Manchester
Metropolitan
University

Mock Examination
Faculty Of Science & Engineering
Department Of Computing And Mathematics
MATHEMATICS UNDERGRADUATE NETWORK
Level 5

Mock examination for

6G5Z0048 Number Theory and Abstract Algebra

Duration : 3 hours

Instructions to students

- You need to answer **FIVE** questions. This must include **TWO** questions from Section A and **TWO** questions from Section B. Your fifth question can then come from any of the remaining questions.
- If you answer more than five questions then you will get the marks from your best five questions, subject to the sectioning requirements above.
- You must show all of your working and explain your reasoning carefully to gain full marks.
- Marks awarded for each question part are shown in square brackets aligned to the right-hand margin.

Permitted materials

- Students are permitted to use their own calculators without mobile communication facilities.

SECTION A – Number Theory questions

1. (a) State precisely the definition of the divisibility relation $a\,|b$ on the integers and use it to prove that for all $a, b, c \in \mathbb{Z}$, if $a\,|b$ and $a\,|c$ then for all $m, n \in \mathbb{Z}$, [6]

$$a\,|(mb + nc).$$

(b) Use the principle of mathematical induction to prove that [5]

$$\forall n \geq 1 \quad 7\,|\left(2^{3n} - 1\right).$$

You should point out in your argument where you make use of the linear combinations result from part (a) above.

(c) Write down the definition of $\gcd(a, b)$. What relation does it have to the set of linear combinations of a and b with integer coefficients? [5]

(d) Prove that for all $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $a|c$ and $b|c$, then $ab|c$. [4]

2. (a) Prove that there are infinitely many prime numbers. State clearly any results about divisibility that you rely on. [10]

(b) Euclid's lemma states that for all primes p and for all $a, b \in \mathbb{Z}$, if $p|ab$ then $p|a$ or $p|b$. Prove this lemma. State any results about divisibility or greatest common divisors that you rely on. [6]

(c) Prove that if an integer of the form $2^m + 1$ is prime then it must be the case that $n = 2^m$ for some positive integer m. [4]

SECTION A – Number Theory questions

3. (a) Carefully state the definition of the congruence relation $a \equiv b \pmod{n}$. How does it relate to the smallest positive remainders left by a and b upon division by n? [3]

   (b) Suppose that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Prove that [10]

$$a + b \equiv a' + b' \pmod{n} \text{ and } ab \equiv a'b' \pmod{n}.$$

   (c) Carefully state the definition of the the Euler totient function ϕ and prove that for any prime p and positive integer n, that ϕ satisfies [7]

$$\phi(p^n) = p^{n-1}(p-1).$$

4. (a) Consider the congruence [7]

$$45x \equiv 15 \pmod{125}.$$

   User relevant result(s) from the theory of congruences to find all the solutions.

   (b) Discuss the role played by the Chinese Remainder Theorem in the solution of a general polynomial congruence of the form [5]

$$f(x) \equiv 0 \pmod{n}.$$

   You do not need to prove the theorem. Give a general outline of how the theorem is used in combination with other results to solve such a congruence.

   (c) Use the Legendre symbol, the law of quadratic reciprocity and other relevant properties to show that there are no integer solutions to the congruence [6]

$$x^2 \equiv 547 \pmod{631}.$$

   (You can use the fact that 547 and 631 are both prime.)

   (d) For how many distinct congruence classes $[a]$ modulo 631 will there be integer solutions x to the congruence [2]

$$x^2 \equiv a \pmod{631}?$$

End of Section A

SECTION B – Abstract Algebra questions

5. (a) Let G be a non-empty set and $*$ a binary operation on G, i.e. [6]

$$\forall\, g_1, g_2 \in G \quad g_1 * g_2 \in G.$$

State the three extra conditions that the pair $(G, *)$ needs to satisfy in order to be called a **group** and explain their meaning. Illustrate each condition with an example drawn from the group $(\mathbb{R}\backslash\{0\}, \times)$.

(b) The Klein Viergruppe can be thought of as the group $V = \{e, r, h, v\}$, consisting of the four symmetries of a non-square rectangle under the operation of composition. They are the identity e, a rotation r and two reflections h and v.

(i) Write down the Cayley table for the group V. Also write down the Cayley table for the group $\mathbb{Z}_4$, the integers under addition modulo 4. [3]

(ii) From the two Cayley tables point out one feature that shows these two groups have a different structure. [2]

(c) State the definition of a **subgroup**. [2]

(d) Let H and K be subgroups of a group G. Prove that the intersection $H \cap K$ must be a subgroup of G. [3]

(e) Let G be a group and let $Z(G)$ denote the subset of G, called the *centre* of G, defined by [4]

$$Z(G) = \{x \in G \;:\; \text{for all } g \in G \; xg = gx\}\,.$$

Prove that $Z(G)$ forms a subgroup of G.

6. (a) Give the definition of the **subgroup generated by an element** of a group, and the definition of the **order of an element** of a group. [3]

(b) Is every finite abelian group cyclic? Prove or disprove. [3]

(c) Is the symmetric group S_3 abelian? Prove or disprove. [3]

(d) Let $\sigma \in S_n$ be a cycle. Prove that σ can be written as the product of at most $n-1$ transpositions. [3]

(e) Prove that the product of two odd permutations is even. [2]

(f) Let G be a group and let $g \in G$. Define a map $\lambda_g : G \to G$ by $\lambda_g(a) = ga$. Prove that λ_g is a permutation of G. [6]

SECTION B – Abstract Algebra questions

7. (a) State Lagrange's theorem on the orders of subgroups of a finite group G. [2]

   (b) Let H be a subgroup of a finite group G.

   (i) State the definition of the **left** and **right cosets** of H in G. [2]

   (ii) Let $g_1, g_2 \in G$. Prove that the left-cosets g_1H and g_2H are either equal or disjoint, i.e. [3]

$$g_1H = g_2H \quad \text{or} \quad g_1H \cap g_2H = \emptyset.$$

   (iii) Prove that all cosets of H in G contain the same number of elements. [3]

   (iv) Then show how parts (ii) and (iii) above can be used to prove Lagrange's theorem. [3]

   (c) The dihedral group D_6 is generated by the pair of elements r, s which are subject to the relations $r^6 = e$, $s^2 = e$ and $sr = r^{-1}s$. Consider the subgroup H of D_6 given by

$$H = \left\{e, r^2, r^4\right\}.$$

   (i) Work out the elements of each left coset of H in D_6. [4]

   (ii) Give an example of a subgroup K of D_6 and an element $x \in D_6$ for which [3]

$$xK \neq Kx.$$

SECTION B – Abstract Algebra questions

8. (a) Give the definition of a **normal subgroup**. [2]

(b) The dihedral group D_6 consists of all products of the two elements r and s, satisfying the relations: [5]

$$r^6 = e,$$
$$s^2 = e,$$
$$srs = r^{-1}.$$

Show that the subgroup $R = \langle r \rangle$ of D_6 generated by r is a normal subgroup of D_6.

(c) Let T be the multiplicative group of non-singular upper triangular 2×2 matrices with entries in $\mathbb{R}$; that is, matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

where $a, b, c \in \mathbb{R}$ and $ac \neq 0$. Let U consist of matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

where $x \in \mathbb{R}$.

(i) Prove that U is a subgroup of T. [2]

(ii) Prove that U is abelian. [2]

(iii) Prove that U is normal in T. [3]

(iv) Prove that the factor group T/U is abelian. [3]

(v) Is T normal in the general linear group $GL_2(\mathbb{R})$? Prove or disprove. [3]

End of Section B

End OF QUESTIONS