Peizé Liu
St. Peter's College
University of Oxford

Problem Sheet 4

B2.2: Commutative Algebra

Overall: α

April 19, 2020

Question 1 α

Re-prove the "Weak Nullstellensatz", Theorem 4.4:

if E is a finitely generated F-algebra where $E \supseteq F$ are fields, then $[E : F]$ is finite

from the "Noether Normalization Lemma", Theorem 8.8.

Proof. By Noether Normalization Lemma, there exists $\{y_1, ..., y_r\} \subseteq E$ that is algebraically independent over F, such that F is a finitely generated $F[y_1, ..., y_r]$-module. In particular E is integral over $F[y_1, ..., y_r]$ by Proposition 7.4. Since E is a field, $F[y_1, ..., y_r]$ is also a field by Proposition 7.7(a). This is possible only if $r = 0$, which means $F = F[y_1, ..., y_r]$. Hence E is a finitely generated F-module and $[E : F] < \infty$. □

Question 2 β+

(i) Let F be an infinite field. Deduce from Sheet 3 Question 4(i) that $J(F[t_1, .., t_k])$ is zero.

(ii) Show that if $R \subseteq S$ is an integral extension then $J(S) \cap R = J(R)$. Deduce that if, in addition, S is an integral domain, then $J(S) = \{0\}$ if and only if $J(R) = \{0\}$.

(iii) Now let F be an arbitrary field. Using the Noether Normalization Lemma, deduce that every finitely generated F-algebra is a Jacobson ring.

Proof. (i) For each $t_i \in \{t_1, ..., t_k\}$ and $a \in F$, $\langle t_i - a \rangle$ is a maximal ideal of $F[t_1, ..., t_k]$. For $f \in J(F[t_1, ..., t_k])$, $f \in \langle t_i - a \rangle$. In particular f vanishes on all $(x_1, ..., x_k) \in F^k$. Since F is infinite, by Sheet 3 Question 4(i), $f = 0$. Hence $J(F[t_1, ..., t_k]) = \{0\}$.

This is not true.

(ii) By Going-up Theorem there is a bijective correspondence between $\operatorname{Spec} R$ and $\operatorname{Spec} S$ which is given by ideal extensions and contractions. By Proposition 7.7(c), this restricts to a bijective correspondence between $\operatorname{MaxSpec} R$ and $\operatorname{MaxSpec} S$. We have:

$$J(S) \cap R = \bigcap_{M \in \operatorname{MaxSpec} S} M \cap R = \bigcap_{\substack{P = M \cap R \\ M \in \operatorname{MaxSpec} S}} P = \bigcap_{P \in \operatorname{MaxSpec} R} P = J(R)$$

Now suppose that S ia an integral domain. That $J(S) = 0$ implies $J(R) = 0$ is trivial. For the other direction, since S is an integral domain. By Proposition 7.6, if $J(S) \neq \{0\}$, then $J(R) = J(S) \cap R \neq \{0\}$.

(iii) Suppose that A is a finitely generated F-algebra. For $P \in \operatorname{Spec} A$, A/P is an integral domain and is a finitely generated F-algebra. By Noether Normalization Lemma, there exists $\{y_1, ..., y_r\} \subseteq A/P$ algebraically independent over F such that A/P is a finitely generated $F[y_1, ..., y_r]$-module. In particular A/P is integral over $F[y_1, ..., y_r]$. Since $\{y_1, ..., y_r\}$ is algebraically independent, $F[y_1, ..., y_r] \cong F[t_1, ..., t_r]$ as F-algebras. Hence $J(F[y_1, ..., y_r]) = \{0\}$ by part (i). It follows from part (ii) that $J(A/P) = \{0\}$. It implies that P is the intersection of all maximal ideals of A that contain P. We conclude that A is a Jacobson ring. □

Question 3 α

(i) Prove that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra.

(ii) Let F be a field which is finitely generated as a $\mathbb{Z}$-algebra. Prove that $\operatorname{char} F \neq 0$.

Hint: Suppose that F has characteristic zero. Consider the three rings $\mathbb{Z} \subseteq \mathbb{Q} \subseteq F$.

(iii) Let S be a finitely generated $\mathbb{Z}$-algebra and M a maximal ideal of S. Prove that $|S/M| < \infty$.

Proof. (i) Note that the polynomial rings over $\mathbb{Z}$ are free objects in the category $\mathbb{Z}$-Alg. Suppose that $\mathbb{Q}$ is a finitely generated $\mathbb{Z}$-algebra. Then there exists an epimorphism $\varphi : \mathbb{Z}[t_1, ..., t_n] \twoheadrightarrow \mathbb{Q}$. Let $p_i/q_i = \varphi(t_i) \in \mathbb{Q}$ for each i, where

$\gcd(p_i, q_i) = 1$. It is not hard to verify that for any $f \in \mathbb{Z}[t_1, ..., t_n]$, the denominator of $\varphi(f)$ divides $q_1, ..., q_n$. Hence $\dfrac{1}{q_1 \cdots q_n + 1} \notin \operatorname{im}\varphi$, which is a contradiction. $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra.

(ii) Suppose that $\operatorname{char} F = 0$. From Part A Rings & Modules we know that F contains $\mathbb{Q}$ as a subfield. If F is a finitely generated $\mathbb{Z}$-algebra, then $\mathbb{Q}$ is also a finitly generated $\mathbb{Z}$-algebra. This is a contradiction as we have proven in part (i). here you use Artin-Tate.

(iii) Note that S/M is a field and is finitely generated as a $\mathbb{Z}$-algebra. We have shown in part (ii) that $\operatorname{char} F \neq 0$. Let $\mathbb{F}_p$ be the prime subfield of S/M. Then S/M is finitely generated as an $\mathbb{F}_p$-algebra. By Hilbert's Weak Nullstellensatz, $[S/M : \mathbb{F}_p]$ is finite. Hence $|S/M| = p[S/M : \mathbb{F}_p] < \infty$. □

Question 4 α

Let R be a subring of a field E and Y a multiplicatively closed subset of R with $1 \in Y$ and $0 \notin Y$. Let S be the integral closure of R in E. Prove that the integral closure of $Y^{-1}R$ in E is $Y^{-1}S$.

Proof. Step 1: *$Y^{-1}S$ is integral over $Y^{-1}R$.*

For $s/y \in Y^{-1}S$, since S is integral over R, there exists $r_0, ..., r_{n-1} \in R$ such that $s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0$. Multiplying by $1/y^n$:

$$\left(\frac{s}{y}\right)^n + \frac{r_{n-1}}{y} \cdot \left(\frac{s}{y}\right)^{n-1} + \cdots + \frac{r_1}{y^{n-1}} \cdot \frac{s}{y} + \frac{r_0}{y^n} = 0$$

This is a monic polynomial in $Y^{-1}R[t]$ that annihilates s/y. Hence s/y is integral over $Y^{-1}R$. $Y^{-1}S$ is integral over $Y^{-1}R$.

Step 2: *$Y^{-1}S$ is the integral closure of $Y^{-1}R$ in E.*

Suppose that $u \in E$ is integral over $Y^{-1}R$. We shall show that $u \in Y^{-1}S$. There exists $r_0, ..., r_m \in R$ and $y_0, ..., y_m \in Y$ such that

$$u^m + \frac{r_{m-1}}{y_{m-1}}u^{m-1} + \cdots + \frac{r_1}{y_1}u + \frac{r_0}{y_0} = 0$$

Multiplying by $y^m := y_0^m \cdots y_{m-1}^m$:

$$(yu)^m + \frac{r_{m-1}y}{y_{m-1}}(yu)^{m-1} + \cdots + \frac{r_1 y^{m-1}}{y_1}yu + \frac{r_0 y^m}{y_0} = 0$$

where $\dfrac{r_{m-1}y}{y_{m-1}}, ..., \dfrac{r_1 y^{m-1}}{y_1}, \dfrac{r_0 y^m}{y_0} \in R$. Hence yu is integral over R. As S is the integral closure of R, we have $yu \in S$. Hence $u = yu/y \in Y^{-1}S$. We conclude that $Y^{-1}S$ is the integral closure of $Y^{-1}R$ in E. □

Remark. This is Proposition 5.12 in *Atiyah & MacDonald.* THE BEST BOOK

Question 5 α

Let R be an integrally closed domain with field of fractions F, let $E \supseteq F$ be an algebraic field extension and let $a \in E$. Show a is integral over R if and only if the (monic) minimal polynomial of a over F lies in $R[t]$.

Hint: consider a suitable splitting field.

Does this necessarily hold if R is not integrally closed?

Proof. If the monic minimal polynomial of a over F lies in $R[t]$, then a is integral over R by definition. For the other direction, suppose that a is integral over R. Let $m_a \in F[t]$ be the minimal polynomial of a over F. Let K be the splitting field of m_a over F. We can express m_a as:

$$m_a(t) = (t - a_1) \cdots (t - a_n) \in K[t]$$

for some $a_1, ..., a_n \in K$. Since a is integral over R, there exists a monic polynomial $f \in R[t]$ such that $f(a) = 0$. By minimality of m_a we have $m_a \mid f$ over $F[t]$. Then $m_a(a_i) = 0$ implies that $f(a_i) = 0$ for each i. In particular $a_1, ..., a_n$ are all integral over R. Since $m_a \in R[a_1, ..., a_n][t]$, the coefficients of m_a are all integral over R. Since R is integrally closed in F and $m_a \in F[t]$, the coefficients of m_a lie in R. We then conclude that $m_a \in R[t]$.

The proposition does not hold for non-integrally closed domains. For example, let $R = \mathbb{Z}[\sqrt{5}]$, $F = \mathbb{Q}[\sqrt{5}]$, and $E = F$. Consider $\frac{1+\sqrt{5}}{2} \in F$. Its minimal polynomial over F is is simply $m(t) = t - \frac{1+\sqrt{5}}{2}$. $\frac{1+\sqrt{5}}{2}$ is also integral over R, as it is a root of $t^2 - t - 1 \in \mathbb{Z}[\sqrt{5}][t]$. But $m \notin \mathbb{Z}[\sqrt{5}][t]$. □

Remark. This is a corollary of Proposition 5.15 in *Atiyah & MacDonald.* I found the counter-example on Wiki: `https://en.wikipedia.org/wiki/Integrally_closed_domain.`

Question 6

Let R be an integrally closed, Noetherian, local, integral domain of dimension 1, with unique maximal ideal P. Using the steps below, or otherwise, prove that R is a principal ideal domain.

(i) Let $0 \neq a \in P$. Show that for some $n \geqslant 1$ we have $P^{n-1} \not\subseteq aR$ and $P^n \subseteq aR$, where $P^0 := R$. Let $b \in P^{n-1} \backslash aR$ and put $y = a^{-1}b$. Show that if $yP \subseteq P$ then $y \in R$. Deduce in fact $yP \not\subseteq P$.

Hint: consider the action of y on the R-module P.

(ii) Now deduce that $yP = R$ and hence that P is a principal ideal.

(iii) Let I be a proper, non-zero ideal of R. Prove that $I = P^n$ for some $n \geqslant 1$.

Hint: first show that there is a maximal n for which $I \subseteq P^n$.

Proof. (i) First we note that the only prime ideals of R are $\{0\}$ and P. If there exists another prime ideal $Q \in \operatorname{Spec} R$, then it is contained in some maximal ideal. But P is the unique maximal ideal of R. Hence there is a chain of prime ideals $\{0\} \subsetneq Q \subsetneq P$, contradicting that $\dim R = 1$.

For $a \in P \backslash \{0\}$, the nilradical $\mathrm{Nil}(R/\langle a\rangle) = P/\langle a\rangle$. Since R is Noetherian, so is $R/\langle a\rangle$. By Proposition 3.4, $\mathrm{Nil}(R/\langle a\rangle)$ is nilpotent. There exists $m \in \mathbb{N}$ such that $(P/\langle a\rangle)^m = \{0\} \implies P^m \subseteq \langle a\rangle$. Notice that we have a descending chain of ideals:

$$R = P^0 \supseteq P \supseteq P^2 \supseteq P^3 \supseteq \cdots$$

Let n be the smallest integer such that $P^n \subseteq \langle a\rangle$. Then $P^{n-1} \not\subseteq \langle a\rangle$.

Let $b \in P^{n-1} \backslash aR$ and put $y = a^{-1}b$. If $yP \subseteq P$, then the multiplication by y defines an R-module endomorphism $\varphi_y \in \mathrm{End}_R(P)$. Since R is Noetherian, P is a finitely generated R-module. By Nakayama Lemma (Theorem 5.2), there exists $r_0, ..., r_{k-1} \in R$ such that

$$\varphi_y^k + r_{k-1}\varphi_y^{k-1} + \cdots + r_1\varphi_y + r_0 = 0$$

In other words,

$$y^k + r_{k-1}y^{k-1} + \cdots + r_1 y + r_0 = 0$$

Therefore, y is integral over R. Since R is integrally closed, we have $y \in R$ as claimed.

However, if $y \in R$, then $b = ay \in \langle a\rangle$, which is a contradiction. Hence we must have $yP \not\subseteq P$.

(ii) Since $b \in P^{n-1}$, $bP \subseteq P^n \subseteq \langle a\rangle$. Hence $yP = a^{-1}bP \subseteq R$. In particular yP is an ideal of R. By part (i) we know that $yP \not\subseteq P$, and P is the unique maximal ideal. Then $yP = R$. Hence $P = y^{-1}R = \langle y^{-1}\rangle$. P is a principal ideal.

(iii) Let I be a proper, non-zero ideal of R. Then $I \subseteq R$. The nilradical $\mathrm{Nil}(R/I) = P/I$ is nilpotent (the same as in part (i)). Hence there exists $k \geqslant 1$ such that $(P/I)^k = P^k/I = \{0\} \Longrightarrow P^k \subseteq I$. As $P^{k+1} \subsetneq P^k \subseteq I \subseteq P$, there exists a maximal $n \geqslant 1$ such that $P^{k+1} \subsetneq I \subseteq P^n$.

Since $I \subseteq P^n$ and $I \not\subseteq P^{n+1}$, there exists $x \in I$ such that $x = uy^{-n}$ and $x \notin P^{n+1}$ for some $u \in R$. Hence $u \notin P$. u is a unit in R. Then $y^{-n} = u^{-1}x$ and $P^n = \langle y^{-n} \rangle \subseteq \langle x \rangle \subseteq I$. We conclude that $I = P^n = \langle y^{-n} \rangle$. Now we have proven that every non-zero proper ideal of R is generated by y^{-n} for some $n \in \mathbb{N}$. R is indeed a principal ideal domain. □

Remark. This is a part of Proposition 9.2 in *Atiyah & MacDonald.*

Question 7 2

Let R be a ring, not necessarily Noetherian. Let P be a prime ideal of $S = R[t]$ with $t \in P$. Show that if $h(P)$ is finite then $h(P) > h(P/tS)$.

Hint: show that if Q is a prime ideal of R, then QS is prime in S.

Deduce that if $\dim R$ is finite then $\dim S > \dim R$.

Proof. Let $\iota : R \hookrightarrow S$ be the embedding. First we shall show that for $Q \in \operatorname{Spec} R$, the extension of the ideal $Q^e \in \operatorname{Spec} S$. Note that

$$Q^e = QS = Q[t] = \left\{ \sum_{i=0}^{n} a_i t^i : a_0, \ldots, a_n \in Q, \ n \in \mathbb{N} \right\}$$

From Part A we know that there exists a ring isomorphism: $R[t]/Q[t] \cong (R/Q)[t]$. This follows from applying First Isomorphism Theorem to the composite homomorphism: $R \xrightarrow{\pi_Q} R/Q \xrightarrow{\tilde{\iota}} (R/Q)[t]$. Since $Q \in \operatorname{Spec} R$, R/Q is an integral domain. Then $(R/Q)[t] \cong R[t]/Q[t]$ is also an integral domain. Hence $Q[t] \in \operatorname{Spec} R[t]$.

Suppose that the height of the prime ideal $h(P) = n$. There exists a chain of prime ideals in $R[t]$ of maximal length:

$$\{0\} = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$$

Consider the contraction of the chain in R:

This is not true!

$$\{0\} = P_0^c \subseteq P_1^c \subseteq \cdots \subseteq P_n^c = P^c$$

where $P_i^c := P_i \cap R$. We claim that there exists $k \in \{1, \ldots, n\}$ such that $P_{k-1}^c = P_k^c$. Let k be the maximal integer such that $t \in P_k$. Then $t \notin P_{k-1}$. Note that $P_{k-1}^{ce} = P_{k-1}^c[t] \supsetneq P_{k-1}$ and that $P_{k-1}^{ce} \subseteq P_k$ is prime in $R[t]$. Then we must have $P_{k-1}^{ce} = P_k$ by maximality of the length of the chain. Hence $P_{k-1}^c = P_{k-1}^{cec} = P_k^c$ and the length of the chain $\{P_i^c\}$ is smaller than $h(P)$.

We claim that the length of the chain $\{P_i^c\}$ equals ~~to~~ $h(P^c)$. If there exists another chain of prime ideals in R:

$$\{0\} = Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_m = P^c$$

then the extension of the chain in $R[t]$ is a chain of prime ideals

$$\{0\} = Q_0^e \subsetneq Q_1^e \subsetneq \cdots \subsetneq Q_m^e = P^{ce} \subseteq P$$

If $m = n = h(P)$, then $\{Q_i^e\}$ is a chain of prime ideals of length at least $h(P)$ and the contraction of $\{Q_i^e\}$ is $\{Q_i\}$ whose length is less than n by our previous argument. We conclude that $m < n$ and hence $h(P^c) < h(P)$.

Finally, note that $P/tS = P/\langle t \rangle = (P \cap R)/\langle t \rangle = P^c/\langle t \rangle$. The chain $\{P_i^c\}$ projects to a chain $\{P_i^c/\langle t \rangle\} \subseteq \operatorname{Spec}(R[t]/\langle t \rangle)$. Hence $h(P/tS) \leqslant h(P^c) < h(P)$.

Suppose that $\dim R$ is finite. Note that the composite homomorphism $R \xrightarrow{\iota} R[t] \xrightarrow{\pi} R[t]/\langle t \rangle$ is a ring isomorphism. There exists a chain of prime ideals in R:

$$\{0\} = Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$$

where $n = \dim R$. By isomorphism it corresponds to a chain of prime ideals in $R[t]/\langle t\rangle$ of the same length. Then $h(Q_n/\langle t\rangle) = n$. Let $Q_n[t] = Q_n^e$ be the extension of Q_n in $R[t]$, which is also a prime ideal in $R[t]$. Note that $Q_n[t]/\langle t\rangle = Q_n/\langle t\rangle$. By the previous part, we have $\dim S \geqslant h(Q_n[t]) > h(Q_n/\langle t\rangle) = n = \dim R$. $\square$