Imperial College London

MATH97063 MATH97174

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2020

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

Algebra 3

Date: 21st May 2020

Time: 13.00pm - 15.30pm (BST)

Time Allowed: 2 Hours 30 Minutes

Upload Time Allowed: 30 Minutes

This paper has 5 Questions.

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

Each sheet of paper should have your CID, Question Number and Page Number on the top.

Only use 1 side of the paper.

Allow margins for marking.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Each question carries equal weight.

SUBMIT YOUR ANSWERS AS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD INCLUDING A COMPLETED COVERSHEET WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

.

In this exam all rings R are assumed commutative with identity unless explicitly stated otherwise.

1. Let R be a ring and $I \subseteq J$ two ideals of R. We define the *ideal quotient* or *colon ideal* $(I : J)$ to be the set of $r \in R$ such that $rj \in I$ for all $j \in J$.

   (a) Show that $(I : J)$ is an ideal of R, and that if R is a domain and $J = \langle r \rangle$ is a principal ideal, then $(I : J) = \frac{1}{r}I$. (4 marks)

   (b) Show that the ideal product $J(I : J)$ is contained in I, and that we have equality if R is a PID. (4 marks)

   (c) Give, with proof, an example of a unique factorization domain R, and ideals $I \subseteq J$ of R, such that $J(I : J)$ is not equal to I. (4 marks)

   (d) Give, with proof, an example of a ring R, and ideals $I \subseteq J$ such that I is principal but $(I : J)$ is not principal. (4 marks)

   (e) Show that if $J, K \subseteq I$ are ideals of R, then $(I : J + K) = (I : J) \cap (I : K)$. (4 marks)

   (Total: 20 marks)

2. Let K be a field with q elements, where $q = p^r$ for some prime number p.

   (a) Let $d > 1$ be a positive integer. Show that the polynomial $X^d - 1$ has exactly $(d, q-1)$ roots in K. (8 marks)

   (b) Show that if $(d, q-1) > 1$ then there exists $a \in K$ such that $X^d - a$ has no roots in K. How many such a are there? (8 marks)

   (c) Factor the polynomial $X^p - a$ in $K[X]$, for $a \in K$. (4 marks)

   (Total: 20 marks)

3. (a) (i) Show that if R is an integral domain, then any polynomial $P(X) \in R[X]$ of degree d has at most d roots in R. (4 marks)

(ii) Give, with proof, an example of a ring R, and a monic polynomial $P(X) \in R[X]$ of degree 2, such that $P(X)$ has more than two roots. How many distinct factorizations does your example have in $R[X]$? (6 marks)

(b) Factor the following polynomials into irreducibles in the given ring. Be sure to show that each factor is indeed irreducible!

(i) $X^8 - 1$ in $\mathbb{Z}[X]$. (5 marks)

(ii) $X^{16} + X^2$ in $\mathbb{F}_2[X]$. (5 marks)

(Total: 20 marks)

4. Let A be the matrix:

$$\begin{pmatrix} 1 & -3 & 1 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & -2 & 2 & 1 \\ 0 & -1 & 0 & 2 \end{pmatrix}.$$

(a) Give the matrix of a presentation of the $\mathbb{Q}[T]$-module M_A associated to the linear transformation

$$A : \mathbb{Q}^4 \to \mathbb{Q}^4.$$

(You do not need to prove it is a presentation.) (3 marks)

(b) Find the Smith normal form of the presentation matrix from part (a). (10 marks)

(c) Find the Jordan normal form of the matrix A. (3 marks)

(d) Find the rational canonical form of the matrix A. (4 marks)

(Total: 20 marks)

5. In this question you may use any results from the lectures or the mastery material, as long as you state them clearly.

Let $K/\mathbb{Q}$ be a finite extension of fields, and let $\mathcal{O}_K$ denote the ring of integers of K. An *order* in $\mathcal{O}_K$ is a subring of $\mathcal{O}_K$ whose field of fractions is K.

(a) Show that if A is an order in $\mathcal{O}_K$ then there exists an element a of A such that $a\mathcal{O}_K$ is contained in A. (4 marks)

(b) Show that if A and a are as in part (a) then $A[\frac{1}{a}]$ is isomorphic to $\mathcal{O}_K[\frac{1}{a}]$, and therefore is a Dedekind domain. (8 marks)

(c) For an ideal I of A, let I' denote the ideal of $A[\frac{1}{a}]$ generated by the elements of I. Show that the map $I \mapsto I'$ gives a bijection between the ideals of A that are prime to a and the ideals of $A[\frac{1}{a}]$, whose inverse is "intersection with A". (Here prime to a means that the ideal sum $I + \langle a \rangle$ is the unit ideal.) (4 marks)

(d) Conclude that any nonzero ideal of A that is prime to a factors as a product of prime ideals of A. (4 marks)

(Total: 20 marks)

M3P8 SOLUTIONS

(1) (a) Let $r \in R$, and $s, t \in (I : J)$. Then sj and tj lie in I for all $j \in J$, so $sj + tj$ and rsj lie in I for all $j \in J$. Thus $s + t$ and rs lie in $(I : J)$, so $(I : J)$ is an ideal. **A2**

If $J = \langle r \rangle$ and I is contained in J, then every element of I is divisible by r, so $\frac{1}{r}I$ is an ideal of R. Let $s \in (I : J)$. Then $sr \in I$, so $s \in \frac{1}{r}I$. Conversely if $s \in \frac{1}{r}I$, then $srt \in I$ for all $t \in R$; since $J = \{rt : t \in R\}$ we thus have $s \in (I : J)$. **A2**

(b) Any element $J(I : J)$ is a sum $j_1k_1 + \cdots + j_nk_n$ with $j_i \in J$ and $k_i \in (I : J)$. By definition each j_ik_i lies in I, so their sum does as well. **A2**

If R is a PID then $J = \langle r \rangle$ for some r; then $(I : J) = \frac{1}{r}I$; if I is generated by s, then $(I : J)$ is generated by $\frac{s}{r}$ and we clearly have $\langle r \rangle \langle \frac{s}{r} \rangle = \langle s \rangle$. **A2**

(c) Let $R = \mathbb{C}[X, Y]$, let $I = \langle X \rangle$, and let $J = \langle X, Y \rangle$. Since R is a UFD and X and Y are irreducibles, if $YP(X, Y)$ is contained in I for some polynomial $P(X, Y)$, then $P(X, Y)$ lies in I. Thus $(I : J)$ is contained in I; the reverse containment is clear. Thus $(I : J) = I$, so $J(I : J) = \langle X^2, XY \rangle$, which is properly contained in I. **A4**

(d) Let $R = \mathbb{Z}[\sqrt{-5}]$, $I = \langle 2 \rangle$, and $J = \langle 2, 1 + \sqrt{-5} \rangle$. Then $(I : J)$ contains 2 and $1 - \sqrt{-5}$, and is properly contained in R (since $I \neq J$). On the other hand, the ideal generated by 2 and $1 - \sqrt{-5}$ is maximal (the quotient is just $\mathbb{F}_2$), so we must have $(I : J) = \langle 2, 1 - \sqrt{-5} \rangle = J$. It thus suffices to show that J is not principal, but any generator of J would have to be a nonunit dividing 2 and $1 + \sqrt{-5}$. Its norm would thus have to divide both 4 and 6; since all elements of norm 1 are units and there are no elements of norm 2 this does not happen. **B4**

(e) It is clear that if $rj \in I$ for all $j \in J$, and $rk \in I$ for all $k \in K$, then $r(j + k) \in I$ for all $j \in J$, $k \in K$, so $r \in (I : J + K)$. Conversely, if $r \in (I : J + K)$ then in particular $r \in (I : J)$ and $r \in (I : K)$, since J and K are subsets of $J + K$. **A4**

(2) (a) The multiplicative group of K is cyclic of order $q - 1$; let g be an element of order exactly $q - 1$ in $K^\times$. Then

$(g^a)^d = 1$ if, and only if, $q-1$ divides ad. This holds precisely when $\frac{q-1}{(d,q-1)}$ divides a. Since the elements of $K^\times$ are $g^0, g^1, \ldots, g^{q-1}$, and precisely $(d, q-1)$ of these exponents are divisible by $\frac{q-1}{(d,q-1)}$ the claim follows. **D8**

(b) Consider the map $x \mapsto x^d$ from $K^\times$ to $K^\times$. This is a homomorphism of finite abelian groups whose kernel has order $(d, q-1)$ by part (a). In particular its image has order $\frac{q-1}{(d,q-1)}$. But this image is precisely the set of $a \in K^\times$ such that $X^d - a$ has roots in K. Thus there are $(q-1)(1-\frac{1}{(d,q-1)})$ elements a of K such that $X^d - a$ has no roots in K. **D8**

(c) We have $a = a^q = (a^{p^{r-1}})^p$, so $X^p - a = (X - a^{p^{r-1}})^p$. **C4**

(3) (a) (i) Let K be the field of fractions of R. Then (since degree is a Euclidean norm on $K[X]$) if $P(r) = 0$, we have $X - r$ divides $P(X)$ in $K[X]$. Since factorizations are unique in $K[X]$, $P(X)$ has at most d distinct linear factors, and thus at most d distinct roots in K. Every root in R is a root in K, so the claim follows. **B4**

(ii) Let $R = \mathbb{Z} \times \mathbb{Z}$; then $X^2 - 1$ has the four roots $(\pm 1, \pm 1)$. **C4**
This corresponds to two factorizations $(X-(1,1))(X-(-1,-1))$ and $(X-(1,-1))(X-(-1,1))$ of X^2-1. **C2**

(b) (i) We have $X^8 - 1 = (X^4+1)(X^2+1)(X+1)(X-1)$. The only factor whose irreducibility is difficult to justify is X^4+1; we note that $(X+1)^4 + 1 = X^4+4X^3+6X^2+4X+2$ is irreducible by Eisenstein's criterion. **A5**

(ii) We have $X^{16} + X^2 = (X^8 + X)^2$ over $\mathbb{F}_2$. Since $X^8 + X$ is the product of the irreducible polynomials of degree dividing 3 we have:

$$X^{16} + X^2 = X^2(X+1)^2(X^3+X+1)^2(X^3+X^2+1)^2;$$

all factors are irreducible because they have no roots in $\mathbb{F}_2$. **C5**

(4) (a) The presentation is given by the matrix:

$$\begin{pmatrix} T-1 & 3 & -1 & -2 \\ 0 & T-1 & 0 & 0 \\ 0 & 2 & T-2 & -1 \\ 0 & 1 & 0 & T-2 \end{pmatrix}$$

A3

(b) The Smith normal form is the matrix whose diagonal entries are 1, 1, $T-1$, $(T-1)(T-2)^2$, up to factors of degree 0. **B10**

(c) The Jordan normal form has two Jordan blocks of eigenvalue 1, each of size 1, and one Jordon block of eigenvalue 2 and size 2. **A3**

(d) The rational canonical form is block diagonal with blocks $\begin{pmatrix}1\end{pmatrix}$ and $\begin{pmatrix}0 & 0 & 4\\ 1 & 0 & -8\\ 0 & 1 & 5\end{pmatrix}$. **A4**

(5) (a) Our proof from the mastery notes that $\mathcal{O}_K$ is a Dedekind domain shows in particular that $\mathcal{O}_K$ is a finite rank $\mathbb{Z}$-module. In particular $\mathcal{O}_K$ is generated as an abelian group by a finite set of elements $x_1, \ldots, x_n$. Since the field of fractions of A is equal to K, we can write each x_i as $\frac{b_i}{a_i}$ for b_i, a_i in A. Letting a be the product of the a_i, it is clear that ax_i lies in A for all i, so $a\mathcal{O}_K$ is contained in A. **Unseen, 4**

(b) Since $a\mathcal{O}_K \subseteq A \subseteq \mathcal{O}_K$, we have $A[\frac{1}{a}] = \mathcal{O}_K[\frac{1}{a}]$. It thus suffices to show that $\mathcal{O}_K[\frac{1}{a}]$ is a Dedekind domain. It is clearly Noetherian (as it is a finitely generated extension of the Noetherian ring $\mathcal{O}_K$). Moreover, for any nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K[\frac{1}{a}]$ its intersection with $\mathcal{O}_K$ is a nonzero prime ideal of $\mathcal{O}_K$, and we have $\mathcal{O}_K[\frac{1}{a}]/\mathfrak{p} \cong \mathcal{O}_K/(\mathcal{O}_K \cap \mathfrak{p})$. Thus every nonzero prime ideal of $\mathcal{O}_K[\frac{1}{a}]$ is maximal. Finally, if x is an element of K that satisfies a monic polynomial $P(X)$ of degree d with coefficients in $\mathcal{O}_K[\frac{1}{a}]$, then $a^r x$ is a root of the monic polynomial $a^{dr}P(\frac{x}{a^r})$ and for r sufficiently large this polynomial will have coefficients in $\mathcal{O}_K$. Since $\mathcal{O}_K$ is integrally closed we have $a^r x \in \mathcal{O}_K$, and thus $x \in \mathcal{O}_K[\frac{1}{a}]$. **Seen similar, 8**

(c) We first show that $I' \cap A = I$; it is clear that I is contained in $I' \cap A$. Let $x \in I' \cap A$; we can write x as an $A[\frac{1}{a}]$-linear combination of elements of I. Thus for some r, $a^r x \in I$; that is, $a^r x$ maps to zero in A/I. On the other hand, since a is prime to I, a is a unit in A/I, so x maps to zero in A/I as well. Thus $x \in I$.

Conversely, if J is an ideal of $A[\frac{1}{a}]$, we must show that $J = (J \cap A)'$. Clearly $(J \cap A)'$ is contained in J. On the other hand, let $x \in J$. Then $a^r x$ lies in $J \cap A$, for some r, so x lies in $(J \cap A)'$. **Unseen, 4**

(d) Note that for I and J two ideals of A, it is clear that $I'J'$ contains $(IJ)'$. On the other hand, if $x \in (IJ)'$, we

can write x as an $A[\frac{1}{a}]$-linear combination of products of elements of I and elements of J, and hence as a sum of products of elements of I' and elements of J'. Thus x lies in $I'J'$. In particular, the bijection between ideals of A prime to a and ideals of $A[\frac{1}{a}]$ preserves products of ideals. It also preserves maximality since it is compatible with inclusion. Thus a factorization of I' as a product of prime ideals in the Dedekind domain $A[\frac{1}{a}]$ gives a factorization of I into prime ideals of A that are prime to a.

Unseen, 4

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.

Please record below, some brief but non-trivial comments for students about how well (or otherwise) the questions were answered. For example, you may wish to comment on common errors and misconceptions, or areas where students have done well. These comments should note any errors in and corrections to the paper. These comments will be made available to students via the MathsCentral Blackboard site and should not contain any information which identifies individual candidates. Any comments which should be kept confidential should be included as confidential comments for the Exam Board and Externals. If you would like to add formulas, please include a sperate pdf file with your email.

ExamModuleCode	Question	Comments for Students	
MATH97063 MATH97174	1	With the exception of part d, this question was fairly routine. In part d one needed to find a ring that was not a UFD.	
MATH97063 MATH97174	2	This was probably the hardest question on the exam, other than the mastery question. There was some ambiguity as to what counted as "different factorizations" in part b; I accepted any reasonable interpretation.	
MATH97063 MATH97174	3	This was fine for most people with the exception of part a, where many people recapitulated the proof for fields (which needs extra care in the setting of abitrary rings!)	
MATH97063 MATH97174	4	I was generous with partial credit in part b; many people made calculation errors but as long as it was clear you understood the process you got most of the points. In parts c and d I gave nearly full marks if your answer was consistent with an incorrect part b.	
MATH97063 MATH97174	5	This question was probably too difficult; all students struggled.	