Queen Mary
University of London

Main Examination period 2019

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.

Only non-programmable calculators that have been approved from the college list of 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

Question 1. [8 marks] Let $f, g \in \mathbb{R}[x]$ be polynomials, with $\deg g > 0$.

(a) The **division rule for polynomials** states that f can be divided by g to produce a quotient q and remainder r. Write down the two conclusions that the division rule states about q and r. **[2]**

(b) How do we tell, from q and r, whether g **divides** f? **[2]**

(c) Suppose that $\deg f = 8$, and $(x-1)^3$ divides f. What can be said about the multiplicity of $x = 1$ as a solution of $f(x) = 0$? **[4]**

Solution (a) First, $f = qg + r$. Second, $\deg r < \deg g$ or $r = 0$ (in which case we have left $\deg r$ undefined).
(b) g divides f if and only if $r = 0$.
(c) $x = 1$ has multiplicity at least 3, and at most 8.

Of Question 1, parts (a,b) are bookwork, and logic like (c) has been part of a coursework question.

Question 2. [14 marks]

(a) Define the following terms:

(i) **Cartesian product** of two sets; **[2]**

(ii) **relation** on a set X. **[2]**

(b) Write down a relation on the set $\{1, 2, 3\}$ which is reflexive and symmetric but not transitive. **[4]**

(c) Let S be the relation on the set $\mathbb{R} \setminus \{0\}$ defined by

$$xSy \text{ if and only if } y/x \in \mathbb{Q}.$$

Prove that S is an equivalence relation. **[6]**

Solution (a)(i) If X and Y are two sets, their Cartesian product is

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

(a)(ii) A relation on X is a subset of $X \times X$.
(b) One such relation is

$$\{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}.$$

(c) For brevity, write $X := \mathbb{R} \setminus \{0\}$.

- Reflexivity: $x/x = 1 \in \mathbb{Q}$ for all $x \in X$.
- Symmetry: If $x, y \in X$ satisfy $y/x \in \mathbb{Q}$ then also $x/y = 1/(y/x) \in \mathbb{Q}$, since $x/y \neq 0$ and $\mathbb{Q}$ contains multiplicative inverses of all its elements.

- Transitivity: If $x, y, z \in X$ satisfy $y/x \in \mathbb{Q}$ and $z/y \in \mathbb{Q}$ then also $z/x = (z/y)(y/x) \in \mathbb{Q}$ because $\mathbb{Q}$ is closed under multiplication.

Of Question 2, parts (a) is bookwork, (b) was mostly on an exercise sheet, and (c) is a standard type of proof in which the relation is unseen but with some seen parallels.

Question 3. [22 marks]

(a) Define the **greatest common divisor** of two positive integers. **[2]**

(b) Use the extended Euclidean algorithm to compute the greatest common divisor d of 206 and 64, and to find integers x and y such that $206x + 64y = d$. **[16]**

(c) Write down another pair of integers (x', y') such that $206x' + 64y' = d$, different from the pair (x, y) you found in part (b). **[4]**

Solution (a) The **greatest common divisor** of the natural numbers a and b is the natural number d with the properties

(a) $d \mid a$ and $d \mid b$;

(b) if e is a natural number satisfying $e \mid a$ and $e \mid b$, then $e \mid d$.

(b) We run the algorithm. The forward phase goes

$$\begin{aligned} 206 &= 3 \cdot 64 + 14 \\ 64 &= 4 \cdot 14 + 8 \\ 14 &= 1 \cdot 8 + 6 \\ 8 &= 1 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

So $d = \gcd(206, 64) = 2$.
Now for the extended phase:

$$\begin{aligned} &2 \\ &= 8 - 1 \cdot 6 \\ = 8 - 1(14 - 1 \cdot 8) &= -1 \cdot 14 + 2 \cdot 8 \\ = -1 \cdot 14 + 2(64 - 4 \cdot 14) &= 2 \cdot 64 - 9 \cdot 14 \\ = 2 \cdot 64 - 9(206 - 3 \cdot 64) &= -9 \cdot 206 + 29 \cdot 64. \end{aligned}$$

Hence we can take $x = -9$ and $y = 29$.
(c) If (x, y) is a particular integer solution to $xa + yb = c$, then the general solution is

$$(x', y') = (x + kb/\gcd(a, b),\ y - ka/\gcd(a, b))$$

for $k \in \mathbb{Z}$. Here, taking $(x, y) = (-9, 29)$ and for example $k = 1$ yields $(x', y') = (23, -74)$.

Of Question 3, part (a) is bookwork, part (b) is a standard algorithm, and part (c) with different constants appeared in coursework.

Question 4. [16 marks]

(a) Give the names of all axioms that must be satisfied in order for a set R with two operations $+$ and $\cdot$ to be a **ring**. [Do not write out what the axioms say.] **[6]**

(b) Name an example of a ring that is not a commutative ring. **[2]**

(c) Let R be a commutative ring. Prove that the identity $x^2 - y^2 = (x+y) \cdot (x-y)$ is true for all x and y in R. Name the axiom or proposition that you are using at each step of the proof. **[8]**

Solution (a) To be a ring, R must satisfy the additive closure, associative, identity, inverse, and commutative laws; the multiplicative closure and associative laws; and the distributive law.
(b) $\mathrm{M}_2(\mathbb{R})$ is an example of a non-commutative ring.
(c) The proof of the identity is

$$\begin{aligned}(x+y)(x-y) &= x(x-y) + y(x-y) \\ &= xx + x(-y) + yx + y(-y) \\ &= x^2 - xy + yx - y^2 \\ &= x^2 - xy + xy - y^2 \qquad (*) \\ &= x^2 - y^2.\end{aligned}$$

The first two equalities use the distributive law. The third equality uses a proposition $x(-y) = -xy$ proved in lectures. The fourth equality uses the commutative law for multiplication. The last uses the additive inverse and identity laws. Several uses of the additive associativity law are hidden by the notation, since I was writing sums of more than two terms without parentheses.

Questions 4(a,b) are bookwork. 4(c) appeared in coursework, though I didn't explicitly ask for naming the axioms.

Question 5. [14 marks]

(a) Define what it means for an element of a ring with identity R to be a **unit**. **[2]**

(b) List all units in the ring $\mathbb{Z}_{12}$. **[4]**

(c) Is the matrix $\begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}$ a unit in the ring $\mathrm{M}_2(\mathbb{Z})$? Justify your answer. **[4]**

(d) Is the matrix $\begin{bmatrix} [2]_{12} & [1]_{12} \\ [-1]_{12} & [2]_{12} \end{bmatrix}$ a unit in the ring $\mathrm{M}_2(\mathbb{Z}_{12})$? Justify your answer. **[4]**

Solution (a) An element $u \in R$ is called a **unit** if there is an element $v \in R$ such that $uv = vu = 1$.
(b) The units of $\mathbb{Z}_{12}$ are $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, and $[11]_{12}$.
(c) This part and part (d) are possible to solve by writing out a general matrix and solving equations, but the determinant provides a quicker way. If R is a commutative ring, then the determinant $\det : \mathbb{M}_n(R) \to R$ is multiplicative:
$\det(AB) = \det(A)\det(B)$. The determinant of the identity matrix is 1. The given matrix has determinant 5, so the determinant of its inverse would have to be a multiplicative inverse of 5 in $\mathbb{Z}$, which does not exist.
(d) There is a formula for the inverse of a 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over a commutative ring is

$$A^{-1} = (\det A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

when $\det A$ is a unit. In particular the inverse exists in this case. For the matrix in the question the determinant $[5]_{12}$ is a unit, by part (b).
In fact $[5]_{12}$ has inverse $[5]_{12}$ so the matrix has inverse

$$[5]_{12}^{-1} \begin{bmatrix} [2]_{12} & -[1]_{12} \\ -[-1]_{12} & [2]_{12} \end{bmatrix} = \begin{bmatrix} [10]_{12} & [7]_{12} \\ [5]_{12} & [10]_{12} \end{bmatrix}.$$

Of Question 5, part (a) is bookwork, (b) is standard, and I have shown standard methods for questions of the type of (c,d) as well.

Question 6. [16 marks] Let g be the element

$$(1\ 9\ 11\ 4\ 6)(2\ 5\ 8)(3\ 10\ 7)$$

of S_{11}, written in cycle notation, and let h be the element

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 4 & 2 & 11 & 6 & 1 & 5 & 9 & 3 & 10 & 8 \end{pmatrix}$$

of S_{11}, written in two-line notation.

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

(b) Find a permutation k such that $k \circ g = h$. Write k in two-line notation. [8]

(c) Define the **order** of a permutation. [2]

(d) Write down the order of g. [3]

Solution (a) This is a matter of tabulating, for each element of $\{1, \dots, 11\}$, which element follows it in the cycle containing it. We get

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 5 & 10 & 6 & 8 & 1 & 3 & 2 & 11 & 7 & 4 \end{pmatrix}.$$

(b) To see what to do we can multiply both sides of the given equation by g^{-1} on the right: $k = kgg^{-1} = hg^{-1}$. We'll work in the two-line notation throughout. We compute g^{-1} by swapping the two rows:

$$g^{-1} = \begin{pmatrix} 9 & 5 & 10 & 6 & 8 & 1 & 3 & 2 & 11 & 7 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{pmatrix}$$

Now, we find $k = hg^{-1}$ by tabulating $h(g^{-1}(x))$ for each $x \in \{1, \dots, 11\}$.

$$k = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 9 & 5 & 8 & 4 & 11 & 10 & 6 & 7 & 2 & 3 \end{pmatrix}$$

(c) More generally, the **order** of an element h of a group is the smallest positive integer n for which $h^n = e$, if such a number exists. If no positive power of h is equal to e, we say that h has infinite order.
(d) The order of a permutation is the lcm of the lengths of its cycles. So the order of g is $\text{lcm}(5, 3, 3) = 15$.

Question 6 is standard.

Resit paper replacement Question 6.

(a) Consider the partition of the set of complex numbers whose parts are the sets

$$A_w = \{z \in \mathbb{C} : z^4 = w\}$$

for each complex number w. How many elements does each part have? What shape does each part make in the complex plane? **[5]**

(b) Write out all elements of the part A_{-4} in the form $a + b\mathrm{i}$ where a and b are real numbers. Show your working. **[11]**

Solution (a) The parts A_w are the sets of fourth roots of individual complex numbers. Each part has cardinality 4 and forms a square in the complex plane centred at the origin, with the exception of the part $\{0\}$, which has cardinality 1 and so gives a single point in the complex plane, the origin itself.
(b) We work in Euler's notation. The complex number $-4 = -4 + 0\mathrm{i}$ is written as $re^{\mathrm{i}\theta}$ by taking $r = |-4| = 4$ and $\cos\theta = -4/r = -1$ so $\theta = \pi$, up to multiples of 2π. Write $z = se^{\mathrm{i}\varphi}$ where $s = |z|$ and $\varphi = \arg(z)$. Then we have

$$s^4 e^{4\mathrm{i}\varphi} = (se^{\mathrm{i}\varphi})^4 = \frac{1}{4}e^{\mathrm{i}\pi}$$

whence

$$s^4 = 4 \quad \text{and} \quad 4\varphi = \pi + 2k\pi \quad \text{for some integer} \quad k,$$

that is $s = \sqrt[4]{4} = \sqrt{2} > 0$, and

$$\varphi \in \left\{\dots, \frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}, \dots\right\}$$

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

$$z = \sqrt{2}e^{\mathrm{i}\pi/4}, \quad z = \sqrt{2}e^{3\mathrm{i}\pi/4}, \quad z = \sqrt{2}e^{5\mathrm{i}\pi/4} \quad \text{and} \quad z = \sqrt{2}e^{7\mathrm{i}\pi/4}.$$

In standard form these are

$$z = 1 + \mathrm{i}, \quad z = -1 + \mathrm{i}, \quad z = -1 - \mathrm{i} \quad \text{and} \quad z = 1 - \mathrm{i}.$$

In the 2017/18 instance of Introduction to Algebra, permutations were missed out due to industrial action, while roots of complex numbers were still in the syllabus, having been removed this year. In this question, the framing in terms of partitions is novel, but once this is peeled back part (a) is bookwork and part (b) a standard algorithm.

Question 7. [10 marks]

(a) Define what it means for a set G with a binary operation $*$ to be a **group**, including the statements of every axiom you cite. **[4]**

(b) Let

$$S = \{a + b\mathrm{i} \in \mathbb{C} : a, b \in \mathbb{R}, a^2 + b^2 = 1\}$$

be the set of all complex numbers of modulus 1. Prove that S is a subgroup of the multiplicative group $\mathbb{C}^{\times}$. **[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 can prove this using the subgroup test. Using the test, what we have to show is that if z and w are elements of S, then so is zw^{-1}.
Modulus of complex numbers is a multiplicative function, that is, $|zw| = |z| \cdot |w|$ for any complex numbers z and w. It follows, from

$$1 = |1| = |zz^{-1}| = |z| \cdot |z^{-1}|,$$

that $|z^{-1}| = 1/|z|$. Therefore, if z and w are elements of S so that $|z| = |w| = 1$, we have

$$|zw^{-1}| = |z| \cdot |w^{-1}| = \frac{|z|}{|w|} = \frac{1}{1} = 1,$$

implying $zw^{-1} \in S$. By the subgroup test, we may conclude that $(S, \cdot)$ is a subgroup of $\mathbb{C}^{\times}$.

Of Question 7, part (a) is bookwork and (b) is coursework.

End of Paper.