PRIFYSGOL ABERYSTWYTH UNIVERSITY

ADRAN MATHEMATEG / DEPARTMENT OF MATHEMATICS

ARHOLIADAU SEMESTER 1 / SEMESTER 1 EXAMINATIONS

IONAWR / JANUARY 2026

MA20310 – Introduction to Abstract Algebra

The questions on this paper are written in English.

Amser a ganiateir - 2 awr

- Gellir rhoi cynnig ar bob cwestiwn.
- Rhoddir mwy o ystyriaeth i berfformiad yn Rhan B wrth bennu marc dosbarth cyntaf.
- Cyfrifianellau Casio FX-83 neu FX-85 YN UNIG a ganiateir.
- Mae modd i fyfyrwyr gyflwyno atebion i'r papur hwn naill ai yn y Gymraeg neu'r Saesneg.

Time allowed - 2 hours

- All questions may be attempted.
- Performance in Section B will be given greater consideration in assigning a first class mark.
- Casio FX-83 or FX-85 calculators ONLY may be used.
- Students may submit answers to this paper in either Welsh or English.

© 2026 Aberystwyth University

Section A

1. Let g be the positive greatest common divisor of 1287 and 884 in $\mathbb{Z}$.

(a) Use the Euclidean Algorithm to evaluate g. [4 marks]

(b) Find **one** pair $(\lambda, \mu) \in \mathbb{Z}^2$ such that $g = 1287\lambda + 884\mu$. [3 marks]

(c) Find **every** pair $(x, y) \in \mathbb{Z}^2$ that satisfies $1287x + 884y = 52$. [3 marks]

2. For integers a and b, recall that we write $a|b$ if a divides b in $\mathbb{Z}$.

(a) State the definition of a greatest common divisor of two integers. [3 marks]

(b) Prove that if $a|b$ and $b \neq 0$ then $|a| \leq |b|$. [3 marks]

(c) Hence, prove that if c is a common divisor of a and b then c is less than or equal to the positive greatest common divisor of a and b. [3 marks]

3. Find the principal residues of

(a) $1234 \pmod{11}$, (c) $628^{3517} \pmod{19}$,

(b) $1284^{2017} \pmod{64}$, (d) $8285^{8005} \pmod{82}$.

[11 marks]

4. (a) Write down the multiplication table for $\mathbb{Z}_6$. [4 marks]

(b) List the units of $\mathbb{Z}_6$. [2 marks]

(c) Using the table, or otherwise, solve the following equations in $\mathbb{Z}_6$

(i) $\overline{5}\, y = \overline{2}$;

(ii) $\overline{3}\, y = \overline{3}$.

[4 marks]

5. (a) State the Rational Root Test Theorem. [2 marks]

(b) Use the Rational Root Test to find all rational roots of the following polynomial: $f = 3x^5 + 11x^4 + 5x^3 + 9x^2 + 2x - 2$. [5 marks]

6. Is the polynomial $g = 4x^2 - 4x - 2$ irreducible in:

(a) $\mathbb{C}[x]$; (b) $\mathbb{R}[x]$; (c) $\mathbb{Q}[x]$; (d) $\mathbb{Z}[x]$?

Justify your answers. Refer to any results from the module you use (you do not need to prove the results). [8 marks]

7. Consider the polynomials

$$a = 12x^3 - 53x^2 - 42x + 48 \text{ and } b = 3x^2 - 17x + 10.$$

(a) Find $\gcd(a, b)$, i.e. the monic greatest common divisor of a and b, in $\mathbb{Q}[x]$.

(b) Find $\lambda, \mu \in \mathbb{Q}[x]$ such that $\gcd(a, b) = \lambda a + \mu b$.

[6 marks]

8. Let $\sim$ be the binary relation on $\mathbb{R}[x]$ defined by

$$f \sim g \iff (x^2 + 1) | (f - g) \text{ in } \mathbb{R}[x].$$

(a) Show that $\sim$ is an equivalence relation. [6 marks]

(b) Find $a, b \in \mathbb{R}[x]$ such that $[x^6 + 2] = [ax + b]$, where $[f]$ denotes the equivalence class of $f \in \mathbb{R}[x]$ with respect to $\sim$. [3 marks]

Section B

9. Define binary operations $\vee$ and $\wedge$ on $\mathcal{P}(\mathbb{N})$ (the family of all subsets of $\mathbb{N}$) by

$$A \vee B = A \cup B \qquad \text{and} \qquad A \wedge B = A \cap B \qquad \text{for all } A, B \in \mathcal{P}(\mathbb{N}).$$

With reference to the axioms on page 5, show that

(a) $\vee$ satisfies axiom A3; [2 marks]

(b) $\wedge$ satisfies axiom M3; [2 marks]

(c) $\vee$ does not satisfy axiom A4; and [3 marks]

(d) $\wedge$ does not satisfy axiom M4. [3 marks]

You may assume, without proof, basic properties of unions and intersections.

10. Let $f \in \mathbb{Q}[x]$.

(a) State what it means for f to be irreducible in $\mathbb{Q}[x]$. [2 marks]

(b) State what it means for f to be prime in $\mathbb{Q}[x]$. [2 marks]

(c) Prove that if $f, g \in \mathbb{Q}[x]$ such that f is irreducible and $f \not| g$ (does not divide) in $\mathbb{Q}[x]$ then the monic greatest common divisor of f and g, $\gcd(f, g)$, is 1. [4 marks]

(d) Hence prove that if f is irreducible in $\mathbb{Q}[x]$ then f is prime in $\mathbb{Q}[x]$. [4 marks]

You may assume, without proof, that Bézout's Identity holds in $\mathbb{Q}[x]$.

11. Find all integer solutions to the following system of simultaneous linear congruences:

$$6x \overset{8}{\equiv} 4, \; 5x \overset{13}{\equiv} 3.$$

[12 marks]

12. Let $\phi : R \to S$ be a mapping from a ring R into a ring S.

(a) State the properties that ϕ must satisfy in order for it be (i) a homomorphism; and (ii) an isomorphism. [3 marks]

From now on assume that ϕ is a homomorphism.

(b) State the definition of the kernel of ϕ, $\ker \phi$. [2 marks]

(c) Prove that $\ker \phi$ is an ideal in R. [5 marks]

(d) Show that $\ker \phi = \mathbb{Z}_8$ for any homomorphism $\phi : \mathbb{Z}_8 \to \mathbb{Z}_3$. [6 marks]

Information

Let S be a non-empty set and $\oplus$ and $\otimes$ be binary operations on S. Listed below are some axioms that may or may not hold in the algebraic system $(S, \oplus, \otimes)$.

Axioms of Addition

A1. $a \oplus b = b \oplus a$ for all $a, b \in S$. [commutativity]

A2. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ for all $a, b, c \in S$. [associativity]

A3. There exists an element $0_S \in S$ such that $0_S \oplus a = a \oplus 0_S = a$ for all $a \in S$. [the existence of an additive identity]

A4. For each $a \in S$ there exists an element $-a \in S$ such that $a \oplus (-a) = (-a) \oplus a = 0_S$. [the existence of an additive inverse]

Axioms of Multiplication

M1. $a \otimes b = b \otimes a$ for all $a, b \in S$. [commutativity]

M2. $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ for all $a, b, c \in S$. [associativity]

M3. There exists an element $1_S \in S$ such that $1_S \otimes a = a \otimes 1_S = a$ for all $a \in S$. [the existence of a multiplicative identity]

M4. For each $a \in S$ such that $a \neq 0_S$ there exists an element $a^{-1} \in S$ such that $a \otimes a^{-1} = a^{-1} \otimes a = 1_S$. [the existence of a multiplicative inverse]

Axioms of Distributivity

D1. For all $a, b, c \in S$, $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

D2. For all $a, b, c \in S$, $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$.

Definition

If the ticked axioms hold in $(S, \oplus, \otimes)$							then $(S, \oplus, \otimes)$ is called a
A1 to A4	M2	D1	D2	M1	M3	M4	
✓	✓	✓	✓	✓	✓	✓	field
✓	✓	✓	✓				ring
✓	✓	✓	✓	✓			commutative ring
✓	✓	✓	✓		✓		ring with identity (or unital ring)