UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Monday, 4 June, 2018 9:00 am to 12:00 pm

PAPER 123

ALGEBRAIC NUMBER THEORY

*Attempt no more than **FOUR** questions.*

*There are **FIVE** questions in total.*

You may use any facts about the Galois theory of cubics, for example that the discriminant of $T^3 + aT + b$ is $\Delta = -4a^3 - 27b^2$, and that the splitting field of $T^3 + aT + b$ contains $\sqrt{\Delta}$.

You may use any facts about polynomials over local fields and their roots, provided you clearly state what you use.

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.

1

Let K be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_K$ and residue field k_K. Write $y \mapsto \overline{y}$ for the reduction map from $\mathcal{O}_K$ to k_K.

(a) State a version of Hensel's lemma for K. Then show that, for any finite extension ℓ/k_K, there is an unramified extension L/K with residue field isomorphic to ℓ over k_K. Show that this L is unique up to isomorphism over K, using your version of Hensel's lemma.

(b) Define the Teichmüller lift map $[-] : k_K \to \mathcal{O}_K$ and state and prove a set of properties of $[-]$ that defines it uniquely (you should prove that the properties you state do define it uniquely).

Let $x = x_0 \in k_K$ and define x_n for $n \geqslant 1$ by $x_n^p = x_{n-1}$. Let $y_n \in \mathcal{O}_K$ satisfy $\overline{y}_n = x_n$. Prove that the sequence $(y_n^{p^n})_{n \geqslant 1}$ converges to $[x]$.

2

(a) Let L/K be a finite extension of number fields and let $\mathfrak{p}$ be a prime of K, with corresponding completion $K_{\mathfrak{p}}$. Let $\overline{K}_{\mathfrak{p}}$ be a (fixed) algebraic closure of $K_{\mathfrak{p}}$. Show that there is a natural bijection between the primes of L above $\mathfrak{p}$ and the $Gal(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$-orbits of the set of K-embeddings of L into $\overline{K}_{\mathfrak{p}}$. [You may assume the equivalence between primes and finite places]. Deduce that, if $L = K(\alpha)$ and $f(T) \in K[T]$ is the minimal polynomial of α, then there is a natural bijection between the set of primes in L above $\mathfrak{p}$ and the irreducible factors of $f(T)$ in $K_{\mathfrak{p}}[T]$.

(b) Let $M = \mathbb{Q}(\beta)$ where β is a root of $g(T) = T^5 + 6T^3 + 252T^2 + 126$. Show that $[M : \mathbb{Q}] = 5$ and compute the number of primes of M above 3 and 7, respectively.

3

If E is a number field, we let Cl_E denote the class group of E and $h_E = \#Cl_E$ denote the class number.

(a) Let $K = \mathbb{Q}(\sqrt{-59})$ and let L be the splitting field over $\mathbb{Q}$ of $f(T) = T^3 + 2T + 1$. Show that $K \subseteq L$, and show that L/K has degree 3 and is unramified everywhere. Deduce that $h_K > 1$. [You may assume that -28 is a simple root of $T^3 + 2T + 1$ in $\mathbb{F}_{59}$.]

(b) Let M/L be a finite extension of number fields. Assume that L has no real places, and that there is a prime $\mathfrak{p}$ of L which is totally ramified in M (i.e. there is a unique prime $\mathfrak{q}$ in M above $\mathfrak{p}$, and $\mathfrak{p}\mathcal{O}_M = \mathfrak{q}^{[M:L]}$). Show that h_L divides h_M.

(c) Show that there are infinitely many cyclotomic fields $\mathbb{Q}(\zeta_n)$ whose ring of integers is not a principal ideal domain. [You may use results about cyclotomic fields from lectures, provided that you clearly state what you use.]

[Throughout this question, you may use any results on Hilbert class fields, provided you clearly state what you use.]

4

(a) Let L/K be a finite Galois extension of local fields with Galois group $G = Gal(L/K)$. Define the ramification groups $G_s = G_s(L/K)$ of L/K in the lower numbering, and then define the upper numbering of the ramification groups (in both cases for all non-negative real numbers).

Assume now that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and let $f(T) \in \mathcal{O}_K[T]$ be the minimal polynomial of α. Let v_L be the normalised valuation on L. Show that

$$v_L(f'(\alpha)) = \sum_{1 \neq \sigma \in G} v_L(\sigma(\alpha) - \alpha) = \sum_{s \in \mathbb{Z}_{\geqslant 0}} (\#G_s - 1).$$

(b) Let M be the splitting field of $g(T) = T^3 - 3T + 3$ over $\mathbb{Q}_3$. Compute the Galois group and the ramification groups in the lower numbering (for all non-negative integers only) of $M/\mathbb{Q}_3$. [You may use that $\sqrt{-5} \in \mathbb{Q}_3$.]

[In both parts of the question you may use results from lectures on ramification groups and totally ramified extensions, provided that you clearly state what you use.]

5

Let L/K be a finite extension of number fields, and let M/K be the Galois closure of L/K, with Galois group $G = Gal(M/K)$. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be a prime of M lying above $\mathfrak{p}$.

(a) Define the decomposition group $D_{\mathfrak{P}|\mathfrak{p}} \subseteq G$. Show that there is a natural bijection between the primes of L above $\mathfrak{p}$ and the double coset space $H \backslash G / D_{\mathfrak{P}|\mathfrak{p}}$, where $H = Gal(M/L)$.

(b) Show that $\mathfrak{p}$ is totally split in L if and only if it is totally split in M.

END OF PAPER