MA3201 Algebra II
Final Exam Solution

AY2021/2022 Semester 2

Written by: Fang Xinyu

Q1

(a)

1. The map Φ is injective. Suppose $f, g \in R[x]$ is such that $\Phi(f) = \Phi(g)$. Then for all $a \in R$, we have

$$\begin{aligned} f(a) = g(a) &\implies (f-g)(a) = 0 \\ &\implies f-g \text{ has infinitely many roots} \\ &\implies f-g \equiv 0 \\ &\implies f \equiv g. \end{aligned}$$

2. The map Φ is not surjective. Let $\phi \in$ Maps(R, R) be defined by

$$\phi(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{otherwise.} \end{cases}$$

If $\phi = \Phi(f)$ for some $f \in R[x]$, then since f has infinitely many roots, it should be the zero polynomial. This is a contradiction since $f(0) \neq 0$.

(b)

Let $R = \mathbb{Z}/4\mathbb{Z}$. Then Φ is not injective since for example by taking $f = x^2$ and $g = x^4$, we have

$$\Phi(g)(x) = \Phi(f)(x) = \begin{cases} 0 & \text{if } x = 2 \text{ or } 4 \\ 1 & \text{if } x = 1 \text{ or } 3. \end{cases}$$

The map Φ is also not surjective since there does not exists an element $f \in R[x]$ such that $\Phi(f)$ maps 0 to 0 and 2 to 1. This is because if $f(0) = 0$, then f has constant term 0 and so $x \mid f$. This mean that $f(2)$ is even, so it cannot be 1.

Q2

Fix $x = a \in \mathbb{Q}$. Then $f(a, y) \in \mathbb{Q}[y]$ vanishes at every $y \in \mathbb{Q}$, so we must have $f(a, y) = 0 \in \mathbb{Q}[y]$. Now regard f as an element of $(\mathbb{Q}[x])[y]$. For each term, the coefficient, as a polynomial in $\mathbb{Q}[x]$, must vanish at every $x \in \mathbb{Q}$. Therefore all coefficients are the zero polynomial in $\mathbb{Q}[x]$. Thus we conclude that $f = 0 \in \mathbb{Q}[x, y]$.

Q3

(a)

Since $\mathbb{Q}[x, y]$ is a UFD, it suffices to show that $x^2 + y^2 - 1$ is irreducible. Regard the polynomial as an element of $(\mathbb{Q}[y])[x]$. We can use Eisenstein's criterion since $\mathbb{Q}[y]$ is an integral domain. We have that $y^2 - 1 \in (y + 1)$ but $y^2 - 1 \notin (y + 1)^2$ (note that $(y + 1)$ is a prime ideal in $\mathbb{Q}[y]$). Therefore $x^2 + y^2 - 1$ is irreducible.

(b)

We prove the isomorphism using elementary methods by constructing explicit homomorphisms $\Phi : Frac(R) \to \mathbb{Q}(t)$ and $\Psi : \mathbb{Q}(t) \to Frac(R)$ and showing that they are inverses of each other. The result can also be seen more directly using the algebraic geometry of curves (see the remark at the end).

Let $I = (x^2 + y^2 - 1) \subset \mathbb{Q}[x, y]$. Let $\phi : \mathbb{Q}[x, y] \to \mathbb{Q}(t)$ be defined by

$$x \mapsto \frac{t^2 - 1}{t^2 + 1}, y \mapsto \frac{2t}{t^2 + 1}.$$

Clearly $I \subset \ker \phi$ by the identity

$$(\frac{t^2 - 1}{t^2 + 1})^2 + (\frac{2t}{t^2 + 1})^2 = 1.$$

Therefore ϕ induces a homomorphism $\overline{\phi} : \mathbb{Q}[x, y]/I \to \mathbb{Q}(t)$ by the universal property of quotient rings. To show that this in turn induces a homomorphism from the fraction field of R to $\mathbb{Q}(t)$, we need to show that every nonzero element is mapped to a unit, which is any non-zero element in the field $\mathbb{Q}(t)$. It suffices to show that $\ker(\phi) \subset I$. Suppose not. Take $f \in \mathbb{Q}[x,y]\backslash I$ such that $\phi(f) = 0$. By performing a long division by (x^2+y^2-1) with respect to x, we may assume that $f(x,y)$ is of the form

$$f(x,y) = p(y)x + q(y)$$

where $p, q \in \mathbb{Q}[y]$ are not both 0. Since $\phi(y) \neq 0$, we may further assume that y does not divide p, q simultaneously (otherwise we may replace them by $p/y, q/y$). Write

$$p(y) = \sum_{i=0}^{k} a_i y^i, q(y) = \sum_{j=0}^{m} b_j y^j,$$

then we have

$$\sum_{i=0}^{k} a_i (\frac{2t}{1+t^2})^i \frac{1-t^2}{1+t^2} + \sum_{j=0}^{m} b_j (\frac{2t}{1+t^2})^j = 0$$

as an identity in t. We assume without loss of generality that $k \geq m$. The other case is similar. We multiply both sides by $(1+t^2)^{k+1}$ and rearrange to get

$$(t^2-1)\sum_{i=0}^{k} a_i (2t)^i (1+t^2)^{k-i} = (t^2+1)\sum_{j=0}^{m} b_j (2t)^j (1+t^2)^{k-j}.$$

Now compare the coefficients for the highest term (degree $2k+2$) and the constant term:

$$\begin{cases} a_0 &= b_0, \\ -a_0 &= b_0 \end{cases} \implies a_0 = b_0 = 0.$$

But this means $y \mid p$ and $y \mid q$, a contradiction.

Now by the universal property of the ring of fractions, $\overline{\phi}$ induces a homomorphism $\Phi : Frac(R) \to \mathbb{Q}(t)$.

We then construct its inverse. Define $\psi : \mathbb{Q}[t] \to Frac(R)$ by $t \mapsto \frac{y}{1+x}$. To show that this induces a homomorphism from $\mathbb{Q}(t)$ to $Frac(R)$, we need to show that any nonzero $f \in \mathbb{Q}[t]$ has a nonzero image under ψ. Take any $f = \sum_{i=0}^{k} a_i t^i \in \mathbb{Q}[t]$ such that $\psi(f) = 0$. Then we have

$$\sum_{i=0}^{k} a_i (\frac{y}{1+x})^i = 0 \in Frac(R)$$

$$\implies \sum_{i=0}^{k} a_i(1-x)^i y^{k-i} = 0 \in R.$$

Now replace y^2 by $1 - x^2 = (1+x)(1-x)$, we have

$$\sum_{k-i \text{ even}} a_i(1-x)^{\frac{k+i}{2}}(1+x)^{\frac{k-i}{2}} + \sum_{k-i \text{ odd}} a_i(1-x)^{\frac{k+i-1}{2}}(1+x)^{\frac{k-i-1}{2}} y = 0$$

in R. Since LHS is now a polynomial of degree 1 in y, we must have

$$g(x) = \sum_{k-i \text{ even}} a_i(1-x)^{\frac{k+i}{2}}(1+x)^{\frac{k-i}{2}} = 0$$

and

$$h(x) = \sum_{k-i \text{ odd}} a_i(1-x)^{\frac{k+i-1}{2}}(1+x)^{\frac{k-i-1}{2}} = 0$$

as polynomials in $\mathbb{Q}[x]$. Apply the automorphism of $\mathbb{Q}[x]$ sending x to $x-1$ on g and h, we see that the images

$$\tilde{g}(x) = \sum_{k-i \text{ even}} a_i(2-x)^{\frac{k+i}{2}} x^{\frac{k-i}{2}} = 0$$

and

$$\tilde{h}(x) = \sum_{k-i \text{ odd}} a_i(2-x)^{\frac{k+i-1}{2}} x^{\frac{k-i-1}{2}} = 0.$$

Consider the coefficients of the constant terms in both polynomials and setting them to 0 (consider the summands with $i = k$ and $i = k-1$ resp.):

$$\begin{cases} 2^k a_k = 0, \\ 2^{k-1} a_{k-1} = 0 \end{cases} \implies a_k = a_{k-1} = 0.$$

Apply this argument inductively, we see that we must have $a_i = 0$ for all i and so $f = 0 \in \mathbb{Q}[t]$. Then ψ induces $\Psi : \mathbb{Q}(t) \to Frac(R)$.

To show that Φ and Ψ are homomorphisms, it suffices to show that $\Phi \circ \Psi = id_{\mathbb{Q}(t)}$ and $\Psi \circ \Phi = id_{Frac(R)}$.

$$\begin{aligned} \Phi \circ \Psi(t) &= \Phi\left(\frac{y}{1+x}\right) = \phi(y)\phi(1+x)^{-1} \\ &= \frac{2t}{1+t^2}\left(1 + \frac{1-t^2}{1+t^2}\right)^{-1} = \frac{2t}{1+t^2} \cdot \frac{1+t^2}{2} = t. \end{aligned}$$

This shows that the subfield of $\mathbb{Q}(t)$ fixed by the field homomorphism $\Phi \circ \Psi$ contains t. $\mathbb{Q}$ is clearly also fixed by both homomorphisms. Therefore this subfield must be the whole $\mathbb{Q}(t)$. On the other hand,

$$\begin{aligned}\Psi \circ \Phi(x) &= \Psi(\frac{1-t^2}{1+t^2}) = (1-(\frac{y}{1+x})^2)/(1+(\frac{y}{1+x})^2) \\ &= \frac{(1+x)^2-y^2}{(1+x)^2+y^2} = \frac{2x+2x^2)}{2x+2} = x,\end{aligned}$$

where we replaced y^2 with $1-x^2$. Similarly,

$$\begin{aligned}\Psi \circ \Phi(y) &= \Psi(\frac{2t}{1+t^2}) = (2\frac{y}{1+x})/(1+(\frac{y}{1+x})^2) \\ &= \frac{2y(1+x)}{(1+x)^2+y^2} = \frac{2y(1+x)}{2x+2} = y.\end{aligned}$$

This shows that the subfield of $Frac(R)$ fixed by the field homomorphism $\Psi \circ \Phi$ contains the generators x and y and thus must be the whole $Frac(R)$. This completes the proof.

Below are two remarks from Prof Chin Chee Whye.

Remark 1 *To see the result more directly, notice that R is the coordinate ring of a plane conic (degree 2 curve), whereas $\mathbb{Q}[t]$ is the coordinate ring of the affine line; both curves are of genus 0 and each has at least one rational point, so their function fields are isomorphic.*

Remark 2 *Let $J = \ker(\phi)$. To show that $J = I$ without doing the computations, we use the fact that $\mathbb{Q}[x, y]$ is of Krull dimension 2 (A-M, chap.11, example after theorem 11.14). Suppose on the contrary that J is strictly larger than I. Then $(0) \subset I \subset J$ would be a chain of prime ideals of length 2, which means that J is a maximal ideal of $\mathbb{Q}[x, y]$, and hence the image of ϕ would be a certain subfield F of $\mathbb{Q}(t)$. By a version of the Nullstellensatz (A-M, chap.5, exerc.18), this F would be a field extension of finite dimension over $\mathbb{Q}$, and contained in $\mathbb{Q}(t)$. Since $\mathbb{Q}(t)$ is purely transcendental over $\mathbb{Q}$, the only finite (or algebraic) extension of $\mathbb{Q}$ contained in $\mathbb{Q}(t)$ is $\mathbb{Q}$ itself — i.e. we must have $F = \mathbb{Q}$. The images of x and y under ϕ are therefore certain rational numbers x_0 and y_0, but this means $(1-t^2)/(1+t^2) = x_0$ and $2t/(1+t^2) = y_0$ as rational functions of t, which is a contradiction.*

Q4

(a)

Let $\pi : P \mapsto P/M$ be the projection. Let $\{m_1, \cdots, m_k\}$ be a set of generators for M, and $\{\overline{p_1}, \cdots, \overline{p_n}\}$ be a set of generators for P/M. Suppose

$$\overline{p_i} = \pi(p_i), \quad \forall\, i \in \{1, \cdots n\}.$$

Then $\{m_1, \cdots, m_k, p_1, \cdots, p_n\}$ generates P. Indeed, for any $p \in P$, we first have

$$\pi(p) = \sum_{i=1}^{n} r_i \overline{p_i}$$

for some $r_i \in R$. Since

$$\pi\left(\sum_{i=1}^{n} r_i p_i\right) = \sum_{i=1}^{n} r_i \pi(p_i) = \sum_{i=1}^{n} r_i \overline{p_i},$$

there exists $m \in M$ such that $p = \sum_{i=1}^{n} r_i p_i + m$. By writing

$$m = \sum_{j=1}^{k} s_j m_j$$

for some $s_j \in R$, we have

$$p = \sum_{i=1}^{n} r_i p_i + \sum_{j=1}^{k} s_j m_j$$

as desired.

(b)

Without loss of generality, we will only prove that M is finitely generated. By the lattice isomorphism theorem, $(M+N)/N \cong M/(M \cap N)$. As $M+N$ is finitely generated, $(M+N)/N$ is finitely generated and thus $M/(M \cap N)$ is also finitely generated. Notice that $M \cap N$ is finitely generated. By (a), M is finitely generated.

Q5

Since $\mathbb{Z}$ is a P.I.D., $A \in M_d(\mathbb{Z})$ has a Smith normal form

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} = PAQ$$

where $P, Q \in GL_d(\mathbb{Z})$, $D = diag(a_1, \cdots, a_k)$ is such that $a_1 | a_2 | \cdots | a_k$, $a_k \neq 0$ and $k \leq d$. Let $B = PAQ$. Then

$$M = \mathbb{Z}^d / \mathrm{Im}(A) \cong \mathbb{Z}^d / \mathrm{Im}(B) = \mathbb{Z}/(a_1) \times \cdots \times \mathbb{Z}/(a_k) \times \mathbb{Z}^{d-k}.$$

Therefore

$$\begin{aligned} M \text{ is finite} &\iff d - k = 0 \\ &\iff \det(B) \neq 0 \\ &\iff \det(A) \neq 0. \end{aligned}$$

When this is the case,

$$|M| = |\mathbb{Z}/(a_1)| \times \cdots \times |\mathbb{Z}/(a_k)| = |a_1| \times \cdots \times |a_k| = |\det(B)| = |\det(A)|.$$