MAGIC073 – Commutative algebra – EXAM 24-25 SOLUTIONS

[Marks: unless otherwise stated, marks are awarded proportionally to the correctness of the answer written. Any correct answers are given full credit. Note that the exam questions aren't difficult, but some require students to find a correct idea, or example, and they must also know and understand the content of the course]

Question 1. Are the following true or false? Briefly prove your claims. If you refer to results in the lecture notes, you must indicate which one(s) precisely.

i. Let R, S be commutative rings. Every prime ideal of $R \times S$ is of the form $P \times Q$, where $P \in \mathrm{Spec}(R)$ and $Q \in \mathrm{Spec}(S)$. [2]

ii. Let R be a commutative ring and let I, J be ideals of R. Then $R/IJ \cong R/I \times R/J$ as rings. [2]

iii. The quotient ring $\mathbb{Z}[x,y]/(x^2 - y^3)$ is Noetherian. [2]

iv. Let S be an extension ring of R, with S commutative. Then $\mathrm{Rad}(R) \subseteq \mathrm{Rad}(S)$. [2]

v. Let R be a commutative ring, let F, M, N be finitely generated R-modules. Suppose that F is free and that $f \in \mathrm{Hom}_R(M, N)$ is injective. Then the induced R-homomorphism $f_* \in \mathrm{Hom}_R(F \otimes_R M, F \otimes_R N)$ is injective, where $f_*(x \otimes y) = x \otimes f(y)$ for all $x \otimes y \in F \otimes_R M$. [2]

vi. Every principal fractional ideal in a PID is invertible. [2]

vii. $\mathbb{Z}[i\sqrt{5}]$ is a PID. [2]

viii. $\mathbb{Z}[x,y]$ is integrally closed. [2]

Solution. [Any correct answer with correct proof 2 marks. Zero for anything else.]

i. FALSE: e.g. $R = S = \mathbb{Z}$, $P = Q = 2\mathbb{Z}$. Then $(R \times S)/(P \times Q) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ is not an ID. [2]

ii. FALSE: e.g. $R = \mathbb{Z}$ and $I = J = 2\mathbb{Z}$. Then $R/IJ = \mathbb{Z}/4 \ncong \mathbb{Z}/2 \times \mathbb{Z}/2 = R/I \times R/J$. [2]

iii. TRUE: by Hilbert's basis theorem (Thm 2.48), $\mathbb{Z}[x,y]$ is Noetherian. Now note that any quotient ring R/I of a Noetherian ring R is Noetherian too since any ascending chain of ideals in R/I lifts to an ascending chain of ideals in R and therefore must stabilise (by definition of Noetherian ring). [2]

iv. FALSE: e.g. in the ring extension $\mathbb{Z}_{(p)} \subset \mathbb{Q}$, we have $\mathrm{Rad}(\mathbb{Z}_{(p)}) = p\mathbb{Z}_{(p)}$, whereas $\mathrm{Rad}(\mathbb{Q}) = (0)$. [2]

v. TRUE: if n is the rank of F, then $F \cong R^n$ is isomorphic to the direct sum of n copies of R. So $F \otimes_R M \cong \oplus_1^n R \otimes_R M \cong \oplus_1^n M$, similarly for $F \otimes_R N$ and under these isomorphisms, $f_* : F \otimes_R M \to F \otimes N$ is $\oplus_1^n (f : M \to N)$. [2]

vi. TRUE: a principal fractional ideal is finitely generated and a PID is Noetherian. So by remark 3.21, such fractional ideal is invertible. [2]

vii. FALSE: $\mathbb{Z}[i\sqrt{5}]$ has irreducible elements which are not prime. E.g. $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ with $1 \pm i\sqrt{5}$ irreducible (seen by solving $1 \pm i\sqrt{5} = (a + bi\sqrt{5})(c + di\sqrt{5})$ or otherwise) but not prime since $1 \pm i\sqrt{5} \nmid 2$ (routine checks). (Alternatively, use the norm: $|1 \pm \sqrt{5}| = 6 = 2 \cdot 3$, which are not quadratic residue mod 5 and therefore no element of $\mathbb{Z}[i\sqrt{5}]$ has norm 2 or 3.) [2]

viii. TRUE: $\mathbb{Z}[x,y]$ is a UFD and by Prop 3.5 any UFD is integrally closed. [2]

Question 2.

i. Let $R = \mathbb{Z}/7[x]$ and let $I = (x^2 + 2)$. Let $\pi : R \to R/I$ denote the quotient map and write $\pi(f) = \overline{f}$ for all $f \in R$.

(a) Prove that R/I is a field. [2]

(b) Find $(\overline{x}^3)^{-1}$ in R/I. [4]

(c) Calculate the fractional ideal I^{-1} and decide whether I is invertible. Prove your answers. [2]

ii. Describe $\mathrm{Spec}(\mathbb{Z}/10 \times \mathbb{Z}/21)$ by listing its clopen sets in the Zariski topology and give the connected components. Explain your method. [12]

Solution.

i. (a) I is a maximal ideal of R since R is a PID and $x^2 + 2$ is irreducible. (Otherwise, $x^2 + 2 = (x + a)(x - a)$ for $a \in \mathbb{Z}/7$, i.e. $a^2 = 5$ in $\mathbb{Z}/7$, but the only squares are $0, 1, 2, 4$.) [2]

(b) Note that $x^3 = x(x^2 + 2) - 2x$, and so $\overline{x}^3 = -\overline{2x} \in R/I$. The Euclidean algorithm (or otherwise) yields $1 = 5x(2x) + 4(x^2 + 2)$ in $\mathbb{Z}/7[x]$, showing that $(\overline{x}^3)^{-1} = \overline{5x}$. [4]

(c) The field of fraction of R is $\mathbb{Z}/7(x)$. We have $\frac{1}{(x^2+1)} I = R$ since $1 = \frac{(x^2+1)}{(x^2+1)}$. So $I^{-1} = \frac{1}{(x^2+1)} R$ and I is invertible. [2]

ii. The points of $\mathrm{Spec}(\mathbb{Z}/10 \times \mathbb{Z}/21)$ are

$$\{I_2 = (2) \times \mathbb{Z}/21,\ I_5 = (5) \times \mathbb{Z}/21,\ J_3 = \mathbb{Z}/10 \times (3),\ J_7 = \mathbb{Z}/10 \times (7)\}.$$

We find the idempotents of $\mathbb{Z}/10 \times \mathbb{Z}/21$. They are of the form (e, f) with $e \in \{0, 1, 5, 6\}$ and $f \in \{0, 1, 7, 15\}$. There are therefore 16 clopen sets:

$$U_{(0,0)} = \emptyset,\ U_{(0,1)} = \{J_3, J_7\},\ U_{(1,0)} = \{I_2, I_5\},\ U_{(1,1)} = \mathrm{Spec}(R),$$

$$U_{(5,0)} = \{I_2\},\ U_{(5,1)} = \{I_2, J_3, J_7\},\ U_{(6,0)} = \{I_5\},\ U_{(6,1)} = \{I_5, J_3, J_7\},$$

$$U_{(0,7)} = \{J_3\},\ U_{(1,7)} = \{I_2, I_5, J_3\},\ U_{(0,15)} = \{J_7\},\ U_{(1,15)} = \{I_2, I_5, J_7\},$$

$$U_{(5,7)} = \{I_2, J_3\},\ U_{(5,15)} = \{I_2, J_7\},\ U_{(6,7)} = \{I_5, J_3\},\ U_{(6,15)} = \{I_5, J_7\}.$$

[8]

The connected components of $\mathrm{Spec}(\mathbb{Z}/10 \times \mathbb{Z}/21)$ are

$$U_{(5,0)} \sqcup U_{(6,0)} \sqcup U_{(0,7)} \sqcup U_{(0,15)}.$$

[4]

Question 3.

i. Let R be a nontrivial commutative ring in which every proper ideal is prime. Prove that R is a field.[2]

ii. Consider the ring extension $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{3}]$, and the ideal (11) of $\mathbb{Z}$. Find all the prime ideals I of $\mathbb{Z}[\sqrt{3}]$ lying over (11), i.e. such that $I \cap \mathbb{Z} = (11)$. You may assume without proof that $\mathbb{Z}[\sqrt{3}]$ is a PID, and that if $a + b\sqrt{3}$ is such that $\pm(a^2 - 3b^2)$ is a prime integer, then $a + b\sqrt{3}$ is irreducible in $\mathbb{Z}[\sqrt{3}]$. [3]

iii. Let R be the subring of the polynomial ring $\mathbb{Z}[x, y]$ formed by the polynomials of the form $\sum_{i,j} a_{ij} x^i y^j$ such that $a_{0,1} = 0$; that is, the term of degree 1 in y is divisible by x. Let $I = (xy, y^2)$. Prove that R is not a PID and that I^2 is not primary. [5]

iv. Let $K = \mathbb{Q}(\sqrt{5})$ be the field of fractions of $R = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$. Find the integral closure of R in K. [10]

Solution.

i. By assumption, $(0) \neq R$ is prime, and so R is an ID. Let $0 \neq a \in R$. Then $a \in R^\times$ or (a) is prime. If we suppose that $a \notin R^\times$, then $(0) \subsetneq (a^n) \subseteq (a)$, and every (a^n) is prime. But (a^2) cannot be prime since $a \notin (a^2)$ and $a \cdot a \in (a^2)$. Hence any nonzero element is invertible. [2]

ii. Recall that $\mathbb{Z}[\sqrt{3}]$ is a PID (in fact an ED), and that $(11) \in \operatorname{Spec}(\mathbb{Z})$. Since $-11 = (8+5\sqrt{3})(8-5\sqrt{3}) = 8^2 - 3 \cdot 5^2$ in $\mathbb{Z}[\sqrt{3}]$, then $(11) \notin \operatorname{Spec}(\mathbb{Z}[\sqrt{3}])$, and $8 \pm 5\sqrt{3}$ is irreducible, hence prime (by hint). Therefore there are exactly two prime ideals of $\mathbb{Z}[\sqrt{3}]$ lying over (11), namely $(8 \pm 5\sqrt{3})$. [3]

iii. Note that R is not a UFD since $x^2y^2 = (xy)^2 = xx(y^2)$, with x irreducible but x is not prime since x does not divide xy in R. A fortiori, R is not a PID either. We have $I^2 = (x^2y^2, xy^3, y^4)$. In the quotient R/I^2, the multiplication by x map is neither injective nor nilpotent. Indeed, $xy^2 \notin I^2$ and $x^2y^2 \in I^2$ (not injective), but $x^i \notin I^2$ for any $i \geq 1$ (not nilpotent). [5]

iv. Let $\overline{\mathbb{Z}}$ denote the integral closure of $\mathbb{Z}$ in K. We claim that $\overline{\mathbb{Z}} = \mathbb{Z} + \mathbb{Z}\big(\frac{1}{2}(1 + \sqrt{5})\big)$ as $\mathbb{Z}$-module.

Proof: Since $\sqrt{5} = 5 \in \mathbb{Z}$, every element of $K = \mathbb{Z}(\sqrt{5})$ that is integral over $\mathbb{Z}$ is the root of a quadratic polynomial in $\mathbb{Z}[x]$, and $a + b\sqrt{5} \in \overline{\mathbb{Z}}$ if and only if $a - b\sqrt{5} \in \overline{\mathbb{Z}}$.

Now, $\frac{1}{2}(1 \pm \sqrt{5})$ is a root of $x^2 - x - 1 \in \mathbb{Z}[x]$ and therefore is integral over $\mathbb{Z}$, which proves the inclusion $\mathbb{Z} + \mathbb{Z}\big(\frac{1}{2}(1 + \sqrt{5})\big) \subseteq \overline{\mathbb{Z}}$.

Conversely, recall that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ since $\mathbb{Z}$ is a UFD. Let $u + v\sqrt{5} \in \overline{\mathbb{Z}}$, where $u, v \in \mathbb{Q}$. We want to show that $u, v \in \mathbb{Z}[\frac{1}{2}]$ with $u - v \in \mathbb{Z}$ (or equivalently, if $u = \frac{a}{2}$ and $v = \frac{b}{2}$, then $a, b \in \mathbb{Z}$ have the same parity).

We calculate $(u + v\sqrt{5})(u - v\sqrt{5}) = u^2 - 5v^2$ and $(u + v\sqrt{5}) + (u - v\sqrt{5}) = 2u$. Therefore, we must have $u^2 - 5v^2, 2u \in \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$ since $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. From $2u \in \mathbb{Z}$, it follows that $u \in \mathbb{Z}[\frac{1}{2}]$, and since $u^2 - 5v^2 \in \mathbb{Z}$, we must have $v \in \mathbb{Z}[\frac{1}{2}]$ too. Write $u = \frac{a}{2}$ and $v = \frac{b}{2}$ with $a, b \in \mathbb{Z}$. Hence, $u^2 - 5v^2 = \frac{1}{4}(a^2 - 5b^2) \in \mathbb{Z}$ implies $a^2 - 5b^2 \in 4\mathbb{Z}$, which forces a and b to have the same parity.

[10]

Question 4. Let R be a commutative ring.

i. Let I, J be ideals of R such that $I \cap J = (0)$. Suppose that R/I and R/J are Noetherian. Prove that R is Noetherian. [5]

ii. Let S be a commutative ring and let $\varphi : R \to S$ be a surjective ring homomorphism.

(a) Prove that $\varphi(\mathrm{Rad}(R)) \subseteq \mathrm{Rad}(S)$. [5]

(b) Find an example with $\varphi(\mathrm{Rad}(R)) \subsetneq \mathrm{Rad}(S)$. [4]

iii. Let M be a simple R-module, that is, the only submodules of M are M and $\{0\}$. Let $I = \{a \in R \mid ax = 0,\ \forall\, x \in M\}$ be the annihilator of M in R. Prove that $I \in \mathrm{MaxSpec}(R)$. [8]

Solution.

i. Consider the R-homomorphism $\pi : R \to R/I \oplus R/J$ where $\pi(a) = (a + I, a + J)$. Since $\ker(\pi) = I \cap J = (0)$, then π is injective. So R is isomorphic to an R-submodule of a Noetherian R-module, since a finite direct sum (or cartesian product) of Noetherian modules is Noetherian (thm 2.42). [5]

ii. Let S be a commutative ring and let $\varphi : R \to S$ be a surjective ring homomorphism.

(a) Let $Q \in \mathrm{MaxSpec}(S)$, so that S/Q is a field. The composition $\overline{\varphi} = \pi\varphi : R \to S \to S/Q$ is surjective, where π is the quotient map. So $\ker(\overline{\varphi}) \in \mathrm{MaxSpec}(R)$ (by the first isomorphism theorem), i.e. $\overline{\varphi}^{-1}(Q) \in \mathrm{MaxSpec}(R)$ for all $Q \in \mathrm{MaxSpec}(S)$. A fortiori, [5]

$$\mathrm{Rad}(S) = \bigcap_{Q \in \mathrm{MaxSpec}(S)} Q = \bigcap_{Q \in \mathrm{MaxSpec}(S)} \varphi\big(\varphi^{-1}(Q)\big) \supseteq \bigcap_{P \in \mathrm{MaxSpec}(R)} \varphi(P) \supseteq \varphi(\mathrm{Rad}(R)).$$

(b) Let $\varphi : \mathbb{Z} \to \mathbb{Z}/4$ be the quotient map. Then, $\varphi(\mathrm{Rad}(R)) = \varphi((0)) = (\overline{0}) \subsetneq (\overline{2}) = \mathrm{Rad}(S)$, where we write $\overline{a}$ the elements in $\mathbb{Z}/4$ to avoid any confusion. [4]

iii. Let M be a simple R-module, and let $I = \{a \in R \mid ax = 0,\ \forall\, x \in M\}$. Note that I is an ideal of R (easy check). Let $0 \neq x \in M$. Since $\{0\} \neq Rx \subseteq M$ is an R-submodule of M and M is simple, we must have $Rx = M$, and $I = \{a \in R \mid ax = 0\}$, so that $M \cong R/I$ as an R-module. Now, for any ideal J of R containing I properly, the quotient R/J is a proper quotient module of M. But M being simple, the only possibility is $R/J = 0$, i.e. $R = J$. Therefore I is a maximal ideal of R. [8]

Question 5.

i. Let R be a commutative ring and let M, N be R-modules.

(a) Let I be an ideal of R and suppose that M is finitely generated. Prove that $\sqrt{\mathrm{Ann}(M/IM)} = \sqrt{\mathrm{Ann}(M) + I}$ in R. Recall that $\mathrm{Ann}(V) = \{a \in R \mid ax = 0,\ \forall\, x \in V\}$ for any R-module V. [5]

(b) Suppose that $M \cap N$ and $M + N$ are finitely generated. Prove that M and N are both finitely generated. [4]

(c) Let $\pi : R \to R/\mathrm{Rad}(R)$ be the quotient map. Suppose that M is finitely generated, and that there is a subset X of M such that $\pi(X)$ generates $\pi(M)$. Prove that X generates M. [3]

ii. Let R be a Noetherian ring and let $M, N_0, \ldots, N_n, Q_0$ be finitely generated R-modules with Q_0 projective. Suppose that we have a diagram

$$\begin{tikzcd} & & & Q_0 \arrow[r, "d_0"] & M \arrow[r] \arrow[d, "\mathrm{Id}_M"] & 0 \\ N_n \arrow[r, "g_n"] & \cdots \arrow[r] & N_1 \arrow[r, "g_1"] & N_0 \arrow[r, "g_0"] & M \arrow[r] & 0 \end{tikzcd}$$

where the two rows are exact sequences. Prove that we can complete the diagram into a commutative diagram of R-modules and R-homomorphisms

$$\begin{tikzcd}
Q_n \arrow[r, "d_n"] \arrow[d, "f_n"] & \cdots \arrow[r] \arrow[d] & Q_1 \arrow[r, "d_1"] \arrow[d, "f_1"] & Q_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & M \arrow[r] \arrow[d, "\mathrm{Id}_M"] & 0 \\
N_n \arrow[r, "g_n"] & \cdots \arrow[r] & N_1 \arrow[r, "g_1"] & N_0 \arrow[r, "g_0"] & M \arrow[r] & 0
\end{tikzcd}$$

with $Q_1, \ldots, Q_n$ projective R-modules and the two rows are exact sequences. [10]

Solution.

i. Let R be a commutative ring and let M, N be R-modules.

(a) Let $a \in \sqrt{\mathrm{Ann}(M) + I}$. That is, $a^n \in \mathrm{Ann}(M) + I$ for some $n \in \mathbb{N}$, and therefore $a^n M \subseteq IM$ since if $a^n = b + c$ with $b \in \mathrm{Ann}(M)$ and $c \in I$, then $a^n x = cx$ for all $x \in M$. Hence $a^n \in \mathrm{Ann}(M/IM)$, i.e. $a \in \sqrt{\mathrm{Ann}(M/IM)}$, showing the inclusion $\sqrt{\mathrm{Ann}(M) + I} \subseteq \sqrt{\mathrm{Ann}(M/IM)}$. Conversely, if $a \in \sqrt{\mathrm{Ann}(M/IM)}$, say $a^n \in \mathrm{Ann}(M/IM)$, then $a^n M \subseteq IM$. By Proposition 2.21, since M is finitely generated, the multiplication by a^n map on M, let's call it $\mu\,\mathrm{End}_R\, M$, satifies an equation of the form $\mu^k + b_1 \mu^{k-1} + \cdots + b_k = 0$, with $b_i \in I$ for all $1 \leq i \leq k-1$ and some $k \in \mathbb{N}$. It follows that $a^{nk} \in \mathrm{Ann}(M) + I$, and proves that $a \in \sqrt{\mathrm{Ann}(M) + I}$. The converse inclusion follows. [5]

(b) Suppose that $M \cap N = \langle x_1, \ldots, x_n \rangle$ and $M + N = \langle y_1, \ldots, y_t \rangle$ with $y_i = u_i + v_i$, where $u_i \in M$ and $v_i \in N$ for all $1 \leq i \leq t$. We claim that $M = \langle x_1, \ldots, x_n, u_1, \ldots, u_t \rangle$. Indeed, if $u \in M$, then $u \in M + N$ and so $u = \sum_i a_i(u_i + v_i) = \sum_i a_i u_i + \sum_i a_i v_i$ for some $a_i \in R$. Note that $u - \sum_i a_i u_i = \sum_i a_i v_i = \sum_j b_j x_j \in M \cap N$ for some $b_j \in R$. Therefore, $u = u - \sum_i a_i u_i + \sum_i a_i u_i = \sum_j b_j x_j + \sum_i a_i u_i \in \langle x_1, \ldots, x_n, u_1, \ldots, u_t \rangle$. Similarly for N. [4]

ii. Write with an overbar the images in $\overline{R} = R/\mathrm{Rad}(R)$. Suppose that $\overline{M} = \langle \overline{X} \rangle$ with X finite and M is finitely generated. So $Y = \pi^{-1}(\overline{X}) = \{x + \mathrm{Rad}(R) \mid x \in X\}$ generates M, that is, $M = \langle X \rangle + \mathrm{Rad}(R)M$. By Nakayama's lemma, we must have $M = \langle X \rangle$ (Corollary 2.26). [3]

iii. Since Q_0 is projective, there exists $f_0 \in \mathrm{Hom}_R(Q_0, N_0)$ such that $d_0 = g_0 f_0$, i.e. we have a commutative diagram with exact rows

$$\begin{tikzcd}
 & 0 \arrow[r] & \ker(d_0) \arrow[r] & Q_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & M \arrow[r] \arrow[d, "\mathrm{Id}_M"] & 0 \\
N_n \arrow[r, "g_n"] & \cdots \arrow[r] & N_1 \arrow[r, "g_1"] & N_0 \arrow[r, "g_0"] & M \arrow[r] & 0
\end{tikzcd}$$

Since $\ker(d_0)$ is finitely generated (R is Noetherian), there exists a finitely generated projective (or free) R-module Q_1 and a surjective R-homomorphism $d_1 : Q_1 \to \ker(d_0)$. The equality $d_0 = g_0 f_0$ shows that $f_0(x) \in \ker(g_0)$ for all $x \in \ker(d_0)$, and so f_0 restricts to an R-hom $f_0 : \ker(d_0) \to \mathrm{im}(g_1)$, since $\mathrm{im}(g_1) = \ker(g_0)$. Hence, we have a diagram with exact bottom row

$$\begin{tikzcd}
 & Q_1 \arrow[d, "f_0 d_1"] & \\
N_1 \arrow[r, "g_1"] & \mathrm{im}(g_1) \arrow[r] & 0
\end{tikzcd}$$

Since Q_1 is projective, there exists $f_1 \in \mathrm{Hom}_R(Q_1, N_1)$ such that $g_1 f_1 = f_0 d_1$. This is the iterative step that can be repeated as required to construct the R-homomorphisms $f_i : Q_i \to N_i$ for $i \geq 1$ that result in a commutative diagram in the category of (finitely generated) R-modules

$$\begin{tikzcd}
Q_n \arrow[r, "d_n"] \arrow[d, "f_n"] & \cdots \arrow[r] \arrow[d] & Q_1 \arrow[r, "d_1"] \arrow[d, "f_1"] & Q_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & M \arrow[r] \arrow[d, "\mathrm{Id}_M"] & 0 \\
N_n \arrow[r, "g_n"] & \cdots \arrow[r] & N_1 \arrow[r, "g_1"] & N_0 \arrow[r, "g_0"] & M \arrow[r] & 0
\end{tikzcd}$$

with $Q_1, \ldots, Q_n$ projective R-modules and the two rows are exact sequences. [10]
