Problem set 6 – Math 699 – Algebraic number theory

(1) Compute the different of the following number fields: $\mathbf{Q}(\sqrt{-d})$ (d squarefree) and $\mathbf{Q}(\zeta_\ell)$ (ℓ prime).

(2) (a) Let $K = \mathbf{Q}(\theta)$ and let p be a rational prime dividing the degree of $K/\mathbf{Q}$. Suppose the minimal polynomial of θ is Eisenstein at p, show that p is wildly ramified in K.

(b) Let m be cubefree. We know 3 is ramified in $K = \mathbf{Q}(m^{1/3})$. Show that 3 is wildly ramified in K if and only if $m \not\equiv \pm 1 \pmod 9$, i.e. if and only if $\mathrm{ord}_3(\Delta(K)) > 1$.

(c) Show that no other primes can be wildly ramified in $\mathbf{Q}(m^{1/3})$.

(d) Find a cubic field in which 2 is wildly ramified. (I don't have a method for this.)

(3) Let K/F be a Galois extension of number fields with Galois group G. We say that a prime $\mathfrak{p}$ of F is *nonsplit* if there's only one prime $\mathfrak{P}$ dividing $\mathfrak{p}$ (i.e. $g = 1$).

(a) Show that if there is an unramified $\mathfrak{p}$ of F which is nonsplit, then G is cyclic.

(b) Conclude that if G is non-cyclic, then there are only finitely many primes $\mathfrak{p}$ of F that are nonsplit in K/F.

(4) Let K/F be a Galois extension of number fields and let $G := \mathrm{Gal}(K/F)$. Fix an embedding $\iota_\infty : F \hookrightarrow \mathbf{C}$ and let $I_\infty := \{\iota : K \hookrightarrow \mathbf{C} : \iota|_F = \iota_\infty\}$. The group G acts on I_∞ (on the right) by composition: $\iota^\sigma := \iota \circ \sigma$ for all $\iota \in I_\infty, \sigma \in G$.

(a) Show that this action is free and transitive (i.e. all stabilizers are trivial and there is only one orbit). Thus, $G \cong I_\infty$ as G-sets.

(b) An embedding $\iota \in I_\infty$ is called real (resp. *nonreal*) if its image is contained in $\mathbf{R}$ (resp. not contained in $\mathbf{R}$). Show that since K/F is Galois, either all elements of I_∞ are real or they are all nonreal. This is an analogue to what we saw in class about the factorization of prime ideals in Galois extensions.

(c) Find a non-Galois extension K/F of number fields where I_∞ contains both real and nonreal embeddings.

(5) Let K/F be a non-Galois extension of number fields of degree $n \geq 2$, let N/F be its Galois closure, and let $G := \mathrm{Gal}(N/F)$. Let $I := \{\iota : K \hookrightarrow N : \iota|_F = \mathrm{id}\} = \{\iota_1, \ldots, \iota_n\}$ with $\iota_1 \in I$ denoting the embedding given by the inclusion $K \subseteq N$. The group G acts on I (on the left) by composition: $\sigma \cdot \iota := \sigma \circ \iota$.

(a) Show that G acts faithfully and transitively on I (i.e. the intersection of all stabilizers is trivial and there is only one orbit). This induces an embedding $\varphi : G \hookrightarrow S_n$.

(b) Let S_{n-1} denote the subgroup of S_n acting as the permutations of $\{\iota_2, \iota_3, \ldots, \iota_n\}$ (i.e. the stabilizer in S_n of ι_1). Let H be the subgroup of G to which K/F corresponds under the Galois correspondence. Show that $H = \mathrm{Stab}_G(\iota_1) = G \cap \varphi^{-1}(S_{n-1})$. Thus, as G-sets, $I \cong H \backslash G$.

(c) Let $\mathfrak{p}$ be a prime of F, let $S_{\mathfrak{p}}(K)$ (resp. $S_{\mathfrak{p}}(N)$) denote the set of primes of K (resp. N) that divide $\mathfrak{p}$. For $\widetilde{\mathfrak{P}} \in S_{\mathfrak{p}}(N)$, let $G_{\widetilde{\mathfrak{P}}} \leq G$ and $I_{\widetilde{\mathfrak{P}}} \leq G_{\widetilde{\mathfrak{P}}}$ denote its decomposition group and its inertia subgroup, respectively. Then, $G_{\widetilde{\mathfrak{P}}}$ acts on $H \backslash G \cong I$ (on the right) by $(H\sigma)^g = H\sigma g$. Show that there is a bijection between (right) $G_{\widetilde{\mathfrak{P}}}$-orbits of $H \backslash G$ and the set $S_{\mathfrak{p}}(K)$. (Hint: show that the map $H \backslash G / G_{\widetilde{\mathfrak{P}}} \to S_{\mathfrak{p}}(K)$ given by $H\sigma G_{\widetilde{\mathfrak{P}}} \mapsto \sigma\widetilde{\mathfrak{P}} \cap K$ is a well-defined bijection.)

(d) Thus, if $g := \#S_{\mathfrak{p}}(K)$, then g equals the number of $G_{\widetilde{\mathfrak{P}}}$-orbits of $H \backslash G$. For $\mathfrak{P} \in S_{\mathfrak{p}}(K)$, let $\mathfrak{O}$ denote the corresponding $G_{\widetilde{\mathfrak{P}}}$-orbit of $H \backslash G$. Show that $e(\mathfrak{P})$ is the size of the $I_{\widetilde{\mathfrak{P}}}$-orbit of an(y) element of $\mathfrak{O}$. Show that $e(\mathfrak{P})f(\mathfrak{P}) = \#\mathfrak{O}$.

(e) Show that $\mathfrak{p}$ in F is ramified in K if and only if it is ramified in N.

(6) Let K/F be a degree n Galois extension of number fields whose Galois group is a non-abelian simple group (such as A_5 or $\mathrm{GL}_3(\mathbf{F}_2)$). Let $\mathfrak{p}$ be a prime of F.

(a) Can $\mathfrak{p}$ have factorization type $(2^{n/2})$? What types of the form (f^e) are possible?

(b) Can $\mathfrak{p}$ factor as $(\mathfrak{P}_1\mathfrak{P}_2)^e$?

(c) If $\mathrm{Gal}(K/F) = A_5$ and there is a prime $\mathfrak{P}$ of K dividing $\mathfrak{p}$ whose inertial degree is ≥ 6, show that $\mathfrak{p}$ is ramified in K/F.