MA3201 Algebra II Suggested Solutions

AY20/21 Semester 2

Author: Chong Jing Quan   Reviewer: Pan Jing Bin

Question 1

Determine whether the following statements are TRUE or FALSE. You do NOT need to justify your answer.

Note: Justifications included for clarity.

(1) *Any finite integral domain is a field.*

True. Let R be a finite integral domain and let a be a non-zero element of R. By the cancellation law, the map $x \mapsto ax$ from R to itself is injective. As R is finite, it follows that the map is surjective too. In particular, one finds $b \in R$ so that $ab = 1$. Hence, a is a unit, and since a is arbitrary, R is a field.

(2) *Let F be a field. Then any subgroup $G \subset F^*$ of the multiplicative group is cyclic.*

False. Take $F = \mathbb{R}$. Then $\mathbb{Q}^* \subset \mathbb{R}^*$ but $\mathbb{Q}^*$ is not cyclic.

(3) *The abelian group $\mathbb{Q}$ is finitely generated as a $\mathbb{Z}$-module.*

False. Suppose otherwise and write $\mathbb{Q} = \mathbb{Z}A$ with $A = \{a_1, a_2, \cdots, a_n\} \subseteq \mathbb{Q}$. For each $1 \leq i \leq n$, put $a_i = \frac{p_i}{q_i}$ for some $p_i, q_i \in \mathbb{Z}$. Then the rational $\frac{1}{q_1 q_2 \cdots q_n + 1}$ is not in $\mathbb{Z}A$, contradiction.

Question 2

Let $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \{a + b\frac{1+\sqrt{5}}{2} \mid a, b \in \mathbb{Z}\}$ be a subring of $\mathbb{R}$. And let $R = \{\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \mid a, b \in \mathbb{Z}\}$ be a subring of $Mat_{2\times 2}(\mathbb{Z})$. Prove that $R \cong \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ as rings.

Consider the map $\phi : R \to \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ by

$$\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \mapsto a + b\frac{1+\sqrt{5}}{2}.$$

This map is clearly well-defined. We first prove the bijectivity of ϕ. The surjectivity of ϕ follows from definition. For injectivity, suppose one has

$$\phi\left(\begin{pmatrix} c & d \\ d & c+d \end{pmatrix}\right) = \phi\left(\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}\right) = a + b\frac{1+\sqrt{5}}{2}.$$

But $\phi\left(\begin{pmatrix} c & d \\ d & c+d \end{pmatrix}\right) = c + d\frac{1+\sqrt{5}}{2}$, so $a = c$ and $b = d$.

We now check that ϕ is a ring homomorphism. One has

$$\begin{aligned}
\phi\left(\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} + \begin{pmatrix} c & d \\ d & c+d \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} a+c & b+d \\ b+d & (a+c)+(b+d) \end{pmatrix}\right) \\
&= (a+c) + (b+d)\left(\frac{1+\sqrt{5}}{2}\right) \\
&= \left(a + b\frac{1+\sqrt{5}}{2}\right) + \left(c + d\frac{1+\sqrt{5}}{2}\right) \\
&= \phi\left(\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}\right) + \phi\left(\begin{pmatrix} c & d \\ d & c+d \end{pmatrix}\right).
\end{aligned}$$

One also has

$$\begin{aligned}
\phi\left(\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}\begin{pmatrix} c & d \\ d & c+d \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} ac+bd & ad+bc+bd \\ bc+ad+bd & bd+(a+b)(c+d) \end{pmatrix}\right) \\
&= \phi\left(\begin{pmatrix} ac+bd & ad+bc+bd \\ ad+bc+bd & bd+ac+ad+bc+bd \end{pmatrix}\right) \\
&= (ac+bd)+(ad+bc+bd)\left(\frac{1+\sqrt{5}}{2}\right)
\end{aligned}$$

and

$$\begin{aligned}
\phi\left(\begin{pmatrix} a & b \\ b & a+b \end{pmatrix}\right)\phi\left(\begin{pmatrix} c & d \\ d & c+d \end{pmatrix}\right) &= \left(a+b\frac{1+\sqrt{5}}{2}\right)\left(c+d\frac{1+\sqrt{5}}{2}\right) \\
&= ac+ad\frac{1+\sqrt{5}}{2}+bc\frac{1+\sqrt{5}}{2}+bd\left(\frac{1+\sqrt{5}}{2}\right)^2 \\
&= ac+ad\frac{1+\sqrt{5}}{2}+bc\frac{1+\sqrt{5}}{2}+bd\frac{3+\sqrt{5}}{2} \\
&= ac+ad\frac{1+\sqrt{5}}{2}+bc\frac{1+\sqrt{5}}{2}+bd+bd\frac{1+\sqrt{5}}{2} \\
&= (ac+bd)+(ad+bc+bd)\left(\frac{1+\sqrt{5}}{2}\right).
\end{aligned}$$

Thus, ϕ is a ring isomorphism and so $R \cong \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Question 3

Let R be a commutative ring with $1 \neq 0$. Prove that if the nilradical of R is a maximal ideal, then every zero divisor in R is nilpotent.

Let $\mathfrak{N}(R)$ be the nilradical of R. If $\mathfrak{N}(R) = \{0\}$, then R is a field and the statement is trivially true.

Otherwise, this forces $\mathfrak{N}(R)$ to be the unique maximal ideal in R. Indeed, suppose there is another ideal $M \neq \mathfrak{N}(R)$ that is maximal in R, so that M is prime too. Then, as the commutativity of R gives

$$\mathfrak{N}(R) = \bigcap_{P \text{ is a prime ideal of } R} P,$$

we have $\mathfrak{N}(R) \subseteq M$, a contradiction as M and $\mathfrak{N}(R)$ are both maximal ideals and $M \neq \mathfrak{N}(R)$.

Hence R is a local ring, so that $R - \mathfrak{N}(R)$ consists of elements that are units, while $\mathfrak{N}(R)$ consists of all elements that are not units. Thus, $\mathfrak{N}(R)$ includes all zero divisors and we are done.

Question 4

Let R be an integral domain. Let P be a prime ideal. Let $D = R - P$.

(1) *Prove that D is multiplicatively closed, that is if $a, b \in D$, then $ab \in D$.*

If $a, b \in D$, then $a, b \notin P$, so that $ab \notin P$. This gives $ab \in D$.

(2) *Let $D^{-1}R$ be the localization of R with respect to D. Prove that $D^{-1}R$ is a local ring, that is, it contains a unique maximal ideal.*

Let N be the set of non-units in $D^{-1}R$. It suffices to show that N is an ideal of $D^{-1}R$. To do so, we first prove a lemma.

Lemma. Let $\frac{a}{b} \in D^{-1}R$. Then $\frac{a}{b} \in N$ if and only if $a \in P$.

Proof. We first show that the lemma is independent of the representative, i.e. if $\frac{a}{b} = \frac{c}{d}$ with $\frac{a}{b} \in N$, then $a \in P \iff c \in P$. Note that the equality above implies $ad = bc$, with $b, d \notin P$. If $a \in P$, then $c \in P$ and vice versa.

Suppose that $a \notin P$, i.e. $a \in D$. Then, the element $\frac{b}{a} \in D^{-1}R$ is an inverse of $\frac{a}{b}$, so that $\frac{a}{b}$ is a unit.

On the other hand, suppose $a \in P$ and assume for the sake of contradiction that $\frac{a}{b}$ is invertible. Let $\frac{u_1}{u_2}$ be its inverse, so that $\frac{a}{b}\frac{u_1}{u_2} = 1 \implies au_1 = bu_2$. From (1), we know that $bu_2 \in D$, but $au_1 \in P$ since P is an ideal. As P is prime, we have $b \in P$ or $u_2 \in P$, a contradiction. □

We now proceed to show that N is an ideal. Let $\frac{a}{b}, \frac{c}{d} \in N$. We first verify that N is a subring of $D^{-1}R$. Since $\frac{a}{b} - \frac{c}{d} = \frac{a}{b} + \frac{-c}{d} = \frac{ad-bc}{bd}$ with $ad - bc \in P$ and $bd \in D$, we see that N is a subgroup of $D^{-1}R$. Then, if $p \in D$, then $\frac{p}{q} \notin N$. As $\frac{c}{d}\frac{a}{b} = \frac{ca}{db}$ with $ca \in P$ and $db \in D$, we conclude that N is an ideal of R.

As such, $D^{-1}R$ is a local ring.

Question 5

Let $f(x) = x^6 + 30x^5 - 15x^3 + 6x - 120 \in \mathbb{Z}[x]$. Prove that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Note that f is monic, 3 divides all the non-leading coefficients but 9 does not divide -120. By Eisenstein's Criterion, f is irreducible in $\mathbb{Z}[x]$.

Question 6

Let

$$A = \begin{pmatrix} -2 & 1 & 4 \\ -5 & 2 & 5 \\ -1 & 1 & 3 \end{pmatrix} \in Mat_{3\times 3}(\mathbb{C}).$$

Find both the rational canonical form and the Jordan Canonical Form of A.

A direct computation shows that the Smith Normal Form of $xI - A$ is given by $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x-2)^2(x+1) \end{pmatrix}$.

Thus, we have $\mathbb{C}^3 \cong \mathbb{C}[x]/((x-2)^2(x+1)) \cong \mathbb{C}[x]/(x^3 - 3x^2 + 4)$.

The rational canonical form of A is then given by

$$\begin{pmatrix} 0 & 0 & -4 \\ 1 & 0 & 0 \\ 0 & 1 & 3 \end{pmatrix}.$$

The Jordan Canonical Form of A is given by

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

as $\mathbb{C}^3 \cong \mathbb{C}[x]/((x-2)^2(x+1)) \cong \mathbb{C}[x]/((x-2)^2) \oplus \mathbb{C}[x]/((x+1))$.

Question 7

Let $A \in Mat_{n\times n}(\mathbb{C})$. Prove that there exists $B, C \in Mat_{n\times n}(\mathbb{C})$ satisfying the following properties:

(1) $A = B + C$;

(2) $BC = CB$;

(3) B is diagonalizable;

(4) C is nilpotent.

As A is a complex-valued matrix, we can write A in its Jordan Canonical Form as follows.

$$A = P \begin{pmatrix} J_{n_1}(\lambda_1) & & & 0 \\ & J_{n_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & J_{n_k}(\lambda_k) \end{pmatrix} P^{-1}.$$

We also have

$$\begin{aligned} A &= P \begin{pmatrix} J_{n_1}(\lambda_1) & & & 0 \\ & J_{n_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & J_{n_k}(\lambda_k) \end{pmatrix} P^{-1} \\ &= P \begin{pmatrix} J_{n_1}(0) + \lambda_1 I_{n_1} & & & 0 \\ & J_{n_2}(0) + \lambda_2 I_{n_2} & & \\ & & \ddots & \\ 0 & & & J_{n_k}(0) + \lambda_k I_{n_k} \end{pmatrix} P^{-1} \\ &= P \begin{pmatrix} J_{n_1}(0) & & & 0 \\ & J_{n_2}(0) & & \\ & & \ddots & \\ 0 & & & J_{n_k}(0) \end{pmatrix} P^{-1} + P \begin{pmatrix} \lambda_1 I_{n_1} & & & 0 \\ & \lambda_2 I_{n_2} & & \\ & & \ddots & \\ 0 & & & \lambda_k I_{n_k} \end{pmatrix} P^{-1}. \end{aligned}$$

Now, put

$$B = P \begin{pmatrix} \lambda_1 I_{n_1} & & & 0 \\ & \lambda_2 I_{n_2} & & \\ & & \ddots & \\ 0 & & & \lambda_k I_{n_k} \end{pmatrix} P^{-1} \text{ and } C = P \begin{pmatrix} J_{n_1}(0) & & & 0 \\ & J_{n_2}(0) & & \\ & & \ddots & \\ 0 & & & J_{n_k}(0) \end{pmatrix} P^{-1}.$$

Note that B is diagonalizable by definition and C is nilpotent since $C^{n_1+n_2+\cdots+n_k} = 0$. Furthermore, B and C commute since B and C are simply block diagonal matrices and $J_{n_i}(0)$ and $\lambda_i I_{n_i}$ commute for each i. We are done.