Main Examination period 2017

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. Fink, S. Beheshti

Question 1. [10 marks] Let x be a real number such that $x \neq 1$. Prove by mathematical induction that

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}$$

for every natural number $n \geqslant 1$. **[10]**

Solution Let $P(n)$ be the statement $1 + x + x^2 + \cdots + x^{n-1} = (x^n - 1)/(x-1)$. The base case requires that we establish $P(1)$. Here $P(1)$ says that $1 = (x-1)/(x-1)$, which is manifestly true by cancelling $x - 1$ from numerator and denominator.
We proceed to the inductive step. Suppose that $P(n)$ is true for **some** n. Then

$$\begin{aligned}(1 + x + x^2 + \cdots + x^{n-1}) + x^n &= \frac{x^n - 1}{x - 1} + x^n \\ &= \frac{x^n - 1 + x^n(x-1)}{x - 1} \\ &= \frac{x^n - 1 + x^{n+1} - x^n}{x - 1} \\ &= \frac{x^{n+1} - 1}{x - 1}.\end{aligned}$$

So $P(n+1)$ is true whenever $P(n)$ is true. Hence by induction, $P(n)$ is true **for all** $n \geqslant 1$.

Question 1 is standard: students have seen an abundance of similar examples in lecture and problem sheets, in this module and others. (Few if any of them have contained a free parameter, though.)

Question 2. [13 marks]

(a) Give the definition of a **partition** of a set X. **[3]**

(b) Write down:

(i) a set X, and a relation on X which is neither symmetric nor transitive. **[2]**

(ii) a partition of $\mathbb{Z}$ in which every part has cardinality two. **[2]**

(c) Let $\{A_1, A_2, \ldots\}$ be a partition of a set X. Prove that the relation R on X defined by

$$xRy \text{ if and only if there is some } i \text{ such that } x \in A_i \text{ and } y \in A_i$$

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

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

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

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

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

[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)(i) One example is $X = \{1,2,3\}$ with the relation $R = \{(1,2),(2,3)\}$.
(ii) One example is

$$\{\{2k, 2k+1\} : k \in \mathbb{Z}\} = \{\dots, \{-2,-1\}, \{0,1\}, \{2,3\}, \{4,5\}, \dots\}$$

(c)

- x and x lie in the same part of the partition $\{A_1, A_2, \dots\}$, 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 of a partition are disjoint. Thus x and z both lie in A_i. So R is transitive.

Thus R is an equivalence relation.

Questions 2(a,c) are bookwork; 2(b) is unseen.

Question 3. [21 marks]

(a) Use Euclid's algorithm to find the greatest common divisor of 288 and 111. Show all your working. **[6]**

(b) Does the equation $288x + 111y = 6$ have a solution where x and y are integers? Find one if so, showing your working, or explain why not if not. **[10]**

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

(d) Is $[111]_{288}$ a unit in the ring $\mathbb{Z}_{288}$? Why or why not? **[3]**

Solution (a) We calculate

$$\begin{aligned}288 &= 2\cdot 111+66\\ 111 &= 1\cdot 66+45\\ 66 &= 1\cdot 45+21\\ 45 &= 2\cdot 21+3\\ 21 &= 7\cdot 3+0,\end{aligned}$$

so the greatest common divisor is 3.
(b) We may use the extended Euclidean algorithm to find an integer solution to $288x'+111y'=3$. For this we unwind the calculations from part (a):

$$\begin{aligned}3 &= 1\cdot 45-2\cdot 21 = 1\cdot 45-2\cdot(66-1\cdot 45)\\ &= -2\cdot 66+3\cdot 45 = -2\cdot 66+3\cdot(111-1\cdot 66)\\ &= 3\cdot 111-5\cdot 66 = 3\cdot 111-5\cdot(288-2\cdot 111)\\ &= -5\cdot 288+13\cdot 111.\end{aligned}$$

So $x'=-5$ and $y'=13$ arrange that $288x'+111y'=3$.
To find a solution to $288x+111y=6$ it suffices to double both sides of the preceding equation. Therefore $x=-10$ and $y=26$ is a solution.
(c) An element $u\in R$ is called a **unit** if there is an element $v\in R$ such that $uv=vu=1$.
(d) No. By Theorem 6.3 from the notes, $[a]_m$ has a multiplicative inverse if and only if $\gcd(a,m)=1$. But we computed the gcd in part (a) and found it to equal 3, not 1.

Question 3(a) is standard; 3(b) is a less standard problem but still one they've seen; 3(c) is bookwork; and 3(d) an easy application of a familiar test.

Question 4. [14 marks] Let $\mathbb{H}=\{\alpha+\beta j:\alpha,\beta\in\mathbb{C}\}$ be the set of quaternions. Define a function $\varphi:\mathbb{H}\to\mathrm{M}_2(\mathbb{C})$ by

$$\varphi(\alpha+\beta j)=\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}.$$

(a) Write down the definition of multiplication for quaternions. **[2]**

(b) Prove that $\varphi(q\cdot r)=\varphi(q)\cdot\varphi(r)$ for any two quaternions $q,r\in\mathbb{H}$. **[4]**

(c) Prove that φ is an injective function. **[3]**

(d) Use parts (b) and (c) to prove that the quaternions satisfy the associative law for multiplication. You may assume that $\mathrm{M}_2(\mathbb{C})$ is a ring. **[5]**

Solution (a) Multiplication in the quaternions is defined by

$$(\alpha+\beta j)(\gamma+\delta j) := (\alpha\gamma-\beta\bar{\delta})+(\alpha\delta+\beta\bar{\gamma})j$$

where $\alpha,\beta,\gamma,\delta\in\mathbb{C}$.
(b) Let $q=\alpha+\beta j$ and $r=\gamma+\delta j$. Then

$$\begin{aligned}\varphi(\alpha+\beta j)\varphi(\gamma+\delta j) &= \begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}\begin{pmatrix}\gamma & \delta\\ -\bar{\delta} & \bar{\gamma}\end{pmatrix}\\ &= \begin{pmatrix}\alpha\gamma-\beta\bar{\delta} & \alpha\delta+\beta\bar{\gamma}\\ -\bar{\beta}\gamma-\bar{\alpha}\bar{\delta} & -\bar{\beta}\delta+\bar{\alpha}\bar{\gamma}\end{pmatrix}\end{aligned}$$

while, by the definition of quaternion multiplication

$$\begin{aligned}\varphi((\alpha+\beta j)(\gamma+\delta j)) &= \varphi((\alpha\gamma-\beta\bar{\delta})+(\alpha\delta+\beta\bar{\gamma})j)\\ &= \begin{pmatrix}\alpha\gamma-\beta\bar{\delta} & \alpha\delta+\beta\bar{\gamma}\\ -(\overline{\alpha\delta+\beta\bar{\gamma}}) & \overline{\alpha\gamma-\beta\bar{\delta}}\end{pmatrix}\\ &= \begin{pmatrix}\alpha\gamma-\beta\bar{\delta} & \alpha\delta+\beta\bar{\gamma}\\ -\bar{\alpha}\bar{\delta}-\bar{\beta}\gamma & \bar{\alpha}\bar{\gamma}-\bar{\beta}\delta\end{pmatrix}\end{aligned}$$

which is equal. In the last step we used the rules $\overline{z+w}=\bar{z}+\bar{w}$, $\overline{zw}=\bar{z}\bar{w}$, and $\bar{\bar{z}}=z$ for complex numbers z and w.
(c) We must show that if $q=\alpha+\beta j$ and $r=\gamma+\delta j$ are two quaternions with $\varphi(\alpha+\beta j)=\varphi(\gamma+\delta j)$, that is

$$\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}=\begin{pmatrix}\gamma & \delta\\ -\bar{\delta} & \bar{\gamma}\end{pmatrix},$$

then $\alpha+\beta j$ equals $\gamma+\delta j$. But this is clear: equating upper-left entries of the matrices gives $\alpha=\gamma$, and equating upper-right entries gives $\beta=\delta$.
(d) Let q, r, and s be quaternions. Then, by part (b) repeatedly,

$$\varphi(q(rs))=\varphi(q)\varphi(rs)=\varphi(q)(\varphi(r)\varphi(s))=(\varphi(q)\varphi(r))\varphi(s)=\varphi(qr)\varphi(s)=\varphi((qr)s),$$

using associativity of multiplication in $\mathrm{M}_2(\mathbb{C})$ in the middle. But by part (c) this implies $q(rs)=(qr)s$, so quaternion multiplication is associative.

Question 4(a) is bookwork; the remainder of the question is verbatim coursework.

Question 5. [14 marks]

(a) Let R be a ring. Define what it means for R to be

(i) a **commutative ring**; **[2]**

(ii) a **skewfield**. **[2]**

Give the full statement of any axioms you invoke.

(b) Let R be a ring. Prove from the axioms that $a\cdot 0=0$ for any $a\in R$. **[6]**

(c) Let R be a ring, and $a\in R$ an element such that $a^2=0$. Must it be true that $a=0$? Justify your answer. **[4]**

Solution (a)(i) A **commutative ring** is a ring R which satisfies the commutative law for multiplication:

$xy = yx$ for all $x, y \in R$.

(ii) A **skewfield** is a ring R which satisfies the identity and inverse laws for multiplication and the nontriviality law. In order, these assert:

there exists an element $1 \in R$ such that $1x = x = x1$ for all $x \in R$;
for all $x \in R \setminus \{0\}$ there exists $y \in R$ such that $xy = 1 = yx$;
$1 \neq 0$.

[I did not make a point of the nontriviality law in lecture, so I will not mark down solutions that omit to mention it.]
(b) We start with $0+0=0$, which holds by the additive identity law. Multiplying this equation on the right by a gives $(0+0)a = 0a$. Using distributivity gives $0a+0a = 0a$. But $0a+0 = 0a$ by the additive identity law. So $0a+0a = 0a+0$. At this point we only need to perform cancellation. As such, adding the additive inverse of $0a$ to each side gives

$$-(0a)+(0a+0a) = -(0a)+(0a+0).$$

Successive invocation on each side of this equation of associativity, the inverse law, and the zero law for addition bring this to $0a = 0$, as required.
(c) No. For example, in the ring $\mathbb{Z}_4$, the element $[2]_4$ is a nonzero element whose square is zero.

Questions 5(a,b) are bookwork; 5(c) is unseen, though examples have been presented explicitly in other contexts.

Question 6. [14 marks]

(a) Let G and H be groups, with respective operations $\circ$ and $*$. Define what it means for

(i) G to be a **subgroup** of H; **[2]**

(ii) G and H to be **isomorphic**. **[2]**

(b) Prove that
$$\{a^2/b^2 : a \text{ and } b \text{ are nonzero integers}\}$$
is a subgroup of the multiplicative group $\mathbb{Q}^\times$. **[6]**

(c) Suppose that G is a nonabelian group and H is an abelian group. With reference to the definition, explain why G and H cannot be isomorphic. **[4]**

Solution (a)(i) G is a **subgroup** of H if G is a subset of H and $g \circ h = g * h$ for all $g, h \in H$.
(ii) G and H are **isomorphic** if there is a bijective function $F : G \to H$ such that $F(g_1 \circ g_2) = F(g_1) * F(g_2)$ for all $g_1, g_2 \in G$.
(b) Let H be the set in question. Clearly $H \subseteq \mathbb{Q}^\times$ as sets. So we may use the subgroup test: we must show that for any two elements $h_1, h_2 \in H$, we also have $h_1(h_2)^{-1} \in H$. By the definition of H, we may write $h_1 = a^2/b^2$ and $h_2 = c^2/d^2$, where a, b, c, d are nonzero integers. Then $(h_2)^{-1} = d^2/c^2$ and $h_1(h_2)^{-1} = (ad)^2/(bc)^2$, which is an element of H. This completes the proof.
(c) Since G is nonabelian, there exist elements $g_1, g_2 \in G$ such that $g_1 \circ g_2 \neq g_2 \circ g_1$. Assuming that G and H were isomorphic, there would exist a bijection F as in part (a)(ii). Then

$$F(g_1) * F(g_2) = F(g_1 \circ g_2) \neq F(g_2 \circ g_1) = F(g_2) * F(g_1),$$

the inequality following from injectivity of F. This is a contradiction, because $F(g_1)$ and $F(g_2)$ are elements of the abelian group H.

Question 6(a) is bookwork; 6(b) is a proof of a type with precedents in lecture and coursework; 6(c) is unseen, though was mentioned in lecture in an unelaborated way.

Question 7. [14 marks] Let g be the element

$$(1\ 3\ 10)(2\ 5\ 12)(4\ 6\ 7\ 11\ 9)$$

of S_{12}, written in cycle notation, and let h be the element

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 12 & 5 & 3 & 10 & 2 & 11 & 1 & 9 & 8 & 7 & 6 \end{pmatrix}$$

of S_{12}, written in two-line notation.

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

(b) Compute $(gh)^{-1}$ and write your answer in cycle notation. **[6]**

(c) Define the **order** of an element of a group. **[2]**

(d) What is the order of h? **[3]**

Solution (a) This is a matter of tabulating, for each element of $\{1,\ldots,12\}$, which element follows it in the cycle containing it (which may be a trivial cycle). We get

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 10 & 6 & 12 & 7 & 11 & 8 & 4 & 1 & 9 & 2 \end{pmatrix}.$$

(b) The product gh is computed by working out $g(h(x))$ for each $x \in \{1,\ldots,12\}$ (bear in mind that we use left actions). Since we want a result in cycle notation, we can work through the values x in the order they arise in cycles in progress. This gives $(gh) = (1\ 6\ 5)(3\ 12\ 7\ 9\ 4\ 10\ 8)$. The inverse can then be computed by reversing all cycles: $(gh)^{-1} = (1\ 5\ 6)(3\ 8\ 10\ 4\ 9\ 7\ 12)$.
(c) 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 converting h to cycle notation, $h = (1\ 4\ 3\ 5\ 10\ 8)(2\ 12\ 6)(7\ 11)$, we readily see that its order is $\mathrm{lcm}(6,3,2,1) = 6$.

Question 7 is standard.

End of Paper.