HOMEWORK 4

DUE WEDNESDAY, NOVEMBER 6, 2019 IN CLASS

Part I: from the textbook

Chapter I, Section 9: **2, 4**

Part II

1. (10 points) Find a prime p and quadratic extensions K and L of $\mathbb{Q}$ illustrating each of the following.

(a) p can be totally ramified in K and L without being totally ramified in KL.

(b) K and L can each contain unique primes lying over p while KL does not.

(c) p can be inert in K and L without being inert in KL.

(d) The residue field extensions of $\mathbb{Z}/p\mathbb{Z}$ can be trivial for K and L without being trivial for KL.

2. (20 points) Let K and L be number fields, L a normal extension of K with Galois group G, and let P be a prime of K. By *intermediate field* we will mean an intermediate field different from K and L.

(a) Prove that if P is inert in L then G is cyclic.

(b) Suppose P is totally ramified in every intermediate field, but not totally ramified in L. Prove that no intermediate fields can exist, hence G is cyclic of prime order.
Hint: inertia field.

(c) Suppose every intermediate field contains a unique prime lying over P but L does not. Prove the same as in part (b).
Hint: decomposition field.

(d) Suppose P is unramified in every intermediate field, but ramified in L. Prove that G has a unique smallest nontrivial subgroup H, and that H is normal in G; use this to show that G has prime power order, H has prime order, and H is contained in the center of G.

(e) Suppose P splits completely in every intermediate field, but not in L. Prove the same as in part (d). Find an example of this over $\mathbb{Q}$.

(f) Suppose P is inert in every intermediate field but not inert in L. Prove that G is cyclic of prime power order.
Hint: Use (a), (c), (d) and something from group theory.

3. (20 points) Let $\zeta = \zeta_m (m \geq 3)$ be a primitive mth root of unity. (One may take $\zeta_m = e^{2\pi i/m}$.) Set $\theta = \zeta + \zeta^{-1}$. Let $K = \mathbb{Q}(\theta)$ and $L = \mathbb{Q}(\zeta)$.

(a) Show that ζ is a root of a polynomial of degree 2 over $\mathbb{Q}(\theta)$.

(b) Show that $K = \mathbb{R} \cap L$ and that L has degree 2 over K.
Hint: $L \supset L \cap \mathbb{R} \supset K$.

(c) Show that K is the fixed field of the automorphism ? of L determined by $\sigma(\zeta) = \zeta^{-1}$.
Hint: σ is just complex conjugation.

(d) Show that $\mathcal{O}_K = \mathbb{R} \cap \mathbb{Z}[\zeta]$.

(e) Let $n = \varphi(m)/2$. Show that

$$1, \zeta, \zeta^{-1}, \zeta^2, \zeta^{-2}, \ldots, \zeta^{n-1}, \zeta^{-(n-1)}, \zeta^n$$

form an integral basis for $\mathbb{Z}[\zeta]$.

(f) Use part (e) to show that

$$1, \zeta, \theta, \theta\zeta, \theta^2, \theta^2\zeta, \ldots, \theta^{n-1}, \theta^{n-1}\zeta$$

is another integral basis for $\mathbb{Z}[\zeta]$.
Hint: Write these in terms of the other basis and look at the resulting matrix.

(g) Show that

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

is an integral basis for $\mathcal{O}_K$. Conclude that $\mathcal{O}_K = \mathbb{Z}[\theta]$.

(h) **[Extra credit]** Suppose m is an odd prime p. Show that $\mathrm{disc}(K) = \pm p^{(p-3)/2}$.