Imperial College
London

MATH70035

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2023

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Algebra 3

Date: 31 May 2023

Time: 10:00 – 12:30 (BST)

Time Allowed: 2.5hrs

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

Candidates should start their answers to each question on a new sheet of paper.

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO

In this exam, a ring will be as defined in the course, i.e. they have a multiplicative identity and are not necessarily commutative. You may use any results proven in the course provided they are clearly stated (and provided they are not the statement you are being asked to prove).

1. Give a proof or counterexample to each of the following statements:

(a) Let R be a commutative ring. Then an ideal $I \subseteq R$ is maximal if and only if R/I is a field. (3 marks)

(b) If R is a unique factorisation domain, then every non-zero prime ideal is maximal. (3 marks)

(c) If R is a finite integral domain, then R is a field. (3 marks)

(d) An integral domain R is a field if and only if it is a Euclidean domain with Euclidean function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ given by $x \mapsto 0$. (3 marks)

(e) Let R be a commutative ring. Then R is a subring of a field if and only if R is an integral domain. (2 marks)

(f) If R is Noetherian, then R is a Euclidean domain. (2 marks)

(g) If R is a principal ideal domain and $S \subseteq R$ is a multiplicative submonoid, then $S^{-1}R$ is a principal ideal domain. (2 marks)

(h) Let R be a commutative ring. If a polynomial $f \in R[X]$ is a unit, then f is a constant polynomial. (2 marks)

(Total: 20 marks)

2. (a) Define what it means for a commutative ring R to be Noetherian. (2 marks)

(b) State and prove Hilbert's basis theorem. (8 marks)

(c) Determine, with proof, which of the following commutative rings are Noetherian:

(i) $\mathbb{Q}[X]$. (2 marks)

(ii) $(\mathbb{Z}/6)^3$. (2 marks)

(iii) $\mathbb{Z}[\sqrt{-7}]$. (2 marks)

(iii) The ring of algebraic integers $\mathbb{A}$ which is a subring of $\mathbb{C}$. (4 marks)

(Total: 20 marks)

3. (a) Define what it means for a ring R to have the invariant basis number property (IBN). (2 marks)

(b) Let R be a ring, let $I \subseteq R$ be a two-sided ideal and let M be an R-module.

(i) Show that

$$IM = \{\sum_{i=1}^{n} a_i \cdot m_i : a_i \in I, m_i \in M, n \geq 0\} \subseteq M$$

is an R-submodule of M. (2 marks)

(ii) Show that M/IM is an R/I-module in a natural way. You should verify that the action is well-defined but you need not check that it makes M/IM into an R/I-module. (2 marks)

(c) Let R be a ring and let $I \subseteq R$ be a two-sided ideal. Prove carefully that, if R/I has IBN, then R has IBN. (6 marks)

(d) Prove that each of the following rings have IBN:

(i) $\mathbb{Z}^n$ for n a positive integer. (3 marks)

(ii) $\mathbb{Z}[G]$ where G is a group. (3 marks)

(iii) $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ which is a subring of $M_2(\mathbb{Z})$. (2 marks)

(Total: 20 marks)

4. (a) Let R be a commutative ring, let $f : M \to N$ be an R-module homomorphism and let $S \subseteq R$ be a multiplicative submonoid.

(i) Show that the function $f_* : S^{-1}M \to S^{-1}N$, $(m, s) \mapsto (f(m), s)$ for $m \in M$, $s \in S$ is an $S^{-1}R$-module homomorphism. (3 marks)

(ii) Show that, if f is injective, then f_* is injective. (3 marks)

(b) Let R be a commutative ring, let $S \subseteq R$ be a multiplicative submonoid and let M and N be R-modules. Prove that $S^{-1}(M \oplus N) \cong S^{-1}M \oplus S^{-1}N$ as $S^{-1}R$-modules. (3 marks)

(c) Let R be an integral domain. Prove carefully that, if $R^n \leq R^m$ is an R-submodule for $n, m \geq 0$, then $n \leq m$. You may use any general facts from linear algebra provided they are clearly stated. (3 marks)

(d) Let R be a Noetherian integral domain such that, for every finitely generated R-module M, there exists $n, r \geq 0$ and $d_1, \cdots, d_r \in R \setminus \{0\}$ such that $M \cong R^n \oplus R/(d_1) \oplus \cdots \oplus R/(d_r)$. Prove that R is a principal ideal domain. (8 marks)

(Total: 20 marks)

5. (a) Let R be a unique factorisation domain. Define what it means for a non-zero polynomial in $R[X]$ to be:

(i) Irreducible. (1 mark)

(ii) Primitive. (1 mark)

(b) Let R be a unique factorisation domain and let F be its field of fractions.

(i) Determine the set of units in $R[X]$. (2 marks)

(ii) Let $f \in R[X]$ be a primitive polynomial. Show that, if f is irreducible in $F[X]$, then f is irreducible in $R[X]$. (4 marks)

(c) Let R be a unique factorisation domain and let $f(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ be primitive where $n \geq 1$ and $a_n \neq 0$. We say that $f(X)$ is *Eisenstein* if there exists a prime $p \in R$ such that $p \mid a_i$ for $0 \leq i < n$, $p \nmid a_n$ and $p^2 \nmid a_0$. We say that $f(X)$ is *shift Eisenstein* if $f(X + m)$ is Eisenstein for some $m \in R$.

(i) Let $f(X) \in R[X]$ be a non-constant polynomial. Prove carefully that $f(X) \in R[X]$ is irreducible if and only if $f(X + m) \in R[X]$ is irreducible for some $m \in \mathbb{Z}$. Deduce that, if $f \in R[X]$ is shift Eisenstein, then f is irreducible. (4 marks)

(ii) Determine the integers $n \in \mathbb{Z}$ for which $X^3 + nX + 1 \in \mathbb{Z}[X]$ is irreducible and shift Eisenstein respectively. (8 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2023

This paper is also taken for the relevant examination for the Associateship.

MATH60035/MATH70035

Algebra 3 (Solutions)

Setter's signature	Checker's signature	Editor's signature
. . . .	. . . .	. . . .

1. (a) True. Suppose R/I is a field. Since fields are non-zero, this implies that $I \subsetneq R$. If $I \subseteq R$ is not maximal, then there exists an ideal J such that $I \subsetneq J \subsetneq I$. This implies that $\{0\} \subsetneq J/I \subsetneq R/I$ is a proper ideal. However, since R/I is a field, every ideal is $\{0\}$ or R/I. This a contradiction. seen ⇓ 3, A

(b) False. Let $R = \mathbb{Z}[X]$ and consider $I = (X)$. Then $R/I \cong \mathbb{Z}$ which is an integral domain but not a field. Hence I is a non-zero prime ideal, but is not maximal. sim. seen ⇓ 3, B

(c) True. Let $a \in R$ be non-zero and consider $f : R \to R, r \mapsto ra$. This is a ring homomorphism. We claim this is injective. If $ra = sa \in R$ for $r, s \in R$, we have $(r-s)a = 0$. Since R is an integral domain, this implies that $r - s = 0$ or $a = 0$. Since $a \neq 0$, this gives that $r = s$. Now, since f is an injective map between finite sets, it must be surjective. Since $1 \in \mathrm{im}(f)$, there exists $r \in A$ such that $ra = 1$ and so $a \in R^\times$. Hence R is a field. seen ⇓ 3, A

(d) True. Suppose R is a field. We will verify that ϕ is a Euclidean function. We first need to check that $\phi(a \cdot b) \geq \phi(a)$ for all $a, b \in R$ such that $a, b \neq 0$. This is clear since both sides are 0. We next need to check that, for all $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\phi(r) < \phi(b)$. Since $b \neq 0$ and R is a field, there exists $c \in R$ such that $bc = 1$. Hence we can take $q = ac$ and $r = 0$. meth seen ⇓

Now suppose R is a Euclidean domain with Euclidean function ϕ. Then, for all $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\phi(r) < \phi(b)$. The latter cannot hold since $\phi(r) = \phi(b)$ for all $r, b \in R \setminus \{0\}$, and so we must have $r = 0$. That is, for all $a, b \in R$, there exists q such that $a = bq$. By taking $a = 1$, we get that every $b \in R$ has an inverse. Hence R is a field. 3, B

(e) True. A field is an integral domain and the subring of an integral domain is an integral domain. In particular, if R is a subring of a field, then R is an integral domain. Conversely, if R is an integral domain, then R is a subring of its field of fractions F. meth seen ⇓ 2, B

(f) False. We know that $\mathbb{Z}$ is Noetherian since it is a PID. By Hilbert's Basis theorem, $\mathbb{Z}[X]$ is Noetherian. However, $\mathbb{Z}[X]$ is not a PID since $(2, X)$ is non-principal. Since every ED is a PID, this implies that $\mathbb{Z}[X]$ is not an ED. unseen ⇓ 2, C

(g) True. Recall the following result from the course: every ideal in $S^{-1}R$ is of the form $S^{-1}I = \{(i, s) : i \in I, s \in S\} \subseteq S^{-1}R$ for some ideal $I \subseteq R$. Since R is a PID, we have that $I = (x)$ for some $x \in R$. We claim that $S^{-1}I = S^{-1}R \cdot (x, 1)$ and so is principal. If $(i, s) \in S^{-1}I$, then $i \in I = (x)$ and so $i = rx$ for some $r \in R$. We have $(rx, s) = (r, s) \cdot (x, 1)$. sim. seen ⇓ 2, A

(h) False. Take $R = \mathbb{Z}/4$ and $f = 1 + 2X$. Then $f^2 = 1 + 4X + 4X^2 = 1$ and so $f \in (\mathbb{Z}/4)[X]$ is a unit. unseen ⇓ 2, C

2. (a) Let R be a commutative ring. We say R is *Noetherian* if, for every ascending chain of ideals in R $\boxed{\text{seen} \Downarrow}$

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

there exists N such that $I_N = I_{i+N}$ for all $i \geq 0$. $\boxed{2, \text{A}}$

(b) Statement: Let R be a commutative ring. If R is Noetherian, then $R[X]$ is Noetherian. $\boxed{\text{seen} \Downarrow}$

We will use that R is Noetherian if and only if every ideal $I \subseteq R$ is finitely generated.

Suppose $I \subseteq R[X]$ is an ideal. It suffices to prove that I is finitely generated. We will assume that $I \neq \{0\}$. For $n \geq 0$, define:

$$I_n = \{r \in R : r \text{ is the leading coefficient of a degree } n \text{ polynomial } f \in I\} \cup \{0\}.$$

Since I is an ideal, it follows easily that $I_n \subseteq R$ is an ideal for each $n \geq 0$. $\boxed{2, \text{A}}$

If $r \in I_n$ is non-zero, then there exists $f \in I$ with $f = rX^n + \cdots$. Since I is an ideal, $fX = rX^{n+1} + \cdots \in I$ and so $r \in I_{n+1}$. In particular, we have an ascending chain

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots .$$

Since R is Noetherian, there exists N such that $I_N = I_{i+N}$ for all $i \geq 0$. $\boxed{2, \text{A}}$

We also know that each I_i is finitely generated. For $0 \leq i \leq N$, we write

$$I_i = (r_1^{(i)}, \cdots, r_{n_i}^{(i)})$$

for some $r_1^{(i)}, \cdots, r_{n_i}^{(i)} \in R$ non-zero. For each i, j, let $f_j^{(i)} \in I$ be the polynomial such that $f_j^{(i)} = r_j^{(i)} X^i + \cdots$. We now claim that

$$I = (\{f_j^{(i)}\}_{1 \leq i \leq N, 1 \leq j \leq n_i})$$

and so is finitely generated. $\boxed{2, \text{A}}$

Let $J = (\{f_j^{(i)}\}_{1 \leq i \leq N, 1 \leq j \leq n_i})$. Since we certainly have $f_j^{(i)} \in I$ for all i, j and so we need to show that $I \subseteq J$. If not, then there exists a polynomial $f \in I \setminus J$ of minimal degree. Then we have $f = rX^m + \cdots$ and $r \in I_m$.

We will start by assuming that $m = \deg(f) \leq N$. We have $r = \sum_{i=1}^{n_m} \lambda_i r_i^{(m)}$ for some $\lambda_i \in R$. Let $F = \sum_{i=1}^{n_m} \lambda_i f_i^{(m)} \in J$. Then F has the same leading coefficient as f and so $\deg(f - F) < \deg(f)$. By minimality, $f - F \in J$. Since $F \in J$, this implies that $f \in J$ which is a contradiction.

If $m = \deg(f) > N$, then $I_m = I_N$ and so $r = \sum_{i=1}^{n_N} \lambda_i r_i^{(N)}$ for some $\lambda_i \in R$. Let $F = X^{m-N} \sum_{i=1}^{n_N} \lambda_i f_i^{(N)} \in J$. Then F has the same leading coefficient as f and so $\deg(f - F) < \deg(f)$. By minimality, $f - F \in J$. Since $F \in J$, this implies that $f \in J$ which is a contradiction. $\boxed{2, \text{A}}$

(c) (i) Every field R is Noetherian since its only ideals are $\{0\}$ and R and so every ascending chain stabilises to one of these ideals. Hence $\mathbb{Q}$ is Noetherian. By Hilbert's Basis theorem, $\mathbb{Q}[X]$ is Noetherian. sim. seen ⇓

2, A

(ii) $(\mathbb{Z}/6)^3$ is Noetherian since it is finite and every finite ring is Noetherian. This is because a finite ring has finitely many ideals and so every ascending chain must eventually stabilise. meth seen ⇓

2, C

(iii) Recall the following result from the course: if R is Noetherian, then R/I is Noetherian for $I \subseteq R$ a two-sided ideal. In particular, by the first isomorphism theorem, if $f : R \to S$ is a surjective ring homomorphism, then S is Noetherian. We know that $\mathbb{Z}$ is Noetherian and, by Hibert's Basis theorem, $\mathbb{Z}[X]$ is Noetherian. The map $f : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{-7}]$ sending $X \mapsto \sqrt{-7}$ is a surjective ring homomorphism. Hence $\mathbb{Z}[\sqrt{-7}]$ is Noetherian. unseen ⇓

2, D

(iv) We will show that $\mathbb{A}$ is not Noetherian by exhibiting ideals $I_1, I_2, \cdots$ such that unseen ⇓

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots .$$

For $n \geq 0$, define $I_n = (2^{1/2^n})$. Note that $\alpha_n = 2^{1/2^n}$ is an algebraic integer since it is a root of $X^{2^n} - 2$ which is monic. We have that $\alpha_{n+1}^2 = \alpha_n$ and so $\alpha_n \in I_{n+1}$ which implies that $I_n \subseteq I_{n+1}$ for all $n \geq 0$.

It remains to show that $I_n \neq I_{n+1}$ for all $n \geq 0$. Suppose for contradiction that there exists $n \geq 0$ for which $I_n = I_{n+1}$. Then $\alpha_{n+1} \in I_n$ and so we have $\alpha_{n+1} = a \cdot \alpha_n$ for some algebraic integer $a \in \mathbb{A}$. We have $a = \alpha_{n+1}/\alpha_n = 2^{-1/2^{n+1}}$ and so $a^{2^n} = 1/2$. If $a \in \mathbb{A}$, then $1/2 = a^{2^n} \in \mathbb{A}$ since $\mathbb{A}$ is a ring. However $1/2 \notin \mathbb{A}$ since $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$, which is a contradiction.

4, D

3. (a) We say that a ring R has the *invariant basis number property (IBN)* if, for all integers $n, m \geq 0$, we have that $R^n \cong R^m$ are isomorphic as (left) R-modules if and only if $n = m$.

seen ⇓

2, A

(b) (i) We first check it is an abelian subgroup. It contains $0_M \in M$ since $0_M = 0 \cdot 0_M$ and $0 \in I$. It is clearly closed under addition and, if $\sum_{i=1}^n a_i \cdot m_i \in IM$, then $-\sum_{i=1}^n a_i \cdot m_i = \sum_{i=1}^n (-a_i) \cdot m_i \in IM$ since $-a_i \in I$ for all i.

sim. seen ⇓

We now check is is closed under the R-action. Let $r \in R$ and let $am \in IM$ for $a \in I$, $m \in M$. Since I is an ideal, we have $ra \in I$ and so $ram = (ra)m \in IM$.

2, A

(ii) We define the action as follows. If $r + I \in R/I$ and $m + IM \in M/IM$, then take $(r + I) \cdot (m + IM) := rm + IM$.

sim. seen ⇓

We first check this is well-defined. If $r + I = r' + I$ and $m + IM = m' + IM$, then $r - r' \in I$ and $m - m' \in IM$, and we need to show that $rm - r'm' \in IM$. This follows from the fact that $rm - r'm' = (r - r')m' + r(m' - m) \in IM$ since $(r - r')m', r(m' - m) \in IM$ and IM is an ideal.

2, A

(c) Let $n, m \geq 0$ be integers and suppose $R^n \cong R^m$ as R-modules. By (b), R^n/IR^n is an R/I-module. We claim that $I^n = IR^n$ where $I^n = \{(a_1, \cdots, a_n) : a_i \in I\} \subseteq R^n$. If $\alpha = (a_1, \cdots, a_n) \in I$, then $\alpha = a_1(1, 0, \cdots, 0) + \cdots + a_n(0, \cdots, 0, 1) \in IR^n$. Conversely, let $\alpha = \sum_{i=1}^m a_i(r_1^{(i)}, \cdots, r_n^{(i)}) \in IR^n$ for some m. Then $\alpha = (\sum_{i=1}^m a_i r_1^{(i)}, \cdots, \sum_{i=1}^m a_i r_n^{(i)}) \in I^n$ since, for each j, we have that $\sum_{i=1}^m a_i r_j^{(i)} \in I$ since I is a two-sided ideal.

unseen ⇓

This implies that $R^n/IR^n = R^n/I^n \cong (R/I)^n$ are isomorphic as R-modules. Now $R^n \cong R^m$ as R-modules implies that $R^n/IR^n \cong R^m/IR^m$ as R/I-modules and so $(R/I)^n \cong (R/I)^m$ as R/I-modules. Since R/I has IBN, this implies that $n = m$. Hence R has IBN.

6, B

(d) (i) Define $f : \mathbb{Z}^n \to \mathbb{Z}/2$, $(r_1, \cdots, r_n) \mapsto r_1 \bmod 2$. This is a surjective ring homomorphism and so, by the first isomorphism theorem, we have that $\mathbb{Z}/2 \cong \mathbb{Z}^n/\ker(f)$. By (c), it suffices to prove that $\mathbb{Z}/2$ has IBN. This is true since $(\mathbb{Z}/2)^n \cong (\mathbb{Z}/2)^m$ as $\mathbb{Z}/2$-modules implies that the sets are in bijection and so $2^n = 2^m$ and $n = m$.

sim. seen ⇓

3, B

(ii) Consider the map $f : \mathbb{Z}[G] \to \mathbb{Z}$, $\sum_{i=1}^n a_i g_i \mapsto \sum_{i=1}^n a_i$ where $a_i \in \mathbb{Z}$ and $g_i \in G$ for all i. This is a surjective ring homomorphism and so, by the first isomorphism theorem, we have $\mathbb{Z} \cong \mathbb{Z}[G]/\ker(f)$. We know $\mathbb{Z}$ has IBN by (i) and this implies that $\mathbb{Z}[G]$ has IBN by (c).

unseen ⇓

3, C

(iii) Consider the map $f : R \to \mathbb{Z}$, $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto a$ for $a, b \in \mathbb{Z}$. This is clearly surjective and we claim that it is a ring homomorphism. This follows since:

unseen ⇓

$$f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}\right) = f\left(\begin{pmatrix} a + a' & b + b' \\ 0 & a + a' \end{pmatrix}\right) = a + a'$$

and

$$f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}\right) = f\left(\begin{pmatrix} aa' & ab' + ba' \\ 0 & aa' \end{pmatrix}\right) = aa'.$$

Similarly to the above, this implies that $\mathbb{Z} \cong R/\ker(f)$. Since $\mathbb{Z}$ has IBN, this implies that R has IBN by (c).

2, D

4. (a) (i) We first check it is a homomorphism of abelian groups. Note that $0_{S^{-1}R} = (0,1)$. We have $f_*(0,1) = (0,1)$ since f is a homomorphism. We have that $\boxed{\text{seen} \Downarrow}$

$$f_*((m_1, s_1) + (m_2, s_2)) = f_*((s_2 m_1 + s_1 m_2, s_1 s_2)) \\ = (s_2 f(m_1) + s_1 f(m_2), s_1 s_2) = (f(m_1), s_1) + (f(m_2), s_2)$$

for $m_i \in M$, $s_i \in S$, using again that f is a homomorphism.

We now check that f respects the $S^{-1}R$-action. If $(r,t) \in S^{-1}R$ and $(m,s) \in S^{-1}M$, then

$$f_*((r,t) \cdot (m,s)) = f_*((rm, ts)) = (rf(m), ts) = (r,t) \cdot (f(m), s).$$

$\boxed{3, \text{A}}$

(ii) Suppose f is injective. Let $(m_1, s_1), (m_2, s_2) \in S^{-1}M$. If $f_*(m_1, s_1) = f_*(m_2, s_2)$, then $(f(m_1), s_1) = (f(m_2), s_2)$ and so there exists $t \in S$ such that $t(s_2 f(m_1) - s_1 f(m_2)) = 0$. Since f is an R-module homomorphism, this implies that $f(t(s_2 m_1 - s_1 m_2)) = 0$. Since f is injective, this implies that $t(s_2 m_1 - s_1 m_2) = 0$ and so $(m_1, s_1) = (m_2, s_2) \in S^{-1}M$. $\boxed{\text{sim. seen} \Downarrow}$ $\boxed{3, \text{A}}$

(b) We claim that $g : S^{-1}(M \oplus N) \to S^{-1}M \oplus S^{-1}N$, $((m,n), s) \mapsto ((m,s),(n,s))$ is an $S^{-1}R$-module isomorphism. $\boxed{\text{meth seen} \Downarrow}$

We first check that g is a homomorphism of abelian groups. We have $g((0,0),1) = ((0,1),(0,1))$ and

$$g(((m_1,n_1),s_1) + ((m_2,n_2),s_2)) = g((s_2 m_1 + s_1 m_2, s_2 n_1 + s_1 n_2), s_1 s_2) \\ = ((s_2 m_1 + s_1 m_2, s_1 s_2), (s_2 n_1 + s_1 n_2, s_1 s_2)) \\ = ((m_1, s_1) + (m_2, s_2), (n_1, s_1) + (n_2, s_2)).$$

We also have closure under the R-action:

$$g((r,t) \cdot ((m,n),s)) = g((rm, rn), ts) = ((rm, ts), (rn, ts)) = (r,t) \cdot ((m,s),(n,s)).$$

Finally, note that f is clearly injective. It is surjective since

$$((m,s),(n,t)) = ((tm, ts), (sn, ts)) = g((tm, sn), ts).$$

$\boxed{3, \text{B}}$

(c) We have that $f : R^n \to R^m$ is an injective R-module homomorphism. Since R is an integral domain, $S = R \setminus \{0\}$ is a multiplicative submonoid and $F = \text{Frac}(R) = S^{-1}R$ is a field. By (a) (i), there is an induced F-module homomorphism $f_* : S^{-1}R^n \to S^{-1}R^m$. $\boxed{\text{unseen} \Downarrow}$

By (b), we get that $S^{-1}R^n \cong (S^{-1}R)^n$ as $S^{-1}R$-modules. In particular, then have that $f_* : F^n \to F^m$ is an injective linear map of F vector spaces and so $F^n \leq F^m$ is a subspace. It is a well known result in linear algebra that, if V is a finite-dimensional vector space and $W \leq V$ is a subspace, then $\dim(W) \leq \dim(V)$. Hence we have $n \leq m$, as required. $\boxed{3, \text{C}}$

(d) Let $I \subseteq R$ be a non-zero ideal. It suffices to prove that $I \cong R$ as R-modules. To see this, suppose $f : R \to I$ be an R-module isomorphism and let $x = f(1) \in I$. Since f is surjective, we get that $I = Rx$ and so $I = (x)$ is a principal ideal. $\boxed{\text{unseen} \Downarrow}$ $\boxed{2, \text{D}}$

We now claim that $I \cong R$ as R-modules. Since R is Noetherian, it follows that I is finitely generated. By assumption, this implies that

$$I \cong R^n \oplus R/(d_1) \oplus \cdots \oplus R/(d_r)$$

as R-modules, for some $n, r \geq 0$ and some non-zero $d_i \in R$. $\boxed{1, \text{D}}$

We can assume without loss of generality that $R/(d_i) \neq \{0\}$ (i.e. that the d_i are non-units).

If $r \geq 1$, let $x \in I$ be the pre-image of the element $(0, 1, 0, \cdots, 0)$ under this isomorphism. Then we have $d_1 \cdot x = 0 \in I \subseteq R$ and, since R is an integral domain and $d_1 \neq 0$, this implies that $x = 0$. This is a contradiction since $1 \neq 0 \in R/(d_1)$ implies that $x \neq 0$. This implies that $r = 0$ and so $I \cong R^n$ as R-modules. $\boxed{3, \text{D}}$

Since $I \subseteq R$, this implies that $R^n \leq R$ is an R-submodule. By (b), this implies that $n \leq 1$, i.e. $n = 0$ or $n = 1$. Since I is non-zero, $n \neq 0$ and so $n = 1$. Hence $I \cong R$ as R-modules. $\boxed{2, \text{D}}$

5. (a) (i) A non-zero polynomial $f \in R[X]$ is *irreducible* if it is a non-unit and if $f = gh$ for $g, h \in R[X]$ implies that g or h is a unit.

seen ⇓

1, M

(ii) A non-zero polynomial $f = a_0 + a_1X + \cdots + a_nX^n$ is *primitive* if $\gcd(a_1, \cdots, a_n) = 1$. This is well-defined since greatest common divisors exist in a unique factorisation domain.

seen ⇓

1, M

(b) (i) Recall from lectures that, if R is an integral domain and $f, g \in R[X]$ are non-zero, then $\deg(f \cdot g) = \deg(f) + \deg(g)$.

seen ⇓

We claim that $R[X]^\times = R^\times$, i.e. that the units are the constant polynomials $f = a_0$ where $a_0 \in R^\times$. It is clear that $R^\times \subseteq R[X]^\times$. We will now prove the converse. If $f \in R[X]$ is a unit, then there exists $g \in R[X]$ such that $fg = 1$. Since R is an integral domain, f and g are non-zero and so $\deg(f) + \deg(g) = \deg(fg) = 0$. This implies that $\deg(f) = \deg(g) = 0$ and so $f, g \in R$. In particular, $f \in R^\times$.

2, M

(ii) We may assume that f is a non-constant polynomial since, if f is constant and primitive, then $f \in R^\times \subseteq R[X]^\times$ and so is not irreducible. By (i), this means we can also assume that f is a non-unit.

seen ⇓

We will prove the contrapositive. Suppose $f \in R[X]$ is not irreducible. Then there exists $g, h \in R[X]$ non-zero non-units such that $f = gh$. To show that f is not irreducible in $F[X]$, it suffices to show that $g, h \in F[X]$ are non-units. If so, suppose without loss of generality that $g \in F[X]$ is a unit. By (i), we have that $F[X]^\times = F^\times = F \setminus \{0\}$. But, since $g \in R[X]$, we have that $g \in R \cap (F \setminus \{0\}) = R \setminus \{0\}$.

If $f = a_0 + a_1X + \cdots + a_nX^n$ then, since $f = gh$ and $g \in R$, we have that $g \mid a_i$ for all i and so $g \mid \gcd(a_1, \cdots, a_n)$. Since f is primitive, we have $\gcd(a_1, \cdots, a_n) = 1$ and so $g \mid 1$, i.e. $g \in R^\times$. This implies that $g \in R[X]^\times$ which is a contradiction.

4, M

(c) (i) Note that a non-constant polynomial in $R[X]$ is non-zero and, since R is an integral domain, (b) implies that it is a non-unit. Hence a non-constant polynomial $f \in R[X]$ is not irreducible if and only if $f = gh$ for non-units g, h.

sim. seen ⇓

Let $f(X) \in R[X]$ be a non-constant polynomial and suppose $f(X + m)$ is irreducible in $R[X]$ for some $m \in \mathbb{Z}$. Note that $f(X + m)$ is non-constant since, for example, it has the same degree as $f(X)$.

Suppose for contradiction that $f(X)$ is not irreducible. Then there exists $g(X), h(X) \in R[X]$ non-units such that $f(X) = g(X)h(X)$. This implies that $f(X + m) = g(X + m)h(X + m) \in R[X]$. If $g(X)$ is non-constant, then $g(X + m)$ is non-constant and so not a unit. If $g(X)$ is constant, then $g(X + m) = g(X)$ and so is a non-unit. This implies that $g(X + m)$ is a non-unit and similarly for $h(X + m)$. Hence $f(X + m)$ is not irreducible, which is a contradiction.

Conversely, suppose $f(X)$ is irreducible and let $m \in \mathbb{Z}$. We want to show that $f(X + m)$ is irreducible. If we take $g(X) = f(X + m)$, then we know that $g(X + (-m)) = f(X)$ is irreducible so we can apply the result above.

Finally, if $f(X)$ is shift Eisenstein, then $f(X+m)$ is Eisenstein for some $m \in \mathbb{Z}$. By Eisenstein's criteria, this implies that $f(X + m)$ is irreducible. Hence, by the results just proven, $f(X)$ is irreducible.

4, M

(c) (ii) For convenience, we will write $f_n = X^3 + nX + 1$. $\boxed{\text{unseen} \Downarrow}$

We first determine when f_n is irreducible. By (b), $\mathbb{Z}[X]^\times = \{\pm 1\}$ and so f_n is a non-zero non-unit. Suppose f_n is not irreducible. Then there exists $g, h \in \mathbb{Z}[X]$ non-zero non-units such that $f_n = gh$. Since $\deg(f) + \deg(g) = \deg(f_n) = 3$, either g or h has degree 1. Hence f is divisible by a polynomial $aX + b$ for $a \neq 0$. Since this is a factor, a divides the leading coefficient of f_n and b divides the last coefficient. Hence $a, b \in \mathbb{Z}^\times = \{\pm 1\}$. It follows that f_n has a root ± 1. We have $f_n(1) = 2 + n$ and $f_n(-1) = -n$ and so $n = 0$ or -2. In both cases, f_n is not irreducible: $f_0 = X^3 + 1 = (X + 1)(X^2 - X + 1)$ and $f_{-2} = X^3 - 2X + 1 = (X - 1)^2$. So f_n is irreducible if and only if $n \neq 0, -2$. $\boxed{2, \text{M}}$

We now determine when f_n is shift Eisenstein. Note that f_n is not Eisenstein itself since the last coefficient 1 is not divisible by any prime $p \in \mathbb{Z}$. Let $m \in \mathbb{Z}$. Then we have:

$$f_n(X + m) = X^3 + 3mX^2 + (3m^2 + n)X + (m^3 + nm + 1).$$

Suppose $f_n(X + m)$ is Eisenstein via the prime $p \in \mathbb{Z}$, which we can assume is positive. That is, $p \mid 3m$, $p \mid 3m^2 + n$, $p \mid m^3 + nm + 1$ and $p^2 \nmid m^3 + nm + 1$. $\boxed{1, \text{M}}$

If $p \mid m$, then $p \mid m^3 + nm + 1$ implies $p \mid 1$ which is a contradiction. Hence $p \nmid m$ and so $p \mid 3m$ implies that $p = 3$. Hence $f_n(X + m)$ is Eisenstein at $p = 3$. So $3 \mid 3m^2 + n$, $3 \mid m^3 + nm + 1$ and $9 \nmid m^3 + nm + 1$. This implies that $3 \mid n$, $3 \mid m^3 + 1$ and $9 \nmid m^3 + nm + 1$. $\boxed{2, \text{M}}$

Now, $m^3 \equiv -1$ mod 3 implies $m \equiv -1$ mod 3, which implies $m^3 \equiv -1$ mod 9. This gives that $9 \mid m^3 + 1$ and so $9 \nmid nm$. Since $m \equiv -1$ mod 3, this implies that $9 \nmid n$. $\boxed{2, \text{M}}$

We have shown that, if f_n is shift Eisenstein, then $3 \mid n$ but $9 \nmid n$. In fact, f_n is shift Eisenstein in all these cases since $f_n(X - 1) = X^3 - 3X^2 + (3 + n)X - n$ is Eisenstein at the prime 3. So f_n is shift Eisenstein if and only if $3 \mid n$ and $9 \nmid n$. $\boxed{1, \text{M}}$

Review of mark distribution:

Total A marks: 32 of 32 marks
Total B marks: 20 of 20 marks
Total C marks: 12 of 12 marks
Total D marks: 16 of 16 marks
Total marks: 100 of 100 marks
Total Mastery marks: 20 of 20 marks

If your module is taught across multiple year levels, you might have received this form for each level of the module. You are only required to fill this out once for each question.

ExamModuleCode	**QuestionNumber**	**Comments for Students**
MATH60035/70035	1	This question was answered well by the majority of students, with a mean mark of 10.91. In (a), the students typically forgot that maximal ideals needed to be proper. There is an error in (g) as stated: the question should have said that S does not contain 0.
MATH60035/70035	2	This question was answered well by the majority of students, with a mean mark of 9.93. Part (c) (iii) proved to be difficult, but was answered successfully by a number of students.
MATH60035/70035	3	This question proved very difficult, with a mean mark of just 6.11. Many students were not able to demonstrate a strong grasp of modules and found distinguishing between R-module homomorphisms and R/I-module homomorphisms difficult. Many students did not realise that part (c) could be done using part (b). However, those who realised this typically did quite well in (c).
MATH60035/70035	4	This question proved was the most poorly answered on the exam, with a mean mark of just 5.39. Most candidates did not realise that part (c) could be done using parts (a) and (b). Likewise part (d) proved to be very difficult, though a few students did obtain a complete proof.
MATH70035	5	This question was of around average difficulty compared to the rest of the paper. The average mark was 7.93.The question turned out to be a good test of student's ability to produce rigorous arguments under time pressure. A major obstacle was that students failed to realise, or take seriously, the fact that irreducibles needed to be non-units. Most did not record this in the definition in (a) (i) and, even those who did, managed to forget this by the time it came to (b) (ii) and (c) (i). Consequently just one student obtained full marks for either of these two parts. Part (b) (ii) typically required the students to prove the contrapositive, though a large number of students did this incorrectly and so attempted to prove that 'f reducible in F[X]' implies 'f reducible in R[X]'. In part (c) (ii), many students though that it sufficed to determine when the polynomial was shift Eisenstein as (they thought) this was equivalent to irreducible.