

4.1 Abstract algebra and number theory

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

KEY WORDS homomorphism • field

Objective

Use groups, subgroups, homomorphisms and quotient structures; Distinguish rings, integral domains and fields; Apply divisibility, congruences and elementary number theory.

Original public practice. Marking guidance is authored locally. Use the topic reference for prerequisites and full theorem statements.

1 Key knowledge and worked examples

homomorphism : A map preserving the relevant operation.

field : A commutative ring where each nonzero element has an inverse.

A group needs closure, associativity, identity and inverses. Commutativity is an additional condition.

Modulo 8, 3 has inverse 3 because $3 \cdot 3 \equiv 9 \equiv 1$. But 2 has no inverse because $\gcd(2,8)=2$. Modulo a prime, every nonzero residue has an inverse; this gives a finite field.

Same addition rule; different invertibility

Ring	Multiplicative units	Check
mod 5	1, 2, 3, 4	every nonzero residue
mod 6	1, 5	2 times 3 is zero

2 Practice

2.1 The integers under addition form: [1]

- A a group
- B a field under integer division
- C a set without identity

2.2 Which has an inverse modulo 9? [1]

- A 3
- B 6
- C 2

2.3 Compare the additive groups and multiplicative structures of $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$. List all multiplicative units in each. Explain why removing zero does not always leave a multiplicative group. [4]

Original course illustration; its values belong to the worked example, not the later practice.

3 Exam-style questions

3.1 The reduction map $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ is given by $\phi(n) = [n]$. Determine its kernel, image and quotient. Solve $2x \equiv 2 \pmod{6}$ completely and explain why cancelling 2 modulo 6 fails. [4]

Solutions

2.1 A. Addition has identity 0 and inverse $-a$. B fails because integer division is not closed, for example $1/2$; C fails because zero is the additive identity.

2.2 C. $\gcd(2,9)=1$; its inverse is 5. Three and six share a factor three with nine; neither product can be one modulo nine. Two times five has remainder one.

2.3 Both whole residue sets are additive groups: closure, associativity and identity come from integer addition, and $-a$ is an additive inverse. A multiplicative residue is a unit precisely when its greatest common divisor with the modulus is one. The units modulo five are 1, 2, 3, 4; modulo six they are 1, 5. Modulo six, $2 \cdot 3 = 0$ although both factors are nonzero. The nonzero set is not even closed under multiplication. Modulo five every nonzero residue has an inverse; this ring is a field. A ring, its additive group and its group of units are different structures.

3.1 The map preserves addition and multiplication. Its kernel is $6\mathbb{Z}$ and its image is all six residues. The quotient identifies integers with the same remainder, so $\mathbb{Z}/\ker\phi \cong \mathbb{Z}/6\mathbb{Z}$. The congruence means $6 \mid 2(x-1)$, equivalently $3 \mid x-1$. Hence $x \equiv 1 \pmod{3}$, giving residues 1 and 4 modulo six. Both substitute correctly. Cancelling 2 while retaining modulus six would discard 4; 2 has no multiplicative inverse there.

Local four-mark guidance for each written task: choose and justify the method; carry through the reasoning; give every requested result; check the relevant restriction, hypothesis or boundary case. These are classroom marks, not GRE scoring.