

DEGREE EXAMINATION

MA2004 Sets and Algebraic Structures

()

Only calculators approved by the Department of Mathematical Sciences may be used in this examination. Calculator memories must be clear at the start of the examination.

Marks may be deducted for answers that do not show clearly how the solution is reached.

Answer FOUR of the five questions. All questions carry equal weight. Use complete grammatical sentences in the English language.

1. (a) If X and Y are sets, what does it mean to say that a function $f: X \rightarrow Y$ is *injective*? What does it mean to say that $f: X \rightarrow Y$ is *surjective*? What does it mean to say that $f: X \rightarrow Y$ is *bijective*?

For the remainder of the question, set $X = \{a, b\}$ and $Y = \{1, 2, 3, 4, 5\}$.

- (b) How many functions are there from X to Y ?

[Do not try to write them all down]

- (c) How many functions are there from Y to X ?

- (d) How many injective functions are there from X to Y ?

[You may find it easier to count how many are not injective and subtract]

- (e) How many surjective functions are there from Y to X ?

- (f) How many bijective functions are there from Y to Y ?

2. (a) What is meant by a *relation* R on a set S ?

- (b) If R is a relation, what does it mean to say that R is an *equivalence relation*?

(c) Consider the relation \sim on the set \mathbb{Z} of integers given by $m \sim n$ if and only if $m - n$ is divisible by 3. Prove that \sim is an equivalence relation, and describe the equivalence classes. How many equivalence classes are there?

(d) Show that if $m \sim n$ and $s \sim t$ then $(m + s) \sim (n + t)$, so that addition gives a well defined operation on equivalence classes. Draw up an addition table for equivalence classes.

3. (a) Define the *greatest common divisor* of two positive integers a and b .
- (b) Using the Euclidean algorithm, find $d = \gcd(2159, 3077)$, and find integers s and t such that $d = 2159s + 3077t$. You should give clean, readable working, and you should remember to check your answer.
- (c) Does the congruence class $[2159]$ have a multiplicative inverse modulo 3077? Explain.
- (d) Find a multiplicative inverse for $[8]$ modulo 29.

4. (a) Write the following permutation of $\{1, 2, 3, 4, 5, 6, 7, 8\}$ in cycle notation, and find its order.

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

Is this an even or an odd permutation?

(b) State Lagrange's theorem about the relationship between the order of a finite group and the order of a subgroup.

(c) State Fermat's little theorem, and use it to find the remainder when 2^{147} is divided by 13.

5. (a) Give the definition of a commutative ring. You may use the term "abelian group" in your definition without defining that term.

(b) Give the definition of a field.

(c) In each of the following cases, say whether the given object is a commutative ring, and whether it is a field. In case the given object is not a commutative ring, say what part of the definition fails.

[In each case, the operations of addition and multiplication are the usual ones for the objects in question]

(i) The complex numbers \mathbb{C} .

(ii) The real numbers \mathbb{R} .

(iii) The rational numbers \mathbb{Q} .

(iv) The integers \mathbb{Z} .

(v) The positive integers $\{0, 1, 2, \dots\}$.

(vi) The 2×2 matrices with real entries.

(vii) The integers modulo p , with p a prime number.

(viii) The integers modulo n , with $n > 1$ a composite number (i.e., *not* a prime number).