D-MATH
HS 2021
Prof. E. Kowalski

Solutions 7

Commutative Algebra

1 a. Let $R := \mathbb{C}[x,y]/(y^2 - x^3 - x)$ and let $K := \mathrm{frac}(R)$. Since $y^2 - x^3 - x$ is irreducible, K is a quadratic extension of $\mathbb{C}(x)$. Moreover, K is a cubic extension of $\mathbb{C}(y)$. Therefore $\{x\}$ and $\{y\}$ are transcendence basis fior K and so the transcendence degree is 1.

If the extension were purely transcendental, it would be equal to $\mathbb{C}(T)$ fort some T. Then there are non-constant rational functions f and g so that

$$f(T)^2 = g(T)^3 + g(T).$$

It's easy to check that we can write

$$g(T) = \frac{u(T)}{w(T)^2}$$

and

$$f(T) = \frac{v(T)}{w(T)^3},$$

where $u, v, w \in \mathbb{C}[T]$. Hence by taking the formal derivative, one has

$$g'(T) = \frac{\text{poly}}{w(T)^3}.$$

Define

$$h(T) := \frac{g'(T)}{f(T)} = \frac{\text{poly}}{v(T)}.$$

Similarly one gets

$$h(T) = \frac{\text{poly}}{2u(T)^2 + w(T)^4}.$$

If the denominator of $h(T)$ has a root $a \in \mathbb{C}$, then

$$v(a) = 3u(a)^2 + w(a) = 0.$$

We can assume $w(a) \neq 0$ (if not, divide both $u(T)$ and $v(T)$ by $T - a$). Thus $f(a)$ and $g(a)$ are well-defined and we get

$$f(a) = 3g(a)^2 + 1$$

as well as

$$f(a)^2 = g(a)^3 + g(a).$$

This is impossible. As f, g are non-constant, h is a non-zero polynomial.
Now, replace $f(T)$ and $g(T)$ by $f(1/T)$ and $g(1/T)$. Then

$$-T^{-2}h(1/T) = \frac{g'(1/T)}{2f(1/T)}.$$

In particular, $f(1/T)$ and $g(1/T)$ in another pair of functions satisfying the equation in the definition of h. But we proved that the quotient $\frac{g'(1/T)}{2f(1/T)}$ is a polynomial, which is impossible.

b. Let $L = \text{frac}(R)$ and $K = \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, it has no nontrivial algebraic extensions, and we showed in a that $\text{frac}(R)/\mathbb{C}$ is not purely transcendental.

2 Let $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_m\}$ be transcendensce basis for L/K and E/L, respectively. The claim is that $X \cup Y$ is a transcendence base for the extension E/K. Let $\alpha \in E$, then there exists $p \in L[X]$, $p \neq 0$ so that

$$p(y_1, \ldots, y_m, \alpha) = 0.$$

Each coefficient of p is an element of L, which is algebraic over $K(x_1, \ldots, x_n)$. Hence we can replace each coefficient of p with a non-zero polynomial of $K[X]$ dependent upon $x_1, \ldots, x_n$. We can then assume p to be the non-zero polynomial $q \in K[X]$ such that

$$q(x_1, \ldots, x_n, y_1, \ldots, y_m, \alpha) = 0.$$

Call $g(T) = q(x_1, \ldots, x_n, y_1, \ldots, y_m, T) \in K(X \cup Y)[T]$. Thus α is algebraic over $K(X \cup Y)$, and so E is algebraic over $K(X \cup Y)$.
To show that $X \cup Y$ is a transcendence basis we have to show that it is maximal. If v is not maximal then there exists some Z that contains $X \cup Y$, which is algebraically independent over K. So we can pick $\beta \in Z$ such that $\{x - 1, \ldots, x_n, y_1, \ldots, y_m, \beta\}$ is an algebraically independent set. However, this gives us that $\{y_1, \ldots, y_m, \beta\}$ is an algebraically independent subset of E over L, which invalidates the maximality of Y.

3 a. Since R_1 are R_2 are finitely generated K-algebras, there are $t, s \geq 1$ and surjective morphisms

$$K[X_1, \ldots, X_t] \longrightarrow R_1,$$

$$K[X_1, \ldots, X_s] \longrightarrow R_2.$$

By the universal property of tensor product and the K-algebras isomorphism

$$K[X_1,\dots,X_t]\otimes_K K[X_1,\dots,X_s]\simeq K[X_1,\dots,X_{t+s}],$$

we have a surjective K-algebras morphism

$$K[X_1,\dots,X_{t+s}]\longrightarrow R,$$

so R is finitely generated as well. It is nonzero, since tensor product of nonzero vector spaces in nonzero.

b. Assume $b_1,\dots,b_t\in R_2$ are l.d. over K, i.e. there are $\lambda_1,\dots,\lambda_t\in K$ not all zero s.t.

$$\lambda_1 b_1+\cdots+\lambda_t b_t=0.$$

Assume $\lambda_1\neq 0$, then $b_1=\lambda_1^{-1}(-\lambda_2 b_2-\cdots-\lambda_t b_t)$. We can then write

$$\begin{aligned}\sum_{i=1}^t a_i\otimes b_i &= \gamma_{12}a_1\otimes b_2+\gamma_{13}a_1\otimes b_3+\cdots+\gamma_{1t}a_1\otimes b_t+\sum_{i=2}^t a_i\otimes b_i\\ &=\sum_{i=2}^t c_i\otimes b_i,\end{aligned}$$

for some coefficients $\gamma_{ij}\in K$ and $c_i\in R_1$. The last sum involves only $b_2,\dots,b_t$ in R_2. Repeat this process until you just use a l.i. set of b_i's.

c. The quotient R_1/m is a finitelky generated K-algebra and a field; then it is an algebraic extension of K, which is algebraically closed, hence isomorphic to K. Let $\varphi=\pi_m\otimes \mathrm{Id}_{R_2}$. Assume $f_1f_2=0$. Since $\varphi(f_1f_2)=\varphi(f_1)\varphi(f_2)=0$, and R_2 is an integral domain, either $\varphi(f_1)=0$ or $\varphi(f_2)=0$. Moreover, one has $\varphi(f_1)=\sum\pi_m(a_i)b_i$ and $\varphi(f_2)=\sum\pi_m(c_i)d_i$. Assume $\varphi(f_2)=0$. Since the (d_i) are l.i., we have $\pi_m(c_i)=0$ for all i. Similarly by assuming $\varphi(f_1)=0$. In any case, $I_1\cap I_2\subseteq m$ for any maximal ideal.

d. In R_1 the nilradical is equal to the Jacobson radical, so evey element of $I_1\cap I_2$ is nilpotent, hence 0, since R_1 is an integral domain.

e. Assume $f\neq 0$. Then $I_1\neq 0$, pick $x\in I_1$, $x\neq 0$. For every $y\in I_2$, one has $xy=0$ by d. Since R_1 is an integral domain, one has $y=0$, hence $I_2=0$, so $f_2=0$. It means that R is an integral domain.

4 a. Let $x \in \overline{\mathbb{Q}}$; then there exist $s \geq 1$, $a_i, b_i \in \mathbb{Z}$, a_i not all zero, $b_i \neq 0$ $(i = 1, \ldots, s)$ so that

$$\frac{a_s}{b_s}x^s + \frac{a_{s-1}}{b_{s-1}}x^{s-1} + \cdots + \frac{a_0}{b_0} = 0.$$

Multiplying by $\operatorname{lcm}(b_0, \ldots, b_s)$, we can assume that the above equation has coefficients in $\mathbb{Z}$; call them $c_s, \ldots, c_0$. Now, if one multiplies by c_s^{s-1}, on gets

$$(c_s x)^s + c_{s-1}(c_s x)^{s-1} + c_{s-2}c_s(c_s x)^{s-2} + \cdots + c_0 c_s^{s-1} = 0.$$

Hence $c_s x \in \overline{\mathbb{Z}}$.

b. We consider the case $k = 1$. The general one can be achieved by induction.
Let I be the ideal of $\mathbb{Z}[y]$ defined by

$$I = (\{\sum_{i=0}^{s-1} a_i y^i : p | a_i \ \forall i\}),$$

where s is the degree of the minimal polynomial of y over $\mathbb{Z}$. The composition ϕ of the following canonical morphisms

$$\mathbb{Z} \hookrightarrow \mathbb{Z}[Y] \twoheadrightarrow \mathbb{Z}[y]/I$$

has kernel $p\mathbb{Z}$. So there is an embedding

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}[y]/I.$$

The above extension is integral and I is a prime ideal. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, $\mathbb{Z}[y]/I$ is a field as well, so $I = m$ maximal.

c. By part a, for any $i = 1, \ldots, k$ there exists an integer n_i so that $n_i y_i$ is integral over $\mathbb{Z}$. in particular, for every i there is an $s_i \geq 1$ and integer coefficients not all zero so that

$$(n_i y_i) s_i + a_{s_i - 1}(n_i y_i)^{s_i - 1} + \cdots + a_0 = 0.$$

If we multiply by $1/n_i^{s_i}$, we get that y_i is integral over $\mathbb{Z}[1/n_i]$ for all i. So we have an integral extension

$$\mathbb{Z}[1/n_1, \ldots, 1/n_k] \subseteq \mathbb{Z}[1/n_1, \ldots, 1/n_k, y_1, \ldots, y_k].$$

But $\mathbb{Z}[1/n_1, \ldots, 1/n_k] = \mathbb{Z}[1/N]$, where $N = \operatorname{lcm}(n_1, \ldots, n_k)$.
One has $\mathbb{Z}[1/N] = S^{-1}\mathbb{Z}$, where $S = \{1, N, N^2, \ldots\}$. Since $p \nmid N$, $p\mathbb{Z} \cap S = \emptyset$. As in b, one can find $m \subseteq \mathbb{Z}[1/N, y]$ maximal so that

$$\mathbb{Z}[1/N]/p\mathbb{Z}[1/N] \hookrightarrow \mathbb{Z}[1/N, y]/m$$

is integral. On the other hand, one has that

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow S^{-1}\mathbb{Z}/pS^{-1}\mathbb{Z}$$

is integral. By composing, we have the integral extension

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}[1/N, y]/m.$$

d. Consider the ideal $I \subseteq \overline{\mathbb{Q}}[X_1, \dots, X_n]$ generated by $f_1, \dots, f_m$, and let $J = I\mathbb{C}[X_1, \dots, X_n]$. The set $Z(V(I))$ is the zero locus (inside $\overline{\mathbb{Q}}[X_1, \dots, X_n]$) of $V(I)$, which is finite, since contained in $V(J)$. Let then $(x_{11}, x_{12}, \dots, x_{1n}), \dots, (x_{s1}, x_{s2}, \dots, x_{sn})$ be the elements of $V(I)$. Consider the polynomials

$$g_1(X_1, \dots, X_n) = (X_1 - x_{11}) \dots (X_1 - x_{s1})$$
$$\vdots$$
$$g_n(X_1, \dots, X_n) = (X_n - x_{1n}) \dots (X_n - x_{sn}).$$

Then $g_i \in Z(V(I))$ for all i and if $(y_1, \dots, y_n)$ is in $V(I)$, it must be one of the points $(a_{i1}, \dots, a_{in})$. By the Nullstellensatz, these polynomials are in $\sqrt{I}$, i.e. for all i there exists k_i such that $g_i^{k_i} \in I$. In particular $g_i^{k_i} \in J$ for all i. This means that if $(y_1, \dots, y_n) \in V(J)$, it must be a zero of each of these polynomials, i.e. y_1 is algebraic (in fact, one of $a_{11}, a_{21}, \dots$), y_2 is algebraic (in fact, one of $a_{12}, a_{22}, \dots$) and so on. Then $(y_1, \dots, y_n) \in V(I)$, whence $V(I) = V(J)$.

e. By part c, for any $x \in \overline{\mathbb{Q}}$ there are infinitely many primes p, an integer $N \geq 1$ so that for a maximal ideal $m \in \mathbb{Z}[1/N, x]$, x mod m is in $\overline{\mathbb{F}}_p$. We call this reduction modulo m, reduction modulo p of x.
Assume there are no solutions in $\mathbb{C}^n$. By d, this is equivalent to assume there are no algebraic solutions. By the Nullstellensatz there are $g_1, \dots, g_m \in \overline{\mathbb{Q}}[X_1, \dots, X_n]$ so that

$$g_1 f_1 + \dots + g_m f_m = 1.$$

The coefficients of g_i are algebraic numbers. Pick then the primes p not dividing a finite number of positive integers (the N's of c). We can reduce those coefficients modulo p and we get

$$g_1 f_1 + \dots + g_m f_m \mod p = 1 \mod p.$$

Again, by the Nullstellensatz, this is equivalent to $\{(x_i) \in \overline{\mathbb{F}}_p^n : f_j((x_i)) = 0 \ \forall j = 1, \dots, m\} = \emptyset$ for all p as above.