D-MATH
HS 2019
Prof. E. Kowalski

Solutions 1

Commutative Algebra

1 If $A = \{0\}$, it is trivial. Suppose $A \neq \{0\}$ and pick $a \in A$, $a \neq 0$. Consider the morphism of A-modules

$$\phi_a : A \longrightarrow A$$

given by $\phi(x) = ax$. Then ϕ_a is injective: if $ax = 0$, since A is an integral domain and $a \neq 0$, we have $x = 0$. But A is finite, so ϕ_a is also surjective. In particular, $1 = ax$ for some $x \in A$, so a is invertible in A.

2

a. $\sqrt{\mathfrak{a}} = \sqrt{\sqrt{\mathfrak{a}}}$:
($\subseteq$) true, since for any ideal I, $I \subseteq \sqrt{I}$;
($\supseteq$) $a \in \sqrt{\sqrt{\mathfrak{a}}} \Longrightarrow (a^m)^n \in \mathfrak{a}$ for some $m, n \Longrightarrow a^{mn} \in \mathfrak{a} \Longrightarrow a \in \sqrt{\mathfrak{a}}$.

b. $\sqrt{\mathfrak{ab}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$:
Since $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$, one has $\sqrt{\mathfrak{ab}} \subseteq \sqrt{\mathfrak{a} \cap \mathfrak{b}}$. Moreover, if $a \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$, then $a^m \in \mathfrak{a}$ and $a^m \in \mathfrak{b}$ for some m, which means $a \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$. Hence

$$\sqrt{\mathfrak{ab}} \subseteq \sqrt{\mathfrak{a} \cap \mathfrak{b}} \subseteq \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}.$$

It remains to show that $\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} \subseteq \sqrt{\mathfrak{ab}}$: let $a \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$, then there exist m, n such that $a^m \in \mathfrak{a}$ and $a^n \in \mathfrak{b}$, thus $a^{m+n} \in \mathfrak{ab}$, i.e. $a \in \sqrt{\mathfrak{ab}}$.
[This implies, by iteration, that $\sqrt{I^k} = \sqrt{I}$ for all ideals I and integers $k > 0$].

c. $\sqrt{\mathfrak{a}} = (1) \Longleftrightarrow \mathfrak{a} = (1)$:
$\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, hence if $1 \in A$, then $1 \in \sqrt{\mathfrak{a}}$. Conversely, $1^m = 1 \in \mathfrak{a}$.

d. if $\mathfrak{p} \subseteq A$ is a prime ideal, then $\sqrt{\mathfrak{p}^k} = \mathfrak{p}$ for all integers $k > 0$:
By *b.* $\sqrt{\mathfrak{p}^k} = \sqrt{\mathfrak{p}}$. It remains to show that $\sqrt{\mathfrak{p}} \subseteq \mathfrak{p}$:
let $a \in \sqrt{\mathfrak{p}}$, so $a^n \in \mathfrak{p}$ for some n. If $n = 0$, we conclude. If $n > 0$, assume by induction that $(a^{n-1} \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p})$. Then $a^n = aa^{n-1} \in \mathfrak{p}$ implies, by the primality of $\mathfrak{p}$, that either $a \in \mathfrak{p}$ or $a^{n-1} \in \mathfrak{p}$. In both cases we can conclude by induction.

3 Write

$$n = \prod_{i=1}^{s} p_i^{\alpha_i}$$

with p_i distinct primes, $\alpha_i \geq 1$ for i$= 1, \dots, s$. Note that $(p_1^{\alpha_1} \dots p_s^{\alpha_s}) = (p_1^{\alpha_1}) \dots (p_s^{\alpha_s})$ as ideals of $\mathbb{Z}$. Moreover, for $i \neq j$, $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = \mathbb{Z}$, then by the Chinese Remainder Theorem, one has

$$\begin{aligned}\sqrt{(n)} &= \sqrt{(p_1^{\alpha_1} \dots p_s^{\alpha_s})} = \sqrt{(p_1^{\alpha_1}) \dots (p_s^{\alpha_s})} \\ &\overset{CRT}{=} \sqrt{(p_1^{\alpha_1}) \cap \dots \cap (p_s^{\alpha_s})} \overset{2b.}{=} \sqrt{(p_1^{\alpha_1})} \cap \dots \cap \sqrt{(p_s^{\alpha_s})} \\ &\overset{2d.}{=} (p_1) \cap \dots \cap (p_s) \overset{CRT}{=} (p_1) \dots (p_s) = (p_1 \dots p_s).\end{aligned}$$

So we can take m as the square-free part of n.

4

a. f is a unit in $A[X]$ if and only if there is a $g \in A[X]$, $g = \sum_{i=0}^{m} b_i X^i$ such that $fg = 1$ in $A[X]$. Then $fg = \sum_{i=0}^{m+n} c_i X^i = 1$ with $c_i = \sum_{k+h=i} a_k b_h$. For $i = 0$, we have $a_0 b_0 = 1$, which implies that a_0 in invertible in A.
For $i = m + n$ we obtain

$$a_n b_m = 0.$$

Multiplying c_{n+m-1} by a_n we have

$$a_n(a_{n-1}b_m + a_n b_{m-1}) = 0 \Longrightarrow a_n^2 b_{m-1} = 0.$$

From this

$$a_n^2 c_{n+m-2} = a_n^2(a_{n-2}b_m + a_{n-1}b_{m-1} + a_n b_{m-2}) = 0 \Longrightarrow a_n^3 b_{m-2} = 0$$

and so on. In particular

$$a_n^{m+1} b_0 = 0,$$

but b_0 is a unit, so it must be $a_n^{m+1} = 0$, which means that a_n is nilpotent.
Now, consider $f - a_n X^n$, which coefficients are $a_0, \dots, a_{n-1}$, and note that

$$\begin{aligned}(1 - a_n g X^n)(1 + a_n g X^n + (a_n g X^n)^2 + \dots + (a_n g X^n)^m) \\ = 1 - (a_n g X^n)^{m+1} = 1,\end{aligned}$$

so $1 - a_n g X^n$ is invertible; but f is also invertible, hence so is $f - a_n X^n$. By repeating the above argument we find that a_{n-1} is nilpotent and so on (induction).

b. If $a_0, \dots, a_n$ are nilpotent then f is nilpotent, since $f \in (a_0, \dots, a_n)A[X]$ and the set of nilpotent elements is an ideal.

Conversely, let $k > 0$ such that $f^k = 0$, then clearly $a_0^k = 0$, so a_0 is nilpotent. Let

$$\begin{cases} f_0 := f \\ f_k := f_{k-1} - a_{k-1}X^{k-1} \quad \text{for } 1 \leq k \leq n-1. \end{cases}$$

Assume by induction that a_h is nilpotent for all $h \leq k-1$. Then $f_{k+1} = f - a_0 - a_1X - \dots - a_kX^k$ is nilpotent, so there is an ℓ such that $f_{k+1}^\ell = 0$, i.e.

$$X^{k\ell}(a_k + \dots + a_nX^{n-k})^\ell = X^{k\ell}(a_k^\ell + \dots) = 0,$$

which implies $a_k^\ell = 0$, i.e. a_k nilpotent.

c. Let $g = \sum_{i=0}^m b_iX^i \in A[X]$, $g \neq 0$ such that $fg = 0$ in $A[X]$. We can assume that $b_0 \neq 0$ by observing that $Xgf = 0 \Leftrightarrow gf = 0$. Take also g of minimum degree.
In particular $a_nb_m = 0$, and of course $(a_ng)f = 0$. Since $\deg(a_ng) < m$, by assumption $a_ng = 0$. From

$$\begin{aligned} fg = a_0 + a_1Xg + \dots + a_{n-1}X^{n-1}g \\ = a_0 + \dots + a_{n-1}b_mX^{n-1+m} = 0 \end{aligned}$$

one has $a_{n-1}b_m = 0$, and again $\deg(a_{n-1}g) < m$, so $a_{n-1}g = 0$. Proceeding, one obtain $a_{n-k}g = 0$ for $k = 0, \dots, n$. In particular $b_0a_k = 0$ for $k = 0, \dots, n$, so $b_0f = 0$.

In general

$$\sqrt{(0)} = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p} \subseteq \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = \mathrm{J}(A[X])$$

since every maximal ideal is prime.
Note: if $f \notin \mathfrak{m}$ for some $\mathfrak{m}$, then

$$\mathfrak{m} \subset (f) + \mathfrak{m}$$

and by the maximality of $\mathfrak{m}$, $(f) + \mathfrak{m} = (1)$. In particular there exist $g \in A[X]$, $h \in \mathfrak{m}$ such that

$$fg + h = 1,$$

so $1 - fg \in \mathfrak{m}$ is not a unit.

Then, if $\in$ J(A[X]) (so $f \in \mathfrak{m}$ for all $\mathfrak{m}$), for all $g \in A[X]$, $1 - fg \in A[X]^\times$. Take $g = -X$. Thus

$$1 + fX = 1 + a_0X + \dots \in A[X]^\times.$$

By 4a. the coefficients $a_0, \dots, a_n$ are nilpotent, and so by 4b. f is nilpotent.

(5) Define

$$\phi : S^{-1}(A[X]) \longrightarrow (S^{-1}A)[X]$$

by

$$\phi\Big(\frac{\sum a_i X^i}{s}\Big) = \sum_{i=0}^{\deg f} \frac{a_i}{s} X^i$$

for $\sum a_i X^i \in A[X]$, $s \in S$. Then ϕ is well-defined, since if $\sum a_i X^i / s = \sum b_i X^i / s'$, there exists $s'' \in S$ such that

$$s''(\sum_{i=0}^{n} (a_i s' - c_i s) X^i) = 0$$

with $c_i = b_i$ if $i \leq m$, 0 otherwise (assuming $n = \deg(\sum a_i X^i) \geq \deg(\sum b_i X^i) = m$). It turns out that

$$s''(a_i s' - c_i s) = 0$$

for $i = 0, \ldots, n$, so $a_i/s = b_i/s'$ in $S^{-1}A$ and $\phi\Big(\sum a_i X^i / s\Big) = \Big(\sum b_i X^i / s'\Big)$.
It remains to show that ϕ is an homomorphism of rings, injective and surjective, which is straightforward.
Alternatively, one can use the universal property of the localization. For the ring homomorphism $\alpha : A[X] \longrightarrow (S^{-1}A)[X]$, $\alpha(\sum a_i X^i) = \sum a_i / s X i$ there is a unique ϕ such that the following diagram commutes

$$\begin{tikzcd} A[X] \arrow[rr, "\alpha"] \arrow[dr, "\Phi"'] & & (S^{-1}A)[X] \\ & S^{-1}(A[X]) \arrow[ur, "\phi"'] & \end{tikzcd}$$

where Φ is the localization map, $\alpha = \phi \circ \Phi$. On the other hand, since $S^{-1}(A[X])$ is a $S^{-1}A-$algebra, by the universal property of the polynomial ring, there is a unique morphism

$$\psi : (S^{-1}A)[X] \longrightarrow S^{-1}(A[X])$$

sending $1/1X$ in $X/1$. We prove now that ψ is the inverse of ϕ. Again, by the universal property, it is sufficient to show it for the indeterminate X:

$$\phi \circ \psi(X) = \phi(X/1) = \phi \circ \Phi(X) = \alpha(X) = X$$
$$\psi \circ \phi(X/1) = \psi \circ \phi \circ \Phi(X) = \psi \circ \alpha(X) = \psi(1/1X) = X/1.$$

6 b. C ring, g, g' rings homomorphisms. If $f \circ g = f \circ g'$ then $g = g'$.

$$\begin{tikzcd} C \arrow[r, bend left, "g"] \arrow[r, bend right, "g'"'] \arrow[rr, bend left=60, "f \circ g"] \arrow[rr, bend right=60, "f \circ g'"'] & A \arrow[r, "f"] & B \end{tikzcd}$$

Let f be a monomorphism, and consider $C = \ker f$, $g = \iota$ the inclusion map, $g' = 0$;

$$\begin{tikzcd} \ker f \arrow[r, bend left, "\iota"] \arrow[r, bend right, "0"'] & A \arrow[r, "f"] & B \end{tikzcd}$$

Then by definition $f \circ \iota(a) = f \circ 0(a)$, so by assumption $a = 0$ for all $a \in \ker f$. The opposite implication follows by the fact that f injective has a left-inverse.

c. C ring, g, g' rings homomorphisms. If $g \circ f = g' \circ f$ then $g = g'$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend left=60, "g \circ f"] \arrow[rr, bend right=60, "g' \circ f"'] & B \arrow[r, bend left, "g'"] \arrow[r, bend right, "g"'] & C \end{tikzcd}$$

As before, if f is surjective, then it has a right-inverse, so by composing both sides of $g \circ f = g' \circ f$ with the right-inverse of f we conclude.

We show now that the inclusion $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook, "\iota"] \arrow[rr, bend left=60, "g \circ \iota"] \arrow[rr, bend right=60, "g' \circ \iota"'] & \mathbb{Q} \arrow[r, bend left, "g'"] \arrow[r, bend right, "g"'] & C \end{tikzcd}$$

Claim: "if $g = g'$ on $\mathbb{Z}$, then $g = g'$ on $\mathbb{Q}$".

Let $a, b \in Z$ coprime, $b \neq 0$. We get

$$g(a/b) = g(a \cdot 1/b) = g(a)g(1/b) = g'(a)g(1/b);$$

it's enough to prove the claim for $1/b \in \mathbb{Q}$, $b \neq 0$. One has

$$1 = g(b \cdot 1/b) = g(b)g(1/b)$$

and

$$1 = g'(b \cdot 1/b) = g(b)g'(1/b)$$

so $g(b)$ is invertible, and by the unicity of the inverse, $g(1/b) = g'(1/b)$.

7 Let $M_\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ for $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. For a polynomial $f \in A$, denote by $\operatorname{supp}(f)$ the set of the monomials in f, that is, $\operatorname{supp}(f) = \{M_\alpha : \alpha \in F\}$ if $f = \sum_{\alpha \in F} \lambda_\alpha M_\alpha$ ($F \subseteq \mathbb{N}^n$ finite set, $\lambda_\alpha \in k$).

a. If a monomial M is in I, then there is a finite set $E' \subseteq E$ and polynomials f_α, $\alpha \in E'$ such that

$$M = \sum_{\alpha \in E'} f_\alpha M_\alpha.$$

Write $f_\alpha = \sum_{\beta \in A_\alpha} \lambda_\alpha^\beta M_\beta$ for some finite set $A_\alpha \subseteq \mathbb{N}^n$, $\lambda_\alpha^\beta \in k$ for all $\alpha \in E'$, $\beta \in A_\alpha$. Hence

$$M = \sum_{\substack{\alpha \in E' \\ \beta \in A_\alpha}} \lambda_\alpha^\beta M_{\alpha+\beta}.$$

Since the monomials in A are linearly independent over k, the monomial M must occur in the RHS, so there are $\alpha \in E'$, $\beta \in A_\alpha$ such that

$$M = M_{\alpha+\beta} = M_\alpha M_\beta.$$

b. Let $f \in I$ with I monomial, $f = \sum_{\text{finite}} \lambda_\gamma M_\gamma$. Then, using the same notations of a.,

$$\sum_{\text{finite}} \lambda_\gamma M_\gamma = \sum_{\substack{\alpha \in E' \\ \beta \in A_\alpha}} \lambda_\alpha^\beta M_{\alpha+\beta}.$$

For every γ', the monomial $M_{\gamma'}$ must occur in the sum $\sum_{\substack{\alpha \in E' \\ \beta \in A_\alpha}} \lambda_\alpha^\beta M_{\alpha+\beta}$, since

$$\lambda_{\gamma'} M_{\gamma'} = \sum_{\substack{\alpha \in E' \\ \beta \in A_\alpha}} \lambda_\alpha^\beta M_{\alpha+\beta} - \sum_{\gamma \neq \gamma'} \lambda_\gamma M_\gamma$$

and $M_{\gamma'}$ doesn't occur in the second sum on the RHS. So every monomial of f is in I.

Conversely, let $f_i, \dots, f_t$ be a set of generators of the ideal I. Since for all $i = 1, \dots, t$, $f_i \in I$, by hypothesis $\mathrm{supp}(f_i) \subseteq I$ for all I, so

$$I = (\mathrm{supp}(f_i))_{i=1,\dots,t}$$

is generated by monomials.

c. Let $I = (M_\alpha)_{\alpha \in E}$ and $J = (M_\beta)_{\beta \in F}$. Clearly one has
$I + J = ((M_\alpha), (M_\beta))_{\alpha,\beta}$;
$IJ = (M_\alpha M_\beta)_{\alpha,\beta}$.
Let's show that $I \cap J$ is monomial: if $f \in I \cap J$, then $\mathrm{supp}(f) \subseteq I \cap J$ and we conclude by point b.. For monomials M_α and M_β let $\mathrm{lcm}(M_\alpha, M_\beta) = X_1^{\max(\alpha_1,\beta_1)} \dots X_n^{\max(\alpha_n,\beta_n)}$ and $\gcd(M_\alpha, M_\beta) = X_1^{\min(\alpha_1,\beta_1)} \dots X_n^{\min(\alpha_n,\beta_n)}$. As a set of generators we can take

$$I \cap J = (\mathrm{lcm}(M_\alpha, M_\beta))_{\alpha,\beta} :$$

($\supseteq$) holds in general;
($\subseteq$) by b. it's enough to prove the inclusion for monomials. Let M be a monomial, $M \in I \cap J$. By a., there are α, β such that $M_\alpha | M$ and $M_\beta | M$ in A, so by definition $\mathrm{lcm}(M_\alpha, M_\beta) | M$ in A.
In general, it's easy to see that

$$I : J = \bigcap_{\beta \in F} I : M_\beta.$$

We now prove that

$$I : M_\beta = (M_\alpha / \gcd(M_\alpha, M_\beta))_\alpha$$

for every α. Use then the above to find monomial generators for $I : J$.
($\supseteq$) clear;
($\subseteq$) if a monomial M is in $I : M_\beta$, then $M M_\beta \in I$, so by a., there are $\alpha \in E$, $\gamma \in \mathbb{N}^n$ such that $M M_\beta = M_\gamma M_\alpha$. It holds $b_i \leq \gamma_i + \alpha_i$ for all i and

$$M = \frac{M_\alpha}{\gcd(M_\alpha, M_\beta)} M'',$$

with $M'' = \frac{M_\gamma M_\alpha}{\mathrm{lcm}(M_\alpha, M_\beta)}$, which is in A since $\max(\alpha_i, \beta_i) \leq \gamma_i + \alpha_i$ for every i.
$\sqrt{I}$ is monomial: let $f \in \sqrt{I}$, with m such that $f^m \in I$. Then $\mathrm{supp}(f^m) \subseteq I$; but for every $M_\alpha \in \mathrm{supp}(f)$, $M_\alpha^m \in \mathrm{supp}(f^m)$, hence $M_\alpha^m \in I$ for every $M_\alpha \in \mathrm{supp}(f)$, which means $\mathrm{supp}(f) \subseteq \sqrt{I}$.
Define the "radical" of a monomial M_α by

$$\sqrt{M_\alpha} := X_1^{\epsilon_1} \dots X_n^{\epsilon_n},$$

where

$$\epsilon_i = \begin{cases} 1 & \text{if } \alpha_i \geq 1 \\ 0 & \text{if } \alpha_i = 0. \end{cases}$$

Then

$$I = (\sqrt{M_\alpha})_\alpha :$$

($\supseteq$) clear since $(\sqrt{M_\alpha})^{\sum \alpha_i} \in I$; ($\subseteq$) $M_\gamma \in \sqrt{I}$ with $M_\gamma^m \in I$. Then $M_\gamma^m = M_{\gamma m} = M_{\gamma'} M_\alpha$ for some $\alpha \in E$, $\gamma' \in \mathbb{N}^n$. Note that $M_\alpha = \sqrt{M_\alpha} M_{\alpha-\epsilon}$ ($\alpha_i - \epsilon_i \geq 0$). Therefore

$$M_\gamma = \frac{M_\gamma^m}{M_\gamma^{m-1}} = \frac{M_{\gamma'} M_{\alpha-\epsilon}}{M_{\gamma(m-1)}} \sqrt{M_\alpha}$$

and $\frac{M_{\gamma'} M_{\alpha-\epsilon}}{M_{\gamma(m-1)}} \in A$ since for $\gamma_i \geq 1$, $(m-1)\gamma_i \leq \gamma_i' + \alpha_i - \epsilon_i$.

8 Clearly $(I : S)S \subseteq I$. Let $J \subseteq A$ be an ideal with $JS \subseteq I$. If $a \in J$, then $aS \subseteq I$, so $a \in (I : S)$. This means that $J \subseteq (I : S)$.