Math 620, Homework 3

1. Let $\zeta = e^{2\pi i/8}$ be a primitive 8th root of unity.
(a) Show that $\sqrt{2} = \zeta + \zeta^{-1}$.
(b) Let p be an odd prime. Show that σ_p (the Galois element that maps ζ to ζ^p) fixes $\sqrt{2}$ if and only if $p \equiv \pm 1 \bmod 8$.
(c) Show that p splits completely in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ if and only if $p \equiv \pm 1 \bmod 8$.
(d) Prove the supplementary law for quadratic reciprocity: $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \bmod 8$.

2. Let L/K be an extension of number fields. Assume that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$. Let $f(X) \in \mathcal{O}_K[X]$ be the minimal polynomial for α. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and let

$$f(X) \equiv h_1(X)^{e_1} \cdots h_g(X)^{e_g} \mod \mathfrak{p}$$

be the factorization of $f(X)$ mod $\mathfrak{p}$ into distinct monic polynomials $h_j(X)$ that are irreducible mod $\mathfrak{p}$. Let $k = \mathcal{O}_K/\mathfrak{p}$. For a fixed j, let P_j be the kernel of the natural map

$$\phi_j : \mathcal{O}_K[\alpha] \simeq \mathcal{O}_K[X]/(f(X)) \to k[X]/(h_j(X))$$

(where h_j is regarded as a polynomial mod $\mathfrak{p}$).
(a) Show that P_j is a prime ideal of $\mathcal{O}_L$ and $[\mathcal{O}_L/P_j : k] = \deg h_j$.
(b) Show that the ideal $(\mathfrak{p}, h_j(\alpha))$ of $\mathcal{O}_L$ is contained in P_j.
(c) Show that $(\mathfrak{p}, h_j(\alpha)) = P_j$. (*Hint:* Suppose $a(\alpha) \in P_j$. Then $a(X) \equiv h_j(X)b(X) \mod \mathfrak{p}$ for some polynomial $b(X)$.)
(d) Show that $h_1(\alpha)^{e_1} h_2(\alpha)^{e_2} \cdots h_g(\alpha)^{e_g} \in \mathfrak{p}\mathcal{O}_L$.
(e) Show that $P_j^{e_j} \subseteq (\mathfrak{p}, h_j(\alpha)^{e_j})$.
(f) Show that

$$P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g} \subseteq (\mathfrak{p},\, h_1(\alpha)^{e_1} h2(\alpha)^{e_2} \cdots h_g(\alpha)^{e_g}) \subseteq \mathfrak{p}\mathcal{O}_L.$$

(g) The result of (f) says that $\mathfrak{p}\mathcal{O}_L$ divides $P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. We also know that $f_j = [\mathcal{O}_L/P_j : k] = \deg h_j$ for each j, by part (a). Use the fact that $e_1 f_1 + \cdots + e_g f_g = \deg f$ to show that no P_j can divide $\mathfrak{p}\mathcal{O}_L$ with an exponent higher than e_j, and that no other primes P of $\mathcal{O}_L$ can occur in the factorization of $\mathfrak{p}\mathcal{O}_L$. (*Note:* e_j and f_j are obtained from the polynomial factorization; this shows that they are the usual e_j and f_j for the prime ideal factorization.)
(h) Technicality that might have been overlooked: Show that if $i \neq j$ then $P_i \neq P_j$. (*Hint:* There is a $k[X]$-linear combination of $h_i(X)$ and $h_j(X)$ that is 1 mod $\mathfrak{p}$.)

3. (a) Let $\zeta_{\mathbb{Q}(i)}(s)$ be the zeta function for $\mathbb{Q}(i)$ and let $L(s, \chi)$ be the Dirichlet L-series for the character $\chi : (Z/4\mathbb{Z})^\times \to \{\pm 1\}$, where $\chi(1) = 1$ and $\chi(3) = -1$. We will show in class that $\zeta_{\mathbb{Q}(i)}(s) = \zeta(s)L(s, \chi)$ by comparing Euler factors at each prime, but we will not treat the factor for 2. Complete the proof by showing that the Euler factors at 2 also agree.

(b) Use the fact that the series for $L(1, \chi)$ is alternating and has decreasing terms to show that $2/3 < L(1, \chi) < 1$.
(d) The class number formula tells us that $L(1, \chi) = \pi h/4$, where h is the class number. Use the fact that h is an integer to deduce that $h = 1$ and $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \pi/4$.