

**BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)  
May 2024**

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

**Algebra 3**

Date: Wednesday, May 8, 2024

Time: 14:00 – 16:30 (BST)

Time Allowed: 2.5 hours

**This paper has 5 Questions.**

**Please Answer All Questions in 1 Answer Booklet**

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.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

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

1. (a) What does it mean for a matrix to be in *Smith normal form*? (2 marks)
- (b) Find the Smith normal form of the following matrix over the ring  $\mathbb{Z}$ :

$$\begin{pmatrix} 1 & 0 & -1 \\ 5 & 2 & 1 \\ 10 & 4 & 12 \end{pmatrix}$$

(4 marks)

- (c) Let  $A$  be the abelian group generated by elements  $a, b, c$ , subject to the relations  $a+5b+10c = 0$ ,  $2b+4c = 0$  and  $-a+b+12c = 0$ . Show that  $A$  is isomorphic to a product of groups of the form  $\mathbb{Z}/k\mathbb{Z}$  (for  $k \in \mathbb{Z}$ ), which you should determine. (4 marks)

- (d) Find the Smith normal form of the following matrix over the ring  $\mathbb{Q}[X]$ :

$$\begin{pmatrix} X & -2X & X^3 \\ -X & X^2 & -X^3 \\ -X & 2X & -5X^2 + 6X \end{pmatrix}$$

(4 marks)

- (e) How many conjugacy classes of invertible  $2 \times 2$  matrices over  $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$  are there, where  $p$  is prime? You may use any results from the course provided you state them clearly, and you must prove your answer.

(6 marks)

(Total: 20 marks)

2. (a) What is the *characteristic* of a ring? (2 marks)
- (b) Prove that if  $\mathbb{F}$  is a field, its characteristic is either 0 or a prime number. (4 marks)
- (c) Let  $I$  be an ideal in a commutative ring  $R$ . Let  $M_n(I)$  be the set of  $n \times n$  matrices over  $R$ , all of whose entries lie in  $I$ .  
Prove that  $M_n(I)$  is a two-sided ideal of  $M_n(R)$ . (4 marks)
- (d) Find a non-zero proper left ideal in the ring of  $2 \times 2$  matrices over  $\mathbb{R}$ ,  $M_2(\mathbb{R})$ . (4 marks)
- (e) Let  $\mathbb{F}$  be a field, and let  $I$  be a two-sided ideal in the ring of  $n \times n$  matrices over  $\mathbb{F}$ ,  $M_n(\mathbb{F})$ .  
Prove that  $I = 0$  or  $I = M_n(\mathbb{F})$ . (6 marks)

(Total: 20 marks)

3. (a) State Gauss's lemma about polynomial rings, and Eisenstein's criterion. (4 marks)

(b) For what  $n \geq 1$  is the polynomial

$$f_n(X) := X^n + X^{n-1} + \dots + 1$$

irreducible in  $\mathbb{Z}[X]$ ?

(6 marks)

(c) Prove that the polynomial

$$g(X) := X^3 + 3X^2 + 52X + 57$$

is irreducible in  $\mathbb{Q}[X]$ .

(4 marks)

(d) Is the polynomial

$$h(X) = (1 - i)X^3 + 2X^2 + (2 + 4i)X + (1 + 3i)$$

irreducible in the ring  $(\mathbb{Z}[i])[X]$  of polynomials over the Gaussian integers? Prove your answer. You may quote results about the Gaussian integers from the course provided you state them clearly.

(6 marks)

(Total: 20 marks)

4. (a) For a matrix  $A \in M_n(\mathbb{R})$ , define  $e^A$  in terms of a power series.

For what matrices  $A$  does this power series converge? (You do not need to prove your answer). (4 marks)

(b) Prove that if  $A, B, C \in M_n(\mathbb{R})$  with  $C$  invertible and  $A = PBP^{-1}$ , then

$$e^A = Pe^BP^{-1}$$

(4 marks)

(c) Let  $Q$  be the matrix

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

We define the *special Lorentz group*, written  $SO(3, 1)$ , to be the set of matrices  $A \in M_4(\mathbb{R})$  such that  $A^TQA = Q$  and  $\det A = 1$ .

(i) Prove that  $SO(3, 1)$  is a closed subset of  $GL_4(\mathbb{R})$ . (3 marks)

(ii) Prove that  $SO(3, 1)$  is a subgroup of  $GL_4(\mathbb{R})$ . (3 marks)

(iii) Let  $V$  be the vector subspace of  $M_4(\mathbb{R})$  defined as follows:

$$V := \{A \in M_4(\mathbb{R}) \mid \text{Tr} A = 0, QA^TQ = -A\} \subseteq M_4(\mathbb{R})$$

Prove that  $V$  is the Lie algebra of  $SO(3, 1)$ .

(6 marks)

(Total: 20 marks)

5. (a) Prove that any Euclidean domain  $R$  is a principal ideal domain. (4 marks)
- (b) Let  $\omega = \frac{1+\sqrt{-3}}{2}$ . Prove that the ring  $\mathbb{Z}[\omega]$  is a Euclidean domain. (6 marks)
- (c) Prove that the ring  $\mathbb{Z}[\sqrt{-7}]$  is not a Euclidean domain.  
(Hint: try factoring an appropriate number.) (4 marks)
- (d) Let  $R$  be the ring of rational numbers with denominator a power of 2. Prove that  $R$  is a Euclidean domain. (6 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2024

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

MATH70035

Algebra 3 (Solutions)

Setter's signature

.....

Checker's signature

.....

Editor's signature

.....

1. (a) A matrix  $A \in M_{m \times n}(R)$  is in *Smith normal form* if  $A$  is a *rectangular diagonal matrix*, i.e.

seen ↓

$$A = \begin{pmatrix} d_1 & & & & 0 \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ 0 & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

and all  $d_i \neq 0$  and  $d_1 | \dots | d_r$ .

2, A

- (b) We perform elementary row and column operations to this matrix until it is in Smith normal form, at each stage replacing the matrix by a similar matrix:

meth seen ↓

$$\begin{aligned} \begin{pmatrix} 1 & 0 & -1 \\ 5 & 2 & 1 \\ 10 & 4 & 12 \end{pmatrix} &\sim \begin{pmatrix} 1 & 0 & 0 \\ 5 & 2 & 6 \\ 10 & 4 & 22 \end{pmatrix} && \text{by adding the first column to the final column} \\ &\sim \begin{pmatrix} 1 & 0 & 0 \\ 5 & 2 & 0 \\ 10 & 4 & 10 \end{pmatrix} && \text{by subtracting triple the middle column to the final column} \\ &\sim \begin{pmatrix} 1 & 0 & 0 \\ 5 & 2 & 0 \\ 0 & 0 & 10 \end{pmatrix} && \text{by subtracting double the second row from the final row} \\ &\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 10 \end{pmatrix} && \text{by subtracting quintuple the first row from the second row} \end{aligned}$$

This final matrix is in Smith normal form.

4, B

- (c)  $A$  is isomorphic to the cokernel of the homomorphism of  $\mathbb{Z}$ -modules  $\phi_M : \mathbb{Z}^3 \rightarrow \mathbb{Z}^3$  given by multiplication (on the left) by the matrix  $M$  from (b). Since similar matrices have isomorphic cokernels, this group is isomorphic to  $\text{coker}(\phi_N)$ , where  $\phi_N$  is given by left multiplication by  $N$ , where

meth seen ↓

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 10 \end{pmatrix}$$

Therefore  $A$  is isomorphic to

$$A \cong \frac{\mathbb{Z}}{\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{10\mathbb{Z}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{10\mathbb{Z}}$$

4, A

- (d) We perform elementary row and column operations to this matrix until it is in Smith normal form, at each stage replacing the matrix by a similar matrix:

meth seen ↓

$$\begin{aligned} \begin{pmatrix} X & -2X & X^3 \\ -X & X^2 & -X^3 \\ -X & 2X & -5X^2 + 6X \end{pmatrix} &\sim \begin{pmatrix} X & -2X & X^3 \\ 0 & X^2 - 2X & 0 \\ 0 & 0 & X^3 - 5X^2 + 6X \end{pmatrix} \\ &\sim \begin{pmatrix} X & 0 & 0 \\ 0 & X^2 - 2X & 0 \\ 0 & 0 & X^3 - 5X^2 + 6X \end{pmatrix} \end{aligned}$$

In the first step, we add the first row to each of the other rows, and in the second, we add multiples of the first column to the other columns.

This final matrix is in Smith normal form.

- (e) As shown in lectures, since  $\mathbb{F}$  is a field, there is a bijection between conjugacy classes in  $M_n(\mathbb{F})$  and sequences of monic polynomials  $f_1, \dots, f_r \in \mathbb{F}[X]$ , with  $f_1 | \dots | f_r$  and  $\sum_i \deg(f_i) = 3$ .

If  $r = 1$ , then  $f_1 = X^3 + aX^2 + bX + c$ , for  $a, b, c \in \mathbb{F}$ , and they can take any value; therefore there are  $p^3$  conjugacy classes with  $r = 1$ .

If  $r = 2$ , then we must have  $\deg(f_1) = 1$  and  $\deg(f_2) = 2$ ;  $f_1 = X + a$  for some  $a \in \mathbb{F}$ , and since  $f_1 | f_2$ , we must have  $f_2 = (X + b)f_1$  for some  $b \in \mathbb{F}$ . So there are  $p^2$  conjugacy classes with  $r = 2$ .

If  $r = 3$ , we must have  $\deg(f_1) = \deg(f_2) = \deg(f_3) = 1$ , and since  $f_1 | f_2 | f_3$  and they're all monic, we must have  $f_1 = f_2 = f_3 = X + a$  for some  $a \in \mathbb{F}$ . So there are  $p$  conjugacy classes with  $r = 3$ .

Therefore there are  $p^3 + p^2 + p$  conjugacy classes total.

4, C

sim. seen ↓

1, A

1, C

2, C

2, C

2. (a) For any ring  $R$ , there is a unique ring homomorphism  $\iota : \mathbb{Z} \rightarrow R$ . Its kernel is an ideal  $I \subseteq \mathbb{Z}$ ; since  $\mathbb{Z}$  is a PID,  $I = (n)$  for some  $n \geq 0$ . Then  $n$  is the characteristic.

seen ↓

- (b) Let  $n \geq 0$  be the characteristic of  $\mathbb{F}$ .

2, A

Suppose  $n = 1$ . Then  $\mathbb{F}$  is the trivial ring and so can't be a field.

seen ↓

Suppose  $n$  isn't prime or 0. Then we can write  $n = uv$ , where  $u, v > 1$  are integers. Therefore  $\iota(u) \cdot \iota(v) = \iota(n) = 0$ , but since  $u, v \notin (n) = \ker(\iota)$ ,  $\iota(u)$  and  $\iota(v)$  are non-zero. So  $\mathbb{F}$  isn't an integral domain, and so can't be a field, hence a contradiction.

1, A

- (c) Let  $A, B \in M_n(I)$ . Since every entry of  $A$  and  $B$  lies in  $I$  and  $I \subseteq R$  is an additive subgroup, every entry of  $A + B$  and  $-A$  also lies in  $I$ , so  $A + B, -A$  both lie in  $M_n(I)$ . So  $M_n(I) \subseteq M_n(R)$  is an additive subgroup.

3, A

unseen ↓

Let  $A \in M_n(I)$ , and  $P \in M_n(R)$ . Then every entry of  $AP$  is a sum of terms of the form  $ap$  where  $a \in I$  and  $p \in R$ , and so lies in  $I$ . Similarly every entry of  $PA$  is a sum of terms of the form  $pa$  where  $a \in I$  and  $p \in R$  and so lies in  $I$ . So  $AP$  and  $PA$  both lie in  $M_n(I)$ .

2, B

2, B

- (d) Let  $I$  be the set of matrices with right column 0:

unseen ↓

$$I = \left\{ \begin{pmatrix} p & 0 \\ q & 0 \end{pmatrix} \mid p, q \in \mathbb{R} \right\}$$

Then  $I$  is non-zero and  $I \neq M_2(\mathbb{R})$ ; it remains to show it's a left ideal.

Clearly  $I \subseteq M_2(\mathbb{R})$  is an additive subgroup.

2, A

Let  $A \in I$  and  $X \in M_2(\mathbb{R})$ . We must show  $XA \in I$ . We write

$$A = \begin{pmatrix} p & 0 \\ q & 0 \end{pmatrix}$$

and

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and multiply to get

$$XA = \begin{pmatrix} ? & 0 \\ ? & 0 \end{pmatrix} \in I$$

Therefore  $I$  is a left ideal in  $M_2(\mathbb{R})$ .

2, C

- (e) Let  $I \subseteq M_n(\mathbb{F})$  be a non-zero two-sided ideal. We will show  $I = M_n(\mathbb{F})$ . Let  $A \in I$  be a non-zero element.

unseen ↓

Since  $A$  is non-zero, there are some  $1 \leq i, j \leq n$  such that  $A_{ij} \neq 0$ . Since  $\lambda A \in I$  for any  $\lambda \in \mathbb{F}$ , setting  $\lambda = A_{ij}^{-1}$  (which we can do since  $\mathbb{F}$  is a field) and replacing  $A$  with  $\lambda A$ , we may assume WLOG that  $A_{ij} = 1$ .

Let  $P_k$  be the matrix with  $P_{kk} = 1$  and all other entries 0. Then since  $I$  is a two-sided ideal,  $B := P_i \cdot A \cdot P_j \in I$  too. But  $B$  has exactly one non-zero entry, which is 1, in position  $ij$ .

2, D

For any  $1 \leq u, v \leq n$ , let  $E_{uv}$  be the matrix with 1 in position  $uv$  and zero everywhere else. Note  $B = E_{ij}$ .

2, D

Since  $E_{uv} = E_{ui} B E_{jv}$  for all  $1 \leq u, v \leq n$  and  $I$  is a two-sided ideal, we find that  $E_{uv} \in I$  for all  $u, v$ , and similarly  $\lambda E_{uv} \in I$  for all  $\lambda \in \mathbb{F}$  too. Since any element of  $M_n(\mathbb{F})$  is a sum of elements of the form  $\lambda E_{uv}$ , we see that  $I = M_n(\mathbb{F})$ .

2, D

3. (a) Gauss' Lemma says that if  $R$  is a unique factorisation domain,  $F$  its field of fractions and  $f \in R[X]$  a primitive polynomial, then  $f$  is irreducible in  $R[X]$  if and only if it is irreducible in  $F[X]$ . Eisenstein's criterion says that if  $R$  is a unique factorisation domain,  $f = a_n X^n + \dots + a_0 \in R[X]$  a primitive polynomial with  $a_n \neq 0$ , and  $p \in R$  an irreducible element such that  $p|a_0, \dots, a_{n-1}$ ,  $p \nmid a_n$  and  $p^2 \nmid a_0$ , then  $f$  is irreducible.
- (b) If  $n+1$  is composite, we can write  $n+1 = uv$ , where  $u, v > 1$ . Then

$$\begin{aligned} f_n &= \frac{X^{n+1} - 1}{X - 1} \\ &= \frac{(X^u)^v - 1}{X - 1} \\ &= \frac{X^u - 1}{X - 1} ((X^u)^{v-1} + (X^u)^{v-2} + \dots + 1) \\ &= (X^{u-1} + X^{u-2} + \dots + 1)((X^u)^{v-1} + (X^u)^{v-2} + \dots + 1) \end{aligned}$$

so  $f_n$  isn't irreducible.

If  $n+1 = p$  is prime, we show  $f_n$  is irreducible with Eisenstein's criterion.

Let  $Y = X + 1$ , then  $f(X) = g(Y - 1)$  where

$$\begin{aligned} g(Y) &= f(X + 1) \\ &= \frac{(X + 1)^p - 1}{X} \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + \dots + \binom{p}{p-1} \end{aligned}$$

which is irreducible by Eisenstein's criterion applied to the prime  $p$ . So  $g$  is irreducible, therefore  $f$  is too.

- (c) Let  $Y = x - 1$ ; we find that  $f(X) = g(Y - 1)$  where

$$\begin{aligned} g(Y) &= f(X - 1) \\ &= X^3 + 49X + 7 \end{aligned}$$

which is irreducible by Eisenstein's criterion using the prime 7.

An alternative solution is to reduce mod 2, and show that the reduction of  $f$  mod 2,  $\tilde{f}$ , has no solutions, and so is irreducible in  $(\mathbb{Z}/2\mathbb{Z})[X]$ , and so  $f$  is irreducible in  $\mathbb{Z}[X]$ .

- (d) Note that  $2 = (1+i)(1-i)$ , and  $1+i$  is irreducible in  $\mathbb{Z}[i]$ :

If  $(1+i) = uv$ , then  $2 = |1+i|^2 = |u|^2|v|^2$ , so one of  $|u|, |v|$  must be 1, so one of  $u, v$  must be a unit.

Now note that  $2 = (1+i)(1-i)$ ,  $(2+4i) = (1+i)^2(2-i)$  and  $1+3i = (1+i)(2+i)$ . However note that  $1+i$  doesn't divide  $2+i$  so  $(1+i)^2$  doesn't divide  $1+3i$ . Recall from the course that  $\mathbb{Z}[i]$  is a unique factorisation domain.

Note that  $h$  is primitive since, for example, the first coefficient is irreducible but doesn't divide the final coefficient.

So by Eisenstein's criterion applied with  $1+i$ , we see that  $h$  is irreducible.

seen ↓

2, A

2, A

unseen ↓

3, B

seen ↓

3, A

sim. seen ↓

4, B

meth seen ↓

2, B

2, C

2, B

4. (a)

seen ↓

$$e^A := \sum_{k=0}^{\infty} \frac{1}{k!} A^k$$

This power series converges for all  $A$ .

2, A

(b) Note  $(PBP^{-1})^k = PB^kP^{-1}$ . So

2, A

$$\begin{aligned} e^A &= e^{PBP^{-1}} \\ &= \sum_{k=0}^{\infty} \frac{1}{k!} (PBP^{-1})^k \\ &= \sum_{k=0}^{\infty} \frac{1}{k!} PB^kP^{-1} \\ &= P \left( \sum_{k=0}^{\infty} \frac{1}{k!} B^k \right) P^{-1} \\ &= Pe^BP^{-1} \end{aligned}$$

seen ↓

Note that since the power series for  $e^A$  is absolutely convergent for all  $A$ , we can rearrange these infinite sums as above.

3, A

1, A

(c) (i) Consider the continuous function  $F : \text{GL}_4(\mathbb{R}) \rightarrow M_4(\mathbb{R})$ , sending  $A$  to  $A^TQA - Q$ . Then  $SO(3, 1) = F^{-1}\{0\} \cap \det^{-1}\{1\}$  is an intersection of two closed subsets and is hence a closed subset of  $\text{GL}_4(\mathbb{R})$ .

sim. seen ↓

3, A

(ii) If  $A, B \in SO(3, 1)$ , then  $(AB)^TQ(AB) = B^TA^TQAB = B^TQB = Q$ , and also  $\det(AB) = \det(A)\det(B) = 1$  so  $AB \in SO(3, 1)$  too. Similarly since  $\det(A) = 1$ ,  $A$  is invertible (alternatively note that since  $Q^2 = I$ ,  $(QA^TQ)A = I$ ), and multiplying the equation  $A^TQA = Q$  on the right by  $A^{-1}$  and the left by  $(A^{-1})^T$ , we find that

sim. seen ↓

$$(A^{-1})^TQA^{-1} = Q$$

so  $A^{-1} \in SO(3, 1)$  too. Therefore  $SO(3, 1) \leq \text{GL}_4(\mathbb{R})$  is a subgroup.

3, B

(ii) Let  $W = \mathfrak{so}(3, 1)$  be the Lie algebra of  $SO(3, 1)$ . We prove that

unseen ↓

$$W = \{A \in M_4(\mathbb{R}) \mid \text{Tr}A = 0, QA^TQ = -A\}$$

First suppose  $A \in W$ . Then  $e^{tA} \in SO(3, 1)$  for all  $t \in \mathbb{R}$ .

Since  $1 = \det(e^A) = e^{\text{Tr}A}$ , we must have that  $\text{Tr}A = 0$ .

Furthermore we must have that

$$(e^{tA})^TQe^{tA} = Q$$

for all  $t$ . Noting that  $Q^2 = I$  (so  $Q = Q^{-1}$ ), we rearrange this, using (b), to find that

$$e^{Q(tA)^TQ} = e^{-tA}$$

for all  $t$ . Choosing  $t > 0$  small enough such that  $-tA$  and  $Q(tA)^TQ$  both live in an open neighbourhood of  $I$  in  $SO(3, 1)$  on which the exponential map is injective, we find that for this  $t$ , we have that

$$Q(tA)^TQ = -tA$$

Dividing by  $t$ , we get:

$$QA^TQ = -A$$

so  $A \in \{A \in M_4(\mathbb{R}) \mid \text{Tr}A = 0, QA^TQ = -A\}$ .

Now suppose  $A \in \{A \in M_4(\mathbb{R}) \mid \text{Tr}A = 0, QA^TQ = -A\}$ ; we show that  $A \in W$  too. To do this, we show that  $e^{tA} \in SO(3, 1)$  for all  $t$ .

First note  $\det(e^{tA}) = e^{\text{Tr}A} = 1$ . Then

$$\begin{aligned}(e^{tA})^T Q e^{tA} &= Q^2 e^{tA^T} Q e^{tA} \\ &= Q e^{QtA^TQ} e^{tA} \\ &= Q e^{-tA} e^{tA} \\ &= Q\end{aligned}$$

for all  $t$ . So  $e^{tA} \in SO(3, 1)$  for all  $t$ , so  $A \in W$ .

3, D

3, D

5. (a) Let  $\theta$  be the Euclidean function for  $R$ . Let  $I \subseteq R$  be an ideal, which we can assume to be non-zero.

seen ↓

Choose  $b \neq 0 \in I$  with  $\theta(b)$  minimised, and let  $a \in I$  be another element. Then there are some  $q, r \in R$  with  $a = qb + r$ , with  $r = 0$  or  $\theta(r) < \theta(b)$ .

2, M

Since  $I$  is an ideal and  $a, b \in I$ ,  $r = a - qb$  also lies in  $I$ . We can't have that  $\theta(r) < \theta(b)$  and  $r \neq 0$  (because of how we chose  $b$ ), so  $r = 0$ . So  $a = qb$ , and so  $a \in (b)$ . Since  $a \in I$  was arbitrary, the ideal  $I = (b)$  is principal.

2, M

- (b) For  $a, b \in \mathbb{Z}$ , let  $\theta(a + b\sqrt{-2}) = |a + b\omega|^2 = a^2 + ab + b^2$ . Note this is at least 1 when  $a + b\omega \neq 0$ .

sim. seen ↓

Note that since  $\theta(zw) = \theta(z)\theta(w)$  and  $\theta(w) \geq 1$  for all non-zero  $z, w \in \mathbb{C}$ , we have that  $\theta(zw) \geq \theta(z)$  for all  $z, w \in \mathbb{Z}[\omega] \setminus \{0\}$ .

2, M

Notice that the lattice  $\mathbb{Z}[\omega]$  in  $\mathbb{C}$  splits  $\mathbb{C}$  into rhombuses of side length 1, so every point in  $\mathbb{C}$  has distance strictly less than 1 from this lattice. So for all  $p \in \mathbb{C}$  there is some  $z \in \mathbb{Z}[\omega]$  with  $|p - z| < 1$ .

2, M

Now choose  $a, b \in \mathbb{Z}[\omega]$  with  $b \neq 0$ . Let  $q \in \mathbb{Z}[\omega]$  satisfy  $|a/b - q| < 1$ , noting that such a  $q$  exists by the above discussion. Then we let  $r = a - bq$ ;  $|r| < |b|$  since  $|r| = |b||a/b - q|$ . So  $q, r \in \mathbb{Z}[\omega]$ ,  $a = qr + b$  and either  $r = 0$  or  $\theta(r) < \theta(b)$ , so  $\mathbb{Z}[\omega]$  is a Euclidean domain.

2, M

- (c) We can factor 8 in two distinct ways:

sim. seen ↓

$$8 = 2 \cdot 2 \cdot 2$$

and

$$8 = (1 - \sqrt{-7})(1 + \sqrt{-7})$$

Then we claim both are factorisations into irreducibles. Let  $\theta(a + b\sqrt{-7}) = a^2 + 7b^2$ . Then  $\theta(zw) = \theta(z)\theta(w)$ , and for  $z \in \mathbb{Z}[\sqrt{-7}]$ ,  $\theta(z) \geq 1$ , with equality if and only if  $z = \pm 1$  is a unit, and if  $\theta(z) > 1$ ,  $\theta(z) \geq 4$ ; if equality holds here,  $z = \pm 2$ .

2, M

So if  $2 = uv$ , then we must have that  $\theta(uv) = 4$  so one of  $u$  or  $v$  is a unit. So 2 is irreducible.

Similarly if  $1 + \sqrt{-7} = uv$ , then  $\theta(uv) = 8$ , so either one of  $u$  and  $v$  is a unit or is 2, but 2 doesn't divide  $1 + \sqrt{-7}$  so it must be irreducible.

Then since Euclidean domains are unique factorisation domains and so have unique factorisations into irreducibles,  $\mathbb{Z}[\sqrt{-7}]$  can't be a Euclidean domain.

2, M

- (d) Let  $\theta(p \cdot 2^k) = |p|$ , for  $p$  odd and any  $k \in \mathbb{Z}$ . This defines a function  $\theta : R \setminus \{0\} \rightarrow \mathbb{N}$ . We show that this is a Euclidean function.

unseen ↓

Let  $p \cdot 2^k, q \cdot 2^l \in R$ , with  $p, q$  odd and  $k, l \in \mathbb{Z}$ . Then  $\theta((p \cdot 2^k) \cdot (q \cdot 2^l)) = |pq| \geq \theta(p \cdot 2^k)$ .

2, M

Now let  $a, b \in R$  with  $b \neq 0$ ; we may also assume  $a \neq 0$ . We can write  $a = p \cdot 2^k$  and  $b = q \cdot 2^l$  with  $p, q, k, l \in \mathbb{Z}$ , and  $p, q$  odd.

By the Euclidean algorithm (for  $\mathbb{Z}$ ), there are integers  $r, s$  such that  $p = rq + s$  and  $|s| < |q|$  (or  $s = 0$ ).

Therefore

$$a = (r \cdot 2^{k-l})b + (s \cdot 2^k)$$

and either  $s \cdot 2^k = 0$  or  $\theta(s \cdot 2^k) \leq |s| < |q|$ .

4, M

**Review of mark distribution:**

Total A marks: 33 of 32 marks

Total B marks: 22 of 20 marks

Total C marks: 13 of 12 marks

Total D marks: 12 of 16 marks

Total marks: 100 of 80 marks

Total Mastery marks: 20 of 20 marks

Question   Marker's comment

- 1 Generally well-answered except the last part, which was quite hard. Answers to question c were generally not very detailed.
- 2 Remember to check all the parts of the definition of an ideal for (c). For (e), make sure to read the question carefully.
- 3 Remember Gauss' lemma and Eisenstein's criterion require the ring to be a UFD.
- 4 In c(iii), make sure to prove inclusions in both directions to prove equality; also make sure to clearly state which direction you're proving as many answers here didn't.

Question   Marker's comment

5   This turned out to be quite a hard question