

## A.2 · Abstract algebra and number theory

Original classroom teaching; not an official form or score predictor

# 1. Scope and prerequisites

## Scope and prerequisites

Undergraduate GRE preparation. Local objectives within the reviewed ETS scope; this is original teaching, not an official test or score predictor.

## 2. Scope and prerequisites

### Scope and prerequisites

Prerequisites: Integer arithmetic, sets, functions and proof by counterexample.

### 3. Scope and prerequisites

#### Scope and prerequisites

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

## 4. Scope and prerequisites

### Scope and prerequisites

homomorphism : A map preserving the relevant operation.

## 5. Scope and prerequisites

### Scope and prerequisites

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

## 6. Choose and justify a method

### Choose and justify a method

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

## 7. Choose and justify a method

### Choose and justify a method

A homomorphism preserves the operation. Its kernel is a normal subgroup and identifies elements mapping to the identity.

## 8. Choose and justify a method

Choose and justify a method

A field permits division by every nonzero element. Integers form a ring but not a field.

## 9. Choose and justify a method

### Choose and justify a method

Work with congruences modulo  $n$ . A residue  $a$  has a multiplicative inverse exactly when  $\gcd(a,n)=1$ .

## 10. Worked reasoning

### Worked reasoning

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

## Figure 11: Worked reasoning

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     |

Check the labelled values and conditions.

## 12. Conditions and counterexamples

### Conditions and counterexamples

Do not cancel a factor in a modular equation without checking that it is invertible.

## 13. Try independently

### Try independently

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.

## 14. Reasoning and check

### Reasoning and check

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.

## 15. Reasoning and check

### Reasoning and check

A ring, its additive group and its group of units are different structures.

## 16. Try independently

### Try independently

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.

## 17. Reasoning and check

### Reasoning and check

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.

## Check yourself

Reconstruct the method without looking back

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.