

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
Summer 2025

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

Algebra 3

Date: Thursday, May 8, 2025

Time: Start time 10:00 – End time 12:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

This is a closed book examination.

Candidates should start their solutions 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.

Credit will be given for all questions attempted.

Allow margins for marking.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO DO SO

N.B.

- (1) When answering a question, or part of a question, you are permitted to quote statements from other questions or parts even if you have not answered them.
- (2) You are permitted to use without proof any statement that is proved in the written notes, provided that you make it clear which statement you are using. Unless instructed otherwise, you must justify all other statements that you make.
- (3) Throughout this paper we use the following **notation**. For a complex number $z = x + yi$ (where $x, y \in \mathbb{R}$), $\bar{z} = z - yi$ denotes the complex conjugate, and $\Re z = x$, $\Im z = y$ denote the real and imaginary part of z . If A is a matrix of complex numbers, A^T and \bar{A} denote the transpose and the complex conjugate of A , and $A^\dagger = \bar{A}^T$. If $A = (a_{ij})$ is a square matrix, then $\text{Tr}(A) = \sum a_{ii}$ denotes the trace of A .

1. For each of the following assertions, either briefly sketch a justification or provide a counterexample (you don't need to prove that your counterexample really is a counterexample).

(i) Let R be a commutative ring and $I, J \subset R$ ideals. The natural ring homomorphism $R/(I \cap J) \rightarrow R/I \times R/J$ is an isomorphism. (4 marks)

(ii) The polynomial

$$1 + 3x + 3x^2 + x^3 + x^3y \in \mathbb{C}[x, y]$$

is irreducible. (3 marks)

(iii) The ring $\mathbb{Z}[x]$ is a principal ideal domain. (3 marks)

(iv) Every \mathbb{C} -subalgebra of $\mathbb{C}[x, y]$ is a finitely generated \mathbb{C} -algebra. (3 marks)

(v) Let R be a commutative ring, M an R -module and $N \leq M$ an R -submodule. If $P = M/N$ is a free module, then M is isomorphic to the direct sum $N \oplus P$. (4 marks)

(vi) The matrix exponential

$$\exp: M_{2 \times 2}(\mathbb{C}) \rightarrow \text{GL}_2(\mathbb{C})$$

is a group homomorphism. (3 marks)

(Total: 20 marks)

2. Recall the following definitions and facts:

(1) A *real quaternion* is an expression

$$z = a + bi + cj + dk \quad \text{where } a, b, c, d \in \mathbb{R},$$

and the set of real quaternions is a ring with multiplication such that

$$i^2 = j^2 = k^2 = -1 \quad \text{and} \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

(2) The *norm* of a real quaternion $z = a + bi + cj + dk$ is the positive real number

$$N(z) = a^2 + b^2 + c^2 + d^2.$$

You may use without proof that for all real quaternions z, w , $N(zw) = N(z)N(w)$.

(3) A *Hurwitz quaternion* is a real quaternion

$$\zeta \in \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k + \mathbb{Z}\frac{1+i+j+k}{2}.$$

- (a) Prove carefully that the set of Hurwitz quaternions is a ring. (6 marks)
- (b) Show that for all real quaternions z , there exists a Hurwitz quaternion ζ such that $N(z-\zeta) < 1$. (7 marks)
- (c) Let α, β be Hurwitz quaternions with $\beta \neq 0$. Show that there are Hurwitz quaternions γ, ρ and γ', ρ' such that

$$\alpha = \gamma\beta + \rho, \quad \alpha = \beta\gamma' + \rho'$$

and $N(\rho) < N(\beta)$, $N(\rho') < N(\beta)$. (7 marks)

(Total: 20 marks)

3. (a) Consider a finite subgroup $G \leq \mathrm{GL}_n(\mathbb{C})$ acting naturally on the polynomial ring $R = \mathbb{C}[x_1, \dots, x_n]$ and denote by R^G the ring of invariants. For $i = 1, \dots, n$, define the polynomials $P^{x_i}(T)$ and briefly explain why the coefficients of $P^{x_i}(T)$ are in R^G . State a result providing an explicit finite set of generators of the ring R^G as a \mathbb{C} -algebra. (The result is a corollary of E. Noether's proof that R^G is a finitely generated \mathbb{C} -algebra but you don't need to say this, nor explain how the result follows from E. Noether's proof.) (5 marks)

- (b) Let now $n \geq 1$ be an integer, and let $G = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$ act on $R = \mathbb{C}[x_1, x_2]$ by:

$$\zeta: x_1 \mapsto \zeta x_1 \quad \text{and} \quad x_2 \mapsto \zeta x_2.$$

For $i = 1, 2$, compute the polynomials $P^{x_i}(T)$. (2 marks)

- (c) Denote by $\rho: R \rightarrow R^G$ the Reynolds operator for the action defined in Part (b). Prove that, for all monomials $M = x_1^{n_1} x_2^{n_2}$,

$$\rho(M) = \begin{cases} M & \text{if } M \in R^G \\ 0 & \text{if } M \notin R^G \end{cases}.$$

(5 marks)

- (d) Consider again the action defined in Part (b). Using all the previous parts, construct an explicit set of generators of R^G .

Write $R^{(n)} = \bigoplus_{k \geq 0} R_{nk}$, where R_{nk} denotes the set of homogeneous polynomials of degree nk . Prove that

$$R^G = R^{(n)}.$$

(8 marks)

(Total: 20 marks)

4. In this question, you may use without proof that

$$\mathrm{SU}_2 = \left\{ \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C}, a\bar{a} + b\bar{b} = 1 \right\}.$$

- (a) Let V be the \mathbb{R} -vector space of complex matrices of the form

$$X = \begin{pmatrix} x_1 + x_2 i & x_3 + x_4 i \\ -x_3 + x_4 i & x_1 - x_2 i \end{pmatrix}$$

where $x_1, x_2, x_3, x_4 \in \mathbb{R}$. Prove that the formula:

$$(X, Y) = \Re \operatorname{Tr}(XY^\dagger)$$

defines a positive definite symmetric bilinear form on V . (6 marks)

- (b) Prove that the formula

$$(g, h): X \mapsto gXh^\dagger$$

defines an action of $\mathrm{SU}_2 \times \mathrm{SU}_2$ on V . (7 marks)

- (c) Prove that the action of Part (b) preserves the inner product of Part (a) and hence it defines a group homomorphism $\mathrm{SU}_2 \times \mathrm{SU}_2 \rightarrow \mathrm{SO}_4(\mathbb{R})$. (7 marks)

(Total: 20 marks)

5. In this question we work with the graded ring $S = \mathbb{C}[y_1, y_2, y_3, y_4]$ and we order the monomial in S lexicographically. If $f \in S$, then $\text{LM } f$ denotes the leading monomial of f .

We will work with the polynomials:

$$f_1 = y_1 y_3 - y_2^2, \quad f_2 = y_1 y_4 - y_2 y_3, \quad f_3 = y_2 y_4 - y_3^2$$

and the ideal $I = (f_1, f_2, f_3) \subset S$. Note that $\text{LM } f_1 = y_1 y_3 > \text{LM } f_2 = y_1 y_4 > \text{LM } f_3 = y_2 y_4$.

- (a) Denote by $S_d \subset S$ the set of polynomials of degree d . Prove that a degree d monomial m is not divisible by any of the $m_i = \text{LM } f_i$ if and only if m is one of the following monomials:
- (1) $m = y_1^a y_2^{d-a}$ with $a > 0$, or
 - (2) $m = y_2^a y_3^{d-a}$ with $a > 0$, or
 - (3) $m = y_3^a y_4^{d-a}$.
- (5 marks)
- (b) Let $g \in S_d$ be a degree d polynomial. Show that there exists an element $f \in I$ such that $g = f + r$, where r is one of the monomials (1), (2), or (3) in Part (a). (5 marks)
- (c) Let now $R = \mathbb{C}[x_1, x_2]$. Show that $I \subset S$ is the kernel of the the ring homomorphism

$$\pi: S \rightarrow R, \quad \text{where} \quad \pi(y_1) = x_1^3, \quad \pi(y_2) = x_1^2 x_2, \quad \pi(y_3) = x_1 x_2^2, \quad \pi(y_4) = x_2^3.$$

(5 marks)

- (d) Let $G = \{\zeta \in \mathbb{C} \mid \zeta^3 = 1\}$ act on $R = \mathbb{C}[x_1, x_2]$ by:

$$\zeta: x_1 \mapsto \zeta x_1 \quad \text{and} \quad x_2 \mapsto \zeta x_2$$

and denote by R^G the ring of invariants. Show that the homomorphism π of Part (c) defines an isomorphism:

$$\pi: \mathbb{C}[y_1, y_2, y_3, y_4]/I \xrightarrow{\cong} R^G.$$

[Hint. You must use Question 3(d).] (5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2025

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

MATH60035/70035

ALGEBRA 3 (Solutions)

Setter's signature

.....

Checker's signature

.....

Editor's signature

.....

1. (i) The statement is false. A counterexample is $R = \mathbb{C}[x, y]$, $I = (x)$, $J = (y)$, $I \cap J = (xy)$. The ring $\mathbb{C}[x, y]/xy$ is not isomorphic to the product ring $\mathbb{C}[x] \times \mathbb{C}[y]$
- seen ↓
- (ii) The polynomial is irreducible: it is linear in y and $\text{hcf}((1+x)^3, x^3) = 1$.
- 4, C
- (iii) The statement is false: the ideal $(2, x) \subset \mathbb{Z}[x]$ is not principal.
- unseen ↓
- (iv) The statement is false; for example consider the \mathbb{C} -subalgebra of $\mathbb{C}[x, y]$ generated by y, xy, x^2y, \dots
- 3, B
- (v) The statement is true. Denote by $\iota: N \rightarrow M$ be the natural inclusion and $\pi: M \rightarrow P$ the homomorphism to the quotient. Let $s: P \rightarrow M$ be such that $\pi \circ s = \text{id}_P$. One verifies that the direct sum homomorphism $(\iota, s): N \oplus P \rightarrow M$ — provided by the universal property of the direct sum construction — is an isomorphism.
- seen ↓
- (vi) The statement is false. A counterexample is given by $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.
(The key point is that these matrices do not commute.)
- 3, A
- seen ↓
- 3, B
- seen ↓
- 4, D
- unseen ↓
- 3, A

2. (a) The key point is to show that the set \mathbb{H} of Hurwitz quaternions is closed under multiplication.

unseen ↓

The calculation:

$$\frac{1+i+j+k}{2}i = -\frac{1}{2} + \frac{i}{2} + \frac{j}{2} - \frac{k}{2} = i + j - \frac{1+i+j+k}{2} \in \mathbb{H},$$

shows that the product $\frac{1+i+j+k}{2}i$, which is *a priori* a real quaternion, is in fact an element of \mathbb{H} . Similar calculations show that the products $\frac{1+i+j+k}{2}j$ and $\frac{1+i+j+k}{2}k$ are also in \mathbb{H} .

Similarly, we see that:

$$\begin{aligned} \frac{1+i+j+k}{2} \frac{1+i+j+k}{2} &= \frac{(1-1-1-1)+(1+1+1-1)i+\dots}{4} \\ &= \frac{-1+i+j+k}{2} \in \mathbb{H}. \end{aligned}$$

6, A

unseen ↓

- (b) We will use the following fact: for all $a \in \mathbb{R}$, either there exists an integer $\alpha \in \mathbb{Z}$ such that $|a - \alpha| < \frac{1}{2}$, or there exists an integer α such that $a = \alpha + \frac{1}{2}$.

Let $z = a + bi + cj + dk$ be a real quaternion. By what we just said:

Either There exists an integer quaternion $\zeta = \alpha + \beta i + \gamma j + \delta k$ where: $|a - \alpha| \leq \frac{1}{2}$, $|b - \beta| \leq \frac{1}{2}$, $|c - \gamma| \leq \frac{1}{2}$, $|d - \delta| \leq \frac{1}{2}$ with at least one strict inequality. In this case

$$N(z - \zeta) < \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$$

and we are done.

Or There exists an integer quaternion $\zeta = \alpha + \beta i + \gamma j + \delta k$ where

$$z = \zeta + \frac{1+i+j+k}{2}.$$

In this case z is a Hurwitz quaternion and we are done.

- (c) First off we prove the left Euclid property: by Part (b) there exists $\gamma \in \mathbb{H}$ such that

7, B

seen ↓

$$N(\alpha\beta^{-1} - \gamma) < 1.$$

Then setting $\rho = \alpha - \gamma\beta$, we have by the multiplicativity of the norm (2) that

$$N(\rho) = N((\alpha\beta^{-1} - \gamma)\beta) = N(\alpha\beta^{-1} - \gamma)N(\beta) < N(\beta)$$

and we are done.

Second, the right Euclid property is similar.

7, B

3. (a) For $i = 1, \dots, n$ we define:

seen ↓

$$P^{x_i}(T) = \prod_{g \in G} (T - g(x_i)) .$$

The coefficients of $P^{x_i}(T)$ lie in R^G because the RHS is manifestly G -invariant.

The ring R^G is generated as a \mathbb{C} -algebra by the coefficients of the $P^{x_i}(T)$ and the

$$\rho(\mathbf{x}^m) \quad \text{for } |m| < |G|$$

where ρ is the Reynolds operator, $m = (m_1, \dots, m_n)$, and $|m| = \max\{m_i\}$.

5, A

(b)

$$P^{x_1}(T) = T^n - x_1^n \quad \text{and} \quad P^{x_2}(T) = T^n - x_2^n .$$

sim. seen ↓

2, A

- (c) It is clear that for all $g \in G$ and all monomials M , gM is a multiple of M . It follows from the formula defining the Reynolds operator that $\rho(M)$ is also a multiple of M , and hence, because $\rho: R \rightarrow R^G$ and $\rho|_{R^G} = \text{id}_{R^G}$, the statement.

sim. seen ↓

- (d) By Parts (a) and (b), R^G is generated by x_1^n, x_2^n , and the $\rho(x_1^a x_2^b)$ where $\max\{a, b\} < n$.

5, B

By Part (c) for all a, b :

sim. seen ↓

$$\rho(x_1^a x_2^b) = \begin{cases} x_1^a x_2^b & \text{if } n|a+b \\ 0 & \text{otherwise} \end{cases} . \quad (1)$$

First off, it follows from this that R^G is generated by the $x_1^a x_2^{n-a}$, $a = 0, \dots, n$.

Second, it follows from Equation 1 that $R^{(n)} \subset R^G$. On the other hand, because R^G is generated by R_n , and $R_n \subset R^{(n)}$, it follows that $R^G \subset R^{(n)}$. Hence $R^G = R^{(n)}$ as stated.

8, C

4. (a) The following explicit computation shows the statement.

unseen ↓

$$\begin{aligned}\Re \operatorname{Tr}(XY^\dagger) &= \Re \operatorname{Tr} \left(\begin{pmatrix} x_1 + x_2i & x_3 + x_4i \\ -x_3 + x_4i & x_1 - x_2i \end{pmatrix} \begin{pmatrix} y_1 - y_2i & -y_3 - y_4i \\ y_3 - y_4i & y_1 + y_2i \end{pmatrix} \right) = \\ &= (x_1 + x_2i)(y_1 - y_2i) + (x_3 + x_4i)(y_3 - y_4i) + \\ &\quad + (-x_3 + x_4i)(-y_3 - y_4i) + (x_1 - x_2i)(y_1 + y_2i) = \\ &= 2(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4).\end{aligned}$$

6, A

- (b) It is enough to show that for all $A \in \mathrm{SU}_2$ and all $X \in V$, $AX \in V$ and $XA \in V$. Writing $A \in \mathrm{SU}_2$ as

$$A = \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$$

with $a = a_1 + a_2i$, $b = -a_3 + a_4i$ we compute:

$$AX = \begin{pmatrix} a_1 + a_2i & a_3 + a_4i \\ -a_3 + a_4i & a_1 - a_2i \end{pmatrix} \begin{pmatrix} x_1 + x_2i & x_3 + x_4i \\ -x_3 + x_4i & x_1 - x_2i \end{pmatrix} \in V,$$

and, similarly, $XA \in V$.

- (c) Acting with $(A, B) \in \mathrm{SU}_2 \times \mathrm{SU}_2$ we get:

7, A

unseen ↓

$$\begin{aligned}\Re \operatorname{Tr} \left((AXB^\dagger)(AYB^\dagger)^\dagger \right) &= \Re \operatorname{Tr} \left((AXB^\dagger)(BY^\dagger A^\dagger) \right) = \\ &= \Re \operatorname{Tr} \left(A(XY^\dagger)A^{-1} \right) = \Re \operatorname{Tr}(XY^\dagger).\end{aligned}$$

Because elements $(A, B) \in \mathrm{SU}_2 \times \mathrm{SU}_2$ act linearly on V , and by Part (a), we get a group homomorphism $\mathrm{SU}_2 \times \mathrm{SU}_2 \rightarrow \mathrm{SO}_3(\mathbb{R})$.

7, C

Mastery. (a) If m is not divisible by y_1y_3 then

Either For some $a \geq 0$, $m = y_1^a m_{2,4}$ where $m_{2,4}$ is a monomial in y_2, y_4 only.

Suppose $a > 0$: if, furthermore, m is not divisible by y_1y_4 , then for some b $m_{2,4} = y_2^b$ and we are in case (1). If $a = 0$, then $m = m_{2,4}$ and the statement is easy.

Or For some $a \geq 0$, $m = y_3^a m_{2,4}$ where $m_{2,4}$ is a monomial in y_2, y_4 only. This case is similar to the previous case.

5, M

(b) The statement is essentially an immediate consequence of the division algorithm in S by the set $\{f_1, f_2, f_3\}$.

3, M

(c) First off, substitution shows that the polynomials f_1, f_2, f_3 are all in $\text{Ker } \pi$ and hence $I \subset \text{Ker } \pi$.

We next show that $\text{Ker } \pi \subset I$. Pick $g \in \text{Ker } \pi$: we claim that $g \in I$. By the division algorithm there is an element $f \in I$ such that $g = f + r$ and either $r = 0$ or $\text{LM } r$ is one of the monomials (1)–(3) of Part (a). If $r = 0$ then $g \in I$ and we are done. We will derive a contradiction assuming that $\text{LM } r$ is one of the monomials (1)–(3) of Part (a). None of these monomials is in $\text{Ker } \pi$ and this, together with the fact that π is graded, implies that $r \notin \text{Ker } \pi$. It follows $g \notin \text{Ker } \pi$, a contradiction.

7, M

(d) By Question 3(d) $R^G = R^{(3)}$ is generated by R_3 as a \mathbb{C} -algebra. It follows from this and the definition of π that $\pi(S) = R^{(3)}$. By Part (c) then $R^{(3)} = S/I$.

5, M

Review of mark distribution:

Total A marks: 32 of 32 marks

Total B marks: 25 of 20 marks

Total C marks: 19 of 12 marks

Total D marks: 4 of 16 marks

Total marks: 100 of 80 marks

Total Mastery marks: 20 of 20 marks

MATH70035 Algebra 3 Markers Comments

- Question 1 This question, in this particular format, is intended to test a variety of areas of the syllabus that are not covered in the other questions. Each of the Parts has a simple answer, but it would be wrong to say that it is "easy". My over-all impression is that the question was done reasonably well. The statement in Part (vi) is false, and a counterexample is needed with two matrices: you ought to start with matrices that do not commute, but you need to compute a bit more to show that you actually have a counterexample.
- Question 2 This was a rather straightforward but still meaningful question. In class, we had practiced similar problems by studying the Euclidean algorithm in $\mathbb{Z}[i]$. In class I only barely stated that something similar works in the noncommutative ring of Hurwitz quaternions. I was very pleased to see the students do well on this question.
- Question 3 This was the question on finding explicit generators for the ring of invariants. This material is new: it was not part of the course as taught in previous years. For this reasons, I taught the material slowly and practiced extensively in class. Given the amount of practice, I would class the question as "standard", i.e., not much problem element. Most students did really well, a small number rather less well: my guess is that the first group is mostly made of those students who regularly attended the lectures.
- Question 4 This question covered matrix Lie groups: arguably, the hardest area of the syllabus. The question is not particularly difficult, but the format is unusual, requiring both calculations and insight. I am not surprised that, of all the questions in this exam, this was the one that gave the more mixed results.
- Question 5 OK so this was the Mastery question; mostly self-study. I feel particularly guilty that I did not offer a huge amount of help (other than providing some references) and did not prepare an example sheet (I advised to study carefully the examples in the references). The material, I think, was not easy. On the whole I was really pleased to see that students did mostly very well on this question.