MA5204 Homework 3

Nguyen Ngoc Khanh - A0275047B

May 20, 2025

Problem 1 (chapter 8 problem 2)

Let A be a Noetherian ring. Prove that the following are equivalent

1. A is Artinian
2. $\operatorname{Spec} A$ is discrete and finite
3. $\operatorname{Spec} A$ is discrete

Proof.

$(1 \implies 2)$ A is Artinian then every prime ideal is maximal and it has finitely many maximal ideals, so $\operatorname{Spec} A$ is finite. Moreover, every maximal ideal in $\operatorname{Spec} A$ is closed, so any subset of $\operatorname{Spec} A$ is finite hence closed. $\operatorname{Spec} A$ admits the discrete topology

$(2 \implies 3)$ by definition

$(3 \implies 1)$ Suppose $\mathfrak{p} \subsetneq \mathfrak{m}$ be a prime ideal that is properly contained in a maximal ideal $\mathfrak{m}$ in A. As $\operatorname{Spec} A$ is discrete, $\{\mathfrak{p}\}$ is closed, hence $\{\mathfrak{p}\} = V(\mathfrak{a})$ for some ideal in A, hence $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$, so $\mathfrak{m} \in V(\mathfrak{a})$, contradiction. So every prime ideal in A is maximal, $\dim(A) = 0$. Since A is Noetherian, A is also Artinian $\square$

Problem 2 (chapter 8 problem 3)

Let k be a field and A be a finite-type k-algebra. Prove that the following are equivalent

1. A is Artinian
2. A is a finite k-algebra (finitely generated as k-module)

Proof.

$(2 \implies 1)$ If A is a finite k-algebra then A is a k-vector space of finite dimension. Any ideal in A is a vector subspaces. Since A is of finite dimension, any decending chain stablizes. A is Artinian

$(1 \implies 2)$ A is Artinian, then $A \cong \prod_{i=1}^m A_i$ for some Artinian local ring A_i. A is finite-type k-algebra, then there exists a surjection $k[x_1, ..., x_n] \twoheadrightarrow A$. Hence, each A_i is also finite-type k-algebra by the composition $k[x_1, ..., x_n] \twoheadrightarrow A \twoheadrightarrow A_i$. Note that each A_i is Artinian, moreover if each A_i is a finite k-algebra then A is also a finite k-algebra by taking all generators in $\{A_i\}$.

Without loss of generality, assume $(A, \mathfrak{m})$ is Artinian local. Let $K = A/\mathfrak{m}$ be the residue field, again $k[x_1, ..., x_n] \twoheadrightarrow A \twoheadrightarrow K$, so K is finite-type k-algebra. Since A is Artinian, $l_A(A) = n$ finite, there exists a finite chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq ... \subsetneq M_n = A$$

so that each $M_i/M_{i-1} = A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of A. Since A is local, each $M_i/M_{i-1} = K$. Moreover,

$$A \cong \bigoplus_{i=1}^n M_i/M_{i-1}$$

Hence, A is finite K-algebra. Together with Nullstellensatz, K a finite algebraic extension of k. So A is a finite k-algebra. $\square$

Problem 3 (chapter 9 problem 2)

Let A be a Dedekind domain. If $f = a_0 + a_1x + ... + a_nx^n$ is a polynomial with coefficients in A, the content of f is the ideal $c(f) = (a_0, ..., a_n)$ in A. Prove Gauss's lemma that $c(fg) = c(f)c(g)$

Lemma 4 (being equal submodules is local)

Let M and N be submodule of an A-module, if $M_{\mathfrak{m}} = N_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of A then $M = N$.

Proof of Lemma 4. Note that, $M \subseteq N$ if and only if $(M+N)/N = 0$. Localize at every maximal ideal $\mathfrak{m}$, $M_{\mathfrak{m}} \subseteq N_{\mathfrak{m}}$ implies $((M+N)/N)_{\mathfrak{m}} = (M_{\mathfrak{m}} + N_{\mathfrak{m}})/N_{\mathfrak{m}} = 0$ (localization commutes with sum and quotient of submodules). Since being zero is local, so $M \subseteq N$. The other direction is the same. □

Proof. Let $g = b_0 + b_1 x + \ldots + b_m x^m$, then

$$fg = \sum_{l=0}^{m+n} \left(\sum_{i=0}^{l} a_i b_{l-i} \right) x^l$$

Localize at every maximal ideal $\mathfrak{m}$ of A, if we can show that

$$c(fg)A_{\mathfrak{m}} = c(f)A_{\mathfrak{m}} \cdot c(g)A_{\mathfrak{m}} = c(f)c(g)A_{\mathfrak{m}}$$

Then Lemma 4 implies $c(fg) = c(f)c(g)$. Note that, each $A_{\mathfrak{m}}$ is a DVR.

Without loss of generality, assume (A, v) is a DVR with uniformizer $y \in A$, $v(y) = 1$. Let $c(f) = (y^s)$ and $c(g) = (y^t)$ for some $s, t \geq 1$, then $c(f)c(g) = (y^{s+t})$. Since $(y^s) = (a_0, \ldots, a_n)$, then y^s is a A-linear combination of $\{a_0, a_1, \ldots, a_n\}$, then $s = v(y^s) \geq v(a_0)$, but $a_0 \in (y^s)$, so $v(a_0) \geq s$. Hence, $v(a_0) = s$. Similarly, $v(b_0) = t$. Hence, one of the coefficient of $c(fg)$ is $a_0 b_0$ has valuation $v(a_0 b_0) = s + t$, so $c(f)c(g) = (y^{s+t}) \subseteq c(fg)$. The other direction is shown above. Hence $c(f)c(g) = (y^{s+t}) = c(fg)$ □

Problem 5 (chapter 9 problem 3)

A valuation ring (other than a field) is Noetherian if and only if it is a discrete valuation ring.

Definition 6

A domain A is a valuation ring if every nonzero $x \in K = \mathrm{Frac}(A)$, it is either $x \in A$ or $x^{-1} \in A$

Lemma 7 (some facts about valuation ring)

If A is a valuation ring

1. there is a total ordering in A by divisibility
2. there is a total ordering of ideals in A by inclustion
3. A is local
4. every finitely generated ideal is principal
5. every ideal $\mathfrak{a}$ in A, if $\mathfrak{a} \subsetneq \mathfrak{m}^k$ then $\mathfrak{a} \subseteq \mathfrak{m}^{k+1}$ for any $k \geq 1$
6. (*is this true?*) every (prime) ideal in A is of the form $\mathfrak{m}^n$

Proof of Lemma 7.

(1) For any nonzero $x, y \in A$, either $x/y \in A$ or $y/x \in A$. If $x/y \in A$, let $z/1 = x/y$ for $z \in A$. So $t(zy - x) = 0$ for some nonzero $t \in A$. Since A is a domain, $x = zy$. So either x divides y or y divides x

(2) Let $\mathfrak{a}, \mathfrak{b}$ be ideals in A. Suppose there exist $x \in \mathfrak{a} - \mathfrak{b}$ and $y \in \mathfrak{b} - \mathfrak{a}$ ($\mathfrak{a} - \mathfrak{b}$ is set elements in $\mathfrak{a}$ and not in $\mathfrak{b}$). (1) induces a contradiction.
(3) If A is not local, then two distinct maximal ideals $\mathfrak{m}, \mathfrak{n}$ must have $\mathfrak{m} \subsetneq \mathfrak{n}$ or $\mathfrak{n} \subsetneq \mathfrak{m}$. contradiction.
(4) Let $\mathfrak{a} = (a_1, ..., a_n)$ be ideal in A, then there exists a generator a_i that divides every other generator, hence $\mathfrak{a} = (a_i)$
(5) Let $\mathfrak{a} \subsetneq \mathfrak{m}^k$ be any ideal in A for some $k \geq 1$, let $x \in \mathfrak{a}$ and $y \in \mathfrak{m}^k - \{a\}$. Since A is a valuation ring and $y \notin \mathfrak{a}$, $x = ay$ for some $a \in A$. Moreover, if $a \notin \mathfrak{m}$, that is a is a unit, then $a^{-1}x = y$ contradicts with $y \notin A$. Hence, $x = ay$ for some $x \in \mathfrak{m}$. So, $x \in \mathfrak{m}^{k+1}$, $\mathfrak{a} \subseteq \mathfrak{m}^{k+1}$
(6) □

Main Proof.
($\Longleftarrow$) DVR is PID, PID is Noetherian since every ideal is generated by finitely many elements.
($\Longrightarrow$) The valuation ring A is Noetherian, then it is local with the unique maximal ideal $\mathfrak{m}$. Since every ideal in A is finitely generated, it is also principal, that is A is PID. A is a Noetherian, local domain with the unique maximal ideal being principal,it suffices to prove that dimension of A is 1, that is, every prime ideal is maximal.
Let $\mathfrak{m} = (y)$ and (x) be a nonzero prime ideal in A, suppose that $(x) \subsetneq (y)$, that means $y \notin (x)$. We must have $x = ay$ for some $a \in \mathfrak{m}$ (using the argument in Lemma 7). Since (x) is prime, and $y \notin (x)$, $a \in (x)$, write $a = bx$ for some nonzero $b \in A$. So

$$x = byx$$

Since A is a domain, using left cancellation, $by = 1$ that makes y a unit, contradiction. □

Problem 8 (chapter 9 problem 5)
Let M be a finitely generated module over a Dedekind domain. Prove that M is flat $\iff$ M is torsion-free

Definition 9
Let M be a module over a domain A, M is torsion-free if for every nonzero $x \in M$ and nonzero $a \in A$, $ax \neq 0$

Lemma 10 (chapter 3 exercise 13)
Let M be a module over a domain A, then M being torsion-free is a local property.

Lemma 11 (chapter 7 exercise 16)
Let M be a finitely generated module over a Noetherian ring A, then M is flat if and only if $M_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$-module for every maximal ideal $\mathfrak{m}$

Lemma 12
free module of finite rank over a domain is torsion free

Proof of Lemma 12. Let $M = A^n$, then every nonzero $m \in M$ can be written as $m = (a_1, ..., a_n) \in A^n$ for some $a_1, ..., a_n \in A$ and some $a_i \neq 0$. If nonzero $r \in A$ such that $0 = rm = (ra_1, ...ra_n)$, then $ra_i = 0$, contradicts the premise A being a domain. □

Lemma 13 (Fundamental Theorem, Existence: Invariant Factor Form - Dummit Foote - chapter 12, section 12.1, theorem 5)
Let A be a PID, and M be a finitely generated A-module, then M is torsion-free implies M is free.

Proof. TODO □

Main Proof.
Localize at a maximal ideal $\mathfrak{m} \subseteq A$
($\Longrightarrow$) A is Dedekind domain, so A is Noetherian. Since M is finitely generated and flat, $M_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module of finite rank. By Lemma 12, $M_\mathfrak{m}$ is torsion-free. Lemma 10 implies M is torsion-free.
($\Longleftarrow$) A is a domain, so $M_\mathfrak{m}$ is also torsion-free as $A_\mathfrak{m}$-module. Moreover, A is Dedekind domain, then $A_\mathfrak{m}$ is a DVR which is PID. By Lemma 13, $M_\mathfrak{m}$ is free. By Lemma 11

□

Problem 14 (chapter 9 problem 7)
Let A be a Dedekind domain and nonzero ideal $\mathfrak{a}$ in A. Show that every ideal in $A/\mathfrak{a}$ is principal. Deduce that every ideal in A can be generated by at most two elements

Proof. Every ideal $\mathfrak{a}$ in Dedekind domain admits a unique decomposition

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_n^{e_n}$$

for some prime ideals $\mathfrak{p}_i$. In dimension 1 domain A, every prime ideal is maximal, by chinese remainder theorem

$$A/\mathfrak{a} = A/\mathfrak{p}_1^{e_1} \times ... \times A/\mathfrak{p}_n^{e_n}$$

Every ideal in $A/\mathfrak{a}$ is a Cartesian product of ideals in $A/\mathfrak{p}_i^{e_i}$, so it suffices to show that ideals in $A/\mathfrak{p}_i^{e_i}$ are principal. Let $\mathfrak{p}^e$ be one of $\mathfrak{p}_1^{e_1}, ..., \mathfrak{p}_n^{e_n}$. Localize each $A/\mathfrak{p}^e$ as quotient of A-modules at $\mathfrak{p} \subseteq A$, we have

$$(A/\mathfrak{p}^e)_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}^e A_\mathfrak{p}$$

as $A_\mathfrak{p}$ modules. Since A is a Dedekind domain, $A_\mathfrak{p}$ is a DVR. In $A_\mathfrak{p}$, $\mathfrak{p}A_\mathfrak{p}$ is the unique maximal ideal that is principal. So the the unique maximal ideal $\mathfrak{p}A_\mathfrak{p} \cap A_\mathfrak{p}/\mathfrak{p}^e A_\mathfrak{p} \subseteq A_\mathfrak{p}/\mathfrak{p}^e A_\mathfrak{p}$ is principal. It remains to show that $A_\mathfrak{p}/\mathfrak{p}^e A_\mathfrak{p}$ is Artinian. It is straightforward since every ideal in DVR $A_\mathfrak{p}$ is a power of its maximal ideal $\mathfrak{p}A_\mathfrak{p}$, any chain of ideals in $A_\mathfrak{p}$ of the form

$$\mathfrak{p}A_\mathfrak{p} \supsetneq ... \supsetneq \mathfrak{p}^e A_\mathfrak{p}$$

is of length at most e. So any chain of ideals in $A_\mathfrak{p}/\mathfrak{p}^e A_\mathfrak{p}$ is of length at most e
Let $\mathfrak{b} \subseteq A$ be an ideal generated by more than one element. Let $a \in \mathfrak{b}$, then $(a) \subsetneq \mathfrak{b}$. So $\mathfrak{b}/(a)$ is a nonzero ideal in $A/(a)$, hence must be principal. Let $\mathfrak{b}/(a)$ generated by $\bar{b}$ for some $b \in \mathfrak{b}$. Then for any $x \in \mathfrak{b}$, $\mathfrak{b}/(a)$ is principal ideal generated by $\bar{b}$, so $\bar{x} = \bar{y}\bar{b}$ for some $y \in A$, so $x = yb + za$ for some $z \in A$. Hence, $\mathfrak{b} = (a, b)$ □

Problem 15 (chapter 9 problem 8)
Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be three ideals in a Dedekind domain. Prove that

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c})$$

Proof. Localization commutes with finite intersection and sum of submodules, it suffices to prove for the case of DVR. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be ideals of a DVR (A, v) with uniformizer (y). Let $\mathfrak{a} = (y^a), \mathfrak{b} = (y^b), \mathfrak{c} = (y^c)$, then either case $b = c$ or $b \neq c$,

$$\mathfrak{b} + \mathfrak{c} = (y^b) + (y^c) = (y^{\min(b,c)})$$
$$\mathfrak{b} \cap \mathfrak{c} = (y^b) \cap (y^c) = (y^{\max(b,c)})$$

It is equivalent to show

$$\max(a, \min(b, c)) = \min(\max(a, b), \max(a, c))$$
$$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$$

Assuming $b \leq c$, then $\max(a, b) \leq \max(a, c)$ and $\min(a, b) \leq \min(a, c)$. We're done. □

Problem 16 (Krull–Akizuki)
Let A be a Dedekind domain with fractional field K. Let L/K be a finite degree field extension and let B be the integral closure of A in L. Prove that B is a Dedekind domain.

Lemma 17 (equivalent formulation for Dedekind domain)
A ring A is a Dedekind domain if and only if it is a dimension 1 Noeatherian integrally closed domain

Proof of Lemma 17. this follows from Proposition 5.13: for a domain A being integrally closed is local. □

Main Proof. L is a finite degree field extension of K which is a vector of finite dimension over K. $B \subseteq L$ is the integral closure of the ring extension $A \hookrightarrow L$

$$A \hookrightarrow B \hookrightarrow L$$

1. (Any ideal I of B intersects A nontrivially) Let nonzero $I \subseteq B$ be an ideal of B, let nonzero $x \in I$, then x satisfies a monic polynomial of minimal degree

$$p(x) = x^n + a_1 x^{n-1} + ... a_{n-1} x - a_n = 0$$

   for some $a_1, ..., a_n \in A$. Since p is of minimal degree, $a = a_n$ is a nonzero element of the ideal $I \cap A$.

2. (I/aB is of finite length as an A-module) Now, $I/aB \subseteq B/aB$ as R-modules. It suffices to show that length B/aB is of finite length. If $aB = B = I$, there is nothing to show. Suppose a is not a unit in B

   If we can show that $a^n B \subseteq a^{n+1} B + A$ for some n, then

$$\frac{B}{aB} \cong \frac{a^n B}{a^{n+1} B} \subseteq \frac{a^{n+1} B + A}{a^{n+1} B} \cong \frac{A}{a^{n+1} B \cap A}$$

   The left isomorphism is from first isomorphism theorem of the map $a^n(-) : B \to a^n B / a^{n+1} B$ with $\ker a^n(-) = aB$ and the right isomorphism is the second isomorphism theorem for submodules over A. $A/(a^{n+1} B \cap A)$ is Artinian since $a^{n+1} B \cap A$ is nonzero, so B/aB is of finite length as an A-module, hence I/aB is of finite length

3. ($a^n B \subseteq a^{n+1} B + A$ for some n) Using the argument in Lemma 4, inclusion of submodules is a local, We can assume that A is a DVR with uniformizer $\mathfrak{m}$.

For any nonzero $y \in B$, consider the "fractional ideal" $y^{-1}A = \{z \in L : zy \in A\} \subseteq L$ intersecting A nontrivially using the same argument as above for integral element y^{-1} over A. Since A is a DVR, the ideal $Ay^{-1} \cap A$ of A contains large power of $\mathfrak{m}$. Since $a \in \mathfrak{m}$, we choose smallest $N_1 \in \mathbb{N}$ so that $a^n y \in A$ for every $n \geq N_1$

Consider the chain of ideals $I_n = a^n B \cap A + aA$ in A/aA. A/aA is Artinian since aA is nonzero, so it must stablize. Let $N_2 \in \mathbb{N}$ so that $I_n = I_{N_2}$ for every $n \geq N_2$.

Note that, N_1 is dependent on y and N_2 is indepdent of y. We claim that $N_1 \leq N_2 + 1$ for every $y \in B$. Suppose the contrary that if $N_2 + 1 < N_1$, let $n = N_1 - 1$, then $I_{n+1} = I_n = I_{n-1}$, then $a^n y \notin A$ and $a^{n+1} y \in A$. Since $a^{n+1} y \in I_{n+1} = I_n = I_{n-1}$, then there exists $z \in B$ and $t \in A$ so that $a^{n-1} z \in A$ and

$$a^{n+1} y = a^n z + at \in a^{n-1} B \cap A + aA$$

Hence, left cancellation implies $a^n y = a^{n-1} z + t \in A$, contradiction. Choose $n = N_2 + 1$, then $I_n = I_{n+1}$ and $a^n B \subseteq A$. Hence

$$a^n B \subseteq I_n = I_{n+1} \subseteq a^{n+1} B + A$$

4. (B is Noetherian) I/aB is of finite length as an A-module, if I is not finitely generated as an ideal in B, then let $I = (a, i_1, i_2, ...)$ for $i_1, i_2, ... \in B$, so the decending chain of ideals containing aB in B which is also a decending chain of submodule of I/aB as an A-module

$$(a, i_1, i_2, i_3, ...) \supseteq (a, i_2, i_3, ...) \supseteq ... \supseteq (a) \supseteq (0)$$

has infinitely many strict inclusions, contradiction.

5. (B is of dimension 1) $A \hookrightarrow B$ is an integral ring extension with A being a domain, by going-down theorem, any chain of prime ideals of strict inclusions in B has a corresponding chain of prime ideals of strict inclusions in A by contraction. Since A is of dimension 1, by going-up theorem, all chain of prime ideals of strict inclusions in B cannot be longer than 2. Hence, since B is subring of field L, B is domain, (0) is prime, B is of dimension 1

6. (B is integrally closed) $\mathrm{Frac}(B) \subseteq L$. Any $x \in \mathrm{Frac}(B)$ is integral over B is also integral over A, so $x \in B$. Hence, B is integrally closed.

$\square$

Problem 18 (optional)
In the notation of the previous problem, if in addition L/K is a separable extension, we can always write $L = K(x)$ for some $x \in L$. Find an example where L/K is separable but we CANNOT write $B = A[x]$ for some $x \in B$

Problem 19 (optional)
Is the ring $A = \mathbb{C}[x, y]/(y^2 - x^3 - x - 1)$ a PID?