UNIVERSITY OF ABERDEEN **SESSION 2005-06**

DEGREE EXAMINATION
MX4033 Number Theory
Monday 16 January 2006 (3 pm to 5 pm)

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 three questions.

1. **(a)** Let p be an odd prime number, a an integer not divisible by p.

Define the *Legendre symbol* $\left(\frac{a}{p}\right)$.

(b) Let p be an odd prime. Show that exactly half of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are quadratic residues modulo p.

(c) State the quadratic reciprocity law.

(d) Determine whether 13 is a quadratic residue modulo 227.

(e) Evaluate the expression

$$\sum_{m=1}^{p-1} \left(\frac{am+b}{p}\right) ,$$

where p is an odd prime and where a, b are integers such that $(a,p)=1$ and $p|b$.

2. Let $K=\mathbb{Q}(i,\sqrt{2})$, where $i^2=-1$.

(a) Define the notion of *algebraic integer* and determine whether $i+\sqrt{2}$ is an algebraic integer in K.

(b) Prove that $K=\mathbb{Q}[i+\sqrt{2}]$.

(c) Determine the minimal polynomials of $i+\sqrt{2}$ and of $i\sqrt{2}$.

(d) Determine a $\mathbb{Q}$-basis of K.

(e) Prove that 3 is not irreducible in the ring of algebraic integers in K.

3. Consider the number field $K = \mathbb{Q}[\sqrt{-17}]$.

(a) Show that the ring of integers of K is equal to $\mathbb{Z}[\sqrt{-17}]$.

(b) Show that $18 = 2 \cdot 3 \cdot 3 = (1 + \sqrt{-17})(1 - \sqrt{-17})$ are two inequivalent factorisations of 18 as product of irreducible numbers in $\mathbb{Z}[\sqrt{-17}]$.

(c) Show that there is no element α in $\mathbb{Z}[\sqrt{-17}]$ satisfying $18 = \alpha^2$ but that the ideal

$$I = \langle 6, 3 + 3\sqrt{-17} \rangle$$

in $\mathbb{Z}[\sqrt{-17}]$ satisfies the equality $\langle 18 \rangle = I^2$ of ideals in $\mathbb{Z}[\sqrt{-17}]$.

(d) Determine whether I is a prime ideal.

(e) Determine the prime factorisation of the ideal $\langle 18 \rangle$ in $\mathbb{Z}[\sqrt{-17}]$.

4. Let ζ be a primitive 6-th root of unity in $\mathbb{C}$ and set $\omega = \zeta i$, where $i^2 = -1$.

(a) Determine the minimal polynomial of ζ.

(b) Find a square–free integer m such that $\mathbb{Q}[\zeta] = \mathbb{Q}[\sqrt{m}]$.

(c) Show that ω is a primitive 12-th root of unity and determine the minimal polynomial g of ω.

(d) Determine all roots of the minimal polynomial g of ω.

(e) Find all subfields of $\mathbb{Q}[\zeta, i]$.