MATH97063 MATH70035

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2022

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

Algebra 3

Date: 24 May 2022

Time: 09:00 – 11:30 (BST)

Time Allowed: 2:30 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 AS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD WITH COMPLETED COVERSHEETS WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

1. (a) Show that the polynomials $X^3 + X^2 + 1$ and $X^3 + X + 1$ are irreducible over $\mathbb{F}_2$. (2 marks)

   (b) Let K and L denote the fields $\mathbb{F}_2(\alpha)$ and $\mathbb{F}_2(\beta)$, where α is a root of $X^3 + X^2 + 1$ and β is a root of $X^3 + X + 1$, and let f be an isomorphism from K to L. Describe, with proof, the possible values of $f(\alpha)$. (8 marks)

   (c) Find the minimal polynomial of $\sqrt{2} + i$ over $\mathbb{Q}$. (5 marks)

   (d) Show that the polynomial $P(X) = X^4 + X^3 + \frac{1}{8}$ is irreducible in $\mathbb{Q}[X]$. (5 marks)

(Total: 20 marks)

2. (a) Find the Smith normal form of the matrix:

$$\begin{pmatrix} 4 & 6 & -4 \\ 2 & -6 & 10 \\ 4 & 12 & 16 \end{pmatrix}.$$

(6 marks)

   (b) Up to isomorphism, how many abelian groups of order 3600 are there? (4 marks)

   (c) Let m and n be relatively prime integers. Show that any abelian group A of order mn has a unique subgroup B of order m and a unique subgroup C of order n, and describe a natural isomorphism from A to $B \times C$. (5 marks)

   (d) Let K be a field, V a finite-dimensional K-vector space, and let $L : V \to V$ a K-linear map. Suppose the characteristic polynomial of f factors as $P(X)Q(X)$ with $P(X)$ and $Q(X)$ relatively prime. Show that V is isomorphic to the direct sum of the kernels of the linear transformations $P(L)$ and $Q(L)$. (5 marks)

(Total: 20 marks)

3. (a) Let R be a ring, M an R-module, and $\mathfrak{m}$ a maximal ideal of R. Let $\mathfrak{m}M$ be the R-submodule of M consisting of all expressions of the form $a_1m_1 + \cdots + a_rm_r$ for r a positive integer, $\{a_i\}$ elements of $\mathfrak{m}$ and $\{m_i\}$ elements of M. Show that the quotient $M/\mathfrak{m}M$ has a natural structure of an $R/\mathfrak{m}$-vector space. (5 marks)

(b) Suppose M is generated as an R-module by a finite set of elements $m_1, \dots, m_s$ of M. Show that the dimension of $M/\mathfrak{m}M$ is at most s. (5 marks)

(c) Let K be a field and let R be the polynomial ring $K[X, Y]$. Let $\mathfrak{m}$ denote the ideal $\langle X, Y \rangle$. Show that $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ has dimension $n + 1$ as a K-vector space. (In particular, R has ideals with an arbitrarily large number of generators). (5 marks)

(d) Let R be any Noetherian ring, and let M be a finitely generated R-module. Let $f : M \to M$ be a surjective homomorphism of R-modules. Show that f is an isomorphism. (5 marks)

(Total: 20 marks)

4. Let R be a ring, and I an ideal of R. The *radical* of I, denoted $\sqrt{I}$, is the subset

$$\{x \in R : \exists n \in \mathbb{Z} > 0 : x^n \in I\}$$

of R.

(a) Show that for any ideal I, $\sqrt{I}$ is an ideal of R. (3 marks)

(b) Show that for any ideals I and J, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. (3 marks)

(c) Show that if $f : R \to S$ is a homomorphism of rings, and J is an ideal of S, then $\sqrt{f^{-1}J} = f^{-1}\sqrt{J}$. (5 marks)

(d) Show that if R is a Principal Ideal Domain then $\sqrt{I + J} = \sqrt{I} + \sqrt{J}$ for any ideals I, J of R. (5 marks)

(e) Give an example of a ring R, and ideals I and J, such that $\sqrt{I + J} \neq \sqrt{I} + \sqrt{J}$. (4 marks)

(Total: 20 marks)

5. Let K be a field, and let $f \in K[X]$ be a nonconstant polynomial of degree d.

(a) Show that the field of rational functions $K(X)$ is a finite extension of the subfield $K(f)$ of $K(X)$, of degree d. (7 marks)

(b) Show that if $g \in K[X]$ is a nonconstant polynomial then there exists a polynomial $P(T, U) \in K[T, U]$ such that $P(f(X), g(X)) = 0$. (6 marks)

(c) Show that if the degrees of f and g are relatively prime, then $K(f, g) = K(X)$. (3 marks)

(d) Suppose $K = \mathbb{F}_q$, let $P(T)$ be an irreducible polynomial with coefficients in $K(T)$, and let $L = K(T)(\alpha)$, where α is a root of $P(T)$. Show that the Frobenius endomorphism $x \mapsto x^q$ is not surjective on L. (4 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2022

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

MATH96038/MATH97063/MATH97174

Algebra 3 (Solutions)

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

1. (a) Both polynomials are of degree three and these are irreducible if they have no root in $\mathbb{F}_2$; this is easily checked. seen ⇓

2, A

(b) Since α is a root of $X^3 + X^2 + 1$, the images of α in $K(\beta)$ must also be roots of $X^3 + X^2 + 1$. Conversely, if γ is any such root in $\mathbb{F}_2(\beta)$, the natural map $\mathbb{F}_2[X] \to K(\beta)$ taking X to γ has kernel equal to $\langle X^3+X^2+1\rangle$ and hence descends to a map $\mathbb{F}_2(\alpha) \to \mathbb{F}_2(\beta)$. This map is injective since it is a ring homomorphism of fields, and surjective by a dimension count, so it is an isomorphism. sim. seen ⇓

We are thus reduced to finding the roots of $X^3 + X^2 + 1$ in $K(\beta)$; there are three such roots, given by $\beta + 1$, $\beta^2 + 1$, and $\beta^2 + \beta + 1$.

8, B

(c) Note that i has degree 2 over $\mathbb{Q}(\sqrt{2})$, since it is a root of the polynomial $X^2 + 1$ but is not contained in $\mathbb{Q}(\sqrt{2})$ (as it is not even contained in $\mathbb{R}$!). Thus $\mathbb{Q}(\sqrt{2}, i)$ is an extension of degree 4 over $\mathbb{Q}$, with basis $\{1, \sqrt{2}, i, i\sqrt{2}\}$. The first four powers of $\sqrt{2} + i$ are 1, $\sqrt{2} + i$, $1 + 2i\sqrt{2}$, $5i - \sqrt{2}$, and $-7 + 4i\sqrt{2}$. The first three of these are linearly independent, and taking linear combinations we see that $\sqrt{2}+i$ is a root of $X^4 - 2X^2 + 9$, which must therefore be the desired minimal polynomial. sim. seen ⇓

5, A

(d) Note that $P(X)$ is irreducible if, and only if, $Q(X) = 2^4 P(\frac{X}{2})$ is irreducible. But $Q(X) = X^4 + 2X^3 + 2$, which is irreducible over $\mathbb{Z}[X]$ by Eisenstein's criterion, and hence also irreducible in $\mathbb{Q}[X]$. sim. seen ⇓

5, C

2. (a) Exchanging the first two rows and then subtracting appropriate multiples of the first column from the next two gives the matrix: meth seen ⇓

$$\begin{pmatrix} 2 & 0 & 0 \\ 4 & 18 & -24 \\ 4 & 24 & -4 \end{pmatrix}.$$

Subtracting twice the first row from each of the next two yields a two in the upper left, and the submatrix

$$\begin{pmatrix} 18 & -24 \\ 24 & -4 \end{pmatrix}$$

in the lower right. It remains to put this submatrix in Smith normal form, but we have seen in lectures that for a 2×2 matrix, the Smith normal form is diagonal with entries (a, b), where a is a gcd of the entries and b is the determinant divided by a. Thus the Smith normal form of the 3×3 matrix is diagonal with entries $2, 2, 252$. 6, A

(b) We have $3600 = 2^4 \cdot 3^2 \cdot 5^2$. There are thus 5 possibilities for the 2-part, namely $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^4$. Similarly there are 2 possibilties for the 3-part and the 5-part, for a total of $5 \cdot 2 \cdot 2 = 20$ possible groups. sim. seen ⇓ 4, B

(c) This can be deduced from the classification but can also be seen directly: let $B = nA$ and $C = mA$. We then have a group homomorphism sim. seen ⇓

$$B \times C \to A$$

that takes (b, c) to $b + c$. To construct an inverse homomorphism, write $1 = sn + rm$ for integers r, s; then for any $a \in A$, $a = sna + rma$ writes a as the sum of an element of B and an element of C, and the map $a \mapsto (sna, rma)$ is a homomorphism from A to $B \times C$ that is inverse to the one constructed above. It remains to show that B has order m and C has order n; note that B is killed by multiplication by m so its order is divisible only by primes dividing m. Similarly the order of C is divisible only by primes dividing n. Since the product of these orders is mn, the claim follows. 5, A

(d) We mimic the argument given above: let V_1 be the kernel of $P(L)$ and V_2 the kernel of $Q(L)$. We have a map: unseen ⇓

$$V_1 \oplus V_2 \to V$$

that takes (v_1, v_2) to $v_1 + v_2$. Conversely, we can write $1 = R(X)P(X) + S(X)Q(X)$ for polynomials $R(X), S(X)$ in $K[X]$. Then for any $v \in V$, we have $v = P(L)R(L)v + Q(L)S(L)v$, and (since $P(L)Q(L) = 0$ by Cayley-Hamilton) $P(L)R(L)v$ lies in the kernel of $Q(L)$, and $Q(L)S(L)v$ lies in the kernel of $P(L)$. Thus $v \mapsto (Q(L)S(L)v, P(L)R(L)v)$ gives a linear map $V \to V_1 \oplus V_2$ inverse to the first map. 5, C

3. (a) It suffices to show that the natural multiplication of R on $M/\mathfrak{m}M$ descends to a multiplication of $R/\mathfrak{m}$ on $M/\mathfrak{m}M$. For $r+\mathfrak{m}$ in $R/\mathfrak{m}$ and $m+\mathfrak{m}M$ in $M/\mathfrak{m}M$, we define $(r+\mathfrak{m})(m+\mathfrak{m}M) = rm+\mathfrak{m}M$. This is well-defined, since if we replace r by r' with $r-r' \in \mathfrak{m}$ then $(r-r')m$ lies in $\mathfrak{m}M$. Similarly if we replace m by m' with $m-m'$ in $\mathfrak{m}M$ then $r(m-m')$ lies in $\mathfrak{m}M$ as well. $\boxed{\text{seen} \Downarrow}$ $\boxed{5, \text{A}}$

(b) The elements $m_1+\mathfrak{m}M, \dots, m_s+\mathfrak{m}M$ generate $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-module and thus span it as a vector space, so the dimension bound follows. $\boxed{\text{sim. seen} \Downarrow}$ $\boxed{5, \text{A}}$

(c) The ideal $\langle X, Y\rangle^n$ is spanned by the monomials in X and Y of degree at least n; in particular the quotient $\langle X, Y\rangle^n/\langle X, Y\rangle^{n+1}$ is spanned by the monomials of degree exactly n. Since no nonzero K-linear combination of such monomials is in the span of the monomials of degree at least $n+1$, they form a basis for this quotient. $\boxed{\text{sim. seen} \Downarrow}$ $\boxed{5, \text{A}}$

(d) Since M is a finitely generated module over the Noetherian ring R, the module M is a Noetherian R-module. Suppose f is not injective, and consider the increasing chain of submodules: $\boxed{\text{unseen} \Downarrow}$

$$\ker f \subseteq \ker f^2 \subseteq \dots$$

Since f is surjective, so is f^n for all n; in particular if a is a nonzero element of $\ker f^n$ that is not in the kernel of f^{n-1}, then any c such that $f(c) = a$ is in the kernel of f^{n+1} but not in the kernel of f^n. Thus the chain of submodules is strictly increasing; this is impossible so f must be injective. $\boxed{5, \text{D}}$

4. (a) It is clear that $\sqrt{I}$ is closed under multiplication by elements of r. For closure under addition, note that if x^n and y^m are in I, then $(x+y)^{n+m}$ is in I, as each term in the expansion is divisible by either x^n or y^m. Thus $x+y$ lies in $\sqrt{I}$ if x and y do. sim. seen ⇓

3, B

(b) If x lies in $\sqrt{I \cap J}$ if and only if there exists an integer n such that x^n lies in $I \cap J$, in which case x^n lies in I and J, so x lies in $\sqrt{I} \cap \sqrt{J}$. Conversely if x lies in $\sqrt{I} \cap \sqrt{J}$ then there exist m and n such that x^m lies in I and x^n lies in J; then for $k \geq m, n$ we have $x^k \in I \cap J$, so $x \in \sqrt{I \cap J}$. sim. seen ⇓

3, A

(c) If x lies in $\sqrt{f^{-1}I}$ then for some n, $f(x^n)$ lies in I. Then $f(x)^n$ lies in I, so $f(x)$ lies in $\sqrt{I}$ and hence x lies in $f^{-1}(\sqrt{I})$. Conversely, if x lies in $f^{-1}(\sqrt{I})$ then $f(x)^n$ lies in I for some n, so $f(x^n)$ lies in I, which implies that x^n lies in $f^{-1}(I)$. So x lies in $f^{-1}(\sqrt{I})$ as required. sim. seen ⇓

5, B

(d) Let I and J be generated by i and j, respectively. Then $\sqrt{I}$ and $\sqrt{J}$ are generated by i' and j', where i' is the product of the primes dividing i and j' is the product of the primes dividing j. On the other hand $I+J$ is generated by a greatest common divisor k of i and j, and thus $\sqrt{I+J}$ is thus generated by the product k' of the primes dividing both i and j. But such a k' is a greatest common divisor of i' and j', so $\sqrt{I+J} = \sqrt{I} + \sqrt{J}$. unseen ⇓

5, D

(e) Let $R = K[X,Y]$ for some field K, and let $I = \langle X \rangle$, and $J = \langle X - Y^2 \rangle$. Then both I and J are prime ideals, since we have $R/I \cong R/J \cong K[Y]$ an integral domain. In particular $\sqrt{I} = I$ and $\sqrt{J} = J$, since I being prime means $x^n \in I$ implies $x \in I$. On the other hand $I + J = \langle X, Y^2 \rangle$, and $\sqrt{I+J} = \langle X, Y \rangle \neq \sqrt{I} + \sqrt{J}$. unseen ⇓

4, D

5. (a) Let $f(X) = a_d X^d + \cdots + a_0$, with $a_i \in K$. Then X is a root of the polynomial $P(T) := a_d T^d + a_{d-1} T^{d-1} + \cdots + a_0 - f$, which lies in $K(f)[T]$. In particular X is algebraic over $K(f)$; we must show that $P(T)$ is irreducible in $K(f)[T]$. On the other hand, $K(f)$ is the field of fractions of $K[f]$, and $P(T)$ is irreducible in $K(f)[T]$ if and only if it is irreducible in $K(f,T)$ and thus if and only if it is irreducible in $K(T)[f]$. But $P(T)$ has degree one in f, so irreducibility in the latter sense is clear. $\boxed{7, \mathrm{M}}$

(b) Certainly $K(f,g)$ is contained in $K(X)$, and thus g is algebraic over $K(f)$. There is thus a polynomial $Q(U)$, with coefficients in $K(f)$, such that $Q(g) = 0$. The coefficients of $Q(U)$ are rational functions in f; clearing denominators we obtain a polynomial $R(U)$, whose coefficients are in $K[f]$, such that $R(g) = 0$. Replacing each occurence of f in this polynomial with the variable T, we obtain a polynomial $P(T,U)$ in $K[T,U]$ such that $P(f,g) = 0$. $\boxed{6, \mathrm{M}}$

(c) The degree of $K(X)$ over $K(f,g)$ divides both the degree of $K(X)$ over $K(f)$ and the degree of $K(X)$ over $K(g)$. Since these degrees are relatively prime we must have $K(f,g) = K(X)$. $\boxed{3, \mathrm{M}}$

(d) Every element of L can be written as a polynomial in X and α, with coefficients in $\mathbb{F}_q$. Since $x \mapsto x^q$ is the identity on K, we see that the image of L under this map is $K(X^q, \alpha^q)$. It thus suffices to show that the degree of L over $K(X^q, \alpha^q)$ is positive. Let d be the degree of α over $K(X)$. Then the degree of L over $K(X^q)$ is dq, by part (a). On the other hand if $P(T) = a_d T^d + \cdots + a_0$, then α^q is a root of the polynomial $a_d^q T^d + \cdots + a_0^q$, which has coefficients in $K(X^q)$ and has degree d. Thus the degree of $K(X^q, \alpha^q)$ over $K(X^q)$ is at most d, and the claim follows. $\boxed{4, \mathrm{M}}$

Review of mark distribution:
Total A marks: 36 of 32 marks
Total B marks: 20 of 20 marks
Total C marks: 10 of 12 marks
Total D marks: 14 of 16 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.

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 separate pdf file with your email.

ExamModuleCode	**QuestionNumber**	**Comments for Students**
Algebra 3_MATH60035 MATH97063 MATH70035	1	The early parts of this question were routine, but several people attempted to do part d "by hand"; this is possible but much harder than finding the equivalent monic polynomial with integral coefficients
Algebra 3_MATH60035 MATH97063 MATH70035	2	It was possible to solve part c by invoking the classification (this makes existence clear) but uniqueness still needs some justification.
Algebra 3_MATH60035 MATH97063 MATH70035	3	I was happy to see as many complete and correct solutions to part d as there were!
Algebra 3_MATH60035 MATH97063 MATH70035	4	Many students struggled with part d, as one has to think in terms of prime factorizations and realize that ideal sum is the same as "greatest common divisor" in a PID
Algebra 3_MATH60035 MATH97063 MATH70035	5	Many students struggled to make the conceptual distinction between the variable X (in the field of coefficients) and the auxiliary variable they needed to introduce in order to make sense of the notion "minimal polynomial of X over K(f)".