UNIVERSITY OF ABERDEEN **SESSION 2006-07**

DEGREE EXAMINATION

MX4545 Number Theory

Friday 25 May 2007 (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 in complete grammatical sentences. All questions carry equal weight.

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

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

(b) Determine all integers a such that $1 \leq a \leq 16$ and such that a is a quadratic residue modulo 17.

(c) State the quadratic reciprocity law.

(d) Determine whether 41 is a quadratic residue modulo 283.

(e) Determine which of the numbers $2^{39} + 1$ and $2^{39} - 1$ is divisible by 79.

Hint: consider $\left(\dfrac{2}{79}\right)$.

2. Let $K = \mathbb{Q}(i, \sqrt{3})$, where $i^2 = -1$. Set $\alpha = \sqrt{3} + 2i$.

(a) Define the notion of *algebraic integer* and determine whether α is an algebraic integer in K.

(b) Prove that $K = \mathbb{Q}(\alpha)$.

(c) Determine the minimal polynomials of α and of $\frac{\alpha}{7}$.

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

(e) Prove that 7 is not irreducible in the ring of algebraic integers in K.

3. Consider the number field $K = \mathbb{Q}(\sqrt{-29})$.

(a) Determine the ring of algebraic integers in K.

(b) Show that $30 = 2 \cdot 3 \cdot 5 = (1 + \sqrt{-29})(1 - \sqrt{-29})$ are two inequivalent factorisations of 30 as product of irreducible numbers in $\mathbb{Z}[\sqrt{-29}]$.

(c) Show that there is no element α in $\mathbb{Z}[\sqrt{-29}]$ satisfying $8 = \alpha^2$ but that the ideal

$$I = \langle 4, 2 + 2\sqrt{-29} \rangle$$

in $\mathbb{Z}[\sqrt{-29}]$ satisfies the equality $\langle 8 \rangle = I^2$ of ideals in $\mathbb{Z}[\sqrt{-29}]$.

(d) Determine whether I is a prime ideal.

(e) Determine the prime factorisation of the ideal $\langle 6 \rangle$ in $\mathbb{Z}[\sqrt{-29}]$.

4. Let ζ be a primitive 10-th root of unity in $\mathbb{C}$.

(a) Determine the minimal polynomials of ζ and of $-\zeta$ over $\mathbb{Q}$.

(b) Show that $1 + 2\zeta^2 + 2\zeta^{-2}$ is equal to one of $\pm\sqrt{5}$.

(c) Show that $\mathbb{Q}(\zeta)$ does not contain i, where $i^2 = -1$.

(d) Decide whether the ideal $\langle 2 \rangle$ generated by 2 in $\mathbb{Z}[\zeta]$ is a prime ideal.

(e) For the following five numbers, decide whether they are algebraic integers in $\mathbb{Q}(\zeta)$ and which of them is an invertible element in the ring of algebraic integers of $\mathbb{Q}(\zeta)$:

$$1 - \sqrt{5}, \quad 2 + \sqrt{5}, \quad 1 - \zeta, \quad \frac{1 + \sqrt{5}}{2}, \quad \frac{1 + \zeta}{2}$$