Queen Mary
University of London

Main Examination period 2018

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.

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

Calculators are not permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

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 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 shall 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.R. Fink, J.N. Bray

Question 1. [10 marks] Find all complex solutions z to the equation

$$z^3 = -3\sqrt{3}$$

and write them in the form $z = a + b\mathrm{i}$ for $a, b \in \mathbb{R}$.

Solution We work in Euler's notation. The complex number $-3\sqrt{3} = -3\sqrt{3} + 0\mathrm{i}$ is written as $re^{\mathrm{i}\theta}$ by taking $r = |-3\sqrt{3}| = 3\sqrt{3}$ and $\cos\theta = -3\sqrt{3}/r = -1$ so $\theta = \pi$, up to multiples of 2π. Write $z = se^{\mathrm{i}\varphi}$ where $s = |z|$ and $\varphi = \arg(z)$. Then we have

$$s^3 e^{3\mathrm{i}\varphi} = (se^{\mathrm{i}\varphi})^3 = 3\sqrt{3}e^{\mathrm{i}\pi}$$

whence

$$s^3 = 3\sqrt{3} \quad \text{and} \quad 3\varphi = \pi + 2k\pi \quad \text{for some integer} \quad k,$$

that is $s = (3\sqrt{3})^{1/3} = \sqrt{3}$ and

$$\varphi \in \left\{ \dots, \frac{\pi}{3}, \pi, \frac{5\pi}{3}, \dots \right\}$$

where the three values written out suffice to give the four distinct solutions

$$z = \sqrt{3}e^{\mathrm{i}\pi/3}, \quad z = \sqrt{3}e^{\mathrm{i}\pi} \quad \text{and} \quad z = \sqrt{3}e^{5\mathrm{i}\pi/3}.$$

In standard form these are

$$z = \frac{\sqrt{3}}{2} + \frac{3}{2}\mathrm{i}, \quad z = -\sqrt{3}, \quad \text{and} \quad z = \frac{\sqrt{3}}{2} - \frac{3}{2}\mathrm{i}.$$

Question 1 is standard, appearing with different constants in the notes and coursework.

Question 2. [12 marks]

(a) Define what it means for $\mathcal{A} = \{A_1, A_2, \dots\}$ to be a **partition** of a set X. **[3]**

(b) Let $\mathcal{A}$ be a partition of X. Prove that

$$R = \{\, (x, y) \in X : \text{there exists } i \text{ such that } x \in A_i \text{ and } y \in A_i \,\}$$

is an equivalence relation on X. **[6]**

(c) Write down a partition of $\mathbb{Z}$ into three parts, exactly two of which are infinite. **[3]**

Solution (a) A **partition** of X is a collection $\{A_1, A_2, \ldots\}$ of subsets of X, called its **parts**, having the following properties:

(i) $A_i \neq \emptyset$ for all i;

(ii) $A_i \cap A_j = \emptyset$ for all $i \neq j$;

(iii) $A_1 \cup A_2 \cup \cdots = X$.

[This is as given in the lecture notes. It implicitly assumes the set of parts is countable; for exam purposes I don't care about that restriction.]
(b)

- x and x lie in the same part of the partition, so R is reflexive.
- If x and y lie in the same part of the partition, then so do y and x; so R is symmetric.
- Suppose that x and y lie in the same part A_i of the partition, and y and z lie in the same part A_j. Then $y \in A_i$ and $y \in A_j$, so $y \in A_i \cap A_j$; so we must have $A_i = A_j$ (since different parts are disjoint). Thus x and z both lie in A_i. So R is transitive.

(c) One answer is $\{\{a \in \mathbb{Z} : a < 0\}, \{0\}, \{a \in \mathbb{Z} : a > 0\}\}$.

Of Question 2, parts (a,b) are bookwork and part (c) is unseen.

Question 3. [13 marks]

(a) Define the divisibility relation $\mid$ on the set of natural numbers. **[2]**

(b) A relation R on a set X is said to be **antisymmetric** if the following condition holds: For all elements $a, b \in X$, if $a \mathrel{R} b$ and $b \mathrel{R} a$ both hold then $a = b$. Prove that $\mid$ is antisymmetric. **[5]**

(c) Define the **least common multiple** of two nonzero natural numbers. **[2]**

(d) Compute the least common multiple of $336 = 2^4 \cdot 3 \cdot 7$ and $180 = 2^2 \cdot 3^2 \cdot 5$. Include an explanation of your method. [If you cite facts from lectures or coursework, you need not prove them.] **[4]**

Solution (a) $\mid$ is the set

$$\{(a, b) \in \mathbb{N}^2 : \text{there exists } k \in \mathbb{N} \text{ such that } b = ka\}.$$

(b) Let a and b be natural numbers so that $a \mid b$ and $b \mid a$. By definition, this implies there are natural numbers k and ℓ so that $b = ka$ and $a = \ell b$. Substituting the second equation into the first shows $a = \ell(ka)$. Assume as one of two cases that $a \neq 0$. Then $1 = \ell k$, and the only way to factorise 1 as a product of two natural numbers is $1 \cdot 1$, so $k = \ell = 1$, which implies that $a = b$. In the other case, $a = 0$, we have $b = k0 = 0$, so $a = b$ in this case as well.
(c) The natural number m is a **common multiple** of a and b if both $a \mid m$ and $b \mid m$. It is the **least common multiple** if it is a common multiple which is less than any other common multiple.
(d) For each prime p, the exponent of p in the prime factorisation of $\operatorname{lcm}(a, b)$ is the maximum of the exponents of p appearing in the factorisations of a and of b. Therefore the lcm sought in this question is $2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 5040$.

Of Question 3, parts (a,c) are bookwork, (b) is coursework, and (d) appeared in lecture with different numbers.

Question 4. [24 marks]

(a) Write down the **multiplicative inverse law** for a ring R. [Pay attention to the quantifiers ("for all", "there exists") and other conditions in the law.] **[3]**

(b) Compute the multiplicative inverse of $[23]_{43}$ in $\mathbb{Z}_{43}$. Show your working. **[14]**

(c) Find a multiplicative inverse of the matrix $\begin{bmatrix} [15]_{43} & [14]_{43} \\ [4]_{43} & [11]_{43} \end{bmatrix}$ in $M_2(\mathbb{Z}_{43})$. **[7]**

Solution (a) For each $a \in R$ which is not equal to 0, there exists an element $b \in R$ such that $ab = ba = 1$.
(b) We use the extended Euclidean algorithm.

$$\begin{aligned}
20 &= 43 - 1 \cdot 23\\
3 &= 23 - 1 \cdot 20\\
2 &= 20 - 6 \cdot 3\\
1 &= 3 - 1 \cdot 2\\
0 &= 2 - 2 \cdot 1
\end{aligned}$$

Then

$$\begin{aligned}
1 &= 3 - 1 \cdot 2\\
&= 3 - 1 \cdot (20 - 6 \cdot 3)\\
&= -1 \cdot 20 + 7 \cdot 3\\
&= -1 \cdot 20 + 7 \cdot (23 - 1 \cdot 20)\\
&= 7 \cdot 23 - 8 \cdot 20\\
&= 7 \cdot 23 - 8 \cdot (43 - 1 \cdot 23)\\
&= -8 \cdot 43 + 15 \cdot 23.
\end{aligned}$$

So $[23]_{43}^{-1} = [15]_{43}$.
(c) Because $\mathbb{Z}_{43}$ is a field, the familiar adjoint formula for inverting 2×2 matrices holds: if A is the given matrix, then

$$A^{-1} = (\det A)^{-1} \begin{bmatrix} [11]_{43} & -[14]_{43} \\ -[4]_{43} & [15]_{43} \end{bmatrix}.$$

Here $\det(A) = [15]_{43}[11]_{43} - [14]_{43}[4]_{43} = [15 \cdot 11 - 14 \cdot 4]_{43} = [109]_{43} = [23]_{43}$, whose inverse we have just computed to be $[15]_{43}$. Thus

$$A^{-1} = [15]_{43} \begin{bmatrix} [11]_{43} & -[14]_{43} \\ -[4]_{43} & [15]_{43} \end{bmatrix} = \begin{bmatrix} [165]_{43} & [-210]_{43} \\ [-60]_{43} & [225]_{43} \end{bmatrix} = \begin{bmatrix} [36]_{43} & [5]_{43} \\ [26]_{43} & [10]_{43} \end{bmatrix}.$$

Of question 4, part (a) is bookwork, part (b) a standard algorithm, and being able to do the computation of part (c) is implicit in some coursework questions.

Question 5. [12 marks]

(a) Give the names of all the axioms that must hold in a **field**. You do not have to write out what the axioms say. **[4]**

(b) Write down the definition of the field $\mathbb{C}$ of complex numbers. You should include a specification of the elements of $\mathbb{C}$ and of its addition and multiplication operations. [You may assume the definition of $\mathbb{R}$ is understood.] **[4]**

(c) Using your definition in part (b), prove that $\mathbb{C}$ satisfies the commutative law for multiplication. [You may assume that $\mathbb{R}$ is a field.] **[4]**

Solution (a) A field must satisfy the closure, associative, identity, inverse, and commutative laws for addition; the closure, associative, identity, inverse, and commutative laws for multiplication; and the distributive law and nontriviality law.
(b) The field $\mathbb{C}$ of complex numbers has set of elements

$$\{a + b\mathrm{i} : a, b \in \mathbb{R}\}$$

and addition and mutiplication operations defined by

$$(a + b\mathrm{i}) + (c + d\mathrm{i}) := (a + c) + (b + d)\mathrm{i},$$
$$(a + b\mathrm{i}) \cdot (c + d\mathrm{i}) := (ac - bd) + (ad + bc)\mathrm{i}.$$

(c) We must prove that

$$xy = yx$$

for complex numbers $x = a + b\mathrm{i}$ and $y = c + d\mathrm{i}$. The left hand side is

$$(a + b\mathrm{i})(c + d\mathrm{i}) = (ac - bd) + (ad + bc)\mathrm{i}$$

while the right hand side is

$$(c + d\mathrm{i})(a + b\mathrm{i}) = (ca - db) + (cb + da)\mathrm{i}$$

which are equal, by the commutative laws for the real numbers.

Question 5 is wholly bookwork.

Question 6. [14 marks]

(a) Let R be a ring. Give the definition of **polynomial in x with coefficients in R**. **[2]**

(b) Define the **degree** of a polynomial. **[2]**

(c) Let $f(x)$ and $g(x)$ be nonzero polynomials in $\mathbb{R}[x]$, of degrees m and n, respectively. Prove that $\deg(f(x)\,g(x)) = m + n$. **[5]**

(d) Give a counterexample to the multiplicative inverse law for the ring $\mathbb{R}[x]$ of polynomials in x with real coefficients. Explain why your counterexample works. **[5]**

Solution (a) Let R be a ring and x a formal symbol. A **polynomial in x with coefficients in R** is an expression

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_0, a_1, \ldots, a_{n-1}, a_n$ are elements of R.
(b) The **degree** of the polynomial $f(x)$ above, if $f(x) \neq 0$, is the greatest i such that $a_i \neq 0$.
[We leave the degree of the zero polynomial undefined.]
(c) By the assumption on their degrees, f and g can be written out as

$$f = a_m x^m + \cdots + a_1 x + a_0,$$
$$g = b_n x^n + \cdots + b_1 x + b_0$$

where $a_0, \ldots, a_m$ and $b_0, \ldots, b_n$ are complex numbers with $a_m \neq 0$ and $b_n \neq 0$.
By definition the product fg is the sum of all products of a term of f and a term of g. A term of f has the form $a_i x^i$ for some natural number i, and a term of g the form $b_j x^j$ for some natural number j; the product of these two is $a_i b_j x^{i+j}$. Since $i \leq m$ and $j \leq n$, the exponent in the product is at most $m+n$, and it can only equal $m+n$ if $i = m$ and $j = n$. Therefore the only term of fg with an x^{m+n} in it is $a_m b_n x^{m+n}$, and there are no terms with higher exponents of x. Since a_m and b_n are nonzero, their product is also nonzero. That is, x^{m+n} has a nonzero coefficient in fg, and all higher powers of x have zero coefficients (they don't appear). This proves $\deg(fg) = m + n$.
(d) The polynomial x has no inverse in $\mathbb{R}[x]$. The zero polynomial cannot be its inverse, and if $f \in \mathbb{R}[x]$ is nonzero then $\deg(xf) = 1 + \deg(f)$ by part (d), which cannot equal $0 = \deg(1)$.

Of Question 6, parts (a,b,d) are bookwork and part (c) is coursework.

Question 7. [15 marks]

(a) Define what it means for a set G with a binary operation $*$ to be a **group**. Include statements of any axioms you invoke, not just their names. **[3]**

(b) Let K be the set of integers with the operation $\circ$ defined by

$$x \circ y = x + y + 1.$$

Prove that K with the operation $\circ$ is a group. **[6]**

(c) Let H be a subset of a group $(G, *)$. Define what it means for H to be a **subgroup** of G. **[2]**

(d) Specify a proper subgroup of the additive group $\mathbb{Z}_6$. The Cayley table of $\mathbb{Z}_6$ is provided below. **[4]**

$+$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

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, written a^*.

(b) We must prove the group axioms.
Closure. We must check that $a \circ b$ is actually an element of G, if a and b are elements of G. This is clear: if a and b are integers, so is $a + b + 1$.
Associativity. We must show that

$$(a \circ b) \circ c = a \circ (b \circ c).$$

The left side is

$$(a \circ b) \circ c = (a + b + 1) \circ c = a + b + 1 + c + 1$$

and the right side is

$$a \circ (b \circ c) = a \circ (b + c + 1) = a + b + c + 1 + 1,$$

which are equal.
Identity. We must find an element $e \in G$ such that $a \circ e = a = e \circ a$ for all $a \in G$. It is easy to see by solving the resulting equation that $e = -1$ works, for then

$$a \circ e = a + (-1) + 1 = a$$

and

$$e \circ a = (-1) + a + 1 = a$$

for any $a \in G$.
Inverses. We must show that for any $a \in G$, there is a $b \in G$ such that $a \circ b = e = b \circ a$, where $e = -1$ is the identity element we found in the previous part. Again, solving the equations that result quickly leads to identifying $b = -a - 2$ as the inverse of a. This works because

$$a \circ b = a + (-a - 2) + 1 = -1 = e$$

and

$$b \circ a = (-a - 2) + a + 1 = -1 = e.$$

(c) H is a **subgroup** of G if is it a nonempty subset closed under $*$ and taking inverses (with respect to $*$).
(d) There are three proper subgroups: $\{[0]_6\}$, $\{[0]_6, [3]_6\}$, and $\{[0]_6, [2]_6, [4]_6\}$. ($\mathbb{Z}_6$ itself is a subgroup but not proper.)

Of Question 7, parts (a,c) are bookwork, (b) is coursework and (d) is strictly speaking unseen.

End of Paper.