Imperial College London

UNIVERSITY OF LONDON

BSc and MSci EXAMINATIONS (MATHEMATICS)

May-June 2006

This paper is also taken for the relevant examination for the Associateship.

M3P15/M4P15

Algebraic Number Theory

Date: Thursday, 1st June 2006 Time: 2 pm – 4 pm

Credit will be given for all questions attempted but extra credit will be given for complete or nearly complete answers.

Calculators may not be used.

1. (i) Give the definitions of

   (a) an algebraic number,

   (b) an algebraic integer,

   (c) a number field.

   (ii) If K is a number field and $\alpha \in K$, then define the trace $Tr_{K/\mathbb{Q}}(\alpha)$ and the norm $N_{K/\mathbb{Q}}(\alpha)$ of α.

   (iii) Find (without proof) a number field K and an algebraic integer $\alpha \in K$ such that $Tr_{K/\mathbb{Q}}(\alpha) = 2$ and $N_{K/\mathbb{Q}}(\alpha) = -1$.

   (iv) If K is a number field and $\alpha \in K$ is such that $Tr_{K/\mathbb{Q}}(\alpha) = 2$ and $N_{K/\mathbb{Q}}(\alpha) = -1$, is α necessarily an algebraic integer? Give either a proof or a counterexample. (*You may assume any results from the course that you need.*)

2. Let d be a squarefree integer not equal to 1. Determine, with proof, the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$.

   You may assume that an algebraic number is an algebraic integer if and only if its minimal polynomial has integral coefficients.

3. Prove that the class group of $\mathbb{Q}(\sqrt{-17})$ is cyclic of order 4.

   You may assume any theorems from the course that you need. In particular, you may assume that every ideal class contains an ideal of norm at most 5. Hint: *are there principal ideals of norm 18?*

4. Show that the equation $y^3 = x^2 + 5$ has no solutions with x, $y \in \mathbb{Z}$.
   You may assume that the class number of $\mathbb{Q}(\sqrt{-5})$ *is* 2, *and that the ring of integers in* $\mathbb{Q}(\sqrt{-5})$ *is* $\mathbb{Z}[\sqrt{-5}]$.

5. Let K be a number field, and R its ring of integers.

   (i) Prove that if I is a nonzero ideal of R, then there exists a nonzero ideal J of R such that IJ is principal.

   You may assume that for any proper ideal A *of* R *there exists a* $\gamma \in K$, $\gamma \notin R$ *such that* $\gamma A \subseteq R$, *and that if* $\gamma \in K$ *is such that* $\gamma A \subseteq A$, *then in fact* $\gamma \in R$.

   (ii) Deduce from (i) that if A, B are nonzero ideals of R, then $A|B$ if and only if $B \subseteq A$.