ExamModuleCode	Question Number	Comments for Students
M45P8	1	The first half of this question was bookwork and most had no difficulty. There was some confusion in part d about passing from a nontrivial submodule of a quotient to a submodule of M. In part e, many looked for non-Noetherian examples, but in fact this is not necessary (even the integers have the desired property).
M45P8	2	Mostly this was routine. Many people forgot that if you want to check irreducibility by reducing modulo a prime, you need the polynomial to be monic.
M45P8	3	This was a hard question, particularly part b. Congratulations to those who worked it out!
M45P8	4	A common mistake on the last part of this problem was to assume all generating sets of an ideal have the same size. Of course this is false: consider the ideal of the integers generated by 4 and 6.
M45P8	5	Another way to think about regular linear transformations here is that they have only a single Jordan block for each eigenvalue.

Imperial College
London

M3P8

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)

May-June 2019

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

Algebra 3

Date: Thursday 09 May 2019

Time: 14.00 - 16.00

Time Allowed: 2 Hours

This paper has 4 Questions.

Candidates should use ONE main answer book.

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

All required additional material will be provided.

- DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO.
- Affix one of the labels provided to each answer book that you use, but DO NOT USE THE LABEL WITH YOUR NAME ON IT.
- Calculators may not be used.

Imperial College
London

M4/5P8

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)

May-June 2019

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

Algebra 3

Date: Thursday 09 May 2019

Time: 14.00 - 16.30

Time Allowed: 2 Hours 30 Minutes

This paper has 5 Questions.

Candidates should use ONE main answer book.

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

All required additional material will be provided.

- DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO.
- Affix one of the labels provided to each answer book that you use, but DO NOT USE THE LABEL WITH YOUR NAME ON IT.
- Calculators may not be used.

In this exam you may use any results from the course as long as you state them clearly. In each problem you may also freely use results from previous parts of the problem. As in the lectures, in this exam "ring" means a commutative ring with identity.

1. (a) Give the definitions of a *finitely generated R-module*, a *Noetherian ring*, and a *Noetherian R-module*.

   (b) Show that if R is a ring and M is an R-module, then M is Noetherian if, and only if, every submodule of M is finitely generated.

   (c) Recall that a nonzero R-module M is *simple* if the only R-submodules of M are M itself and the zero module. Show that every nonzero Noetherian R-module has a simple quotient, that is, for any nonzero Noetherian R-module M, there exists an R-submodule N of M such that M/N is simple.

   (d) Give (with proof!) an example of a ring R and an R-module M such that M has no simple submodules.

2. (a) Factor the given polynomials into irreducible factors over the given rings. Be sure to show that all factors are irreducible!

   (i) $X^{15} + X^5 + 1$ over $\mathbb{F}_5[X]$

   (ii) $X^7 + X^6 + X^5 + X + 1$ over $\mathbb{F}_2[X]$.

   (b) Show that the given polynomials are irreducible over the given rings.

   (i) $X^6Y^2 + Y + 1$ over $\mathbb{C}[X, Y]$.

   (ii) $X^4 + 2X^3 + 3X^2 + X + \frac{1}{8}$ over $\mathbb{Q}[X]$.

3. (a) Let K be a finite field of order q. Show that the polynomial $X^{q^r} - X$ factors, in $K[X]$, as the product of all irreducible monic polynomials of degree dividing r.

   (b) Let K be a finite field of order q, let L/K be a field extension of degree d, and let $P(X)$ be an irreducible polynomial of degree e in $K[X]$. Show that $P(X)$ factors in $L[X]$ as the product of r irreducible polynomials, each of degree $\frac{e}{r}$, where r is the greatest common divisor of e and d.

4. (a) Give the definition of a *Dedekind domain*.

   (b) Let R be a Dedekind domain, let $\mathfrak{p}$ be a prime ideal of R, and let n be a positive integer. Show that the nonzero ideals of $R/\mathfrak{p}^n$ are the images, under the natural map:

   $$R \to R/\mathfrak{p}^n,$$

   of the ideals $R, \mathfrak{p}, \ldots, \mathfrak{p}^{n-1}$ of R.

   (c) Show that every ideal of $R/\mathfrak{p}^n$ is principal. [HINT: use 4b!]

(d) Let R be a Dedekind domain and let I be a nonzero ideal of R. Show that every ideal of R/I is principal.

(e) Show that every ideal of a Dedekind domain R can be generated by at most two elements.

5. Let K be a field, let V be a K-vector space of dimension d, and let $L : V \to V$ be a K-linear map. Let M_L be the $K[T]$-module corresponding to L.

   (a) Give the definition of the *minimal polynomial* of L.

   (b) Give (without proof) a description of the minimal polynomial and characteristic polynomial of L in terms of the module M_L and the classification of finitely generated $K[T]$-modules.

   (c) We say L is *regular* if the minimal polynomial of L is equal to its characteristic polynomial. Show that L is regular if, and only if, the module M_L is generated by a single element.

   (d) An element v of V is a *cyclic vector* for L if the set $\{v, Lv, L^2v, \ldots, L^{d-1}v\}$ is a basis for V. Show that there exists a cyclic vector for L if, and only if, L is regular.

M345P8 SOLUTIONS

(1) (a) An R-module M is *finitely generated* if there exists a finite set of elements $m_1, \ldots, m_d$ of M such that every element m of M can be written as $r_1 m_1 + \cdots + r_d m_d$ for some $r_1, \ldots, r_d \in R$. **Cat A, 1**

An R-module M is Noetherian if every increasing chain of submodules

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$$

eventually stabilizes; that is, there exists an integer n such that $M_i = M_n$ for all $i \geq n$. **Cat A, 1**

A ring R is a Noetherian ring if R is Noetherian as an R-module. **Cat A, 1**

(b) Suppose M is Noetherian and let N be a submodule of N. Suppose N is not finitely generated. Then inductively define submodules as follows: set $N_0 = \{0\}$, and for each $i > 0$, choose an element n_i in N but not N_{i-1}, and let N_i be the submodule generated by $\{n_1, n_2, \ldots, n_i\}$. (Such an n_i always exists since N is not finitely generated, so $N_i \subsetneq N$.) Then we have an infinite ascending chain:

$$N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \ldots$$

of submodules of M so M is not Noetherian. **Cat A, 2**

Conversely, suppose that every submodule of M is finitely generated, and let

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$$

be an ascending chain of submodules of M. Let N be the union of the N_i; then N is a submodule of M and thus generated by a finite set $n_1, \ldots, n_d$. Since these are in N, each lives in some N_i, so there exists n such that n_i is an element of N_n for all i. Then N_n contains N, so $N_n = N$. For all $i > n$, $N_n \subseteq N_i \subseteq N$, so $N_i = N$ and the tower stabilizes. **Cat A, 3**

(c) Let M be Noetherian and suppose that no quotient M/N of M is simple. We construct a strictly increasing chain of submodules of M inductively as follows: fix a submodule N_0 of M, not equal to M. For each i, M/N_i the quotient

is nonzero and not simple, so there exists a submodule J_i of M/N_i that is nonzero and not all of N_i. Let N_{i+1} be the preimage of J_i under the map $M \to M/N_i$. Then N_{i+1} strictly contains N_i and is strictly contained in M. We thus obtain an infinite chain:

$$N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \dots$$

contradicting the fact that M is Noetherian. **Cat A, 8**

(d) There are many possible examples. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}$. Then any nonzero submodule of M is of the form $n\mathbb{Z}$ for some nonzero integer n, and this is not simple since it properly contains $2n\mathbb{Z}$. **Cat B, 4**

(2) (a) (i) We have $X^{15} + X^5 + 1 = (X^3 + X + 1)^5$ over $\mathbb{F}_5$, and $X^3 + X + 1$ is irreducible since it has degree 3 and no roots in $\mathbb{F}_5$. **Cat A, 5**

(ii) We have $X^7 + X^6 + X^5 + X + 1 = (X^4 + X^3 + 1)(X^3 + X + 1)$. Both factors are irreducible since they have no roots over $\mathbb{F}_2$, hence no linear factors, and the degree 4 polynomial is not divisible by $X^2 + X + 1$. (The easiest way to find the degree 3 factor without trial and error is to take the GCD with $X^8 - X$.) **Cat B, 5**

(b) (i) We view $X^6Y^2 + Y + 1$ as a polynomial in Y with coefficients in $\mathbb{C}[X]$. The GCD of the coefficients is 1, so this polynomial is irreducible if and only if it is irreducible in $\mathbb{C}(X)[Y]$. Since it is quadratic in Y it suffices to show it has no roots in $\mathbb{C}(X)$; this holds if and only if its discriminant $1 - 4X^6$ is not a square in $\mathbb{C}(X)$. But $1 - 4X^6$ factors into distinct linear factors in $\mathbb{C}[X]$, so is not a square. **Cat A, 5**

(ii) Let $P(X) = X^4 + 2X^3 + 3X^2 + X + \frac{1}{8}$, and $Q(X) = 2^4 P(\frac{X}{2})$. Then $Q(X)$ is irreducible if and only if $P(X)$ is irreducible, and $Q(X) = X^4 + 4X^3 + 12X^2 + 16X + 2$. By Gauss' lemma $Q(X)$ is irreducible over $\mathbb{Q}[X]$ if, and only if, it is irreducible in $\mathbb{Z}[X]$, and it is irreducible in the latter by Eisenstein's criterion. **Cat B, 5**

(3) (a) We first show that every irreducible polynomial of degree d dividing r in $K[X]$ divides $X^{q^r} - X$. Let $P(X)$ be such a polynomial, and let α be a root of $P(X)$. Then the field $K(\alpha)$ is a field of order q^d, so $\alpha^{q^d} = \alpha$ in $K(\alpha)$. Then $\alpha^{q^r} = \alpha$ as well. Thus α is a root of $X^{q^r} - X$; since $P(X)$ is the minimal polynomial of α over K we must have $P(X)$ divides $X^{q^r} - X$ in $K[X]$. **Cat C, 4**

We next show that $X^{q^r} - X$ has no repeated factors; this is because its derivative is -1 in $K[X]$ and any repeated factor would divide the derivative.

Cat C, 4

Finally, we show that any irreducible factor of $X^{q^r} - X$ has degree dividing r. Let $P(X)$ be such a factor. Since $X^{q^r} - X$ factors into linear factors in a field L of q^r elements, $P(X)$ has a root α in L. Thus $K(\alpha)$ is a subfield of L, so the degree of α divides r. But the degree of α is equal to the degree of $P(X)$.

Cat C, 4

(b) By part (a), $P(X)$ divides $X^{q^n} - X$ if e divides n, and has no common factors with $X^{q^n} - X$ otherwise. It follows that $P(X)$ divides $X^{q^{dm}} - X$ if $\frac{e}{r}$ divides m, and has no common factors with $X^{(q^d)^m} - X$ otherwise. Thus any irreducible factor $Q(X)$ of $P(X)$ over L divides $X^{(q^d)^{\frac{e}{r}}} - X$, and hence has degree less than or equal to $\frac{e}{r}$. Since $Q(X)$ does not divide $X^{(q^d)^s} - X$ for any $s < \frac{e}{r}$, the degree of $Q(X)$ cannot be less than $\frac{e}{r}$ and the claim follows.

Cat D, 8

(4) (a) A Dedekind domain is an integral domain that is Noetherian and integrally closed, in which every nonzero prime ideal is maximal.

Cat A, 2

(b) Let I be an ideal of $R/\mathfrak{p}^n$. Then the preimage J of I in R is an ideal of R containing $\mathfrak{p}^n$. By unique factorization of ideals in a Dedekind domain, we have $J = \mathfrak{p}^i$ for $0 \leq i \leq n$. Then I is the image of J in $R/\mathfrak{p}^n$, since the natural map $R \to R/\mathfrak{p}^n$ is surjective.

Cat A, 4

(c) Let I be an ideal of $R/\mathfrak{p}^n$. Then I is the image of $\mathfrak{p}^i$ in $R/\mathfrak{p}^n$ for some i. By unique factorization of ideals, $\mathfrak{p}^i$ contains, but is not equal to $\mathfrak{p}^{i+1}$. Thus there exists an element x of $\mathfrak{p}^i$ that is not contained in $\mathfrak{p}^{i+1}$. Let y be the image of x in $R/\mathfrak{p}^n$. The ideal generated by y is contained in I but not contained in the image of $\mathfrak{p}^{i+1}$, and must therefore equal all of I, so I is principal.

Cat D, 4

(d) Write $I = {\mathfrak{p}_1}^n {\mathfrak{p}_2}^{n_2} \dots {\mathfrak{p}_r}^{n_r}$. By the Chinese remainder theorem, we have

$$R/I \cong R/{\mathfrak{p}_1}^{n_1} \times \cdots \times R/{\mathfrak{p}_r}^{n_r},$$

so any ideal J of R/I is a product of ideals J_i of $R/{\mathfrak{p}_i}^{n_i}$. Let y_i generate J_i; then the product of the y_i generates J, so J is principal.

cat B, 6

(e) Let I be a nonzero ideal of R, and let a be an element of I. Let J be the image of I in $R/\langle a \rangle$. Then J is principal,

so generated by an element y of J. There thus exists an element x of I mapping to y. We will show that $I = \langle x, a\rangle$. Certainly x and a are in I. On the other hand, let z be any element of I. Then the image of z in J is an element ry for some $r \in R$. Thus $z - rx$ is zero in $R/\langle a\rangle$ and thus equal to sa for some $s \in R$. Then $z = rx + sa$, so I is contained in $\langle x, a\rangle$. **cat D, 4**

(5) (a) The minimal polynomial of a linear map L is the unique monic generator of the ideal $\{P(T) : P(L) = 0\}$ of $K[T]$. **SEEN, 2**

(b) By the classification of finitely generated $K[T]$-modules, there exist unique nonconstant monic polynomials $P_1(T), \ldots, P_r(T)$ such that $P_1(T)|P_2(T)|\ldots|P_r(T)$ and

$$M_L \cong K[T]/\langle P_1(T)\rangle \times \cdots \times K[T]/\langle P_r(T)\rangle.$$

The minimal polynomial of L is $P_r(T)$ and the characteristic polynomial of L is $P_1(T)P_2(T)\ldots P_r(T)$. **SEEN, 4**

(c) If $P_r(T) = P_1(T)P_2(T)\ldots P_r(T)$ then $r = 1$, so $M_L \cong K[T]/\langle P_1(T)\rangle$. Conversely, if $M_L \cong K[T]/\langle P_1(T)\rangle$ then by the uniqueness of the invariant factors $P_i(T)$ we must have $r = 1$. **UNSEEN, 6**

(d) If L is regular then $M_L \cong K[T]/\langle P_1(T)\rangle$. The latter has a basis $1, T, T^2, \ldots T^{d-1}$, where d is the degree of $P_1(T)$. If v is the element of V that corresponds to $1 \in K[T]/\langle P_1(T)\rangle$, then T^i corresponds to $L^i v$. Thus $v, Lv, \ldots, L^{d-1}v$ is a basis for V. Conversely, if $v, Lv, \ldots, L^{d-1}v$ are linearly independent, then the minimal polynomial $P(T)$ of L cannot have degree less than d (as then $P(L)v = 0$ would give a linear dependence among $v, Lv, \ldots, L^{d-1}v$.) On the other hand, since the minimal polynomial of L divides the characteristic polynomial of L, and the latter has degree d, the minimal polynomial must equal the characteristic polynomial. **UNSEEN, 8**