Imperial College
London

MATH97063 MATH97174

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2021

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

Algebra 3

Date: Tuesday, 1 June 2021

Time: 09:00 to 11:30

Time Allowed: 2.5 hours

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

1. (a) Factor each of the following polynomials into irreducibles in $\mathbb{F}_3[X]$. Be sure to show that each factor is irreducible!

   (i) The polynomial $X^6 + X^3 + 1$. (5 marks)

   (ii) The polynomial $1 + X + X^2 + X^3 + X^4 + X^5 + X^6 + X^7$. (5 marks)

   (b) Let p be a prime and $q = p^r$ for some $r > 0$. Show that a polynomial $P(X)$ in $\mathbb{F}_q[X]$ is squarefree if, and only if, there exists an integer $d > 0$ such that $P(X)$ divides $X^{q^d} - X$. (10 marks)

(Total: 20 marks)

2. Let L be the abelian subgroup of $\mathbb{Z}^3$ generated by the vectors $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, $\begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$, and $\begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$.

   (a) Find a presentation matrix A for the abelian group $\mathbb{Z}^3/L$. (2 marks)

   (b) Find the Smith Normal Form of the matrix A from part a. (6 marks)

   (c) Find integers $r \geq 0$ and $a_1, \ldots, a_s$, with $a_1 | a_2 | \ldots | a_s$ such that $\mathbb{Z}^3/L$ is isomorphic to

$$\mathbb{Z}^r \times \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_s\mathbb{Z}.$$

   (4 marks)

   (d) Show that if M is an n by n matrix with entries in $\mathbb{Z}$ and nonzero determinant, and L' is the subgroup of $\mathbb{Z}^n$ generated by the columns of M, then $\mathbb{Z}^n/L'$ is a finite abelian group, and its number of elements is equal to $|\det(M)|$. (8 marks)

(Total: 20 marks)

3. For each claim, prove or give a counterexample.

(a) If R is a ring, M is an R-module, and N_1 and N_2 are finitely generated R-submodules of M, then $g(N_1 + N_2) = g(N_1) + g(N_2)$, where for any finitely generated R-submodule N of M, $g(N)$ denotes the smallest integer r such that N can be generated by r elements. (4 marks)

(b) If R is a Noetherian ring, and M is a finitely generated R-module, then any two minimal generating sets for M have the same number of elements. (A generating set S for M is said to be *minimal* if no proper subset of S generates M.) (4 marks)

(c) If R is a Noetherian ring, M is a finitely generated R-module, and N is an R-submodule of M, then $g(N) \leq g(M)$. (4 marks)

(d) If R is a principal ideal domain, and $N \subseteq R^m$ is a submodule, then N is generated by at most m elements. (8 marks)

(Total: 20 marks)

4. Let R be a principal ideal domain, and r, s nonzero elements of R such that r divides s.

(a) Show that we can write $s = s_1 s_2$, where s_1 and r are relatively prime, and s_2 is divisible only by primes dividing r. (2 marks)

(b) Using the Chinese remainder theorem, or otherwise, show that the natural quotient map:

$$(R/\langle s\rangle)^\times \to (R/\langle s_2\rangle)^\times$$

is surjective. (6 marks)

(c) Show that r divides s_2, and that the natural quotient map:

$$(R/\langle s_2\rangle)^\times \to (R/\langle r\rangle)^\times$$

is surjective. (6 marks)

(d) Show that the natural quotient map:

$$(R/\langle s\rangle)^\times \to (R/\langle r\rangle)^\times$$

is surjective. (3 marks)

(e) Give an example of a principal ideal domain R and an element r of R such that the natural quotient map:

$$R^\times \to (R/\langle r\rangle)^\times$$

is *not* surjective. (3 marks)

(Total: 20 marks)

5. Let R be a ring. The *Krull dimension* of R is the longest length r of a strictly increasing chain:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

of prime ideals $\mathfrak{p}_i$ of R. (We say that the Krull dimension is infinite if such chains exist of arbitrary length.)

(a) Show that a field has Krull dimension zero, and a principal ideal domain has Krull dimension one. [Recall that we do not consider fields to be principal ideal domains.] (3 marks)

(b) Give an example of an integral domain with Krull dimension greater than one. (3 marks)

(c) Let α be an irrational complex number, and $P(X)$ a nonzero monic polynomial with integer coefficients that has α as a root. Let r be an element of the ring $\mathbb{Z}[\alpha]$. Show that there exists a nonzero integer n such that r divides n in $\mathbb{Z}[\alpha]$. (5 marks)

(d) Show that for α as in part c, and I any nonzero ideal of $\mathbb{Z}[\alpha]$, the quotient $\mathbb{Z}[\alpha]/I$ is finite. (4 marks)

(e) Using part d, or otherwise, show that $\mathbb{Z}[\alpha]$ has Krull dimension one. (5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2021

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

XXX

Algebra 3 (Solutions)

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

1. (a) (i) We have $X^6 + X^3 + 1 = (X^2 + X + 1)^3 = (X - 1)^6$. $\boxed{5,\ \mathrm{A}}$

(ii) We have $X^9 - X = X(X-1)(1 + X + X^2 + X^3 + X^4 + X^5 + X^6 + X^7)$. We know that $X^9 - X$ factors over $\mathbb{F}_3$ as the product of all the irreducible monic polynomials of degree one or two, so $1 + X + X^2 + \cdots + X^7$ factors as $(X+1)(X^2+1)(X^2 - X - 1)(X^2 + X - 1)$ (the quadratic factors are irreducible as they have no roots.) $\boxed{5,\ \mathrm{A}}$

(b) Since the derivative of $X^{q^d} - X$ is -1 over $\mathbb{F}_q$, the polynomial $X^{q^d} - X$ is squarefree, so any divisor is likewise squarefree. $\boxed{4,\ \mathrm{C}}$

Conversely, if $P(X)$ is squarefree of degree d in $\mathbb{F}_q[X]$, then each irreducible factor has degree less than or equal to d, and occurs with multiplicity one in $P(X)$. Each such factor also occurs with multiplicity one in $X^{q^{d!}} - X$, so $P(X)$ divides $X^{q^{d!}} - X$. $\boxed{6,\ \mathrm{C}}$

2. (a) This quotient is generated by the classes of the standard basis $\{e_1, e_2, e_3\}$, and the relations are of the form $ae_1 + be_2 + ce_3 = 0$ for $(a, b, c) \in L$. Since L is generated by $(1, 2, 3)$, $(2, 3, 1)$, and $(3, 1, 2)$, the relations are generated by $e_1 + 2e_2 + 3e_3$, $2e_1 + 3e_2 + e_3$, and $3e_1 + e_2 + 2e_3$. Therefore, a presentation matrix is $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$.

2, A

(b) Applying row operations to zero out the bottom two entries in the first column yields the matrix:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -5 \\ 0 & -5 & -7 \end{pmatrix}.$$

One can then use the first column to zero out the two rightmost entries in the first row. One obtains:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -5 \\ 0 & -5 & -7 \end{pmatrix}.$$

Multiplying the second row by -1 and performing a further row and column operation to zero out the entries in positions $(2, 3)$ and $(3, 2)$, we find that the Smith normal form is diagonal with entries $1, 1, 18$.

6, A

(c) The Smith normal form constructed in part b shows that a suitable set of generators f_1, f_2, f_3 for $\mathbb{Z}^3/L$ satisfy the relations $f_1 = f_2 = 18f_3 = 0$. Thus $\mathbb{Z}^3/L$ is isomorphic to $\mathbb{Z}/18\mathbb{Z}$.

4, A

(d) The matrix M is a presentation matrix for $\mathbb{Z}^3/L'$. It can be put into Smith Normal Form by elementary row and column operations; these operations preserve the absolute value of the determinant of M. The Smith Normal Form of M is thus a diagonal matrix, and the product of the absolute values of the diagonal entries of this matrix is the absolute value of the determinant of M. If the diagonal entries are $a_1, \ldots, a_n$, then all of these are nonzero and we have an isomorphism:

$$\mathbb{Z}^3/L' \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}.$$

Thus the number of elements of $\mathbb{Z}^3/L'$ is the absolute value of the determinant of M.

8, D

3. (a) This is false. For instance, one can consider the any situation in which N_1 is nonzero and contained in N_2, as then $g(N_2)$ is nonzero, but $N_1 + N_2 = N_1$, so that $g(N_1 + N_2) = g(N_1)$. [4, B]

   (b) This is false. For instance, $\{1\}$ and $\{2, 3\}$ are minimal generating sets for $\mathbb{Z}$ as a $\mathbb{Z}$-module. [4, A]

   (c) This is also false. For instance, the ideal $\langle X, Y\rangle$ of $\mathbb{C}[X, Y]$ is contained in $\mathbb{C}[X, Y]$, but $g(\mathbb{C}[X, Y]) = 1$, and $g(\langle X, Y\rangle) = 2$. [4, B]

   (d) This is true. Indeed, by the classification of modules over a principal ideal domain, N is isomorphic to a module of the form

$$R^r \oplus R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_s\rangle$$

   for suitable elements $a_1, \ldots, a_s$. Since N is contained in the torsion-free R-module R^m, we must have $s = 0$; that is, N is free of rank r over R, and is in particular generated by r elements. It thus remains to show that $r \leq m$. Let K be the field of fractions of R, so that $K = S^{-1}R$ where S is the multiplicative system of nonzero elements of R. Then $S^{-1}N$ and $S^{-1}R^m$ are K-vector spaces, isomorphic to K^r and K^m, respectively. Since the former is contained in the latter we must have $r \leq m$ and the resutl follows. [8, D]

4. (a) We can certainly factor $s = p_1^{m_1} \dots p_a^{m_a} q_1^{n_1} \dots q_b^{n_b}$, where the p_i are distinct primes of R not dividing r and the q_j are distinct primes of R dividing r. We can then take $s_1 = p_1^{m_1} \dots p_a^{m_a}$ and $s_2 = q_1^{n_1} \dots q_b^{n_b}$. 2, A

(b) By construction s_1 and s_2 are relatively prime, as they have no common prime divisor. We thus have:

$$(R/\langle s_1 s_2 \rangle)^\times \cong (R/s_1)^\times \times (R/\langle s_2 \rangle)^\times$$

by the Chinese remainder theorem. The composition of this isomorphism with projection onto the second factor is the natural map

$$(R/\langle s \rangle)^\times \to (R/\langle s_2 \rangle)^\times$$

and since this is a composition of two surjections it is surjective. 6, B

(c) Since r divides $s = s_1 s_2$, and r and s_1 are relatively prime, we have that r divides s_2. In particular the primes dividing s_2 are precisely the same as those dividing r. Let $x \in (R/\langle r \rangle)^\times$; then there is an element x' of R that represents the class of x mod r. Note that x and s_2 are relatively prime; indeed, if p is a prime dividing both x and s_2, then p divides both x and r, which is impossible since x is invertible modulo r. Thus the image of x' in $R/\langle s_2 \rangle$ is an element of $(R/\langle s_2 \rangle)^\times$ that maps to x in $(R/\langle r \rangle)^\times$. 6, B

(d) The composition of the two surjections from parts c and d is the natural map $(R/\langle s \rangle)^\times \to (R/\langle r \rangle)^\times$, so the latter is surjective. 3, A

(e) We can take $R = \mathbb{Z}$, and $r = 5$. 3, B

5. (a) In a field the only prime ideal (indeed, the only ideal at all) is the zero ideal, so every chain has length zero. If R is a principal ideal domain then every nonzero prime ideal is maximal, so there are chains of length one, of the form $\{0\} \subsetneq \mathfrak{m}$ for $\mathfrak{m}$ a nonzero maximal ideal, but no longer chains. 3, M

(b) The ring $\mathbb{C}[X, Y]$ admits the chain $\{0\} \subseteq \langle X \rangle \subseteq \langle X, Y \rangle$ so has Krull dimension at least two (in fact its Krull dimension is precisely two.) 3, M

(c) Since r lies in $\mathbb{Q}(\alpha)$, it is algebraic over $\mathbb{Q}$. Let $Q(X)$ be the minimal polynomial of r over $\mathbb{Q}$, and choose an integer n so that $nQ(X)$ has integral coefficients. Note that $Q(0)$ is nonzero as $Q(X)$ is irreducible. Then $nQ(r) = 0$, and $nQ(r) - nQ(0)$ lies in the ideal generated by α. So $nQ(0)$ is a nonzero integer in the ideal generated by α. 5, M

(d) Let I be a nonzero ideal of $\mathbb{Z}[\alpha]$, and n a nonzero integer in I. Then $\mathbb{Z}[\alpha]/I$ is a quotient of $\mathbb{Z}[\alpha]/\langle n \rangle$. Note that (since $P(\alpha) = 0$), $\mathbb{Z}[\alpha]$ is spanned over $\mathbb{Z}$ by $1, \alpha, \dots, \alpha^{d-1}$, where d is the degree of $P(X)$. Thus $\mathbb{Z}[\alpha]/\langle n \rangle$ is spanned over $\mathbb{Z}/n\mathbb{Z}$ by at most d elements, and so consists of at most n^d elements. Thus $\mathbb{Z}[\alpha]/I$ is finite. 4, M

(e) We will show that every nonzero prime ideal of $\mathbb{Z}[\alpha]$ is maximal; the claim will then follow by the same argument as in part a. Let I be a nonzero prime ideal of $\mathbb{Z}[\alpha]$. Then $\mathbb{Z}[\alpha]/I$ is a finite integral domain, hence a field. $\boxed{5,\ \mathrm{M}}$

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	QuestionNumber	Comments for Students
MATH96038 MATH97063 MATH97174	1	This question was generally fine.
MATH96038 MATH97063 MATH97174	2	Most people had little trouble with this, although a few gave the presentation for the Q(T)-module attached to the matrix. Many more people got part d correct than I expected!
MATH96038 MATH97063 MATH97174	3	Parts a to c tested your ability to come up with simple counterexamples, and most people did well (particularly on part b). Part d is most easily solved by introducing denominators and working with vector spaces over the field of fractions, but other arguments are possible, and many of you found reasonable inductive arguments.
MATH96038 MATH97063 MATH97174	4	Part c in particular gave people far more difficulty than I expected; the solution to part b led many people to attempt to use the Chinese remainder theorem in part c, where it is of limited help. In particular note that a surjection of rings does not imply a surjection on units, as many people claimed (in spite of providing a counterexample to this very claim in part e!)
MATH96038 MATH97063 MATH97174	5	Part c was the most difficult part of this question, and amounted to showing that r satisfied a polynomial with integer coefficients. For this the easiest approach is to pass to the corresponding field extension, and then clear denominators in the minimal polynomial of r, but there were other arguments, using more of the theory of algebraic integers, that were also effective.