Queen Mary University of London

MTH4104 Introduction to Algebra

Exam solutions **Semester B main exam period, 2021**

The solutions below pertain to just one of the possible randomly generated exam variants (namely, the chronologically first version of each question, without the question numbers being shuffled). Where I don't comment further, the randomisation affects just the numbers vel sim.

Each question is worth 10 marks. Questions 1 through 8 were marked by Moodle, questions 9 and 10 by hand.

2019/20 candidates were not taught about groups due to strike action, so their exam featured some replacement questions. Instances of these can be found at the end of this document.

Question 1 Let $f = (1\ 3\ 5\ 2\ 6\ 7\ 4)$ and $g = (1\ 4\ 2\ 6\ 7\ 5\ 3)$ be permutations in S_7, written in cycle notation.

(a) What is the second line of f in two-line notation? Enter it as a list of numbers separated by single spaces.

(b) Let $h = f \circ g^{-1}$. What is h in cycle notation? Enter single spaces between the numbers in each cycle. Do not type spaces anywhere else in your answer.

Solution These can be computed by the standard algorithms which were covered in the lectures and course notes. In this instance the answers are

(a) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 1 & 2 & 7 & 4 \end{pmatrix}$ so the answer is $\boxed{3\ 6\ 5\ 1\ 2\ 7\ 4}$. [$3\frac{1}{3}$ marks]

(b) $\boxed{(1\ 5\ 4\ 3\ 2)}$. [$6\frac{2}{3}$ marks]

Question 2 Fill in the blanks in the table below so that it becomes the Cayley table of a group with elements {a, b, c, d}.

	a	**b**	**c**	**d**
a	__	__	__	__
b	__	__	__	__
c	__	__	b	c
d	__	__	__	__

Solution In each variant of this question, one of the given entries equals its row or column index, implying that the other index is the identity element. In this case $\mathrm{c} \cdot \mathrm{d} = \mathrm{c}$ so d must be the identity element:

	a	**b**	**c**	**d**
a	__	__	__	a
b	__	__	__	b
c	__	__	b	c
d	a	b	c	d

All the remaining entries can now be filled in using the property that any Cayley table is a Latin square, starting with the row and column that have exactly two blanks. Here the final answer is

	a	**b**	**c**	**d**
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	b	c	d

.

Each box filled correctly is worth $\frac{5}{7}$ marks. I covered a similar question for 3×3 Cayley tables in an exam revision lecture.

Question 3 Carry out Euclid's algorithm to find $d = \gcd(372, 88)$. In the notation of the lecture notes, $b_0 = 372$ and $b_1 = 88$.

(a) Enter the first two remainders, b_2 and b_3, produced by the algorithm.

(b) Now carry out the extension to Euclid's algorithm. In the course of the algorithm, you will express d as an integer linear combination of each pair of successive remainders. Enter the integer coefficients that arise for the last three steps.

- $d = \_\_\_\_ \cdot b_2 + \_\_\_\_ \cdot b_3$
- $d = \_\_\_\_ \cdot b_1 + \_\_\_\_ \cdot b_2$
- $d = \_\_\_\_ \cdot b_0 + \_\_\_\_ \cdot b_1$. (This line is the final output of the algorithm. The last number you entered should have absolute value less than 46.)

Solution Euclid's algorithm and its extension were taught in lectures and course notes; this question merely required carrying out the algorithm. In every case the gcd is found as b_4.

(a) $\boxed{b_2 = 20,\ b_3 = 8}$ (and $d = b_4 = 4$). [$2\frac{1}{2}$ marks, $1\frac{1}{4}$ per answer]

(b) The first nontrivial step of the extension of Euclid's algorithm is the first one to be entered:

- $d = \boxed{1} b_2 + \boxed{(-2)} b_3$
- $d = \boxed{-2} b_1 + \boxed{9} b_2$
- $d = \boxed{9} b_0 + \boxed{(-38)} b_1$. [$7\frac{1}{2}$ marks, $1\frac{1}{4}$ per answer]

Question 4 Enter the multiplicative inverse of the element $[42]_{49}x+[9]_{49}$ in the ring $\mathbb{Z}_{49}[x]$.

When you enter your answer, make sure that all congruence classes are in the form $[a]_{49}$ with $0 \leq a < 49$. You don't have to type the brackets. For example, if your answer is $[2]_{49}x^2+[3]_{49}$, you can type `2x^2+3`.

Solution Suppose the inverse of the given element $f = [42]_{49}x+[9]_{49}$ has the form $f^{-1} = \cdots + a_2x^2 + a_1x + a_0$. We multiply this by f, equate coefficients with $1_{Z_{49}[x]} = \cdots + [0]_{49}x^2 + [0]_{49}x + +[1]_{49}$, and solve for $a_0, a_1, \ldots$ sequentially.

The product is

$$ff^{-1} = \cdots + ([42]_{49}\,a_1 + [9]_{49}\,a_2)x^2 + ([42]_{49}\,a_0 + [9]_{49}\,a_1)x + ([9]_{49}\,a_0).$$

The constant coefficient gives the equation $[9]_{49}a_0 = [1]_{49}$, implying $a_0 = [9]_{49}^{-1} = [11]_{49}$, e.g. by Euclid's algorithm. [5 marks]

Now, the linear coefficient gives the equation $[42]_{49}\,a_0 + [9]_{49}\,a_1 = [0]_{49}$. Substituting in the known value for a_0 gives

$$[0]_{49} = [42]_{49}\,[11]_{49} + [9]_{49}\,a_1 = [21]_{49} + [9]_{49}a_1$$

so $a_1 = -[21]_{49}[9]_{49}^{-1} = [-21 \cdot 11]_{49} = [14]_{49}$, reusing the modular inverse computed above. [5 marks]

The same procedure for a_2 gives $a_2 = [0]_{49}$, and then $a_3 = [0]_{49}$, at which point it is clear that the computation is repeating itself, so we will get zeroes from this point on and can stop. We conclude $f^{-1} = \boxed{[14]_{49}x+[11]_{49}}$.

This question was unseen, but there were questions on coursework sheets about computing multiplicative inverses in a novel ring given the definition of multiplication, for which my solutions used the same technique of setting up equations and solving.

Question 5 Let $R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$. You may assume that R is a ring with the usual matrix addition and multiplication operations. True or false:

(a) R is a commutative ring.

(b) R is a ring with identity.

(c) R is a skewfield.

Solution This question had variants with different matrix subrings, with up to three indeterminates (and enough zeroes that the multiplications were manageable). I expected the students to work out the product of two elements of the subring and be able to use that formula to observe (or solve for) whether the axioms hold. In none of the subrings were all three true and false answers the same as in $\mathrm{M}_n(\mathbb{R})$ itself. In the case at hand:

(a) True: if $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, then

$$AB = BA = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$

(b) True: R contains $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ so this is still an identity element.

(c) True: if A above is not zero, then it has an inverse $\frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

In this example a student who noticed the isomorphism with $\mathbb{C}$ could exploit that.

Each part was worth $3\frac{1}{3}$ marks. This question was precedented by coursework asking these questions for unseen rings.

Question 6 Let $f = z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in \mathbb{C}[z]$ be a polynomial of degree $n \geq 1$. Which of the factorisations below must exist? Select one or more:

(a) $f = (z-c_1)(z-c_2)\cdots(z-c_n)$, where $c_1, \ldots, c_n$ are complex numbers

(b) $f = (z-c_1)(z-c_2)\cdots(z-c_n)$, where $c_1, \ldots, c_n$ are different complex numbers

(c) $f = (z^2+r_1z+s_1)\cdots(z^2+r_kz+sk)$, where $r_1, \ldots, r_k$ and $s_1, \ldots, s_k$ are real numbers

(d) $f = g_1(z)\cdots g_k(z)$, where $g_1, \ldots, g_k \in \mathbb{C}[z]$ each have exactly one root, and all these roots are different

(e) $f = g_1(z)\cdots g_k(z)$, where $g_1, \ldots, g_k \in \mathbb{C}[z]$ each have exactly one root, and their degrees are all different

Solution This question is what bookwork looks like in our strange new online world. It had three variants, all relatively different as each was based on variations of the statement of a different theorem. Look at QMPlus for more information.

In this case:

(a) Yes, this is one of our statements of the Fundamental Theorem of Algebra.

(b) No, $f = z^2$ has no such factorisation.

(c) No, $f = z - \mathrm{i}$ has no such factorisation.

(d) Yes, group the factors from part (a) together when their c_i are equal.

(e) No, $f = z(z-1)$ has no such factorisation.

Marking: The correct answer for each variant has two Yesses and three Nos. 5 marks per correct Yes, $-3\frac{1}{3}$ marks per incorrect Yes. (This scheme is unfortunate but the Moodle question type I used insists that an answer consisting of all Nos score 0.)

Question 7 Below is a proposition about rings, and a short proof in which the use of the axioms and other properties of rings is not made explicit.

Proposition. Let R be a ring with identity. Suppose that a and b are nonzero elements of R such that $ab = 0$. Then a does not have a multiplicative inverse.

Proof. Suppose that a had a multiplicative inverse. The given equation implies that $a^{-1}ab = 0$. But also $a^{-1}ab = b$, contradicting the fact that $b \neq 0$.

(a) Which property is used to prove $a^{-1}ab = 0$? ____

(b) Which two properties are used to prove $a^{-1}ab = b$? Put them in the order you would use them when simplifying $a^{-1}ab$ to b. First ____, then ____

(c) One more property is needed in this proof, but the notation makes it ambiguous exactly where it is used. Which property is this? ____

Please look at the lecture notes to remind yourself e.g. what "Proposition 3.13" is. [It is the proposition that for all $a \in R$, $0a = 0 = a0$.]

[The following choices were available to fill the blanks:]

- associative law for $+$
- identity law for $+$
- definition of inverse for $+$
- commutative law for $+$
- associative law for $\cdot$
- identity law for $\cdot$
- definition of inverse for $\cdot$
- commutative law for $\cdot$
- cancellation property
- Proposition 3.13

Solution This is another bookwork-esque question, testing ability to recognise use of the axioms. There were two variants of the question; the other also had four blanks and the same choices.

(a) $\boxed{\text{Proposition 3.13}}$ [$2\frac{1}{2}$ marks]

(b) First $\boxed{\text{definition of inverse for } \cdot}$ [$2\frac{1}{2}$ marks], then $\boxed{\text{identity law for } \cdot}$ [$2\frac{1}{2}$ marks]

(c) $\boxed{\text{associative law for } \cdot}$ [$2\frac{1}{2}$ marks]

Question 8 Let $X = \{1,2,3,4\}$. Let $R = \{(1,1),(1,4),(2,2),(3,2),(3,3),(3,4),(4,2),(a,b)\}$, where a and b are elements of X. If R is a transitive relation on X, what is the pair (a,b)?

Solution I taught the students in lecture how to draw relations as directed graphs and what the transitivity property looks like in such a drawing. If R without the pair (a,b) is drawn as a directed graph, it should be easy to spot that there is exactly one pair of arrows which don't have a single arrow "shortcut", so this arrow corresponds to the pair that must be inserted. In this case the two pairs for which transitivity doesn't yet hold are $(1,4)$ and $(4,2)$, so $(a,b) = \boxed{(1,2)}$.

There were no part marks implemented for this question, aside from a mark of 9/10 awarded for a correct answer but with wrong notation for an ordered pair.

This question for reflexive and symmetric, rather than transitive, appeared in my formative weekly quizzes.

Question 9 Prove that the set of intervals $P = \{[2 \cdot 3^k, 6 \cdot 3^k) : k \in \mathbb{Z}\}$ is a partition of $\mathbb{R}_{>0}$, the set of positive real numbers.

Please upload your proof as a single PDF file relating to only this question.

Solution We prove that P satisfies the definition of partition, i.e. that the following three properties hold:

(a) No part of P is $\emptyset$.

(b) Distinct parts of P are disjoint.

(c) The union of all parts of P is $\mathbb{R}_{>0}$.

(a) A general part $[2 \cdot 3^k, 6 \cdot 3^k)$ of P contains $2 \cdot 3^k$, so is not empty.
(b) Let $A_k = [2 \cdot 3^k, 6 \cdot 3^k)$ and $A_l = [2 \cdot 3^l, 6 \cdot 3^l)$ be parts of P with $k \neq l$. Without loss of generality $k < l$, implying $k+1 \leq l$. As

$$6 \cdot 3^k = 2 \cdot 3 \cdot 3^k = 2 \cdot 3^{k+1} \leq 2 \cdot 3^l,$$

every element of A_k is less than $2 \cdot 3^l$ while no element of A_l is. Therefore A_k and A_l are disjoint.
(c) An arbitrary $x \in \mathbb{R}_{>0}$ lies in $[2 \cdot 3^k, 6 \cdot 3^k)$ when $k = \lfloor \log_3(x/2) \rfloor$. □

This is a standard kind of proof. One of the homework questions for submission was to prove something a partition.

The question had variants with other partitions of $\mathbb{R}_{>0}$ following geometric progressions or $\mathbb{R}$ following arithmetic progressions, as well as partitions of a set of sets according to its minimum or maximum, or its intersection with a given subset. In each case the top-level mark scheme was: 4 marks for correctly invoking the definition of a partition, 2 marks for the proof of each of the three properties.

Question 10 Let $G = \{z \in \mathbb{C} : z^3 \text{ is a positive real number}\}$. Prove that G with the operation of multiplication is a subgroup of $\mathbb{C}^\times$.

Please upload your proof as a single PDF file relating to only this question.

Solution By the subgroup test from the course notes, it is enough to show that G is nonempty and that, for all $g, h \in G$, we have $gh^{-1} \in G$.

Because G contains 1, it is nonempty.

Let $g, h \in G$, so g^3 and h^3 are positive real numbers. Then $(gh^{-1})^3 = g^3(h^3)^{-1}$ is the ratio of two positive real numbers, and is therefore a positive real number itself. This shows $gh^{-1} \in G$. □

This question was another standard proof, with precedents in lectures and notes and on the coursework.

Some variants pertained to other subgroups of $\mathbb{C}^\times$; others used cyclic subgroups of $\mathbb{Z}_n$ or $\mathbb{Z}_n^\times$, in the latter case with the generator g being chosen so that g^{-1} was recognisably a power of g. The dominant approaches were to use the group axioms directly (often with an observation that associativity is automatic), or to use a subgroup test, either the one I use above from lectures or another with two checks. The mark scheme allots 4 marks for a correct approach and 2 marks for each of the closure law, identity law, and associative law. For the subgroup test these last $3 \cdot 2$ marks were reassigned to the computations in a hopefully comparable way.

Replacement for Question 1 for 2019/20 candidates Let R be the relation $\{(x, y) \in \mathbb{Z}^2 : 10|xy\}$ on the set $\mathbb{Z}$ of integers. True or false:

(a) R is reflexive.

(b) R is symmetric.

(c) R is transitive.

Solution Variants of this question had different relations, but all of them were amenable to inspection. In this case:

(a) $\boxed{\text{False}}$, e.g. $(1,1) \notin R$ [$3\frac{1}{3}$ marks]

(b) $\boxed{\text{True}}$, because $xy = yx$ [$3\frac{1}{3}$ marks]

(c) $\boxed{\text{False}}$, e.g. $(2,5) \in R$ and $(5,2) \in R$ but $(2,2) \notin R$ [$3\frac{1}{3}$ marks]

These properties of relations were actually taught in the prior module *Numbers, Sets and Functions*; what's new in this module is presenting relations as ordered pairs. In any case, because of that, questions like this one appeared on coursework and in the weekly formative quizzes.

Replacement for Question 2 for 2019/20 candidates Let n be a positive integer such that $\gcd(n, 2^3 \cdot 3 \cdot 5^4) = 2^3 \cdot 5^2$. Suppose the prime factorisation of n is $n = 2^e \cdot 3^f \cdot 5^g \cdots$. What are the possible values that e and g may have?

The possible values of e are:

(a) 3 only

(b) all integers greater than or equal to 3

(c) all nonnegative integers less than or equal to 3

(d) all nonnegative integers

The possible values of g are:

(a) 2 only

(b) all integers greater than or equal to 2

(c) all nonnegative integers less than or equal to 2

(d) all nonnegative integers

Solution The possible values of e are $\boxed{\text{(b) all integers greater than or equal to 3}}$ [5 marks]. The possible values of g are $\boxed{\text{(a) 2 only}}$ [5 marks].

This was a perhaps advanced bookwork-interpretation question on how to compute with integers in prime factorisation. The same question appeared on my 2019/20 exam, so for resitting candidates it was familiar, up to which variant they got; otherwise, it is unseen. Other variants pertained to the lcm or to divisibility relations.

Replacement for Question 10 for 2019/20 candidates Suppose we try to define a function $f : \mathbb{Z}_m \to \mathbb{Z}_5$ by the definition

$$f([a]_m) = \begin{cases} [2^a]_5 & \text{if } a \geq 0 \\ ([2^{-a}]_5)^{-1} & \text{if } a < 0. \end{cases}$$

Whether f is well defined depends on the value of m. What is the smallest positive integer m for which f is well defined?

Solution $\boxed{m = 4}$. 5/10 marks awarded for giving a multiple of the correct answer, so that well-definedness is true but the answer is not the smallest one.

This unseen question was meant to examine understanding of our discussion of well-definedness in modular arithmetic. One of the examples I gave in lecture was, in this question's notation, the observation that $m = 5$ did not produce a well-defined function (though I did not use this setup in lecture). The intended solution was that the student make a table of values of $[2^a]_5$ and notice the period of the function.