D-MATH
HS 2021
Prof. E. Kowalski

Solutions 5

Commutative Algebra

1) We consider the case $n = 2$, the general case follows by induction. First, note that all the ideals of $A_1 \times A_2$ are of the form $I \times J$, with I, J ideals of A_1 and A_2, respectively. Moreover, it's easy to show that the prime ideals of $A_1 \times A_2$ are of the form $\wp_1 \times A_2,\ A_1 \times \wp_2$ with $\wp_1 \subseteq A_1,\ \wp_2 \subseteq A_2$ prime ideals. Therefore, any chain of prime ideals in $A_1 \times A_2$ arises from either a chain of primes in A_1 or a chain of primes in A_2. The longest chain must come from the longest chain in A_1 or A_2.

2)
a. Let $\mathcal{F}$ be the set of non-principal ideals of R. If $\mathcal{F}'$ is a chain in $\mathcal{F}$, then $\bigcup_{I \in \mathcal{F}'} I$ is an ideal of $\mathcal{F}$, which is not principal, if not, one of the $I \in \mathcal{F}'$ would be principal.

b. Since R is a domain of dimension 1, any non-zero prime ideal $\wp$ has height 1. Let $a \in \wp$, write

$$a = \prod_{i=1}^{n} a_i,$$

where a_i are irreducible. Since $\wp$ is prime, there exists $i \in \{1, \ldots, n\}$ so that $a_i \in \wp$. But now

$$0 \subset (a_i) \subseteq \wp$$

is a chain of prime ideals. Because $\mathrm{ht}(\wp) = 1$, one gets $\wp = (a_i)$.

Assume $\mathcal{F} \neq \emptyset$. By Zorn's lemma, $\mathcal{F}$ has a maximal element I. In particular, I is not prime, pick then $a, b \notin I$ with $ab \in I$. Since

$$I + (a) \supset I$$

and

$$I + (b) \supset I,$$

by the maximality of I, both $I + (a)$ and $I + (b)$ are principal. Let $I + (a) = (x)$. Consider the ideal $J = I :_R (I + (a))$; it contains $I + (b)$, so it is principal generated by y, say. One has

$$I = I + (ab) = (I + (a))J = (xy),$$

a contradiction.

3 Suppose $a \notin S^{-1}\mathfrak{p}_i$, $a \notin k$. After clearing denominators, we may assume $a \in A$. Then a includes a monomial not including any of the generators of $\mathfrak{p}_i$ as a factor. By removing monomials in a belonging to $\mathfrak{p}_i$, we may assume a contains no monomial such as X_{m_i+1} with nonzero coefficients; then $a + X_{m_i+1} \in S$, hence it is a unit.
Next, any $x \in A$, $x \neq 0$ can be in only finitely many $S^{-1}\mathfrak{p}_i$. It's enough to check for the variables, which is obvious.
By the above, in particular $S^{-1}A$ satisfies condition 2 of the Lemma. To see that $S^{-1}A_{S^{-1}\mathfrak{p}_i}$ is noetherian, note that it coincides with

$$A_{\mathfrak{p}_i} \simeq k(X_j)[X_{m_i+1}, \dots, X_{m_{i+1}}]_{(X_{m_i+1},\dots,X_{m_{i+1}})},$$

a localization of a noetherian ring, where $j \in \mathbb{N} \setminus \{m_i + 1, \dots, m_{i+1}\}$. This will satisfy condition 1 of the Lemma. Hence it suffices to prove a generalization of the prime avoidance lemma:
any ideal $I \subseteq A$ so that $I \subseteq \bigcup_i \mathfrak{p}_i$ is contained in $\mathfrak{p}_i$ for some i.

Proof. Assume I is not contained in $\bigcup\limits_{k \in K} \mathfrak{p}_k$ for $K \subseteq \mathbb{N}$ finite set (if not, it is the usual prime avoidence). Let $f \in A$ and define

$$D(f) := \{i \in \mathbb{N} : f \in S^{-1}\mathfrak{p}_i\}.$$

Let $f \in I$, then if there is no $g \in I$ so that $D(f) \cap D(g) \neq \emptyset$, then

$$I \subseteq \bigcup_{i \in D(f)} \mathfrak{p}_i$$

and $D(f)$ is finite. Hence there exists $g \in I$ such that $D(f) \cap D(g) = \emptyset$. Note that is $D(f) = \emptyset$ or $D(g) = \emptyset$ then one or the other lies outside of $\bigcup_i \mathfrak{p}_i$, contradicting $I \subseteq \bigcup_i \mathfrak{p}_i$. Hence we may assume $D(f) \neq \emptyset$ and $D(g) \neq \emptyset$.
Let $\sigma \in D(g)$, $d = \deg f$. The claim is that $D(f + X_{m_\sigma+1}^{d+1} g) = \emptyset$, proving a contradiction.
Clearly $D(X_{m_\sigma+1}^{d+1} g) = D(g)$, and since $D(f) \cap D(g) = \emptyset$,

$$f + X_{m_\sigma+1}^{d+1} g \notin \mathfrak{p}_\ell \quad \forall \ell \in D(f) \cup D(g).$$

Moreover, since the term of lowest degree of $X_{m_\sigma+1}^{d+1} g$ is of greater degree than the term of highest degree of f, there can be no cancellation among the monomials, so, by fixing an index ℓ, if $f \notin \mathfrak{p}_\ell$, f has a nonzero monomial not in $\mathfrak{p}_\ell$, and that monomial persists with the same nonzero coefficient in $f + X_{m_\sigma+1}^{d+1} g$, hence $f + X_{m_\sigma+1}^{d+1} g$ cannot lie in $\mathfrak{p}_\ell$, since for a polynomial to lie in $\mathfrak{p}_\ell$, every monomial must lie in $(X_{m_\ell+1}, \dots, X_{m_{\ell+1}})$. $\square$

4 a. Consider the $\mathbb{C}$-algebras morphism

$$\begin{aligned}\Psi : \mathbb{C}[X,Y] &\longrightarrow \mathbb{C}[T]\\ X &\longmapsto T^2\\ Y &\longmapsto T^3.\end{aligned}$$

We prove that $\ker\Psi = (Y^2 - X^3)$. From this, we deduce that R is isomorphic to a subring of $\mathbb{C}[T]$, which is an integral domain. Indeed, $R \simeq \mathbb{C}[T^2, T^3]$.
($\supseteq$): Clear.
($\subseteq$): Any $f \in \mathbb{C}[X,Y]$ can be written as

$$f = f_0(X) + f_1(X)Y + (Y^2 - X^3)g(X,Y).$$

To see this, note that

$$X^mY^n = (Y^2 - X^3)X^mY^{n-2} + X^{m+3}Y^{n-2}$$

for all $m \in \mathbb{N}$, $n \geq 2$. Hence by induction

$$X^mY^n = (Y^2 - X^3)p(X,Y) + q_0(X) + q_1(X)Y.$$

Let $f \in \ker\Psi$, then

$$\begin{aligned}0 &= \Psi(f(X,Y)) = f(T^2, T^3)\\ &= f_0(T^2) + f_1(T^2)T^3.\end{aligned}$$

The even terms of $f_0(T^2) + f_1(T^2)T^3$ are $f_0(T^2)$, the odd terms are $f_1(T^2)T^3$. Thus $f_0(T^2) = 0$ and $f_1(T^2) = 0$, i.e. $f_0(X) = 0$ and $f_1(X) = 0$. Thus

$$f = (Y^2 - X^3)g(X,Y).$$

Finally, we have that the Krull dimension of R is ≥ 1, since it is not a field. Also,

$$\dim R \leq \dim \mathbb{C}[X,Y] - \operatorname{ht}(Y^2 - X^3) = 2 - \operatorname{ht}(Y^2 - X^3).$$

The height of $(Y^2 - X^3)$ is 1: suppose

$$0 \neq \wp \subseteq (Y^2 - X^3)$$

is a chain of primes; take an irreducible $g \in \wp$, then $g = r \cdot (Y^2 - X^3)$. But then r is a constant, so

$$\wp \supseteq (g) = (Y^2 - X^3).$$

Hence $\dim R = 1$.

b. The element $\frac{Y}{X} \in \mathrm{frac}(R) \setminus R$ satisfies the integral equation

$$\left(\frac{Y}{X}\right)^2 - X = 0.$$

c. One sees by evaluating at $(1,1)$ that $(Y^2 - X^3) \subseteq (X-1, Y-1)$. Moreover,

$$R/p \simeq \mathbb{C}[X,Y]/(X-1, Y-1) \overset{f \mapsto f(1,1)}{\simeq} \mathbb{C}.$$

d. The maximal ideal of R_p is principal:

$$pR_p = (X-1)R_p,$$

since $Y - 1 = (X-1)(X^2+X+1)/(Y+1)$. Then it is a PID.

5 a. The polynomial $X^2 - 5$ is irreducible in $\mathbb{Z}[X]$ (Eisenstein criterion for instance), so prime, so R is an integral domain. Also, $\mathrm{ht}(X^2 - 5) = 1$ since it is principal. The dimension of R is ≥ 1, since it is not a field. It is also ≤ 1 by the inequality

$$\dim R \leq \dim \mathbb{Z}[X] - \mathrm{ht}(X^2-5) \leq 2 - 1 = 1.$$

The fraction field is

$$\mathrm{frac}(\mathbb{Z}[\sqrt{5}]) = \left\{ \frac{a+b\sqrt{5}}{c+d\sqrt{5}} : a,b,c,d \in \mathbb{Z},\ (c,d) \neq (0,0) \right\} = \mathbb{Q}(\sqrt{5}),$$

by noting that

$$\frac{a+b\sqrt{5}}{c+d\sqrt{5}} = \frac{(a+b\sqrt{5})(c-d\sqrt{5})}{c^2-5d^2}.$$

b. Observe that

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+5+2\sqrt{5}}{4} = \frac{1+\sqrt{5}}{2} + 1.$$

Then $\alpha := \frac{1+\sqrt{5}}{2}$ satisfies

$$\alpha^2 - \alpha - 1 = 0$$

and α is not in R.

c. Let $x = a + b\sqrt{5}$ be integral over $\mathbb{Z}$, with $a, b \in \mathbb{Q}$. Consider the automorphism

$$\begin{aligned} \sigma : \mathbb{Q}(\sqrt{5}) &\longrightarrow \mathbb{Q}(\sqrt{5}) \\ \sqrt{5} &\longmapsto -\sqrt{5}. \end{aligned}$$

Then $x + \sigma(x)$ and $x\sigma(x)$ are integral over $\mathbb{Z}$, since $\sigma(x)$ is. But

$$x + \sigma(x) = 2a;$$
$$x\sigma(x) = a^2 - 5b^2$$

are both elements of $\mathbb{Q}$ integral over $\mathbb{Z}$, which is integrally closed. Hence

$$2a, a^2 - 5b^2 \in \mathbb{Z} \tag{1}$$

On the other hand, x is a root of

$$X^2 - 2aX + a^2 - 5b^2 \in \mathbb{Z}[X],$$

so by assuming (1) one has

$$4(a^2 - 5b^2) = (2a)^2 - 5(2b)^2 \Longrightarrow 5(2b)^2 \in \mathbb{Z} \Longrightarrow 2b \in \mathbb{Z}.$$

Write

$$a = \frac{u}{2}, \quad b = \frac{v}{2},$$

where $u, v \in \mathbb{Z}$. Condition (1) translates to

$$u^2 - 5v^2 \in 4\mathbb{Z} \tag{2}$$

- if v is even, then (2) implies u even as well, so $a, b \in \mathbb{Z}$ and $x \in R$;
- if v is odd, then $v^2 \equiv 1 \mod 4$ and by (2) also $u^2 \equiv 1 \mod 4$.

In particular

$$x = \frac{1}{2}(u + \sqrt{5}v)$$

where u and v are either both even or both odd.