $\mathfrak{p}A_\mathfrak{p}$. By lemma 2, $PB_\mathfrak{p}$ is the unique maximal ideal of $B_\mathfrak{p}$. Thus, $B_\mathfrak{p}$ is the local ring whose maximal ideal is $PB_\mathfrak{p}$. Moreover, this implies that $B \setminus P$ are unit in $B_\mathfrak{p}$. Hence, $\mathfrak{p}B_\mathfrak{p} = PB_\mathfrak{p}$, which implies that $B_P = B_\mathfrak{p}$.

2. $\dim A \le \dim B$ by Theorem 9.3. (i) and Going up theorem; (from sequence of prime ideals of A, get a prime ideal of B lying over the minimal prime ideal of the sequence by 9.3(i), and use going up theorem to get the sequence of prime ideals of B with the same length.) For $\dim A \ge \dim B$, suppose that there exists a sequence of prime ideals of B with inclusion. Then, for distinct P and P' in the sequence, $P \cap A \neq P' \cap A$ by theorem 9.3(ii). Thus, taking intersection with A gives the sequences of prime ideals of A with the same length.

3. Replace A and B by $A_\mathfrak{p}$ and $B_\mathfrak{p}$. Then, $\mathfrak{p}$ is maximal in A. Let $k = A/\mathfrak{p}$. Then, $k \otimes_A B = B/\mathfrak{p}B$ is a finite k-module. From Exercise 8.3 of [2], $B/\mathfrak{p}B$ is Artinian, hence has finitely many maximal ideals, which all lying over $\mathfrak{p}$.

4. Actually, $x \in K$ implies $x = a/b$ for some $a, b \in A$ with nonzero b. Since x is integral over A, suppose the degree of monic polynomial over A having x as as zero is n. Then, x^m can be written as linear combination of $\{1, x, \cdots, x^{n-1}\}$ over A, thus we only need to find $a \in A$ such that $ax^i \in A$ for all $i \le n$. Take $a = b^n$, we are done.

   Conversely, let x is almost integral over A with $ax^n \in 0$ for all n, then let $M := \frac{1}{a}A$. Then, $A[x] \subseteq M$; to see this, notes that $a'x^m = \frac{aa'x^m}{a} = \frac{1}{a}a'ax^m \in M$ for any $a' \in A$. Therefore, since A is Noetherian, then M is also Noetherian (since it is finite module over Noetherian module) thus its submodule is finite. Hence, the subring $A[x]$ is a finitely generated A-module. Now Theorem 9.1 assures that x is integral over A.

5. Actually, this holds to the polynomial ring. Let f be an element of the field of fractions of $A[X]$ (resp. $A[[X]]$) and suppose that there exists a non-zero element $g \in A[X]$ (resp. $g \in A[[X]]$) such that $gf^n \in A[X]$ (resp. $gf^n \in A[[X]]$) for every integer $n \ge 0$. If K is the field of fractions of A, $A[X]$ (resp. A[[X]]) is a subring of $K[X]$ (resp. $K[[X]]$). Also, both $K[X]$ and $K[[X]]$ are PID, which is a special case of UFD, thus they are integrally closed (see below claim.) Moreover, they are Noetherian by Hilbert Basis Theorem (Theorem 7.5 in [2]). Thus, by the Exercise 9.4, $K[X]$ and $K[[X]]$ are completely integrally closed. Thus, $f \in K[X]$ (resp. $f \in K[[X]]$).

Now, assume $f = \sum_{k=0}^{\infty} a_k X^k$ where $a_k \in K$ and $g = \sum_{k=0}^{\infty} b_k \mathbf{X}^k$. If all $a_k \in A$, done. Otherwise, pick the least $l > 0$ such that $a_l \notin A$. Then, let $f' := \sum_{k=0}^{l-1} a_k X^k$. Thus, $g(f-f')^n \in A[[X]]$ (or $A[X]$) for all $n \geq 0$. Now, set $j > 0$ be the least index such that $b_j \neq 0$. Then, $g(f-f')^n \in A[[X]]$ (or $A[X]$) has the least nonzero term $b_j a_l^n X^{j+nl}$, which is in $A[[X]]$ (or $A[X]$). Hence $b_j a_l^n \in A$ for all n. Thus, a_l is almost integral over A. Since A is completely integrally closed, $a_l \in A$, which contradicting the assumption that $a_l \notin A$.

Claim 6. *For a field k, $k[X]$ and $k[[X]]$ are PID.*

Proof. For $k[X]$, use division algorithm. For $k[[X]]$, if I is nonempty ideal, let $n(I) := \min_{f \in I} \operatorname{ord}(f)$. Then, pick $g \in I$ such that $n(I) = \operatorname{ord}(g)$, then $g = X^{n(I)} g_0$ with $\operatorname{ord}(g_0) = 0$, which implies g_0 is unit (since its constant is unit.) Hence, $I = \langle X^n \rangle$. □

6. Let $f = gh$ for some monic $g, h \in K[X]$. Now, roots of g are roots of f, thus they are integral over A. Hence, the coefficients of g are integral over A. Since A is integrally closed, $g \in A[X]$. Similarly, $h \in A[X]$.

7. Notes that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. (To see this, use the rational root theorem.) Let $x \in \mathbb{Q}[\sqrt{m}]$ such that x is integral over $\mathbb{Z}$. We may write $x = a + b\sqrt{m}$, and $(x-a)^2 - b^2 m = 0$ implies that $f(x) = x^2 - 2ax + a^2 - b^2 m$ is the minimal polynomial of x over $\mathbb{Q}$. Now, for the minimal integral polynomial of x, $f(x)$ should divide it in $Q[x]$, thus by the Exercise above, $f(x)$ has integer coefficients; thus $2a \in \mathbb{Z}, a^2 - b^2 m \in \mathbb{Z}$. If $a = \frac{a'}{2}$ for some odd a', then $b = b'/2$ for some odd b'; otherwise $a^2 - b^2 m \notin \mathbb{Z}$. Hence, $(a')^2 - (b')^2 m \equiv 0 \bmod 4$. Since both a' and b' are odd, $(a')^2 \equiv 1 \equiv (b')^2$, thus $m \equiv 1 \bmod 4$. Therfore, $\mathbb{Z}[\frac{1}{2}, \frac{\sqrt{m}}{2}]$ contains the integral closure. Now we claim that $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ is contained in the integral closure, since all $(a' + b'\sqrt{m})/2$ are in $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$, by subtracting or adding 1 or $\sqrt{m}$ properly. Conversely, if x is in the integral closure, then $x = a + b\sqrt{m}$ has integer a, b or $a = a'/2, b = b'/2$ with nonzero odd a', b'. In any cases $x \in \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$.

   Otherwise, if a is integer, $b^2 m \in \mathbb{Z}$, which implies $b \in \mathbb{Z}$. This holds for all m regardless of m mod 4. Hence, $\mathbb{Z}[\sqrt{m}]$ is the integral closure.

8. Suppose $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ be the chain of prime ideals giving the height of $\mathfrak{p}$ as n. Now suppose $P_0 \subsetneq \cdots \subsetneq P_m = P$ be the chain of prime ideals giving the height of P as m. If $m > n$, then $P_0 \cap A \subseteq \cdots \subseteq P_m \cap A = \mathfrak{p}$ is the chain of prime ideals of $\mathfrak{p}$. By the height of $\mathfrak{p}$, there exists at least one $i \in \{1, 2, \cdots, n\}$ such that $P_i \cap A = P_{i+1} \cap A$. However, this contradict Theorem 9.3 (ii) that there are no inclusion between two prime ideals of B lying over the same prime ideal of A.

9. Again, let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ be the chain of prime ideals giving the height of $\mathfrak{p}$ By the going down theorem, we have a chain of prime ideals $P_0 \subsetneq \cdots \subsetneq P_n = P$. Hence, the height of P is greater than or equal to that of $\mathfrak{p}$.

10. First of all $L[X]$ is a free-module over $K[X]$ since L is an extension of K. Therefore, the going down theorem holds by Theorem 9.5. Thus, by Exercise 9.9, height of P is greater than or equal to height of $\mathfrak{p}$. This can be extended for any polynomial ring over $L[X]$ and $K[X]$.

    If L is algebraic over K, then $L[X]$ is integral over $K[X]$. To see this, notes that any $a \in L$ has monic polynomial $y^n + a_1 y^{n-1} + \cdots + a_n = 0$ where $a_i \in K \subseteq K[X]$. Also, $X \in K[X]$. Since sum and multiplication of two elemens integral over $K[X]$ are also integral over $K[X]$ (see Corollary 5.3 in [2]) $L[X]$ is integral over $K[X]$. Also, this holds for all finite number of indeterminates. Hence, by Exercise 9.8, The equality holds.

    Next, if f, g have a common factor $\alpha(X)$ in $L[X]$ then set $P = (\alpha(X))$, so that ht $P = 1$ (Use Corollary 11.17 (Krull's principal ideal theorem) in [2]). Hence ht $\mathfrak{p} \leq 1$. But $f, g \in \mathfrak{p}$, so that ht $\mathfrak{p} = 1$. Hence, there is an irreducible divisor h of f in $\mathfrak{p}$ and $\mathfrak{p} = (h)$ so $h \mid g$.

11. For (i), if there is an embedded prime ideal of (0), say P, then $P = \operatorname{ann}(x) \supsetneq \mathfrak{p}_i$ for some fixed i. Pick $a \in P \setminus \mathfrak{p}_i$. Then, in $A_{\mathfrak{p}_i}$, $(a/1)$ is a unit and nonzero divisor, hence $A_{\mathfrak{p}_i} = 0$. Since zero ring is not an integral domain, contradiction. Hence, no such P exists. Therefore, (i) holds.

For (ii) the intersection is equal to nilradical follows from (i). Lastly, for (iii), notes that $\mathfrak{p}_i$ cannot contain the intersection; otherwise, by Proposition 1.11(ii) of [2], $\mathfrak{p}_i$ contain another minimal prime ideal, contradiction. Thus there exists $x \in (\bigcap_{j\neq i} \mathfrak{p}_j)\backslash\mathfrak{p}_i$. Then, there exists $y \in A$ such that $xy = 0 \in \mathfrak{p}_i$, thus $y \in \mathfrak{p}_i$. Moreover, for any $y' \in \mathfrak{p}_i$, $xy' \in \bigcap_j \mathfrak{p}_j = \sqrt{(0)}$, thus $(xy')^d = 0$ for some $d \geq 1$.

Now, suppose that $\mathfrak{p}_i + (\bigcap_{j\neq i} \mathfrak{p}_j) \subseteq \mathfrak{m} \neq A$ for some maximal ideal $\mathfrak{m}$. Then, in $A_\mathfrak{m}$, it suffices to show that $x/1, y/1$ are nonunits and nonzeros. Nonunits are easy; if they are, then $t(xs - s) = 0$ for some $t, s \in A \setminus \mathfrak{m}$, which implies that $xst = st$. But $xst \in \mathfrak{p}_i \subset \mathfrak{m}$ while $st \in A \setminus \mathfrak{m}$, this is contradiction. Same argument can be applied for $y/1$. Also, they are nonzeros; if they are zero, then $\exists t \in A \setminus \mathfrak{m}$ such that $t(x - 0) = 0$. This means that $xt \in \mathfrak{p}_i$. However, since $x \notin \mathfrak{p}_i$, $t \in \mathfrak{p}_i \subseteq \mathfrak{m}$, contradiction. Hence, $A_\mathfrak{m}$ is not the integral domain, contradiction.

Then, (ii) and (iii) with Chinese remainder theorem gives us the desired result.

10 General valuation

To see $R \subset R' \subset K$ implies R' is valuation ring, let $x \in K \setminus R'$; then $x^{-1} \in R \subseteq R'$. For proof 10.5, (β) is came from that; if none of $Z_i \notin \mathscr{A}$, then for each i, we may find finitely many $F_{ij} \in \mathscr{A}$ such that $Z_i \cap \bigcap_j F_{ij} = \emptyset$ for all i, hence $(\cup_i Z_i) \cap_i (\cap_j F_{ij}) = \emptyset$, contradiction. Also, in the last paragraph, if $1 \notin I$, then it resides inside of the maximal ideal containing I, then apply 10.2 on $A[\Gamma]$ to get a valuation ring whose maximal ideal containing I, i.e., containing Γ.

In p.75, to see G is totally ordered set, let $x \neq y \in K$. If $xa \in xR$ but $xa \notin yR$, then we have $xa/y \notin R$ (otherwise $y(xa/y) = xa \in yR$. Thus, $y/xa \in R \implies y/x \in R$. Hence, $x \cdot y/x = y \in xR$, thus $yR \subseteq xR$.

Claim 7. *Suppose a field K has two valuations $v : K \to H$ and $v' : K \to H'$ with the same valuation ring $R_v = R = R_{v'}$. Then, there exists an order isomorphism $\varphi : H \to H'$ such that $v' = \varphi v$.*

Matsumura did not write the surjectivity condition of v and v', but we need this; otherwise, we may create distinct valuations.

Proof. φ is canonically defined as $v(x) \mapsto v'(x)$. First of all, this is well-defined; if $v(x) = v(x')$ for some $x, x' \in K$, then by the homomorphism $v(x) - v(x') = v(x) + v((x')^{-1}) = v(x(x')^{-1}) = 0$ implies that $x(x')^{-1}$ is unit in R, Hence $0 = v'(x(x')^{-1}) = v'(x) - v'(x')$. Next, φ is surjective; for any $t \in H'$, $t = v'(x)$ for some $x \in K$ by surjectivity of v', thus $t = \varphi(v(x))$. Lastly, φ is injective. If $\varphi(t) = 0$ for some $t \in H$, $t = v(x)$ by surjectivity of v, thus $\varphi(v(x)) = 0$ implies $v'(x) = 0$, thus $x \in R$ is unit, hence $v(x) = 0$. □

In the proof of Theorem 10.6, the injectivity came from the given condition that there exists n such that $n(y - y') > x$. Now pick 10^r such that $n < 10^r$.

In the last paragraph of proof of Theorem 10.7, ηR is $\mathfrak{m}$-primary, since its radical is the intersection of all prime ideals containing it, but R has the unique prime ideal $\mathfrak{m}$.

1. Suppose I is generated by $a_1, \cdots, a_n$. Then, since the set of all ideals of the valuation ring is totally ordered by inclusion, there exists the maximal element of $\{\langle a_i \rangle\}_i$, say a_1. Hence, $I = \langle a_1 \rangle$.

2. From Theorem 7.7, it suffices to show that M is torsion-free iff every finitely generated ideal I of R has the injective canonical map $I \otimes_R M \to R \otimes_R M$. From the exercise above, we always this condition is equivalent that $\langle a \rangle \otimes M \to R \otimes M$ is injective for any nonzero $a \in R$. To see this, suppose M is flat. Then, $\langle a \rangle \otimes M \to R \otimes M$ is injective; this means that for any $m \in M$, $a \otimes m \mapsto am \neq 0$. This holds for arbitrarily nonzero a, so M is torsion free. Conversely, if M is torsion free, then $a \otimes m \mapsto am \neq 0$, hence if $ab \otimes m \mapsto 0$, then $abm = 0$ implies $ab = 0$, thus $ab \otimes m = 0$. This shows the desired injectivity.

3. Point is choosing $\mathfrak{p}$ containing $(\mathfrak{m}_A, y)$ instead of $yA[y]$.

   Write B' for the intersection of all valuation rings of K dominating A, so that by the previous theorem we have $B' \supset B$. To prove the opposite inclusion it is enough to show that for any element $x \in K$ which is not integral over A there is a valuation ring of K dominating A but not containing x. Set $x^{-1} = y$. The ideal $(\mathfrak{m}, y)A[y]$ of $A[y]$ does not contain 1: for if $1 = a_1y + a_2y^2 + \cdots + a_ny^n$ with $a_i \in A$ then x would be integral over A, contradicting the assumption. Therefore there is a maximal ideal $\mathfrak{p}$ of

$A[y]$ containing $(\mathfrak{m}, y)A[y]$, and by Theorem 2 there exists a valuation ring R of K such that $\mathbf{R} \supset A[y]$ and $m_R \cap A[y] = \mathfrak{p}$, and $m_R \cap A = \mathfrak{p} \cap A = \mathfrak{m}_A$. Now $y = x^{-1} \in \mathfrak{m}_R$, so that $x \notin R$

4. Let $0 \subset p_1 \subset p_2$ be a strictly increasing chain of prime ideals of R and let $0 \neq b \in \mathfrak{p}_1, a \in \mathfrak{p}_2 - \mathfrak{p}_1$. Then, $b/a^n \in R$, otherwise $a^n/b \in R$ thus $b \cdot (a^n/b) = a^n \in \mathfrak{p}_1$, contradiction. Take $f = \sum_1^\infty u_i X^i$ to be root of $f^2 + af + X = 0$. Then $u_1 = -a^{-1}$, $u_1^2 + au_2 = 0$ implies $u_2 = a^{-3}$, $2u_2u_1 + au_3 = 0$ implies $u_3 = 2a^{-5}$, and so on; thus $(\sum_{i=1}^{n-1} u_i u_{n-i}) + au_n = 0$ implies that $u_n \in a^{-2i+1-2(n-i)+1-1}R = a^{-2n+1}R$. Thus, $bf(X) \in R[[X]]$ but $f(X) \notin R[[X]]$. This shows that $R[[X]]$ is not integrally closed.

5. If there exists a ring R' such that $R \subset R' \subset K$, then R' is also a valuation ring of K and $\mathfrak{m}_{R'} \subseteq \mathfrak{m}_R$ by Theorem 1. Since R has Krull dim. 1, $\mathfrak{m}_{R'} = 0$ which implies $R' = K$. Conversely, if R is the maximal proper subring of a field K and R is not a field, then by Lemma 1 of Section 9, (by thinking $A = R, B = K$) K is not integral over A, otherwise R is field by the Lemma, contradiction. Thus, the integral closure of R in K is proper ring of K containing R. By the maximality condition of R, R is the integral closure of R in K. For any $x \in K \setminus R$, we knows that $R[x] = K$ by the maximality of R, hence $x^{-1} \in R[x]$, thus $x^{-1} = a_0 + a_1 x + \cdots + a_n x^n$, which implies that $x^{-n-1} - a_0 x^{-n} + \cdots + a_n = 0$, thus x^{-1} is integral over R, thus $x^{-1} \in R$. Therefore, R is a valuation ring. If $\dim R > 1$, then there exists a prime ideal $\mathfrak{p}$ distinct from (0) and from $\mathfrak{m}_R$, thus $R_\mathfrak{p}$ is intermediate between R and K, contradicting the the maximality of R.

6. It suffices to show that $v(\alpha + \beta) \leq \min(v(\alpha), v(\beta))$. WLOG, suppose $v(\alpha) > v(\beta)$. Let R be the valuation ring with the maximal ideal $\mathfrak{m}$. Then, $\alpha/\beta \in \mathfrak{m}$ since $v(\alpha/\beta) = v(\alpha) - v(\beta) > 0$. Hence, $1 + \alpha/\beta$ is unit, Thus, $v(\alpha + \beta) = v(\beta(1 + \alpha/\beta)) = v(\beta)$. This shows the equality.

7. If $n = 2$, then $\infty = v(0) = v(\alpha_1 + \alpha_2) = \min(v(\alpha), v(\beta))$ implies $\alpha = \beta = 0$. Suppose it holds for $n - 1$. Then, the inductive hypothesis shows that $v(\alpha_1 + \cdots + \alpha_n) = 0$ implies $\alpha_1 = \alpha_2$ or $\alpha_j = \alpha_i$ for some distinct $i, j \in \{3, \cdots, n\}$. In any cases, the statement holds.

8. Choose nonzero $x_1, \ldots, x_e \in L$ such that $v(x_1), \ldots, v(x_e)$ represent the different cosets of G' in G, (we may not choose 0 because there is no zero-field.) and $y_1, \ldots, y_f \in S$ such that their images in k are linearly independent over k'. Now we claim that $\{x_i y_j\}_{i \in [e], j \in [f]}$ is linearly independent over K; suppose not; then
$$\alpha_{00} + \cdots + \alpha_{ef} = 0$$
where $\alpha_{ij} = a_{ij} x_i y_j$ for some $a_{ij} \in K$. Moreover, by multiplying suitable elements of S, we may assume that $a_{ij} \in R$ and $a_{ij} x_{ij} \in S$ for all i, j. Then, rewrite the equation above as $\sum_i (\sum_j a_{ij} y_j) x_i = 0$.

   Now, by applying the $\infty = v(\alpha + \beta) \implies \alpha = \beta = 0$ e-times on $0 = \sum_{i=1}^e (\sum_j a_{ij} y_j) x_i$, we may assume $\sum_j a_{ij} y_j x_i = 0$ for all i. Now, by choice of x_i, $x_i \neq 0$, thus in S, which is domain, we may assume $\sum_j a_{ij} y_j$. Then, $\sum_j a_{ij} y_j = 0$. Now take a quotient by $\mathfrak{m}_S$ (since S is a valuation ring, thus it is already local, therefore $S = S_{\mathfrak{m}_S}$) we have $\sum_j \overline{a_{ij} y_j} = 0$ in k. Since $\{\overline{y_j}\}$ is linearly independent over k', and $\overline{a_{ij}} \in k'$ (since $a_{ij} \in R$), $\overline{a_{ij}} = 0$. Thus, $a_{ij} \in \mathfrak{m}_R$.

   Now, applying $\infty = v(\alpha + \beta) \implies \alpha = \beta = 0$ f-times on $0 = \sum_{j=1}^f (\sum_i a_{ij} x_i) y_j$, we have $(\sum_i a_{ij} x_i) y_j = 0$ for each j. Again, by choice of y_j, we knows that y_j is nonzero. Thus, $(\sum_i a_{ij} x_i) = 0$. By applying the $\infty = v(\alpha + \beta) \implies \alpha = \beta = 0$ e-times on $(\sum_i a_{ij} x_i) = 0$, $v(a_{ij} x_i) = \infty$ for all i. Since $x_i \neq 0$, $a_{ij} = 0$. Since i and j were arbitrarily chosen, $a_{ij} = 0$ for all i, j. Hence, $\{x_i y_j\}$ is linearly independent over K.

9. If $S \subset S_1$ then by Theorem 10.1 (iii) the residue field k_1 of S_1 contains a valuation ring $A = S/\mathfrak{m}_{S_1} \neq k_1$ such that S is the composite of S_1 and A. Since $\mathfrak{m}_S \supset \mathfrak{m}_{S_1}$, we have $k \subset A \subset k_1$, but by the previous exercise, k_1 is an algebraic extension field of k, thus k_1 is integral over k, hence integral over A. But by Theorem 10.3, A is integrally closed, therefore $A = k_1$, a contradiction. In case of $S_1 \subset S$, do the same thing.

10. Let $v' : K \to H \cup \{\infty\}$ such that $v'(a/b) = v(a) - v(b)$ for any $a, b \in A$. Then, for any $a, b, c, d \in A$ with nonzero b, d,

    - $v'((a/b) \cdot (c/d)) = v(a) + v(c) - (v(b) + v(d)) = v(ac) - v(bd) = v'(ac/bd)$

- $v'((a/b)+(c/d)) = v'((ad+bc)/cd) = v(ad+bc)-v(cd) \geq \min(v(a)+v(d), v(b)+v(c))-v(c)-v(d)$. If $v(a)+v(d) < v(b)+v(c)$, then this equals to $v'(a/c)$, otherwise, it equals to $v'(c/d)$, thus $\min(v(a/c), v(a/d))$.
- $v'(0) = v(0) = \infty$. Conversely, if $v'(a/b) = \infty$, then $v(b) \neq \infty$ since $b \neq 0$, thus $v(a) = \infty$, which implies $a/b = 0$.

Thus v' is the additive valuation. If $s : K \to H \cup \{\infty\}$ is another extension of v, then, $v(a) = s(a) = s((a/b)\cdot b) = s(a/b) + v(b)$, thus $s(a/b) = v(a) - v(b) = v'(a/b)$. Thus v' is unique.

11. Notes that, by taking $\alpha > 1$ or $\alpha < 1$, we may have a term order on tuples of indices such that $(n, m) < (n', m')$ iff $n + m\alpha < n' + m'\alpha$ and for any $(p, q) \in \mathbb{N}^2$, $(n, m) + (p, q) < (n', m') + (p, q)$. Hence, by using this term order, $v(fg) = v(f) + v(g)$ is clear. Also, $v(f + g) \geq \min(v(f), v(g))$ is also clear. Lastly, by definint $\min(\emptyset) = \infty$, we have all three conditions of additive valuation. Extend it using the above exercise.

11 DVRs and Dedekind rings

In the proof of Theorem 1, (2) $\implies$ (1), π should be changed to v. In the remark, g is unit in S (since g is not zero in $\overline{R}$, a DVR of k.) That's why we need $f, fg^{-1}, \cdots$ to generate $\mathfrak{m}_R$ since in R, g^{-1} is not a unit.

In the proof of Theorem 2, (1) $\implies$ (4), R is normal, since it is integrally closed in its field of fraction (that is the property of valuation ring) and it is reduced, i.e., there is no nilpotent elements except 0.

In p.81,

Claim 8. *For a fractional ideal I over R, every R-linear map from I to R is given by multiplication by some element of K.*

Proof. If $I = 0$, clear. Otherwise, let ϕ be the given R-linear map. for all $b/c \in I$, we have $b \in I$ and $\phi(b) = \phi(c(b/c)) = c\phi(b/c)$, so
$$\phi(b/c) = \phi(b)/c.$$
Now fix $a_0 \in I \cap R$ non-zero. Let $x = b/c \in I$. Then
$$a_0\phi(x) = \phi(a_0x) = \phi(a_0b/c) = b\phi(a_0/c) = b\phi(a_0)/c.$$
So
$$\phi(x) = (\phi(a_0)a_0^{-1})x, \quad \forall x \in I.$$
□

Honestly, in the proof (2) to (1), nonzero λ_is are finitely many because of the dual basis theorem

Definition 1 (. Dual basis)**.** *Given a R-module M,* dual basis *of M is a set of functions $\{f_i\} \subseteq \mathrm{Hom}_R(M, R)$ and a set of elements $\{m_i : i \in I\}$ where $m_i \in M$ such that*

1. *$\forall m \in M$, $\{i \in I : f_i(m) \neq 0\}$ is finite*
2. *$\forall m \in M$, $m = \sum_i f_i(m)m_i$.*

Theorem 1 (Dual basis theorem)**.** *An R-module M is projective if and only if it has a dual basis.*

Proof. If it has dual basis, then let $g : \bigoplus_I R \to M$ by $e_i \mapsto m_i$. This is R-linear by construction, and surjective. Let $f : M \to \oplus_I R$ by $x \mapsto \sum_{i\in I} f_i(x)e_i$. Then, $g \circ f(x) = \sum_{i\in I} f_i(x)x_i = x$ Hence, $0 \to \ker g \to \bigoplus_I R \xrightarrow{g} M \to 0$ is split exact, hence M is direct summand of a free module, thus projective.

Conversely, if M is projective, let $g : F \to M$ be a surjective map from a free module with basis $\{e_i\}_{i\in I}$. Then, we have a section $h : M \to F$ such that $gh = 1_M$. Then, $h(x) = \sum_{i\in I} f_i(x)e_i$. Then, $f_i : M \to R$ is in $\mathrm{Hom}_R(M, R)$. Also, by the definition of basis, for each x, $f_i(x) = 0$ all but finitely many, and $x = gh(x) = \sum_{i\in I} f_i(x)x_i$. □

For the proof of Theorem 11.3 (1) $\implies$ (3), one of a_ib_i must be outside of P, otherwise $1 \in PR_P$, contradiction. Hence, a_ib_i is unit in R_P. Then, for any $x/y \in I_P$ with $x \in I, y \in R \setminus P$, $x/y = a_ib_i(x/y)$ since a_ib_i is unit, hence $x/y = a_i(b_ix)/y \subseteq a_iR_P$. Conversely, $a_iR_P \subseteq I_P$, which implies $a_iR_P = I_P$.

In the proof of (i) of Theorem 11.5, P is a prime divisor of aR, which means that there exists $\bar{b} \in R/(a)$ such that $P = ann(\bar{b})$. Hence, $aR : b = P$. Then, in R_P, $bPR_P \subseteq aR_p$ implies $aR_P : b = PR_P = \mathfrak{m}$. Thus, $ba^{-1}\mathfrak{m} = a^{-1}bPR_P \subseteq a^{-1}aR_P = R_P$. This implies $ba^{-1} \in \mathfrak{m}^{-1}$. Moreover, $ba^{-1} \notin R_P$, otherwise $PR_P \supseteq ba^{-1}PR_P = R_P$, contradiction. Also, determinant trick means Theorem 2.1. Also, R_P is integrally closed since R is normal.

In the proof of (ii) of 11.5, $aR_{P_i} \cap R \underbrace{=}_{\text{Proposition 4.8 in [2]}} (R - P_i)\mathfrak{q}_i \cap \bigcap_{j \neq i} R_{P_i} \cap R = (R - P_i)\mathfrak{q}_i \cap R = \mathfrak{q}_i$.

In the corollary, the necessity comes from this; suppose R is normal. Then, (b) is from Theorem 11.5. (a) is from Theorem 11.2(4). In the sufficient condition, if a is integral over R, then it is integral over all R_P with height P, hence a is in R_P with all height 1 primes by (a), thus $a \in R$.

In proof of Theorem 11.6, (2) $\implies$ (1), when R is 1-dimensional Noetherian normal domain, the for every maximal ideal P, R_P is 1-dimensional Noetherian local normal domain, thus by Theorem 11.2 (3), R_P is DVR as well as PID. Also, PR_P is principal. Then, if $(x/y)R_P = PR_P$, then $xR_P = PR_P$ since y is unit, hence $(x) = P$. Thus all maximal ideals of R are principal. Now, R is one-dimensional domain, thus all prime ideals are principal. Hence, by the below claim, R is PID. Lastly, to see R is Dedekind ring, we will use Theorem 11.3 by showing that every finitely generated fractional ideal I is principal when it is localized by any maximal ideal. Let I be a finitely generated fractional ideal. Then, I_P is also a fractional ideal of R_p, thus there exists $\alpha \in R_P$ such that $\alpha I_P \subseteq R_P$. Thus, αI_P is a submodule of R_P. Hence, αI_P is a principal ideal (maybe non-proper), so we may say $\alpha I_P = (\beta)$. Then, I_P is generated by (β/α), hence principal fractional ideal.

Claim 9. *For an integral domain R, PID is local property; in other words, the followings are equivalent.*

1. *R is PID*
2. *all elements of* $\operatorname{Spec}(R)$ *are principal.*

Proof. Since (1) $\implies$ (2) is obvious, I just show (2) $\implies$ (1). Let N be collections of all nonprincipal ideal ordered by inclusion. Suppose R is not PID. Then, N is nonempty. Also, for an ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$, let $\mathfrak{a} = \bigcap_{i=1}^{\infty} \mathfrak{a}_i$. Then, $\mathfrak{a}$ is an ideal; to see this, for any $a \in \mathfrak{a}$, $a \in \mathfrak{a}_i$ for some i, thus $aR \subseteq \mathfrak{a}$. Also, it is closed under addition. Moreover, $\mathfrak{a}$ is not a principal; if it was, then we may say $\mathfrak{a} = (b)$ for some $b \in R$. Then, $b \in \mathfrak{a}_i$, thus $(b) \subseteq \mathfrak{a}_i \subseteq (b)$ implies $\mathfrak{a}_i$ is principal, contradicting the assumption that $\mathfrak{a}_i \in N$. Hence, by Zorn's lemma, N has maximal elements. Let $\mathfrak{a}$ be such a maximal element. Then, it is not a principal, thus by (2), it is not a prime. Hence, there exist $b, c \in R$ such that $b, c \notin \mathfrak{a}$ but $bc \in \mathfrak{a}$. Then, let $\mathfrak{b} := (\mathfrak{a}, b), \mathfrak{c} := (\mathfrak{a}, c)$. Since both contains $\mathfrak{a}$, thus they are not in N, thus principal; let $\mathfrak{b} = (\beta), \mathfrak{c} = (\gamma)$. Then, let $P = (\mathfrak{a} : \beta)$. First of all, P contains $\mathfrak{a}$ by definition of ideal, thus P is principal; say $P = (\beta')$. Then, $\beta'\beta \in \mathfrak{a}$, hence $P\mathfrak{b} \subseteq \mathfrak{a}$. Conversely, both P and $\mathfrak{b}$ contains $\mathfrak{a}$, thus $P\mathfrak{b} \supseteq \mathfrak{a}$, which implies $P\mathfrak{b} = \mathfrak{a}$, contradicting the assumption that $\mathfrak{a}$ is not principal. □

In the proof (1) $\implies$ (3), J should be changed to I. And, if $I = IP$, $I_P = I_PPR_P$, thus by NAK, $I_P = 0$. Thus, I=0, which lead contradiction that zero ideal is also a product.

In step 2 of (3) $\implies$ (1), $a^2R + P = I^2 = (P + aR)^2$. In step 3, if P_i is just prime ideal, then we have an ideal I strictly greater than P_i, then step 2 implies $IP_i = P_i$, and P_i is invertible, since bR is invertible. Thus, by multiplying P_i^{-1} both sides, get $I = R$.

In the Krull-Akizuki theorem, the remark can be derived from Proposition 2.8 of [2], a vector space version of NAK.

In the proof of Lemma, such $t \in A$ exists since $\eta \otimes 1 = \sum_{i=1}^{r} a_i\xi_i \otimes 1/b_i$ in $M \otimes_A K$, thus we may let $t = \prod_i^r b_i$. Also, each $\mathfrak{p}_i$ maximal implies that the chain is actually a composition series, hence length is m. Also, the inequality $l(M/aM) \leq l(E/aE)$ can be derived by letting $n > m$. Lastly, B/P is Artinian since $l(B/P) \leq l(B/pB) < \infty$, thus descending chain condition already holds. Lastly,

Claim 10. *If R is an Artinian Integral domain, then R is a field.*

Proof. Given $x \in R$, (x^i) gives us descending chain of ideals, thus from Artinian, $(x^N) = (x^{N+1})$ for some $N > 0$. Then, $x^{N+1}y = x^N$ for some $y \in R$. Thus, $x^N(xy-1) = 0$ implies y is inverse of x, since it is integral domain. Hence every elements has its inverse. $\square$

1. Let B be a valuation ring of $\overline{K}$ dominating A, and G its value group. Then for $\alpha \in \mathfrak{m}_B$ we have $\sqrt{\alpha} \in \mathfrak{m}_B$ because $\sqrt{\alpha} \in \overline{K}$ and $v_B(\sqrt{\alpha}) > 0$, so that G has no minimal element.

   Moreover, given $\alpha \in \mathfrak{m}_B$, α is algebraic over A, thus $\sum_i^n a_i\alpha^i = 0$ for suitable n. Thus, $(\sum_i^n iv(a_i))v(\alpha) \in v(K^*)$. Hence, a multiple of $v(\alpha)$ belongs to $v(K^*) \cong \mathbb{Z}$. Thus, we may assume G be a subgroup of $\mathbb{Q}$, hence G is Archimedean. By Theorem 10.7, B is of 1-dimension. Moreover, for any $m \in \mathbb{N}$, we may take $\sqrt[m]{\alpha} \in B$ for any nonzero $\alpha \in \mathfrak{m}_A$, hence $v(\alpha)/m \in G$ for any m. This shows that $G \cong \mathbb{Q}$. Hence, G is strictly bigger than $\mathbb{Z}$, which implies that B is non-discrete valuation ring.

2. If B is a valuation ring of L dominating A, then by Krull-Akizuki theorem, B is a Noetherian local ring of dimension 1 (since $\mathfrak{m}_B$ is cannot be zero due to the fact that B dominates A, i.e., $\mathfrak{m}_B \cap A = \mathfrak{m}_A \neq 0$ by construction) Now, we will use Theorem 11.2 (3) to show that B is DVR. (Remark; it seems difficult to use (4) since there are no clues to show that B is normal.) Since B is Noetherian, $\mathfrak{m}_B$ is finitely generated, say $\mathfrak{m}_B = (a_i)_{i=1}^n$ for some $n > 0$. Now, wlog, we may assume $v(a_1) < v(a_i)$ for all $i > 1$. Then, $v(a_i/a_1) > 0$ implies $a_i/a_1 \in B$, thus $\mathfrak{m}_B = (a_1)$, thus principal.

3. Suppose $(t) = \mathfrak{m}_A$. Notes that in the completion of DVR, the valuation of Cauchy sequence $\{b_i\}$ of A is determined as $v(\{b_i\}) = \lim_{n\to\infty} v(b_n)$. To see this converges, notes that every Cauchy sequence $\{b_i\}$ is of form $\{b_i = \sum_{j=1}^i a_j\}$ where $a_i \in \mathfrak{m}^i \subset A$. In our cases of DVR, let $a_i = u_it^i$ where u_i is unit or zero. Thus, let k be the minimal index such that $u_i \neq 0$. Then, for $i > k$, $b_i = u_kt^k + u_{k+1}t^{k+1} + \cdots + u_it^i = t^k(u_k + t(\cdots))$. Since A is local ring, $(u_k + t(\cdots))$ is unit, thus $b_i \in (t^k)$ for all $i > k$. Hence, $\lim_{n\to\infty} v(b_n) = k$. Thus, the function v is well-defined. Moreover, $v(\{b_i\}\{c_i\}) = v(\{b_i\}) + v(\{c_i\})$ since multiplication of the smallest nonzero t-term induces the sum of two smallest t-term in each Cauchy. Likewise, $v(x+y) \geq \min(v(x), v(y))$ and $v(x) = \infty \iff x = 0$ is clear. Hence, $\tilde{A}$ is DVR.

4. Suppose an open ball $B_r(\alpha)$ by d at $\alpha \in K$ with radius c^r. Then, $\beta \in B_r(\alpha)$ iff $v(\alpha - \beta) \leq r$. Let $\alpha \in R$. Then, $B_r(0) \cap R = \{\beta \in R : v(-\beta) < r\} = \mathfrak{m}_R^{\lfloor r \rfloor}$. Moreover, for any $\alpha \in R$, $B_r(\alpha) \cap R = \{\alpha + \beta \in R : v(-\beta) < r\} = \alpha + \mathfrak{m}_R^{\lfloor r \rfloor}$. Hence, the base of subspace topology of R coincide with $\mathfrak{m}$-adic topology on R.

5. From Theorem 5.7, the ideal I is generated by at most $\sup\{\mu(p, I) + \operatorname{coht}\mathfrak{p} : \mathfrak{p} \in \operatorname{Supp}(I)\}$ where $\mu(p, I)$ the dimension over $\kappa(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ of $I \otimes \kappa(\mathfrak{p})$. Here, $\operatorname{coht}\mathfrak{p} \leq 1$ by Theorem 11.6. Also, if $\mathfrak{p}$ is a maximal ideal containing I, then $A_\mathfrak{p}$ is DVR, which means that $I_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^n$ for some $n > 0$, thus $I \otimes \kappa(\mathfrak{p}) = 0$, which implies $\mu(p, I) = 0$. Otherwise, if $I \cap A - \mathfrak{p} \neq 0$, then $I_\mathfrak{p} = A_\mathfrak{p}$, hence $I \otimes \kappa(\mathfrak{p}) = \kappa(\mathfrak{p})$, thus $\mu(I, \mathfrak{p}) = 1$. In any cases, $\mu(I, \mathfrak{p}) \leq 1$, this implies I is generated by at most 2 elements.

6. First of all, for $a + b\sqrt{10} \in \mathbb{Q}(\sqrt{10})$ with $a, b \in \mathbb{Q}$, then it is a solution of $x^2 - 2ax + a^2 - 10b^2 = 0$ Thus, $a + b\sqrt{10}$ is integral over $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{10})$ iff $2a \in \mathbb{Z}$ and $a^2 - 10b^2 \in \mathbb{Z}$. So for a, there are two cases; first of all, if $a \in \mathbb{Z}$, then $10b^2 \in \mathbb{Z}$ implies $b \in \mathbb{Z}$. Otherwise, if $a = \frac{a'}{2}$ for some odd $a' \in \mathbb{Z}$, then $\frac{(a')^2}{4} - 10b^2 \in \mathbb{Z}$. Hence, $10b^2 = \frac{(a')^2}{4}$, thus $(a')^2 = 40b^2$. However, this cannot hold, since the lefthandside is odd, while the righthandside is even. Hence, $A = \mathbb{Z}[\sqrt{10}] = \mathbb{Z}[X]/(X^2 - 10)$.

   Next, to see it is not a principal ideal domain, choose $I = (2)$. Then, $A/I = A/2A \cong \mathbb{Z}[X]/(2, X^2 - 10) \cong \mathbb{Z}[X]/(2, X^2) \cong \mathbb{Z}/2\mathbb{Z}[X]/(X^2)$, which is not a domain. However, in case of $J = (2, \sqrt{10})$, $A/J \cong \mathbb{Z}[X]/(2, X, X^2 - 10) \cong \mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$, which is a field. Hence, J is prime (and maximal), and $J \neq I$. One can show it is not principal by norm-argument in undergraduate algebraic number theory; if $a + b\sqrt{10}$ generates J, then $N(a + b\sqrt{10}) = a^2 - 10b^2$ should be ± 2. However, $a^2 \equiv \pm 2 \bmod 5$ has no solution, so it is impossible.

7. Let $\{P_i\}_{i=1}^n$ be m-Spec of A. This coincide with Spec $A \setminus \{(0)\}$ since A is Dedekind ring, thus by 11.6(2), all nonzero prime ideals are maximal. Then, we may choose $\alpha \in P_1$ such that $\alpha \notin P_1^2 \cup P_2 \cup \cdots \cup P_n$. To see this, by Proposition 1.11 of [2], P_1 cannot be contained in $P_2 \cup \cdots \cup P_n$, hence $P = P_1 \setminus (P_2 \cup \cdots \cup P_n)$

is nonempty. Moreover, if $P \subseteq P_1^2$, then all generators of P_1 should be inside of $(P_2 \cup \cdots \cup P_n)$, which implies $P_1 \subseteq (P_2 \cup \cdots \cup P_n)$, contradiction. Hence, for each i, we may choose $\alpha_i \in P_i \setminus (P_i^2 \cup \bigcup_{j \neq i} P_j)$. Then, in A_{P_i}, $\alpha A_{P_i} = P_i A_{P_i}$ since $v(\alpha) = 1$ and A_{P_i} is DVR. Hence, $P_i = \alpha_i A$. Then, since by Theorem 11.6(3), any ideal is product of primes, thus principal.

8. As we did in Exercise 10.2, we will use Theorem 7.7. If M is flat, then for any principal ideal (a), $(a) \otimes M \to A \otimes M \cong M$ is injective for any a. Hence, $am \neq 0$ for any $m \in M$ if $a \neq 0$, thus M is torsion-free. Conversely, if M is torsion-free, then by Exercise 11.5, we may assume $I = (a, b)$ for some $a, b \in R$. Then, for any element $ta + ub \in I$ for some $t, u \in A$, $(ta + ub) \otimes m \mapsto (ta + ub)m \neq 0$ if $ta + ub \neq 0$ since M is torsion free. Hence, if $(ta + ub) \otimes m$ is in kernel of $I \otimes M \to A \otimes M \cong M$, then $ta + ub = 0$. Hence, the kernel is zero, and $I \otimes M \to M$ is injective for any ideal I.

9. If (1) holds, then for any A-module M, M_P is flat iff M_P is torsion-free for any maximal ideal P by Exercise 10.2. By Propostion 3.10 in [2], flatness is local property, thus M is flat iff M_P is torsion free for all maximal ideal P. Thus, it suffices to show that M is torsion free iff M_P is torsion free for all maximal ideals P.

   If M is torsion free, then for any $0 \neq a \in A, m \in M$, $am \neq 0$. Thus, if $(a/b)(m/s) = 0$ in M_P where $0 \neq a \in A, b \in A \setminus P$, then $tam = 0$ for some $t \in A \setminus P$, hence $ta = 0$; since $t \neq 0$, and A is domain, thus $a = 0$, contradiction. Hence, M_P is torsion-free. Conversely, suppose M_P is torsion-free for any maximal ideal P of A. Then, if $am = 0$ for some nonzero $a \in A$, $m \in M$, then $(a/1)(m/1) = 0$ in M_P for some maximal ideal P, thus one of $a/1$ or m should be zero; which implies either a or m is zero, contradiction.

10. By Exercise 11.8, a finite torsion-free module is flat, thus projective. Now, we use induction on rank, where rank of a finitely generated module M over the domain A is $\dim_K(M \otimes_A K)$ where K is field of fraction of A.

    First of all, if rank of finitely generated torsion-free module M is 1, then $M = M \otimes A \subseteq M \otimes K = K$ since M is flat and $0 \to A \to K$ is exact. Hence, M is a submodule of K. Also, M is finitely generated; hence if $M = (a_1/b_1, \cdots, a_n/b_n)$, then $b = b_1 \cdots b_n$ makes $bM \subseteq A$. Thus, M is a fractional ideal, and isomorphic to an ideal bM by the multiplication map $\cdot b$ and $\cdot 1/b$, done. Suppose it holds for rank with less than n. Then, in M, pick a submodule M' generated by a preimage of basis except one element of $M \otimes_A K$. Then, M' is of rank $n-1$, thus M' is a direct sum of ideals by inductive hypothesis. Now, $0 \to M' \to M \to M/M' \to 0$. Here, M/M' is of rank 1, thus fractional ideal by the same argument we did for the base case of rank 1, hence projective. Thus, $M = M' \oplus M/M'$, and both M' and M/M' are direct sum of ideals, so is M.

12 Krull rings

In the proof of lemma 1 (Nagata), when $a \notin R_i$, then $a^{-1} \in \mathfrak{m}_i$ by DVR, and notes that $a^i \notin R_i$ also; otherwise a^{-1} is unit, contradiction. Hence, $1 + a + \cdots + a^{s-1} \notin R_i$ thus $(1 + a + \cdots + a^{s-1})^{-1} \in R_i$. Also, $a(1 + a + \cdots + a^{s-1})^{-1} \in R_i$, otherwise, $a^{-1}(1 + a + \cdots + a^{s-1}) \in R_i$, thus $(1 + a + \cdots + a^{s-1}) \in R_i$ since we have a^{-1}, and by some iterative calculation one can conclude that $a \in R_i$, contradiction.

Also, if $1 - a^t \notin m_i$ for any t, then $(1 - a^s)$ is unit, thus $(1 - a^s)^{-1} = (1 - a)^{-1} \cdot (1 + a + \cdots + a^{s-1})^{-1}$, hence $(1 - a)(1 - a^s)^{-1} = (1 + a + \cdots + a^{s-1})^{-1}$ exists in R_i. Moreover, $a(1 + a + \cdots + a^{s-1})^{-1} \in R_i$ since $a \in R_i$ also.

If $(1 - a) \in m_i$ and s is not the characteristic of R_i/m_i, then $1 - (1 - a) = a$ is unit. By reducing mod m_i, the element $1 + a + \cdots + a^{s-1}$ becomes sa, which is invertible. Since R is a local ring, any element of R which is invertible mod R is invertible in R, thus $1 + a + \cdots + a^{s-1}$ is invertible in R.

If $(1 - a) \notin m_i$ but $1 - a^t \in m_i$ for some $t > 1$, let t_0 be the smallest one such that $1 - a^{t_0} \in m_i$. Then, again a^{t_0} is unit, and $1 - a^{dt_0}$ is multiple of $(1 - a^{t_0})$ with suitable $(1 + a + \cdots + a^s)$, thus is in m_i. This shows that $1 - a^s \in m_i$ when s is multiple of t_0. In this case, $(1 + a + \cdots + a^{s-1})^{-1} \notin R_i$, otherwise $(1 - a) \in m_i$, contradicting the assumption. If s is not a multiple of t_0, then by mod m_i, $1 - a^s = \equiv a^{t_0} - a^s$. If we suppose $s < t_0$, then $1 - a^{t_0 - s} \in R/m_i$. This should be nonzero for not contradicting the minimality of t_0. If $s > t_0$, then there exists $d > 0$ such that $0 < r := s - dt_0 < t_0$. Since $1 - a^{dt_0} \in m_i$,

$1 - a^s = \equiv a^{dt_0} - a^s \equiv a^{dt_0}(1 - a^r) \in R/m_i$. Again, $(1 - a^r) \neq 0$ in R/m_i, otherwise it contradicts the minimality of t_0. In any cases, $1 - a^s \notin m_i$, hence $1 - a^s$ is unit, thus $(1 - a) \cdot (1 - a^s) = 1 + a + \cdots + a^{s-1}$ is invertible in R.

In the proof of Theorem 12.2, if R_is are DVR, the choice of x_i is from the argument in Exercise 11.7; see the solution of the exercise in this note. Also, when showing $\mathcal{F}_0$ is defining family, then the implication is just restate of $b/a \in \bigcap A_P \implies b/a \in A$. For example, if there are another prime ideal P belonging to aA, then we may take $t \in aA \cap (P \setminus \bigcup_{\mathcal{F}_0} \mathfrak{p}_i$, and t is unit in each localization, thus the implication implies $aA = A$, contradiction when a is nonunit. Also, this only can be done when the primary decomposition of aA by height 1 prime ideals exists. Also, "Theorem 2 implies $\mathcal{F}'$ is infinite" is came from the fact that PID is 1-(Krull) dimensional. The existence of R' come from that $v(a) > 0$ is finitely many. Now, $A_{p_1} \subset R'$ implies $p' \subset p_1$ is came from Theorem 10.1(i). Lastly, $b/a \in A$ lead contradiction such that $b = (b/a)a \in aA$, but by construction $b \notin aA$.

Claim 11. *PID ring R is 1-dimensional.*

Proof. Let (a) be a nonzero prime ideal. If it is not maximal, then there exists a maximal ideal (b) containing (a). Then, $a = br$ for some $r \in R$. Since $b \notin (a)$, $r \in (a)$ since (a) is prime. Thus, $r = ac$ for some $c \in R$, thus $a(1 - bc) = 0$ implies that $1 - bc = 0$. Thus $(b) = R$, contradiction. $\square$

Claim 12. *PID is Dedekind domain.*

Proof. It is integrally closed since ufd, and its localizations are pid, thus all integrally closed (again, ufd) so normal, and 1-dimensional Noetherian domain, thus Dedekind. $\square$

Claim 13. *Dedekind domain is Krull ring.*

Proof. it is intersection of all localizations by maximal ideal, and by the finiteness of primary decomposition (from Noetherian) assures the finitely many nonzero condition for valuation at specific element., $\square$

In the proof of Theorem 12.4, (i) Theorem 11.5 with finite primary decomposition (from Noetherian property) just satisfy the definition of Krull ring. For (ii), given families of DVRs for A_i, by taking intersection with K, we all assumes that $A_i \cap K$ are Krull ring in K, and the finiteness condition of valuation still holds. For (iii), since all PID is Dedekind domain thus Krull ring. Also,

Claim 14. $K[X] \cap A[X]_{P[X]} = A_P[X]$

Proof. By construction, $K[X] \cap A[X]_{P[X]} \supseteq A_P[X]$. Conversely, let $f(x) \in K[X] \cap A[X]_{P[X]}$. Then, $f(x) = \sum_i^n a_i x^i$ with $a_i \in K \cap A[X]_{P[X]} = A_P$, done. $\square$

Lastly, in B_λ, don't forget that X is unit; thus $\varphi(X) = X^r(a_r + \cdots)$, and it is unit iff $(a_r + \cdots$ is unit in B_λ as well as $R_\lambda[[X]]$, which holds iff a_r is unit.

Honestly, I think theorem 12.5 should be suggested in front of the section.

1. Given a finite extension, take a finite normal extension containing that finite extension (for example, Theorem VI.1.12 of Lang for this), thus we may assume L/K is Galois. Let O be a valuation ring of L dominating R. Then, let R^* be the integral closure of R in L. Then, since O is integrally closed in L, O contains R^*. Moreover, $\mathfrak{m}_O \cap R^*$ is also maximal ideal of R^* lying over $\mathfrak{m}_R$. By Theorem 9.3 (iii), all such prime ideals of R^* lying over $\mathfrak{m}_R$ are conjugate over K. This implies that there are always finitely many such O, since all possible $\mathfrak{m}_O \cap R^*$ are of finite.

   Now, let $G = \mathrm{Aut}_K(L)$. Let S_1 and S be valuation rings of L dominating R, and let $S_1, S_2, \ldots, S_r$ be the conjugates of S_1 by elements of G, and $A = S_1 \cap \cdots \cap S_r \cap S$. If $S \neq S_i$ for any i then by Exercise 10.9, there are no inclusions among $S_1, \ldots, S_r, S$, and we can apply Theorem 12.2. Letting $\mathfrak{n}, \mathfrak{n}_i$ be the maximal ideals of S, S_i, and setting $\mathfrak{n} \cap A = \mathfrak{p}, \mathfrak{n}_i \cap A = \mathfrak{p}_i$ we have $\mathfrak{p}_1 \cdots \mathfrak{p}_r \not\subseteq \mathfrak{p}$, so that we can choose $x \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ with $x \notin \mathfrak{p}$. Then $x \notin \mathfrak{n}$, but since $x \in (\mathfrak{n}_1)^{\sigma^{-1}}$ for all $\sigma \in G$, all the conjugates of x over K belong to $\mathfrak{n}_1$. Thus, by Vieta's formula, all the coefficients of the minimal polynomial of x over K belongs to not only K but $\mathfrak{n}_1$, i.e., in $\mathfrak{n}_1 \cap K = \mathfrak{m}_R$ (recall that R is valuation ring, thus local, and by domination, $S \cap K = S_i \cap K = R$ for all i.) Thus, these coefficients are contained in $\mathfrak{p}$, thus the minimal polynomial of x evaluated at x is in $\mathfrak{p}$, hence x is not unit in $A_\mathfrak{p}$, thus $x \in \mathfrak{p}$, which implies $x \in \mathfrak{n}$, a contradiction.

2. This is the same as Proposition 6 of [3][§8, Proposition 6, p.427]. Let v_R be the valuation map over R. We claim that

Claim 15. *Let $\mathcal{B}$ be the set of all valuation rings on L whose valuation map extends v_R. Then, the map $V \mapsto m(V) \cap \overline{R}$ and and $\mathfrak{m} \mapsto \overline{R}_{\mathfrak{m}}$ induces a bijection between $\mathcal{B}$ and $m-\mathrm{Spec}(\overline{R})$.*

Proof. By Lemma 2 of Section 9, Every maximal ideal $\mathfrak{m}$ of $\overline{R}$ is such that $\mathfrak{m} \cap R$ is the maximal ideal of R. Also, by Theorem 10.2, for each maximal ideal $\mathfrak{m}$ of $\overline{R}$, there exists a valuation ring V of L such that V dominates $\overline{R}_{\mathfrak{m}}$. Thus, $V \supseteq \overline{R}_{\mathfrak{m}}$. Now, we claim $V = \overline{R}_{\mathfrak{m}}$. To see this, we may assume that L is the union of a directed family of sub-extensions K_α of L which are finite over K. Hence, $V = \overline{R}_{\mathfrak{m}}$ iff $V \cap K_\alpha = \overline{R}_{\mathfrak{m}} \cap K_\alpha$ for all α. Now let $\overline{R}_\alpha := \overline{R} \cap K_\alpha$, then $\overline{R}_\alpha$ is the integral closure of R in K_α. Hence by Exercise 10.3, it is intersection of valuation rings of K_α dominating R. Thus, by Exercise 10.10, all valuations of valuation rings consisting of the intersection actually extends v_R. Moreover, by Exercise 12.1, valuation rings consisting of the intersection is finitely many. Also, by Theorem 12.2, since $\overline{R}_\alpha$ is the intersection of distinct valuation rings, it is a semi-local ring, moreover, each valuation ring consisting of the intersection is just the localization of $\overline{R}_\alpha$ by its maximal ideal. Thus, we may write that given $m-\mathrm{Spec}(\overline{R}_\alpha) := \{\mathfrak{m}_1, \cdots, \mathfrak{m}_n\}$, $\bigcap_{i=1}^n (\overline{R}_\alpha)_{\mathfrak{m}_i} = \overline{R}_\alpha$ and $\{(\overline{R}_\alpha)_{\mathfrak{m}_i}\}_{i=1}^n$ are all valuation rings dominating R in K_α. Thus, since $V \cap K_\alpha$ is still a valuation ring dominating R, it should be one of $\{(\overline{R}_\alpha)_{\mathfrak{m}_i}\}_{i=1}^n$. WLOG, let $V \cap K_\alpha = (\overline{R}_\alpha)_{\mathfrak{m}_1}$. Now, we claim that $\mathfrak{m} \cap \overline{R}_\alpha = \mathfrak{m}_1$, which completes the proof (if it holds, then $V \cap K_\alpha = (\overline{R}_\alpha)_{\mathfrak{m}_1} \subseteq \overline{R}_{\mathfrak{m}} \cap K_\alpha$.) To see this, again, by Lemma 2 of Section 9 with the fact that $\overline{R}$ is integral closure of $\overline{R}_\alpha$ in L, $\mathfrak{m} \cap \overline{R}_\alpha = \mathfrak{m}_i$ for some i. Also notes that $\overline{R}_{\mathfrak{m}} \cap K_\alpha = (\overline{R}_\alpha)_{\mathfrak{m}_i}$ ($\supseteq$ is obvious; if $x/y \in \overline{R}_{\mathfrak{m}} \cap K_\alpha$, then we may assume $x, y \in K_\alpha$ by suitable multiplication, then $x, y \in \overline{R} \cap K_\alpha = \overline{R}_\alpha$ and $y \in \overline{R}_\alpha \setminus \mathfrak{m} = \overline{R}_\alpha \setminus \mathfrak{m}_i$ implies the equality.) Hence, $i = 1$, otherwise $V \cap K_\alpha = (\overline{R}_\alpha)_{\mathfrak{m}_1}$ contains $(\overline{R}_\alpha)_{\mathfrak{m}_i}$, implying $\mathfrak{m}_1 \subseteq \mathfrak{m}_i$, contradicting maximality of $\mathfrak{m}_1$. Thus, $V \cap K_\alpha = (\overline{R}_\alpha)_{\mathfrak{m}_i} \subseteq \overline{R}_{\mathfrak{m}}$, which completes the proof that $V = \overline{R}$.

Conversely, if $V \in \mathcal{B}$, then by Theorem 12.2, $V \supseteq \overline{R}$ (since V dominates R, so contain R's integral closure). Let $\mathfrak{m}_V$ be the maximal ideal of V, and let $\mathfrak{m} = \mathfrak{m}_V \cap \overline{R}$. Then, $\mathfrak{m} \cap R = \mathfrak{m}_V \cap R$ is the maximal ideal of R, thus by Lemma 2 of Section 9, $\mathfrak{m}$ is the maximal ideal of $\overline{R}$. Then, by the above argument with the facts that $\mathfrak{m}_V \cap \overline{R}_{\mathfrak{m}} = \mathfrak{m}R_{\mathfrak{m}}$ (thus V dominates $R_{\mathfrak{m}}$) $V = \overline{R}_{\mathfrak{m}}$. ☐

3. Let $\{A_i\}_{i \in \Lambda}$ be the defining collection of DVRs of A. Let $\overline{A_i}$ be the integral closure of A_i. By the corollary of Krull-Akizuki theorem, $\overline{A_i}$ is a Dedekind ring. By Corollary of Theorem 11.5, for any nonzero prime ideal P of $\overline{A_i}$, (since its height is 1), $\overline{A_i}_P$ is DVR dominating A_i. By Exercise 12.1, there are finitely many valuation rings dominating A_i, and by Exercise 12.2, all such valuation ring dominating A_i is of form $\overline{A_i}_P$, thus $\overline{A_i}$ is semi-local. Hence, $B = \bigcap_i \overline{A_i} = \bigcap_i \bigcap_{P \in \mathrm{Spec}(A_i) \setminus \{0\}} \overline{A_i}_P$ where for each i, $|\mathrm{Spec}(A_i)| < \infty$. Thus, B satisfy the first condition of Krull ring.

   Instead of showing the second condition, I will use Theorem 12.4 (ii); since each $\overline{A_i}_P$ is DVR, thus Krull rings, so it suffices to show that given any nonzero $b \in B$, $b\overline{A_i}_P = \overline{A_i}_P$ for all but finitely many i (with some P). To see this, let $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ since b is integral over A. Then, for each a_i is units for all but finitely many. Hence, we may assume that $\{a_i\}_{i=0}^{n-1}$ is a set of units for all but finitely many i. Then, pick such A_j where all a_is are unit. Then, since $a_0 = -b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)$, $1 = -b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)a_0^{-1} \in \overline{A_j}$ implies that b is unit. Hence, except for finitely many js, b is unit. Done.

4. Let $\mathscr{P}$ be the set of height 1 prime ideals of A, and for $\mathfrak{p} \in \mathscr{P}$ by Theorem 12.3 $A_{\mathfrak{p}}$ is DVR, so Dedekind, hence every fractional ideals of $A_{\mathfrak{p}}$ is invertible. Hence, by Theorem 11.3 (iii), set $I_{\mathfrak{p}} = a_{\mathfrak{p}}A_{\mathfrak{p}}$. for some $a_{\mathfrak{p}} \in K$ Then $x \in \tilde{I} \Leftrightarrow xI^{-1} \subset A_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathscr{P} \Leftrightarrow x \in a_{\mathfrak{p}}A$ for all $\mathfrak{p} \in \mathscr{P}$. (To see the last iff, for $y \in I^{-1}$, then $yI \subseteq A \iff$ for $y \in I^{-1}$, $yI_{\mathfrak{p}} \subseteq A_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathscr{P} \iff$ for $y \in I^{-1}$, $ya_{\mathfrak{p}} \in A_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathscr{P} \iff$ for $y \in I^{-1}$, $y \in a_{\mathfrak{p}}^{-1}A_{\mathfrak{p}}$. Hence, for any $y \in I^{-1}$, $xy \in A_{\mathfrak{p}}$ implies that $x \in a_{\mathfrak{p}}A_{\mathfrak{p}}$; to see this, $y = a_p^{-1}b$ for some $b \in A_{\mathfrak{p}}$, and we may write $a_{\mathfrak{p}} = c/d$ for some $c, d \in A_{\mathfrak{p}}$, hence $y = bc/d$, thus $xy \in A_{\mathfrak{p}}$ implies that $x = c \cdot e$ for some $e \in A_{\mathfrak{p}}$, hence $x = a_{\mathfrak{p}}d \in A_{\mathfrak{p}}$. The converse is obvious.)

   Now notes that by Theorem 12.3, the family of DVR generating A is $\{A_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{P}}$, and since A is Krull ring, the valuation of x in $A_{\mathfrak{p}}$ is 0 except finitely many such localizations. If $x \in a_{\mathfrak{p}}A_{\mathfrak{p}}$ has zero from the valuation of $A_\mathfrak{p}$, then $x = a_\mathfrak{p} b$ for some $b \in A_\mathfrak{p}$ is unit in $A_\mathfrak{p}$. Hence, $I_\mathfrak{p} = A_\mathfrak{p}$ since I is not only a fractional ideal but also the ideal of $A_\mathfrak{p}$. Thus, we may write

$$I = (\bigcap_{i=1}^{n} I_{\mathfrak{p}_i} \cap A) \cap (\bigcap_{\mathfrak{p} \in \mathcal{P} \setminus \{\mathfrak{p}_i\}} (I_\mathfrak{p} \cap A)) = (\bigcap_{i=1}^{n} I_{\mathfrak{p}_i} \cap A) \cap (\bigcap_{\mathfrak{p} \in \mathcal{P} \setminus \{\mathfrak{p}_i\}} (A_\mathfrak{p} \cap A)) = (\bigcap_{i=1}^{n} I_{\mathfrak{p}_i} \cap A) \cap A = (\bigcap_{i=1}^{n} I_{\mathfrak{p}_i} \cap A).$$

13 Graded rings, the Hilbert function and the Samuelson function

In p.93, $J_n^*/J_{n+1}^* = J_n^{n+1}$ is (maybe) typo; it should be $J_n^*/J_{n+1}^* = J_n/J_{n+1}$.

Claim 16. *A finitely generated module M over an Artinian ring R is of finite length.*

Proof. Since M is finitely generated, we may have an exact sequence $0 \to \ker f \to R^n \xrightarrow{f} M \to 0$ for suitable n and f. Then, R^n is Artinian, thus is of finite length, and its submodule $\ker f$ is also of finite length. Hence, so is M. □

In the proof of 13.2, $g(t)$ is came from difference between $\sum_{i=d_r} l(M_{n+d_r}) - l(L_{n+d_r}$ and $P(M,t) - P(L,t)$.

In the example 1 in p.96, $l(R_n) = l(R_0) \cdot \binom{n+r}{r}$ since we have direct sum inside of R_n of a form (R_0-submodule)$\cdot$(monomial in R_n). Hence, we can add like $N_0 x \to N_1 x \to \cdots N_k x \to N_k x \oplus N_0 y \to \cdots$ and so on.

In example 2, $l(R_n) = \binom{n+r}{r} - \binom{n-s+r}{r}$ since $R_n/(F(x) \cap R_n)$ is nothing but the modding out R_n by image of $R_{n-s} \xrightarrow{F} R_n$; that's why $\binom{n-s+r}{r}$ should be got rid of.

In example 3, $d \geq t$ follows from $(1-t)^{-d} = \sum_{n=0}^{\infty} \binom{d+n-1}{d-1} t^n$.

In p.98, $an + a - 1$ is came from by constructing $\chi_M^{I^a}$ with the fact that $I \subset J$ implies $l(M/I^n M) \geq I(M/J^n M)$.

In p.98, proof of Theorem 13.4, $\mathfrak{m}$ is the defining ideal of A, and $d(A)$ is defined as a degree of $\chi_A^{\mathfrak{m}}(n)$ for suitably big n. By definition, $\sum_{i=0}^{n} l(A/\mathfrak{m}^i) = \sum_{i=0}^{n+1} l(A/\mathfrak{m}^i)$ for some sufficiently big n, which implies $A/\mathfrak{m}^n = A/\mathfrak{m}^{n+1}$. Now apply NAK with the fact that $\mathfrak{m}$ is Jacobson radical. Then, $\mathfrak{m}^n = 0$ implies that Jacobson radical, the intersection of maximal ideals, are nilradical, the intersection of all prime ideals. Hence, there are no prime ideal which are not maximal. For M, $l(M/I^j M) = l(M_n/(M_{n-1} + I^j M_n)) + l(M_{n-1}/(M_{n-2} + I^j M_{n-1})) + \cdots + l(M_1/(M_{0-1} + I^j M_1))$, hence the Samuelson function can be obtained by taking sum for each module as $A/\mathfrak{p}_i$, then the degree is nothing but the largest degree term, which coincides with one of $d(A/\mathfrak{p}_i)$. For the dimension, by applying exact sequences n-times, we have $\operatorname{Supp}(M) = \bigcup_i \operatorname{Supp}(A/\mathfrak{p}_i)$. Hence, $\dim M = \sup\{\operatorname{coht} P : P \in \operatorname{Supp} M\} = \sup\{\operatorname{coht} P : P \in \operatorname{Supp}(A/\mathfrak{p}_i)\} = \max \dim A/\mathfrak{p}_i$.

In step 2, the last inequality came from $\mathfrak{m}^{n-1} M \supseteq (\mathfrak{m}^n M : x_1)$. In step 3, $\mathfrak{m}^n$ is in the annihilator of M for large n since A is Noetherian. Also, such x can be obtained, otherwise, by Proposition 1.11 in [2], $\mathfrak{m}$ is inside of one of $\mathfrak{p}_i$.

In proof of 13.6 (iii), he uses Corollary 5 to get the inequality.

In the proof of Theorem 13.8, $\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong M^n/M^{n+1}$ is isomorphic as a $k = (A/\mathfrak{m}) = R/M$-vector space. Also, the inequality $1 + \deg \varphi \geq \operatorname{tr.deg}_k R$ can be derived from $\deg \chi = d(A) = \delta(A)$ from Theorem 13.4, since if we pick such $\deg \chi$ elements making $l(A) < 0$ and quotient, then it does not have any trascendental elements.

1. $T_u(R_n) = R_n$ is clear. Suppose I is homogenous. If $I = (x_i)_{i=1}^{\infty}$ where each x_i is homogeneous, then $T_u(I) \supseteq I$ by representing $x_i = x_i u^{-k} u^k$ where $k = \deg x_i$. By the same notation we have $T_u(I) = I$. Thus, only if statement holds for any graded ring. Conversely, if $T_u(I) = I$, then let $x \in I$, not necessarily homogeneous. Then we may set $x = y_0 + \cdots + y_n$ where each $y_i \in R_i$. Now, choose $\alpha_i \in k$ with $i \in \{1, \cdots, n\}$ so that

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^n \\ \cdots & & & & \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^n \end{pmatrix} \begin{pmatrix} y_1 \\ \cdots \\ y_n \end{pmatrix} = \begin{pmatrix} T_{\alpha_1}(x) \\ \cdots \\ T_{\alpha_n}(x) \end{pmatrix}$$

Thus, if we can solve this matrix equation, we are done. And the only condition we need to check is that the Vandermonde matrix is invertible; it is well-known that the determinant of Vandermonde matrix is $\prod_{i<j}(\alpha_j - \alpha_i)$. This is nonzero when we choose all distinct α_i. Since k is infinitely many, we can choose such invertible Vandermonde matrix for any $n > 0$. Therefore, I is homogeneous.

2. If I is homogeneous, $T_t(IR') = IR'$ is obvious using the argument in previous exercise. Conversely, if $T_t(IR') = IR'$, let $x \in I \setminus \{0\}$ with $x = y_0 + \cdots + y_n$ where $y_i \in R_i$. Then, $T_t(x) = y_0 + y_1 t + \cdots + y_n t^n \in IR'$. Since IR' consisting of all Laurent polynomial of t whose coefficients are from I, this implies $y_i \in I$.

3. Let $P \in \operatorname{Ass} A$ be the embedded associate prime, i.e.,ht $P \geq 1$ given by problem. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be the prime divisors of (a). If $P \not\subset \mathfrak{p}_i$ for all i, then pick $x \in P \setminus \mathfrak{p}_i$ (this is nonempty by Proposition 1.11 of [2]). Then $(a) : x = (a)$, since for any $b \in (a) : x$, $bx \in (a) \subseteq \mathfrak{q}_i$ implies $b \in \mathfrak{q}_i$ for all i (from $x^n \notin \mathfrak{q}_i$), thus $b \in (a)$, where $\mathfrak{q}_i$ is primary component of (a).

   However, if $xy = 0 \in (a) : x$ implies that $y \in (a)$, thus say $y = ay'$. Then, $xy'a = 0$. But since a is a non-zero divisor, $xy' = 0$, thus $y' \in (a)$. By repeating this, we can conclude that $y \in \bigcap_n a^n A = \{0\}$, thus x is nonzero divisor, contradicting the fact that x is a zero divisor since $x \in P \in \operatorname{Ass} A$. Thus,

   Hence, $P \subseteq \mathfrak{p}_i$ for some i, thus $P + (a) \subseteq \mathfrak{p}_i$. Therefore, $\operatorname{ht} \mathfrak{p}_i \geq 2$. Thus, $\mathfrak{p}_i$ is not a minimal prime ideal according to Theorem 13.5.

4. (i) Let $xy \in P^*$ with $x = x_0 + \cdots + x_n, y = y_0 + \cdots + y_m$ s.t. $x_i, y_i \in R_i$. To get the contradiction, suppose both x and y are not in P^*; then there exists the smallest p and q such that $x_p \notin P^*$ and $y_q \notin P^*$. Hence, the $(p+q)$-grade element of xy, $\sum_{i+j=p+q} x_i y_i$ has a property that all the components except $x_p y_q$ are in P^*. Also, the $(p+q)$-grade component of xy is in P^*, since P^* is a homogeneous ideal. Hence, $x_p y_q \in P^* \subseteq P$ as well, thus x_p or y_q is in P^* since it is homogeneous elements, contradicting assumption that both are not in P^*.

   (a) It suffices to show that $f \notin P, g \notin Q^*$ implies $fg \notin Q^*$. Let $f = f_1 + \cdots + f_r, g = g_1 + \cdots + g_s$ with f_i, g_i are homogenous and $\deg f_i \leq \deg f_{i+1}, \deg g_i \leq \deg g_{i+1}$ for all $i \in [r]$ or $i \in [s]$. If $r = s = 1$, then $g \notin Q^*$ implies $g \notin Q$, thus done.

   Now, suppose $r > 1$. Pick the smallest p and q such that $f_p \notin P$, $g_q \notin Q^*$. Then, $(p+q)$-graded part of fg can be denoted as $\sum_{i+j=p+q} f_i g_j$. Here, all the components except $f_p g_q$ are inside of Q^*. Hence, the $(p+q)$-graded part of fg is not nilpotent on R/Q^*, thus fg is not in Q^*, otherwise $(p+q)$-graded part of fg is in Q^* since Q^* is homogeneous, which implies that $f_p g_q \in Q^*$, contradiction.

5. First of all, we may define grade function $\deg(x/y) := \deg x - \deg y$, which is well-defined. Thus, the direct sum can be derived by partitioning R_S by preimages of elements of $\mathbb{Z}$ under deg map. Hence R_S is graded. Next, $(R_S)_0 = K$ form a field, since all elements are invertible, thus only proper ideal of K is zero ideal. Next, if $R_S \neq K$, then let $t \in R_S$ be an element with smallest positive degree, which coincides with the greatest common divisor of the degrees of elements in S. Now, $\varphi : K[X, X^{-1}] \to R_S$ which maps K to $(R_S)_0 = K$ and X to t. Now give grading on $K[X, X^{-1}]$ by giving $\deg X := \deg t$.

   We claim φ is isomorphism. To show injectivity, let $f \in \ker \varphi$ with $f = \sum_{i \in \mathbb{Z}} a_i X^i$. Then, $\varphi(f) = 0$ implies that $a_i t^i = 0$ since 0 is homogeneous. Thus, all $a_i = 0$ by invertibility of t, thus $\ker \varphi = 0$. To show surjectivity, pick $a \in R_S$ with degree k. If $k = 0$, done. If $k \neq 0$, then $k = j \deg t + r$ with $0 \leq r < \deg t$. Hence, at^{-j} has degree r, which implies that $at^{-j} \in K$ since the least positive degree in R_S is $\deg t$. Now send $(at^{-j})t^j$ by φ to get desired one.

6. First half: let S be the multiplicative set made up of homogeneous elements of R not in P; then $R_S/P^* R_S$ can be viewed as the localisation of R/P^* with respect to all non-zero homogeneous elements, and by the previous question this is $\simeq K\left[X, X^{-1}\right]$, which is a one-dimensional ring. Thus there cannot be chain containing more than P/P^* and $0/P^*$.

   Second half: proof by induction on ht $P = n$; take a prime ideal $Q \subset P$ with ht $Q = n-1$. If $Q \neq P^*$ then Q is inhomogeneous, $Q^* \subset P^*$ and ht $(P/Q^*) \geqslant 2$, so by the first half, $P^* \neq Q^*$, hence ht $P^* \geqslant$ ht $Q^* + 1 = n - 1$.

In the proof of lemma p.104, PB/J' is prime ideal by the same argument; if $f(x)g(x) \in PB$ but $f, g \notin PB$, then we may assume that f and g has the lowest p, q such that the coefficient of f, g at x^p, x^q is not in P, then by comparing with the coefficient of x^{p+q} we get the contradiction.

Also, in the last line of proof, "applying previous argument" means that localizing $R[X]$ by $P[X]$, which makes $a_{11} + X$ is invertible.

14 System of parameters and multiplicity

In the first paragraph, by 13.4 means the argument before Theorem 13.4 about the case when $M = A$.

In the counterexample of proof of 14.1, $(y, x+z)$ is system of parameter since, by calculation $y, x, z \in \sqrt{(y, x+z)}$, i.e., $(y, x+z)$ is m-primary.

For the completing argument of the proof of 14.3, suppose $ax = 0$ for some $a \in R$. Then, ax should be inside of one of the minimal prime ideals contained in xR. However, by the argument in the book, such minimal prime ideal is zero, but x is nonzero, which implies $a = 0$, thus x is not a zero-divisor.

In the proof of Theorem 14.4, it uses the fact that degree of Samuelson function is at most degrees of coefficients of Hilbert polynomials, since Samuelson function is nothing but sums of these coefficients.

In the proof of Theorem 14.5, $\varphi(n) \cdot l(A/q)$ is the upperbound of the length of modules in q^n/q^{n+1} since we may generate a chain as $0 \to x \to Mx \to M'x \to \cdots (m/q)x \to (m/q)x \oplus y \to$, seen in the example 1 of p.96. (Definitely, this chain may contain a repetition due to moding out by q^{n+1}, that's why this is upper bound.) Also, degree of φ is at most $d-1$ by Example 2 of section 13.

Formula 14.2 follows from the fact that degree of Samuelson function is less than d iff $\dim M < d$, thus by definition $e(q, M) = 0$. Formular 14.3 is from $l(M/(q^r)^{n+1}) = \chi_M^q)(rn)$. 14.4 is just from the fact that $q^n M \supseteq (q')^n M$, therefore the difference between Samuelson function should be positive no matter how n goes big, which implies that the leading coefficient must have some orders.

In the proof of Theorem 14.6, first inequality of length came from $M'' = M/M'$ and M'.

First equation of Theorem 14.10 can be obtained by Fomula 14.1 with the case that $d = 0$. Also, in the last equation, the difference in the middle is came from $l\left(M/\mathfrak{q}^n M\right) - l\left(\left(q^{n+1}M : x_1\right)/\mathfrak{q}^n M\right)$, but the first term gives degree d term, but the second term is of at most degree $d-2$, hence it does not effect on the leading coefficient.

In p.113, the assumption $d > 0$ implies that $P_i \not\supset V$, otherwise $P_i = (X_1, \cdots, X_s)$, thus $d = \dim k[X]/Q = \mathrm{ht}(P_i) = 0$, contradiction.

The condition k is infinite implies $V \neq \bigcup_{i=1}^t (V \cap P_i)$ by [7], which is pretty simple. Next, by adding linear forms, and applying the Krull's hauptidealsatz succesively, we may assume that $N = k[X]/(Q, l_1, \cdots, l_d)$ is dimension 0. Hence, for any x_i, there exists n_i such that $x_i^{n_i} \in (Q, l_1, \cdots, l_d)$, otherwise $N \supseteq k[X_1]$ as a subring which implies $\dim N \geq 1$, contradiction. Thus, pick $n := \prod_i n_i$, then $((x_i)_i^s)^{sn} \subseteq (Q, l_1, \cdots, l_d) \subseteq (x_i)_{i=1}^s$, which implies that it is a primary.

In p.114, "If $\varphi_{nv}(\alpha_{ij})$ for $1 \leqslant v \leqslant p_n$ are the $c_n \times c_n$ minors of this matrix then the necessary and sufficient condition for $(X_1, \ldots, X_s)^n \subset (Q, l_1, \ldots, l_d)$ to hold is that at least one of the $\varphi_n(\alpha_{ij})$ is non-zero." can be shown as this argument; for example, if all of $c_n \times c_n$ minors of the given matrix M are zero, then M has rank less than c_n, thus

$$M^T \cdot (n\text{-monomials}) = \begin{pmatrix} K_1 \\ \cdots \\ K_w \end{pmatrix}$$

shows that V_n is not embedded in span of K_is, which is degree n graded parts of $(Q, l_1, \ldots, l_d)$. Otherwise, this map is rank c_n, so V_n is embedded in $(Q, l_1, \ldots, l_d)$.

Next, in Shafarevich's argument, he mentions the fact from [2] that $f \in A[x]$ is zero divisor iff $\exists a \neq 0 \in A$ such that $af = 0$. Thus, if f contains a coefficients from unit, there is no such a, hence not a zero divisor. Also, $l_A(A/\mathfrak{q}^n) = l_{A(x)}(A(x)/\mathfrak{q}^n A(x))$ is came from the general statement $IA(x)/I'A(x) \cong (I/I') \otimes_A A(x) \cong k \otimes A(x) \cong A(x)/\mathfrak{m}A(x)$ as follow; For $I/\mathfrak{q}^n \supsetneq I'/\mathfrak{q}^n$, with $(I/\mathfrak{q}^n)/(I'/\mathfrak{q}^n)$ is simple implies $I/I' \cong k$ and hence $(IA(x)/\mathfrak{q}^n A(x))/(I'A(x)/\mathfrak{q}^n A(x))$ is also simple using the hint so that the two lengths become equal.

1. (a) (Use $I = \mathfrak{m}$ for notation) Suppose $ab = 0$ for some nonzero $a, b \in A$. Then there exists the smallest n, m such that $a \in I^n$ and $b \in I^m$. Thus, $(a + I^{n+1}) \in I^n/I^{n+1}, (b + I^{m+1}) \in I^m/I^{m+1}$ both are

nonzero. Hence, $(a+I^{n+1})(b+I^{m+1})=(ab+I^{n+m+1})$. Since $\mathrm{gr}_I(A)$ is domain, $(ab+I^{n+m+1})$ is nonzero, thus $ab\in I^{n+m}$ but not in I^{n+m-1}, thus ab is nonzero. Hence A is domain.

(b) $(y+\mathfrak{m}^2)(y+\mathfrak{m}^2)=(y^2+\mathfrak{m}^3)=(-x^3+\mathfrak{m}^3)=0$.

2. (a) $(a+\mathfrak{m}^{i_a})(b+\mathfrak{m}^{i_b})=(ab+\mathfrak{m}^{i_a+i_b+1})\neq 0$ implies that $ab\notin\mathfrak{m}^{i_a+i_b})$ and $ab\in\mathfrak{m}^{i_a+i_b}$. This shows the equality.

   (b) Again, $a^*+b^*\neq 0$ implies that $(a+b)$ has leading term in the same graded part.

   (c) First of all, $B/\mathfrak{n}\cong A/\mathfrak{m}$. Also, gives a map $\mathrm{gr}_\mathfrak{n}(B)\to G/I^*$ by $(\overline{a}+\mathfrak{n}^i)\mapsto a^*+I^*$. To see it is well-defined, let $b\in A$ such that $(\overline{a}+\mathfrak{n}^i)=(\overline{b}+\mathfrak{n}^i)$. Then, a^* and b^* in G have the same degree, and $a=b+c$ for some $c\in I$. Thus, $a^*=(b+c)^*=b^*+c^*$ by previous exercise, thus $a^*+I^*=b^*+I^*$.

   Next, this map is surjective; for any a^*+I^*, take the preimage of a^* in A, say a, which gives $(\overline{a}+\mathfrak{n}^i)$ by the construction of a. Also, this map is injective, since if $(\overline{a}+\mathfrak{n}^i)$ sent to 0, then $a^*\in I^*$, hence $a\in I$, thus $\overline{a}=0$, which implies $(\overline{a}+\mathfrak{n}^i)=0$.

3. First statement is came from Exercise 14.2 (i). For the second, this is from [4][Exercise 4.6.12(b)] Let $R=K[[X,Y,Z]]$ and $I=(X^2,XY+Z^3)$. Then $XZ^*\in I^*$ since $X(XY+Z^3)-X^2Y=XZ^3$, but $(X^2)^*=X^2,(XY+Z^3)^*=(XY)$, hence $XZ^3\notin(X^2,XY)$. Moreover, the associated graded ring is just $k[X,Y,Z]$, which is an integral domain.

4. (a) For any $a/b\in K$, then extends $v(a/b)=v(a)-v(b)$, which is defined well since regular local ring is UFD.

   (b) By definition of regular system of parameters, $\mathfrak{m}=(x_1,\cdots,x_d)$ and no set of elements generate $\mathfrak{m}$ if the number of elements in the set is less than d.

   Now, notes that P contains $x_1,\cdots,x_d$, thus $B/P=A/\mathfrak{m}[x_2/x_1,\cdots,x_d/x_1]=k[x_2/x_1,\cdots,x_d/x_1]$, which is integral domain. (If there is a relation $\sum_{i=2}^d c_ix_i/x_1$, then this induces relation between $x_2,\cdots,x_d$ on $\mathfrak{m}/\mathfrak{m}^2$, contradicting the fact that they extends to the canonical basis of $\mathfrak{m}/\mathfrak{m}^2$.)

   Next, to show $R=B_P$, first of all notes that $x_i/x_j\in B_P$ for any i,j. Now, let $t:=a/(b+c_1+\cdots+c_n)$ where $v(a),v(c_i)\geq v(b)$ for some homogeneous elements a,b,c_i in A generated by system of parameters. First of all, $v(b+c_1+\cdots+c_n)=v(b)$, thus $v(a/(b+c_1+\cdots+c_n))=v(a)-v(b)\geq 0$. If $v(a)=v(b)$, then $b/a+c_1/a+\cdots c_n/a$ is inverse of t, and b/a is unit in R_P, and $\sum_i^n c_i/a$ is elements of P, thus $b/a+c_1/a+\cdots c_n/a$ is unit in B_P, which implies $t\in B_P$. If $v(a)>v(b)$, then we may assume that $a=a'd$ for some $a',d\in A$ with $v(a')=v(b)$, then $a/(b+c_1+\cdots+c_n)$ is unit in B_P, thus still $t\in B_P$.

   Lastly, let $t:=(a_0+a_1+\cdots+a_m)/(b+c_1+\cdots+c_n)=\sum_{i=0}^m a_i/(b+c_1+\cdots+c_n)$ with each a_i are also homogeneous elements generated by system of parameters. Then, each component of the sum is in B_P, so $t\in B_P$. Since all $a/b\in K$ with $v(a/b)\geq 0$ are of form $(a_0+a_1+\cdots+a_m)/(b+c_1+\cdots+c_n)$, thus $R\subseteq B_P$. Conversely, all generators of B_P are A and x_i/x_j, which haves non-negative valuations, thus $B_P\subseteq R$, which shows $R=B_P$.

5. Let $s=v(f)$. From the equation $\sum_{i=0}^n l\left(M_i'\right)=l\left(M/I^{n+1}M\right)$ in p. 97, we knows that $l((A/(f))/\mathfrak{m}^n(A/(f)))=\sum_{i=0}^n\mathfrak{m}^i(A/(f))/\mathfrak{m}^{i+1}(A/(f))=\sum_{i=0}^{s-1}\binom{i+d}{d}+\sum_{i=s}^n\left(\binom{i+d}{d}-\binom{i-s+d}{d}\right)=\sum_{i=0}^n\binom{i+d}{d}-\sum_{i=s}^n\binom{i-s+d}{d}$.

   Now use the formula $\sum_{v=0}^n\begin{pmatrix}d+v-1\\d-1\end{pmatrix}=\begin{pmatrix}d+n\\d\end{pmatrix}$ in p.97,

$$l((A/(f))/\mathfrak{m}^n(A/(f)))=\sum_{i=0}^n\binom{i+d}{d}-\sum_{i=s}^n\binom{i-s+d}{d}=\binom{d+1+n}{d+1}-\binom{d+1+n-s}{d+1}.$$

   Hence, by the same argument in Example 2 of p.96, $l((A/(f))/\mathfrak{m}^n(A/(f)))=\frac{s}{d!}x^d+$(lower degree terms), hence the multiplicity is $s=v(f)$.

6. This is the main theorem of [5], whose proof from the Lemma of the book (which is Theorem 2 in [5]) is too long to write down.

7. Recall that Jacobson ring A is a ring such that every prime ideal P should be expressible as an intersection of maximal ideals. To see this, notes that $\operatorname{Spec} A_f = \{\mathfrak{p} \in \operatorname{Spec}(A) : f \notin \mathfrak{p}\}$. So pick $\mathfrak{p} \in \operatorname{Spec} A_f$ as a prime ideal of A. Since $\mathfrak{p} \neq \mathfrak{m}$ (since $f \in \mathfrak{m}$) we knows that $\dim A/\mathfrak{p} \geq 1$. If $\dim A/\mathfrak{p} = 1$, then $(f, \mathfrak{p}) = \mathfrak{m}$, hence $\mathfrak{p}A_f$ is maximal, done. Suppose $r := \dim A/\mathfrak{p} > 1$. Now, pick an arbitrary $g \in \mathfrak{m} - \mathfrak{p}$. Then, choose $x_2, \cdots, x_r \in \mathfrak{m}$ such that

$$\operatorname{ht}(\mathfrak{p}, f, x_2, \ldots, x_i)/\mathfrak{p} = \operatorname{ht}(\mathfrak{p}, g, x_2, \ldots, x_i)/\mathfrak{p} = i$$

for $2 \leqslant i \leqslant r$. (We can choose such element by the fact that $\mathfrak{m} \setminus (\mathfrak{p}, f, g, x_2, \cdots, x_i) \neq \emptyset$ when $i < r-1$. If $i = r-1$, use the fact that $\mathfrak{m}$ is not subset of union of minimal prime divisors of $(p, f, x_2, \cdots, x_i)$ and $(p, g, x_2, \cdots, x_i)$, otherwise by Proposition 1.11, $\mathfrak{m}$ is subset of such minimal divisors, which is nonsense since their coheight in A is 1, but coheight of $\mathfrak{m}$ is 0.) Then any minimal prime divisor P of $(\mathfrak{p}, x_2, \ldots, x_r)$ satisfies $\dim A/P = 1$. Also, $f \notin P$, otherwise P is minimal prime divisor of $(\mathfrak{p}, f, x_2, \cdots, x_r)$ also, thus $P = \mathfrak{m}$, contradiction. Likewise $g \notin P$.

Thus, collect all such minimal prime divisors for arbitrary $g \notin \mathfrak{m} - \mathfrak{p}$. Then, $\mathfrak{p}$ is nothing but intersection of all these collection, which are subst of $m - \operatorname{Spec}(A_f)$.

15 The dimension of extension rings

According to p.47 48, if we let $C = B \otimes_A \kappa(\mathfrak{p}) := B_{f(S)}/\mathfrak{p}B_{f(S)}$ where $S = A \setminus \mathfrak{p}$ and $f(S)$ is its image in B, then for any $P \in \operatorname{Spec}(B)$ with $P = P^* \cap B$ for some $P^* \in C$, $C_{P^*} = B_P/\mathfrak{p}B_P$. Hence, $\dim B_P/\mathfrak{p}B_P \leq \dim B \otimes_A \kappa(\mathfrak{p})$ in the proof of Theorem 15.2.

In the proof of 15.3, we can find Q_0 applying going down theorem on $\mathfrak{p} \supset \mathfrak{q}$ with P_0. $\operatorname{ht}(T_i/Q_0) = 1$ by Krull's Principal ideal theorem with quotienting by Q_0. Also, $P_1 \setminus (\bigcup_i T_i) \neq \emptyset$, otherwise, by [2][Proposition 1.11] $P_1 \subseteq T_i$ for some i, contradicting that their heights are differ.

For choosing Q_1, since P_1 contains $Q_0 + yB$, so there must be a minimal prime divisor contained in P_1, since intersection of all minimal prime divisors are the radical of $Q_0 + yB$, which is inside of P_1, thus use [2][Proposition 1.11] again to assure that Q_1 exists. Next, if $\varphi(x) \in Q_1$, then Q_1 is minimal prime divisor of $Q_0 + xB$, which contradicts the fact that $Q_1 \neq T_i$ for all i.

In the proof of Theorem 15.4, the author implicitly uses the fact that any localization by a prime ideal of $\kappa(\mathfrak{p})[X]$ is again dimension 1.

In remark 2, the generic fiber of $A \to A[[X]]$ is $C := A[[X]] \otimes \kappa(0)$, and $\operatorname{Spec} C = \{Q \in \operatorname{Spec} A[[X]] : Q \cap A = 0\}$. Since $P = \ker\varphi \in \operatorname{Spec} C$, every prime ideal inside of P are in C, thus $\dim C = 2$.

Recall from section 5 that a ring A is catenary if for any $\mathfrak{p} \subseteq \mathfrak{p}'$ with $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec}(A)$, there exists a saturated chain of prime ideals starting from $\mathfrak{p}$ and ending at $\mathfrak{p}'$, and all such chains have the same finite length. Saturated chain is a chain such that for any two consecutive prime ideals $P \subseteq Q$ in the chain has $\operatorname{ht}(Q/P) = 1$, i.e., no primes exists inbetween P and Q.

In the equality proof of theorem 15.5 with $Q = (0)$, if $P = \mathfrak{p}B$, then $\operatorname{ht} P = \operatorname{ht} p$, and $\operatorname{tr.deg}_{\kappa(\mathfrak{p})}\kappa(P) = \operatorname{tr.deg}_k \kappa(k[X]) = 1 = \operatorname{tr.deg}_A A[X]$. If $\operatorname{ht}(P/\mathfrak{p}B) = 1$, then $\operatorname{ht} P = \operatorname{ht} p + 1$, and $\operatorname{tr.deg}_{\kappa(\mathfrak{p})}\kappa(P) = \operatorname{tr.deg}_k \kappa(k[X]/(f)) = 0$, while $\operatorname{tr.deg}_A A[X] = 1$.

In the last line of the proof of Theorem 15.5, notes that $\operatorname{ht} P \geq \operatorname{ht}\mathfrak{p}$, which came from a special property of polynomial ring that $(\mathfrak{q}, f)$ is a prime in $A[X]$ for any irreducible one, and these are only primes we can have in $A[X]$, thus equality holds.

In the proof of only if part of 15.6, when $Q = 0$, there is nothing to prove, since domain formula holds for polynomial ring over A. If $Q \neq 0$, then $\operatorname{ht} P = \operatorname{ht} P^* - \operatorname{ht} Q$ implies the equality as in the proof of 15.5.

In the proof of if part of 15.6, $b \in Q\mathfrak{q}_2 \cdots \mathfrak{q}_r - P$ exists; to see this, notes that $Q \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_r \subseteq P$ implies that P contains one of $\mathfrak{q}_i$ or Q, which does not make sense by the given assumption; thus $T := Q \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_r \setminus P \neq \emptyset$. Hence, by taking $r+1$ exponentiation for any elements of T we get an element of $Q\mathfrak{q}_2 \cdots \mathfrak{q}_r - P$.

Now, $I : b^v B \supseteq \mathfrak{q}_1$ is clear; conversely, if $t \in I : b^v B$, then $tb^v \in I$. Since $b^v \in Q\mathfrak{q}_2 \cdots \mathfrak{q}_r$ but $b^v \notin \mathfrak{q}_1$, $t \notin \mathfrak{q}_1$ implies that $tb^v \notin I$, which contradicts the fact that $tb^v \in I$.

Next, if $z \in J \cap B$, then for the form $z = u/b^k$, u should contain b^k term. Also, z is a polynomial of y_is with no constant (B-elements), thus $u \in I$ since u is a polynomial of a_is with B-coefficients without constant term. This implies $J \cap B \subseteq \mathfrak{q}_1$. Conversely, if $t \in \mathfrak{q}_1$, then $tb \in I$, so we let $tb = \sum_{i=1}^{h} a_i b_i$ for some $b_i \in B$, which means that $t = \sum_{i=1}^{h} y_i b_i \in J$. Hence, $\mathfrak{q}_1 \subseteq J \cap B$.

Actually, $\dim C_M \leq h + d$ can be derived by Exercise 16.1., since $y_1, \cdots, y_h$ form a C_M-regular sequence. Or you may use Theorem 154 of [9].

Last inequality of p.122 is actually $\dim(R/uR) = \operatorname{ht}\mathfrak{m}' = \operatorname{ht}\mathfrak{m} = \dim A$. Notes that this condition only holds when A is local; otherwise, $\dim G \leq \dim A$ since $\operatorname{ht}\mathfrak{m} \leq \dim A$ in general.

1. $P \cap A \supseteq \mathfrak{p}$ is clear since $X = Y \cdot (X/Y)$. Conversely, suppose $f \in P \cap A$, then f is a polynomial of X, Y over a field coefficient; also, f has zero constant term, otherwise $f \notin P$ contradiction; thus $f \in \mathfrak{p}$.

   Also, Theorem 13.5 shows that $\operatorname{ht} P \leq 2$, and $(0) \subseteq (Y) \subseteq (Y, X/Y)$ is a chain of prime ideals, thus its height is 2. Also, height of $\mathfrak{p}$ is 2 clearly. Now to check height of $B_P/\mathfrak{p}B$, set $Z = X/Y$. Then, $X = YZ$, $B = k[Y, Z] \supset A = k[YZ, Y]$, thus $\mathfrak{p}B = YB$. Thus, $B/\mathfrak{p}B \cong k[Z]$, hence $\dim B_P/\mathfrak{p}B_P = \dim k[Z]_{(Z)} = 1$. Thus $\operatorname{ht} P = 2 < 3 = \operatorname{ht}\mathfrak{p} + \dim B_P/\mathfrak{p}B_P$.

   To make an example showing that going-down theorem does not hold between A and B, let $\mathfrak{p}' = (X - \alpha Y)A$ for $0 \neq \alpha \in k$. If Q is a minimal prime ideal of B containing $(X - \alpha Y) = (YZ - \alpha Y) = Y(Z - \alpha)$, then Q must contain Y or $Z - \alpha$. Also, the minimal prime ideal containing $Y(Z - \alpha)$ in B must have height less than 1, so it means that $Q = (Y)B$ or $Q = (Z - \alpha)B$ since they have height 1. However, $YB \cap A = YA \neq \mathfrak{p}'$ since $X - \alpha Y \notin YA$, and $Z - \alpha \notin P$, thus there does not exist any prime ideal of B contained in P and lying over $\mathfrak{p}'$, however $\mathfrak{p}' \subseteq \mathfrak{p}$ and P is lying over $\mathfrak{p}$.

2. No. Set $f = XY - 1$. Then fB is a prime ideal of B, and $fB \cap A = (0)$. Since $fB + XB = B$ there does not exist any prime ideal of B containing fB and lying over XA; in other words, when $(0) \subseteq (X)$ and fB is lying over (0), then there are no prime ideal containing fB lying over (X).

3. See Nagata's example in [2][Exercise 11.4]; Let k be a field and let $A = k[x_1, x_2, \ldots, x_n, \ldots]$ be a polynomial ring over k in a countably infinite set of indeterminates. Let $m_1, m_2, \ldots$ be an increasing sequence of positive integers such that $m_{i+1} - m_i > m_i - m_{i-1}$ for all $i > 1$. Let $\mathfrak{p}_i = \left(x_{m_1+1}, \ldots, x_{m_{i+1}}\right)$ and let S be the complement in A of the union of the ideals $\mathfrak{p}_i$ Each $\mathfrak{p}_i$ is a prime ideal and therefore the set S is multiplicatively closed. The ring $S^{-1}A$ is Noetherian by Chapter 7, Exercise 9. Each $S^{-1}p_i$ has height equal to $m_{i+1} - m_i$, hence $\dim S^{-1}A = \infty$.

   Here, let A_S as our ring, and set $I = x_{m_2}A_S$, which is contained in $\mathfrak{m}_2 := (x_{m_1+1}, \cdots, x_{m_2})$, which is maximal ideal of A_S. Then, by constructing Rees algebra and using the argument in the proof of Theorem 15.7, $\dim G = \operatorname{ht}\mathfrak{m}_2 = m_2 - m_1 < \infty = \dim A$.

16 Regular sequences

In the last line of proof of Theorem 16.1, $a_i\eta_1 \in a_1M + \cdots + a_{i-1}M$ implies $\eta_1 \in a_1M + \cdots + a_{i-1}M$, because, if $\eta_1 \notin a_1M + \cdots + a_{i-1}M$, then $\overline{\eta_1}$ is nonzero in $M/(a_1M + \cdots + a_{i-1}M)$, thus $a_i\overline{\eta_1} \neq 0$ in $M/(a_1M + \cdots + a_{i-1}M)$, contradiction.

In the proof of Theorem 16.2, to show $n = 1$ case, pick a monomial mX^v for some $v > 0$, then assume $ma_1^v \in I^{v+1}M$. Hence, $ma_1^v = m'a_1^{v+1}$, thus $a_1^v(m - a_1m') = 0$. Since a_1 is M-regular, this implies $m = a_1m'$, which implies that the coefficient m is in IM.

In the proof of Theorem 16.3, $a_1\xi = 0$ implies that $F(X) := \xi X_1$ has a property that $F(a) = 0 \in I^vM$ for all v. Since a_i is quasi-regular, $\xi \in IM$. Then, $\xi = \sum a_i\eta_i$. Then, $G(X) := \sum \eta_i X_i X_1$. Then, $G(a) = 0$ with quasi-regularity implies that $\eta_i \in IM$. Repeating this procedure, we knows that $\xi \in \cap I^vM = (0)$.

Also, in the proof of Theorem 16.3, $i \leq v$ since F is v-homogeneous, therefore $a_1\omega \in I^vM$.

For corollary, permutation holds since in case of M-quasi-regular, permutation is nothing but permuting indeterminates.

In the counter example, $X \cdot Z(Y-1) = 0$ in $A/(X(Y-1))$ while $X \neq 0$ in $A/(X(Y-1))$.

In the proof of Theorem 16.6, the last exact sequence $0 \to \operatorname{Ext}_A^i(N, M) \to \operatorname{Ext}_A^i(N, M)$ is came from the long exact sequence of ext over $0 \to M \to M \to M_1 \to 0$, thus for any $i \leq n$, $\operatorname{Ext}_A^i(N, M) \cong \operatorname{Ext}_A^i(N, M)$. Now, large power f_t^n annihilates $\operatorname{Ext}_A^i(N, M)$ means that the map $(\cdot f_t)$ has kernel as f_t^{n-1}, which implies that $\operatorname{Ext}_A^i(N, M) = 0$.

To get $\operatorname{Hom}_A(A/I, M_n) \cong \operatorname{Ext}^1_A(A/I, M_{n-1}) \cong \cdots \cong \operatorname{Ext}^n_A(A/I, M)$, notes that for any $A-$module N, M, $\operatorname{ann}(\operatorname{Ext}^i_A(N, M) \supseteq \operatorname{ann}(N)$; to see this, pick an injective resolution $M \to I^\bullet$, then $\operatorname{Ext}^i_A(N, M) := \ker(\operatorname{Hom}_A(N, I^i) \to \operatorname{Hom}_A(N, I^i))/\operatorname{Im}(\operatorname{Hom}_A(N, I^{i-1}) \to \operatorname{Hom}_A(N, I^i))$. Pick $[g] \in \operatorname{Ext}^i_A(N, M)$ for some $g \in \operatorname{Hom}_A(N, I^i)$ in the kernel. Then, for any $f \in \operatorname{ann}(N)$, $fg(n) = g(fn) = g(0) = 0$ implies that $fg = 0$. Hence, $[fg] = 0$, which implies the desired result. Now observes, from the given situation (I has length n M-regular sequence) that the long exact sequence of $\operatorname{Ext}^\bullet_A(A/I, -)$ on $0 \to M \xrightarrow{f_1} M \to M_1 \to 0$ gives that

$$\operatorname{Ext}^{n-1}_A(A/I, M) = 0 \to \operatorname{Ext}^{n-1}_A(A/I, M_1) \to \operatorname{Ext}^n_A(A/I, M) \xrightarrow{f_1} \operatorname{Ext}^n_A(A/I, M) \to \cdots$$

but since $f_1 \in \operatorname{ann}(A/I) = I$, this implies $\operatorname{Ext}^{n-1}_A(A/I, M) = 0 \to \operatorname{Ext}^{n-1}_A(A/I, M_1) \to \operatorname{Ext}^n_A(A/I, M)$. Now apply induction. Next, if $\operatorname{Ext}^n_A(A/I, M) = 0$, then Theorem 16.6 implies that there exists length $n+1$ M-regular sequence. Moreover, we can extend it by thinking M-regular sequence on $A/(x_1, \cdots, x_n)$ with $I/(x_1, \cdots, x_n)$ using Theorem 16.6.

$V(I) = V(I')$ implies that depths are equal came from statement (1) and (2') of Theorem 16.6.

In the proof of Corollary of p.131, the last iff came from Theorem 16.5(i)

1. To see $\dim M' \geq \dim M - r$, let $k = \dim M'$. Then, by Theorem 13.4, there exists $\overline{y_1}, \cdots, \overline{y_k}$ which is the system of parameters of M' in $A/(a_1, \cdots, a_r)$. Then, $\dim M/(a_1, \cdots, a_r, y_1, \cdots, y_k)M = 0$ since $\dim M = \delta(M) = 0$ by Theorem 13.4. (See p.98) Thus, $r + k \geq \dim M$, which implies that $\dim M' \geq \dim M - r$.

   Conversely, to see $\dim M' \leq \dim M - r$, by induction it suffices to show that $r = 1$ case. When $r = 1$, then $a_1 \notin \operatorname{ann} M$, thus height of (a_1) in $A/\operatorname{ann} M$ is 1. Now, notes that $\operatorname{ann}(M') = \operatorname{ann}(M/a_1M)$ contains $(a_1, \operatorname{ann}(M))$, thus the height of $\operatorname{ann}(M')/\operatorname{ann}(M) \geq 1$. Thus, from $\dim A/\operatorname{ann}(M') + \operatorname{ht}\operatorname{ann}(M')/\operatorname{ann}(M) \leq \dim A/\operatorname{ann}(M)$, we have $\dim M' \leq \dim M - \operatorname{ht}\operatorname{ann}(M')/\operatorname{ann}(M) \leq \dim M - 1$. Apply this argument r times to get $\dim M' \leq \dim M - r$.

2. Apply Theorem 16.9 with $M = A/\mathfrak{a}$, $N = A/\mathfrak{b}$ to get $\operatorname{Ext}^i_A(A/\mathfrak{a}, A/\mathfrak{b}) = 0$ for $i < \operatorname{grade}\mathfrak{a} - \operatorname{proj}\dim A/\mathfrak{b}$. Since $\operatorname{grade}\mathfrak{a} - \operatorname{proj}\dim A/\mathfrak{b}$ is positive, $\operatorname{Hom}_A(A/\mathfrak{a}, A/\mathfrak{b}) = \operatorname{Ext}^0_A(A/\mathfrak{a}, A/\mathfrak{b}) = 0$. To see this implies $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$, let $f \in A$ such that $f\mathfrak{a} \subseteq \mathfrak{b}$. Then, $A \xrightarrow{f} A/\mathfrak{b}$ has kernel containing $\mathfrak{a}$, thus we may regard $(\cdot f) \in \operatorname{Hom}_A(A/\mathfrak{a}, A/\mathfrak{b})$, but this implies that $(\cdot f)$ is zero map; hence $f \in \mathfrak{b}$. The converse is clear.

3. Let $P \in \operatorname{Ass}(A/I)$. Since grade I is nothing but the maximal length of A-sequence in I, which also form an A-sequence of P, thus grade of P is greater than or equal to k. If grade $P > k$, then Exercise 16.2 shows that $I : P = I$, contradiction; to see why it is problematic, let $\bigcap_{i=1}^{l} Q_i = I$ be the primary decomposition of I, with $\sqrt{Q_1} = P$. Then, $(Q_1 : P) \cap \bigcap_{i=2}^{l} Q_i \subseteq I : P$. Hence, it suffices to show that $(Q_1 : P) \neq Q_1$.

   If $Q_1 = P$, then $(P : P) = A \neq Q_1$, thus we may assume $Q_1 \neq P$. In this case, $(Q_1 : P) \subseteq P$ since for any $x \in (Q_1 : P)$, $xy \in Q_1$ with $y \in P \setminus Q_1$ implies that $x \in \sqrt{Q_1} = P$ by primary-ness of Q_1. Thus, by localization we may assume that P is the maximal ideal in Noetherian local ring A, and Q_1 is P-primary in A. Now in A/Q_1, $(Q_1 : P)/Q_1 = (\overline{0} : P/Q_1)$, thus we may regard the problem as showing $(0 : P) \neq 0$ for a Noetherian local ring (A, P). Now by Corollary 7.16 of [2], we may assume that P is nilpotents, i.e., $P^n = 0$ for some n. Further, we may assume that n is the smallest integer such that $P^n = 0$. If $n = 1$, then $P = Q_1$, contradiction. Thus $n > 1$. Then, $(0 : P) \supseteq P^{n-1} \neq 0$. This shows that $(0 : P) \neq 0$.

   Claim 17. *A is Noetherian ring, I is proper ideal. Then* grade $I \leq \operatorname{proj}\dim A/I$.

   Proof. Otherwise, by Exercise 16.2, $\operatorname{Hom}_A(A/I, A/I) = 0$, contradicting the fact that the identity map exists. ☐

4. Notes that $0 \to M \xrightarrow{a_1} M \to M/a_1M \to 0$ is exact. Since B is flat over A,

$$0 \to M \otimes_A B \xrightarrow{f(a_1)} M \otimes_A B \to (M/a_1M) \otimes B \to 0$$

is exact. By five lemma with the exact sequence $0 \to M \otimes_A B \xrightarrow{f(a_1)} M \otimes_A B \to M \otimes B / f(a_1) M \otimes B \to 0$, $(M/a_1M) \otimes B \cong M \otimes B/f(a_1)M \otimes B \neq 0$. Since $(M/a_1M) \otimes B$ is nonzero module, $f(a_1)$ is $(M \otimes B)$-sequence. Now apply the same argument on $a_2, \cdots, a_r$.

5. Before going further, we prove a result about Ext when $M = IM$.

   Claim 18. *When A is Noetherian, I is a proper ideal, and M is a finite A-module s.t. $M = IM$ then $\operatorname{Ext}^i_A(A/I, M) = 0$ for all i.*

   Proof. From the given condition, [8][Proposition 3.3.10] shows that $\operatorname{Ext}^i_A(A/I, M)_P \cong \operatorname{Ext}^i_{A_P}(A_P/IA_P, M_P)$. If a prime ideal P does not contain I, then A_P/IA_P=0.If P contains I, then $M = IM$ implies $M/PM = 0$ (since $PM \supseteq IM = M$), thus $M_P = 0$ by NAK (apply NAK on A_P with $PM_P = M_P$). Hence, in any cases, $\operatorname{Ext}^i_A(A/I, M)_P \cong \operatorname{Ext}^i_{A_P}(A_P/IA_P, M_P) = 0$, which implies $\operatorname{Ext}^i_A(A/I, M) = 0$. ☐

   Thus, if $M = PM$, then depth of both M an M_P are infinite, thus the inequality holds. If $M \neq PM$, to define depth. To see $\operatorname{depth}(P, M) \leq \operatorname{depth}(PA_P, M_P)$, notes that $f : A \to A_P$ is a flat homomorphism, hence Exercise 16.4 implies that any M-sequence $p_1, \cdots, p_r$ gives M_P-sequence $f(p_1), \cdots, f(p_r)$ when $M_P/(f(p_1), \cdots, f(p_r))M_P \neq 0$. If $P \notin \operatorname{Supp}(M)$, then [8][Proposition 3.3.10] shows that $\operatorname{Ext}^i_A(A/I, M)_P \cong \operatorname{Ext}^i_{A_P}(A_P/IA_P, M_P) = 0$, thus the inequality holds. If $P \in \operatorname{Supp}(M)$, then $M_P \neq PM_P$, otherwise NAK implies that $M_P = 0$, contradicting the assumption that $P \in \operatorname{Supp}(M)$. Hence, Exercise 16.4 implies that every M-sequence gives M_P-sequences, which implies the desired inequality.

   To get the counterexample, suppose that $(A, \mathfrak{m})$ is local; then if $\mathfrak{m} \in \operatorname{Ass}(A)$, then $\mathfrak{m} = \operatorname{ann}(x)$ for some nonzero $x \in A$, thus $\mathfrak{m}$ is nilradical, which implies that $\mathfrak{m}$ has no A-regular sequence. Thus, $\operatorname{depth} A = 0$. However, if there exists a prime ideal P in A whose height is nonzero, and P is not in the associated prime of A, then $\operatorname{depth} A_P > 0$, which gives a counterexample. For example, let $A = k[X, Y, Z]_{(X,Y,Z)}/(X, Y, Z)^2 \cap (Z)$. Then, $\operatorname{Ass}(A) = \operatorname{Ass}_{k[X,Y,Z]}((X, Y, Z)^2 \cap (Z)) = \{(X, Y, Z), (Z)\}$. Now think $P = (X, Z)$. Then, $A_P = k[X, Y, Z]_{(X,Z)}/(X, Y, Z)^2 \cap (Z) = k[X, Y, Z]_{(X,Z)}/(Z^2, ZX, ZY) = k[X, Y, Z]_{(X,Z)}/(Z) \cong k[X, Y]_{(X)}$, which is a domain. Here, $PA_P = (X)$, thus it contains A_P regular element X, such that $A_P/(X) \cong k(Y)$ and A_P is domain. Hence $\operatorname{depth} A_P \geq 1$.

6. Let $I = (a_1, \cdots, a_n)$. Suppose not; then there exists a polynomial $f(x) \in k[X_1, \cdots, X_r]$ such that $f(\underline{a}) = 0$. Now, let $f = f_0 + f_1 + \cdots + f_r$ as a sum of homogeneous polynomials. Then, $f_0(\underline{a}) = -\sum_{i=1}^r f_i(\underline{a}) \in I$ implies $f_0 \in I$. Since $f_0 \in k$, thus this implies that $f_0 = 0$; (since all nonzero elements in I is not unit, however all nonzero elements of k is unit in A.) Then, $f_1(\underline{a}) \in I^2$ implies $f_1 \in I[X_1, \cdots, X_n]$, thus $f_1 = 0$. By doing this argument for all i, we can conclude that $f = 0$.

7. Let $\underline{x} = (x_1, \ldots, x_n)$ be a maximal M -sequence in $\mathfrak{m}$, and set $M' := M/\sum x_i M$. Then, by [4][Proposition 1.2.1], $\mathfrak{m} \in \operatorname{Ass}_A(M')$ since the only prime ideal containing $\mathfrak{m}$ is $\mathfrak{m}$ itself. Thus, $\mathfrak{m} = \operatorname{ann}(\xi)$ for some $\xi \in M'$. Hence, $\mathfrak{m}B(\xi) = 0$. Since $\mathfrak{m}B$ is $\mathfrak{n}$-primary, $\mathfrak{n}^v \subseteq \mathfrak{m}B$ by [2][Cor 7.16]. Hence, $\mathfrak{n}^v$ is a set of zero divisor, thus [4][Proposition 1.2.1] implies that $\mathfrak{n}^v$ should lie on an associate prime of M' in B, which is $\mathfrak{n}$ since that associate prime must contain the radical of $\mathfrak{n}^v$, which is $\mathfrak{n}$, the maximal ideal. Hence, $\overline{x}$ is also the maximal M sequence in $\mathfrak{n}$.

8. We may assume that there are no redundant primes. By assumption, there exists $a \in A, b \in I$ such that $xa + b \notin P_i$ for all i. Also, if $x \in P_i$ then $b \notin P_i$. Hence, let $S := \{i : x \in P_i\}, S^c := [r] \setminus S$. If $S^c = \emptyset$, then $x + b \notin \bigcup_i P_i$, done.

   If S^c is not empty nor $[r]$, we claim $\bigcap_{i \in S^c} P_i \setminus \bigcup_{i \in S} P_i$ is nonempty; if it is empty, then $\bigcap_{i \in S^c} P_i$ is a subset of union, thus [2][Prop 1.11 (i)] implies that the intersection is in P_i for some $i \in S$, then [2][Prop 1.11 (ii)] implies that $P_i \supseteq P_j$ for some $j \in S^c$, contradiction. Take $c \in \bigcap_{i \in S^c} P_i \setminus \bigcup_{i \in S} P_i$. Now we claim $x + bc \notin \bigcup_i P_i$; if $i \in S$, then $x \in P_i$ implies $b \notin P_i$; also by construction $c \notin P_i$, hence $x + bc \notin P_i$. If $i \in S^c$, then $x \notin P_i$ but $c \in P_i$, hence $x + bc \notin P_i$.

   Lastly, if If $S^c = [r]$ and $\bigcap_{i \in S^c} P_i \neq \emptyset$, then $x + 0 \notin P_i$ for all i, done.

9. This holds when $n = 0$ vacuously. Suppose $n > 0$, let $I = (x_1, \cdots, x_n)$. If grade $I = 0$, done. Otherwise, I has a regular element, thus $I \not\subset D(A)$, where $D(M)$ is a set of zero divisors of M. By definition of associate primes as a maximal elements of annihilators of elements of A, we knows that $D(A) = \bigcup_{P \in \mathrm{Ass}(A)} P$. Now, let $x := x_1, I' := (x_2, \cdots, x_n)$. Since $xA + I' = I \not\subseteq \bigcup_{P\in\mathrm{Ass}(A)} P$, the above exercise shows that there exists $y \in I'$ such that $x + y \notin \bigcup_{P\in\mathrm{Ass}(A)} P = D(M)$. Thus let $u_1 := x_1 + y$. If grade $I = 1$, done. Otherwise, I/u_1A has a regular element of A/u_1A.

   Now we claim that $I'/u_1A \not\subseteq D(A)$; to see this, notes that every element of I can be written as A-linear combination of $u_1, x_2, \cdots, x_n$ (since x_1 can be replaced with u_1 by suitable coordination of coefficients of x_i) so $I'/u_1A \subseteq D(A)$ implies that $I/(u_1A) \subseteq D(A)$, contradicting the assumption that I/u_1A has a regular element. Thus, applying the above exercise again on $x = x_2$ and $I'' := (x_3, \cdots, x_n)/u_1A$, we get $y' \in I''$ such that $u_2 := x_2 + y'$ is regular. Now continue this process until it reach its own grade. And notes that if grade $I = n$, then we may find $u_1, \cdots, u_{n-1}$, and by the same argument $(x_n) \not\subseteq D(A/(u_1, \cdots, u_n)A)$. Hence, we may pick a regular element u_n from (x_n); especially x_n is regular, otherwise any u_n cannot be regular. and since $(u_1, \cdots, u_n) = (x_1, \cdots, x_n)$, thus I is generated by A-sequences. Also, grade$I$ cannot exceed n, since by definition of maximal A-sequence, $u_1, \cdots, u_n, b$ cannot form A-sequence since $b \in I = (u_1, \cdots, u_n)$.

10. (a) Suppose $r = 1$. Then, $P = (a_1)$ is principal thus its minimal prime divisor, which is P itself has height 1 by given condition. Thus there exists a prime ideal Q such that $P \neq Q$, $P \supseteq Q$. If $y \in Q$, then $y = xa_1$ for some $x \in A$, and since $a_1 \notin Q$ (otherwise $Q = P$) thus $x \in Q$. So $Q = a_1Q$. When A is local ring, then since a_1 is in the maximal ideal $\mathfrak{m}$, thus $\mathfrak{m}Q \supseteq a_1Q = Q$, therefore NAK implies $Q = (0)$. Thus there is only one minimal prime of A, which is (0), thus A is integral domain. Or, if A is $\mathbb{N}$-graded and a_1 is homogeneous of positive degree, we may assume Q is also graded by Theorem 13.7 then $Q = a_1Q$ implies that $Q \subseteq R_0$, however $P = (a_1) \subseteq \oplus_{i>0} R_1$, which implies that $Q \subset R_0 \cap \oplus_{i>0} R_1 = 0$. Again, A is integral domain.

    Now, to use induction, suppose that it holds for $1, 2, \cdots, r-1$. Then, $P/(a_1, \cdots, a_{r-1})A = (a_r)/(a_1, \cdots, a_{r-1})A$ is principal prime ideal. Since a minimal prime divisor of $(a_1, \cdots, a_{r-1})$ has height $r-1$, P is not a minimal prime divisor of $(a_1, \cdots, a_{r-1})$, thus $P/(a_1, \cdots, a_{r-1})A$ has height 1. Thus, by applying $r = 1$ case on $(a_r)/(a_1, \cdots, a_{r-1})A$, $A/(a_1, \cdots, a_{r-1})A$ is integral domain, thus $P' := (a_1, \cdots, a_r)$ is prime ideal. Then height of P' is at most $r-1$ by Theorem 13.5. Now, localize A by P, then (A_P, PA_P) is a regular local ring, thus integral domain (Theorem 14.3). Thus, Theorem 13.5 implies that (a_r) in A_P has height 1. Moreover, $a_1, \cdots, a_r$ is A_P-regular, since $A_P/(a_1, \cdots, a_i)A_P$ is dimension $r-i$ local ring whose maximal ideal is generated by $r-i$ elements, thus regular local ring, for any i. Now, notes that the maximal A-sequences of P' is its generators, thus its depth is $r-1$. Thus, by Exercise 16.4, the maximal ideal $P'A_{P'}$ of $(A_P)_{P'} = A_{P'}$ has also depth $r-1$. Now apply the claim below to have height of P' is at least $r-1$ (by localizing A by P'). This implies that height of P' is $r-1$. Thus, P' in A (not A_P) has also height $r-1$. Now apply the inductive hypothesis to get the desired result.

    Claim 19. *Given a regular local ring $(A, \mathfrak{m})$, depth of $\mathfrak{m}$ is less than equal to height of $\mathfrak{m}$.*

    Proof. First of all, Exercise 16.1 shows that $\dim A - \operatorname{depth}\mathfrak{m} = \dim A/\mathfrak{m} \geq 0$. Hence, $\operatorname{ht}\mathfrak{m} = \dim A \geq \operatorname{depth}\mathfrak{m}$. ☐

    (b) For any $Q \in \mathrm{Ass}(A)$ we have $QA_Q \in \mathrm{Ass}\,(A_Q)$; if we had such P inside of Q, then PA_Q is in A_Q with the same height and same number of generators, thus (i) implies that A_Q is an integral domain, contradicting that $QA_Q \neq 0$. Hence $P \not\subset Q$. Therefore using the process we used for the proof of Exercise 16.9, we see that P can be generated by an A-sequence.

    For a counterexample let $A = k[x,y,z] = k[X,Y,Z]/(X(1-YZ))$; $P = (x,y,z) = (y,z) = \big(y - y^2z, z\big)$ is a prime ideal of height 2, but $y - y^2z$ is a zero-divisor in A such that $x(y - y^2z) = y(x(1-yz)) = 0$.

17 Cohen-Macaulay rings

To see that $\operatorname{Ext}^i_A(N_j/N_{j+1}, M) = 0$ implies $\operatorname{Ext}^i_A(N, M) = 0$, use the short exact sequence

$$0 \to N_j/N_{j+1} \to N_0/N_{j+1} \to N_0/N_j \to 0.$$

and take $\operatorname{Ext}^i_A(-, M)$ successively to conclue that $\operatorname{Ext}^i_A(N_0/N_j, M) = 0$ for all j.

Also, in the second last line of p.133, $\dim N' < r$ since x is A/P-regular, thus $A/(P, x)$ has dimension less than r by Exercise 16.1.

In the proof of 17.2, if $P \in \operatorname{Ass}(M)$, then $\operatorname{depth}(P, M) = 0$, which implies $\operatorname{Ext}^0_A(A/P, M) = \operatorname{Hom}_A(A/P, M) \neq 0$.

In the proof of Theorem 17.3(iii), $\operatorname{depth} M_P \geq \operatorname{depth}(P, M)$ is from Exercise 16.5. Also, $\dim M_P = \dim A_P/\operatorname{ann}(M_P) = \dim A_P/PA_P = 0$. Also, $M'_P \neq 0$ since if it is zero, then $aM_P = M_P$, and since $a \in P$, thus NAK implies that $M_P = 0$, contradicting the given assumption that $M_P \neq 0$.

In the proof of Theorem 17.4 (iii), $\operatorname{ht}(a_1) < \operatorname{ht}(a_1, a_2) < \cdots$ came from this argument; notes that a_2 is not a zero divisor of $A/(a_1)$, thus a_2 is not in any minimal prime divisor of (a_1). Hence, (a_2, a_1) in $A/(a_1)$ should have height at least 1 since its minimal prime divisor is not minimal prime divisor of (a_1).

In the proof of Theorem 17.4 (iii) (4) $\implies$ (1), if $x_1 \in P$, then height of $(x_1, \cdots, x_n)/P = (x_2, \cdots x_n)/P$ has height at most $n - 1$, thus it is not the maximal ideal, contradicting the fact that $(x_1, \cdots, x_n)$ in A has the maximal ideal as its minimal prime divisor.

In the proof of Theorem 17.4 (i) we may choose it as follow; since $I \setminus D(A) \neq \emptyset$, where $D(A)$ is the set of zero divisors of A, thus we may choose $a_1 \in I \setminus D(A)$, then height of (a_1) is 1. Now, do the same thing on $A/(a_1)$ to choose a_2. Done.

At the last line of p.135, "take an A-sequence" should be changed to "take a maximal A-sequence of P".

In proof of Theorem 17.5, we may use the fact that $A \to \hat{A}$ is flat (Theorem 8.8) thus any A-sequences form $A \otimes \hat{A} \cong \hat{A}$-sequence by Exercise 16.4, since $(A/(\underline{a})) \otimes \tilde{A} = \tilde{A}/(\underline{a}) \neq 0$. Honestly, I don't know how to show $\operatorname{Ext}^i_A(A/\mathrm{m}, A) \otimes \hat{A} = \operatorname{Ext}^i_A(\hat{A}/m\hat{A}, \hat{A})$ for all i.

The condition of Theorem 13.5 (General Krull's principal ideal theorem) is that A is Noetherian, I is an ideal generated by r elements.

In the proof of Theorem 17.6 showing that CM-ness shows unmixedness, notes that A/I is CM local ring is clear. Now, theorem 17.3 (i) shows that every prime divisor of A/I has the same coheight, and since A is CM-ring, thus every prime divisor has the same height, contradiction.

In the proof of 17.7, we assume that $A_\mathfrak{m}$ is dimension n CM ring, thus it has system of parameters $a_1, \cdots, a_n$ generating $\mathfrak{m}$.

For the proof of 17.9, let A/I be a quotient of CM ring with $\operatorname{ht} I = r$. Then, By theorem 17.4, depth of I is r, thus we may pick $(a_1, \cdots, a_r)$ an A-sequence in I, which is the maximal I sequence. Also, by Theorem 17.4, $(a_1, \cdots, a_r)$ is a part of a system of parameter, say $a_1, \cdots, a_n$. By proof of Theorem 17.4, $a_1, \cdots, a_n$ is also A-sequence, and $a_{r+1}, \cdots, a_n$ are not in union of minimal prime divisors of I, thus $\operatorname{depth}(\mathfrak{m}/I, A/I) = n - r$ as desired. Thus, it suffices to show that any finitely generated algebra over a CM ring A is catenary. If B is finite algebra over A, then $B \cong A[X_1, \cdots, X_n]/I$ for some n, then by Theorem 17.7, $A[X_1, \cdots, X_n]$ is CM, thus its quotient is CM, done.

In proof of Theorem 17.10, Not theorem 16.2 but the argument above the Theorem 16.2 was used. Also, in the last statement, A is regular because the minimal generators of $\mathfrak{m}$ is r (by $\dim \mathfrak{m}/\mathfrak{m}^2 = r$ with Theorem 2.3) which is equal to $\dim A = r$.

1. (a) Noetherian can be dropped; Let A be a zero-dimensional commutative ring and I be its nilradical. Then we knows that $I = \bigcap_{\mathfrak{m} \in \operatorname{Spec} A} \mathfrak{m}$. It is minimal decomposition, otherwise, if we may omit one prime ideal, then prime avoidance (Proposition 1.11 (ii) in [2]) implies that that prime has height 1, contradicting $\dim A = 0$. Then, by Theorem 4.5 of [2], $\mathfrak{m} = \sqrt{(I : x)}$ for some $x \in A$. Hence, for any $y \in \mathfrak{m}$, $(yx)^n$ is nilpotent; in other words, y is zero divisor. Hence, $\mathfrak{m}$ has no regular element. Thus, $\operatorname{depth}(\mathfrak{m}, A_\mathfrak{m}) = 0 = \dim A_\mathfrak{m}$.

   (b) Let A be a 1-dimensional reduced commutative ring. If $\mathfrak{m}$ is a prime ideal with height 0, then $A_\mathfrak{m}$ is CM by above. If $\mathfrak{m}$ is of height 1, then $(A_\mathfrak{m}, \mathfrak{m})$ is 1-dimensional local ring. We claim that $\mathfrak{m}$ has a regular element; suppose not. Then, since set of zero divisors are union of minimal prime ideals in the reduced ring, $\mathfrak{m}$ is subset of this union, therefore prime avoidance shows that $\mathfrak{m}$ is minimal prime, contradiction. Thus $1 = \dim A_\mathfrak{m} \geq \operatorname{depth}(\mathfrak{m}, A_\mathfrak{m}) \geq 1$, done.

Lastly, to get the counter example, let k be a field; then $A = k[X,Y]/\left(XY, Y^2\right)$ is a one-dimensional ring. However, we claim its depth is 0. To see this, localize it by (X,Y); then for any $f(x,y) \in (X,Y)$, $f(X,Y)$ is zero divisor; thus it is not regular. Hence, depth $= 0$ while $\dim A_{(X,Y)} = 1$ since $(X,Y) \supset (Y)$ form a chain of prime ideal.

Claim 20. *In the reduced commutative ring with unity, set of zero divisors are union of minimal prime ideal.*

Proof. For any zero divisor x such that $xy = 0$ for some $y \neq 0$, then $y \notin \mathfrak{p}$ for some minimal prime ideal $\mathfrak{p}$; otherwise y is in the intersection of all minimal prime ideals, which is (0), contradiction. Hence, $x \in \mathfrak{p}$. This shows one direction.

For other direction, given minimal prime ideal $\mathfrak{p}$, let $S := \{xy : x \notin \mathfrak{p}, y \text{ is not zero divisor}\}$. Then S is multiplicatively closed and does not contain 0. Let $\mathfrak{q}$ be a prime ideal maximal with respect to being disjoint from S; then $\mathfrak{q}$ cannot contain nonzerodivisor y; otherwise $1 \cdot y \in \mathfrak{q} \cap S$, contradiction. Also, if $x \in \mathfrak{q}$ is not in $\mathfrak{p}$, then $x \cdot 1 \in S$, contradiction. Hence, $\mathfrak{q} \subseteq \mathfrak{p}$. By minimality of $\mathfrak{p}$, $\mathfrak{q} = \mathfrak{p}$.

Now we claim $\bigcap_{\text{minimal } \mathfrak{p}} S_\mathfrak{p} = \{\text{nonzero divisors}\}$. $\supseteq$ is clear. Conversely, if $xy \in \bigcap_{\text{minimal } \mathfrak{p}} S_\mathfrak{p}$ but a zero divisor, then $zxy = 0$ for some nonzero $z \in A$. Since y is nonzero divisor, $zx = 0$. Hence, x is zero divisor. But the above argument showing that zero divisor is contained in the union of minimal primes, x is in some minimal prime ideal, contradicting that x is not in any of minimal prime ideal. Hence, the claim shows that union of minimal prime ideal contains zero divisors, too. ☐

2. In the first example, x^3, y^3 is an A-sequence; to see this notes that y^3 is nonzero divisor of $A/(x^3)$; if there is a, b, c, d, e, f such that $a(3,0) + b(2,1) + c(1,2) = d(2,1) + e(1,2) + f(0,3)$, then y^3 is zero divisor; thus it suffices to show that this equation has no nonnegative (nontrivial) integer solution with $f > 0$. If we allow integer, then we may write down as $a(3,0) + b(2,1) + c(1,2) = d(0,3)$ for some $b, c \in \mathbb{Z}, a, d \in \mathbb{N}$. Then, $3a + 2b + c = 0$, and $b + 2c = 3d$. Thus,
$$b + 2c > 0, \quad 2b + c \leq 0.$$
If $b = 0$, then $0 < c \leq 0$, contradiction. If $b > 0$, then $c \leq -2b < 0$. Then, $0 < b + 2c \leq b - 4b = -3b < 0$, contradiction. If $b < 0$, then $2c > -b > 0$. Thus, $c > -b/2 > 0$. Hence, $2b + c > 3b/2 > 0$ but $3b/2 < 0$, contradiction. Thus there are no nontrivial solution; hence y^3 is regular. Thus x^3, y^3 form an A-seqeunce. Hence also an R -sequence (since localization is flat and nonzero). so that R is CM.
However, in the second case, y^4 is zero divisor, since $y^4(x^3y)^2 = x^4(xy^3)^2 = 0$ in $A/(x^4)$.
3. Since A is normal, A_P integrally closed domain for any prime ideal P, and again normal (since its prime ideals are inherited from A.) If P is height 0 or 1, then by Exercise 17.1, they are CM. Thus, all we need to deal with is localization by maximal ideal. Let $\mathfrak{m}$ be a maximal ideal of A. Then, $(A_\mathfrak{m}, \mathfrak{m})$ is 2-dimensional integral domain. By Theorem 11.5 (i), all the prime divisors of a nonzero principal ideal has height 1. Hence, choose an element $a_1 \in \mathfrak{m}$. Since $A_\mathfrak{m}$ is integral domain, a_1 is $A_\mathfrak{m}$-regular. Now, by Theorem 11.5(i) $\mathfrak{m}$ is not a prime divisor of I, thus it does not contained in union of all prime divisors; otherwise prime avoidance shows that $\mathfrak{m}$ is inside of prime divisor, contradicting their heights. Hence, we may choose another element $a_2 \in \mathfrak{m}$ but outside of all prime divisors of (a_1). Then, since all zero divisors of $A/(a_1)$ is union of minimal primes of $A/(a_1)$, a_2 is not a zerodivisor of $A/(a_1)$, thus a_2 is $A/(a_1)$-regular. This shows that depth of $A_\mathfrak{m}$ is 2, equal to $\dim A_\mathfrak{m}$.
4. By localization, we may assume A is local ring. Theorem 17.3 (ii) shows that A/J is CM. Thus, $\dim A/J = \operatorname{depth} A/J$, say r. Let k be the residue class field of A. Then, $\operatorname{Ext}^i_A(k, A/J) = 0$ for $i < r$ from depth $A/J = r$. Using the exact sequence
$$0 \to J^v/J^{v+1} \longrightarrow A/J^{v+1} \longrightarrow A/J^v \to 0$$
and the fact that J^v/J^{v+1} is isomorphic to a direct sum of a number of copies of A/J we get by induction that $\operatorname{Ext}^i_A(k, A/J^v) = 0$ for $i < r$.

5. (a) Let $x_1, \cdots, x_r$ be a maximal A-sequence in P, and extend to a maximal A sequence in $\mathfrak{m}$ as $x_1, \cdots, x_r, y_1, \cdots, y_s$. There exists $Q \in \mathrm{Ass}_A(A/(x_1, \ldots, x_r))$ containing P (since P is minimal prime containing $(x_1, \cdots, x_r)$), so that by Theorem 17.2,

$$\dim A/P \geq \dim A/Q \underbrace{\geq}_{\text{Thm 17.2}} \operatorname{depth} A/(x_1, \ldots, x_r) = s.$$

Here depth $A/(x_1, \ldots, x_r) = s$ is came from; if it has longer sequnce, then it forms a A-sequence with longer than maximal A-sequence of $\mathfrak{m}$, contradiction. And $s = \operatorname{depth} A - \operatorname{depth}(P, A)$, done.

(b) $\dim A - \operatorname{ht} P \geq \dim(A/P) \geq \operatorname{depth} A - \operatorname{depth}(P, A) \geq \operatorname{depth} A - \operatorname{depth} A_P$. Here, $\operatorname{depth} A_P \geq \operatorname{depth}(P, A)$ came from Exercise 16.5.

6. By definition of symbolic power, $P^{(n)} := P^n A_P \cap A = \{a \in A : sa \in P^n \text{ for some } s \notin P\}$ contains P^n. Suppose they are not equal; then pick $a \in P^{(n)} \setminus P^n$. We have $s \notin P$ such that $sa \in P^n$. Thus $a \in P$. Hence, a should lie in P^r/P^{r+1} for some $1 \leq r < n$. Now, in $\mathrm{gr}_P(A)$, $(s+P)$ is grade 0 element, $(a+P^{r+1})$ is graded $r+1$ element, thus $(s+P)\cdot(a+P^{r+1}) = (sa+P^{r+1}) \in P^r/P^{r+1}$, however $sa = 0$ implies $(sa+P^{r+1})$=0. Hence, $\mathrm{gr}_P(A)$ is not an integral domain.

18 Gorenstein rings

In p.140, $\mathrm{Hom}(A, M) \to \mathrm{Hom}(I, M) \to 0$ is another expression that every map $\phi : I \to M$ is extended to $\phi : A \to M$. Also, the $\mathrm{Ext}^{n+1}_A(A/I, M) \cong \mathrm{Ext}^1_A(A/I, C)$ came from the fact that every long exact sequence can be splitted into short exact sequences with syzygies. Lastly, in case of Noetherian is just reusing argument in the proof of Theorem 17.1. See earliear part of this notes for details.

In Lemma 2, if you think about the injective resolution of M and $\overline{M}$ derived by horseshoe lemma, then $\mathrm{Ext}^i_A(N, M) \xrightarrow{x} \mathrm{Ext}^i_A(N, M)$ is nothing but the map sending quotient of $f : N \to I_i$ to a quotient of $xf : N \to I_i$, and for any $n \in N$, $xf(n) = f(xn) = f(0) = 0$ implies that $xf = 0$. Hence, x induces zero map in the long exact sequence, which implies that $\mathrm{Ext}^1_A(N, M) \cong \mathrm{Hom}_A(N, \overline{M})$. Since any action of xA on $f : N \to \overline{M}$ makes it zero, and N also can be regarded as B-module, $\mathrm{Hom}_A(N, \overline{M}) \cong \mathrm{Hom}_B(N, \overline{M})$. The rest step is a standard procedure to showing that T^i is derived functor. (Lastly, projective dimension of B over A is 1 since $0 \to A \to A \to B = A/xA \to 0$ gives a projective resolution of B as A-module.

In the proof of Lemma2(ii), $N = \mathrm{Hom}_B(B, N)$ since $f : B \to N$ was determined by $f(1)$.

In the proof of Lemma 3, by p.12's argument with the fact that I is $\mathfrak{m}$-primary and Notherianity gives $I \supseteq \mathfrak{m}^v$ for some v, we have such a composition series of N such that $N_i/N_{i+1} \cong A/\mathfrak{m} = k$. Now, use the argument in the proof of lemma 1 to conclude that ext of $(A/(P + xA), N)$ is vanished.

In the proof of Theorem 18.1 (1) to (1'), if $\mathfrak{m} \in \mathrm{Ass}(A)$, then $\mathfrak{m} = \mathrm{ann}(a)$ for some $a \in A$, hence $A/\mathrm{ann}(a) \cong Aa \subseteq A$, therefore $0 \to k \to aA \subseteq A$ is exact.

In the proof of Theorem 18.1 (1') to (2), A is injective A-module, thus $\mathrm{Hom}(-, A)$ is exact. This is part of definition.

In the proof of Theorem 18.1 (3) to (1), $T(M)$ has finite length since $\mathrm{Supp}(T(M)) \subseteq \{\mathfrak{m}\}$. In other words, $\mathfrak{m} \in \mathrm{Ass}(A/\mathrm{ann}(M))$, thus $\dim\dim(A/\mathrm{ann}(M)) = 0$, which implies the finite length. This came from the claim below;

Claim 21. *If A is Noetherian ring then A-module M has finite length iff M is finitely generated and $\dim(A/\mathrm{ann}(M)) = 0$.*

Proof. Suppose first that M has a composition series

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M$$

with $M_i/M_{i-1} \simeq A/\mathfrak{m}_i$ for $1 \leq i \leq r$, where each $\mathfrak{m}_i$ is a maximal ideal of A. Since each M_i/M_{i-1} is finitely generated, we conclude that M is finitely generated. Moreover, we have $\prod_{i=1}^r \mathfrak{m}_i \subseteq \mathrm{Ann}_A(M)$, hence the only primes containing $\mathrm{Ann}(A)$ are the $\mathfrak{m}_i$. This implies that $\dim(A/\mathrm{Ann}_A(M)) = 0$. Conversely, if M is finitely generated over a Noetherian ring, then it follows from Theorem 6.4

$$0 = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_r = M$$

such that $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$ for $1 \leq i \leq r$, where each $\mathfrak{p}_i$ is a prime ideal in A. If we have $\dim(A/\operatorname{Ann}_A(M)) = 0$, then every prime ideal in $A/\operatorname{Ann}_A(M)$ is a maximal ideal. Since we clearly have $\operatorname{Ann}_A(M) \subseteq \mathfrak{p}_i$ for all i, we conclude that each quotient M_i/M_{i-1} is a simple module, hence M has finite length. □

Also, if M is of finite length, then M is Artinian; then you can use below lemma to show that every injective endomorphism of Artinian module is surjective.

Claim 22. *$f : M \to M$ is an injective endomorphism of Artinian module M. Then f is surjective.*

Proof. Notes that $(\operatorname{Im} f^i)$ form a descending chain of submodules, thus stabilizes at some point, say n. Then, $M = \ker f^n + \operatorname{Im} f^n$. Now pick $x \in M$, then $f^n(x) \in \operatorname{Im} f^n = \operatorname{Im} f^{2n}$. Thus, $\exists y \in M$ such that $f^{2n}(y) = f^n(x)$. Then, $x = (x - f^n(y)) + f^n(y)$, where $x - f^n(y) \in \ker f^n = 0$. Thus, $x \in \operatorname{Im} f^n$, which shows f is surjective. □

In the proof of Theorem 18.1 (5') to (2), $f(k)$ must be minimal ideal, otherwise k has a proper ideal, contradiction.

For lemma 5, I don't understand why $\mathfrak{a}$ is finitely generated implies $\operatorname{Hom}_{A_S}(-, I_S)$ exact; see [10][Theorem 4.88] for more modern proof.

In Theorem 18.2, we not only uses Lemma 5 but also the fact that localization is flat.

If $E \subset M$ and E is injective module, then extension of $1_E : E \to E$ to $f : M \to E$ so that $M = E \oplus \ker f$ exists; this is another definition of injective module.

In proof of Theorem 18.4 (ii), $P \in \operatorname{Ass}(N)$ shows that $P = \operatorname{ann}(n)$ for some $n \in N$, thus the map $A \to nA \subseteq N$ gives A/P as a submodule of N.

In proof of Theorem 18.4 (vi), automorphism gives not only $(\cdot x)$ but also $(\cdot 1/x)$ as a map.

Claim 23. *If A be a commutative ring, $M \subset N$ be A-modules. Then, N is an essential extension of M iff $\forall x \in N$, there exists $f \in A$ such that $fx \in M \setminus \{0\}$.*

Proof. If N is essential, then for any $x \in N$, $Ax \cap M \neq 0$. Conversely, if N' be a nonzero submodule of N. Pick $x \in N'$. Then there exists $f \in A$ such that $fx \in M$ and fx is nonzero. Thus, $N' \cap M \neq 0$. □

Hence, in Example 1, if A is domain and K is its field of fraction, we can show that A is essential extension since for any nonzero $a/b \in K$, $b(a/b) \in A$ is nonzero. Also, K is injective since $\operatorname{Hom}_A(M, K) = \operatorname{Hom}_K(M_{(0)}, K)$; to see this, suppose $f : M \to K$ be a nonzero A-homomorphism. Then we can extend f as $f : M_{(0)} \to K$ by $f(m/s) = f(m)/s$ for any nonzero $s \in A$. Conversely, if two maps in $\operatorname{Hom}_K(M_{(0)}, K)$ are equal then its restriction is equal; hence they are isomorphic. Now, $\operatorname{Hom}_K((-)_{(0)}, K)$ is a composition of localization and taking $\operatorname{Hom}_K(-, K)$, both are exact since localization is flat and $\operatorname{Hom}_K(-, K)$ is a functor over vector space; hence K is injective.

In the proof of 18.5 (i), the author uses Baer's criterion. Also, recall

Claim 24. *Direct summand of injective module is injective.*

Proof. Let $I = C \oplus C'$ be an injective module. For any monomorphism $M \to M'$ with $M \to C$, then injectivity of I in with $M \to C \to C \oplus C' = I$ induces the map $M' \to I$, then the restriction $M' \to I \to C$ is extension of $M \to C$. □

In the proof of 18.6 (ii), $\operatorname{Hom}(k, E) = \operatorname{Hom}(k, k)$ by this identification; if $f : k \to E$, then f is totally determined by where $f(1)$ goes. Then, $f(1) \in V := \{x \in E : \mathfrak{m}x = 0\}$. To see this, suppose not; then we may pick $a \in \mathfrak{m}$ such that $af(1) \neq 0$ but $af(1) = f(a) = f(0) = 0$, contradicting the fact that f is A-homomorphism. Also, any $x \in V$ determines map $k \to E$ by sending 1 to x, hence $\operatorname{Hom}(k, E) \cong V = \operatorname{Hom}(k, V)$, where last equaltiy came from the fact that $f(k) \subset V$. Since E contains k, $V \supseteq k$. If $V \neq k$, then we may pick $w \in V \setminus k$, and kw form a submodule of $E(k)$ such that $kw \cap k$, contradicting the fact that k is essential submodule of $E(k)$. Hence, $\operatorname{Hom}(k, E) = \operatorname{Hom}(k, k)$. Notes that this argument can be generalized for any residue fields; see [4][Lemma 3.2.7 (b)].

Also, in the same proof, $l(M') = l(M'')$ by applying the exact functor $\operatorname{Hom}(-, E)$ again on $0 \to k' \to M \to M_1' \to 0$. Isomorhpism came from claim 22.

In the proof of (iii), Theorem 18.4 (v) implies the first statement of the proof.

Claim 25. *Let M be a A module, with $(A, \mathfrak{m}, k)$ is a Noetherian local ring. If every element of M is annihilated by some power of $\mathfrak{m}$, then $M \to \hat{M} = M \otimes_A \hat{A}$ is surjective.*

Proof. Notes that $\hat{A}$ is inverse limit of $(A/\mathfrak{m}_i, p_{ij,i\leq j} : A/\mathfrak{m}^j \to A/\mathfrak{m}^i)$ where p_{ij} is canonical projection. Thus, for any $\xi \in \hat{A}$, $\xi = (\xi_1, \xi_2, \cdots)$ such that $\xi_i \in A/\mathfrak{m}_i$ with $xi_i/\mathfrak{m}^j = \xi_j$ for any $j \leq i$.

Now, think the map $M \to M \otimes_A \hat{A}$. Pick $m \otimes \xi \in M \otimes_A \hat{A}$. We claim that $m \otimes \xi = m' \otimes 1$ where $1 = (1, 1, \cdots) \in \hat{A}$. Now, pick the smallest n such that $\mathfrak{m}^n m = 0$. Then, pick $a \in A$ such that $a/\mathfrak{m}^n = \xi_n$. Now we claim $am \otimes 1 = m \otimes \xi$. To see this, notes that $am \otimes 1 = m \otimes a$ where $a = (\overline{a}, \overline{a}, \cdots) \in \hat{A}$. Then, $\xi - a = (0, \cdots, 0, \xi_{n+1} - \overline{a}, \cdots) \in \hat{A}$. Pick the smallest n' such that $\xi_{n'} - \overline{a}$ is nonzero. Then, $\xi - a \in \mathfrak{m}^{n'} A \subset \mathfrak{m}^n A$, hence we may write it as $\sum_i r_i s_i$ for some $r_i \in \mathfrak{m}^n$ and $s_i \in \hat{A}$. Then,

$$m \otimes \xi - am \otimes 1 = m \otimes (\xi - a) = m \otimes \sum_i r_i s_i = \sum_i r_i m \otimes s_i = 0.$$

This shows that the map is surjective. □

Also, in the proof of (iii), F is injective hull of k as follow; for any $\hat{A}$-submodule N of F, $N \cap E$ is nonempty; and since $N \cap E$ has A-module structure, $N \cap E \cap k$ is nonempty; hence F is essential extension of k as $\hat{A}$-module. Then we may apply 18.4 (v) on F to say that every element of F is annihilated by power of maximal ideal of $\hat{A}$, which is $\mathfrak{m}\hat{A}$. Also, split of F as $E \oplus C$ is came from the injectivity of E.

In the proof of (iv), again the author uses technique in the proof of 18.6 (ii), which I explained above, to showing that $\mathrm{Hom}_A(A/\mathfrak{m}^v, E) \cong E_v$ and $\mathrm{Hom}_A(E_v, E_v) = \mathrm{Hom}_A(E_v, E)$.

In the proof of (v), M can be viewed as an $\hat{A}$-module by for any $\xi = (\xi_1, \cdots) \in \hat{A}$ and $m \in M$, $\xi m = \xi_v m$. This works well with A-module structure of M.

In the proof of (v), (E/M') seems errata of $(E/M)'$. And the identification $(E/M)' \cong M^\perp$ as follow; for any $\overline{f} \in \mathrm{Hom}_A(E/M, E)$, f can be extended to a homomorphism $f : \mathrm{Hom}_A(E, E)$ such that $\ker f \supseteq M$. Since the identification gives us f as the map $f(x) = ax$ for any $x \in E$, we claim $a \in M^\perp$; if $a \notin M^\perp$, then $\ker f \not\supseteq M$. Then nonzero conditoin of φ implies $\varphi(x/M) = ax$ for some $a \in M^\perp$. Also $x \notin M^{\perp\perp}$ otherwise $\varphi(x/M) = 0$. Thus, $E - M \subseteq E - M^{\perp\perp}$ implies $M \supseteq M^{\perp\perp}$, therefore equality holds.

Lastly, in case of $M \in \mathcal{A}$, to pick $\varphi : M \to E^n$ is injection, think about the generator $\{m_1, \cdots, \} \subset M$. Then we may construct $\sum_{i=1}^n Am_i \to E^n$ by $\oplus\varphi_i$ where φ_i was chosen by (i) so that $\varphi_i(m_i) \neq 0$. Now extend this map $\oplus_{i=1}^n \varphi_i : \oplus_{i=1}^n Am_i \to E^n$ to $\phi_n : M \to E^n$ by letting $\phi_n(m) = 0$ for all $j > n$ and $mM \setminus \sum_{i=1}^n Am_i$. Then, $\{\ker \phi_n\}_{n\in\mathbb{N}}$ form a descending chain of submodules of M, hence it stabilizes at some point; say n. Then, $\ker \phi_n = \ker \phi_{n+1} = \cdots$. Hence, if $\ker \phi_n \neq 0$, then pick $m \in \ker \phi_n$; then m is a finite A-linear combination of generators, thus there exists some $n' > n$ such that $\phi_{n'}(m) \neq 0$, contradiction. This induces the injective map.

Lastly, the double dual is isomorphic to original is well-explained in [4][p.106] proof of (c).

In the proof of Theorem 18.7, the identification $\mathrm{Hom}_A(k, I^i) = T_i$ is from the same techinque of the proof of Theorem 18.6 (iv). Also, we may assume that I^i is an essential extension of $d(I^{i-1})$ by construction of injective resolution; I^0 is just essential extension of M, and I^1 is essential extension of I^0/M, and I^2 is essential extension of $I^1/d(I^0)$, and so on. Also, $d(I^{i-1}) \cap k \neq 0$ implies $K \subset d(I^{i-1})$ since k is simple. Lastly, Theorem 4 (iii) should be changed to Theorem 5 (iii).

In the proof of Theorem 18.9, $\mathrm{Ext}^r_A(N, M) \neq 0$ by Lemma 1. And the last condition inequality came from the fact that the projective dimension of N should be defined as supremum of $\{n \in \mathbb{N} : \mathrm{Ext}^n_A(N, M) \neq 0 \text{ for some } M\}$.

1. Exercise 16.1 implies that A is CM iff B is CM. Assume $\dim A = n$. Thus, if A is Gorenstein, then take the maximal A sequence $x_1, \cdots, x_n$ containing $x_1, \cdots, x_r$. Then, $(x_1, \cdots, x_n)$ is irreducible, by Theorem 18.1 (5), thus its image in B is irreducible. Conversely, if B is Gorenstein, we have an irreducible parameter ideal by Theorem 18.1 (5'), then its preimage in A is irreducible, otherwise it is reducible in B, contradiction.

2. I don't know.

3. Given a prime ideal P of $A[X]$, by localising A at $P \cap A$ and factoring out by a system of parameters we reduce to proving that if (A, m, k) is a zerodimensional Gorenstein local ring, and P a prime ideal

of $A[X]$ such that $P \cap A = m$ then $B = A[X]_P$ is Gorenstein. Then we may assume $P = (m, f)$ where $m \in A$ and $f(X)$ is a monic polynomial in $A[X]$. Since P is prime, $A[X]/P \cong k[X]/(f)$ is domain, thus the image of f in $k[X]$ is irreducible. Since f is B-regular (because of monic), if we set $C = B/(f)$ then the maximal ideal of C is mC, and $C \simeq A[X]/(f)$; this is a free A -module of finite rank, so that $\mathrm{Hom}_C(C/mC, C) = \mathrm{Hom}_A(k, A) \otimes_A C($ by Ex. 7.7$) \simeq C/mC$. So C is Gorenstein by Theorem 18.1 (4) with $n = 0$, therefore B also by Exercise 18.1.

4. Let $R = k[x^3, x^2y, xy^2, y^3]$. From the Exercise 17.1, we knows that (x^3, y^3) form R-sequence. Then, $R/\left(x^3, y^3\right) = k\left[x^3, y^3, x^2y, xy^2\right] / \left(x^3, y^3\right) \simeq k[U, V] / \left(U^2, V^2, UV\right)$. In this ring $(0) = (U) \cap (V)$ as a parameter ideal is not irreducible, so that it is not Gorenstein, thus Exercise 18.1, R is not Gorenstein.

5. For $0 \neq a \in A$, the ideal aA is isomorphic to $\simeq A/\operatorname{ann}(a)$ with $\operatorname{ann}(a) \neq A$, so there exists a non-zero map $\varphi : aA \cong A/\operatorname{ann}(a) \longrightarrow A/\mathfrak{m} = k \subset E$. By Baer's criterion, φ extends to $A \longrightarrow E$, so that $0 \neq \operatorname{Im}\varphi \subset aE$ since $\varphi(ab) = \overline{a}\overline{b}$ for $\overline{b} \in k$, thus $a \cdot \overline{b}$ in E.

6. Since M is essential extension of k, it is contained in the injective hull $E = E_A(k)$; thus we can consider M as a submodule of E. Now, pick $f : M \to M$ from $\mathrm{Hom}_A(M, M)$. Then, for any nonzero $m \in M$, there exists $a \in A$ such that $am \neq 0$, thus if $f(n) = m$ then $af(n) = f(an) = am \neq 0$. Now, think $A1_M$ as a submodule of $\mathrm{Hom}_A(M, M)$. If $f_a : m \mapsto am$ and $f_b : m \mapsto bm$ is equal, then $(b - a)m = 0$ for all $m \in M$, thus $b - a \in \operatorname{ann}(M) = 0$, thus $b = a$; this shows that $A \to \mathrm{Hom}_A(M, M)$ by $a \mapsto f_a = a1_M$ is injective. Thus $A \cong A1_M \subset \mathrm{Hom}_A(M, M) \subset \mathrm{Hom}_A(M, E)$.

   Now, think the short exact sequence $0 \to M \to E \to E/M \to 0$, then take the Hom functor $\mathrm{Hom}_A(-, E)$. Since E is injective, the Hom functor is exact, thus

   $$0 \to \mathrm{Hom}_A(E/M, E) \to \mathrm{Hom}_A(E, E) \to \mathrm{Hom}_A(M, E) \to 0$$

   is exact. Now from A is complete, $\mathrm{Hom}_A(E, E) \cong A$ by Theorem 18.6 (iv). Moreover, (iv) says that any endomorphism $E \to E$ is nothing but just multiplication by elements of A, and since $M \to E$ is just injective, we knows that image of $\mathrm{Hom}_A(E, E)$ in $\mathrm{Hom}_A(M, E)$ is just multiplication by elements of A, i.e., the image is equal to $A1_M$; since the map $\mathrm{Hom}_A(E, E) \to \mathrm{Hom}_A(M, E)$ is surjective, $\mathrm{Hom}_A(M, E) = A1_M$. Hence, the kernel of $\mathrm{Hom}_A(E, E) \to \mathrm{Hom}_A(M, E)$ is zero, thus $\mathrm{Hom}_A(E/M, E) = 0$. Therefore, $E/M = 0$, by Exercise 18.6 (i).

7. Notes that E has also a $\hat{A}$-module structure, since for any $f \in \hat{A}, m \in E$, terms of f whose total degree is greater than absolute value of the smallest total degree of m as a polynomial over x_i^{-1} does not affect on m. Thus now we think A as $\hat{A}$.

   By Theorem 18.4 (vi), $E_S(S/P) = E_A(k)$ is clear. Thus, it suffices to show that $E = E_A(k)$. Definitely, E is an essential extension of k; to see this, pick a nonzero submodule N of E. Then N contains a nonzero polynomial $f(x_1^{-1}, \cdots, x_n^{-1})$. Pick the monomial of f with the smallest total degree, say x^α with $\alpha \in -\mathbb{N}^n$. Then, we can pick $x^{-\alpha} \in A$ so that $x^{-\alpha} f \in k$, which shows $N \cap k \neq 0$. Also, we claim that E is a faithful A-module. Suppose $f \in \operatorname{ann}(E) \subset A$; then $fc = 0$ for any $c \in k \subset E$, thus $f = 0$. Now Exercise 18.6 says that $E = E_A(k)$.

8. First of all, A is 1-dimensional domain (since $A/(t^3) \cong k[u, v]/(u^3, uv, v^3))$ with the Krull's Hauptidealsatz implies) and also depth is 1 (since t^3 is a regular element of A) therefore A is Cohen-Macaulay.

   To see A is not Gorenstein, we will show that $B := A/(t^3) \cong k[u, v]/(u^3, uv, v^3))$ is not Gorenstein. And in B, $(0) = (u) \cap (v)$, thus (0) as a parameter ideal is not irreducible, thus it is not Gorenstein.

   Likewise, for $A = k[[t^3, t^4, t^5]]$, $A/(t^3) \cong k[[u, v]]/(u^3, v^3, uv)$ which is not Gorenstein by the same reason that (0) is not irreducible. For $A = k[[t^4, t^5, t^6]]$, $A/(t^4) \cong k[[u, v]]/(u^2, v^2)$ by thinking $u = t^5, v = t^6$. (Notes that $t^{10} = t^4 \cdot t^6$, thus u^2 should be eliminated.) Hence, (0) is an irreducible parameter ideal; to see this, if $I \cap J = (0)$ for some nonzero ideals I and J, then for any generators $u^i v^j$ in I and $u^t v^s \in J$ it satisfies $u^{i+t} v^{j+s} = 0$. (Notes that we may assume all generators are monomial since A is local ring with unique monomial maximal ideal.) Hence, $i + t \geq 2$ or $j + s \geq 2$. The only possible cases are $(i, t) = (1, 1)$ or $(j, s) = (1, 1)$. In otherwords, all generators of I and J must form u or uv. Then $I \cap J = (u)$ or (uv), contradiction. Thus (0) is irreducible, therefore Gorenstein by Theorem 18.1 (5').

   For more general criterion, see [4][Theorem 4.4.8].

19 Regular rings

Let $(A, \mathfrak{m}, k)$ be a local ring, M, N are finite A modules. Given $\varphi : M \to N$ a A-linear maps, let $\overline{\varphi} : M \otimes k \to N \otimes k$.

Claim 26. *$\overline{\varphi}$ is isomorphism $\iff$ φ is surjective and* $\ker \varphi \subset \mathfrak{m}M$.

Proof. Suppose φ is surjective and $\ker \varphi \subset \mathfrak{m}M$. By NAK, we have generators $(x_1, \cdots, x_n)$ of M which gives basis of $M/\mathfrak{m}M \cong M \otimes k$ as a k-vector space. Then, $\varphi(x_1), \cdots, \varphi(x_n)$ generates N also by the assumption that φ is surjective. Since $N \cong M/\ker \varphi$ and $\ker \varphi \subset \mathfrak{m}M$, thus $N \otimes k \cong N/\mathfrak{m}N \cong (M/\ker \varphi)/(\mathfrak{m}M/\ker \varphi) \cong M/\mathfrak{m}M$. Also notes that $\varphi(x_i) \notin \mathfrak{m}N$, since otherwise, $N/\mathfrak{m}N \cong M/\mathfrak{m}M$ is generated by elements smaller than n, thus $\dim_k N/\mathfrak{m}N < \dim_k(M/\mathfrak{m}M)$, contradiction. Moreover, by the same reason, $\varphi(x_1), \cdots, \varphi(x_n)$ form a basis of $N/\mathfrak{m}N$ (otherwise dimension is less than that of $M/\mathfrak{m}M$). Thus, $\overline{\varphi}$ is a map sending basis to basis, thus it is an isomorphism.

Conversely, if $\overline{\varphi}$ is isomorphism, then again using NAK pick a generator $(x_1, \cdots, x_n)$ of M which gives basis of $M/\mathfrak{m}M \cong M \otimes k$ as a k-vector space. Still $\{\overline{\varphi}(x_i)\}_{i=1}^n$ generates $N/\mathfrak{m}N$, thus we claim that $\{\varphi(x_i)\}$ generates N; to see this $\varphi(M) \supsetneq N$, thus $\varphi(M)/\mathfrak{m}\varphi(M) = N/\mathfrak{m}N$ implies that $N \setminus \varphi(M) \subseteq \mathfrak{m}N$, thus we may find a generators of N in $\varphi(M)$ by the Nakayama lemma (Theorem 2.3 (i)), which implis that $\varphi(M)$ generates N. This shows that φ is surjective.

Also, now we claim $\ker \varphi \subseteq \mathfrak{m}N$. Suppose not; since φ is surjective, $N \cong M/\ker \phi$. Hence $N \otimes k \cong M/(\ker \phi + \mathfrak{m}M)$ which is a proper subspace of $M/\mathfrak{m}M \cong M \otimes k$, which contradicting the fact that $N \otimes k \cong M \otimes k$. □

Also, next iff statement is just application of Exercise 2.4 (b). Especially, $\det \varphi \notin \mathfrak{m}$ implies φ is isomorphism since given minimal basis $\{m_1, \cdots, m_n\}$ of M, $\sum_{i=1}^n a_i \varphi(m_i) = 0$, then $[a_1, \cdots, a_n][\varphi] = [b_1, \cdots, b_n]$ gives a linear combination such that $\sum_i b_i m_i = 0$ but this implies that $b_i \in \mathfrak{m}$. Hence there is a linear combination of rows of $[\varphi]$ which makes 0 in $A/\mathfrak{m}$, thus this implies that determinant of $[\varphi]$ should be 0 in $A/\mathfrak{m}$, contradiction.

Claim 27. *Any two minimal free resolution are isomorphic as a complex.*

Proof. Suppose $F^\bullet \to M$ and $G^\bullet \to M$ are two minimal free resolution. Now we will construct $\phi^\bullet$ as follow.

$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{f_3} & F_2 & \xrightarrow{f_2} & F_1 & \xrightarrow{f_1} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle Id} & & \\
\cdots & \xrightarrow{g_3} & G_2 & \xrightarrow{g_2} & G_1 & \xrightarrow{g_1} & M & \longrightarrow & 0
\end{array}$$

First of all, from the surjectivity of g_1 and F_1 is free (thus projective) we get ϕ_1 which commutes in the rectangular above. Now, by tensoring with k on the rectangular we have

$$\begin{array}{ccc}
F_1/\mathfrak{m}F_1 & \xrightarrow{\bar{f_1}} & M/\mathfrak{m}M \\
\downarrow{\scriptstyle \bar{\phi_1}} & & \downarrow{\scriptstyle Id} \\
G_1/\mathfrak{m}G_1 & \xrightarrow{\bar{g_1}} & M/\mathfrak{m}M
\end{array}$$

and since all $\overline{f_1}, \overline{g_1}$, and $\overline{1_M}$ are isomorphism, thus $\overline{\phi_1}$ is isomorphism. Therefore, by the second iff statement in p.153, ϕ_1 is isomorphism.

Then, ϕ_{i+1} can be obtained by thinking free resolution of $f_{i+1}(F_{i+1}) \cong g_{i+1}(F_{i+1})$ in $F_i \cong G_i$, and by the same argument ϕ_{i+1} are isomorphism, thus ϕ^* induces isomorphism of chain complexes. □

In the example, Koszul complex is minimal resolution since (1) each K_i is finite free A-module, (2) by construction each d_i is multiplication by elements of $\mathfrak{m}$, thus $d_i K_i \subset \mathfrak{m}K_{i-1}$ and (3) $K_0 = A \to A/(x_1, \cdots, x_n)$ is surjective and its kernel is inside of $\mathfrak{m}$, thus $K_0 \otimes k \to (A/(x_1, \cdots, x_n)) \otimes k$ is isomorphism by the first iff statement of p.153.

In the proof of Lemma 1, by taking $\mathrm{Hom}_A(-, k)$ on $L^\bullet \to M$, we knows that for any $f \in \mathrm{Hom}_A(A^n, k)$, $f(\mathfrak{m}A^n) = 0$ otherwise f is not homomorphism since $f(am) \neq 0$ but $af(m) = 0$ for some $a \in \mathfrak{m}$. Thus, any map $f : A^n \to k$ should induce $k^n \to k$ and vice versa, thus $\mathrm{Hom}_A(A^n, k) \cong \mathrm{Hom}_k(k^n, k)$, and by definition of minimal resolution, d_i maps A^n to $\mathfrak{m}A^m$ for some m, thus differential in $\mathrm{Hom}_A(L^\bullet, k)$ are zero maps; this implies that $\dim_k \mathrm{Ext}^i_A(M, k) = \mathrm{rank} L^i$.

Also, (ii) came from the fact that the projective dimension of M is less than the length n of $L^\bullet$. Also, if projective dimension of M is less than n, then $\mathrm{Tor}^n_A(M, N) = 0$ for any module N. However, $\dim_k \mathrm{Tor}^n_A(M, k) = \mathrm{rank} L_n$ thus $\mathrm{Tor}^n_A(M, k) \neq 0$, which implies the projective dimension is greater than or equal to n. Hence we can say that projective dimension of M is equal to the length of $L^\bullet$. Likewise, in the viewpoint of k, projective dimension of k should be greater than n, otherwise n-th Tor should be zero.

In (iii), NAK was followed with the fact that $(N/\mathfrak{m}N)^r$ is nonzero by assumption that $N \neq 0$.

In the proof of 19.1, the last exact sequence implies that if the middle is nonzero, then at least one of $\mathrm{Ext}^i(k, A)$ or $\mathrm{Ext}^{i+1}(k, A)$ should be nonzero, thus $\operatorname{depth} A \leq \operatorname{depth} M + 1$ which implies $\operatorname{depth} A - 1 \leq \operatorname{depth} M$. Conversely, if $i = \operatorname{depth} A$, then $\mathrm{Ext}^{i-1}_A(k, M) \neq 0$ by the exact sequence, which implies $\operatorname{depth} M \leq \operatorname{depth} A - 1$. Hence the equality holds.

Also, in the proof of 19.1, induction parts can be elaborated as follow; by inductive hypothesis, $h - 1 + \operatorname{depth} M' = \operatorname{depth} A$. Thus, it suffices to show that $\operatorname{depth} M = \operatorname{depth} M' - 1$. By the given exact sequence, take long exact sequence of $\mathrm{Ext}^i_A(k, -)$ to get

$$\cdots \to \mathrm{Ext}^{i-1}_A(k, M) \to \mathrm{Ext}^i_A(k, M') \to \mathrm{Ext}^i_A(k, A)^n \to \mathrm{Ext}^i_A(k, M) \to \mathrm{Ext}^{i+1}_A(k, M') \to \cdots$$

Let $m = \operatorname{depth} A := \inf\{i : \mathrm{Ext}^i_A(k, A) \neq 0\}$. Then, for any $i < m$,

$$\mathrm{Ext}^{i-1}_A(k, M) \cong \mathrm{Ext}^i_A(k, M')$$

since $\operatorname{depth} M' < m$, this induces $\operatorname{depth} M = \operatorname{depth} M' - 1$.

For lemma 2, (4) to (1), see [8][Lemma 4.1.6].

In the proof of Theorem 19.2 (II), they use Lemma 2 (ii) of section 18. Also, $\operatorname{proj\,dim}_B \mathfrak{m}/x\mathfrak{m} \leq r$ is came from Lemma 2 (4) $\implies$ (1) of this section. Also, the map $\mathfrak{m}/xA \to \mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/xA$ gives us split as $\mathfrak{m}/x\mathfrak{m} = \mathfrak{m}/xA \oplus \ker(\mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/xA)$ since the composition is identity, which induces $\mathfrak{m}/xA \cap \ker(\mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/xA) = 0$. Then the inequality of projective dimension are came from the fact that a projective resolution of direct sum can be constructed as a direct sum of two projective resolutions for each summand. Also, given a projective resolution $L^\bullet \to \mathfrak{m}/xA$, we can extend it to a projective resolution $L^\bullet \to B \to k$ using the short exact sequence. Hence projective dimension of k is less than $r + 1$.

Now, since the embedding dimension of B is $s - 1$, thus the inductive hypothesis with global dimension is less than infinity implies that B is regular. Hence, embedding dimension of B is equal to dimension of B, and since x is A-regular, we can conclude that A is regular local ring.

In Theorem 19.3, $L^\bullet \otimes A_P$ is also projective resolution since L is actually free (notes that projective module over a local Noetherian ring is free.) thus each tensor product is A_P-free module.

In the proof of 19.4, if we localize a regular ring A by a height 1 prime ideal P, then A_P is CM ring by Theorem 17.8, thus by Theorem 17.4, we can pick A_P-regular element, say a, in PA_P, then height of (a) is 1, and since a is also a part of system of parameter, $PA_P = (a)$. Hence, A_P is a Noetherian local ring with dimension greater than 0, and its maximal ideal is principal; thus By theorem 11.2 (3), it is DVR. Hence it satisfies Corollary of Theorem 11.5 (a). For the condition (b) of Theorem 11.5, replace A with a localization by a prime ideal. So we may assume A is regular local ring. Again, by Theorem 17.8, A is CM. Pick a nonzero nonunit $b \in A$. Since b is not a unit, $b \in \mathfrak{m}$. Since A is integral domain by Theorem 14.3, b is A-regular, thus all of its prime divisor have height 1 by unmixedness theorem.

In the proof of Theorem 19.5, let $\varphi : A \to A[X]$ the canonical injection. Then, $\mathfrak{m} = P \cap A$, and $\dim A[X]_P/\mathfrak{m}[X]_P = \dim(A[X]/\mathfrak{m}[X])_P = \dim k[X]_{(f(x))} = 1$. Since [2][Exercise 2.5] shows that φ is flat, we have the desired equality.

In the proof of Theorem 19.5 for $A[[X]]$, since $A[[X]]$ is (X)-adic completion, we can apply Theorem 8.2 (i) to say $X \in M$. However, honestly I don't know why $B_M \not\supseteq A_{\mathfrak{m}}[[X]]$ but their completions are the same; so I will try to introduce new simple proof.

Claim 28. *If A is regular, then $A[[X]]$ is regular.*

Proof. since $A[[X]]$ is (X)-adic completion, we can apply Theorem 8.2 (i) to say $X \in M$. Also, $X \notin M^2$, which is clear. And $A[[X]]/(X) \cong A$ is regular. Now we use below claim to conclude that $A[[X]]$ is regular. $\square$

Claim 29. *Let R be a commutative noetherian ring, $x \in R$ a non-zero divisor, and $x \in \mathfrak{m} - \mathfrak{m}^2$ for every maximal ideal $\mathfrak{m}$ of R. If $R/(x)$ is regular, then R is regular.*

Proof. Suppose $\dim R/(x) = n$. Pick an arbitrary maximal ideal $\mathfrak{m}$. Then, we may assume $R/(x)$ as a regular local ring by localizing it by $\mathfrak{m}$. Since $R/(x)$ is regular local ring, thus $\mathfrak{m}/(x)$ is generated by n-elements, say $x_2 + (x), \cdots, x_{n+1} + (x)$. Now we claim $(x, x_2, \cdots, x_{n+1}) = \mathfrak{m}$. To see this, for any $m \in \mathfrak{m}$, $m + (x) = (\sum_{i=2}^{n+1} a_i x_i) + (x)$. Hence, $m = (\sum_{i=2}^{n+1} a_i x_i) + ax$ for some $a \in A$, which implies the equality. Hence embedding dimension of R is $n+1$, thus $\dim R \leq n+1$. And, $\dim R/(x) + \mathrm{ht}(x) \leq \dim R$. Thus it suffices to show that height of x is 1. Since $\{x, x_2, \cdots, x_{n+1}\}$ form a system of parameter, Theorem 14.1 (ii) assures that there are another choice of system of parameters with length $n+1$ which generates a height $n+1$ ideal. This implies $\dim R \geq n+1$, done. $\square$

For the remark of 19.6, if A has depth 0 then 19.1 says that projective dimension of M for any finite module M is 0, which means that M is projective thus free.

Also, proof of Theorem 19.6 actually uses (reversed) induction; it shows that cokernel N is free, thus $F_n = 0$, then we can think next cokernel, and also shows that $F_{n-1} = 0$, and repeat this until it shows that M is free.

In the proof of Theorem 19.8, if $I_P = 0$, then for each generator $a \in I$, there exists $b \in A - P$ such that $a/1 = ab/b = 0/b = 0$. Since A is Noetherian, I is finitely generated, thus there exists $b \in A - P$ such that $bI = 0$. Hence $J = \mathrm{ann}(I) \not\subset P$ since $b \in J$. This argument also used to say $\mathrm{ann}(M) \not\subset P$ in (2) to (3).

In the proof of Theorem 19.9, If I is generated by A-sequences, then by Theorem 16.2, the generators are quasi regular. Then, we can show that I/I^2 is A/I-free module as follow; suppose $I = (a_1, \cdots, a_n)$, then there is a map $(A/I)^n \to I/I^2$ mapping $(b_1, \cdots, b_n) \mapsto \sum_i b_i a_i$. If there is a nonzero element in its kernel, say $(b_1, \cdots, b_n)$, then by letting $F = \sum_i b_i X_i$ and $F(a) \in I^2$ implies that all b_i's are in I, thus 0 in A/I. This can be applied for any $v > 0$ with I^v/I^{v+1}.

Also, in the proof of Theorem 19.9, ¡- this side, $\mathfrak{m}I$ should be replaced with I^2; and this can be sure, since all $I - I^2$ are in the union of associate primes, then I is inside of an associate prime by prime avoidance, contradiction.

In the remark, (a_{ij}) is invertible since it induces a map between two basis of $(I/I^2) \otimes A/\mathfrak{m}$. Therefore x_i form a quasi regular sequence since this matrix map induces an automorphism of $A/I[X_1, \cdots, X_n]$.

1. Since $R_\mathfrak{m}$ is n-dimensional regular local ring, we can say that $\mathfrak{m}R_\mathfrak{m} = (x_1, \cdots, x_n)$ such that x_i form a regular sequence as well as a system of parameter. Now, let $\phi : R \to k[y_i, \cdots, y_n]$ by sending x_i to y_i, where degree of y_i should be set to degree of x_i. Since every element of R can be expressed as a sum $\sum_{i=0}^{t} r_i$ with $r_i \in R_i$, and each r_i can be denoted as $\sum_{j=1}^{n} a_{ji} x_j$ with $\deg(a_{ji}) < i$. By repeating this argument again and again on a_{ji}, we may represent every element of R as a polynomial over x_is. Thus, we may set a map $\phi : R \to k[y_i]$ by sending x_i to y_i with positive degree equal to degree of x_i. This map is clearly surjective; also, if $f(x) \in \ker \phi$, then each homogeneous part of $f(x)$ makes x_i zero. However, by Theorem 16.2, x_i forms a quasi-regular sequence, thus this implies that each homogeneous part of $f(x)$ has zero constant (since it does not make sense that coefficient is in $\mathfrak{m}$ because we changed it all as in k.) Hence kernel is zero, therefore ϕ is isomorphism.

2. Use induction on the length of finite free resolution of a projective module M. If length is 0, then M is free therefore stably free, done. Suppose the length n is greater than 1. Then, given a finite free resolution $F^\bullet \to M$ as
$$0 \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to M \to 0,$$
take kernel of $F_0 \to M$ as M_1. Then, $0 \to M_1 \to F_0 \to M \to 0$ is exact sequence. Since M is projective, $F_0 \cong M_1 \oplus M$. Therefore M_1 is projective since it is a direct summand of free module. Since M_1 has length $n-1$ finite free resolution, by inductive hypothesis M_1 is stably free. Thus, $M_1 \oplus F$ is free for some free module F, thus $F_0 \oplus F \cong M \oplus (M_1 \oplus F)$ is free, thus M is stably free.

3. If $0 \to P_r \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \to 0$ is an exact sequence and each P_i is finite and projective, and if $P_0 \oplus A^n \simeq A^m$, then $\cdots \longrightarrow P_2 \longrightarrow P_1 \oplus A^n \longrightarrow P_0 \oplus A^n \longrightarrow M \to 0$ is again exact, with $P_0 \oplus A^n$ free. Proceeding in the same way, adding a free module to P_i at each stage, we get an FFR $0 \to L_{r+1} \longrightarrow L_r \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \to 0$

4. For every maximal ideal $\mathfrak{m}$ of A, since the A -module $A/\mathfrak{m}$ has an FFR, also the $A_{\mathfrak{m}}$ -module $A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$ has an FFR, so that the projective dimension of any module over $A_{\mathfrak{m}}$ is bounded by the length of FFR of $A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$ by Lemma 1. Thus global dimension of $A_{\mathfrak{m}}$ is finite, therefore Serre theorem (19.2) implies that $A_{\mathfrak{m}}$ is a regular local ring. Since $\mathfrak{m}$ was arbitrarily chosen, A is regular.

20 UFDs

In a Noetherian integral domains, every element is product of irreducible; to see this, suppose not; then pick such an element x which is not a product of irreducibles. Then, x is not irreducible, thus $x = yz$ for some y and z, and at least one of y and z are not a product of irreducibles, say y is not. Then $(x) \subseteq (y)$. By repeating this argument the chain of ideal stabilizes, contradiction.

Also, such a product of irreducibles is finite product, otherwise you can also an infinite ascending chain of ideals.

In proof of Theorem 20.1, the minimal prime divisor P of (a) is height greater than 0 since (0) is prime ideal in the integral domain.

In proof of Theorem 20.2, if $\dim A = 1$, then A is 1-dimensional Noetherian local ring, thus Theorem 11.2 implies that it is DVR; this is also UFD since every height 1 prime ideal is principal (with Theorem 20.1.)

In the proof of Theorem 20.3, P_Q is free; If P is not a subideal of Q, then P_Q contains a A_Q unit, thus $P_Q \cong A_Q$. If P is a subideal of Q, then P_Q is principal, thus $P_Q \cong A_Q$ as a module. In any cases, it is free.

In the proof of Theorem 20.4, $P \oplus A^n \subset A^{n+1}$. Since P is stably free, we may choose n such that $P \oplus A^n \cong A^m$ for some m. Then, $n < m \leq n+1$ implies $m = n+1$. That's why we can apply Lemma 1.

In Lemma 2 of p.164, since $e \in (a)$, $e = at$ for some t, thus $ab = ed = atd$ implies $b = td$. Also, since xst is divisible by e, $ed = xxst = xet'$ for some t', thus $d = xt'$.

In the proof of Theorem 20.5, ascending chain condition part is just corollary of Remark2, and two elements have lcm is another corollary of the proof of Remark2, since every elements has unique decomposition of irreducibles, thus their union gives us the lcm. The ascending chain condition on principal ideals gives finite products as follow; suppose a is not a finitely many product of irreducibles. Then, $a = a_1 b$, where one of a_1 or b is not a finitely many product of irreducibles, then $(a) \subsetneq (b)$. Now, we can repeat it infinitely so that we have infinitely ascending chains, contradiction.

In theorem 20.6, recall that freeness is not a local property, but projective is.

In theorem 20.7, he uses Theorem 11.3 that projective is equivalent to injective; thus if α is projective, then by 11.3 it is invertible, hence we may find $u_i \in K, a_i \in \alpha$ such that $\sum_i u_i a_i = 1$.

In the proof of 20.8, ascending chain conditions of principal ideal can be shown easily; if a chain start with nonconstant power series, say f whose minimal degree term is t, then this chain ends at finitely many times, since there are only finite length ascending chain of prime ideals consisting of power series whose minimal degree is t, but different A-coefficients by ASCofP in A, after than the next principal ideal should be generated by power series with smaller minimal degree terms, and so on.

Also, in the proof of 20.8, $B \otimes_B A = A$, thus $\mathfrak{a} \otimes_B A$ is projective as A-module, by taking tensors on the free module having $\mathfrak{a}$ as a direct summand. Also, now suppose $r := \min_{f \in \mathfrak{a}} \deg(f)$ where $\deg(f)$ means the least degree term of f. If $r = 0$, let $\mathfrak{b} = \mathfrak{a}$. Otherwise, for any $f \in \mathfrak{a}$, $f = X^r f'$ for some f' with nonzero constant in A, hence we may set $\mathfrak{b}$ is generated by such f', thus $\mathfrak{a} = X^r \mathfrak{b}$ with $\mathfrak{b} \not\subseteq XB$. Isomorphism $\mathfrak{a}/X\mathfrak{a} \cong \mathfrak{b}/X\mathfrak{b}$ are came from the correspondence between primitive elements.

Now since B is regular, thus normal by Theorem 19.4, therefore by Theorem 11.5, all the prime divisors of a nonzero principal ideal have height 1. Though $\mathfrak{b}$ itself may not be principal, but for any localization by maximal ideal of B, this induces a formal power series ring over regular local ring, thus also regular local, and hence 20.3 implies that the localization by maximal ideal is also UFD, and since localization of projective ideal is also projective, hence principal by Theorem 20.7. That's why $\mathfrak{b}$ is locally principal; since any prime divisor of $\mathfrak{B}$ also form a prime divisor in some of localization by a maximal ideal, thus it should have height 1 prime divisor by normality and Theorem 11.5. Here, NAK can be applied since X is in the Jacobson radical.

In the remark of divisor class group, we assume that A is Krull ring; that's why $C(A) = 0$ implies A is UFD.

In p.166,

$$A_{\mathfrak{p}} \otimes_A M \otimes_A M^* \cong M_{\mathfrak{p}} \otimes_A M^* \cong A_{\mathfrak{p}} \otimes_A M^* \cong \mathrm{Hom}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}, A_{\mathfrak{p}}) \cong \mathrm{Hom}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}, A_{\mathfrak{p}}) \cong A_{\mathfrak{p}}.$$

Also, if A is local, then every projective module is free, so there is only one isomorphism class, which makes picard group 0.

Also, if A is Krull ring, I is a fractional ideal of A, let $\mathcal{P}$ be the set of all height 1 prime ideals and $v_{\mathfrak{p}}(I) = \min\{v_{\mathfrak{p}}(x) : x \in I\}$. Then,

Claim 30. *$v_{\mathfrak{p}}(I)$ is nonzero for finitely many $\mathfrak{p}$.*

Proof. Suppose not; then we have an infinite subset $\{\mathfrak{p}_i\}$ of $\mathcal{P}$ such that $v_{\mathfrak{p}_i}(I) > 0$. This implies that $\mathfrak{p}_i \supset I$. Then, $\bigcap_i \mathfrak{p}_i \neq 0$ since $I \neq 0$. However, for any $x \in \bigcap_i \mathfrak{p}_i$, $v_{\mathfrak{p}_i}(x) > 0$, contradicting the fact that every elements in the Krull ring has at most finitely many nonzero valuations. $\square$

If I and I' are invertible, then $\mathrm{div}(I) = \mathrm{div}(I')$ implies $-\mathrm{div}(I^{-1}) = \mathrm{div}(I')$, thus $\mathrm{div}(I') + \mathrm{div}(I^{-1}) = \mathrm{div}(I^{-1}I') = 0$. Hence, $I^{-1}I' = A$. Thus $I' = I$.

1. Since A is UFD, every irreducibles are prime. Thus, It suffices to show that for any prime element p, it cannot divides all coefficients of fg. To see this, from f and g are primitive, let r (resp. s) be the greatest number less than $\deg f$ (resp. $\deg g$) such that the coefficient of f (resp. g) is divisible by p. Then, the $(r+s)$-degree part of fg has coefficients $\cdots + a_{r+1}b_{s-1} + a_r b_s + a_{r-1}b_{s+1} + \cdots$ where a_i (resp. b_i) is coefficient of f (resp. g) at degree i. Then, except $a_r b_s$, all other terms are divisible by p. Hence, the coefficient is not divisible by p. Since p was arbitrarily chosen, fg is primitive.

2. Let $f \in A[x]$ and K be field of fraction of A. Since $K[x]$ is PID, thus UFD, hence $f = cp_1(x)\cdots p_r(x)$ where $p_i(x)$ is irreducible in $K[x]$. By multiplying denominators occuring on all p_i, we may assume $p_i(x) \in A[x]$. Moreover, by extracting g.c.d. of coefficients of p_i, we also may assume that p_i is primitive in $A[x]$. This shows the existence of prime factorization of f. If f has another factorization by primitive polynomials, $f = dq_1(x)\cdots q_r(x)$, then it also form a factorization in $K[x]$, thus $r = s$, and using UFD of $K[X]$ we may assume that $q_i(x) = a_i p_i(x)$ for some $a_i \in K$. Since both p_i and q_i are primitive, a_i should have content 1, which implies that a_i is unit. Thus factorization is unique.

3. For any height 1 prime ideal P, it is principal by Theorem 20.1. Thus, assume $P = (p)$. Then a P-primary ideal Q should be inside of p. Now pick n such that $Q \subset (p^n)$ but $Q \not\subset (p^{n+1})$. Then, since $\sqrt{Q} = (p)$, $p^k \in Q$ for some k. If $k < n$, then $Q \not\subset (p^n)$ because $p^k \notin (p^n)$, contradiction; thus $k \geq n$. If $k \neq n$, then $k > n$, thus $Q \setminus (p^k) \neq$. Then we may pick $y \in Q \setminus (p^k)$. By prime factorization, $y = p^{n+t}q$ for some q which is not divisible by p, and $n + t < k$. Then, both p^{n+t} and q are not element of $\mathfrak{q}$, contradicting the fact that Q is P-primary. Hence, $k = n$, thus $Q = (p^n)$

   From this the intersection of primary ideals are intesection of principal ideals, thus by Remark 2 p.164, it is principal.

4. Exercise 8.3 shows that for any ideal I in A has a property that $I\hat{A}$ is principal, then I is principal. From this, every ascending chain of principal ideals of A should form ascending chain of principal ideals in $\hat{A}$, thus stabilizes, which implies that the chain in A also stabilizes.

   For the second condition, pick arbitrary two elements $a, b \in A$, then they has lcm in $\hat{A}$, say $\tilde{c}$. Then, $(a) \cap (b)\hat{A} = (\tilde{c})$, which is principal, thus $(a) \cap (b)$ is principal in A, say $(a) \cap (b) = (c)$, which implies that a and b has lcm in A.

5. Pick a height 1 prime ideal P in A. Suppose $\mathfrak{m}_i$ is a maximal ideal for $i = 1, 2, \cdots n$. Then, $PA_{\mathfrak{m}_i}$ is principal, say (u_i) for some $u_i \in A_{\mathfrak{m}_i} \subset K$. Also, if $u_i = a/b$ for some $a \in A, b \in A - \mathfrak{m}_i$, then $a/b = \sum_i p_i t_i$ for some $p_i \in P, t_i \in A_{\mathfrak{m}}$, thus $a \in P$ by combining rationals. Thus, we may assume that $u_i A_{\mathfrak{m}_i} = aA_{\mathfrak{m}_i}$ since b is unit in $A_{\mathfrak{m}}$. Thus, for any i, we may assume $u_i \in A$. Thus, for any $p \in P$, $p = u_i a/b$ for some $a \in A, b \in A \setminus m$, but since $p \in A$ and A is integral domain, $b = 1$, hence $P \subset (u_i)_{i=1}^n \subset P$, thus P is finitely generated.

   Next, we will use the Swan's theorem to conclude that P is principal. First of all, since A is semilocal, its m-Spec A satisfy descending chain condition, therefore Noetherian. Also, j-Spec (defined in p. 36) has the same combinatorial dimension with m-spec. Since maximal ideals in are not contained to others in each other, the combinatorial dimension is 0.

Now, pick a height 1 prime ideal P in A. Then for any j-prime ideal Q, if $Q \supset P$, then $P \otimes \kappa(Q) = 0$ since $PA_Q \subset QA_Q$. Otherwise, if $Q \not\supset P$, then $P \cap (A \setminus Q) \neq \emptyset$, thus $PA_Q = A_Q$. Hence, $P \otimes \kappa(Q) \cong PA_Q/PQA_Q = \kappa(Q)$. Hence, $\mu(P, Q)$ is at most 1 for any Q in j-spec.Hence, Theorem 5.8 implies that P is generated by 1 element, done.

6. Since $IR_{\mathfrak{m}} = a/bR_{\mathfrak{m}}$ for some $a \in R$, $b \in R \setminus \oplus_{n>0} R_n$, $g \in R_0$, hence b is also unit in R. Moreover, since $IR_{\mathfrak{m}}$ is also homogeneous ideal, we may assume a/b is homogeneous, which implies that a is homogeneous since $b \in R_0$. Since $a/b = \sum_i p_i t_i$ for some $p_i \in I, t_i \in R_{\mathfrak{m}}$, by combining $p_i t_i$ as a rational form we can conclude that $a \in I$. Hence, $IR_{\mathfrak{m}} = aR_{\mathfrak{m}}$. Now we claim $I = (a)$. $I \supset (a)$ is clear. For any homogeneous $g \in I$, $g/1 \in IR_{\mathfrak{m}}$, thus $g/1 = a/b \cdot c/d$ for some homogeneous $c \in R$ and $d \in R_0$. Thus, $tac = tdbg$ for some $t \in R_0$, thus $g = d^{-1}b^{-1}ca$, which implies that $g \in (a)$. Hence, $I = (a)$.

21 Complete intersection rings

In p.170, $0 \to L_n \to L_{n-1}$tensor with $A = R/\mathfrak{a}$ is still injective, thus $E_\bullet$ is still projective resolution of k as A-module.

Also in the second exact sequence, $\mathrm{Tor}_1^R(k, R) = 0$ since R is flat R-module. And $\mathrm{Tor}_1^R(kl, A)$ is typo of $\mathrm{Tor}_1^R(k, A)$. Also, since $k \otimes_R \to k \otimes A$ is a nonzero map $k \to k$ between simple modules so isomorphism. From this $k \otimes_R \mathfrak{a} \to k \otimes_R R$ 0. (Or you can think it as the image of $\mathfrak{a} \to R$ is inside of the maximal ideal of R.) Thus $\mathrm{Tor}_1^R(k, A) \cong k \otimes_R \mathfrak{a} \cong \mathfrak{a}/\mathfrak{n}\mathfrak{a}$. Here, you can check that $\mathfrak{n} \otimes \mathfrak{a} \cong \mathfrak{n}\mathfrak{a}$ by sending map $n \otimes a \to na$ which is surjective by construction, and injective by the fact that regular local ring is UFD, thus integral domain. Notes that $\mathfrak{a} \cong \mathfrak{n}\mathfrak{a}$ is k-module thus is vector space. Hence, $\mu(\mathfrak{a})$ is the number of basis element of $\mathfrak{a} \cong \mathfrak{n}\mathfrak{a} = \mathrm{Tor}_1^R(k, A) = H_1(E_\bullet)$, thus $\epsilon_1(A)$.

In the proof of Theorem 21.1 (ii), $\mu(\mathfrak{a}) \geq \mathrm{ht}\,\mathfrak{a}$ came from the Krull's Hauptidealsatz, and for regular local ring. Also $\dim R = \operatorname{emb}\dim A$ holds since in the previous argument about Koszul complex of A we showed that $\operatorname{emb}\dim A = \operatorname{emb}\dim R$.

In the proof of Theorem 21.3, Theorem 18.3 implies $\hat{A}$ is Gorenstein iff A is Gorenstein.

1. Given $P \in \operatorname{Spec} R$ with $P \supset I$, let $P/I = \mathfrak{p}$. Then, $A_{\mathfrak{p}}$ is c.i. iff (by Theorem 21.2 (ii)) I_p is generated by an R_P-sequence iff (by Theorem 19.9) $(I/I^2)_{\mathfrak{p}}$ is free over $A_{\mathfrak{p}}$. Since I/I^2 is a finite A-module, Theorem 4.10 implies that $\{P \in \operatorname{Spec} R : (I/I^2)_P \text{ is free over } R_P\}$ is open in $\operatorname{Spec} R$. Hence,
$$\{\mathfrak{p} \in \operatorname{Spec} A : A_{\mathfrak{p}} \text{ is c.i.}\} = \{P \in \operatorname{Spec} R : (I/I^2)_P \text{ is free over } R_P\} \cap \operatorname{Spec} A$$
is open in $\operatorname{Spec} A$ as a subspace topology.

2. We can assume that A is complete. Then $A = R/I$ with R regular and $\dim R = \dim A + 1$. Now ht $I = 1$ and A is a CM ring, so that all the prime divisors of I have height 1. Since R is a UFD, I is principal. Thus, $1 = \mu(I) = \dim R - \dim A$, hence A is c.i.

3. As a k-vector space, $A \cong k\{1, x, y, z, x^2\}$. Moreover, $x^2 = y^2 = z^2$ and $xy = yz = zx$. Thus, x, y, z are nilpotent, which implies that $\mathfrak{m}$ is the only prime ideal of A. Hence A is zero dimensional Noetherian ring, hence Cohen-Macaulay by Exercise 17.1 (a). Thus, by the argument of proof (1') to (2) in Theorem 18.1, using $0 \to k \to A$ by $\mathfrak{m} = \mathrm{ann}(x^2)$, we knows that $\mathrm{Ext}_A^1(k, A) = \mathrm{Hom}(k, A) \cong k$. Hence, A is Gorenstein.

   To see it is not c.i., Set $I = \left(X^2 - Y^2, Y^2 - Z^2, XY, YZ, ZX\right)$ and $M = (X, Y, Z)$. Then, MI has $X^3 = X(X^2 - Y^2) - Y(XY)$, $-Y^3 = Y(X^2 - Y^2) - X(XY), -Z^3 = Z(Y^2 - Z^2) - Y(YZ)$, and all other of degree 3 monomials, thus $MI = M^3$. Thus, $I/MI = I/M^3 \to M^2/M^3$ has five k-vector space dimensional image, so that $\mu(I) = 5$. However, $\dim R = 3, \dim A = 0$, thus $\mu(I) \neq \dim R - \dim A$, hence A is not c.i.

22 The local flatness criterion

In the proof of Theorem 1, M is J-adically separted by Krull's intersection theorem (Thm 8.10). In the proof of Theorem 2, exactness can be easily checked using diagram chasing.

For the example of I-adically separated case, $I(\mathfrak{a}\otimes M) \cong \mathfrak{a}\otimes IM$ since I acting via M. Thus, $\bigcap_{i=1}^{\infty} I^i(\mathfrak{a}\otimes M) = (\mathfrak{a}\otimes \bigcap_{i=1}^{\infty} I^i M) = 0$by applying Krull's intersection theorem on B.

In the proof of Theorem 3, (3) and (3') are just came from the long exact sequence of Tor in the third line of p.175. In (3') to (2), $\mathrm{Tor}_1^A(N, M)$ is came from the condition that $N \otimes_A M = N \otimes_{A_0} M_0$, thus tor can be derived from A-tensor with M. IN (3) to (4), $I \otimes M \cong IM$ implies $I^2 \otimes M \cong I^2 M$ since the injective map $I^2 \otimes M \to I \otimes M \to IM$ gives image $I^2 M$ inside of IM. In (4) to (5), there is a typo on the diagram; the first row should be

$$(I^{i+1}/I^{n+1}) \otimes M \to (I^i/I^{n+1}) \otimes M \to I^i/I^{i+1} \otimes M \to 0$$

which induced from tensoring M with the exact sequence $0 \to (I^{i+1}/I^{n+1}) \to (I^i/I^{n+1}) \to I^i/I^{i+1} \to 0$. In the induction, α_{n+1} is isomorphism by putting $i = n$.

In Theorem 22.4, local homomorphism $A \to B$ means that the maximal ideal of A will be sent to inside of maximal ideal of B. For proof (i), notes that $\hat{B}$ is faithfully flat over B. If M is flat over A, then for any exact sequence $N_1 \to N_2 \to N_3$ of A-modules, $N_i \otimes_A M = N_i \otimes_A B \otimes_B M$ is exact as a (A, B)-bimodule. Hence, by taking tensor with $\hat{B}$, which is faithfully over B, $N_1 \otimes_A \hat{M} \to N_2 \otimes_A \hat{M} \to N_3 \otimes_A \hat{M}$ is exact as a (A, B)-bimodule, hence $\tilde{M}$ is exact in A-module. Conversely, if $\hat{M}$ is flat over A, then for any exact sequence $N_1 \to N_2 \to N_3$ of A-modules, $N_1 \otimes_A \hat{M} \to N_2 \otimes_A \hat{M} \to N_3 \otimes_A \hat{M}$ is exact as (A, B)-bimodule. Since $N_i \otimes_A \hat{M} = N_i \otimes_A M \otimes_B \hat{B}$ and $\hat{B}$ is faithfully flat, $N_1 \otimes_A \hat{M} \to N_2 \otimes_A \hat{M} \to N_3 \otimes_A \hat{M}$ is exact as a (A, B)-bimodule, thus M is flat over A.

For the second equivalence of Theorem 22.4 (i), if $\hat{M}$ is flat over A, then cTheorem 22.1 implies that $\hat{M}/\mathfrak{m}^n\hat{M}$ is flat over A for all $n > 0$. Then, $\hat{M}/\mathfrak{m}^n\hat{M}$ is flat over $A/\mathfrak{m}^n$ for all $n > 0$ since all exact sequences of $A/\mathfrak{m}^n$-modules are those of A-modules. Now we claim that $\hat{M}/\mathfrak{m}^n\hat{M}$ is flat over $\hat{A}$, since any $\hat{A}$-modules has also an A-modules structure via $A \to \hat{A}$ which is faithfully flat by Theorem 8.14. Conversely, if $\hat{M}$ is flat over $\hat{A}$, then for any exact sequences of A-moduels, tensor with $\hat{A}$ is also exact, thus tensor with $\hat{M}$ is also exact, hence $\hat{M}$ is flat over A.

(ii) is similar. Indeed, local condition implies that $\mathfrak{m}B \subset \mathfrak{n}$ so that we can use Theorem 8.14 again.

In the proof of 22.5, let $f : A \to B$ be the local homomorphism. if (1) holds, then $0 \to M \to N \to N/u(M) \to 0$ is exact. Now take a long exact sequence from $\mathrm{Tor}_{\bullet}^A(-, k)$ to get the exact seqeunce $0 = \mathrm{Tor}_1^A(N/u(M), k) \to M \otimes k \to N \otimes k \to (N/u(M)) \otimes k \to 0$, which implies that $\overline{u}$ is injective.

In the proof of (2) to (1), $\bigcap_n \mathfrak{m}^n M = 0$ is from Krull's intersection theorem with the fact that $\mathfrak{m}B \subset \mathfrak{n}$, and the vanishing of $\mathrm{Tor}_1^A(k, N/u(M)) = 0$ is came from the long exact sequence of tor, $\overline{u}$ is injective, and N is flat.

For the corollary in p.177, (2) to (1) is just setting $M = N = M$ in the setting of Theorem 22.5 and apply theorem inductively. Also, (1) to (2) is just inductively use Theorem 22.5 (1) to (2) for each i forwardly, with the fact that M_i is flat.

In theorem 22.6, $M/(P \cap A) = M \otimes_A A/(P \cap A)$. Then, by replacing A with $A_{(P\cap A)}$ M is flat over A which is local ring whose maximal ideal is $(P \cap A)$, then we may apply the first corollary (2) to (1) in p.177 to get b is $M_{(A\cap P)}$ regular and $M_{(A\cap P)}/bM_{(A\cap P)}$ is flat.

Claim 31 (Remark in p.177 (Flatness of a graded module))**.** *Let G be an Abelian group, $R = \bigoplus_{g\in G} R_g$ a G-graded ring and $M = \bigoplus_{g\in G} M_g$ a graded R-module, not necessarily finitely generated. Then the following three conditions are equivalent:*

(a) M is R-flat;

(b) If $\mathscr{S} : \cdots \longrightarrow N \longrightarrow N' \longrightarrow N'' \longrightarrow \cdots$ is an exact sequence of graded R -modules and R -linear maps preserving degrees, then $\mathscr{S} \otimes M$ is exact.

(c) Tor $_1^R(M, R/H) = 0$ for every finitely generated homogeneous ideal H of R.

This proof is from [6]

Proof. (a) to (c) is clear by definition. (c) to (b) is clear by thinking $N^{''}$ or N as a direct sum of R/H for some graded quotients, and think the commutativity between direct sum and Tor. Now it suffices to show that (b) to (a).

To see this, we will use Theorem 7.6 in Matsumura. Suppose $a_i \in R, x_i \in M$ where $i \in I$ with $|I| < \infty$ with the property that $\sum_{i\in I} a_i x_i = 0$. Then for each i, we may assume $a_i = \sum_{g\in G} a_{i,g}, x_i = \sum_{g\in G} x_{i,g}$ with $a_{i,g} \in R_g, x_{i,g} \in M_g$. Then the condition $\sum_{i\in I} a_i x_i = 0$ is equivalent to

$$\sum_{i\in I, h\in G} a_{i,g-h} x_{i,h} = 0 \text{ for any } g \in G.$$

Now construct a free R-module F whose base is $\{e_{i,g} : i \in I, g \in G\}$ and F' whose base is $\{e'_g : g \in G\}$, then let $f : F \to F'$ by $f(e_{i,h}) = \sum_{g\in G} a_{i,g-h} e'_g$ for any $g \in G, i \in I$. Then, giving degree $-h$ to $e_{i,h}$ and degree $-g$ to e'_g, F and F' become graded R-modules and f is a graded homomorhpism. Thus,

$$0 \to \ker f \otimes_R M \to F \otimes_R M \xrightarrow{f\otimes 1} F' \otimes_R M$$

is exact by (b). Since

$$f \otimes 1 \left(\sum_{i\in I, h\in G} e_{i,h} \otimes x_{i,h} \right) = \sum_{i\in I, h\in G} (\sum_{g\in G} a_{i,g-h} e_g) \otimes x_{i,h} = \sum_{g\in G} (e_g) \otimes \sum_{i\in I, h\in G} a_{i,g-h} x_{i,h} = \sum_{g\in G} (e_g) \otimes 0 = 0,$$

we can conclude that $\sum_{i\in I, h\in G} e_{i,h} \otimes x_{i,h} = \sum_{j\in J} b^{(j)} \otimes y^{(j)}$ for some $b^{(j)} \in \ker f$, $y^{(j)} \in M$ with $b^{(j)} = \sum_{i\in I, h\in G} b^{(j)}_{i,h} e_{i,h}$. Then, set $b^{(j)}_i = \sum_{h\in G} b^{(j)}_{i,h}$, which implies $\sum_{i\in I} b^{(j)}_i a_i = 0$ (by applying f on $b^{(j)}$ and thinking grade g terms of $f(b^{(j)})$). □

Claim 32. *From the above claim, let I be a (not necessarily homogeneous) ideal of R. Suppose that*

1. *for every finitely generated homogeneous ideal H of R, the R -module $H \otimes_R M$ is I -adically separated;*
2. *$M_0 = M/IM$ is R/I -flat;*
3. $\mathrm{Tor}_1^R(M, R/I) = 0$.

Then M is R -flat.

Again, this proof is from [6]

Proof. It suffices to show that for every finitely generated homogeneous ideal H of R, $\mathrm{Tor}_1^R(R/H, M) = 0$, i.e., $H \otimes_R M \to M$ is injective. Now (2) and (3) gives the condition (3') of Theorem 22.3, thus M is flat over A, thus $\mathrm{Tor}_1^R(R/H, M) = 0$. □

Claim 33. *Let $A = \bigoplus_{n\geqslant 0} A_n$ and $B = \bigoplus_{n\geqslant 0} B_n$ be graded Noetherian rings. Assume that A_0, B_0 are local rings with maximal ideals m, n and set $M = m+ A_1 + A_2 + \cdots, N = \mathrm{n} + B_1 + B_2 + \cdots$ let $f : A \longrightarrow B$ be a ring homomorphism of degree 0 such that $f(m) \subset n$. Then the following are equivalent:*

1. *B is A -flat;*
2. *B_N is A -flat;*
3. *B_N is A_M -flat.*

This is just proposition 3.6.

Proof. Since localization is flat algebra, thus (1) implies (2). (2) implies $0 = \mathrm{Tor}_1^A(C, B_N) \cong \mathrm{Tor}_1^{A_{N\cap A}}(C, B_N) = \mathrm{Tor}_1^{A_M}(C, B_N)$ for any A-module C. Since every A_M module is also an A-module, this implies that B_N is flat over A_M. Now, to see (3) implies (1), notes that condition 3 gives us $0 = \mathrm{Tor}_1^A(k, B_N) \cong \mathrm{Tor}_1^{A_{N\cap A}}(k, B_N) = \mathrm{Tor}_1^{A_M}(k, B)_N$ where $k = A/M$. Also, since $\mathrm{Tor}_1^{A_M}(k, B)$ is graded module, $\mathrm{Tor}_1^{A_M}(k, B) = 0$. Moreover, $B_0 = B/f(N)B$ is A/N-flat since it is a vector space over A/N. Moreover, for any finitely generated homogeneous ideal H of A, $H \otimes_A B$ is M-adically separated since B is N-adically separated (to see this, use Krull's intersection theorem for $\mathfrak{n}$ part and and grades goes to infinity) and $f(M) \subset N$, thus B is M-adically separated therefore so $H \otimes_A B$ is. Hence, by the above claim B is flat over A. □

1. This uses the claim for flatness.

 Claim 34. *Let $A \subset B$ be Noetherian rings, let $M^* := m - \operatorname{Spec} B$ and $M := \{\mathfrak{m} \cap A : \mathfrak{m} \in m - \operatorname{Spec} B\} \cap \operatorname{Spec} A$. Then, B is flat over A iff for any $\mathfrak{m}$-primary ideal $\mathfrak{q}$ over $\mathfrak{m} \in M$ and $b \in A$ such that $\mathfrak{q} : (b) = \mathfrak{m}$, $\mathfrak{q}B : bB = \mathfrak{m}B$.*

 Proof. Only if part is just directly came from Theorem 7.4 (iii). Suppose if part. Notes that the all conditions still hold if we replace A and B with $A_{\mathfrak{m}\cap A}$ and $B_{\mathfrak{m}}$ for any $\mathfrak{m} \in M^*$. Since flatness is a local property, assume that A and B are local ring and $\mathfrak{m} \cap A$ is the maximal ideal of A. We will show that B is flat using Theorem 7.7. Let I be an ideal of A.

 Case 1: Suppose $\mathfrak{m} \cap A$ is nilpotent. If length of A is 1, then A is field, thus using the assertion holds. If length of A is greater than 1, pick $b \in I$ (using Krull's principal ideal theorem) such that $l_A(bA) = 1$. This implies that $0 : bA = \mathfrak{m} \cap A$, since $b(\mathfrak{m} \cap A) = (b) \cap (\mathfrak{m} \cap A)$ is a submodule of bA, which is a simple module, thus $b(\mathfrak{m} \cap A) = 0$. By inductive assumption, B/bB is flat over A/bA, thus $I/(bA) \otimes_{A/bA} B/bB \to B/bB$ is injective. Hence, the kernel of $I \otimes B \to B$ is in $bA \otimes B$. Since $0 : bB = (\mathfrak{m} \cap A)B$ by the if condition, bB and $b \otimes B$ are faithful modules over $B/(\mathfrak{m} \cap A)B$, which is reduced ring. Thus, for any nonzero element $b \otimes c$ (thus $c \in B \setminus (\mathfrak{m} \cap A)B$), its annihilator in $B/(\mathfrak{m} \cap A)B$ does not exist, hence $bc \neq 0$, which implies that kernel is zero.

 Case 2: In general, by case 1, for any $n > 0$, $B/(\mathfrak{m} \cap A)^n B$ is flat over $A/(\mathfrak{m} \cap A)^n$. Hence, $I/((\mathfrak{m} \cap A)^n \cap I) \otimes B/(\mathfrak{m} \cap A)^n B$ is inside of $A/(\mathfrak{m} \cap A)^n \otimes B/(\mathfrak{m} \cap A)^n B$, which implies that the kernel should be contained in $((\mathfrak{m} \cap A)^n \cap I) \otimes B$ in $I \otimes B$. Now, by Artin-Rees lemma, we have r such that $((\mathfrak{m} \cap A)^n \cap I) \subset (\mathfrak{m} \cap A)^{n-r} I$, thus the kernel is inside of $(\bigcap_n (\mathfrak{m} \cap A)^{n-r} I) \otimes B \cong I \otimes (\bigcap_n (\mathfrak{m} \cap A)^{n-r} B$. Now since $\mathfrak{m} \cap A \subset \mathfrak{m}$ which is Jacobson radical of B, the Krull's intersection theorem concludes that this module is zero. □

 Now let's prove Nagata's flatness theorem. Because of the lemma, it suffices to show that the equation of lenghths are equivalent to the condition that for any $\mathfrak{m}$-primary ideal $\mathfrak{q}$ and $b \in A$ such that $\mathfrak{q} : bA = \mathfrak{m}$, $\mathfrak{q}B : bB = \mathfrak{m}B$.

 Set $\mathfrak{q}' = \mathfrak{q} + bA$. Then the length of $(A/\mathfrak{q})$ is equal to the length of $(A/\mathfrak{q}')$ plus 1 (since b is not unit by the condition $\mathfrak{q} : bA = \mathfrak{m}$). Also, $\mathfrak{q}'$ is also $\mathfrak{m}$ primary since $\mathfrak{q} : bA = \mathfrak{m}$. Thus, by the formular of lengths gives

 $$l_A(A/\mathfrak{q}) l_B(B/\mathfrak{m}B) = l_B(B/\mathfrak{q}B),$$
 $$l_A(A/\mathfrak{q}') l_B(B/\mathfrak{m}B) = l_B(B/\mathfrak{q}'B),$$
 $$l_A(A/\mathfrak{q}') + 1 = l_A(A/\mathfrak{q})$$

 implies that

 $$l_B(B/\mathfrak{q}'B) + l_B(B/\mathfrak{m}B) = l_B(B/\mathfrak{q}B).$$

 On the other hand, from

 $$l_B(B/\mathfrak{q}B) = l_B(B/\mathfrak{q}'B) + l_B(\mathfrak{q}'B/\mathfrak{q}B),$$

 we have $l_B(\mathfrak{q}'B/\mathfrak{q}B) = l_B(B/\mathfrak{m}B)$. Here,

 $$l_B(B/\mathfrak{m}B) = l_B(\mathfrak{q}'B/\mathfrak{q}B) = l_B(bB/(bB \cap \mathfrak{q}B)) = l_B(B/(\mathfrak{q}B : bB)).$$

 This implies $\mathfrak{m}B = \mathfrak{q}B : bB$. (Notes that $\supset$ is clear from definition, and $\subset$ is from the equation above.)

 Conversely, we can use induction on $l_A(A/\mathfrak{q})$. If length is 1, then $\mathfrak{q} = \mathfrak{m}$, thus the length equation holds. For any $n > 1$, we get all the equations reversely to get $l_A(A/\mathfrak{q}) l_B(B/\mathfrak{m}B) = l_B(B/\mathfrak{q}B)$ under the inductive hypothesis.

2. Algebraic independence comes from Theorem 16.2, (i). If $f \in k[X_1, \cdots, X_n]$ gives a relation s.t. $f(x_i) = 0$, notes that f has zero constant term, otherwise $k \cap (x_i) \neq 0$, contradiction. Hence, we may let v be the least degree of terms in f. Then, by replacing X_i with x_i suitably, we may find g, which is a v-homogeneous such that whose the least degree term has coefficient in k and $g(x_i) = 0$. However,

since x_i is A-quasi-regular by Theorem 16.2 (i), $g(x_i) = 0$ implies that the least degree term of g should be inside of I, thus the coefficient should be zero, contradiction. Hence, no such relation f exists.

Before proving flatness, notes that k is a subfield of the residue field $A/\mathfrak{m}$.

To prove flatness, let $I = \sum x_i C$. Then A_0 in Theorem 22.3 is k, M in Theorem 22.3 is A. Hence, M_0 in Theorem 22.3 is $A/(x_1, \cdots, x_n)$ which is flat over A_0 since $A_0 = k$ is field, thus $A/(x_1, \cdots, x_n)$ is nothing but vector spaces. Thus, to see $M = A$ is flat over C, it suffices to show that $\operatorname{Tor}_1^C(k, A) = 0$. Since $\underline{x}$ is a C -sequence, the Koszul complex $L_\bullet = K_\bullet(\underline{x}, C)$ constructed from C and x is a free resolution of the C-module $k = C/I$, and $\operatorname{Tor}_1^C(k, A) = H_1(L_\bullet \otimes_C A)$, from the argument in Section 19 Regular rings and minimal free resolution. However, $L_\bullet \otimes_C A$ is just the Koszul complex constructed from A and x, and since $\underline{x}$ is an A -sequence, $H_1(L_. \otimes A) = 0$ by Theorem 16.5.

3. We need only show that $\operatorname{Tor}_1^A(k, M) = 0$. By Lemma 18.2, $\operatorname{Tor}\ _1^A(k, M) = \operatorname{Tor}_1^{A/xA}(k, M/xM)$, but by assumption the right-hand side is 0.

4. I-adic completion of B as an A-module is equal to IB-adic completion of B as B-module (since I acts on B as IB), thus equal to J-adic completion of B since $IB \subset J$ by Exercise 8.2. Thus, $\hat{B} = B \otimes_A \hat{A}$ is flat over A since tensor with B over exact sequence of A module is exact, and tensor with $\hat{A}$ is also exact by Theorem 8.8. Then, for any exact sequence $M \to N \to L$ of $\hat{A}$ modules, this is actually an exact sequence of A-modules, thus tensor with $\hat{B}$ is exact, which shows that $\hat{B}$ is flat over $\hat{A}$.

23 Flatness and fibres

In the proof of Theorem 23.1, $\dim A' = \dim A - 1$ is came from the regularity of A and $x \in \mathfrak{m} - \mathfrak{m}^2$. Also, if x as an element of B is a part of system of parameter, then by Theorem 17.4 $\dim B' = \dim B - 1$. Otherwise, height of x maybe 0, thus $\dim B' > \dim B - 1$. In any cases, $\dim B' \geq \dim B - 1$. Lastly, if x is both A and B-regular, then by Lemma 2 in p.140, the claim holds.

In the proof of Theorem 23.2 (i), $G \otimes_A (A/\mathfrak{p})$ is $A/\mathfrak{p}$ flat as follow; for any exact sequences of $A/\mathfrak{p}$ modules, we can rewrite it as $(A/\mathfrak{p})$-tensored with $A/\mathfrak{p}$, however this still can be regarded as A-modules, thus A-tensor with G is exact by flatness of G, which coincide with $A/\mathfrak{p}$-tensor with $G \otimes_A (A/\mathfrak{p})$, done.

In the proof of Theorem 23.3, p.181, N_1 is flat implies that $\operatorname{Tor}_1^A(M_r, N_1) = 0$, which implies $0 \to M_r \otimes N \to M_r \otimes N \to M_r \otimes N_1 \to 0$ is exact. Lastly, the assertion derived when we set $E = M_r$, $G = N_s, \mathfrak{p} = \mathfrak{m}$ in Theorem 23.2 (ii).

In the proof of Theorem 23.4, let $f : A \to B$ be the given local homomorphism. Then $f(x_i)$ in B form B-regular sequences by Exercise 16.4. Also, to see $\overline{B}$ is flat $\overline{A}$ modules, notes that the corollary of Theorem 22.5 (2) to (1) implies that $B/(\underline{y})B$ is flat over A. Now, notes $\{0\}$ is also a trivial $M \otimes k$-sequence (in terms of Theorem 22.5), hence apply the corollary again with x_i from A, setting $M = B/(\underline{y})B$, we can get the statement that $\overline{B}$ is flat over $\overline{A}$.

Now, $\operatorname{Hom}_R(R/M, R) = (0 : M)_R$ is from the condition $f(1) \in (0 : M)_R$ for all $f \in \operatorname{Hom}_R(R/M, R)$. The phrase "$I$ is of the form $I \cong (A/\mathfrak{m})^t$ for some t means that I is $A/\mathfrak{m}$-vector space. Also, since B is flat, $(0 : \mathfrak{m}B) = IB$ by Theorem 7.4.

In the proof of Theorem 23.5, regularity of the localization of polynomial ring over a field or power series ring came from the fact that any of their maximal ideal has of form $(x_i - a_i)$. (Recall that A is regular local ring if the minimal number of generators of the maximal ideal is equal to the Krull-dim.)

In Theorem 23.6, any localization of Gorenstein ring is Gorenstein, but I highly doubt that $A \otimes K$ is a localization by a prime; however the conclusion still hold, since all the primes in a localization is just inherited from primes in original ring which do not intersect with multiplicative set, thus localization of $A \otimes K$ by a prime coincides with localization of $A[X]$ by some prime.

In the proof of 23.7, B is faithfully flat since local homomorphism implies $\mathfrak{m}B \neq B$ with Theorem 7.2.(3). Then tor vanishes by thinking long exact sequence splited from the long exact sequence of projective resolution of k tensored with k such that whose part tensored with B has vanishing cohomology. Also, since B is flat over A, if $f : A \to B$ has nonzero kernel, then $0 \to \ker f \to A \to A/\ker f \to 0$ induces $0 \to \ker f \otimes B \to B \to B \to 0$, which implies $\ker f \otimes B = 0$ which contradict Theorem 7.2 (2). Hence f is injective.

In p. 183, if A has an embedded associate prime P, then $\min(\operatorname{ht} P, 1) = 1$ while $\operatorname{depth} A_P = 0$, thus S_1 cannot hold. Again, if A is an integral domain, and P is an embedded associate prime of (a) for some nonzero principal ideal, then $\min(\operatorname{ht} P, 2) = 2$ since (Krull's Hauptidealsatz implies that) all minimal prime divisor has height 1, however A_P/a has no regular element, thus $\operatorname{depth} A_P = 1$. Hence S_2 implies the condition in textbook.

Form Theorem 14.3, 1-dim regular local ring is just another name of DVR. That's why 11.2 implies R_1. Also 11.5 implies S_2 is clear.

In the proof of Theorem 23.8, $a^n + \sum_1^n c_i a^{n-i} b^i = 0$ can be seen as an integral equation over $b_P A_P$. Since A_P is normal, thus $b_P A_P$ is integrally closed, hence $a_P \in b_P A_P$ from the localized integral equation.

In the proof of Theorem 23.9, all such bounds of height of prime ideals between A and B are came from going down theorem because of faithfully flat algebra B.

1. This just came from the fact that completion of Gorenstein local ring is Gorenstein (Theorem 18.3) and Theorem 23.4, and completion of Cohen-Macaulay local ring is Cohen-Macaulay (Theorem 17.5) and Corollary of Theorem 23.3.

2. By Theorem 23.9, it suffices to show that all fibers of $A \to \hat{A}$ satisfy S_i. From the given condition, let $A = R/I$ where R is CM local ring, and I is an ideal. Pick $\mathfrak{p} \in \operatorname{Spec} A$ such that $\mathfrak{p}'/I = \mathfrak{p}$ for some $\mathfrak{p}' \in \operatorname{Spec} R$. Then, set $B' = \hat{R}$ and $B = B'/IB' = \hat{R}/I\hat{R} = (\widehat{R/I}) = \hat{A}$ from Theorem 8.11. Then by the argument in p.184 185, fibre of $A \to \hat{A}$ at $\mathfrak{p}$ is equal to that of $R \to \hat{R}$ at $\mathfrak{p}'$. Thus, it suffices to show that all fibers of $R \to \hat{R}$ satisfy S_i. This is true by Exercise 23.1, done. Especially, if A does not have embedded associate prime, then A follows S_1, thus $\hat{A}$ follows S_1, which implies the desired statement.

3. I don't know.

24 Generic freeness and open loci results

In the proof of Theorem 24.1, for $S_k M'/S_{k-1}M$ cases, by letting $E = S_k M'$, $F = S_{k-1}M'$, $B = S_{k-1}$, $C = S_k$ as in Lemma to get the conclusion. For E/SM' cases, by letting $B = S_{k-1}, C = S, E = E', F = E_{k-1}$ to get the finite filtrations of S_{k-1}modules, which also gave finite filtrations of S-modules by induction hypothesis, done.

In the proof of topological Nagata criterion, the third line means that the property actually contradicts the irreducibility of V_i

In the proof of Theorem 24.3, honestly I don't know how he can find W; instead, using Theorem 24.1, pick $a \in A \setminus \mathfrak{p}$ which makes $(M/\mathfrak{p}M)_a$ be a free $(A_\mathfrak{p})_a$ module. Then, $(M/\mathfrak{p}M)_a$ is flat. Now, from $M_a = M_{f(a)}$ by letting $f : A \to B$ the algebra map, we can see that $(M/\mathfrak{p}M)_a = B_{f(a)} \otimes_B M \otimes_A \hat{A}$. Then by the fact that flatness is a local property, for any $Q \notin V(aB)$ which lies over $\mathfrak{p}$, $((M/\mathfrak{p}M)_a)_Q = (M/\mathfrak{p}M)_Q$ is A-flat since flatness is local property. Since $\mathfrak{p} = P \cap A$, Q lies over $\mathfrak{p}$ iff $Q \supset P$, hence all prime ideals in $V(P) \setminus V(aB)$ makes $(M/\mathfrak{p}M)$ flat. Since $V(P) \cap V(aB)^c$ is open neighborhood of P at U, and P was arbitrarily chosen, we can see that U is open. (Remark that $V(aB)^c = \emptyset$ iff a is unit, but in this case, $M/\mathfrak{p}M$ is free, thus $V(P)$ is contained in U, hence its nonempty open subset is contained in U, thus (2) of Theorem 24.2 holds)

In Theorem 24.4, W can be obtained by taking $a \in \bigcap_{Q \in \operatorname{Ass}(x_1, \cdots, x_n)} Q \setminus P$, then we may set $W = \bigcup_a V(a)^c$. Notes that if $Q \in W$ is outside of $V(P)$, then $PA_Q = A_Q$ and thus radical of $(x_1, \cdots, x_n)A_Q$ is A_Q which implies that $(x_1, \cdots, x_n)A_Q = A_Q$, hence the equation trivially holds. If $Q \in W \cap V(P)$, then $(x_1, \cdots, x_n)A_Q$ has only one prime divisor PA_Q, with the assumption that "regular" system of parameter gives the equation.

In the proof of Theorem 24.5, since y_i is A-sequence, it is also A_Q-sequence, hence that's why the reason A_Q is CM is equivalent to saying that A_Q/IA_Q is CM by Exercise 17.4. Also, if $x_1 \in A$ is A/P-regular but not A-regular, then there exists $b \in A$ such that $x_1 b \in P$, but since P is prime, $b \in P$. Now, b is nonzero in P^i/P^{i+1} for some i, but since P^i/P^{i+1} is free, hence $x_1 b \neq 0$, contradicting the assumption that $x_1 b = 0$. Hence, such b does not exist. Therefore, x_1 is A-regular. Now do the induction to get whose A/P-sequences are indeed A-sequences. The last equality $\dim A_Q/PA_Q = \dim A_Q$ came from the fact that $P^r = 0$.

In the proof of Theorem 24.6, if we take Ext functor on the given exact sequence, we have the long exact sequence as below.

$$0 \to \mathrm{Hom}_A(P/P^i, A) \to \mathrm{Hom}_A(P/P^{i+1}, A) \to \mathrm{Hom}_A(P^i/P^{i+1}, A)$$
$$\to \mathrm{Ext}^1_A(P/P^i, A) \to \mathrm{Ext}^1_A(P/P^{i+1}, A) \to \mathrm{Ext}^1_A(P^i/P^{i+1}, A) = 0 \to \cdots$$

since P^i/P^{i+1} is free A/P module, thus $\mathrm{Ext}^1_A(P^i/P^{i+1}, A)$ is direct sum of $\mathrm{Ext}^1_A(A/P, A)$, which is 0. Then, when $i = 1$, one can get $\mathrm{Ext}^1_A(P/P^2, A) = 0$ from the given information that P/P^2 is free thus projective. If $i = 2$, then one can get $\mathrm{Ext}^1_A(P/P^3, A) = 0$, thus by increasing i to $r-1$, one can get $\mathrm{Ext}^1_A(P/P^r, A) = \mathrm{Ext}^1_A(P, A) = 0$. Now by using

$$0 \to P \to A \to A/P \to 0$$

with $\mathrm{Ext}^1_A(P, A) = 0, \mathrm{Ext}^2_A(A, A) = 0$ (since A is free thus projective) we have $\mathrm{Ext}^2_A(A/P, A) = 0$, and next we can calculate again using above long exact sequence to get $\mathrm{Ext}^2_A(P, A) = 0$, and from this we can get $\mathrm{Ext}^3_A(A/P, A) = 0$, and so on.

1. By theorem 6.3 with the exact sequence $0 \to I^i/I^{i+1} \to A/I^{i+1} \to A/I^i \to 0$, $\mathrm{Ass}(A/I^{i+1}) \subset \mathrm{Ass}(I^i/I^{i+1}) \cup \mathrm{Ass}(A/I^i)$. Now since I^i/I^{i+1} is a free A/I-module, $\mathrm{Ass}(I^i/I^{i+1}) = \mathrm{Ass}(A/I)$. Thus, $\mathrm{Ass}(A/I^{i+1}) \subset \mathrm{Ass}(A/I) \cup \mathrm{Ass}(A/I^i)$. Moreover, $\mathrm{Ass}(A/I^i) \subset \mathrm{Ass}(A/I)$ by an argument using annihilator, hence
$$\mathrm{Ass}(A/I^{i+1}) \subset \mathrm{Ass}(A/I).$$
However, if $P \in \mathrm{Ass}(A/I)$, then $Pa = 0$ for some $a \in A \setminus I$, now take $\bar{b} \in I^i/I^{i+1} \cong (A/I)^l$ such that b corresponds to $a(1, \cdots, 1) \in (A/I)^l$, $P\bar{b} = 0$ means that $Pb \subset I^{i+1}$, hence
$$\mathrm{Ass}(A/I) \subset \mathrm{Ass}(A/I^{i+1}).$$
This implies that $\mathrm{Ass}(A/I) = \mathrm{Ass}(A/I^{i+1})$. Since i war arbitrarily chosen, we knows that $\mathrm{Ass}(A/I) = \mathrm{Ass}(A/I^i)$ for all i. By choosing $i > r$, we can conclude that $\mathrm{Ass}(A/I) = \mathrm{Ass}(A)$.

   If $\underline{x}$ form an A-sequence, then it also form an A/I sequence from the fact that they are not in the union of height zero ideals. If they form an A/I-sequence, then they are not in associate primes of A, too, thus they form A-sequences.

2. By Theorem 5, it is enough to show that for a prime ideal $\mathfrak{p}$ of $A, \mathrm{CM}(A/\mathfrak{p})$ contains a non-empty open. Let P be the inverse image of $\mathfrak{p}$ in R, so that $A/\mathfrak{p} = R/P$. If $x_1, \ldots, x_n \in P$ are chosen to form a system of parameters of R_P then since R_P is CM, they form an R_P -sequence. Thus passing to a smaller neighbourhood of P, we can assume (i) P is the unique minimal prime divisor of $(\underline{x}) = (x_1, \ldots, x_n) R$, and (ii) $\underline{x}$ is an R -sequence. Now replacing R by $R/(\underline{x})$, we can assume that P is nilpotent; moreover, we can take P^i/P^{i+1} to be free R/P -modules. Now by the Exercise 24.1, R-sequences are equivalent to R/P-sequences, hence if R is CM then R/P is CM because their depths are equal.

3. By Theorem 5, it is enough to show that for a prime ideal $\mathfrak{p}$ of $A, \mathrm{Gor}(A/\mathfrak{p})$ contains a non-empty open. Given $A = R/I$ where R is Gorenstein, Let P be the inverse image of $\mathfrak{p}$ in R, so that $A/\mathfrak{p} = R/P$. If $x_1, \ldots, x_n \in P$ are chosen to form a system of parameters of R_P then since R_P is CM, they form an R_P -sequence. Thus passing to a smaller neighbourhood of P, we can assume (i) P is the unique minimal prime divisor of $(\underline{x}) = (x_1, \ldots, x_n) R$, and (ii) $\underline{x}$ is an R -sequence. Now replacing R by $R/(\underline{x})$, we can assume that P is nilpotent; moreover, like Theorem 24.6, we may assume that P is the unique minimal prime ideal of R. The rest is just the same as proof of Theorem 24.6, starting from calculating ext and hom.

25 Derivations

For any $a, b \in A$, $[D, D'](a + b) = D(D'a + D'b) - D'(Da + Db) = DD'a + DD'b - D'Da - D'Db = [D, D']a + [D, D']b$ and

$$\begin{aligned}[D, D']ab &= D(bD'a + aD'b) - D'(bDa + aDb) = bDD'a + D'aDb + D'bDa + aDD'b - bD'Da - DaD'b - DbD'a - aD'Db \\ &= bDD'a + aDD'b - bD'Da - aD'Db = b[D, D']a + a[D, D']b.\end{aligned}$$

In the diagram of p.191, to see $h-h'$ is k-derivation, notes that $(h-h')(a+b) = (h-h')(a)+(h-h')(b)$ is clear, and for any $b \in C, n \in N$, b acts on n as $h(b)n = h'(b)n$. Thus,

$$b \cdot (h-h')(a) + a \cdot (h-h')(b) = h'(b)h(a) - h'(b)h'(a) + h(a)h(b) - h(a)h'(b) = (h-h')(ab).$$

Also, $(h-h') \circ (k \to C) = 0$ is clear.

In p. 191, μ should maps to A, not k, otherwise we cannot explain μ'. Also, in p.191, $A * M = A \times M$ form an A-algebra by defining $(a,b)\cdot(c,d) = (ac, 0)$. This induces $f : I/I^2 \to M$. Also, uniqueness of f is just came from this simple argument; if f' is another linear map, then it also maps da to Da, hence $f = f'$ by linearity.

In p. 193, to see A is 0-unramified over k is equivalent to $\Omega_{A/k} = 0$, compare the diagram of p.193 to that of 191; then if A is 0-ramified, then $\mathrm{Der}_k(A, N) = 0$, otherwise we have another lifting $v+D$ for some nonzero $D \in \mathrm{Der}_k(A, N)$. Now, for any A-module M, let $C = k[M]$, $N = M \subset C$. By 0-unramified condition of A, $\mathrm{Der}_k(A, M) = 0$. Hence, from $\mathrm{Der}_k(A, -) = \mathrm{Hom}_A(\Omega_{A/k}, -)$, we knows that $\mathrm{Hom}_A(\Omega_{A/k}, -) = 0$, thus $\Omega_{A/k} = 0$ since 0 is the universal element of $\mathcal{M}_A$. Conversely, if $\Omega_{A/k} = 0$, then $\mathrm{Der}_k(A, M) = 0$ for all $M \in \mathcal{M}_A$, therefore v is unique.

To see A_S is 0-etale over A, notes that $u(1/s) = c + N$ for some $c \in C$, then c is unit in C by Exercise 1.1. Thus, we may construct v by choosing image of $1/s$ from u. If v and v' are two liftings such that $v(1/s) = c, v'(1/s) = c + n$, then, $D = v' - v$ gives nonzero $D \in \mathrm{Der}_A(A_S, N)$. However, in $A_S \otimes_A A_S$,

$$a/s \otimes 1 - 1 \otimes a/s = a(1/s \otimes 1 - 1 \otimes 1/s) = as(1/s \otimes 1/s - 1/s \otimes 1/s) = 0,$$

whichi implies that $\Omega_{A_S/A} = 0$. Thus, $D = 0$, which implies that there is the unique lifting v.

In the proof of Theorem 25.1, suppose we take $T = N/\operatorname{Im}\alpha$. Then, pick $f \in \mathrm{Hom}_B(N, N/\operatorname{Im}\alpha)$ the canonical injection. Then, $\alpha^*(f) = f \circ \alpha : N' \to N \to N/\operatorname{Im}\alpha = 0$. Thus, $f \in \operatorname{Im}\beta^*$, i.e., $f = g \circ \beta : N \to N'' \to N/\operatorname{Im}\alpha$ for some $g \in \mathrm{Hom}(N'', N/\operatorname{Im}\alpha)$. Thus, $g(N) \subset N'' \to N/\operatorname{Im}\alpha$ is surjective. Hence, if $x \in \ker\beta \setminus \operatorname{Im}\alpha$, then $0 = g \circ \beta(x) = f(x) \neq 0$, contradiction; therefore $\ker\beta = \operatorname{Im}\alpha$. The rest is obvious; if $D \in \mathrm{Der}_A(B, T)$, then definitely it is k-Derivation since $A \supset k$ as a k-algebra, and for $D \in \mathrm{Der}_k(B, T)$, $D \circ g = 0$ in $\mathrm{Der}_k(A, T)$, then D is A-derivation by definition. And this exact sequence of Derivation modules is nothing but taking $\mathrm{Hom}(-, T)$ on the given sequence.

Next, in the proof of Theorem 25.1 when B is 0-smooth over A, then to see $D' \in \mathrm{Der}_k(B, T)$ is derivation, we need to check $D'(bb') = bD'b' + b'D'b$. To see this, we can rotate the diagram as below.

$$\begin{tikzcd} B * T \arrow[r, "/T"] & B \\ & B \arrow[u, "1_B"'] \arrow[ul, "h"] \end{tikzcd}$$

Then, by the argument of p.191, with the fact that $B \to B * T$ by $b \mapsto (b, 0)$ is another lifting map, we can conclude that $D' : B \to T$ is k-derivation of B to T, and $D = D' \circ g$ by construction, and from $\mathrm{Der}_k(B, T) \cong \mathrm{Hom}_B(\Omega_{B/k}, T)$ there exists a corresponding map $\alpha' \in \mathrm{Hom}_B(\Omega_{B/k}, T)$ such that $D' = \alpha' \circ d_{B/k}$. Now, set $T = \Omega_{A/k} \otimes B$ and D as $D(a) = d_{A/k}(a) \otimes 1$. Then,

$$\alpha' \circ \alpha(d_{A/k}(a) \otimes b) = \alpha'(bd_{B/k}(g(a))) = b\alpha'(d_{B/k}(g(a))) = bD'(g(a)) = bD(a) = d_{A/k}(a) \otimes b$$

Hence, $\alpha' \circ \alpha = 1_T$, done.

If $A \to B$ is surjective, then it gives surjective α in (1), thus $\Omega_{B/A} = 0$ by the exact sequence.

In the proof of Theorem 25.2, let $D = f \circ (d_{A/k} \otimes 1)$ for some $f : \Omega_{A/k} \otimes_A B \to T$. Then, if $\delta^*(D) = 0$, then $f \circ \delta = 0$, thus $\ker f \supset d_{A/k}(\mathfrak{m}) \otimes 1$, which implies $D(\mathfrak{m}) = 0$. Also, if B is 0-smooth over k, then

$$\begin{tikzcd} B = A/\mathfrak{m} \arrow[r, "1_B"] & B = A/\mathfrak{m} \\ k, \arrow[u] \arrow[r] & A/\mathfrak{m}^2 \arrow[u, "/\mathfrak{m}"'] \end{tikzcd}$$

gives the map $s : B \to A/\mathfrak{m}^2$ such that $/\mathfrak{m} \circ s = 1_B$, thus make the exact sequence $0 \to \mathfrak{m}/\mathfrak{m}^2 \to A/\mathfrak{m}^2 \to B \to 0$ split. Now, let $D = 1 - sg$. Then, $A \to A/\mathfrak{m}^2 \xrightarrow{D} \mathfrak{m}/\mathfrak{m}^2$ is derivation; to see this, from $gsg = g$, we knows that for any $a \in A$, $sg(a) = a + m_a$ for some $m_a \in \mathfrak{m}$. Hence,

$$D(ab) = ab - ab - m_a b - m_b a = -m_a b - m_b a = bDa + aDb.$$

Thus, $D' : A \to A/\mathfrak{m}^2 \xrightarrow{D} \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\psi} T$ is also derivation in $\mathrm{Der}_k(A, T)$. Now we claim that $\delta^*(D') = \psi$. To see this, notes that we may identify $D' = \alpha \circ d_{A/k}$ where

$$\alpha : \Omega_{A/k} \xrightarrow{-\otimes 1} \Omega_{A/k} \otimes_A B \to T, d_{A/k} : A \to \Omega_{A/k}.$$

Then, for any $\overline{x} \in \mathfrak{m}/\mathfrak{m}^2$

$$\begin{aligned} \delta^*(D')(\overline{x}) = \delta^*(\alpha)(\overline{x}) &= \alpha \circ \delta(x) = \alpha \circ (d_{A/k}x) = D'(x) \\ &= \psi(D(\overline{x})) = \psi(\overline{x} - sg(\overline{x})) = \psi(\overline{x}) \end{aligned}$$

with the fact that $sg(\overline{x}) = 0$ from the fact that g annihilates $\mathfrak{m}/\mathfrak{m}^2$. Hence δ^* is surjective. Now by letting $T = \mathfrak{m}/\mathfrak{m}^2$, there exists $D'' \in \mathrm{Der}_k(A, \mathfrak{m}/\mathfrak{m}^2)$ such that $\delta^*(D'') = 1_{\mathfrak{m}/\mathfrak{m}^2}$. Hence, D'' induces $A/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2$ whose composition with δ is identity on $\mathfrak{m}/\mathfrak{m}^2$, thus (5) splits.

In theorem 25.3, "as is well-known in field theory" means primitive element theorem. Also, $\Omega_{L/K} = 0$ is came from L is 0-unramified over K, whose necessary and sufficient condition is $\Omega_{L/K} = 0$.

In theorem 25.4, subtracting a times our original relation means subtract a times with $D^i = c_{i-1}D^{i-1} + \cdots + c_0$.

1. $$\begin{aligned} [aD, bD'] &= aD(bD') - bD'(aD) = abDD' + aD'(-)D(b) - baD'D - bD(-)D'(a) \\ &= ab[D, D'] + aD(b)D' - bD'(a)D. \end{aligned}$$

2. If $xy = 0$, $0 = D(xy) = yDx + xDy$ implies that $y \in xA$. Now, we claim $y \in \bigcap_n x^n A = \{0\}$. Suppose that $y \in x^n A$, and set $y = x^n z$ then $0 = D\left(x^{n+1}z\right) = (n+1)x^n z + x^{n+1}Dz$, and $y \in x^{n+1}A$

3. This is from Leibniz rule. $D(x_1 x_2 \cdots x_n) = \sum_{j=1}^n D(x_j)x_1 \cdots x_{j-1}x_{j+1} \cdots x_n$ and since $D(x_j)x_1 \in I$, this is inside of I^n.

4. **Claim 35.** *If $0 \to A \to B \to C \to 0$ is split exact sequences of R-modules, then for any module M, $0 \to A \otimes M \to B \otimes M \to C \otimes M \to 0$ is exact.*

   Proof. Since tensor is right exact, we only need to check $A \otimes M \to B \otimes M$ is injective. By split exactness, for given $f : A \to B$ there exists $r : B \to A$ such that $rf = 1_A$ by splitting lemma. Thus, if $a \otimes m \in \ker f \otimes 1$, then

   $$0 = (r \otimes 1)(0) = (r \otimes 1) \circ (f \otimes 1)(a \otimes 1) = rf(a) \otimes 1 = a \otimes 1$$

   implies that $a \otimes 1 = 0$, which shows the injectivity. □

   Now, from p. 191-192s notation, we have

   $$0 \to I \to A \otimes_k A \xrightarrow{u} A \to 0$$

   as a split exact seqeunce, where $u(a \otimes b) = ab$. Thus,

   $$0 \to I \otimes_k k' \to \underbrace{A \otimes_k A \otimes_k k'}_{A' \otimes_k A'} \to \underbrace{A \otimes_k k'}_{A'} \to 0$$

is exact, where $A \otimes_k A \otimes_k k' = A \otimes_k (k' \otimes_{k'} (A \otimes_k k')) = A' \otimes_{k'} A'$. Thus,

$$\Omega_{A'/k'} \cong (I \otimes_k k') / (I \otimes_k k')^2 = (I/I^2) \otimes_k k' = \Omega_{A/k} \otimes_k k'.$$

For A_S, from the fact that A_S is 0 -etale over A and Theorem 25.1, we have

$$0 \to \Omega_{A/k} \otimes A_S \to \Omega_{A_S/k} \to \Omega_{A_S/A} = 0 \to 0.$$

5. Indeed, this is equivalent to Theorem 27.3(i).

26 Separability

In Theorem 26.2, $k^{1/p} = \{x \in \overline{k} : x^p \in k\}$. Hence, it is an extension. Thus, (2) to (1) is just from definition of separable extension.

In p.202, notes that for any $K = k(B)$ with B are transcendence basis of K, $x \otimes 1 - 1 \otimes x \neq 0 \in K \otimes_k K$ when $x \in B$ but zero if $x \in k$. Hence, $\Omega_{K/k}$ is k-vector space over K, thus we have such a derivation D_i stated in p.202.

1. (a) Let $\alpha \in K \cap K'$; then $1, \alpha \in K$ are linearly dependent over K', hence also over k, so $\alpha \in k$.

   (b) Assume that $\alpha_1, \ldots, \alpha_n \in K$ are linearly independent over k', and that $\sum \alpha_i \xi_i = 0$ with $\xi_i \in k'(K')$; we show that $\xi_i = 0$. Clearing denominators, we can assume that $\xi_i \in k'[K']$. Choosing a basis $\{\omega_j\}$ of K' over k we can write $\xi_i = \sum c_{ij}\omega_j$ with $c_{ij} \in k'$. Then since $\sum_{i,j} c_{ij}\alpha_i\omega_j = 0$ we get $\sum_i c_{ij}\alpha_i = 0$ by property (a) of linearly disjointness between K and K', therefore $c_{ij} = 0$ for all i, j by linearly independentness of α_i over k'.

2. If we show that $K((T))$ and $L^p((T^p))$ are linearly disjoint over $K^p((T^p))$, then $L^p((T^p))$ is separable over $K^p((T^p))$ by Theorem 20.4, thus $L((T))$ is separable over $K((T))$ because of definition of separability and freshman's dream; (just take the separable minimal polynomial h over $K^P((T^P))$, then you can always find $g^p = h$ for some g over $K((T))$.) Then, the desired lemma can be derived by an induction.

   Assume that $\omega_1(T), \ldots, \omega_r(T) \in K((T))$ are linearly independent over $K^p((T^p))$, and that $\sum \varphi_i\omega_i = 0$ with $\varphi_i \in L^p((T^p))$; we show that $\varphi_i = 0$ for all i. Clearing denominators, we can assume that $\omega_i \in K[[T]]$ and $\varphi_i \in L^p[[T^p]]$. Letting $\{\xi_\lambda\}$ be a basis of L over K we can in a unique way write $\varphi_i = \sum \xi_\lambda^p \varphi_{i\lambda}(T^p)$ with $\varphi_{i\lambda}(T^p) \in K^p[[T^p]]$. Here $\sum \xi_\lambda^p \varphi_{i\lambda}$ is in general an infinite sum, but only a finite number of terms appear in the sum for the coefficient of some monomial in the T 's, so that the sum is meaningful. Then $\sum_\lambda \xi_\lambda^p (\sum_i \varphi_{i\lambda}(T^p)\omega_i(T)) = 0$, thus for any evaluation of T, the equation gives 0, hence $\sum_i \varphi_{i\lambda}(T^p)\omega_i = 0$ for all λ. Now since ω_i are linearly independent over $K^p((T^p))$, so $\varphi_{i\lambda} = 0$ for all i, λ.

27 Higher Derivation

In the proof of 27.3(i), $D^i(a - x^iD^ia/i!) = D^ia - D^ia - x^iD^{2i}a/i! = 0$. Also, In the proof of 27.3(ii), K is separable over k with Theorem 26.4 (i) gives K and $k^{1/p}$ are linearly disjoint, thus x, ω_i are linearly independent over $k^{1/p}$.

1. This is nothing but checking module structure.

2. Let characteristic to be 3. Then, think $(D_0, 2D_1, D_2)$ which is given from the iterative extension (D_0, D_1, D_2). Then, this is also iterative higher derivation; especially, you can check that $2D_1 \circ 2D_1 = 4D_1 \circ D_1 = D_1 \circ D_1 = 2D_2$. Hence, it is not unique.

28 I-smoothness

In Example 1, (i) is from Theorem 28.1, (ii) is directly came from setting $B = A, A' = \hat{A}$ in Theorem 28.2. Example 2 is just special case of Example 1.

In the proof of Theorem 28.4 (1) to (2), getting λ and v' with derivation was found in the proof of Theorem 25.1. Again, in the proof for (2) to (1), viewing D as an element of $\mathrm{Der}_k(A, N)$ is came from p.191 diagram. Lastly, indeed what we found about derivations are via the map $C = B/I^v$, thus $\mathrm{Der}_k(A, N)$ can be viewed as $\mathrm{Hom}(\Omega_{A/k} \otimes B/I^v, N)$.

In the proof of Lemma 2, p.218, Suppose $\overline{u}$ is the left inverse of $\overline{v}$. Then, $\overline{u}$ is surjective from the direct summand of L/IL, thus projectivity of M induces a map, say t, from M to the direct summand. Also, a map from L to that direct summand via L/IL is also a surjective, thus M induces a map v which lifts t. By result of such lifting we have commutative diagram in p.218.

To see w induces the identity, notes that $\overline{u} : L/IL \to L/\ker u \to M \to M/IM$, where the first and third maps are canonical projection, and second one is induced by first isomorphism theorem, with the fact that $IL \subset \ker u$. Hence, we have commuting diagram

$$\begin{tikzcd}
M \arrow[d, "j"] & L \arrow[l, "u"'] \arrow[d, "i"] \\
M/IM \arrow[r, shift left, "\overline{v}"] & L/IL \arrow[l, shift left, "\overline{u}"]
\end{tikzcd}$$

with the fact that $\overline{v}$ is left inverse of $\overline{u}$.

Now, w induces isomorphism on L/IL means that for any $l \in L$,

$$i(l) = \overline{v}ju(l) = ivu(l) = iw(l).$$

where first equality came from commuting diagram above, and the second equality is came from the commuting diagram in p. 218 over $u(l) \in M$.

In proof of Theorem 28.7, A' is finite module since k' is finite extension. Also, the exact sequence $J/J^2 \xrightarrow{f} \Omega_{A[T_1,\cdots]} \otimes B \to \Omega_B \to 0$ in p.220 (the bottom one) is came from Theorem 25.2, and the map f send $T_i^p - x_i$ to $pd(T^{p-1}) - d(x_i) = -d(x_i)$, that's why kernel is generated by dx_is. Now, even if there is no condition that B is 0-smooth on $A[T_1, \cdots, T_r]$, we already knows that rank of the kernel is r, which implies that the map f is injective, thus dx_is are linearly independent.

In p.221, to verify the necessary and sufficient condition for u to have a lifting, suppose such g exist. Then, v is lifting of u since C/N-part of $v(x) = \overline{x} = u(x)$. Conversely, if v is a lifting, thn we may set $g(x)$ be the N-part of $v(x)$. Then, we may write $v(y) = (\overline{y}, g(y))$, thus from $v(xy) = v(x)v(y)$ by B-homomorphic property of v,

$$0 = (\overline{x}, g(x)) \cdot (\overline{y}, g(y)) - (\overline{xy}, g(xy)) = (0, -f(x, y) + xg(y) + yg(x) - g(xy)).$$

In the proof of Theorem 28.8 (ii), from $f(x, y) := \lambda(xy) - \lambda(x)\lambda(y)$ and $x \cdot \xi = \lambda(x)\xi$, we have

$$\lambda(x)\lambda(yz) - \lambda(x)\lambda(y)\lambda(z) - \lambda(xyz) + \lambda(xy)\lambda(z) + \lambda(xyz) - \lambda(x)\lambda(yz) - \lambda(xy)\lambda(z) + \lambda(x)\lambda(y)\lambda(z) = 0$$

Lastly, notes that $g(x)g(y) = 0$ in the last equation of the proof.

1. Let N be a B -module satisfying $m^v N = 0$, and $D : B \longrightarrow N$ a derivation over A; then D induces a derivation $\bar{D} : B_0 = B/\mathfrak{m}B \longrightarrow N/\mathfrak{m}N$. Since B_0 is 0-unramified over k, $\bar{D} = 0$, so that $D(B) \subset \mathfrak{m}N$. Now do the same thing for $D : B \longrightarrow \mathfrak{m}N$, D induces a derivation $\bar{D} : B_0 = B/\mathfrak{m}B \longrightarrow \mathfrak{m}N/\mathfrak{m}^2N$ we can conclude that $D(B) \subset \mathfrak{m}^2N$. Repeat this v times so that $D = 0$. The statement about etale is just putting together those for smooth and unramified.

2. Pick $(a^{1/p} \otimes 1) - (1 \otimes a^{1/p}) \in k(a^{1/p}) \otimes_k k^{1/p}$. Then, $((a^{1/p} \otimes 1) - (1 \otimes a^{1/p}))^p = a \otimes 1 - 1 \otimes a = 0$. Hence, $k(a^{1/p}) \otimes_k k^{1/p}$ is non-reduced. Thus by Theorem 26.2 (2), $k(a^{1/p})$ is inseparable over k.

   To see next statement, since k is non-perfect field of positive characteristic, k is not finite, thus we may assume a cannot be represented by the sum of 1s. Therefore, a is came from a transcendence extension of $\mathbb{F}_p$, thus we may have $D \in \mathrm{Der}(k,k)$ such that $D(a) \neq 0$. Since this can be extended to a derivation of $A = k[X]_{(X^p - a)}$, thus if $a \in A^p$, then $a = f^p$ for some $f \in A$, thus $Df^p = 0$, contradiction. Hence $a \notin A^p$. If k' were a coefficient field containing k then we would have to have $a \in (k')^p \subset A^p$.

Also, A is 0-smooth over k because $k[X]$ is. Notes that

$$\begin{array}{ccc} k[X] & \xrightarrow{u} & C/N \\ \uparrow & & \uparrow \\ k & \longrightarrow & C \end{array}$$

from this diagram, any preimage of $u(X)$ on C determines map $k[X] \to C$, and such maps always commute with other maps.

29 The structure theorem for complete local rings

In the proof of Theorem 29.1, A_1 is DVR since tA' is of height 1. In p.224, there is typo; since B' is integral over B, every maximal ideal of B' contains tB (not tB').

In the proof of Theorem 29.2, k is separable extension of k_0 since k_0 is the prime subfield, hence perfect.

In the proof of Theorem 29.8, let $f(X)$ be the minimal polynomial of x_1 over A_0. By the textbook, $a_n \in \mathfrak{m}_0$. Thus, over $K = A_0/\mathfrak{m}_0$, f is reducible in $K[X]$, hence Hensel lemma assure that there exist $g(X), h(X) \in A_0[X]$ such that $gh = f$. However, since $g(x_1)h(x_1) \in \mathfrak{m}$, thus we may assume that $g(x_1) \in \mathfrak{m}$, thus the constant term of $g(X)$ is in $\mathfrak{m}_0$, then applying Hensel lemma again on $g(X) - X^{\deg g} - c$ where c is the constant term of $g(X)$, we may also assume that the coefficient of X in $g(X)$ is in $\mathfrak{m}_0$. By applying this argument repeatedly, we may assume that all coefficients of f is in $\mathfrak{m}_0$.

1. By Theorem 29.7 complete p-ring is regular local ring, thus Theorem 29.8 implies that its Eisenstein extension is also regular local ring. Dimension 2 is also clear from $0 \subset (p) \subset (p, x)$. Suppose that $C = R[[t]]$ with R a DVR; if we let u be a uniformising element of R then pR is a power of uR, so that pC has the single prime divisor uC. However, in fact, in our case $C/pC = (B/pB)[X]/(x(x+y))$, so that pC has the two prime divisors (p, x) and $(p, x+y)$.

2. When k is perfect, then Exercise 28.1 says that R is pR -etale over $\mathbb{Z}_{p\mathbb{Z}}$ (see Ex. 28.1).

30 Connections with derivations

In the proof of Theorem 30.1, $D_i' x_j = \delta_{ij}$ is clear if we think their matrix forms as $(D_i x_j) = (x_i)^t (D_i)$.

In Lemma 1 of p.233, I don't know why $\sum_{\mathfrak{p}} t_{\mathfrak{p}} A = A$ since as an ideal it is not contained in any of maximal ideal of A.

Honestly, I did not go over after Theorem 3.

References

[1] Hideyuki Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989. Translated from the Japanese by M. Reid. MR1011461

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802

[3] Nicolas Bourbaki, *Elements of mathematics. Commutative algebra*, Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972. Translated from the French. MR0360549

[4] Winfried and Herzog Bruns Jürgen, *Cohen-Macaulay rings*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, Cambridge, 1993.

[5] Christer Lech, *On the associativity formula for multiplicities*, Ark. Mat. **3** (1957), 301–314, DOI 10.1007/BF02589424. MR85245

[6] Manfred Herrmann and Ulrich Orbanz, *Two notes on flatness*, Manuscripta Math. **40** (1982), no. 1, 109–133, DOI 10.1007/BF01168239. MR679124

[7] Pete L. Clark, *Covering numbers in linear algebra*, preprint (2012).

[8] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR1269324

[9] Irving Kaplansky, *Commutative rings*, Revised edition, The University of Chicago Press, Chicago, Ill.-London, 1974. MR0345945

[10] Joseph J. Rotman, *An introduction to homological algebra*, 2nd ed., Universitext, Springer, New York, 2009. MR2455920