University of Bath

**DEPARTMENT OF MATHEMATICAL SCIENCES**

**MA10209**

**Algebra 1A**

**Monday 11th January 2016**
**13:00 – 15:00**
**2 hours**

**Answer all questions in Section A and TWO questions from Section B.**

**No calculators may be brought in and used.**

PLEASE FILL IN THE DETAILS ON THE FRONT OF YOUR ANSWER BOOK/COVER AND SIGN IN THE SECTION ON THE RIGHT OF YOUR ANSWER BOOK/COVER, PEEL AWAY ADHESIVE STRIP AND SEAL.

TAKE CARE TO ENTER THE CORRECT CANDIDATE NUMBER AS DETAILED ON YOUR DESK LABEL.

DO NOT TURN OVER YOUR QUESTION PAPER UNTIL INSTRUCTED TO BY THE CHIEF INVIGILATOR.

## Section A

1. In each case, write T or F as the statement is true or false. No justification is required.

   (a) Suppose that $X$ and $Y$ are finite sets and that there is a bijection $\theta : P(X) \to P(Y)$ between their power sets. It follows that there is a bijection between $X$ and $Y$.

   (b) There is a bijection between $\mathbb{Z}$ and $\mathbb{Q}$.

   (c) We have an injective map $f : A \longrightarrow B$ and a surjective map $g : B \longrightarrow C$. It follows that their composition $g \circ f$ is bijective.

   (d) There are exactly two bijections $\theta$ from $\{1, 2, 3\}$ to $\{1, 2, 3\}$ such that $\theta \circ \theta \circ \theta$ is the identity map.

   (e) Suppose that $p$ is a prime number and both $m$ and $n$ are integers. If $p$ divides $mn$ then $p$ divides $m$ and $p$ divides $n$.

   (f) The additive inverse of 1 is multiplicatively invertible in $\mathbb{Z}_m$ for all integers $m \geq 2$.

   (g) Suppose that $G$ is a group written multiplicatively with identity element $1_G$, then the set $\{h \mid h \in G, h^2 = 1_G\}$ is a subgroup of $G$.

   (h) Let $\varphi$ be Euler's phi-function. If $m$ and $n$ are positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.

   (i) There are exactly 8 multiplicatively invertible elements of $\mathbb{Z}_{20}$.

   (j) $3^{90} \equiv 1 \bmod 91$.

[10]

2. (a) Define the term *injective map*. [2]

   (b) Define the term *surjective map*. [2]

   (c) Suppose that $f : A \to B$ is an injective map and that $A$ is not the empty set. Prove that there is a map $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on $A$. [2]

   (d) How many injective maps are there from $\{1, 2, 3\}$ to $\{1, 2, 3, 4, 5\}$? No justification is required. [2]

   (e) How many surjective maps are there from $\{1, 2, 3\}$ to $\{1, 2\}$? No justifiction is required. [2]

3. (a) Give an example of an integral domain which is not a field. [2]

(b) Give an example of a ring which is not an integral domain. [2]

(c) Give an example of a ring $R$ with the property that $x + x + x = 0_R$ for all $x \in R$, but $R$ is not a field. [2]

(d) Let $\mathbb{G} = \{x + iy \mid x, y \in \mathbb{Z}\}$ be the ring of Gaussian integers. Show that 5 can be factorized as $5 = uv$ here neither $u$ nor $v$ is a unit of $\mathbb{G}$. [2]

(e) Give an example of a ring which has infinitely many units. [2]

4. Let $I_5 = \{1, 2, 3, 4, 5\}$ and let $G = S_5 = \{f \mid f : I_5 \longrightarrow I_5, f \text{ is bijective}\}$, a group under composition of maps. We use the cycle notation to describe elements of $G$.

(a) How many elements of $G$ have order 2? Explain your reasoning. [2]

(b) Give an example of two elements of $G$ which commute and have orders 2 and 3. [2]

(c) Give an example of two elements of $G$ which commute and have orders 2 and 4. [2]

(d) Give examples of two subgroups $H_1$ and $H_2$ of $G$ such that $|H_1| = |H_2| = 6$ and $|H_1 \cap H_2| = 1$. [2]

(e) Give examples of two subgroups $K_1$ and $K_2$ of $G$ such that $|K_1| = |K_2|$ but $K_1$ and $K_2$ are not isomorphic groups. [2]

## Section B

5. (a) Suppose that $m, n \in \mathbb{Z}$ are integers, and at least one of them is not 0. Prove that the *greatest common divisor* of $m$ and $n$ is the smallest positive integer which can be written as $\lambda m + \mu n$. [2]

(b) Find integers $\lambda$ and $\mu$ such that $23\lambda + 29\mu = 1$. [3]

(c) Suppose that $m_1, m_2, \ldots, m_t$ are positive integers and $a_1, a_2, \ldots, a_t$ are integers. What condition on $m_1, m_2, \ldots, m_t$ is necessary to guarantee that there is an integer $x$ such that $x \equiv a_i \bmod m_i$ for all integers $i$ in the range $1 \leq i \leq t$. [2]

(d) Prove that there are 1000 consecutive integers, each of which is divisible by the square of a prime number. [3]

6. (a) Suppose that $\alpha : G \longrightarrow H$ where $G$ and $H$ are groups. What does it mean to say that $\alpha$ is a homomorphism? [1]

(b) Let $G$ be a group written multiplicatively, and the map $\theta : G \to G$ be defined by $\theta(g) = g^{-1}$ for each $g \in G$. Suppose that $\theta$ is a homomorphism. Prove that $G$ is an abelian group. [3]

(c) Suppose that $G$ is a finite group written multiplicatively, and $g \in G$. What is the order $o(g)$ of $g$, and how is this related to $|G|$? [3]

(d) Suppose that $\beta : G \to H$ is a homomorphism of groups. Suppose that $|G|$ and $|H|$ are coprime integers. Prove that $\beta(x) = 1_H$ for all $x \in G$. [3]

7. (a) Suppose that $S$ is a set with power set $P(S)$. Prove that $S$ and $P(S)$ are not in bijective correspondence. [5]

(b) Suppose that $T$ is a set. Let $F(T) = \{X \mid X \subseteq T, X \text{ is finite}\}$. Prove that $T$ is uncountable if, and only if, $F(T)$ is uncountable. [5]