UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Wednesday, 8 June, 2011 1:30 pm to 4:30 pm

PAPER 25

ALGEBRAIC NUMBER THEORY

Attempt no more than ***THREE*** *questions.*

There are ***FOUR*** *questions in total.*

The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

SPECIAL REQUIREMENTS
None

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

ζ_n denotes a primitive n-th root of unity.

1

(i) State and prove the Chinese Remainder Theorem for ideals in the ring of integers of a number field.

(ii) Let K be a number field. Explain what is meant by the *norm* $N(\mathfrak{a})$ of a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$. Prove that it is finite and satisfies

$$|N_{K/\mathbb{Q}}(\alpha)| = N((\alpha)), \qquad N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}) \qquad \text{and} \qquad N(\mathfrak{a}\mathcal{O}_L) = N(\mathfrak{a})^{[L:K]},$$

for $\alpha \in \mathcal{O}_K$, $\mathfrak{b}$ a non-zero ideal of $\mathcal{O}_K$ and L/K a field extension of finite degree.

(iii) Define the terms *residue degree* and *ramification degree* and prove the formula

$$\sum_{i=1}^{m} e_i f_i = [L:K],$$

when a prime $\mathfrak{p}$ of K splits into primes $\mathfrak{q}_1 \dots \mathfrak{q}_m$ of L with residue and ramification degrees $f_1, \dots f_m$ and $e_1, \dots e_m$, respectively. For $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-5})$, give an example of a prime for which $e = f = 1$ and an example for which $e = 2, f = 1$.

2

Let $F = \mathbb{Q}(\zeta_5, \sqrt[5]{75})$, a field of degree 20 over $\mathbb{Q}$. Determine the decomposition and inertia groups in $\mathrm{Gal}(F/\mathbb{Q})$ for primes in F above $3, 5, 11$ and 89. Find the number of primes above $3, 5, 11$ and 89 in the subfield $\mathbb{Q}(\sqrt[5]{75})$, together with their ramification and residue degrees over $\mathbb{Q}$.

(*You do not need to describe the primes explicitly, nor to give explicit generators for the decomposition and inertia groups.)*

3

(i) Define the Artin L-function $L(\rho, s)$ for a representation of the Galois group of an extension of number fields. Using the fact that Artin L-functions of 1-dimensional representations have an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$ in the case of the trivial representation, prove that $L(\rho, s)$ has an analytic continuation to $s = 1$ whenever ρ is a non-trivial irreducible representation.

(Basic properties of Artin L-functions, as well as Artin's or Brauer's Induction Theorem, may be used without proof, provided that they are clearly stated.)

(ii) Let $F = \mathbb{Q}(\zeta_p)$ for some prime number p, and let ρ be a non-trivial 1-dimensional representation of $\mathrm{Gal}(F/\mathbb{Q})$. Show that the Artin L-function of ρ coincides with the Dirichlet L-function of a suitable Dirichlet character.

(iii) Let L/K be a Galois extension of number fields whose Galois group is cyclic of order 3. By considering the Dedekind ζ-functions of L and K, prove that infinitely many primes of K do not split in L.

(You may assume that only finitely many primes ramify in L/K.)

4

(i) State the Main Theorem of Class Field Theory, and use it to prove the Kronecker–Weber theorem.

(ii) Let $\mathfrak{m} = (5 + 3\zeta_3)$ be a modulus of $K = \mathbb{Q}(\zeta_3)$. Show that the Galois group $\mathrm{Gal}(F/K)$ of its ray class field F is cyclic of order 3. Deduce that F is of the form

$$F = K\left(\sqrt[3]{\zeta_3^k \cdot (5 + 3\zeta_3)}\right).$$

By considering the Frobenius element at $(4 + 3\zeta_3)$, or otherwise, determine F.

(You may assume that the ideal class group of $\mathbb{Q}(\zeta_3)$ is trivial, and that its group of units is generated by ζ_6.)

END OF PAPER