Attempt no more than THREE questions.

There are FOUR questions in total.

The questions carry equal weight.
1

State and prove the Kummer–Dedekind theorem.
Verify that \((4 + \sqrt{5})\) is a prime of \(\mathbb{Q}(\sqrt{5})\) with residue field \(\mathbb{F}_{11}\), and determine its prime factorisation in \(\mathbb{Z}[\zeta_5]\). Here \(\zeta_5\) denotes a primitive fifth root of unity that satisfies \(\zeta_5 + \zeta_5^{-1} = \frac{-1 + \sqrt{5}}{2}\).

[You may assume that \(\mathbb{Z}[\zeta_5]\) is the ring of integers of \(\mathbb{Q}(\zeta_5)\).]

2

Define the terms decomposition group, inertia subgroup and Frobenius element.

(i) Let \(F/K\) be a Galois extension of number fields and \(\mathfrak{q}\) a prime above \(\mathfrak{p}\). Show that the order of the inertia subgroup at \(\mathfrak{q}\) is equal to the ramification degree of \(\mathfrak{q}\) over \(\mathfrak{p}\).

Suppose that the Galois group of \(F\) over \(K\) is cyclic of order \(l^2\) for some prime \(l\), and let \(L\) denote the unique intermediate field of \(F/K\). Prove that if \(\mathfrak{p}\) ramifies in \(L/K\), then it must be totally ramified in \(F/K\).

(ii) Show that 7 is unramified in \(\mathbb{Q}(\zeta_{25})/\mathbb{Q}\) and determine the corresponding Frobenius element. How many primes are there above 7 in this extension? Justify your answer.

[\(\zeta_{25}\) denotes a primitive 25th root of unity.]

3

(i) State the Main Theorem of Class Field Theory.

(ii) Prove that the ray class field for the modulus (5) of \(\mathbb{Q}\) is \(\mathbb{Q}(\sqrt{5})\).

(iii) Let \(p\) and \(q\) be distinct primes congruent to 1 modulo 4. Show that the Hilbert class field of \(\mathbb{Q}(\sqrt{pq})\) contains \(\mathbb{Q}(\sqrt{p}, \sqrt{q})\) and deduce that the ideal class group of \(\mathbb{Q}(\sqrt{pq})\) has even order.
State and prove Chebotarev’s Density Theorem. You may assume that the $L$-function $L(\rho, s)$ of any 1-dimensional Artin representation $\rho$ has an analytic continuation to $\mathbb{C}$, except for a simple pole at $s = 1$ if $\rho$ is trivial, and that $L(\rho, s)$ is analytic and non-zero at $s = 1$ if $\rho$ is non-trivial.

[Basic properties of $L$-functions, as well as Artin’s or Brauer’s Induction Theorem, may be used without proof. You may also assume that only finitely many primes ramify in any given extension of number fields.]