Imperial College London

Department of Mathematics

M3P8 Algebra III

Question	Examiner's Comments
Q 1	This question was relatively easy and was successfully answered by most students
Q 2	The last part was a bit more difficult, although it was attempted by almost all
Q 3	This question was about right
Q 4	The final part was a bit more challenging.

Printed: 27/07/2018 11:47:55

Imperial College London

Department of Mathematics

M45P8 Algebra III

Question	Examiner's Comments
Q 5	This question was a bit too easy. A vast majority have answered it correctly

Printed: 27/07/2018 11:47:56

Imperial College
London

M4/5P8

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)

May-June 2018

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

Algebra III

Date: Wednesday, 30 May 2018

Time: 10:00 AM - 12:30 PM

Time Allowed: 2.5 hours

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.
- Each question carries equal weight.
- Calculators may not be used.

1. (a) Let R be an integral domain.

   (i) Give the definition of a *unit* of R.

   (ii) Give the definition of an *irreducible element* of R.

   (iii) What does it mean that $a, b \in R$ are associates?

   (iv) Prove that $a, b \in R$ are associates if and only if $aR = bR$.

   (v) Give the definition of a *unique factorisation domain* (UFD).

   (vi) Is $\mathbb{Z}[\sqrt{-2017}]$ a UFD? (You need to justify your answer. You can use any results from lectures provided you state them clearly.)

   (b) Let R be the set of rational numbers $\frac{a}{b}$, where $a, b \in \mathbb{Z}$ are such that b is coprime to 6.

   (i) Prove that R is an integral domain.

   (ii) Determine the units of R.

   (iii) Determine the irreducible elements of R.

   (iv) Is R a UFD?
   (In parts (ii), (iii), (iv) you are asked to briefly justify your answers. You can use any results from lectures provided you state them clearly.)

2. (a) (i) Give the definition of a *Euclidean domain*.

   (ii) Give the definition of a *principal ideal domain* (PID).

   (iii) Prove that every Euclidean domain is a PID.

   (b) Let

$$R = \left\{ a + \frac{1+\sqrt{-7}}{2} b, \text{ where } a, b \in \mathbb{Z} \right\} \subset \mathbb{C}.$$

   (i) Prove that R is an integral domain.

   (ii) Prove that R is a Euclidean domain with respect to the complex norm.

3. (a) Let R be an integral domain.

(i) Give the definition of a *prime* ideal of R.

(ii) Give the definition of a *maximal* ideal of R.

(iii) Prove that every maximal ideal of R is prime.

(iv) Give an example of an integral domain R and a prime ideal $P \subset R$ which is not maximal. (You need to justify your answer.)

(b) Determine which of the principal ideals (2), (3), (5) of $\mathbb{Z}[\sqrt{-1}]$ are maximal.

(c) (i) Find an irreducible polynomial of degree 3 over $\mathbb{Z}/5$. (You need to justify your answer.)

(ii) Let p be a prime number and let F be a field with p^4 elements. Prove that F contains a field with p^2 elements.

4. (a) (i) State and prove Eisenstein's Irreducibility Criterion. (You can use any results from lectures provided you state them clearly.)

(ii) Prove that the polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible.

(b) Determine all values of $n \in \mathbb{Z}$ for which the polynomial $x^3 + nx^2 - n^2x + 1 \in \mathbb{Q}[x]$ is irreducible. (You need to justify your answer.)

(c) Let F be a field with p^2 elements, where p is prime, $p \neq 3$. Show that there is an element $a \in F$ such that the polynomial $x^3 - a \in F[x]$ is irreducible.

5. (a) In this question all rings are assumed to be commutative.

(i) Give the definition of a Noetherian commutative ring.

(ii) State the Hilbert Basis Theorem. (No proof is required.)

(iii) Let R be a Noetherian commutative ring. Let $R[x_1, \ldots, x_n]$ be the polynomial ring in variables $x_1, \ldots, x_n$, and let $I \subset R[x_1, \ldots, x_n]$ be an ideal. Prove that the ring $R[x_1, \ldots, x_n]/I$ is Noetherian. (You can use any results from lectures provided you state them clearly.)

(b) Are the following rings Noetherian? (You need to justify your answers. You can use any results from lectures provided you state them clearly.)

(i) $\mathbb{Z}[\sqrt{-1}]$;

(ii) $\mathbb{Z}[\sqrt[3]{2018}]$;

(iii) $\mathbb{C}[x,y]/(f(x,y))$, where $f(x,y) \in \mathbb{C}[x,y]$ is a polynomial;

(iv) the subring of $\mathbb{C}[x]$ consisting of the polynomials with integer constant term;

(v) the ring of continuous functions $\mathbb{C} \to \mathbb{C}$;

(vi) the ring R from Question 2(b);

(vii) the ring R from Question 1(b).

M3/4/5 P8 Sols

B=Bookwork, S=Seen or seen similar, N=New question

1. (a) (i) **1 mark, B** An element $a \in R$ is called a unit if $ab = 1$ for some $b \in R$.

(ii) **1 mark, B** A non-zero element of R is called irreducible if it is not a unit and is not a product of two non-units.

(iii) **1 mark, B** $a, b \in R$ are associates if and only if $a = bu$, where u is a unit of R.

(iv) **3 marks, B** Suppose that $a = bu$, where u is a unit of R. Then $ra = rub$, hence $aR \subset bR$. The opposite inclusion is proved in the same way. Conversely, if $aR = bR$, then $a = a \cdot 1 = br_1$ for some $r_1 \in R$. Similarly, $b = b \cdot 1 = ar_2$ for some $r_2 \in R$. By the cancellation property $a = a(r_1 r_2)$ implies $r_1 r_2 = 1$. Thus a and b are associates.

(v) **2 marks, B** An integral domain R is a UFD if (1) every non-zero element which is not a unit is a product of finitely many irreducibles; (2) two factorisations as in (1) are the same up to the order of factors and replacing irreducible elements by associates.

(vi) **3 marks, S** No. We have $2018 = 2 \times 1009 = (1 + \sqrt{-2017})(1 - \sqrt{-2017})$. Taking the complex norm one shows that 2 is an irreducible element. If $\mathbb{Z}[\sqrt{-2017}]$ is a PID, then, by a result from lectures, 2 divides $1 + \sqrt{-2017}$ or $1 - \sqrt{-2017}$. This is not the case, so $\mathbb{Z}[\sqrt{-2017}]$ is not a PID.

(b) (i) **2 marks, N** R is closed under addition, subtraction and multiplication, and contains 1. Thus R is a subring of $\mathbb{Q}$, so R is commutative and has no zero divisors. Hence R is an integral domain.

(ii) **2 marks, N** From the definition of a unit it is immediate that the units are the fractions $\frac{a}{b}$, where $a, b \in \mathbb{Z}$ are both coprime to 6.

(iii) **3 marks, N** From the definition of an irreducible element it is clear that 2 and 3 are irreducibles. The fundamental theorem of arithmetic implies that every non-zero element of R is uniquely written as $u2^n3^m$, where u is a unit and $n, m \geq 0$. Hence the irreducible elements of R are 2 and 3 (up to multiplication by units).

(iv) **2 marks, N** The factorisation $u2^n3^m$ from part (iii) is unique, so R is a UFD.

2. (a) (i) **2 marks, B** An integral domain R is called a Euclidean domain if there is a function $\varphi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for any non-zero $a, b \in R$ we have $\varphi(ab) \geq \varphi(a)$, and for any $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$.

(ii) **1 mark, B** An integral domain is called a PID if every ideal is principal.

(iii) **3 marks, B** Let $I \subset R$ be a non-zero ideal. Choose $a \in I$, $a \neq 0$, with the least value of $\varphi(a)$. Let's show that $I = (a)$. Take any $b \in I$. Either $b = qa$ or $b = qa + r$, where $r \neq 0$ and $\varphi(r) < \varphi(a)$. The second possibility leads to a contradiction because $r = b - qa \in I$.

(b) (i) **3 marks, S** R is closed under addition, subtraction, and contains 1. Write $\delta = \frac{1+\sqrt{-7}}{2}$. We have $\delta^2 = \delta - 2$, hence R is closed under multiplication. Thus R is a subring of $\mathbb{C}$, so R is commutative and has no zero divisors. Hence R is an integral domain.

(ii) **11 marks, N** The complex norm is multiplicative, so to prove that $|ab| \geq |b|$ it is enough to prove that $|a| \geq 1$ for any non-zero $a \in R$. Indeed, we have $|m + n\delta| = (m + n/2)^2 + 7(n/2)^2 \geq 1$. **(4 marks for this part)**
Now let $a, b \in R$, $b \neq 0$. Write $\frac{a}{b} \in \mathbb{Q}(\sqrt{-7})$ as $x + y\sqrt{-7}$ with $x, y \in \mathbb{Q}$. It is enough to find $z \in R$ such that $|x + y\sqrt{-7} - z| < 1$. Since $\mathbb{Z}[\sqrt{-7}] \subset R$, we can assume that $0 \leq x, y \leq 1$. If $y \leq 1/4$, we take $z = 0$ if $x \leq 1/2$ and $z = 1$ if $x > 1/2$. If $y \geq 3/4$, we take $z = \sqrt{-7}$ if $x \leq 1/2$ and $z = 1 + \sqrt{-7}$ if $x > 1/2$. Otherwise take $z = \delta = 1/2 + \sqrt{-7}/2$. Then $|x + y\sqrt{-7} - z| \leq (1/2)^2 + 7(1/4)^2 < 1$. **(7 marks)**

3. (a) (i) **1 mark, B** An ideal $I \subset R$ is prime if R/I is an integral domain. (Any equivalent definition is fine.)

(ii) **1 mark, B** An ideal $I \subset R$ is maximal if R/I is a field. (Any equivalent definition is fine.)

(iii) **1 mark, B** A field has no zero divisors, hence the result.

(iv) **2 mark, S** Let $R = \mathbb{C}[x, y]$ and $I = (x)$. Then $R/I = \mathbb{C}[y]$ is an integral domain, so I is prime. As $\mathbb{C}[y]$ is not a field (e.g. y is not invertible), I is not maximal. (Alternatively, I is contained in a larger ideal (x, y).)

(b) **6 marks, S** By lectures, the ring $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain, hence a PID. By another result in lectures, the maximal ideals of a PID are the ideals generated by irreducible elements.
We have $2 = (1 + i)(1 - i)$, where neither factor is a unit as its norm is 2. Thus 2 is not irreducible in $\mathbb{Z}[\sqrt{-1}]$, hence (2) is not a maximal ideal of $\mathbb{Z}[\sqrt{-1}]$.
We have $5 = (2 + i)(2 - i)$, where neither factor is a unit as its norm is 5. Hence (5) is not a maximal ideal of $\mathbb{Z}[\sqrt{-1}]$.
Let's show that 3 is an irreducible element of $\mathbb{Z}[\sqrt{-1}]$, so that (3) is maximal. Write $3 = (a + bi)(c + di)$, where $a, b, c, d \in \mathbb{Z}$. Taking norms we get $9 = (a^2 + b^2)(c^2 + d^2)$. Since $a^2 + b^2 = 3$ has no solutions in $\mathbb{Z}$, we see that either $a + bi$ or $c + di$ is a unit in $\mathbb{Z}[\sqrt{-1}]$. Thus 3 is irreducible in $\mathbb{Z}[\sqrt{-1}]$.

(c) (i) **3 marks, N** $x^3 + 1$ and $x^3 - 1$ are obviously reducible, so we try $x^3 + x + 1$. By a result from lectures, it is enough to check that $x^3 + x + 1$ has no roots in $\mathbb{Z}/5$. This is straightforward.

(ii) **6 marks, N** Let K be the set of roots of $x^{p^2} - x$ in F. Since F has characteristic p, K is closed under addition and subtraction. The non-zero elements of K are the roots of $x^{p^2-1} = 1$, hence they form a group under multiplication. Thus K is a subfield of F.
In lectures we proved that the separable polynomial $x^{p^4} - x$ is a product of p^4 pairwise different factors $x - a$, where $a \in F$, that is, the roots of $x^{p^4} - x$ are all the elements of F. Since $x^{p^2-1} - 1$ divides $x^{p^4-1} - 1$, the polynomial $x^{p^2} - x$ has p^2 pairwise different roots in F. Thus $|K| = p^2$.

4. (a) (i) **6 marks, B** Eisenstein's Irreducibility Criterion: a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ of degree n, where $a_i \in \mathbb{Z}$, is irreducible in $\mathbb{Q}[x]$ when there is a prime p such that (1) p does not divide a_n, (2) p divides $a_0, \ldots, a_{n-1}$, (3) p^2 does not divide a_0. **(2 marks)**

Proof. If $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Q}[x]$, then, by the Gauss lemma, we can assume that $g(x), h(x) \in \mathbb{Z}[x]$. Let $\tilde{g}(x)$ and $\tilde{h}(x)$ be the reductions modulo p. Let m be the degree of $g(x)$. We have $\tilde{g}(x) = bx^m$, $\tilde{h}(x) = cx^{n-m}$, where $b, c \in \mathbb{Z}/p$ are non-zero. But this implies that a_0 is divisible by p^2, a contradiction. **(4 marks)**

(ii) **4 marks, B** Let $t = x - 1$. We have

$$x^6 + \ldots + 1 = \frac{x^7 - 1}{x - 1} = \frac{(t+1)^7 - 1}{t} = t^6 + \ldots$$

By the binomial formula, each coefficient of this polynomial, except the leading coefficient, is divisible by 7. The constant term is divisible by 7 but not by 49. Thus we can apply Eisenstein's Irreducibility Criterion to conclude that the original polynomial is irreducible over $\mathbb{Q}$.

(b) **5 marks, N** If $x^3 + nx^2 - nx + 1 \in \mathbb{Q}[x]$ is reducible over $\mathbb{Q}$, then, by the Gauss lemma, it has a root in $\mathbb{Z}$. It must be 1 or -1. In the first case $2 = 0$ is a contradiction. In the second case we get $n = 0$ which gives the reducible polynomial x^3+1. Thus $x^3+nx^2-nx+1 \in \mathbb{Q}[x]$ is irreducible if and only if $n \neq 0$.

(c) **5 marks, N** $x^3 - a$ is irreducible in $F[x]$ if and only if a is not a third power in F. By a result from lectures, the group F^* is cyclic of order $p^2 - 1$. Since $p \neq 3$, we see that 3 divides $p^2 - 1$, hence the homomorphism $F^* \to F^*$ given by $x \mapsto x^3$, is not surjective. Any $a \in F^*$ not in the image of this map does the job.

5. (a) (i) **1 mark, B** A commutative ring R is called Noetherian if every ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ of R stabilises, i.e. there is a positive integer n such that $I_n = I_m$ for any $m \geq n$.

(ii) **1 mark, B** Hilbert Basis Theorem: If a commutative ring R is Noetherian, then the polynomial ring $R[x]$ is also Noetherian.

(iii) **3 marks, B** Applying the Hilbert Basis Theorem n times we obtain that $R[x_1, \ldots, x_n]$ is Noetherian. Let J be an ideal of $R[x_1, \ldots, x_n]/I$. Its inverse image in $R[x_1, \ldots, x_n]$ is finitely generated, say by $f_1, \ldots, f_m$, since $R[x_1, \ldots, x_n]$ is Noetherian. The images of $f_1, \ldots, f_m$ in $R[x_1, \ldots, x_n]/I$ generate J. Thus every ideal of $R[x_1, \ldots, x_n]/I$ is finitely generated, hence $R[x_1, \ldots, x_n]/I$ is Noetherian, by a result from lectures.

(b) (i) **2 marks, S** $\mathbb{Z}$ is Noetherian, since it is a PID. We conclude by applying (a) (iii) to $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[x]/(x^2 + 1)$. (Alternatively, $\mathbb{Z}[\sqrt{-1}]$ is Euclidean, hence a PID, hence is Noetherian.)

(ii) **2 marks, N** The same proof as in (i) works.

(iii) **2 marks, N** $\mathbb{C}$ is a field, hence is Noetherian. Now apply (a) (iii).

(iv) **2 marks, S** Consider the ascending chain of ideals $(x) \subset (x/2) \subset \ldots \subset (x/2^n) \subset \ldots$ These ideals are all different, as 2^n is not a unit because $1/2^n$ is not in the ring. So we have an ascending chain of ideals that does not stabilise.

(v) **2 marks, N** The set of continuous functions $f : \mathbb{C} \to \mathbb{C}$ such that $f(z) = 0$ for $|z| > n$ is an ideal. Call it I_n. We get an ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ that does not stabilise.

(vi) **2 marks, S** This ring is Euclidean by the result of Question 2(b)(ii), hence a PID, hence is Noetherian.

(vii) **3 marks, N** Let's show that R is a PID, hence Noetherian. Let $I \subset R$ be an ideal. Then $I \cap \mathbb{Z} = a\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$ for some $a \in \mathbb{Z}$, since $\mathbb{Z}$ is a PID. It follows that $I = aR$. Indeed, if $\frac{n}{m} \in I$, then $n \in I \cap \mathbb{Z}$, hence $n = ak$ for some $k \in \mathbb{Z}$. Thus $\frac{n}{m} = a\frac{k}{m} \in aR$, so $I \subset aR$. It is clear that $aR \subset I$, so $I = aR$.