Queen Mary
University of London

Main Examination period 2023 – May/June – Semester B

MTH4104: Introduction to Algebra

Duration: 2 hours

Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.

The exam is intended to be completed within **2 hours**. However, you will have a period of **3 hours** to complete the exam and submit your solutions.

You should attempt ALL questions. Marks available are shown next to the questions.

The exam is closed-book, and **no outside notes are allowed**.

Only approved non-programmable calculators are permitted in this examination. Please state on your answer book the name and type of machine used.

Complete all rough work in the answer book and cross through any work that is not to be assessed.

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any unauthorised notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately.

It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms, it will be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the examination room.

Examiners: A. Fink, F. Rincón

 Turn Over

Question 1 [16 marks].

(a) Use Euclid's Algorithm to find the greatest common divisor of 165 and 37. Show all your working. **[8]**

(b) Use the Extended Euclidean Algorithm to compute the multiplicative inverse of $[37]_{165}$. Show all your working. **[8]**

Solution (a) We calculate

$$\begin{aligned} 165 &= 4 \cdot 37 + 17 \\ 37 &= 2 \cdot 17 + 3 \\ 17 &= 5 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

so the greatest common divisor is 1.
(b) We may use the extended Euclidean algorithm to find an integer solution to $165x + 37y = 1$. For this we unwind the calculations from Part (a):

$$\begin{aligned} 1 &= 1 \cdot 3 - 1 \cdot 2 = 1 \cdot 3 - 1 \cdot (17 - 5 \cdot 3) \\ &= -1 \cdot 17 + 6 \cdot 3 = -1 \cdot 17 + 6 \cdot (37 - 2 \cdot 17) \\ &= 6 \cdot 37 - 13 \cdot 17 = 6 \cdot 37 - 13 \cdot (165 - 4 \cdot 37) \\ &= -13 \cdot 165 + 58 \cdot 37. \end{aligned}$$

So $x = -13$ and $y = 58$ arrange that $165x + 37y = 1$.

Question 1 is application of standard algorithms.

Question 2 [14 marks].

(a) Let X be a set. Define what it means for R to be a **relation** on X. **[3]**

Now let R be the relation on the set $\mathbb{R}[x]$ of polynomials with real coefficients defined by

$$(f, g) \in R \text{ if and only if } x^2 + 1 \text{ divides } g - f.$$

(b) Prove that R is transitive. **[5]**

For part (c) below, you may assume that R is an equivalence relation.

(c) Find a polynomial h with $\deg h \leqslant 1$ such that h is an element of the equivalence class $[x^3 + 2x^2 + 3x + 4]_R$. **[6]**

Solution (a) A relation R on X is a subset of $X \times X$.
(b) Suppose $f, g, h \in \mathbb{R}[x]$ satisfy fRg and gRh. This means there exist $k, l \in \mathbb{R}[x]$ such that $g - f = k(x^2+1)$ and $h - g = l(x^2+1)$. Then

$$h - f = (h - g) + (g - f) = (k + l)(x^2 - 1)$$

implying fRh. This proves that R is transitive.
(c) The polynomial division rule provides $q, r \in \mathbb{R}[x]$ such that $x^3 + 2x^2 + 3x + 4 = q(x^2+1) + r$ and either $r = 0$ or $\deg r \leqslant 1$. The first equality implies that $x^2 + 1$ divides $r - (x^3 + 2x^2 + 3x + 4)$, so $h = r$ is exactly the polynomial we need, providing it doesn't turn out to be 0. We carry out polynomial division to find r:

$$\begin{array}{rrl|llll} & & & & & x & +2 \\ \hline x^2 & +1 &) & x^3 & +2x^2 & +3x & +4 \\ & & & x^3 & & +x & \\ \hline & & & & 2x^2 & +2x & +4 \\ & & & & 2x^2 & & +2 \\ \hline & & & & & 2x & +2 \end{array}$$

So the answer is $\boxed{2x+2}$.

Question 2(a) is bookwork, and 2(b,c) are coursework.

Question 3 [13 marks].

(a) State the definition of a **partition** of a set X. **[4]**

(b) Let R be an equivalence relation on X. The Equivalence Relation Theorem describes how to use R to produce a partition P of X. Write down how P is defined in terms of R. Your answer should include how the parts of P are defined [i.e. don't just use a symbol for each part without explaining what it means]. **[4]**

(c) Give an example of a partition of $\mathbb{C}$ with exactly two parts. **[2]**

(d) Write down all possible partitions of the set $\{1, 2\}$. **[3]**

Solution (a) A partition $\mathcal{P}$ of X is a set, whose elements are called **parts**, such that:

(i) $\emptyset$ is not a part of $\mathcal{P}$;

(ii) if A and B are distinct parts of $\mathcal{P}$, then $A \cap B = \emptyset$;

(iii) The union of all parts of $\mathcal{P}$ is X.

(The parts of $\mathcal{P}$ are subsets of X, but this is implied by the definition above and need not be stated separately.)
(b) $P = \{[x]_R : x \in X\}$, where $[x]_R = \{y \in X : (x, y) \in R\}$.
(c) One of very many possibilities is $\{\{0\}, \mathbb{C}^\times\}$.
(d) There are two, $\{\{1, 2\}\}$ and $\{\{1\}, \{2\}\}$.

Questions 3(a,b) are bookwork. 3(c) is like an example from lectures. 3(d) is unseen.

Question 4 [10 marks].

(a) Let R be a ring. In order to be a **field**, R must satisfy four further axioms. Write down the names of these axioms. You need not write out what the axioms assert. **[4]**

(b) The ring $\mathbb{Z}_{35}$ is not a field. Name one of the axioms from your list in part (a) that is not satisfied by $\mathbb{Z}_{35}$. Write down a counterexample to this axiom in $\mathbb{Z}_{35}$, and explain why your counterexample is valid. **[6]**

Solution (a) These are the multiplicative identity law, the multiplicative inverse law, the multiplicative commutative law, and the nontriviality law.
(b) $\mathbb{Z}_{35}$ does not satisfy the multiplicative inverse law. A counterexample to this law is that $[5]_{35}$ has no inverse. For any $[a]_{35} \in \mathbb{Z}_{35}$, the product $[5]_{35}[a]_{35} = [5a]_{35}$ cannot equal $[1]_{35}$: if it did, we would have $5a \equiv_{35} 1$, that is $5a - 1 = 35k$ for some integer k, but 5 divides the right side of that equation and not the left side.

Question 4(a) is bookwork, and 4(b) has been discussed in lectures although not in this exact form.

Question 5 [14 marks]. Let U be the set $\{ (a, b, c) : a, b, c \in \mathbb{R} \}$. Two operations $+$ and $\cdot$ on U are defined by

$$(a, b, c) + (d, e, f) = (a + d, b + e, c + f),$$
$$(a, b, c) \cdot (d, e, f) = (ad, ae + bf, cf).$$

(a) Prove the multiplicative identity law for U. **[8]**

(b) Prove that $(2, 1, 0)$ is not a unit in U. **[6]**

Solution (a) The multiplicative identity element for U is $(1, 0, 1)$, as is shown by the equalities

$$(1, 0, 1) \cdot (a, b, c) = (1a, 1b + 0c, 1c) = (a, b, c)$$
$$(a, b, c) \cdot (1, 0, 1) = (a1, a0 + b1, c1) = (a, b, c)$$

for any $(a, b, c) \in U$.
(b) We must show that $(2, 1, 0)$ has no multiplicative inverse. If (a, b, c) were its multiplicative inverse, the product of these two elements in either order must equal the identity $(1, 0, 1)$ from part (a). But

$$(a, b, c) \cdot (2, 1, 0) = (a \cdot 2, a \cdot 1 + b \cdot 0, c \cdot 0)$$

whose last component cannot equal 1.

Question 5 is an unseen question with parallels in tutorial exercises and coursework.

Question 6 [15 marks].

(a) Define what it means for a set G with a binary operation $*$ to be a **group**. Include the full statements of the axioms. **[5]**

Now let $G = \{ x \in \mathbb{R} : x > -1 \}$, with the binary operation $*$ given by $a * b = ab + a + b$.

(b) Prove that $*$ is associative. **[6]**

(c) Write down the identity element of $(G, *)$, and a formula for the inverse of an element $x \in G$. You need not provide the proofs. **[4]**

Solution (a) $(G, *)$ is a group if the following axioms are satisfied:

Closure law: for all $a, b \in G$, we have $a * b \in G$.

Associative law: for all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.

Identity law: there is an element $e \in G$ (called the **identity**) such that $a * e = e * a = a$ for any $a \in G$.

Inverse law: for all $a \in G$, there exists $b \in G$ such that $a * b = b * a = e$, where e is the identity. The element b is called the **inverse** of a.

[Technically the closure law is redundant with the definition of binary operation, so it is OK if this is omitted.]

(b) To prove the associative law, we must show that $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$. We expand

$$(a * b) * c = (ab + a + b) * c = (ab + a + b)c + (ab + a + b) + c$$
$$= abc + ac + bc + ab + a + b + c$$

and

$$a * (b * c) = a * (bc + b + c) = a(bc + b + c) + a + (bc + b + c)$$
$$= abc + ab + ac + a + bc + b + c.$$

getting equal results.
(c) $\boxed{0 \in G}$ is the identity element because [not required!]

$$a * 0 = a0 + a + 0 = a,$$
$$0 * a = 0a + 0 + a = a.$$

The inverse of $a \in G$ is $\boxed{a^{-1} := -a/(a+1).}$ Proof [not required!] This inverse lies in G: since $a + 1$ is positive, $-a/(a+1) > -1$ is equivalent to $-a > -1(a+1)$, which is true. Now to check the equation:

$$a * a^{-1} = a \cdot \frac{-a}{a+1} + a + \frac{-a}{a+1} = \frac{-a^2 + a(a+1) - a}{a+1} = 0,$$

which is our identity element. Since $*$ is visibly commutative, $a^{-1} * a$ will come out to 0 as well.

Question 6(a) is bookwork, and 6(b,c) are unseen.

Question 7 [18 marks].

(a) Let n be a positive integer. Define the **symmetric group** S_n. Make sure to specify both the set S_n and the definition of its group operation. **[4]**

(b) How many elements does S_n have? **[2]**

Now let g be the element

$$(1\,4\,6\,9)(2\,5\,8)(3\,10\,7)$$

of S_{10}, written in cycle notation, and let h be the element

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 9 & 2 & 7 & 5 & 6 & 1 & 8 & 10 \end{pmatrix}$$

of S_{10}, written in two-line notation.

(c) Write g in two-line notation. **[3]**

(d) Compute $h^{-1} \circ g^{-1}$, and write it in cycle notation. Show all your working. **[9]**

Solution (a) S_n is the set of all permutations on $\{1, \ldots, n\}$, that is, bijections from this set to itself. Its group operation is composition: given $f, g \in S_n$, composition yields the permutation $f \circ g$ defined by $(f \circ g)(x) = f(g(x))$ for all $x \in \{1, \ldots, n\}$.
(b) $|S_n| = n!$.
(c) This is a matter of tabulating, for each element of $\{1, \ldots, 10\}$, which element follows it in the cycle containing it. We get

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 5 & 10 & 6 & 8 & 9 & 3 & 2 & 1 & 7 \end{pmatrix}.$$

(d) We can save ourselves one step by using the fact that $h^{-1}g^{-1} = (gh)^{-1}$. We'll work in the two-line notation until the end. We find gh by tabulating $g(h(x))$ for each $x \in \{1, \ldots, 10\}$.

$$gh = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 1 & 5 & 3 & 8 & 9 & 4 & 2 & 7 \end{pmatrix}$$

Now, we invert the product by swapping the two rows. I've also sorted the first row back into order.

$$(gh)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 9 & 5 & 8 & 4 & 1 & 10 & 6 & 7 & 2 \end{pmatrix}$$

Finally we convert to cycle notation. In the cycle notation for f, each cycle has the form $(a\ f(a)\ f(f(a))\ \ldots)$, where we use the two-line notation to look up the values of f, and we stop once we come round to a again. We do this until each element of $\{1, \ldots, 10\}$ is in some cycle. Cycles with just one element in need not be written down. The final answer is

$$h^{-1}g^{-1} = (gh)^{-1} = (1\,3\,5\,4\,8\,6)(2\,9\,7\,10).$$

Questions 7(a,b) are bookwork, and 7(c,d) are standard algorithms.

End of Paper.